重庆 4 号机器被植入挖矿木马记录_2020-03-22

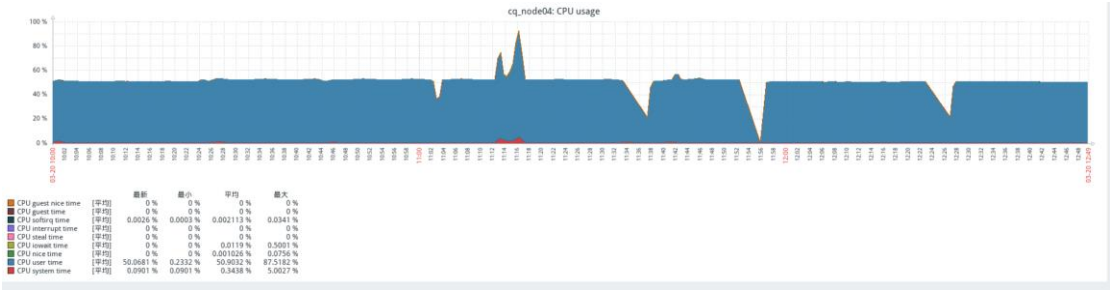
概述：

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。

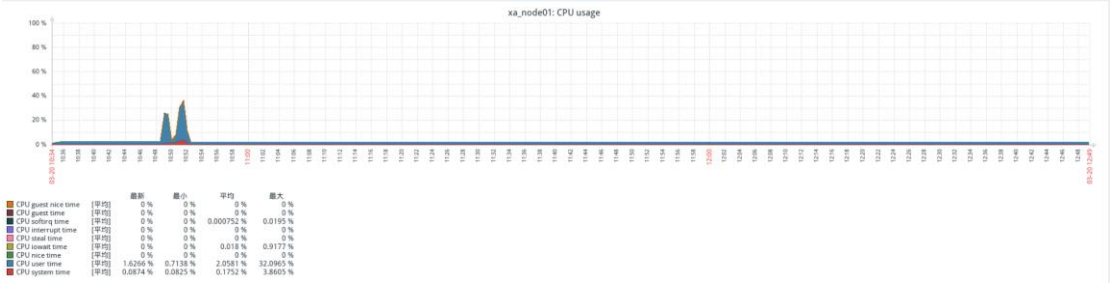
详细信息：

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

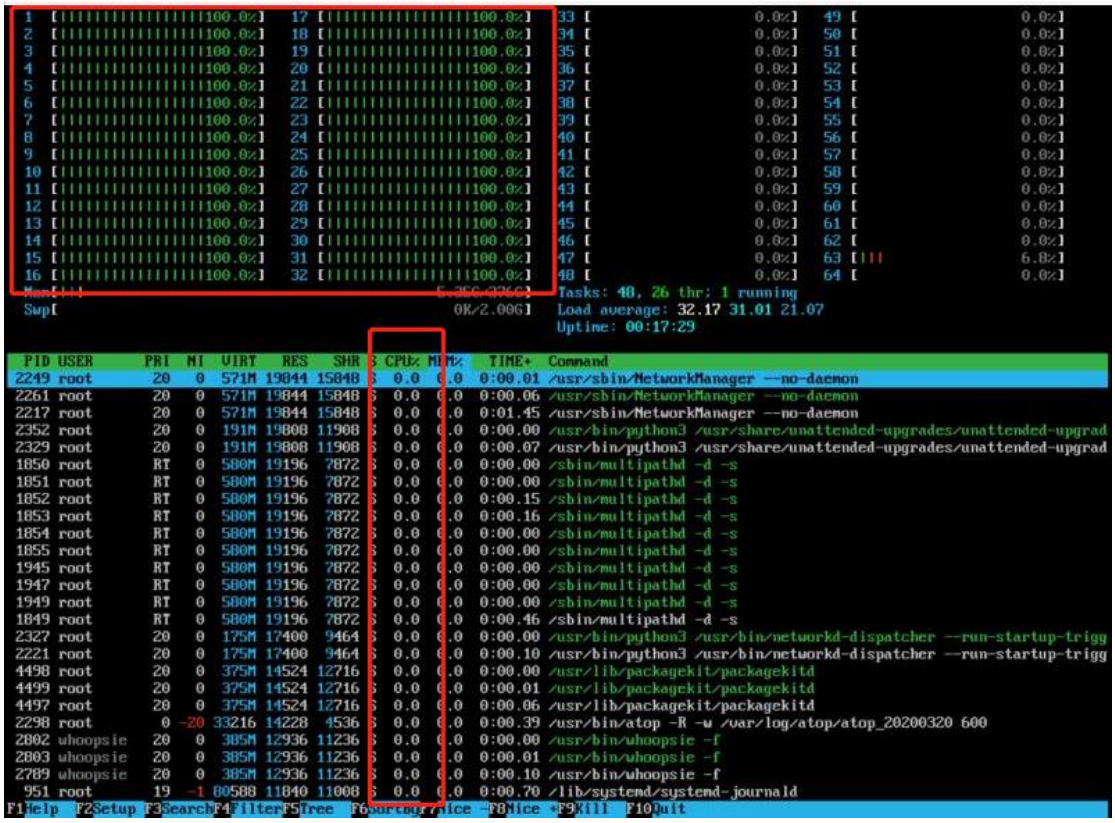


当时多台服务器正在进行 bench 性能测试，而其他的服务器在跑 bench 测试过程中并没有出现该情况。如图

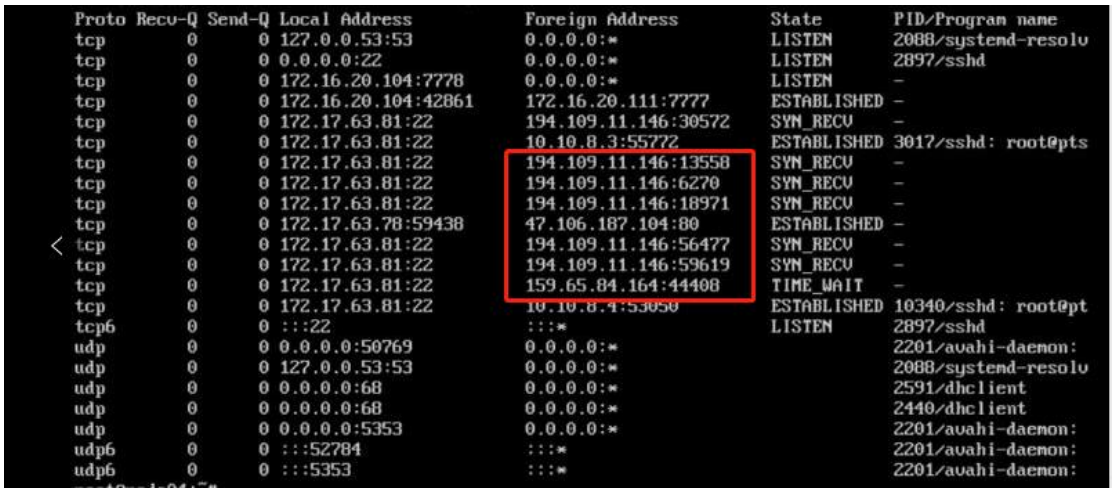


所以便通过 ssh 登陆重庆 04 号机器检查。

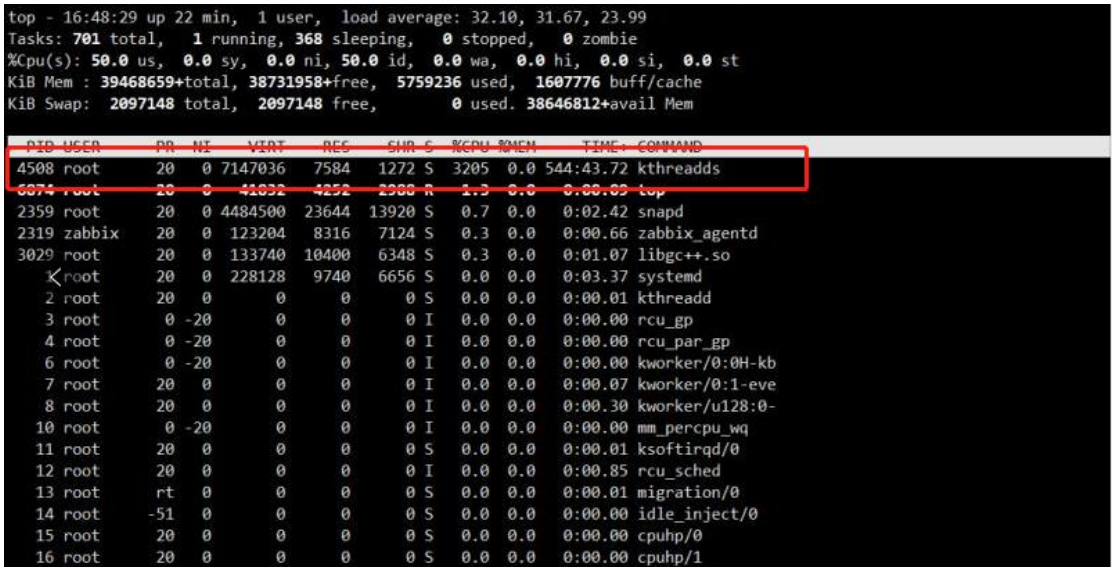
使用 htop 和 top 查看运行的进程。htop 显示 CPU 使用达到了 50%，但是没有发现高占用的进程，如图：



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：



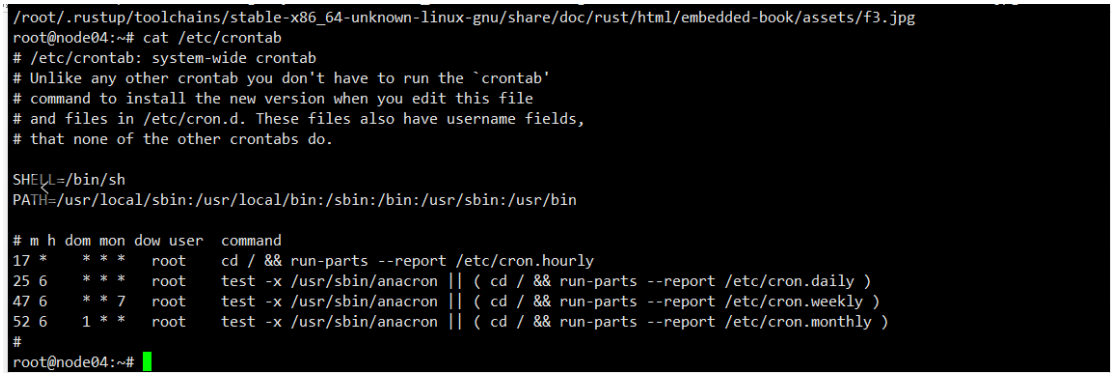
使用 ps、top 等命令无法查询到病毒进程，推测病毒可能修改 ps 或 top 指令，把进程隐藏了。所以这里使用 busybox 代替系统命令（系统命令已不可信，操作优先采用 busybox）例如 busybox top,如图：



果然找到了这个程序。

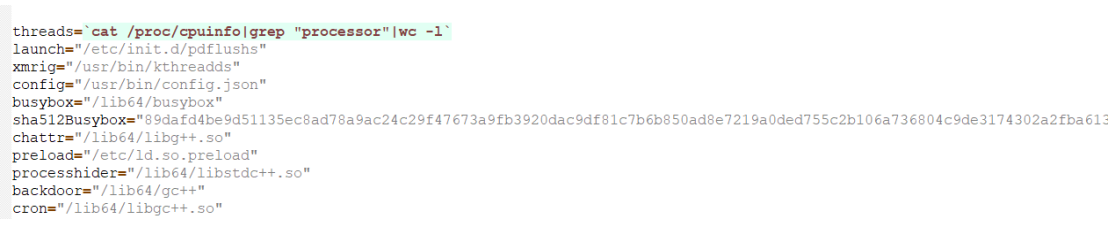
1、 解决过程

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：



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。



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。