Logfile of Trend Micro HijackThis v2.0.2

Scan saved at 6:13:15 PM, on 4/6/2010

Platform: Windows Vista SP2 (WinNT 6.00.1906)

MSIE: Internet Explorer v8.00 (8.00.6001.18904)

Boot mode: Normal

Running processes:

C:\Program Files (x86)\Adobe\Reader 9.0\Reader\reader_sl.exe

C:\Program Files (x86)\Sensible Vision\Fast Access\FATrayMon.exe

C:\Program Files (x86)\Dell Webcam\Dell Webcam Central\WebcamDell.exe

C:\Program Files (x86)\Dell\MediaDirect\PCMService.exe

C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe

C:\Program Files (x86)\Sensible Vision\Fast Access\FATrayAlert.exe

C:\Program Files\Logitech\SetPoint\x86\SetPoint32.exe

C:\Program Files (x86)\Trend Micro\HijackThis\HijackThis.exe

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = http://g.msn.com/USCON/1

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page =
http://go.microsoft.com/fwlink/?LinkId=54896

R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page = http://google.com/

R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL =
http://go.microsoft.com/fwlink/?LinkId=69157

R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL =
http://go.microsoft.com/fwlink/?LinkId=54896

R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page =
http://go.microsoft.com/fwlink/?LinkId=54896

R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Start Page = http://go.microsoft.com/fwlink/?LinkId=69157

R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant =

R0 - HKLM\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =

R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Local Page = C:\Windows\SysWOW64\blank.htm

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Window Title = Internet Explorer provided by Dell

R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName =

R3 - URLSearchHook: Yahoo! Toolbar - {EF99BD32-C1FB-11D2-892F-0090271D4F88} - C:\Program Files (x86)\Yahoo!\Companion\Installs\cpn\yt.dll

O1 - Hosts: ::1 localhost

O2 - BHO: &Yahoo! Toolbar Helper - {02478D38-C3F9-4efb-9B51-7695ECA05670} - C:\Program Files (x86)\Yahoo!\Companion\Installs\cpn\yt.dll

O2 - BHO: AcroIEHelperStub - {18DF081C-E8AD-4283-A596-FA578C2EBDC3} - c:\Program Files (x86)\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll

O2 - BHO: RealPlayer Download and Record Plugin for Internet Explorer - {3049C3E9-B461-4BC5-8870-4C09146192CA} - C:\ProgramData\Real\RealPlayer\BrowserRecordPlugin\IE\rpbrowserrecordplugin.dll

O2 - BHO: Search Helper - {6EBF7485-159F-4bff-A14F-B9E3AAC4465B} - C:\Program Files (x86)\Microsoft\Search Enhancement Pack\Search Helper\SEPsearchhelperie.dll

O2 - BHO: FAIESSO Helper Object - {A2F122DA-055F-4df7-8F24-7354DBDBA85B} - C:\Program Files (x86)\Sensible Vision\Fast Access\FAIESSO.dll

O2 - BHO: Java(tm) Plug-In 2 SSV Helper - {DBC80044-A445-435b-BC74-9C25C1C588A9} - C:\Program Files (x86)\Java\jre6\bin\jp2ssv.dll

O2 - BHO: SingleInstance Class - {FDAD4DA1-61A2-4FD8-9C17-86F7AC245081} - C:\Program Files (x86)\Yahoo!\Companion\Installs\cpn\YTSingleInstance.dll

O3 - Toolbar: Yahoo! Toolbar - {EF99BD32-C1FB-11D2-892F-0090271D4F88} - C:\Program Files (x86)\Yahoo!\Companion\Installs\cpn\yt.dll

O4 - HKLM\..\Run: [Adobe Reader Speed Launcher] "c:\Program Files (x86)\Adobe\Reader 9.0\Reader\Reader_sl.exe"

O4 - HKLM\..\Run: [FATrayAlert] C:\Program Files (x86)\Sensible Vision\Fast Access\FATrayMon.exe

O4 - HKLM\..\Run: [Dell Webcam Central] "C:\Program Files (x86)\Dell Webcam\Dell Webcam Central\WebcamDell.exe" /mode2

O4 - HKLM\..\Run: [PCMService] "C:\Program Files (x86)\Dell\MediaDirect\PCMService.exe"

O4 - HKLM\..\Run: [AT&T Communication Manager] "C:\Program Files (x86)\AT&T\Communication Manager\ATTCM.exe" -a

O4 - HKLM\..\Run: [SunJavaUpdateSched] "C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe"

O4 - HKLM\..\Run: [TkBellExe] "C:\Program Files (x86)\Common Files\Real\Update_OB\realsched.exe" -osboot

O4 - HKLM\..\Run: [QuickTime Task] "C:\Program Files (x86)\QuickTime\QTTask.exe" -atboottime

O4 - HKCU\..\Run: [msnmsgr] "C:\Program Files (x86)\Windows Live\Messenger\msnmsgr.exe" /background

O4 - HKUS\S-1-5-19\..\Run: [Sidebar] %ProgramFiles%\Windows Sidebar\Sidebar.exe /detectMem (User 'LOCAL SERVICE')

O4 - HKUS\S-1-5-19\..\Run: [WindowsWelcomeCenter] rundll32.exe oobefldr.dll,ShowWelcomeCenter (User 'LOCAL SERVICE')

O4 - HKUS\S-1-5-20\..\Run: [Sidebar] %ProgramFiles%\Windows Sidebar\Sidebar.exe /detectMem (User 'NETWORK SERVICE')

O4 - .DEFAULT User Startup: Dell Dock First Run.lnk = C:\Program Files\Dell\DellDock\DellDock.exe (User 'Default user')

O4 - Global Startup: Logitech SetPoint.lnk = ?

O4 - Global Startup: QuickSet.lnk = ?

O8 - Extra context menu item: E&xport to Microsoft Excel - res://C:\PROGRA~2\MICROS~2\Office12\EXCEL.EXE/3000

O9 - Extra button: Research - {92780B25-18CC-41C8-B9BE-3C9C571A8263} - C:\PROGRA~2\MICROS~2\Office12\REFIEBAR.DLL

O10 - Unknown file in Winsock LSP: bmnet.dll

O10 - Unknown file in Winsock LSP: bmnet.dll

O10 - Unknown file in Winsock LSP: bmnet.dll

O13 - Gopher Prefix:

O18 - Protocol: cozi - {5356518D-FE9C-4E08-9C1F-1E872ECD367F} - C:\Program Files (x86)\Cozi Express\CoziProtocolHandler.dll

O20 - Winlogon Notify: FastAccess - C:\Program Files (x86)\Sensible Vision\Fast Access\FALogNot.dll

O23 - Service: Andrea ST Filters Service (AESTFilters) - Unknown owner - C:\Windows\System32\DriverStore\FileRepository\stwrt64.inf_cce24a4c\AESTSr64.exe (file missing)

O23 - Service: @%SystemRoot%\system32\Alg.exe,-112 (ALG) - Unknown owner - C:\Windows\System32\alg.exe (file missing)

O23 - Service: AT&T RcAppSvc (ATTRcAppSvc) - SmithMicro Inc. - C:\Program Files (x86)\AT&T\Communication Manager\RcAppSvc.exe

O23 - Service: AT&T Con App Svc (CAATT) - SmithMicro Inc. - C:\Program Files (x86)\AT&T\Communication Manager\ConAppsSvc.exe

O23 - Service: Crypkey License - Unknown owner - crypserv.exe (file missing)

O23 - Service: @dfsrres.dll,-101 (DFSR) - Unknown owner - C:\Windows\system32\DFSR.exe (file missing)

O23 - Service: Dock Login Service (DockLoginService) - Stardock Corporation - C:\Program Files\Dell\DellDock\DockLogin.exe

O23 - Service: FAService - Sensible Vision - C:\Program Files (x86)\Sensible Vision\Fast Access\FAService.exe

O23 - Service: GameConsoleService - WildTangent, Inc. - C:\Program Files (x86)\WildTangent\Dell Games\Dell Game Console\GameConsoleService.exe

O23 - Service: @keyiso.dll,-100 (KeyIso) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)

O23 - Service: Logitech Bluetooth Service (LBTServ) - Logitech, Inc. - C:\Program Files\Common Files\Logitech\Bluetooth\LBTServ.exe

O23 - Service: @comres.dll,-2797 (MSDTC) - Unknown owner - C:\Windows\System32\msdtc.exe (file missing)

O23 - Service: @%SystemRoot%\System32\netlogon.dll,-102 (Netlogon) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)

O23 - Service: @%systemroot%\system32\psbase.dll,-300 (ProtectedStorage) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)

O23 - Service: @%systemroot%\system32\Locator.exe,-2 (RpcLocator) - Unknown owner - C:\Windows\system32\locator.exe (file missing)

O23 - Service: @%SystemRoot%\system32\samsrv.dll,-1 (SamSs) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)

O23 - Service: Trend Micro Central Control Component (SfCtlCom) - Trend Micro Inc. - C:\Program Files\Trend Micro\Internet Security\SfCtlCom.exe

O23 - Service: @%SystemRoot%\system32\SLsvc.exe,-101 (slsvc) - Unknown owner - C:\Windows\system32\SLsvc.exe (file missing)

O23 - Service: @%SystemRoot%\system32\snmptrap.exe,-3 (SNMPTRAP) - Unknown owner - C:\Windows\System32\snmptrap.exe (file missing)

O23 - Service: @%systemroot%\system32\spoolsv.exe,-1 (Spooler) - Unknown owner - C:\Windows\System32\spoolsv.exe (file missing)

O23 - Service: Audio Service (STacSV) - Unknown owner - C:\Windows\System32\DriverStore\FileRepository\stwrt64.inf_cce24a4c\STacSV64.exe (file missing)

O23 - Service: stllssvr - MicroVision Development, Inc. - C:\Program Files (x86)\Common Files\SureThing Shared\stllssvr.exe

O23 - Service: Trend Micro Unauthorized Change Prevention Service (TMBMServer) - Trend Micro Inc. - C:\Program Files\Trend Micro\BM\TMBMSRV.exe

O23 - Service: Trend Micro Personal Firewall (TmPfw) - Trend Micro Inc. - C:\PROGRA~1\TRENDM~1\INTERN~1\TmPfw.exe

O23 - Service: Trend Micro Proxy Service (tmproxy) - Trend Micro Inc. - C:\Program Files\Trend Micro\Internet Security\TmProxy.exe

O23 - Service: @%SystemRoot%\system32\ui0detect.exe,-101 (UI0Detect) - Unknown owner - C:\Windows\system32\UI0Detect.exe (file missing)

O23 - Service: @%SystemRoot%\system32\vds.exe,-100 (vds) - Unknown owner - C:\Windows\System32\vds.exe (file missing)

O23 - Service: @%systemroot%\system32\vssvc.exe,-102 (VSS) - Unknown owner - C:\Windows\system32\vssvc.exe (file missing)

O23 - Service: Dell Wireless WLAN Tray Service (wltrysvc) - Unknown owner - C:\Windows\System32\WLTRYSVC.EXE (file missing)

O23 - Service: @%Systemroot%\system32\wbem\wmiapsrv.exe,-110 (wmiApSrv) - Unknown owner - C:\Windows\system32\wbem\WmiApSrv.exe (file missing)

O23 - Service: @%ProgramFiles%\Windows Media Player\wmpnetwk.exe,-101 (WMPNetworkSvc) - Unknown owner - C:\Program Files (x86)\Windows Media Player\wmpnetwk.exe (file missing)

--

End of file - 9401 bytes