วันที่ 28 เมษายน 2569

มัลแวร์แบ็กดอร์ FIRESTARTER โจมตีอุปกรณ์ Cisco Firepower และยังคงอยู่ได้แม้อัปเดตแพตช์แล้ว

หน่วยงาน Cybersecurity and Infrastructure Security Agency (CISA) ของสหรัฐฯ เปิดเผยเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ หลังหน่วยงานรัฐบาลพลเรือนแห่งหนึ่งถูกเจาะระบบในเดือนกันยายน 2025 โดยผู้โจมตีมุ่งเป้าไปที่อุปกรณ์ **Cisco Firepower** ที่รันซอฟต์แวร์ **Adaptive Security Appliance (ASA)** พร้อมติดตั้งมัลแวร์ตัวใหม่สุดอันตรายในชื่อ **"FIRESTARTER"**

วิเคราะห์กลไก FIRESTARTER: แบ็กดอร์ล่องหนและการควบคุมจากระยะไกล

CISA และ National Cyber Security Centre (NCSC) ของสหราชอาณาจักร ระบุว่า FIRESTARTER คือแบ็กดอร์ที่ถูกออกแบบมาเพื่อควบคุมระบบจากระยะไกล โดยเชื่อว่าเป็นฝีมือของกลุ่มผู้โจมตีระดับสูง (APT) ที่ใช้ช่องโหว่ (ซึ่งปัจจุบันมีแพตช์แล้ว) เป็นประตูทางเข้า ดังนี้:

- CVE-2025-20333 (CVSS: 9.9): ช่องโหว่ร้ายแรงที่อนุญาตให้ผู้โจมตีที่มีบัญชี VPN ถูกต้อง สามารถส่งคำขอ HTTP เพื่อรันโค้ดในสิทธิ์ root ได้
- CVE-2025-20362 (CVSS: 6.5): ช่องโหว่ที่เปิดให้ผู้โจมตีที่ไม่ต้องยืนยันตัวตน สามารถเข้าถึง URL ที่ถูกจำกัดไว้ได้ผ่านคำขอ HTTP พิเศษ

ความน่ากลัว: มัลแวร์ตัวนี้สามารถฝังตัวอยู่ในอุปกรณ์ Cisco ASA หรือ Firepower Threat Defense (FTD) ได้อย่างถาวร แม้จะมีการติดตั้งแพตช์ในภายหลัง ผู้โจมตีก็ยังสามารถกลับเข้ามาควบคุมอุปกรณ์ได้โดยไม่ต้องใช้ช่องโหว่ซ้ำ

LINE VIPER: ชุดเครื่องมือยึดสิทธิ์และควบคุมระบบหลังการบุกรุก

จากการตรวจสอบพบว่าผู้โจมตีใช้เครื่องมือชื่อ LINE VIPER ร่วมด้วยเพื่อจัดการระบบหลังการเจาะ โดยมีความสามารถดังนี้:

- รันคำสั่ง CLI และดักจับแพ็กเก็ตข้อมูลในเครือข่าย
- ข้ามระบบยืนยันตัวตน (AAA) ของอุปกรณ์
- ปิดการบันทึก Log (syslog) เพื่อลบร่องรอย
- สั่งรีบูตเครื่องแบบหน่วงเวลาเพื่อพรางตัว

LINE VIPER ถูกใช้เป็นบันไดในการติดตั้ง FIRESTARTER ลงบนอุปกรณ์ก่อนวันที่ 25 กันยายน 2025 ทำให้การเข้าถึงระบบเป็นไปอย่างต่อเนื่องจนถึงปัจจุบัน

เทคนิคการฝังตัว: อัปเดตเฟิร์มแวร์ก็เอาไม่ออก

FIRESTARTER เป็นไฟล์แบบ Linux ELF ที่มีพฤติกรรมคล้าย Bootkit (เหมือนกับ RayInitiator ที่เคยพบก่อนหน้า) มัลแวร์จะเข้าไปแก้ไขรายการ Boot ของอุปกรณ์เพื่อให้ถูกเรียกใช้งานทุกครั้งที่เครื่องเปิด

***คำเตือนจากผู้เชี่ยวชาญ**: "FIRESTARTER จะดักแก้ไขการทำงานของ LINA (ส่วนประมวลผลหลักของ Cisco) เพื่อเปิดทางให้รัน shell code หรือติดตั้ง LINE VIPER ซ้ำได้ตลอดเวลา แม้อัปเดตเฟิร์มแวร์แล้วมัลแวร์ก็ยังไม่หายไป"*

การเชื่อมโยงและกลยุทธ์ "เครือข่ายแฝง" จากแฮ็กเกอร์จีน

แม้ยังระบุต้นตอไม่ได้ 100% แต่การวิเคราะห์จาก Censys และประวัติของกลุ่ม UAT4356 (Storm-1849) ชี้ให้เห็นความเชื่อมโยงกับแคมเปญ ArcaneDoor ของจีน ซึ่งมีพฤติกรรมมุ่งเป้าอุปกรณ์เครือข่ายเพื่อสอดแนม

ปัจจุบัน แฮ็กเกอร์กลุ่มต่างๆ เช่น Volt Typhoon และ Flax Typhoon ได้ปรับกลยุทธ์จากการสร้างโครงสร้างพื้นฐานเอง ไปเป็นการใช้ "เครือข่ายแฝง" โดยเจาะอุปกรณ์ IoT และเราเตอร์ตามบ้าน (SOHO) เพื่อใช้เป็นจุดผ่านในการโจมตี ทำให้ตรวจจับได้ยากมากเนื่องจากทราฟฟิกดูเหมือนมาจากพื้นที่เดียวกับเป้าหมาย

แนวทางแก้ไข: วิธีเดียวคือต้อง "ถอดปลั๊ก"

Cisco ยืนยันว่าหากอุปกรณ์ถูกเจาะ การอัปเดตซอฟต์แวร์ตามปกติ ไม่สามารถ ลบ FIRESTARTER ออกได้ โดยมีคำแนะนำดังนี้:

1. **Reimage:** แนะนำอย่างยิ่งให้ติดตั้งระบบใหม่ทั้งหมดและอัปเกรดเป็นเวอร์ชันล่าสุด

2. **Cold Restart (ตัดไฟจริง):** หากยังไม่สามารถติดตั้งระบบใหม่ได้ทันที ต้องทำการ **ถอดปลั๊กไฟออกแล้วเสียบใหม่เท่านั้น** เพราะการสั่ง Reboot ผ่านคำสั่ง CLI ไม่สามารถกำจัดมัลแวร์นี้ได้
3. **ล้างค่าคอนฟิก:** หากยืนยันการบุกรุก ควรถือว่าการตั้งค่าเดิมทั้งหมดไม่ปลอดภัยและไม่สามารถเชื่อถือได้อีกต่อไป

Sergey Shykevich จาก Check Point Software เสริมว่า การโจมตีในปี 2025-2026 มุ่งเน้นไปที่อุปกรณ์ขอบเครือข่าย (Edge/Perimeter) เนื่องจากเป็นจุดบอดที่มักขาดการอัปเดต องค์กรจึงต้องให้ความสำคัญกับการป้องกันทุกจุดเชื่อมต่อ ไม่ใช่เพียงแค่การรอตรวจจับทราฟฟิกที่ผิดปกติเท่านั้น

(บทความนี้ได้รับการอัปเดตภายหลังการเผยแพร่ เพื่อเพิ่มข้อมูลจาก Check Point Software)

ข้อมูลอ้างอิง

Apr 24, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/04/firestarter-backdoor-hit-federal-cisco.html