02

OPEN ORIENTED

凹 凸 实 验 室

记一次病毒清理

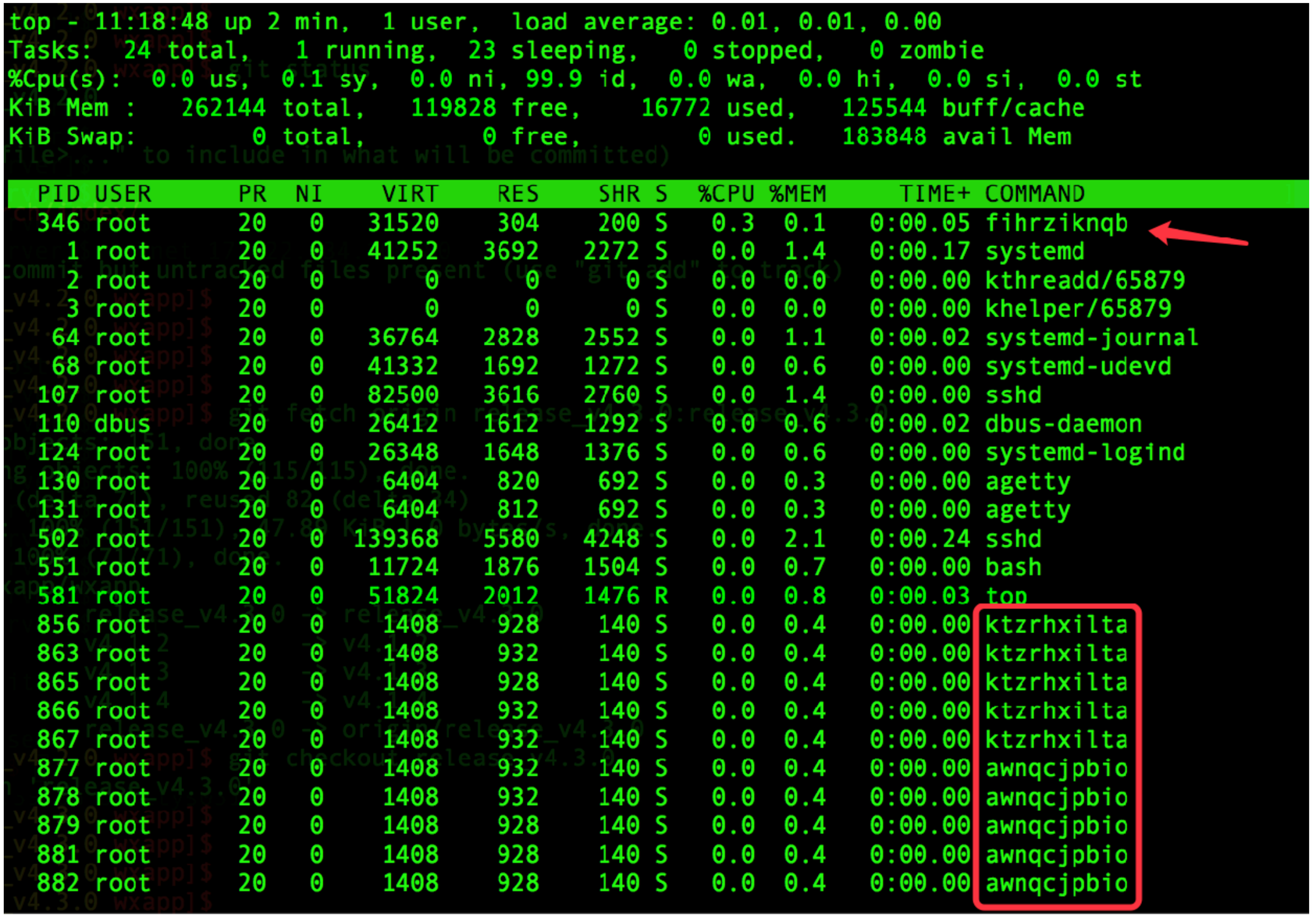
Secbone

事情要从一次宕机说起...

重启

又宕掉了！

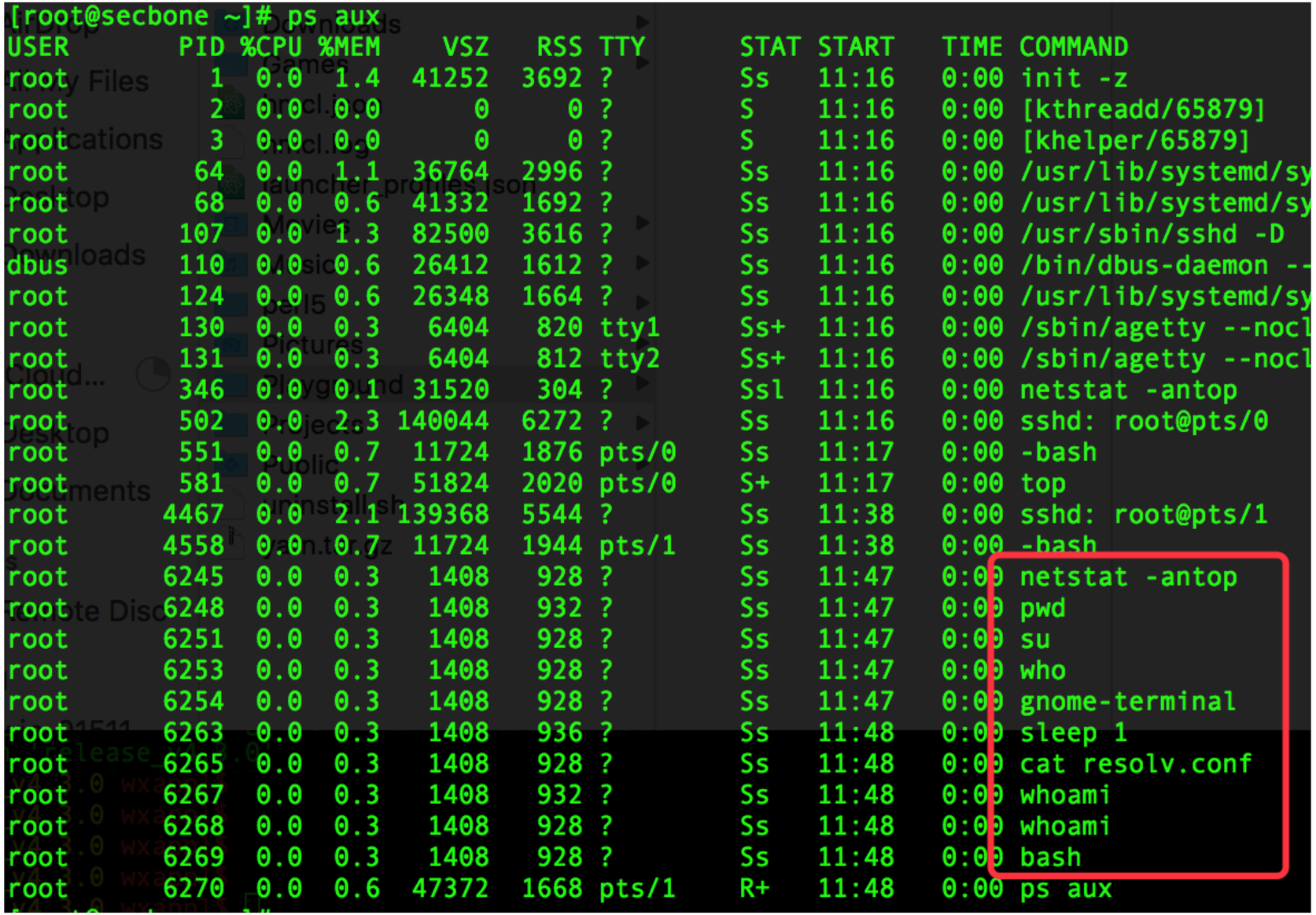

可达鸭眉头一皱
发现事情并不简单

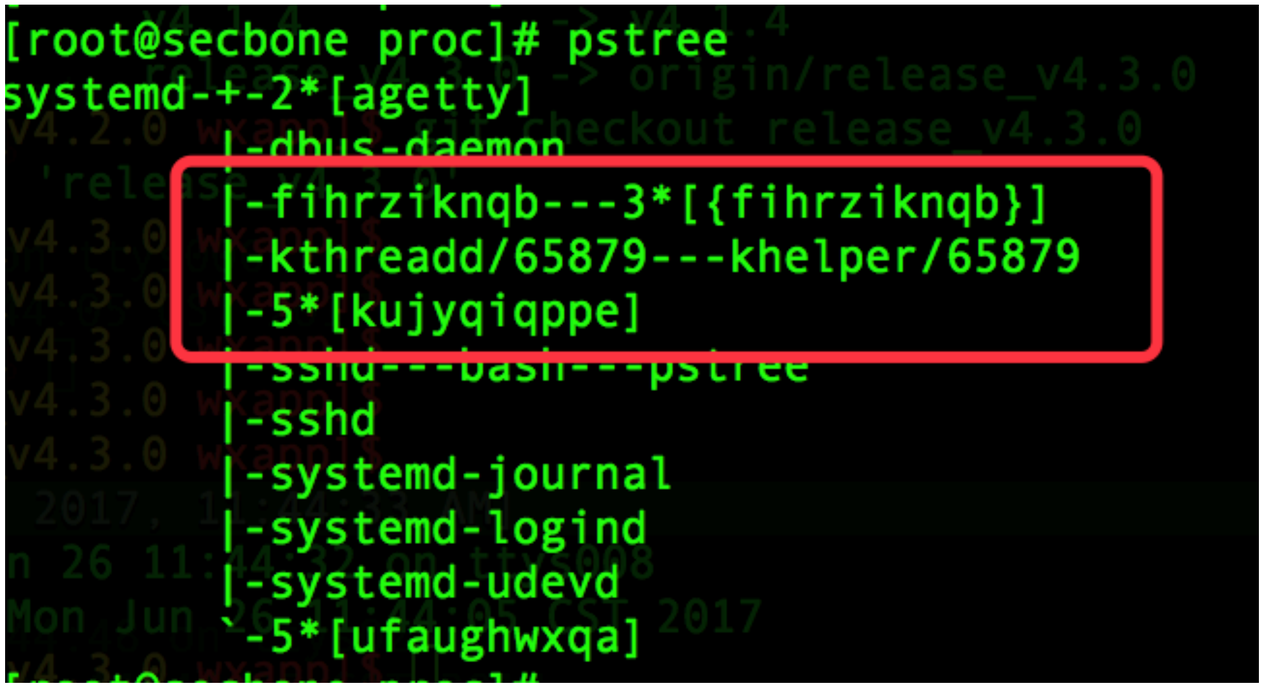

top - 11:18:48 up 2 min, 1 user, load average: 0.01, 0.01, 0.00
Tasks: 24 total,   1 running, 23 sleeping,   0 stopped,   0 zombie
%Cpu(s): 0.0 us, 0.1 sy, 0.0 ni, 99.9 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem :   262144 total,   119828 free,   16772 used,   125544 buff/cache
KiB Swap: 0 total,   0 free,   0 used.   183848 avail Mem
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
346 root 20 0 31520 304 200 S 0.3 0.1 0:00.05 fihrziknqb
1 root 20 0 41252 3692 2272 S 0.0 1.4 0:00.17 systemd
2 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kthreadd/65879
3 root 20 0 0 0 0 S 0.0 0.0 0:00.00 khelper/65879
64 root 20 0 36764 2828 2552 S 0.0 1.1 0:00.02 systemd-journal
68 root 20 0 41332 1692 1272 S 0.0 0.6 0:00.00 systemd-udevd
107 root 20 0 82500 3616 2760 S 0.0 1.4 0:00.00 sshd
110 dbus 20 0 26412 1612 1292 S 0.0 0.6 0:00.02 dbus-daemon
124 root 20 0 26348 1648 1376 S 0.0 0.6 0:00.00 systemd-logind
130 root 20 0 6404 820 692 S 0.0 0.3 0:00.00 agetty
131 root 20 0 6404 812 692 S 0.0 0.3 0:00.00 agetty
502 root 20 0 139368 5580 4248 S 0.0 2.1 0:00.24 sshd
551 root 20 0 11724 1876 1504 S 0.0 0.7 0:00.00 bash
581 root 20 0 51824 2012 1476 R 0.0 0.8 0:00.03 top
856 root 20 0 1408 928 140 S 0.0 0.4 0:00.00 ktzrhxilta
863 root 20 0 1408 932 140 S 0.0 0.4 0:00.00 ktzrhxilta
865 root 20 0 1408 928 140 S 0.0 0.4 0:00.00 ktzrhxilta
866 root 20 0 1408 932 140 S 0.0 0.4 0:00.00 ktzrhxilta
867 root 20 0 1408 932 140 S 0.0 0.4 0:00.00 ktzrhxilta
877 root 20 0 1408 932 140 S 0.0 0.4 0:00.00 awnqcjpbio
878 root 20 0 1408 932 140 S 0.0 0.4 0:00.00 awnqcjpbio
879 root 20 0 1408 928 140 S 0.0 0.4 0:00.00 awnqcjpbio
881 root 20 0 1408 928 140 S 0.0 0.4 0:00.00 awnqcjpbio
882 root 20 0 1408 928 140 S 0.0 0.4 0:00.00 awnqcjpbio

kill 删除

又出现了！

小明甩了下头发
发现事情不简单


[root@secbone ~]# ps aux
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.0 1.4 41252 3692 ? Ss 11:16 0:00 init -z
root 2 0.0 0.0 0 0 ? S 11:16 0:00 [kthreadd/65879]
root 3 0.0 0.0 0 0 ? S 11:16 0:00 [khelper/65879]
root 64 0.0 1.1 36764 2996 ? Ss 11:16 0:00 /usr/lib/systemd/sy
root 68 0.0 0.6 41332 1692 ? Ss 11:16 0:00 /usr/lib/systemd/sy
root 107 0.0 1.3 82500 3616 ? Ss 11:16 0:00 /usr/sbin/sshd -D
dbus 110 0.0 0.6 26412 1612 ? Ss 11:16 0:00 /bin/dbus-daemon --
root 124 0.0 0.6 26348 1664 ? Ss 11:16 0:00 /usr/lib/systemd/sy
root 130 0.0 0.3 6404 820 tty1 Ss+ 11:16 0:00 /sbin/agetty --nocl
root 131 0.0 0.3 6404 812 tty2 Ss+ 11:16 0:00 /sbin/agetty --nocl
root 346 0.0 0.1 31520 304 ? Ssl 11:16 0:00 netstat -antop
root 502 0.0 2.3 140044 6272 ? Ss 11:16 0:00 sshd: root@pts/0
root 551 0.0 0.7 11724 1876 pts/0 Ss 11:17 0:00 -bash
root 581 0.0 0.7 51824 2020 pts/0 S+ 11:17 0:00 top
root 4467 0.0 2.1 139368 5544 ? Ss 11:38 0:00 sshd: root@pts/1
root 4558 0.0 0.7 11724 1944 pts/1 Ss 11:38 0:00 -bash
root 6245 0.0 0.3 1408 928 ? Ss 11:47 0:00 netstat -antop
root 6248 0.0 0.3 1408 932 ? Ss 11:47 0:00 pwd
root 6251 0.0 0.3 1408 928 ? Ss 11:47 0:00 su
root 6253 0.0 0.3 1408 928 ? Ss 11:47 0:00 who
root 6254 0.0 0.3 1408 928 ? Ss 11:47 0:00 gnome-terminal
root 6263 0.0 0.3 1408 936 ? Ss 11:48 0:00 sleep 1
root 6265 0.0 0.3 1408 928 ? Ss 11:48 0:00 cat resolv.conf
root 6267 0.0 0.3 1408 932 ? Ss 11:48 0:00 whoami
root 6268 0.0 0.3 1408 928 ? Ss 11:48 0:00 whoami
root 6269 0.0 0.3 1408 928 ? Ss 11:48 0:00 bash
root 6270 0.0 0.6 47372 1668 pts/1 R+ 11:48 0:00 ps aux


[root@secbone proc]# pstree
systemd-+-2*[agetty]
|-dbus-daemon
|-fihrziknqb---3*[{fihrziknqb}]
|-kthreadd/65879---khelper/65879
|-5*[kujyqiqppe]
|-sshd---bash---pstree
|-sshd
|-systemd-journal
|-systemd-logind
|-systemd-udevd
`-5*[ufaughwxqa]

事情变得有趣了起来

Rootkit

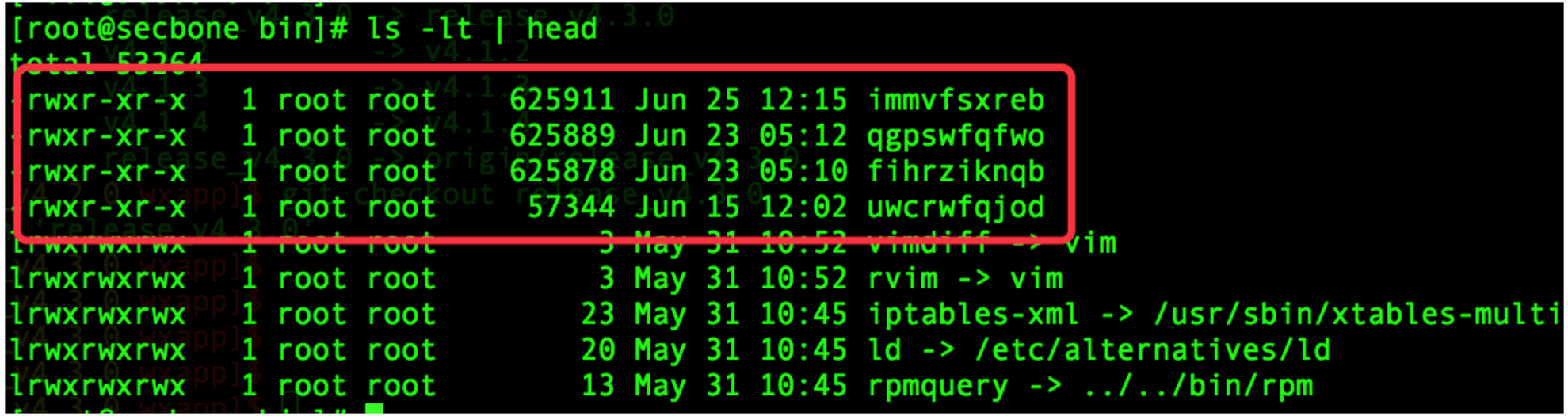

你是不是想把事情搞大！！

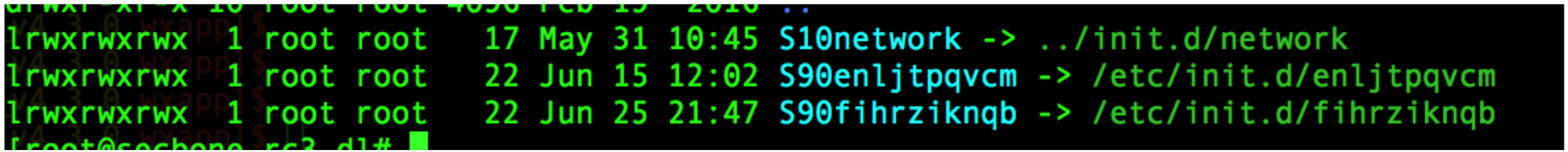
XOR.DDoS

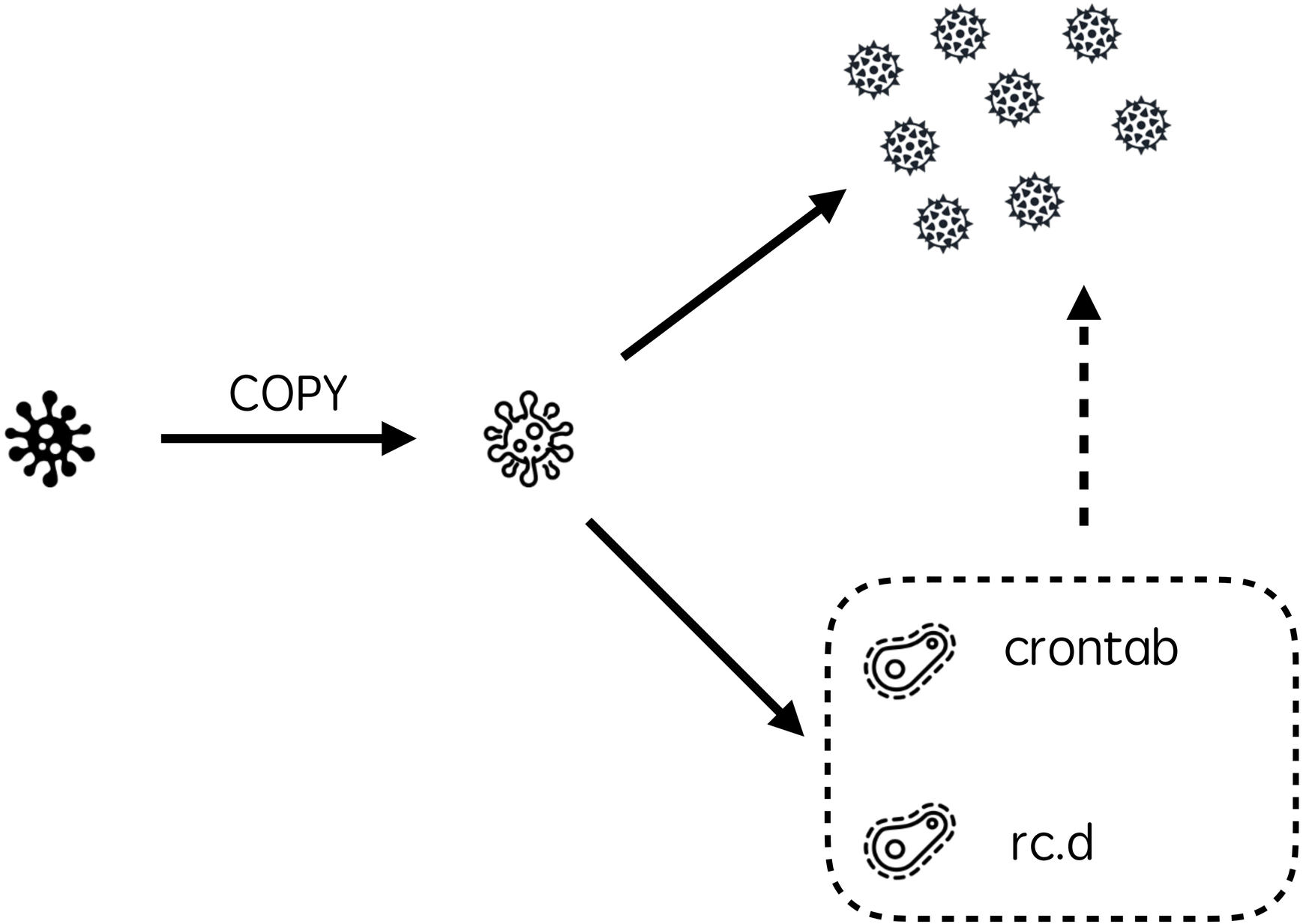
- 32 randomly generated lower-case characters stored in /var/run/mount.pid
- Copies itself to /lib/libgcc.so
- Copies itself to /usr/bin/ with a filename of 10 random lowercase characters
- Creates symlink to /usr/bin/ copy and placed in /etc/init.d/
- Creates symlinks to /usr/bin/ in /etc/rc[1-5].d/S90[Session ID]
- Creates symlinks to /usr/bin/ in /etc/rc.d/rc[1-5].d/S90[Session ID]
- Cron script to turn on network interfaces, copy /lib/libgcc.so to /lib/libgcc.so.bak, execute /lib/libgcc.so.bak
- Uses XOR key: BB2FA36AAA9541F0

```
# /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
```


[root@secbone bin]# ls -lt | head
total 53264
-rwxr-xr-x 1 root root 625911 Jun 25 12:15 immvfsxreb
-rwxr-xr-x 1 root root 625889 Jun 23 05:12 qgpswfqfwo
-rwxr-xr-x 1 root root 625878 Jun 23 05:10 fihrziknqb
-rwxr-xr-x 1 root root 57344 Jun 15 12:02 uwcrwfqjod
lrwxrwxrwx 1 root root 3 May 31 10:52 vimdiff -> vim
lrwxrwxrwx 1 root root 3 May 31 10:52 rvim -> vim
lrwxrwxrwx 1 root root 23 May 31 10:45 iptables-xml -> /usr/sbin/xtables-multi
lrwxrwxrwx 1 root root 20 May 31 10:45 ld -> /etc/alternatives/ld
lrwxrwxrwx 1 root root 13 May 31 10:45 rpmquery -> ../../bin/rpm


lrwxrwxrwx 1 root root 17 May 31 10:45 S10network -> ../init.d/network
lrwxrwxrwx 1 root root 22 Jun 15 12:02 S90enljtpqvcm -> /etc/init.d/enljtpqvcm
lrwxrwxrwx 1 root root 22 Jun 25 21:47 S90fihrziknqb -> /etc/init.d/fihrziknqb


COPY
crontab
rc.d

清理

抽完这跟烟
老子打死你

```
int __cdecl DelService(char *a1)
{
  char filename; // [sp+20h] [bp-408h]@1
  int i; // [sp+420h] [bp-8h]@1
  int v4; // [sp+424h] [bp-4h]@1

  i = 0;
  memset(&filename, 0, 1024);
  v4 = abstract_file_name(a1);
  remove(a1);
  snprintf(&filename, 1024, "/etc/init.d/%s", v4);
  remove(&filename);
  for ( i = 1; i <= 5; ++i )
  {
    snprintf(&filename, 1024, "/etc/rc%d.d/S90%s", i, v4);
    unlink(&filename);
    remove(&filename);
  }
  LinuxExec_Argv2("chkconfig", "--del", v4);
  LinuxExec_Argv2("update-rc.d", v4, "remove");
  return 0;
}
```

/etc/init.d**/tmoogsb**

/etc/cron.hourly/gcc.sh

/etc/rc1.d/S90tmoogsb

/etc/rc2.d/S90tmoogsb

/etc/rc3.d/S90tmoogsb

/etc/rc4.d/S90tmoogsb

/etc/rc5.d/S90tmoogsb

/etc/rc.d/rc1.d/S90tmoogsb

/etc/rc.d/rc2.d/S90tmoogsb

/etc/rc.d/rc3.d/S90tmoogsb

/etc/rc.d/rc4.d/S90tmoogsb

/etc/rc.d/rc4.d/S90tmoogsb

chkconfig – del tmoogsb

update-rc.d tmoogsb remove

/etc/ssh/sshd_config

PasswordAuthentication no

PermitRootLogin no

1Password

rkhunter

chkrootkit

Q&A

THANKS

FOR YOUR WATCHING