แจ้งเตือน : ช่องโหว่

Alert

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

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน พบ SteelFox มัลแวร์ใหม่ โจมตีผู้ใช้ซอฟต์แวร์ละเมิดลิขสิทธิ์

วันที่แจ้งเตือน 18 พฤศจิกายน 2567

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้เผยแพร่เกี่ยวกับการพบมัลแวร์ใหม่ที่มีชื่อว่า SteelFox ซึ่งกำลังแพร่กระจายผ่านโปรแกรมละเมิดลิขสิทธิ์ที่แอบอ้างเป็นซอฟต์แวร์ที่นิยม เช่น Foxit PDF Editor, AutoCAD และ JetBrains เป็นต้น โดยมัลแวร์นี้เริ่มโจมตีตั้งแต่เดือนกุมภาพันธ์ 2023 จนถึงปัจจุบัน และได้แพร่กระจายไปยังผู้ใช้งานจำนวนมาก

มัลแวร์ SteelFox มีวิธีการทำงานที่สามารถหลบเลี่ยงการตรวจจับและใช้เทคนิคขั้นสูงในการโจมตี โดยเมื่อเข้าสู่ระบบแล้ว มัลแวร์จะรวบรวมข้อมูลสำคัญจาก web browser ที่ใช้งาน ทั้งประวัติการท่องเว็บ ข้อมูลการเข้าสู่ระบบต่าง ๆ รวมถึงข้อมูลที่ถูกบันทึกไว้ นอกจากนี้ยังสามารถเก็บข้อมูลการตั้งค่าระบบและมีความสามารถในการยกระดับสิทธิเป็นระดับ Privilege User ผ่านการใช้ประโยชน์จาก driver ที่มีช่องโหว่ ซึ่งอาจส่งผลกระทบต่อองค์กรได้

เพื่อลดความเสี่ยงที่อาจได้รับผลกระทบจากมัลแวร์ดังกล่าว องค์กรจึงควรพิจารณาแนวทางการป้องกัน โดยให้ความสำคัญต่อการสร้างวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์ เริ่มจากการสร้างความตระหนักรู้ ให้ความรู้แก่พนักงานเกี่ยวกับภัยคุกคามจากมัลแวร์และวิธีการป้องกัน การกำหนดนโยบายการใช้ซอฟต์แวร์ที่ชัดเจน และการสนับสนุนให้ใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้อง ซึ่งจะช่วยสร้างระบบนิเวศด้านความมั่นคงปลอดภัยที่แข็งแกร่ง และควรมีระบบตรวจสอบและเฝ้าระวังการใช้งานที่ผิดปกติ รวมทั้งมีการเตรียมแผนรับมือภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น และปฏิบัติตามแนวทางการรักษาความมั่นคงปลอดภัยอย่างเคร่งครัด

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

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 12 พ.ย. 2567
2) https://hackread.com/steelfox-malware-software-to-steal-browser-data/
3) https://www.bleepingcomputer.com/news/security/new-steelfox-malware-hijacks-windows-pcs-using-vulnerable-driver/