วันที่ 27 มิถุนายน 2568

นักวิจัยด้านความปลอดภัยพบวิธีการหยุดยั้งแคมเปญ การขุดสกุลเงินดิจิทัล

นักวิจัยด้านความปลอดภัยไซเบอร์ได้ค้นพบ 2 วิธีใหม่สุดล้ำที่สามารถใช้ขัดขวางการทำงานของบอตเน็ตขุดคริปโตเคอร์เรนซีได้อย่างมีประสิทธิภาพ วิธีการเหล่านี้อาศัยการออกแบบโครงสร้างการขุดคริปโตทั่วไป เพื่อหยุดกระบวนการขุดอย่างสิ้นเชิง ตามรายงานล่าสุดจากบริษัท Akamai

"เราได้พัฒนาเทคนิคสองอย่างที่ใช้โครงสร้างการขุดและนโยบายของพูลเป็นจุดอ่อน ซึ่งช่วยให้เราลดประสิทธิภาพของบอตเน็ตขุดคริปโตลงได้จนถึงขั้นปิดมันได้โดยสมบูรณ์ ทำให้ผู้โจมตีต้องเปลี่ยนแปลงโครงสร้างพื้นฐานครั้งใหญ่ หรือแม้กระทั่งละทิ้งการโจมตีทั้งหมด" Maor Dahan นักวิจัยด้านความปลอดภัยจาก Akamai กล่าว

บริษัทโครงสร้างพื้นฐานเว็บไซต์ระบุว่า เทคนิคเหล่านี้อาศัยการเจาะช่องโหว่ในโปรโตคอลการขุด Stratum เพื่อทำให้พร็อกซีหรือวอลเล็ตของผู้โจมตีถูกแบน ส่งผลให้การทำงานทั้งหมดหยุดชะงัก

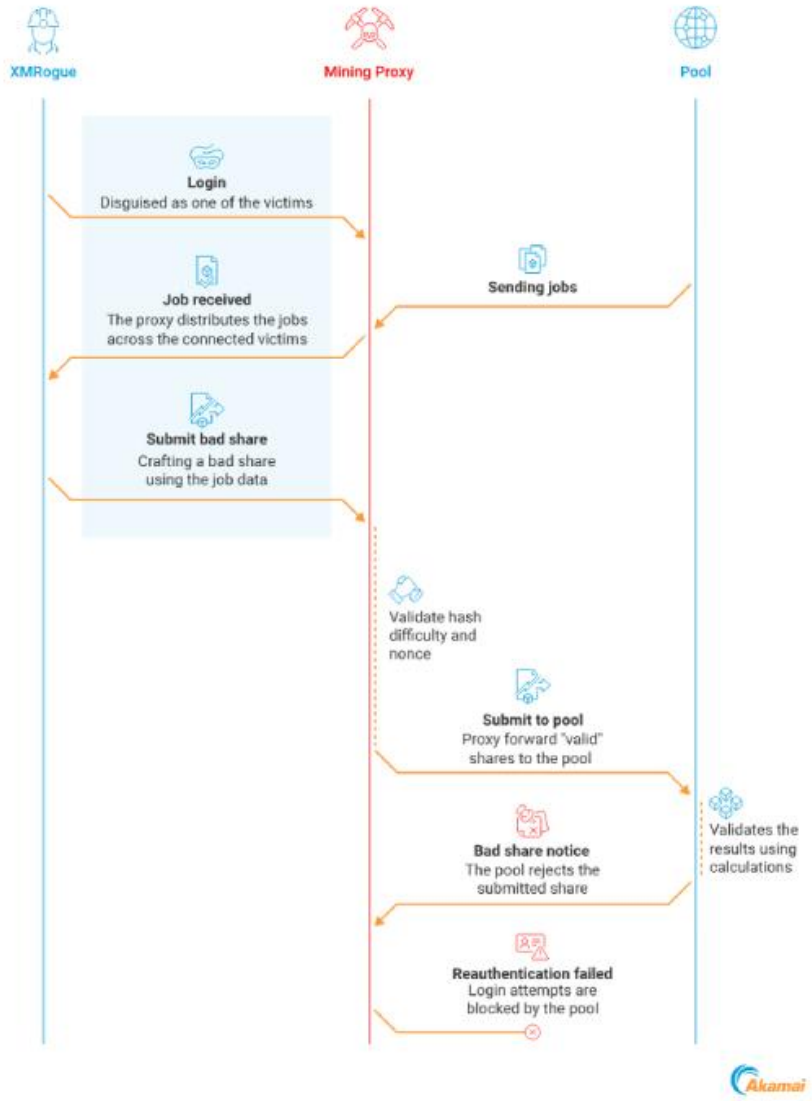
วิธีที่ 1: การโจมตี "Bad Shares"

วิธีแรกมีชื่อว่า "bad shares" โดยจะทำให้พร็อกซีขุดถูกแบนออกจากเครือข่าย ส่งผลให้การขุดทั้งหมดหยุดลง และทำให้การใช้งาน CPU ของเหยื่อลดจาก 100% เหลือ 0%

แม้ว่าพร็อกซีขุดจะทำหน้าที่เป็นตัวกลางและช่วยปกป้องพูลขุดของผู้โจมตี รวมถึงที่อยู่วอลเล็ตของพวกเขา แต่มันก็กลายเป็นจุดอ่อนเพียงจุดเดียวที่สามารถโจมตีได้ด้วยการรบกวนการทำงานปกติของมัน

"แนวคิดง่ายมาก: โดยการเชื่อมต่อเข้ากับพร็อกซีที่เป็นอันตรายในฐานะนักขุด เราสามารถส่งผลการขุดที่ไม่ถูกต้อง bad shares ซึ่งจะผ่านการตรวจสอบของพร็อกซีไปได้ และจะถูกส่งต่อไปยังพูล" Dahan อธิบาย

"เมื่อมี bad shares ต่อเนื่องกัน ในที่สุดพร็อกซีก็จะถูกแบน ทำให้การขุดของบอตเน็ตขุดคริปโตทั้งระบบหยุดชะงัก"



วิธีนี้จะใช้เครื่องมือที่พัฒนาขึ้นเองชื่อว่า XMRogue เพื่อปลอมตัวเป็นนักขุด เชื่อมต่อกับพร็อกซีขุด แล้วส่ง bad shares อย่างต่อเนื่อง จนทำให้พร็อกซีถูกแบนออกจากพูล

วิธีที่ 2: แบนวอลเล็ตโดยตรง (กรณีไม่มีพร็อกซี)

วิธีที่สองที่ Akamai คิดค้นขึ้น ใช้ในกรณีที่นักขุดเหยื่อต่อเข้ากับพูลสาธารณะโดยตรง โดยไม่ผ่านพร็อกซี โดยอาศัยเงื่อนไขว่าพูลจะสามารถแบนที่อยู่วอลเล็ตได้เป็นเวลา 1 ชั่วโมง ถ้ามีเวิร์กเกอร์เชื่อมต่อพร้อมกันเกิน 1,000 ตัว

พูดง่ายๆ คือ ถ้าเริ่มการเชื่อมต่อมากกว่า 1,000 ครั้งพร้อมกันโดยใช้วอลเล็ตของผู้โจมตี จะบังคับให้พูลแบนวอลเล็ตของผู้โจมตีได้ อย่างไรก็ตาม วิธีนี้ไม่ได้แก้ปัญหาแบบถาวร เพราะเมื่อหยุดการเชื่อมต่อหลายครั้ง บัญชีก็จะกลับมาใช้งานได้อีกครั้ง

Akamai ระบุว่า แม้ว่าวิธีเหล่านี้จะถูกใช้กับนักขุด Monero แต่ก็สามารถนำไปประยุกต์ใช้กับคริปโตเคอร์เรนซีอื่นๆ ได้เช่นกัน

ผลกระทบและความสำคัญ

"เทคนิคที่นำเสนอข้างต้น แสดงให้เห็นว่าฝั่งผู้ใช้สามารถปิดการทำงานของแคมเปญขุดคริปโตที่เป็นอันตรายได้อย่างมีประสิทธิภาพ โดยไม่กระทบต่อการทำงานของพูลที่ถูกต้องตามกฎหมาย โดยอาศัยนโยบายของพูลเอง" Dahan กล่าว

"นักขุดที่ถูกกฎหมายสามารถกู้คืนจากการโจมตีแบบนี้ได้อย่างรวดเร็ว เพราะพวกเขาสามารถเปลี่ยน IP หรือวอลเล็ตของตัวเองได้ง่ายๆ ในเครื่อง แต่สำหรับนักขุดที่เป็นอันตราย การแก้ไขจะยากกว่ามาก เพราะต้องปรับโครงสร้างของบอตเน็ตทั้งระบบ สำหรับนักขุดที่มีความซับซ้อนไม่มาก วิธีป้องกันนี้อาจทำให้บอตเน็ตหยุดทำงานไปเลยก็ได้"

การค้นพบครั้งนี้ถือเป็นความก้าวหน้าครั้งสำคัญในการต่อสู้กับบอตเน็ตขุดคริปโต ที่มักใช้ทรัพยากรคอมพิวเตอร์ของผู้ใช้โดยไม่ได้รับอนุญาต วิธีการของ Akamai ช่วยให้เรามีเครื่องมือที่มีประสิทธิภาพมากขึ้นในการหยุดยั้งการโจมตีเหล่านี้ และลดผลกระทบต่อผู้ใช้งานทั่วโลก

ข้อแนะนำ

- บล็อกการเข้าถึง Command & Control (C2)
- จำกัดสิทธิ์ผู้ใช้และ network segmentation
- หลีกเลี่ยงการให้สิทธิ์ local admin โดยไม่จำเป็น
- ตรวจสอบการใช้ทรัพยากร เนื่องจากมัลแวร์ขุดคริปโตมักใช้ CPU/GPU สูงผิดปกติ

ข้อมูลอ้างอิง

Jun 24, 2025 By Ravie Lakshmanan

- https://thehackernews.com/2025/06/researchers-find-way-to-shut-down.html