.. /csi.exe

Execute

Command line interface included with Visual Studio.

Paths:
c:\Program Files (x86)\Microsoft Visual Studio\2017\Community\MSBuild\15.0\Bin\Roslyn\csi.exe
c:\Program Files (x86)\Microsoft Web Tools\Packages\Microsoft.Net.Compilers.X.Y.Z\tools\csi.exe

Resources:
- https://twitter.com/subTee/status/781208810723549188
- https://enigma0x3.net/2016/11/17/bypassing-application-whitelisting-by-using-dnx-exe/

Acknowledgements:
- Casey Smith (@subtee)

Detections:
- Sigma: proc_creation_win_csi_execution.yml
- Sigma: proc_creation_win_csi_use_of_csharp_console.yml
- Elastic: defense_evasion_unusual_process_network_connection.toml
- Elastic: defense_evasion_network_connection_from_windows_binary.toml
- BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules

Execute

Use csi.exe to run unsigned C# code.

```
csi.exe file
```

Use case: Local execution of unsigned C# code.
Privileges required: User
Operating systems: Windows
ATT&CK® technique: T1127: Trusted Developer Utilities Proxy Execution