

Re: ie,...again

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6.browser/2004-09/4824.htm>

From: Jan Il (abuse_at_localhost.com)

Date: 09/20/04

Date: Mon, 20 Sep 2004 13:50:40 -0700

Hi Pussn :-)

> *I should have also mentioned in my first post that I have*
> *absolutely no access to any of the four accounts on the*
> *pc. As soon as I try one, it says 'loading personal*
> *settings', then promptly shuts down, logging off etc. So*
> *there is NO way I can install a program on that pc. I've*
> *tried safe mode, and I'm still getting the same results.*
> *This suuucks.*

Okie Doke! Here are a couple of AV's you can use and run from DOS, and hopefully, they may kill enough of the junkware to allow you access the Windows Explorer and run the other cleaning programs.

F-Prot - Home Use - Free

http://www.f-prot.com/products/home_use/win/

Here is how to create the 3.5 floppy disks to run it from.

<http://crowleys.crsc.k12.ar.us/documents/fprot.htm>

Follow all the instructions carefully. Prepare the floppy's from the other machine to run on yours.

and

AVG6 Free:

http://www.grisoft.com/us/us_dwnl_free.php

Copy AVG files to the hard drive and then follow the steps here:

Start the computer in MS-DOS mode (hold down F8 key while computer is booting up, then from Windows start-up menu select "start in MS-DOS mode" or "Command prompt only").

Switch to AVG Anti-Virus destination folder using these steps (assuming this is the path AVG is installed to) C:\Program Files\Grisoft\AVG6 as destination folder):

Start AVG for MS-DOS application: avg

In this DOS application, every feature could be selected by pressing the key

with other color (or the key in combination with ALT key). So it is necessary to choose the Test menu, Complete test item, and start the test. Select "Heal virus"

In case of infection of some system files should be necessary to reinstall operating system, to restore the files from backup or to extract the files from installation *.cab archives .

Or...install the AVG on the other machine and then burn the folder to the CD. Try to copy the folder to the hard drive of your machine and run from there, but, if not, then try to run it from the CD, using the path to the CD as the location. Don't know about that for sure, but.....you can try. :-)

Please post back with the results and any error messages you may get.

Jan :)

Smiles are meant to be shared,
that's why they're so contagious.

Please reply to the newsgroup so others may benefit.
Replies are posted only to the newsgroup for the benefit of other readers.

How to make a good newsgroup post:
<http://www.dts-l.org/goodpost.htm>

>
>
>
>> -----Original Message-----
>> Hi Pussn :-)
>>
>> *Don't give up so easy! So.....let's work together a bit here and
>> try to take back your PC. :-))*
>>
>> *(NOTE: If you can not download these programs from the Internet, if
>> your PC has CD read capabilities, go to another computer with CD-
>> ROM burning capabilities. Create a folder on the hard drive of the
>> other computer called HOLD, download the programs to that folder,
>> then burn that folder to a CD. Copy the HOLD folder to your HD and
>> then install the programs from there and run them. After you have IE
>> access again, update all programs where possible to get the latest
>> definitions and run them again to be sure there are no lingering
>> items on the system.) Hopefully, you know someone with a PC you
>> can use that has CD burner capability, or go to a public library.
>>*
>> *Understand that reinstalling IE or your OS at this point will not
>> resolve the problem, and may even make it worse, so please, DO NOT
>> try to reinstall anything until you have cleaned your system. Do
>> the following, and the parts you can't do from your PC, do from
>> another, but, do them. We can't do the work there for you there,
>> so, this is your end of the partnership. <g> However, if at any time
>> you have a question or problem, post back here and we'll help you*

>> work through it. OK? :-))
>> ~~~~~
>> Please follow all instructions carefully:
>>
>> Courtesy of Jim Byrd:
>>
>> Sounds like this might be a variant of some malware called
>> CoolWebSearch (if CWShredder doesn't fix it, then see AdAware,
>> SpyBot, and HijackThis, below, in that order). Do the following:
>>
>>
>> #####IMPORTANT#####
>> Before you try to remove spyware using any of the programs below,
>> download both a copy of LSPFIX here:
>>
>> <http://www.cexx.org/lspfix.htm>
>>
>> AND a copy of Winsockfix
>> <http://www.tacktech.com/pub/winsockfix/WinsockFix.zip>
>> Directions here: <http://www.tacktech.com/display.cfm?tid=257>
>>
>> The process of removing certain malware may kill your internet
>> connection. If this should occur, these programs, LSPFIX and
>> WINSOCKFIX, will enable you to regain your connection.
>>
>> NOTE: It is reported that in XP SP2, the command
> netsh winsock reset
>> will fix this problem without the need for these programs.
>> #####IMPORTANT#####
>>
>>
>>
>> #####IMPORTANT#####
>> All of the following removal tools should be run from Safe mode when
>> possible.Reboot and test if the malware is fixed after using each
>> tool. #####IMPORTANT#####
>>
>>
>> Download and run Stinger.exe, here:
>> [http://download.nai.com/products/mcafee-](http://download.nai.com/products/mcafee-avert/stinger.exe)
> avert/stinger.exe or from the link
>> on this page: <http://vil.nai.com/vil/stinger/>
>>
>>
>> Download sysclean.com, from Trend Micro, here:
>> <http://www.trendmicro.com/download/dcs.asp> along with the latest
>> pattern file, here:
> <http://www.trendmicro.com/download/pattern.asp> (You
> might also
>> want to get Art's updater, SYS-UP.Zip, here for future updating of
>> these: <http://home.epix.net/~artnpeg/>). Place them in a dedicated

>> folder after appropriate unzipping, and then run. (If you download
>> and use the updater from the beginning, it will automatically handle
>> downloading the other files.)
>>
>>
>> Sometimes the tools below will find files which they are unable to
>> delete because they are in use. A program called Copylock, here,
>> <http://noeld.com/programs.asp?cat=misc#CopyLock> can aid in the
>> process of "replacing, moving, renaming or deleting one or many
>> files which are currently in use (e.g. system files like
>> comctl32.dll, or virus/trojan files.)"
>>
>>
>> Download, UPDATE before running, and run:
>> <http://209.133.47.200/~merijn/files/CWShredder.exe> or here:
>> <http://hem.bredband.net/b157129/f/cwshredder.zip> or here:
>> <http://www.softpedia.com/public/scripts/downloadhero/10-17-150/> or
>> here: <http://www.zerosrealm.com/downloads/CWShredder.zip>
>> to remove the parasite. Be sure to close all instances of IE and OE.
>>
>> There's a good tutorial about CWS and using CWShredder here:
>> [http://www.bleepingcomputer.com/forums/index.php?](http://www.bleepingcomputer.com/forums/index.php?showtutorial=47#domain)
>> [showtutorial=47#domain](http://www.bleepingcomputer.com/forums/index.php?showtutorial=47#domain)
>>
>> BE SURE that you get v.1.59.0.1 or later!
>>
>> You will need to show Hidden files first and then at the end clear
>> the malware garbage from your System Restore backups after you've
>> cleaned up. It's best to perform CWShredder (and most other malware
>> fixers too) from Safe mode and then reboot. AFTER cleaning things
>> up, then you can disable and then re-enable System Restore. See
>> ***** below.
>>
>> The following links give instructions on how to do these various
>> functions:
>>
>> HOW TO Restart in Safe Mode
>> [http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/](http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2001052409420406)
>> [2001052409420406](http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2001052409420406)
>>
>> HOW TO Enable Hidden Files
>> [http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/](http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2002092715262339)
>> [2002092715262339](http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2002092715262339)
>>
>> HOW TO Disable/Flush System Restore (do this at the end AFTER
>> cleaning or use the suggested procedure for XP at the *****'s)
>> [http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/](http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2001111912274039)
>> [2001111912274039](http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2001111912274039) (WinXP)
>> [http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/](http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2001012513122239)
>> [2001012513122239](http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2001012513122239) (WinME)
>>

>> Then download and run:
>> http://www.kellys-korner-xp.com/regs_edits/iegentabs.reg to restore
>> your tabs and remove any restrictions that the parasite has put in
>> place.
>>
>> Now download and run:
>> http://www.kellys-korner-xp.com/regs_edits/RestoreSearch2.REG to restore
>> your search functions if they've been affected (as they probably
>> will have been).
>>
>> Be sure that you also download and install hotfix Q816093, here:
>> <http://support.microsoft.com/?kbid=816093>
>> which blocks the exploit upon which this parasite family depends.
>>
>> However, this also indicates that you may have acquired some other
>> malware along the way. If you go to this page at Jim Eshelman's
>> site, here: <http://aumha.org/a/noads.htm> and wait a little bit (be
>> patient), an analysis of a number of possible parasites on your
>> machine will be made to help you identify and remove them. NOTE: You
>> will need to disable Ad Blocking in Zone Alarm 3.x or later, if
>> present or any other Ad Blocking software which interferes with Java
>> Scripting for this scan to work. You should get a message between
>> the two lines of **** giving the results of the scan.
>>
>> Get Ad-Aware SE Personal Edition, here:
>> <http://www.lavasoftusa.com/support/download/>. UPDATE, set it up in
>> accordance with this:
>> <http://forum.aumha.org/viewtopic.php?t=5877> or the
>> directions immediately below and run this regularly to get rid of
>> most "spyware/hijackware" on your machine. If it has to fix
>> things, be sure to re-boot and rerun AdAware again and repeat this
>> cycle until you get a clean scan. The reason is that it may have to
>> remove things which are currently "in use" before it can then clean
>> up others. Configure Ad-aware for a customized scan, and let it
>> remove any bad files found.....
>>
>> <Begin Setup Directions>
>> Then, courtesy of NonSuch at Lockergnome, open Ad-aware then click
>> the gear wheel at the top and check these options to configure Ad-
>> aware for a customized scan:
>>
>> General> activate these: "Automatically save log-file" and
>> "Automatically quarantine objects prior to removal"
>>
>> Scanning > activate these: "Scan within archives", "Scan active
>> processes", "Scan registry", "Deep scan registry," "Scan my IE
>> Favorites for banned sites," and "Scan my Hosts file"
>>
>> Tweaks > Scanning Engine> activate this: "Unload recognized
>> processes during scanning."

>>
>> *Tweaks > Cleaning Engine: activate these: "Automatically try to
>> unregister objects prior to deletion" and "Let Windows remove files
>> in use after reboot."*
>>
>> *Click "Proceed" to save your settings, then
> click "Start." Make sure
>> "Activate in-depth scan" is ticked green, then scan your system.
>> When the scan is finished, the screen will tell you if anything has
>> been found, click "Next." The bad files will be listed. Right click
>> the pane and click "Select all objects" – This will put a check mark
>> in the box at the side, click "Next" again and click "OK" at the
>> prompt "# objects will be removed. Continue?"*
>> *<End Setup Directions>*
>>
>> *Courtesy of
> http://www.nondisputandum.com/html/anti_spyware.html:
> HINT: If
>> Ad Aware is automatically shut-down by a malicious software, first
>> run AWCloak.exe,
> <http://www.lavasoftnews.com/downloads/AAWCloak.exe>, before
>> opening Ad Aware. When AAWCloak is open, click "Activate Cloak".
>> Than open Ad Aware and scan your system.*
>>
>>
>> *Another excellent program for this purpose is SpyBot Search and
>> Destroy available here: <http://security.kolla.de/> SpyBot Support
>> Forum here: [http://www.net-integration.net/cgi-
> bin/forums/ikonboard.cgi](http://www.net-integration.net/cgi-bin/forums/ikonboard.cgi). I recommend
>> using both normally. After UPDATING and fixing ONLY RED things with
>> SpyBot S&D, be sure to re-boot and rerun SpyBot again and repeat
>> this cycle until you get a clean "no red" scan. The reason is that
>> SpyBot sometimes has to remove things which are currently "in use"
>> before it can then clean up others.*
>>
>> *Note that sometimes you need to make a judgement call about what
>> these programs report as spyware. See here, for example:
>> <http://www.imilly.com/alexah.htm>*
>>
>> *Both of these programs should normally be UPDATED and run after
>> doing any other fix such as CWShredder and, as a minimum, normally
>> at least once a week.*
>>
>> *If they don't fix it then start here:*
>>
>> *Download HijackThis, free, here:
>> <http://209.133.47.200/~merijn/files/HijackThis.exe> (Always download
>> a new fresh copy of HijackThis [and CWShredder also] – It's UPDATED
>> frequently.) You may also get it here if that link is blocked:
>> [http://www.majorgeeks.com/downloadget.php?
> id=3155&file=3&evp=3304750663b552982a8baee6434cfc13](http://www.majorgeeks.com/downloadget.php?id=3155&file=3&evp=3304750663b552982a8baee6434cfc13)*

>> or here:

> <http://www.bleepingcomputer.com/files/spyware/hijackthis.z>

> ip

>>

>> In Windows Explorer, click on Tools/Folder Options/View and check

>> "Show hidden files and folders" and uncheck "Hide protected

>> operating system files". (You may want to restore these when you're

>> all finished with HijackThis.)

>>

>> Place HijackThis.exe or unzip HijackThis.zip into its own dedicated

>> folder at the root level such as C:\HijackThis (NOT in a Temp folder

>> or on your Desktop), reboot to Safe mode, start HT (have ONLY HT

>> running – IE MUST be closed) then press Scan. Click on SaveLog when

>> it's finished which will create hijackthis.log. Now click the Config

>> button, then Misc Tools and click on Generate StartupList.log which

>> will create Startuplist.txt

>>

>> Then go to one of the following forums:

>>

>> Spyware and Hijackware Removal Support, here:

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

>>

>> or Net-Integration here:

>> [http://www.net-integration.net/cgi-](http://www.net-integration.net/cgi-bin/forum/ikonboard.cgi?s=d3c2c886d536d57b5f65b6e40c55365e;act=ST;f=27;t=6949)

> [bin/forum/ikonboard.cgi?](http://www.net-integration.net/cgi-bin/forum/ikonboard.cgi?s=d3c2c886d536d57b5f65b6e40c55365e;act=ST;f=27;t=6949)

> [s=d3c2c886d536d57b5f65b6e40c55365e;act=ST;f=27;t=6949](http://www.net-integration.net/cgi-bin/forum/ikonboard.cgi?s=d3c2c886d536d57b5f65b6e40c55365e;act=ST;f=27;t=6949)

>>

>> or Tom Coyote here:

> <http://forums.tomcoyote.org/index.php?act=idx>

>> or Jim Eshelman's site here: <http://forum.aumha.org/>

>> or Bleepingcomputer here:

> <http://www.bleepingcomputer.com/>

>> or Computer Cops here:

> <http://www.computercops.biz/forums.html>

>>

>>

>> Register if necessary, then sign in and READ THE DIRECTIONS at the

>> beginning of the particular site's HiJackThis forum, then copy and

>> paste both files into a message asking for assistance, Someone will

>> answer with detailed instructions for the removal of your

>> parasite(s). Be sure you include at the beginning of your post a

>> description of "What specific problem(s)/symptoms you're trying to

>> solve" and "What steps you've already taken."

>>

>>

>> *****

>> ONLY IF you've successfully eliminated the malware, you can now make

>> a new, clean Restore Point and delete any previously saved (possibly

>> infected) ones. The following suggested approach is courtesy of Gary

>> Woodruff: For XP you can run a Disk Cleanup cycle and then look in

>> the More Options tab. The System Restore option removes all but the

>> *latest Restore Point. If there hasn't been one made since the system
>> was cleaned you should manually create one before dumping the old
>> possibly infected ones. ******
>>
>> *Once you get this cleaned up, you might want to consider installing
>> Eric Howes' IESpyAds, SpywareBlaster and SpywareGuard here to help
>> prevent this kind of thing from happening in the future:*
>>
>> *IESpyads –
> <https://netfiles.uiuc.edu/ehowes/www/resource.htm> "IE–
> SPYAD adds
>> a long list of sites and domains associated with known advertisers,
>> marketers, and crapware pushers to the Restricted sites zone of
>> Internet Explorer. Once you merge this list of sites and domains
>> into the Registry, the web sites for these companies will not be
>> able to use cookies, ActiveX controls, Java applets, or scripting to
>> compromise your privacy or your PC while you surf the Net. Nor will
>> they be able to use your browser to push unwanted pop-ups, cookies,
>> or auto-installing programs on your PC." Read carefully.*
>>
>> *<http://www.javacoolsoftware.com/spywareblaster.html> (Prevents
>> malware Active X installs) (BTW, SpyWareBlaster is not memory
> resident ... no CPU or memory
>> load – but keep it UPDATED) The latest version as of this writing
>> will prevent installation or prevent the malware from running if it
>> is already installed, and it provides information and fixit-links
>> for a variety of parasites.*
>>
>> *<http://www.javacoolsoftware.com/spywareguard.html> (Monitors for
>> attempts to install malware) Keep it UPDATED. All three Very Highly
>> Recommended*
>>
>> *Finally, go to Windows Update and ensure that ALL Critical updates
>> are installed.*
>>
>>
>> *If these steps do not resolve your problem, please post back to this
>> thread with the details and any error messages.*
>>
>>
>> *Hope this helps*
>>
>> *Jan :)*
>> *Smiles are meant to be shared,
>> that's why they're so contagious.*
>>
>> *Please reply to the newsgroup so others may benefit.
>> Replies are posted only to the newsgroup for the benefit or other
>> readers.*
>>
>>
>> *How to make a good newsgroup post:*

>> <http://www.dts-l.org/goodpost.htm>

>>

>>

>>

>>

>>

>>

>>

>>

>>

>>

>>>> -----Original Message-----

>>>> Hi again

>>>>

>>>> I'm still having a problem with IE6! OS is XP with
>>>> SP2 (I'm assuming, I see windows SR 2.0 in my programs
>>>> list), and I think I've been attacked by a virus or
>>>> whatever is out there that's taken out my browser. It
>>>> comes up but doesn't connect to the internet. I've gone
>>>> to Microsoft to download it again, but it still doesn't
>>>> work!

>>>> I've gone back to several posts screaming for help
>>>> but the responses are a little confusing to this still
>>>> newbie. Registry? Backing it up? How does one do that?
>>>> How does one check it for viruses? I think what I need
>>>> here is someone to lead me by the hand, I'm that nervous
>>>> about digging around that deep inside the pc. Or would it
>>>> better for me just to scrub everything clean (format) and
>>>> start fresh?

>>>> So, is there anyone out there willing to give this
>>>> ole gal a helping hand? Please? I'll bake you a
> pie ;O)

>>>>

>>>> Regards and thanks in advance, Pussn

>>>>

>>>> PS--Not much meat to the info, I know, so please, go ahead
>>>> and ask! I just don't know what else to add. Thanks

>>>> .

>>>>

>>>>

>>> Never mind....whatever it was that took out my browser
>>> has now locked me out completely from the pc, can't even
>>> get into my own account. Nothing. Stoopit hackers. I hate
>>> em all!

>>

>>

>> .