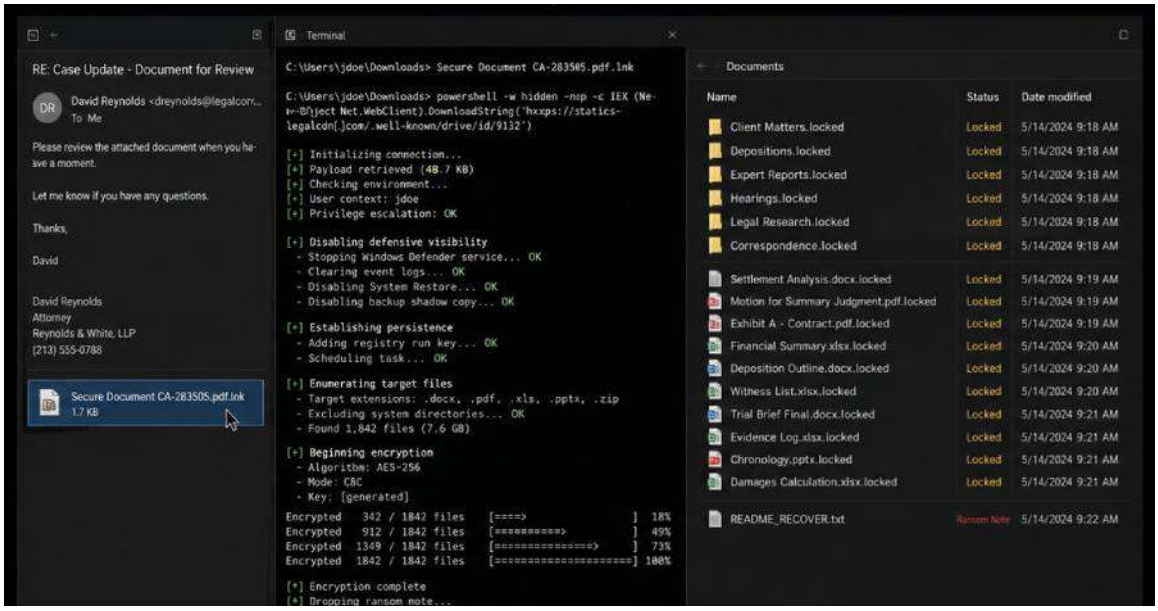
วันที่ 8 กรกฎาคม 2569

เฟรมเวิร์กมัลแวร์ใหม่ Avalon มาพร้อมความสามารถของแรนซัมแวร์ CrownX



นักวิจัยด้านความมั่นคงปลอดภัยไซเบอร์ค้นพบเฟรมเวิร์กมัลแวร์แบบ Modular ตัวใหม่ที่ไม่เคยมีการเปิดเผยมาก่อน ซึ่งมีชื่อรหัสว่า Avalon โดยแพร่กระจายผ่านการโจมตีแบบฟิชชิงหลายขั้นตอน (Multi-stage Phishing) ที่สามารถหลบเลี่ยงระบบป้องกันแบบดั้งเดิมได้

Avalon รวมความสามารถหลายด้านไว้ในเฟรมเวิร์กเดียว ทั้งการขโมยข้อมูลรับรอง (Credentials) การเคลื่อนที่ภายในเครือข่าย (Lateral Movement) การเข้าควบคุมเครื่องจากระยะไกล (Remote Access) การทำลายความสามารถในการกู้คืนระบบ และการเรียกใช้แรนซัมแวร์ โดยส่วนของแรนซัมแวร์ถูกตั้งชื่อภายในว่า CrownX

การโจมตีเริ่มต้นจากอีเมลปลอมที่แอบอ้างว่าเป็นเอกสารทางกฎหมาย พร้อมลิงก์ไปยังไฟล์บีบอัดที่ตั้งรหัสผ่านไว้บน Proton Drive" นักวิจัย Nevan Beal และ Sam Decker จาก Blackpoint Cyber กล่าว โค้ดอันตรายถูกซ่อนอยู่ภายในไฟล์อิมเมจแบบ ISO แทนที่จะแนบมากับอีเมลโดยตรง ทำให้มีโอกาสน้อยลงที่จะถูกตรวจจับตั้งแต่ชั้นของระบบอีเมล

หากผู้รับอีเมลเปิดไฟล์ Windows Shortcut ที่ปลอมเป็นเอกสารชื่อ "Secure Document CA-283505.pdf.lnk" ภายในไฟล์ ISO ที่ถูกเมานต์ไว้ จะทำให้กระบวนการติดมัลแวร์หลายขั้นตอนเริ่มทำงาน และจบลงด้วยการติดตั้ง Avalon ลงบนเครื่อง โดย Shortcut ดังกล่าวจะสั่งรันคำสั่งเพื่อเปิดโปรเจกต์ MSBuild ที่อยู่ภายในไฟล์ ISO

จากนั้นโปรเจกต์ MSBuild จะโหลด .NET Assembly ที่ฝังไว้ภายใน ซึ่งจะเข้าไปรบกวนการทำงานของ Event Tracing for Windows (ETW) เพื่อลดโอกาสในการเก็บหลักฐานสำหรับการสืบสวน และดาวน์โหลด Payload ขั้นถัดไปผ่าน HTTPS เพื่อเริ่มทำงานของ Avalon

เฟรมเวิร์กมัลแวร์ตัวนี้ยังมีระบบหลบเลี่ยงการตรวจจับ (Defense Evasion) ที่ค่อนข้างสมบูรณ์ โดยมีวิธีหลบซ่อนการทำงานจากเครื่องมือรักษาความปลอดภัยหลายราย เช่น Microsoft Defender, SentinelOne, CrowdStrike, Sophos, Elastic Endpoint, FortiEDR, ESET, McAfee และ Bitdefender ความสามารถเหล่านี้ทำให้เฟรมเวิร์กสามารถลดข้อมูล Telemetry หลบเลี่ยงการตรวจสอบในระดับ User Mode และปรับเปลี่ยนรูปแบบการทำงานให้เหมาะกับระบบป้องกันที่ตรวจพบบนเครื่องของเหยื่อ

ความสามารถทั้งหมดที่พบใน Avalon มีดังนี้

- ขโมยข้อมูลบัญชีผู้ใช้ คุกกี้ ประวัติการใช้งาน และบุ๊กมาร์กจากเว็บเบราว์เซอร์ที่ใช้ Chromium รวมถึง Mozilla Firefox
- รวบรวมข้อมูลจากแอปกระเป๋าเงินคริปโต เช่น MetaMask, Phantom, Coinbase Wallet, Exodus, Electrum, Atomic Wallet, Ledger Live และ Bitcoin Core รวมถึง Discord, Slack, Microsoft Teams, OpenVPN, WireGuard และ Windows Credential Manager
- เก็บข้อมูล SSH Known Hosts, รายการการเชื่อมต่อ RDP ที่บันทึกไว้, รหัสผ่าน Wi-Fi และข้อมูล cpassword จาก Group Policy Preferences
- ส่งข้อมูลที่ขโมยได้ไปยังเซิร์ฟเวอร์ระยะไกล helloxcherry[.]com และติดต่อกลับไปยังเซิร์ฟเวอร์อย่างต่อเนื่องเพื่อรับคำสั่งเพิ่มเติม
- สำรวจระบบและจัดลำดับความสำคัญของเครื่องที่สามารถใช้ขยายการโจมตีต่อได้
- เข้ารหัสไฟล์ที่เกี่ยวข้องกับการดำเนินธุรกิจ การพัฒนาซอฟต์แวร์ งานวิศวกรรม ระบบจัดเก็บข้อมูล และโครงสร้างพื้นฐานเสมือน (Virtual Infrastructure) โดยใช้ Windows Cryptography API พร้อมสร้างข้อความเรียกค่าไถ่ที่มีรายละเอียดการชำระเงิน และตัวนับเวลาที่แสดงระยะเวลาก่อนยอดค่าไถ่จะเพิ่มขึ้น
- ป้องกันการกู้คืนระบบ โดยหยุดการทำงานของ Volume Shadow Copy Service และลบ Shadow Copies ทั้งหมด
- ลบร่องรอยของไฟล์และข้อมูลที่เกี่ยวข้องผ่านระบบ Anti-Forensics เพื่อให้การตรวจสอบเหตุการณ์ทำได้ยากขึ้น
- เข้าถึงโครงสร้างของดิสก์โดยตรง ซึ่งคาดว่ามีเป้าหมายเพื่อทำลายข้อมูลพาร์ทิชัน Boot Record หรือส่วนสำคัญอื่นๆ ของดิสก์ จนทำให้ระบบไม่สามารถใช้งานได้

CrownX เป็นเพียงขั้นตอนสุดท้ายของการเรียกค่าไถ่เท่านั้น แต่ความเสียหายที่เกิดขึ้นมีมากกว่าการเข้ารหัสไฟล์" บริษัทกล่าว "เมื่อข้อความเรียกค่าไถ่ปรากฏขึ้น เฟรมเวิร์กได้ขโมยข้อมูลรับรอง สร้างการเชื่อมต่อกับเซิร์ฟเวอร์ C2 เตรียมเส้นทางสำหรับการเคลื่อนที่ภายในเครือข่ายหลายรูปแบบ และลดความสามารถในการกู้คืนระบบของเครื่องเหยื่อไปเรียบร้อยแล้ว

รายละเอียดที่น่าสนใจอีกประการคือ Avalon มีลักษณะที่บ่งชี้ว่าอาจได้รับการพัฒนาด้วยความช่วยเหลือของปัญญาประดิษฐ์ (AI) โดยเป็นการนำโมดูลหลายส่วนมาประกอบเข้าด้วยกัน แม้จะยังขาดความละเอียดในด้านเทคนิคการหลบซ่อนหรือการรักษาความปลอดภัยในการปฏิบัติการ ซึ่งโดยปกติแล้วจำเป็นต้องอาศัยความเชี่ยวชาญค่อนข้างสูงในการพัฒนา

ผลการวิจัยครั้งนี้สะท้อนให้เห็นอีกครั้งว่า AI กำลังลดข้อจำกัดในการพัฒนามัลแวร์ ทำให้ผู้โจมตีสามารถสร้างเครื่องมือที่มีความสามารถสูงได้ด้วยเวลาและความพยายามที่น้อยลง แม้จะมีความรู้หรือทรัพยากรด้านเทคนิคไม่มากก็ตาม กล่าวคือ การที่มัลแวร์มีความสามารถซับซ้อน ไม่ได้หมายความว่าผู้โจมตีจะต้องมีความเชี่ยวชาญหรือมีความพร้อมด้านปฏิบัติการในระดับสูงเสมอไป

ลำดับการโจมตีทั้งหมดแสดงให้เห็นว่า เหยื่อล่อทางธุรกิจที่พบเห็นได้ทั่วไป สามารถนำไปสู่การติดตั้งเฟรมเวิร์กมัลแวร์ที่นำกลับมาใช้ซ้ำได้ ซึ่งออกแบบมาเพื่อขโมยข้อมูลรับรอง ดาวน์โหลด Payload เพิ่มเติมทั้งหมดผ่านหน่วยความจำ และเตรียมการโจมตีต่อเนื่องหลายรูปแบบจากเครื่องที่ถูกเจาะเพียงเครื่องเดียว" Blackpoint Cyber กล่าว

LLM อยู่เบื้องหลังการโจมตีด้วย Agentic Ransomware

การเปิดเผยข้อมูลครั้งนี้เกิดขึ้นพร้อมกับรายงานของ Sysdig ที่ระบุว่า บริษัทได้พบการโจมตีด้วยแรนซัมแวร์แบบ Agentic ที่ขับเคลื่อนโดย Large Language Model (LLM) ตั้งแต่ต้นจนจบเป็นครั้งแรกที่มีการเปิดเผยต่อสาธารณะ โดย AI สามารถลองใหม่ ปรับเปลี่ยนวิธีการ และแก้ไขการทำงานของตัวเองแบบเรียลไทม์จนภารกิจสำเร็จ ผู้โจมตีกลุ่มนี้ถูกตั้งชื่อว่า JADEPUFFER

ผู้โจมตี "เริ่มต้นจากการเข้าถึงระบบ Langflow ที่เปิดให้ใช้งานผ่านอินเทอร์เน็ตด้วยช่องโหว่ CVE-2025-3248 จากนั้นดำเนินการโจมตีแบบอัตโนมัติที่สามารถปรับเปลี่ยนพฤติกรรมได้เอง ก่อนจะเคลื่อนที่ไปยังเป้าหมายที่ต้องการ และดำเนินการเรียกค่าไถ่ด้วยการทำลายฐานข้อมูลบนเซิร์ฟเวอร์ Production ของเหยื่อ" Michael Clark จาก Sysdig กล่าว

ปัจจุบันอุปสรรคด้านทักษะในการก่อเหตุด้วยแรนซัมแวร์ลดลงเหลือเพียงค่าใช้จ่ายในการใช้งาน AI Agent และหาก Agent ตัวนั้นทำงานด้วยข้อมูลรับรองที่ได้มาจากการโจมตีแบบ LLMjacking ต้นทุนของผู้โจมตีก็แทบจะเป็นศูนย์

AI Malware ที่ใช้ LLM ในการโจมตีแบบไม่ต้องเขียนคำสั่ง

นอกจากนี้ นักวิจัยยังค้นพบมัลแวร์อีกตัวที่ผสานการทำงานระหว่าง Telegram Bot และ Public LLM API เพื่อให้ผู้โจมตีสามารถสั่งงานได้โดยไม่จำเป็นต้องเขียนคำสั่งของระบบปฏิบัติการ (Codeless Attack)

เมื่อมัลแวร์เริ่มทำงาน มันจะส่งข้อมูลพื้นฐานของเครื่องที่ติดมัลแวร์ไปยัง Telegram Bot ของผู้โจมตี จากนั้นจะเข้าสู่ลูป Command-and-Control (C2) โดยตรวจสอบข้อความใหม่จาก Bot API ทุกๆ 5 วินาที และส่งผลลัพธ์ของคำสั่งที่ถูกรันกลับไปยังผู้โจมตีผ่านช่องทางเดียวกัน

จุดเด่นของมัลแวร์ตัวนี้คือ ทุกข้อความที่ผู้โจมตีส่งผ่าน Telegram จะถูกส่งต่อไปยัง Public LLM API ที่ api.groq[.]com /openai/v1/chat/completions จากนั้น LLM จะทำหน้าที่แปลข้อความที่เป็นภาษาธรรมดาให้กลายเป็นคำสั่ง Shell ที่สามารถนำไปรันบนเครื่องเหยื่อได้โดยอัตโนมัติ ตัวอย่างมัลแวร์ดังกล่าวถูกอัปโหลดขึ้นบนแพลตฟอร์ม VirusTotal เมื่อวันที่ 11 มีนาคม 2026 และจนถึงปัจจุบันยังไม่ถูกตรวจพบจากระบบตรวจจับของเอนจินใดเลย

"งานวิจัยนี้แสดงให้เห็นการเพิ่มชั้นการแปลคำสั่งด้วย LLM ซึ่งเข้ามาแทนการเขียนคำสั่ง Shell โดยตรง ผู้โจมตีเพียงพิมพ์ข้อความธรรมดาผ่าน Telegram จากนั้น LLM จะเปลี่ยนข้อความเหล่านั้นให้เป็นคำสั่ง Shell และเครื่องของเหยื่อจะนำคำสั่งไปทำงานโดยอัตโนมัติ ผู้โจมตีจึงไม่จำเป็นต้องมีความรู้เกี่ยวกับการใช้งาน Command Line อีกต่อไป" Palo Alto Networks Unit 42 กล่าว

ข้อมูลอ้างอิง

Jul 3, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/07/new-avalon-malware-framework-packs.html