17 พ.ค. 2560

RANSOMWARE
ระบาดหนักทั่วโลก

InterRisk Asia (Thailand) Co., Ltd.

ระวัง!!! WannaCry Malware กำลังระบาด

เมื่อวันที่ 12 พฤษภาคม 2560 มีการแพร่ระบาดของมัลแวร์เรียกค่าไถ่ชื่อ WannaCry ไปทั่วโลก ซึ่งส่งผลกระทบต่อธุรกิจและสถาบันต่างๆ เช่น
ระบบการขนส่งในประเทศสหรัฐอเมริกา
ระบบรถไฟในเยอรมนี
บริษัทโทรคมนาคมของสเปนมหาวิทยาลัยในเอเชีย
กระทรวงมหาดไทยของรัสเซีย
ผู้ผลิตรถยนต์ของฝรั่งเศสและอังกฤษ
และระบบโรงพยาบาลของอังกฤษ
มัลแวร์ดังกล่าวมีจุดประสงค์หลักเพื่อเข้ารหัสลับข้อมูลในคอมพิวเตอร์เพื่อเรียกค่าไถ่
หากไม่จ่ายเงินตามที่เรียก จะไม่สามารถเปิดไฟล์ได้
จึงถูกเรียกว่า ransomware

> *วิกฤตนี้ยังไม่สิ้นสุด ... เตรียมระบบความปลอดภัยให้พร้อมกับการโจมตีอีกครั้ง*
>
> **- @MALWARETECHBLOG**

มัลแวร์นี้สามารถแพร่กระจายตัวเองจากคอมพิวเตอร์หนึ่งไปยังคอมพิวเตอร์เครื่องอื่นๆในเครือข่ายได้อย่างง่ายดาย WannaCry ransomware ใช้ช่องโหว่ “SMB (Server Message Block)” Remote Execution Vulnerability ของระบบความปลอดภัย Microsoft Window ผู้ใช้งานที่ไม่อัปเดตระบบของ Windows มีความเสี่ยงที่จะติดมัลแวร์นี้

ในช่วงเดือนเมษายน 2560
มีการแพร่กระจายมัลแวร์สู่สาธารณะ ถึงแม้ทาง Microsoft
จะเผยแพร่ข้อมูลการอัปเดตแก้ไขช่องโหว่ดังกล่าวไปตั้งแต่วันที่ 14 มีนาคม 2560 แล้ว
แต่ก็ยังพบว่าปัจจุบันมีคอมพิวเตอร์ที่ยังไม่ได้อัปเดตแพตช์ดังกล่าวและถูกโจมตีจากมัลแวร์นี้มากกว่า 230,000 เครื่อง ใน 150 ประเทศ

ในประเทศไทยพบว่ามีผู้ติดมัลแวร์ตัวนี้อยู่บางส่วน
ตัวอย่างล่าสุดคือระบบของสำนักงานตำรวจแห่งชาติมีปัญหาเกิดขึ้นกับป้ายดิจิทัลบนถนนวิทยุในวันที่ 14 พ.ค ที่ผ่านมา สำนักข่าวรอยเตอร์สกล่าวว่า เมื่อเวลา 21.00 น. ตามเวลาประเทศไทย
แฮกเกอร์ได้รับเงินจำนวน 55,165
เหรียญสหรัฐหรือเกือบ 2 ล้านบาทจาก 209 รายแล้ว

ระบบที่ถูกโจมตีโดยมัลแวร์นี้ มีตั้งแต่ Windows XP Windows Server 2003 ไปจนถึง Windows 10 และ Windows Server 2016 ซึ่งทาง Microsoft ไม่ได้ออกอัปเดตแก้ไขช่องโหว่นี้ให้กับ Windows XP และ Windows Server 2003 เนื่องจากสิ้นสุดระยะเวลาสนับสนุนไปแล้ว อย่างไรก็ตาม เนื่องจากปัจจุบันยังมีเครื่องคอมพิวเตอร์ที่ใช้งานสองระบบปฏิบัติการดังกล่าวและยังเชื่อมต่อกับอินเทอร์เน็ตอยู่ จึงทำให้ถูกโจมตีได้ Microsoft จึงออกอัปเดตฉุกเฉินมาเพื่อแก้ไขปัญหานี้ โดยผู้ใช้สามารถดาวน์โหลดอัปเดตดังกล่าวได้จากเว็บไซต์ของ Microsoft

ขอแนะนำในการป้องกัน:

1.อัปเดตแอนติไวรัสและอัปเดตฐานข้อมูลอย่างสม่ำเสมอ
2.สำรองข้อมูลบนคอมพิวเตอร์อย่างสม่ำเสมอ และเก็บข้อมูลที่ทำการสำรองไว้ในอุปกรณ์ที่ไม่มีการเชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายอื่นๆ
3.การอัปเดตวินโดวส์เพื่ออุดช่องโหว่
4.ปิดโปรโตคอล Server Message Block (SMB)
5.ผู้ใช้ควรตระหนักถึงความเสี่ยงของการเปิดไฟล์แนบในอีเมลที่น่าสงสัย
6.เปิด smart screen (Internet Explorer) ซึ่งช่วยเตือนภัยต่างๆ เช่นเว็บไซต์มัลแวร์และฟิชชิ่งจากการดาวน์โหลด
7.เปิด pop-up blocker บนเว็บเบราเซอร์ของคุณ

มัลแวร์เช่น ransomware มีการปรับปรุงเวอร์ชั่นใหม่ๆตลอดเวลา ซึ่งผู้ใช้คอมพิวเตอร์ควรมีการปรับระบบความปลอดภัยให้เป็นเวอร์ชันล่าสุด เช่นโปรแกรม antivirus และเก็บข้อมูลที่สำคัญไว้นอกระบบ นอกจากนี้ทางกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้มอบหมายให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ (ThaiCERT) และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ หรือ ETDA ดำเนินการแจ้งเตือนและให้คำแนะนำแก่ผู้ใช้คอมพิวเตอร์ทั่วไปหรือผู้ดูแลระบบคอมพิวเตอร์ของหน่วยงานต่างๆหากตกเป็นเหยื่อ

REFERENCES

https://www.thaicert.or.th/alerts/user/2017/al2017us001.html
http://www.sciencealert.com/experts-are-warning-the-global-wannacry-ransomware-hack-isn-t-over
http://www.npr.org/sections/thetwo-way/2017/05/14/528355526/repercussions-continue-from-global-ransomware-attack
https://www.it24hrs.com/2017/wannacry-ransomware-malware-effect/
https://www.blognone.com/node/92410
http://www.bangkokpost.com/news/general/1250106/cyber-worm-slows-hobbles-chinese-police-schools
http://fingfx.thomsonreuters.com/gfx/rngs/CYBER-ATTACK/010041552FY/index.html
http://www.reuters.com/article/us-cyber-attack-idUSKCN18B0AC
http://www.aljazeera.com/news/2017/05/ransomware-avoid-170513041345145.html