

Safe Computing 101

Things are not always what they appear to be...

What colour is the following word.....**GREEN**. Did you say 'green' first then say Blue? Most people will, and it's this kind of mind trick that many virus writers exploit. For example, have a look at the Windows explorer screen shot below. I've circled a file in red. What kind of file is this?

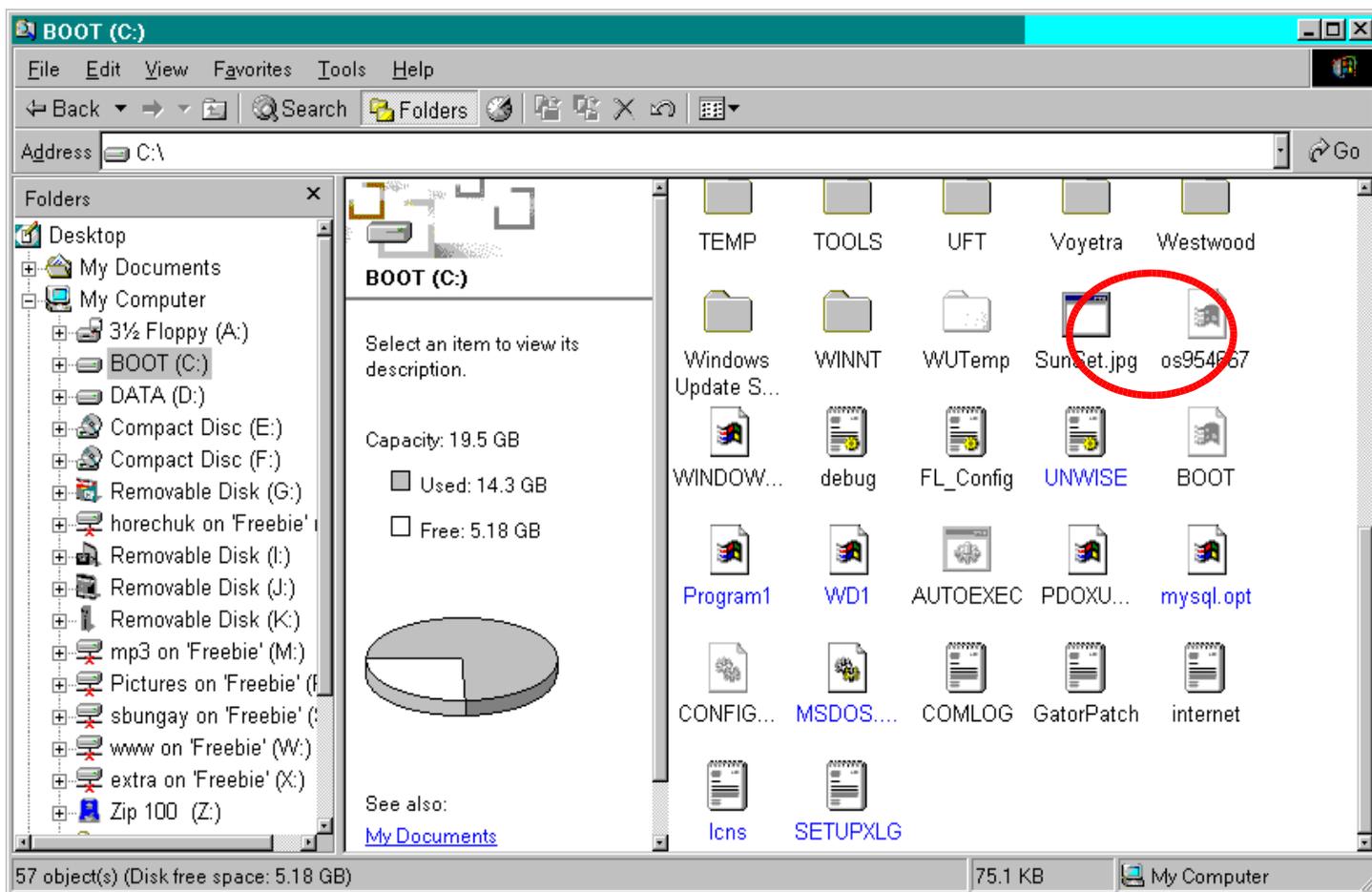


Figure 1

If you said it was a JPG (pronounced "Jay Peg") file then you would be in the majority. Lets double click on it and see the picture. Click click... and you've just been infected by a virus, or perhaps a Trojan, or some other nasty piece of malicious software. Take another look at the file name but this time also pay attention to the icon... it doesn't look like an icon for a picture file does it? Why didn't you notice this the first time? The answer is that your intelligence and higher thought process were taken advantage of. Different parts of the brain are used for reading comprehension skills than are used for image processing and there is a kind of an intuitive disconnect between the two.

Take a look at the screen shot up above one more time and notice that some files have extensions after them and some files do not. Windows, by default, will hide the file extensions for "known file types", and this is the root of our problem. You see, that file I have circled up there is actually called "SunSet.jpg.exe", but Windows "knows" what an EXE file is and it hides the extension from you. Why doesn't it hide the ".JPG" extension too? Windows assumes that only the last three characters of a file name are the extension, and that these last three characters MUST be preceded by a period ".", so it ignores everything to the left (and hides everything to the right) of the last period in the file name.

Now as it happens most people are not aware that Microsoft has done them this "favour", and so when they see the file "SunSet.jpg" they expect (and rightly so) that it is a picture,.. probably of a nice "SunSet", and they double click on it to see it, much to their later regret.

Fixing the “problem”

Now that you understand how you got duped, how do you make it so it doesn't happen again? Open up your Windows explorer and click on the “Tools” menu at the top of the screen... one of the menu items presented in the Tools Menu is “Folder Options”. Select “Folder Options” and the following window should appear (it will look different in different versions of Windows, but they are all pretty close and have the same functionality).

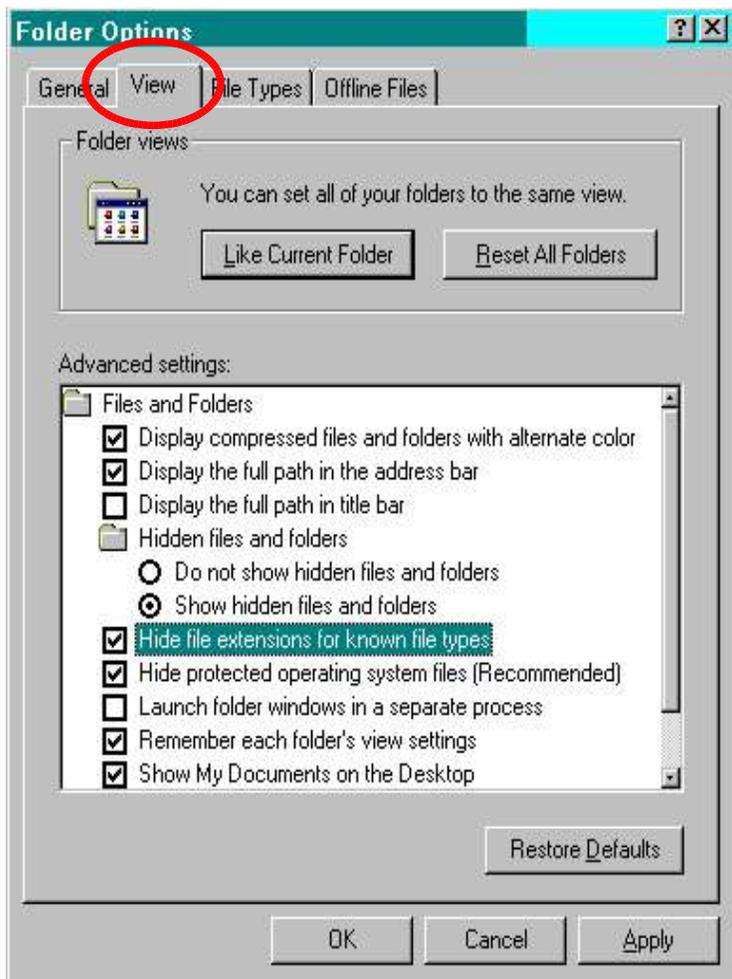


Figure 2



Figure 3

Select the “View” tab (circled in Red in “Figure 2” above) and look for the entry labeled “Hide file extensions for known file types” (it's the one that is shown as being highlighted). Click on the check mark to “uncheck” this item and make it look like “Figure 3” above right.

To make your changes stick you can click on either the “Apply” or the “OK” button. The “OK” button will apply your changes and get rid of the Folder options window allowing you to see and use Windows explorer once again. The “Apply” button will apply your changes but will not close the “Folder Options” window because it assumes that you have more changes to make.

On the next page is the screen shot of what Windows Explorer shows after we have applied our changes to the “Folder Options” window “View” tab. Turn the page and have a peek.

Reality revealed

Once again I've put a red circle around the file in question. You will have to SINGLE CLICK on the file to see the entire name. There's that pesky ".exe" file extension that Windows hid from us. Now we know the picture file wasn't a picture file at all!

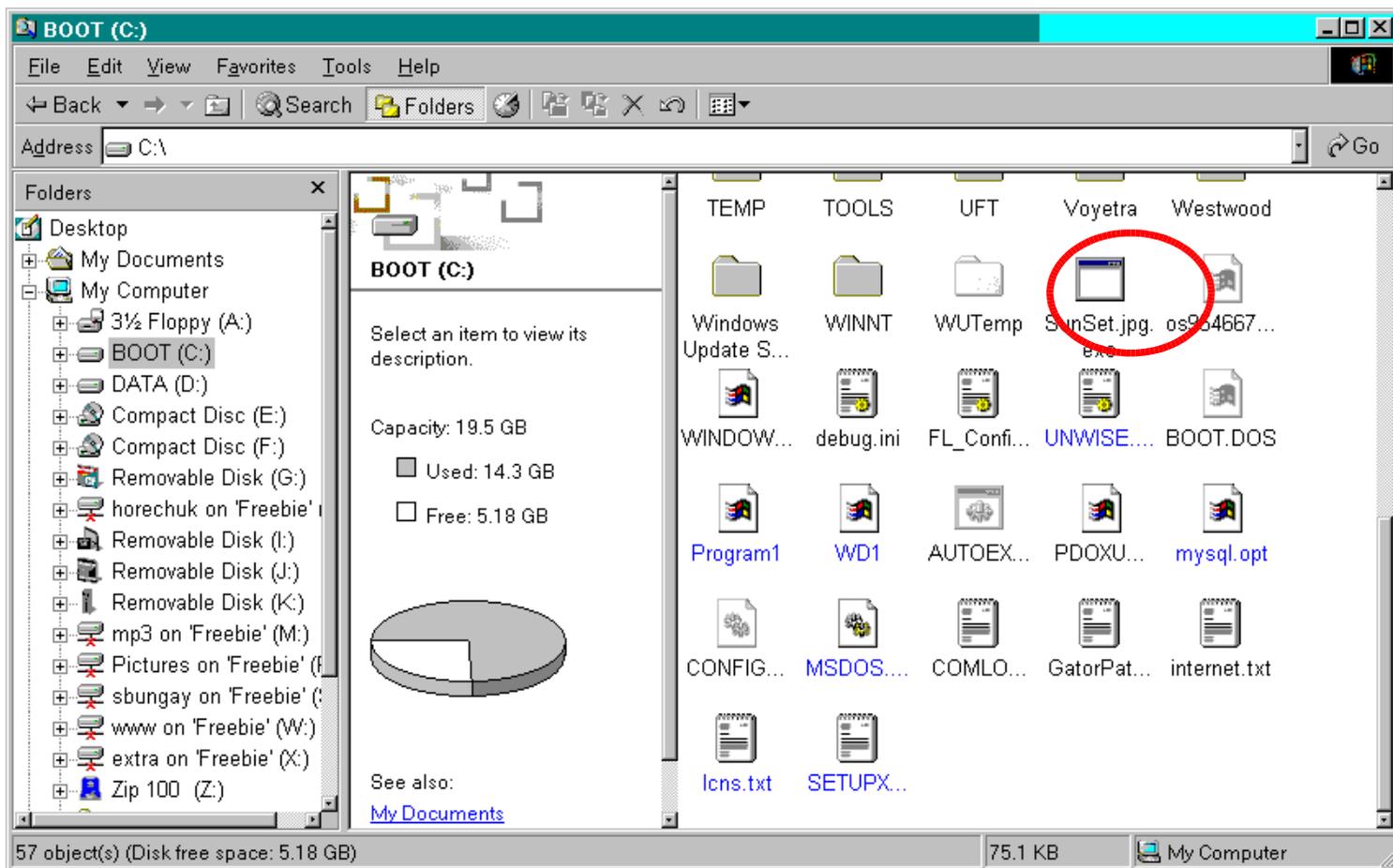


Figure 3

**Computer distress?
Send an SOS!
Call Smarts On Site!**

© 2004 by Stephen A. Bungay

Permission is hereby granted by the author to copy and distribute this document, with no modification, no Front-Cover Texts, and no Back-Cover Texts, as long as this copyright notice and permission notice are included and legible.