วันที่ 18 มีนาคม 2569

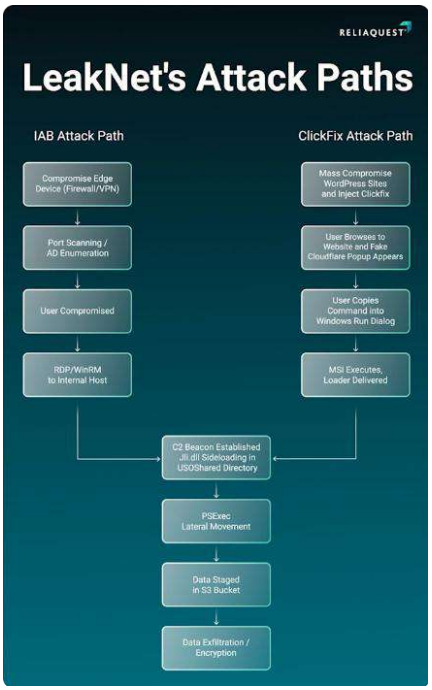
LeakNet Ransomware ใช้เทคนิค ClickFix ผ่านเว็บไซต์ที่ถูกแฮ็กและใช้ Deno Loader ที่ทำงานในหน่วยความจำ

LeakNet กลุ่มแรนซัมแวร์ที่ปรากฏตัวครั้งแรกในเดือนพฤศจิกายน 2024 โดยอ้างตัวเองว่าเป็น "ผู้เฝ้าระวังโลกดิจิทัล" ที่สนับสนุนเสรีภาพและความโปร่งใสบนอินเทอร์เน็ต กลับถูกพบว่าโจมตีองค์กรในภาคอุตสาหกรรมด้วย ตามข้อมูลที่รวบรวมโดย Dragos

ล่าสุด กลุ่มนี้เพิ่งเปลี่ยนกลยุทธ์การโจมตีครั้งสำคัญ โดยหันมาใช้เทคนิคหลอกลวงที่เรียกว่า ClickFix ผ่านเว็บไซต์จริงที่ถูกแฮ็กเอาไว้ แทนที่จะซื้อข้อมูลบัญชีผู้ใช้งานที่ถูกขโมยมาจากตลาดมืดเหมือนเดิม การโจมตีของ LeakNet ยังไม่ได้จำกัดอยู่ในอุตสาหกรรมใดเป็นพิเศษ แต่เป็นการหว่านเป้าหมายในวงกว้างเพื่อให้ได้เหยื่อมากที่สุดเท่าที่เป็นไปได้

ClickFix คืออะไร และทำไมถึงอันตราย

ClickFix คือเทคนิคหลอกลวงทางจิตวิทยา (Social Engineering) ที่หลอกให้ผู้ใช้งานรันคำสั่งอันตรายด้วยมือตัวเอง โดยแสดงหน้า CAPTCHA ปลอม บนเว็บไซต์ที่ถูกแฮ็ก แล้วบอกว่าต้องยืนยันตัวตนด้วยการคัดลอกและวางคำสั่ง msiexec.exe ลงในหน้าต่าง Windows Run เสมือนว่าเป็นการ "แก้ไขข้อผิดพลาด" ที่เกิดขึ้น ซึ่งในความเป็นจริงข้อผิดพลาดนั้นไม่ได้มีอยู่จริงเลย เทคนิคนี้ได้ผลดี เพราะอาศัยความคุ้นชินของผู้ใช้งาน ทำให้รู้สึกว่าการรันคำสั่งผ่านเครื่องมือของ Windows เป็นเรื่องปกติและปลอดภัย



ทำไม LeakNet ถึงเปลี่ยนวิธี

ตามรายงานทางเทคนิคที่เผยแพร่โดยบริษัทด้านความปลอดภัยไซเบอร์ ReliaQuest การที่ LeakNet หันมาใช้ ClickFix นับเป็น "การเปลี่ยนแปลงเชิงกลยุทธ์ที่สำคัญ" เนื่องจากก่อนหน้านี้กลุ่มนี้พึ่งพา Initial Access Brokers (IABs) หรือกลุ่มคนกลางที่ขายข้อมูลการเข้าถึงระบบที่ถูกขโมยมา

การเปลี่ยนมาใช้ ClickFix มีข้อได้เปรียบหลายอย่าง ได้แก่ ลดการพึ่งพาซัพพลายเออร์ภายนอก ลดต้นทุนต่อเหยื่อแต่ละราย และไม่ต้องรอให้บัญชีมูลค่าสูงถูกนำออกมาขาย ยิ่งไปกว่านั้น เนื่องจากการโจมตีใช้เว็บไซต์จริงที่ถูกแฮ็กเป็นสื่อกลาง จึงไม่ทิ้งสัญญาณผิดปกติในระดับเครือข่ายเหมือนกับโครงสร้างพื้นฐานที่ผู้โจมตีสร้างขึ้นเอง ทำให้ตรวจจับได้ยากขึ้น

เจาะลึกเทคนิค Deno Loader ในหน่วยความจำ

ประเด็นเทคนิคที่น่าสนใจอีกอย่างคือ LeakNet ใช้ ตัวโหลดคำสั่งควบคุม (C2 Loader) แบบหลายขั้นตอนที่สร้างบน Deno ซึ่งเป็น JavaScript runtime ตัวหนึ่ง

Deno Loader นี้รัน JavaScript ที่ถูกเข้ารหัสแบบ Base64 โดยตรงในหน่วยความจำของระบบ โดยไม่เขียนไฟล์ลงดิสก์เลย ส่งผลให้หลบเลี่ยงการตรวจจับได้ดีและไม่ทิ้งร่องรอยให้เหยื่อตรวจพบได้โดยง่าย เมื่อเพย์โหลดทำงาน มันจะเก็บข้อมูลเกี่ยวกับระบบที่ถูกเจาะ และติดต่อเซิร์ฟเวอร์ภายนอกเพื่อดาวน์โหลดมัลแวร์ในขั้นถัดไป หลังจากนั้นจะเข้าสู่กระบวนการ polling ที่จะดึงโค้ดเพิ่มเติมมารันผ่าน Deno อย่างต่อเนื่อง

ReliaQuest ยังพบกรณีที่ผู้โจมตีใช้ฟิชชิงผ่าน Microsoft Teams เพื่อหลอกให้ผู้ใช้รันเพย์โหลด ซึ่งท้ายที่สุดก็นำไปสู่การทำงานของ Deno-based loader ในลักษณะเดียวกัน แนวทางนี้ถูกเรียกว่า "Bring Your Own Runtime (BYOR)" และอาจบ่งชี้ว่า LeakNet กำลังขยายช่องทางการโจมตี หรือกลุ่มผู้โจมตีอื่นเริ่มนำเทคนิคนี้ไปใช้ด้วย

ขั้นตอนการโจมตีหลังเจาะระบบสำเร็จ

ReliaQuest ระบุว่า ไม่ว่า LeakNet จะใช้วิธีใดในการเข้าระบบ กระบวนการหลังจากนั้นจะเหมือนกันทุกครั้ง ซึ่งเป็นข้อดีสำหรับฝ่ายป้องกัน เพราะสามารถนำพฤติกรรมที่ตรวจพบได้มาใช้หยุดการโจมตีในแต่ละขั้นตอน ก่อนที่แรนซัมแวร์ตัวจริงจะถูกปล่อยออกมาโดยขั้นตอนการโจมตีมีดังนี้:

- ผู้โจมตีเริ่มต้นด้วยการส่ง Loader เข้ามาเพื่อรันเทคนิค DLL Side-loading ซึ่งเป็นการหลอกให้โปรแกรมที่น่าเชื่อถือเรียกใช้งานไฟล์ DLL ที่เป็นอันตราย เพื่อหลบเลี่ยงการตรวจจับของซอฟต์แวร์ความปลอดภัย
- หลังจากนั้นผู้โจมตีจะทำการสำรวจสิทธิ์และบัญชี โดยรันคำสั่ง cmd.exe /c klist ซึ่งเป็นคำสั่ง Windows ที่ใช้แสดงข้อมูลการยืนยันตัวตน (Kerberos tickets) ที่กำลังใช้งานอยู่ในระบบ วิธีนี้ทำให้ผู้โจมตีรู้ทันทีว่าบัญชีและบริการใดสามารถเข้าถึงได้ โดยไม่ต้องขอข้อมูลรับรองใหม่
- เมื่อทราบสิทธิ์การเข้าถึงแล้ว ผู้โจมตีจะเคลื่อนย้ายภายในเครือข่ายโดยใช้ PsExec ซึ่งเป็นเครื่องมือที่ผู้ดูแลระบบใช้กันทั่วไป ทำให้ดูผสมกลมกลืนกับกิจกรรมปกติ
- และผู้โจมตีจะขโมยข้อมูล โดยใช้ S3 buckets (บริการเก็บไฟล์บนคลาวด์ของ Amazon) เพื่อส่งข้อมูลออกจากระบบ ทำให้ทราฟฟิกดูเหมือนการใช้งานคลาวด์ปกติและช่วยลดโอกาสในการถูกตรวจจับ หลังจากนั้นจะทำการเข้ารหัสข้อมูลด้วยแรนซัมแวร์ ขั้นตอนสุดท้ายที่ล็อกข้อมูลของเหยื่อเพื่อเรียกค่าไถ่

ภาพรวมสถานการณ์แรนซัมแวร์ในปัจจุบัน

พัฒนาการนี้เกิดขึ้นในช่วงที่ Google เปิดเผยว่า Qilin (หรือ Agenda), Akira (หรือ RedBike), Cl0p, Play, SafePay, INC Ransom, Lynx, RansomHub, DragonForce (หรือ FireFlame และ FuryStorm) และ Sinobi เป็น 10 กลุ่มแรนซัมแวร์ที่มีจำนวนเหยื่อถูกเผยแพร่บนเว็บไซต์ Data Leak มากที่สุด

Google Threat Intelligence Group (GTIG) ระบุว่า ในประมาณหนึ่งในสามของเหตุการณ์โจมตี ช่องทางการเข้าถึงระบบในระยะแรกได้รับการยืนยันหรือคาดว่าเกิดจากการใช้ประโยชน์จากช่องโหว่ โดยส่วนใหญ่เกิดขึ้นกับอุปกรณ์ VPN และไฟร์วอลล์ที่ใช้กันอย่างแพร่หลาย นอกจากนี้ ยังพบว่า 77% ของการโจมตีแรนซัมแวร์ที่ถูกวิเคราะห์ มีการขโมยข้อมูลร่วมด้วย ซึ่งเพิ่มขึ้นจาก 57% ในปี 2024

ข้อมูลอ้างอิง

Mar 17, 2026, By Ravie Lakshmanan

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