วันที่ 2 มิถุนายน 2568

อาชญากรไซเบอร์อาศัยเครื่องมือ AI ปลอม เพื่อหลอกเหยื่อให้ติดตั้งแรนซัมแวร์และมัลแวร์

Executive Summary

นักวิจัยด้านความปลอดภัยจาก Cisco Talos ออกมาเตือนภัยเกี่ยวกับการระบาดของมัลแวร์และแรนซัมแวร์ในรูปแบบใหม่ที่ตอนนี้เริ่มแพร่กระจายผ่านเครื่องมือ AI ปลอมบนเว็บไซต์ต่างๆ โดยหลอกให้ผู้ใช้งานทั่วไปเข้าใจว่าเป็นซอฟต์แวร์ AI ของจริง และดาวน์โหลดไปติดตั้งบนคอมพิวเตอร์ของตัวเอง แนวโน้มนี้เริ่มต้นตั้งแต่ปีที่แล้วจากการใช้เนื้อหา Deepfake หลอกเหยื่อ และขณะนี้ได้พัฒนาเป็นการสร้างเว็บไซต์เครื่องมือ AI ปลอมที่ทำ Poisoned SEO และโฆษณามัลแวร์ เพื่อให้ติดอันดับการค้นหาบน Google ซึ่งจะส่งผลกระทบต่อระบบอย่างรุนแรงในหลายรูปแบบ

CyberLock เป็นแรนซัมแวร์ที่ทำงานผ่าน PowerShell ถูกแพร่กระจายผ่านเว็บไซต์ปลอมชื่อ novaleadsai[.]com โดยอ้างว่าเป็นแพลตฟอร์ม AI ชื่อดัง พร้อมเสนอบริการทดลองใช้ฟรี 12 เดือนเพื่อจูงใจให้เหยื่อดาวน์โหลดตัวติดตั้ง .NET ซึ่งเมื่อรันแล้วจะติดตั้งแรนซัมแวร์ที่เข้ารหัสไฟล์หลายพาร์ติชัน พร้อมเพิ่มนามสกุล .cyberlock และเรียกค่าไถ่ 50,000 ดอลลาร์ในสกุลเงิน Monero โดยอ้างว่าจะนำเงินไปใช้เพื่อการกุศลในปาเลสไตน์ ยูเครน แอฟริกา และเอเชีย

Lucky_Gh0$t คือแรนซัมแวร์สายพันธุ์ใหม่ที่พัฒนาจาก Yashma/Chaos ซึ่งใช้ไฟล์ติดตั้งปลอมชื่อ ChatGPT 4.0 เวอร์ชั่นเต็ม - Premium.exe ที่บรรจุอยู่ในไฟล์เก็บถาวรแบบ Self-Extracting Archive (SFX) พร้อมเครื่องมือ AI ของ Microsoft ที่ถูกต้อง เพื่อหลบเลี่ยงการตรวจจับจากโปรแกรมป้องกันไวรัส มัลแวร์ตัวนี้จะเข้ารหัสเฉพาะไฟล์ที่มีขนาดไม่เกิน 1.2GB และลบไฟล์ที่ใหญ่กว่านั้นโดยแทนที่ด้วยไฟล์ขยะ พร้อมเพิ่มนามสกุลแบบสุ่ม 4 ตัวอักษรให้กับไฟล์ที่ถูกล็อก โดยผู้โจมตีจะให้เหยื่อติดต่อผ่านแอปเข้ารหัสอย่าง Session เพื่อเจรจาและจ่ายค่าไถ่

ส่วน Numero เป็นมัลแวร์ชนิดใหม่ที่ไม่ได้เข้ารหัสไฟล์หรือขโมยข้อมูล แต่เน้นทำลายระบบให้ไม่สามารถใช้งานได้ โดยปลอมตัวมาเป็นตัวติดตั้งของ InVideo AI ที่ภายในประกอบด้วยไฟล์ .bat, VBScript และไฟล์ wintitle.exe ซึ่งเมื่อทำงานแล้วจะเข้าสู่ลูปไม่รู้จบที่เขียนทับหน้าต่าง ปุ่ม และเนื้อหาทุกอย่างบนหน้าจอด้วยตัวเลข “1234567890” ทำให้ระบบเสียหายทางภาพถาวรและไม่สามารถใช้งานได้ตามปกติ

คำแนะนำ (Recommendation)

- อย่าดาวน์โหลดซอฟต์แวร์ AI หรือเครื่องมือใดๆ จากเว็บไซต์ที่ไม่รู้จัก
- ดาวน์โหลดเครื่องมือ AI เฉพาะจากเว็บไซต์ทางการของผู้พัฒนา เช่น OpenAI, Microsoft หรือเว็บไซต์ที่ได้รับการยืนยันความปลอดภัย
- ระมัดระวังการคลิกลิงก์จากโพสต์บนโซเชียลมีเดียหรือผลการค้นหาที่ดูน่าสงสัย
- ใช้โปรแกรมป้องกันไวรัสและอัปเดตซอฟต์แวร์อย่างสม่ำเสมอ

ข้อมูลอ้างอิง

- https://www.bleepingcomputer.com/news/security/cybercriminals-exploit-ai-hype-to-spread-ransomware-malware/