Hiding files is not the same as protecting them

devblogs.microsoft.com/oldnewthing/20070305-00

March 5, 2007

Raymond Chen

An anonymous commenter suggested that we should give up on "hiding protected operating system files". After all, if we "protect operating system files", that should be enough, shouldn't it? Well, except that some files are still hidden even though they are not protected. For example, your encryption keys are fully accessible to you (after all, they're your encryption keys), but they are marked as hidden because if you deleted them, your encrypted files are in trouble. "If visibility itself is core to somebody's security, why not safeguard against a file's enumeration via the ACL?" The purpose of hiding protected system files is to avoid showing users things that would create confusion, would present an attractive nuisance, or would result in "trouble" if they messed with them. Those encryption keys are one example. A user might see them and say, "Huh, what's this? I'm not using it. Let me delete it and free up some disk space." And then boom, they can't recover their encrypted data. One category of files that are an "attractive nuisance" are all those programs in your System32 directory. Feedback from the product support team told us that many users just go into their system directory and double-click everything in it, just to see what happens. If any of those programs happened to do something destructive, you had a very unhappy user on your hands. (So much for the mantra that "nothing you do can physically harm a computer.") We've learned the hard way that none of these programs can do anything dangerous if run with no command line options. For example, `shutdown.exe` with no parameters doesn't actually shut down your computer.

An example of files that the user has access to but probably shouldn't be messing with is those `desktop.ini` files that the shell scatters about the system to mark various directories and files. These files are marked as "protected operating system files" because messing with them changes the plumbing of how Explorer treats those directories. Delete those files, and your Fonts folder stops working, your Temporary Internet Files become inaccessible, and if you're running, say, Windows with the German language pack, all your beautiful German directory names lose their German magic and switch to English. That's because the `desktop.ini` file recorded that the Fonts folder is the Fonts folder, that the Temporary Internet Files folder should show your Temporary Internet Files, and that the folder "My Pictures" should be called "Eigene Bilder" in Germany.

Raymond Chen

Follow