วันที่ 11 สิงหาคม 2569

การโจมตีแบบ ClickFix ส่งมัลแวร์ขโมยข้อมูลบน macOS ที่สามารถดูดเงินจากกระเป๋าเงินคริปโตได้

การโจมตีรูปแบบ ClickFix เพื่อส่งมัลแวร์ที่พัฒนาด้วยภาษา Go ซึ่งสามารถขโมยสินทรัพย์ดิจิทัล รวมถึงรหัสผ่านที่เก็บไว้ใน Browser, ข้อมูล Apple iCloud Keychain และข้อมูลรับรองตัวตนที่ถูกเก็บไว้ใน Cache

กระบวนการโจมตีที่มุ่งเป้าไปยัง macOS ถูกออกแบบมาเพื่อส่ง Shell Script ที่จะตรวจสอบข้อมูลของเครื่อง จากนั้นจึงดาวน์โหลด Payload ของมัลแวร์สำหรับ macOS ที่ตรงกับสถาปัตยกรรม CPU ของคอมพิวเตอร์เครื่องนั้น แม้ Payload ของมัลแวร์จะสามารถขโมยรหัสผ่านได้ แต่ฟังก์ชันที่น่าสนใจที่สุดคือความสามารถในการค่อยๆ ดูดเงินออกจากบัญชีคริปโต โดยโอนสินทรัพย์เหล่านั้นไปยังบัญชีที่อยู่ภายใต้การควบคุมของผู้โจมตี Andrew Brandt นักวิจัยด้านความปลอดภัยของ Huntress กล่าว

กระบวนการโจมตีเริ่มต้นจากการนำคำสั่ง ClickFix ไปวางในแอป Terminal ซึ่งจะทำให้ Bash Profiler/Loader ทำงาน โดยจะรวบรวมข้อมูลระบบจำนวนมาก จากนั้นดาวน์โหลด Payload แบบ Mach-O ที่ตรงกับสถาปัตยกรรมของหน่วยประมวลผล ของเหยื่อ Payload ดังกล่าวเป็นมัลแวร์ขโมยข้อมูลที่พัฒนาด้วยภาษา Go ซึ่งสามารถขโมยรหัสผ่านจาก Browser, ข้อมูลจาก Apple Keychain และข้อมูลรับรองตัวตนที่เก็บอยู่ใน Cache ก่อนส่งข้อมูลเหล่านี้ไปยัง Server ที่อยู่ภายใต้การควบคุมของผู้โจมตี

เช่นเดียวกับมัลแวร์ขโมยข้อมูลบน macOS ประเภทอื่น มัลแวร์นี้พยายามเพิ่มสิทธิ์ในการเข้าถึงระบบ โดยหลอกให้เหยื่อกรอกข้อมูลรับรองตัวตนของเครื่องผ่านหน้าต่างแจ้งเตือนปลอม ซึ่งอ้างว่าเกิด "ข้อผิดพลาดของระบบที่ไม่คาดคิด" และอ้างว่ากำลังดำเนินการกู้คืนไฟล์ระบบที่เสียหาย

สิ่งที่น่าสนใจคือ มัลแวร์ยังมีฟังก์ชัน "DRAIN" ซึ่งจะตรวจสอบว่ากระเป๋าเงินคริปโตมีเงินอยู่หรือไม่ และหากพบว่ามีเงิน ก็จะโอนเงินบางส่วนหรือทั้งหมดไปยังกระเป๋าเงินที่ผู้โจมตีควบคุมอยู่ มัลแวร์มีฟังก์ชันหลายรูปแบบสำหรับคริปโตแต่ละประเภทที่ตกเป็นเป้าหมาย ซึ่งรวมถึง Bitcoin, Litecoin, Dogecoin, Monero, Ethereum และ XRP ของ Ripple

แม้ว่านี่อาจไม่ใช่ความสามารถใหม่ทั้งหมด แต่ครั้งนี้เป็นครั้งแรกที่เราเห็นมัลแวร์ซึ่งสามารถดูดเงินออกจากกระเป๋าเงินคริปโตโดยสามารถเลือกดูดเงินออกมาในจำนวนที่น้อยกว่ามูลค่าทั้งหมดของกระเป๋าเงินได้ Huntress ระบุ มัลแวร์มีฟังก์ชันแยกกันเพื่อคำนวณว่าเงินจำนวน 1% ของยอดในกระเป๋าเงินมีมูลค่าเท่าใด โดยจะขึ้นอยู่กับว่ามัลแวร์กำลังโจมตีคริปโตประเภทใด

Server ที่ใช้เก็บ Payload ที่เป็นอันตรายและ Server สำหรับสั่งการและควบคุม (C2) ทั้งหมดเชื่อมโยงกลับไปยัง Infrastructure ที่เป็นของ Aeza Group ซึ่งเป็นผู้ให้บริการ Bulletproof Hosting จากรัสเซีย และถูกสหรัฐฯ สหราชอาณาจักร และออสเตรเลียคว่ำบาตร เนื่องจากให้บริการที่เอื้อให้ผู้ไม่หวังดีสามารถดำเนินกิจกรรมต่างๆ ได้ การเปิดเผยข้อมูลดังกล่าวเกิดขึ้นในช่วงที่มีการรายงานการโจมตีแบบ ClickFix หลายรูปแบบในช่วงไม่กี่สัปดาห์ที่ผ่านมา

แคมเปญ ClickFix บน macOS ที่เผยแพร่มัลแวร์ MacSync และ Atomic Stealer โดยใช้กลุ่ม Domain ที่มีหน้าตาคล้ายเว็บไซต์จริงหลายแห่ง และใช้ระบบตรวจสอบ Fingerprint ของ Browser และตรวจสอบ Hardware จากฝั่ง Server เพื่อเลือกแสดงหน้าเหยื่อล่อเฉพาะผู้เข้าชมที่สภาพแวดล้อมดูสอดคล้องกับ Browser บน macOS จริง ขณะที่จะบล็อก Crawler, Sandbox และเครื่องมือวิเคราะห์อัตโนมัติบางประเภท

ClickFix อีกหนึ่งรูปแบบที่นำ Program Compatibility Assistant ("pcalua.exe") ซึ่งเป็น Binary ที่ถูกต้องของ Windows มาใช้เป็นตัวเปิดโปรแกรม เพื่อหลบเลี่ยงการตรวจสอบที่อาศัยความสัมพันธ์ของ Process ต้นทาง "เหยื่อจะถูกหลอกผ่านหน้า ClickFix ให้คัดลอกคำสั่งที่ถูกสร้างขึ้นเป็นพิเศษไปวาง ซึ่งจะเรียกใช้ PowerShell จากนั้นใช้ WMI เพื่อสร้าง cmd.exe, Mount Remote WebDAV Share และโหลด DLL ที่เป็นอันตรายผ่าน rundll32.exe" Palo Alto Networks Unit 42 ระบุ "WebDAV Share จะถูกเปิดให้เข้าถึงผ่าน HTTPS โดยใช้ Infrastructure ที่อยู่หลัง CDN และใช้ URL ที่มี Token เฉพาะเหยื่อในรูปแบบ UUIDv4 Path เพื่อส่ง DLL ที่เป็นอันตราย เมื่อโหลด DLL แล้ว มัลแวร์จะใช้ DLL ดังกล่าวเพื่อติดตั้งความสามารถในการขโมยข้อมูลลงบนเครื่องที่ถูกโจมตี"

แคมเปญ ClickFix อีกหนึ่งรายการที่ใช้การสร้าง Module WebAssembly (Wasm) แบบทันทีและใช้ Steganography หรือการซ่อนข้อมูลภายในรูปภาพ SVG เพื่อหลบเลี่ยงการตรวจจับในระดับ Network กิจกรรมดังกล่าวใช้เว็บไซต์ที่ถูกต้องตามปกติแต่ถูกบุกรุก เพื่อเรียกใช้ JavaScript ที่เป็นอันตรายซึ่งถูกแทรกเข้าไป โดย JavaScript จะสร้าง Wasm Module ที่ส่งออก URL ซึ่งเป็นที่อยู่สำหรับดาวน์โหลดไฟล์ SVG และนำไฟล์เหล่านั้นมาสร้าง ClickFix URL "จากนั้น ClickFix URL สุดท้ายจะถูกใส่ลงใน DOM ด้วย Script Tag เพื่อแสดงหน้าตรวจสอบปลอม" Unit 42 ระบุ "หน้าตรวจสอบปลอมจะแสดงช่อง Checkbox และเมื่อผู้ใช้คลิก Checkbox หน้าเว็บจะแสดงคำแนะนำให้วางข้อมูลลงในหน้าต่าง Run"

การค้นพบดังกล่าวเกิดขึ้นในช่วงเดียวกับการพบแคมเปญมัลแวร์ขโมยข้อมูลอีกสองรายการ โดยรายการแรกเผยแพร่ Lumma Stealer ผ่านไฟล์ที่ปลอมเป็นภาพยนตร์ The Odyssey ในรูปแบบ 1080p WEBRip และ Blu-ray ซึ่งเป็นภาพยนตร์ที่เพิ่ง

ออกฉายและดัดแปลงมาจากมหากาพย์กรีกโบราณของ Homer ที่มีชื่อเดียวกัน ส่วนอีกแคมเปญใช้ซอฟต์แวร์ Crack และเหยื่อล่อที่เป็นการละเมิดลิขสิทธิ์บนเว็บไซต์ปลอม โดยใช้วิธี SEO Poisoning เพื่อให้เว็บไซต์เหล่านั้นปรากฏในผลการค้นหาและนำไปสู่การติดตั้ง Remus ซึ่งเป็น Lumma Stealer รุ่น 64-bit

ข้อมูลอ้างอิง

Aug 07, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/08/clickfix-attacks-deliver-macos-stealer.html