วันที่ 3 มีนาคม 2569

พบช่องโหว่ 'ClawJacked' ยึด AI Agent ผ่านหน้าเว็บ – OpenClaw สั่งอัปเดตแพตช์ทันที

ล่าสุดแพลตฟอร์ม AI agent อย่าง OpenClaw ได้ออกแพตช์แก้ไขช่องโหว่ร้ายแรงที่ชื่อว่า "ClawJacked" ซึ่งหากถูกโจมตีสำเร็จ ผู้ไม่หวังดีจะสามารถเชื่อมต่อเข้ากับ AI agent ที่ทำงานอยู่บนเครื่องของคุณ และเข้าควบคุมการทำงานได้ทั้งหมด

รายงานจาก Oasis Security ระบุว่าช่องโหว่นี้ไม่ได้เกี่ยวกับปลั๊กอินหรือสิ่งที่ผู้ใช้ติดตั้งเพิ่ม แต่เป็นจุดอ่อนใน OpenClaw gateway เวอร์ชันพื้นฐานโดยตรง

ทำความรู้จักกับ "ClawJacked"

การโจมตีนี้มุ่งเป้าไปที่นักพัฒนาที่ใช้งาน OpenClaw บนแล็ปท็อป (ผ่าน localhost) โดยอาศัยจังหวะที่ผู้ใช้เผลอเข้าเว็บไซต์ที่ถูกสร้างขึ้นเพื่อโจมตี (ผ่าน Social Engineering หรือวิธีอื่นๆ)

ลำดับการโจมตีมีขั้นตอนดังนี้:

1. **การเชื่อมต่อเว็บไซต์อันตรายฝัง JavaScript**: สคริปต์พยายามเปิดการเชื่อมต่อ WebSocket ไปยัง localhost ที่พอร์ตของ OpenClaw gateway
2. **เดารหัสผ่าน:** สคริปต์จะสุ่มรหัสผ่านของ gateway โดยอาศัยจุดอ่อนที่ระบบ ไม่มีการจำกัดจำนวนครั้งในการลอง (rate limiting)
3. **เข้ายึดระบบ:** เมื่อเดารหัสผ่านสำเร็จ สคริปต์จะลงทะเบียนตัวเองเป็น "อุปกรณ์ที่เชื่อถือได้" ทันที โดยที่ระบบจะอนุมัติให้อัตโนมัติและไม่แจ้งเตือนผู้ใช้
4. **ควบคุม AI agent ได้ทั้งหมด:** ผู้โจมตีจะสามารถสั่งงาน AI agent, ดึงข้อมูลการตั้งค่า, ตรวจสอบโหนด หรือแม้แต่อ่านไฟล์ log ของระบบได้ทั้งหมด

สาเหตุหลัก: เบราว์เซอร์ปกติจะไม่บล็อกการเชื่อมต่อ WebSocket แบบข้ามแหล่งที่มา (Cross-origin) และตัว gateway เองก็ไว้ใจ การเชื่อมต่อจาก localhost มากเกินไป จนลดมาตรการรักษาความปลอดภัยลง

สิ่งที่คุณต้องทำทันที

- **อัปเดตด่วน:** ทาง OpenClaw ได้ปล่อยแพตช์แก้ไขในเวอร์ชัน 2026.2.25 เมื่อวันที่ 26 กุมภาพันธ์ 2026 แล้ว โปรดอัปเดตทันที
- **ตรวจสอบสิทธิ์:** หมั่นตรวจสอบสิทธิ์การเข้าถึงของ AI agent และควบคุมการใช้งานบัญชีที่ไม่ใช่มนุษย์ (agentic identities) ให้เข้มงวดขึ้น

สรุปภาพรวมความเสี่ยงอื่นๆ ของ OpenClaw

เหตุการณ์นี้เกิดขึ้นในช่วงที่ระบบนิเวศของ OpenClaw กำลังถูกเพ่งเล็งด้านความปลอดภัยอย่างหนัก เนื่องจาก AI agent มักมีสิทธิ์เข้าถึงข้อมูลในองค์กรสูง

1. ปัญหาด้านความปลอดภัยที่ผ่านมา

- Log Contamination (เวอร์ชัน 2026.2.13): ช่องโหว่ที่ทำให้ผู้โจมตีเขียนข้อมูลอันตรายลงในไฟล์ log ผ่าน WebSocket เพื่อหลอกล่อให้ agent อ่านและตีความผิด (Prompt Injection ทางอ้อม) ทำให้เกิดพฤติกรรมที่ไม่ตั้งใจ เช่น การเปิดเผยข้อมูล หรือการตัดสินใจที่ผิดพลาด
- รายการช่องโหว่อื่นๆ: มีการแก้ไข CVE จำนวนมาก (เช่น CVE-2026-25593, 24763, 25157, 25475, 26319, 26322, 26329) ซึ่งครอบคลุมตั้งแต่การรันโค้ดจากระยะไกล ไปจนถึงการเข้าถึงไฟล์ที่ควรเป็นความลับ ทั้งหมดได้รับการแก้ไขแล้วในเวอร์ชันที่ปลอดภัย 2026.1.20, 2026.1.29, 2026.2.1, 2026.2.2 และ 2026.2.14

2. มัลแวร์ใน ClawHub (Marketplace)

งานวิจัยพบว่ามี Skill อันตรายบน ClawHub ถูกใช้แพร่มัลแวร์ Atomic Stealer บน macOS โดยกลุ่มอาชญากร Cookie Spider

- เทคนิคหลอกลวง: ใช้ไฟล์ SKILL.md ที่ดูปกติและผ่านการตรวจจาก VirusTotal แต่จะใช้คำสั่งแฝงให้ LLM ดาวน์โหลดมัลแวร์จาก IP 91.92.242.30
- แคมเปญ Social Engineering: พบผู้ใช้ชื่อ @liuhui1010 หลอกให้รันคำสั่งใน Terminal โดยอ้างว่าเพื่อแก้ปัญหาบน macOS
- สถิติที่น่าตกใจ: Straiker วิเคราะห์ Skill 3,505 รายการ พบว่าเป็นมัลแวร์ถึง 71 รายการ บางส่วนแฝงมาขโมยเหรียญคริปโตโดยเฉพาะ

การโจมตีแบบ Agent-to-Agent

พบการใช้ Skill ชื่อ bob-p2p-beta และ runware โดยผู้โจมตีชื่อ "26medias" และ "BobVonNeumann" หลอกล่อ AI ตัวอื่นบนโซเชียลเน็ตเวิร์ก Moltbook ให้ขโมย Private Key ของกระเป๋าเงิน Solana หรือโอนเงินผ่านระบบของผู้โจมตี โดยอาศัยความเชื่อใจที่ AI มีต่อกัน

3. คำแนะนำจาก Microsoft

Microsoft เตือนว่า อย่าติดตั้ง OpenClaw บนเครื่องที่ใช้งานทั่วไป เพราะมีความเสี่ยงสูงต่อการรั่วไหลของข้อมูลรับรองและการยึดเครื่อง

แนวทางปฏิบัติสำหรับองค์กร:

- ติดตั้งในสภาพแวดล้อมที่แยกส่วน (Isolated) เช่น เครื่องเสมือน (VM) หรือเครื่องเฉพาะ
- ใช้บัญชีสิทธิ์ต่ำ (Low-privileged account)
- จำกัดการเข้าถึงข้อมูลเฉพาะข้อมูลที่ไม่สำคัญ
- มีระบบเฝ้าระวังต่อเนื่องและแผนสำรองข้อมูลเสมอ

ข้อมูลอ้างอิง

Feb 28, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/02/clawjacked-flaw-lets-malicious-sites.html