



# /Devtoolslauncher.exe ☆ Star 7,060

Execute

Binary will execute specified binary. Part of VS/VScode installation.

### Paths:

c:\windows\system32\devtoolslauncher.exe

### Resources:

- [https://twitter.com/\\_felamos/status/1179811992841797632](https://twitter.com/_felamos/status/1179811992841797632)

### Acknowledgements:

- felamos ([@\\_felamos](#))

### Detections:

- Sigma: [proc\\_creation\\_win\\_lolbin\\_devtoolslauncher.yml](#)
- IOC: DeveloperToolsSvc.exe spawned an unknown process

## Execute

1. The above binary will execute other binary.

```
devtoolslauncher.exe LaunchForDeploy [PATH_TO_BIN] "argument here" test
```

**Use case:** Execute any binary with given arguments and it will call developertoolssvc.exe. developertoolssvc is actually executing the binary.

**Privileges required:** User

**Operating systems:** Windows 7 and up with VS/VScode installed

**ATT&CK® technique:** [T1127: Trusted Developer Utilities Proxy Execution](#)

2. The above binary will execute other binary.

```
devtoolslauncher.exe LaunchForDebug [PATH_TO_BIN] "argument here" test
```

**Use case:** Execute any binary with given arguments.

**Privileges required:** User

**Operating systems:** Windows 7 and up with VS/VScode installed

**ATT&CK® technique:** [T1127: Trusted Developer Utilities Proxy Execution](#)