วันที่ 6 มกราคม 2569

RondoDox Botnet ใช้ช่องโหว่ร้ายแรง React2Shell เข้ายึดอุปกรณ์ IoT และเว็บเซิร์ฟเวอร์

นักวิจัยด้านความปลอดภัยไซเบอร์ได้เปิดเผยรายละเอียดของแคมเปญการโจมตีที่ดำเนินมาอย่างต่อเนื่องยาวนานถึง 9 เดือน โดยมุ่งเป้าไปที่อุปกรณ์ Internet of Things (IoT) และเว็บแอปพลิเคชันเพื่อดึงเข้าเป็นส่วนหนึ่งของเครือข่ายบอตเน็ตขนาดใหญ่ในชื่อ RondoDox

ความน่ากลัวล่าสุดในเดือนธันวาคม 2025 คือการที่บอตเน็ตกลุ่มนี้ได้เริ่มนำช่องโหว่ระดับวิกฤตที่เพิ่งถูกเปิดเผยอย่าง React2Shell (CVE-2025-55182) มาใช้เป็นหัวหอกหลักในการเจาะระบบ ตามรายงานวิเคราะห์จาก CloudSEK

ทำความรู้จักช่องโหว่ React2Shell (CVE-2025-55182)

React2Shell คือช่องโหว่ความรุนแรงระดับสูงสุด (CVSS: 10.0) ที่เกิดขึ้นใน React Server Components (RSC) และ Next.js ซึ่งเปิดทางให้ผู้โจมตีที่ไม่ได้ผ่านการยืนยันตัวตนสามารถสั่งรันคำสั่งจากระยะไกล (Remote Code Execution) ได้ทันที

จากสถิติของ Shadowserver ณ วันที่ 31 ธันวาคม 2025 พบว่าทั่วโลกยังมีระบบที่มีความเสี่ยงสูงถึง 90,300 แห่ง โดยกระจายตัวอยู่ใน:

- สหรัฐอเมริกา: 68,400 แห่ง
- เยอรมนี: 4,300 แห่ง
- ฝรั่งเศส: 2,800 แห่ง
- อินเดีย: 1,500 แห่ง

วิวัฒนาการ 3 ระยะของ RondoDox สู่การโจมตีอัตโนมัติ

บอตเน็ต RondoDox เริ่มปรากฏตัวตั้งแต่ต้นปี 2025 และขยายตัวผ่านการสะสมช่องโหว่แบบ N-day ใหม่ๆ เช่น CVE-2023-1389 และ CVE-2025-24893 (ซึ่งสอดคล้องกับรายงานจาก Darktrace, Kaspersky และ VulnCheck) โดยแคมเปญนี้ถูกแบ่งออกเป็น 3 ระยะหลักดังนี้:

1. มีนาคม – เมษายน 2025: ระยะเริ่มต้นในการสำรวจเป้าหมายและสแกนหาช่องโหว่ด้วยวิธีการ Manual (ทำด้วยมือ)
2. เมษายน – มิถุนายน 2025: เริ่มสแกนหาช่องโหว่จำนวนมากรายวันในเว็บแอปพลิเคชันยอดนิยมอย่าง WordPress, Drupal, Struts2 และอุปกรณ์ IoT เช่น เราเตอร์ Wavlink
3. กรกฎาคม – ต้นธันวาคม 2025: ยกระดับสู่การปล่อยการโจมตีอัตโนมัติขนาดใหญ่ (Mass Automated Attacks) แบบรายชั่วโมง

กลไกการเจาะระบบและเพย์โหลดสุดอันตราย

ในการโจมตีเมื่อเดือนธันวาคม 2025 ผู้โจมตีจะเริ่มจากการสแกนหาเซิร์ฟเวอร์ Next.js ที่มีช่องโหว่ จากนั้นจะส่งไฟล์อันตรายเข้าสู่ระบบที่ติดเชื้อผ่านชุดคำสั่งเฉพาะในไดเรกทอรี /nuts/ ดังนี้:

- /nuts/poop: ตัวขุดคริปโตเคอร์เรนซี (Cryptojacking)
- /nuts/bolts: ตัวโหลดบอตเน็ต (Botnet Loader) และตัวตรวจสอบสถานะ
- /nuts/x86: บอตเน็ต Mirai เวอร์ชันดัดแปลง

ความซับซ้อนของไฟล์ /nuts/bolts: ไฟล์นี้ไม่ได้แค่ติดตั้งมัลแวร์ แต่ทำหน้าที่เป็น "นักเลงเจ้าที่" โดยจะทำการหยุดการทำงานของมัลแวร์หรือโปรแกรมขุดเหรียญตัวอื่นที่มีอยู่ก่อนหน้า จากนั้นจึงดาวน์โหลดไฟล์บอตหลักจากเซิร์ฟเวอร์ควบคุม (C2) ของผู้โจมตี โดยเวอร์ชันที่ตรวจพบมีความสามารถในการลบซอฟต์แวร์บอตเน็ตคู่แข่ง, ลบเพย์โหลดที่รันผ่าน Docker, ลบร่องรอยแคมเปญเก่า รวมถึง Cron Job ที่เกี่ยวข้อง และทำการตั้งค่าการคงอยู่ (Persistence) ของตัวเองผ่านไฟล์ /etc/crontab

นอกจากนี้ CloudSEK ยังระบุถึงกลไกการผูกขาดระบบว่า: "มันจะสแกนไฟล์ใน /proc อย่างต่อเนื่องเพื่อตรวจสอบโปรแกรมที่กำลังรัน และจะสั่งปิดโปรเซสที่ไม่อยู่ในรายการอนุญาต (Allowlist) ทุกๆ 45 วินาที เพื่อป้องกันไม่ให้คู่แข่งรายอื่นเข้ามาติดมัลแวร์ซ้ำได้"

แนวทางการป้องกันสำหรับองค์กร

เพื่อป้องกันไม่ให้ระบบของคุณถูกดึงเข้าเป็นส่วนหนึ่งของบอตเน็ต RondoDox องค์กรควรดำเนินการดังนี้:

- อัปเดตด่วน: อัปเดต Next.js ให้เป็นเวอร์ชันล่าสุดที่แก้ไขช่องโหว่ React2Shell แล้วทันที
- Network Segregation: แยกอุปกรณ์ IoT ออกไปอยู่ใน VLAN เฉพาะ เพื่อจำกัดการแพร่กระจาย
- Security Tools: ติดตั้งและใช้งาน Web Application Firewall (WAF) เพื่อกรองทราฟฟิกอันตราย
- Monitoring: เฝ้าระวังโปรเซสที่ทำงานผิดปกติในระบบ (โดยเฉพาะการทำงานใน /proc)
- Threat Intel: บล็อกโครงสร้างพื้นฐานหรือ IP Address ที่เกี่ยวข้องกับ C2 ของ RondoDox ตามฐานข้อมูลที่รู้จัก

ข้อมูลอ้างอิง

Jan 1, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/01/rondodox-botnet-exploits-critical.html