WannaCry บทความโดย G-Able Security Consulting Team

WannaCry บทความโดย G-Able Security Consulting Team

หากเราพูดถึงเรื่องของไวรัส (Virus) หรือมัลแวร์ (Malware) ในช่วงเวลานี้คงจะต้องพูดถึง Ransomware ตัวหนึ่งที่ชื่อ WannaCry หรือ WannaCrypt เพราะเป็น Ransomware ที่ทำให้ทุกคนในโลกได้ตระหนักถึงภัยร้ายของ Malware อีกชนิดที่ไม่เพียงแต่สร้างความเสียหายให้กับระบบคอมพิวเตอร์และเน็ตเวิร์ค แต่มีลักษณะของการโจรกรรมเรียกค่าไถ่ของไฟล์ด้วยการเข้ารหัสไฟล์ในเครื่องคอมพิวเตอร์ (Encryption) จนระบบปฏิบัติการหรือซอฟต์แวร์ที่อยู่ในเครื่องคอมพิวเตอร์เหล่านั้นไม่สามารถทำงานต่อได้ จากนั้นจะแสดงข้อความเพื่อบอกวิธีการให้จ่ายเงินในรูปแบบของ Bitcoin ซึ่งเป็นการโอนผ่านระบบอินเตอร์เน็ตที่ง่ายและไม่สามารถตรวจสอบปลายทางได้ให้กับผู้สร้างมัลแวร์ตัวนี้ ซึ่งก็มีหลายองค์กรหรือหลายบริษัทจำเป็นต้องจ่ายเงินให้เพื่อแลกกับคีย์ (Key) ในการใช้มาถอดรหัสของระบบไฟล์บนเครื่องคอมพิวเตอร์เพื่อให้สามารถทำงานต่อได้โดยเฉพาะกับเซิร์ฟเวอร์ที่ให้บริการในงานทางธุรกิจและส่งผลกระทบต่องานหลักของธุรกิจนั้น

ที่มา: https://devcentral.f5.com/articles/security-trends-in-2016-the-problem-of-ransomware-24933

ในความเป็นจริงแล้วมัลแวร์ประเภท Ransomware ได้เกิดขึ้นมานานแล้ว เพียงแต่ความร้ายแรงยังอยู่ในวงจำกัดที่สามารถป้องกันและยับยั้งการทำงานได้ แต่หากย้อนกลับไปเมื่อเดือนสิงหาคม 2559 ได้มีกลุ่มแฮกเกอร์ที่ชื่อว่า “The Shadow Broker” สามารถแฮกเข้าไปใช้เครื่องมือระดับสูงที่ใช้ในการค้นหาช่องโหว่ของซอฟต์แวร์หรือระบบปฏิบัติการจาก NSA ของสหรัฐ และเรียกร้องเงินจำนวน 1 ล้านเหรียญสหรัฐ แต่ไม่มีหน่วยงานไหนยอมจ่าย จึงได้ทำการปล่อยเครื่องมือและข้อมูลช่องโหว่ที่ค้นหาได้ออกสู่สาธรณะในช่วงเมษายน 2560

ข้อมูลช่องโหว่นี้เองเป็นจุดกำเนิดที่ทำให้มีผู้พัฒนา Ransomware ที่ชื่อ WannaCry ออกมาโดยใช้ข้อมูลช่องโหว่ของ Windows ที่เรียกว่า EternalBlue ซึ่งจะใช้การเข้าถึง Protocal และ Services ของ SMB (Simple Message Block) Version 1 หรืออาจเรียกอีกอย่างหนึ่งว่า CIFS (Common Internet File System) ที่ใช้ในระบบการแชร์ไฟล์ (File Sharing), ปริ้นท์เตอร์ (Printer) และซีเรียลพอร์ท (Serial Port) ของระบบปฏิบัติการ Windows ถึงแม้ว่าทาง Microsoft จะได้มีการออกแพตช์ (Patch) ที่ใช้ในการแก้ไขช่องโหว่นี้มาตั้งแต่มีนาคม 2560 แล้วก็ตาม แต่เครื่องคอมพิวเตอร์หลายเครื่องก็ไม่ได้มีการติดตั้งแพตช์นี้เอาไว้

การทำงานของ WannaCry จะทำการสแกนค้นหาบนเครื่องที่อยู่ในระบบเน็ตเวิร์คที่มีช่องโหว่ข้างต้น ซึ่งเมื่อเจอก็

จะทำการสำเนาตัวเองไปยังเครื่องเหล่านั้น และทำการเข้ารหัสไฟล์สำคัญบนเครื่องตัวเองเช่น .docx, .pptx, .mpeg, .zip, .backup แล้วแสดงข้อความเรียกค่าไถ่เป็นเงิน $300 เหรียญสหรัฐทาง Bitcoin

ที่มา: https://thehackernews.com/2017/05/wannacry-ransomware-cyber-attack.html

การทำงานของมัลแวร์ WannaCry เริ่มพบครั้งแรกเมื่อวันที่ 12 พฤษภาคม ที่ผ่านมา ภายใต้ชื่อ Wcry/ WanaCrypt0r/ WannaCry/ WanaCypt0r/ Wanacryptor และแพร่กระจายอย่างรวดเร็ว คาดว่ามีคอมพิวเตอร์ที่ติดมัลแวร์นี้มากกว่า 100,000 เครื่องทั่วโลกในระยะเวลาไม่ถึง 1 วัน จนกระทั่งมีผู้พบการหยุดการแพร่กระจายชั่วคราว มีหน่วยงานที่เป็นที่รู้จักซึ่งได้รับผลกระทบจากมัลแวร์ตัวนี้ หนึ่งในนั้นคือ NHS (Nation Health Service) ซึ่งดูแลระบบประกันสุขภาพของประชาชนในอังกฤษ ได้ถูก WannaCry โจมตีและเข้ารหัสข้อมูล จนคนไข้จำนวนมากไม่สามารถรับการผ่าตัดได้ในวันนั้น จนทำให้ NHS ต้องยอมจ่ายค่าไถ่เพื่อกู้ข้อมูลที่สำคัญกลับคืนมา

ถึงแม้ว่าจะมีการค้นพบวิธีการหยุด WannaCry ด้วยการใช้ “Kill Switch” ฟังก์ชั่น ที่ซ่อนอยู่ในมัลแวร์ตัวนี้เพื่อตรวจค้นหา URL ที่ชื่อ “iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com” ในอินเตอร์เน็ต ซึ่งเมื่อเจอก็จะหยุดการทำงานของมัลแวร์ได้แล้ว แต่ก็ยังจะมีผู้พัฒนามัลแวร์ในลักษณะนี้ต่อไปและอาจจะไม่ได้ใส่ Kill Switch เพื่อหยุดมัลแวร์นั้นก็เป็นได้

เมื่อเราได้ทราบถึงวิธีการทำงานของมัลแวร์ในลักษณะนี้แล้วก็ทำให้เราสามารถหาวิธีการป้องกันการโจมตีจากมัลแวร์เหล่านี้ได้ในอนาคต โดยวิธีการที่จะช่วยให้ปลอดภัยจากการคุกคามนี้ก็คือ

- เครื่องคอมพิวเตอร์ส่วนบุคคลควรหมั่นตรวจสอบการอัปเดตแพตช์ (Patch) ทั้งส่วนของระบบปฏิบัติการ (OS) และโปรแกรมที่ใช้ภายในเครื่อง สำหรับผู้บริหารระบบไอทีขององค์กรควรติดตั้งระบบจัดการแพตช์ (Patch Management) เพื่อให้เครื่องแม่ข่ายและเครื่องของผู้ใช้ได้มีการติดตั้งแพตช์ให้ทันสมัยอยู่เสมอเพื่อลดความเสี่ยงจากการถูกโจมตีทางช่องโหว่ของซอฟต์แวร์เหล่านั้น
- ทำการสำรองข้อมูลอย่างสม่ำเสมอทั้งส่วนของระบบปฏิบัติการ ซอฟต์แวร์ และข้อมูลของผู้ใช้ เพื่อเพิ่มโอกาสในการกู้คือข้อมูลเมื่อเกิดความเสียหายจากมัลแวร์
- ตัดการเชื่อมต่อระบบเน็ตเวิร์คของเครื่องที่ติดมัลแวร์นั้นทันทีเมื่อตรวจพบ และตรวจสอบเครื่องอื่นในระบบเน็ตเวิร์คที่เหลือ
- ติดตั้งซอฟต์แวร์ป้องกันไวรัสและหมั่นอัพเดตฐานข้อมูลไวรัสให้ทันสมัยอยู่เสมอเพื่อป้องกันไวรัสหรือมัลแวร์ที่จะเกิดขึ้นในอนาคต
- ผู้ดูแลระบบเน็ตเวิร์คควรติดตั้งระบบติดตามและตรวจสอบพฤติกรรมของการใช้งานระบบเน็ตเวิร์คเพื่อให้สามารถสังเกตพฤติกรรมของการใช้งานที่น่าจะเกิดจากการแพร่กระจายของมัลแวร์ได้
- หลีกเลี่ยงการใช้ซอฟต์แวร์ที่ไม่ถูกลิขสิทธิ์เพราะนอกจากจะไม่สามารถอัพเดตแพทช์แล้วในบางกรณียังมีการซ่อนเร้นมัลแวร์บางชนิดมาด้วย

• หมั่นตรวจสอบช่องโหว่ของระบบปฏิบัติการ (OS) และซอฟต์แวร์ที่ติดตั้งในเครื่องและทำการปิดช่องโหว่นั้น โดยอาจจะใช้ซอฟต์แวร์ของผู้ผลิตที่มีให้ เช่น MBSA (Microsoft Baseline Analyzer)

• คอยติดตามข่าวสารของภัยคุกคามที่มาจากไวรัส มัลแวร์ หรือภัยคุกคามจากหน่วยงานที่เกี่ยวข้อง เช่น ThaiCERT (ETDA) , SANS หรือจากผู้ผลิตโปรแกรมป้องกันไวรัส เช่น Avast, McAfee, TrendMicro, Symantec เป็นต้น

ข้อมูลอ้างอิง :

• Customer Guidance for WannaCrypt Attack by MS (https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/)
• Microsoft Security Bulletin MS17-010 (https://technet.microsoft.com/en-us/library/security/ms17-010.aspx)
• How to enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server (https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
• Windows DNS Server Sinkhole Domains Tool (https://cyber-defense.sans.org/blog/2010/08/31/windows-dns-server-blackhole-blacklist)
• Microsoft Baseline Security Analyzer (https://www.microsoft.com/en-us/download/details.aspx?id=7558)
• Microsoft Windows Server Update Services (https://www.microsoft.com/en-us/download/details.aspx?id=5216)