แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

การโจมตีด้วยมัลแวร์ XWorm ผ่านอีเมลฟิชชิงหลายรูปแบบ ด้วยช่องโหว่เก่า (CVE-2018-0802)

วันที่แจ้งเตือน 6 มีนาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการรายงานเกี่ยวกับแคมเปญการโจมตีที่ใช้มัลแวร์ XWorm Remote Access Trojan (RAT) ผ่านอีเมลฟิชชิงหลายรูปแบบ ซึ่งผู้ไม่ประสงค์ดีสามารถควบคุมระบบคอมพิวเตอร์ได้จากระยะไกลหลังจากติดตั้งมัลแวร์สำเร็จ โดยเริ่มจากส่งอีเมลฟิชชิงที่ปลอมแปลงเป็นเอกสารสำคัญเพื่อหลอกลวงให้เหยื่อเปิดไฟล์แนบประเภท Excel เมื่อเปิดไฟล์แล้วจะใช้ประโยชน์จากช่องโหว่ CVE-2018-0802 ใน Microsoft Equation Editor เพื่อเรียกใช้โค้ดอันตรายและดาวน์โหลดไฟล์ HTA ลงสู่เครื่องคอมพิวเตอร์ของเหยื่อ จากนั้นจะใช้ PowerShell โหลดโมดูล .NET แบบ fileless และใช้เทคนิค process hollowing เพื่อฝังมัลแวร์ XWorm ลงในกระบวนการ Msbuild.exe ที่สร้างขึ้นใหม่ เพื่อหลีกเลี่ยงการตรวจจับจากระบบป้องกันภัยคุกคาม เมื่อมัลแวร์ถูกติดตั้งสำเร็จ ระบบของเหยื่อจะเชื่อมต่อกับเซิร์ฟเวอร์ควบคุม (Command-and-Control: C2) เพื่อรับคำสั่งจากผู้ไม่หวังดี ทั้งนี้ มัลแวร์ XWorm สามารถดำเนินการหลายรูปแบบ เช่น ดาวน์โหลดและรันไฟล์เพิ่มเติม การควบคุมระบบจากระยะไกล การบันทึกการกดแป้นพิมพ์ การดาวน์โหลดปลั๊กอินเพิ่มเติม รวมถึงการขโมยข้อมูลจากระบบที่ถูกบุกรุก เป็นต้น

เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบพิจารณาดำเนินมาตรการที่เหมาะสม โดยเพิ่มความระมัดระวังต่ออีเมลที่มีไฟล์แนบหรือข้อความที่น่าสงสัย พร้อมทั้งอัปเดตระบบปฏิบัติการและซอฟต์แวร์ตามคำแนะนำของผู้ผลิต รวมถึงจำกัดการเปิดใช้งานไฟล์แนบที่อาจมีความเสี่ยง เช่น ไฟล์ Excel ที่มี macro หรือ OLE object จากแหล่งที่ไม่เชื่อถือ เสริมมาตรการตรวจจับอีเมลและระบบป้องกันฟิชชิง เฝ้าระวังพฤติกรรมของโปรเซสที่ผิดปกติ เช่น การเรียกใช้งาน PowerShell, mshta.exe หรือ msbuild.exe จากไฟล์ที่ได้รับผ่านอีเมล เป็นต้น และเพิ่มการตรวจสอบบันทึกเหตุการณ์ (log monitoring) เพื่อให้สามารถตรวจจับและตอบสนองต่อการโจมตีได้อย่างทันท่วงที และควรพิจารณาทบทวนและปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยของบริษัทให้ทันต่อเหตุภัยคุกคามไซเบอร์

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อหน่วยงานในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1. https://www.fortinet.com/blog/threat-research/deep-dive-into-new-xworm-campaign-utilizing-multiple-themed-phishing-emails
2. https://nvd.nist.gov/vuln/detail/cve-2018-0802
3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2018-0802

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ