ประกาศ

จากการแจ้งเตือนให้หน่วยงานเฝ้าระวังการโจมตีของกลุ่ม Hacker ที่ใช้ ransomware ในการโจมตี เพื่อเป็นการยกระดับการเฝ้าระวังและป้องกัน หน่วยงานควรดำเนินการเฝ้าระวัง ดังนี้

- ให้ "ทบทวน" และ พิจารณา "ปิด" Service Port ทั้ง Internet และ Intranet ทุกช่องทาง ดังนี้
  - Service Port ที่ไม่ได้มีการใช้งานแล้ว
  - Service Port ที่ไม่จำเป็นต่อการปฏิบัติงาน
  - Service Port ที่ไม่มีความปลอดภัย
  - Service Port ที่ไม่มีความเหมาะสมหรือไม่มีมาตรฐาน
- ปิดกั้น IP จากต่างประเทศ หรือในประเทศ หากพบว่ามีพฤติกรรมที่น่าสงสัยโดยทันที
- ติดตั้ง EDR หรือ Antivirus ที่เครื่อง Server และ Client
- เฝ้าระวังและติดตามพฤติกรรมที่ผิดปกติในทุกระบบอย่างน้อยทุก 4 ชั่วโมง
- จัดเตรียมเวรที่สามารถเข้าถึงห้อง Server ได้ ในกรณีที่เกิดเหตุการณ์ฉุกเฉินทาง Cyber ให้ตัดออกจากเครือข่ายโดยทันที
- ทบทวนแผนการ Backup และจัดหา External HDD เพื่อการดำเนินการทำ Backup แบบ Incremental โดยแบ่งแต่ละวันอย่างน้อย 7 วัน (7 วัน 7 ชุด) และต้องทำ Full Backup แบบ Offsite Backup อย่างสม่ำเสมอ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CERT)
เว็บไซต์ข่าวสาร : cyber.moph.go.th
เว็บไซต์แจ้งเหตุ : health-cirt.moph.go.th

ประกาศ

- ปิดกั้น Indicator of Compromise (IOCs) ที่เกี่ยวข้องกับกลุ่ม Hacker บน Firewall ดังนี้

IP/Domain

- 185.229.191[.]41
- 172.67.129[.]176
- 62.233.50[.]25
- 104.21.1[.]180
- 192.229.221[.]95
- 101.97.36[.]61
- assist.zoho[.]eu
- eu1-dms.zoho[.]eu
- 168.100.9[.]137
- 185.20.209[.]127
- 185.230.212[.]83
- 206.188.197[.]22
- 54.84.248[.]205
- 141.98.9[.]137
- fixme[.]it
- unattended.techinline[.]net

ใส่ [.] เพื่อไม่ให้เป็น Hyperlink ป้องกันไม่ให้คลิกแล้วไปยัง IP หรือโดเมนนั้นๆ โดยไม่ตั้งใจ

ประกาศ

Filename/Hash:

- 7c6a3c8c11ec2b82adc8f89727138d0b
- 61df82f02e9e91508a7a45705fe93c4e
- 858f391aaa0f538ee5a3cbb9bbb098a8
- 74705552a7bf4e91b135bd6a3fb1b8f4
- 89f1c02231f3c310d90373a33e53db17
- 6e14deb9eea0058a129bab0ccff076ac
- 5eab14e3a707dd56223632fec5dcc9b5
- 3ce9d145f7e596bfdadd1d809cb78347
- 359debfe43f7fc05f20b601e7af33590
- 96c2fb8960dea379939d34622197ccc7
- 7375e4cb311fae1008cb6051e7f59953
- 5a9bb2310c95592a60c12f8901c34e48
- b12a4c056c94cfdb486a2cae59ebf3a3
- b964a0f25fb5789307167cf6bf8934e2
- 7bf3dcd533d3a6ee7b8d32e71c553fbe
- 841a77350d73eed29eb93b1e17bd4768
- 4bde527aaf353205265cb073387c7a4e
- 461d852b230a5b9710a5a1e01c6b7194
- f9cb9f6f6db424b7ad937ccdec446e39
- d0c312c9ffdf8ae9f4095f21251d8751
- e20bbba66becc7268a6f056e82fe0fc1
- 3996d8e587a72956bb288dd4bf6b7b6f
- 2ae9d4ad3e1ad7da6ee9d30594869767

ประกาศ

Filename/Hash:

- 10e19887bdad9934fbf17cbb938804cb
- 78618875697063 9e7ec7178bca995fab
- d587668fb815cffe1584e279161b7f38
- 082ad5313ac6b6468059af049e6101a5
- 129e219b86297cfd1586b61da6fcdd58
- cbf0b4c15db4303cd4806d848a20fcc1
- 37d88f8fdae6a417cae0d43248aa6c73
- 40a5b856c8125cf9f68d827d86e58db9
- aa2a4880c0bdaebf2e3db15b4ad38ba4
- 49f50c9c471a802f9d0b9bc12c40cf47
- 5335056da9b7fd054fcf00588c1421b5
- 6d4ecdf5846e953532ab7bfdfba5fa2e
- 9b354fdb01a93680b8d56225ed2035df
- 8b99992980ed3ca45aa270a7d679c5f7
- 6d6b0290f90de6d15e36d01828c30f53
- 2281533d0a450740c8c96577fd76a2fb
- 9adb6bf8417eae9f52fccd3edb7f4f04
- aa2008219625871ffa894082470c4fc6
- 6943dc6b660d6ac86aef8733bcd7f9cc
- 8e051fef7f85037e5ca6dc7bb7edf7f8
- 6fac12e9d0416388fb21d0d3890781ca
- 7605952735e062ab0886708bd6b662c2
- 4bec7d13868da4793538c81f138db44e

ประกาศ

Filename/Hash:

- c3cb3ee3e75edf3f2faec2a116308ce4
- 8b99992980ed3ca45aa270a7d679c5f7
- 2281533d0a450740c8c96577fd76a2fb
- d63f39951a9c19987d02d7f3109b24fd
- aa2008219625871ffa894082470c4fc6
- 5335056da9b7fd054fcf00588c1421b5
- 6943dc6b660d6ac86aef8733bcd7f9cc
- 9adb6bf8417eae9f52fccd3edb7f4f04
- 7605952735e062ab0886708bd6b662c2
- 6d6b0290f90de6d15e36d01828c30f53
- 6fac12e9d0416388fb21d0d3890781ca
- 6d4ecdf5846e953532ab7bfdfba5fa2e
- 84b92859d81dc10ada167e5008403166
- aa5ab0bea11c8d0088e6941f87477201
- 59c50901dd498783918508ffb751bfc5
- 7e3b62034dc1142a33bf560e537ebc35

*** หากมีการอัพเดท Health-CERT จะทำการแจ้ง IOCs เพื่อให้หน่วยงานดำเนินการบล็อคเพิ่มเติมต่อไป**