Posted on 2018-05-01

← Previous Next →

wab.exe as a LOLBin

WAB stands for Windows Address Book. It's also a name of a tool typically located inside these two file paths:

- c:\Program Files (x86)\Windows Mail\wab.exe
- c:\Program Files\Windows Mail\wab.exe

In the past the program was used to manipulate .wab files, but nowadays it is a legacy tool and is not used that much anymore.

Still, we can use it to do one more thing for us…

When launched, it tries to load a wab32.dll library. The actual location and the name of a DLL is determined by the following Registry key:

- HKLM\Software\Microsoft\WAB\DLLPath

which typically points to:

- %CommonProgramFiles%\System\wab32.dll

By changing this path you can load any DLL of your choice.

Only if the DLLPath Registry path is not resolved the tool will try to load the wab32.dll from a current directory. So yet another opportunity for side-loading…

Last, but not least – on older systems it could act as a persistence mechanism.

This entry was posted in **Anti-Forensics**, **Autostart (Persistence)**, **Living off the land**, **LOLBins** by **adam**. Bookmark the **permalink**.