




Can't Copy or Cut in Firefox?

 Posted on Monday 1st May 2006 @ 3:04pm BST

This entry has been updated. See [bottom of page](#) for updates.

A few weeks ago I heard about [PHP Architect magazine](#) and wanted to read a trial issue to see if it was any good. On their website, they were asking for too many personal details to download a free trial so I decided to see if there were any copies floating around on the file-sharing networks. This was a big mistake!

The first file I downloaded was a setup.exe file. Thinking this was a self extractor for the book and source code (...hey, Microsoft did it for the VB 2005 Express source code and pdf book I believe!) I ran the setup file. I couldn't find where it had installed the magazine anywhere! Anyway... it wasn't long before I soon discovered that I couldn't cut or copy stuff from Firefox.

I tried a lot of things, ran dozens of leading spyware destroyers and it still didn't fix it. Many Google searches later, I [believed it must be a bug](#), I waited patiently for a bug fix. When the [bug was apparently fixed in Minefield](#), I gave the new Firefox build a go but the cut/copy flaw was still there (however I could still paste in stuff from other applications).

I wasn't convinced this was a bug in Firefox but anyway... I had tried everything and it was still not working so I switch to Opera.





Then this morning I disabled Norton Internet Security and CSS pop-ups appeared on the Google homepage in both Firefox and Opera!!! I checked the Norton Internet Security Activity logs and whenever I opened up Firefox (where the homepage is the standard Firefox Google page) it also tried to connect to <http://www.Iduhtrp.net/image-1848326-10417792> which redirected to <http://advertismen.com/getads.php?id=15> and displayed a crap popup.

I came back to [this bug report](#) and tried the [afirefox.exe trick](#). It worked! So I was sure this was malware.

So I updated and re-ran all the usual spyware destroyers – nothing! Installed, updated and ran [Windows Defender](#) – nothing! I played around with Defender and accidentally turned on “join Microsoft SpyNet with advanced membership”. Little did I know that this means that if Defender detects any changes made by unclassified software it will inform you of the changes and ask you what you want to do....

Since my system was already infected I saw no harm in running the original malware install file again. This time I read the EULA...

> **PREFACE. You are about to install the following program:**

> **Software developed for advertismen.com:**

...blah blah....

> **It adds discreet advertisements to your Internet Explorer, Netscape, Opera or**

> **Firefox browser windows that will display links to internet tools and pages.**

It also mentioned that this software could be removed using the Add/Remove Programs feature in Control Panel. After hunting around it seemed that this wasn't the case. **There is no uninstaller for this malware/adware despite the EULA saying that there is.**

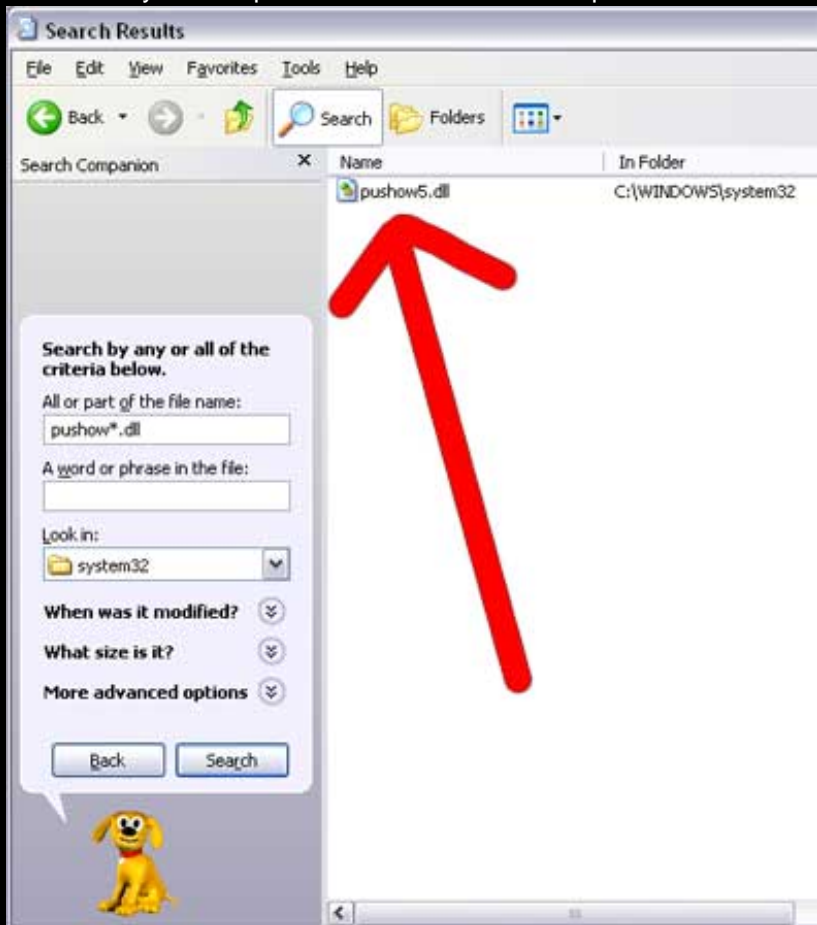
Clicked install and suddenly Windows Defender sprung up telling me that the b*gger was trying to alter the registry and install some files in the system32 folder. Even more helpful... it told me exactly which registry keys and which files it was installing.

I removed the offending items and my system is completely fixed!! Completely!!! It feels so good to have a normal firefox installation working which I can cut and paste in!

Since the instructions require you to close any open browsers, you might like to [download a text version](#) for opening in notepad instead. Thanks to Jimmy for this tip :)

Ok, here is what you need to do to remove the **Avertisemen.com** malware: -

1. **Important!** Close all **Firefox**, **Opera** and **Internet Explorer** windows.
2. Click Start > Run...
3. Type "regedit.exe" and press OK.
4. Get to the following location in the registry: -
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows
5. In the pane on the right-hand side of regedit you should see a String called "AppInit_DLLs" with a value of "pushow**.dll" where ** is some random number.
6. Right-click on this String and click Delete.
7. Click Start > Run...
8. Type "C:\windows\system32\" and press OK.
9. Click on the Search toolbar button in the explorer window that just appeared.
10. Click "All files and folders" on the search panel that has appeared on the left hand side of the window.
11. Where it says "All or part of the file name:" enter "pushow*.dll" and click Search.



12. Once the search has finished select the pushow**.dll file (there will be multiple copies if you ran the setup file more than once). **Delete** the file or files.
13. Start Firefox and feel really good at being able to cut and paste properly again :)

Firefox is a great piece of open source software. It seems it wasn't a bug after all but a piece of malware that affected most major web browsers. If anything, Firefox was the only browser that flagged up any problems and I doubt I would have worked it out otherwise... Hopefully this will have fixed your problem. I've spent many, many, many hours trying to fix this so it would be great if you could drop me an email saying thanks if this works for you.

Update 2006/05/02 A guy named Chris emailed me to say that he was having trouble deleting the file. Windows reported that the file couldn't be deleted because it was locked - in-use. He used a piece of freeware called

Unlocker to successfully unlock the file and delete it. It can be downloaded from [here](#).

Update 2006/05/04 **As soon as I found out about this piece of malware I uploaded it to the Symantec response centre along with a link to my blog entry on this malware. I got an email from Symantec a few days ago thanking me for the sample, accurate info and apparently “The Patrick Kavangh quote was cool also”. :) Not sure who Patrick Kavangh is or where I have quoted him but anyway... Symantec have updated their definition files and after downloading the latest RapidRelease files from the [Symantec ftp site](#), Norton Internet Security will now pickup the adware/malware!**

Update 2006/06/20 **Jimmy emailed me to say “perhaps you could save the instructions in a txt file? i wanted to copy/paste your instructions so i could close firefox to remove adware.. and i’m sure you could see how that was a problem” Well Jimmy, I’ve done just that... you can now [download a text version](#) :).**

[Most Recent Posts](#) [About Me](#) [Contact Me](#)