แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แคมเปญมัลแวร์ PlugX ใช้เว็บไซต์ปลอมหลอกติดตั้งโปรแกรม Claude AI

วันที่แจ้งเตือน 17 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการรายงานเกี่ยวกับแคมเปญใช้เว็บไซต์ปลอม แอบอ้างบริการ Claude AI ของ Anthropic เพื่อหลอกให้ผู้ใช้งานดาวน์โหลดโปรแกรมติดตั้งที่ฝังมัลแวร์ บนระบบปฏิบัติการ Windows

การโจมตีดังกล่าวจะใช้หน้าเว็บไซต์ปลอมแจกจ่ายไฟล์ติดตั้งในรูปแบบ ZIP ซึ่งภายในประกอบด้วยโปรแกรมเลียนแบบการติดตั้งซอฟต์แวร์จริง โดยเมื่อผู้ใช้งานทำการติดตั้ง โปรแกรมจะทำงานได้ตามปกติ แต่มีการหลีกเลี่ยงการตรวจจับ และรันสคริปต์ VBScript เพื่อติดตั้งมัลแวร์ลงในระบบ การโจมตีจะใช้เทคนิค DLL sideloading โดยอาศัยไฟล์ executable ที่ถูกต้องและมีการลงนามดิจิทัลเพื่อโหลดไฟล์ DLL ที่ถูกสร้างขึ้น ทำการถอดรหัส payload และติดตั้งมัลแวร์ PlugX (Remote Access Trojan :RAT) ที่สามารถควบคุมระบบของเหยื่อจากระยะไกล รวมถึงมีการเชื่อมต่อไปยังเซิร์ฟเวอร์ Command-and-Control (C2) อย่างรวดเร็วหลังการติดตั้ง เพื่อรับคำสั่งจากผู้ไม่หวังดี

สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบพิจารณาดำเนินมาตรการที่เหมาะสม โดยสร้างความตระหนักให้แก่พนักงานเกี่ยวกับภัยคุกคามเฝ้าระวัง และติดตามความผิดปกติในระบบงานต่าง ๆ วิเคราะห์บันทึกเหตุการณ์ (Log Monitoring) อย่างต่อเนื่อง และควรพิจารณาทบทวนและปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยของบริษัทให้ทันต่อเหตุภัยคุกคามไซเบอร์ที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อหน่วยงานในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1. https://securityaffairs.com/190754/malware/fake-claude-ai-installer-abuses-dll-sideloading-to-deploy-plugx.html
2. https://www.malwarebytes.com/blog/scams/2026/04/fake-claude-site-installs-malware-that-gives-attackers-access-to-your-computer