

重庆 4 号机器被植入挖矿木马记录_2020-03-22

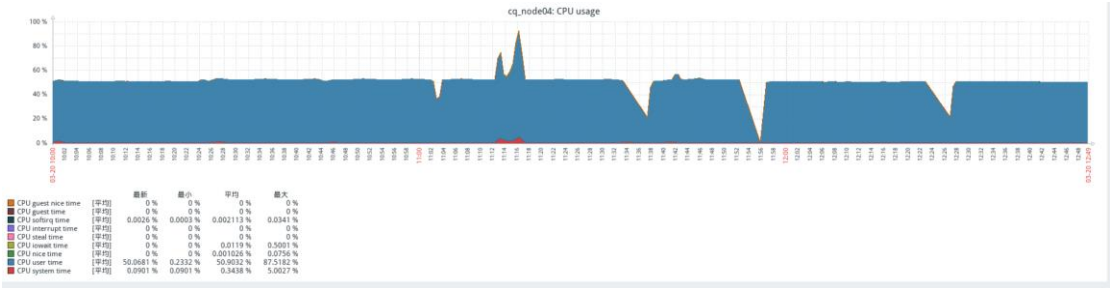
概述：

本文主要介绍服务器被植入挖矿木马的现象以及排查步骤。

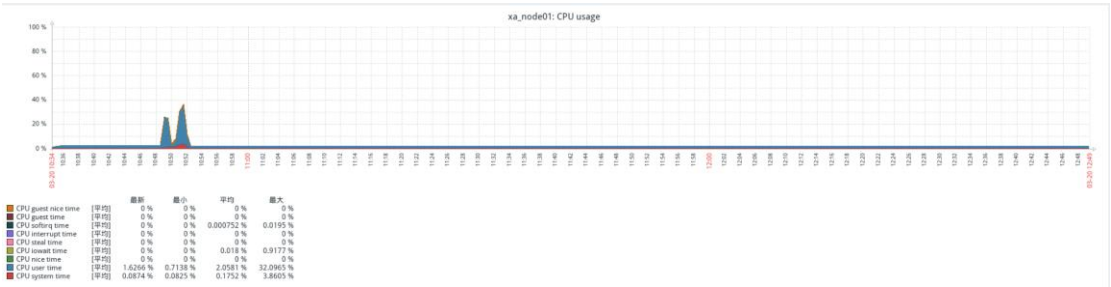
详细信息：

1、发现过程

在巡检系统监控时候发现重庆 4 号服务器 cpu 使用情况不正常，cpu 的使用率出现持续性的使用记录。如图



当时多台服务器正在进行 bench 性能测试，而其他的服务器在跑 bench 测试过程中并没有出现该情况。如图



所以便通过 ssh 登陆重庆 04 号机器检查。

使用 htop 和 top 查看运行的进程。htop 显示 CPU 使用达到了 50%，但是没有发现高占用的进程，如图：

```
1 [|||||100.0%] 17 [|||||100.0%] 33 [|||||0.0%] 49 [|||||0.0%]
2 [|||||100.0%] 18 [|||||100.0%] 34 [|||||0.0%] 50 [|||||0.0%]
3 [|||||100.0%] 19 [|||||100.0%] 35 [|||||0.0%] 51 [|||||0.0%]
4 [|||||100.0%] 20 [|||||100.0%] 36 [|||||0.0%] 52 [|||||0.0%]
5 [|||||100.0%] 21 [|||||100.0%] 37 [|||||0.0%] 53 [|||||0.0%]
6 [|||||100.0%] 22 [|||||100.0%] 38 [|||||0.0%] 54 [|||||0.0%]
7 [|||||100.0%] 23 [|||||100.0%] 39 [|||||0.0%] 55 [|||||0.0%]
8 [|||||100.0%] 24 [|||||100.0%] 40 [|||||0.0%] 56 [|||||0.0%]
9 [|||||100.0%] 25 [|||||100.0%] 41 [|||||0.0%] 57 [|||||0.0%]
10 [|||||100.0%] 26 [|||||100.0%] 42 [|||||0.0%] 58 [|||||0.0%]
11 [|||||100.0%] 27 [|||||100.0%] 43 [|||||0.0%] 59 [|||||0.0%]
12 [|||||100.0%] 28 [|||||100.0%] 44 [|||||0.0%] 60 [|||||0.0%]
13 [|||||100.0%] 29 [|||||100.0%] 45 [|||||0.0%] 61 [|||||0.0%]
14 [|||||100.0%] 30 [|||||100.0%] 46 [|||||0.0%] 62 [|||||0.0%]
15 [|||||100.0%] 31 [|||||100.0%] 47 [|||||0.0%] 63 [|||||6.8%]
16 [|||||100.0%] 32 [|||||100.0%] 48 [|||||0.0%] 64 [|||||0.0%]

Mem[|||||5.36G/32G] Tasks: 48, 26 thr: 1 running
Sup[|||||0K/2.00G] Load average: 32.17 31.01 21.07
Uptime: 00:17:29

PID USER PRI NI VIRT RES SHR CPU% MEM% TIME+ Command
2249 root 20 0 571M 19844 15848 0.0 0.0 0:00.01 /usr/sbin/NetworkManager --no-daemon
2261 root 20 0 571M 19844 15848 0.0 0.0 0:00.06 /usr/sbin/NetworkManager --no-daemon
2217 root 20 0 571M 19844 15848 0.0 0.0 0:01.45 /usr/sbin/NetworkManager --no-daemon
2352 root 20 0 191M 19808 11908 0.0 0.0 0:00.00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrad
2329 root 20 0 191M 19808 11908 0.0 0.0 0:00.07 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrad
1850 root RT 0 580M 19196 7872 0.0 0.0 0:00.00 /sbin/multipathd -d -s
1851 root RT 0 580M 19196 7872 0.0 0.0 0:00.00 /sbin/multipathd -d -s
1852 root RT 0 580M 19196 7872 0.0 0.0 0:00.15 /sbin/multipathd -d -s
1853 root RT 0 580M 19196 7872 0.0 0.0 0:00.16 /sbin/multipathd -d -s
1854 root RT 0 580M 19196 7872 0.0 0.0 0:00.00 /sbin/multipathd -d -s
1855 root RT 0 580M 19196 7872 0.0 0.0 0:00.00 /sbin/multipathd -d -s
1945 root RT 0 580M 19196 7872 0.0 0.0 0:00.00 /sbin/multipathd -d -s
1947 root RT 0 580M 19196 7872 0.0 0.0 0:00.00 /sbin/multipathd -d -s
1949 root RT 0 580M 19196 7872 0.0 0.0 0:00.00 /sbin/multipathd -d -s
1849 root RT 0 580M 19196 7872 0.0 0.0 0:00.46 /sbin/multipathd -d -s
2327 root 20 0 175M 17400 9464 0.0 0.0 0:00.00 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-trigg
2221 root 20 0 175M 17400 9464 0.0 0.0 0:00.10 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-trigg
4498 root 20 0 375M 14524 12716 0.0 0.0 0:00.00 /usr/lib/packagekit/packagekitd
4499 root 20 0 375M 14524 12716 0.0 0.0 0:00.01 /usr/lib/packagekit/packagekitd
4497 root 20 0 375M 14524 12716 0.0 0.0 0:00.06 /usr/lib/packagekit/packagekitd
2298 root 0 -20 33216 14228 4536 0.0 0.0 0:00.39 /usr/bin/atop -R -u /var/log/atop/atop_20200320 600
2802 uhoopsie 20 0 305M 12936 11236 0.0 0.0 0:00.00 /usr/bin/uhoopsie -f
2803 uhoopsie 20 0 305M 12936 11236 0.0 0.0 0:00.01 /usr/bin/uhoopsie -f
2789 uhoopsie 20 0 305M 12936 11236 0.0 0.0 0:00.10 /usr/bin/uhoopsie -f
951 root 19 -1 80588 11840 11008 0.0 0.0 0:00.70 /lib/systemd/systemd-journald
F1[help] F2[Setup] F3[Search] F4[Filter] F5[Free] F6[Sort] F7[Trace] F8[Nice] F9[Xkill] F10[Quit]
```

2.2 通过 netstat 查看端口监听情况，也可以看到异常的连接，如图：

```
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 0.0.0.0:53 0.0.0.0:* LISTEN 2088/systemd-resolu
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 2897/sshd
tcp 0 0 172.16.20.104:7778 0.0.0.0:* LISTEN -
tcp 0 0 172.16.20.104:42861 172.16.20.111:7777 ESTABLISHED -
tcp 0 0 172.17.63.81:22 194.109.11.146:30572 SYN_RECV -
tcp 0 0 172.17.63.81:22 10.10.8.3:55772 ESTABLISHED 3017/sshd: root@pts
tcp 0 0 172.17.63.81:22 194.109.11.146:13558 SYN_RECV -
tcp 0 0 172.17.63.81:22 194.109.11.146:6270 SYN_RECV -
tcp 0 0 172.17.63.81:22 194.109.11.146:18971 SYN_RECV -
tcp 0 0 172.17.63.78:59438 47.106.187.104:80 ESTABLISHED -
tcp 0 0 172.17.63.81:22 194.109.11.146:56477 SYN_RECV -
tcp 0 0 172.17.63.81:22 194.109.11.146:59619 SYN_RECV -
tcp 0 0 172.17.63.81:22 159.65.84.164:44408 TIME_WAIT -
tcp 0 0 172.17.63.81:22 10.10.8.4:53050 ESTABLISHED 10340/sshd: root@pt
tcp6 0 0 :::22 :::* LISTEN 2897/sshd
udp 0 0 0.0.0.0:50769 0.0.0.0:* 2201/avahi-daemon:
udp 0 0 127.0.0.53:53 0.0.0.0:* 2088/systemd-resolu
udp 0 0 0.0.0.0:68 0.0.0.0:* 2591/dhclient
udp 0 0 0.0.0.0:68 0.0.0.0:* 2440/dhclient
udp 0 0 0.0.0.0:5353 0.0.0.0:* 2201/avahi-daemon:
udp6 0 0 :::52784 :::* 2201/avahi-daemon:
udp6 0 0 :::5353 :::* 2201/avahi-daemon:
```

使用 ps、top 等命令无法查询到病毒进程，推测病毒可能修改 ps 或 top 指令，把进程隐藏了。所以这里使用 busybox 代替系统命令（系统命令已不可信，操作优先采用 busybox）例如 busybox top,如图：

```
top - 16:48:29 up 22 min, 1 user, load average: 32.10, 31.67, 23.99
Tasks: 701 total, 1 running, 368 sleeping, 0 stopped, 0 zombie
%Cpu(s): 50.0 us, 0.0 sy, 0.0 ni, 50.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 39468659+total, 38731958+free, 5759236 used, 1607776 buff/cache
KiB Swap: 2097148 total, 2097148 free, 0 used. 38646812+avail Mem

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
4508 root 20 0 7147036 7584 1272 S 3205 0.0 544:43.72 kthreadds
6074 root 20 0 41032 4252 2900 R 1.3 0.0 0:00.05 top
2359 root 20 0 4484500 23644 13920 S 0.7 0.0 0:02.42 snapd
2319 zabbix 20 0 123204 8316 7124 S 0.3 0.0 0:00.66 zabbix_agentd
3029 root 20 0 133740 10400 6348 S 0.3 0.0 0:01.07 libgc++.so
1 root 20 0 228128 9740 6656 S 0.0 0.0 0:03.37 systemd
2 root 20 0 0 0 0 S 0.0 0.0 0:00.01 kthreadd
3 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_gp
4 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 rcu_par_gp
6 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 kworker/0:0H-kb
7 root 20 0 0 0 0 I 0.0 0.0 0:00.07 kworker/0:1-eve
8 root 20 0 0 0 0 I 0.0 0.0 0:00.30 kworker/u128:0-
10 root 0 -20 0 0 0 I 0.0 0.0 0:00.00 mm_percpu_wq
11 root 20 0 0 0 0 S 0.0 0.0 0:00.01 ksoftirqd/0
12 root 20 0 0 0 0 I 0.0 0.0 0:00.85 rcu_sched
13 root rt 0 0 0 0 S 0.0 0.0 0:00.01 migration/0
14 root -51 0 0 0 0 S 0.0 0.0 0:00.00 idle_inject/0
15 root 20 0 0 0 0 S 0.0 0.0 0:00.00 cpuhp/0
16 root 20 0 0 0 0 S 0.0 0.0 0:00.00 cpuhp/1
```

果然找到了这个程序。

1、解决过程

首先 kill 上面这个占 CPU 高的 kthreadds 进程，但是该进程被 kill 后，会自动重新启动。挖矿程序一般都设置了定时任务启动脚本程序，查看定时任务，`crontab -l` 查看是找不到的。得看 `/etc/crontab` 文件。果然有任务在启动程序，如图：

```
/root/.rustup/toolchains/stable-x86_64-unknown-linux-gnu/share/doc/rust/html/embedded-book/assets/f3.jpg
root@node04:~# cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
root@node04:~#
```

删除掉定时任务。

并且需要 `cd /etc/cron.*` 相关的目录，查看是否也有对应的定时任务。如图，这里查询到一个在 `init.d` 目录下的启动脚本脚本的参数。

```
threads=`cat /proc/cpuinfo|grep "processor"|wc -l`
launch="/etc/init.d/pdflushs"
xmrig="/usr/bin/kthreadds"
config="/usr/bin/config.json"
busybox="/lib64/busybox"
sha512Busybox="89dafd4be9d51135ec8ad78a9ac24c29f47673a9fb3920dac9df81c7b6b850ad8e7219a0ded755c2b106a736804c9de3174302a2fba613"
chattr="/lib64/libg++.so"
preload="/etc/ld.so.preload"
processhider="/lib64/libstdc++.so"
backdoor="/lib64/gc++"
cron="/lib64/libgc++.so"
```

根据上面参数的绝对路径，删除病毒相关执行文件和启动脚本。

结果显示文件是被加了锁的，使用 `root` 用户去 `rm`、`mv`、`chmo/chown` 改权限，或者清空文件，任何操作都会报 `Permission denied`（没权限）。

因此需要确认文件是否枷锁，`lsattr` 命令查看。再用 `chattr` 命令撤销权限。即可完成删除。

再 **top** 观察 CPU，确认不再无故飙高，任务就完成了。