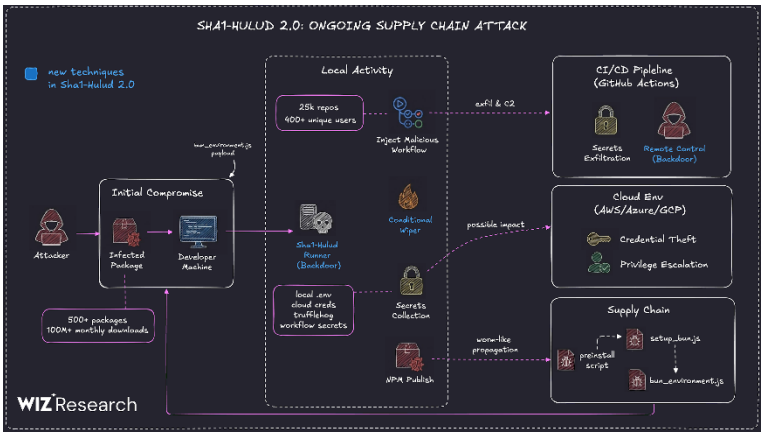
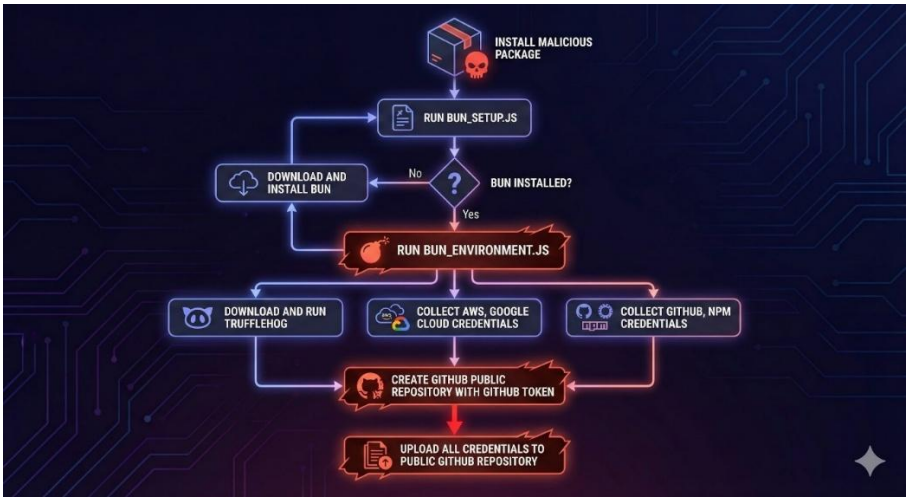
วันที่ 27 พฤศจิกายน 2568

คลื่นโจมตี Sha1-Hulud ที่สองส่งผลกระทบต่อคลังข้อมูลกว่า 25,000 แห่งผ่านการขโมยข้อมูลประจำตัวการติดตั้งล่วงหน้าของ npm



ผู้ให้บริการด้านความปลอดภัยหลายรายกำลังส่งสัญญาณเตือนเกี่ยวกับคลื่นการโจมตีซัพพลายเชนระลอกที่สองที่พุ่งเป้าไปยัง npm registry ซึ่งถูกตั้งชื่อว่า “Sha1-Hulud” หรือ “Sha1-Hulud: The Second Coming” การโจมตีครั้งนี้มีความดุเดือดและมีเป้าหมายที่ร้ายแรงกว่าคลื่นแรกอย่างมาก

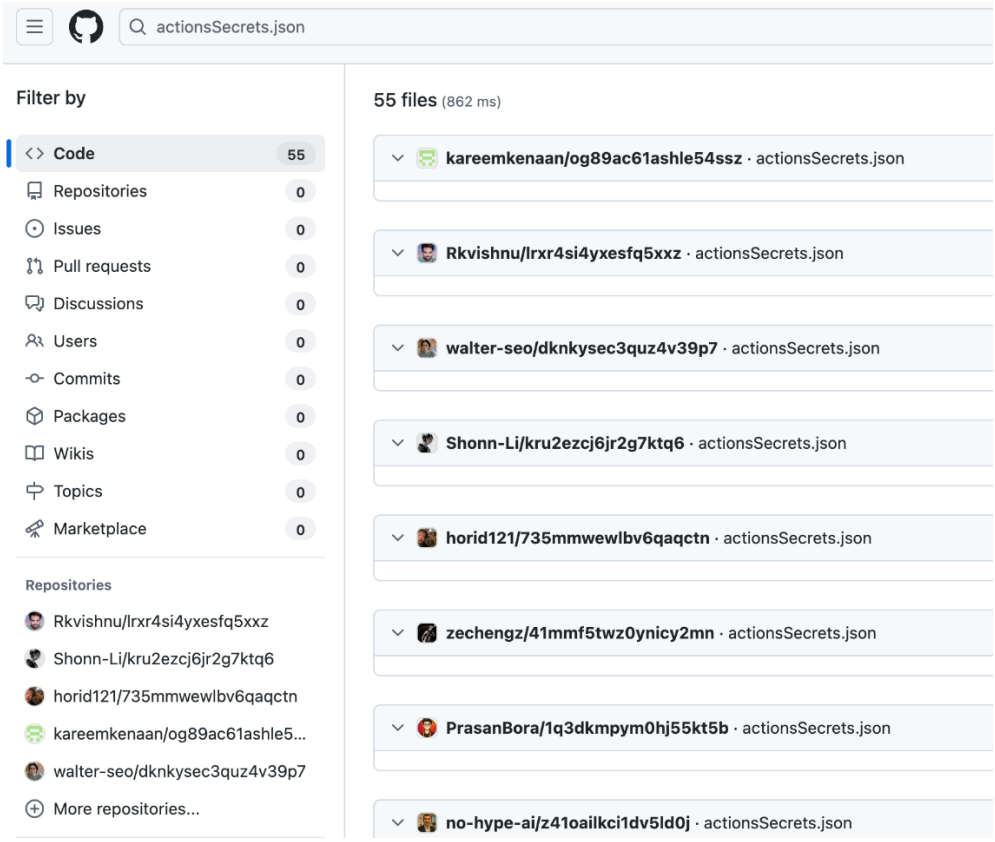
แพ็กเกจ npm หลายร้อยรายการถูกฝังโค้ดอันตรายและอัปโหลดในช่วงวันที่ 21–23 พฤศจิกายน 2025 จากรายงานของ Aikido, HelixGuard, JFrog, Koi Security, ReversingLabs, SafeDep, Socket, Step Security และ Wiz โดยกระทบแพ็กเกจยอดนิยมขององค์กรใหญ่อย่าง Zapier, ENS Domains, PostHog และ Postman รวมถึงโปรเจกต์อื่นๆ อีกมากมาย



กลไกโจมตีที่ยกระดับ: พุ่งเป้า "Pre-install" และ Runtime ของ Bun

แคมเปญนี้ได้เปลี่ยนวิธีการโจมตีที่ชาญฉลาดขึ้นมาก โดยนักวิจัยของ Wiz ชี้ว่ามันรันโค้ดอันตรายในช่วง preinstall ซึ่งทำให้มีโอกาสแพร่กระจายไปยังสภาพแวดล้อมการ build และ runtime ได้มากขึ้นโดยไม่ต้องรอการกระทำของมนุษย์

- จุดเริ่มการโจมตี: ผู้โจมตีแทรกสคริปต์ preinstall ("setup_bun.js") ลงในไฟล์ package.json ซึ่งถูกตั้งให้ติดตั้งหรือค้นหา runtime ของ Bun แบบลับๆ พร้อมทั้งรันสคริปต์อันตราย ("bun_environment.js") ที่ซ่อนอยู่ภายใน
- เป้าหมายหลัก: เหมือนกับคลื่นแรก คือการใช้เครื่องมือ TruffleHog เพื่อสแกนและขโมยข้อมูลลับทั้งหมดจากเครื่องนักพัฒนา เช่น NPM Tokens, AWS/GCP/Azure credentials และ Environment Variables
- การแพร่กระจายอัตโนมัติ (Self-Propagation): มัลแวร์จะดึงรายการแพ็กเกจสูงสุด 100 รายการที่เชื่อมโยงกับ npm token ที่ใช้งานได้ จากนั้นก็แทรกสคริปต์อันตราย ดันเลขเวอร์ชันแพ็กเกจ (x.y.z ⟶ x.y.z+1) แล้วอัปโหลดขึ้น npm repository ทันที การแพร่กระจายแบบอัตโนมัติอย่างกว้างขวางนี้กระทบกว่า 27,000 รีโพ จากผู้ใช้งานประมาณ 350 ราย และมีรีโพใหม่ถูกสร้างเพิ่มกว่า 1,000 รีโพทุกๆ 30 นาที ในช่วงหลายชั่วโมงที่ผ่านมา



การสร้าง Persistence และโหมด "ทำลายล้าง"

แคมเปญ Sha1-Hulud 2.0 มีการสร้างช่องทางการเข้าถึงที่ซับซ้อน และมีฟังก์ชัน “ทำลายล้าง” ที่น่ากลัวมาก (Koi Security)

1. ช่องทางการเข้าถึงแบบถาวร (Persistence)

- Self-hosted Runner: มัลแวร์จะลงทะเบียนเครื่องที่ติดเชื้อให้เป็น self-hosted runner ชื่อ “SHA1HULUD”
- GitHub Workflow Backdoor: จากนั้นจะเพิ่ม workflow ชื่อ .github/workflows/discussion.yaml ที่มีช่องโหว่การแทรกคำสั่ง และถูกตั้งให้รันบน self-hosted runner เท่านั้น ซึ่งอนุญาตให้ผู้โจมตีสามารถรันคำสั่งใดก็ได้บนเครื่องที่ติดเชื้อเพียงแค่เปิด discussion ในรีโพ GitHub
- Exfiltration ผ่าน GitHub: มัลแวร์จะดูดข้อมูลลับจาก GitHub Actions ทั้งหมด อัปโหลดเป็น artifact ชื่อ actionsSecrets.json ไปยังรีโพสำหรับ exfiltration หลังจากนั้น workflow ที่สร้างไว้จะถูกลบออกเพื่อกลบรอย
- การเข้ารหัสและฟื้นตัว: ข้อมูลที่ถูกส่งออกจะถูก เข้ารหัส Base64 ซ้อนกันสามชั้น ก่อนอัปโหลด มัลแวร์จะค้นหารีโพ GitHub สาธารณะที่มีข้อความสัญญาณ “Sha1-Hulud: The Second Coming.” เพื่อดึง GitHub access token ที่ถูกซ่อนไว้มาใช้เป็นข้อมูลยืนยันตัวตนหลัก ทำให้มัลแวร์สามารถ ฟื้นตัวได้เอง หากเหยื่อลบรีโพอันตรายเก่าๆ ออก

2. การยกระดับสิทธิ์และการทำลายข้อมูล

- ยกระดับสิทธิ์สู่ Root: มัลแวร์ยังถูกพบว่าสามารถยกระดับสิทธิ์เป็น root บน Linux โดยรันคำสั่ง Docker เพื่อ mount root filesystem ของเครื่องโฮสต์เข้าไปในคอนเทนเนอร์ที่มีสิทธิ์สูง จากนั้นก๊อปปี้ไฟล์ sudoers อันตรายเข้าไป ทำให้ผู้โจมตีสามารถใช้คำสั่ง root ได้โดยไม่ต้องใส่รหัสผ่าน
- โหมดทำลายล้าง (Destructive Mode): Koi Security ระบุว่ามัลแวร์จะพยายาม ลบโฟลเดอร์ home ทั้งหมดของเหยื่อ หากไม่สามารถยืนยันตัวตนหรือสร้างความคงอยู่ (persistence) ได้ เงื่อนไขที่ทำให้โหมดลบข้อมูลถูกกระตุ้น คือ:
    - ไม่สามารถยืนยันตัวตนกับ GitHub ได้
    - ไม่สามารถสร้างรีโพ GitHub ได้
    - ไม่สามารถดึง GitHub token ได้
    - ไม่สามารถหา npm token ได้

ข้อแนะนำเร่งด่วนในการบรรเทาความเสี่ยง

Justin Moore จาก Palo Alto Networks Unit 42 ชี้ว่า แคมเปญนี้เป็นการยกระดับครั้งใหญ่ องค์กรควรดำเนินการทันที

1. สแกนและลบแพ็กเกจ: สแกน endpoint ทั้งหมดเพื่อหาแพ็กเกจที่ได้รับผลกระทบและลบเวอร์ชันที่ถูกเจาะออกทันที
2. เปลี่ยนข้อมูลรับรอง: เปลี่ยน NPM Tokens และข้อมูลรับรอง AWS/GCP/Azure credentials ใหม่ทั้งหมด
3. ตรวจสอบ Persistence: ตรวจสอบรีโพ GitHub ขององค์กรว่ามีช่องทางฝังตัวหรือ persistence หรือไม่ โดยเฉพาะไฟล์ต้องสงสัยใน .github/workflows/ (เช่น shai-hulud-workflow.yml) และตรวจหา branch ที่ไม่คาดคิด

ข้อมูลอ้างอิง

Nov 24, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/11/second-sha1-hulud-wave-affects-25000.html