

Forum:[Hack Forums](#)

Thread: [Windows Application Shimming](#)

CyberStrike - December 6, 2017, 6:38 pm

Required Files:

Windows Application Compatibility ToolKit
Windows Assessment and Deployment Kit
sdbinst.exe (Often comes with Windows)
sdb-explorer.exe (Created by John Erickson)
sdb2xml (Heath Stewart)
python-sdb

What is application shimming? Well it's rather simple, if you remember the days of Windows 95/98 Microsoft kept a lot of backwards compatibility, in order to allow users to use older software. When we look at Windows 7 there are many hardcoded references to old software, such as WordPerfect 8, this is software circa 1996. Microsoft made it easy for a developer to install the Shim Database (sdb).

Let us take a look at the tools involved, which are for free and from Microsoft, first for Windows XP, Vista, 7, 2000, 2003 you would use Application Compatibility Toolkit (ACT), for anything newer you will want to use Windows Assessment and Deployment Kit (ADK). Now realizing that this is used to "fix" applications to ensure that they will run on the latest and greatest let us take a quick look at a few options, that are included.

Now it should be noted that there are several here, but some of these can allow our application to RunAsAdmin, InjectDll, MofidyShellLinkPath and ForceAdminAccess, and several more. So now after modifying our application we will be saving the SDB file which we may use sdbinst.exe to install the file. The installer will create a GUID for the application and corresponding registry keys in %SystemRoot%\AppPatch\Custom\<GUID>.sdb & HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom\<GUID>.sdb and \InstalledSDB\<GUID>.sdb if installation was successful. After the installation the sdb file will be checked for matching sdb application shimming rules and any metadata for the application will be found in Application Compatibility Cache, as of the last reboot. One thing to note is that any application from Microsoft has escalated privileges due to <autoElevate>true</autoElevate> being on as a flag.

This translates into nearly every application/process is vulnerable and only a few which cannot be shimmed. Also another positive here will be that autoruns from sysinternals suite does not detect the auto-run of a shimmed application. Using various options you can intercept, and modify a process and the information in that process. Also using shims such as RedirectEXE, InjectDll, and others you can now backdoor a piece of software, and enable persistence. Shims may also be used to disable defenses, such as DisableWindowsDefender, DisableASLR, and others, would help prevent detection.

So what does this all mean? Simply said you are now able to bypass UAC and trojanize legitimate applications. For example we can provide our own backdoored DLL and using InjectDll shim now when our application which is shimmed is started we get out connection, in addition since autoruns from SysInternals does not recognize the auto-run capability of a shimmed application you can hide your backdoor a bit better, and evade a nosy Administrator.

Now there is a downside, you must be an Administrator in order to successfully carry out this attack. In addition if the application name is changed the shim will not work, also shims work in user-mode so manipulation of the kernel is not possible.

Since shims do have control over redirection and manipulation over the various processes memory, detection detection can be done by analyzing those processes and for anomalies, with products such as Shim-Detector-Lite, which is free on github. In addition Shim-Gaurd-Lite can and will detect new sdb installs.

lwrist - December 8, 2017, 10:12 pm

Something to do post exploitation! Root > elevate > shim it up

Thanks for writing this tutorial and taking the time to explain it to the community. It's well written. Hopefully others will be able to benefit practically and theoretically from it! Thanks again!

CyberStrike - December 8, 2017, 10:46 pm

Thank you, I might do a series based on the MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)

lwrist - December 9, 2017, 7:38 am

I'll be looking forward to that!

CyberStrike - December 12, 2017, 7:25 am

If anyone wants to do some further reading application/kernel shims were discussed at this years BlachHoodie17

https://www.blackhoodie.re/assets/archive/Kernel_Shim_Engine_for_fun_-_pwissenlit.pdf

Hopsin - December 13, 2017, 3:38 pm

I'll bookmark this thread for later read, knowledge is power. Thank you for sharing.

Rsynced - December 13, 2017, 3:43 pm

Thanks this is very great knowledge. I am gathering I could use shimming to just simply run older legit software not compatible with windows 7/10?

CyberStrike - December 13, 2017, 3:44 pm

Awesome, you are welcome. I might turn this into a MITRE ATT&CK Thread, where every couple of days I take a new attack method.