Invoke-Obfuscation-Bypass + PS2EXE 绕过主流杀软

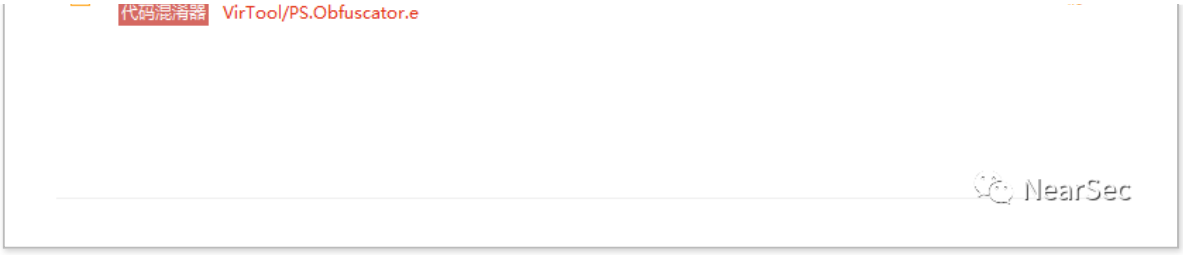
本文通过混淆器对 cs 生成的 powershell 文件进行混淆，并打包成 exe 的方式，来绕过主流杀软，提供一个简单思路

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

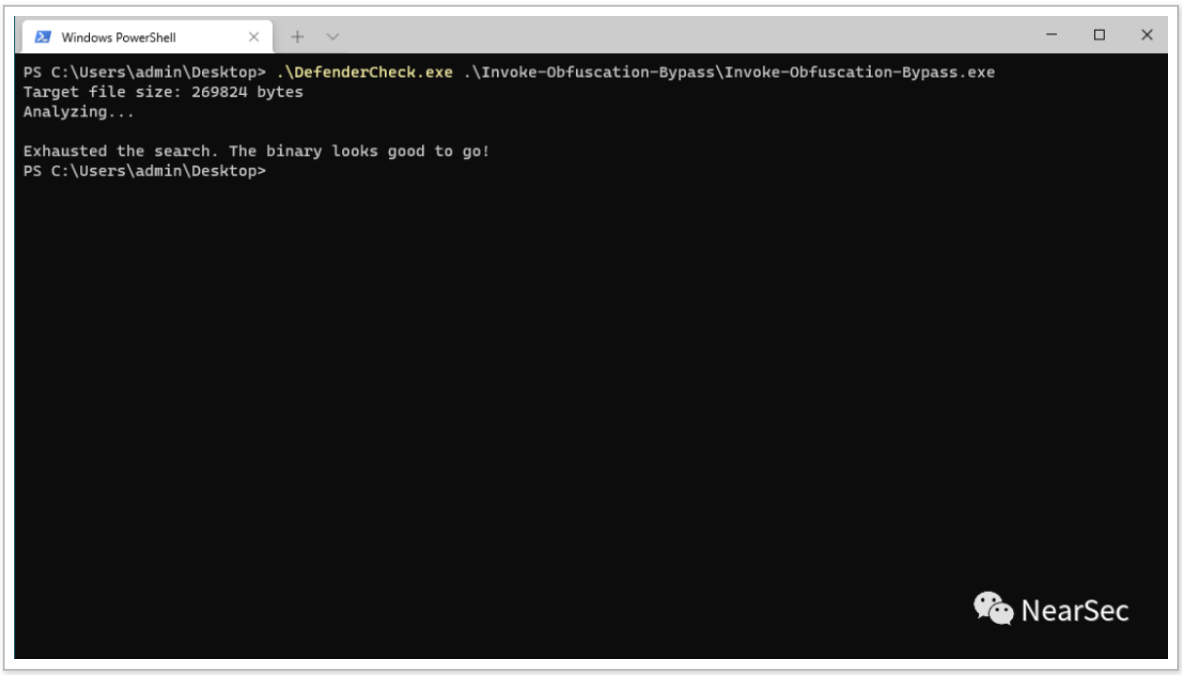


将原项目中的以下文件混淆后进行测试

```
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
```

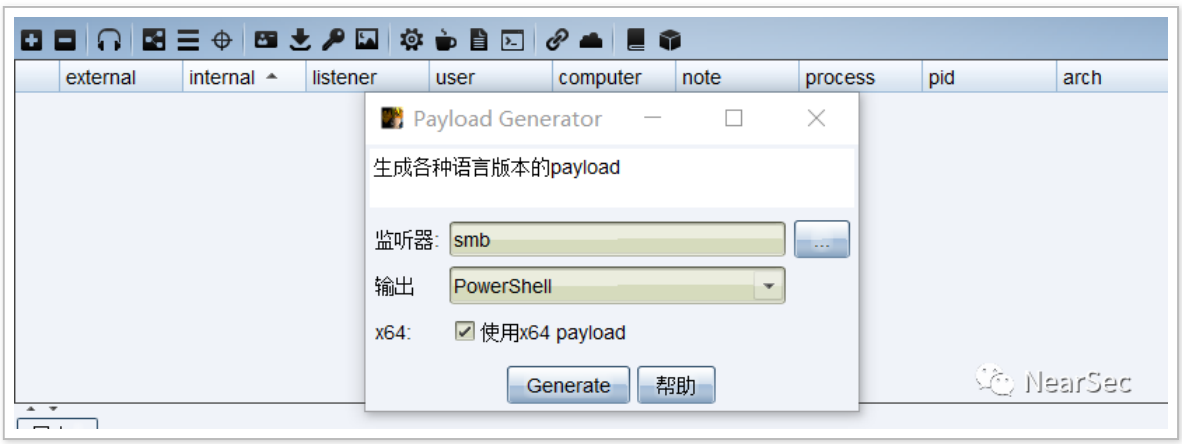
再次运行不会被拦截

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

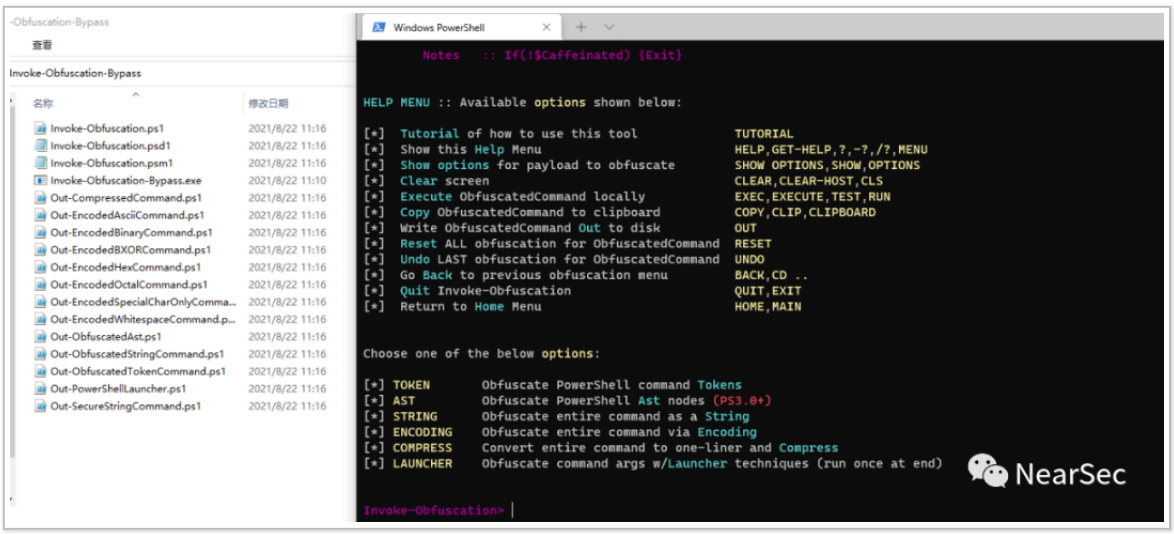


下面通过 Invoke-Obfuscation-Bypass 对 powershell 文件进行混淆

用 cs 生成 powershell 的 payload

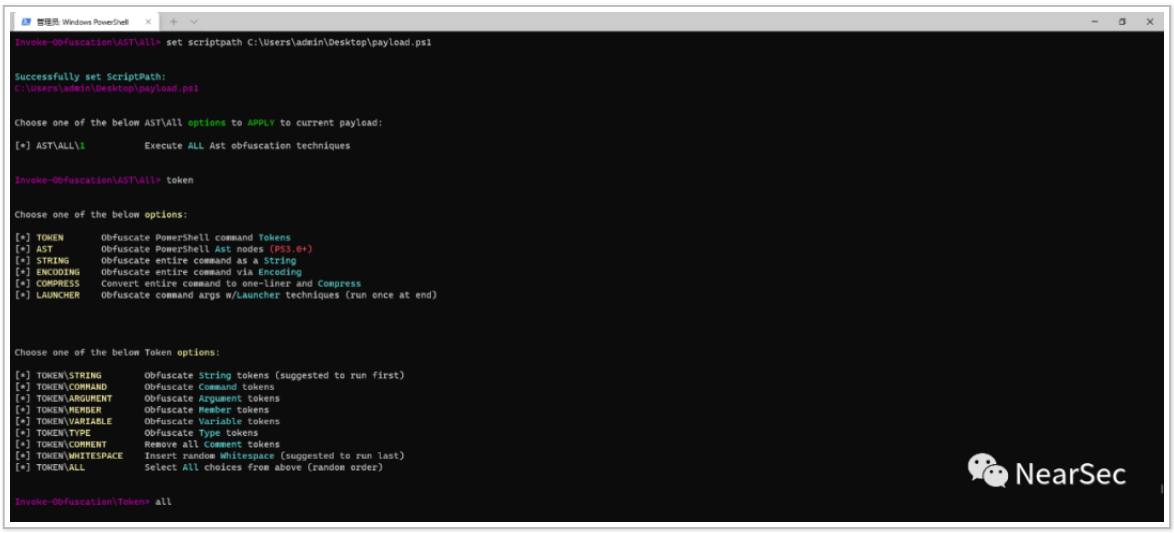


用 powershell 启动 Invoke-Obfuscation-Bypass.exe，或者双击打开，会在同目录生成混淆后的 Invoke-Obfuscation



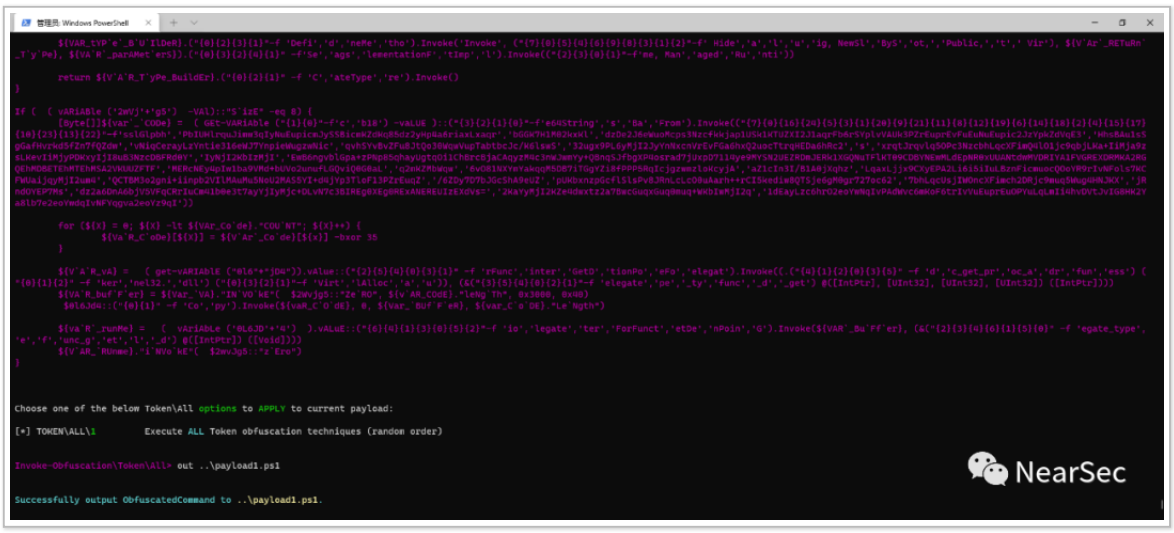
依次输入选项进行混淆（其他混淆方式自测）

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



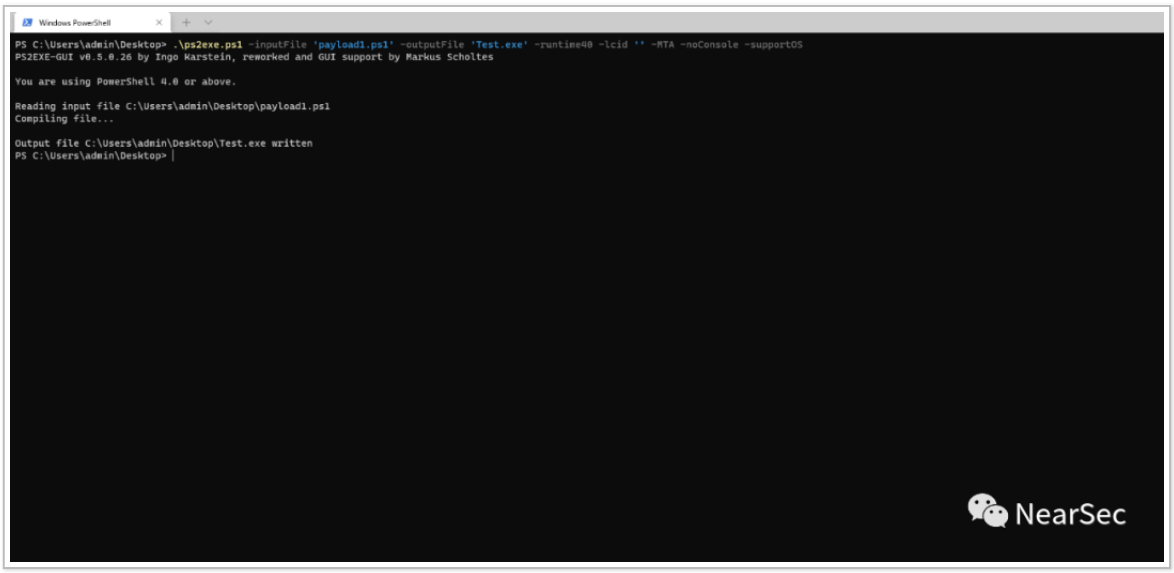
导出混淆后的 payload

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

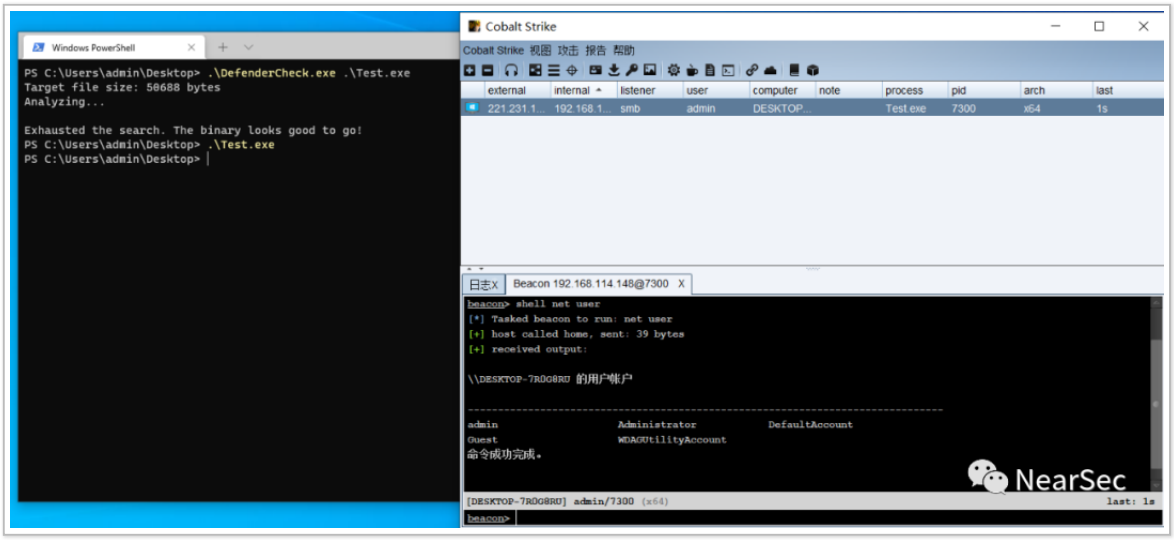


使用 ps2exe 将混淆后的 ps1 文件转为 exe

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



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