# TTP Detail – T1183

## TTP Information

Name: Image File Execution Options Injection

Description: Image File Execution Options (IFEO) enable a developer to attach a debugger to an application. When a process is created, a debugger present in an application’s IFEO will be prepended to the application’s name, effectively launching the new process under the debugger (e.g., “C:\dbg\ntsd.exe -g notepad.exe”). (Citation: Microsoft Dev Blog IFEO Mar 2010)

IFEOs can be set directly via the Registry or in Global Flags via the GFlags tool. (Citation: Microsoft GFlags Mar 2017) IFEOs are represented as <code>Debugger</code> values in the Registry under <code>HKLM\SOFTWARE{\Wow6432Node}\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<executable></code> where <code><executable></code> is the binary on which the debugger is attached. (Citation: Microsoft Dev Blog IFEO Mar 2010)

IFEOs can also enable an arbitrary monitor program to be launched when a specified program silently exits (i.e. is prematurely terminated by itself or a second, non kernel-mode process). (Citation: Microsoft Silent Process Exit NOV 2017) (Citation: Oddvar Moe IFEO APR 2018) Similar to debuggers, silent exit monitoring can be enabled through GFlags and/or by directly modifying IEFO and silent process exit Registry values in <code>HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\</code>. (Citation: Microsoft Silent Process Exit NOV 2017) (Citation: Oddvar Moe IFEO APR 2018)

An example where the evil.exe process is started when notepad.exe exits: (Citation: Oddvar Moe IFEO APR 2018)

\* <code>reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\notepad.exe" /v GlobalFlag /t REG\_DWORD /d 512</code>
\* <code>reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe" /v ReportingMode /t REG\_DWORD /d 1</code>
\* <code>reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe" /v MonitorProcess /d "C:\temp\evil.exe"</code>

Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), these values may be abused to obtain persistence and privilege escalation by causing a malicious executable to be loaded and run in the context of separate processes on the computer. (Citation: Elastic Process Injection July 2017) Installing IFEO mechanisms may also provide Persistence via continuous invocation.

Malware may also use IFEO for Defense Evasion by registering invalid debuggers that redirect and effectively disable various system and security applications. (Citation: FSecure Hupigon) (Citation: Symantec Ushedix June 2008)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: privilege-escalation

**•** mitre-attack: persistence

**•** mitre-attack: defense-evasion