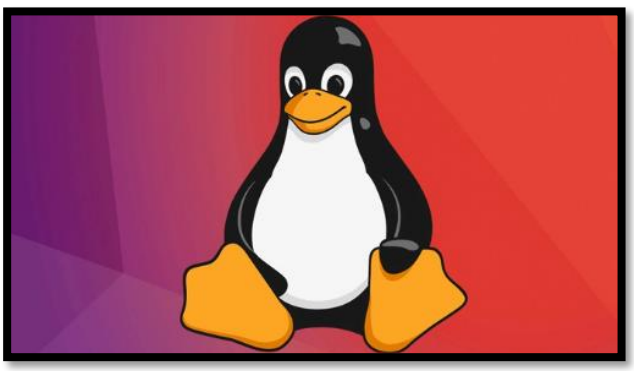
ประจำวันอังคารที่ 24 พฤษภาคม 2565

Microsoft เตือนมัลแวร์ XorDdos ที่มุ่งเป้าไปยังอุปกรณ์ Linux

มัลแวร์บ็อตเน็ต Linux ที่รู้จักกันในชื่อ XorDdos พบว่ามีกิจกรรมเพิ่มขึ้น 254% ในช่วง 6 เดือนที่ผ่านมา ซึ่งโทรจันได้รับการตั้งชื่อตามการโจมตีแบบปฏิเสธการให้บริการบนระบบ Linux และการใช้การเข้ารหัสแบบ XOR สำหรับการสื่อสารด้วย command-and-control (C2) กับเซิร์ฟเวอร์ โดยลักษณะโมดูลาร์ของ XorDdos ช่วยให้ผู้โจมตีมีโทรจันอเนกประสงค์ที่สามารถแพร่ระบาดในระบบ Linux ที่หลากหลายได้

การโจมตี SSH ด้วยวิธี brute-force ซึ่งเป็นเทคนิคที่ค่อนข้างง่ายแต่มีประสิทธิภาพในการเข้าถึง root แก่เป้าหมาย การควบคุมระยะไกลสำหรับ IoT ที่มีช่องโหว่และอุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ตอื่น ๆ นั้นมาจากการโจมตีแบบ brute-force (SSH) ทำให้การเปิดใช้มัลแวร์จะสร้างบ็อตเน็ตที่มีความสามารถในการโจมตีแบบปฏิเสธการให้บริการ (DDoS) แบบกระจาย นอกจากจะถูกคอมไพล์สำหรับสถาปัตยกรรม ARM, x86 และ x64 แล้ว มัลแวร์ยังได้รับการออกแบบมาเพื่อรองรับ Linux รุ่นต่างๆ อีกด้วย

ในช่วงไม่กี่ปีที่ผ่านมา XorDdos ได้พุ่งเป้าไปที่เซิร์ฟเวอร์ Docker ที่ไม่มีการป้องกันด้วยพอร์ตที่เปิดเผย (2375) โดยใช้ระบบที่ถูกโจมตีเพื่อควบคุมเครือข่ายเป้าหมายหรือบริการที่มีการรับส่งข้อมูลปลอมเพื่อให้ไม่สามารถเข้าถึงได้ โดย XorDdos ได้กลายเป็นภัยคุกคามอันดับต้นๆ ที่กำหนดเป้าหมายไปยัง Linux ในปี 2021 ตามมาด้วย Mirai และ Mozi ซึ่งคิดเป็นมากกว่า 22% ของมัลแวร์ IoT ทั้งหมดที่ตรวจพบ ตามบริษัทด้านความปลอดภัยทางไซเบอร์ CrowdStrike



ที่มาของข่าว: https://thehackernews.com/2022/05/microsoft-warns-rise-in-xorddos-malware.html