

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability



พบบอทเน็ต SSHStalker มุ่งเป้า Linux Server โดยอาศัยช่องโหว่เดิม

วันที่แจ้งเตือน 13 กุมภาพันธ์ 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพ์และผู้ประกอบธุรกิจสินทรัพ์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพ์และตลาดหลักทรัพ์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบรายงานการตรวจพบกรณีบอทเน็ต SSHStalker มุ่งเป้า Linux Server โดยใช้วิธีสแกนวงกว้างและ brute force เพื่อเข้าถึงระบบ ทั้งนี้ พบว่าบอทเน็ตดังกล่าวใช้ช่องโหว่ Linux kernel รุ่นเก่า (โดยเฉพาะตระกูล 2.6.x) หลายรายการ ได้แก่ CVE-2009-2692, CVE-2009-2698, CVE-2010-3849, CVE-2010-1173, CVE-2009-2267, CVE-2009-2908, CVE-2009-3547, CVE-2010-2959 และ CVE-2010-3437 โดยพบว่ามีการโจมตีจำนวนมาก

รายงานดังกล่าวระบุว่า SSHStalker ทำงานโดยฝังตัวแบบ persistent access และใช้การตั้งค่า cron jobs เพื่อให้สามารถเรียกใช้งานได้อัตโนมัติพร้อมทั้งมีการลบไฟล์บันทึกเหตุการณ์ (log) เพื่อหลีกเลี่ยงการตรวจจับ

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจที่มีการใช้ Linux Server พิจารณาดำเนินการใช้งานพอร์ต 22 (SSH) ที่เหมาะสม การจำกัดการเข้าถึงเฉพาะเครือข่ายหรือ IP เท่าที่จำเป็น ใช้การยืนยันตัวตนแบบ SSH key-based authentication หรือ Multi-Factor Authentication (MFA) รวมทั้งอัปเดตระบบปฏิบัติการ Security Patch เป็นเวอร์ชันล่าสุด โดยเฉพาะระบบที่ยังใช้ Linux kernel รุ่นเก่า รวมทั้ง ทบทวนแผนตอบสนองเหตุการณ์ (Incident Response Plan) ให้มีความพร้อมในการปฏิบัติอย่างต่อเนื่อง

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

ข้อมูลอ้างอิง

- <https://securityaffairs.com/187833/malware/sshstalker-botnet-targets-linux-servers-with-legacy-exploits-and-ssh-scanning.html>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ

