Home   Services   Products & Freebies   🔎 Search

Case Studies   Contact Us

Posted on **2018-04-27**   ← Previous   Next →

I shot the sigverif.exe – the GUI-based LOLBin

File Signature Verification has nothing to do with launching arbitrary applications, but it is just a similar case to odbcad32.exe – the GUI apps can sometimes be abused to produce undesired effects – ones that their authors most likely have not anticipated…
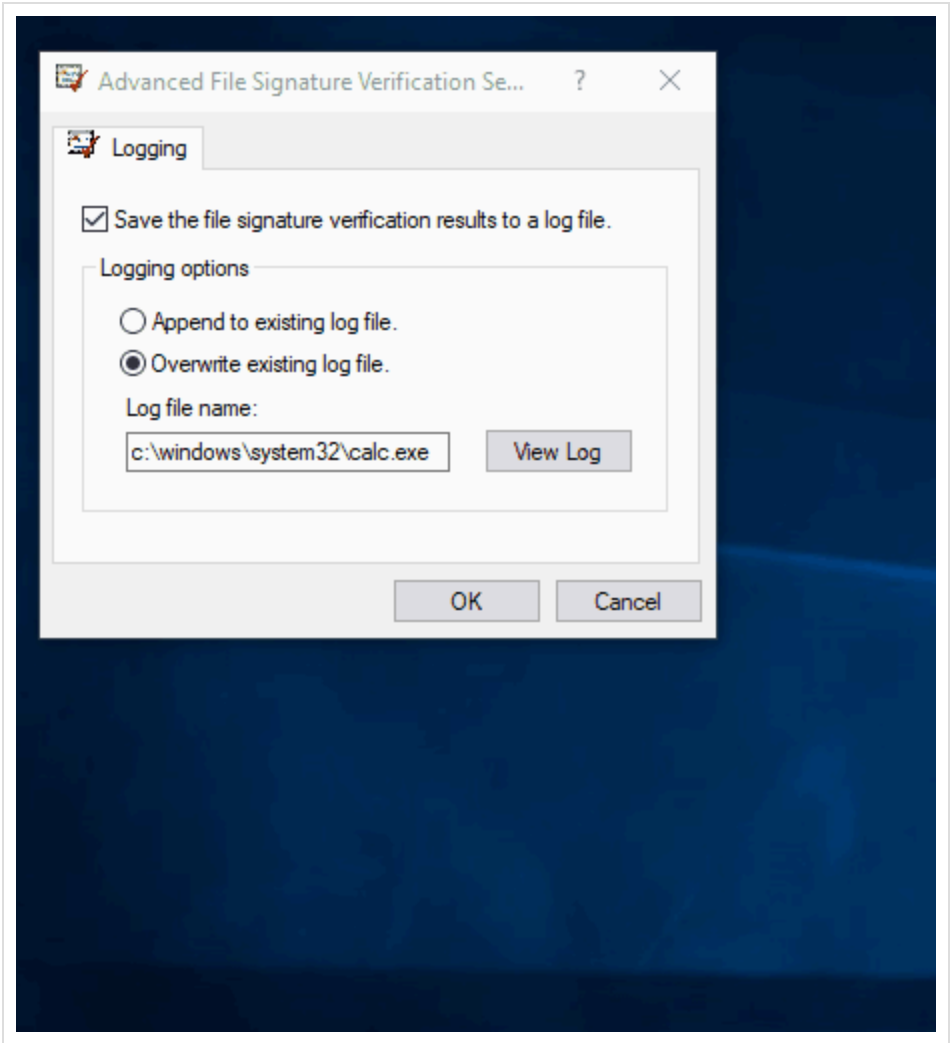
Time for the recipe.

So we launch the sigverif.exe:
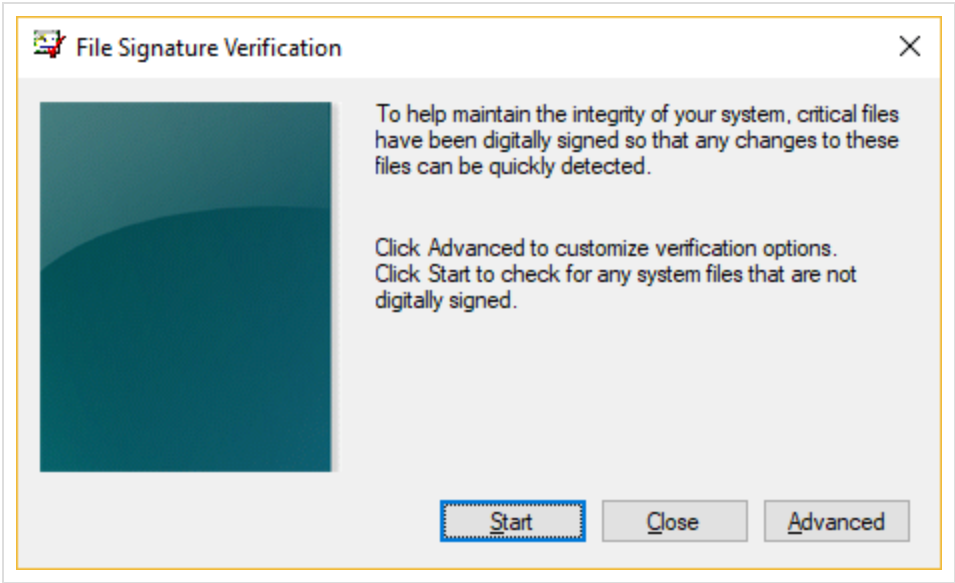
Then we go to Advanced settings by clicking the Advanced button, and we choose … the log file. And while we are at it why shouldn't we choose the c:\windows\system32\calc.exe as a destination?
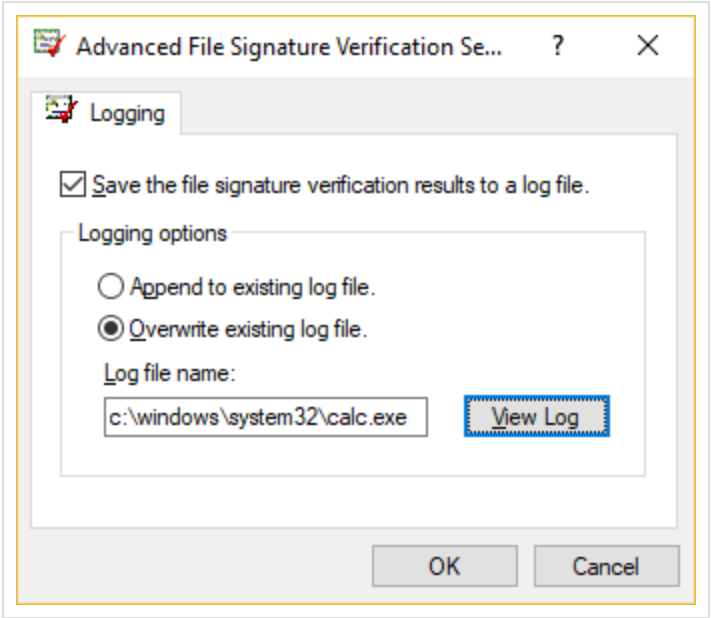
We then hit the View Log button, and voila. Calculator is on the screen:

This entry was posted in **Living off the land**, **LOLBins** by **adam**. Bookmark the **permalink**.

Privacy Policy | **Proudly powered by WordPress**