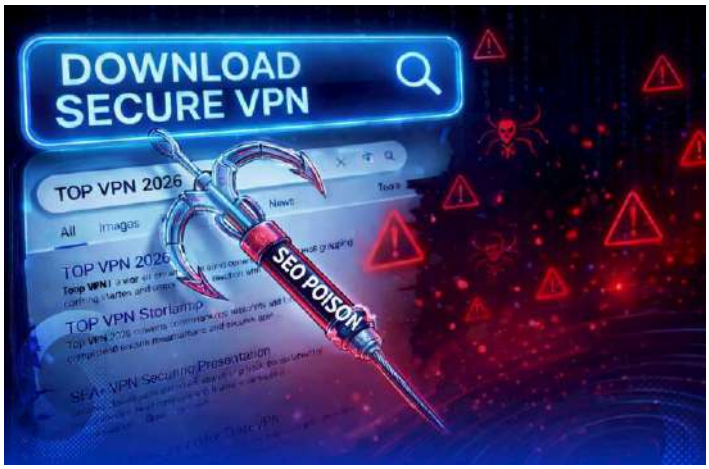
วันที่ 16 มีนาคม 2569

Storm-2561 แพร่กระจาย VPN ปลอมผ่านเทคนิค SEO Poisoning เพื่อขโมยข้อมูลล็อกอิน



Microsoft ออกโรงเตือนถึงแคมเปญขโมยข้อมูลล็อกอิน (Credential Theft) รูปแบบใหม่ที่กำลังแพร่ระบาด โดยผู้โจมตีใช้เทคนิค SEO poisoning เพื่อดันเว็บไซต์ปลอมให้ขึ้นมาอยู่อันดับต้นๆ ของผลการค้นหา หลอกล่อให้ผู้ใช้ที่กำลังมองหาซอฟต์แวร์ VPN สำหรับองค์กรดาวน์โหลดไฟล์อันตรายไปติดตั้งโดยไม่รู้ตัว

ทีม Microsoft Threat Intelligence และ Microsoft Defender Experts ระบุว่า เมื่อเหยื่อหลงเชื่อคลิกดาวน์โหลดไฟล์ ZIP จากเว็บไซต์ที่กลุ่มแฮกเกอร์ควบคุมไว้ ระบบจะทำการติดตั้งมัลแวร์ประเภทโทรจันที่มีการเซ็นลายเซ็นดิจิทัลเพื่อสร้างความน่าเชื่อถือ โดยตัวโปรแกรมจะปลอมตัวเป็นซอฟต์แวร์ VPN ชื่อดัง แต่เป้าหมายที่แท้จริงคือการดักจับชื่อผู้ใช้และรหัสผ่าน

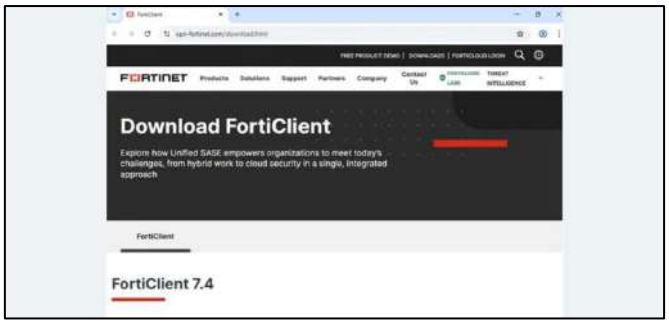
ย้อนรอยเส้นทางกลุ่ม Storm-2561

ยักษ์ใหญ่ผู้พัฒนา Windows ตรวจพบความเคลื่อนไหวนี้ครั้งแรกในช่วงกลางเดือนมกราคม 2026 และเชื่อมโยงว่าเป็นฝีมือของกลุ่ม Storm-2561 ซึ่งมีประวัติการโจมตีในลักษณะนี้มาตั้งแต่เดือนพฤษภาคม 2025 โดยกลุ่มนี้เชี่ยวชาญการใช้ SEO poisoning และการแอบอ้างชื่อผู้ผลิตซอฟต์แวร์ที่มีชื่อเสียง

ข้อมูลจาก Cyjax เคยบันทึกไว้ว่า กลุ่มนี้ใช้เทคนิคดังกล่าวเปลี่ยนเส้นทางผู้ใช้ที่ค้นหาซอฟต์แวร์จากบริษัทชั้นนำ เช่น SonicWall, Hanwha Vision และ Pulse Secure (หรือ Ivanti Secure Access ในปัจจุบัน) บน Search Engine อย่าง Bing ให้ไปยังเว็บไซต์ปลอม เพื่อหลอกให้ดาวน์โหลดตัวติดตั้งแบบ MSI ที่ฝังมัลแวร์ Bumblebee loader

ต่อมาในเดือนตุลาคม 2025 Zscaler ได้พบการยกระดับการโจมตีผ่านเว็บไซต์ปลอมอย่าง “ivanti-vpn[.]org” เพื่อหลอกให้เหยื่อดาวน์โหลด Ivanti Pulse Secure VPN เวอร์ชันดัดแปลงที่มีเป้าหมายชัดเจนในการขโมยข้อมูลล็อกอิน VPN จากเครื่องของเหยื่อโดยเฉพาะ

กลโกงแนบเนียน ใช้ GitHub และหน้าล็อกอินปลอม



Microsoft ชี้ให้เห็นว่าผู้โจมตีอาศัยความไว้วางใจที่ผู้ใช้มีต่อผลการค้นหาและชื่อแบรนด์มาเป็นเครื่องมือทาง Social Engineering โดยครั้งนี้มีความซับซ้อนขึ้นเนื่องจากมีการใช้แพลตฟอร์มที่น่าเชื่อถืออย่าง GitHub เป็นที่เก็บไฟล์ติดตั้ง (Repository) ภายในไฟล์ ZIP จะบรรจุตัวติดตั้ง MSI ที่ดูเหมือนซอฟต์แวร์จริง แต่ในระหว่างขั้นตอนการติดตั้ง ระบบจะแอบโหลดไฟล์ DLL ที่เป็นอันตรายเข้ามาทำงานในเครื่อง

กระบวนการขโมยข้อมูลประกอบด้วย:

- การดักข้อมูล: มัลแวร์ Hyrax จะสร้างหน้าต่างล็อกอิน VPN ปลอมที่ดูสมจริงขึ้นมา
- การหลอกล่อ: เมื่อเหยื่อกรอกข้อมูล ระบบจะแสดงข้อความแจ้งข้อผิดพลาด และแนะนำให้ดาวน์โหลดโปรแกรมใหม่อีกครั้ง หรือในบางครั้งจะเปลี่ยนเส้นทางไปยังเว็บไซต์ทางการของ VPN นั้นๆ เพื่อไม่ให้เหยื่อสงสัย
- การฝังตัว: มัลแวร์จะใช้คีย์รีจิสทรี Windows RunOnce เพื่อสร้างความคงอยู่ (Persistence) ทำให้โปรแกรมอันตรายรันอัตโนมัติทุกครั้งที่รีสตาร์ตเครื่อง

การตอบโต้จาก Microsoft

Microsoft ระบุว่าปฏิบัติการของกลุ่ม Storm-2561 มีวัตถุประสงค์เพื่อผลประโยชน์ทางการเงิน โดยพบว่ามัลแวร์บางส่วนถูกเซ็นด้วยใบรับรองดิจิทัลของบริษัท “Taiyuan Lihua Near Information Technology Co., Ltd.” ล่าสุด Microsoft ได้สั่งปิด Repository บน GitHub และเพิกถอนใบรับรองดิจิทัลดังกล่าวเพื่อระงับการโจมตีแล้ว

ข้อแนะนำเพื่อความปลอดภัย: เพื่อป้องกันภัยคุกคามนี้ องค์กรและผู้ใช้งานควรเปิดใช้งานระบบยืนยันตัวตนหลายขั้นตอน (MFA) ในทุกบัญชี และเพิ่มความระมัดระวังในการดาวน์โหลดซอฟต์แวร์ โดยควรตรวจสอบให้มั่นใจว่าดาวน์โหลดจากแหล่งที่มาอย่างเป็นทางการและเชื่อถือได้เท่านั้น

ข้อมูลอ้างอิง

Mar 13, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/03/storm-2561-spreads-trojan-vpn-clients.html