Program names in file type handlers need to be fully-qualified

devblogs.microsoft.com/oldnewthing/20050830-11

August 30, 2005

Raymond Chen

Most people probably haven't noticed this, but there was a change to the requirements for file type handlers that arrived with Windows XP SP 2: Paths to programs now must be fully-qualified if they reside in a directory outside of the Windows directory and the System directory.

The reason for this is security with a touch of predictability thrown in.

Security, because one of the places that the `SearchPath` function searches is the current directory, and it searches the current directory before searching standard system directories or the PATH. This means that somebody can attack you by creating a file like say "Super secret information.txt" and creating a hidden NOTEPAD.EXE file in the same directory. The victim says, "Oh wow, look, super secret information, let me see what it is," and when they double-click it, the trojan NOTEPAD.EXE is run instead of the one in the Windows directory. Requiring paths to be fully-qualified removes the current directory attack.

Predictability, because the contents of the PATH environment variable can vary from process to process. Consequently, the relative path could resolve to different programs depending on who is asking. This in turn results in having to troubleshoot problems like "It works when I double-click it from Explorer, but not if I run it from a batch file."

Raymond Chen

Follow