

Beyond good ol' Run key, Part 123

 hexacorn.com/blog/2019/11/18/beyond-good-ol-run-key-part-123

November 18, 2019 in *[Anti-Forensics](#)*, *[Autostart \(Persistence\)](#)*

Yet another quick post. This time about a subset of libraries (and possibly programs, but I only saw the libraries) that reference [Intel® VTune™ Amplifier](#).

As explained in a linked article, one can define following environment variables to ensure the ITT libraries are loaded during the program run-time:

- INTEL_LIBITTNOTIFY32=<DLL>
- INTEL_LIBITTNOTIFY64 =<DLL>

It's probably a poor choice for a potential persistence mechanism. I only saw these referenced by [tbbmalloc.dll](#), but there may be more programs/libraries. Even Mozilla seems to be using it in some of its [builds](#).

Comments are closed.