วันที่ 4 มีนาคม 2569

แคมเปญโจมตี FortiGate เชื่อมโยงเครื่องมือ AI โอเพนซอร์ส “CyberStrikeAI”

จากเหตุการณ์โจมตีอุปกรณ์ Fortinet FortiGate ครั้งใหญ่ที่เคยถูกเปิดเผยว่ามีการใช้ AI เข้าช่วย ล่าสุดพบหลักฐานสำคัญว่าผู้โจมตีได้ใช้แพลตฟอร์ม "CyberStrikeAI" ซึ่งเป็นเครื่องมือทดสอบความปลอดภัยแบบโอเพนซอร์สที่ออกแบบมาเพื่อ AI โดยเฉพาะ มาใช้เป็นหัวใจหลักในการโจมตีอย่างเป็นระบบ

แกะรอยต้นตอ จากรัสเซียสู่เงาของรัฐบาลจีน

ข้อมูลจากบริษัทวิเคราะห์ภัยคุกคาม Team Cymru ระบุว่า พวกเขาตรวจพบการใช้งานเครื่องมือนี้ผ่านการวิเคราะห์ที่อยู่ IP 212.11.64[.]250 ซึ่งเชื่อมโยงกับกลุ่มแฮกเกอร์ที่ใช้ภาษารัสเซีย โดยใช้สแกนหาช่องโหว่ของอุปกรณ์แบบอัตโนมัติในวงกว้าง

อย่างไรก็ตาม ตัวซอฟต์แวร์ CyberStrikeAI กลับถูกพัฒนาโดยนักพัฒนาชาวจีนนามแฝงว่า "Ed1s0nZ" ซึ่งนักวิจัยด้านความปลอดภัย Will Thomas (@BushidoToken) ชี้ให้เห็นว่า นักพัฒนารายนี้อาจมีความเชื่อมโยงลึกซึ้งกับรัฐบาลจีน

CyberStrikeAI คืออะไร?

ในหน้า GitHub ของโครงการ อธิบายว่ามันคือ “เครื่องมือความปลอดภัยเชิงรุกที่ขับเคลื่อนด้วย AI” พัฒนาด้วยภาษา Go และรวบรวมเครื่องมือด้านความปลอดภัยไว้มากกว่า 100 รายการ เพื่อทำหน้าที่:

- ค้นหาช่องโหว่ อย่างรวดเร็ว
- วิเคราะห์ลำดับการโจมตี (Attack Chain)
- ดึงข้อมูลความรู้ ที่เกี่ยวข้องกับเป้าหมาย
- สรุปผลลัพธ์ ให้อ่านง่าย เพื่อให้แฮกเกอร์ตัดสินใจโจมตีได้ทันที

สถิติการโจมตีที่น่ากังวล

ก่อนหน้านี้ Amazon Threat Intelligence เคยตรวจพบการใช้ AI เชิงสร้างสรรค์อย่าง Anthropic Claude และ DeepSeek โจมตี FortiGate จนส่งผลกระทบต่ออุปกรณ์กว่า 600 เครื่อง ใน 55 ประเทศ

ล่าสุด Team Cymru พบว่าในช่วงวันที่ 20 มกราคม - 26 กุมภาพันธ์ 2026 มี IP อย่างน้อย 21 รายการที่ใช้งาน CyberStrikeAI โดยเซิร์ฟเวอร์ส่วนใหญ่กระจุกตัวอยู่ใน จีน, สิงคโปร์, และฮ่องกง รวมถึงบางส่วนในสหรัฐฯ, ญี่ปุ่น และสวิตเซอร์แลนด์

เปิดคลังแสงของ "Ed1s0nZ"

นอกจาก CyberStrikeAI แล้ว บัญชี GitHub ของ Ed1s0nZ ยังมีเครื่องมืออีกมากมายที่สะท้อนถึงความเชี่ยวชาญในการเจาะระบบและเลี่ยงกฎ AI:

- banana_blackmail: แรนซัมแวร์ (มัลแวร์เรียกค่าไถ่) พัฒนาด้วยภาษา Go
- PrivHunterAI: ใช้โมเดล AI (Kimi, DeepSeek, GPT) หาช่องโหว่เพื่อยกระดับสิทธิ์ (Privilege Escalation)
- ChatGPTJailbreak: ชุดคำสั่งหลอกให้ ChatGPT เข้าสู่โหมด DAN (Do Anything Now) เพื่อข้ามขีดจำกัดด้านความปลอดภัย
- InfiltrateX: เครื่องมือสแกนหาช่องโหว่การยกระดับสิทธิ์ที่พัฒนาด้วย Golang
- VigilantEye: เครื่องมือที่ใช้ Golang เพื่อตรวจจับการเปิดเผยข้อมูลอ่อนไหว เช่น หมายเลขโทรศัพท์ หรือเลขบัตรประชาชนในฐานข้อมูล และตั้งค่าให้แจ้งเตือนผ่านบอต WeChat Work หากพบความเสี่ยงข้อมูลรั่วไหล

ความเชื่อมโยงกับปฏิบัติการไซเบอร์ของรัฐบาลจีน

Will Thomas ระบุว่า กิจกรรมของ Ed1s0nZ มีปฏิสัมพันธ์กับองค์กรที่สนับสนุนรัฐบาลจีน รวมถึงบริษัทความปลอดภัย Knownsec 404 ซึ่งถูกขนานนามว่าเป็น “ผู้รับเหมาด้านไซเบอร์” ให้กับกองทัพ (PLA) และกระทรวงความมั่นคงแห่งรัฐ (MSS)

เบื้องลึกของ Knownsec 404:

- ปลายปีที่ผ่านมาเกิดเหตุข้อมูลรั่วไหล เผยให้เห็นเอกสารกว่า 12,000 รายการ ทั้งข้อมูลพนักงานและเครื่องมือแฮ็ก
- พบข้อมูลที่ขโมยมา เช่น บันทึกการโทรของเกาหลีใต้ และข้อมูลโครงสร้างพื้นฐานของไต้หวัน
- มีเครื่องมืออย่าง ZoomEye ที่ช่วยให้จีนสอดส่องระดับโลก จัดเก็บข้อมูล IP และโดเมนต่างชาติหลายล้านรายการตามความสำคัญเชิงยุทธศาสตร์

ความพยายาม "ลบร่องรอย"

พบว่า Ed1s0nZ ได้แก้ไขไฟล์ README.md ในรีโพซิทอรีของตนเอง โดยลบข้อความที่เคยระบุว่าได้รับรางวัล Level 2 Contribution Award จาก China National Vulnerability Database of Information Security (CNNVD) และยังยืนยันว่า “ทุกอย่างที่แบ่งปันที่นี่มีวัตถุประสงค์เพื่อการวิจัยและการเรียนรู้เท่านั้น”

นักวิจัยมองว่านี่คือความพยายามปกปิดตัวตนเพื่อให้เครื่องมือยังคงถูกใช้งานต่อไปได้โดยไม่ถูกจับตามอง เนื่องจาก CyberStrikeAI กำลังได้รับความนิยมสูงขึ้นอย่างรวดเร็ว

บทสรุป: อนาคตที่น่ากังวลของอาวุธไซเบอร์ AI

เหตุการณ์นี้คือสัญญาณเตือนภัยที่ชัดเจนว่า เครื่องมือโอเพนซอร์สที่สร้างขึ้นมาเพื่อทดสอบระบบ สามารถถูกเปลี่ยนเป็นอาวุธร้ายแรง ได้ทันทีเมื่อผสานเข้ากับ AI

Will Thomas เตือนว่าการแพร่กระจายของเครื่องมือโจมตีที่เสริมพลังด้วย AI อย่าง CyberStrikeAI ถือเป็นพัฒนาการที่น่ากังวลอย่างยิ่งในโลกไซเบอร์ปัจจุบัน

ข้อมูลอ้างอิง

Mar 3, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/03/open-source-cyberstrikeai-deployed-in.html