

# Re: Malicious Software / Worm ???

---

*Source:*

[http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.network\\_web/2005-04/msg02173.html](http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.network_web/2005-04/msg02173.html)

---

- *From:* Chuck <[none@xxxxxxxxxxx](mailto:none@xxxxxxxxxxx)>
  - *Date:* 28 Apr 2005 23:23:04 -0500
- 

On Thu, 28 Apr 2005 21:10:05 -0700, "Bruce" <[Bruce@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Bruce@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote:

- >I have been unfortunate enough to be the victim of someone who has designed
- >an internet blocking "search engine" that they have called NETSTER.
- >
- >Once it has bedded itself in my computer it overrides any other web site
- >that I may request, placing its own page on the screen.
- >
- >It consists of what appears at first glance to be a search engine page but
- >is only one of two "dummy" pages.
- >
- >I am at a loss to know how to remove this malicious crap.
- >
- >Any ideas??
- >
- >Bruce.

Bruce,

How current is your virus protection? Try one or more of these free online virus scans, which should complement your current protection:

- <<http://www.bitdefender.com/scan/license.php>>
- <<http://www.pandasoftware.com/activescan>>
- <<http://www.ravantivirus.com/scan/>>
- <<http://security.symantec.com/ssc/home.asp>>
- <[http://housecall.trendmicro.com/housecall/start\\_corp.asp](http://housecall.trendmicro.com/housecall/start_corp.asp)>

Now check for, and learn to defend against, non-viral malware. Have you downloaded these programs before? Download them again, as the latest version may be needed to keep up with the current level of malware being attempted constantly – get the absolutely most current version of each product listed. They're all free – and most pretty small, so they download quickly enough.

Start by downloading each of the following additional free tools – and download each individual product from each link as listed:

- AdAware <<http://www.lavasoftusa.com/>>
- CWShredder <[http://www.intermute.com/spysubtract/cwshredder\\_download.html](http://www.intermute.com/spysubtract/cwshredder_download.html)>

Re: Malicious Software / Worm ???

HijackThis <<http://www.tomcoyote.com/hjt/>>  
LSP-Fix <<http://www.cexx.org/lspfix.htm>>  
WinsockXPFix <<http://www.spychecker.com/program/winsockxpfix.html>>  
Spybot S&D <<http://www.safer-networking.org/index.php?page=download>>  
Stinger <<http://us.mcafee.com/virusInfo/default.asp?id=stinger>>  
TrendMicro Sysclean <<http://www.ik-cs.com/got-a-virus.htm>>

Create a separate folder for HijackThis, such as C:\HijackThis – copy the downloaded file there. Create a separate folder for the TrendMicro files, such as C:\TrendMicro – copy the downloaded files there (unzipped if necessary). AdAware, CWSshredder, and Spybot S&D have install routines – run them. The other downloaded programs can be copied into, and run from, any convenient folder.

First, close all Internet Explorer and Outlook windows.

Run Stinger. Have it remove all problems found.

Run CWSshredder. Have it fix all problems found.

Empty your temporary files folders:

- "C:\WINDOWS\Temp"
- "C:\Documents and Settings\(\Username)\Local Settings\Temporary Internet Files".

Next, disable System Restore.

<<http://vil.nai.com/vil/SystemHelpDocs/DisableSysRestore.htm>>

Boot your computer into Safe Mode.

<http://support.microsoft.com/?id=315222>

Run SysClean per instructions. Delete any infections found. Reboot your computer, and re enable System Restore.

Next, run AdAware. First update it, configure for full scan

(<<http://forums.spywareinfo.com/index.php?showtopic=11150>>), then scan. When scanning finishes, remove all Critical Objects found.

Next, run Spybot S&D. First update it, then run a scan. Trust Spybot, and delete everything ("Fix Problems") that is displayed in Red.

Then, run HijackThis ("Scan"). Do NOT make any changes immediately. Save the HJT Log.

<<http://forums.spywareinfo.com/index.php?showtopic=227>>

Finally, have your HJT log interpreted by experts at one or more of the following security forums (and please post a link to your forum posts, here):

Aumha: <<http://forum.aumha.org/index.php>>

Net-Integration: <<http://forums.net-integration.net/>>

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

Spyware Warrior: <<http://spywarewarrior.com/index.php>>

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

If removal of any spyware affects your ability to access the internet (some

## Re: Malicious Software / Worm ???

spyware builds itself into the network software, and its removal may damage your network), run LSP-Fix and / or WinsockXPFIx.

Finally, improve your chances for the future.

Harden your browser. There are various websites which will check for vulnerabilities, here are three which I use.

<http://www.jasons-toolbox.com/BrowserSecurity/>

<http://bcheck.scanit.be/bcheck/>

[http://testzone.secunia.com/browser\\_checker/](http://testzone.secunia.com/browser_checker/)

Consider using an alternative browser, like Firefox, for the majority of your browsing activities.

<<http://www.spreadfirefox.com/?q=affiliates&id=4507&t=61>>

Block Internet Explorer ActiveX scripting from dangerous websites (Restricted Zone).

<<https://netfiles.uiuc.edu/ehowes/www/main.htm>> (IE-SpyAd)

Block known dangerous scripts from running.

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

Block known spyware from installing.

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

Make sure that the spyware detection / protection products that you use are reliable:

[http://www.spywarewarrior.com/rogue\\_anti-spyware.htm](http://www.spywarewarrior.com/rogue_anti-spyware.htm)

Harden your operating system. Check at least monthly for security updates.

<http://windowsupdate.microsoft.com/>

Block possibly dangerous websites with a Hosts file. Three Hosts file sources I use:

[http://www.accs-net.com/hosts/get\\_hosts.html](http://www.accs-net.com/hosts/get_hosts.html)

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

(The third is included, and updated, with Spybot (see above)).

Maintain your Hosts file (merge / eliminate duplicate entries) with:

eDexter <[http://www.accs-net.com/hosts/get\\_hosts.html](http://www.accs-net.com/hosts/get_hosts.html)>

Hostess <<http://accs-net.com/hostess/>>

Secure your operating system, and applications. Don't use, or leave activated, any accounts with names or passwords with trivial (guessable) values. Don't use an account with administrative authority, except when you're intentionally doing administrative tasks.

Use common sense. Yours. Don't install software based upon advice from unknown sources. Don't install free software, without researching it carefully. Don't open email unless you know who it's from, and how and why it was sent.

Re: Malicious Software / Worm ???

Educate yourself. Know what the risks are. Stay informed. Read Usenet, and various web pages that discuss security problems. Check the logs from the security products that you use regularly, look for things that don't belong, and take action when necessary.

How did I get infected in the first place?

<http://forums.net-integration.net/index.php?showtopic=3051>

Essential tips for infection prevention

<http://forums.spywareinfo.com/index.php?showtopic=24339>

<http://www1.spywareinfo.com/articles/hijacked/prevent.php>

---

Cheers,

Chuck

Paranoia is not necessarily a bad thing – it comes from experience.

My email is AT DOT

actual address pchuck sonic net.

.

---

• *Follow-Ups:*

- ◆ *Re: Malicious Software / Worm ???*

◇ *From:* Jack

• *References:*

- ◆ *Malicious Software / Worm ???*

◇ *From:* Bruce

- Prev by Date: *Re: Network browser problem*
- Next by Date: *Re: Unable to access shared folder in Win95 machine*
- Previous by thread: *Malicious Software / Worm ???*
- Next by thread: *Re: Malicious Software / Worm ???*
- Index(es):
  - ◆ *Date*
  - ◆ *Thread*