วันที่ 12 มีนาคม 2569

อุปกรณ์ FortiGate ถูกใช้เป็นช่องทางเจาะเครือข่ายและขโมยข้อมูลบัญชีบริการ

นักวิจัยด้านความปลอดภัยไซเบอร์ได้ออกมาแจ้งเตือนถึงแคมเปญการโจมตีรูปแบบใหม่ โดยผู้ไม่หวังดีใช้ประโยชน์จากอุปกรณ์ **FortiGate Next-Generation Firewall (NGFW)** เป็นจุดเริ่มต้นสำคัญในการเจาะเข้าสู่เครือข่ายภายในของเหยื่อ การโจมตีนี้เริ่มจากการใช้ช่องโหว่ความปลอดภัยที่เพิ่งถูกเปิดเผย หรือการอาศัยรหัสผ่านที่ตั้งค่าไว้ไม่แข็งแรง เพื่อดึงไฟล์คอนฟิกออกมา ซึ่งภายในไฟล์ดังกล่าวประกอบด้วยข้อมูลสำคัญ เช่น ข้อมูลบัญชีบริการ (Service Account) และแผนผังโครงสร้างเครือข่ายภายในองค์กร

จากรายงานของ SentinelOne ที่เผยแพร่ในวันนี้ ระบุว่ากลุ่มเป้าหมายหลักของการโจมตีมุ่งไปที่องค์กรในภาคสาธารณสุข หน่วยงานรัฐบาล และผู้ให้บริการ Managed Service Provider (MSP) เนื่องจากอุปกรณ์ FortiGate มักได้รับสิทธิ์ในการเข้าถึงสภาพแวดล้อมเครือข่ายอย่างกว้างขวางเพื่อทำหน้าที่ป้องกันระบบ ตามที่นักวิจัย Alex Delamotte, Stephen Bromfield, Mary Braden Murphy และ Amey Patne ได้ตั้งข้อสังเกตไว้

ช่องโหว่จากการเชื่อมต่อระบบยืนยันตัวตน (AD/LDAP)

โดยปกติแล้ว อุปกรณ์เหล่านี้จะมีการตั้งค่าบัญชีบริการเพื่อเชื่อมต่อกับระบบยืนยันตัวตนขององค์กร เช่น Active Directory (AD) และ LDAP เพื่อใช้ในการตรวจสอบสิทธิ์และกำหนดบทบาท (Roles) ของผู้ใช้ตามนโยบายแบบ Role-based ซึ่งช่วยให้การตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทำได้รวดเร็วขึ้น อย่างไรก็ตาม นักวิจัยระบุว่าสิทธิ์การเข้าถึงในลักษณะนี้อาจถูกนำไปใช้ในทางที่ผิด หากผู้โจมตีสามารถเจาะเข้าอุปกรณ์ผ่านช่องโหว่ที่เป็นที่รู้จัก (เช่น CVE-2025-59718, CVE-2025-59719 และ CVE-2026-24858) หรือผ่านการตั้งค่าที่ไม่รัดกุม

เจาะลึกพฤติกรรม Initial Access Broker

ในกรณีศึกษาหนึ่ง พบว่าผู้โจมตีสามารถเจาะเข้าอุปกรณ์ FortiGate ได้ตั้งแต่เดือนพฤศจิกายน 2025 และแอบสร้างบัญชีผู้ดูแลระบบชื่อ **"support"** ขึ้นมาใหม่ เพื่อใช้สร้างนโยบายไฟร์วอลล์เพิ่มเติม 4 รายการ ซึ่งอนุญาตให้บัญชีนี้เข้าถึงทุกโซนของเครือข่ายได้โดยไม่มีข้อจำกัด

พฤติกรรมนี้สอดคล้องกับกลุ่ม **Initial Access Broker (IAB)** ที่เน้นการสร้างจุดยึดในระบบไว้ก่อน แล้วจึงนำสิทธิ์การเข้าถึงดังกล่าวไปขายต่อให้กับกลุ่มอาชญากรไซเบอร์รายอื่นเพื่อหวังผลกำไร โดยพบความเคลื่อนไหวอีกครั้งในเดือนกุมภาพันธ์ 2026 เมื่อผู้โจมตีดึงไฟล์คอนฟิกที่มีข้อมูลบัญชีบริการ LDAP ซึ่งถูกเข้ารหัสไว้ออกไป

"หลักฐานแสดงให้เห็นว่า ผู้โจมตีสามารถยืนยันตัวตนเข้าสู่ Active Directory ด้วยรหัสผ่านแบบข้อความปกติ (Clear text) จากบัญชีบริการ fortidcagent ซึ่งบ่งชี้ว่าผู้โจมตีสามารถถอดรหัสไฟล์คอนฟิกและดึงข้อมูลบัญชีออกมาได้สำเร็จ" SentinelOne ระบุ

หลังจากได้ข้อมูลบัญชีบริการ ผู้โจมตีได้ทำการลงทะเบียนเครื่องคอมพิวเตอร์ปลอมเข้าไปใน Active Directory เพื่อแทรกซึมเข้าสู่ระบบภายในให้ลึกยิ่งขึ้น และเริ่มสแกนเครือข่ายเพื่อหาเป้าหมายถัดไป ซึ่งเป็นจุดที่ทีมรักษาความปลอดภัยตรวจพบการบุกรุกและระงับเหตุได้ทันท่วงที

การแพร่กระจายมัลแวร์และการขโมยข้อมูลระดับลึก

นอกจากนี้ยังมีอีกกรณีในช่วงปลายเดือนมกราคม 2026 ที่ผู้โจมตีสามารถเปลี่ยนจากการเข้าถึงไฟร์วอลล์ไปสู่การติดตั้งเครื่องมือรีโมต เช่น Pulseway และ MeshAgent ได้อย่างรวดเร็ว พร้อมทั้งดาวน์โหลดมัลแวร์จาก Cloud Storage ผ่านคำสั่ง PowerShell โดยใช้โครงสร้างพื้นฐานของ AWS

มัลแวร์ที่เขียนด้วยภาษา Java ถูกเรียกใช้งานผ่านเทคนิค DLL side-loading เพื่อขโมยข้อมูลสำคัญจากไฟล์ NTDS.dit และไฟล์ SYSTEM registry hive แล้วส่งออกไปยังเซิร์ฟเวอร์ภายนอก (IP: 172.67.196[.]232) แม้จะพบการพยายามนำข้อมูลไปถอดรหัส แต่ในขณะนี้ยังไม่พบหลักฐานการนำข้อมูลบัญชีเหล่านั้นไปใช้ต่อก่อนที่เหตุการณ์จะถูกควบคุมไว้ได้

บทสรุปและความเสี่ยงของอุปกรณ์ NGFW

อุปกรณ์ Next-Generation Firewall กลายเป็นหัวใจสำคัญขององค์กรเนื่องจากความสามารถในการตรวจสอบและควบคุมความปลอดภัยที่ซับซ้อน แต่ในขณะเดียวกัน อุปกรณ์เหล่านี้ก็กลายเป็นเป้าหมายที่มีมูลค่าสูง (High-value target) สำหรับผู้โจมตี ไม่ว่าจะเป็นกลุ่มที่ได้รับการสนับสนุนจากรัฐที่มุ่งหวังการสอดแนม หรือกลุ่มอาชญากรที่ต้องการผลประโยชน์ทางการเงิน เช่น การโจมตีด้วยแรนซัมแวร์

ข้อมูลอ้างอิง

Mar 10, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/03/fortigate-devices-exploited-to-breach.html