**Tampering with Windows Registry**

**Description 1**

DLLs that are specified in the AppInit\_DLLs value in the Registry key HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows are loaded by user32.dll into every process that loads user32.dll. In practice this is nearly every program. This value can be abused to obtain persistence by causing a DLL to be loaded into most processes on the computer. The AppInit DLL functionality is disabled in Windows 8 and later versions when secure boot is enabled.

References

[1]<https://attack.mitre.org/wiki/Privilege_Escalation>

[2]https://support.microsoft.com/en-us/help/197571/working-with-the-appinit-dlls-registry-value