链滴

Linux gcc.sh 病毒的处理记录

作者：Andy

原文链接：https://ld246.com/article/1533623557825

来源网站：链滴

最近发现服务器不停的向外发包，且CPU持续100%，远程登录后查看发现有一长度为10的随机字符进程，kill掉，会重新生成另外长度为10的字符串进程。删除文件也会重复生成，查阅crond相关日志发现实际执行的内容为/lib/libudev.so ，以此为关键字进行查询，找到如下内容：

1.网络流量暴增，使用 top 观察至少有一个 10个随机字符组成的进程执行，占用大量 CPU 使用率。除这些程序，马上又生成新的进程。

2.检查/etc/crontab每三分钟执行gcc.sh

```
/3 * * * * root /etc/cron.hourly/gcc.sh
```

3.查看病毒文件 gcc.sh，可以看到病毒本身是 /lib/libudev.so。

```
cat /etc/cron.hourly/gcc.sh
#!/bin/sh
PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin:/usr/X11R6/bin
for i in cat `/proc/net/dev|grep :|awk -F: {'print $1'}`; do ifconfig $i up& done
cp /lib/libudev.so /lib/libudev.so.6
/lib/libudev.so.6
```

4.删除上一行定时任务，并且删除 gcc.sh文件，并设置 /etc/crontab 无法变更，否则又会马上生成的文件。

```
# rm -f /etc/cron.hourly/gcc.sh ; chattr +i /etc/crontab
```

5.使用 top 查看病毒为 vmsykoezbr，id 为 825，不要直接杀掉进程，否则会重新生成新的进程，而将他停止。

```
# kill -STOP 825
```

6.删除 /etc/init.d 内的文件。

```
# find /etc -name '*vmsykoezbr*' | xargs rm -f
```

7.删除 /usr/bin 下的文件。

```
# rm -f /usr/bin/vmsykoezbr
```

8.查看 /usr/bin 最近变动的文件，如果是病毒也一起删除，其他可疑的其他可疑目录也一样。

```
# ls -lt /usr/bin | head
```

9.现在杀掉病毒进程，就不会重新生成了。

```
# pkill vmsykoezbr
```

10.删除病毒

```
# rm -f /lib/libudev.so
```