วันที่ 10 มีนาคม 2569

แพ็กเกจ npm อันตรายปลอมตัวเป็นตัวติดตั้ง OpenClaw เพื่อติดตั้ง RAT และขโมยข้อมูลสำคัญจาก macOS

นักวิจัยด้านความปลอดภัยไซเบอร์ได้ตรวจพบภัยคุกคามครั้งใหม่ใน npm registry เมื่อมีการค้นพบแพ็กเกจที่เป็นอันตรายซึ่งแฝงตัวมาในชื่อ **"@openclaw-ai/openclawai"** โดยหลอกว่าเป็นตัวติดตั้งสำหรับ OpenClaw แต่แท้จริงแล้วมีเป้าหมายเพื่อติดตั้งมัลแวร์ประเภท รีโมตแอ็กเซสโทรจัน (RAT) และกวาดข้อมูลสำคัญจากเครื่องของเหยื่อ

แพ็กเกจนี้ถูกอัปโหลดโดยผู้ใช้ที่ชื่อ "openclaw-ai" เมื่อวันที่ 3 มีนาคม 2026 แม้จะเพิ่งปรากฏขึ้นไม่นานแต่กลับมียอดดาวน์โหลดแล้วถึง 178 ครั้ง และที่น่ากังวลคือไลบรารีดังกล่าวยังคงเปิดให้ดาวน์โหลดได้อยู่ในขณะที่รายงานนี้ถูกเผยแพร่

กลไกการทำงานของมัลแวร์ "GhostLoader"

บริษัท JFrog ผู้ค้นพบระบุว่าแพ็กเกจนี้ถูกออกแบบมาเพื่อโจมตีอย่างรอบด้าน ตั้งแต่การขโมยข้อมูลล็อกอิน, ข้อมูลเบราว์เซอร์, กระเป๋าเงินคริปโต, กุญแจ SSH ไปจนถึงฐานข้อมูล Apple Keychain และประวัติ iMessage นอกจากนี้ยังมีการติดตั้ง RAT แบบถาวรที่ช่วยให้แฮกเกอร์ควบคุมเครื่องจากระยะไกล ใช้งาน SOCKS5 proxy และโคลนเซสชันของเบราว์เซอร์ได้แบบเรียลไทม์

นักวิจัยด้านความปลอดภัยให้ความเห็นว่า มัลแวร์ตัวนี้มีชื่อเรียกในตัวเองว่า **"GhostLoader"** โดยมีความน่าสนใจตรงที่สามารถรวบรวมข้อมูลได้มหาศาล และมีโครงสร้างการควบคุมแบบ C2 (Command-and-Control) ที่ค่อนข้างซับซ้อน

กลไกอันตรายจะเริ่มทำงานผ่าน postinstall hook ซึ่งจะสั่งติดตั้งแพ็กเกจใหม่แบบ global ด้วยคำสั่ง npm i -g @openclaw-ai/openclawai ทันที เมื่อเสร็จสิ้น ไฟล์ไบนารีของ OpenClaw จะถูกตั้งค่าให้ชี้ไปที่ไฟล์ scripts/setup.js ผ่าน property ที่ชื่อว่า "bin" ในไฟล์ package.json ซึ่งตามหลักการแล้ว field bin นี้มีไว้กำหนดไฟล์ executable เพื่อให้โปรแกรมสามารถเรียกใช้งานผ่าน command-line ได้จากทุกที่ในระบบนั่นเอง

ขั้นตอนการฝังตัวและข้ามระบบป้องกัน

ไฟล์ setup.js ทำหน้าที่เป็นตัว dropper ระยะแรก โดยจะสร้างหน้าต่าง command-line ปลอมที่มีแถบความคืบหน้า (Progress bar) เพื่อหลอกให้เหยื่อตายใจว่ากำลังติดตั้ง OpenClaw จริงๆ หลังจากนั้นจะมีการแสดงหน้าต่างอนุญาต iCloud Keychain ปลอมขึ้นมาเพื่อหลอกให้ผู้ใช้กรอกรหัสผ่านของระบบ

ในขณะเดียวกัน สคริปต์จะแอบดึง payload JavaScript ระยะที่สอง ที่ถูกเข้ารหัสมาจากเซิร์ฟเวอร์ C2 (trackpipe[.]dev) เพื่อนำมาถอดรหัสและรันเป็น child process อยู่เบื้องหลัง โดยไฟล์ชั่วคราวนี้จะถูกลบออกภายใน 60 วินาทีเพื่อทำลายหลักฐาน

JFrog เสริมว่า หากมัลแวร์ไม่สามารถเข้าถึงโฟลเดอร์ Safari ได้เนื่องจากติดสิทธิ์การเข้าถึง มันจะแสดงหน้าต่าง AppleScript เพื่อขอให้ผู้ใช้อนุญาต Full Disk Access ให้กับ Terminal พร้อมคำแนะนำทีละขั้นตอน ซึ่งหากเหยื่อหลงเชื่อและอนุญาต มัลแวร์จะสามารถขโมยข้อมูลจาก Apple Notes, iMessage, ประวัติ Safari และข้อมูลจาก Mail ได้ทันที

เจาะลึกความสามารถในการขโมยข้อมูลและควบคุมระยะไกล

JavaScript ระยะที่สองมีความยาวกว่า 11,700 บรรทัด ทำหน้าที่เป็นเฟรมเวิร์กสำหรับขโมยข้อมูลและควบคุมเครื่องแบบ RAT เต็มรูปแบบ โดยสามารถเข้าถึงข้อมูลที่หลากหลาย เช่น:

- ข้อมูลจาก macOS Keychain รวมถึงฐานข้อมูล iCloud Keychain ทั้งหมด
- รหัสผ่าน คุกกี้ และบัตรเครดิตจากเบราว์เซอร์ตระกูล Chromium (Chrome, Edge, Brave, Opera ฯลฯ)
- Seed phrase และข้อมูลจากแอปกระเป๋าเงินคริปโต
- กุญแจ SSH และข้อมูลบัญชีสำหรับนักพัฒนาและคลาวด์ เช่น AWS, Microsoft Azure, Google Cloud, Kubernetes, Docker และ GitHub
- ข้อมูลส่วนตัวที่ถูกป้องกันด้วย Full Disk Access เช่น Apple Notes และบัญชี Apple

ข้อมูลทั้งหมดจะถูกบีบอัดเป็นไฟล์ tar.gz และส่งออกไปยังเซิร์ฟเวอร์ C2 ผ่านช่องทางต่างๆ เช่น Telegram Bot API และ GoFile.io

ฟีเจอร์อันตราย เฝ้าดู Clipboard และ Browser Cloning

นอกจากนี้ มัลแวร์ยังยกระดับความน่ากลัวด้วยการเข้าสู่โหมด **daemon แบบถาวร** เพื่อเฝ้าดูข้อมูลใน clipboard ของผู้ใช้ทุกๆ 3 วินาที โดยจะส่งข้อมูลออกทันทีหากพบรูปแบบที่ตรงกับแพตเทิร์นสำคัญ 9 แบบ เช่น private key, WIF key, SOL private key, RSA private key, ที่อยู่ Bitcoin, ที่อยู่ Ethereum ไปจนถึงกุญแจสำคัญอย่าง AWS key, OpenAI key และ Strike key

ความร้ายกาจของมัลแวร์ตัวนี้ยังครอบคลุมถึงการตรวจสอบโปรเซสที่กำลังทำงานอยู่ในเครื่อง การสแกนข้อความ iMessage ที่เข้ามาแบบเรียลไทม์ และการรอรับคำสั่งจากเซิร์ฟเวอร์ C2 เพื่อปฏิบัติการต่างๆ ได้อย่างอิสระ ดังนี้:

- รันคำสั่ง shell ใดๆ ก็ได้, ดาวน์โหลดมัลแวร์เพิ่มเติม หรืออัปโหลดไฟล์จากเครื่องเหยื่อออกไป
- สั่งเปิด URL บนเบราว์เซอร์ของเหยื่อ หรือเปิด-ปิด SOCKS5 proxy เพื่อใช้เครื่องเป็นทางผ่าน
- แสดงรายการเบราว์เซอร์ที่ติดตั้ง, สั่งโคลนโปรไฟล์เบราว์เซอร์และเปิดในโหมด headless หรือสั่งหยุดการโคลน
- สามารถสั่งอัปเดตตัวมัลแวร์เอง หรือสั่งลบตัวเองออกจากระบบเพื่อทำลายหลักฐาน

ที่สำคัญที่สุดคือความสามารถในการโคลนเบราว์เซอร์ โดยผู้โจมตีสามารถสั่งรัน Chromium ในโหมด headless (ทำงานเบื้องหลังโดยไม่มีหน้าต่าง) โดยใช้โปรไฟล์เดิมของเหยื่อที่มีคุกกี้และเซสชันล็อกอินอยู่แล้ว ทำให้แฮกเกอร์เข้าถึงบัญชีต่างๆ ได้ทันทีโดยไม่ต้องใช้รหัสผ่าน

JFrog ทิ้งท้ายว่าแพ็กเกจ @openclaw-ai/openclawai คือการมัดรวมเทคนิคอันตรายไว้ในหนึ่งเดียว ทั้งการหลอกลวงผู้ใช้ การส่ง payload เข้ารหัส การขโมยข้อมูลมหาศาล และการฝังตัวของ RAT แบบถาวร

จุดตายสำคัญคือ ตัวติดตั้ง CLI และหน้าต่างขออนุญาต Keychain ปลอม ที่ทำออกมาได้สมจริงมาก จนนักพัฒนาหลายคนหลงเชื่อกรอกรหัสผ่านระบบ เปิดทางให้ผู้โจมตีเข้าถอดรหัสข้อมูลใน macOS Keychain และรหัสผ่านเบราว์เซอร์ ซึ่งปกติระบบปฏิบัติการจะป้องกันไว้อย่างดี

ข้อมูลอ้างอิง

Mar 9, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/03/malicious-npm-package-posing-as.html