



# /Dotnet.exe ☆ Star 7,060

[AWL bypass](#) [Execute](#)

dotnet.exe comes with .NET Framework

### Paths:

C:\Program Files\dotnet\dotnet.exe

### Resources:

- [https://twitter.com/\\_felamos/status/1204705548668555264](https://twitter.com/_felamos/status/1204705548668555264)
- <https://gist.github.com/bohops/3f645a7238d8022830ecf5511b3ecfbc>
- <https://bohops.com/2019/08/19/dotnet-core-a-vector-for-awl-bypass-defense-evasion/>
- <https://learn.microsoft.com/en-us/dotnet/fsharp/tools/fsharp-interactive/>

### Acknowledgements:

- felamos ([@\\_felamos](#))
- Jimmy ([@bohops](#))
- yamalon ([@mavinject](#))

### Detections:

- Sigma: [proc\\_creation\\_win\\_lolbin\\_dotnet.yml](#)
- BlockRule: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules>
- IOC: dotnet.exe spawned an unknown process

## AWL bypass

1. dotnet.exe will execute any dll even if applocker is enabled.

```
dotnet.exe [PATH_TO_DLL]
```

**Use case:** Execute code bypassing AWL  
**Privileges required:** User  
**Operating systems:** Windows 7 and up with .NET installed  
**ATT&CK® technique:** [T1218: System Binary Proxy Execution](#)

2. dotnet.exe with msbuild (SDK Version) will execute unsigned code

```
dotnet.exe msbuild [Path_TO_XML_CSPROJ]
```

**Use case:** Execute code bypassing AWL  
**Privileges required:** User  
**Operating systems:** Windows 10 and up with .NET Core installed  
**ATT&CK® technique:** [T1218: System Binary Proxy Execution](#)

## Execute

1. dotnet.exe will execute any DLL.

```
dotnet.exe [PATH_TO_DLL]
```

**Use case:** Execute DLL  
**Privileges required:** User  
**Operating systems:** Windows 7 and up with .NET installed  
**ATT&CK® technique:** [T1218: System Binary Proxy Execution](#)

2. dotnet.exe will open a console which allows for the execution of arbitrary F# commands

```
dotnet.exe fsi
```

**Use case:** Execute arbitrary F# code  
**Privileges required:** User  
**Operating systems:** Windows 10 and up with .NET SDK installed  
**ATT&CK® technique:** [T1059: Command and Scripting Interpreter](#)