Yes indeed, all Microsoft files are (or should be) digitally signed

devblogs.microsoft.com/oldnewthing/20070827-00

August 27, 2007

Raymond Chen

Yes indeed, all Microsoft files are (or should be) digitally signed (as far as I'm aware). So I'm not quite sure what commenter Dave is getting at:

> The Microsoft file should have embedded vendor/product information saying it's from Microsoft and will be cryptographically signed by Microsoft. Similarly-named malware won't be signed by Microsoft, unless Verisign slipped up *again* and issued another bogus certificate.

Wow, this is such a great idea, that it's been true for many years now. All Microsoft files are digitally signed. They have to be; otherwise, Windows File Protection wouldn't be able to tell whether this new version of `shell32.dll` is a security update or just some malware trying to replace a system file. As I noted quite some time ago, you can run the `sigverif` program to validate the digital signatures of all system files.

> Long descriptive names are just as much an opportunity to malware makers as they are to legit software developers. Gee, why would you want to stop a file named "Critical Security Update Service.exe" for example?

And that's why Windows XP Service Pack 2 added the ability to mark a file as "I got this from the Internet." (Internet Explorer applies this marking when you download a file from the Internet.) Before you run such a file, Explorer will prompt you with a warning and show you the digital signature information so that you can confirm that the download is what it purports to be and has not been tampered with. This is just one example of a commenter who suggests that Windows do things that it already does: Drop down lists do let you type multiple characters. Here's another example. Windows has been multilingual since Windows 2000.

For now, I'm going to keep ignoring them. Just because you say something in my presence and I don't raise an objection doesn't mean that I agree. Or that what you said is even true.

Raymond Chen

Follow