

Re: IEsp.mht

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6.browser/2004-07/7248.htm>

From: LuckyStrike (*LS_at_smokedamagedfurniture.youcandriveitawaytoday.com*)

Date: 07/27/04

Date: Tue, 27 Jul 2004 15:57:32 -0600

Geoff -

It sure sounds like this to me:

<http://www.pchell.com/support/onlythebest.shtml>

Then there is this from Jim Byrd MS-MVP. (Copied and pasted below. Thanks Jim) :

<paste>

I'm informed that the 01R325 AdAware update of 6/28 or later supposedly completely removes this for some variants/malware implementations; however, I haven't been able to independently verify this and have also heard contrary info. Try it first (UPDATED and then from Safe mode), and if it doesn't work then:

See these threads first:

<http://zerosrealm.com/index.php?page=dllfix> (Read very carefully!)

<http://forums.spywareinfo.com/index.php?showtopic=7447>

<http://forums.spywareinfo.com/index.php?showtopic=7261>

<http://forums.spywareinfo.com/index.php?showtopic=7281>

Then from merijn, here: <http://www.spywareinfo.com/~merijn/index.html>

June 18, 2004:

Please stop emailing me about the new CWS variant that hijacks you to res://<random>.dll/sp.html#96676. I am aware of this new thing, but it's a beast to remove.

A solution is being worked on, see this thread on the SWI forums

<http://forums.spywareinfo.com/index.php?showtopic=7447>.

If it's not working for you, or it's too complicated, I heard from several people that this workaround works as well:

Open the DLL you get hijacked to in Notepad

Select all content (Ctrl-A) and delete it

Save the file and exit Notepad

Re: IEsp.mht

Find the file in Explorer, right-click it, select Properties, put a checkmark in 'Read-Only' and click OK.

If you can't find the DLL file, make sure your settings allow you to view "Hidden files". Open up any explorer windows and click on "Tools", "Folder Options", "View" and be sure to check off "Show Hidden Files and Folders".

</paste>

~~~~~

Quick and basic scans from any of the following sites:

Doxdesk parasite scan

<http://doxdesk.com/parasite/>

Jim Eshelmans WSC on-line quick scan

<http://www.aumha.org/a/noads.htm>

Bugs Glitches and Stuff-ups

<http://inetexplorer.mvps.org/Darnit.htm>

More In-Depth on-line scanners for parasites and Trojans:

GFI free on-line Trojan scanner

<http://www.windowsecurity.com/trojanscan/>

Sygate Technologies Trojanscan

<http://scan.sygatetech.com/pretrojanscan.html>

PestPatrol on-line scan

<http://www.pestscan.com/home.asp>

SpywareChecker on-line scan

[http://www.spywareguide.com/txt\\_onlinescan.html](http://www.spywareguide.com/txt_onlinescan.html)

Parasites, spyware malware basics:

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

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

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

Check for Spyware:

\*Most important\* – Before you try to remove spyware using any of the following programs, realize that the process of cleaning and removing certain spyware and malware may possibly interrupt and kill your internet connection. Therefore, you should obtain a copy of LSPFIX, and Winsockfix which will then make it possible for you to re-establish your internet connection if it gets terminated.

Download LSPFIX from either of the following sites:

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

<http://www.spychecker.com/program/winsockxpfix.html> (For Win2k or XP)

Download Winsockfix here

<http://members.shaw.ca/installations/WinsockFix.zip>

Then, install the respective programs and then update them immediately, so that they have the current versions, and definitions. Read the Help Files and Tutorials.

After you've Updated Spybot S & D, and SpywareBlaster, you \*must\* ENABLE the protections as well. These two programs do not automatically enable the newest definitions and updates, so this process but must be done by you manually.

Run them one at a time. With Ad-Aware you may have it generally clean whatever it finds. The same applies for CWShredder. Spybot S&D requires special attention (listed below), as does HijackThis (Only more so. Details listed below) The programs are listed in order of their general strength, safety, and purpose. It is perhaps best to install and run these in this order of appearance. All are freeware programs, but if you are pleased with the results and quality of the utilities, donations to the respective Authors are cheerfully accepted.

Another thing to consider doing is to run a program (only run one program at a time) a few times consecutively. The reason for this is that the first pass may kill certain Spyware programs, but may not be able to terminate and kill all files and programs which may be running at the time. That is why a second pass may be necessary to be thoroughly effective.

Also, under the most stubborn cases, running the programs in Safe-Mode will allow for the best cleaning conditions, as there will be a minimum of interference from processes running in the background.

Ad -Aware

<http://www.lavasoftusa.com/support/download/>

Ad-Aware Tutorial (might help if you look through this)

<http://www.bleepingcomputer.com/forums/index.php?showtutorial=48>

CWShredder (cleans all Cool Web Search malware)

<http://www.majorgeeks.com/download4086.html>

CWShredder Tutorial

<http://www.bleepingcomputer.com/forums/index.php?showtutorial=47>

Coolwebsearch Smartkiller

<http://www.safer-networking.org/files/delcwssk.zip>

The above item is sometimes necessary if CWShredder detects a SmartSearch2 variant on your PC.

Spybot S&D

<http://www.safer-networking.org/index.php?page=download>

Spybot Tutorial (Must Read)

<http://www.safer-networking.org/index.php?page=tutorial>

Other tutorials for Spybot S&D (Also must read)

<http://www.bleepingcomputer.com/forums/index.php?showtutorial=43>

<http://tomcoyote.com/SPYBOT/index1.php>

<http://tomcoyote.com/SPYBOT/index2.php>

This item below is designed to \*prevent\* installation of malware and the like by comparing known CLSID's of these "bad guys" with what is in its

definitions. By enabling a \*Kill Bit\* it prevents known malignant ActiveX from being installed or run on your machine. It doesn't remove anything, nor will it fix anything that is already in your PC. Rather, it will prevent installation or re-installation of the item once it has been removed either manually, or by the use of another program which will perform the duty of removing the spyware.

SpywareBlaster (prevents installation of spyware, Trojans, etc.)

<http://www.javacoolsoftware.com/spywareguard.html>

SpywareBlaster Tutorial

<http://www.bleepingcomputer.com/forums/index.php?showtutorial=49>

SpywareGuard (companion program to SWB, above)

<http://www.javacoolsoftware.com/spywareguard.html>

SpywareGuard Tutorial

<http://www.bleepingcomputer.com/forums/index.php?showtutorial=50>

If you use Spybot S & D, be sure to clean \*ONLY\* the items displayed in \*RED\*. DO NOT clean any items displayed in Black or Green at this time.

Lastly there is HijackThis. Hijack this is a very powerful, last resort type of program which is generally best used in conjunction with help from those who deal with the findings of the log created by the HijackThis scan.

It does nothing in the scan itself; it merely says what is in and running on your PC. The items must be checked-marked to be "cleaned". You must know \*exactly\* what you are checking-off before you proceed.

If you don't, you can quite possibly disable many useful and vital functions of your PC. Remember; read the Tutorials, and seek help at SpywareInfo Forums, Net-Integration, or TomCoyote forums for safety's sake.

HijackThis

<http://www.spywareinfo.com/~merijn/downloads.html>

If the preceding site is down, you may get HijackThis from Major Geeks (amongst other sites as well)

Hijack This (from Major Geeks)

<http://www.majorgeeks.com/download3155.html>

HijackThis Tutorials **\*\*(MUST READ)\*\***

<http://www.spywareinfo.com/~merijn/htlogtutorial.html>

<http://www.bleepingcomputer.com/forums/index.php?showtutorial=42>

<http://hjt.wizardsofwebsites.com/>

Where to seek help with your HijackThis scan log

SpywareInfo Forums

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

other help forums for HijackThis:

Net-Integration

<http://forums.net-integration.net/index.php?c=19>

TomCoyote

<http://forums.tomcoyote.com/index.php?showforum=27>

Anti-Virus Tools

AVG Anti-virus by Grisoft

<http://free.grisoft.com/freeweb.php/doc/2/Ing/us/tpl/v5>

avast! Virus Cleaner – free virus & worm removal tool

[http://www.avast.com/eng/avast\\_cleaner.html](http://www.avast.com/eng/avast_cleaner.html)

McAfee AVERT Stinger

<http://vil.nai.com/vil/stinger/>

NOTE: With the above tools, particularly Avast Virus cleaner, be sure to disable your background PC Anti-virus utility.

F-Prot for DOS (I don't know if this will work on XP systems however)

[http://www.f-prot.com/products/home\\_use/dos/](http://www.f-prot.com/products/home_use/dos/)

[http://www.f-prot.com/products/home\\_use/](http://www.f-prot.com/products/home_use/)

<http://www.claymania.com/f-prot.html>

If you can use this program, be sure to make certain the most recent Updates are obtained for it.

[http://www.f-secure.com/download-purchase/dos\\_updates.shtml](http://www.f-secure.com/download-purchase/dos_updates.shtml)

F-Secure Anti-Virus for DOS (F-PROT edition)

Update Macro.def to your system to get up-to-date macro virus protection.

The other Anti-Virus databases, Sign.def and Sign2.def are updated weekly.

They have definitions for all other kinds of viruses except macro-viruses.

MACRO.DEF definition file

SIGN.DEF definition file

SIGN2.DEF definition file

On-Line Virus scanners:

RAV Antivirus Online Virus Scan

<http://www.ravantivirus.com/scan/>

Command on Demand

<http://www.authentium.com/solutions/cod/index.cfm>

Freedom on-line virus check

<http://www.freedom.net/viruscenter/onlineviruscheck.html>

TrendMicro Housecall (also detects some Trojans)

<http://housecall.trendmicro.com/>

BitDefender Scan Online

<http://www.bitdefender.com/scan/licence.php>

Kaspersky Online Virus Scanner

<http://www.kaspersky.com/remoteviruschk.html>

The above scanner works differently from most; it is a server based scanner, and will only scan individual files, or directories which are

limited  
to 1 MB in total size. It will not do a full system scan.

Hauri LiveCall Online virus scanning  
<http://www.globalhauri.com/html/products/livecall.html>  
The above is also server based if I remember correctly

Panda on-line virus scan  
<http://www.pandasoftware.com/activescan/activescan.asp>

McAfee FreeScan  
<http://us.mcafee.com/root/mfs/default.asp>

Symantec Security Check (page offers security and/or virus scan)  
<http://snipurl.com/7gz1>

More general info you should be aware of:  
The Parasite Fight; Quick Fix Protocol  
<http://www.aumha.org/a/quickfix.htm>  
How to surf the Internet more safely with Internet Explorer  
<http://www.infinisource.com/techfiles/surf-safe.html>  
So how did I get infected in the first place?  
<http://boards.cexx.org/viewtopic.php?t=957>  
Rogue/Suspect Anti-Spyware Products & Web Sites  
[http://www.spywarewarrior.com/rogue\\_anti-spyware.htm](http://www.spywarewarrior.com/rogue_anti-spyware.htm)

HTH –  
--

LuckyStrike  
LS@smokedamagedfurniture.youcandriveitawaytoday.com

How to make a good newsgroup post:  
<http://www.dts-l.org/goodpost.htm>  
<http://home.satx.rr.com/badour/html/post.html>

---

"Geoff Saunders" <anonymous@discussions.microsoft.com> wrote in message  
news:530a01c47410\$f89157b0\$a301280a@phx.gbl...

> *Does anyone know what this is? It appeared 2 days ago and*  
> *seemed to take control of the PC. It replaced*  
> *www.wanadoo.fr as my Default Address in my Browser and*  
> *everytime I tried to exit it, it came back. The PC was*  
> *being heavily used even tho I was doing nothing.*  
>  
> *Eventually I did a restore, and deleted the file, but it*  
> *keeps coming back – it seems to be in the boot program*  
> *somewhere.*  
>  
> *Initially I found it in: res://c:\DOCUME1\Geoff\LOCALS1*  
> *\Temp\drive.res/error.htm#[http://sendweb2.com/passthrough/](http://sendweb2.com/passthrough/index.html?http.c:\windows\SYSTEM32\IEsp.mht)*  
> *index.html?http.c:\windows\SYSTEM32\IEsp.mht*

- >
- > *Now in Tools, Internet Options, Home Page Address it*
- > *replaces the normal homepage but I can backspace it out*
- > *and click on Current to get to where I want to be.*
- >
- > *How do I get rid of it? I have Searched, found and*
- > *deleted a dozen times now.*