

The Abuse of ASSOC Explained

Author : Mi4night

Date : Sunday, January 09, 2011

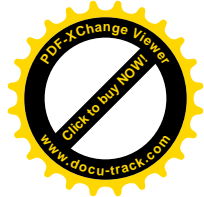


Table of Contents

Introduction.....	2
The Use of ASSOC	Error! Bookmark not defined.
The Evil Use of ASSOC.....	Error! Bookmark not defined.
About	6

Introduction

"The quieter you become the more you're able to hear"

In this paper I will **cover** the use of the command line command ASSOC, and **explain** a little about its **dangerous** use by **malware** coders. What is ASSOC you might ask yourself; well it's a command line application by Microsoft which is found on every Windows Operating System. Its **purpose** is to display or **modify** file extension associations.

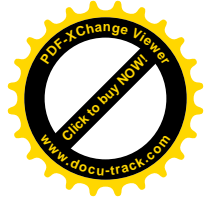
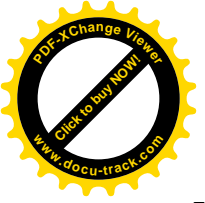
Well that's a really useful command from my point, and I will show you some of the basic uses of this command and afterwards I will also show you how **dangerous** this command can be, and how malware coders may use this command for their purposes.

Keep in mind I wrote this article for learning purposes only, I'm not responsible for your actions.

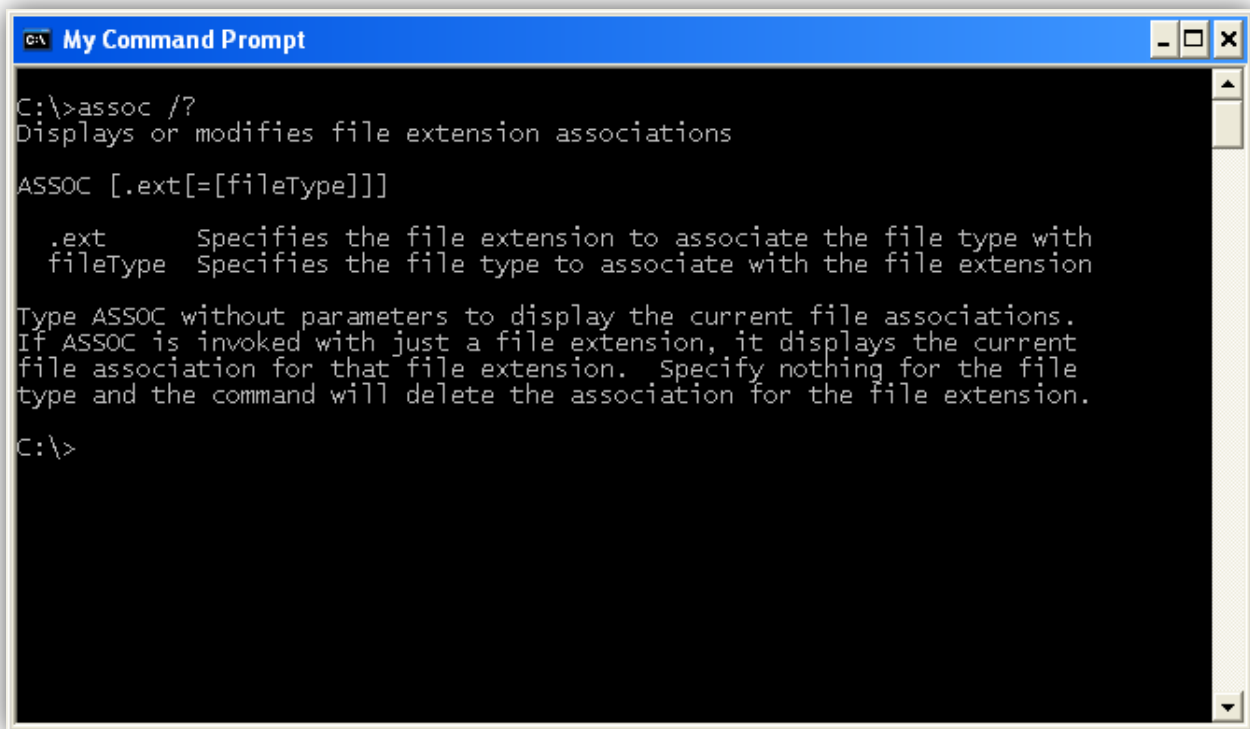
The Use of ASSOC

ASSOC is a Windows based command line command that displays or modifies file extension associations, and it's found on every Windows NT OS, I'm not sure if you can use the command also on Windows 95, Windows 98 or Windows 2000 so you have to try on your own.

The use of ASSOC is pretty simple and as all commands you can request more information/help on the command by typing the command in a command prompt window followed with \?



Example: Type into the command prompt **ASSOC /?** and you will get this output:



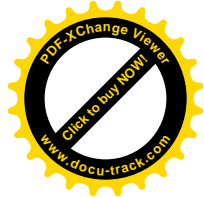
```
C:\>assoc /?
Displays or modifies file extension associations

ASSOC [.ext]=[fileType]]

    .ext      Specifies the file extension to associate the file type with
    fileType  Specifies the file type to associate with the file extension

Type ASSOC without parameters to display the current file associations.
If ASSOC is invoked with just a file extension, it displays the current
file association for that file extension. Specify nothing for the file
type and the command will delete the association for the file extension.

C:\>
```



As you can see it doesn't really have a lot of functionality apart from displaying all existing file extensions and their file associations, to see a list of all associations just execute `assoc` without parameters like in the screenshot below and you'll get the list of associations.

```
C:\>assoc
.xix=
.xlam=
.xlb=
.xlc=
.xls=
.xlsb=
.xlt=
.xltm=
.xltx=
.xm=Winamp.File.xm
.xml=xmlfile
.xpp=SqlServerReplication.Xpp
.xps=XPSViewer.Document
.xsl=xslfile
.xspf=VLC.xspf
.xe=WinRAR
.z=WinRAR
.z96=
.zap=zapfile
.ZFSendToTarget=CLSID\{888DCA60-FC0A-11CF-8F0F-00C04FD7D062}
.zip=WinRAR.ZIP
C:\>
```

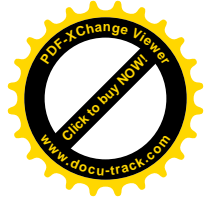
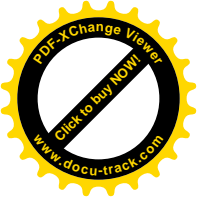
Here you can see a part of my extensions and their file associations.

For example the last line in the command prompt `.zip=WinRAR.ZIP` this line gives a lot of information first the `.zip` tells us that this is an extension `WinRAR` after the equal tells us which application is used to execute the `.zip` file, and at last the `.ZIP` again I'm not 100% sure what this is means but I guess it just shows again the extension which is associated to WinRAR, but I guess I might be wrong I'll look after it later when I finish this article.

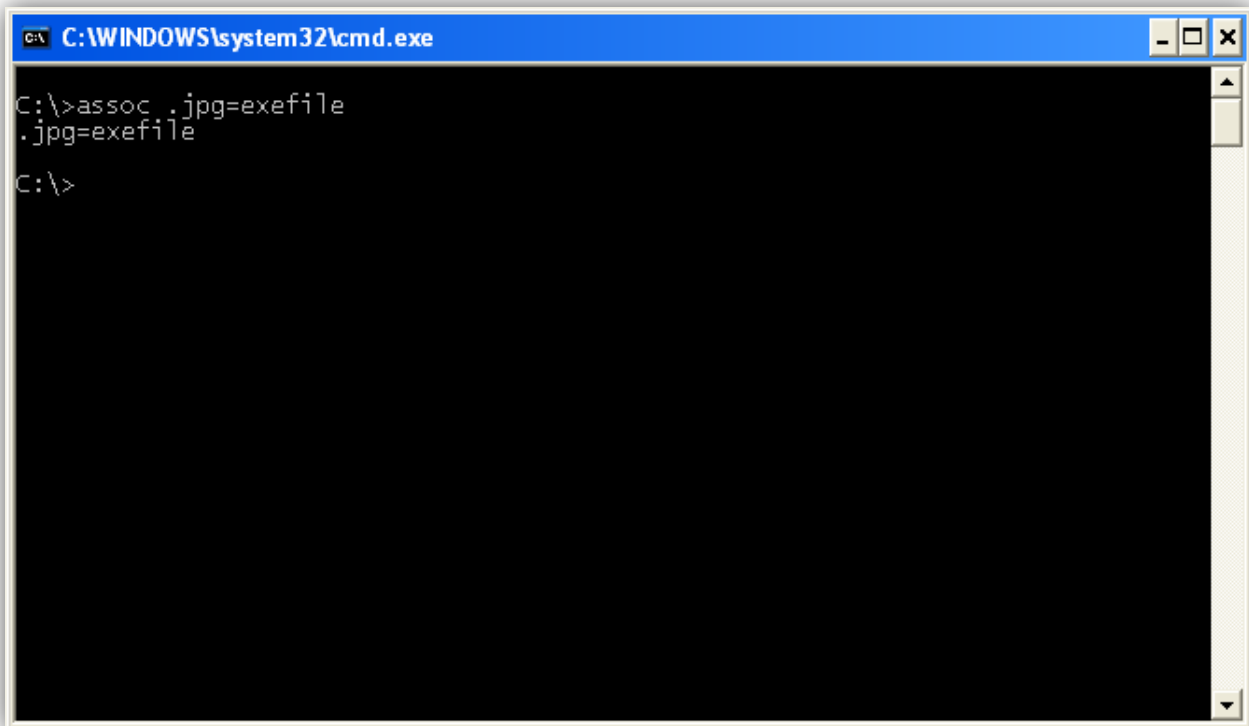
The Evil Use of ASSOC

Now let's talk about the interesting part - the ability to create our own associations or the ability to change existing ones.

Here we will talk a little about how to create our own associations, and we will go deeper and talk about how associations are used for malicious purposes by malware coders and other bad people that want to harm us.



To create our own file association all we have to do is execute assoc with the parameters [.ext=[fileType]] like in the screen below.



```
C:\WINDOWS\system32\cmd.exe
C:\>assoc .jpg=exefile
.jpg=exefile
C:\>
```

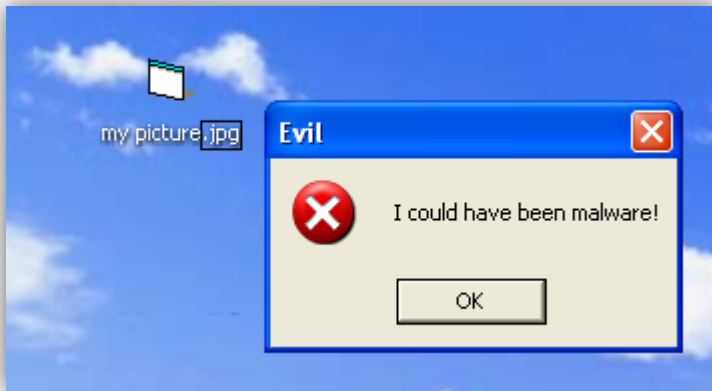
So here we have just changed the association of the .jpg files (Image Files). Now all .jpg files will be treated as an exe file which means they will be able to execute as normal.

You may be thinking that this is harmless. Let's view it from the malware coder's point of view. What a malware coder can now do is for example; send a batch file to his victim that does nothing else than change the file association of a particular extension. Let's say like the victim is a power user that knows how to protect himself, but he executed the batch file, and now he gets an email with an .jpg file in it.

The user downloads it, but he's a smart pc user he has unchecked from [Folder Options >> Hide extensions for known file type](#), and now he can see if he's executing an exe file or not, because he was told that exe files which he receives from people he doesn't know could be dangerous, which in many cases is true.

But he has just forgotten that malware coders are smart too. The malware coder has changed the icon of the exe file to make it look like a .jpg file and he has changed the extension to .jpg to make sure the user doesn't end up seeing an unknown icon when he wants to view the image.

To have a better understanding of what I'm saying I have created a simple exe file that displays a Message Box. I have also unchecked Hide extensions for known file types so you can see the extension of the file.



The fake image is executed and any code could have been executed, not just a Message Box. This article was meant to teach you to be more careful and not trust any files that you receive from anyone or even new files that you find on your system. The methods shown in this article can also be achieved using the windows registry by changing or adding registry keys, but that's something you can find on your own or if asked, I will explain it in another article.

In my next article I will talk about the way to execute files with non executable extension without the use of associations.

About

I'm just like all the people out there who can't stop digging inside computer systems. My passions are computer security, programming, networking and everything else that has to do with computers.

This is my first article that I have ever written, and I hope I can help a lot of people with further articles, tutorials and other stuff to the security/programming communities that have always given me a bunch of information and feedback to achieve more and more.

Thank you for taking the time to read this article!

For any suggestions or questions you can contact me at mi4night@hotmail.com.

Thanks to all of my friends out there, and greetings to Sys32-Hack, nuclear, Slaylord7, Pro-Tec and all www.ic0de.org and www.opensc.org members sorry if I didn't mention all but you know that I mean you guys who helped me all this years also I greet those who are not anymore in the scene.