This LOLBIN doesn’t exist…

I have written about Nullsoft installer a few times before. I am a bit fascinated by it, because there is not that much research about it, in general, and even less – about its esoteric, yet omnipresent DLL plug-ins…

One of the more interesting plug-ins that I know of, and yet, one that you will never really see residing on any system, is… *ShellDispatch.dll*.

It’s a rarely used Nullsoft Plug-In DLL that is known to be used by the installer of WinAmp, yes.. THE WinAmp… and even there… it is used temporarily, as it is immediately deleted from the file system after delivering the required functionality.

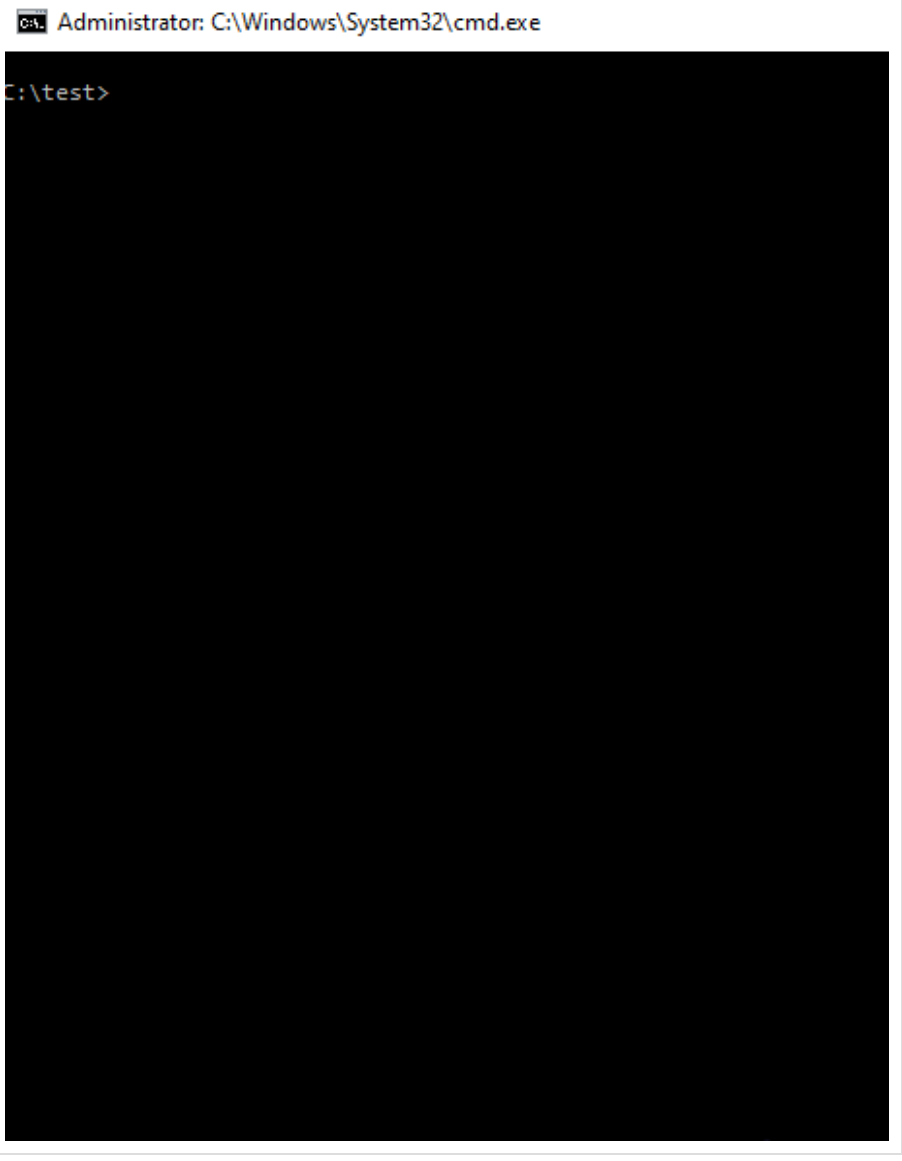
What’s so special about it?

The *ShellDispatch.dll* exports a few functions:

- AddRef
- GetInterface
- Release
- RunDll_ShellExecuteW
- ShellExecute

The *RunDll_ShellExecuteW* is the most interesting to us as it is a callback function specifically crafted to respond to invocations via *rundll32.exe*, and since it’s a wrapper for *ShellExecute* API we can use it to launch any program of our choice, f.ex, calculator:

```
rundll32 ShellDispatch.dll, RunDll_ShellExecute open calc
```



Again, the chances you will ever see it abused are VERY LOW.

This entry was posted in **LOLBins** by **adam**. Bookmark the **permalink**.