Dubious security vulnerability: Messing with the Recycle Bin

devblogs.microsoft.com/oldnewthing/20151217-00

December 17, 2015

Raymond Chen

Today's dubious security vulnerability goes like this:

> The $RECYCLE.BIN directory can be used to drop files into an arbitrary directory. To do this, navigate into a user's Recycle Bin directory and find a file in it. Edit the file to contain the data you would like to drop, and edit the Recycle Bin database to say that the file in question should be restored to a directory of your choosing. When the user opens the Recycle Bin in Explorer, right-clicks the file, and selects Restore, the file will be dropped in the directory you chose.

The idea here is that you can falsify the information in the Recycle Bin so that it looks like the attack file was deleted from the attack directory, so that "restoring" the file will drop the file into the directory.

Sure, but you're only messing with yourself.

It's like going into your kitchen pantry, opening a box of cookies, and replacing the cookies with rocks. Now, the next time you go to the pantry to get some cookies, you open the box, and instead of cookies, you get rocks! Woot! Security vulnerability!

There is no vulnerability here, because you are just attacking yourself. You have access to the pantry because it's your pantry. You have access to the box of cookies because it's your box of cookies. If you want to put rocks in a box labeled *Cookies*, then more power to you.

There is no elevation because the Restore operation will not be able to drop the file anywhere the user doing the restoring doesn't already have write access to. If you say "Um, yeah, this file should be restored to C:\Windows," then the Restore operation will say, "Sorry, you don't have access there. But if you enter the administrator password, then I can do it."

The default security on the Recycle Bin folder grants access only to Administrators, System, and the owner of the Recycle Bin. Therefore, the only person who can carry out this attack is the user himself. And if you want to drop a file in a directory a much easier way to do this is to use the `COPY` command.

Raymond Chen

Follow