Beyond good ol' Run key, Part 136

hexacorn.com/blog/2022/01/18/beyond-good-ol-run-key-part-136

January 18, 2022 *in* *Autostart (Persistence)*, *Living off the land*, *LOLBins*

I love Office-based Persistence mechanisms, because there is always… one more to discover

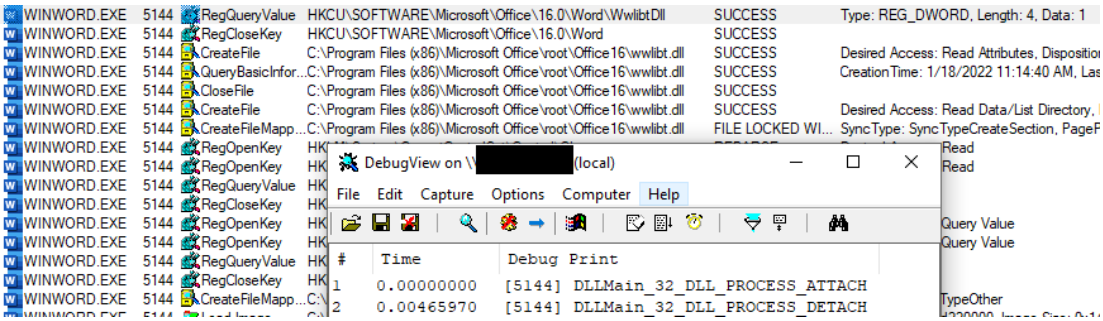
Take your *Winword.exe* from Office 2021 or Office 365. When it loads, it check if the following value exists in Registry and is not equal 0:

```
HKCU\SOFTWARE\Microsoft\Office\16.0\Word\WwlibtDll != 0
```

And if it is the case… instead of loading *wwlib.dll*, it will load *wwlibt.dll*.

So, place your payload in *wwlibt.dll* and winword will load it for you.

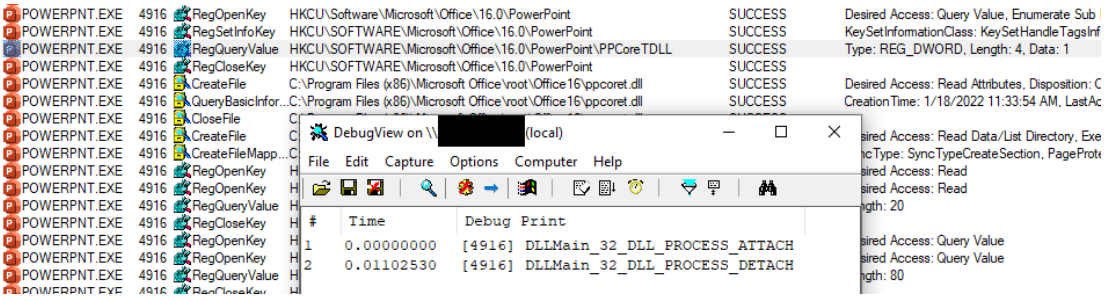
This trick can be used as a traditional sideloading LOLBIN, and as a persistence mechanism, because *wwlibt.dll* could be made to load the *wwlib.dll*. Or, could temporary remove the value inRegistry and re-launch *winword.exe*.



Interestingly, PowerPoint has the same 'feature':

```
HKCU\SOFTWARE\Microsoft\Office\16.0\PowerPoint\PPCoreTDLL != 0
```

and the DLL name is *ppcoret.dll* (instead of *ppcore.dll*).



Comments are closed.