第4篇：盖茨木马

0x00 前言

Linux盖茨木马是一类有着丰富历史，隐藏手法巧妙，网络攻击行为显著的DDoS木马，主要恶意特点是具备了后门程序，DDoS攻击的能力，并且会替换常用的系统文件进行伪装。木马得名于其在变量函数的命名中，大量使用Gates这个单词。分析和清除盖茨木马的过程，可以发现有很多值得去学习和借鉴的地方。

0x01 应急场景

某天，网站管理员发现服务器CPU资源异常，几个异常进程占用大量网络带宽：

```
top - 15:31:56 up  4:11,  3 users,  load average: 2.38, 2.23, 1.59
Tasks: 391 total,   2 running, 387 sleeping,   1 stopped,   1 zombie
Cpu(s): 49.1%us, 23.4%sy,  0.0%ni, 25.6%id,  0.0%wa,  0.0%hi,  1.8%si,  0.0%st
Mem:  16334216k total,  7405560k used,  8928656k free,   170724k buffers
Swap:  8241144k total,        0k used,  8241144k free,   601492k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 1871 root      20   0 34184 3072  208 S 99.1  0.0   8:44.75 kaxvikpoxk
 1886 root      20   0 52488  816  208 S 74.9  0.0  11:48.19 sryetfcwyo
 7059 root      20   0  238m  53m 3780 R 70.9  0.3  62:31.19 python
 2750 root      20   0 5894m 599m  26m S  1.7  3.8   7:36.29 java
 2786 root      20   0 4793m 414m  13m S  1.3  2.6   4:05.13 java
 4301 root      20   0 2593m  37m 6548 S  1.0  0.2   2:23.14 python
 2188 root      20   0 4015m 193m  16m S  0.7  1.2   0:43.98 java
 3644 root      20   0 5810m 1.1g  29m S  0.7  7.4   2:08.47 java
 7066 root      20   0  212m  12m 5180 S  0.7  0.1   0:15.46 python
30875 root      20   0 15304 1484  948 R  0.7  0.0   0:00.17 top
    1 root      20   0 19368 1556 1240 S  0.3  0.0   0:07.44 init
 2206 root      20   0  427m  30m 5256 S  0.3  0.2   0:55.12 python
 2213 root      20   0 1311m  29m 7024 S  0.3  0.2   0:14.60 python
 2591 redisuse  20   0  134m 8028 1216 S  0.3  0.0   0:21.44 redis-server
 3764 root      20   0  217m  13m 5296 S  0.3  0.1   0:04.83 python
 3845 root      20   0 1324m  22m 5332 S  0.3  0.1   0:24.35 python
 3901 root      20   0  214m  12m 5212 S  0.3  0.1   0:03.77 python
 3925 root      20   0  222m  15m 5296 S  0.3  0.1   0:40.85 python
 4272 postgres  20   0  337m  15m  12m S  0.3  0.1   0:06.87 postmaster
 4436 root      20   0 1638m  88m 6200 S  0.3  0.6   2:58.12 python
 5582 root      20   0  304m  21m 5668 S  0.3  0.1   0:55.51 python
 5594 root      20   0  305m  21m 5668 S  0.3  0.1   0:56.38 python
 7109 root      20   0  650m 455m 5268 S  0.3  2.9   0:22.28 hekad
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
    3 root      RT   0     0    0    0 S  0.0  0.0   0:00.78 migration/0
```

0x02 事件分析

异常IP连接：

```
[root@localhost bsd-port]# netstat -anplt
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN      5670/sshd
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LISTEN      1527/cupsd
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN      1991/master
tcp        0      0 0.0.0.0:48227               0.0.0.0:*                   LISTEN      1451/rpc.statd
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN      1431/rpcbind
tcp        0      1 192.168.8.146:47015         103.57.108.162:6001         SYN_SENT    15076/./getty
tcp        0     52 192.168.8.146:22            192.168.8.1:48821           ESTABLISHED 5734/sshd
tcp        0      0 :::22                       :::*                        LISTEN      5670/sshd
tcp        0      0 ::1:631                     :::*                        LISTEN      1527/cupsd
tcp        0      0 ::1:25                      :::*                        LISTEN      1991/master
tcp        0      0 :::57286                    :::*                        LISTEN      1451/rpc.statd
tcp        0      0 :::111                      :::*                        LISTEN      1431/rpcbind
```

异常进程：

查看进行发现ps aux进程异常，进入该目录发现多个命令，猜测命令可能已被替换

登录服务器，查看系统进程状态，发现不规则命名的异常进程、异常下载进程：

```
root      2124  0.0  0.0   3020   496 ?        Ss   14:48   0:00 /usr/sbin/atd
root      2291  0.0  0.0   2004   472 tty2     Ss+  14:48   0:00 /sbin/mingetty /dev/tty2
root      2293  0.0  0.0   2004   476 tty3     Ss+  14:48   0:00 /sbin/mingetty /dev/tty3
root      2295  0.0  0.0   2004   472 tty4     Ss+  14:48   0:00 /sbin/mingetty /dev/tty4
root      2297  0.0  0.1   3360  1828 ?        S<   14:48   0:00 /sbin/udevd -d
root      2298  0.0  0.1   3360  1832 ?        S<   14:48   0:00 /sbin/udevd -d
root      2300  0.0  0.0   2004   500 tty5     Ss+  14:48   0:00 /sbin/mingetty /dev/tty5
root      2305  0.0  0.0   2004   472 tty6     Ss+  14:48   0:00 /sbin/mingetty /dev/tty6
root      5322  0.0  0.2  22732  3084 ?        Sl   14:49   0:00 /usr/sbin/console-kit-daemon --no-daemon
root      5670  0.0  0.1   9008  1040 ?        Ss   14:49   0:00 /usr/sbin/sshd
root      5734  0.0  0.3  12076  3808 ?        Ss   14:50   0:01 sshd: root@pts/0
root      5757  0.0  0.1   6952  1808 pts/0    Ss   14:50   0:00 -bash
root      8510  0.0  0.0   2004   472 tty1     Ss+  15:04   0:00 /sbin/mingetty /dev/tty1
root     10628  0.0  0.0  93636   868 ?        Ssl  15:13   0:00 /usr/bin/dpkgd/ps aux
root     10704  0.0  0.0  11716   544 ?        Ssl  15:13   0:00 /usr/bin/.sshd
root     14033  0.0  0.0   1372   924 ?        Ss   15:27   0:00 gnome-terminal
root     14036  0.0  0.0   1372   924 ?        Ss   15:27   0:00 su
root     14038  0.0  0.0   1372   924 ?        Ss   15:27   0:00 echo "find"
root     14039  0.0  0.0   1372   924 ?        Ss   15:27   0:00 ifconfig eth0
root     14040  0.0  0.1   6544  1060 pts/0    R+   15:27   0:00 ps aux
[root@localhost dpkgd]# ^C
[root@localhost dpkgd]# cd  /usr/bin/dpkgd
[root@localhost dpkgd]#
[root@localhost dpkgd]# ls -lh
总用量 1.6M
-rwxr-xr-x. 1 root root 144K 9月   3 14:56 lsof
-rwxr-xr-x. 1 root root 121K 9月   3 14:56 netstat
-rwxr-xr-x. 1 root root 1.2M 9月   3 14:56 ps
-rwxr-xr-x. 1 root root  73K 9月   3 14:56 ss
```

异常启动项

进入rc3.d目录可以发现多个异常进行：

/etc/rc.d/rc3.d/S97DbSecuritySpt

/etc/rc.d/rc3.d/S99selinux

```
[root@localhost rc.d]# ls
init.d  rc  rc0.d  rc1.d  rc2.d  rc3.d  rc4.d  rc5.d  rc6.d  rc.local  rc.sysinit
[root@localhost rc.d]# cd init.d/
[root@localhost init.d]# ls
abrt-ccpp  auditd           cgred         functions     ip6tables   kugpfxroiy   mysqld      nfslock  portreserve  restorecond  rpcsvcgssd  single     vmware-tools
abrtd      autofs           cpuspeed      haldaemon     iptables    lvm2-lvmetad netconsole  ntpd     postfix      rngd         rsyslog     smartd     vmware-tools-thinprint
abrt-oops  blk-availability crond         halt          irqbalance  lvm2-monitor netfs       ntpdate  psacct       rpcbind      sandbox     sshd       winbind
acpid      certmonger       cups          htcacheclean  kdump       mdmonitor    network     numad    quota_nld    rpcgssd      saslauthd   sssd       xinetd
atd        cgconfig         DbSecuritySpt httpd         killall     messagebus   nfs         oddjobd  rdisc        rpcidmapd    selinux     udev-post  ypbind
[root@localhost init.d]# more DbSecuritySpt
#!/bin/bash
/usr/bin/dpkgd/ps
[root@localhost init.d]# more selinux
#!/bin/bash
/usr/bin/bsd-port/getty
```

```
lrwxrwxrwx. 1 root root 20 12月 22 14:48 S90kugpfxroiy -> ../init.d/kugpfxroiy
lrwxrwxrwx. 1 root root 13 1月  10 2016 S95atd -> ../init.d/atd
lrwxrwxrwx. 1 root root 25 9月   3 14:56 S97DbSecuritySpt -> /etc/init.d/DbSecuritySpt
lrwxrwxrwx. 1 root root 20 1月  10 2016 S99certmonger -> ../init.d/certmonger
lrwxrwxrwx. 1 root root 11 1月  10 2016 S99local -> ../rc.local
lrwxrwxrwx. 1 root root 19 9月   3 14:56 S99selinux -> /etc/init.d/selinux
```

搜索病毒原体

find / -size -1223124c -size +1223122c -exec ls -id {} \; 搜索1223123大小的文件

```
[root@localhost rc3.d]# find / -size -1223124c -size +1223122c -exec ls -id {} \;
529599 /bin/ps
524140 /bin/netstat
659226 /usr/bin/bsd-port/getty
659230 /usr/bin/dpkgd/ps
278271 /usr/bin/.sshd
271230 /usr/sbin/ss
284915 /usr/sbin/lsof
find: “ /proc/16353” : 没有那个文件或目录
find: “ /proc/16356” : 没有那个文件或目录
find: “ /proc/16358” : 没有那个文件或目录
find: “ /proc/16359” : 没有那个文件或目录
find: “ /proc/16375/task/16375/fd/5” : 没有那个文件或目录
find: “ /proc/16375/task/16375/fdinfo/5” : 没有那个文件或目录
find: “ /proc/16375/fd/5” : 没有那个文件或目录
find: “ /proc/16375/fdinfo/5” : 没有那个文件或目录
```

从以上种种行为发现该病毒与“盖茨木马”有点类似，具体技术分析细节详见：

Linux平台“盖茨木马”分析

http://www.freebuf.com/articles/system/117823.html

悬镜服务器卫士丨Linux平台“盖茨木马”分析

http://www.sohu.com/a/117926079_515168

手动清除木马过程：

1、简单判断有无木马

```
#有无下列文件
cat /etc/rc.d/init.d/selinux
cat /etc/rc.d/init.d/DbSecuritySpt
ls /usr/bin/bsd-port
ls /usr/bin/dpkgd
#查看大小是否正常
ls -lh /bin/netstat
ls -lh /bin/ps
ls -lh /usr/sbin/lsof
ls -lh /usr/sbin/ss
```

2、上传如下命令到/root下

```
ps netstat ss lsof
```

3、删除如下目录及文件

```
rm -rf /usr/bin/dpkgd (ps netstat lsof ss)
rm -rf /usr/bin/bsd-port     #木马程序
rm -f /usr/bin/.sshd         #木马后门
rm -f /tmp/gates.lod
rm -f /tmp/moni.lod
rm -f /etc/rc.d/init.d/DbSecuritySpt(启动上述描述的那些木马变种程序)
rm -f /etc/rc.d/rc1.d/S97DbSecuritySpt
rm -f /etc/rc.d/rc2.d/S97DbSecuritySpt
rm -f /etc/rc.d/rc3.d/S97DbSecuritySpt
rm -f /etc/rc.d/rc4.d/S97DbSecuritySpt
rm -f /etc/rc.d/rc5.d/S97DbSecuritySpt
rm -f /etc/rc.d/init.d/selinux(默认是启动/usr/bin/bsd-port/getty)
rm -f /etc/rc.d/rc1.d/S99selinux
rm -f /etc/rc.d/rc2.d/S99selinux
rm -f /etc/rc.d/rc3.d/S99selinux
rm -f /etc/rc.d/rc4.d/S99selinux
```

```
rm -f /etc/rc.d/rc5.d/S99selinux
```
4、找出异常程序并杀死
5、删除含木马命令并重新安装

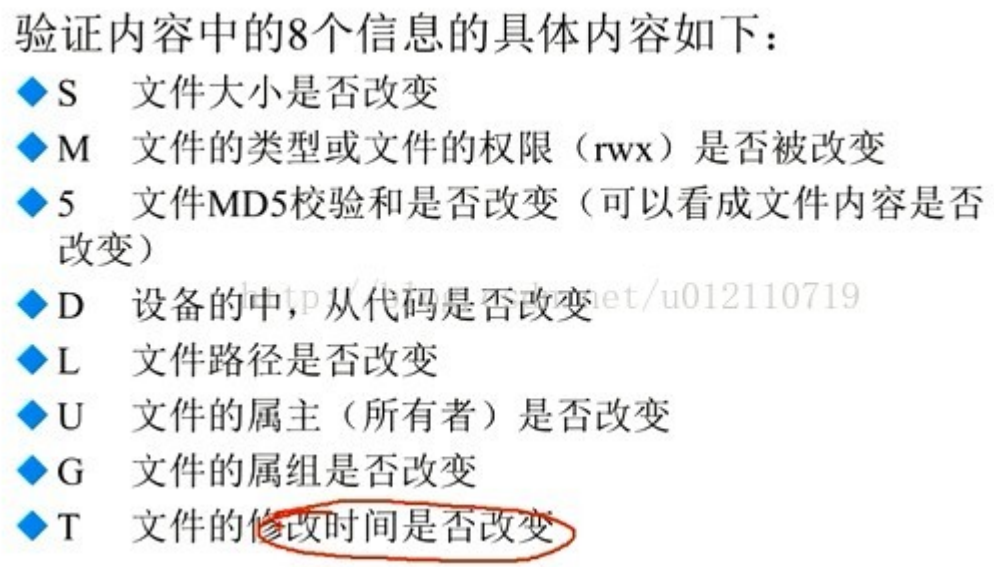
0x03 命令替换

RPM check检查：

系统完整性也可以通过rpm自带的-Va来校验检查所有的rpm软件包，有哪些被篡改了，防止rpm也被替换，上传一个安全干净稳定版本rpm二进制到服务器上进行检查

```
./rpm -Va > rpm.log
```

如果一切均校验正常将不会产生任何输出。如果有不一致的地方，就会显示出来。输出格式是8位长字符串，``c 用以指配置文件，接着是文件名. 8位字符的每一个 用以表示文件与RPM数据库中一种属性的比较结果 。``.（点）表示测试通过。.下面的字符表示对RPM软件包进行的某种测试失败：



命令替换：

```
rpm2cpio 包全名 |  cpio -idv .文件绝对路径    rpm包中文件提取
Rpm2cpio  将rpm包转换为cpio格式的命令
Cpio 是一个标准工具，它用于创建软件档案文件和从档案文件中提取文件

Cpio 选项 < [文件|设备]
-i：copy-in模式，还原
-d：还原时自动新建目录
-v：显示还原过程
```

文件提取还原案例：

rpm -qf /bin/ls 查询ls命令属于哪个软件包
mv /bin/ls /tmp
rpm2cpio /mnt/cdrom/Packages/coreutils-8.4-19.el6.i686.rpm | cpio -idv ./bin/ls 提取rpm包中ls命令到当前目录的/bin/ls下
cp /root/bin/ls /bin/ 把ls命令复制到/bin/目录 修复文件丢失

挂载命令rpm包:
mkdir /mnt/chrom/ 建立挂载点
mount -t iso9660 /dev/cdrom /mnt/cdrom/ 挂在光盘
mount/dev/sr0 /mnt/cdrom/

卸载命令
umount 设备文件名或挂载点
umount /mnt/cdrom/

```
[root@localhost mnt]# ls
cdrom  chrom  hgfs
[root@localhost mnt]# rpm -qf /bin/ps
procps-3.2.8-30.el6.i686
[root@localhost mnt]# rpm2cpio /mnt/cdrom/Packages/procps-3.2.8-30.el6.i686.rpm  | cpio -idv ./bin/ps
./bin/ps
862 块
[root@localhost mnt]# ls
bin  cdrom  chrom  hgfs
[root@localhost mnt]# cd bin
[root@localhost bin]# ls
ps
[root@localhost bin]# cp ps /bin/ps
cp：是否覆盖"/bin/ps"？ yes
```

后续持续更新内容，将发布在公众号Bypass--，同时公众号提供了该项目的PDF版本，关注后回复"应急响应" 即可下载。