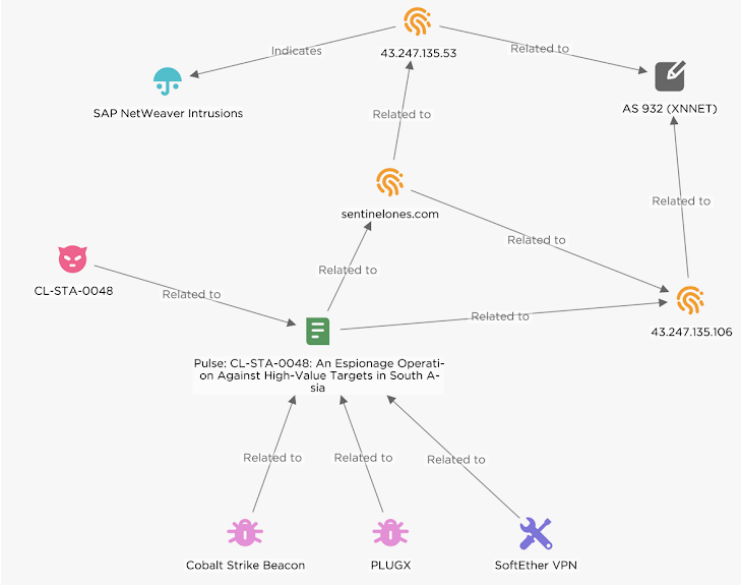
22 พฤษภาคม 2568

กลุ่มแฮ็กเกอร์ที่เชื่อมโยงกับจีน เจาะระบบสำคัญ 581 แห่งทั่วโลก ผ่านช่องโหว่ใน SAP NetWeaver



Executive Summary

นักวิจัยพบว่าแฮ็กเกอร์ที่มีความเกี่ยวข้องกับรัฐบาลจีน กำลังใช้ช่องโหว่ร้ายแรงในระบบ SAP NetWeaver เพื่อแฮ็กระบบขององค์กรสำคัญทั่วโลก เช่น โรงงานน้ำประปา แหล่งพลังงาน และหน่วยงานรัฐบาลกว่า 581 แห่ง โดยสามารถควบคุมระบบจากระยะไกลได้โดยไม่ต้องมีรหัสผ่าน

ช่องโหว่นี้มีชื่อว่า CVE-2025-31324 ซึ่งอนุญาตให้แฮ็กเกอร์ส่งไฟล์อันตรายเข้าไปยังระบบ SAP NetWeaver และเข้าควบคุมเครื่องเซิร์ฟเวอร์จากระยะไกลได้ทันที (Remote Code Execution: RCE) โดยปัจจุบันมีรายงานการโจมตีระบบสาธารณูปโภคในอังกฤษ เช่น ระบบประปา น้ำเสีย ก๊าซธรรมชาติ, โรงงานผลิตอุปกรณ์ทางการแพทย์ และบริษัทพลังงานในสหรัฐฯ กระทรวงรัฐบาลในซาอุดิอาระเบีย ที่ดูแลเรื่องการลงทุนและการเงิน

โดยเหตุการณ์นี้มีกลุ่มแฮ็กเกอร์ที่เกี่ยวข้องได้แก่ UNC5221, UNC5174, CL-STA-0048 ซึ่งทั้งหมดนี้เชื่อมโยงกับจีน โดยใช้วิธีฝัง Web Shell เพื่อแอบอยู่ในระบบ และสั่งงานจากระยะไกลและติดตั้งมัลแวร์หลายชนิด เช่น KrustyLoader, SNOWLIGHT, GOREVERSE

นักวิจัยยังพบไฟล์ชื่อ CVE-2025-31324-results.txt ซึ่งบันทึกรายชื่อระบบ SAP ที่ถูกแฮ็กไปแล้ว 581 ระบบ พร้อมอีก 800 โดเมนที่อาจจะถูกโจมตีในอนาคต โดยนอกจากนี้ ยังมีช่องโหว่ร้ายแรงอีกตัวชื่อว่า CVE-2025-42999 ซึ่งทำให้ผู้ใช้บางประเภทสามารถอัปโหลดโค้ดอันตรายเข้าไปได้หากยังไม่ได้อัปเดตแพตช์

Preventative Measures & Takeaways

- อัปเดตระบบ SAP NetWeaver ทันที โดยติดตั้งแพตช์จาก SAP หมายเลข 3594142 และ 3604119
- ตรวจสอบเซิร์ฟเวอร์ของตนเอง ว่ามีไฟล์หรือโปรแกรมไม่พึงประสงค์หรือไม่
- ปิดไม่ให้คนนอกเข้าถึงระบบ SAP จากภายนอกอินเทอร์เน็ต
- จำกัดสิทธิ์การเข้าถึง เฉพาะผู้ที่จำเป็นเท่านั้น
- ตรวจสอบบันทึกการใช้งานระบบ เพื่อดูว่ามีอะไรผิดปกติหรือไม่

Reference information

1. https://thehackernews.com/2025/05/deepfake-defense-in-age-of-ai.html