How can I programmatically inspect and manipulate a registry hive file without mounting it?

devblogs.microsoft.com/oldnewthing/20181015-00

October 15, 2018

Raymond Chen

Say you have a registry hive file. One way to inspect and manipulate its contents is by calling the `RegLoadKey` function to mount it in the registry and then use the normal registry operations.

This option may be undesirable for various reasons.

First of all, the `RegLoadKey` function requires administrator privileges, so that's a problem.

Second, even after you load the hive, you are still subject to the security settings of the keys in the hive. If somebody sets the security on a registry key to "Deny access to administrators", then you won't be able to read it even though you've elevated to administrator.

Furthermore, once the hive is loaded, it is globally visible, and any other process can go in and see the contents and possibly even modify the hive behind your back.

What you would prefer is something that lets you operate directly on the hive file without having to mount it. A local solution to a local problem.

Fortunately, there's a solution for you. The Offline Registry Library allows you to read and optionally modify registry hive files. It also bypasses all security on registry keys, so you can wander through the entire file with impunity. There is no security vulnerability here because you already had access to the registry hive file.

Bonus chatter: There is also `RegLoadAppKey` which does not require administrator privileges. However, it also requires that all keys in the hive have the same security attributes. If you are loading arbitrary registry hives (say for offline servicing), you are unlikely to satisfy those requirements.

Raymond Chen

Follow