KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | RapperBot Brute forces into Linux SSH servers

Tracker ID: TN0810 **Date:** 09/Aug/2022 **Category:** Malware **Industry:** All **Region**: All

Background

A new botnet known as "RapperBot" has been discovered in the wild, with assaults focused on brute-forcing Linux SSH servers to get system access. It deviates from the original MiraiBot's way of propagating to the devices. It has limited DDoS capabilities, appears to be concentrated on initial server access, and is likely to be utilized as a stepping stone for lateral network movement. The new botnet had scanned and attempted to brute-force on Linux SSH servers using over 3,500 unique IP addresses from around the world, over the past 1.5 months.

RapperBot has its own command and control (C2) protocol and unique post-compromise activities (for a botnet). Unlike the majority of Mirai variants, which natively brute force Telnet servers using default or weak passwords, RapperBot exclusively scans and attempts to brute force SSH servers configured to accept password authentication.

The bulk of the malware code comprises an SSH 2.0 client, which allows it to connect to and brute force any SSH server that supports Diffie-Hellmann key exchange with 768-bit or 2048-bit keys and AES128-CTR data encryption. It uses host-specific TCP requests to download a list of credentials for the SSH brute-force attack and reports success to the C2. Later versions of the malware disguised SSH-related strings further by employing techniques such as XOR encoding.

RapperBot uses a self-propagation technique using a remote binary downloader post-compromise. One of the contemporary variations in use exchanges the victim's SSH keys for the actor's using a shell command, ensuring persistence even after SSH password changes. It also included a mechanism to add the threat actor's SSH key to the host's "~/.ssh/authorized keys," which aids in maintaining access to the server even if the malware is discovered and removed. In the most recent sample, the root user "suhelper" is added by the bot on the compromised endpoints. The bot also sets up a Cron job to add the user again every hour in case an administrator finds the account and deletes it.

Despite sharing a lot of code with Mirai and its descendants, this threat varies in some areas. The removal of self-propagation techniques, as well as the installation of persistence and detection-avoidance methods, suggests that the botnet's operators are interested in selling early access to ransomware perpetrators. RapperBot has undergone several significant and unusual changes, obscuring its primary motivation. As its primary mode of propagation is brute-force SSH credentials, this threat can be avoided by using complex passwords for devices or removing SSH password authentication (where possible).

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

JAESON SCHULTZ AT 8:00 AM

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | RapperBot Brute forces into Linux SSH servers

Tracker ID: TN0810 **Date:** 09/Aug/2022 **Category:** Malware **Industry:** All **Region**: All

MITRE ATT&CK Tactics

Initial Access, Persistence, Lateral Movement, Defense Evasion, and Command and Control.

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.
- Validate the IOCs attached and implement the detection & prevention accordingly.
- Set strong passwords for devices or remove password authentication for SSH wherever possible.
- Perform regular data backup procedures and maintain up-to-date incident response and recovery procedures.
- Implement network segmentation to limit or block lateral movement. Follow multilayered defense solutions and active monitoring to detect and thwart threats.
- Monitor the beacon on the network level to prevent data exfiltration by malware or threat actors.
- Use endpoint detection and response systems that can detect and remediate suspicious activity automatically.

References

- Joie Salvio and Roy Tay , So RapperBot, What Ya Bruting For?, 03rd July 2022, Fortinet, External Link (fortinet.com)
- Bill Toulas, New Linux malware brute-forces SSH servers to breach networks, 04th August 2022, Bleeping Computer, External Link (bleepingcomputer.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 9176 471 471

JAESON SCHULTZ AT 8:00 AM

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | RapperBot Brute forces into Linux SSH servers

Tracker ID: TN0810 **Date:** 09/Aug/2022 **Category:** Malware **Industry:** All **Region**: All

*

SHA256 HASH	URL	IP
92ae77e9dd22e7680123bb230ce43ef602998e6a1c6756d9e2ce5822a09b37b4	hxxp://31[.]44[.]185[.]235/x86	31[.]44[.]185[.]235
a31f4caa0be9e588056c92fd69c8ac970ebc7e85a68615b1d9407a954d4df45d	hxxp://31[.]44[.]185[.]235/mips	2[.]58[.]149[.]116
e8d06ac196c7852ff71c150b2081150be9996ff670550717127db8ab855175a8	hxxp://31[.]44[.]185[.]235/arm7	194[.]31[.]98[.]244
23a415d0ec6d3131f1d537836d3c0449097e98167b18fbdbf2efca789748818a	hxxp://2[.]58[.]149[.]116/arm	185[.]225[.]73[.]196
c83f318339e9c4072010b625d876558d14eaa0028339db9edf12bbcafe6828bb	hxxp://2[.]58[.]149[.]116/spc	
05c78eaf32af9647f178dff981e6e4e43b1579d95ccd4f1c2f1436dbfa0727ad	hxxp://2[.]58[.]149[.]116/mips	
88bbb772b8731296822646735aacbfb53014fbb7f90227b44523d7577e0a7ce6	hxxp://2[.]58[.]149[.]116/x86_64	
e8f1e8ec6b94ea54488d5f714e71e51d58dcdfe4be3827c55970d6f3b06edf73	hxxp://2[.]58[.]149[.]116/ssh/arm7	
23256f231f3d91b0136b44d649b924552607a29b43a195024dbe6cde5b4a28ad	hxxp://2[.]58[.]149[.]116/ssh/mips	
77b2e5fb5b72493bde35a6b29a66e6250b6a5a0c9b9c5653957f64a12c793cd5	hxxp://2[.]58[.]149[.]116/ssh/x86	
dcdeedee4736ec528d1a30a585ec4a1a4f3462d6d25b71f6c1a4fef7f641e7ae	hxxp://2[.]58[.]149[.]116/ssh/spc	
ebb860512a55c1cdc8be1399eec44c4481aedb418f15dbda4612e6d38e9b9010	hxxp://194[.]31[.]98[.]244/ssh/new/spc	
9d234e975e4df539a217d1c4386822be1f56cea35f7dd2aa606ae4995894da42	hxxp://194[.]31[.]98[.]244/ssh/new/x86	
1975851c916587e057fa5862884cbac3fa1e80881ddd062392486f5390c86865	hxxp://194[.]31[.]98[.]244/ssh/new/mips	
8380321c1bd250424a0a167e0f319511611f73b53736895a8d3a2ad58ffcd5d5	hxxp://194[.]31[.]98[.]244/ssh/new/arm7	
f5ff9d1261af176d7ff1ef91aa8c892c70b40caa02c17a25de22539e9d0cdd26	hxxp://194[.]31[.]98[.]244/ssh/new/arm	
2298071b6ba7baa5393be064876efcdbd9217c212e0c764ba62a6f0ffc83cc5a	hxxp://194[.]31[.]98[.]244/ssh/new/x86	
2479932a6690f070fa344e5222e3fbb6ad9c880294d5b822d7a3ec27f1b8b8d5	hxxp://194[.]31[.]98[.]244/ssh/new/mips	
1d5e6624a2ce55616ef078a72f25c9d71a3dbc0175522c0d8e07233115824f96	hxxp://194[.]31[.]98[.]244/ssh/new/arm7	
746106403a98aea357b80f17910b641db9c4fedbb3968e75d836e8b1d5712a62	hxxp://194[.]31[.]98[.]244/ssh/new/arm	
ddf5aff0485f395c7e6c3de868b15212129962b4b9c8040bef6679ad880e3f31	hxxp://185[.]225[.]73[.]196/ssh/new/arm	
e56edaa1e06403757e6e2362383d41db4e4453aafda144bb36080a1f1b899a02	hxxp://185[.]225[.]73[.]196/ssh/new/arm7	
55ff25b090dc1b380d8ca152428ba28ec14e9ef13a48b3fd162e965244b0d39b	hxxp://185[.]225[.]73[.]196/ssh/new/mips	
8e9f87bb25ff83e4ad970366bba47afb838028f7028ea3a7c73c4d08906ec102	hxxp//185[.]225[.]73[.]196/ssh/new/x86	
d86d158778a90f6633b41a10e169b25e3cb1eb35b369a9168ec64b2d8b3cbeec		
ff09cf7dfd1dc1466815d4df098065510eec504099ebb02b830309067031fe04		