

Re: trojan/virus/highjack problem

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2005-12/msg03888.htm

- *From:* "David H. Lipman" <DLipman~nospam~@Verizon.Net>
 - *Date:* Sun, 25 Dec 2005 10:47:26 -0500
-

From: "far22" <far22@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

| Hie,

| I'm on XP pro,use Norton antivirus 2006 and use IE for internet connection.

| The problem is,a couple of days ago,my antivirus programme found
| trojan.zlob.d on my laptop.however,it couldnt fully resolve it and said it
| would quarantine it.

| (The second last virus it found was trojan.spaxe but this was deleted so i
| dont its the ccause of the problem.)

| I've been having problems since, as my home page is been highjacked to
| www.needupdate.com where it tells me my pc is under control of remote
| computer 227.4.167.118 and that it is accessing Windows; Program
| Files\Internet Explorer; My Documents and C:\ files.

| It says i should click to download official anti-spyware software. (which i
| havent done).

| I have since run norton but it cant detect a virus now.

| I've also tried avast,which didnt find anything.

| I've tried deleting nvctrl.exe in Registry Editor,as i've seen on norton
| website that related viruses of zlob.d ;i.e. versions e, f and g create this
| value in the registry to run everytime i start IE.

| I delete this value but as soon as come back i find it there again.

| I've even tried deleting it with my computer in Safe mode but it reappears
| soon as i start the internet (in normal mode).

| There is wininet.dll in the same part of registry but i dont know if its
| safe or not?

| I read also that the trojan.zlob creates or copies a file called
| mssearchnet.exe i think.i searched my pc and i DO have this file/folder but
| dont know if its safe to delete or not?

| I eventually turned to microsoft's Microsoft did find 3 viruses and 7 files
| infected;it resolved 6 of the files but the 7th wasnt and i still have 1
| virus according to microsoft;which is JS/loop i thnk.

Re: trojan/virus/highjack problem

|
| i am having a terrible xmas bcoz of this problem and if someone can cheer me
| up with a solution it would be very appreciated.

|
| i am not techy so plz put things in 1,2,3 steps!

|
| Sorry for long question but was trying to be as specific as possible.

|
| Thanx in advance...

Two part reply..

Perform Part 1 and then perform Part 2.

Use the alternate if the first two parts are ineffective...

Note: Alternate only for Win2K, WinXP and Win2003 Server

Part 1

Use noahdfear's SmitFraud and SpyAxe removal tool --- SmitRem.exe

<http://noahdfear.geekstogo.com/click%20counter/click.php?id=1>

<http://www.bleepingcomputer.com/forums/topic36868.html>

Part 2

Download SmitFraud.exe from the URL ---

<http://www.ik-cs.com/programs/virttools/SmitFraud.exe>

Execute; SmitFraud.exe { Note: You must accept the default of C:\McAfee }

Choose; Unzip

Choose; Close

NOTE: You may have to disable your software FireWall or allow WGET.EXE to go through your FireWall to enable WGET.EXE to download the needed McAfee related files.

Execute; c:\mcafee\clean.bat

{ or Double-click on 'Clean Link' in c:\mcafee }

A final report in HTML format called C:\mcafee\ScanReport.HTML will be generated. At the end of the scan, it will be displayed in your browser (Opera, FireFox or Internet Explorer).

It is suggested that you move the report out of c:\mcafee before performing another scan.

Alternate:

Secured2K's SpyAxe, PSGuard, Smitfraud, Sinnaka and Alemod removal tool.

<http://secured2k.home.comcast.net/tools/AntiPuper.exe>

Re: trojan/virus/highjack problem

Re: trojan/virus/highjack problem

<http://forums.mcafeehelp.com/viewtopic.php?t=65072>

Please Copy and Paste the contents of the HTML Log file; C:\mcafee\ScanReport.HTML in your reply.

* * * Please report back your results * * *

—

Dave

<http://www.claymania.com/removal-trojan-adware.html>

<http://www.ik-cs.com/got-a-virus.htm>

.

• *Follow-Ups:*

◆ **[Re: trojan/virus/highjack problem](#)**

◇ *From: far22*

- Prev by Date: **[Windows – Corrupt File – Help](#)**
- Next by Date: **[Re: 2 HDD with XP on each?](#)**
- Previous by thread: **[Re: trojan/virus/highjack problem](#)**
- Next by thread: **[Re: trojan/virus/highjack problem](#)**
- Index(es):
 - ◆ **[Date](#)**
 - ◆ **[Thread](#)**