วันที่ 24 มีนาคม 2569

Microsoft เตือนแคมเปญฟิชชิงปลอมเป็น IRS กระทบผู้ใช้กว่า 29,000 ราย และใช้มัลแวร์ RMM เข้าควบคุมเครื่อง

Microsoft เตือนถึงแคมเปญฟิชชิงใหม่ที่อาศัยช่วงฤดูกาลยื่นภาษีในสหรัฐฯ เพื่อขโมยข้อมูลบัญชีผู้ใช้และแพร่กระจายมัลแวร์ โดยอีเมลจะปลอมเป็นการแจ้งเงินคืนภาษี แบบฟอร์มเงินเดือน การเตือนยื่นภาษี หรือคำขอจากผู้เชี่ยวชาญด้านภาษี เพื่อหลอกให้เหยื่อเปิดไฟล์แนบ สแกน QR Code หรือคลิกลิงก์อันตราย

ทีม Microsoft Threat Intelligence ระบุว่า นอกจากบุคคลทั่วไปแล้ว แคมเปญเหล่านี้ยังมุ่งเป้าไปที่นักบัญชีและผู้เชี่ยวชาญที่ต้องจัดการเอกสารทางการเงิน ซึ่งมักได้รับอีเมลเกี่ยวกับภาษีในช่วงนี้เป็นประจำ

กลยุทธ์การเจาะระบบผ่านฟิชชิงและซอฟต์แวร์ควบคุมระยะไกล

บางแคมเปญจะพาผู้ใช้ไปยังเว็บไซต์ฟิชชิงที่สร้างผ่านแพลตฟอร์ม Phishing-as-a-Service (PhaaS) เพื่อขโมยข้อมูลบัญชี ขณะที่บางกรณีจะติดตั้งเครื่องมือควบคุมเครื่องระยะไกลที่เป็นซอฟต์แวร์จริง เช่น

- ConnectWise ScreenConnect
- Datto
- SimpleHelp

ซึ่งเปิดทางให้ผู้โจมตีเข้าควบคุมระบบของเหยื่อได้อย่างต่อเนื่อง

แคมเปญโจมตีขนาดใหญ่สวมรอยหน่วยงานสรรพากร

เมื่อวันที่ 10 กุมภาพันธ์ 2026 มีการตรวจพบหนึ่งในแคมเปญการโจมตีขนาดใหญ่ ซึ่งส่งผลกระทบต่อผู้ใช้มากกว่า 29,000 รายจาก 10,000 องค์กร โดยประมาณ 95% ของเป้าหมายอยู่ในสหรัฐอเมริกา ครอบคลุมอุตสาหกรรมการเงิน เทคโนโลยี และค้าปลีก แคมเปญนี้ใช้วิธีส่งอีเมลฟิชชิงปลอมเป็นหน่วยงาน Internal Revenue Service (IRS) โดยอ้างว่าพบการยื่นภาษีผิดปกติภายใต้หมายเลข Electronic Filing Identification Number (EFIN) ของผู้รับ จากนั้นจึงหลอกให้เหยื่อดาวน์โหลดโปรแกรมชื่อ “IRS Transcript Viewer”

กลวิธีหลบเลี่ยงการตรวจจับและแคมเปญอื่นๆ ที่เกี่ยวข้อง

อีเมลถูกส่งผ่านบริการ Amazon Simple Email Service (SES) และมีปุ่ม “Download IRS Transcript View 5.1” ซึ่งจะพาผู้ใช้ไปยังโดเมน smartvault[.]im ที่ปลอมเป็นแพลตฟอร์มจัดการเอกสาร SmartVault

เว็บไซต์ดังกล่าวใช้ Cloudflare เพื่อป้องกันการตรวจจับจากบอท ก่อนจะส่งไฟล์ ScreenConnect ที่ถูกฝังมัลแวร์ให้ผู้ใช้ดาวน์โหลด เมื่อรันไฟล์ ผู้โจมตีจะสามารถเข้าควบคุมเครื่อง ขโมยข้อมูล และดำเนินการโจมตีต่อไปได้ทันที นอกจากนี้ยังพบแคมเปญรูปแบบอื่นๆ เช่น การสร้างหน้า Google Meet และ Zoom ปลอม, การปลอมเว็บไซต์ดาวน์โหลด Telegram, การใช้ไฟล์ ZIP ปลอมเป็นซอฟต์แวร์ต่างๆ ตลอดจนการใช้บริการ URL rewriting จากหลายผู้ให้บริการ

แนวทางป้องกันและสถิติการใช้เครื่องมือ RMM ในทางที่ผิด

Microsoft แนะนำให้องค์กรลดความเสี่ยงด้วยการ

- เปิดใช้ 2FA สำหรับผู้ใช้ทุกคน
- ใช้นโยบาย Conditional Access
- ตรวจสอบอีเมลและเว็บไซต์ที่เข้าถึง
- บล็อกโดเมนอันตราย

รายงานจาก Huntress ระบุว่า การนำเครื่องมือ Remote Monitoring and Management (RMM) มาใช้ในทางที่ผิดนั้นเพิ่มขึ้นถึง 277% เมื่อเทียบกับปีก่อน เนื่องจากซอฟต์แวร์ประเภทนี้มักถูกมองว่าเป็นเครื่องมือที่เชื่อถือได้ในสภาพแวดล้อมขององค์กร ผู้เชี่ยวชาญจึงแนะนำให้องค์กรตรวจสอบระบบอย่างสม่ำเสมอ เพื่อค้นหาการใช้งานเครื่องมือ RMM ที่ไม่ได้รับอนุญาตและป้องกันการเข้าถึงระบบโดยผู้ไม่หวังดี

ข้อมูลอ้างอิง

Mar 23, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/03/microsoft-warns-irs-phishing-hits-29000.html