

## Re: Incredifind

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6.browser/2004-07/3340.htm>

---

**From:** Vince ([willgivewhenneeded\\_at\\_ok.com](mailto:willgivewhenneeded_at_ok.com))

**Date:** 07/11/04

Date: Sun, 11 Jul 2004 11:48:59 -0400

Ignore the previous message. I am tired now and going to bed will check back later to see what you think about deleting the other files.

"Jim Byrd" <[jrbyrd@spamlessadelphia.net](mailto:jrbyrd@spamlessadelphia.net)> wrote in message news:%23COYTA1ZEHA.212@TK2MSFTNGP12.phx.gbl...

> *Hi Vince – Well, start here:*

> <http://www.2-spyware.com/parasite-incredifind.html> for manual removal instructions. PestPatrol is also supposed to be able to remove this one, > also. I would recommend that after you do the manual removal steps, you > follow the directions below:

>  
>  
>

> *Note that this symptom often indicates the possibility of other malware.*

> *You might want go to this page at Jim Eshelman's site, here:*

> <http://aumha.org/a/noads.htm> or here:

> <http://inetexplorer.mvps.org/parasite.htm> and wait a little bit (be > patient), while 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, 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.

>  
>

> *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://members.shaw.ca/installations/WinsockFix.zip>

>

> *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.
- >
- >
- > In the following, all of these removal tools should be run from Safe mode
- > when possible
- >
- >
- > For the general hijack case, the best way to start is to get Ad-Aware 6.0,
- > Build 181 or later, here: <http://www.lavasoftusa.com/support/download/>.
- > UPDATE 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.
- >
- > 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>. I recommend
- > using both normally. After UPDATING and fixing 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/alexa.htm>
- >
- >
- > A currently common parasite is some malware called CoolWebSearch. Do the
- > following:
- >
- > Download, UPDATE before running, and run:
- > <http://209.133.47.200/~merijn/files/CWShredder.exe> to remove the parasite.
- > Be sure to close all instances of IE and OE. You may also get it here if
- > that link is blocked: <http://www.zerosrealm.com/downloads/CWShredder.zip>
- >
- > BE SURE that you get v.1.59.0.1 or later!
- >
- > There's a good tutorial about CWS and using CWShredder here:
- > <http://www.bleepingcomputer.com/forums/index.php?showtutorial=47#domain>
- >
- > 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/2001052409420406>>

>

> *HOW TO Enable Hidden Files*

>

> <<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/2001111912274039>>

> *(WinXP)*

>

> <<http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2001012513122239>>

> *(WinME)*

>

>

>

>

> *Then download and run:*

> *[http://www.kellys-korner-xp.com/regs\\_edits/iegentabs.reg](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](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.*

>

>

> *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 CWS shredder 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>*

> *or here: <http://www.bleepingcomputer.com/files/spyware/hijackthis.zip>*

>

> *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), start it 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;t=>

>  
> *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/>*

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

> *of the particular sites 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 "What problem(s) 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 the*
- > *SpywareBlaster and SpywareGuard here to help prevent this kind of thing*
- > *from*
- > *happening in the future:*
- >
- > <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. Both Very Highly Recommended*
- >
- >
- > *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:uUHsei0ZEHA.996@TK2MSFTNGP12.phx.gbl,*
- > *Vince <willgivewhenneeded@ok.com> typed:*
- > *> Hello:*
- > *> Today I was browsing and came across a page that installed*
- > *> incredifind in my system, I have my active x set to prompt me before*
- > *> installing anything, however that did not help with this one. The*
- > *> darn program installed without any notice. Just froze up my system*
- > *> and crashed my Satalite service. After restarting my system works but*
- > *> I have the incredifind search on it. This really makes me mad. The*
- > *> infected computer is the proxy server and if it goes down I loose*
- > *> every computer in the system.*
- > >
- > *> I have found many pages on this problem but also have found that the*
- > *> problems may or may not be corrected by following the procedures. In*
- > *> some cases the internet is completley lost.*
- > >
- > *> I also understand the normal tools such as Ad–Aware and Spybot etc do*
- > *> not fix this problem.*
- > >
- > *> Any suggestions as to what will work before I try to fix the problem?*

microsoft.public.windows.inetexplorer.ie6.browser: Re: Incredifind

> >

> > *Going to bed should have been there 2 hours ago just as I was getting*

> > *off this darn program hijacked me.*

> >

> > *Vince*

>