วันที่ 4 สิงหาคม 2569

แรนซัมแวร์ INC ก้าวขึ้นเป็นผู้โจมตีรายหลักที่ใช้ประโยชน์จากช่องโหว่ใน SonicWall SMA 1000

ปฏิบัติการแรนซัมแวร์ INC กลายเป็น “ผู้โจมตีที่โดดเด่นที่สุด” ในการใช้ประโยชน์จากช่องโหว่ด้านความปลอดภัยที่เพิ่งถูกเปิดเผยของอุปกรณ์ VPN รุ่น SonicWall Secure Mobile Access (SMA) 1000 ในรายงานที่เผยแพร่เมื่อช่วงสุดสัปดาห์ที่ผ่านมา Resecurity ระบุว่า พบว่า INC Ransomware เร่งการโจมตีอย่างต่อเนื่องตั้งแต่ต้นเดือนสิงหาคม 2026 พร้อมเพิ่มรายชื่อเหยื่อหลายรายบนเว็บไซต์เผยแพร่ข้อมูลที่ขโมยมา ตามสถิติจาก Ransomware.Live กลุ่มดังกล่าวอ้างว่ามีเหยื่อแล้วทั้งหมด 885 ราย โดยเหยื่อรายล่าสุดถูกเพิ่มเมื่อวันที่ 2 สิงหาคม 2026

การโจมตีครั้งนี้อาศัยการใช้ประโยชน์จากช่องโหว่ CVE-2026-15409 และ CVE-2026-15410 ซึ่งสามารถนำมาใช้ร่วมกันเพื่อรันคำสั่งตามต้องการบนระบบ และเข้าควบคุมอุปกรณ์ที่มีช่องโหว่ได้ SonicWall ได้ออกแพตช์แก้ไขช่องโหว่ทั้งสองรายการนี้ตั้งแต่ช่วงกลางเดือนกรกฎาคม 2026 ช่องโหว่ทั้งสองถูกประเมินว่า ถูกนำไปใช้โจมตีในฐานะช่องโหว่แบบ Zero-Day โดย Rapid7 ระบุว่า ผู้โจมตีใช้การเข้าถึงระบบในช่วงแรกเพื่อขโมยข้อมูลสำคัญ เช่น ข้อมูลรับรองการเข้าสู่ระบบที่มีสิทธิ์สูง ฐานข้อมูลเซสชันที่ยังใช้งานอยู่ และข้อมูล Seed Configuration ของระบบยืนยันตัวตนหลายปัจจัย (MFA) ที่ใช้รหัสผ่านแบบใช้ครั้งเดียวตามเวลา (TOTP) เพื่อรักษาสิทธิ์การเข้าถึงระบบในระยะยาว และท้ายที่สุดใช้เป็นจุดเริ่มต้นในการเคลื่อนที่ไปยังระบบภายในองค์กร

ในรายงานฉบับถัดมา Volexity ระบุว่า การโจมตีที่เกิดขึ้นก่อนการเปิดเผยช่องโหว่ ซึ่งเริ่มตั้งแต่วันที่ 22 มิถุนายน 2026 เป็นฝีมือของกลุ่มผู้โจมตีที่ติดตามในชื่อ UTA0533 โดยการโจมตีประกอบด้วยการติดตั้งสคริปต์ภาษา Python ชื่อ KNUCKLEBALL เพื่อใช้เปิดใช้งาน Suo5 ซึ่งเป็น HTTP Proxy แบบโอเพนซอร์ส รวมถึงติดตั้ง Java Web Shell แบบปรับแต่งเองที่มีลักษณะคล้าย Behinder ซึ่งมีชื่อว่า ORANGETAIL ต่อมา Rapid7 ให้ข้อมูลกับ The Hacker News ว่าแคมเปญการโจมตีดังกล่าวมีรูปแบบการดำเนินการหลายอย่างที่สอดคล้องกับผลการสืบสวนของบริษัท ความสอดคล้องทางเทคนิคที่ชัดเจนนี้ บ่งชี้ว่าผู้โจมตีรายเดียวหรือกลุ่มที่ประสานงานกัน เป็นผู้ค้นพบและใช้ประโยชน์จากช่องโหว่ Zero-Day นี้ Douglas McKee ผู้อำนวยการฝ่ายวิเคราะห์ข่าวกรองด้านช่องโหว่ของ Rapid7 กล่าว และในช่วงหลัง INC Ransomware ได้กลายเป็นผู้โจมตีหลักที่นำชุดช่องโหว่นี้ไปใช้โจมตีอย่างต่อเนื่อง

Resecurity ระบุว่า เหยื่อรายใหม่ที่ปรากฏบนเว็บไซต์ของ INC Ransomware ระหว่างวันที่ 17 กรกฎาคม ถึง 1 สิงหาคม 2026 ครอบคลุมทั้งองค์กรภาคเอกชนและหน่วยงานภาครัฐในออสเตรเลีย สหรัฐอเมริกา สหรัฐอาหรับเอมิเรตส์ โคลอมเบีย สวิตเซอร์แลนด์ และประเทศอื่นๆ บริษัทยังเปิดเผยอีกว่า เหยื่อรายใหม่หลายรายได้รับทั้งอีเมลและโทรศัพท์จากองค์กรที่ไม่รู้จัก ซึ่งอ้างว่าสามารถช่วยเหลือเกี่ยวกับเหตุการณ์แรนซัมแวร์ได้ ในบางกรณี เหยื่อยังได้รับการติดต่อจากบุคคลที่ใช้ชื่อว่า “Andrew” โดยใช้หมายเลขโทรศัพท์ +1 (304) 384-0401 เขาอ้างว่าโทรมาจากกลุ่มแฮกเกอร์ และแจ้งว่าเครือข่ายของเหยื่อถูกเจาะระบบแล้ว บริษัทระบุก่อนจบการสนทนา บุคคลดังกล่าวได้ให้ที่อยู่อีเมล info@helprans[.]com เพื่อใช้ในการเจรจาต่อ และวางสายไป วิธีลักษณะนี้มักถูกกลุ่มแรนซัมแวร์ใช้เป็นกลยุทธ์กดดัน ต่อเหยื่อ

ลูกค้าที่ใช้งานอุปกรณ์ SMA 1000 ควรอัปเดตแพตช์เป็นเวอร์ชันล่าสุดโดยทันที หากยังไม่ได้ดำเนินการ นอกจากนี้ Resecurity ยังแนะนำให้ดำเนินการค้นหาภัยคุกคามเชิงรุกอย่างครอบคลุม เปลี่ยนข้อมูลรับรองการเข้าสู่ระบบทั้งหมด และตรวจสอบความถูกต้องสมบูรณ์ของระบบควบคู่กับการติดตั้งแพตช์ เพื่อป้องกันความเสี่ยงจากภัยคุกคามดังกล่าว นอกจากนี้ บริษัทยังแนะนำให้ตรวจสอบแหล่งที่มาภายนอกที่มีการเชื่อมต่อกับ /wsproxy หรือมีการใช้พารามิเตอร์ที่ผิดปกติ พร้อมนำข้อมูลดังกล่าวไปเปรียบเทียบกับบันทึกการยืนยันตัวตนภายในองค์กร และกิจกรรมที่บ่งชี้ถึงการเคลื่อนที่ของผู้โจมตีภายในเครือข่าย เพื่อช่วยตรวจจับการบุกรุกได้อย่างมีประสิทธิภาพ

ข้อมูลอ้างอิง

Aug 03, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/08/inc-ransomware-emerges-as-dominant.html