The Danger of Scrap Files

Magnus Mischel

Introduction

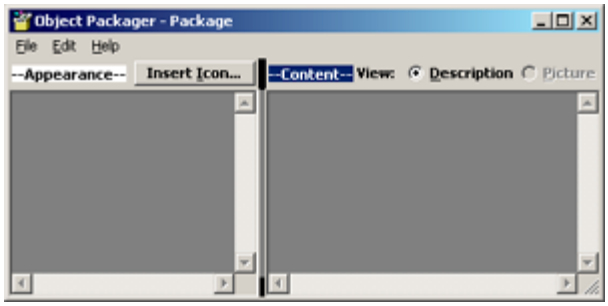
Many Internet users today know that they should never run executable or script files they receive via e-mail because of the danger of malicious code. So they set their Windows Explorer settings to show file extensions so they can recognize the dangerous file extensions like .exe, .vbs et. al. But what if there was a file type that could contain malicious code, and the file extension was automatically hidden from the user by Windows no matter what the Explorer settings? And what if that file had an icon that resembled a harmless text file? And what if double-clicking on such a file would execute the malicious code embedded in it?
Well, the bad news is that there does exist such a file type; it's called a *Scrap File*. The good news is that this article will teach you the basics about it, and how you can protect yourself.

What Is a Scrap File?

Scrap Files are part of a Microsoft Windows concept called "Object Linking and Embedding" (OLE). This feature has existed in the Windows operating system since version 3.1, and exists still in Windows 2000. The Microsoft Windows 3.1 User's Guide states that (translated from Swedish):

> "Objects can be linked or embedded in two ways. You can embed the object itself or a so called *package*, an icon representing the object, in the document. You use the Windows-accessory `packager.exe` to create a package."

This method enables a user to open `packager.exe` and create a package and then embed this package in a document. That seems rather harmless; you would have to open the document and then double-click the embedded object to execute its commands. Not a very effective method to spread for example a trojan horse program.
But there is a way to turn the embedded object to a stand alone file. After creating a package and inserting it into a document, you can drag and drop the object's icon into a folder. This will create a *Scrap File*. These files have an extension of `.SHS` (for Shell scrap object), but this extension is never shown by Windows Explorer - even if the user has set his preferences to show file extensions. As you will see in a screen-shot farther down, these files have an icon that resembles that of a text-file, even though they can contain arbitrary code.

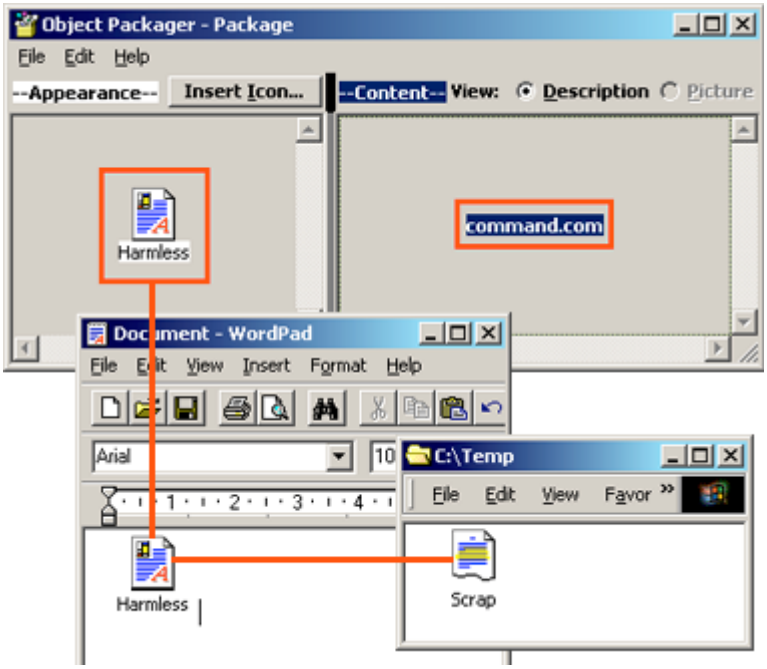


A Real-Life Example

In this section, I will generate a scrap file with an embedded command to illustrate the dangers of these files. This method is the same one that is used by malicious programmers to distribute trojans, and the aim is to show you that you should distrust all and any scrap files that you yourself did not personally create.

To begin with, I start up the Object Packager by choosing Start/Run and `packager.exe`. By selecting Edit/Command Line, I insert the command `command.com` which when executed under

Windows will start an MS-DOS shell. This is a harmless command by itself; however, it could just as easily be replaced by `deltree /y c:\*.*` which will obliterate the entire C drive. Next I select an icon to use for the package when it is embedded in another document. For this example, I used the standard icon for a rich-text document. Finally, I label the package "Harmless" by selecting Label from the Edit menu.



Now I'm ready to use Edit/Copy Package to copy my package. After doing so, I fire up WordPad and paste the copied package into the empty document. Now I have a package embedded in the document that when double-clicked will open up an MS-DOS shell.

The final step is to convert the package into a scrap file, and this is done by single-clicking it and dragging it into a Windows Explorer file window. This will create a file named "Scrap", without a file extension. When double-clicked, this file will execute its embedded command (`command.com` in this case) without requiring any confirmation by the user. What's more, a scrap file when executed by Windows will be locked - you can confirm this yourself by following the steps in my above example and notice that when you try to close the opened MS-DOS shell, Windows will pop up with a "Task Not Responding" dialog. A DOS shell started the normal way would not behave this way with no program running inside it.

Inspecting Scrap Files

If you receive a scrap file, you need a way to inspect its contents for malicious code. There is no direct way to do this, like for example right-clicking it in Windows Explorer. Instead you should follow these steps:

1. Open WordPad
2. Drag and drop the scrap file into word pad (make sure you don't accidentally double-click it!)
    - If text appears in WordPad instead of an icon after you drop it, then the scrap file only contained text and was harmless.
    - If an icon appears in WordPad, then there is reason to be wary - the object could contain malicious code; proceed to step three.
3. Right-click the icon and select Package Object/Edit Package. This will open up the package in the Package Editor and you can inspect any commands executed by the package.

Conclusion

You should never double-click a scrap-file before you know what its contents are. This is a flaw in the OLE system that Microsoft should have corrected, given its implications in the security area. Even experienced computer users can be lured into running these files since they might assume that the file is harmless since it has no extension.