วันที่ 14 พฤศจิกายน 2568

ช่องโหว่ Triofox ถูกใช้โจมตีเพื่อติดตั้งเครื่องมือเข้าถึงระยะไกลผ่านฟีเจอร์แอนตี้ไวรัส

ทีม Mandiant Threat Defense ของ Google ได้ออกรายงานเตือนถึงการใช้ประโยชน์แบบ n-day ต่อช่องโหว่ร้ายแรงที่ตอนนี้ถูกแพตช์แล้วในแพลตฟอร์มแชร์ไฟล์และการเข้าถึงระยะไกล Triofox ของ Gladinet โดยกลุ่มผู้คุกคามที่ติดตามในชื่อ UNC6485

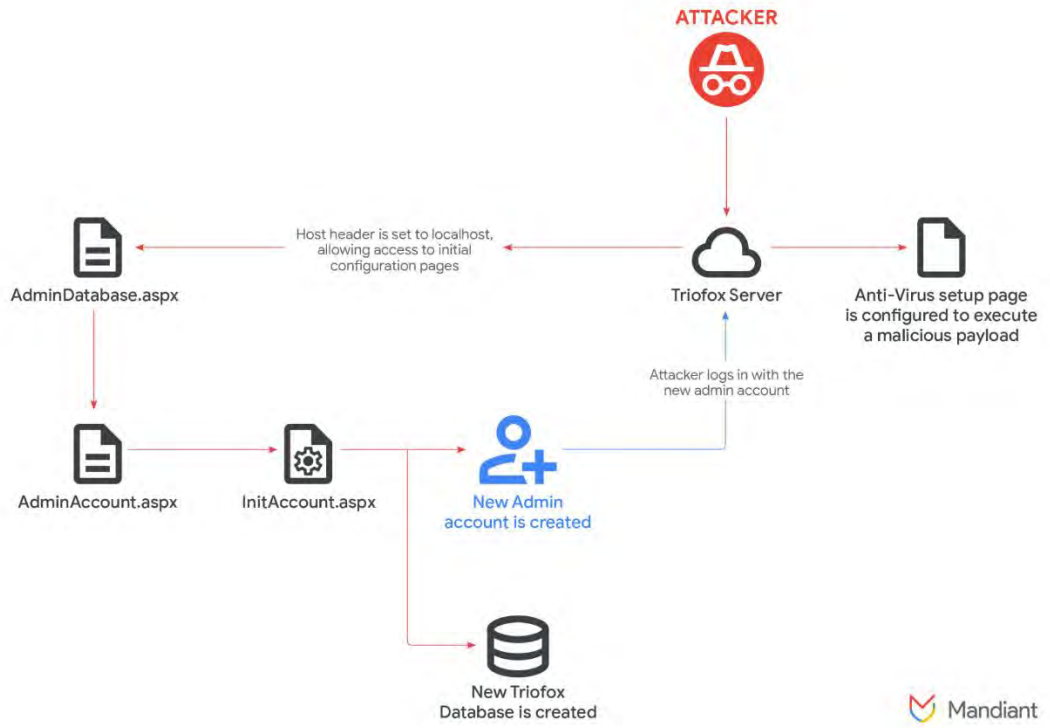
ช่องโหว่ร้ายแรงนี้ถูกติดตามในชื่อ CVE-2025-12480 (คะแนน CVSS: 9.1) ซึ่งอนุญาตให้ผู้โจมตี ข้ามการพิสูจน์ตัวตน และเข้าถึงหน้าการตั้งค่าคอนฟิกูเรชันได้โดยตรง ส่งผลให้สามารถอัปโหลดและรันเพย์โหลดใด ๆ ก็ได้ภายใต้สิทธิ์ที่สูง

เส้นทางการโจมตี: จาก Zero-Auth สู่ SYSTEM Privilege

Mandiant ระบุว่าพบกลุ่ม UNC6485 ใช้ช่องโหว่นี้ตั้งแต่วันที่ 24 สิงหาคม 2025 ซึ่งเป็นเวลาประมาณหนึ่งเดือนหลังจาก Gladinet ได้ปล่อยแพตช์สำหรับเวอร์ชัน 16.7.10368.56560 ควรสังเกตว่า CVE-2025-12480 เป็นช่องโหว่ใน Triofox รายที่สามที่ถูกใช้งานจริงในปีนี้ หลังจาก CVE-2025-30406 และ CVE-2025-11371

- ขั้นตอนที่ 1: การข้ามการพิสูจน์ตัวตนและการตั้งค่า Persistence: ผู้โจมตีใช้ช่องโหว่การเข้าถึงแบบไม่ต้องพิสูจน์ตัวตนเพื่อเข้าถึง หน้าการตั้งค่า (setup) (ซึ่งบันทึกการเปลี่ยนแปลงระบุว่า "เพิ่มการป้องกันสำหรับหน้าการตั้งค่าเริ่มต้น" หน้าดังกล่าวจะไม่สามารถเข้าถึงได้อีกหลังจาก Triofox ถูกตั้งค่าแล้ว) จากนั้นใช้หน้าดังกล่าวสร้างบัญชีแอดมินท้องถิ่นใหม่ชื่อ Cluster Admin โดยการรันกระบวนการตั้งค่า บัญชีแอดมินที่สร้างขึ้นใหม่ถูกใช้ดำเนินการกิจกรรมต่อเนื่อง
- ขั้นตอนที่ 2: การรันโค้ดระดับ SYSTEM: ผู้โจมตีล็อกอินด้วยบัญชีแอดมินที่สร้างขึ้นใหม่ และอัปโหลดไฟล์ที่เป็นอันตรายเพื่อรันผ่านฟีเจอร์แอนตี้ไวรัสที่มีมาให้

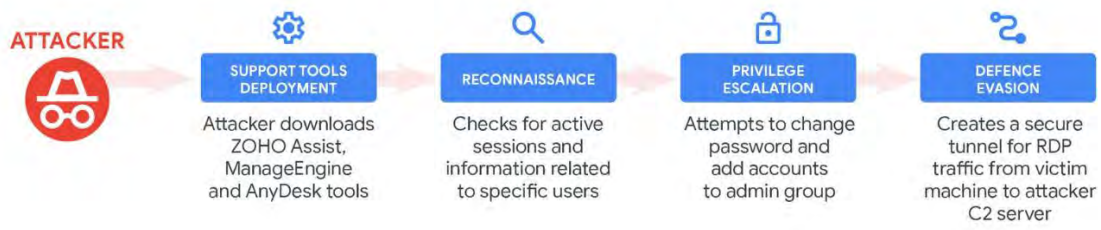
นักวิจัยกล่าวว่า: “เมื่อตั้งค่าฟีเจอร์แอนตี้ไวรัส ผู้ใช้สามารถระบุพาธใดก็ได้สำหรับโปรแกรมสแกนแอนตี้ไวรัส ไฟล์ที่ถูกกำหนดเป็นตำแหน่งของสแกนเนอร์จึงสืบทอดสิทธิ์ของกระบวนการแม่ของ Triofox ทำงานภายใต้บริบทของบัญชี SYSTEM”



เครื่องมือและการอำพราง

ผู้โจมตีรันสคริปต์แบ็ตช์ที่เป็นอันตรายชื่อ “centre_report.bat” โดยตั้งค่าพาธของเอนจินแอนตี้ไวรัสให้ชี้ไปยังสคริปต์ดังกล่าว

- การติดตั้ง RAT: สคริปต์ออกแบบมาเพื่อลงโปรแกรมติดตั้ง Zoho Unified Endpoint Management System (UEMS) จากที่อยู่ 84.200.80[.]252 และใช้เพื่อติดตั้งโปรแกรมเข้าถึงระยะไกลอย่าง Zoho Assist และ AnyDesk บนโฮสต์
- การยกระดับสิทธิ์ภายใน: การเข้าถึงระยะไกลผ่าน Zoho Assist ถูกใช้สำหรับรวบรวมข้อมูลข่าวกรอง (reconnaissance) ตามด้วยความพยายามเปลี่ยนรหัสผ่านของบัญชีที่มีอยู่และเพิ่มบัญชีเหล่านั้นเข้าไปในกลุ่ม local administrators และ “Domain Admins” เพื่อลอบยกระดับสิทธิ์
- อุโมงค์เข้ารหัสและ C2: เพื่อเลี่ยงการตรวจจับ ผู้โจมตีดาวน์โหลดเครื่องมืออย่าง Plink และ PuTTY เพื่อตั้ง อุโมงค์เข้ารหัส ไปยังเซิร์ฟเวอร์คำสั่งควบคุม (C2) ผ่านพอร์ต 433 โดยมีเป้าหมายสุดท้ายเพื่ออนุญาตการรับ RDP เข้ามา (inbound RDP)



ข้อแนะนำเร่งด่วนสำหรับผู้ใช้งาน Triofox

คำแนะนำสำหรับผู้ใช้ Triofox คือ:

1. อัปเดตทันที: อัปเดต Triofox เป็นเวอร์ชันล่าสุดเพื่อแก้ไขช่องโหว่
2. ตรวจสอบบัญชีแอดมิน: ตรวจสอบบัญชีแอดมิน และลบ/ล็อกบัญชีที่ไม่คาดคิด โดยเฉพาะบัญชี Cluster Admin
3. ตรวจสอบการตั้งค่า Antivirus: ยืนยันว่าเอนจินแอนตี้ไวรัสของ Triofox ไม่ได้ถูกตั้งค่าให้รันสคริปต์หรือไบนารีที่ไม่ได้รับอนุญาต

แม้ว่าจุดประสงค์สุดท้ายของแคมเปญยังไม่แน่ชัด แต่คำแนะนำสำหรับผู้ใช้ Triofox คือให้อัปเดตเป็นเวอร์ชันล่าสุด ตรวจสอบบัญชีแอดมิน และยืนยันว่าเอนจินแอนตี้ไวรัสของ Triofox ไม่ได้ถูกตั้งค่าให้รันสคริปต์หรือไบนารีที่ไม่ได้รับอนุญาต

ข้อมูลอ้างอิง

Nov 10, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/11/hackers-exploiting-triofox-flaw-to.html