# TTP Detail – T1546.009

## TTP Information

Name: AppCert DLLs

Description: Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by AppCert DLLs loaded into processes. Dynamic-link libraries (DLLs) that are specified in the <code>AppCertDLLs</code> Registry key under <code>HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Session Manager\</code> are loaded into every process that calls the ubiquitously used application programming interface (API) functions <code>CreateProcess</code>, <code>CreateProcessAsUser</code>, <code>CreateProcessWithLoginW</code>, <code>CreateProcessWithTokenW</code>, or <code>WinExec</code>. (Citation: Elastic Process Injection July 2017)

Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), this value 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. Malicious AppCert DLLs may also provide persistence by continuously being triggered by API activity.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

**•** mitre-attack: persistence

## Malware

* PUNCHBUGGY