วันที่ 24 กุมภาพันธ์ 2569

พบผู้โจมตีใช้ AI สนับสนุนการเจาะอุปกรณ์ FortiGate มากกว่า 600 เครื่อง ใน 55 ประเทศ

รายงานล่าสุดจาก Amazon Threat Intelligence เปิดเผยกิจกรรมน่ากังวลในช่วงต้นปี 2026 เมื่อผู้ก่อภัยคุกคามที่พูดภาษารัสเซียและมุ่งหวังผลกำไร ได้นำ Generative AI มาเป็นเครื่องมือหลักในการเจาะระบบอุปกรณ์ FortiGate มากกว่า 600 เครื่อง ใน 55 ประเทศ รวมถึงในภูมิภาคเอเชียตะวันออกเฉียงใต้ด้วย

AI ยกระดับผู้โจมตีทักษะต่ำ ให้ทำงานเสมือนทีมใหญ่

Amazon ระบุว่าผู้โจมตีรายนี้มีทักษะเทคนิคไม่สูงนัก แต่ใช้เครื่องมือ Generative AI เชิงพาณิชย์หลายตัวช่วยในทุกขั้นตอนของการโจมตี ตั้งแต่เขียนโค้ดเครื่องมือ วางแผนเจาะระบบ ไปจนถึงสั่งควบคุมอุปกรณ์ที่ถูกเจาะ

แม้ AI ตัวหนึ่งเป็นศูนย์กลางของปฏิบัติการ แต่ผู้โจมตีมีอีกตัวเป็นตัวสำรองเพื่อช่วยขยายสิทธิ์ภายในเครือข่ายที่ถูกเจาะแล้ว โดยไม่มีการเปิดเผยชื่อเครื่องมือ AI ที่ใช้

ผู้โจมตีถูกประเมินว่าต้องการประโยชน์ทางการเงิน ไม่ใช่กลุ่ม APT ที่รัฐสนับสนุน ซึ่งสอดคล้องกับข้อสังเกตของ Google ที่ระบุว่าผู้โจมตีทั่วไปกำลังหันมาใช้ Generative AI มากขึ้น เพื่อขยายขนาดและเร่งความเร็วของปฏิบัติการ แม้จะไม่ได้สร้างเทคนิคใหม่ที่ล้ำหน้าก็ตาม

การเกิดขึ้นของเครื่องมือ AI ทำให้ความสามารถที่เคยเอื้อมไม่ถึงสำหรับผู้โจมตีมือใหม่ กลายเป็นเรื่องธรรมดา ลดอุปสรรคในการเข้าสู่วงการอาชญากรรมไซเบอร์ และเพิ่มความสามารถในการออกแบบแคมเปญโจมตีแบบครบวงจร

“Moses” นักวิเคราะห์ของ Amazon ระบุว่า “มีแนวโน้มว่านี่คือบุคคลหรือกลุ่มเล็ก ๆ ที่ต้องการผลกำไร แต่ด้วย AI เขาสามารถขยายปฏิบัติการได้ในระดับที่เดิมต้องใช้ทีมใหญ่และทักษะสูงกว่านี้มาก”

เจาะ Active Directory ดึงฐานข้อมูลรหัสผ่าน พร้อมเล็งระบบสำรองข้อมูล

การสืบสวนของ Amazon พบว่าผู้โจมตีสามารถเจาะระบบ Active Directory (ระบบจัดการบัญชีผู้ใช้ขององค์กร) ของหลายบริษัท และดึงฐานข้อมูลข้อมูลรับรองทั้งหมดออกมาได้ นอกจากนี้ยังพุ่งเป้าไปยังระบบสำรองข้อมูล ซึ่งเป็นขั้นตอนทั่วไปก่อนปล่อยแรนซัมแวร์

ที่น่าสังเกตคือ ผู้โจมตีไม่เลือกเป้าหมายที่มีความปลอดภัยสูง แต่หันไปหาเหยื่อที่ตั้งค่าระบบอ่อนแอกว่า ใช้ AI ช่วยหาจุดที่ง่ายที่สุดในการเจาะ

Amazon ยังพบโครงสร้างพื้นฐานที่ผู้โจมตีใช้แบบเปิดสู่สาธารณะ โดยมีไฟล์เกี่ยวกับแคมเปญจำนวนมาก เช่น แผนโจมตีที่สร้างด้วย AI ไฟล์การตั้งค่าของเหยื่อ และซอร์สโค้ดเครื่องมือที่เขียนเอง ทั้งหมดนี้มีลักษณะเหมือน “สายพานการโจมตีที่ขับเคลื่อนด้วย AI”

แกนสำคัญ: เจาะ FortiGate เพื่อดึงค่าตั้งค่าทั้งหมด

จุดเริ่มต้นคือการเจาะอุปกรณ์ FortiGate เพื่อดึงข้อมูลตั้งค่า เช่น รหัสผ่าน โครงสร้างเครือข่าย และรายละเอียดการคอนฟิกอื่น ๆ ซึ่งใช้เป็นกุญแจในการบุกลึกเข้าเครือข่ายขององค์กร

โจมตีแบบสแกนกว้าง: เริ่มจากพอร์ตจัดการที่เปิดทิ้งไว้

กระบวนการเริ่มจากการสแกนอินเทอร์เฟซจัดการของ FortiGate ที่เปิดสู่ภายนอกบนพอร์ต 443, 8443, 10443 และ 4443 จากนั้นพยายามเข้าสู่ระบบด้วยรหัสผ่านที่ใช้ซ้ำ การโจมตีไม่ได้จำกัดอุตสาหกรรมใด แต่เป็นการสแกนอัตโนมัติจำนวนมากเพื่อหาเหยื่อ โดยมีต้นทางมาจาก IP 212.11.64[.]250

ข้อมูลที่ขโมยไปถูกนำมาใช้เพื่อเจาะลึกเข้าเครือข่าย ทำกิจกรรมหลังการเจาะ เช่น สำรวจระบบ สแกนช่องโหว่ด้วย Nuclei เจาะ Active Directory เก็บรหัสผ่าน และพยายามเข้าถึงระบบสำรองข้อมูล ซึ่งเข้ากับรูปแบบเตรียมปล่อยแรนซัมแวร์

ข้อมูลของ Amazon ยังพบการเจาะระดับองค์กรหลายแห่งในภูมิภาคเอเชียใต้ ละตินอเมริกา แคริบเบียน แอฟริกาตะวันตก ยุโรปเหนือ และเอเชียตะวันออกเฉียงใต้ โดยหลายองค์กรมีอุปกรณ์ FortiGate ถูกเข้าถึงพร้อมกัน

“หลังจากผู้โจมตีได้สิทธิ์ VPN จะติดตั้งเครื่องมือสำรวจระบบที่พัฒนาเอง ทั้งเวอร์ชัน Go และ Python” Amazon ระบุ “การวิเคราะห์ซอร์สโค้ดพบลักษณะที่ชี้ว่าเขียนด้วย AI เช่น คอมเมนต์ซ้ำซ้อน อธิบายฟังก์ชันแบบตรงตัว โครงสร้างเรียบง่าย แต่เน้นจัดรูปแบบ การจับคู่ JSON แบบง่ายแทนใช้งานตามมาตรฐาน และมีโค้ดเสริมความเข้ากันได้ของภาษาแต่ไม่มีเอกสารประกอบ”

ขั้นตอนหลังการสำรวจระบบที่พบ ได้แก่

- เจาะโดเมนด้วยเทคนิค DCSync
- เคลื่อนย้ายในเครือข่ายด้วย pass-the-hash / pass-the-ticket, NTLM relay และรันคำสั่งระยะไกลบน Windows

• พุ่งเป้าเซิร์ฟเวอร์ Veeam Backup & Replication เพื่อติดตั้งตัวดึงรหัสผ่าน และใช้ช่องโหว่ที่รู้แล้ว เช่น CVE-2023-27532 และ CVE-2024-40711

อีกประเด็นคือ ผู้โจมตีล้มเหลวเมื่อพยายามเจาะระบบที่เกินกว่า “เส้นทางโจมตีอัตโนมัติที่ง่ายที่สุด” เอกสารภายในระบุว่าบางเป้าหมายอุดช่องโหว่ ปิดพอร์ต หรือไม่มีช่องโหว่ใช้ประโยชน์

วิธีป้องกัน: ปิดประตูไม่ให้ AI เจาะเข้าบ้าน

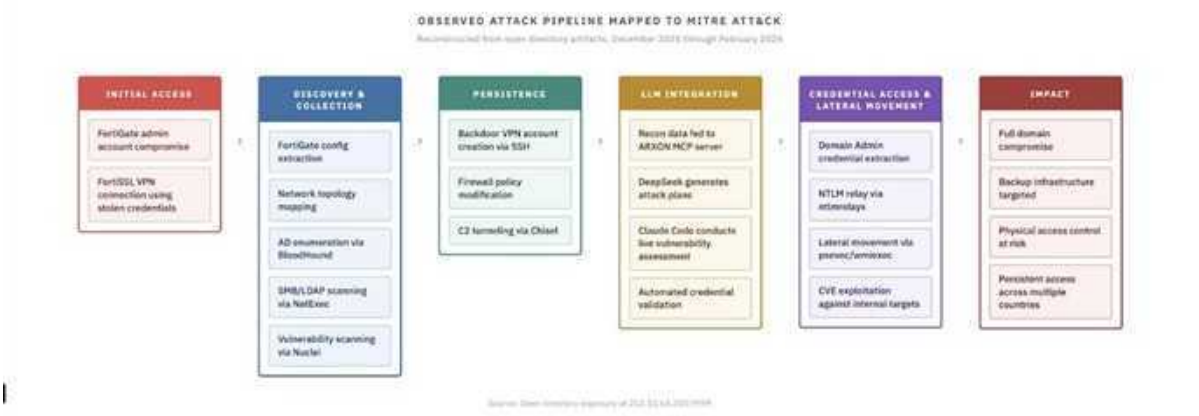
เมื่ออุปกรณ์ Fortinet ถูกเล็งโจมตีมากขึ้น องค์กรควรดำเนินการดังนี้:

- **ปิดการเข้าถึงจากภายนอก:** ห้ามเปิดพอร์ตจัดการระบบ FortiGate สู่สาธารณะ
- **MFA คือหัวใจ:** เปิดใช้การยืนยันตัวตนหลายชั้น (Multi-Factor Authentication) ทั้งในส่วนของผู้ดูแลระบบและ VPN
- **จัดการรหัสผ่าน:** เปลี่ยนรหัสผ่านเริ่มต้นและหมุนเวียนรหัสผ่าน SSL-VPN สม่ำเสมอ
- **ดูแลระบบสำรอง:** อัปเดตแพตช์ระบบ **Veeam** (เช่น CVE-2024-40711) และแยกเครือข่ายสำรองข้อมูลออกจากเครือข่ายหลัก (Network Segmentation)

อัปเดต: Cyber และ Ramen พบข้อมูลเพิ่ม เกี่ยวข้องกับ DeepSeek, Claude, HexStrike AI

งานวิจัยเพิ่มเติมจาก Cyber และ Ramen เปิดเผยว่าผู้โจมตีใช้ DeepSeek และ Anthropic Claude สร้างแผนโจมตี ในเดือนธันวาคม 2025 เซิร์ฟเวอร์เดียวกันนี้เคยใช้โฮสต์เฟรมเวิร์ก AI แบบเชิงรุกชื่อ HexStrike AI

นักวิจัยด้านความปลอดภัยเผยว่า
“DeepSeek ถูกใช้สร้างแผนโจมตีจากข้อมูลที่เก็บได้ ส่วนเอเจนต์เขียนโค้ดของ Claude ช่วยประเมินช่องโหว่ระหว่างเจาะระบบ และยังถูกตั้งค่าให้รันเครื่องมือเชิงรุกบนเครื่องเหยื่อด้วย ระบบยังมีเซิร์ฟเวอร์ Model Context Protocol (MCP) ที่ไม่เคยถูกเปิดเผยมาก่อน ใช้เชื่อมต่อโมเดลภาษาและเก็บฐานความรู้ที่เพิ่มขึ้นจากจำนวนเหยื่อ”



เซิร์ฟเวอร์ IP 212.11.64[.]250 มีไฟล์กว่า 1,400 ไฟล์ใน 139 โฟลเดอร์ รวมถึงโค้ดโจมตีช่องโหว่ ซอร์สสแกน Nuclei ค่าตั้งค่า FortiGate ตัวดึงรหัสผ่าน Veeam และข้อมูล BloodHound (เครื่องมือวิเคราะห์ AD)

ยังพบ MCP แบบกำหนดเองชื่อ ARXON ใช้ประมวลผลผลสแกนและข้อมูลสำรวจ เรียกใช้ DeepSeek เพื่อสร้างแผนโจมตีและแก้ไขโครงสร้างพื้นฐานของเหยื่อโดยอัตโนมัติ อีกหนึ่งเครื่องมือคือ CHECKER2 เขียนด้วย Go ใช้สแกน VPN และประมวลผลเป้าหมายจำนวนมากพร้อมกัน

นักวิจัยสรุปว่า
“จุดเด่นของแคมเปญนี้คือการผสาน AI และ LLM ในทุกขั้นตอน ผู้โจมตีเพียงคนเดียวสามารถแฮกได้หลายประเทศพร้อมกัน เพราะมี AI วิเคราะห์และช่วยตัดสินใจให้ตลอดเวลา โมเดลภาษาช่วยให้ผู้โจมตีทักษะต่ำขยายจำนวนเหยื่อที่จัดการได้พร้อมกันได้อย่างมหาศาล”

ข้อมูลอ้างอิง

Feb 21, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/02/ai-assisted-threat-actor-compromises.html