

/Ilasm.exe

Compile

used for compile c# code into dll or exe.

Paths:

C:\Windows\Microsoft.NET\Framework\v4.0.30319\ilasm.exe
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ilasm.exe

Resources:

- https://github.com/LuxNoBullshit/BeforeCompileBy-ilasm/blob/master/hello_world.txt

Acknowledgements:

- Hai Vaknin(Lux) ([@VakninHai](#))
- Lior Adar

Detections:

- IOC: Ilasm may not be used often in production environments (such as on endpoints)
- Sigma:

https://github.com/SigmaHQ/sigma/blob/bea6f18d350d9c9fdc067f93dde0e9b11cc22dc2/rules/windows/process_creation/proc_creation_win_lolbin_ilasm.yml

Compile

. Binary file used by .NET to compile C#/intermediate (IL) code to .exe

```
ilasm.exe C:\public\test.txt /exe
```

Use case: Compile attacker code on system. Bypass defensive counter measures.
Privileges required: User
Operating systems: Windows 7, Windows 10, Windows 11
ATT&CK® technique: T1127

. Binary file used by .NET to compile C#/intermediate (IL) code to dll

```
ilasm.exe C:\public\test.txt /dll
```

Use case: A description of the usecase
Privileges required: User
Operating systems: Windows 7, Windows 10, Windows 11
ATT&CK® technique: T1127