

[ASM] Windows Toolkit

Introduction

Cette page va vous donner toutes les ressources nécessaires pour préparer votre environnement de développement de Malware sur Windows 10.

Outils

- **Visual Studio** avec la suite de "Développement desktop en C++" (SDK).
- **x64dbg** (pour débbuger).
- **IDA Freeware**.

Script de compilation

x64

```
@echo off
set /p prog=[+] program name (without extension):
"C:\Program Files\Microsoft Visual
Studio\2022\Community\VC\Tools\MSVC\14.39.33519\bin\Hostx64\x64\ml64.exe" ^
%prog%.asm /link /subsystem:windows ^
/defaultlib:"C:\Program Files (x86)\Windows Kits\10\Lib\10.0.22621.0\um\x64\ntdll.lib" ^
/defaultlib:"C:\Program Files (x86)\Windows Kits\10\Lib\10.0.22621.0\um\x64\kernel32.lib" ^
/defaultlib:"C:\Program Files (x86)\Windows Kits\10\Lib\10.0.22621.0\um\x64\user32.lib" ^
/entry:Start ^
/LARGEADDRESSAWARE:NO ^
/out:%prog%.exe ^
/RELEASE
del %prog%.obj
del *.lnk
```

pause

x32

```
@echo off
set /p prog=[+] program name (without extension):
"C:\Program Files\Microsoft Visual Studio\2022\Community\VC\Tools\MSVC\14.43.34808\bin\Hostx64\x86\ml.exe"
^
%prog%.asm /link /subsystem:windows ^
/defaultlib:"C:\Program Files (x86)\Windows Kits\10\Lib\10.0.22621.0\um\x86\ntdll.lib" ^
/defaultlib:"C:\Program Files (x86)\Windows Kits\10\Lib\10.0.22621.0\um\x86\kernel32.lib" ^
/defaultlib:"C:\Program Files (x86)\Windows Kits\10\Lib\10.0.22621.0\um\x86\user32.lib" ^
/defaultlib:"C:\Program Files (x86)\Windows Kits\10\Lib\10.0.22621.0\um\x86\Ws2_32.lib" ^
/entry:Start ^
/LARGEADDRESSAWARE:NO ^
/out:%prog%.exe ^
/RELEASE
del %prog%.obj
del *.lnk
pause
```

Vérifiez les chemins en remplaçant les numéros de version puis ajoutez vos DLL si besoin avec l'argument **defaultlib** .

Hello world

Voici un hello world pour vérifier que la compilation fonctionne correctement :

```
extrn MessageBoxA :PROC
extrn ExitProcess :PROC

.data
msg DB "Hello world", 0
caption DB "Caption", 0

.code
Start PROC
sub rsp, 28h
```

```
⌘XOR rcx, rcx
⌘LEA rdx, msg
⌘LEA r8, caption
⌘XOR r9, r9
⌘CALL MessageBoxA
⌘CALL ExitProcess
Start ENDP
```

End

Revision #4

Created 30 July 2024 08:30:39 by Elieroc

Updated 1 April 2025 12:32:24 by Elieroc