วันที่ 10 กรกฎาคม 2569

Microsoft วิเคราะห์ GigaWiper แบ็กดอร์บน Windows ที่รวมความสามารถการล้างข้อมูล การปลอมเป็น Ransomware และสอดแนมไว้ในตัวเดียว

Microsoft เปิดเผยผลการวิเคราะห์มัลแวร์บน Windows ตัวใหม่ที่เรียกว่า GigaWiper ซึ่งมีลักษณะเด่นคือไม่ได้เป็นเพียงมัลแวร์ตัวเดียว แต่เป็นการนำเครื่องมือทำลายข้อมูลรุ่นเก่าถึง 3 ตัวมารวมไว้ในแบ็กดอร์เดียว โดยผู้โจมตีสามารถเลือกใช้งานคำสั่งแต่ละคำสั่งที่ถูกออกแบบมาเพื่อทำลายเครื่องในรูปแบบที่แตกต่างกัน ไม่ว่าจะเป็นการล้างข้อมูลทั้งดิสก์ การเขียนทับไดรฟ์ Windows หรือการทำงานในลักษณะคล้าย Ransomware ที่เข้ารหัสไฟล์ แต่ไม่เก็บกุญแจถอดรหัสไว้ ทำให้ไม่สามารถกู้คืนข้อมูลได้

เนื่องจาก GigaWiper เป็นมัลแวร์ ไม่ใช่ช่องโหว่ของซอฟต์แวร์ จึงไม่มีแพตช์สำหรับแก้ไข สิ่งที่ผู้โจมตีทำคือใช้มัลแวร์ตัวนี้หลังจากสามารถเจาะเข้าสู่ระบบได้แล้ว ดังนั้น การตรวจจับให้เร็วที่สุด รวมถึงการมีข้อมูลสำรองแบบออฟไลน์ (Offline Backup) ที่สามารถเชื่อถือได้ จึงเป็นแนวทางป้องกันที่สำคัญที่สุด ที่น่าสนใจคือ ไฟล์มัลแวร์ชุดเดียวกันนี้ถูกบริษัท Binary Defense ตรวจพบก่อนหน้านี้ในชื่อ BLUERABBIT

Microsoft ระบุแฮชของไฟล์ GigaWiper ทั้งหมด 4 ค่า ซึ่งตรงกับแฮชที่ Binary Defense ใช้ระบุ BLUERABBIT รวมถึงเซิร์ฟเวอร์ควบคุม (Command-and-Control Server) ก็เป็นชุดเดียวกัน

Binary Defense ซึ่งอ้างอิงข้อมูลจาก Google Threat Intelligence Group (GTIG) ประเมินว่ามัลแวร์ดังกล่าวมีความเชื่อมโยงกับกลุ่มผู้โจมตีที่น่าจะมีความเกี่ยวข้องกับอิหร่าน และมุ่งโจมตีองค์กรในอิสราเอล ขณะที่ Microsoft ไม่ได้ระบุถึงประเทศหรือกลุ่มผู้โจมตี

สามวิธีในการทำลายเครื่อง

GigaWiper ถูกพัฒนาด้วยภาษา Go (Golang) และทำงานบนระบบปฏิบัติการ Windows โดยรับคำสั่งผ่านหมายเลขคำสั่ง (Command ID) ซึ่งมีอยู่ 3 คำสั่งหลักที่ใช้ทำลายระบบ ได้แก่

- **Disk Wiper** ที่เขียนทับข้อมูลลงบนฮาร์ดดิสก์โดยตรง พร้อมลบตารางพาร์ทิชัน (Partition Table) ซึ่งเป็นข้อมูลที่ใช้กำหนดโครงสร้างของดิสก์ ก่อนสั่งรีบูตเครื่อง วิธีนี้ไม่ได้ลบไฟล์ทีละไฟล์ แต่ทำลายข้อมูลระดับดิสก์โดยตรง ทำให้แทบไม่สามารถกู้คืนได้
- **Fake Ransomware** ที่พัฒนาต่อยอดจากโค้ดของมัลแวร์ชื่อ Crucio โดยจะเข้ารหัสไฟล์ เพิ่มนามสกุลไฟล์เป็น .candy และเปลี่ยนภาพพื้นหลังของเดสก์ท็อปเป็นข้อความเตือนคล้ายการเรียกค่าไถ่ แต่ไม่มีการสร้างข้อความเรียกค่าไถ่ และไม่มีการเก็บกุญแจถอดรหัสไว้ จึงไม่มีทางจ่ายเงินเพื่อกู้ข้อมูลกลับคืนได้ เป้าหมายที่แท้จริงคือการทำลายข้อมูล ไม่ใช่การเรียกค่าไถ่
- **Windows Drive Wiper** ที่มุ่งทำลายเฉพาะไดรฟ์ Windows โดยเขียนทับข้อมูลหลายรอบด้วยรูปแบบข้อมูลที่แตกต่างกัน Microsoft ระบุว่าเป็นการนำมัลแวร์ล้างข้อมูล FlockWiper มาเขียนใหม่ด้วยภาษา Go

ทั้งสามวิธีไม่มีช่องทางให้กู้คืนข้อมูลได้ ไม่ว่าจะเป็นไฟล์ที่ถูกเข้ารหัสซึ่งไม่มีคีย์สำหรับถอดรหัส หรือดิสก์ที่ถูกเขียนทับจนต้องติดตั้งระบบใหม่จากข้อมูลสำรองเท่านั้น เป้าหมายคือทำให้เครื่องไม่สามารถใช้งานได้ ไม่ใช่เพื่อเรียกค่าไถ่

ไม่ได้แค่ทำลายข้อมูล แต่ยังสอดแนมผู้ใช้งานได้ด้วย

นอกจากความสามารถในการทำลายระบบแล้ว GigaWiper ยังสามารถสอดแนมและควบคุมเครื่องที่ติดมัลแวร์ได้อย่างเงียบๆ มัลแวร์สามารถจับภาพหน้าจอของจอภาพทุกตัว บันทึกวิดีโอหน้าจอระหว่างที่ผู้ใช้งานกำลังทำงาน และเปิดเซสชัน VNC แบบซ่อนตัว เพื่อให้ผู้โจมตีสามารถดูหน้าจอ ควบคุมเมาส์ และพิมพ์คำสั่งจากระยะไกลได้ นอกจากนี้ ยังสามารถรวบรวมข้อมูลของระบบ จัดการโปรแกรมและบริการที่กำลังทำงาน แก้ไขรีจิสทรีของ Windows รวมถึงลบ Windows Event Log เพื่อปกปิดร่องรอยหลังการโจมตี Microsoft ยังพบว่าภายในตัวอย่างมัลแวร์มีคำสั่งอีกหลายรายการที่ยังไม่ถูกเปิดใช้งาน เช่น ส่วนของ **Keylogger** และเครื่องมือล้างข้อมูลเพิ่มเติม

ปลอมตัวเป็น OneDrive เพื่อหลบการตรวจจับ

เพื่อหลีกเลี่ยงการถูกสังเกต GigaWiper จะปลอมตัวเป็น OneDrive โดยมัลแวร์จะสร้าง Scheduled Task ชื่อ OneDrive Update ให้ทำงานทุกๆ 1 นาที และบันทึกข้อมูลของตัวเองไว้ในรีจิสทรีที่ HKCU\SOFTWARE\OneDrive\Environment

เมื่อเปิดช่องทางควบคุมจากระยะไกล มัลแวร์ยังสร้างกฎของ Windows Firewall โดยใช้ชื่อ Microsoft.Windows.CloudExperienceHost ซึ่งเป็นชื่อขององค์ประกอบจริงใน Windows เพื่อให้ดูเหมือนเป็นทราฟฟิกที่ถูกต้อง สำหรับการสื่อสารกับเซิร์ฟเวอร์ควบคุม GigaWiper ไม่ได้ใช้การเชื่อมต่อเว็บทั่วไป แต่เลือกใช้บริการที่องค์กรจำนวนมากใช้งานอยู่แล้ว ได้แก่ RabbitMQ สำหรับรับคำสั่ง Redis สำหรับส่งผลลัพธ์ และ MinIO สำหรับขโมยข้อมูลออกจากระบบ

เนื่องจากทั้งหมดเป็นซอฟต์แวร์ที่ถูกใช้งานอย่างถูกต้องในหลายองค์กร ทราฟฟิกที่เกิดขึ้นจึงอาจดูเหมือนการทำงานปกติของระบบ และทำให้ตรวจจับได้ยากยิ่งขึ้น

ที่มาของ GigaWiper

Microsoft ระบุว่าโค้ดส่วน Fake Ransomware ของ GigaWiper มีต้นกำเนิดมาจาก Crucio ขณะที่ฟังก์ชันล้างข้อมูลหลายรอบถูกพัฒนาต่อยอดมาจาก FlockWiper และประเมินว่าเครื่องมือทั้งสามน่าจะถูกพัฒนาโดยผู้สร้างรายเดียวกัน แม้ Microsoft จะไม่ได้ระบุประเทศที่อยู่เบื้องหลัง แต่ Crucio ไม่ใช่มัลแวร์ที่ไม่เคยถูกพบมาก่อน โค้ดของ Crucio เคยถูกระบุว่าเป็น Ransomware ที่น่าสงสัยในประกาศของ CISA เมื่อเดือนธันวาคม 2023 ซึ่งเกี่ยวข้องกับกลุ่ม CyberAv3ngers ที่เชื่อมโยงกับ Islamic Revolutionary Guard Corps (IRGC) ของอิหร่าน

ก่อนหน้านี้ The Hacker News เคยรายงานว่า กลุ่มดังกล่าวเคยโจมตีระบบโครงสร้างพื้นฐานด้านน้ำและพลังงานในสหรัฐฯ อิสราเอล สหราชอาณาจักร และไอร์แลนด์ เมื่อปี 2023 โดยเจาะเข้าสู่ Industrial Controller ที่เปิดเผยบนอินเทอร์เน็ต และในกรณีหนึ่งสามารถเข้าควบคุมสถานีสูบน้ำของหน่วยงานประปาในรัฐเพนซิลเวเนียได้

Microsoft ยังพบข้อความ "GRAT" ปรากฏทั้งใน Debug Path ของ FlockWiper และภายในชื่อฟังก์ชันของ GigaWiper ซึ่งเป็นหลักฐานที่เชื่อมโยงเครื่องมือทั้งสองเข้าด้วยกัน และอาจบ่งชี้ว่ายังมีองค์ประกอบอื่นที่ยังไม่ถูกค้นพบ ด้านช่วงเวลาการพบมัลแวร์ ทั้งสองบริษัทให้ข้อมูลแตกต่างกัน โดย Microsoft ระบุว่ากิจกรรมทำลายระบบเริ่มตั้งแต่เดือนตุลาคม 2025 ขณะที่ Binary Defense ตรวจพบไฟล์ชุดเดียวกันในชื่อ BLUERABBIT ครั้งแรกเมื่อเดือนมีนาคม 2026

เป็นส่วนหนึ่งของกระแสการโจมตีที่ใหญ่ขึ้น

ตลอดปี 2025 และ 2026 มีการแจ้งเตือนเกี่ยวกับการโจมตีด้วยมัลแวร์ล้างข้อมูลที่เชื่อมโยงกับอิหร่านและมุ่งเป้าไปยังอิสราเอลหลายครั้ง ทีม Unit 42 ของ Palo Alto Networks รายงานว่าพบการโจมตีในลักษณะเดียวกันเพิ่มขึ้นอย่างต่อเนื่อง โดยส่วนหนึ่งเกี่ยวข้องกับกลุ่ม Handala Hack ขณะที่ในเดือนมีนาคม 2026 หน่วยงาน Israel National Cyber Directorate (INCD) ก็ได้ออกประกาศเตือนองค์กรภายในประเทศเกี่ยวกับการโจมตีด้วยมัลแวร์ล้างข้อมูลจากกลุ่มที่เชื่อมโยงกับอิหร่าน เทคนิคที่ GigaWiper ใช้ไม่ใช่เรื่องใหม่ เพราะ NotPetya ในปี 2017 ก็เคยปลอมตัวเป็น Ransomware ทั้งที่เป้าหมายจริงคือการทำลายข้อมูล การปลอมตัวลักษณะนี้ช่วยให้ผู้โจมตีมีเวลาเพิ่มขึ้น เพราะในช่วงแรกผู้ดูแลระบบอาจเข้าใจว่าเป็นการโจมตีแบบเรียกค่าไถ่ที่ยังมีโอกาสกู้คืนข้อมูล ทั้งที่ความจริงแล้วข้อมูลถูกทำลายไปโดยไม่มีทางกู้กลับ

Microsoft มองว่า GigaWiper สะท้อนแนวโน้มที่ผู้โจมตีนำเครื่องมือหลายประเภทมารวมไว้ในแพลตฟอร์มเดียว สำหรับทีมป้องกันระบบ สิ่งนี้หมายความว่า เมื่อแบ็กดอร์เพียงตัวเดียวสามารถสอดแนม ขโมยข้อมูล หรือทำลายระบบได้ทั้งหมด การพบมัลแวร์เพียงอย่างเดียวก็ไม่สามารถบอกเจตนาของผู้โจมตีได้อีกต่อไป เพราะผู้โจมตีสามารถเลือกใช้ความสามารถที่ต้องการได้หลังจากเข้าควบคุมระบบสำเร็จแล้ว นอกจากนี้ การที่เครื่องมือดังกล่าวยังมีคำสั่งบางส่วนที่ยังไม่เปิดใช้งาน ยังสะท้อนว่า GigaWiper อาจอยู่ระหว่างการพัฒนาและมีความสามารถเพิ่มเติมในอนาคต

สิ่งที่องค์กรควรเฝ้าระวัง

Microsoft ระบุว่าการตรวจจับ GigaWiper ให้ได้ตั้งแต่ระยะแรก ควรสังเกตสัญญาณสำคัญ ได้แก่

- มี Scheduled Task ชื่อ OneDrive Update ที่ถูกตั้งให้ทำงานทุก 1 นาที
- พบทราฟฟิกของ RabbitMQ หรือ Redis ออกจากเครื่องผู้ใช้งานทั่วไป แทนที่จะเป็นเซิร์ฟเวอร์
- พบโปรเซสเรียกใช้คำสั่ง takeown และ icacls เพื่อเข้าครอบครองไฟล์สำคัญสำหรับการบูต เช่น bootmgr และ ntoskrnl.exe นอกช่วงเวลาบำรุงรักษาระบบ

Microsoft ยังแนะนำให้องค์กรเปิดใช้งาน Tamper Protection เพื่อป้องกันไม่ให้ผู้โจมตีปิดการทำงานของโปรแกรมป้องกันไวรัส บล็อกเซิร์ฟเวอร์ควบคุมที่ทราบแล้ว ได้แก่ 185.182.193[.]21 และ 212.8.248[.]104 เปิดใช้งาน Endpoint Detection and Response (EDR) in Block Mode รวมถึง Cloud-delivered Protection และ Automatic Remediation

รายละเอียดเพิ่มเติม เช่น ค่าแฮชของไฟล์ ที่อยู่ของเซิร์ฟเวอร์ และชื่อการตรวจจับต่างๆ ได้ถูกเผยแพร่ไว้ในรายงานของ Microsoft แล้ว

ท้ายที่สุด The Hacker News ระบุว่า ได้ติดต่อ Microsoft และ Binary Defense เพื่อขอให้ยืนยันว่า GigaWiper และ BLUERABBIT เป็นมัลแวร์ตัวเดียวกันหรือไม่ รวมถึงสอบถามรายละเอียดเกี่ยวกับจำนวนผู้ได้รับผลกระทบและการระบุผู้ที่อยู่เบื้องหลังการโจมตี หากมีข้อมูลเพิ่มเติม จะมีการอัปเดตในภายหลัง

ข้อมูลอ้างอิง

Jul 9, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/07/new-gigawiper-windows-backdoor-bundles.html