.. /le4uinit.exe

Execute

Executes commands from a specially prepared ie4uinit.inf file.

Paths:
c:\windows\system32\ie4uinit.exe
c:\windows\sysWOW64\ie4uinit.exe
c:\windows\system32\ieuinit.inf
c:\windows\sysWOW64\ieuinit.inf

Resources:
- https://bohops.com/2018/03/10/leveraging-inf-sct-fetch-execute-techniques-for-bypass-evasion-persistence-part-2/

Acknowledgements:
- Jimmy (@bohops)

Detections:
- IOC: ie4uinit.exe copied outside of %windir%
- IOC: ie4uinit.exe loading an inf file (ieuinit.inf) from outside %windir%
- Sigma: https://github.com/SigmaHQ/sigma/blob/bea6f18d350d9c9fdc067f93dde0e9b11cc22dc2/rules/windows/process_creation/proc_creation_win_lolbin_ie4uinit.yml

Execute

Executes commands from a specially prepared ie4uinit.inf file.

```
ie4uinit.exe -BaseSettings
```

Use case: Get code execution by copy files to another location
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1218