วันที่ 13 พฤษภาคม 2569

ช่องโหว่ cPanel CVE-2026-41940 กำลังถูกโจมตีอย่างต่อเนื่องเพื่อติดตั้งแบ็กดอร์ Filemanager

กลุ่มผู้ไม่หวังดีที่ใช้ชื่อว่า Mr_Rot13 ถูกระบุว่าเป็นผู้ที่ใช้ประโยชน์จากช่องโหว่ร้ายแรงล่าสุดของ cPanel เพื่อฝังแบ็กดอร์ที่มีชื่อว่า Filemanager ลงในระบบที่ถูกเจาะสำเร็จ การโจมตีครั้งนี้อาศัยช่องโหว่ CVE-2026-41940 ซึ่งส่งผลกระทบต่อ cPanel และ WebHost Manager (WHM) โดยช่องโหว่นี้อาจทำให้ผู้โจมตีสามารถข้ามขั้นตอนการยืนยันตัวตน และเข้าควบคุมระบบบริหารจัดการเว็บไซต์ได้ในระดับสูง

จากรายงานล่าสุดของ QiAnXin XLab ระบุว่า หลังจากมีการเปิดเผยช่องโหว่นี้ต่อสาธารณะเมื่อช่วงปลายเดือนที่ผ่านมา ได้มีหลายกลุ่มผู้โจมตีเริ่มนำช่องโหว่นี้ไปใช้ทันที โดยก่อให้เกิดกิจกรรมที่เป็นอันตรายหลายรูปแบบ เช่น การติดตั้งโปรแกรมขุดคริปโทเคอร์เรนซี การปล่อยแรนซัมแวร์ การแพร่กระจายมัลแวร์แบบบอตเน็ต และการฝังแบ็กดอร์เพื่อให้กลับเข้ามาควบคุมระบบได้อีกในภายหลัง

สถานการณ์การโจมตีทั่วโลก

นักวิจัยของ XLab ระบุว่า ข้อมูลจากระบบเฝ้าระวังพบว่า ขณะนี้มีที่อยู่ IP ของผู้โจมตีกว่า 2,000 รายการจากทั่วโลก ที่กำลังใช้ระบบอัตโนมัติเพื่อโจมตีและก่ออาชญากรรมไซเบอร์ผ่านช่องโหว่นี้ โดย IPเหล่านี้กระจายอยู่ในหลายภูมิภาค และส่วนใหญ่มาจากประเทศเยอรมนี สหรัฐอเมริกา บราซิล เนเธอร์แลนด์ และประเทศอื่นๆ

เทคนิคและขั้นตอนการโจมตี

จากการวิเคราะห์เพิ่มเติม พบว่าสคริปต์ที่ใช้ในการโจมตีจะอาศัยคำสั่ง wget หรือ curl เพื่อดาวน์โหลดโปรแกรมที่เขียนด้วยภาษาGo จากเซิร์ฟเวอร์ภายนอก (cp.dene[.]de[.]com) โดยโปรแกรมดังกล่าวมีหน้าที่ฝังคีย์ SSH สาธารณะของผู้โจมตีลงในระบบ เพื่อให้สามารถกลับเข้ามาใช้งานเครื่องได้อย่างต่อเนื่องในอนาคต

นอกจากนี้ ยังมีการติดตั้ง PHP Web Shell ซึ่งเป็นเครื่องมือที่ช่วยให้ผู้โจมตีสามารถอัปโหลดและดาวน์โหลดไฟล์ รวมถึงสั่งรันคำสั่งต่างๆ บนเซิร์ฟเวอร์จากระยะไกลได้ จากนั้น Web Shell จะถูกใช้เพื่อแทรกโค้ดJavaScript ลงในหน้าเว็บไซต์ เพื่อแสดงหน้าล็อกอินปลอมที่ถูกปรับแต่งขึ้นมาโดยเฉพาะสำหรับขโมยชื่อผู้ใช้และรหัสผ่าน ก่อนส่งข้อมูลดังกล่าวไปยังเซิร์ฟเวอร์ของผู้โจมตี (wrned[.]com) ซึ่งถูกเข้ารหัสด้วยเทคนิค ROT13

การติดตั้งแบ็กดอร์ข้ามแพลตฟอร์มและขโมยข้อมูล

หลังจากขโมยข้อมูลสำเร็จ ขั้นตอนสุดท้ายของการโจมตีคือการติดตั้งแบ็กดอร์แบบข้ามแพลตฟอร์ม ซึ่งสามารถทำงานได้ทั้งบน Microsoft Windows, macOS และ Linux โปรแกรมที่ใช้ในการแพร่กระจายมัลแวร์ยังสามารถรวบรวมข้อมูลสำคัญจากเครื่องที่ถูกโจมตีได้อีกด้วย เช่น ประวัติการใช้คำสั่งใน Bash ข้อมูล SSH รายละเอียดของอุปกรณ์ รหัสผ่านฐานข้อมูล และข้อมูล cPanel Virtual Aliases (valiases) ก่อนส่งข้อมูลทั้งหมดไปยังกลุ่ม Telegramที่มีสมาชิกเพียง 3 คน ซึ่งถูกสร้างขึ้นโดยผู้ใช้ที่ใช้ชื่อว่า “0xWR”

ในกรณีที่ XLab วิเคราะห์ แบ็กดอร์ Filemanagerถูกติดตั้งผ่านสคริปต์ที่ดาวน์โหลดจากโดเมน wpsock[.]com โดยแบ็กดอร์นี้รองรับความสามารถหลัก ได้แก่ การจัดการไฟล์ การสั่งรันคำสั่งจากระยะไกล และการเปิดเชลล์เพื่อควบคุมระบบโดยตรง

การแฝงตัวอย่างยาวนานของกลุ่มผู้โจมตี

นอกจากนี้ ยังมีหลักฐานที่บ่งชี้ว่าผู้โจมตีรายนี้อาจดำเนินกิจกรรมอย่างเงียบๆ มาเป็นเวลาหลายปี โดยประเมินจากการที่โดเมนควบคุมการทำงาน (C2) ซึ่งถูกฝังอยู่ในโค้ด JavaScript เดียวกัน เคยถูกใช้ใน PHP Backdoor ที่ชื่อ helper.php ซึ่งถูกอัปโหลดขึ้นสู่ VirusTotal ตั้งแต่เดือนเมษายน 2022 ขณะที่โดเมนดังกล่าวถูกจดทะเบียนครั้งแรกตั้งแต่เดือนตุลาคม 2020

XLab สรุปว่า ตลอดระยะเวลา 6 ปี ตั้งแต่ปี 2020 จนถึงปัจจุบัน ตัวอย่างมัลแวร์และโครงสร้างพื้นฐานที่เกี่ยวข้องกับ Mr_Rot13 แทบไม่ถูกตรวจพบโดยผลิตภัณฑ์ด้านความปลอดภัย ทำให้ปฏิบัติการของกลุ่มนี้สามารถดำเนินต่อไปได้โดยไม่เป็นที่สังเกต

ข้อมูลอ้างอิง

May 11, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/05/cpanel-cve-2026-41940-under-active.html