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

CYBER GUIDANCE ISSUE 0296

SHELLBOT VARIANTS TARGET LINUX SERVERS

DATE ISSUED: 27th March 2023

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

ASEC researchers have discovered ShellBot malware variants designed to take control of Linux-based servers and IoT devices. It could allow attackers to execute arbitrary commands, steal data, and launch distributed denial-of-service (DDoS) attacks.

BREAKDOWN

New variants of ShellBot malware are actively exploiting vulnerabilities in unpatched Linux servers. In the recent campaign, threat actors used a scanner or brute-forcer malware to discover systems with SSH port 22 open and initiate a dictionary attack against a list of commonly used SSH account credentials. The first two variants - LiGhT's Modded perlbot v2 and DDoS PBot v2.0, offer a variety of DDoS attack commands using HTTP, TCP, SQL, and UDP protocols. The third variant - PowerBots (C) GohacK, has an additional feature to install a backdoor in the server that could be leveraged to launch different attacks. These variants can implement sophisticated obfuscation techniques to evade detection by antivirus software.

REMEDIATION STEPS

- Install anti-malware software: To protect endpoints from malware, regularly update the agent to detect and block the latest threat.
- Keep software up to date: Keep operating systems, software applications, and plug-ins updated with the latest security patches.
- Use strong passwords: Implement robust password policies and two-factor authentication to prevent unauthorised access to servers and devices.
- Monitor network traffic: Use network traffic monitoring tools to identify unusual traffic and behaviour patterns that may indicate malware activity.

REFERENCES & RESOURCES

The Hacker News https://thehackernews.com/2023/03/new-shellbot-ddos-malware-targeting.html