วันที่ 30 ตุลาคม 2568

แฮ็กเกอร์รัสเซียโจมตีองค์กรในยูเครนด้วยเทคนิค "Living-Off-the-Land"

รายงานล่าสุดจากทีม Symantec และ Carbon Black Threat Hunter ได้เปิดเผยถึงปฏิบัติการโจมตีทางไซเบอร์ที่ซับซ้อน โดยกลุ่มผู้ไม่หวังดีที่มีต้นตอจากรัสเซีย ซึ่งมุ่งเป้าไปที่องค์กรต่าง ๆ ในยูเครน โดยเป้าหมายหลักคือการขโมยข้อมูลสำคัญและรักษาการเข้าถึงเครือข่ายที่ถูกบุกรุกไว้ให้ได้นานที่สุด

การโจมตีนี้ประสบความสำเร็จในการแทรกซึมบริษัทด้านบริการรายใหญ่ในยูเครนได้นานถึงสองเดือนเต็ม และยังโจมตีหน่วยงานรัฐบาลท้องถิ่นอีกแห่งหนึ่งเป็นเวลาหนึ่งสัปดาห์

กลยุทธ์ Living-Off-the-Land (LotL): เน้นเครื่องมือถูกต้องตามกฎหมาย

หัวใจสำคัญของการโจมตีครั้งนี้คือการใช้เทคนิค "Living-off-the-Land" (LotL) ร่วมกับเครื่องมือที่ใช้งานได้ทั้งในทางปกติและทางร้าย (dual-use tools) แฮ็กเกอร์ใช้มัลแวร์ในปริมาณน้อยที่สุด เพื่อลดร่องรอยทางดิจิทัลและหลบหลีกการตรวจจับให้นานที่สุด

ทีมความปลอดภัยของ Broadcom กล่าวว่า “แฮ็กเกอร์ได้เข้าถึงเครือข่ายของบริษัทบริการรายใหญ่ โดยการติดตั้งเว็บเชลล์ (webshell) บนเซิร์ฟเวอร์ที่เปิดให้ใช้งานจากภายนอก ซึ่งคาดว่าน่าจะเกิดจากการโจมตีช่องโหว่ที่ยังไม่ได้อัปเดตแพตช์”

เว็บเชลล์ที่ถูกใช้ชื่อว่า “Localolive” ซึ่งเคยถูก Microsoft ตรวจพบว่าเป็นเครื่องมือที่กลุ่มย่อยของกลุ่ม “Sandworm” (กลุ่มแฮ็กเกอร์รัสเซียที่เชื่อมโยงกับรัฐบาล) ใช้ภายใต้ปฏิบัติการ “BadPilot” โดย Localolive ถูกออกแบบมาเพื่อส่งต่อ payload ขั้นต่อไป เช่น Chisel, plink และ rsockstun และมีการใช้งานมาอย่างน้อยตั้งแต่ปลายปี 2021

ไทม์ไลน์การโจมตี: การสอดแนมอย่างละเอียด

สัญญาณแรกของกิจกรรมที่น่าสงสัยเริ่มตั้งแต่วันที่ 27 มิถุนายน 2025 หลังจากติดตั้งเว็บเชลล์ แฮ็กเกอร์ได้ทำการสอดแนมและดำเนินการหลายอย่างที่แสดงถึงความเข้าใจอย่างลึกซึ้งในระบบ Windows:

- **ช่วงแรก**: ใช้คำสั่ง PowerShell เพื่อยกเว้นโฟลเดอร์ Downloads จากการสแกนของ Microsoft Defender Antivirus และตั้งตารางงาน (Scheduled Task) ให้ทำการ dump หน่วยความจำทุก ๆ 30 นาที
- **2 สัปดาห์ต่อมา:** บันทึกข้อมูล registry hive ลงในไฟล์ชื่อ “1.log” และติดตั้งเว็บเชลล์เพิ่มเติม ใช้เว็บเชลล์เพื่อแสดงรายการไฟล์ทั้งหมดในโฟลเดอร์ผู้ใช้
- **เป้าหมาย KeePass**: รันคำสั่งเพื่อแสดง process ทั้งหมดที่ขึ้นต้นด้วยคำว่า “kee” ซึ่งน่าจะมุ่งเป้าไปที่โปรแกรมเก็บรหัสผ่าน KeePass
- **การควบคุมระยะไกล:** แสดงรายการ session ผู้ใช้ที่กำลังใช้งานอยู่ในเครื่องที่สอง และใช้คำสั่งสอดแนมในเครื่องที่สาม พร้อมทำการ dump หน่วยความจำด้วยเครื่องมือ Microsoft Windows Resource Leak Diagnostic (RDRLeakDiag)
- **การสร้างช่องทางถาวร**: แก้ไขค่า registry เพื่ออนุญาตให้เชื่อมต่อ RDP จากภายนอกได้ ใช้คำสั่ง PowerShell เพื่อดึงข้อมูลการตั้งค่าของระบบ Windows ในเครื่องที่สี่
- **เครื่องมือแฮ็ก**: รันโปรแกรม RDPclip เพื่อเข้าถึงข้อมูลคลิปบอร์ดของการเชื่อมต่อ Remote Desktop และติดตั้ง OpenSSH เพื่อใช้เข้าถึงเครื่องจากระยะไกล พร้อมใช้คำสั่ง PowerShell เพื่อเปิดพอร์ต TCP 22
- **การฝัง Backdoor**: สร้าง Scheduled Task เพื่อรัน PowerShell backdoor ที่ไม่ทราบชนิดชื่อ “link.ps1” ทุก 30 นาที โดยใช้บัญชีผู้ใช้ในโดเมนรันสคริปต์ภาษา Python ที่ไม่ทราบหน้าที่
- **เครื่องมือ Dual-Use**: ติดตั้งโปรแกรมบริหารจัดการเราเตอร์ MikroTik ของแท้ (“winbox64.exe”) ลงในโฟลเดอร์ Downloads (ซึ่งเครื่องมือนี้เคยถูก CERT-UA บันทึกว่าเกี่ยวข้องกับแคมเปญของ Sandworm ที่โจมตีหน่วยงานด้านพลังงาน)

บทสรุป: ความชำนาญที่แทบไม่ทิ้งร่องรอย

Symantec และ Carbon Black ระบุว่าแม้ไม่พบหลักฐานชัดเจนที่เชื่อมโยงการโจมตีครั้งนี้กับกลุ่ม Sandworm แต่มีแนวโน้มสูงว่าเป็นฝีมือของกลุ่มที่มีต้นทางจากรัสเซีย

“แม้ผู้โจมตีจะใช้มัลแวร์เพียงเล็กน้อยในกระบวนการโจมตี แต่กิจกรรมส่วนใหญ่ที่เกิดขึ้นล้วนใช้เครื่องมือที่ถูกต้องตามระบบ ไม่ว่าจะเป็นโปรแกรมที่มีอยู่ใน Windows อยู่แล้ว หรือซอฟต์แวร์ที่สามารถใช้ได้ทั้งในทางดีและทางร้าย”

“ผู้โจมตีแสดงให้เห็นถึงความเข้าใจอย่างลึกซึ้งเกี่ยวกับเครื่องมือใน Windows และพิสูจน์ให้เห็นว่าผู้เชี่ยวชาญสามารถโจมตีและขโมยข้อมูลสำคัญ เช่น ข้อมูลรับรองผู้ใช้ ได้โดยแทบไม่ทิ้งร่องรอยใด ๆ ในเครือข่ายเป้าหมาย”

ภัยคุกคามอื่น ๆ: WinRAR และการควบคุมของรัฐรัสเซีย

การเปิดเผยครั้งนี้เกิดขึ้นพร้อมกับรายงานจาก Gen Threat Labs ที่เตือนว่ากลุ่ม Gamaredon ใช้ช่องโหว่ในโปรแกรม WinRAR ที่ได้รับการแพตช์แล้ว (CVE-2025-8088, คะแนน CVSS: 8.8) เพื่อโจมตีหน่วยงานรัฐบาลในยูเครน โดยหลอกให้ผู้ใช้เปิดไฟล์ PDF ที่ภายในมีการฝังไฟล์ RAR ซึ่งสามารถวางมัลแวร์ HTA ลงในโฟลเดอร์ Startup ได้โดยอัตโนมัติ

นอกจากนี้ รายงานยังสอดคล้องกับข้อมูลจาก Recorded Future ที่ระบุว่ารัฐบาลเครมลินกำลังปรับความสัมพันธ์กับกลุ่มอาชญากรรมไซเบอร์รัสเซียจาก “การปล่อยปละละเลย” มาเป็น “การควบคุมโดยตรง” ผ่านปฏิบัติการระหว่างประเทศอย่าง “Operation Endgame”

- **ความสัมพันธ์ซับซ้อน:** บุคคลระดับสูงในกลุ่มอาชญากรรมไซเบอร์มักมีความสัมพันธ์กับหน่วยข่าวกรองรัสเซีย ทั้งในรูปแบบการให้ข้อมูล รับภารกิจ หรือใช้การเมืองเพื่อให้รอดพ้นจากการจับกุม
- **การปรับตัว:** กลุ่มอาชญากรรมไซเบอร์เริ่มกระจายอำนาจการทำงาน เพื่อลดความเสี่ยงจากการถูกตรวจจับ
- **ข้อตกลงลับ:** รัฐบาลใช้กลยุทธ์ “เลือกได้หลายแบบ” เช่น รับสมัครผู้เชี่ยวชาญ เพิกเฉยต่อการโจมตีที่สอดคล้องกับผลประโยชน์ หรือบังคับใช้กฎหมายเมื่อผู้โจมตีกลายเป็น “ภาระทางการเมือง”

“โลกอาชญากรรมไซเบอร์ใต้ดินของรัสเซียกำลังแตกร้าวภายใต้แรงกดดันทั้งจากการควบคุมของรัฐและความไม่ไว้วางใจกันภายใน ขณะที่การเฝ้าสังเกตในฟอรัมลับและการสนทนาของกลุ่มแรนซัมแวร์เผยให้เห็นถึงความหวาดระแวงที่เพิ่มขึ้นในหมู่ผู้ปฏิบัติการ” รายงานสรุป

ข้อมูลอ้างอิง

Oct 29, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/10/russian-hackers-target-ukrainian.html