วันที่ 6 สิงหาคม 2568

ช่องโหว่ PAM 'Plague' ใหม่เปิดเผยระบบ Linux สำคัญต่อการโจรกรรมข้อมูลประจำตัว

นักวิจัยด้านความปลอดภัยไซเบอร์ออกมาเตือนเกี่ยวกับช่องโหว่ใหม่ในระบบ Linux ซึ่งถูกตั้งชื่อว่า “Plague” ซึ่งเป็นแบ็กดอร์แบบใหม่ที่ไม่เคยถูกบันทึกมาก่อน และสามารถแอบซ่อนตัวจากการตรวจจับได้นานนับปี

“ตัวมัลแวร์นี้ถูกสร้างขึ้นมาในรูปแบบของโมดูล PAM (Pluggable Authentication Module) ที่เป็นอันตราย ทำให้ผู้โจมตีสามารถหลบเลี่ยงกระบวนการยืนยันตัวตนของระบบได้อย่างเงียบๆ และเข้าถึงระบบผ่าน SSH ได้อย่างถาวร” Pierre-Henri Pezier นักวิจัยจากบริษัท Nextron Systems ระบุ

PAM หรือ Pluggable Authentication Modules คือชุดของไลบรารีที่ใช้จัดการการยืนยันตัวตนของผู้ใช้ในระบบปฏิบัติการ Linux และ UNIX เนื่องจากโมดูล PAM ถูกโหลดเข้าไปในกระบวนการที่มีสิทธิพิเศษสูงสำหรับการตรวจสอบตัวตน การที่มีโมดูลที่เป็นอันตรายแอบแฝงอยู่จึงสามารถนำไปสู่การขโมยข้อมูลชื่อผู้ใช้และรหัสผ่าน การหลบเลี่ยงการตรวจสอบสิทธิ์ และสามารถซ่อนตัวจากเครื่องมือรักษาความปลอดภัยได้อย่างง่ายดาย

ทางบริษัทได้ตรวจพบไฟล์ที่เกี่ยวข้องกับ Plague หลายไฟล์ที่ถูกอัปโหลดไปยัง VirusTotal ตั้งแต่วันที่ 29 กรกฎาคม 2024 แต่ไม่มีเครื่องมือป้องกันไวรัสใดสามารถตรวจจับได้ว่าไฟล์เหล่านี้เป็นอันตราย ยิ่งไปกว่านั้น การที่พบไฟล์หลายตัว ยังบ่งชี้ว่ามัลแวร์นี้กำลังอยู่ในระหว่างการพัฒนาอย่างต่อเนื่องโดยกลุ่มผู้ไม่หวังดีที่ยังไม่ทราบตัวตน

ความสามารถหลักของ Plague:

- ใช้ข้อมูลล็อกอินแบบตายตัว (Static Credentials) เพื่อแอบเข้าระบบ
- มีเทคนิคป้องกันการวิเคราะห์และการย้อนรอย เช่น การต่อต้านการดีบักและการซ่อนข้อความในโค้ด
- มีความสามารถในการซ่อนตัวขั้นสูง เช่น ลบหลักฐานการใช้งาน SSH ออกจากระบบ

การลบหลักฐานนี้จะทำผ่านคำสั่ง unsetenv เพื่อเอาตัวแปรสภาพแวดล้อมอย่าง SSH_CONNECTION และ SSH_CLIENT ออกไป รวมถึงเปลี่ยนเส้นทางไฟล์ประวัติคำสั่ง (HISTFILE) ไปยัง /dev/null เพื่อไม่ให้มีการบันทึกคำสั่งที่ถูกใช้งานไว้ในระบบ

“Plague ฝังตัวลึกเข้าไปในกระบวนการยืนยันตัวตนของระบบ ดำรงอยู่ได้แม้จะมีการอัปเดตระบบ และแทบไม่ทิ้งร่องรอยใดๆ ไว้ให้ตรวจสอบทางนิติวิทยาศาสตร์” Pezier กล่าวเพิ่มเติม “เมื่อรวมกับการปกปิดโค้ดหลายชั้นแล้ว ยิ่งทำให้มันยากที่จะตรวจจับหรือวิเคราะห์ได้”

แบ็กดอร์ Plague แสดงให้เห็นถึงภัยคุกคามที่ซับซ้อนและมีเป้าหมายระยะยาวต่อระบบ Linux การที่มัลแวร์นี้สามารถซ่อนตัวได้อย่างแนบเนียนและฝังลึกในระบบ ทำให้การตรวจจับทำได้ยาก ผู้ดูแลระบบ Linux ควรเพิ่มความระมัดระวังและตรวจสอบความผิดปกติในระบบ PAM อย่างละเอียด เพื่อป้องกันการโจมตีที่อาจเกิดขึ้น

ข้อมูลอ้างอิง

Aug 4, 2025 By Ravie Lakshmanan

- https://thehackernews.com/2025/08/new-plague-pam-backdoor-exposes.html