

Re: Unidentified Files

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-02/0039.html>

From: Frank Saunders, MS-MVP IE/OE (franksaunders_at_mvps.org)

Date: 02/01/05

Date: Tue, 1 Feb 2005 06:06:54 -0600

"Edward W. Thompson" <thomeduk1@btopenworld.com> wrote in message news:uP\$06BECFHA.1260@TK2MSFTNGP12.phx.gbl

- > *I have recently acquired several files of the form BQSHYJ2R.ocx in the*
- > *Windows folder. From a 'Goggle' search I understand these files are*
- > *associated with ActiveX controls but in what respect I couldn't*
- > *determine.*
- > *Are these files dangerous in any way and require removal or are they*
- > *an essential part of the 'system'?*

Right click it and choose Properties. Go to the Version tab. It should tell you what it is and where it is from. If it doesn't or you don't recognize it as something you want, delete it. If it's something you need you will be asked to download it again.

The fact that it isn't in Downloaded Program Files is suspicious. I would also do the following:

First eliminate any spyware.

What You Should Know About Spyware

<http://www.microsoft.com/athome/security/spyware/deviuoussoftware.mspx>

CAUTION!!!! Removing some spyware can damage the Winsock stack. Before you try to remove spyware using any of these programs, download a copy of LSP-Fix – a free program to repair damaged Winsock 2 stacks (all Windows versions)

<http://www.cexx.org/lspfix.htm>

Winsockfix for W95, W98, ME, NT, 2000, XP

<http://www.tacktech.com/pub/winsockfix/WinsockFix.zip>

Directions here: <http://www.tacktech.com/display.cfm?ttid=257>

WinXP:

Get WinSockxpFix

<http://www.spychecker.com/program/winsockxpfix.html>

How to Reset Internet Protocol (TCP/IP) in Windows XP

<http://support.microsoft.com/kb/299357>

In WinXP SP2: You can fix Winsock by going to Start | Run and typing CMD

In the command window type

netsh winsock reset

See

Dealing with Unwanted Malware, Parasites, Toolbars and Search Engines

<http://mvps.org/winhelp2002/unwanted.htm>

Note that AdAware and SpyBot S & D will each catch some things the other won't. Also, each needs to be updated with the program's update function before every use, even when just downloaded. There's also a lot more to do than just those two programs. CWShredder is also available here:

<http://www.intermute.com/products/cwshredder>

**Post your HijackThis log to

<http://www.spywareinfo.com/forums/>

<http://forums.tomcoyote.org/>

<http://castlecops.com/forum67.html>

<http://www.wilderssecurity.com/> or the Spyware forum at

<http://forum.aumha.org/viewforum.php?f=30> for expert analysis, not here.**

Alternative download pages for Ad-Aware, Spybot, HijackThis and CWShredder may be found on this page:

<http://aumha.org/a/parasite.htm>.

See this link for information about malware:

<http://arstechnica.com/articles/paedia/malware.ars>

If nothing there helps, please post back to this thread.

--

Frank Saunders, MS-MVP, IE/OE

Please respond in Newsgroup only. Do not send email

<http://www.fismjs.com>

Protect your PC

<http://www.microsoft.com./athome/security/protect/default.aspx>

<http://defendingyourmachine.blogspot.com/>