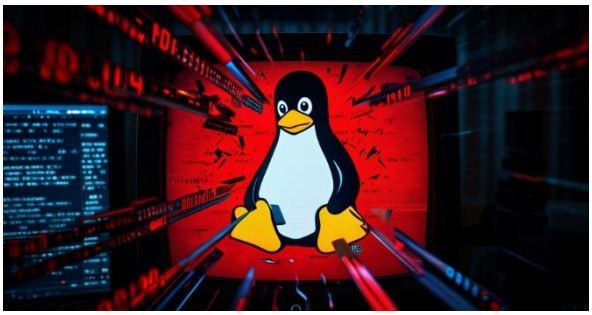
วันที่ 12 กุมภาพันธ์ 2569

SSHStalker บอตเน็ตใช้ IRC เป็น C2 เพื่อควบคุมระบบ Linux ผ่านช่องโหว่เคอร์เนลรุ่นเก่า

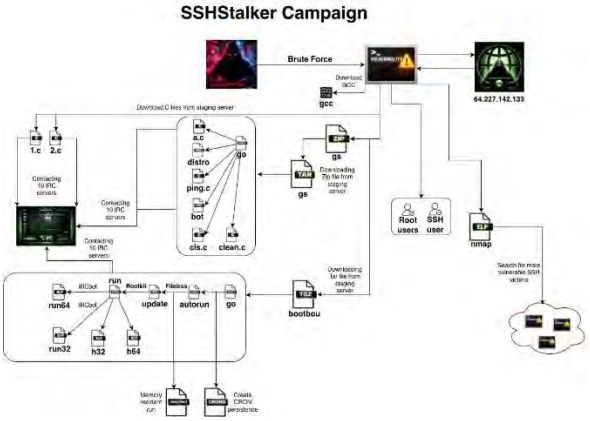


นักวิจัยด้านความปลอดภัยไซเบอร์ได้เปิดเผยรายละเอียดของปฏิบัติการบอตเน็ตตัวใหม่ชื่อว่า SSHStalker ซึ่งอาศัยโปรโตคอล Internet Relay Chat (IRC) ในการสื่อสารเพื่อสั่งการและควบคุม (C2) ชุดเครื่องมือนี้ผสมผสานเทคนิคการซ่อนตัวเข้ากับการโจมตี Linux ยุคเก่า โดยนอกจากจะมีเครื่องมือทำความสะอาด log (แก้ไขไฟล์ utmp/wtmp/lastlog) และองค์ประกอบระดับรูทคิทแล้ว ผู้โจมตียังเก็บคลังช่องโหว่ของ Linux เคอร์เนลตระกูล 2.6.x จากช่วงปี 2009–2010 ไว้จำนวนมาก บริษัทความปลอดภัยไซเบอร์ Flare ระบุว่า แม้ช่องโหว่เหล่านี้จะไม่ค่อยได้ผลกับระบบสมัยใหม่ แต่ยังคงใช้ได้กับโครงสร้างพื้นฐานที่ถูกลืมหรือระบบเก่าที่ยังใช้งานอยู่

SSHStalker ผสมกลไกบอตเน็ตแบบ IRC เข้ากับกระบวนการเจาะระบบอัตโนมัติในวงกว้าง โดยใช้ตัวสแกน SSH และเครื่องมือสแกนที่หาได้ทั่วไป เพื่อเข้าควบคุมระบบที่มีช่องโหว่และดึงเข้าสู่เครือข่าย พร้อมลงทะเบียนเข้าไปยังช่อง IRC สำหรับรับคำสั่ง อย่างไรก็ตาม ต่างจากแคมเปญอื่นๆ ที่มักใช้บอตเน็ตในลักษณะฉวยโอกาส เช่น การโจมตีแบบ DDoS การแอบใช้ทรัพยากรเป็นพร็อกซี หรือการขุดคริปโต SSHStalker กลับมุ่งเน้นการคงการเข้าถึงระบบในระยะยาว โดยไม่พบพฤติกรรมการโจมตีต่อเนื่องหลังจากเจาะระบบสำเร็จ พฤติกรรมที่ดูเหมือน “เงียบไว้ก่อน” นี้ทำให้มันแตกต่าง และอาจบ่งชี้ว่าโครงสร้างพื้นฐานที่ถูกยึดครองนั้นถูกใช้เป็นจุดพัก เตรียมการทดสอบ หรือเก็บสิทธิ์การเข้าถึงไว้ใช้ในอนาคต

องค์ประกอบหลักของ SSHStalker คือสแกนเนอร์ที่พัฒนาด้วยภาษา Golang ซึ่งทำหน้าที่สแกนพอร์ต 22 เพื่อค้นหาเซิร์ฟเวอร์ที่เปิดบริการ SSH และแพร่กระจายตัวเองในลักษณะคล้ายเวิร์ม นอกจากนี้ยังมีการปล่อยเพย์โหลดหลายรูปแบบ รวมถึงบอตที่ควบคุมผ่าน IRC และบอตไฟล์ Perl ที่เชื่อมต่อไปยังเซิร์ฟเวอร์ UnrealIRCd เข้าร่วมช่องควบคุม และรอรับคำสั่งเพื่อทำการโจมตีแบบส่งทราฟฟิกถล่มเป้าหมาย รวมถึงควบคุมบอตเครื่องอื่นๆ

การโจมตียังมีลักษณะเด่นคือมีการรันไฟล์โปรแกรมภาษา C เพื่อทำความสะอาดประวัติการเชื่อมต่อ SSH และลบร่องรอยกิจกรรมที่เป็นอันตรายออกจาก log เพื่อลดโอกาสถูกตรวจสอบย้อนหลัง นอกจากนี้ในชุดมัลแวร์ยังมีส่วนประกอบ “keep-alive” ที่จะสั่งให้โปรแกรมหลักเริ่มทำงานใหม่ภายใน 60 วินาที หากถูกเครื่องมือรักษาความปลอดภัยปิดการทำงาน



SSHStalker น่าสนใจตรงที่ผสมผสานการเจาะระบบอัตโนมัติในวงกว้างเข้ากับคลังช่องโหว่เคอร์เนล Linux ถึง 16 รายการ บางรายการย้อนกลับไปถึงปี 2009 ช่องโหว่ที่ถูกใช้ในโมดูลโจมตี เช่น CVE-2009-2692, CVE-2009-2698, CVE-2010-3849, CVE-2010-1173, CVE-2009-2267, CVE-2009-2908, CVE-2009-3547, CVE-2010-2959 และ CVE-2010-3437 จากการตรวจสอบโครงสร้างพื้นฐานที่ใช้เป็นจุดพักไฟล์ของผู้โจมตี Flare พบว่ามีคลังเครื่องมือโจมตีแบบโอเพนซอร์สและตัวอย่างมัลแวร์ที่เผยแพร่มาก่อนหน้านี้จำนวนมาก เช่น

- รูทคิทสำหรับช่วยซ่อนตัวและคงการทำงานในระบบ
- โปรแกรมขุดคริปโตเคอร์เรนซี
- สคริปต์ Python ที่รันไฟล์ไบนารีชื่อ “website grabber” เพื่อขโมยข้อมูลของ AWS จากเว็บไซต์ที่เปิดเผยข้อมูลไว้
- EnergyMech บอต IRC ที่ใช้สำหรับควบคุมและรันคำสั่งจากระยะไกล

มีการตั้งข้อสังเกตว่าผู้โจมตีอาจมีต้นกำเนิดจากโรมาเนีย เนื่องจากพบชื่อเล่น สำนวนภาษา และรูปแบบการตั้งชื่อแบบโรมาเนียภายในช่อง IRC และไฟล์กำหนดค่าต่างๆ อีกทั้งรูปแบบการปฏิบัติการยังมีความคล้ายคลึงกับกลุ่มแฮกเกอร์ที่รู้จักกันในชื่อ Outlaw (หรือ Dota)

SSHStalker ดูเหมือนจะไม่ได้มุ่งพัฒนาช่องโหว่ใหม่หรือสร้างรูทคิทแบบไม่เคยมีมาก่อน แต่แสดงให้เห็นถึงการควบคุมปฏิบัติการอย่างเป็นระบบ ผ่านการพัฒนาแกนหลักด้วยภาษา C สำหรับบอตและส่วนที่ทำงานระดับล่าง ใช้เชลล์สคริปต์สำหรับจัดการลำดับงานและความคงอยู่ในระบบ และใช้ Python กับ Perl ในวงจำกัดเพื่อช่วยงานด้านยูทิลิตี้หรือระบบอัตโนมัติในขั้นตอนการโจมตี รวมถึงการรัน IRC bot Flare กล่าว

ผู้โจมตีไม่ได้สร้างซีโร่เดย์หรือรูทคิทใหม่ ๆ แต่แสดงให้เห็นถึงวินัยในการปฏิบัติการที่แข็งแกร่ง ทั้งในด้านกระบวนการเจาะระบบจำนวนมาก การนำโครงสร้างพื้นฐานกลับมาใช้ซ้ำ และการคงการเข้าถึงระยะยาวในสภาพแวดล้อม Linux ที่หลากหลาย

ข้อมูลอ้างอิง

Feb 11, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/02/sshstalker-botnet-uses-irc-c2-to.html