.. /Wfc.exe

AWL bypass

The Workflow Command-line Compiler tool is included with the Windows Software Development Kit (SDK).

Paths:
C:\Program Files (x86)\Microsoft SDKs\Windows\v10.0A\bin\NETFX 4.8 Tools\wfc.exe

Resources:
- https://bohops.com/2020/11/02/exploring-the-wdac-microsoft-recommended-block-rules-part-ii-wfc-fsi/

Acknowledgements:
- Matt Graeber (@mattifestation)
- Jimmy (@bohops)

Detections:
- BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules
- Sigma: https://github.com/SigmaHQ/sigma/blob/6b34764215b0e97e32cbc4c6325fc933d2695c3a/rules/windows/process_creation/proc_creation_win_lolbin_wfc.yml
- IOC: As a Windows SDK binary, execution on a system may be suspicious

AWL bypass

Execute arbitrary C# code embedded in a XOML file.

```
wfc.exe c:\path\to\test.xoml
```

Use case:	Execute proxied payload with Microsoft signed binary to bypass WDAC policies
Privileges required:	User
Operating systems:	Windows 10 2004 (likely previous and newer versions as well)
ATT&CK® technique:	T1127