

วันที่ 21 ตุลาคม 2569

กลุ่มแรนซัมแวร์ Qilin และ INC ใช้ประโยชน์จากช่องโหว่ของ Palo Alto Networks เพื่อข้ามระบบยืนยันตัวตน MFA



Palo Alto Networks เปิดเผยว่า ยังคงพบกลุ่มแรนซัมแวร์ใช้ประโยชน์จากช่องโหว่ด้านความปลอดภัยที่ส่งผลกระทบต่อ PAN-OS และ Prisma Access แม้ว่าช่องโหว่ดังกล่าวจะได้รับการแก้ไขไปแล้วก็ตาม

การโจมตีครั้งนี้เกี่ยวข้องกับช่องโหว่ CVE-2026-0257 (คะแนน CVSS 7.8) ซึ่งเป็นช่องโหว่ที่ทำให้ผู้โจมตีสามารถข้ามขั้นตอนการยืนยันตัวตนและสร้างการเชื่อมต่อ VPN โดยไม่ได้รับอนุญาต โดย Palo Alto Networks ได้ออกแพตช์แก้ไขช่องโหว่นี้ตั้งแต่เดือนพฤษภาคม 2026 และสำนักงานความมั่นคงปลอดภัยไซเบอร์และโครงสร้างพื้นฐานของสหรัฐฯ (CISA) ได้เพิ่มช่องโหว่ดังกล่าวลงในรายการช่องโหว่ที่ถูกนำไปใช้โจมตีจริง (Known Exploited Vulnerabilities หรือ KEV) เมื่อวันที่ 13 พฤษภาคม 2026

นักวิจัยจาก Unit 42 ระบุในรายงานอัปเดตที่เผยแพร่เมื่อวันจันทร์ว่า กลุ่มแรนซัมแวร์ที่ใช้ประโยชน์จากช่องโหว่ CVE-2026-0257 ได้แก่ Spikey Scorpion หรือที่รู้จักกันในชื่อ Qilin และ Tarnished Scorpion หรือ INC โดยข้อมูลดังกล่าวถูกเปิดเผยเพียงไม่กี่วันหลังจาก ReliaQuest รายงานว่า ตรวจพบกลุ่มแรนซัมแวร์ Qilin และ Settra กำลังใช้ประโยชน์จากช่องโหว่นี้ในการโจมตีเพื่อหวังผลประโยชน์ทางการเงิน

ตามรายงานของ Unit 42 ผู้โจมตีใช้ช่องโหว่นี้เป็นช่องทางเริ่มต้นในการบุกรุกเข้าสู่เครือข่ายขององค์กร ก่อนจะข้ามระบบยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication หรือ MFA) เพื่อสร้างการเชื่อมต่อ VPN เข้าสู่ระบบ

หลังจากเชื่อมต่อ VPN ได้สำเร็จ พบว่าผู้โจมตีมีการดำเนินกิจกรรมเพิ่มเติมภายในเครือข่าย ดังนี้

- สำรวจระบบและเครือข่ายภายในองค์กร โดยใช้เครื่องมือสำหรับตรวจสอบและจัดการระบบจากระยะไกล (Remote Monitoring and Management หรือ RMM) ซึ่งเป็นเครื่องมือที่สามารถนำไปใช้ได้ทั้งในงานดูแลระบบตามปกติและการโจมตี
- เคลื่อนย้ายการโจมตีไปยังเครื่องหรือระบบอื่นภายในเครือข่ายผ่านโปรโตคอล RDP และ SMB
- เตรียมเครื่องมือเพิ่มเติมสำหรับขโมยข้อมูลบัญชีผู้ใช้งาน ลักลอบนำข้อมูลออกจากระบบ และติดตั้งแรนซัมแวร์

การโจมตีของกลุ่มเหล่านี้มุ่งเป้าไปยังองค์กรในหลากหลายภาคส่วน ได้แก่ การศึกษา การเงิน การดูแลสุขภาพ เทคโนโลยีขั้นสูง ธุรกิจโรงแรมและการบริการ การผลิต บริการวิชาชีพและกฎหมาย หน่วยงานภาครัฐ การขนส่งและโลจิสติกส์ สาธารณูปโภคและพลังงาน รวมถึงธุรกิจค้าปลีก

Unit 42 ระบุว่า การเปลี่ยนแปลงที่สำคัญที่สุดในด้านกลยุทธ์ เทคนิค และขั้นตอนการโจมตี (Tactics, Techniques and Procedures หรือ TTPs) หลังจากใช้ประโยชน์จากช่องโหว่ CVE-2026-0257 ได้สำเร็จ คือการที่ผู้โจมตีเปลี่ยนเป้าหมายไปยังระบบจัดการเครื่องเสมือน (Virtualization) โดยตรง

ในเหตุการณ์หนึ่งที่น่าสนใจ ผู้โจมตีสามารถเคลื่อนย้ายจาก VPN Gateway ที่ถูกบุกรุกไปยังระบบจัดการ vCenter จากนั้นจึงปิดการทำงานของมาตรการรักษาความปลอดภัยบน ESXi Hypervisor (execInstalledOnly) และใช้เครื่องมือที่พัฒนาขึ้นเองเพื่อดึงข้อมูลบัญชีผู้ใช้งานและรหัสผ่านจากไฟล์ดิสก์เสมือน (VMDK) ของ Domain Controller โดยตรง ในขณะที่ระบบไม่ได้ทำงานอยู่

Palo Alto Networks อธิบายเพิ่มเติมว่า วิธีการดังกล่าวช่วยให้ผู้โจมตีหลบเลี่ยงระบบตรวจจับและตอบสนองภัยคุกคามบนเครื่องปลายทาง (Endpoint Detection and Response หรือ EDR) รวมถึงมาตรการรักษาความปลอดภัยที่ทำงานอยู่ภายในเครื่องเสมือนได้ ทำให้ผู้โจมตีสามารถเข้าถึงข้อมูลบัญชีผู้ใช้งานและรหัสผ่านที่ครอบคลุมทั้งโดเมนขององค์กร

นอกจากนี้ ยังพบว่าผู้โจมตีใช้ช่องทางการบุกรุกเริ่มต้นดังกล่าวร่วมกับเครื่องมือโจมตีช่องโหว่อื่นๆ โดยมีความพยายามมุ่งเป้าไปยังระบบสำรองข้อมูล Veeam ผ่านการใช้ประโยชน์จากช่องโหว่ที่เป็นที่รู้จักอยู่แล้วอย่าง CVE-2023-27532 เพื่อสร้างความเสียหายให้กับองค์กรให้มากที่สุด

ทั้งนี้ Arctic Wolf เคยรายงานตั้งแต่เดือนกรกฎาคม 2026 ว่า กลุ่มแรนซัมแวร์ Qilin มีการใช้ประโยชน์จากช่องโหว่ CVE-2026-0257 ในการโจมตี โดยรูปแบบการโจมตีมีตั้งแต่การเข้ารหัสไฟล์อย่างรวดเร็วเพียงอย่างเดียว ไปจนถึงการโจมตีแบบเรียกค่าไถ่สองชั้น (Double Extortion) ซึ่งเป็นการขโมยข้อมูลออกไปก่อนเข้ารหัสไฟล์ และใช้ข้อมูลที่ขโมยมาเป็นเครื่องมือกดดันให้เหยื่อจ่ายค่าไถ่เพิ่มเติม

นอกจากการติดตั้งแพตช์แก้ไขช่องโหว่ให้เป็นเวอร์ชันล่าสุดแล้ว Palo Alto Networks ยังแนะนำให้องค์กรตรวจสอบและค้นหาร่องรอยการบุกรุก (Indicators of Compromise หรือ IOC) ภายในระบบเชิงรุก และหากตรวจพบเหตุการณ์ที่มีการเชื่อมต่อผ่าน Gateway ได้สำเร็จและเข้าข่ายการโจมตี ควรเริ่มดำเนินการตามขั้นตอนตอบสนองต่อเหตุการณ์ด้านความปลอดภัย (Incident Response) อย่างเหมาะสมโดยเร็วที่สุด

ข้อมูลอ้างอิง

Oct 20, 2026, By Ravie Lakshmanan

- <https://thehackernews.com/2026/10/qilin-and-inc-ransomware-groups-exploit.html>