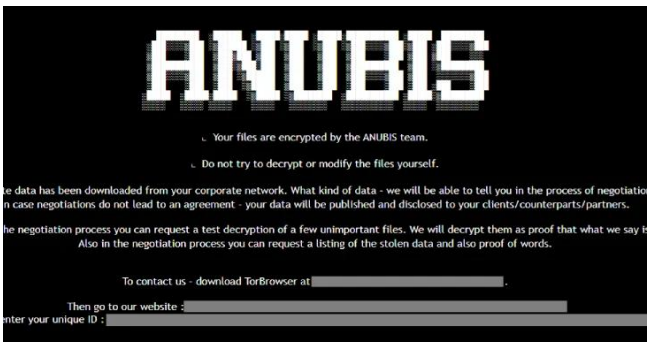
วันที่ 17 มิถุนายน 2568

Anubis Ransomware เข้ารหัสและลบไฟล์ ทำให้ไม่สามารถกู้คืนได้



ระวัง! Anubis แรนซัมแวร์สายพันธุ์ใหม่ เข้ารหัสแล้วยังลบทิ้งถาวร ไม่สนค่าไถ่!

นักวิจัยจาก Trend Micro ได้ค้นพบแรนซัมแวร์สายพันธุ์ใหม่ โดยมันไม่เพียงแค่เข้ารหัสไฟล์ แต่ยังถูกออกแบบมาให้ **ลบไฟล์ทิ้งอย่างถาวร** ด้วย ซึ่งถือเป็นภัยคุกคามที่โจมตีได้ถึงสองด้านในตัวเดียว รายงานนี้ถูกเปิดเผยโดย Maristel Policarpio, Sarah Pearl Camiling และ Sophia Nilette Robles เมื่อสัปดาห์ที่ผ่านมา

แรนซัมแวร์ตัวนี้มาพร้อมฟีเจอร์ **"wipe mode"** ที่จะลบเนื้อหาไฟล์จนหมดสิ้น ทำให้ไม่สามารถกู้คืนได้แม้เหยื่อจะยอมจ่ายค่าไถ่แล้วก็ตาม

รู้จักกับ Anubis: ผู้ให้บริการ Ransomware-as-a-Service (RaaS)

กลุ่มผู้ให้บริการแรนซัมแวร์ในรูปแบบ RaaS ที่อยู่เบื้องหลังมัลแวร์ตัวนี้มีชื่อว่า **Anubis** เริ่มเคลื่อนไหวตั้งแต่เดือนธันวาคม 2024 โดยมีเหยื่อในอุตสาหกรรมสาธารณสุข, โรงแรม, และการก่อสร้าง ในประเทศออสเตรเลีย, แคนาดา, เปรู และสหรัฐอเมริกา รายงานระบุว่าตัวอย่างแรกๆ ของแรนซัมแวร์นี้เคยใช้ชื่อ **Sphinx** ก่อนจะเปลี่ยนมาเป็น Anubis ในเวอร์ชันสุดท้าย

ข้อควรทราบ: กลุ่มอาชญากรรมไซเบอร์นี้ไม่มีความเกี่ยวข้องกับมัลแวร์โทรจันขโมยเงินบน Android หรือมัลแวร์แบ็คดอร์ที่เขียนด้วย Python ซึ่งใช้ชื่อเดียวกัน โดยมัลแวร์ Python ถูกเชื่อมโยงกับกลุ่ม **FIN7** หรือที่รู้จักในชื่อ **GrayAlpha**

Anubis ดำเนินโครงการกับพันธมิตร โดยเปิดให้ต่อรองส่วนแบ่งรายได้ได้ตามเงื่อนไข และยังรองรับการหารายได้เพิ่มจากการขโมยข้อมูลหรือขายสิทธิ์เข้าถึงระบบ สำหรับส่วนแบ่งรายได้จะจัดสรรเป็น 80/20 สำหรับค่าไถ่, 60/40 สำหรับการขโมยข้อมูล และ 50/50 สำหรับการขายสิทธิ์เข้าถึง

กลยุทธ์การโจมตีของ Anubis:

Anubis เริ่มต้นการโจมตีด้วยการส่งอีเมลฟิชชิ่งเพื่อเจาะเข้าระบบ จากนั้นจะยกระดับสิทธิ์, สำรวจข้อมูล และลบข้อมูลสำรอง (Volume Shadow Copies) ก่อนที่จะเข้ารหัสไฟล์ และหากจำเป็นก็จะลบไฟล์ทิ้งถาวรด้วย โดยวิธีนี้จะทำให้ไฟล์มีขนาดเหลือ 0 KB แต่ยังคงชื่อไฟล์หรือสกุลไฟล์เดิมไว้ ทำให้ไม่สามารถกู้กลับมาได้ และเพิ่มแรงกดดันให้เหยื่อต้องยอมจ่ายค่าไถ่

นักวิจัยเผยว่า แรนซัมแวร์นี้มีฟีเจอร์ลบถาวรผ่านคำสั่ง **/WIPEMODE** ซึ่งจะลบเนื้อหาไฟล์จนหมดสิ้น ป้องกันไม่ให้มีโอกาสกู้ไฟล์คืนได้อีก ความสามารถในการเข้ารหัสและลบข้อมูลอย่างถาวรนี้ยิ่งเพิ่มความเสี่ยงให้เหยื่อ และกดดันให้ต้องยอมจ่ายค่าไถ่ตามแผนที่กลุ่มอาชญากรรมไซเบอร์ต้องการ ซึ่งเป็นแนวทางของปฏิบัติการแรนซัมแวร์ส่วนใหญ่ในปัจจุบัน

เชื่อมโยงกับการเคลื่อนไหวใหม่ของ FIN7?

การค้นพบพฤติกรรมทำลายข้อมูลของ Anubis เกิดขึ้นในช่วงเดียวกับที่ Recorded Future เปิดเผยโครงสร้างพื้นฐานใหม่ของกลุ่ม **FIN7** ที่แอบอ้างเป็นซอฟต์แวร์หรือบริการถูกกฎหมาย เพื่อแอบปล่อย **NetSupport RAT**

บริษัทข่าวกรองภัยคุกคามในเครือ Mastercard ระบุว่าในช่วงปีที่ผ่านมา พบวิธีปล่อยมัลแวร์ 3 ช่องทาง ได้แก่:

1. **หน้าอัปเดตเบราว์เซอร์ปลอม:** จะโหลดตัวโหลดมัลแวร์ชื่อ **MaskBat** เพื่อรัน remote access trojan
2. **หน้าโหลด 7-Zip ปลอม:** ใช้ PowerShell loader ชื่อ **PowerNet** เพื่อคลายไฟล์และรันมัลแวร์
3. **TAG-124 (หรือชื่ออื่น 404 TDS, Chaya_002, Kongtuke และ LandUpdate808):** ใช้ PowerShell loader ชื่อ **PowerNet** เพื่อคลายไฟล์และรันมัลแวร์

Insikt Group ของ Recorded Future ระบุว่า **MaskBat** คล้ายกับ **FakeBat** แต่มีการเข้ารหัสซับซ้อนขึ้น และมีสตริงที่เชื่อมโยงกับ **GrayAlpha** ทั้งนี้ แม้พบว่ามีการใช้ช่องทางโจมตีทั้งสามพร้อมกัน แต่ในเวลาที่เขียนรายงาน (เมษายน 2025) พบว่าเหลือเพียงหน้าโหลด 7-Zip ปลอมที่ยังคงใช้งานอยู่ โดยมีโดเมนใหม่จดทะเบียนล่าสุดเมื่อเดือนเมษายน 2025

Anubis แรนซัมแวร์ตัวใหม่นี้เป็นภัยคุกคามที่รุนแรงและอันตรายยิ่งกว่าเดิม ด้วยความสามารถในการเข้ารหัสและลบข้อมูลอย่างถาวร ทำให้เหยื่อไม่มีทางเลือกในการกู้คืนไฟล์ได้เลยแม้จะจ่ายค่าไถ่ ดังนั้น การป้องกันและสำรองข้อมูลอย่างสม่ำเสมอจึงมีความสำคัญอย่างยิ่งยวดในยุคที่ภัยคุกคามไซเบอร์พัฒนาไปอย่างไม่หยุดยั้ง

คำแนะนำ (Recommendation)

- สำรองข้อมูลอย่างสม่ำเสมอและจัดเก็บสำเนาสำรองไว้นอกเครือข่ายหลัก
- อัปเดตระบบปฏิบัติการและซอฟต์แวร์ ให้เป็นเวอร์ชันล่าสุดอย่างสม่ำเสมอ
- ใช้งานโซลูชันด้านความปลอดภัย เช่น EDR, IDS/IPS

ข้อมูลอ้างอิง

Jun 16, 2025 By Ravie Lakshmanan

- https://thehackernews.com/2025/06/anubis-ransomware-encrypts-and-wipes.html