วันที่ 7 พฤษภาคม 2569

ช่องโหว่ Critical ใน cPanel ถูกนำไปใช้โจมตี เป้าหมายเป็นหน่วยงานรัฐและเครือข่าย MSP

มีการตรวจพบผู้ไม่หวังดีรายใหม่ที่ก่อนหน้านี้ยังไม่เป็นที่รู้จัก กำลังโจมตีหน่วยงานรัฐบาลและกองทัพในภูมิภาคเอเชียตะวันออกเฉียงใต้ รวมถึงกลุ่มผู้ให้บริการ Managed Service Providers (MSPs) และผู้ให้บริการโฮสติ้งบางส่วนในประเทศฟิลิปปินส์ ลาว แคนาดา แอฟริกาใต้ และสหรัฐอเมริกา โดยอาศัยช่องโหว่ที่เพิ่งถูกเปิดเผยใน cPanel

เหตุการณ์นี้ถูกตรวจพบโดย Ctrl-Alt-Intel เมื่อวันที่2 พฤษภาคม 2026 โดยเป็นการโจมตีผ่านช่องโหว่CVE-2026-41940 ซึ่งเป็นช่องโหว่ระดับร้ายแรงใน cPanelและ WebHost Manager (WHM) ที่อาจทำให้ผู้โจมตีสามารถข้ามขั้นตอนการยืนยันตัวตน และเข้าควบคุมระบบได้ในระดับสูงจากระยะไกล

การโจมตีมาจาก IP address "95.111.250[.]175" โดยเน้นเป้าหมายไปที่โดเมนของหน่วยงานรัฐและกองทัพในฟิลิปปินส์ (*.mil.ph และ .ph) และลาว (.gov.la)รวมถึง MSPs และผู้ให้บริการโฮสติ้ง โดยใช้โค้ดตัวอย่างโจมตี (PoC) ที่เปิดเผยสู่สาธารณะ

ชุดการโจมตีและการหลบเลี่ยงระบบป้องกัน

นอกจากนี้ Ctrl-Alt-Intel ยังพบว่าผู้โจมตีได้ใช้ชุดการโจมตี (exploit chain) แบบเฉพาะเจาะจงกับพอร์ทัลฝึกอบรมของภาคกลาโหมในอินโดนีเซียก่อนหน้านี้ โดยใช้ทั้งช่องโหว่ SQL Injection ที่ต้องมีการล็อกอิน และการรันโค้ดจากระยะไกล (Remote Code Execution) ซึ่งในกรณีนี้ ผู้โจมตีมีข้อมูลบัญชีผู้ใช้งานที่ถูกต้องอยู่แล้ว

“สคริปต์ที่ใช้มีการฝังข้อมูลบัญชีผู้ใช้ไว้ล่วงหน้า และสามารถหลบเลี่ยง CAPTCHA ได้ โดยการอ่านค่าที่ถูกต้องจาก session cookie ที่เซิร์ฟเวอร์ส่งมา แทนที่จะต้องแก้ CAPTCHA ตามปกติ” ทาง Ctrl-Alt-Intel ระบุ

“เมื่อเข้าสู่ระบบและผ่าน CAPTCHA ได้แล้ว ผู้โจมตีจะไปยังฟังก์ชันจัดการเอกสาร โดยช่องโหว่อยู่ที่ช่องสำหรับตั้งชื่อเอกสาร ซึ่งสคริปต์จะใส่คำสั่ง SQL ลงไปในช่องนี้ตอนส่งข้อมูลไปยังระบบบันทึกเอกสาร”

การขยายการโจมตีและขโมยข้อมูล

จากการวิเคราะห์เพิ่มเติมพบว่า ผู้โจมตีใช้เฟรมเวิร์กควบคุมเครื่องจากระยะไกลชื่อ AdaptixC2 เป็นศูนย์ควบคุม (C2) เพื่อสั่งงานเครื่องที่ถูกเจาะ นอกจากนี้ยังใช้เครื่องมืออย่าง OpenVPN และ Ligolo เพื่อสร้างการเข้าถึงระบบภายในอย่างต่อเนื่อง

“ผู้โจมตีได้สร้างช่องทางเข้าถึงระบบระยะยาวด้วย OpenVPN, Ligolo และการตั้งค่า systemd เพื่อให้ทำงานอัตโนมัติ จากนั้นใช้การเข้าถึงนี้เพื่อขยายการโจมตีเข้าไปในเครือข่ายภายใน และขโมยข้อมูลจำนวนมากที่เกี่ยวข้องกับโครงการรถไฟของจีน” Ctrl-Alt-Intel กล่าวเพิ่มเติม

ผลกระทบวงกว้างและคำแนะนำ

ขณะนี้ยังไม่ทราบว่าใครเป็นผู้อยู่เบื้องหลังการโจมตีครั้งนี้ แต่มีข้อมูลจาก Censys ระบุว่าช่องโหว่ cPanelนี้ถูกนำไปใช้โจมตีโดยหลายกลุ่มภายในเวลาเพียง 24 ชั่วโมงหลังจากถูกเปิดเผย รวมถึงมีการนำไปใช้แพร่กระจายมัลแวร์ Miraiเวอร์ชันต่างๆ และแรนซัมแวร์ชื่อ Sorry

ข้อมูลจาก Shadowserver Foundation ระบุว่า มี IP อย่างน้อย 44,000 รายการ ที่คาดว่าอาจถูกยึดผ่านช่องโหว่ CVE-2026-41940 และนำไปใช้สแกนและbrute-force โจมตี honeypot เมื่อวันที่30 เมษายน 2026 และตัวเลขลดลงเหลือ 3,540รายการ ณ วันที่ 3 พฤษภาคม

ในขณะเดียวกัน ทาง cPanel ได้ปล่อยเวอร์ชันใหม่ของสคริปต์ตรวจจับ เพื่อช่วยลดการแจ้งเตือนผิดพลาด (false positive) ผู้ใช้งานควรรีบอัปเดตแพตช์โดยเร็วที่สุด และตรวจสอบระบบของตนเอง หากพบสัญญาณการถูกเจาะ (IoCs) ควรดำเนินการแก้ไขและทำความสะอาดระบบทันที

ข้อมูลอ้างอิง

May 4, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/05/critical-cpanel-vulnerability.html