วันที่ 23 พฤษภาคม 2568

พบส่วนขยาย Chrome อันตรายกว่า 100 รายการ ปลอมเป็น Fortinet และ YouTube เพื่อขโมยข้อมูลผู้ใช้

Executive Summary

ทีม CSOC ได้ตรวจพบรายงานความมั่นคงปลอดภัยไซเบอร์ล่าสุดโดย DomainTools พบแคมเปญใหญ่ที่มีส่วนเกี่ยวข้องกับส่วนขยายของ Chrome มากกว่า 100 รายการที่ปลอมเป็นแบรนด์ที่น่าเชื่อถือ เช่น Fortinet YouTube และ DeepSeek AI โดยมีเป้าหมายในการขโมยข้อมูลผู้ใช้งาน เช่น session cookie การฝังสคริปต์อันตราย และการเปลี่ยนเส้นทาง ซึ่งส่วนขยายเหล่านี้มักถูกกระจายผ่านเว็บไซต์ปลอมและแพลตฟอร์มโซเชียลมีเดีย เช่น Facebook โดยแฝงตัวมาในรูปของเครื่องมือที่ดูเหมือนมีประโยชน์ เช่น VPN หรือผู้ช่วยด้าน AI แต่เมื่อผู้ใช้ติดตั้งส่วนขยายนี้จะเชื่อมต่อกับเซิร์ฟเวอร์จากระยะไกลเพื่อรันคำสั่งโดยไม่ได้รับอนุญาตและส่งข้อมูลออกไป อีกทั้งยังอาศัยสิทธิ์เข้าถึงของเบราว์เซอร์ในการแทรกโฆษณาหรือทำตัวเป็นพร็อกซี่ แม้ว่า Google จะลบส่วนขยายเหล่านี้ออกไปหลายรายการแล้ว แต่ยังมีบางส่วนที่ใช้งานอยู่ จึงเน้นย้ำถึงความจำเป็นเร่งด่วนที่ผู้ใช้ต้องตรวจสอบความน่าเชื่อถือของส่วนขยายอย่างรอบคอบ

คำแนะนำ (Recommendation)

- ระมัดระวังการติดตั้งส่วนขยายจากแหล่งที่ไม่น่าเชื่อถือ และควรตรวจสอบความถูกต้องก่อนการติดตั้ง
- ตรวจสอบสิทธิ์และระวังส่วนขยายที่ร้องขอสิทธิ์เข้าถึง โดยเฉพาะสิทธิ์ที่สามารถอ่านและเปลี่ยนแปลงข้อมูลบนทุกเว็บไซต์
- ดำเนินการตรวจสอบรายการ Malware Chrome Extensions ตามข้อมูลอ้างอิงด้านล่าง

ข้อมูลอ้างอิง

- https://www.bleepingcomputer.com/news/security/data-stealing-chrome-extensions-impersonate-fortinet-youtube-vpns/
- https://github.com/DomainTools/SecuritySnacks/blob/main/2025/DualFunction-Malware-Chrome-Extensions