แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

การโจมตีของ ClickFix รูปแบบใหม่โดยใช้ Cmdkey บน Windows

วันที่แจ้งเตือน 28 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการรายงานเกี่ยวกับการโจมตี ClickFix รูปแบบใหม่โดยใช้ cmdkey ซึ่งเป็นยูทิลิตี้บนระบบปฏิบัติการ Windows พร้อมส่ง Payload จากระยะไกล แทนการใช้ PowerShell ในรูปแบบเดิม

วิธีการดังกล่าว จะหลอกให้ผู้ใช้งานคัดลอกและดำเนินการคำสั่งผ่าน Command Prompt (Win+R) ซึ่งอ้างว่าเป็นการแก้ไขปัญหาทางเทคนิค และใช้แสดงรายการข้อมูลที่จัดเก็บไว้ใน Windows Credential Manager ทำให้ผู้ไม่หวังดีสามารถนำข้อมูลดังกล่าวไปใช้เข้าถึงระบบหรือทรัพยากรภายในเครือข่ายขององค์กรได้ และนำไปสู่การทำ lateral movement การเปลี่ยนไปใช้ cmdkey แทน PowerShell เพื่อหลีกเลี่ยงการตรวจจับจากระบบรักษาความปลอดภัย เนื่องจาก cmdkey เป็นเครื่องมือที่ถูกใช้งานทั่วไปและอาจไม่ถูกตรวจสอบ ส่งผลให้การโจมตีสามารถทำได้โดยอาศัยการทำงานของผู้ใช้งานเอง และยากต่อการป้องกัน

เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบดำเนินการสร้างความตระหนักรู้แก่ผู้ใช้งานเกี่ยวกับความเสี่ยงของการคัดลอกและรันคำสั่งจากแหล่งที่ไม่น่าเชื่อถือ กำหนดแนวทางการใช้งานเครื่องมือระบบอย่างเหมาะสม พร้อมทั้งเฝ้าระวังและติดตามพฤติกรรมการใช้งานคำสั่งหรือเครื่องมือระบบ รวมถึงเฝ้าระวังและตรวจสอบวิเคราะห์บันทึกเหตุการณ์ (log) เพื่อให้สามารถตรวจจับและตอบสนองต่อการโจมตีได้อย่างทันท่วงที และควรพิจารณาทบทวนและปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยของบริษัทให้ทันต่อเหตุภัยคุกคามไซเบอร์

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

ข้อมูลอ้างอิง

1. https://cybersecuritynews.com/clickfix-attack-replaces-powershell-with-cmdkey/
2. https://www.cyberproof.com/blog/beyond-powershell-analyzing-the-multi-action-clickfix-variant/

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ