# TTP Detail – T1546.010

## TTP Information

Name: AppInit DLLs

Description: Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by AppInit DLLs loaded into processes. Dynamic-link libraries (DLLs) that are specified in the <code>AppInit\_DLLs</code> value in the Registry keys <code>HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows</code> or <code>HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows</code> are loaded by user32.dll into every process that loads user32.dll. In practice this is nearly every program, since user32.dll is a very common library. (Citation: Elastic Process Injection July 2017)

Similar to Process Injection, these values can be abused to obtain elevated privileges by causing a malicious DLL to be loaded and run in the context of separate processes on the computer. (Citation: AppInit Registry) Malicious AppInit DLLs may also provide persistence by continuously being triggered by API activity.

The AppInit DLL functionality is disabled in Windows 8 and later versions when secure boot is enabled. (Citation: AppInit Secure Boot)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

**•** mitre-attack: persistence

## Malware

* Cherry Picker
* Ramsay
* T9000

## APTs (Intrusion Sets)

* APT39