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

FIRESTARTER Backdoor Malware มุ่งโจมตีอุปกรณ์ Cisco

วันที่แจ้งเตือน 27 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการรายงานของหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ของสหรัฐอเมริกา (CISA) และสหราชอาณาจักร (NCSC) ออกแจ้งเตือนเกี่ยวกับมัลแวร์ FIRESTARTER Backdoor ในอุปกรณ์ Cisco Firepower และ Secure Firewall

มัลแวร์ดังกล่าวมีความเชื่อมโยงกับแคมเปญ ArcaneDoor (กลุ่ม UAT4356 หรือ Storm-1849) โดยผู้ไม่หวังดีใช้ประโยชน์จากช่องโหว่ด้านการตรวจสอบสิทธิ์ที่ไม่เหมาะสม (CVE-2025-20333) และช่องโหว่ buffer overflow (CVE-2025-20362) ก่อนทำการยกระดับและหลบหลีกการตรวจจับโดยใช้ Line Viper เพื่อสร้างเครือข่ายเสมือนและเข้าถึงข้อมูลสำคัญของอุปกรณ์ เช่น administrative credentials, certificates และ private keys เป็นต้น ก่อนติดตั้ง FIRESTARTER backdoor เพื่อให้เข้าถึงและคงอยู่ในระบบได้ บนอุปกรณ์และซอฟต์แวร์ระบบ Cisco Adaptive Security Appliance (ASA) และ Firepower Threat Defense (FTD) เพื่อทำให้มัลแวร์สามารถติดตั้งตัวเองใหม่ได้โดยอัตโนมัติและสามารถทำงานเป็นแบ็กดอร์สำหรับรับคำสั่งจากระยะไกล รวมถึงการทำ shellcode injection โจมตีในหน่วยความจำของอุปกรณ์ เพื่อเข้าควบคุมระบบและเข้าถึงข้อมูลสำคัญขององค์กร

เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบดำเนินการ อัปเดตแพตช์ของระบบและอุปกรณ์เครือข่ายตามคำแนะนำของผู้ผลิต รวมถึงติดตามและวิเคราะห์บันทึกเหตุการณ์ (logs) เฝ้าระวังพฤติกรรมที่ผิดปกติของระบบและการเข้าถึงจากแหล่งที่ไม่น่าเชื่อถือ ตรวจสอบการเชื่อมต่อเครือข่ายที่ผิดปกติ พร้อมทั้งติดตามตรวจสอบบันทึกเหตุการณ์ (Log Monitoring) เพื่อให้สามารถตรวจจับและตอบสนองต่อความพยายามโจมตี และสามารถรับมือกับภัยคุกคามได้อย่างทันท่วงที

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

ข้อมูลอ้างอิง

1. https://thehackernews.com/2026/04/firestarter-backdoor-hit-federal-cisco.html
2. https://www.cisa.gov/sites/default/files/2026-04/AR26-113A_MAR_FIRESTARTER_backdoor.pdf
3. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-CISAED25-03
4. https://nvd.nist.gov/vuln/detail/CVE-2025-20333
5. https://nvd.nist.gov/vuln/detail/CVE-2025-20362