Logfile of Trend Micro HijackThis v2.0.4
Scan saved at 23:57:58, on 28.06.2010
Platform: Windows 7 (WinNT 6.00.3504)
MSIE: Internet Explorer v8.00 (8.00.7600.16385)
Boot mode: Normal

Running processes:
C:\Windows\System32\smss.exe
C:\Windows\system32\csrss.exe
C:\Windows\system32\wininit.exe
C:\Windows\system32\csrss.exe
C:\Windows\system32\services.exe
C:\Windows\system32\lsass.exe
C:\Windows\system32\lsm.exe
C:\Windows\system32\winlogon.exe
C:\Windows\system32\svchost.exe
C:\Windows\system32\nvvsvc.exe
C:\Windows\system32\svchost.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\svchost.exe
C:\Windows\system32\svchost.exe
C:\Windows\System32\DriverStore\FileRepository\stwrt.inf_x86_neutral_ef7356bc77a65e9e\STacSV.exe
C:\Windows\system32\svchost.exe
C:\Windows\system32\nvvsvc.exe
C:\Windows\system32\svchost.exe
C:\Windows\System32\spoolsv.exe
C:\Windows\system32\svchost.exe
C:\Windows\system32\Dwm.exe
C:\Windows\Explorer.EXE
C:\Program Files\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe
C:\Program Files\Bonjour\mDNSResponder.exe
C:\Windows\system32\taskhost.exe
C:\Program Files\DU Meter\DUMeterSvc.exe
C:\Windows\system32\svchost.exe
C:\Program Files\Intel\Intel Desktop Utilities\iptray.exe
C:\Program Files\IDT\WDM\sttray.exe
C:\Program Files\ThreatFire\TFTray.exe
C:\Program Files\Logitech\SetPointP\SetPoint.exe
C:\Program Files\Microsoft Office\Office12\GrooveMonitor.exe
C:\Program Files\Razer\Lachesis\razerhid.exe
C:\Program Files\Common Files\LogiShrd\KHAL3\KHALMNPR.EXE
C:\Program Files\Razer\Lachesis\OSD.exe
C:\Windows\Samsung\PanelMgr\SSMMgr.exe
C:\Program Files\Spybot - Search & Destroy\TeaTimer.exe
C:\Program Files\Windows Sidebar\sidebar.exe

C:\Program Files\DU Meter\DUMeter.exe
C:\Program Files\DAEMON Tools Lite\DTLite.exe
C:\Program Files\Razer\Lachesis\razertra.exe
C:\Program Files\Microsoft Office\Office12\ONENOTEM.EXE
C:\Program Files\Razer\Lachesis\razerofa.exe
C:\Program Files\Winamp\winamp.exe
C:\PROGRAM FILES\STREAMRIPPER\wstreamripper.exe
C:\Program Files\Common Files\Nero\Nero BackItUp 4\NBService.exe
C:\Program Files\NVIDIA Corporation\3D Vision\nvSCPAPISvr.exe
C:\Windows\system32\svchost.exe
C:\Program Files\ThreatFire\TFService.exe
C:\Program Files\Spybot - Search & Destroy\SDWinSec.exe
C:\Program Files\Windows Media Player\wmpnetwk.exe
C:\Program Files\Intel\Intel Desktop Utilities\iduServ.exe
C:\Program Files\Mozilla Thunderbird\thunderbird.exe
C:\Programme\Firefox\firefox.exe
C:\Programme\Firefox\plugin-container.exe
C:\Windows\System32\svchost.exe
C:\Program Files\Soulseek\slsk.exe
C:\Windows\system32\SearchIndexer.exe
C:\Program Files\VideoLAN\VLC\vlc.exe
C:\Program Files\TuneUp Utilities 2010\Integrator.exe
C:\Program Files\TuneUp Utilities 2010\TuneUpUtilitiesService32.exe
C:\Program Files\TuneUp Utilities 2010\TuneUpUtilitiesApp32.exe
C:\Windows\system32\mspaint.exe
C:\Windows\system32\SearchProtocolHost.exe
C:\Windows\system32\SearchFilterHost.exe
C:\Users\fizzbitch\Downloads\HiJackThis204.exe
C:\Windows\system32\wbem\wmiprvse.exe

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://go.microsoft.com/fwlink/?LinkId=69157
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 =
R1 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyOverride = *.local
R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName =

O2 - BHO: AcroIEHelperStub - {18DF081C-E8AD-4283-A596-FA578C2EBDC3} - C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll
O2 - BHO: Spybot-S&D IE Protection - {53707962-6F74-2D53-2644-206D7942484F} - C:\PROGRA~1\SPYBOT~1\SDHelper.dll
O2 - BHO: Groove GFS Browser Helper - {72853161-30C5-4D22-B7F9-0BBC1D38A37E} - C:\Program Files\Microsoft Office\Office12\GrooveShellExtensions.dll
O2 - BHO: SkypeIEPluginBHO - {AE805869-2E5C-4ED4-8F7B-F1F7851A4497} - C:\Program Files\Skype\Toolbars\Internet Explorer\skypeieplugin.dll
O2 - BHO: Java(tm) Plug-In 2 SSV Helper - {DBC80044-A445-435b-BC74-9C25C1C588A9} - C:\Program Files\Java\jre6\bin\jp2ssv.dll
O4 - HKLM\..\Run: [ipTray.exe] "C:\Program Files\Intel\Intel Desktop Utilities\ipTray.exe"
O4 - HKLM\..\Run: [SysTrayApp] %ProgramFiles%\IDT\WDM\sttray.exe
O4 - HKLM\..\Run: [ThreatFire] C:\Program Files\ThreatFire\TFTray.exe
O4 - HKLM\..\Run: [EvtMgr6] C:\Program Files\Logitech\SetPointP\SetPoint.exe /launchGaming
O4 - HKLM\..\Run: [QuickTime Task] "C:\Program Files\QuickTime\QTTask.exe" -atboottime
O4 - HKLM\..\Run: [GrooveMonitor] "C:\Program Files\Microsoft Office\Office12\GrooveMonitor.exe"
O4 - HKLM\..\Run: [Adobe Reader Speed Launcher] "C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"
O4 - HKLM\..\Run: [Adobe ARM] "C:\Program Files\Common Files\Adobe\ARM\1.0\AdobeARM.exe"
O4 - HKLM\..\Run: [Lachesis] C:\Program Files\Razer\Lachesis\razerhid.exe
O4 - HKLM\..\Run: [Samsung PanelMgr] C:\Windows\Samsung\PanelMgr\SSMMgr.exe /autorun
O4 - HKCU\..\Run: [SpybotSD TeaTimer] C:\Program Files\Spybot - Search & Destroy\TeaTimer.exe
O4 - HKCU\..\Run: [Sidebar] C:\Program Files\Windows Sidebar\sidebar.exe /autoRun
O4 - HKCU\..\Run: [DU Meter] C:\Program Files\DU Meter\DUMeter.exe
O4 - HKCU\..\Run: [DAEMON Tools Lite] "C:\Program Files\DAEMON Tools Lite\DTLite.exe" -autorun
O4 - HKCU\..\Run: [Skype] "C:\Program Files\Skype\Phone\Skype.exe" /nosplash /minimized
O4 - HKUS\S-1-5-19\..\Run: [Sidebar] %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun (User 'LOKALER DIENST')
O4 - HKUS\S-1-5-19\..\RunOnce: [mctadmin] C:\Windows\System32\mctadmin.exe (User 'LOKALER DIENST')
O4 - HKUS\S-1-5-20\..\Run: [Sidebar] %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun (User 'NETZWERKDIENST')
O4 - HKUS\S-1-5-20\..\RunOnce: [mctadmin] C:\Windows\System32\mctadmin.exe (User 'NETZWERKDIENST')
O4 - Startup: OneNote 2007 Bildschirmausschnitt- und Startprogramm.lnk = C:\Program Files\Microsoft Office\Office12\ONENOTEM.EXE
O8 - Extra context menu item: Add to Google Photos Screensa&ver - res://C:\Windows\system32\GPhotos.scr/200
O8 - Extra context menu item: Nach Microsoft E&xel exportieren - res://C:\PROGRA~1\MICROS~1\Office12\EXCEL.EXE/3000
O9 - Extra button: An OneNote senden - {2670000A-7350-4f3c-8081-5663EE0C6C49} - C:\PROGRA~1\MICROS~1\Office12\ONBttnIE.dll
O9 - Extra 'Tools' menuitem: An OneNote s&enden - {2670000A-7350-4f3c-8081-5663EE0C6C49} - C:\PROGRA~1\MICROS~1\Office12\ONBttnIE.dll

O9 - Extra button: Skype add-on for Internet Explorer - {898EA8C8-E7FF-479B-8935-AEC46303B9E5} - C:\Program Files\Skype\Toolbars\Internet Explorer\skypeieplugin.dll
O9 - Extra 'Tools' menuitem: Skype add-on for Internet Explorer - {898EA8C8-E7FF-479B-8935-AEC46303B9E5} - C:\Program Files\Skype\Toolbars\Internet Explorer\skypeieplugin.dll
O9 - Extra button: Research - {92780B25-18CC-41C8-B9BE-3C9C571A8263} - C:\PROGRA~1\MICROS~1\Office12\REFIEBAR.DLL
O9 - Extra button: (no name) - {DFB852A3-47F8-48C4-A200-58CAB36FD2A2} - C:\PROGRA~1\SPYBOT~1\SDHelper.dll
O9 - Extra 'Tools' menuitem: Spybot - Search & Destroy Configuration - {DFB852A3-47F8-48C4-A200-58CAB36FD2A2} - C:\PROGRA~1\SPYBOT~1\SDHelper.dll
O16 - DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000} (Shockwave Flash Object) - http://fpdownload2.macromedia.com/get/shockwave/cabs/flash/swflash.cab
O17 - HKLM\System\CCS\Services\Tcpip\..\{64545FE8-F364-4B23-BDB6-C3868933AE75}: NameServer = 62.2.24.162,62.2.17.60
O17 - HKLM\System\CS1\Services\Tcpip\..\{64545FE8-F364-4B23-BDB6-C3868933AE75}: NameServer = 62.2.24.162,62.2.17.60
O17 - HKLM\System\CS2\Services\Tcpip\..\{64545FE8-F364-4B23-BDB6-C3868933AE75}: NameServer = 62.2.24.162,62.2.17.60
O18 - Protocol: grooveLocalGWS - {88FED34C-F0CA-4636-A375-3CB6248B04CD} - C:\Program Files\Microsoft Office\Office12\GrooveSystemServices.dll
O18 - Protocol: skype-ie-addon-data - {91774881-D725-4E58-B298-07617B9B86A8} - C:\Program Files\Skype\Toolbars\Internet Explorer\skypeieplugin.dll
O18 - Protocol: skype4com - {FFC8B962-9B40-4DFF-9458-1830C7DD7F5D} - C:\PROGRA~1\COMMON~1\Skype\SKYPE4~1.DLL
O23 - Service: Apple Mobile Device - Apple Inc. - C:\Program Files\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe
O23 - Service: Dienst "Bonjour" (Bonjour Service) - Apple Inc. - C:\Program Files\Bonjour\mDNSResponder.exe
O23 - Service: DU Meter Service (DUMeterSvc) - Hagel Technologies Ltd. - C:\Program Files\DU Meter\DUMeterSvc.exe
O23 - Service: Google Updater Service (gusvc) - Google - C:\Program Files\Google\Common\Google Updater\GoogleUpdaterService.exe
O23 - Service: Intel(R) Desktop Utilities Service (IduService) - Intel(R) Corporation - C:\Program Files\Intel\Intel Desktop Utilities\iduServ.exe
O23 - Service: iPod-Dienst (iPod Service) - Apple Inc. - C:\Program Files\iPod\bin\iPodService.exe
O23 - Service: Logitech Bluetooth Service (LBTServ) - Logitech, Inc. - C:\Program Files\Common Files\LogiShrd\Bluetooth\lbtserv.exe
O23 - Service: Nero BackItUp Scheduler 4.0 - Nero AG - C:\Program Files\Common Files\Nero\Nero BackItUp 4\NBService.exe
O23 - Service: NVIDIA Display Driver Service (nvsvc) - NVIDIA Corporation - C:\Windows\system32\nvvsvc.exe
O23 - Service: SBSD Security Center Service (SBSDWSCService) - Safer Networking Ltd. - C:\Program Files\Spybot - Search & Destroy\SDWinSec.exe
O23 - Service: Audio Service (STacSV) - IDT, Inc. - C:\Windows\System32\DriverStore\FileRepository\stwrt.inf_x86_neutral_ef7356bc77a65e9e\STacSV.exe

O23 - Service: NVIDIA Stereoscopic 3D Driver Service (Stereo Service) - NVIDIA Corporation - C:\Program Files\NVIDIA Corporation\3D Vision\nvSCPAPISvr.exe
O23 - Service: ThreatFire - PC Tools - C:\Program Files\ThreatFire\TFService.exe
O23 - Service: @C:\Program Files\TuneUp Utilities 2010\TuneUpDefragService.exe,-1 (TuneUp.Defrag) - TuneUp Software - C:\Program Files\TuneUp Utilities 2010\TuneUpDefragService.exe
O23 - Service: TuneUp Utilities Service (TuneUp.UtilitiesSvc) - TuneUp Software - C:\Program Files\TuneUp Utilities 2010\TuneUpUtilitiesService32.exe

--
End of file - 10742 bytes