วันที่ 15 กันยายน 2568

Ransomware HybridPetya ใหม่สามารถหลบเลี่ยง UEFI Secure Boot ด้วยช่องโหว่ CVE-2024-7344

นักวิจัยด้านความปลอดภัยไซเบอร์ได้ค้นพบแรนซัมแวร์สายพันธุ์ใหม่ชื่อ HybridPetya ซึ่งมีความคล้ายกับมัลแวร์ Petya/NotPetya ที่เป็นที่รู้จักดี แต่มีความสามารถพิเศษที่อันตรายกว่ามากคือสามารถเลี่ยงกลไก Secure Boot บนระบบที่ใช้ UEFI (Unified Extensible Firmware Interface) โดยอาศัยช่องโหว่ที่เคยถูกเปิดเผยและอัปเดตแพตช์ไปแล้ว บริษัทความปลอดภัยไซเบอร์จากสโลวาเกีย ESET ระบุว่าตัวอย่างไฟล์ของ HybridPetya ถูกอัปโหลดขึ้นไปบนแพลตฟอร์ม VirusTotal ในเดือนกุมภาพันธ์ 2025

“HybridPetya เข้ารหัสตารางข้อมูลหลักของระบบไฟล์ (Master File Table – MFT) ซึ่งเป็นส่วนที่เก็บข้อมูลสรุปของไฟล์ทั้งหมดบนพาร์ติชันที่ฟอร์แมตเป็น NTFS” นักวิจัยด้านความปลอดภัย มาร์ติน สโมลาร์ กล่าว “แตกต่างจาก Petya/NotPetya ดั้งเดิม HybridPetya สามารถโจมตีระบบสมัยใหม่ที่ใช้ UEFI ได้โดยการติดตั้งโปรแกรม EFI ที่เป็นอันตรายลงบนพาร์ติชัน EFI System Partition”

กล่าวอีกนัยหนึ่ง โปรแกรม UEFI ที่ถูกติดตั้งไว้จะเป็นองค์ประกอบสำคัญที่ทำหน้าที่เข้ารหัสไฟล์ MFT ซึ่งเก็บเมตาดาต้าของไฟล์ทั้งหมดบนพาร์ติชัน NTFS

กลไกการทำงานของ HybridPetya

HybridPetya ประกอบด้วยสองส่วนหลักคือ bootkit และ installer โดย bootkit มีสองเวอร์ชันที่ปรากฏให้เห็น ส่วนที่เป็น bootkit ถูกติดตั้งโดย installer และมีหน้าที่หลักคือโหลดการตั้งค่า (configuration) และตรวจสอบสถานะการเข้ารหัส ซึ่งมีได้สามค่า:

- 0 - พร้อมสำหรับการเข้ารหัส
- 1 - เข้ารหัสแล้ว
- 2 - จ่ายค่าไถ่แล้ว ดิสก์ถูกถอดรหัส

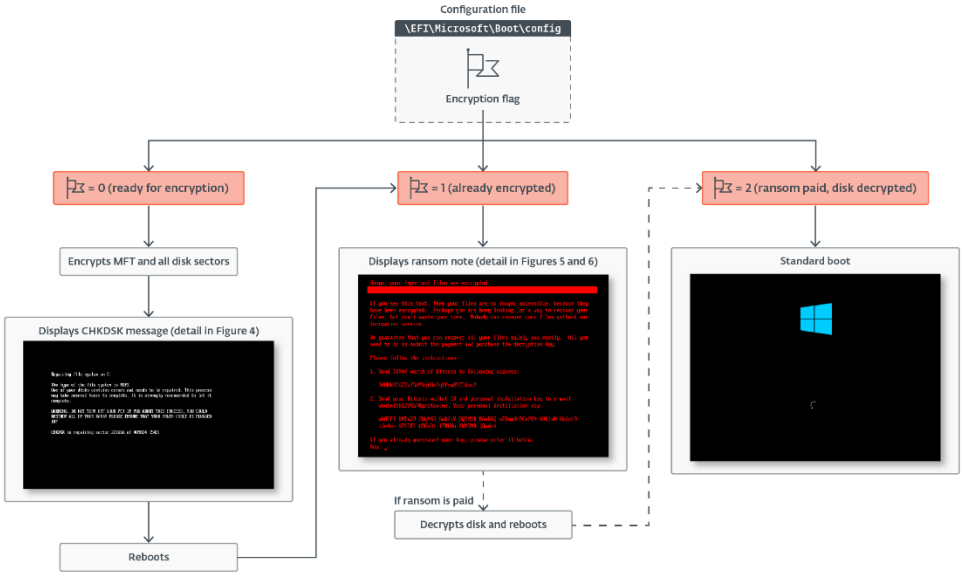
ถ้าค่าเป็น 0 มันจะเปลี่ยนเป็น 1 แล้วเข้ารหัสไฟล์ \EFI\Microsoft\Boot\verify ด้วยอัลกอริธึม Salsa20 นอกจากนี้ยังสร้างไฟล์ชื่อ \EFI\Microsoft\Boot\counter บน EFI System Partition ก่อนเริ่มกระบวนการเข้ารหัสของทุกพาร์ติชันที่เป็น NTFS ไฟล์นี้ใช้เก็บจำนวนคลัสเตอร์ของดิสก์ที่ถูกเข้ารหัสแล้ว เพื่อให้ติดตามสถานะได้

นอกจากนี้ bootkit ยังอัปเดตข้อความ “CHKDSK” ปลอมที่แสดงให้เหยื่อเห็นบนหน้าจอ ให้แสดงข้อมูลสถานะการเข้ารหัสขณะทำงาน เพื่อหลอกให้ผู้ใช้คิดว่าระบบกำลังซ่อมแซมข้อผิดพลาดของดิสก์อยู่ หาก bootkit ตรวจพบว่าดิสก์ถูกเข้ารหัสแล้ว (ค่าเป็น 1) มันจะแสดงโน้ตเรียกค่าไถ่แก่เหยื่อ โดยเรียกเงิน 1,000 ดอลลาร์เป็น Bitcoin ไปยังที่อยู่กระเป๋าเงิน 34UNkKSGZZvf5AYbjkUa2yYYzw89ZLWxu2 ซึ่งปัจจุบันกระเป๋าเงินดังกล่าวว่างอยู่ แต่ระหว่างกุมภาพันธ์ถึงพฤษภาคม 2025 มีเงินเข้าไปรายการหนึ่งเป็นจำนวน $183.32

กระบวนการถอดรหัสและจุดที่แตกต่างจาก NotPetya

หน้าจอเรียกค่าไถ่ยังมีตัวเลือกให้ผู้เสียหายกรอก “deception key” ที่ซื้อจากผู้ปฏิบัติการหลังจ่ายเงิน เมื่อกรอกคีย์ถูกต้อง bootkit จะยืนยันคีย์แล้วพยายามถอดรหัสไฟล์ EFI\Microsoft\Boot\verify หากคีย์ตรง ค่าจะถูกตั้งเป็น 2 และเริ่มขั้นตอนการถอดรหัสโดยอ่านข้อมูลจากไฟล์ \EFI\Microsoft\Boot\counter “การถอดรหัสจะหยุดเมื่อจำนวนคลัสเตอร์ที่ถอดรหัสได้เท่ากับค่าที่อยู่ในไฟล์ counter” สโมลาร์กล่าว “ระหว่างกระบวนการถอดรหัส MFT bootkit จะแสดงสถานะการถอดรหัสให้เห็นแบบเรียลไทม์”

ขั้นตอนการถอดรหัสยังรวมถึงการกู้คืนบูตโหลดเดอร์ของระบบที่ถูกต้อง - \EFI\Boot\bootx64.efi และ \EFI\Microsoft\Boot\bootmgfw.efi - จากสำเนาสำรองที่สร้างขึ้นก่อนติดตั้ง เมื่อเสร็จแล้วผู้ใช้จะถูกแจ้งให้รีบูตเครื่องวินโดวส์



ควรสังเกตว่าการเปลี่ยนแปลงบูตโหลดเดอร์ที่ installer ทำในระหว่างติดตั้ง bootkit UEFI จะทำให้ระบบเกิดการแครช (หรือที่เรียกว่า Blue Screen of Death - BSoD) และบังคับให้ไบนารีของ bootkit ถูกเรียกใช้งานเมื่ออุปกรณ์ถูกเปิดเครื่องครั้งต่อไป

ESET ระบุว่าตัวอย่างของ HybridPetya บางรุ่นพบว่าสามารถใช้ประโยชน์จาก CVE-2024-7344 (คะแนน CVSS: 6.7) ซึ่งเป็นช่องโหว่รันโค้ดจากระยะไกลในแอปพลิเคชัน UEFI ชื่อ Howyar Reloader (reloader.efi ถูกเปลี่ยนชื่อในอาร์ติแฟกต์เป็น \EFI\Microsoft\Boot\bootmgfw.efi) ซึ่งอาจนำไปสู่การเลี่ยง Secure Boot ได้

ตัวไวรัสรุ่นนี้ยังบรรจุไฟล์พิเศษชื่อ cloak.dat ซึ่งสามารถโหลดผ่าน reloader.efi ได้ และภายในไฟล์นี้มีไบนารีของ bootkit ที่ถูก XOR ไว้ Microsoft ได้เพิกถอน (revoke) ไบนารีเก่าที่เปราะบางตัวนั้นเป็นส่วนหนึ่งของการอัปเดต Patch Tuesday ในเดือนมกราคม 2025

“เมื่อไบนารี reloader.efi (ถูกวางเป็น bootmgfw.efi) ถูกเรียกใช้งานในช่วงบูต มันจะค้นหาไฟล์ cloak.dat บน EFI System Partition แล้วโหลดแอปพลิเคชัน UEFI ที่ฝังไว้จากไฟล์นี้ในวิธีที่ไม่ปลอดภัยมาก โดยไม่ตรวจสอบความสมบูรณ์ใดๆ จึงทำให้สามารถเลี่ยงระบบ UEFI Secure Boot ได้” ESET กล่าว

อีกจุดหนึ่งที่ HybridPetya แตกต่างจาก NotPetya คือแทนที่จะทำลายอย่างเดียว ตัวชิ้นงานใหม่นี้อนุญาตให้ผู้โจมตีสร้างคีย์ถอดรหัสคืนจากคีย์การติดตั้งส่วนบุคคลของผู้เสียหายได้

UEFI และภัยคุกคามใหม่

จากเทเลเมทรีของ ESET ยังไม่พบหลักฐานว่า HybridPetya ถูกใช้โจมตีในวงกว้าง บริษัทความปลอดภัยยังชี้ว่าเมื่อเร็วๆ นี้มีการค้นพบ Proof-of-Concept (PoC) ของ UEFI Petya โดยนักวิจัยด้านความปลอดภัย Aleksandra “Hasherezade”

Doniec และเป็นไปได้ว่าอาจมีความสัมพันธ์บางอย่างระหว่างสองกรณีนี้ แต่ ESET ก็ไม่ได้ตัดทิ้งความเป็นไปได้ว่า HybridPetya อาจเป็น PoC เช่นกัน

“ณ ตอนนี้ HybridPetya ถือเป็นตัวอย่างที่สี่ที่เป็นที่รู้จักของบูตคิต UEFI จริงหรือ PoC ที่มีความสามารถเลี่ยง UEFI Secure Boot โดยก่อนหน้านี้มี BlackLotus (ใช้ประโยชน์จาก CVE-2022-21894), BootKitty (ใช้ประโยชน์จาก LogoFail), และ Hyper-V Backdoor PoC (ใช้ประโยชน์จาก CVE-2020-26200)” ESET กล่าว “นี่แสดงให้เห็นว่าการเลี่ยง Secure Boot ไม่ใช่เรื่องเป็นไปไม่ได้ แต่กำลังเป็นเรื่องที่พบได้บ่อยขึ้นและน่าสนใจทั้งสำหรับนักวิจัยและผู้โจมตี”

UEFI ซึ่งเป็นทายาทของ BIOS (Basic Input/Output System) เป็นเป้าหมายที่มีค่ามากสำหรับผู้โจมตี เพราะ UEFI ทำงานก่อนระบบปฏิบัติการในช่วงบูต หากมัลแวร์สามารถแทรกตัวในกระบวนการบูตได้ มันจะสามารถเลี่ยงซอฟต์แวร์ความปลอดภัยแบบเดิมๆ, รันโค้ดด้วยสิทธิ์ระดับสูง และทำให้ยากต่อการตรวจจับและกำจัด

การค้นพบ HybridPetya เกิดขึ้นพร้อมกับที่นักวิจัยความปลอดภัยจาก FFRI Security - Kazuki Matsuo นำเสนอเทคนิคชื่อ Shade BIOS ซึ่งอนุญาตให้มัลแวร์ทำงานได้โดยแยกจากการป้องกันระดับระบบปฏิบัติการทั้งหมดและทำกิจกรรมที่เป็นอันตรายโดยไม่ต้องพึ่งพาฮาร์ดแวร์ในระหว่างรันไทม์ Shade BIOS ถูกอธิบายว่าเป็นมัลแวร์ “แบบบริสุทธิ์บน BIOS” (pure-BIOS) ที่คง BIOS ไว้ในหน่วยความจำแม้หลังจากระบบปฏิบัติการบูตขึ้นแล้ว ทำให้ยังสามารถใช้ฟังก์ชันของ UEFI และใช้ไดรเวอร์ในระหว่างรันไทม์ ซึ่งให้พลังในการล้วงและทำลายการป้องกันไซเบอร์แทบทุกชนิด

Shade BIOS “แยกมัลแวร์ UEFI ออกจากการป้องกันระดับระบบปฏิบัติการ” Matsuo กล่าว ในการนำเสนอที่ Black Hat 2025 เมื่อเดือนที่ผ่านมา และว่าเทคนิคนี้ไม่จำเป็นต้องรู้ว่าอุปกรณ์เป้าหมายใช้ฮาร์ดแวร์แบบใด หรือจำเป็นต้องเขียนสแตกไดรเวอร์ทั้งหมดหรือเข้าถึง I/O โดยตรง

ข้อมูลอ้างอิง

Sep 12, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/09/new-hybridpetya-ransomware-bypasses.html