

Re: Can't get rid of Trojan horse Backdoor

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-11/0256.html>

From: Jim Byrd (jrbyrd_at_spamlessadelphia.net)

Date: 11/14/04

Date: Sun, 14 Nov 2004 09:07:34 -0800

Hi Bob – Here's what I would suggest that you try. Use the Clean Boot approach and then do the following in order – read carefully first. Note the file deletion tools, particularly Delete Invalid File at the end, if the AV's can't remove it and/or you have problems doing so manually:

#####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 for W95, W98, and ME

<http://www.tacktech.com/pub/winsocfix/WinsockFix.zip>

Directions here: <http://www.tacktech.com/display.cfm?tid=257>

or here for Win2k/XP <http://files.webattack.com/localdl834/WinsockxpFix.exe>

Info here: <http://www.spychecker.com/program/winsocxpfix.html>

Directions here: <http://www.iup.edu/house/resnet/wifix.shtm>

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. (You can also try this if you're on XP SP1. There has also been one, as yet unconfirmed, report that this also works there.) Also, one MS technician suggested the following sequence:

```
netsh int reset all
ipconfig /flushdns
```

See also: <http://windowsxp.mvps.org/winsock.htm> for additional XPSP2 info/approaches using the netsh command.

#####IMPORTANT#####

#####IMPORTANT#####

Show hidden files and run all of the following removal tools from Safe mode

microsoft.public.security.virus: Re: Can't get rid of Trojan horse Backdoor

or a "Clean Boot" when possible. Reboot and test if the malware is fixed after using each tool.

HOW TO Enable Hidden Files

<http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2002092715262339>

Clean Boot: 1. Start|Run enter msconfig.

2. In the Startup tab, click the "Disable All" button.

3. In the Services tab, check the "Hide All Microsoft Services" checkbox, and then click the "Disable All" button.

4. Click OK and then reboot.

#####IMPORTANT#####

Download and run Stinger.exe, here:

<http://download.nai.com/products/mcafee-avert/stinger.exe> or from the link

on this page: <http://vil.nai.com/vil/stinger/> ME/XP users be sure to read:

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

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> Be sure to read the "How-to" info here:

<http://www.trendmicro.com/ftp/products/tsc/readme.txt> (You might also want to get Art's updater, SYS-UP.Zip, here for future updating of these:

<http://home.epix.net/~artnpeg/>). (If you download and use the updater from the beginning, it will automatically handle downloading the other files.

This is my Recommended approach.) Place them in a dedicated folder (or use the updater from one) after appropriate unzipping. Show hidden and system files (HowTo here:

<http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2002092715262339>)

Disable Restore if you're on XP or ME (directions here:

<http://vil.nai.com/vil/SystemHelpDocs/DisableSysRestore.htm>), then boot to

Safe mode (HowTo here:

<http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2001052409420406>)

Read tscreadme.txt carefully, then do a complete scan of your system in Safe mode and clean or delete anything it finds. Reboot to normal mode and re-run the scan again.

This scan may take a long time, as Sysclean is VERY extensive and thorough.

For example, one user reported that Sysclean found 69 hits that an immediately prior Norton AV v. 11.0.2.4 run had missed.

Sometimes these tools 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.)" Another is Killbox, here:

<http://www.downloads.subratam.org/KillBox.zip>

A third which is a bit different but often useful is Delete Invalid File, here: <http://www.purgeie.com/delinv.htm> which handles invalid/UNC file/folder name deleting, rather than the in use problem

Re: Can't get rid of Trojan horse Backdoor

microsoft.public.security.virus: Re: Can't get rid of Trojan horse Backdoor

--

Please respond in the same thread.

Regards, Jim Byrd, MS-MVP

In news:OGrRNojyEHA.4004@tk2msftngp13.phx.gbl,

BH2 <NOSPAMfurness50@hotmail.com> typed:

> Jim,

> Will give that a try, so far all I ever get is that the file cannot be
> accessed, looks like I may have to format the drive to get rid of it.

> What will Happen if I just delete the infected file ?,

> (C:\WINDOWS\system32\d3dcfo.dll) that is if it lets me !!

> regards

> Bob H

>

> "Jim Byrd" <jrbyrd@spamlessadelphia.net> wrote in message

> news:%23iI2XleyEHA.2804@TK2MSFTNGP15.phx.gbl...

>> Hi BH2 - To suppliment what David said, you can also try a "Clean

>> Boot" approach:

>>

>> Clean Boot:

>>

>> 1. Start|Run enter msconfig.

>> 2. In the Startup tab, click the "Disable All" button.

>> 3. In the Services tab, check the "Hide All Microsoft Services"

>> checkbox, and then click the "Disable All" button.

>> 4. Click OK and then reboot.

>>

>>

>> --

>> Please respond in the same thread.

>> Regards, Jim Byrd, MS-MVP

>>

>>

>>

>> In news:OlJCwsdyEHA.3376@TK2MSFTNGP12.phx.gbl,

>> BH2 <NOSPAMfurness50@hotmail.com> typed:

>>> For some reason it won't let me start the computer in the safe mode,

>>> I go to and accept the safe mode, It also load some drivers and

>>> shows them in text what it is loading, then just stops with a

>>> blank screen. Regards

>>> Bob

>>>

>>> "BH2" <NOSPAMfurness50@hotmail.com> wrote in message

>>> news:OMz3ocWyEHA.260@TK2MSFTNGP10.phx.gbl...

>>>> Hi,

>>>> I need some help please. I run AVG virus checker, it has picked

>>>> up a Trojan

>>>> horse in C:\WINDOWS\system32\d3dcfo.dll Trojan

>>>> horse.Backdoor.agent.BA. AVG

>>>> has detected the virus, but it will not delete or rename it or

>>>> isolate it.

>>>> I downloaded the AVG cleaner but can't get into the safe mode to

>>>> run it. Everytime I open any program the AVG splash screen comes

>>>> up and tells me about the virus and where it is.

>>>> Would appreciate any help in getting rid of it, it is driving me

>>>> nuts. Also because I am infected does this mean that AVG is not

>>>> very good. Thanks for any help

>>>> Regards

>>>> Bob H