Beyond good ol’ Run key, Part 128

hexacorn.com/blog/2020/09/18/beyond-good-ol-run-key-part-128

September 18, 2020 *in* *Anti-Forensics*, *Autostart (Persistence)*

It’s been a long time since I looked at phantom DLLs (non-existing DLLs that are expected to be present in predictable locations). So, a quick rundown what we can see on Win10 today folows:

- C:\Windows\System32\edgegdi.dll
  - loaded by gdi.dll, but not present on the most up to date win10 pro installation; it must be signed
  - loaded by a number of processes backgroundTaskHost.exe, BackgroundTransferHost.exe, DllHost.exe, dmclient.exe, HxTsr.exe, LockApp.exe, LogonUI.exe, Microsoft.Photos.exe, mousocoreworker.exe and many others; existing work: found some EoP research on Twitter
- C:\Windows\SysWOW64\rpcss.dll
- C:\Windows\System32\UsoSelfhost.dll
  loaded by mousocoreworker.exe — possible EoP?
- C:\Windows\System32\Speech_OneCore\common\sapi_onecore.dll
  loaded by SearchApp.exe
- C:\Windows\System32\windowscoredeviceinfo.dll
  loaded by taskhostw.exe

There are more, but I reserve them for a possible future post.