แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แรนซัมแวร์ JADEPUFFER ใช้ AI Agent ในการโจมตีระบบแบบอัตโนมัติ

วันที่แจ้งเตือน 7 กรกฎาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบกรณีนักวิจัยรายงานเกี่ยวกับแรนซัมแวร์ JADEPUFFER ซึ่งเป็นการใช้ AI Agent ในการโจมตีทางไซเบอร์แบบอัตโนมัติตลอดกระบวนการ

การโจมตีได้ใช้ประโยชน์จากช่องโหว่ CVE-2025-3248 เป็นช่องโหว่ประเภท Remote Code Execute ใน Langflow (Open source platform) ที่ผู้ไม่หวังดีเข้าโจมตีโดยข้ามผ่านการยืนยันตัวตนได้ จากนั้น AI Agent จะรวบรวมข้อมูลภายในระบบ ค้นหาและรวบรวมข้อมูลสภาพแวดล้อมภายใน ข้อมูล Credential และ API Keys รวมถึงตรวจสอบบริการต่าง ๆ ก่อนติดตั้ง Cron job เพื่อให้สามารถเชื่อมต่อและส่งข้อมูลให้ผู้ไม่หวังดีอย่างต่อเนื่อง จากนั้นเคลื่อนย้ายไปยังระบบอื่นภายในเครือข่าย ก่อนใช้แรนซัมแวร์เข้ารหัสข้อมูล การตั้งค่าระบบ และแสดงข้อความเรียกค่าไถ่ พร้อมทั้งปรับเปลี่ยนวิธีการโจมตีตามสถานการณ์ได้เอง เหตุการณ์ดังเกล่าวแสดงให้เห็นว่า AI Agent สามารถโจมตีที่ซับซ้อนได้เอง และโจมตีทางไซเบอร์ได้อย่างรวดเร็วและรุนแรงมากขึ้น

เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้น ขอให้ผู้ประกอบธุรกิจพิจารณาดำเนินการมาตรการด้านการรักษาความมั่นคงปลอดภัย อัปเดตแพตช์ หลีกเลี่ยงการเปิดใช้บริการผ่านอินเตอร์เน็ตที่ไม่จำเป็น พร้อมทั้งจำกัดสิทธิ์การเข้าถึงระบบและบัญชีผู้ใช้งานที่มีสิทธิ์สูง ตรวจสอบการจัดเก็บ Credential และ API Keys รวมถึงเฝ้าระวังกิจกรรมที่ผิดปกติ และติดตามข่าวสารด้านภัยคุกคามอย่างต่อเนื่อง เพื่อช่วยลดความเสี่ยงจากการโจมตีโดยใช้ AI Agent

ข้อมูลอ้างอิง

1. https://nvd.nist.gov/vuln/detail/CVE-2025-3248
2. https://www.sysdig.com/blog/jadepuffer-agentic-ransomware-for-automated-database-extortion
3. https://www.bleepingcomputer.com/news/security/jadepuffer-ransomware-used-ai-agent-to-automate-entire-attack/

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ