วันที่ 4 สิงหาคม 2568

Akira Ransomware โจมตี SonicWall VPN โดยอาจใช้ช่องโหว่ Zero-Day บนอุปกรณ์ที่อัปเดตล่าสุดแล้ว

SonicWall SSL VPN กลายเป็นเป้าหมายใหม่ของกลุ่มแรนซัมแวร์ Akira ซึ่งเป็นส่วนหนึ่งของกิจกรรมการโจมตีที่เพิ่มขึ้นอย่างน่าเป็นห่วงในช่วงปลายเดือนกรกฎาคม 2025

“จากการตรวจสอบ พบการบุกรุกระบบหลายกรณีในระยะเวลาไล่เลี่ยกัน โดยทั้งหมดมีจุดเริ่มต้นจากการเข้าถึงผ่าน SonicWall SSL VPN” Julian Tuin นักวิจัยจาก Arctic Wolf Labs กล่าวในรายงาน

บริษัทด้านความมั่นคงไซเบอร์รายนี้ตั้งข้อสังเกตว่า การโจมตีอาจเกิดจากการใช้ช่องโหว่ความปลอดภัยที่ยังไม่ถูกเปิดเผย หรือที่เรียกว่า Zero-Day เนื่องจากบางเหตุการณ์เกิดขึ้นบนอุปกรณ์ SonicWall ที่มีการอัปเดตล่าสุดแล้ว อย่างไรก็ตาม ยังไม่สามารถตัดความเป็นไปได้ของการใช้ข้อมูลบัญชี (credential-based attacks) ในการเข้าถึงระบบได้เช่นกัน

พฤติกรรมการโจมตีที่น่าสงสัย

การโจมตีผ่าน SonicWall SSL VPN ถูกตรวจพบครั้งแรกเมื่อวันที่ 15 กรกฎาคม 2025 แต่ Arctic Wolf ระบุว่าเคยพบพฤติกรรมการเข้าสู่ระบบ VPN ที่น่าสงสัยในลักษณะเดียวกันมาตั้งแต่เดือนตุลาคม 2024 ซึ่งแสดงให้เห็นถึงความพยายามอย่างต่อเนื่องในการเจาะระบบเหล่านี้

“มีช่วงเวลาค่อนข้างสั้นระหว่างการเข้าถึงบัญชีผ่าน SSL VPN กับการเริ่มเข้ารหัสข้อมูลด้วยแรนซัมแวร์” รายงานระบุ

“ต่างจากการเข้าสู่ระบบ VPN ของผู้ใช้จริง ซึ่งมักมาจากเครือข่ายของผู้ให้บริการอินเทอร์เน็ตทั่วไป กลุ่มแรนซัมแวร์มักใช้เซิร์ฟเวอร์เสมือน (Virtual Private Server หรือ VPS) เพื่อเข้าสู่ระบบ VPN ในสภาพแวดล้อมที่ถูกเจาะระบบแล้ว”

เมื่อมีการสอบถามไปยัง SonicWall เพื่อขอข้อมูลเพิ่มเติมเกี่ยวกับเหตุการณ์ดังกล่าว ยังไม่มีการตอบกลับใดๆ จนถึงเวลาที่บทความนี้ถูกเผยแพร่

คำแนะนำเร่งด่วนเพื่อลดความเสี่ยง

เพื่อเป็นการลดความเสี่ยง องค์กรต่างๆ ควรพิจารณา ปิดการใช้งาน SonicWall SSL VPN ชั่วคราว จนกว่าจะมีแพตช์แก้ไขออกมาและสามารถติดตั้งได้ เนื่องจากมีแนวโน้มว่าจะเป็นช่องโหว่ Zero-Day

แนวทางปฏิบัติอื่นๆ ที่ควรทำเพิ่มเติม ได้แก่:

- เปิดใช้ระบบ ยืนยันตัวตนหลายขั้นตอน (MFA) สำหรับการเข้าระบบจากภายนอก
- ลบบัญชีผู้ใช้งานที่ไม่ได้ใช้งานออกจากระบบไฟร์วอลล์
- ดูแลจัดการรหัสผ่านอย่างถูกต้องและปลอดภัย

Akira: กลุ่มแรนซัมแวร์ที่กำลังมาแรง

นับตั้งแต่ช่วงต้นปี 2024 กลุ่ม Akira ถูกประเมินว่ากวาดเงินค่าไถ่ไปแล้วประมาณ 42 ล้านดอลลาร์สหรัฐ จากการโจมตีเหยื่อมากกว่า 250 ราย โดยกลุ่มนี้เริ่มปรากฏตัวครั้งแรกในเดือนมีนาคม 2023

สถิติจาก Check Point ระบุว่า Akira เป็นกลุ่มแรนซัมแวร์ที่มีกิจกรรมมากเป็นอันดับสองในไตรมาสที่สองของปี 2025 รองจากกลุ่ม Qilin โดยมีเหยื่อถึง 143 รายในช่วงเวลาดังกล่าว

“กลุ่มแรนซัมแวร์ Akira ให้ความสำคัญกับเป้าหมายในอิตาลีเป็นพิเศษ โดยมีเหยื่อถึง 10% ที่เป็นบริษัทในประเทศอิตาลี เทียบกับค่าเฉลี่ยทั่วไปที่อยู่ที่เพียง 3%” บริษัทไซเบอร์ซีเคียวริตี้กล่าว

ข้อมูลอ้างอิง

Aug 2, 2025 By Ravie Lakshmanan

- https://thehackernews.com/2025/08/akira-ransomware-exploits-sonicwall.html