Beyond good ol' Run key, Part 129

October 17, 2020 *in Anti-Forensics, Autostart (Persistence)*

Browsing through windows libraries I came across a few that had an intriguingly named function being resolved during run-time: DllBidEntryPoint.

The libraries referencing this API are:

- msado15.dll
- msadomd.dll
- msadox.dll
- msadrh15.dll
- msadce.dll
- msadco.dll
- msadds.dll
- msdaprst.dll
- msdarem.dll
- msdaora.dll
- msdasql.dll
- msdatl3.dll
- oledb32.dll
- sqloledb.dll

As usual, the first thing was to go to Google and soon I discovered that it's a part of a documented tracing interface used by SQL Server called Built-in Diagnostics (BID).

One can use one of these keys:

- HKLM\Software\Microsoft\BidInterface\Loader
- HKEY_LOCAL_MACHINE\software\Wow6432Node\Microsoft\BidInterface\Loader

and add ':Path ' value name pointing to a DLL that will act as a tracing DLL.

As usual, the linked document contains all the gore details.