

Re: Computer Infected:

Re: Computer Infected:

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2009-02/msg03070.html>

- *From:* Navyguy <magineeer@xxxxxxxxxxx>
 - *Date:* Sun, 15 Feb 2009 16:25:50 -0800 (PST)
-

On Feb 15, 8:22 am, "PA Bear [MS MVP]" <PABear...@xxxxxxxxxx> wrote:

...would
reinstalling the OS correct this or perhaps using the Recovery disk
install with repair option?

A format & reinstall would take care of it, yes, but a Repair Install would not.

Some notes:

=> Reinstalling will leave you with the equivalent of a "new computer" so you'll need to take care of everything here again:

5 steps to help protect your new computer before you go
online <http://www.microsoft.com/protect/computer/advanced/xppc.mspx>

=> If a Norton or McAfee free-trial came with the machine when you bought it, the free-trial will be reinstalled, too, but it will NOT be valid!
Before installing a replacement anti-virus app (see below), you'll need to uninstall the free-trial via Add/Remove Programs AND THEN run the appropriate removal tool:

Norton Removal

Tool <http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/200503310816...>

McAfee Consumer Products Removal Tool three-step fix

[Do Steps #1 & #2 only] <http://service.mcafee.com/FAQDocument.aspx?id=TS100507>

=> You've had AVG Free installed yet you ended up with an infection. I would not recommend relying on it after your reinstall Windows. I can recommend NOD32 or Kaspersky (not the suites); If cost is a factor, I'd recommend Avira AntiVir (free).

Good luck!

Protect Your PC! <http://www.microsoft.com/athome/security/computer/default..mspx>

Re: Computer Infected:

Steps To Help Prevent

Spyware<http://www.microsoft.com/protect/computer/spyware/prevent.mspix>

Steps to Help Prevent Computer

Worms<http://www.microsoft.com/protect/computer/viruses/worms/prevent.mspix>

~Robear Dyer (PA Bear)

MS MVP-IE, Mail, Security, Windows Desktop Experience – since 2002

AumHa VSOP & Admin<http://aumha.net>

DTS-L<http://dts-l.net/>

Navyguy wrote:

It does seem like a mouthfull but I think I can handle it in the steps as you outlined, and everyone has offered similar but separate advice which I do appreciate, but let me ask this if I may, would reinstalling the OS correct this or perhaps using the Recovery disk install with repair option? I want to thank everyone for being so helpful with their suggestions, I appreciate it.

1. See if you can download/run the MSRT manually:<http://www.microsoft.com/security/malwareremove/default.mspix>

2. Run this online scan (in safe mode w/networking, if need be):<http://onecare.live.com/site/en-us/center/howsafe.htm>

3. Run a /thorough/ check for hijackware, including posting the requested logs in an appropriate forum.

Checking for/Help with

Hijackware<http://aumha.net/viewtopic.php?f=30&t=4075><http://mvps.org/winhelp2002...>
<http://inetexplorer.mvps.org/tshoot.html><http://www.mvps.org/sramesh2k...>

**Seek expert assistance

in<http://spywarehammer.com/simplemachinesforum/index.php?board=10.0.htm...>,
or other appropriate forums.**

Re: Computer Infected:

If the procedures look too complex – and there is no shame in admitting this isn't your cup of tea – take the machine to a local, reputable and independent (i.e., not BigBoxStoreUSA) computer repair shop.

--

Navyguy wrote:

I have a Dell Dimension 8200 with XP SP3, with DSL connection. I have Windows Firewall, AVG, Spyware Blaster and Hive Cleanup. Recently it became infected with a Trojan Horse virus:

Trojan horse Downloader.Generic8.TVN

It was under Local Settings\Temp Internet Files
Content.IE5\PWT3Az83\getfile-081220-aps(1).gif

I was able to delete it successfully but as I understand, it still resides in my computer on another program. In addition to this, with the aid of remote assistance I was told that my MFT was corrupted. My question is this, is there some way of tracking down the host program with the virus and deleting it? Also is there a way that I can tell for myself if my MFT is actually corrupted? If not, what are your recommendations?

Thanks,

Robert– Hide quoted text –

Re: Computer Infected:

– Show quoted text — Hide quoted text –

– Show quoted text –

Whew, so much information! I hardly know where to begin!

Well let me try to encapsulate in brief; This all started when my MSN Msgr stopped logging in automatically about a month ago. I had posted the problem on other groups in hopes of resolving the problem but the only suggestions were that I uninstall and reinstall which is what I did. I was then infected with the Trojan virus and deleted it, and at this point I accepted help via remote assistance and it was then that it was discovered that my MFT was corrupted he said. He made many changes to my system and at one point I couldn't access the user accounts or system restore. After further changes it required a system restart but it did not come back up. I had to use another computer which I have at my disposal to help rbrin my computer back up. With the Recovery disk inserted and with the bios changed previously to select the cd/dvd drive but before I could select install or repair the computer came back on its own, why or how I don't know. However the boot sequence has changed so that this is what happens now: Startup>Dell Splash>Windows Splash>Defragging>Logon Message> then I get (2) boxes, the first is highlighted and says: Unable to log you on because of an account restriction, behind that is a logon box grayed out with username–Administrator and underneath password. Once I click the OK in the first highlighted box however it says Windows starting up, To begin, check on your username> I do this and it takes me Windows>Desktop. MsnMsgr still does not sign in automatically however once clicked everything works as before.

I downloaded and ran a MSRT full system scan and it found nothing.

I have uninstalled AVG and installed Avira in its place (I understand theres a risk of uninstalling and reinstalling too much and I may have done so with AVG). I've updated it and run a full system scan which found (8) Detections and (3) warnings, however after the scan I could only see the following (5) in the quarantine which it apparently put there automatically:

TR/Crypt.XPACK.Gen

C:\System Volume Information_restore{3141675–6CBE–4639 etc and ends with .exe

C:\Program Files\My Document Programs\setup.exe

Contains recognition pat.

Re: Computer Infected:

Re: Computer Infected:

C:\Documents and Settings\my name\Local Settings\Application Data
\Microsoft\Wind...\500055A6-0000009B.eml
C:\Documents and Settings\my name\Local Settings\Application Data
\Microsoft\Wind...\0A2633B2-0000008C.eml
C:\Documents and Settings\my name\Local Settings\Application Data
\Microsoft\Wind...\064831119-0000008B.eml

This is an extract of the Notepad after scanning

Version information:

BUILD.DAT : 8.2.0.337 16934 Bytes 11/18/2008 13:05:00
AVSCAN.EXE : 8.1.4.10 315649 Bytes 11/18/2008 17:21:26
AVSCAN.DLL : 8.1.4.0 40705 Bytes 5/26/2008 16:56:40
LUKE.DLL : 8.1.4.5 164097 Bytes 6/12/2008 21:44:19
LUKERES.DLL : 8.1.4.0 12033 Bytes 5/26/2008 16:58:52
ANTIVIR0.VDF : 7.1.0.0 15603712 Bytes 10/27/2008 20:30:36
ANTIVIR1.VDF : 7.1.2.12 3336192 Bytes 2/11/2009 20:48:21
ANTIVIR2.VDF : 7.1.2.13 2048 Bytes 2/11/2009 20:48:22
ANTIVIR3.VDF : 7.1.2.27 79360 Bytes 2/15/2009 20:48:23
Engineversion : 8.2.0.79
AEVDF.DLL : 8.1.1.0 106868 Bytes 2/15/2009 20:48:37
AESCRIP.T.DLL : 8.1.1.47 348539 Bytes 2/15/2009 20:48:35
AESCN.DLL : 8.1.1.7 127347 Bytes 2/15/2009 20:48:34
AERDL.DLL : 8.1.1.3 438645 Bytes 11/4/2008 22:58:38
AEPACK.DLL : 8.1.3.8 397684 Bytes 2/15/2009 20:48:33
AEOFFICE.DLL : 8.1.0.33 196987 Bytes 2/15/2009 20:48:32
AEHEUR.DLL : 8.1.0.90 1573237 Bytes 2/15/2009 20:48:31
AEHELP.DLL : 8.1.2.0 119159 Bytes 2/15/2009 20:48:27
AEGEN.DLL : 8.1.1.16 332148 Bytes 2/15/2009 20:48:26
AEEMU.DLL : 8.1.0.9 393588 Bytes 10/14/2008 19:05:56
AECORE.DLL : 8.1.6.5 176501 Bytes 2/15/2009 20:48:24
AEBB.DLL : 8.1.0.3 53618 Bytes 10/14/2008 19:05:56
AVWINLL.DLL : 1.0.0.12 15105 Bytes 7/9/2008 17:40:05
AVPREF.DLL : 8.0.2.0 38657 Bytes 5/16/2008 18:28:01
AVREP.DLL : 8.0.0.2 98344 Bytes 7/31/2008 21:02:15
AVREG.DLL : 8.0.0.1 33537 Bytes 5/9/2008 20:26:40
AVARKT.DLL : 1.0.0.23 307457 Bytes 2/12/2008 17:29:23
AVEVTLOG.DLL : 8.0.0.16 119041 Bytes 6/12/2008 21:27:49
SQLITE3.DLL : 3.3.17.1 339968 Bytes 1/23/2008 02:28:02
SMTPLIB.DLL : 1.2.0.23 28929 Bytes 6/12/2008 21:49:40
NETNT.DLL : 8.0.0.1 7937 Bytes 1/25/2008 21:05:10
RCIMAGE.DLL : 8.0.0.51 2371841 Bytes 6/12/2008 22:48:07
RCTEXT.DLL : 8.0.52.0 86273 Bytes 6/27/2008 22:34:37

Configuration settings for the scan:

Jobname.....: Complete system scan
Configuration file.....: c:\program files\avira\antivir
personaledition classic\sysscan.avp
Logging.....: low
Primary action.....: interactive
Secondary action.....: ignore

Re: Computer Infected:

Re: Computer Infected:

Scan master boot sector.....: on
Scan boot sector.....: on
Boot sectors.....: C:,
Process scan.....: on
Scan registry.....: on
Search for rootkits.....: off
Scan all files.....: Intelligent file selection
Scan archives.....: on
Recursion depth.....: 20
Smart extensions.....: on
Macro heuristic.....: on
File heuristic.....: medium

Start of the scan: Sunday, February 15, 2009 14:50

The scan of running processes will be started

Scan process 'avscan.exe' - '1' Module(s) have been scanned
Scan process 'avcenter.exe' - '1' Module(s) have been scanned
Scan process 'wltuser.exe' - '1' Module(s) have been scanned
Scan process 'iexplore.exe' - '1' Module(s) have been scanned
Scan process 'avgnt.exe' - '1' Module(s) have been scanned
Scan process 'avguard.exe' - '1' Module(s) have been scanned
Scan process 'sched.exe' - '1' Module(s) have been scanned
Scan process 'wlcomm.exe' - '1' Module(s) have been scanned
Scan process 'msnmsg.exe' - '1' Module(s) have been scanned
Scan process 'ctfmon.exe' - '1' Module(s) have been scanned
Scan process 'eBayTBDaemon.exe' - '1' Module(s) have been scanned
Scan process 'explorer.exe' - '1' Module(s) have been scanned
Scan process 'alg.exe' - '1' Module(s) have been scanned
Scan process 'uphclean.exe' - '1' Module(s) have been scanned
Scan process 'SeaPort.exe' - '1' Module(s) have been scanned
Scan process 'nvsvc32.exe' - '1' Module(s) have been scanned
Scan process 'mdm.exe' - '1' Module(s) have been scanned
Scan process 'LSSrvc.exe' - '1' Module(s) have been scanned
Scan process 'ioloServiceManager.exe' - '1' Module(s) have been scanned
Scan process 'InCDsrv.exe' - '1' Module(s) have been scanned
Scan process 'spoolsv.exe' - '1' Module(s) have been scanned
Scan process 'svchost.exe' - '1' Module(s) have been scanned
Scan process 'svchost.exe' - '1' Module(s) have been scanned
Scan process 'svchost.exe' - '1' Module(s) have been scanned
Scan process 'svchost.exe' - '1' Module(s) have been scanned
Scan process 'svchost.exe' - '1' Module(s) have been scanned
Scan process 'svchost.exe' - '1' Module(s) have been scanned
Scan process 'lsass.exe' - '1' Module(s) have been scanned
Scan process 'services.exe' - '1' Module(s) have been scanned
Scan process 'winlogon.exe' - '1' Module(s) have been scanned
Scan process 'csrss.exe' - '1' Module(s) have been scanned
Scan process 'smss.exe' - '1' Module(s) have been scanned
31 processes with 31 modules were scanned

Starting master boot sector scan:

Re: Computer Infected:

Re: Computer Infected:

Master boot sector HD0
[INFO] No virus was found!

Start scanning boot sectors:
Boot sector 'C:\'
[INFO] No virus was found!

Starting to scan the registry.
The registry was scanned ('62' files).

Starting the file scan:

Begin scan in 'C:\'
C:\hiberfil.sys
[WARNING] The file could not be opened!
C:\JSetup.exe
[0] Archive type: CAB SFX (self extracting)
--> \disk1\data1.cab
[WARNING] No further files can be extracted from this archive.
The archive will be closed
C:\pagefile.sys
[WARNING] The file could not be opened!

End of the scan: Sunday, February 15, 2009 15:51
Used time: 1:01:08 Hour(s)

The scan has been done completely.

8439 Scanning directories
284164 Files were scanned
0 viruses and/or unwanted programs were found
0 Files were classified as suspicious:
0 files were deleted
0 files were repaired
0 files were moved to quarantine
0 files were renamed
2 Files cannot be scanned
284162 Files not concerned
5354 Archives were scanned
3 Warnings
0 Notes

Should I now proceed to One Care full scan via Safe Mode or do something else?

Thanks,
Robert

.

Re: Computer Infected: