Why do I get notified for changes to HKEY_CLASSES_ROOT when nobody is writing to HKEY_CLASSES_ROOT?

devblogs.microsoft.com/oldnewthing/20121205-00

December 5, 2012

Raymond Chen

A customer had a question about the `RegNotifyChangeKeyValue` function.

> We are using it to monitor the `HKEY_CLASSES_ROOT` tree as follows:
>
> ```
> RegNotifyChangeKeyValue(
>     HKEY_CLASSES_ROOT,
>     true, // monitor entire subtree
>     REG_NOTIFY_CHANGE_NAME | REG_NOTIFY_CHANGE_LAST_SET,
>     eventRegKeyChanged,
>     true); // asynchronous mode
> ```
>
> If I understand the documentation correctly, this registers for notifications when subkeys are added, deleted, or when values are changed. However, it seems that my event becomes signaled at many other times, for example, when I switch folders in an Explorer window. I fired up Process Monitor and confirmed that nobody (not even Explorer) is writing to `HKEY_CLASSES_ROOT`.
>
> Why are we getting spurious notifications? Have we misunderstood what this function does?

Everything is working as expected; it's just that your expectations are wrong.

Recall that the `HKEY_CLASSES_ROOT` registry key is really a combined view of `HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`. Specifically, it is a combined view of `HKEY_LOCAL_MACHINE\Software\Classes` and `HKEY_CURRENT_USER\Software\Classes`. And `HKEY_CURRENT_USER\Software\Classes` is itself just an alias for `HKEY_USERS\«SID»_Classes`. Therefore, if you're going to look in Process Monitor, you need to be looking at all of those locations to see changes that eventually get reported as changes in `HKEY_CLASSES_ROOT`.

In this particular case, Explorer was making changes to `HKEY_USERS\«SID»_Classes\Local Settings`, which shows up as `HKEY_CLASSES_ROOT\Local Settings`.

Upon receiving this explanation, the customer understood what was going on, and also remarked that they were going to look to see if they could register their notification on a location that isn't quite so broad.

Raymond Chen

Follow