KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Unique “ShellBot” DDoS Malware Targeting Linux SSH Servers

Tracker ID: TN2349 **Date:** March 24, 2023 **Category:** Campaign **Industry:** All **Region**: All

Background

In recent campaigns, Linux SSH servers with poor management are becoming the targets of the new variant of "ShellBot" malware. ShellBot is a well-known malware family that has been around for a long time and is still used to perform attacks against Linux systems. The primary targets are the poorly managed or vulnerable services that are prone to exploits as they have not been patched to the most secure version. The Perl-based ShellBot, often known as PerlBot, is a "DDoS" bot malware that typically communicates with the C&C server using the IRC protocol. Attackers are aggressively distributing bitcoin miners to Linux hosts using the ShellBot script compiler.

Poorly managed services with default account credentials leaves the server open to dictionary attacks and add an easy attack vector for infiltration. Secure Shell (SSH) services are often the focus of the assaults on Linux servers. A list of known SSH credentials is used to initiate a dictionary attack to breach the server and deploy the payload, after which it leverages the Internet Relay Chat (IRC) protocol to communicate with a remote server. Moreover, the Telnet service is found to be vulnerable to dictionary attacks in IoT setups with deployed outdated Linux servers or embedded Linux OSes. The attackers are also observed targeting prominent services including MS-SQL and Remote Desktop Protocol (RDP) in Windows operating systems.

Threat actors employ scanners and SSH BruteForce malware to attack systems that have SSH port 22 open. A dictionary attack is initiated using a list of known SSH credentials to compromise the server and release the payload and it then connects to a remote server using the Internet Relay Chat (IRC) protocol. Once compromised, ShellBot is deployed on servers with weak or default passwords. The malware could execute instructions and perform DDoS attacks while also exposing the stolen data.

LiGhT's Modded PerlBot v2, DDoS PBot v2.0, and PowerBots (C) GohacK are the three identified unique ShellBot versions, the first two of which provide a variety of DDoS attack commands using HTTP, TCP, and UDP protocols whereas PowerBots has more backdoor-like features that allow it to grant reverse shell access and upload any file from the compromised server. ShellBot was used in attacks on Linux servers in which bitcoin miners were disseminated via a shell script compiler.

Linux systems that have been compromised with ShellBot malware could be used as DDoS Bots to launch DDoS assaults against specific targets in response to commands from threat actors. Additionally, the threat actor could employ several additional backdoor features to add new malware or launch various assaults from the hacked servers. Therefore, administrators are advised to implement complex passwords for the accounts and change them periodically to protect the Linux server from brute force attacks and dictionary attacks and update to the latest patch to prevent vulnerability attacks.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Unique “ShellBot” DDoS Malware Targeting Linux SSH Servers

Tracker ID: TN2349 **Date:** March 24, 2023 **Category:** Campaign **Industry:** All **Region**: All

MITRE ATT&CK Tactics

Initial Access, Execution, Command and Control and Exfiltration.

Indicators of Compromise *

Please refer to the attached sheet for IOCs.

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- To safeguard the Linux server, administrators are advised to disable the default passwords and use a complex passwords for their accounts.
- Implement a password rotation policy and multi-factor authentication to access critical systems.
- Apply the most recent patch for software to shield against vulnerability attacks.
- Use security programs such as firewalls for publicly accessible servers to restrict access by attackers.
- In order to prevent malware or TAs from stealing data, keep an eye on the beacon at the network level.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

References

- Sanseo, ShellBot Malware Being Distributed to Linux SSH Servers, AhnLabs, March 17, 2023, External Link (asec.ahnlab.com).
- Ravie Lakshmanan, New ShellBot DDoS Malware Variants Targeting Poorly Managed Linux Servers, Hacker News, March 21, 2023, External Link (thehackernews.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI

KPMG in India Cyber Response Hotline : +91 9176471471

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Unique “ShellBot” DDoS Malware Targeting Linux SSH Servers

Tracker ID: TN2349 **Date:** March 24, 2023 **Category:** Campaign **Industry:** All **Region**: All

*

MD5	IP	Domain/URL
bef1a9a49e201095da0bb26642f65a78	164.90.240[.]68:6667	x-x-x[.]online/ak
3eef28005943fee77f48ac6ba633740d	206.189.139[.]152:6667	193.233.202[.]219/mperl
55e5bfa75d72e9b579e59c00eaeb6922	176.123.2[.]3:6667	193.233.202[.]219/niko1
6d2c754760ccd6e078de931f472c0f72	164.132.224[.]207:80	hxxp://34.225.57[.]146/futai/perl
7ca3f23f54e8c027a7e8b517995ae433	51.195.42[.]59:8080	80.94.92[.]241/bash
2cf90bf5b61d605c116ce4715551b7a3	192.3.141[.]163:6667	hxxp://185.161.208[.]234/test.jpg
7bc4c22b0f34ef28b69d83a23a6c88c5	49.212.234[.]206:3303	hxxp://39.165.53[.]17:8088/iposzz/dred
176ebfc431daa903ef83e69934759212		hxxp://80.68.196[.]6/ff
		gsm.ftp[.]sh:1080

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

home.kpmg/in

Follow us on home.kpmg/in/socialmedia