链滴

转载：记一次清理挖矿后门程序的过程

作者：SmiteLi
原文链接：https://ld246.com/article/1582265248234
来源网站：链滴

原文地址

```
strace -tt -T -f -e trace=file -o /opt/strace.log -s 1024 -p  $(lsof -i:$(netstat -na | awk '/51./&&SYN_SENT/{gsub(".*:","",$4);print $4}') | awk 'NR>1{print $2}')
```

先检查当前服务器的网络连接，查看是否有陌生IP

```
netstat -na|awk '/ESTABLISHED/{print $5}'|awk -F: '{print $1}'|sort -r |uniq -c
```

查看到有一个默认IP是 51.x.x.x，将IP放到 ip138网站一查，是国外的IP，又查了下中国的公网地址，发现中国没有51.x.x.x的地址段。遂在安全组里面先把 这个IP设置成黑名单。让他无法与外网完成TP连接，当安全组配置好以后，再检查发现，这个挖矿程序总共有4个IP，继续通过查网络连接的脚本个IP都获取到，然后放到安全组里面加入黑名单，这样几个黑名单的IP就都无法与外网完成TCP连接。

然后就是通过端口查进程，但发现这个进程几乎秒关。完全无法获悉到。既然手动查进程不行，就用本来搞

因为51开头的IP都已经被限制了访问，所以网络连接状态一直是SYN_SENT。按照这个思路，用下面本把本地端口获取到。

```
netstat -na | awk '/51./&&/SYN_SENT/{gsub(".*:","",$4);print $4}'
```

单独开一个窗口监控进程的命令

```
watch -d -n1 'netstat -na |grep 51.'
```

获取到端口以后，我考虑通过 lsof -i:端口 来查进程PID。 然后把上面的命令结合起来，就能指导进程ID了

```
lsof -i:$(netstat -na | awk '/51./&&/SYN_SENT/{gsub(".*:","",$4);print $4}') | awk 'NR>1{print $2
'
```

有了PID就好办了。我们可通过 ls -l /proc/PID来查看这个进程的状态。但要想把进程调用的所有文复制出来还是不是很容易（因为进程1秒左右就被自动干掉了），所以我想了个方法：捕获进程调用内存信息。这样就可以看到他跑了哪些信息，为了方便看数据，我就用starce来跑了。并把结果存储一个日志文件中。这样就可以观察到整个程序是怎么工作的

```
strace -tt -T -f -e trace=file -o /opt/strace.log -s 1024 -p  $(lsof -i:$(netstat -na | awk '/51./&&SYN_SENT/{gsub(".*:","",$4);print $4}') | awk 'NR>1{print $2}')
```

快速杀死进程，避免产生复制程序和软连接（单独杀一个进程是杀不死的） 其实在处理之前我也观察下，有4个主进程，且每个进程的长度都是10为，且全为连续的小写字母。这就为我做过滤提供了非准确的信息。为甚么这些进程是10位呢。因为是通过 systemd-udev来生成的。

```
ls -l --full-time /usr/bin/* /bin/* /tmp/* | awk -F'/' "/^-/&&/$(date +%F)/&&length(\$NF)==1"|awk '{print $NF}' | xargs rm -rf
```