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

แจ้งเตือนกรณีพบการปลอมผลลัพธ์จาก AI Chatbot และ Search Engine หลอกเหยื่อเพื่อติดตั้งมัลแวร์

วันที่แจ้งเตือน 12 มิถุนายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

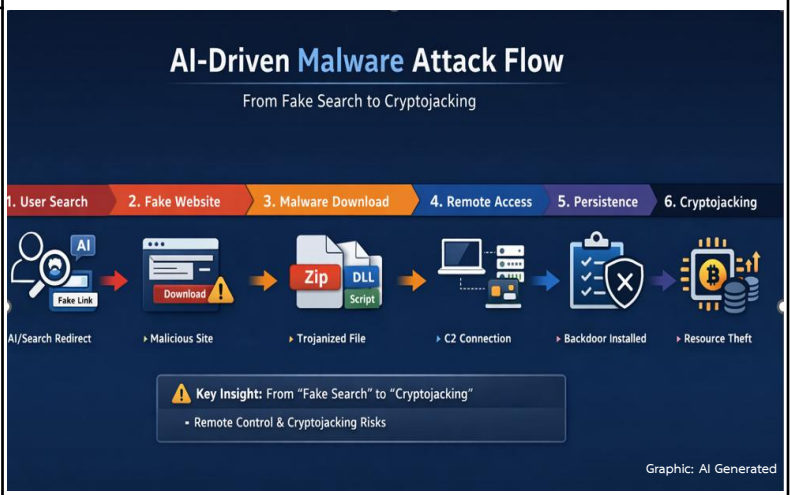
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้เผยแพร่รายงานเกี่ยวกับภัยคุกคามทางไซเบอร์ กรณีผู้ไม่หวังดีใช้เทคนิคการปลอมผลลัพธ์จาก AI Chatbot และ Search Engine นำไปสู่การติดตั้งมัลแวร์ โดยมีรายละเอียดดังนี้

การโจมตี	รายละเอียด	ผลกระทบ
ผู้ไม่หวังดีใช้เทคนิค Search Engine Optimization (SEO) Poisoning และ AI Manipulation เพื่อควบคุมผลลัพธ์การค้นหา และ AI Chatbot เพื่อหลอกให้ผู้ใช้งานดาวน์โหลดโปรแกรมจากเว็บไซต์ที่เลียนแบบเว็บไซต์ซอฟต์แวร์ยอดนิยม และมุ่งหวังเข้าควบคุมเครื่องเหยื่อ หรือเพื่อขุดเหรียญ Crypto (Cryptojacking)	1) สร้างเว็บไซต์ปลอม 2) ดันเว็บไซต์ปลอมให้ติดอันดับผ่านผลลัพธ์ที่ได้จาก SEO และ AI Chatbot (แนะนำลิงก์ปลอม) 3) หลอกดาวน์โหลดไฟล์ติดตั้งหรือเรียกใช้สคริปต์อันตราย 4) ติดตั้ง ScreenConnect/ Remote Access 5) ใช้ PowerShell/.NET โหลดมัลแวร์เพิ่มเติม 6) ฝัง Persistence เพื่อให้มัลแวร์ทำงานต่อเนื่อง 7) ใช้ CPU/GPU เพื่อขุดเหรียญ Crypto	ด้านธุรกิจ: เสี่ยงข้อมูลรั่วไหล กระทบต่อการให้บริการ และเสียชื่อเสียง ด้านเทคนิค: เครื่องทำงานช้า CPU/GPU Usage สูง และระบบอาจถูกควบคุม ด้านปฏิบัติการ: เพิ่มภาระตรวจสอบ และ Incident Response

คำแนะนำด้านความมั่นคงปลอดภัย

- ควรดาวน์โหลดซอฟต์แวร์จากเว็บไซต์ทางการของผู้พัฒนาเท่านั้น
- หลีกเลี่ยงการดาวน์โหลดโปรแกรมจากลิงก์ที่ได้รับผ่าน AI Chatbot หรือ Search Engine
- ตรวจสอบ URL และใบรับรองเว็บไซต์ก่อนดาวน์โหลดไฟล์ทุกครั้ง
- ใช้งานระบบ Endpoint Detection and Response (EDR) หรือระบบตรวจจับภัยคุกคาม
- กำหนดนโยบายควบคุมการใช้งาน PowerShell และ Script Execution ภายในองค์กร
- เฝ้าระวังการใช้งานทรัพยากรเครื่องผิดปกติ เช่น CPU หรือ GPU Usage สูงอย่างต่อเนื่อง
- จัดอบรมสร้างความตระหนักรู้ด้านภัยคุกคามไซเบอร์แก่ผู้ใช้งาน

ภาพจำลองการโจมตี



ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 9 มิ.ย. 2569
2. https://thehackernews.com/2026/05/ai-chatbot-recommendations-redirect.html?
3. https://www.microsoft.com/en-us/security/blog/2026/05/26/poisoned-search-results-gpu-mining-cryptojacking-campaign-abusing-screenconnect-microsoft-net-utilities/?/