Invoke-Obfuscation-Bypass + PS2EXE 绕过 主流杀软

本文通过混淆器对 cs 生成的 powershell 文件进行混淆,并打包成 exe 的方式,来绕过主流杀软,提供一个简单思路

项目地址:

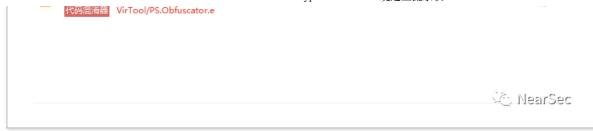
https://github.com/AdminTest0/Invoke-Obfuscation-Bypass

原混淆器运行后, 某 60 云查杀会报毒 11 个文件



某绒会报毒 4 个文件





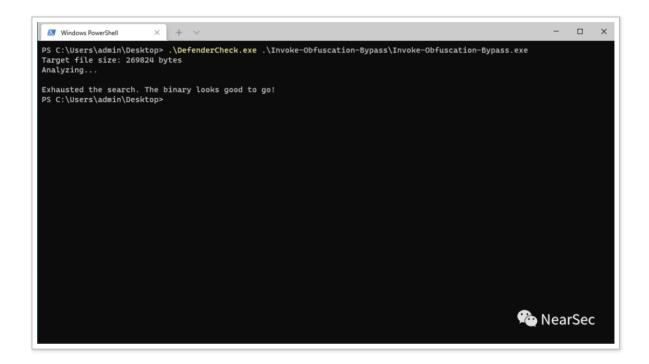
将原项目中的以下文件混淆后进行测试

```
Invoke-Obfuscation.ps1
Out-EncodedAsciiCommand.ps1
Out-EncodedBinaryCommand.ps1
Out-EncodedHexCommand.ps1
Out-CompressedCommand.ps1
Out-EncodedBXORCommand.ps1
Out-EncodedOctalCommand.ps1
Out-ObfuscatedStringCommand.ps1
Out-PowerShellLauncher.ps1
Out-SecureStringCommand.ps1
Out-EncodedWhitespaceCommand.ps1
```

再次运行不会被拦截



将 Invoke-Obfuscation-Bypass 打包成 exe, 绕过 defender



下面通过 Invoke-Obfuscation-Bypass 对 powershell 文件进行混淆

用 cs 生成 powershell 的 payload



用 powershell 启动 Invoke-Obfuscation-Bypass.exe,或者双击打开,会在同目录生成混淆后的 Invoke-Obfuscation

```
HELP MENU :: Available options shown below:
                                                                                                                                           Tutorial of how to use this tool
Show this Help Menu
Show options for payload to obfuscate
Clear screen
Execute ObfuscatedCommand locally
Copy ObfuscatedCommand to clipboard
Write ObfuscatedCommand Out to disk
Reset AlL obfuscation for ObfuscatedCo
Undo LAST obfuscation for ObfuscatedCo
Go Back to previous obfuscation menu
Quit Invoke-Obfuscation
Return to Home Menu
                                                                                   2021/8/22 11:16
                                                                                                                                                                                                                                                                              TUTORIAL
HELP,GET-HELP,?,-?,/?,MENU
SHOW OPTIONS,SHOW,OPTIONS
CLEAR,CLEAR-HOST,CLS
EXEC,EXECUTE,TEST,RUN
COPY,CLIP,CLIPBOARD
Invoke-Obfuscation.psd1
Invoke-Obfuscation.psm1
Invoke-Obfuscation-Bypass.exe
                                                                                   2021/8/22 11:16
2021/8/22 11:16
2021/8/22 11:10
 Out-EncodedAsciiCommand.ps1
Out-EncodedAsciiCommand.ps1
Out-EncodedBinaryCommand.ps1
                                                                                   2021/8/22 11:16
                                                                                   2021/8/22 11:16 2021/8/22 11:16
  Out-EncodedBXORCommand.ps1
                                                                                   2021/8/22 11:16

    Out-EncodedHexCommand.ps1
    Out-EncodedOctalCommand.ps1

                                                                                   2021/8/22 11:16
  Out-EncodedSpecialCharOnlyComma... 2021/8/22 11:16

    Out-EncodedWhitespaceCommand.p...
    Out-ObfuscatedAst.ps1

    Out-ObfuscatedStringCommand.ps1

                                                                                                                                  Choose one of the below options:
                                                                                2021/8/22 11:16

        @ Out-ObfuscatedTokenCommand.ps1

      2021/8/22 11:16

        @ Out-PowerShellLauncher.ps1

      2021/8/22 11:16

                                                                                                                                                                            Obfuscate PowerShell command Tokens
Obfuscate PowerShell Ast nodes (P53.8+)
Obfuscate entire command as a String
Obfuscate entire command via Encoding
Convert entire command to one-Liner and Compress
Obfuscate command args w/Launcher techniques (run once at end)
 Out-SecureStringCommand.ps1
                                                                                 2021/8/22 11:16
                                                                                                                                                                                                                                                                                                                                                                         🕰 NearSec
```

依次输入选项进行混淆(其他混淆方式自测)

```
set scriptpath C:\Users\用户名\Desktop\payload.ps1
token
all
```

```
Involve-Obfascation/STAILID set scriptpath C:\Users\adein\Desktep\payload.psi

Successfully set Scriptpath
C:\Users\adein\Desktep\payload.psi

Successfully set Scriptpath
C:\Users\adein\Desktep\payload.psi

[c] Scripts\Desktep\Desktep\payload.psi

[r] ASTAILID: Execute ALL Ast obfascation techniques

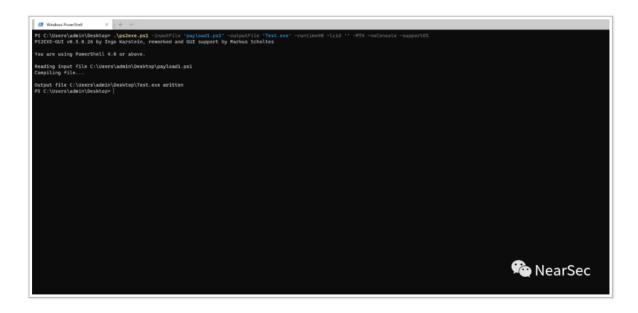
Involve-Obfascation\Users\Adein\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\Desktep\
```

导出混淆后的 payload

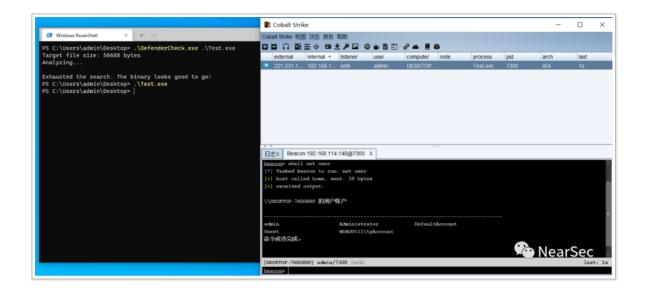
```
out ..\payload1.ps1
```

使用 ps2exe 将混淆后的 ps1 文件转为 exe

.\ps2exe.ps1 -inputFile 'payload1.ps1' -outputFile 'Test.exe' -runtime40 -lcid '' -MTA -noConsole -support0S



绕过 defender 动态



参考链接:

https://github.com/danielbohannon/Invoke-Obfuscation

https://github.com/MScholtes/TechNet-Gallery/blob/master/PS2EXE-GUI/ps2exe.ps1

https://github.com/cseroad/bypassAV