เตือนภัย global cyberattack เรียกค่าไถ่ระลอกใหม่ จาก ransomware อีกตัว ชื่อ Petwrap (บางค่ายตั้งชื่อว่า NotPetya เพราะมีลักษณะคล้าย ransomware ตัวเก่า ชื่อ Petya แต่ดูเหมือนจะแตกต่างกัน)

กลไกการโจมตี ใช้ช่องโหว่ของ Windows อันเดียวกันกับ WannaCry

หากติด ransomware แล้ว หน้าจอจะขึ้นสีน้ำเงิน และเมื่อ restart จะ lock เข้ารหัสข้อมูลและขึ้นข้อความสีแดงบนพื้นสีดำว่าติดเชื้อแล้ว

<u>วิธีป้องกันก่อนติดเชื้อ</u>

1. อุด patch ของ Windows โดยเฉพาะช่องโหว่เดียวกับ WannaCry คือ MS17-10

เครื่อง Windows เก่าๆ เช่น Windows XP Microsoft ก็ออก patch ช่องโหว่นี้แล้วเช่นกัน จึงควร patch ด้วย

2. หาก patch ไม่ได้ ควรปิด port SMBv1 หากไม่จำเป็นต้องใช้ (เครื่องภายในองค์กรควรปรึกษา IT Admin ก่อน)

3. Backup ข้อมูลสำคัญไว้นอกเครื่องเป็นประจำ

4. มีพฤติกรรมระวังในการเปิดลิงก์หรือไฟล์แนบของอีเมลอยู่เสมอ

<u>วิธีแก้ไขเบื้องต้นเมื่อติด NotPetya แล้ว</u>

1. เมื่อขึ้นหน้าจอสีน้ำเงิน แสดงว่าติดแล้ว อย่าเพิ่ง restart เครื่อง เพราะ ransomware จะเริ่มทำการเข้ารหัสข้อมูล

2. ให้ Shut Down เครื่อง, ถอดสาย LAN (ถ้ามี) แต่อย่า start เครื่องกลับมา

3. แจ้ง IT Admin ของหน่วยงานเพื่อ backup ข้อมูลจาก hard drive โดยไม่เปิดเครื่อง

4. พิจารณาปรึกษา ThaiCERT (หน่วยงานดูแลและเชี่ยวชาญเรื่อง cybersecurity ของประเทศไทย) โทร. 0-2123-1212

<u>แหล่งข้อมูล</u>

https://www.thaicert.or.th/alerts/user/2017/al2017us002.html

http://www.bbc.com/news/technology-40416611

https://motherboard.vice.com/en_us/article/qv4gx5/a-ransomware-outbreak-is-infecting-computers-across-the-world-right-now

นพ.นวนรรน ธีระอัมพรพันธุ์

"หมอไอที"

www.facebook.com/InformaticsRound