Beyond good ol’ Run key, Part 120

hexacorn.com/blog/2019/10/23/beyond-good-ol-run-key-part-120

October 23, 2019 *in Anti-Forensics, Autostart (Persistence), Living off the land, LOLBins*

This is a phantom DLL case on Windows 7 – funny bug in c:\WINDOWS\system32\spreview.exe.

When it starts it loads *wdscore.dll* library, but it does it incorrectly, and as a result it tries to load C:\WINDOWS\system32\spreview.exewdscore.dll file first.

So, if you place such library on a system, anytime spreview is launched, the spreview.exewdscore.dll DLL will be loaded. It’s also a Lolbin, of cuz.

The bad news – it’s used very rarely as it’s related to Service Pack installation. The better news — since spreview.exe is a part of a OS and signed, you could add it to any startup location and it will load that funnily-named DLL when it starts.