

## RE: CMD Slowing machine

**Source:**

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-12/9104.html>

---

**From:** taipan541 (taipan541\_at\_discussions.microsoft.com)

**Date:** 12/13/04

Date: Mon, 13 Dec 2004 07:45:04 -0800

"Boenerge" wrote:

- > I am running XP home edition with SP2. The cmd.exe is running 5-6 processes
- > in the task manager which is using 100% of the CPU - slowing the machine down.
- > I have run a full system virus check (norton), also spyware (spybot, ad aware
- > and spyblaster). I also ran hijackthis, here are the results:
- > 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\cmd.exe
- > C:\WINDOWS\system32\svchost.exe
- > C:\WINDOWS\system32\cmd.exe
- > C:\WINDOWS\system32\cmd.exe
- > C:\WINDOWS\system32\cmd.exe
- > C:\WINDOWS\System32\svchost.exe
- > C:\Program Files\Common Files\Symantec Shared\ccSetMgr.exe
- > C:\Program Files\Common Files\Symantec Shared\ccEvtMgr.exe
- > C:\WINDOWS\Explorer.exe
- > C:\WINDOWS\system32\spoolsv.exe
- > C:\WINDOWS\system32\cisvc.exe
- > C:\Program Files\Norton AntiVirus\navapvc.exe
- > C:\WINDOWS\system32\nvsvc32.exe
- > C:\Program Files\Norton AntiVirus\SAVScan.exe
- > C:\WINDOWS\System32\svchost.exe
- > C:\Program Files\Common Files\Symantec Shared\CCPD-LC\symclscvc.exe
- > C:\Program Files\Common Files\Symantec Shared\Security Center\SymWSC.exe
- > C:\Program Files\Thomson\SpeedTouch USB\Dragdiag.exe
- > C:\Program Files\Common Files\Symantec Shared\ccApp.exe
- > C:\Program Files\Advanced System Optimizer\adblock.exe
- > C:\WINDOWS\system32\ctfmon.exe
- > C:\WINDOWS\system32\cmd.exe
- > C:\WINDOWS\system32\cmd.exe
- > C:\WINDOWS\system32\cmd.exe
- > C:\WINDOWS\system32\wuauclt.exe

microsoft.public.windowsxp.general: RE: CMD Slowing machine

- > C:\Program Files\Internet Explorer\iexplore.exe
- > C:\Program Files\Norton AntiVirus\OPScan.exe
- > D:\temp\Computer\HijackThis.exe
- >
- > R0 – HKCU\Software\Microsoft\Internet Explorer\Main,Start Page =
- > <http://www.tesco.net/>
- > R0 – HKLM\Software\Microsoft\Internet Explorer\Main,Start Page =
- > R1 – HKLM\Software\Microsoft\Internet Explorer\Main,Default\_Page\_URL =
- > <http://www.tesco.net>
- > R0 – HKLM\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =
- > R0 – HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant =
- > F0 – system.ini: Shell=Explorer.exe winsock.scr
- > F2 – REG:system.ini: Shell=Explorer.exe winsock.scr
- > O2 – BHO: (no name) – {02478D38–C3F9–4efb–9B51–7695ECA05670} – C:\Program
- > Files\Yahoo!\common\ycomp5\_2\_3\_0.dll
- > O2 – BHO: (no name) – {06849E9F–C8D7–4D59–B87D–784B7D6BE0B3} – C:\Program
- > Files\Adobe\Acrobat 6.0\Reader\ActiveX\AcroIEHelper.dll
- > O2 – BHO: (no name) – {53707962–6F74–2D53–2644–206D7942484F} –
- > C:\PROGRA~1\SPYBOT~1\SDHelper.dll
- > O2 – BHO: NAV Helper – {BDF3E430–B101–42AD–A544–FADC6B084872} – C:\Program
- > Files\Norton AntiVirus\NavShExt.dll
- > O3 – Toolbar: BT Yahoo! Companion – {EF99BD32–C1FB–11D2–892F–0090271D4F88} –
- > C:\Program Files\Yahoo!\common\ycomp5\_2\_3\_0.dll
- > O3 – Toolbar: Norton AntiVirus – {42CDD1BF–3FFB–4238–8AD1–7859DF00B1D6} –
- > C:\Program Files\Norton AntiVirus\NavShExt.dll
- > O4 – HKLM\..\Run: [SpeedTouch USB Diagnostics] "C:\Program
- > Files\Thomson\SpeedTouch USB\Dragdiag.exe" /icon
- > O4 – HKLM\..\Run: [ccApp] "C:\Program Files\Common Files\Symantec
- > Shared\ccApp.exe"
- > O4 – HKLM\..\Run: [NvCplDaemon] RUNDLL32.EXE
- > C:\WINDOWS\system32\NvCpl.dll,NvStartup
- > O4 – HKLM\..\Run: [dxset.exe] C:\WINDOWS\dxsetu.exe
- > O4 – HKCU\..\Run: [Systweak Ad and Popup Blocker] "C:\Program Files\Advanced
- > System Optimizer\adblock.exe"
- > O4 – HKCU\..\Run: [ctfmon.exe] C:\WINDOWS\system32\ctfmon.exe
- > O8 – Extra context menu item: E&xport to Microsoft Excel –
- > res://C:\PROGRA~1\MICROS~2\OFFICE11\EXCEL.EXE/3000
- > O9 – Extra button: Research (HKLM)
- > O12 – Plugin for .mp3: C:\Program Files\Internet
- > Explorer\PLUGINS\npqtplugin3.dll
- > O14 – IERESET.INF: START\_PAGE\_URL=<http://www.tesco.net>
- > O16 – DPF: NTLSignup – <https://register.tesco.net/tesco/NTLSignup.cab>
- > O16 – DPF: {166B1BCA–3F9C–11CF–8075–444553540000} (Shockwave ActiveX
- > Control) – <http://download.macromedia.com/pub/shockwa...director/sw.cab>
- > O16 – DPF: {1803B9EF–9905–4F34–AFC4–05D1BAB28801} (RegUserCfgUI Class) –
- > <http://download.yahoo.com/dl/installs/bt/yregucfg.cab>
- > O16 – DPF: {30528230–99F7–4BB4–88D8–FA1D4F56A2AB} (YInstStarter Class) –
- > <http://download.yahoo.com/dl/installs/yinst.cab>
- > O16 – DPF: {3E68E405–C6DE–49FF–83AE–41EE9F4C36CE} (Office Update
- > Installation Engine) –
- > <http://office.microsoft.com/officeupdate/c...ontent/opuc.cab>

microsoft.public.windowsxp.general: RE: CMD Slowing machine

- > O16 – DPF: {4E888414–DB8F–11D1–9CD9–00C04F98436A} (Microsoft.WinRep) –  
> <https://webresponse.one.microsoft.com/OAS/A...iveX/winrep.cab>
- > O16 – DPF: {567A0EA2–5C76–497C–B95A–471944A1C843} (olConfig.onelogConfig) –  
> <http://webrouter.hud.ac.uk/downloads/files/olBrow.CAB>
- > O16 – DPF: {9F1C11AA–197B–4942–BA54–47A8489BB47F} –  
> <http://v4.windowsupdate.microsoft.com/CAB/...8043.2035648148>
- > O16 – DPF: {A8658086–E6AC–4957–BC8E–7D54A7E8A78E} (SassCln Object) –  
> <http://www.microsoft.com/security/controls.../20/SassCln.CAB>
- > O16 – DPF: {EC5A4E7B–02EB–451D–B310–D5F2E0A4D8C3} (webhelper Class) –  
> <http://register.btinternet.com/templates/b...bcontrol023.cab>
- > O17 –  
> HKLM\System\CCS\Services\Tcpip\..\{E94222E0–078C–4CB5–A855–7D596302C61E}:  
> NameServer = 194.168.4.100 194.168.8.100
- >
- > Any further help will be gratefully received.
- > Thanks

Hi Boenerge!!

Hm, i am amazed that there is cmd runnin in da task manager??izzit in da background or foreground? is this matter juz happened or it had been happenin long time ago since you start using?? well, some viruses use stealth status that it cant be detected by almost all anti–viruses program. Also some viruses injects itself into other application and it is difficult for anti–virus software to scan. So all you gotta do is to investigate this virus. Try ending task at task manager one by one and try your machine. then if u get the correct name for the virus, try to search that file and delete it in 'safe mode'. ( only delete application that u suspect there is virus).  
>From the list you showed, i can name you some of adware/spyware you have got. well, hope it helps. Byezzz!!!~~~