วันที่ 12 ฤศจิกายน 2568

จาก Log4j ถึง IIS — แฮ็กเกอร์จีนเปลี่ยมช่องโหว่เก่าให้กลายเป็นเครื่องมือสอดแนมระดับโลก

กลุ่มปฏิบัติการทางไซเบอร์ที่เชื่อมโยงกับจีนถูกกล่าวถึงว่าเป็นผู้ดำเนินการโจมตีที่มุ่งเป้าไปยังองค์กรไม่แสวงหาผลกำไรในสหรัฐฯ โดยมีเป้าหมายเพื่อสร้างการอยู่รอดถาวร (persistence) ในระบบ กิจกรรมนี้เป็นส่วนหนึ่งของการรณรงค์ในวงกว้างที่มุ่งเป้าไปยังหน่วยงานสหรัฐฯ ที่เกี่ยวข้องหรือมีส่วนร่วมกับประเด็นนโยบายระหว่างประเทศ

ตามรายงานจากทีม Symantec และ Carbon Black ของ Broadcom องค์กรที่ตกเป็นเป้าหมายนี้ “มีบทบาทในการพยายามชักจูงนโยบายของรัฐบาลสหรัฐฯ ในประเด็นระหว่างประเทศ” โดยผู้โจมตีสามารถเข้าถึงเครือข่ายได้เป็นเวลาหลายสัปดาห์ในเดือนเมษายน 2025

ห่วงโซ่การโจมตี: จากการสแกนสู่ RAT ในหน่วยความจำ

1. การเข้าถึงเบื้องต้น: สัญญาณแรกของกิจกรรมเกิดขึ้นเมื่อวันที่ 5 เมษายน 2025 เมื่อพบการสแกนขนาดใหญ่ต่อเซิร์ฟเวอร์ โดยใช้ช่องโหว่ที่เป็นที่รู้จักหลากหลายรายการ รวมถึง CVE-2022-26134 (Atlassian), CVE-2021-44228 (Apache Log4j), CVE-2017-9805 (Apache Struts) และ CVE-2017-17562 (GoAhead Web Server) Symantec และ Carbon Black บอกว่าไม่มีหลักฐานชี้ว่าความพยายามในการโจมตีเหล่านี้ประสบความสำเร็จ คาดว่าผู้โจมตีอาจได้การเข้าถึงเบื้องต้นจากการโจมตีแบบเดารหัสผ่าน (brute-force) หรือการใช้ บัญชีและรหัสผ่านที่รั่วไหล (credential stuffing)
2. การสำรวจและตั้งค่า Persistence: หลังจากนั้นไม่มีการกระทำเพิ่มเติมจนกระทั่งวันที่ 16 เมษายน เมื่อผู้โจมตีรันคำสั่ง curl หลายคำสั่งเพื่อตรวจสอบการเชื่อมต่ออินเทอร์เน็ต จากนั้นรันเครื่องมือ netstat ของวินโดวส์เพื่อเก็บข้อมูลการกำหนดค่าเครือข่าย ตามด้วยการตั้งค่าความคงทนด้วยการสร้างงานที่ทำงานตามตารางเวลา (scheduled task)

- งานนี้ถูกออกแบบให้เรียกใช้ไบนารีที่ถูกต้องตามกฎหมายของไมโครซอฟท์ msbuild.exe เพื่อรันเพย์โหลดที่ไม่ระบุ
- นอกจากนี้ยังสร้าง scheduled task อีกตัวซึ่งตั้งค่าให้รันทุก 60 นาที ในสิทธิ์ผู้ใช้ระดับสูง SYSTEM

3. การโหลดเพย์โหลด: งานใหม่ตัวนี้ ตามที่ Symantec และ Carbon Black กล่าว สามารถโหลดและฉีดโค้ดไม่ทราบชนิดลงใน csc.exe ซึ่งท้ายที่สุดเปิดการสื่อสารกับเซิร์ฟเวอร์คำสั่ง-ควบคุม (C2) ที่ 38.180.83[.]166 ต่อมา ผู้โจมตีถูกสังเกตเห็นว่ารันตัวโหลดแบบกำหนดเองเพื่อขยายและรันเพย์โหลดที่ไม่ระบุ ซึ่งน่าจะเป็นโทรจันเข้าถึงระยะไกล (RAT) ในหน่วยความจำ

การใช้เครื่องมือร่วมกัน (Tool Sharing) และการเชื่อมโยงกลุ่ม

การโจมตีนี้แสดงให้เห็นแนวโน้มการใช้เครื่องมือร่วมกันระหว่างกลุ่มปฏิบัติการที่เชื่อมโยงกับจีน:

- มีการสังเกตการรันคอมโพเนนต์ของแอนตี้ไวรัส Vipre ที่ถูกต้องตามกฎหมาย (vetysafe.exe) เพื่อทำ DLL sideloading กับตัวโหลด DLL (sbamres.dll)
- คอมโพเนนต์นี้เคยถูกใช้ในการ sideload DLL ร่วมกับ Deed RAT (หรือ Snappybee) ในกิจกรรมก่อนหน้านี้ที่เชื่อมโยงกับ Salt Typhoon (หรือ Earth Estries) และยังเคยถูกใช้ในการโจมตีที่เชื่อมโยงกับ Earth Longzhi ซึ่งเป็นกลุ่มย่อยของ APT41
- Broadcom กล่าวว่า สำเนาของ DLL ที่เป็นอันตรายนี้เคยถูกใช้ในการโจมตีที่เชื่อมโยงกับกลุ่มปฏิบัติการจีนที่รู้จักในชื่อ Space Pirates และตัวแปรของคอมโพเนนต์นี้ก็เคยถูกใช้โดยกลุ่ม APT จีน Kelp (หรือ Salt Typhoon) ในเหตุการณ์แยกกัน
- เครื่องมืออื่น ๆ ที่พบในเครือข่ายเป้าหมายรวมถึง Dcsync และ Imjpuexc
- เป้าหมาย: "จากกิจกรรมบนเหยื่อชัดเจนว่าผู้โจมตีตั้งใจจะสร้างการอยู่รอดที่แอบแฝงและถาวรในเครือข่าย และพวกเขาสนใจเป้าหมายที่เป็น domain controller ซึ่งอาจทำให้แพร่กระจายไปยังเครื่องอื่น ๆ ในเครือข่ายได้" Symantec และ Carbon Black กล่าว
- การแบ่งปันเครื่องมือ: "การแบ่งปันเครื่องมือระหว่างกลุ่มเป็นแนวโน้มที่มีมานานในกลุ่มปฏิบัติการที่เชื่อมโยงกับจีน ทำให้ยากที่จะระบุได้ว่าเหตุการณ์ชุดหนึ่ง ๆ เป็นของกลุ่มใดโดยเฉพาะ"

นอกจากนี้ นักวิจัยความปลอดภัยที่ใช้ชื่อออนไลน์ว่า BartBlaze ยังเปิดเผยการใช้ประโยชน์จากช่องโหว่ของ WinRAR (CVE-2025-8088) โดย Salt Typhoon เพื่อเริ่มชุดการโจมตีที่ sideload DLL ซึ่งทำหน้าที่รัน shellcode บนโฮสต์ที่ถูกบุกรุก เพย์โหลดสุดท้ายถูกออกแบบมาเพื่อติดต่อกับเซิร์ฟเวอร์ระยะไกล (mimosa.gleeze[.]com)

ภาพรวมกิจกรรมจากกลุ่มแฮ็กจีนอื่น ๆ (ESET Report)

รายงานจาก ESET ยืนยันว่ากลุ่มที่สอดคล้องกับจีนยังคงเคลื่อนไหวอย่างต่อเนื่องเพื่อสนับสนุนเป้าหมายเชิงภูมิรัฐศาสตร์ของปักกิ่ง:

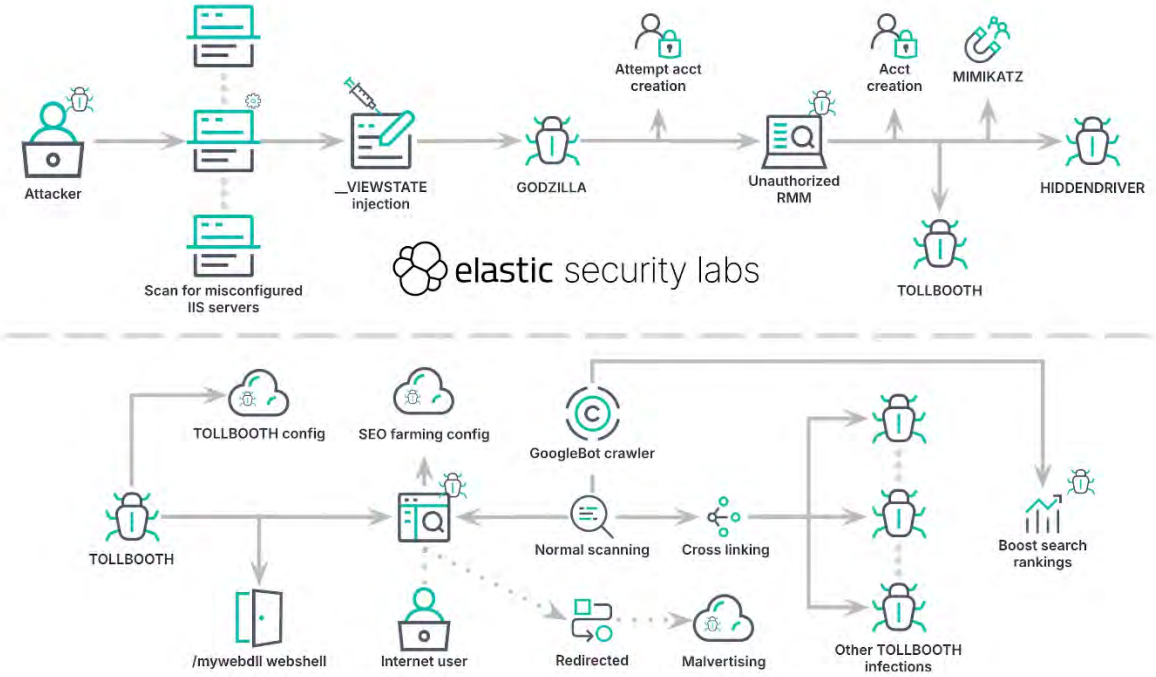
- Speccom (IndigoZebra / SMAC): โจมตีภาคพลังงานในเอเชียกลางใน ก.ค. 2025 ผ่านอีเมลฟิชชิ่งเพื่อส่งตัวแยกข้อมูล BLOODALCHEMY และแบ็กดอร์แบบกำหนดเอง เช่น kidsRAT และ RustVoralix
- DigitalRecyclers: โจมตีองค์กรยุโรปใน ก.ค. 2025 โดยใช้เทคนิคความคงทนที่ผิดปกติซึ่งเกี่ยวข้องกับการใช้เครื่องมือช่วยเข้าถึงชื่อ Magnifier เพื่อยกระดับสิทธิ์เป็น SYSTEM
- FamousSparrow: โจมตีหน่วยงานรัฐบาลในละตินอเมริกา (อาร์เจนตินา เอกวาดอร์ กัวเตมาลา ฮอนดูรัส และปานามา) ระหว่าง มิ.ย. - ก.ย. 2025 โดยน่าจะใช้ช่องโหว่ ProxyLogon ใน Microsoft Exchange Server เพื่อปล่อย SparrowDoor
- SinisterEye (LuoYu และ Cascade Panda): โจมตีบริษัทไต้หวันในภาคการบินเชิงพาณิชย์, องค์กรการค้าสหรัฐฯ ในจีน, สำนักงานรัฐบาลกรีซในจีน, และรัฐบาลเอกวาดอร์ ระหว่าง พ.ค. - ก.ย. 2025 เพื่อส่งมัลแวร์ WinDealer (สำหรับ Windows) และ SpyDealer (สำหรับ Android) ผ่านการโจมตีแบบ adversary-in-the-middle (AitM) เพื่อยึดกลไกอัปเดตซอฟต์แวร์ที่ถูกต้องตามกฎหมาย
- PlushDaemon: โจมตีบริษัทญี่ปุ่นและบริษัทข้ามชาติในกัมพูชาในเดือน มิ.ย. 2025 ผ่านวิธี AitM poisoning เพื่อส่ง SlowStepper โดยบุกรุกอุปกรณ์เครือข่าย (เช่น เราเตอร์) และปรับใช้เครื่องมือ EdgeStepper เพื่อเปลี่ยนเส้นทางการจ่าย DNS จากเครือข่ายเป้าหมายไปยังเซิร์ฟเวอร์ DNS ที่ผู้โจมตีควบคุม ซึ่งจะส่ง SlowStepper ซึ่งเป็นแบ็กดอร์ตัวหลัก

การโจมตีเซิร์ฟเวอร์ IIS ที่กำหนดค่าไม่ถูกต้อง

นักล่าภัยคุกคามยังตรวจพบกลุ่มที่พูดภาษาจีนเป้าหมายไปยัง เซิร์ฟเวอร์ IIS ที่กำหนดค่าไม่ถูกต้อง โดยใช้คีย์เครื่อง (machine keys) ของ ASP.NET ที่เผยแพร่สู่สาธารณะเพื่อติดตั้งแบ็กดอร์ที่เรียกว่า TOLLBOOTH (หรือ HijackServer) ซึ่งมาพร้อมโมดูล SEO cloaking และความสามารถของเว็บเชลล์

- REF3927 เป็นผู้ที่นำคีย์เครื่อง ASP.NET ที่เปิดเผยสาธารณะมาใช้งานเพื่อลอบเข้าครอบครองเซิร์ฟเวอร์ IIS และติดตั้งโมดูล TOLLBOOTH การติดเชื้อมุ่งเน้นที่อินเดียและสหรัฐฯ โดยติดเชื้อเซิร์ฟเวอร์จำนวนหลายร้อยเครื่องทั่วโลก
- การโจมตียังพยายามใช้อำนาจจากการเข้าถึงเบื้องต้นเพื่อลงโมดูลที่เป็นอันตราย เช่น การวาง Godzilla web shell, การรัน GotoHTTP remote access tool, การใช้ Mimikatz เพื่อเก็บข้อมูลประจำตัว (credentials) และ

การปล่อย HIDDENDRIVER ซึ่งเป็นเวอร์ชันปรับแต่งของ rootkit แบบโอเพนซอร์ส Hidden เพื่อปกปิดการมีอยู่ของเพย์โหลดที่เป็นอันตรายบนเครื่องที่ติดเชื้อ



กลุ่มเหล่านี้เป็นสมาชิกล่าสุดในรายชื่อกลุ่มปฏิบัติการจีนที่ยาว เช่น GhostRedirector, Operation Rewrite และ UAT-8099 ที่เคยโจมตีเซิร์ฟเวอร์ IIS มาก่อน

- ความเสี่ยง: บริษัทความปลอดภัยฝรั่งเศสกล่าวว่า แม้ผู้ปฏิบัติการที่เป็นอันตรายจะใช้ประโยชน์จากการบุกรุกเพื่อสนับสนุนการทำ SEO แต่โมดูลที่ติดตั้งนั้นให้ช่องทางถาวรและไม่ต้องพิสูจน์ตัวตน ซึ่งอนุญาตให้ใครก็ได้รันคำสั่งจากระยะไกลบนเซิร์ฟเวอร์ที่ได้รับผลกระทบ

ข้อมูลอ้างอิง

Nov 7, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/11/from-log4j-to-iis-chinas-hackers-turn.html