.. /Devtoolslauncher.exe

Execute

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

Paths:
c:\windows\system32\devtoolslauncher.exe

Resources:

- https://twitter.com/_felamos/status/1179811992841797632

Acknowledgements:

- felamos (@_felamos)

Detections:

- Sigma:
https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_devtoolslauncher.yml
- IOC: DeveloperToolsSvc.exe spawned an unknown process

Execute

. 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

. 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