

Event Triggered Execution: Application Shimming, Sub-technique T1546.011 - Enterprise

Archived: 2026-04-05 12:53:40 UTC

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by application shims. The Microsoft Windows Application Compatibility Infrastructure/Framework (Application Shim) was created to allow for backward compatibility of software as the operating system codebase changes over time. For example, the application shimming feature allows developers to apply fixes to applications (without rewriting code) that were created for Windows XP so that it will work with Windows 10. [\[1\]](#)

Within the framework, shims are created to act as a buffer between the program (or more specifically, the Import Address Table) and the Windows OS. When a program is executed, the shim cache is referenced to determine if the program requires the use of the shim database (.sdb). If so, the shim database uses hooking to redirect the code as necessary in order to communicate with the OS.

A list of all shims currently installed by the default Windows installer (sdbinst.exe) is kept in:

- `%WINDIR%\AppPatch\sysmain.sdb` and
- `hk\m\software\microsoft\windows nt\currentversion\appcompatflags\installedsdb`

Custom databases are stored in:

- `%WINDIR%\AppPatch\custom & %WINDIR%\AppPatch\AppPatch64\Custom` and
- `hk\m\software\microsoft\windows nt\currentversion\appcompatflags\custom`

To keep shims secure, Windows designed them to run in user mode so they cannot modify the kernel and you must have administrator privileges to install a shim. However, certain shims can be used to [Bypass User Account Control](#) (UAC and RedirectEXE), inject DLLs into processes (InjectDLL), disable Data Execution Prevention (DisableNX) and Structure Exception Handling (DisableSEH), and intercept memory addresses (GetProcAddress).

Utilizing these shims may allow an adversary to perform several malicious acts such as elevate privileges, install backdoors, disable defenses like Windows Defender, etc. [\[2\]](#) Shims can also be abused to establish persistence by continuously being invoked by affected programs.

Source: <https://attack.mitre.org/techniques/T1546/011>