วันที่ 12 พฤษภาคม 2569

Quasar Linux RAT ขโมยข้อมูลรับรองของนักพัฒนา เพื่อใช้โจมตีซัพพลายเชนของซอฟต์แวร์

มัลแวร์สำหรับระบบ Linux ที่ไม่เคยถูกเปิดเผยมาก่อน ซึ่งมีชื่อรหัสว่า Quasar Linux RAT (QLNX) กำลังมุ่งเป้าโจมตีเครื่องของนักพัฒนา เพื่อแฝงตัวอยู่ในระบบอย่างเงียบๆ และเปิดทางให้ผู้โจมตีสามารถดำเนินการต่างๆ ได้หลังจากยึดเครื่องสำเร็จ เช่น ขโมยข้อมูลรับรอง (Credentials) ดักจับการพิมพ์จากแป้นพิมพ์ แก้ไขไฟล์ เฝ้าติดตามข้อมูลในคลิปบอร์ด และสร้างช่องทางเชื่อมต่อเครือข่ายแบบซ่อนตัว

มัลแวร์ QLNX มุ่งเป้าโจมตีนักพัฒนาและขโมยข้อมูลรับรอง

นักวิจัย Aliakbar Zahravi และ Ahmed Mohamed Ibrahim จาก Trend Micro ระบุในการวิเคราะห์ทางเทคนิคว่าQLNX มุ่งโจมตีข้อมูลรับรองของนักพัฒนาและทีม DevOps ซึ่งเป็นจุดสำคัญในซัพพลายเชนของซอฟต์แวร์ โมดูลสำหรับขโมยข้อมูลรับรองของมันสามารถดึงข้อมูลลับจากไฟล์สำคัญหลายประเภท เช่น .npmrc (โทเคนของ npm), .pypirc (ข้อมูลเข้าสู่ระบบของPyPI), .git-credentials, .aws/credentials, .kube/config, .docker/config.json, .vault-token, ข้อมูลรับรองของ Terraform,โทเคนของ GitHub CLI และไฟล์ .env

หากข้อมูลเหล่านี้ถูกขโมย ผู้โจมตีอาจใช้เพื่ออัปโหลดแพ็กเกจที่เป็นอันตรายไปยังคลัง NPM หรือ PyPI เข้าถึงโครงสร้างพื้นฐานบนคลาวด์ หรือใช้เป็นทางผ่านไปยังระบบ CI/CD ได้

ความเสี่ยงต่อซัพพลายเชนซอฟต์แวร์

ความสามารถของมัลแวร์ในการรวบรวมข้อมูลรับรองจากหลายแหล่งอย่างเป็นระบบ ทำให้สภาพแวดล้อมของนักพัฒนามีความเสี่ยงอย่างมาก หากผู้โจมตีสามารถติดตั้ง QLNX ลงบนเครื่องของผู้ดูแลแพ็กเกจได้สำเร็จ ก็จะสามารถเข้าถึงกระบวนการเผยแพร่ซอฟต์แวร์ และอัปโหลดเวอร์ชันที่ฝังโค้ดอันตราย ซึ่งอาจส่งผลกระทบต่อผู้ใช้งานและระบบปลายทางจำนวนมากในวงกว้าง

เทคนิคการซ่อนตัวและการควบคุมระยะไกล (Fileless & C2)

QLNX ทำงานแบบ fileless หรือทำงานอยู่ในหน่วยความจำโดยไม่ทิ้งไฟล์หลักไว้บนดิสก์ และปลอมตัวเป็นโปรเซสของระบบ เช่น kworker หรือ ksoftirqdนอกจากนี้ยังสามารถตรวจสอบสภาพแวดล้อมของเครื่องว่าทำงานอยู่ภายในคอนเทนเนอร์หรือไม่ ลบไฟล์บันทึกเหตุการณ์ (Logs) เพื่อปกปิดร่องรอย และตั้งค่าการทำงานอัตโนมัติหลังรีบูตด้วยวิธีมากถึง 7 รูปแบบ เช่น systemd, crontab และการแทรกคำสั่งลงในไฟล์ .bashrc

นอกจากนี้ มัลแวร์ยังส่งข้อมูลที่ขโมยได้กลับไปยังเซิร์ฟเวอร์ของผู้โจมตี และสามารถรับคำสั่งจากระยะไกลเพื่อดำเนินการต่างๆ เช่น รันคำสั่งบนเชลล์ จัดการไฟล์ ฉีดโค้ดเข้าไปในโปรเซส ถ่ายภาพหน้าจอ บันทึกการกดแป้นพิมพ์ สร้าง SOCKS Proxy และ TCP Tunnel รัน Beacon Object Files (BOFs) รวมถึงจัดการเครือข่ายแบบ Peer-to-Peer (P2P)

ขณะนี้ยังไม่ทราบแน่ชัดว่ามัลแวร์ถูกส่งเข้าสู่ระบบด้วยวิธีใด แต่เมื่อสามารถยึดเครื่องได้แล้ว มันจะเข้าสู่ขั้นตอนการทำงานหลัก โดยวนลูปอย่างต่อเนื่องเพื่อพยายามเชื่อมต่อกับเซิร์ฟเวอร์ควบคุมและสั่งการ (C2) ผ่านโปรโตคอล TCP, HTTPS และ HTTP โดย QLNX รองรับคำสั่งทั้งหมด 58 คำสั่ง ซึ่งทำให้ผู้โจมตีสามารถควบคุมเครื่องที่ติดมัลแวร์ได้แทบทุกด้าน

การดักจับข้อมูลและการใช้สถาปัตยกรรม Rootkit

QLNX ยังมีแบ็กดอร์ที่ทำงานร่วมกับ Pluggable Authentication Module (PAM) โดยใช้เทคนิค inline-hook เพื่อดักจับชื่อผู้ใช้และรหัสผ่านในรูปแบบข้อความปกติระหว่างการยืนยันตัวตน บันทึกข้อมูลของเซสชัน SSH ขาออก และส่งข้อมูลทั้งหมดกลับไปยังเซิร์ฟเวอร์ของผู้โจมตี มัลแวร์ยังมีตัวดักจับข้อมูลรับรองอีกชุดหนึ่งที่อาศัย PAM เช่นกัน โดยจะถูกโหลดเข้าไปในทุกโปรแกรมที่เชื่อมโยงแบบไดนามิก เพื่อดึงข้อมูลชื่อบริการ ชื่อผู้ใช้ และโทเคนสำหรับการยืนยันตัวตน

QLNX ใช้สถาปัตยกรรม Rootkit แบบสองชั้น ได้แก่ Rootkit ระดับ Userland ที่อาศัยกลไกLD_PRELOAD ของ Linux Dynamic Linker เพื่อซ่อนไฟล์และโปรเซสของมัลแวร์ และยังมีองค์ประกอบระดับเคอร์เนลที่ใช้เทคโนโลยี eBPF ผ่าน BPF subsystem เพื่อซ่อนโปรเซส ไฟล์ และพอร์ตเครือข่ายจากเครื่องมือทั่วไป เช่น ps, ls และ netstat เมื่อได้รับคำสั่งจากเซิร์ฟเวอร์ C2

บทสรุป

Trend Micro สรุปว่า QLNX ถูกออกแบบมาเพื่อแฝงตัวในระบบระยะยาวและมุ่งขโมยข้อมูลรับรอง สิ่งที่ทำให้มันอันตรายอย่างยิ่งไม่ใช่ความสามารถเพียงอย่างใดอย่างหนึ่ง แต่เป็นการทำงานต่อเนื่องอย่างเป็นระบบ ตั้งแต่เข้ายึดเครื่อง ลบตัวเองออกจากดิสก์ ตั้งค่าการคงอยู่ด้วยหลายวิธี ซ่อนตัวทั้งในระดับผู้ใช้และระดับเคอร์เนล และสุดท้ายขโมยข้อมูลรับรองที่มีความสำคัญสูงที่สุด

ข้อมูลอ้างอิง

May 8, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/05/quasar-linux-rat-steals-developer.html