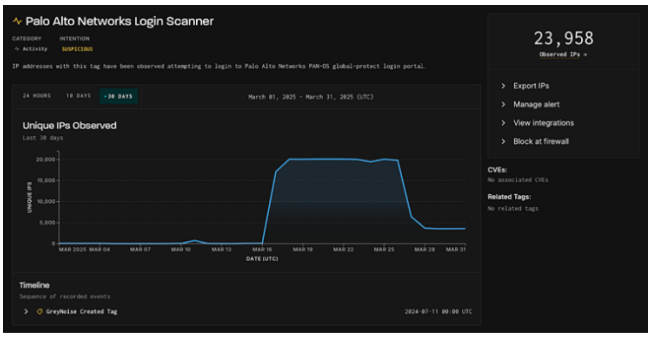
วันที่ 10 เมษายน 2568

Firewall Palo Alto มากกว่า 2,000 ตัวถูกเจาะระบบโดยใช้ช่องโหว่จากแพตช์ที่ได้รับการแก้ไขแล้ว

Executive Summary

ในช่วงเดือนมีนาคมที่ผ่านมา มีการตรวจพบความพยายามเข้าถึงระบบ GlobalProtect Portal ของ Palo Alto Networks PAN-OS โดยไม่ได้รับอนุญาตจาก IP ที่ไม่ซ้ำกันเกือบ 24,000 รายการ ซึ่งการโจมตีมีแนวโน้มเพิ่มขึ้นตั้งแต่วันที่ 17 มีนาคม 2568 และเริ่มลดลงภายในวันที่ 26 มีนาคม 2568 โดย ประเทศต้นทางหลัก ได้แก่ สหรัฐอเมริกาและแคนาดา ในขณะที่เป้าหมายหลักคือระบบใน สหรัฐอเมริกา สหราชอาณาจักร ไอร์แลนด์ รัสเซีย และสิงคโปร์ เหตุการณ์นี้แสดงถึงการประสานงานในหลายภูมิภาค และความเสี่ยงต่อองค์กรที่ใช้ระบบของ Palo Alto Networks



ผู้มีส่วนเกี่ยวข้องหลักในการโจมตีที่สามารถเชื่อมโยงกลับไปยังผู้ให้บริการโฮสติ้ง เช่น 3xK Tech GmbH, PureVoltage Hosting Inc., Fast Servers Pty Ltd. และ Oy Crea Nova Hosting Solution Ltd. อีกทั้งยังตรวจพบ JA4h hashes จำนวน 3 รายการที่ชี้ถึงการใช้เครื่องมือเฉพาะสำหรับการสแกนพอร์ทัลเข้าสู่ระบบ ได้แก่

- po11nn11enus_967778c7bec7_000000000000
- po11nn09enus_fb8b2e7e6287_000000000000
- po11nn060000_c4f66731b00d_000000000000

ซึ่งทั้งหมดสะท้อนถึงการวางแผนโจมตีที่มีระบบและเป็นขั้นตอนอย่างชัดเจน

คำแนะนำ (Recommendation)

- ดำเนินการตรวจสอบ Log ย้อนหลังในช่วงเดือนมีนาคม เพื่อตรวจสอบพฤติกรรมที่ผิดปกติ
- ดำเนินการ Block IP ที่เป็นอันตราย โดยอ้างอิงตามรายงานและข่าวสารต่างๆ เพื่อลดความเสี่ยง
- ดำเนินการ Update Patch ที่ได้รับการแก้ไขช่องโหว่แล้วบนอุปกรณ์ Firewall Palo Alto

ข้อมูลอ้างอิง

- https://gbhackers.com/hackers-deploy-24000-ips-to-breach-palo-alto-networks/#google_vignette