วันที่ 23 มีนาคม 2569

Trivy Supply Chain Attack ทำให้เกิดหนอน CanisterWorm ที่แพร่กระจายตัวเองผ่านแพ็กเกจ npm กว่า 47 รายการ

กลุ่มผู้โจมตีที่อยู่เบื้องหลังการโจมตีแบบ Supply Chain ซึ่งมุ่งเป้าไปที่เครื่องมือสแกนความปลอดภัยยอดนิยมอย่าง Trivy ถูกสงสัยว่ากำลังดำเนินการโจมตีเป็นระลอกอย่างต่อเนื่อง ซึ่งนำไปสู่การฝังมัลแวร์ในแพ็กเกจ npm จำนวนมาก พร้อมกับการค้นพบหนอนคอมพิวเตอร์ชนิดใหม่ที่สามารถแพร่กระจายตัวเองได้ ซึ่งก่อนหน้านี้ยังไม่เคยมีการบันทึกมาก่อน โดยถูกตั้งชื่อว่า CanisterWorm ชื่อนี้มาจากการที่มัลแวร์ใช้ ICP canister ซึ่งเป็นสมาร์ตคอนแทรกต์แบบป้องกันการแก้ไขบนบล็อกเชน Internet Computer ทำหน้าที่เป็น dead drop resolver สำหรับค้นหาที่อยู่ของเซิร์ฟเวอร์ควบคุม (C2)

สรุปแพ็กเกจที่ได้รับผลกระทบ

นักวิจัยจาก Aikido Security อย่าง Charlie Eriksen กล่าวว่า นี่ถือเป็นครั้งแรกที่มีการบันทึกการนำ ICP canister มาใช้ในทางที่เป็นอันตราย เพื่อดึงข้อมูลตำแหน่งของเซิร์ฟเวอร์ C2 โดยตรง รายการแพ็กเกจที่ได้รับผลกระทบมีดังนี้

- 28 แพ็กเกจใน scope @EmilGroup
- 16 แพ็กเกจใน scope @opengov
- @teale.io/eslint-config
- @airtm/uuid-base32
- @pypestream/floating-ui-dom

จุดเริ่มต้นและกระบวนการทำงานของมัลแวร์

เหตุการณ์นี้เกิดขึ้นเพียงหนึ่งวันหลังจากผู้โจมตีใช้ข้อมูลรับรอง (Credentials) ที่ถูกขโมยมา เพื่อเผยแพร่แพ็กเกจอันตราย ได้แก่ trivy, trivy-action และ setup-trivy ซึ่งถูกฝังโปรแกรมขโมยข้อมูลรับรองไว้ คาดว่าการโจมตีนี้เชื่อมโยงกับ "TeamPCP" กลุ่มอาชญากรรมไซเบอร์ที่มุ่งเป้าโจมตีระบบคลาวด์

กระบวนการติดมัลแวร์จากแพ็กเกจ npm เริ่มจากการใช้ postinstall hook รันโปรแกรมตัวโหลด (Loader) จากนั้นตัวโหลดจะปล่อย Python backdoor ลงในเครื่อง ซึ่งจะทำหน้าที่ติดต่อไปยัง ICP canister เพื่อดึง URL ของ payload ขั้นต่อไป และเนื่องจากโครงสร้างของ dead drop นี้ถูกสร้างขึ้นบนระบบแบบกระจายศูนย์ (Decentralized) ทำให้ยากต่อการบล็อกหรือสั่งปิดระบบ

การแฝงตัวและระบบควบคุมสั่งการ

Eriksen อธิบายว่า ผู้ควบคุม canister สามารถเปลี่ยน URL ได้ตลอดเวลา จึงส่งไฟล์ไบนารีใหม่ไปยังเครื่องที่ติดมัลแวร์ได้โดยไม่ต้องแก้ไขตัวมัลแวร์บนเครื่องเลย มัลแวร์สร้างการแฝงตัวในระบบ (Persistence) โดยตั้งค่า systemd user service เพื่อให้ Python backdoor ทำงานใหม่อัตโนมัติใน 5 วินาทีหากถูกปิดไป โดยมีการตั้งค่า Restart=always นอกจากนี้ service ยังปลอมตัวเป็นโปรแกรมของ PostgreSQL ชื่อ pgmon เพื่อหลบเลี่ยงการตรวจจับ Backdoorจะติดต่อไปยัง ICP canister ทุกๆ 50 นาที โดยปลอม User-Agent ของเบราว์เซอร์ เพื่อดึง URL ข้อความธรรมดา จากนั้นจะดาวน์โหลดและรันไฟล์ดังกล่าว

หาก URL ที่ดึงมามีคำว่า youtube[.]com สคริปต์จะไม่ทำงาน ซึ่งถือเป็นสถานะพักของ canister ผู้โจมตีสามารถ เปิดการโจมตีได้ โดยเปลี่ยน URL ให้ชี้ไปยังไบนารีจริง และ “ปิดการทำงาน” ได้โดยเปลี่ยนกลับไปเป็นลิงก์ YouTube หากผู้โจมตีเปลี่ยน URL ไปยังไฟล์ใหม่ เครื่องที่ติดมัลแวร์ทั้งหมดจะดาวน์โหลด payload ใหม่ในการเชื่อมต่อครั้งถัดไป แต่ไฟล์เดิมจะยังทำงานอยู่เบื้องหลัง ก่อนหน้านี้ บริษัท Wiz เคยพบ kill switch ที่ใช้ youtube[.]com แบบเดียวกันนี้ใน Trivy เวอร์ชัน 0.69.4 ที่ถูกฝังโทรจัน โดยมัลแวร์จะติดต่อ ICP canister เดียวกันผ่าน Python dropper อีกตัวหนึ่งชื่อ sysmon.py

ณ เวลานั้น URL ที่ส่งกลับมาจากเซิร์ฟเวอร์ C2 เป็นเพียงวิดี Rickroll บน YouTube เท่านั้น การวิเคราะห์เพิ่มเติมโดย The Hacker News พบว่า ICP canister นี้มี 3 คำสั่งหลัก ได้แก่

- get_latest_link,
- http_request
- update_link

ซึ่งคำสั่ง update_link ช่วยให้ผู้โจมตีเปลี่ยนพฤติกรรมของมัลแวร์เพื่อส่งเพย์โหลดจริงในอนาคตได้ทุกเมื่อ

การยกระดับสู่ “หนอนคอมพิวเตอร์” ที่แพร่กระจายตัวเองอัตโนมัติ

ความรุนแรงเพิ่มขึ้นเมื่อพบ CanisterWorm ในแพ็กเกจ @teale.io/eslint-config (เวอร์ชัน 1.8.11 และ 1.8.12) ซึ่งสามารถแพร่กระจายตัวเองได้โดยอัตโนมัติ ต่างจากเวอร์ชันแรกที่แฮกเกอร์ต้องรันไฟล์ deploy.js ด้วยตนเอง โดยเวอร์ชันใหม่นี้มีการฝังฟังก์ชัน findNpmTokens() ไว้ในไฟล์ index.js ซึ่งจะทำงานอัตโนมัติในช่วง postinstall

สคริปต์จะสแกนหา npm authentication token จากเครื่องนักพัฒนาหรือระบบ CI Pipeline และใช้สิทธิ์จาก Token นั้นสั่งรัน deploy.js เป็นโปรเซสเบื้องหลังเพื่อแพร่กระจายมัลแวร์ไปยังโปรเจกต์อื่นๆ ที่บัญชีนั้นเข้าถึงได้ทันที ทั้งนี้มีการตั้งข้อสังเกตว่า ผู้โจมตีได้เปลี่ยน Payload ให้เป็นเพียงข้อความทดสอบ “hello123” ชั่วคราว เพื่อตรวจสอบความถูกต้องของห่วงโซ่การโจมตีก่อนปล่อยมัลแวร์ตัวจริง

Charlie Eriksen กล่าวสรุปว่า: นี่คือจุดเปลี่ยนสำคัญที่การโจมตีวิวัฒนาการจากการแฮ็กบัญชีเพื่อปล่อยมัลแวร์ กลายเป็น "มัลแวร์ที่เข้ายึดบัญชีเพื่อแพร่พันธุ์ตัวเอง" ส่งผลให้ระบบที่ติดตั้งแพ็กเกจนี้กลายเป็นตัวกลางในการแพร่กระจายมัลแวร์โดยไม่รู้ตัว และวงจรนี้จะวนซ้ำไปเรื่อยๆ ตราบเท่าที่ยังมีการเข้าถึง Token ในเครื่องเหยื่อได้

ข้อมูลอ้างอิง

Mar 21, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/03/leaknet-ransomware-uses-clickfix-via.html