Logfile of Trend Micro HijackThis v2.0.4
Scan saved at 17:36:20, on 30.12.2011
Platform: Windows Vista SP2 (WinNT 6.00.1906)
MSIE: Internet Explorer v9.00 (9.00.8112.16421)
Boot mode: Normal

Running processes:
C:\Windows\system32\Dwm.exe
C:\Windows\Explorer.EXE
C:\Windows\system32\taskeng.exe
C:\Program Files\pdf24\pdf24.exe
C:\Program Files\Canon\Canon IJ Network Scan Utility\CNMNSUT.EXE
C:\Acer\Empowering Technology\eAudio\eAudio.exe
C:\Program Files\Canon\SolutionMenu\CNSLMAIN.EXE
C:\Program Files\Canon\MyPrinter\BJMYPRT.EXE
C:\Program Files\avmwlanstick\WLanGUI.exe
C:\Windows\System32\spool\drivers\w32x86\3\WrtMon.exe
C:\Windows\RtHDVCpl.exe
C:\Program Files\CyberLink\PowerDVD9\PDVD9Serv.exe
C:\Program Files\ScanSoft\OmniPageSE4\OpWareSE4.exe
C:\Windows\System32\rundll32.exe
C:\Windows\System32\rundll32.exe
C:\Windows\System32\spool\drivers\w32x86\3\WrtProc.exe
C:\Users\Master\AppData\Local\Temp\RtkBtMnt.exe
C:\Program Files\TuneUp Utilities 2012\TuneUpUtilitiesApp32.exe
C:\Program Files\Logitech\SetPointP\SetPoint.exe
C:\Acer\Empowering Technology\eDataSecurity\eDSLoader.exe
C:\Program Files\CyberLink\Shared Files\brs.exe
C:\Program Files\Apoint2K\Apoint.exe
C:\Program Files\Google\GoogleToolbarNotifier\GoogleToolbarNotifier.exe
C:\Program Files\Windows Sidebar\sidebar.exe
C:\Program Files\Windows Media Player\wmpnscfg.exe
C:\Program Files\GamesBar\SearchEngineProtection.exe
C:\Windows\ehome\ehtray.exe
C:\Program Files\TechSmith\Snagit 10\Snagit32.exe
C:\Program Files\WinZip\WZQKPICK.EXE
C:\Program Files\Microsoft Office\Office12\ONENOTEM.EXE
C:\Acer\Empowering Technology\ENET\ENMTRAY.EXE
C:\Acer\Empowering Technology\EPOWER\EPOWER_DMC.EXE
C:\Program Files\Windows Sidebar\sidebar.exe
C:\Acer\Empowering Technology\ACER.EMPOWERING.FRAMEWORK.SUPERVISOR.EXE
C:\Acer\Empowering Technology\eRecovery\ERAGENT.EXE
C:\Windows\ehome\ehmsas.exe
C:\Program Files\Apoint2K\Apntex.exe
C:\Program Files\TechSmith\Snagit 10\TSCHelp.exe
C:\Program Files\Common Files\LogiShrd\KHAL3\KHALMNPR.EXE
C:\Program Files\TechSmith\Snagit 10\snagiteditor.exe
C:\Windows\system32\conime.exe
C:\Program Files\Internet Explorer\iexplore.exe
C:\Program Files\Internet Explorer\iexplore.exe
C:\Program Files\Google\Google Toolbar\GoogleToolbarUser_32.exe
C:\Windows\system32\Macromed\Flash\FlashUtil11e_ActiveX.exe
C:\Users\Master\Downloads\HiJackThis204.exe

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar = Preserve
R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page =
http://www.t-online.de/
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 =
R3 - URLSearchHook: Winamp Search Class - {57BCA5FA-5DBB-45a2-B558-1755C3F6253B} - C:\Program Files\Winamp Toolbar\winamptb.dll
O1 - Hosts: ::1 localhost
O2 - BHO: SnagIt Toolbar Loader - {00C6482D-C502-44C8-8409-FCE54AD9C208} - C:\Program Files\TechSmith\Snagit 10\SnagitBHO.dll
O2 - BHO: &Yahoo! Toolbar Helper - {02478D38-C3F9-4efb-9B51-7695ECA05670} - C:\Program Files\Yahoo!\Companion\Installs\cpn\yt.dll
O2 - BHO: AcroIEHelperStub - {18DF081C-E8AD-4283-A596-FA578C2EBDC3} - C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll
O2 - BHO: Winamp Toolbar Loader - {25CEE8EC-5730-41bc-8B58-22DDC8AB8C20} - C:\Program Files\Winamp Toolbar\winamptb.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: Norton Identity Protection - {602ADB0E-4AFF-4217-8AA1-95DAC4DFA408} - C:\Program Files\Norton Internet Security\Engine\19.2.0.10\coIEPlg.dll
O2 - BHO: Norton Vulnerability Protection - {6D53EC84-6AAE-4787-AEEE-F4628F01010C} - C:\Program Files\Norton Internet Security\Engine\19.2.0.10\IPS\IPSBHO.DLL
O2 - BHO: Softonic Deutsch FF Toolbar - {9d81af43-de53-48d0-a199-42c2a226b24c} - C:\Program Files\Softonic_Deutsch_FF\tbSoft.dll
O2 - BHO: Google Toolbar Helper - {AA58ED58-01DD-4d91-8333-CF10577473F7} - C:\Program Files\Google\Google Toolbar\GoogleToolbar_32.dll
O2 - BHO: GamesBarBHO Class - {CB0D163C-E9F4-4236-9496-0597E24B23A5} - C:\Program Files\GamesBar\2.0.1.67\oberontb.dll
O2 - BHO: Java(tm) Plug-In 2 SSV Helper - {DBC80044-A445-435b-BC74-9C25C1C588A9} - C:\Program Files\Java\jre7\bin\jp2ssv.dll
O2 - BHO: SingleInstance Class - {FDAD4DA1-61A2-4FD8-9C17-86F7AC245081} - C:\Program Files\Yahoo!\Companion\Installs\cpn\YTSingleInstance.dll
O3 - Toolbar: Acer eDataSecurity Management - {5CBE3B7C-1E47-477e-A7DD-396DB0476E29} - C:\Windows\system32\eDStoolbar.dll
O3 - Toolbar: Snagit - {8FF5E183-ABDE-46EB-B09E-D2AAB95CABE3} - C:\Program Files\TechSmith\Snagit 10\SnagitIEAddin.dll
O3 - Toolbar: Yahoo! Toolbar - {EF99BD32-C1FB-11D2-892F-0090271D4F88} - C:\Program Files\Yahoo!\Companion\Installs\cpn\yt.dll
O3 - Toolbar: Softonic Deutsch FF Toolbar - {9d81af43-de53-48d0-a199-42c2a226b24c} - C:\Program Files\Softonic_Deutsch_FF\tbSoft.dll
O3 - Toolbar: Winamp Toolbar - {EBF2BA02-9094-4c5a-858B-BB198F3D8DE2} - C:\Program Files\Winamp Toolbar\winamptb.dll
O3 - Toolbar: GamesBar - {6F282B65-56BF-4BD1-A8B2-A4449A05863D} - C:\Program Files\GamesBar\2.0.1.67\oberontb.dll
O3 - Toolbar: Norton Toolbar - {7FEBEFE3-6B19-4349-98D2-FFB09D4B49CA} - C:\Program Files\Norton Internet Security\Engine\19.2.0.10\coIEPlg.dll
O3 - Toolbar: Google Toolbar - {2318C2B1-4965-11d4-9B18-009027A5CD4F} - C:\Program Files\Google\Google Toolbar\GoogleToolbar_32.dll
O4 - HKLM\..\Run: [PDFPrint] C:\Program Files\pdf24\pdf24.exe
O4 - HKLM\..\Run: [IJNetworkScanUtility] C:\Program Files\Canon\Canon IJ Network Scan Utility\CNMNSUT.EXE
O4 - HKLM\..\Run: [Google Quick Search Box] "C:\Program Files\Google\Quick Search Box\GoogleQuickSearchBox.exe" /autorun
O4 - HKLM\..\Run: [eAudio] "C:\Acer\Empowering Technology\eAudio\eAudio.exe"
O4 - HKLM\..\Run: [CanonSolutionMenu] C:\Program Files\Canon\SolutionMenu\CNSLMAIN.exe /logon
O4 - HKLM\..\Run: [CanonMyPrinter] C:\Program Files\Canon\MyPrinter\BJMyPrt.exe /logon
O4 - HKLM\..\Run: [AVMWlanClient] C:\Program Files\avmwlanstick\wlangui.exe
O4 - HKLM\..\Run: [Acer Tour Reminder] C:\Acer\AcerTour\Reminder.exe
O4 - HKLM\..\Run: [Adobe Reader Speed Launcher] "C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"
O4 - HKLM\..\Run: [WrtMon.exe] C:\Windows\system32\spool\drivers\w32x86\3\WrtMon.exe
O4 - HKLM\..\Run: [Windows Defender] %ProgramFiles%\Windows Defender\MSASCui.exe -hide
O4 - HKLM\..\Run: [WarReg_PopUp] C:\Acer\WR_PopUp\WarReg_PopUp.exe
O4 - HKLM\..\Run: [Skytel] Skytel.exe

O4 - HKLM\..\Run: [RtHDVCpl] RtHDVCpl.exe
O4 - HKLM\..\Run: [RemoteControl9] "C:\Program Files\CyberLink\PowerDVD9\PDVD9Serv.exe"
O4 - HKLM\..\Run: [PDVD9LanguageShortcut] "C:\Program Files\CyberLink\PowerDVD9\Language\Language.exe"
O4 - HKLM\..\Run: [OpwareSE4] "C:\Program Files\ScanSoft\OmniPageSE4\OpwareSE4.exe"
O4 - HKLM\..\Run: [NvSvc] RUNDLL32.EXE C:\Windows\system32\nvsvc.dll,nvsvcStart
O4 - HKLM\..\Run: [NvMediaCenter] RUNDLL32.EXE C:\Windows\system32\NvMcTray.dll,NvTaskbarInit
O4 - HKLM\..\Run: [NvCplDaemon] RUNDLL32.EXE C:\Windows\system32\NvCpl.dll,NvStartup
O4 - HKLM\..\Run: [LManager] C:\PROGRA~1\LAUNCH~1\LManager.exe
O4 - HKLM\..\Run: [EvtMgr6] C:\Program Files\Logitech\SetPointP\SetPoint.exe /launchGaming
O4 - HKLM\..\Run: [Everything] "C:\Program Files\Everything\Everything.exe" -startup
O4 - HKLM\..\Run: [eDataSecurity Loader] C:\Acer\Empowering Technology\eDataSecurity\eDSloader.exe
O4 - HKLM\..\Run: [BDRegion] C:\Program Files\Cyberlink\Shared Files\brs.exe
O4 - HKLM\..\Run: [Apoint] C:\Program Files\Apoint2K\Apoint.exe
O4 - HKCU\..\Run: [swg] "C:\Program Files\Google\GoogleToolbarNotifier\GoogleToolbarNotifier.exe"
O4 - HKCU\..\Run: [Sidebar] C:\Program Files\Windows Sidebar\sidebar.exe /autoRun
O4 - HKCU\..\Run: [WMPNSCFG] C:\Program Files\Windows Media Player\WMPNSCFG.exe
O4 - HKCU\..\Run: [Skype] "C:\Program Files\Skype\\Phone\Skype.exe" /nosplash /minimized
O4 - HKCU\..\Run: [SearchEngineProtection] C:\Program Files\Gamesbar\SearchEngineProtection.exe
O4 - HKCU\..\Run: [ehTray.exe] C:\Windows\ehome\ehTray.exe
O4 - HKUS\S-1-5-18\..\Run: [Acer Tour Reminder] C:\Acer\AcerTour\Reminder.exe (User 'SYSTEM')
O4 - HKUS\.DEFAULT\..\Run: [Acer Tour Reminder] C:\Acer\AcerTour\Reminder.exe (User 'Default user')
O4 - .DEFAULT User Startup: DSL-Manager.lnk = C:\Program Files\T-Online\DSL-Manager\DslMgr.exe (User 'Default user')
O4 - Startup: OneNote 2007 Bildschirmausschnitt- und Startprogramm.lnk = C:\Program Files\Microsoft Office\Office12\ONENOTEM.EXE
O4 - Global Startup: Empowering Technology Launcher.lnk = ?
O4 - Global Startup: Snagit 10.lnk = C:\Program Files\TechSmith\Snagit 10\Snagit32.exe
O4 - Global Startup: SnagIt 9.lnk = C:\Program Files\TechSmith\SnagIt 9\SnagIt32.exe
O4 - Global Startup: WinZip Quick Pick.lnk = C:\Program Files\WinZip\WZQKPICK.EXE
O8 - Extra context menu item: &ieSpell Options - res://C:\Program Files\ieSpell\iespell.dll/SPELLOPTION.HTM
O8 - Extra context menu item: &Winamp Search - C:\ProgramData\Winamp Toolbar\ieToolbar\resources\en-US\local\search.html
O8 - Extra context menu item: Add to Google Photos Screensa&ver - res://C:\Windows\system32\GPhotos.scr/200
O8 - Extra context menu item: Check &Spelling - res://C:\Program Files\ieSpell\iespell.dll/SPELLCHECK.HTM
O8 - Extra context menu item: Lookup on Merriam Webster - file://C:\Program Files\ieSpell\Merriam Webster.HTM
O8 - Extra context menu item: Lookup on Wikipedia - file://C:\Program Files\ieSpell\wikipedia.HTM
O9 - Extra button: ieSpell - {0E17D5B7-9F5D-4fee-9DF6-CA6EE38B68A8} - C:\Program Files\ieSpell\iespell.dll
O9 - Extra 'Tools' menuitem: ieSpell - {0E17D5B7-9F5D-4fee-9DF6-CA6EE38B68A8} - C:\Program Files\ieSpell\iespell.dll
O9 - Extra button: (no name) - {1606D6F9-9D3B-4aea-A025-ED5B2FD488E7} - C:\Program Files\ieSpell\iespell.dll
O9 - Extra 'Tools' menuitem: ieSpell Options - {1606D6F9-9D3B-4aea-A025-ED5B2FD488E7} - C:\Program Files\ieSpell\iespell.dll
O9 - Extra button: (no name) - {1A93C934-025B-4c3a-B38E-9654A7003239} - C:\Program Files\GamesBar\2.0.1.67\oberontb.dll

O9 - Extra 'Tools' menuitem: GamesBar - {1A93C934-025B-4c3a-B38E-9654A7003239} - C:\Program Files\GamesBar\2.0.1.67\oberontb.dll
O9 - Extra button: An OneNote senden - {2670000A-7350-4f3c-8081-5663EE0C6C49} - C:\PROGRA~1\MICROS~2\Office12\ONBttnIE.dll
O9 - Extra 'Tools' menuitem: An OneNote s&enden - {2670000A-7350-4f3c-8081-5663EE0C6C49} - C:\PROGRA~1\MICROS~2\Office12\ONBttnIE.dll
O9 - Extra button: Research - {92780B25-18CC-41C8-B9BE-3C9C571A8263} - C:\PROGRA~1\MICROS~2\Office12\REFIEBAR.DLL
O11 - Options group: [ACCELERATED_GRAPHICS] Accelerated graphics
O20 - AppInit_DLLs: eNetHook.dll
O22 - SharedTaskScheduler: Component Categories cache daemon - {8C7461EF-2B13-11d2-BE35-3078302C2030} - C:\Windows\system32\browseui.dll
O23 - Service: Apple Mobile Device - Apple Inc. - C:\Program Files\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe
O23 - Service: Automatisches LiveUpdate - Scheduler - Unknown owner - C:\Program Files\Symantec\LiveUpdate\ALUSchedulerSvc.exe (file missing)
O23 - Service: AVM WLAN Connection Service - AVM Berlin - C:\Program Files\avmwlanstick\WlanNetService.exe
O23 - Service: Dienst "Bonjour" (Bonjour Service) - Apple Inc. - C:\Program Files\Bonjour\mDNSResponder.exe
O23 - Service: eDSService.exe (eDataSecurity Service) - HiTRSUT - C:\Acer\Empowering Technology\eDataSecurity\eDSService.exe
O23 - Service: eLock Service (eLockService) - Acer Inc. - C:\Acer\Empowering Technology\eLock\Service\eLockServ.exe
O23 - Service: eNet Service - Acer Inc. - C:\Acer\Empowering Technology\eNet\eNet Service.exe
O23 - Service: eRecovery Service (eRecoveryService) - Acer Inc. - C:\Acer\Empowering Technology\eRecovery\eRecoveryService.exe
O23 - Service: eSettings Service (eSettingsService) - Unknown owner - C:\Acer\Empowering Technology\eSettings\Service\capuserv.exe
O23 - Service: Google Update Service (gupdate1ca5330839357c3) (gupdate1ca5330839357c3) - Google Inc. - C:\Program Files\Google\Update\GoogleUpdate.exe
O23 - Service: Google Update-Dienst (gupdatem) (gupdatem) - Google Inc. - C:\Program Files\Google\Update\GoogleUpdate.exe
O23 - Service: Google Software Updater (gusvc) - Google - C:\Program Files\Google\Common\Google Updater\GoogleUpdaterService.exe
O23 - Service: PIXMA Extended Survey Program (IJPLMSVC) - Unknown owner - C:\Program Files\Canon\IJPLM\IJPLMSVC.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: LightScribeService Direct Disc Labeling Service (LightScribeService) - Hewlett-Packard Company - C:\Program Files\Common Files\LightScribe\LSSrvc.exe
O23 - Service: MobilityService - Unknown owner - C:\Acer\Mobility Center\MobilityService.exe
O23 - Service: Norton Internet Security (NIS) - Symantec Corporation - C:\Program Files\Norton Internet Security\Engine\19.2.0.10\ccSvcHst.exe
O23 - Service: Cyberlink RichVideo Service(CRVS) (RichVideo) - Unknown owner - C:\Program Files\CyberLink\Shared Files\RichVideo.exe
O23 - Service: ServiceLayer - Nokia - C:\Program Files\PC Connectivity Solution\ServiceLayer.exe
O23 - Service: DSL-Manager (TDslMgrService) - T-Systems Enterprise Services GmbH - C:\Program Files\T-Online\DSL-Manager\DslMgrSvc.exe
O23 - Service: @%SystemRoot%\System32\TUProgSt.exe,-1 (TuneUp.ProgramStatisticsSvc) - TuneUp Software - C:\Windows\System32\TUProgSt.exe
O23 - Service: TuneUp Utilities Service (TuneUp.UtilitiesSvc) - TuneUp Software - C:\Program Files\TuneUp Utilities 2012\TuneUpUtilitiesService32.exe
O23 - Service: ePower Service (WMIService) - acer - C:\Acer\Empowering Technology\ePower\ePowerSvc.exe
O23 - Service: XAudioService - Conexant Systems, Inc. - C:\Windows\system32\DRIVERS\xaudio.exe

--

End of file - 14767 bytes