วันที่ 16 พฤษภาคม 2568

มัลแวร์ขโมยข้อมูลชนิดใหม่ “Chihuahua Stealer” ผ่านเอกสาร Google Drive

Executive Summary

Chihuahua Stealer เป็นมัลแวร์ขโมยข้อมูลตัวใหม่ที่พัฒนาด้วยเทคโนโลยี .NET ถูกค้นพบครั้งแรกโดยนักวิจัยจาก G DATA ในเดือนเมษายน 2025 จุดเด่นของมัลแวร์นี้คือการใช้เอกสารบน Google Drive เป็นช่องทางในการกระจายสคริปต์ PowerShell อันตราย ซึ่งเมื่อเหยื่อเปิดเอกสารดังกล่าว จะเริ่มกระบวนการติดตั้งและตั้งค่าให้ทำงานซ้ำผ่าน Scheduled Tasks ตัวมัลแวร์จะขโมยข้อมูลสำคัญจากเครื่องเหยื่อ เช่น ข้อมูลล็อกอินจากเบราว์เซอร์ คุกกี้ และกระเป๋าเงินดิจิทัล โดยจะดึง payload จากเซิร์ฟเวอร์ C2 หลายแห่ง พร้อมส่งข้อมูลกลับในรูปแบบเข้ารหัสด้วย AES-GCM ผ่านการเชื่อมต่อ HTTPS เพื่อหลบเลี่ยงการตรวจจับ เทคนิคที่ใช้ประกอบด้วยการเข้ารหัสด้วย Windows Cryptography API (CNG) และการล้างแคช DNS หลังถูกเรียกใช้งาน จะมีการถอดรหัสและโหลดสคริปต์ในขั้นตอนถัดไป พร้อมสร้าง Scheduled Task ชื่อ “f90g30g82” ที่ทำงานทุก 1 นาที เพื่อตรวจสอบไฟล์ในโฟลเดอร์ Recent Files หากพบไฟล์นามสกุล .normaldaki มัลแวร์จะเชื่อมต่อกับเซิร์ฟเวอร์ “cdn.findfakesnake[.]xyz” เพื่อโหลด payload เพิ่มเติม หากเชื่อมต่อไม่ได้ จะใช้เซิร์ฟเวอร์สำรอง “cat-watches-site[.]xyz” payload สุดท้ายที่โหลดมาจะเป็น .NET assembly ซึ่งถูกฝังในหน่วยความจำและใช้ในการขโมยข้อมูล โดยข้อมูลที่ได้จะถูกส่งกลับในรูปแบบไฟล์เข้ารหัสนามสกุล .chihuahua

คำแนะนำ (Recommendation)

- ดำเนินการตรวจสอบ Log PowerShell บนเครื่อง Windows ที่ได้รับผลกระทบ
- จำกัดสิทธิ์การใช้งานและการเข้าถึงของสคริปต์ PowerShell ที่ไม่ได้รับอนุญาต
- ตรวจสอบไฟล์ที่มีนามสกุล .normaldaki หากตรวจพบให้ดำเนินการลบออกทันที
- ระมัดระวังและไม่เปิดไฟล์เอกสารจากแหล่งที่ไม่น่าเชื่อถือ

ข้อมูลอ้างอิง

- https://cybersecuritynews.com/chihuahua-stealer-leverages-google-drive-document/
- https://www.gdatasoftware.com/blog/2025/05/38199-chihuahua-infostealer