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

Google Chrome Extensions กว่า 100 รายการ แฝงมัลแวร์และติดตั้ง Backdoor เพื่อขโมยข้อมูล

วันที่แจ้งเตือน 17 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการรายงานเกี่ยวกับ Google Chrome Extensions (ส่วนขยาย) กว่า 100 รายการ แฝงด้วยมัลแวร์อันตราย ซึ่งถูกออกแบบมาเพื่อขโมยข้อมูลบัญชีผู้ใช้งานและข้อมูลสำคัญ รวมถึงติดตั้ง backdoor สำหรับโจมตีเพื่อสั่งควบคุมระบบจากระยะไกล (Remote Code Execution :RCE)

รายงานระบุว่า ส่วนขยายดังกล่าวถูกพัฒนาโดยนักพัฒนาหลายราย แต่ใช้โครงสร้างพื้นฐาน Command and Control (C2) ร่วมกัน โดยปลอมแปลงเป็นเครื่องมือทั่วไป เช่น เครื่องมือสำหรับแอปพลิเคชันโซเชียลมีเดีย แอปพลิเคชันเกม และเครื่องมือแปลภาษา เป็นต้น เพื่อหลอกลวงให้ผู้ใช้งานติดตั้ง เมื่อถูกติดตั้งแล้วส่วนขยายจะทำงานตามฟังก์ชันที่โฆษณาไว้ แต่มีพฤติกรรมแฝง เช่น การขโมยบัญชี Google ผ่าน OAuth2 โดยดึง bearer token และข้อมูลผู้ใช้งาน การฝังสคริปต์ลงในหน้าเว็บ การเปิด URL จากเซิร์ฟเวอร์ของผู้ไม่หวังดี และการโหลดเพย์โหลดเพิ่มเติมเข้าสู่ระบบ เป็นต้น โดยบางส่วนขยายสามารถทำงานเป็น backdoor ติดต่อกับเซิร์ฟเวอร์ของผู้ไม่หวังดี เพื่อรับคำสั่งเพิ่มเติม และสามารถทำงานได้แม้ผู้ใช้งานไม่ได้เปิดใช้งานส่วนขยายโดยตรง

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบพิจารณาตรวจสอบและจำกัดการใช้งานส่วนขยายบนเบราว์เซอร์ รวมทั้งถอนการติดตั้งส่วนขยายที่ไม่จำเป็นหรือไม่ทราบแหล่งที่มา พิจารณาใช้เฉพาะส่วนขยายจากผู้พัฒนาที่เชื่อถือได้ และเฝ้าระวังพฤติกรรมการเข้าถึงบัญชีหรือการใช้งานระบบที่ผิดปกติ เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นกับระบบงานขององค์กร

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

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/over-100-chrome-extensions-in-web-store-target-users-accounts-and-data/
2. https://socket.dev/blog/108-chrome-ext-linked-to-data-exfil-session-theft-shared-c2

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ