

Re: home page

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6.browser/2004-09/4269.htm>

From: Pat O'Leary (ghoffleith_at_discussions.microsoft.com)

Date: 09/18/04

Date: Sat, 18 Sep 2004 06:25:11 -0700

Jim: I've been reading your response to Dee. Thanks for taking the time to inform us. I will definitely print out your reply. I have a thread on "Email Jumps to the Desktop". No one is responding. Would you have an answer? I will be typing a message. If I "undo" it (or out of the blue) I will find the typed message on my desktop. Email is also scanned on the desktop. Would there possibly be a button clicked on that shouldn't be or some such abnormality? I am in the wrong thread I know. Sorry, Dee. Jim, if you can help, I'd really appreciate it. Please reply in my thread. Thanks!

"Jim Byrd" wrote:

- > *Hi Dee – It sounds like you might need some assistance removing this particular malware.*
- >
- > *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>*
- >
- > *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 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://216.180.233.162/~swicom/forums/>

>

> or Net-Integration here:

>

> <http://www.net-integration.net/cgi-bin/forum/ikonboard.cgi?s=d3c2c886d536d57b5f65b6e40c55365e;act=ST:f=27;>

>

> or Tom Coyote here: <http://forums.tomcoyote.org/index.php?act=idx>

>

> Sign in, 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).

>

>

> *****

> 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

>

> Next, install and keep updated a good HOSTS file. It can help you avoid
> most adware/malware. See here: <http://www.mvps.org/winhelp2002/hosts.htm>
> (Be sure it's named/renamed HOSTS – all caps, no extension) Additional

> *tutorials here:*

>

> <http://www.bleepingcomputer.com/forums/index.php?s=14f3f9225081133297a8acdd11137c5b&showtutorial=51>

> *(detailed) and here: <http://www.spywarewarrior.com/viewtopic.php?t=410>*

> *(overview)*

>

>

>

> *Finally, go to Windows Update and ensure that ALL Critical updates are*

> *installed.*

>

>

>

> --

> *Please respond in the same thread.*

> *Regards, Jim Byrd, MS-MVP*

>

>

>

> *In news:0b8301c49ccb\$3ddfd570\$a501280a@phx.gbl,*

> *dee <dee@discussions.microsoft.com> typed:*

> > *I get a blank page everytime i try to go to my home page*

>

>