UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0281

MIRAI TARGETS LINUX SERVERS TO LAUNCH DDOS

DATE ISSUED: 20th February 2023

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A new Mirai botnet variant, known as V3G4, is being used by attackers to target Internet of Things (IoT) devices and Linux-based servers. Mirai is a software that is used to create a malicious botnet – a large number of connected devices (bots) that can be controlled to attack others on the Internet without owner's consent.

BREAKDOWN

Researchers from Palo Alto Networks' Unit 42 have spotted a new variant of the infamous Mirai botnet, spreading to Linux-based servers and IoT devices in order to create an enormous swarm of Dedicated Denial of Service (DDoS) attacks. The attack begins by leveraging 13 known vulnerabilities in Linux Servers which are known for leading to Remote Code Execution(RCE). Some of the notable flaws relate to critical flaws in Atlassian Confluence Server and Data Center, DrayTek Vigor routers, and Geutebruck IP cameras, among others. The oldest flaw in the list is CVE-2012-4869, an RCE bug in FreePBX. Once the malware is deployed it take extra steps to terminate other competing botnets such as Mozi, Okami, and Yakuza. V3G4 spreads itself by brute-forcing weak/default credentials through Telnet/SSH. It continuously scans for other devices that may be vulnerable, attempting to login with a list of known credentials. It also establishes contact with a Command-and-Control (C2) server to await commands for launching DDoS attacks against targets via UDP, TCP, and HTTP protocols.

REMEDIATION STEPS

- Update and patch systems to the latest version.
- Secure the devices with strong, unique passwords.
- Check out Importance of strong passwords and practices — Unisphere Solutions Ltd for more information on best practice and policy or password creation.

REFERENCES & RESOURCES

The Bleeping Computer https://www.bleepingcomputer.com/news/security/new-mirai-malware-variant-infects-linux-devices-to-build-ddos-botnet/

Reseller News https://www.reseller.co.nz/article/705694/new-mirai-botnet-variant-v3g4-targets-linux-servers-iot-devices/