วันที่ 13 สิงหาคม 2568

VPN SSL ของ Fortinet ได้รับผลกระทบจากการโจมตีแบบ Brute-Force ทั่วโลก

นักวิจัยด้านความปลอดภัยไซเบอร์จากบริษัท GreyNoise กำลังเตือนถึง “การพุ่งสูงอย่างมีนัยสำคัญ” ของทราฟฟิกแบบ brute-force ที่มุ่งเป้าไปยังอุปกรณ์ Fortinet SSL VPN

จากข้อมูลของ GreyNoise พบว่ากิจกรรมแบบประสานงานนี้เกิดขึ้นเมื่อวันที่ 3 สิงหาคม 2025 โดยมี มากกว่า 780 หมายเลข IP ที่ไม่ซ้ำกัน เข้าร่วมโจมตี ภายใน 24 ชั่วโมงที่ผ่านมา มีการตรวจพบหมายเลข IP ที่ไม่ซ้ำกันถึง 56 หมายเลข ซึ่งทั้งหมดถูกจัดให้เป็น IP อันตราย ต้นทางมาจากสหรัฐอเมริกา, แคนาดา, รัสเซีย และเนเธอร์แลนด์ ขณะที่เป้าหมายของการ brute-force ได้แก่ สหรัฐอเมริกา, ฮ่องกง, บราซิล, สเปน และญี่ปุ่น

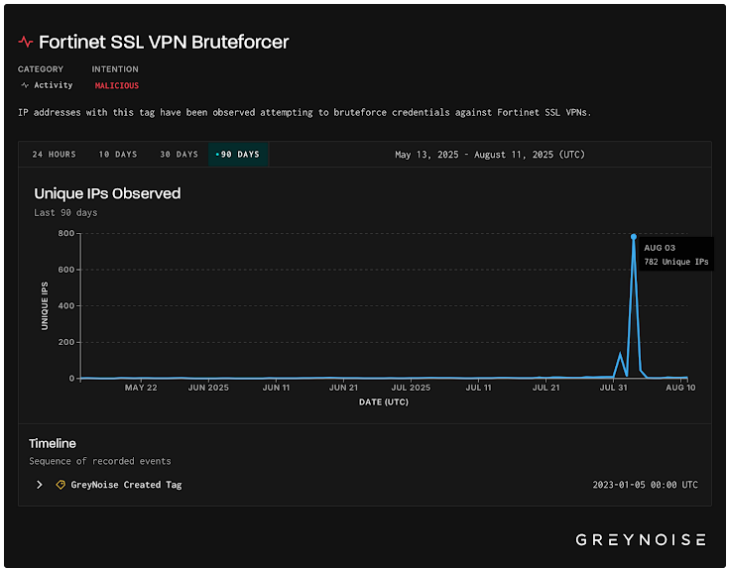
“สิ่งที่สำคัญคือทราฟฟิกที่พบยังมีการมุ่งเป้าไปที่โปรไฟล์ FortiOS ของเรา ซึ่งบ่งบอกถึงการเจาะจงโจมตี Fortinet’s SSL VPNs อย่างตั้งใจ” GreyNoise กล่าว “นี่ไม่ใช่การโจมตีแบบสุ่ม แต่เป็นกิจกรรมที่มีการโฟกัสชัดเจน”

รูปแบบการโจมตีที่เปลี่ยนแปลงไป

บริษัทฯ ยังชี้ว่าพบคลื่นการโจมตีที่แตกต่างกันสองระลอก ก่อนและหลังวันที่ 5 สิงหาคม ได้แก่:

1. การ brute-force ระยะยาว ที่ใช้ TCP signature เดียวกัน ซึ่งเกิดอย่างต่อเนื่องและค่อนข้างคงที่
2. การพุ่งขึ้นอย่างฉับพลัน ของทราฟฟิกที่มี TCP signature ต่างออกไป

“แม้ว่าทราฟฟิกวันที่ 3 สิงหาคมจะมุ่งเป้าที่โปรไฟล์ FortiOS แต่ตั้งแต่วันที่ 5 สิงหาคมเป็นต้นไป ทราฟฟิกที่มีการระบุ TCP และ client signatures หรือ meta signature กลับไม่โจมตี FortiOS อีก” บริษัทฯ ระบุ “แต่มุ่งเป้าไปที่ FortiManager อย่างต่อเนื่องแทน”



สิ่งนี้ชี้ให้เห็นถึงการเปลี่ยนแปลงพฤติกรรมของผู้โจมตี และอาจเป็นไปได้ว่ามีการใช้โครงสร้างพื้นฐานหรือเครื่องมือชุดเดียวกันเปลี่ยนเป้าหมายไปยังบริการอื่นของ Fortinet

เบาะแสและข้อสันนิษฐาน

การตรวจสอบเชิงลึกของข้อมูลย้อนหลังที่เกี่ยวข้องกับ TCP fingerprint หลังวันที่ 5 สิงหาคม พบการพุ่งสูงในเดือนมิถุนายน ซึ่งมี client signature เฉพาะที่ชี้ไปยังอุปกรณ์ FortiGate ในเครือข่าย ISP ภายในบ้านที่จัดการโดย Pilot Fiber Inc. ทำให้เกิดความเป็นไปได้ว่าเครื่องมือ brute-force อาจถูกทดสอบหรือเริ่มต้นการโจมตีจากเครือข่ายในบ้าน หรืออีกทางหนึ่งอาจเป็นการใช้ residential proxy

ความเคลื่อนไหวนี้เกิดขึ้นท่ามกลางข้อค้นพบที่ว่าการพุ่งสูงของกิจกรรมอันตราย มักตามมาด้วยการเปิดเผยช่องโหว่ CVE ใหม่ที่เกี่ยวข้องกับเทคโนโลยีเดียวกันภายใน 6 สัปดาห์

“รูปแบบนี้พบเฉพาะในเทคโนโลยีสำหรับเครือข่ายองค์กรที่อยู่ขอบระบบ เช่น VPN, firewall และเครื่องมือ remote access ซึ่งเป็นประเภทระบบที่ตกเป็นเป้าหมายมากขึ้นโดยผู้โจมตีขั้นสูง” บริษัทฯ กล่าวในรายงาน Early Warning Signals ที่เผยแพร่เมื่อปลายเดือนที่แล้ว

ข้อมูลอ้างอิง

Aug 12, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/08/fortinet-ssl-vpns-hit-by-global-brute.html