วันที่ 6 มิถุนายน 2568

ผู้เชี่ยวชาญด้านความปลอดภัยเตือนถึงมัลแวร์ RAT เวอร์ชันใหม่ “Chaos RAT” พุ่งเป้าโจมตี Windows และ Linux

ผู้เชี่ยวชาญด้านความปลอดภัยของ Acronis ได้ออกมาเตือนถึงมัลแวร์ประเภท Remote Access Trojan (RAT) ตัวใหม่ที่ชื่อว่า Chaos RAT ซึ่งถูกนำไปใช้ในการโจมตีล่าสุด โดยมุ่งเป้าไปที่ทั้งระบบปฏิบัติการ Windows และ Linux

“Chaos RAT เป็นมัลแวร์แบบโอเพ่นซอร์สที่เขียนด้วยภาษา Golang ซึ่งสามารถทำงานข้ามแพลตฟอร์มได้ทั้งบน Windows และ Linux” นักวิจัยด้านความปลอดภัย Santiago Pontiroli, Gabor Molnar และ Kirill Antonenko กล่าวผ่านรายงานที่แชร์กับ The Hacker News

Chaos RAT ได้แรงบันดาลใจจากเฟรมเวิร์กยอดนิยม เช่น **Cobalt Strike** และ **Sliver** โดยมาพร้อมกับ **แผงควบคุม (Admin Panel)** สำหรับสร้างเพย์โหลด เปิดเซสชัน และควบคุมเครื่องเป้าหมายจากระยะไกล

แม้เครื่องมือนี้จะถูกพัฒนามาตั้งแต่ปี 2017 แต่เพิ่งถูกนำไปใช้ในการโจมตีเมื่อ **ธันวาคม 2022** โดยพบในแคมเปญโจมตีเว็บแอปพลิเคชันที่เปิดพอร์ตบนระบบ Linux พร้อมฝังตัว **XMRig** (เครื่องมือขุดเหรียญคริปโต)

หลังการติดตั้ง มัลแวร์จะเชื่อมต่อกับเซิร์ฟเวอร์จากภายนอก และรอรับคำสั่งที่มีสามารถดังนี้

- เปิด reverse shell
- อัปโหลด ดาวน์โหลด ลบไฟล์
- ตรวจสอบไฟล์และไดเรกทอรี
- ถ่ายภาพหน้าจอ
- ดึงข้อมูลระบบ
- ล็อคหน้าจอ / รีสตาร์ท / ปิดเครื่องคอมพิวเตอร์
- เปิดเว็บไซต์ตามที่กำหนด

ปัจจุบัน Chaos RAT เวอร์ชันล่าสุดคือ **5.0.3** ซึ่งเปิดตัวเมื่อวันที่ **31 พฤษภาคม 2024**

Acronis ระบุว่า **มัลแวร์เวอร์ชัน Linux ถูกพบในเหตุการณ์โจมตีจริงแล้ว** และมักจะเกี่ยวข้องกับแคมเปญ **ขุดเหรียญคริปโต** โดยแผนการโจมตีมักใช้ **อีเมลฟิชชิ่ง** ที่มีลิงก์หรือไฟล์แนบอันตราย

ไฟล์เหล่านี้มักจะ **วางสคริปต์อันตราย** ที่จะแก้ไข crontab (เครื่องมือกำหนดงานตามเวลาใน Linux) เพื่อดาวน์โหลดมัลแวร์ซ้ำๆ เป็นการสร้าง **ช่องทางการเข้าถึงเป้าหมายให้คงอยู่เสมอ (persistence)**

“ในแคมเปญช่วงแรก Chaos RAT มักถูกติดตั้งแยกจากตัวขุดเหรียญ แสดงให้เห็นว่าถูกใช้เพื่อสอดแนมและเก็บข้อมูลจากระบบเป้าหมายก่อน” นักวิจัยกล่าว

การวิเคราะห์ไฟล์ตัวอย่างที่เพิ่งถูกอัปโหลดขึ้น VirusTotal ในเดือนมกราคม 2025 จากประเทศอินเดีย โดยใช้ชื่อว่า "NetworkAnalyzer.tar.gz" ทำให้เกิดข้อสันนิษฐานว่า ผู้ใช้งานอาจถูกหลอกให้ดาวน์โหลดมัลแวร์นี้ ด้วยการปลอมแปลงเป็นเครื่องมือสำหรับแก้ปัญหาเครือข่ายบนระบบ Linux

นอกจากนี้ แผงควบคุมของ Chaos RAT ยังมีช่องโหว่สำคัญ 2 รายการ ได้แก่

1. **Command Injection** CVE-2024-30850 (คะแนน CVSS: 8.8)
2. **Cross-site Scripting (XSS)** CVE-2024-31839 (คะแนน CVSS: 4.8)

นอกจากนี้ แผงควบคุม (admin panel) ที่ใช้สำหรับสร้าง payload และจัดการเครื่องที่ติดมัลแวร์ ถูกพบว่ามีช่องโหว่ command injection ซึ่งสามารถนำไปใช้ร่วมกับช่องโหว่ cross-site scripting เพื่อสั่งรันโค้ดใดๆ บนเซิร์ฟเวอร์ด้วยสิทธิ์ระดับสูงได้ โดยช่องโหว่ทั้งสองนี้ได้รับการแก้ไขโดยผู้ดูแล Chaos RAT แล้วตั้งแต่เดือนพฤษภาคม 2024

แม้ปัจจุบันจะยังไม่ชัดเจนว่าใครอยู่เบื้องหลังการใช้งาน Chaos RAT ในการโจมตีจริง แต่เหตุการณ์นี้แสดงให้เห็นอีกครั้งว่าผู้ไม่หวังดีสามารถนำเครื่องมือโอเพ่นซอร์สมาประยุกต์ใช้เป็นเครื่องมือสำหรับโจมตี ได้อย่างต่อเนื่อง และยากต่อการสืบหาตัวตนของผู้โจมตี (Attribution)

คำแนะนำ (Recommendation)

- หลีกเลี่ยงการดาวน์โหลดไฟล์จากแหล่งที่ไม่น่าเชื่อถือ
- อัปเดตซอฟต์แวร์ป้องกันไวรัสและเปิดใช้ระบบป้องกันแบบ Real-time
- ตรวจสอบกระบวนการทำงานและการเชื่อมต่อภายนอก เพื่อตรวจสอบกระบวนการที่ผิดปกติ
- การจัดทำระบบสำรองข้อมูล (Backup) และแยกระบบสำรองข้อมูลออกจากระบบปฏิบัติการหลัก

ข้อมูลอ้างอิง

- https://thehackernews.com/2025/06/chaos-rat-malware-targets-windows-and.html