

Summary (was Re: Ok, so I'm a lazy moron – Explorer crashes at startup)

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-05/28553.html>

From: Steve Nielsen (*steve_nielsen_at_nospam.nowhere.net*)

Date: 05/28/04

Date: Fri, 28 May 2004 11:35:48 -0700

At David Candy's request I am posting a summary of what's been done.

The original and continuing error is:

Explorer.exe application error

The instruction at "0x734301d5" referenced memory at "0x734301d5"

The memory could not be "read"

Click Ok to terminate the program

Click cancel to debug the program

This occurs within a couple of seconds after login (user does not matter) and occurs in Safe Mode. It also occurs when running an a/v program, Spybot S&D and Ad-aware and randomly with other programs, but ALWAYS with a/v, Spybot and AAW. The programs still function after Explorer automatically reloads. The error also occurs randomly when opening My Computer or other folders but not consistently. Otherwise the system seems fairly functional, just this error keeps occurring. I've checked Event viewer which shows:

"The shell stopped unexpectedly and Explorer.exe was restarted."

Visiting the Help and Support Center says the same thing and adds "No user action is required."

I have tested the RAM for over 20 hours (no errors) using M\$'s memory tester downloaded from:

<http://oca.microsoft.com/en/windiag.asp>

Memtest86 3.0 bootable CD would not boot; instantly restarts, and another memory tester on a BBS Linux CD also instantly restarts the machine (guessing a HW incompatibility with those tests).

I posted my original problem on the tablet PC group and the only suggestion was to swap RAM just in case the test may have missed something. I have swapped out the RAM with a known good module and the condition persists. I believe a RAM problem has been sufficiently ruled out.

microsoft.public.windowsxp.general: Summary (was Re: Ok, so I'm a lazy moron – Explorer crashes at startup)

Up to date antivurs (CSAV 4.90.4 w/latest deffiles) finds nothing.
On–line virus scan at TrendMicro finds nothing.
Up to date CWSredder finds nothing (even in Safe Mode).
Updated Ad–aware 6.181 finds nothing (even in Safe Mode).
Updated Spybot S&D 1.3 originally found the following:

DSO Exploit: Data source object exploit (Registry change, fixed)

HKEY_USERS\S–1–5–21–2065366691–533095778–4141000609–500\Software\Microsoft\Windows\CurrentVersion\Settings\Zones\0\1004!=W=3

Xer0x : Settings (Registry key, fixed)
HKEY_LOCAL_MACHINE\Software\xerox

After re–booting it has found the same things. After fixing them again for the 4th or 5th time I ran RegCleaner, rebooted (the Explorer error occurs after every reboot) and subsequent Spybot S&D scans still show:

Xer0x : Settings (Registry key, fixed)
HKEY_LOCAL_MACHINE\Software\xerox

I have searched some a/v sites which IDs this as W32.HLLW.Loxar worm and the manual removal instructions say to turn off System Restore, remove two reg entries:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run = xerox

HKEY_LOCAL_MACHINE\SOFTWARE\Xerox = Xeroxlocation

These registry entries do NOT exist.

and search for and delete certain files:

- * Xex0x.exe
- * Xer0x.exe
- * X3rox.exe
- * X3r0x.exe
- * Xerox.com
- * Xer0x.com
- * X3rox.com
- * X3r0x.com
- * X3xox.exe

The files do NOT exist (I am viewing hidden and protected system files).

Symantec also states:

"After the payload check, the worm searches all subfolders on the C drive for Kazaa.exe. If the file is found, then the worm copies itself to \My Shared Folder as one of these files:

Summary (was Re: Ok, so I'm a lazy moron – Explorer crashes at startup)

microsoft.public.windowsxp.general: Summary (was Re: Ok, so I'm a lazy moron – Explorer crashes at startup)

- * XXX.exe
- * Gutter sluts.exe
- * Britney naked.exe
- * Buffy nude.exe
- * Sex sex sex.exe
- * Teen blow jobs.exe
- * Rapes video.mpeg.exe
- * Teen sex.mpeg.exe
- * 9 naked girls.exe
- * FULL SEX MOVIES.mpeg.exe"

None of the above files exist on the machine.

I have rebooted, gotten the error, Spybot finds the Xer0x problem, which I left unfixed this time to see if I could locate infected files and registry entries, then searched for the files and registry entries again and they do not exist.

I've run HijackThis and StartupList, neither show anything suspicious I've posted the HijackThis log twice in this thread already, but I'll include it again at the end of this post for easier reference. There is a LOT of stuff loading but all the extra stuff appears to me tablet PC goodies. I've searched on filenames in the log that I didn't recognize and they all seem to have to do with tablet PC hardware and accessories.

I have repeated all of the above checks many times in Safe Mode and Normal Mode. The results are always the same; only Spybot S&D finds anything and it's always the same Xer0x thing, it removes it and after a reboot (even in Safe Mode) it returns.

I have also run SFC /SCANNOW and it asks for a Windows XP Professional SP2 CD (SP2 ??? The Beta SP2 hasn't been installed that I can tell), won't accept any other XP Pro CD I've tried, will not read files from the i386 folder even though I edited the registry to point to the local drive path for SourcePath in two registry locations in accordance with instructions at:

<http://www.updatexp.com/scannow-sfc.html>

I do not have a Windows XP Tablet PC Edition CD, all that was supplied is a 3 CD re-imaging set, so I cannot refresh the i386 folder contents, nor do a repair install, nor boot to recovery console (it is not installed on the local disk and without a proper XP Tablet PC CD I cannot install it, nor perform an inplace upgrade.

I have removed all M\$ Hotfixes that had (SP2) in their names just in case that was throwing SFC off, ran SFC again with no change in results.

I've run CHKDSK a couple of times and there are no disk or file system errors.

Summary (was Re: Ok, so I'm a lazy moron – Explorer crashes at startup)

microsoft.public.windowsxp.general: Summary (was Re: Ok, so I'm a lazy moron – Explorer crashes at startup)

I don't think I've left anything out.

Now I've got the user's data backed up and I'm looking at blowing the whole Mary–Anne away and using the restore CD set unless I can find a real fix for this. I am 90% certain this is a worm but perhaps a new variant as yet "undiscovered" by the A/V folks.

I certainly appreciate everyone's advice and attempts at helping me with this. Big thanks–you's all around! But if anyone tells me to run CWS shredder, Spybot S&D, Ad–aware, HijackThis, A/v, or any on–line virus/spyware scans again I'm gonna PUKE!

Steve

Logfile of HijackThis v1.97.7
Scan saved at 11:34:14 AM, on 5/26/2004
Platform: Windows XP SP1 (WinNT 5.01.2600)
MSIE: Internet Explorer v6.00 SP1 (6.00.2800.1106)

Running processes:

C:\WINDOWS\System32\smss.exe
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\services.exe
C:\WINDOWS\system32\lsass.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\System32\svchost.exe
C:\WINDOWS\system32\spoolsv.exe
C:\Program Files\Command Software\Command AntiVirus\avinitnt.exe
C:\WINDOWS\System32\curvc.exe
C:\Program Files\Common Files\Command Software\dvpapi.exe
C:\WINDOWS\System32\gearsec.exe
C:\Program Files\Common Files\Microsoft Shared\VS7Debug\mdm.exe
C:\WINDOWS\System32\NALNTSRV.EXE
C:\Program Files\Command Software\Command AntiVirus\schscnt.exe
C:\WINDOWS\System32\wm.exe
C:\NOVELL\ZENRC\wuser32.exe
C:\NOVELL\ZENRC\WUOLService.exe
C:\WINDOWS\SYSTEM32\WISPTIS.EXE
C:\WINDOWS\System32\tabbtntu.exe
C:\WINDOWS\System32\ctfmon.exe
C:\Program Files\Common Files\microsoft shared\ink\TabTip.exe
C:\Program Files\Common Files\microsoft shared\ink\TPA.exe
C:\WINDOWS\System32\igfxtray.exe
C:\WINDOWS\System32\hkcmd.exe
C:\Program Files\Acer\Notebook Manager\almxptry.exe
C:\Program Files\Synaptics\SynTP\SynTPLpr.exe
C:\Program Files\Synaptics\SynTP\SynTPEnh.exe
C:\Progra~1\Launch Manager\LaunchAp.exe
C:\Progra~1\Launch Manager\PowerKey.exe

Summary (was Re: Ok, so I'm a lazy moron – Explorer crashes at startup)

microsoft.public.windowsxp.general: Summary (was Re: Ok, so I'm a lazy moron – Explorer crashes at startup)

C:\Progra~1\Launch Manager\HotkeyApp.exe
C:\Progra~1\Launch Manager\CtrlVol.exe
C:\Progra~1\Launch Manager\Wbutton.exe
C:\WINDOWS\System32\NWTRAY.EXE
C:\Program Files\Microsoft Hardware\Keyboard\type32.exe
C:\PROGRA~1\COMMAN~1\COMMAN~1\untray.exe
C:\PROGRA~1\COMMAN~1\COMMAN~1\dvprpt.exe
C:\PROGRA~1\COMMAN~1\COMMAN~1\avtray.exe
C:\Program Files\Palm\AlarmApp.exe
C:\WINDOWS\Explorer.exe
C:\WINDOWS\System32\wuauclt.exe
C:\temp\HijackThis\HijackThis.exe

R0 – HKCU\Software\Microsoft\Internet Explorer\Main,Start Page =

<http://global.acer.com>

R1 – HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL =

<http://global.acer.com>

R1 – HKCU\Software\Microsoft\Internet Connection Wizard,Shellnext =

<http://global.acer.com/>

O2 – BHO: (no name) – {06849E9F–C8D7–4D59–B87D–784B7D6BE0B3} –

C:\Program Files\Adobe\Acrobat 6.0\Acrobat\ActiveX\AcroIEHelper.dll

O2 – BHO: (no name) – {4E7BD74F–2B8D–469E–C0FF–FD60B590A87D} –

C:\PROGRA~1\COMMON~1\Real\Toolbar\realbar.dll

O2 – BHO: (no name) – {53707962–6F74–2D53–2644–206D7942484F} –

C:\Program Files\Spybot – Search & Destroy\SDHelper.dll

O2 – BHO: (no name) – {AA58ED58–01DD–4d91–8333–CF10577473F7} –

c:\program files\google\googletoolbar1.dll

O2 – BHO: (no name) – {AE7CD045–E861–484f–8273–0445EE161910} –

C:\Program Files\Adobe\Acrobat 6.0\Acrobat\AcroIEFavClient.dll

O3 – Toolbar: &Radio – {8E718888–423F–11D2–876E–00A0C9082467} –

C:\WINDOWS\System32\msdxm.ocx

O3 – Toolbar: Adobe PDF – {47833539–D0C5–4125–9FA8–0819E2EAAC93} –

C:\Program Files\Adobe\Acrobat 6.0\Acrobat\AcroIEFavClient.dll

O3 – Toolbar: REALBAR – {4E7BD74F–2B8D–469E–C0FF–FD60B590A87D} –

C:\PROGRA~1\COMMON~1\Real\Toolbar\realbar.dll

O3 – Toolbar: &Google – {2318C2B1–4965–11d4–9B18–009027A5CD4F} –

c:\program files\google\googletoolbar1.dll

O4 – HKLM\..\Run: [TabletTip] "C:\Program Files\Common Files\microsoft shared\ink\tabtip.exe" /resume

O4 – HKLM\..\Run: [IgfxTray] C:\WINDOWS\System32\igfxtray.exe

O4 – HKLM\..\Run: [HotKeysCmds] C:\WINDOWS\System32\hkcmd.exe

O4 – HKLM\..\Run: [AcerNotebookManager] C:\Program Files\Acer\Notebook Manager\almxp trays.exe

O4 – HKLM\..\Run: [SynTPLpr] C:\Program Files\Synaptics\SynTP\SynTPLpr.exe

O4 – HKLM\..\Run: [SynTPEnh] C:\Program Files\Synaptics\SynTP\SynTPEnh.exe

O4 – HKLM\..\Run: [LaunchAp] C:\Progra~1\Launch Manager\LaunchAp.exe

O4 – HKLM\..\Run: [PowerKey] "C:\Progra~1\Launch Manager\PowerKey.exe"

O4 – HKLM\..\Run: [HotkeyApp] C:\Progra~1\Launch Manager\HotkeyApp.exe

O4 – HKLM\..\Run: [CtrlVol] C:\Progra~1\Launch Manager\CtrlVol.exe

O4 – HKLM\..\Run: [Wbutton] "C:\Progra~1\Launch Manager\Wbutton.exe"

O4 – HKLM\..\Run: [NWTRAY] NWTRAY.EXE

Summary (was Re: Ok, so I'm a lazy moron – Explorer crashes at startup)

microsoft.public.windowsxp.general: Summary (was Re: Ok, so I'm a lazy moron – Explorer crashes at startup)

O4 – HKLM\..\Run: [IntelliType] "C:\Program Files\Microsoft Hardware\Keyboard\type32.exe"
O4 – HKLM\..\Run: [ZENRC Tray Icon] zentray.exe
O4 – HKLM\..\Run: [untray] C:\PROGRA~1\COMMAN~1\COMMAN~1\untray.exe
O4 – HKLM\..\Run: [dvprpt] C:\PROGRA~1\COMMAN~1\COMMAN~1\dvprpt.exe
O4 – HKLM\..\Run: [avtray] C:\PROGRA~1\COMMAN~1\COMMAN~1\avtray.exe
O4 – HKLM\..\Run: [CSAV_CheckViruses] C:\PROGRA~1\COMMAN~1\COMMAN~1\vchk.exe
O4 – HKCU\..\Run: [ctfmon.exe] C:\WINDOWS\System32\ctfmon.exe
O4 – HKCU\..\Run: [Zinio DLM] C:\Program Files\Zinio\ZDLM.exe /hide
O4 – Global Startup: SketchBook Snapshot.Ink = C:\Program Files\AliasWavefront\Alias SketchBook Pro 1.0\SketchBookSnap.exe
O4 – Global Startup: Alarm Manager.LNK = C:\Program Files\Palm\AlarmApp.exe
O9 – Extra button: FlingIt (HKLM)
O9 – Extra button: Research (HKLM)
O16 – DPF: {166B1BCA-3F9C-11CF-8075-444553540000} (Shockwave ActiveX Control) –
<http://download.macromedia.com/pub/shockwave/cabs/director/swdir.cab>
O16 – DPF: {1E2941E3-8E63-11D4-9D5A-00902742D6E0} (iNotes Class) –
<http://webmail.lincoln.k12.or.us/iNotes.cab>
O16 – DPF: {3BFFE033-BF43-11D5-A271-00A024A51325} (iNotes6 Class) –
<http://webmail.lincoln.k12.or.us/iNotes6.cab>
O16 – DPF: {41F17733-B041-4099-A042-B518BB6A408C} –
<http://a1408.g.akamai.net/7/1408/9955/20031218/akamai.info.apple.com/iTunes4/WW/win/019-0123.20031218.zes4>
O16 – DPF: {6F74F92E-8DD8-4DDE-8FB8-CBB882A68048} (Microsoft Office XP Professional Step by Step Interactive) – file://C:\Program Files\Microsoft Interactive Training\O10C\mitm0026.cab
O16 – DPF: {74D05D43-3236-11D4-BDCD-00C04F9A3B61} (HouseCall Control) –
<http://a840.g.akamai.net/7/840/537/7d90ae05585062/housecall.antivirus.com/housecall/xscan53.cab>
O16 – DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000} (Shockwave Flash Object) –
<http://fpdownload.macromedia.com/pub/shockwave/cabs/flash/swflash.cab>