**安全事件应急响应操作指南**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 版本 | 姓 名 | 时 间 | 备 注 |
| 创建者 | V1.0 |  | 2017/09/01 | 创 建 |
| 修 改 |  |  |  |  |

目 录

[一、操作准备 3](#_Toc494372631)

[二、工具介绍 3](#_Toc494372632)

[1. Linux工具 3](#_Toc494372633)

[A.Chkrootkit 3](#_Toc494372634)

[B. Unhide 3](#_Toc494372635)

[C. Clamav 4](#_Toc494372636)

[D.rkhunter 5](#_Toc494372637)

[2. Windows 5](#_Toc494372638)

[3. 脚本介绍 5](#_Toc494372639)

[A. 脚本文件 5](#_Toc494372640)

[B. 检查内容 5](#_Toc494372641)

[4. 注意事项 6](#_Toc494372642)

[三、案例分享 7](#_Toc494372643)

[1. 2017.3.28日A系统应急响应 7](#_Toc494372644)

[2. 2017.4.05日B系统应急响应 7](#_Toc494372645)

[3. 2017.4.08日C系统应急响应 8](#_Toc494372646)

[4. 2017.5.12日D系统应急响应 9](#_Toc494372647)

[5. 2017.6.27日应急响应 10](#_Toc494372648)

[6. 2017.7.21日内网虚拟机应急响应 11](#_Toc494372649)

[7. 2017.7.27日E系统排查 12](#_Toc494372650)

[8. 2017.8.24日F系统应急排查 13](#_Toc494372651)

[四、复盘： 15](#_Toc494372652)

# 一、操作准备

脚本支持yum与apt-get安装，首先查看源有没有相关安装包，Apt包管理：

apt-get -y update

apt-cache search rkhunter

apt-cache search unhide

apt-cache search clamav

yum包管理：

yum search unhide rkhunter clamav epel-release

没有安装包或者安装不上的情况，可以用 offline.sh 脱机脚本检查。获取

git clone https://github.com/scopion/Emergency-Response

下面的工具中，脚本没有用到Chkrootkit 跟 clamav 工具。

Chkrookit 是因为其用法没必要用。

Clamav 是因为运行时间很长，所以把它注释掉了。可以自己单开一个窗口运行它。

# 二、工具介绍

## 1. Linux工具

### A.Chkrootkit

Chkrootkit：文件对比工具。使用系统命令检查系统命令文件有没有被篡改。

在操作系统刚被安装之后，或者说服务器开放之前，备份 chkrootkit 使用的系统命令，在一些必要的时候（怀疑系统命令已被修改的情况等等），让 chkrootkit 使用初始备份的系统命令进行工作。

安装包：chkrootkit.tar.gz

编译：make sense

使用：备份系统初始命令

Mkdir –p /usr/share/.commands/

cp $(which --skip-alias awk cut echo find egrep id head ls netstat ps strings sed uname ssh) /usr/share/.commands/

检测病毒

./chkrootkit

./chkrootkit -p /usr/share/.commands/ #commands是一个存放原生命令的目录。检查过程中调用这个目录里面的命令而不再使用系统命令（有被篡改的风险）

### B. Unhide

Unhide：隐藏进程及端口查询工具。使用多种方式查询隐藏进程。安装包：unhide-20121229.tgz

centos安装：yum -y install epel-release

yum install -y unhide

ubuntu安装：apt-get -y install unhide

编译：

If you ARE using a Linux kernel >= 2.6

gcc -Wall -O2 --static -pthread unhide-linux\*.c unhide-output.c -o unhide-linux

gcc -Wall -O2 --static unhide\_rb.c -o unhide\_rb

gcc -Wall -O2 --static unhide-tcp.c unhide-tcp-fast.c unhide-output.c -o unhide-tcp

ln -s unhide-linux unhide

Else (Linux < 2.6, \*BSD, Solaris and other Unice)

gcc --static unhide-posix.c -o unhide-posix

ln -s unhide unhide-posix

使用

./unhide sys >>/tmp/unhide.log

./unhide brute >>/tmp/unhide.log

./unhide proc >>/tmp/unhide.log

./unhide procall >>/tmp/unhide.log

./unhide procfs >>/tmp/unhide.log

./unhide quick >>/tmp/unhide.log

./unhide reverse >>/tmp/unhide.log

./unhide-tcp >>/tmp/unhide.log

unhide-20121229 文件夹是已编译好的。

### C. Clamav

Clamav：Linux下病毒查杀程序。

安装包：clamav-0.99.2.tar.gz

编译安装

yum install openssl\* -y

./configure --with-user=root --with-group=root

make

make install

centos安装：yum -y install epel-release

yum install -y clamav

ubuntu安装：apt-get -y install clamav

使用配置文件,将freshclam.conf 文件复制到/usr/local/etc/

1、升级

freshclam (升级病毒库) 保证你的LINUX可以正常上网哦.

mkdir -p /var/lib/clamav/

文件clamdb.tar.gz 是2017.6.12升级的病毒库文件。解压之后放在/var/lib/clamav/下。

2、杀毒

clamscan --查杀当前目录下的文件

clamscan -r --查杀当前目录的所有文件及目录

clamscan dir --查杀dir目录

clamscan -r dir --查杀目录dir下的所有文件及目录

nohup clamscan -r --bell -i / >> /tmp/clamav.log

卸载

./configure --with-user=root --with-group=root

sudo make uninstall

### D.rkhunter

rkhunter：Linux下杀毒软件。

安装包：rkhunter-1.4.2.tar.gz

安装：./installer.sh –install

centos安装：yum -y install epel-release

yum install -y rkhunter

ubuntu安装：apt-get -y install rkhunter

使用：rkhunter -c --sk >>check/rkhunter.log

卸载：./installer.sh --remove

## 2. Windows

365门神程序：365MSInst\_V2.0.exe 。知道创宇出品防御产品

官网：https://www.yunaq.com/365menshen/

安全狗程序：safedogfwqV5.0，safedogIISV4.0.exe，safedogwzApache.exe

官网：http://www.safedog.cn/

隐藏进程排查工具：unhide.exe

官网：http://www.unhide-forensics.info/

日志查看工具：elex\_setup.exe

官网：https://eventlogxp.com/

## 3. 脚本介绍

### A. 脚本文件

liunx\_security\_check.sh

offline.sh

### B. 检查内容

**Linux检查项：**

1.系统信息（系统版本，启动时间，内存情况，网络情况，系统文件）

2.异常用户

3.系统服务

4.开机启动项

5.计划任务

6.远程服务

7.进程列表

8.网络连接

9.异常文件

10.登录信息

11.网马脚本

12.系统关键文件

13.系统隐藏进程与端口

14.后门文件

15.系统日志

**Windows检查项：**

Windows 排查有文件排查，用户排查，进程排查，服务排查，日志排除。

文件排查：可以使用安全软件进行病毒以及后门网马的排查

用户排查：查看系统所有用户及创建时间。

进程排查：进程的异常表现有CPU，内存，文件位置，文件名称

服务排查：服务异常表现有名称，描述，启动类型

日志排除。重点是安全日志 ，服务日志 以及应用日志。从电脑管理找日志，然后导出查看更加方便。

## 4. 注意事项

脚本中的应用日志信息排查语句注释掉了。应用日志信息要根据进程及服务信息确定目录位置，然后使用脚本中的语句排查。

找到异常进程的PID之后，可ls –la /proc/pid 查看相关信息。结合lsof + L1，可发现更多信息。

注意保存截图，注意备份恶意文件。

根据脚本排查出的信息确定攻击的时间，然后根据时间再去查询对应日志，可把攻击梳理的更加清晰。

可以使用Strings 查看文件中的字符串，针对二进制文件，进程文件更有用。

Stat 输出说明：Access time(atime):是指取用文件的时间，所谓取用，常见的操作有：使用编辑器查看文件内容，使用cat命令显示文件内容，使用cp命令把该文件（即来源文件）复制成其他文件，或者在这个文件上运用grep sed more less tail head 等命令，凡是读取而不修改文件的操作，均衡改变文件的Access time.

Modify time(mtime)：是指修改文件内容的时间，只要文件内容有改动（如使用转向输出或转向附加的方式）或存盘的操作，就会改变文件的Modify time,我们使用ls–l查看文件时，显示是Modify time。

Change time(ctime):是指文件属性或文件位置改动的时间，如使用chmod，chown,mv指令集使用ln做文件的硬是连接，就会改变文件的Change time.

Note：如果修改文件（使用编辑器存盘或使用） >>转向操作）,则Modify time和Change time 会同步更新成写入的时间，但Access time不变。

如果执行touch文件，则3种时间全部改变。

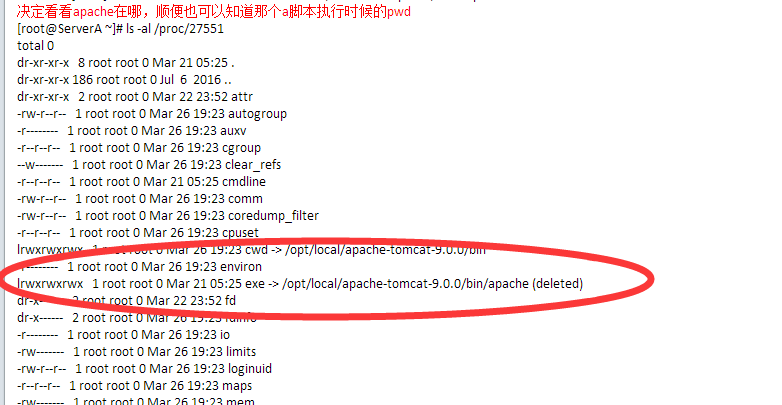
用ln –s做文件的软式连接，会改变文件的取用时间。

用ls –la查看一般文件不会更改这三种时间，但如果这个文件是符号链接，会改变（Access time）。

# 三、案例分享

## 1. 2017.3.28日A系统应急响应

找到的异常进程的pid，然后使用 Ls –la /proc/pid 查看详细



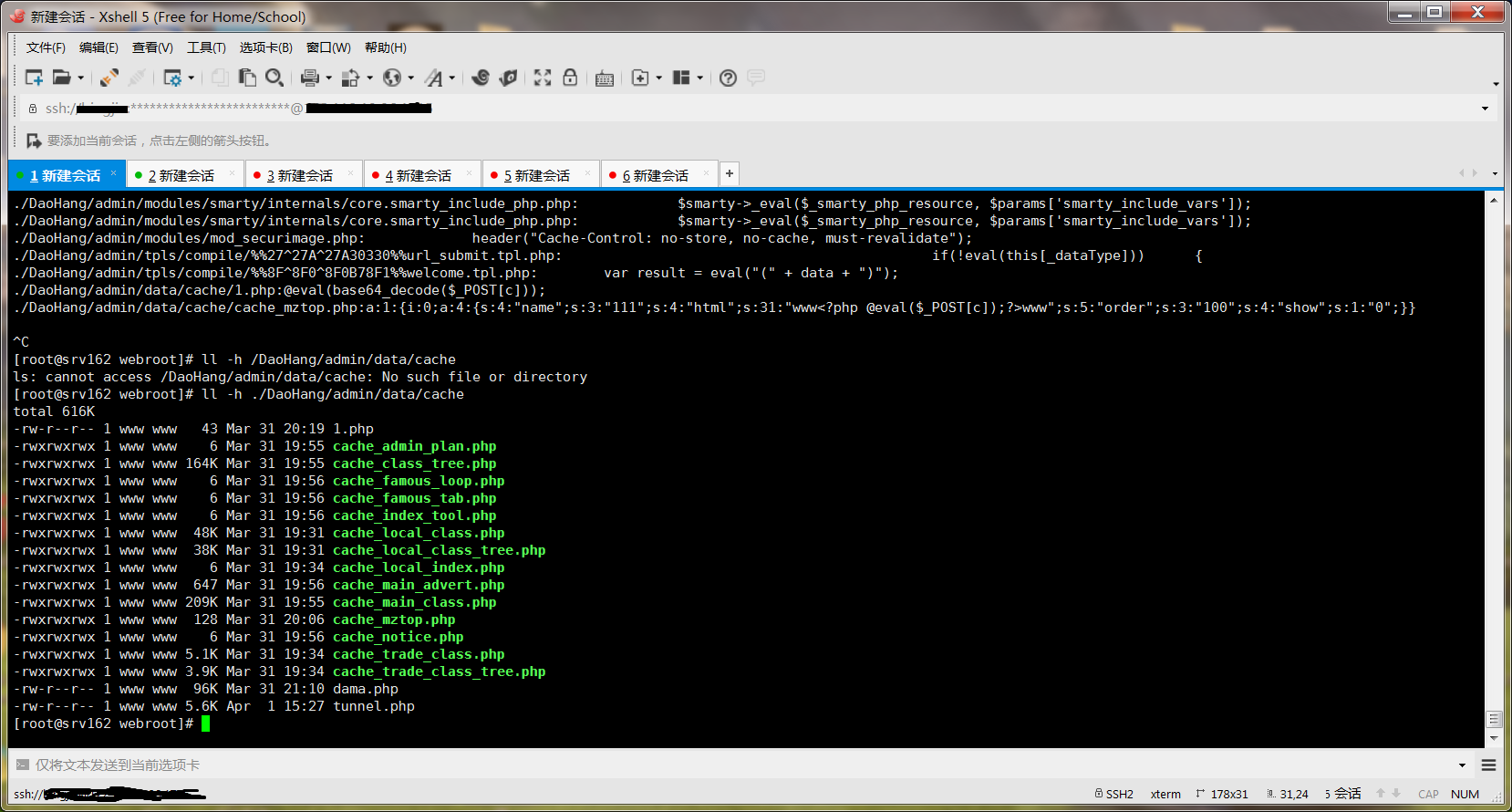
结合排查脚本查出struts2 的包



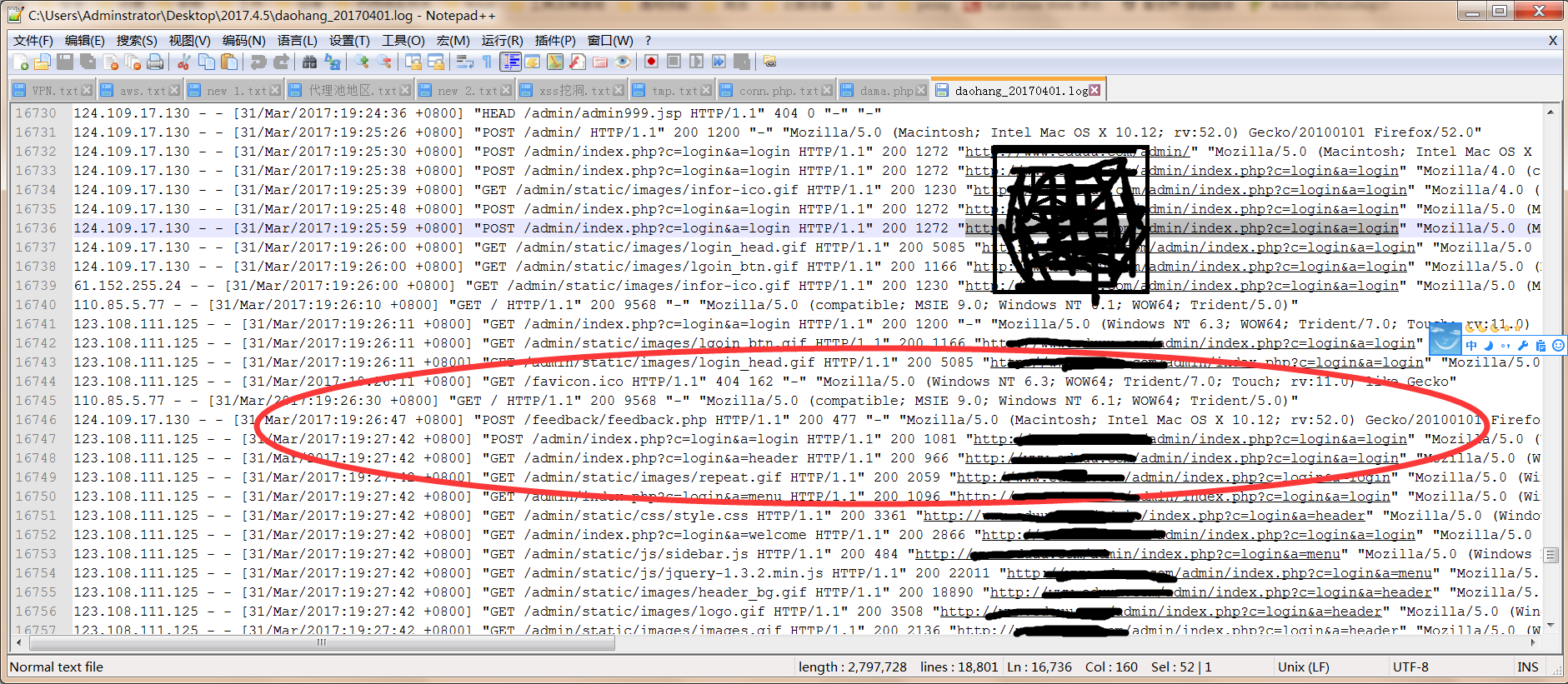
判断出这是因为struts 漏洞入侵的。遗憾的是当时没有找到对应的日志。

## 2. 2017.4.05日B系统应急响应

根据反弹shell 的异常进程信息，在日志中排查异常登录，命令执行。没有发现有价值信息。排查网马以及上传记录，发现4个网马文件。没有发现上传记录。



然后根据网马位置，找到对应的日期的日志文件，查看相应时间段内的记录



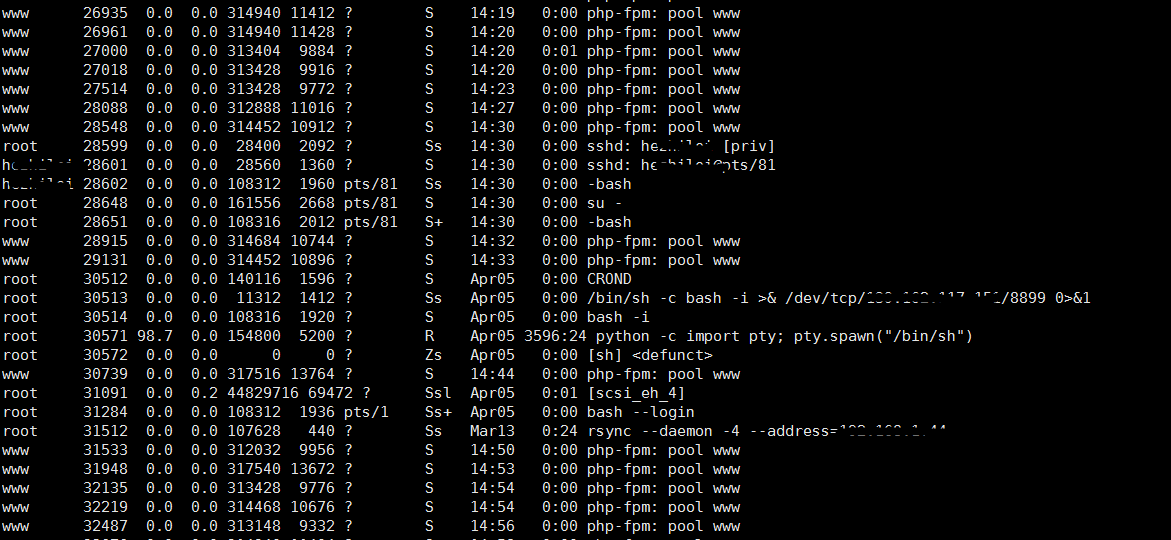
访问站点发现站点框架是 114啦网址导航，从上面日志可以看出其使用了两个组合漏洞达到了getshell的目的。使用feedback注入获取用户密码，然后登录后台，在后台getshell生成网马。

访问后来上传的大马文件，发现左侧提权里边反弹提权选项，可确定python异常进程是从这里发起的。

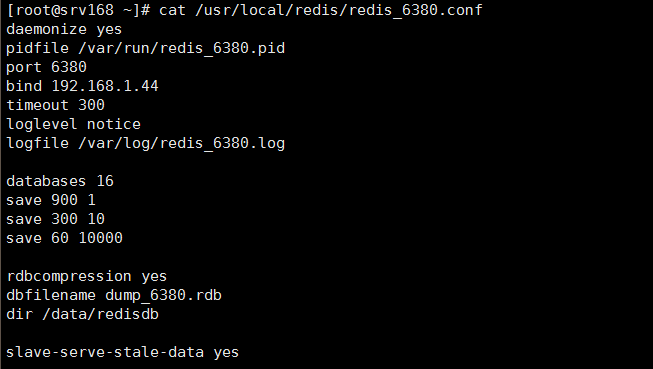


## 3. 2017.4.08日C系统应急响应

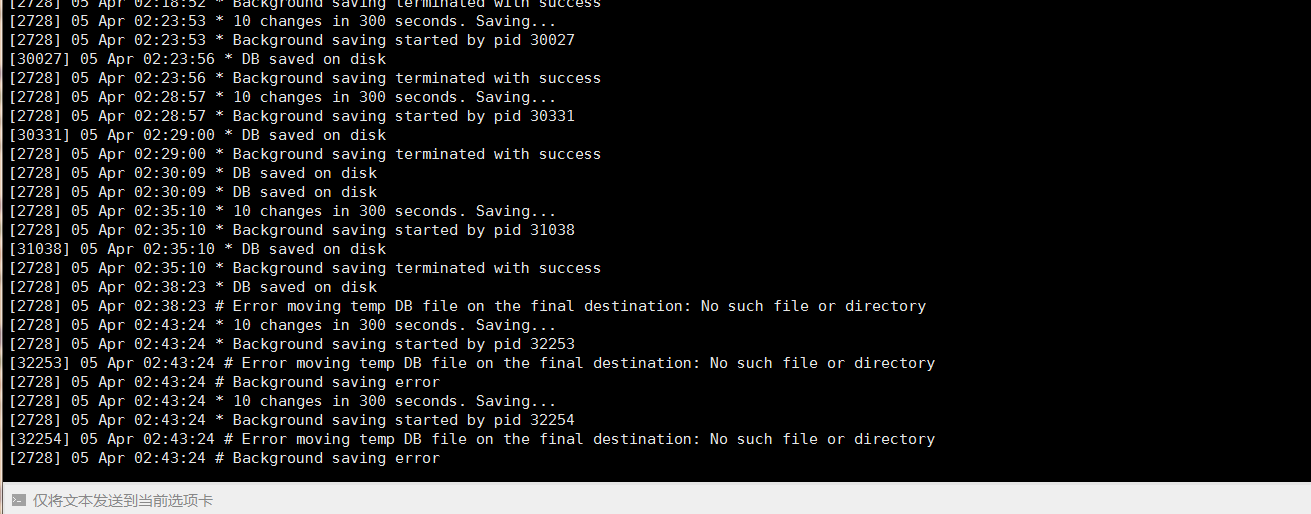
这是内网系统的入侵，跟上面的有联系。查看登录日志没有发现异常登录情况，恶意进程是反弹shell



发现redis 进程并且redis没有用户验证。



然后查看日志文件发现 数据库 改变的 异常信息

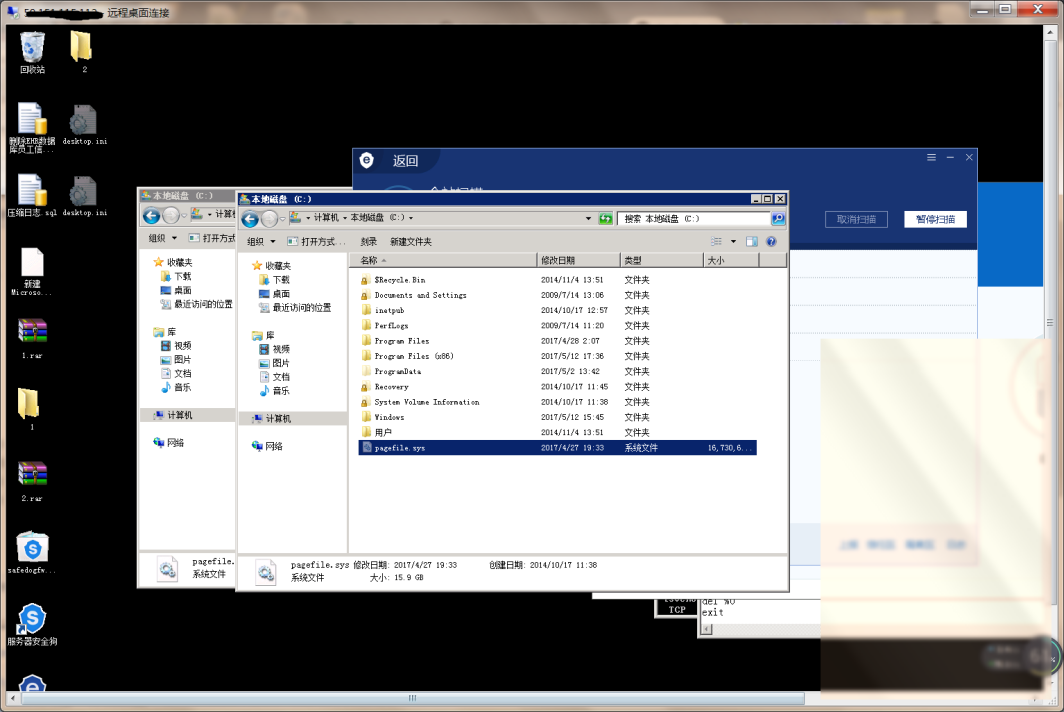


这里报错是因为其更改数据路径获取权限之后，登录机器将 auth 授权文件删除的报错。然后将系统文件替换成一些后门文件。网马查询语句还在系统中发现了一个2016年的网马文件。

## 4. 2017.5.12日D系统应急响应

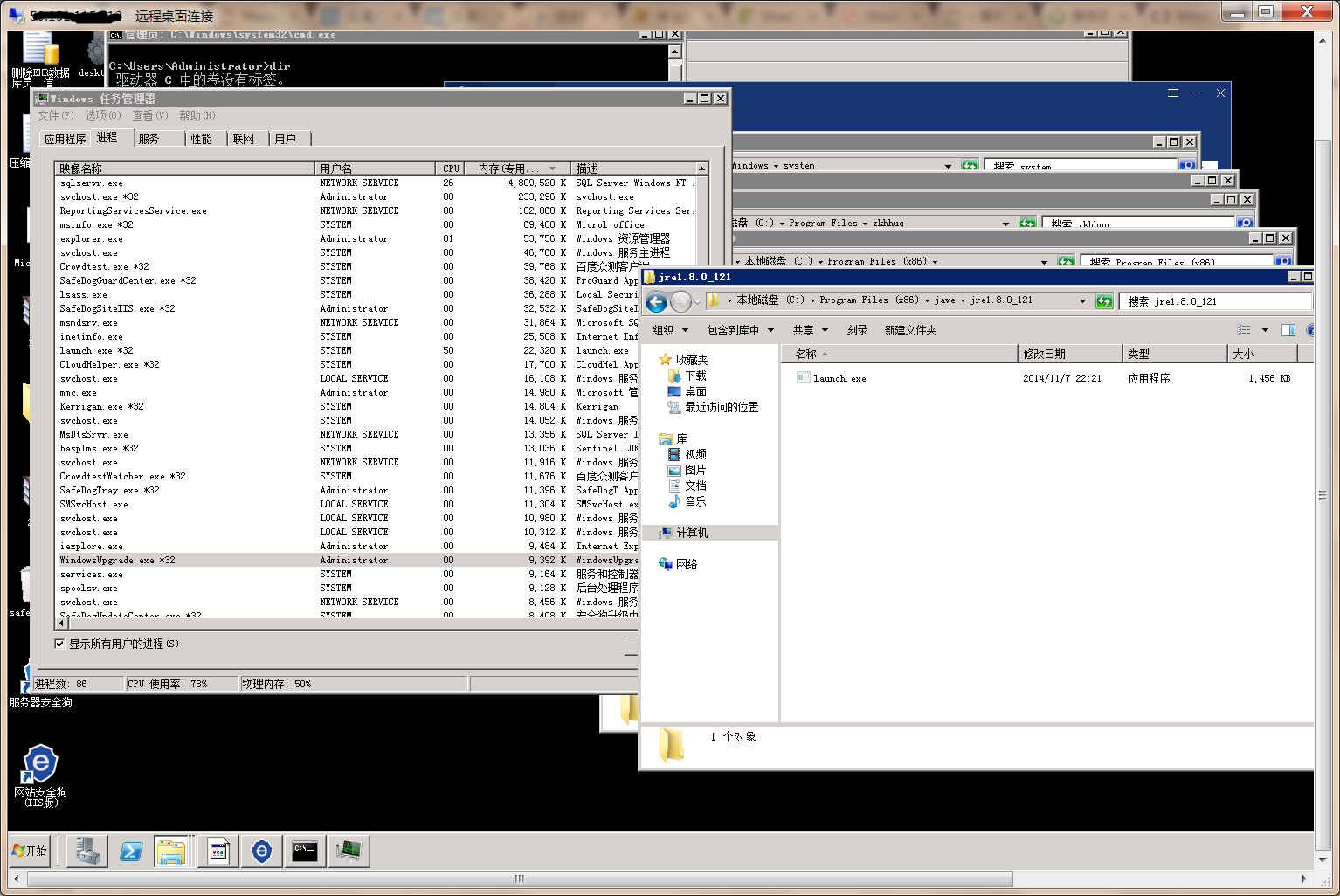
Windows机器，没有安装安全软件，没自动打补丁。使用安全狗扫描了下web目录，没有发现异常。

然后查看了下系统用户跟病毒文件，发现文件时间戳是2014.11.7。很早就被人入侵，用作挖矿了。这个进程的CPU使用率在50%。





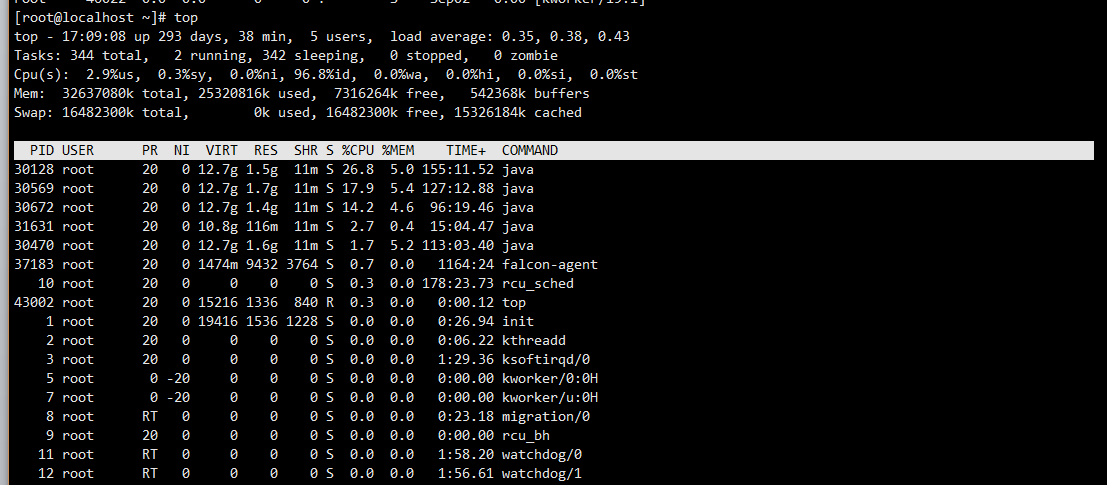
然后发现的流量异常怀疑是黑客重新登录机器传输大文件导致的。怀疑文件目标为：

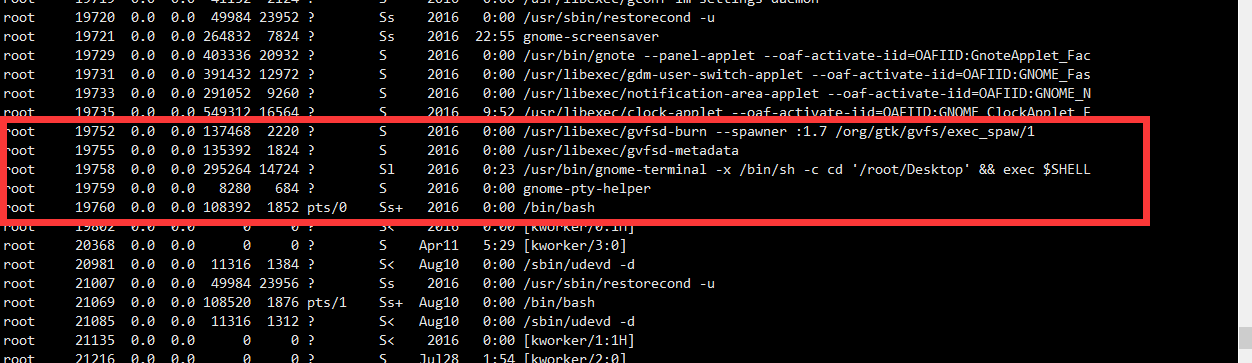


然后排查异常文件时间，发现时间跨度很大，有2014.11.7，2015，2017.4.20。猜测是不同黑客的多次入侵行为。怀疑通过系统漏洞进入。

## 5. 2017.6.27日应急响应

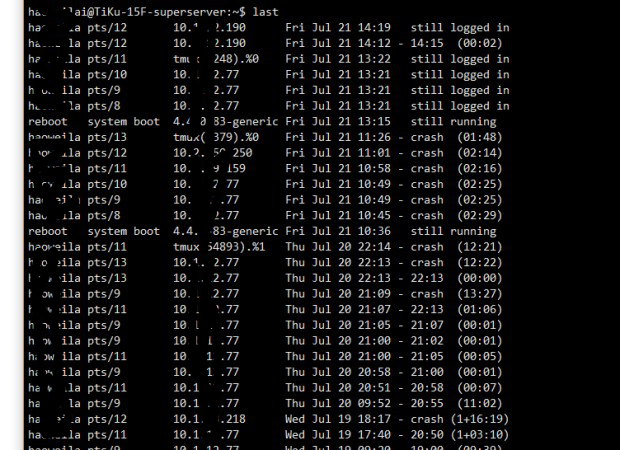
根据反馈，简单的排查了一下，发现是用户自己的问题。几个java进程的CPU使用不稳定：



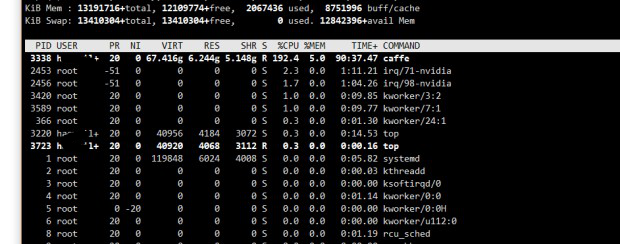


## 6. 2017.7.21日内网虚拟机应急响应

根据反馈，简单的看了下，发现是用户自己的问题。自己的session 复用不对，一直用着有问题的会话，导致崩溃频繁。然后就是自己程序的200% 的 cpu使用率过高。

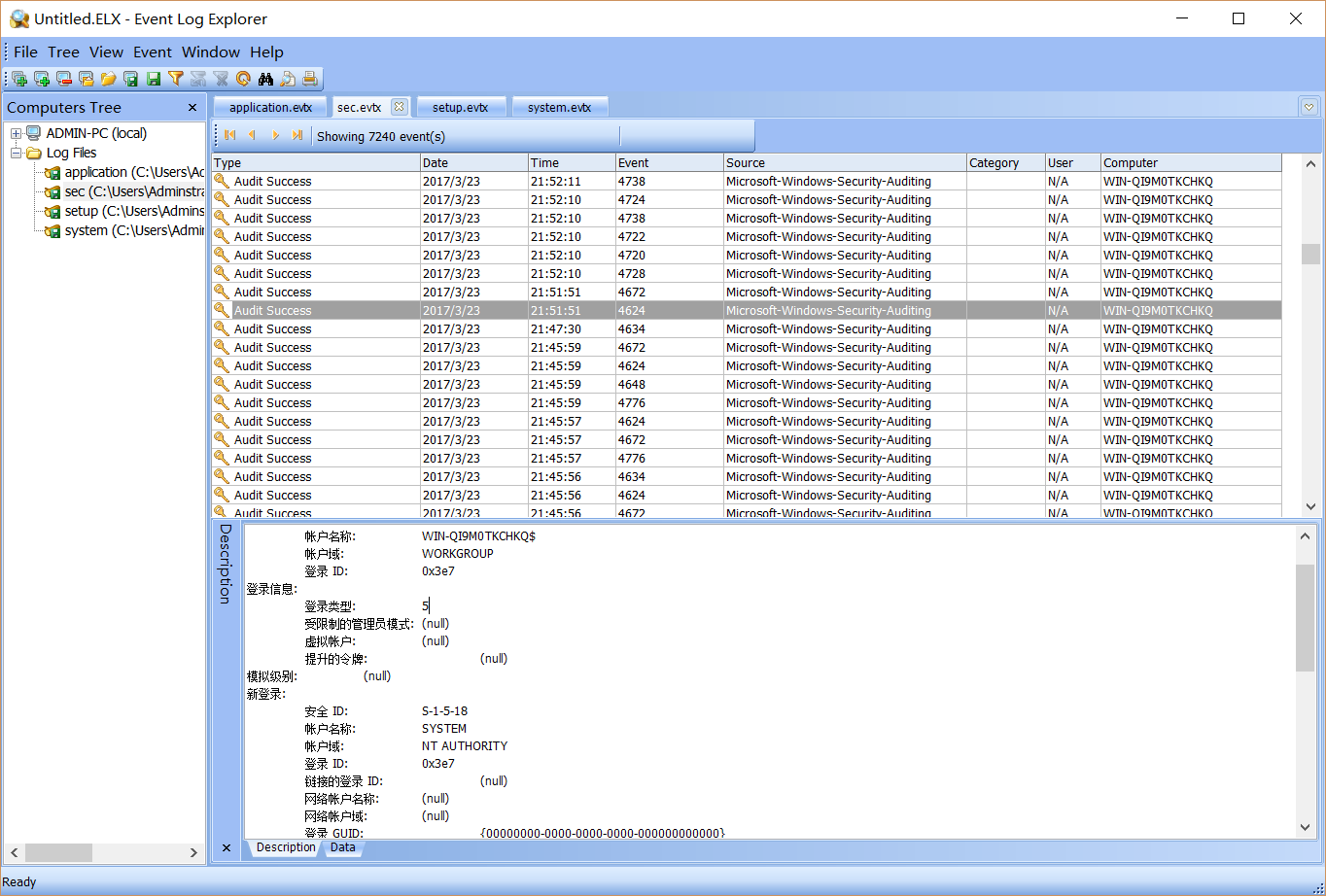




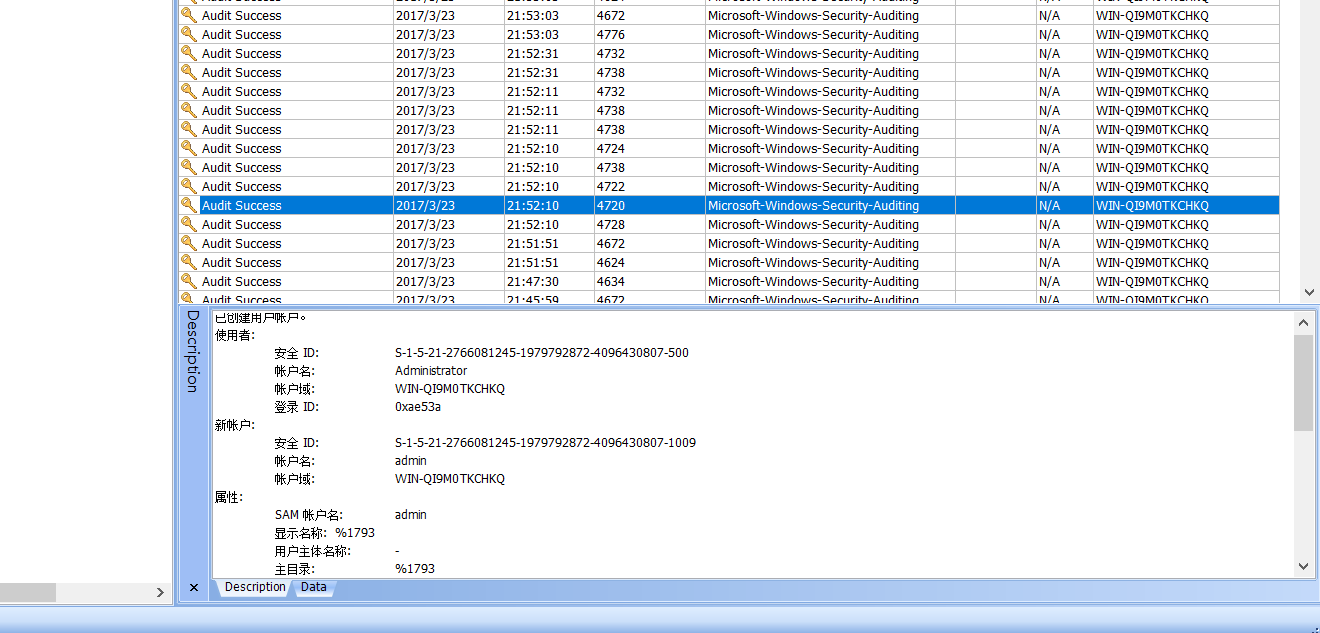


## 7. 2017.7.27日E系统排查

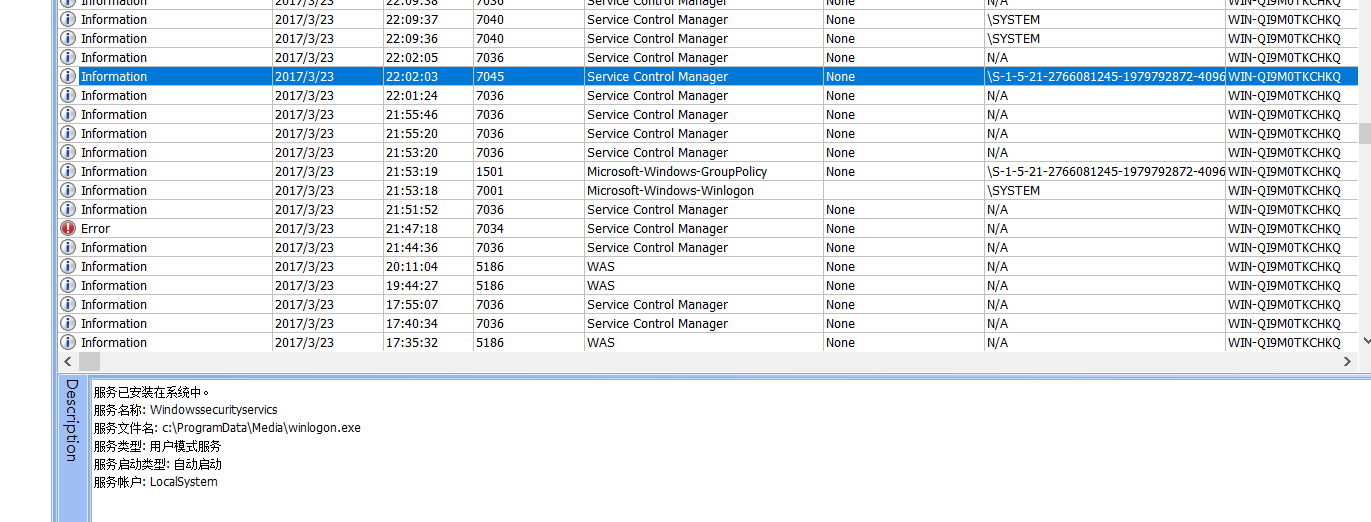
2台Linux机器，71，81。用脚本没发现问题，2台 window 机器，74，75历史被入侵过，重装75，74排查内容。4种日志结合排查，在异常行为时间点到其他日志中查找，相互结合可以判断入侵等恶意行为。2017.3.23，21:51:51从 WIN-K78VE784J3H 用Administrator 登陆机器，登录system之后：



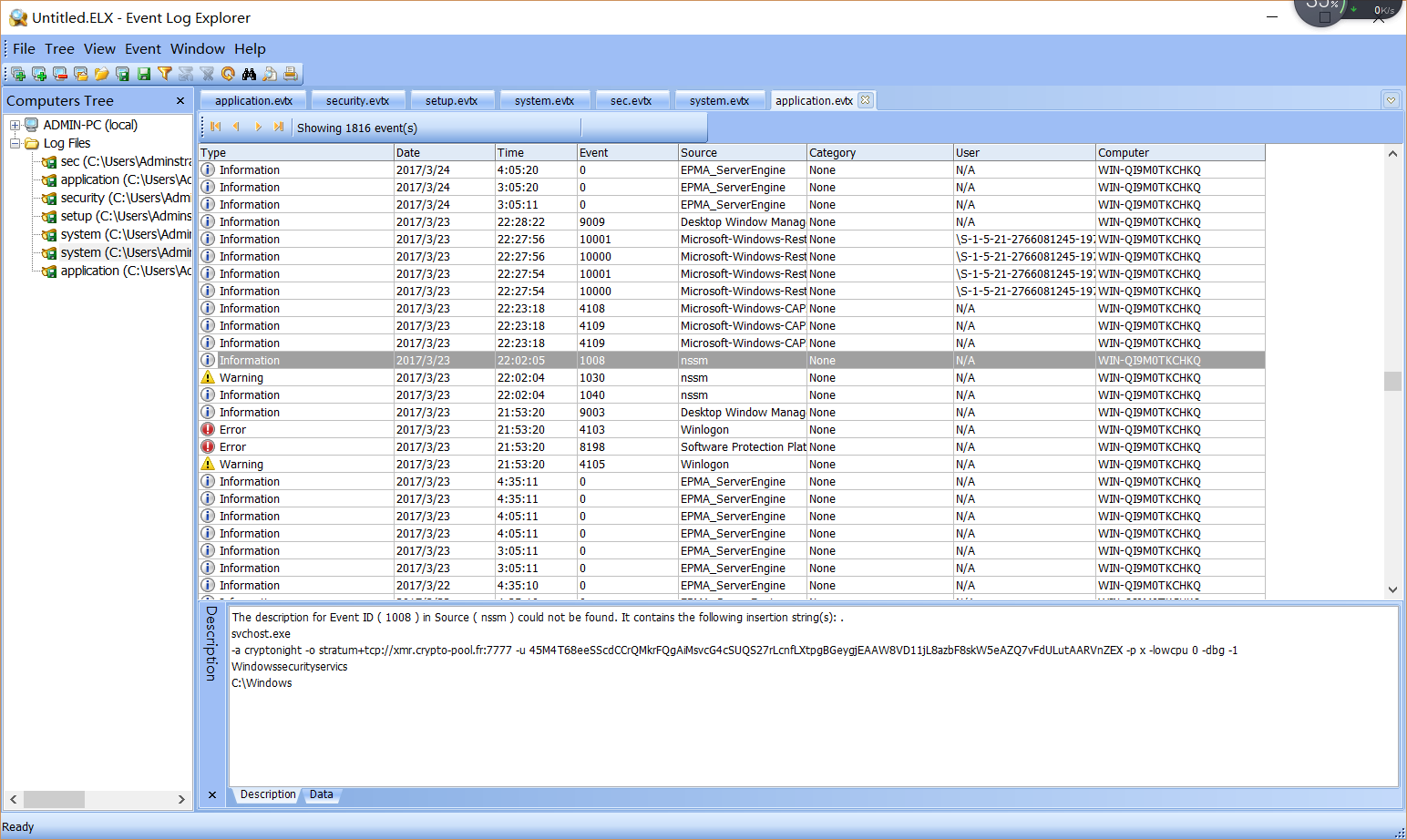
2017.3.23日21：52：10，创建新用户admin



改admin密码，切换到该用户。22：02：03安装恶意文件服务。C:\programData\media\winlogin.exe：

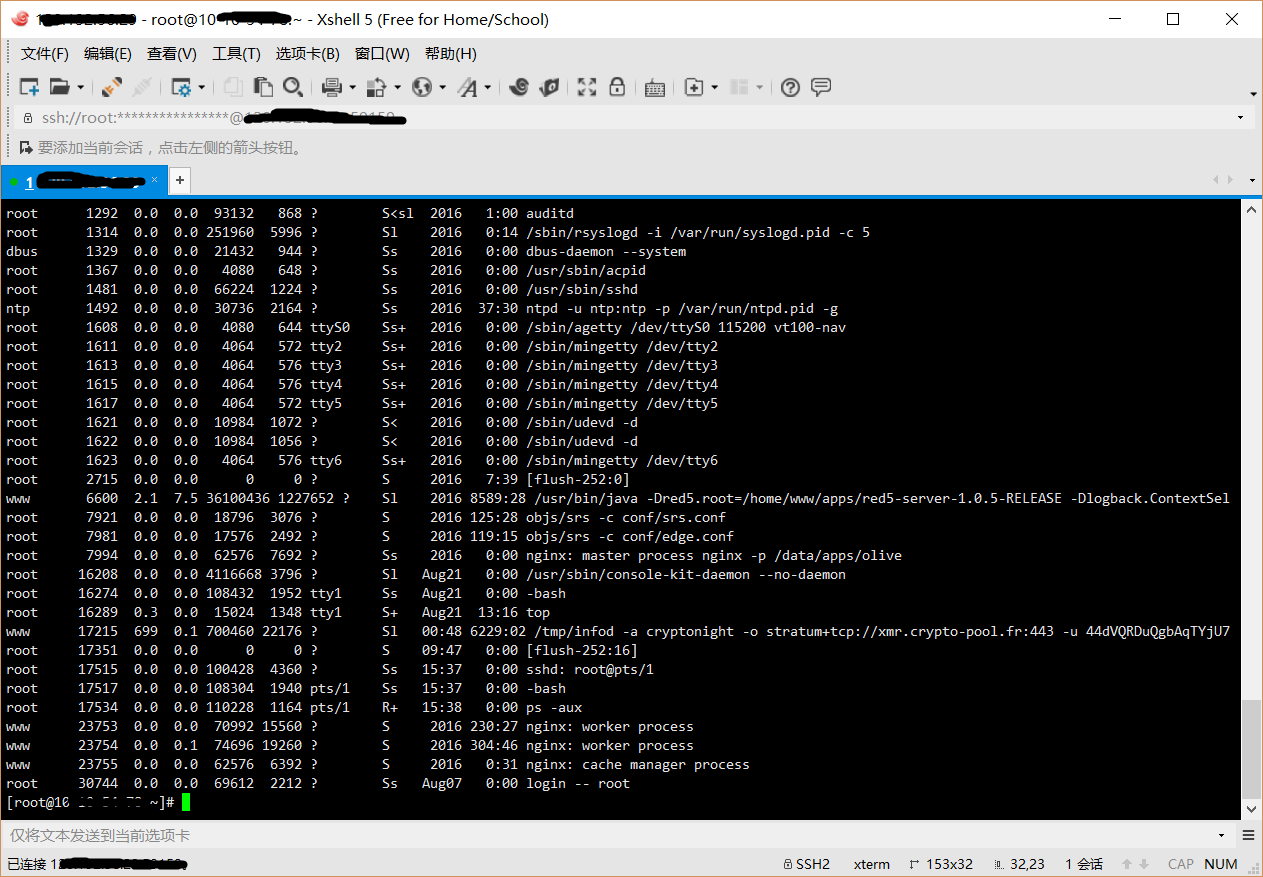


挖矿程序

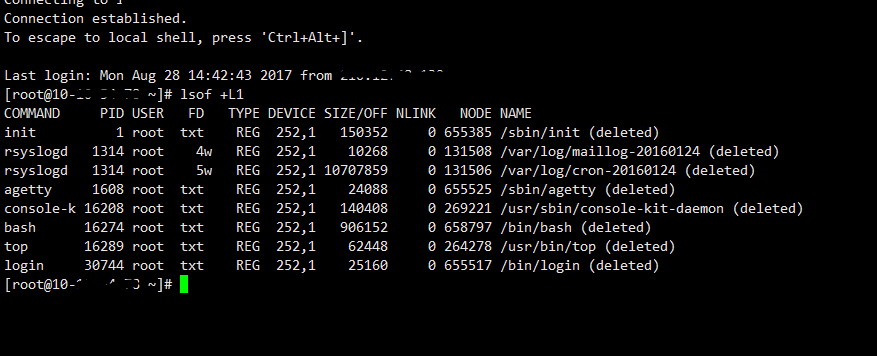


## 8. 2017.8.24日F系统应急排查

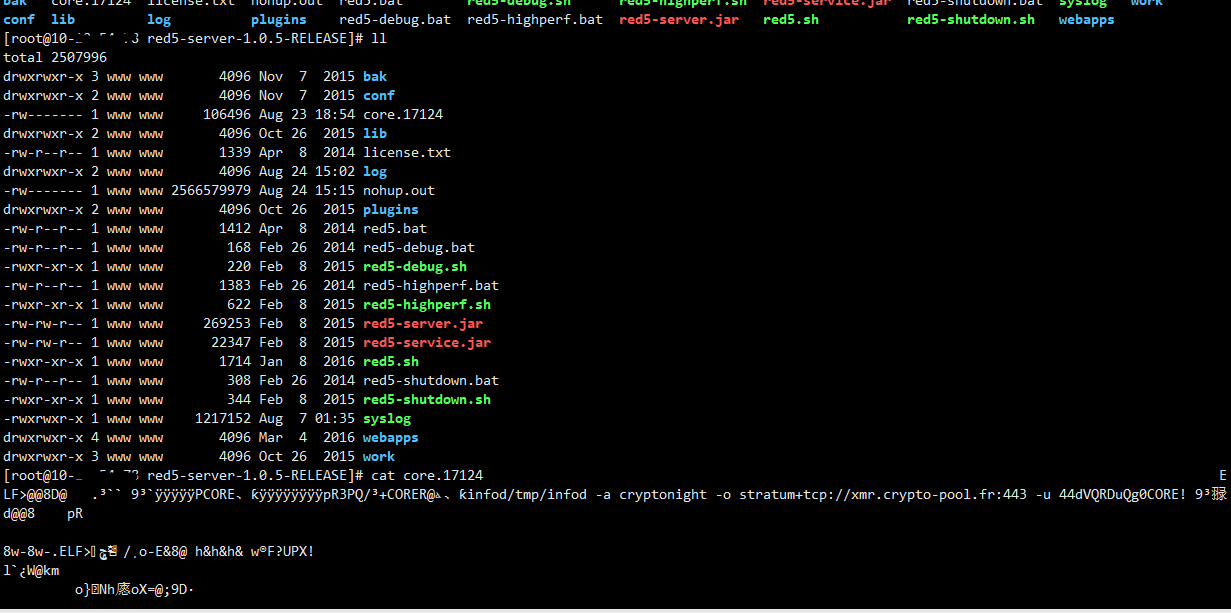
使用排查脚本发现的异常是



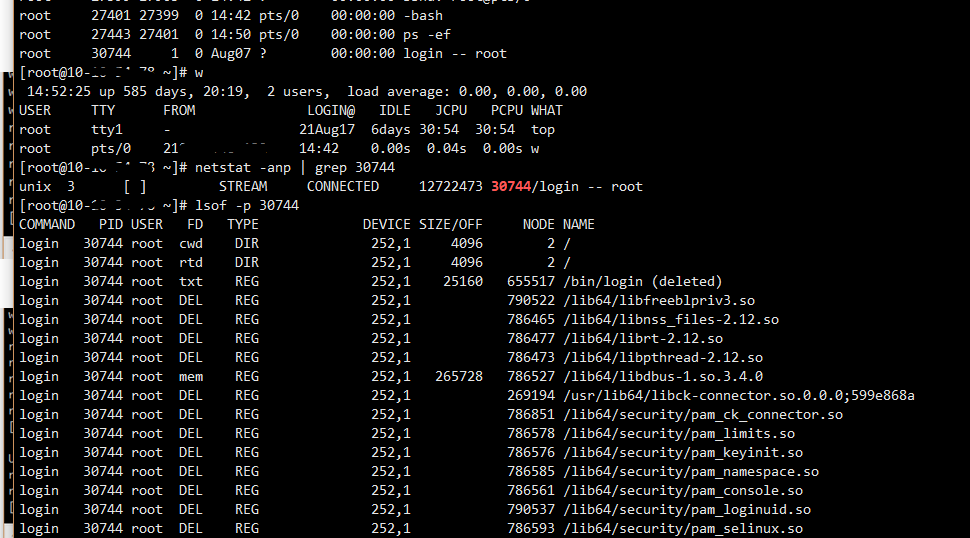
异常进程为挖矿程序，删除的程序文件：



挖矿进程的父进程ID 为1，正好对应上面的init程序。可以确定机器中被植入了病毒文件并且在启动之后就删掉了。排查脚本没有发现其他异常文件或记录。观察挖矿进程的用户信息发现是www用户启动，而另外一个www用户启动的进程是red5的视频服务程序。进入red5目录：



发现一个 core.17124 进程崩溃文件，查看文件内容，发现挖矿程序启动命令。到这里怀疑漏洞入口可能在red5 这里。使用挖矿相关字符串 匹配应用服务日志，没有任何匹配，查看异常进程信息。



从这些异常进程相关文件得到几个时间点：2016，2017.3.22，2017.8.7，2017.8.21，不确定入侵时间，也没有找到任何漏洞信息。也没有合理怀疑。

# 四、复盘：

第一个案例检查的不彻底，不系统，没有脚本只能想到什么检查什么。

现在有了检查脚本就应该注意检查的系统性。

第二三个案例，在内网环境的应急排查要注意内网机器的相关性跟入侵扩散的可能性。

相关性在前期的信息收集表中已经加上了。

下一步升级的计划是看看有没有方法获取机器对内网的扫描或入侵行为。（history记录等）

第四个案例，尝试下内核漏洞的攻击，排查服务组件攻击，排查系统日志

第五六个案例，前期信息收集到位的话可以避免很多无用功，简单的命令即可确定问题。

第七个案例，查看日志的时候记录详细时间点，然后注意各日志时间点间的关联，可以排除入侵行为与普通系统异常。

第八个案例，第一遍排查没有发现异常的时候，要多注意已经获取的各信息之间的关联。可以打开思路，确定排查方向。

第九个案例，不要完全相信运维人员给出的信息，这次给出的信息只有一台服务器，没想到测试服务器（另一个业务线）也有问题，这次是跨业务线的传播病毒。同时，应急前一定要确认运维人员“全部”具体操作（包括删除的文件具体信息），方便做出最正确的判断。

应急响应完成之后应该建一个工单，督促提醒业务线重装系统。