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

Microsoft เปิดเผยการโจมตีแบบ ClickFix ผ่าน DNS โดยใช้คำสั่ง Nslookup ก่อนติดตั้งมัลแวร์

วันที่แจ้งเตือน 16 กุมภาพันธ์ 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการรายงานว่าบริษัท Microsoft เปิดเผยการโจมตีแบบ ClickFix รูปแบบใหม่ ซึ่งใช้วิธีการหลอกลวงทาง Social Engineering ให้ผู้ใช้งาน Windows Run dialog

ผู้ไม่ประสงค์ดีสามารถรันคำสั่ง “nslookup” เพื่อสืบค้นข้อมูลผ่านระบบ Domain Name System (DNS) ไปยังเซิร์ฟเวอร์ภายนอกที่กำหนดไว้ ก่อนนำไปประมวลผลเป็น payload และใช้ในการโจมตีในขั้นถัดไป ทั้งนี้ เทคนิค ClickFix เคยถูกนำมาใช้เพื่อการโจมตีอย่างต่อเนื่องร่วมกับแคมเปญ CAPTCHA ปลอม อีเมลฟิชชิง เว็บไซต์ถูกบุกรุก หรือหน้าเว็บไซต์ที่ปลอมเป็นอยู่ระหว่างการแก้ไขปัญหาระบบ

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจพิจารณาดำเนินการดังนี้

- เฝ้าระวังการเรียกใช้คำสั่ง nslookup หรือคำสั่งที่เกี่ยวข้องกับ DNS lookup ที่ผิดปกติ
- ตรวจสอบทราฟฟิก DNS ที่เชื่อมต่อไปยัง DNS Server ภายนอกที่ไม่ได้รับอนุญาต
- ตรวจสอบไฟล์ในโฟลเดอร์ Startup และ Scheduled Tasks เพื่อค้นหากลไก Persistence ที่ผิดปกติ
- อัปเดตระบบ Endpoint Detection and Response (EDR) และระบบเฝ้าระวังภัยคุกคามให้เป็นปัจจุบัน

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

ข้อมูลอ้างอิง

1. https://thehackernews.com/2026/02/microsoft-discloses-dns-based-clickfix.html