คุณสมบัติของมัลแวร์เรียกค่าไถ่ที่ชื่อ WannaCry และแนวทางการใช้งานอย่างปลอดภัย

ข้อมูลรายละเอียด	คำอธิบาย
ชื่อโปรแกรมประสงค์ร้าย	WannaCry
ประเภท	มัลแวร์
ผลกระทบกับระบบ	Windows sever และ ระบบปฏิบัติการ Windows
แหล่งที่มา	- แฝงมาในรูปแบบเอกสารแนบทางอีเมล์ - แฝงมาในรูปแบบของโฆษณา ไม่ว่าจะเป็นโฆษณาที่ฝังมากับซอฟต์แวร์หรือตามหน้าเว็บไซต์ต่าง - การเข้าเยี่ยมชมหน้าเว็บที่ถูกผู้ไม่หวังดีเข้ามาควบคุม แล้วใช้ประโยชน์จากข้อบกพร่องหรือช่องโหว่ด้านความปลอดภัยในเบราว์เซอร์ แอพลิเคชั่น หรือระบบปฏิบัติการ ที่พบมากที่สุดก็คือใน FLASH
อาการหลังจากติดไวรัส	- จะทำการเข้ารหัสหรือล็อคไฟล์ เช่น ไฟล์เอกสาร รูปภาพ วีดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใดๆ ได้เลยหากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งถูกเข้ารหัสจะต้องใช้คีย์ในการปลดล็อคเพื่อกู้ข้อมูลคืนมา ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ “เรียกค่าไถ่” ที่ปรากฏ
คำแนะนำ	- Backup ข้อมูลอย่างสม่ำเสมอ และหากเป็นไปได้ให้เก็บข้อมูลที่ถูก Backup ไว้ในอุปกรณ์ที่ปกติไม่ได้เชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายอื่นๆ - ติดตั้ง/อัปเดตโปรแกรมป้องกันไวรัส รวมถึงอัปเดตโปรแกรมอื่นๆ โดยเฉพาะโปรแกรมที่มีช่องโหว่ เช่น Java และ Adobe Reader และอัปเดตระบบปฏิบัติการอย่างสม่ำเสมอ - ไม่คลิกลิงค์หรือเปิดไฟล์ที่มาพร้อมกับอีเมล์ที่น่าสงสัย หากไม่มั่นใจว่าเป็นที่น่าเชื่อถือหรือไม่ ให้สอบถามจากผู้ส่งโดยตรง - หากมีการแชร์ข้อมูลร่วมกันผ่านระบบเครือข่าย ให้ตรวจสอบสิทธิ์ในการเข้าถึงข้อมูลแต่ละส่วน และกำหนดสิทธิ์ให้ผู้ใช้มีสิทธิ์อ่านหรือแก้ไขเฉพาะไฟล์ที่มีความจำเป็นต้องใช้สิทธิ์เหล่านั้น - ตั้งค่า Policy ของระบบปฏิบัติการ เพื่อป้องกันไม่ให้มัลแวร์สามารถ ทำงานตาม Directory หรือ Path ที่ระบุได้
แหล่งข้อมูลเพิ่มเติม	https://www.it.chula.ac.th/th/node/3351 https://www.thaicert.or.th/papers/technical/2013/pa2013te011.h

เวอร์ชั่น 02
13 พ.ค.2560 เวลา 19.00 น.

กระทรวง DE เตือนภัย

มัลแวร์เรียกค่าไถ่ WannaCry ระบาดผ่านช่องโหว่ของวินโดว์

WannaCry ระบาดผ่านช่องโหว่ของ Microsoft Windows (SMB Remote Execution Vulnerability)
ที่ไม่ Update หรือที่ไม่ปรับระบบ (บางครั้งเรียกว่า ไม่แพช (Patch) ระบบ ให้เป็นเวอร์ชั่นล่าสุด)

WannaCry ทำงานและร้ายแรงอย่างไร

เมื่อคอมพิวเตอร์ติด WannaCry โปรแกรมมัลแวร์นี้ จะเอาข้อมูลในเครื่องของเหยื่อ
ไปเข้ารหัสลับไว้ ทำให้ผู้ตกเป็นเหยื่อจะเข้าไปอ่านหรือใช้ข้อมูลในเครื่องตนไม่ได้

Hacker ที่สร้างมัลแวร์ WannaCry ต้องการอะไร

ต้องการเรียกค่าไถ่ โดยให้จ่ายค่าไถ่เป็น Bit Coin

1

มัลแวร์ถูกดาวน์โหลดและติดตั้ง
ลงในเครื่องของเหยื่อ และขู่เรียกค่าไถ่

2

ค่าไถ่ถูกเรียกเป็น Bit Coin
300 ดอลลาร์ พร้อมบอกวิธีการ
จ่ายค่าไถ่ และเริ่มนับเวลาถอยหลัง

3

หน้าจอของเครื่องคอมพิวเตอร์
ที่ตกเป็นเหยื่อ

ผลกระทบที่เกิดขึ้นแล้ว

เครื่องคอมพิวเตอร์มากกว่า 100,000 เครื่องติด WannaCry ทั่วโลก
ในอังกฤษ โรงพยาบาลมากกว่า 10 แห่ง ต้องระงับการให้บริการบางประเภท
ในประเทศไทยพบการติดมัลแวร์บ้างแล้ว

ควรสำเนาข้อมูลสำคัญใน External Hardisk อย่างสม่ำเสมอ

แนวทางการป้องการการติด Ransomware

1. ไม่เปิดเอกสารแนบอีเมลโดยไม่จำเป็น
ควรตรวจสอบที่มาของไฟล์ที่แนบมา
ให้แน่ใจ ก่อนเปิดอ่าน

2. ปรับปรุงระบบปฏิบัติการ
หรือ OS ของระบบ Windows
ให้เป็นเวอร์ชั่นล่าสุด

แนวทางการป้องกันการแพร่ระบาด (หากพบการติดแล้ว)

สำหรับผู้ใช้งานทั่วไป

ให้ปิดเครื่องและแจ้งผู้ดูแลระบบ
หรือติดต่อ OCC
Online Complaint Center
โทร. 1212

สำหรับผู้ดูแลระบบ (สามารถ ติดต่อThaiCERT ETDA (24 ชม.) โทร. 02 123 1212)

ปิดบริการ SMBv1
ที่ Windows servers

ปิดการเข้าถึงพอร์ต
TCP/UDP 135-139
และ TCP 445
ที่อุปกรณ์ Firewall

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ (ThaiCERT)
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ThaiCERT ETDA

ThaiCERT ThaiCERT thaicert.or.th

แนวปฏิบัติในการป้องกันผลกระทบจาก

Ransomware WannaCry สำหรับผู้ดูแลระบบ

เวอร์ชั่น 02
15 พ.ค.2560
เวลา 8.30 น.

1. ปรับปรุงระบบปฏิบัติการของคอมพิวเตอร์ในหน่วยงานให้เป็นปัจจุบัน

2. ปิดบริการ SMBv1 ของคอมพิวเตอร์ในหน่วยงาน

3. ปิดกันการสื่อสารผ่านพอร์ต SMB (TCP 137, 139, 445 และ UDP 137, 138) เข้ามายังหน่วยงาน เพื่อป้องกันการติด Ransomware ผ่านช่องโหว่ของระบบปฏิบัติการ

4. ปิดกั้นการสื่อสารจากภายในหน่วยงานออกไปยังเครือข่าย TOR เนื่องจาก Ransomware อาจจะมีการสื่อสารกับคอมพิวเตอร์ควบคุมผ่านเครือข่าย TOR

5. ปิดกั้นการสื่อสารจากภายในหน่วยงานไปยังเครื่อง Command and Control เพื่อชะลอการทำงานของ Ransomware (ตรวจสอบรายการของเครื่อง Command and Control ได้ที่ https://www.thaicert.or.th

6. สำเนาข้อมูลไปยังที่สำรองข้อมูลแบบออฟไลน์หรือแบบ Cloud และสำรองเป็นเวอร์ชัน เพื่อป้องกันการเข้ารหัสข้อมูลที่สำรองไว้ และป้องกันการสำเนาข้อมูลที่ถูกเข้ารหัสแล้วทับข้อมูลที่สำรองไว้

7. ใช้ระบบกรองอีเมลเพื่อคัดอีเมลที่มีไฟล์แนบที่อาจเป็น Ransomware ก่อนที่ผู้ใช้งานจะเปิดไฟล์แนบดังกล่าว

8. ปิดกั้นการเข้าถึงเว็บไซต์ที่อาจจะเป็นแหล่งการแพร่ Ransomware

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ (ThaiCERT)
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ThaiCERT
ETDA

ThaiCERT ThaiCERT thaicert.or.th