วันที่ 14 พฤษภาคม 2568

ตรวจพบการโจมตีรอบสองผ่านช่องโหว่ SAP NetWeaver CVE-2025-31324

Executive Summary

หลังจากการโจมตีรอบแรกเมื่อเดือนเมษายน 2025 ผ่านช่องโหว่ CVE-2025-31324 ที่เปิดช่องทางให้ผู้โจมตีสามารถอัปโหลดไฟล์อันตรายได้จากระยะไกล ในขณะที่ได้มีการตรวจพบการโจมตีในรอบที่สองโดยอาศัย WebShell ที่แฝงมาในระบบตั้งแต่ก่อนหน้า เพื่อดำเนินการโจมตีในลักษณะ Remote Command Execution (RCE) เป้าหมายส่วนใหญ่ในการโจมตีนี้คือองค์กรที่มีความสำคัญเชิงโครงสร้าง เช่น พลังงาน อุตสาหกรรมการผลิต และระบบสาธารณูปโภค โดยข้อมูลจาก Forescout ระบุว่ากลุ่มแฮกเกอร์หน้าใหม่จากจีนที่ใช้ชื่อว่า Chaya_004 ได้อยู่เบื้องหลังเหตุการณ์นี้ โดยพวกเขาใช้โครงสร้างพื้นฐานบนระบบคลาวด์ของจีน เช่น Alibaba และ Tencent ควบคู่กับเครื่องมือเจาะระบบอย่าง Cobalt Strike และ SoftEther VPN เพื่อฝังตัวและเลี่ยงการตรวจจับ

เพื่อแก้ไขปัญหาดังกล่าว SAP จึงได้ออกแพตช์แก้ไขเร่งด่วนตั้งแต่วันที่ 24 เมษายน พร้อมจัดเตรียมเครื่องมือสำหรับตรวจหาการบุกรุก ในขณะที่หน่วยงาน CISA ของสหรัฐฯ ได้กำหนดให้ทุกองค์กรอุดช่องโหว่นี้ภายในวันที่ 20 พฤษภาคม เพื่อป้องกันความเสียหายเพิ่มเติม

คำแนะนำ (Recommendation)

- ดำเนินการอัปเดต Software ให้เป็นเวอร์ชั่นปัจจุบัน
- ดำเนินการตรวจสอบระบบย้อนหลังเพื่อค้นหา WebShell หรือร่องรอยของการเข้าถึงที่ไม่ได้รับอนุญาต
- เฝ้าระวังพฤติกรรมต้องสงสัย เช่น การใช้เครื่องมือ Cobalt Strike, SoftEther VPN
- จำกัดการเข้าถึง Visual Composer จากเครือข่ายภายนอกและการควบคุมสิทธิ์อย่างเข้มงวดในระบบที่เกี่ยวข้อง

ข้อมูลอ้างอิง

- https://www.securityweek.com/second-wave-of-attacks-hitting-sap-netweaver-after-zero-day-compromise/
- https://www.cybersecuritydive.com/news/sap-netweaver-exploitation-second-wave/747661/