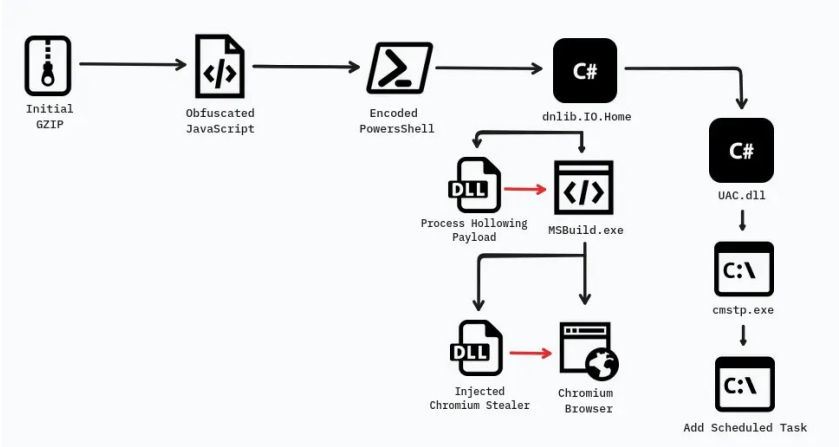
27 พฤษภาคม 2568

Katz Stealer มัลแวร์ใหม่ขโมยรหัสผ่านจาก Chrome, Edge, Brave และ Firefox

Executive Summary

ภัยคุกคามรูปแบบใหม่ที่ชื่อว่า *Katz Stealer* ปรากฏตัวในฐานะ Malware-as-a-Service ที่พุ่งเป้าโจมตีผู้ใช้งานเบราว์เซอร์ชื่อดังอย่าง Chrome, Edge, Brave และ Firefox โดยสามารถหลบหลีกกลไกความปลอดภัยสมัยใหม่ได้ โดยมีจุดมุ่งหมายเพื่อขโมยข้อมูลบัญชีผู้ใช้, กระเป๋าเงินคริปโต และข้อมูลจากแอปพลิเคชั่นต่างๆ อย่างแนบเนียน

โดยนักวิจัยจาก Nextron Systems เปิดเผยการค้นพบ Katz Stealer มัลแวร์ตัวใหม่ที่มีความสามารถสูง ถูกออกแบบมาเพื่อล้วงข้อมูลการเข้าสู่ระบบ และขโมยข้อมูลสำคัญจากผู้ใช้เบราว์เซอร์ยอดนิยมอย่าง Google Chrome, Microsoft Edge, Brave และ Firefox โดยเฉพาะอย่างยิ่ง มัลแวร์นี้สามารถหลบหลีกเทคโนโลยีป้องกันรหัสผ่านของ Chrome ที่ชื่อว่า App-Bound Encryption ได้สำเร็จ



การโจมตีเริ่มต้นจาก ไฟล์ GZIP ที่ซ่อนสคริปต์ JavaScript ซึ่งถูกออกแบบมาให้ซับซ้อนเพื่อหลีกเลี่ยงการตรวจจับ

จากนั้นจะรัน สคริปต์ PowerShell ที่ถูกเข้ารหัสแบบ base64 เพื่อดาวน์โหลดไฟล์เพิ่มเติมจาก archive.org โดยใช้เทคนิค steganography ซ่อนโค้ดอันตรายไว้ในภาพธรรมดา

หลังจากโหลดเพย์โหลดสำเร็จ Katz Stealer จะใช้ .NET Reflection โหลดโค้ดเข้าสู่หน่วยความจำโดยไม่ติดต่อกับดิสก์ และดำเนินการ Process Hollowing ฝังตัวเองเข้าไปในโปรเซส Windows ที่ชื่อว่า MSBuild.exe เพื่อปกปิดการทำงาน พร้อมทั้งเปิดการเชื่อมต่อกับเซิร์ฟเวอร์ควบคุม (C2) ที่ IP 185.107.74.40

จากนั้น มัลแวร์จะเริ่มดูดข้อมูลรหัสผ่านจากเบราว์เซอร์, กระเป๋าคริปโต, แอปแชทอย่าง Discord, Telegram, แพลตฟอร์มเกมเช่น Steam, และอีเมลไคลเอนต์อย่าง Outlook

นอกจากนี้ Katz Stealer ยังแสดงความสามารถในการหลีกเลี่ยงการวิเคราะห์ได้ดีเยี่ยม เช่น

- จำกัดพื้นที่ (Geofencing) โดยจะไม่ทำงานในประเทศกลุ่ม CIS
- ตรวจจับเครื่องเสมือน (VM detection)
- วิเคราะห์ลักษณะ Sandbox จากขนาดหน้าจอและเวลาการทำงานของระบบ

Preventative Measures & Takeaways

- หลีกเลี่ยงการคลิกลิงก์หรือดาวน์โหลดไฟล์จากแหล่งที่ไม่น่าเชื่อถือ
- เปิดใช้งานฟีเจอร์รักษาความปลอดภัยของเบราว์เซอร์ เช่น App-Bound Encryption
- ติดตั้งซอฟต์แวร์ป้องกันภัยขั้นสูง เช่น EDR ที่สามารถตรวจจับพฤติกรรมในหน่วยความจำได้
- ตรวจสอบกระบวนการทำงานของระบบเป็นระยะ เช่น การทำงานของ MSBuild.exe
- อัปเดตระบบและเบราว์เซอร์ให้เป็นเวอร์ชันล่าสุดเสมอ

Reference information

1. https://cybersecuritynews.com/katz-stealer-attacking-chrome-edge-brave-firefox/