.. /Microsoft.Workflow.Compiler.exe

☆ Star 7,060

Execute AWL bypass

A utility included with .NET that is capable of compiling and executing C# or VB.net code.

Paths:
C:\Windows\Microsoft.Net\Framework64\v4.0.30319\Microsoft.Workflow.Compiler.exe

Resources:

- https://twitter.com/mattifestation/status/1030445200475185154
- https://posts.specterops.io/arbitrary-unsigned-code-execution-vector-in-microsoft-workflow-compiler-exe-3d9294bc5efb
- https://gist.github.com/mattifestation/3e28d391adbd7fe3e0c722a107a25aba#file-workflowcompilerdetectiontests-ps1
- https://gist.github.com/mattifestation/7ba8fc8f724600a9f525714c9cf767fd#file-createcompilerinputxml-ps1
- https://www.forcepoint.com/blog/security-labs/using-c-post-powershell-attacks
- https://www.fortynorthsecurity.com/microsoft-workflow-compiler-exe-veil-and-cobalt-strike/
- https://medium.com/@Bank_Security/undetectable-c-c-reverse-shells-fab4c0ec4f15

Acknowledgements:

- Matt Graeber (@mattifestation)
- John Bergbom (@BergbomJohn)
- FortyNorth Security (@FortyNorthSec)
- Bank Security (@Bank_Security)

Detections:

- Sigma: proc_creation_win_lolbin_workflow_compiler.yml
- Splunk: suspicious_microsoft_workflow_compiler_usage.yml
- Splunk: suspicious_microsoft_workflow_compiler_rename.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
- IOC: Microsoft.Workflow.Compiler.exe would not normally be run on workstations.
- IOC: The presence of csc.exe or vbc.exe as child processes of Microsoft.Workflow.Compiler.exe
- IOC: Presence of "<CompilerInput" in a text file.

Execute

1. Compile and execute C# or VB.net code in a XOML file referenced in the test.xml file.

```
Microsoft.Workflow.Compiler.exe tests.xml results.xml
```

Use case:	Compile and run code
Privileges required:	User
Operating systems:	Windows 10S, Windows 11
ATT&CK® technique:	**T1127**: Trusted Developer Utilities Proxy Execution

2. Compile and execute C# or VB.net code in a XOML file referenced in the test.txt file.

```
Microsoft.Workflow.Compiler.exe tests.txt results.txt
```

Use case:	Compile and run code
Privileges required:	User
Operating systems:	Windows 10S, Windows 11
ATT&CK® technique:	**T1127**: Trusted Developer Utilities Proxy Execution

AWL bypass

Compile and execute C# or VB.net code in a XOML file referenced in the test.txt file.

```
Microsoft.Workflow.Compiler.exe tests.txt results.txt
```

Use case:	Compile and run code
Privileges required:	User
Operating systems:	Windows 10S, Windows 11
ATT&CK® technique:	**T1127**: Trusted Developer Utilities Proxy Execution