วันที่ 25 สิงหาคม 2569

Microsoft Defender มีไดรเวอร์ของตัวเองที่สามารถถูกนำไปใช้ลบซอฟต์แวร์รักษาความปลอดภัย

Check Point Research เปิดเผยเทคนิคที่ใช้ไดรเวอร์สำหรับแก้ไขปัญหาของ Microsoft Defender ซึ่งมีลายเซ็นถูกต้องและทำงานตั้งแต่ช่วงเริ่มเปิดเครื่อง เพื่อนำมาใช้ดำเนินการกับไฟล์และ Registry ในระดับ Kernel บนระบบ Windows ตั้งแต่ Windows 7 จนถึง Windows 11 25H2 โดยไม่จำเป็นต้องอาศัยช่องโหว่ของซอฟต์แวร์ และไม่ต้องนำไดรเวอร์จากภายนอกเข้ามาในเครื่อง

ไดรเวอร์ดังกล่าวมีชื่อว่า BTR.sys (Boot Time Removal Tool) และเป็นส่วนประกอบที่ Windows จำเป็นต้องมี ซึ่งหมายความว่า ไม่สามารถเพิ่มไดรเวอร์นี้เข้าไปใน Microsoft's Vulnerable Driver Blocklist หรือบล็อกผ่าน Windows Defender Application Control (WDAC) ได้โดยไม่กระทบต่อการทำงานของ Defender เอง

Jiří Vinopal นักวิจัยด้านภัยคุกคามและผู้เชี่ยวชาญด้าน Reverse Engineering จาก Check Point Research ได้นำเสนอผลการค้นพบนี้ในการบรรยายหลักบนเวที Black Hat USA 2026 และ DEF CON 34 ที่เมืองลาสเวกัส พร้อมเผยแพร่เอกสารวิจัยและเครื่องมือ Proof-of-Concept ชื่อ BTR_CLI เมื่อวันที่ 20 สิงหาคม 2026 โดย Check Point Research ระบุว่ายังไม่พบหลักฐานว่าเทคนิคดังกล่าวถูกนำไปใช้ในการโจมตีจริง

จากการวิเคราะห์ตัวอย่างและข้อมูล Telemetry ทั้งหมดที่เราเก็บรวบรวมมา เราไม่พบหลักฐานการนำ BTR.sys ไปใช้โจมตีจริงในลักษณะที่แสดงให้เห็นในการวิจัยนี้ ซึ่งแสดงให้เห็นว่าเทคนิคดังกล่าวยังไม่เป็นที่รู้จักหรือยังไม่ได้ถูกนำไปใช้โดยกลุ่มผู้โจมตี ทำให้ยังสามารถพัฒนาระบบตรวจจับเชิงรุกได้ก่อนที่เทคนิคนี้จะถูกนำไปใช้งานจริงในวงกว้าง Check Point Research ระบุ

BTR.sys ถูกฝังอยู่ภายใน MpEngine.dll ของ Defender ในรูปแบบ Resource ที่ชื่อว่า BOOTTIMETOOL และจะถูกนำมาใช้งานเมื่อ Defender จำเป็นต้องดำเนินการลบมัลแวร์ให้เสร็จสิ้นหลังจากรีบูตเครื่อง โดยสามารถลบไฟล์หรือรายการ Registry ที่ถูกล็อกไว้ในขณะที่ Windows กำลังทำงาน

Vinopal ทำ Reverse Engineering กับโปรโตคอลการทำงานของไดรเวอร์ที่เป็นกรรมสิทธิ์และไม่มีการเปิดเผยรายละเอียดต่อสาธารณะ และพบว่า Configuration Blob ทุกชุดที่ส่งให้ BTR.sys จะถูกเข้ารหัสด้วย RC4 โดยใช้คีย์ขนาด 256 ไบต์ที่ถูกกำหนดไว้ตายตัวในส่วน .rdata ของ BTR.sys ทุกเวอร์ชันที่ถูกส่งมาพร้อม Windows ตั้งแต่ Windows 7 โดยมีการตรวจสอบแล้วว่าไม่เปลี่ยนแปลงใน BTR.sys แบบ 64-bit จำนวน 18 เวอร์ชันที่แตกต่างกัน

BTR_CLI ซึ่งเป็นเครื่องมือ Proof-of-Concept จะค้นหา MpEngine.dll ภายใต้โฟลเดอร์ Defender Definition Updates และดึงไฟล์ไบนารี BTR.sys ที่ฝังอยู่ภายในออกมา

จากนั้นเครื่องมือจะสร้าง Transaction ที่เข้ารหัสอย่างถูกต้อง ก่อนติดตั้งไดรเวอร์เป็น Service ผ่านการเขียน Registry ใน HKLM โดยตรง และกำหนดค่า Type=1, Start=1 และ Group="Boot Bus Extender" วิธีการนี้สามารถข้าม Service Control Manager ได้ทั้งหมด และไม่สร้าง Event ID 7045 ของ Windows ซึ่งเป็นเหตุการณ์ที่ระบุว่า Service ถูกติดตั้ง

เมื่อถูกโหลด BTR.sys จะดำเนินการตามคำสั่งที่ถูกเตรียมไว้จาก Ring 0 โดยข้อมูล Telemetry จะระบุว่าการทำงานมาจาก System process (PID 4) และสามารถลบไฟล์และไดเรกทอรีที่ถูกล็อกอยู่ ย้ายไฟล์ไปยังตำแหน่งใดก็ได้ รวมถึง System32\drivers ลบ Registry Key และ Value รวมถึงเขียน Registry Value ใหม่ได้ทุกประเภท

การทำงานอีกโหมดหนึ่งสามารถตั้งเวลาให้คำสั่งเหล่านี้ถูกดำเนินการในระหว่างการรีบูตครั้งถัดไป จากนั้นไดรเวอร์จะทำงานในช่วงที่ Vinopal เรียกว่า “golden window” ซึ่งเป็นช่วงเวลาหลังจาก File System สามารถเขียนข้อมูลได้แล้ว แต่ก่อนที่ Service ของ Defender ในระดับ User Mode จะเริ่มทำงาน ทำให้ BTR.sys สามารถลบไฟล์ไบนารีของระบบรักษาความปลอดภัย เช่น WdFilter.sys และ MsMpEng.exe ได้ ก่อนที่ไฟล์เหล่านี้จะสามารถป้องกันตัวเองด้วยการล็อกไฟล์

การสาธิตแบบสดในงาน Black Hat แสดงให้เห็นว่า BTR_CLI สามารถลบส่วนประกอบทั้งหมดของ Defender ออกจากเครื่อง Windows 11 25H2 ที่ได้รับการอัปเดตล่าสุดและเปิดใช้งาน Tamper Protection อยู่ได้

การใช้เทคนิคนี้จำเป็นต้องมีบัญชีผู้ดูแลระบบที่มีสิทธิ์ SeLoadDriverPrivilege โดย BTR_CLI สามารถเปิดใช้งานสิทธิ์ดังกล่าวโดยอัตโนมัติสำหรับบัญชีที่มีสิทธิ์นี้อยู่แล้ว

แตกต่างจากการโจมตีที่ใช้เทคนิค Bring Your Own Vulnerable Driver (BYOVD) ซึ่งต้องอาศัยไดรเวอร์จากผู้ผลิตรายอื่นที่มีช่องโหว่และมีลายเซ็นถูกต้อง และสามารถนำไดรเวอร์เหล่านั้นเข้าสู่รายการบล็อกได้ เทคนิค BTR Reforged ใช้ไดรเวอร์ที่มีอยู่ใน Windows ทุกเครื่องตั้งแต่ Windows 7 เป็นต้นมา

ประเด็นนี้ไม่ใช่ช่องโหว่ในความหมายแบบทั่วไป แต่เป็นเรื่องของขอบเขตความเชื่อถือในสถาปัตยกรรม ซึ่งสามารถถูกข้ามได้หากผู้โจมตีมีสิทธิ์ระดับผู้ดูแลระบบอยู่ก่อนแล้ว หลังจากมีการเปิดเผยข้อมูลตามกระบวนการที่เหมาะสม MSRC ยืนยันว่าผลการค้นพบนี้ไม่เข้าเกณฑ์ที่จะต้องออกแพตช์โดยทันที เนื่องจากเทคนิคดังกล่าวต้องอาศัยสิทธิ์ระดับผู้ดูแลระบบที่มีอยู่ก่อนแล้ว (SeLoadDriverPrivilege) Check Point Research ระบุใน เอกสารวิจัย

Repository ของ BTR_CLI บน GitHub ที่จัดทำโดย Vinopal ระบุเพิ่มเติมว่า “No patch is planned” หรือ “ยังไม่มีแผนออกแพตช์” อย่างไรก็ตาม Microsoft ยังไม่ได้ยืนยันข้อความดังกล่าวต่อสาธารณะ

ก่อนหน้านี้ BTR.sys เคยถูกนักวิจัยด้านความปลอดภัยตรวจสอบจากช่องโหว่อีกประเภทหนึ่งในไดรเวอร์เดียวกันเมื่อ 5 ปีก่อน ในเดือนกุมภาพันธ์ 2021 Kasif Dekel นักวิจัยจาก SentinelLabs เปิดเผยช่องโหว่ CVE-2021-24092 ซึ่งเป็นช่องโหว่ยกระดับสิทธิ์ที่ทำให้ผู้ใช้ในเครื่องซึ่งไม่มีสิทธิ์ผู้ดูแลระบบสามารถเขียนทับไฟล์ใดๆ ได้ โดยการสร้าง Hard Link ไว้ที่ตำแหน่งไฟล์ Log ของไดรเวอร์ Microsoft ได้ออกแพตช์แก้ไข CVE-2021-24092 เมื่อวันที่ 9 กุมภาพันธ์ 2021

“เราคาดว่าช่องโหว่นี้ยังไม่ถูกค้นพบจนถึงตอนนี้ เนื่องจากโดยปกติแล้วไดรเวอร์จะไม่ได้อยู่บนฮาร์ดดิสก์ แต่จะถูกนำออกมาและเปิดใช้งานเมื่อจำเป็น โดยใช้ชื่อแบบสุ่ม จากนั้นจึงถูกลบออก” Kasif Dekel กล่าวใน รายงานการเปิดเผยช่องโหว่ของ SentinelLabs

การนำไดรเวอร์ที่มีอยู่ใน Windows มาใช้เป็นเครื่องมือระดับ Kernel สำหรับการโจมตี แทนการใช้ไดรเวอร์จากผู้ผลิตรายอื่นที่มีช่องโหว่ เคยถูกสาธิตมาก่อนในกรณีของ FIN7's AvNeutralizer ซึ่งใช้ไดรเวอร์ Windows ProcLaunchMon.sys ร่วมกับไดรเวอร์ของ Process Explorer เพื่อแก้ไขหรือปิดการทำงานของซอฟต์แวร์รักษาความปลอดภัยบน Endpoint

งานวิจัยนี้เริ่มต้นขึ้นระหว่างการตรวจสอบเหตุการณ์ที่ระบบถูกบุกรุก ซึ่งพบข้อมูล Telemetry บางส่วนของ Endpoint ที่ดูน่าสงสัย แต่ท้ายที่สุดกลับพบว่ามีต้นเหตุมาจากกิจกรรมการแก้ไขมัลแวร์ที่ถูกต้องตามปกติของ Windows Defender Check Point Research ระบุในเอกสารวิจัย

Check Point Research ระบุเงื่อนไขจาก Sysmon และ Windows Event ที่สามารถใช้เป็นตัวบ่งชี้ว่ามีการนำ BTR.sys ไปใช้งานในลักษณะที่น่าสงสัย ได้แก่

- Sysmon Event ID 15 (FileCreateStreamHash) ซึ่งชื่อไฟล์เป้าหมายลงท้ายด้วย .sys:changelist โดยเป็นการบันทึก Alternate Data Stream ที่มี Configuration ซึ่งถูกเข้ารหัสและเขียนลงในไฟล์ไดรเวอร์
- RegistryEvent (Sysmon Event ID 12 หรือ 13) ที่มีการสร้าง Service Key ซึ่งค่า Args มี :changelist และ Group เป็น "Boot Bus Extender" โดยเฉพาะกรณีที่ไม่พบ Windows Event ID 7045 (Service Installed) ประกอบกัน
- Sysmon Event ID 11 (FileCreate) และ 23 (FileDelete) ที่แสดงการสร้างและลบไฟล์ \SystemRoot\Temp\BootClean.log อย่างรวดเร็วโดย System process (PID 4) ซึ่งเป็นตำแหน่ง Log ที่กำหนดไว้ตายตัวในไดรเวอร์และจะเกิดขึ้นไม่ว่าผู้เรียกใช้งานจะเป็นใคร
- Sysmon Event ID 6 (DriverLoad) ที่ตามมาทันทีด้วย Sysmon Event ID 23 (FileDelete) และระบุว่าเป็นการทำงานของ System process (PID 4) ซึ่งเป็นลักษณะเฉพาะของการเรียกใช้ BTR.sys ในโหมด Kernel ที่กำลังทำงานอยู่

Check Point Research ยังแนะนำให้จำกัดการกำหนดสิทธิ์ SeLoadDriverPrivilege ให้กับบัญชีที่จำเป็นต้องใช้งาน โดยถือเป็นมาตรการหลักในการลดความเสี่ยง

BTR_CLI สามารถเข้าถึงได้ผ่าน github.com/Dump-GUY/BTR_CLI ภายใต้สัญญาอนุญาต MIT โดย Repository มีไฟล์ไบนารีที่สร้างไว้ล่วงหน้าสำหรับระบบ x64 และ x86 อยู่ในส่วน Releases

The Hacker News ได้ติดต่อ Microsoft เพื่อขอความคิดเห็นเกี่ยวกับจุดยืนของบริษัทต่อเทคนิคที่ใช้ BTR.sys รวมถึงติดต่อ Check Point Research เพื่อขอรายละเอียดทางเทคนิคเพิ่มเติม แต่ทั้งสองฝ่ายยังไม่ได้ตอบกลับก่อนที่บทความจะเผยแพร่

ข้อมูลอ้างอิง

Aug 21, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/08/microsoft-defenders-own-driver-can-be.html