Linux Malware RapperBot Brute Forcing SSH Servers

Published: 2022-08-08 · Archived: 2026-04-05 14:51:38 UTC

RapperBot is an IoT botnet malware that has spread through brute force since it was first identified in June 2022. Over 3,500 unique IPs were utilized by the RapperBot to **brute force** into a rising number of hacked SSH servers.

“RapperBot has switched from self-propagation to maintaining **remote access** into the brute-forced SSH servers,” researchers say.

RapperBot works as a DDoS tool for SSH. The attacks leverage a credentials list obtained from a remote server to perform brute force on targets. After a successful **SSH server hack**, the malware exfiltrates the newly acquired valid credentials to the C2.

Attack Details

A unique file named **/.ssh/authorized_keys** is used to get access by inserting the operators’ SSH public key. This enables the attacker to log in and authenticate to the server using the associated private key without providing a password. As a result, threat actors can access hacked SSH servers even after changing their SSH credentials or disabling SSH password authentication.

In addition, since the file is changed, all currently allowed keys are removed, preventing **authorized users** from connecting to the SSH server using public key authentication.

RapperBot’s attack scenario (Source: Fortinet)

A Possible Mirai Malware Variant

Despite having many similarities to the original **Mirai source code**, RapperBot differs from other IoT malware families in that it can brute force credentials and connect to SSH servers rather than Telnet, which was how Mirai implemented their attacks.

Also, RapperBot’s developers have begun adding code to preserve persistence. This gives threat actors access to **compromised devices** via SSH after the device reboots, or the malware is deleted.

The motive behind RapperBot’s botnet creation attacks is still unclear since there’s no evidence of post-compromise activity. SSH servers with default or weak passwords are being targeted; thus, using strong passwords is advised, and **password authentication** for SSH should be disabled if possible.

RapperBot IoCs

Files:

92ae77e9dd22e7680123bb230ce43ef602998e6a1c6756d9e2ce5822a09b37b4
a31f4caa0be9e588056c92fd69c8ac970ebc7e85a68615b1d9407a954d4df45d
e8d06ac196c7852ff71c150b2081150be9996ff670550717127db8ab855175a8
23a415d0ec6d3131f1d537836d3c0449097e98167b18fbdbf2efca789748818a
c83f318339e9c4072010b625d876558d14eaa0028339db9edf12bbcafe6828bb
05c78eaf32af9647f178dff981e6e4e43b1579d95ccd4f1c2f1436dbfa0727ad
88bbb772b8731296822646735aacbfb53014fbb7f90227b44523d7577e0a7ce6
e8f1e8ec6b94ea54488d5f714e71e51d58dcdfe4be3827c55970d6f3b06edf73
23256f231f3d91b0136b44d649b924552607a29b43a195024dbe6cde5b4a28ad
77b2e5fb5b72493bde35a6b29a66e6250b6a5a0c9b9c5653957f64a12c793cd5
dcdeedee4736ec528d1a30a585ec4a1a4f3462d6d25b71f6c1a4fef7f641e7ae
ebb860512a55c1cdc8be1399eec44c4481aedb418f15dbda4612e6d38e9b9010
9d234e975e4df539a217d1c4386822be1f56cea35f7dd2aa606ae4995894da42
1975851c916587e057fa5862884cbac3fa1e80881ddd062392486f5390c86865
8380321c1bd250424a0a167e0f319511611f73b53736895a8d3a2ad58ffcd5d5
f5ff9d1261af176d7ff1ef91aa8c892c70b40caa02c17a25de22539e9d0cdd26
2298071b6ba7baa5393be064876efcdbd9217c212e0c764ba62a6f0ffc83cc5a

2479932a6690f070fa344e5222e3fbb6ad9c880294d5b822d7a3ec27f1b8b8d5
1d5e6624a2ce55616ef078a72f25c9d71a3dbc0175522c0d8e07233115824f96
746106403a98aea357b80f17910b641db9c4fedbb3968e75d836e8b1d5712a62
ddf5aff0485f395c7e6c3de868b15212129962b4b9c8040bef6679ad880e3f31
e56edaa1e06403757e6e2362383d41db4e4453aafda144bb36080a1f1b899a02
55ff25b090dc1b380d8ca152428ba28ec14e9ef13a48b3fd162e965244b0d39b
8e9f87bb25ff83e4ad970366bba47afb838028f7028ea3a7c73c4d08906ec102
d86d158778a90f6633b41a10e169b25e3cb1eb35b369a9168ec64b2d8b3cbeec
ff09cf7dfd1dc1466815d4df098065510eec504099ebb02b830309067031fe04

Download URLs:

hxxp://31[.]44[.]185[.]235/x86
hxxp://31[.]44[.]185[.]235/mips
hxxp://31[.]44[.]185[.]235/arm7
hxxp://2[.]58[.]149[.]116/arm
hxxp://2[.]58[.]149[.]116/spc
hxxp://2[.]58[.]149[.]116/mips
hxxp://2[.]58[.]149[.]116/x86_64
hxxp://2[.]58[.]149[.]116/ssh/arm7
hxxp://2[.]58[.]149[.]116/ssh/mips
hxxp://2[.]58[.]149[.]116/ssh/x86
hxxp://2[.]58[.]149[.]116/ssh/spc
hxxp://194[.]31[.]98[.]244/ssh/new/spc
hxxp://194[.]31[.]98[.]244/ssh/new/x86
hxxp://194[.]31[.]98[.]244/ssh/new/mips
hxxp://194[.]31[.]98[.]244/ssh/new/arm7
hxxp://194[.]31[.]98[.]244/ssh/new/arm
hxxp://194[.]31[.]98[.]244/ssh/new/x86
hxxp://194[.]31[.]98[.]244/ssh/new/mips
hxxp://194[.]31[.]98[.]244/ssh/new/arm7
hxxp://194[.]31[.]98[.]244/ssh/new/arm
hxxp://185[.]225[.]73[.]196/ssh/new/arm
hxxp://185[.]225[.]73[.]196/ssh/new/arm7
hxxp://185[.]225[.]73[.]196/ssh/new/mips
hxxp//185[.]225[.]73[.]196/ssh/new/x86

C2 Servers:

31[.]44[.]185[.]235
2[.]58[.]149[.]116
194[.]31[.]98[.]244
185[.]225[.]73[.]196

Threat Actor SSH Public Key:

AAAAB3NzaC1yc2EAAAADAQABAAACAQC/yU0iqklqw6etPlUon4mZzxslFWq8G8sRyluQMD3i8tpQWT2cX/mwGgSRCz7HMLyxt87olYIPemTI
GGm1KpWg8lrXeMW+5jIXTFmEFhbJ18wc25Dcds4QCM0DvZGr/Pg4+kqJ0gLyqYmB2fdNzBcU05QhhWW6tSuYcXcyAz8Cp73JmN6TcPuVqHeFY
NBa5W2LyZ4b1v6324IEJuxImARIxTc96Igaf30LUza8kbZyc3bewY6IsFUN1PjQJcJi0ubVLyWyyJ554Tv8BBfPdY4jqCr4PzaJ2Rc1JFJYUSVVT4yX2p
giIlb+0EHtFWc2QH7yz/ZBjnun7opIoslLVvYJ9cxMoLeLr5Ig+zny+IEA3x090xtcL62X0jea6btVnYo7UN2BARziisZze6oVuOTCBijuyvOM6ROZ6s/wl4
BAodNaUPFfTxggH3tZrnnU8Dge5/1JNa08F3WNUPM1S1x8L2HMatwc82x35jXyBSp3AMbdxMPhvyYI8v2J1PqJH8OqGTVjdWe40mD2osRgLo1EC

Threat Actor Root User:

/etc /passwd suhelper:x:0:0::/:

/etc /shadow suhelper:$1$1OJBlhUV$E9DMK0xdoZb8W8wVOibPQ/:19185:0:99999:7:::

Source: https://socradar.io/linux-malware-rapperbot-brute-forcing-ssh-servers/