

RE: SVCHost running at 99.9%

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2006-08/msg01041.htm

- *From:* TheNightElf <TheNightElf@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 25 Jul 2006 17:41:02 -0700
-

Jonathan, I had the exact same problem. I went to symantecs website and they decribed a virus which renames itself svchost and if u try to delete says is a critical sys file. They had removal tools which cured my comp

Try It Out.

TheNightElf

"jonathan.maughan@xxxxxxx" wrote:

I have a problem with a HP Laptop running Windows XP SP2 IE6 – All critical updates have been installed! The Virus checker is update to date which Sophos 5.2.3 and have performed a full virus sweep its clean – I have just installed Web Root Spy Sweeper that is fully update even thou old engine! Just a couple of doggie cookies not to worry about.

Additional tools used Process Explorer from sysinterns – When SVChosts process runs at 99% it refers to 1900 I don't know if this is refers to a TCP Port or not? The program does seem to very descriptive!

I have checked the hosts file and that is default (no changes)

I have also tried LSP Fix

With the followsing LSP's

msocket.dll – Gather this is ms winsock (No awards there)
winnr.dll – I think this is OK
wshbth.dll – Bluetooth namespace
bmi_lsp.dll – I am not sure what this?
rsvsp.dll – Don't know what this relates to!

Also I have used Hyena version v1.99.1 Log below

Logfile of HijackThis v1.99.1
Scan saved at 09:52:31, on 10/07/2006
Platform: Windows XP SP2 (WinNT 5.01.2600)

RE: SVCHost running at 99.9%

MSIE: Internet Explorer v6.00 SP2 (6.00.2900.2180)

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:\WINDOWS\system32\Ati2evxx.exe
C:\Program Files\WIDCOMM\Bluetooth Software\bin\btwdins.exe
C:\Program Files\Cisco Systems\VPN Client\cvpnd.exe
C:\Program Files\Common Files\Microsoft Shared\VS7DEBUG\MDM.EXE
C:\Program Files\lotus\notes\ntmulti.exe
C:\Program Files\Sophos\Sophos Anti-Virus\SAVAdminService.exe
C:\Program Files\Sophos\Remote Management System\ManagementAgentNT.exe
C:\Program Files\Sophos\Remote Management System\AutoUpdateAgentNT.exe
C:\Program Files\Sophos\AutoUpdate\ALsvc.exe
C:\Program Files\Sophos\Remote Management System\RouterNT.exe
C:\Program Files\Analog Devices\SoundMAX\SMAgent.exe
C:\WINDOWS\Explorer.EXE
C:\WINDOWS\system32\wuauclt.exe
C:\WINDOWS\AGRSMMMSG.exe
C:\Program Files\ATI Technologies\ATI Control Panel\atiptaxx.exe
C:\Program Files\Synaptics\SynTP\SynTPLpr.exe
C:\Program Files\Synaptics\SynTP\SynTPEnh.exe
C:\Program Files\HPQ\Quick Launch Buttons\EabServr.exe
C:\WINDOWS\system32\rundll32.exe
C:\Program Files\Nokia\Nokia PC Suite 6\LaunchApplication.exe
C:\Program Files\Common Files\PCSuite\DataLayer\DataLayer.exe
C:\Program Files\Hewlett-Packard\HP Mobile Printing\HPBMOBIL.EXE
C:\WINDOWS\system32\ctfmon.exe
C:\PROGRA~1\COMMON~1\PCSuite\Services\SERVIC~1.EXE
C:\Program Files\Sophos\AutoUpdate\ALMon.exe
C:\Program Files\Internet Explorer\iexplore.exe
C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32\wuauclt.exe
C:\Hijack This\HijackThis.exe

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

<http://www.hp.com/>

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

<http://www.hp.com>

R1 – HKCU\Software\Microsoft\Windows\CurrentVersion\Int

ernet Settings,ProxyServer = ftpukproxy:8080

O2 – BHO: AcroIEHlprObj Class – {06849E9F-C8D7-4D59-B87D-784B7D6BE0B3}

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

O4 – HKLM\..\Run: [ATIModeChange] Ati2mdxx.exe

O4 – HKLM\..\Run: [AGRSMMMSG] AGRSMMSG.exe

O4 – HKLM\..\Run: [ATIPTA] C:\Program Files\ATI Technologies\ATI

RE: SVCHost running at 99.9%

RE: SVCHost running at 99.9%

Control Panel\atiptaxx.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: [eabconfig.cpl] C:\Program Files\HPQ\Quick Launch Buttons\EabServr.exe /Start
O4 – HKLM\..\Run: [Cpqset] C:\Program Files\HPQ\Default Settings\cpqset.exe
O4 – HKLM\..\Run: [Synchronization Manager] %SystemRoot%\system32\mobsync.exe /logon
O4 – HKLM\..\Run: [BluetoothAuthenticationAgent] rundll32.exe bthprops.cpl,,BluetoothAuthenticationAgent
O4 – HKLM\..\Run: [PCSuiteTrayApplication] C:\Program Files\Nokia\Nokia PC Suite 6\LaunchApplication.exe –onlytray
O4 – HKLM\..\Run: [DataLayer] C:\Program Files\Common Files\PCSuite\DataLayer\DataLayer.exe
O4 – HKCU\..\Run: [HP Mobile Printing] C:\Program Files\Hewlett-Packard\HP Mobile Printing\HPBMOBIL.EXE
O4 – HKCU\..\Run: [ctfmon.exe] C:\WINDOWS\system32\ctfmon.exe
O4 – Global Startup: AutoUpdate Monitor.lnk = C:\Program Files\Sophos\AutoUpdate\ALMon.exe
O4 – Global Startup: BTTray.lnk = ?
O4 – Global Startup: Cisco Systems VPN Client.lnk = C:\Program Files\Cisco Systems\VPN Client\vpngui.exe
O8 – Extra context menu item: E&xport to Microsoft Excel – res://C:\PROGRA~1\MICROS~2\OFFICE11\EXCEL.EXE/3000
O8 – Extra context menu item: Send To &Bluetooth – C:\Program Files\WIDCOMM\Bluetooth Software\btsendto_ie_ctx.htm
O9 – Extra button: (no name) – {08B0E5C0-4FCB-11CF-AAA5-00401C608501} – C:\Program Files\Java\j2re1.4.2\bin\npjpi142.dll
O9 – Extra 'Tools' menuitem: Sun Java Console – {08B0E5C0-4FCB-11CF-AAA5-00401C608501} – C:\Program Files\Java\j2re1.4.2\bin\npjpi142.dll
O9 – Extra button: Research – {92780B25-18CC-41C8-B9BE-3C9C571A8263} – C:\PROGRA~1\MICROS~2\OFFICE11\REFIEBAR.DLL
O9 – Extra button: @btrez.dll,-4015 – {CCA281CA-C863-46ef-9331-5C8D4460577F} – C:\Program Files\WIDCOMM\Bluetooth Software\btsendto_ie.htm
O9 – Extra 'Tools' menuitem: @btrez.dll,-4017 – {CCA281CA-C863-46ef-9331-5C8D4460577F} – C:\Program Files\WIDCOMM\Bluetooth Software\btsendto_ie.htm
O9 – Extra button: eBay – Homepage – {EF79EAC5-3452-4E02-B8BD-BA4C89F1AC7A} – C:\Program Files\IrfanView\Ebay\Ebay.htm
O9 – Extra button: Messenger – {FB5F1910-F110-11d2-BB9E-00C04F795683} – C:\Program Files\Messenger\msmsgs.exe
O9 – Extra 'Tools' menuitem: Windows Messenger – {FB5F1910-F110-11d2-BB9E-00C04F795683} – C:\Program Files\Messenger\msmsgs.exe
O10 – Unknown file in Winsock LSP: c:\windows\system32\bmi_lsp.dll

RE: SVCHost running at 99.9%

RE: SVCHost running at 99.9%

O10 – Unknown file in Winsock LSP: c:\windows\system32\bmi_lsp.dll
O10 – Unknown file in Winsock LSP: c:\windows\system32\bmi_lsp.dll
O14 – IERESET.INF: START_PAGE_URL=<http://www.hp.com>
O23 – Service: Ati HotKey Poller – Unknown owner –
C:\WINDOWS\system32\Ati2evxx.exe
O23 – Service: Bluetooth Service (btwdins) – WIDCOMM, Inc. – C:\Program
Files\WIDCOMM\Bluetooth Software\bin\btwdins.exe
O23 – Service: Cisco Systems, Inc. VPN Service (CVPND) – Cisco Systems,
Inc. – C:\Program Files\Cisco Systems\VPN Client\cvpnd.exe
O23 – Service: HP WMI Interface (hpqwmi) – Hewlett-Packard Development
Company, L.P. – C:\Program Files\HPQ\SHARED\HPQWMI.exe
O23 – Service: Multi-user Cleanup Service – Unknown owner – C:\Program
Files\lotus\notes\ntmulti.exe
O23 – Service: Sophos Anti-Virus status reporter (SAVAdminService) –
Sophos plc – C:\Program Files\Sophos\Sophos
Anti-Virus\SAVAdminService.exe
O23 – Service: Sophos Anti-Virus (SAVService) – Sophos plc – C:\Program
Files\Sophos\Sophos Anti-Virus\SavService.exe
O23 – Service: Sophos Agent – Unknown owner – C:\Program
Files\Sophos\Remote Management System\ManagementAgentNT.exe" –service
–name Agent (file missing)
O23 – Service: Sophos AutoUpdate Agent – Unknown owner – C:\Program
Files\Sophos\Remote Management System\AutoUpdateAgentNT.exe" –service
–name ALC (file missing)
O23 – Service: Sophos AutoUpdate Service – Sophos plc – C:\Program
Files\Sophos\AutoUpdate\ALsvc.exe
O23 – Service: Sophos Message Router – Unknown owner – C:\Program
Files\Sophos\Remote Management System\RouterNT.exe" –service –name
Router –ORBListenEndpoints iiop://:8193/ssl_port=8194 (file missing)
O23 – Service: SoundMAX Agent Service (SoundMAX Agent Service
(default)) – Analog Devices, Inc. – C:\Program Files\Analog
Devices\SoundMAX\SMAgent.exe

The user reported the problems occurred after a print driver was installed, I deleted the print driver via control panel – Server Properties and drivers and deleted the relevant driver and the problem still exists!

Would appreciate any advise on this matter, I also think it suspicious that bmi_lsp.dll appears three times within the log of hyena!

Thanks