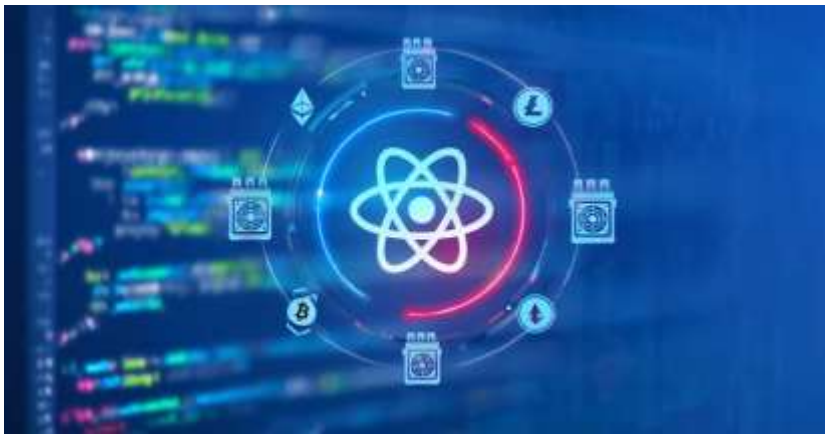
วันที่ 12 ธันวาคม 2568

React2Shell Exploitation Delivers Crypto Miners and New Malware Across Multiple Sectors



การโจมตีซัพพลายเชนซอฟต์แวร์ที่เรียกว่า React2Shell กำลังทวีความรุนแรงขึ้นอย่างมาก โดยผู้ไม่หวังดีใช้ประโยชน์จากช่องโหว่ความรุนแรงระดับสูงสุดใน React Server Components (RSC) (รหัส CVE-2025-55182) ซึ่งเปิดให้ผู้ไม่ผ่านการยืนยันตัวตนสามารถรันโค้ดจากระยะไกล (RCE) ได้

Huntress, Palo Alto Networks Unit 42, Rapid7 และ Wiz ได้ยืนยันว่าช่องโหว่นี้ที่เกิดขึ้นใน Next.js กำลังถูกนำไปใช้โจมตีจริงในหลายอุตสาหกรรมทั่วโลก โดยเฉพาะอุตสาหกรรมการก่อสร้างและบันเทิง มีกลุ่มผู้โจมตีมากกว่า 15 กลุ่ม ที่เข้ามาใช้ประโยชน์นี้ และมีการพบความพยายามปล่อย Payload สำหรับ Linux ลงบน Windows ซึ่งบ่งบอกถึงการใช้เครื่องมือโจมตีอัตโนมัติ

การค้นพบครั้งแรกและการโจมตีอัตโนมัติ

การโจมตีที่บันทึกไว้ครั้งแรกบน Windows โดย Huntress เกิดขึ้นเมื่อวันที่ 4 ธันวาคม 2025 เมื่อผู้โจมตีที่ไม่ทราบตัวตนใช้ประโยชน์จาก Next.js ที่มีช่องโหว่เพื่อปล่อยสคริปต์ shell จากนั้นตามด้วยคำสั่งเพื่อติดตั้งตัวขุดคริปโตและแบ็กดอร์บน Linux ในอีกสองกรณี

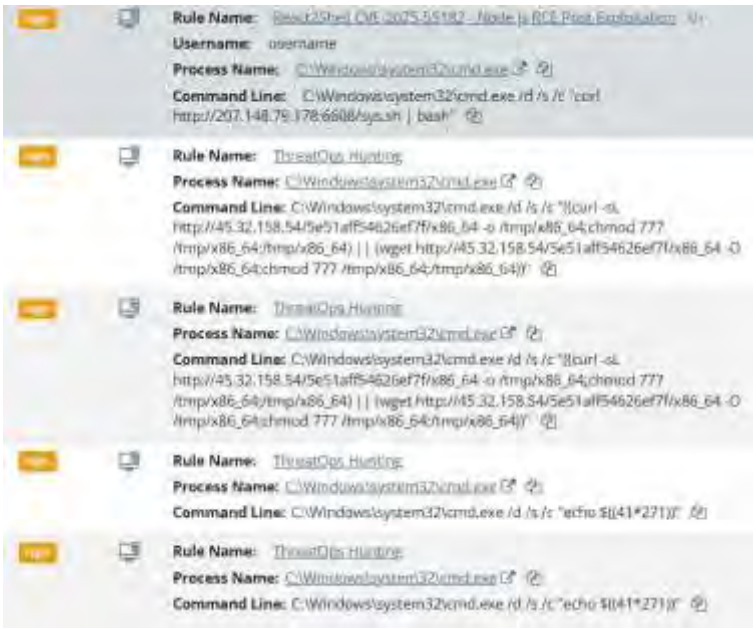
ผู้โจมตีถูกพบว่ารันคำสั่งค้นหาระบบและพยายามดาวน์โหลด payload หลายชุดจากเซิร์ฟเวอร์สั่งการและควบคุม (C2) โดยมีการบุกรุกบางครั้งที่พุ่งเป้าหมายไปยังระบบ Linux เพื่อปล่อยตัวขุด XMRig รวมถึงใช้เครื่องมือบน GitHub ที่เปิดให้สาธารณะเพื่อค้นหา Next.js ที่มีช่องโหว่ก่อนเริ่มโจมตี Huntress ระบุว่า จากรูปแบบที่เหมือนกันบนหลาย endpoint ไม่ว่าจะเป็น probe ช่องโหว่ ชุดทดสอบ shell code และโครงสร้าง C2 ที่เหมือนกัน จึงประเมินว่าผู้โจมตีน่าจะใช้เครื่องมือโจมตีอัตโนมัติ หลักฐานเพิ่มเติมคือการพยายามปล่อย payload สำหรับ Linux ลงบน Windows ซึ่งบ่งบอกว่าระบบอัตโนมัติไม่ได้แยกแยะระบบปฏิบัติการ

กลไกการโจมตีและสถิติความเสี่ยง

- การโจมตีอัตโนมัติ: ผู้โจมตีใช้เครื่องมือสาธารณะบน GitHub เพื่อค้นหา Next.js ที่มีช่องโหว่ก่อนเริ่มโจมตี จากนั้นปล่อยสคริปต์ Shell เพื่อติดตั้งตัวขุดคริปโตและแบ็กดอร์
- สถิติความเสี่ยง: ณ วันที่ 8 ธันวาคม 2025 Shadowserver Foundation พบ IP ที่มีโค้ดที่มีช่องโหว่มากกว่า 165,000 รายการ โดยกว่า 99,200 อินสแตนซ์อยู่ในสหรัฐฯ ตามด้วยเยอรมนี (14,100), ฝรั่งเศส (6,400) และอินเดีย (4,500)
- เป้าหมายกว้าง: องค์กรกว่า 50 แห่งจากหลายภาคส่วนได้รับผลกระทบ เช่น การเงิน ธุรกิจ การศึกษา เทคโนโลยี หน่วยงานรัฐ บริษัท Consulting สื่อ กฎหมาย โทรคมนาคม และค้าปลีก โดยสหรัฐฯ, เอเชีย, อเมริกาใต้ และตะวันออกกลางคือภูมิภาคที่ได้รับผลมากที่สุด

Payload ร้ายแรงที่ถูกพบในการโจมตี

การโจมตี React2Shell ครั้งนี้ได้ยกระดับไปสู่การติดตั้งแบ็กดอร์และเครื่องมือ Post-exploitation ระดับสูงหลายตระกูล โดยมี Payload สำคัญที่ถูกตรวจพบดังนี้:



1. PeerBlight: เป็นแบ็กดอร์บน Linux ที่มีโค้ดบางส่วนคล้ายกับมัลแวร์ RotaJakiro และ Pink ที่เคยพบในปี 2021 โดย PeerBlight จะติดตั้งบริการ systemd เพื่อสร้างความคงอยู่ในระบบ และจะปลอมตัวเป็นโปรเซส ksoftirqd เพื่อหลบเลี่ยงการตรวจจับ ความสามารถทางเทคนิคที่ซับซ้อนของมันคือการใช้ Domain Generation Algorithm (DGA) และเครือข่าย BitTorrent Distributed Hash Table (DHT) เป็น C2 สำรอง โดยเมื่อเข้าร่วมเครือข่าย DHT แบ็กดอร์จะลงทะเบียน Node ID ที่ขึ้นต้นด้วย Prefix ที่ถูกฮาร์ดโค้ดไว้คือ LOLlolLOL ซึ่งใช้ระบุ Node ที่ติดเชื้อหรือ Node ของผู้โจมตีที่เก็บข้อมูล C2 แบ็กดอร์นี้รองรับการอัปโหลด/ดาวน์โหลด/ลบไฟล์ เปิด Reverse Shell แก้ไขสิทธิ์ไฟล์ รันไบนารีใดๆ และมีความสามารถในการอัปเดตตัวเองได้

2. ZinFoq: เป็นไบนารี ELF สำหรับ Linux ที่เขียนด้วย Go โดยทำหน้าที่เป็นเครื่องมือ Post-exploitation ระดับสูง มันสามารถทำหน้าที่เป็น Shell แบบโต้ตอบ, จัดการไฟล์, Pivot เครือข่าย, และมีความสามารถในการแก้ไข Timestamps (การเข้าถึงไฟล์) เพื่อกลบร่องรอย นอกจากนี้ ZinFoq ยังจะลบประวัติ Bash และมีกลไกการพรางตัวที่ซับซ้อน โดยปลอมตัวเป็นบริการ Linux ที่ถูกต้องกว่า 44 แบบ อาทิ /sbin/audispd หรือ /usr/sbin/ModemManager

3. CowTunnel: เป็นเครื่องมือ Reverse Proxy ที่มีความสามารถในการเลี่ยงไฟร์วอลล์ที่มักตรวจจับเฉพาะการเชื่อมต่อขาเข้า โดย CowTunnel จะเปิดการเชื่อมต่อออกไปยังเซิร์ฟเวอร์ Fast Reverse Proxy (FRP) ของผู้โจมตีแทน

4. มัลแวร์โจมตีอื่น ๆ และ Dropper Scripts: มีการพบสคริปต์ Dropper หลายตัว เช่น sex.sh ซึ่งดึง XMRig 6.24.0 (ตัวขุดคริปโต) โดยตรงจาก GitHub, สคริปต์ d5.sh ที่ใช้ติดตั้ง Sliver C2 framework, และ fn22.sh ซึ่งเป็นเวอร์ชันดัดแปลงของ d5.sh ที่เพิ่มระบบอัปเดตตัวเอง นอกจากนี้ยังพบมัลแวร์ wocaosinm.sh ซึ่งเป็นมัลแวร์ Kaiji เวอร์ชันใหม่สำหรับทำ DDoS

การเชื่อมโยงและการยกระดับความรุนแรง

- Unit 42 พบกิจกรรมที่น่าจะเกี่ยวข้องกับแคมเปญ Contagious Interview ที่ใช้ปล่อย EtherRAT และยังพบมัลแวร์ BPFDoor และ Auto-Color
- Rapid7 เห็นสัญญาณเชื่อมโยงกับเครื่องมือที่เคยใช้โดย กลุ่มแรนซัมแวร์
- VulnCheck เตือนว่าการโจมตี React2Shell น่าจะ "ลากยาว" และแนะนำให้องค์กรคำนึงถึงโค้ด PoC เวอร์ชันดัดแปลงและ Payload แบบใหม่

ข้อแนะนำด่วนสำหรับการป้องกัน

Christiaan Beek จาก Rapid7 ชี้ว่า "นี่คือสถานการณ์ที่ต้องแพตช์ทันที เพราะการโจมตี กำลังเกิดขึ้นพร้อมกันทั่วทั้งโลกไซเบอร์"

องค์กรที่ใช้คอมโพเนนต์เหล่านี้ควรอัปเดตทันที:

- react-server-dom-webpack
- react-server-dom-parcel
- react-server-dom-turbopack

ข้อมูลอ้างอิง

Dec 10, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/12/react2shell-exploitation-delivers.html