# TTP Detail – T1182

## TTP Information

Name: AppCert DLLs

Description: Dynamic-link libraries (DLLs) that are specified in the AppCertDLLs 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 CreateProcess, CreateProcessAsUser, CreateProcessWithLoginW, CreateProcessWithTokenW, or WinExec. (Citation: Elastic Process Injection July 2017)

Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), this value can be abused to obtain persistence and privilege escalation by causing a malicious DLL to be loaded and run in the context of separate processes on the computer.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

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