มหันตภัยร้าย Malware เรียกค่าไถ่ข้อมูลสายพันธุ์ใหม่ (WannaCry Ransomware)

1. ทำความรู้จักกับ WannaCry

เมื่อเหยื่อโดน WannaCry Ransomware โจมตี ไฟล์ข้อมูลทั้งหมดภายในเครื่องคอมพิวเตอร์จะถูกเข้ารหัส และทำให้อยากจะร้องไห้ นี่คือความหมายของชื่อ Malware ตัวนี้ ซึ่งสาเหตุที่ทำให้ Malware ตัวนี้โด่งดังและผู้ใช้ระบบคอมพิวเตอร์ทั่วโลกหวาดผวาก็เพราะมันสามารถแพร่พันธุ์ด้วยตัวของมันเองอย่างรวดเร็ว โดยผู้ใช้ไม่ต้องคลิ๊กลิงค์ หรือรันโปรแกรมจากไฟล์แนบจากอีเมลแต่อย่างใด โดยมันจะค้นหาเป้าหมายที่มีช่องโหว่ของบริการแชร์ไฟล์และเครื่องพิมพ์ที่ชื่อว่า SMB(Server Message Block) ผ่านทางพอร์ต 445 ของระบบปฏิบัติการ Windows ในระบบเครือข่าย และเริ่มโจมตีเครื่องคอมพิวเตอร์เป้าหมายทันที

จากนั้น WannaCry จะเข้ารหัสไฟล์ข้อมูลทั้งหมด พร้อมกับแสดงข้อความแจ้งเตือน ให้โอนเงินผ่านทาง Bitcoin ซึ่งเป็นสกุลเงินเสมือนจริง และไม่มีกลไกในการระบุตัวตน จำนวน $300 ภายใน 3 วัน มิฉะนั้น จะต้องโอนเงินให้เป็น 2 เท่า หรือ $600 เพื่อแลกกับรหัสผ่านสำหรับกู้คืนข้อมูล และถ้ายังไม่โอนเงินให้ภายใน 7 วัน ข้อมูลทั้งหมดจะถูกลบทิ้งอย่างถาวร

2. มาตรการป้องกัน

2.1 Update Patch บนระบบปฏิบัติการ Windows เพื่ออุดช่องโหว่ทันที สำหรับผู้ที่ใช้ระบบปฏิบัติการ Windows สามารถ Update โปรแกรมสำหรับอุดช่องโหว่ได้ที่เว็บไซต์ **tinyurl.com/winspatch** ส่วน Windows XP SP3 สามารถดาวน์โหลดได้ที่ **tinyurl.com/winxp3patch**

2.2 หากไม่ได้ใช้บริการแชร์ไฟล์หรือเครื่องพิมพ์ ให้ปิดบริการ SMB หรือ ใช้โปรแกรม Firewall บนระบบปฏิบัติการ Windows ตั้งกฎเพื่อปิดกั้นพอร์ต TCP 139,445

2.3 ติดตั้งโปรแกรม Anti-Virus หรือ End Point Protection และ Update ข้อมูลสายพันธุ์ Malware ให้ทันสมัยทุกวัน หรืออย่างน้อยสัปดาห์ละ 1 ครั้ง

2.4 หมั่นสำรองไฟล์ข้อมูลสำคัญไว้ในหน่วยจัดเก็บข้อมูลภายนอก ได้แก่ External Hard Disk, Flash Drive, DVD เป็นต้น

2.5 ใช้โปรแกรมจำลองสภาพแวดล้อมเสมือนจริงเพื่อใช้งานบนเครือข่ายอินเทอร์เน็ต ได้แก่ Sandboxie.com, Bromium.com, VMware.com, Virtualbox.org เป็นต้น

3. การแก้ไขปัญหาเมื่อถูกโจมตี

3.1 อย่าโอนเงินให้กับคนร้ายตามที่เรียกร้อง เพราะจะทำให้กลุ่มคนร้ายยิ่งได้ใจ และพัฒนา Malware สายพันธุ์ใหม่ออกมาเรื่อย ๆ

3.2 แยกคอมพิวเตอร์ที่ถูกโจมตีออกจากระบบเครือข่ายทันที ด้วยการดึงสายเคเบิ้ลของระบบเครือข่ายออกจากเครื่องคอมพิวเตอร์ เพื่อป้องกันการแพร่ระบาด

3.3 แจ้งเจ้าหน้าที่ หรือผู้เชี่ยวชาญ ให้จัดเก็บพยานหลักฐานทางอิเล็กทรอนิกส์จากหน่วยความจำของเครื่องคอมพิวเตอร์

3.4 ปิดเครื่องคอมพิวเตอร์ด้วยการดึงปลั๊กจ่ายไฟฟ้าออกจากหลังเครื่องคอมพิวเตอร์ และถอดฮาร์ดดิกส์ลูกที่ถูกโจมตีเก็บไว้ หมั่นตรวจสอบข้อมูลจากเว็บไซต์ NoMoreRansom.org รอจนกระทั่งมีการพัฒนาโปรแกรมสำหรับถอดรหัสข้อมูลออกมาแล้วนำไปใช้ถอดรหัสข้อมูลที่ถูกเรียกค่าไถ่ เพื่อกู้คืนข้อมูลกลับคืนมา

3.5 ติดตั้งระบบปฏิบัติการลงในฮาร์ดดิสก์ลูกใหม่และใช้ทำงานต่อไป

ด้วยความปรารถนาดีจาก

กองบังคับการสนับสนุนทางเทคโนโลยี

สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ

HighTechCrime.org