# TTP Detail – T1546.012

## TTP Information

Name: Image File Execution Options Injection

Description: Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by Image File Execution Options (IFEO) debuggers. IFEOs 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., <code>C:\dbg\ntsd.exe -g notepad.exe</code>). (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>&lt;executable&gt;</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 IFEO 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)

Similar to [Accessibility Features](https://attack.mitre.org/techniques/T1546/008), on Windows Vista and later as well as Windows Server 2008 and later, a Registry key may be modified that configures "cmd.exe," or another program that provides backdoor access, as a "debugger" for an accessibility program (ex: utilman.exe). After the Registry is modified, pressing the appropriate key combination at the login screen while at the keyboard or when connected with [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1021/001) will cause the "debugger" program to be executed with SYSTEM privileges. (Citation: Tilbury 2014)

Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), these values may also be abused to obtain 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 triggered invocation.

Malware may also use IFEO to [Impair Defenses](https://attack.mitre.org/techniques/T1562) 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

## Malware

* SDBbot
* SUNBURST