Could I be getting ERROR_KEY_DELETED for HKEY_CURRENT_USER\Software when the user logs off?

devblogs.microsoft.com/oldnewthing/20250102-00

January 2, 2025

In the comments to my earlier discussion of the `ERROR_KEY_DELETED` error code, Igor Glucksmann reported that they were seeing `ERROR_KEY_DELETED` coming from code that used a key that was open to `HKEY_CURRENT_USER\Software`, which is unlikely to be deleted. Could this be due to the user logging off?

When the user logs off, a bunch of things happen. Programs that are still running in the session are terminated, services are notified of the logoff, and then the user hive is force-unloaded.

Historically, Windows did not force-unload the user hive because it expected that services would do the right thing and clean up resources associated with the user when the user logs off. In practice, the team discovered that there were many recalcitrant services which failed to close user registry keys when the user logged off, causing the user hive to get stuck in memory and never unloaded. This in turn caused roaming profiles to stop working because the system couldn't copy the user's profile back to the profile server.

I suspect that many of these ill-behaved services weren't being recalcitrant on purpose. They probably made the mistake of accessing `HKEY_CURRENT_USER` from a service while impersonating, which then caused the `HKEY_CURRENT_USER` key to be a reference to the registry of whatever user was being impersonated. The service didn't break this reference when the user logged off because it wasn't even aware that the reference had been created in the first place!

In response to this unfortunate reality of services which fail to close all their open keys to users who are logging off, the user profile team held their noses and added code to give services what felt like a reasonable amount of time to do their per-user logoff cleanup (I think it was around 30 seconds, but I'm not sure), and if there were still outstanding references to that user's registry, it would just force-unload the user registry and leave those services with broken registry keys.

This problem with force-unloaded registry hives should only be an issue with programs (like services) which outlive the user logon session. I don't know if that applies to Igor's situation.

Next time, I'll try to force the error to occur in a regular user-session programs that isn't a service.