วันที่ 8 เมษายน 2568

กลุ่ม Outlaw ใช้ SSH Brute-Force เพื่อติดตั้งมัลแวร์ Cryptojacking บนเซิร์ฟเวอร์ Linux

Executive Summary

นักวิจัยด้านความมั่นคงปลอดภัยไซเบอร์ได้วิเคราะห์ภัยคุกคามต่อเนื่องจาก Outlaw หรือรู้จักกันในชื่อ Dota ซึ่งเป็น Cryptocurrency mining botnet ที่สามารถแพร่กระจายตัวเองได้ และมุ่งเป้าไปที่ระบบ Linux ที่มีรหัสผ่าน SSH อ่อนแอ ซึ่งกลุ่มภัยคุกคามนี้เชื่อมโยงกับประเทศโรมาเนียและเริ่มมีการใช้งานตั้งแต่ปี 2018 โดยอาศัยเทคนิคการเดารหัสผ่าน SSH แบบ Brute-force การแพร่กระจายตัวเอง และการฝังตัวเพื่อเข้าควบคุมระบบระยะยาว

Threat Summary

Outlaw malware สามารถเข้าถึงระบบเริ่มต้นได้ผ่านการ Brute-force SSH และ Telnet เพื่อสแกนและแพร่กระจายตัวเองไปยังระบบ พร้อมดึงข้อมูลเป้าหมายจากเซิร์ฟเวอร์ C2 ที่ใช้ SSH ติดตั้งสคริปต์ tddwrt7s.sh ที่ดาวน์โหลดไฟล์ dota3.tar.gz และมี payload ที่ทำความสะอาดระบบและลบหลักฐาน โดยมัลแวร์ตัวนี้ยังเพิ่มการควบคุมระบบด้วยการเพิ่ม SSH key ลงในไฟล์ authorized_keys และใช้ cron job เพื่อสร้างความคงอยู่ในระบบ พร้อมทั้งติดตั้ง SHELLBOT ที่ควบคุมผ่าน IRC เพื่อรันคำสั่งต่าง ๆ ในการทำ DDoS และขโมยข้อมูล ส่วนสำหรับการขุดคริปโตนั้นจะติดตั้ง XMRig ที่ถูกดัดแปลง และเปิดใช้งาน hugepages บน CPU Core เพื่อเพิ่มประสิทธิภาพและใช้ไบนารี kswap01 เพื่อรักษาการเชื่อมต่อกับ C2 นอกจากนี้ยังใช้ประโยชน์จากช่องโหว่ที่ยังไม่ได้รับการแก้ไข เช่น CVE-2016-8655 และ Dirty COW (CVE-2016-5195)

คำแนะนำ (Recommendation)

- การใช้ระบบยืนยันตัวตน เช่น MFA
- ดำเนินการปิดหรือจำกัดการเข้าถึง SSH/Telnet จากภายนอก
- ดำเนินการตรวจสอบ SSH key ที่ไม่ได้รับอนุญาตและไฟล์ต้องสงสัย
- ดำเนินการตรวจสอบการเชื่อมต่อกับ C2 ผ่าน IRC หรือการใช้งาน SSH ที่ผิดปกติหรือต้องสงสัย

ข้อมูลอ้างอิง

- https://thehackernews.com/2025/04/outlaw-group-uses-ssh-brute-force-to.html