Logfile of Trend Micro HijackThis v2.0.4
Scan saved at 21:08:47, on 29.10.2012
Platform: Windows XP SP3 (WinNT 5.01.2600)
MSIE: Internet Explorer v8.00 (8.00.6001.18702)
Boot mode: Normal

Running processes:
C:\WINDOWS\System32\smss.exe
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\services.exe
C:\WINDOWS\system32\lsass.exe
C:\PROGRA~1\ENIGMA~1\SPYHUN~1\SH4SER~1.EXE
C:\WINDOWS\system32\svchost.exe
C:\Programme\Gemeinsame Dateien\G Data\GDScan\GDScan.exe
C:\Programme\G Data\InternetSecurity\AVK\AVKWCtl.exe
C:\WINDOWS\System32\svchost.exe
C:\WINDOWS\system32\spoolsv.exe
C:\Programme\Gemeinsame Dateien\Acronis\Schedule2\schedul2.exe
C:\Programme\Adobe\Elements 10 Organizer\PhotoshopElementsFileAgent.exe
C:\WINDOWS\Explorer.EXE
C:\Programme\Adobe\Elements 11 Organizer\PhotoshopElementsFileAgent.exe
C:\Programme\Adobe\Photoshop Elements 7.0\PhotoshopElementsFileAgent.exe
C:\Programme\Gemeinsame Dateien\Acronis\CDP\afcdpsrv.exe
C:\Programme\Gemeinsame Dateien\G Data\AVKProxy\AVKProxy.exe
C:\Programme\G Data\InternetSecurity\AVK\AVKService.exe
C:\Dokumente und Einstellungen\All Users.WINDOWS\Anwendungsdaten\Browser Manager\2.3.811.154\{61d8b74e-8d89-46ff-afa6-33382c54ac73}\browsermngr.exe
C:\WINDOWS\system32\crypserv.exe
C:\Dokumente und Einstellungen\All Users.WINDOWS\Anwendungsdaten\Browser Manager\2.3.811.154\{61d8b74e-8d89-46ff-afa6-33382c54ac73}\browsermngr.exe
C:\Programme\Gemeinsame Dateien\DATA BECKER Shared\DBService.exe
C:\WINDOWS\eHome\ehRecvr.exe
C:\WINDOWS\eHome\ehSched.exe
C:\Programme\Gemeinsame Dateien\MAGIX Services\Database\bin\FABS.exe
C:\Programme\Canon\IJPLM\IJPLMSVC.EXE
C:\Programme\Java\jre7\bin\jqs.exe
C:\Programme\Malwarebytes' Anti-Malware\mbamscheduler.exe
C:\WINDOWS\system32\PSIService.exe
C:\WINDOWS\system32\svchost.exe
C:\Programme\TuneUp Utilities 2013\TuneUpUtilitiesService32.exe
C:\Programme\Web Assistant\ExtensionUpdaterService.exe
C:\Programme\Canon\CAL\CALMAIN.exe
C:\WINDOWS\system32\dllhost.exe
C:\Programme\TuneUp Utilities 2013\TuneUpUtilitiesApp32.exe
C:\Programme\G Data\InternetSecurity\AVKTray\AVKTray.exe
C:\WINDOWS\RTHDCPL.EXE
C:\Programme\Enigma Software Group\SpyHunter\SpyHunter4.exe
C:\Programme\Enigma Software Group\RegHunter\RegHunter.exe
C:\WINDOWS\system32\ctfmon.exe
C:\Programme\Spybot - Search & Destroy\TeaTimer.exe
C:\Dokumente und Einstellungen\Klaus-Dieter\Eigene Dateien\Downloads\HijackThis.exe

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar =
http://feed.helperbar.com/?publisher=OPENCANDY&dpid=OPENCANDYAPRIL&co=DE&userid=81&af
fid=110774&searchtype=ds&babsrc=lnkry&q={searchTerms}
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page =
http://feed.helperbar.com/?publisher=OPENCANDY&dpid=OPENCANDYAPRIL&co=DE&userid=81&af
fid=110774&searchtype=ds&babsrc=lnkry&q={searchTerms}
R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page = http://www.google.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
R1 - HKCU\Software\Microsoft\Internet Explorer\Search,Default_Search_URL =
http://feed.helperbar.com/?publisher=OPENCANDY&dpid=OPENCANDYAPRIL&co=DE&userid=81&af
fid=110774&searchtype=ds&babsrc=lnkry&q={searchTerms}
R1 - HKCU\Software\Microsoft\Internet Explorer\Search,SearchAssistant =
http://feed.helperbar.com/?publisher=OPENCANDY&dpid=OPENCANDYAPRIL&co=DE&userid=81&af
fid=110774&searchtype=ds&babsrc=lnkry&q={searchTerms}
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =
R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Local Page =
R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Local Page =
O1 - Hosts: ï»¿# Copyright (c) 1993-1999 Microsoft Corp.
O2 - BHO: AcroIEHelperStub - {18DF081C-E8AD-4283-A596-FA578C2EBDC3} -
C:\Programme\Gemeinsame Dateien\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll
O2 - BHO: CBAbzockschutz.InitToolbarBHO - {2e250b90-0e7a-42a3-9d65-e39f9f227fa4} - mscoree.dll
(file missing)
O2 - BHO: RealPlayer Download and Record Plugin for Internet Explorer - {3049C3E9-B461-4BC5-
8870-4C09146192CA} - C:\Dokumente und Einstellungen\All
Users.WINDOWS\Anwendungsdaten\Real\RealPlayer\BrowserRecordPlugin\IE\rpbrowserrecordplug
in.dll
O2 - BHO: Canon Easy-WebPrint EX BHO - {3785D0AD-BFFF-47F6-BF5B-A587C162FED9} -
C:\Programme\Canon\Easy-WebPrint EX\ewpexbho.dll
O2 - BHO: Spybot-S&D IE Protection - {53707962-6F74-2D53-2644-206D7942484F} -
C:\PROGRA~1\SPYBOT~1\SDHelper.dll
O2 - BHO: Java(tm) Plug-In SSV Helper - {761497BB-D6F0-462C-B6EB-D4DAF1D92D43} -
C:\Programme\Java\jre7\bin\ssv.dll
O2 - BHO: URLRedirectionBHO - {B4F3A835-0E21-4959-BA22-42B3008E02FF} -
C:\PROGRA~1\MICROS~2\Office14\URLREDIR.DLL
O2 - BHO: G Data BankGuard - {BA3295CF-17ED-4F49-9E95-D999A0ADBFDC} -
C:\Programme\Gemeinsame Dateien\G DATA\AVKProxy\BanksafeBHO.dll
O2 - BHO: Java(tm) Plug-In 2 SSV Helper - {DBC80044-A445-435b-BC74-9C25C1C588A9} -
C:\Programme\Java\jre7\bin\jp2ssv.dll
O3 - Toolbar: (no name) - {D0F4A166-B8D4-48b8-9D63-80849FE137CB} - (no file)
O4 - HKLM\..\Run: [G Data AntiVirus Tray Application] C:\Programme\G
Data\InternetSecurity\AVKTray\AVKTray.exe
O4 - HKLM\..\Run: [RTHDCPL] RTHDCPL.EXE
O4 - HKLM\..\Run: [NvCplDaemon] RUNDLL32.EXE C:\WINDOWS\system32\NvCpl.dll,NvStartup
O4 - HKLM\..\Run: [NvMediaCenter] RUNDLL32.EXE
C:\WINDOWS\system32\NvMcTray.dll,NvTaskbarInit
O4 - HKLM\..\Run: [TkBellExe] "C:\programme\real\realplayer\update\realsched.exe" -osboot

O4 - HKLM\..\Run: [BluetoothAuthenticationAgent] rundll32.exe bthprops.cpl,,BluetoothAuthenticationAgent
O4 - HKCU\..\Run: [ctfmon.exe] C:\WINDOWS\system32\ctfmon.exe
O4 - HKCU\..\Run: [SpybotSD TeaTimer] C:\Programme\Spybot - Search & Destroy\TeaTimer.exe
O4 - HKUS\S-1-5-19\..\Run: [CTFMON.EXE] C:\WINDOWS\system32\CTFMON.EXE (User 'LOKALER DIENST')
O4 - HKUS\S-1-5-20\..\Run: [CTFMON.EXE] C:\WINDOWS\system32\CTFMON.EXE (User 'NETZWERKDIENST')
O4 - HKUS\S-1-5-18\..\Run: [CTFMON.EXE] C:\WINDOWS\system32\CTFMON.EXE (User 'SYSTEM')
O4 - HKUS\.DEFAULT\..\Run: [CTFMON.EXE] C:\WINDOWS\system32\CTFMON.EXE (User 'Default user')
O4 - Startup: desktop.ini~U2JM58FN
O4 - Global Startup: desktop.ini~49KG52FT
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
O9 - Extra button: (no name) - {e2e2dd38-d088-4134-82b7-f2ba38496583} - C:\WINDOWS\Network Diagnostic\xpnetdiag.exe
O9 - Extra 'Tools' menuitem: @xpsp3res.dll,-20001 - {e2e2dd38-d088-4134-82b7-f2ba38496583} - C:\WINDOWS\Network Diagnostic\xpnetdiag.exe
O16 - DPF: {17492023-C23A-453E-A040-C7C580BBF700} (Windows Genuine Advantage Validation Tool) - http://go.microsoft.com/fwlink/?linkid=39204
O16 - DPF: {6E32070A-766D-4EE6-879C-DC1FA91D2FC3} (MUWebControl Class) - http://www.update.microsoft.com/microsoftupdate/v6/V5Controls/en/x86/client/muweb_site.cab?1329248140421
O17 - HKLM\System\CCS\Services\Tcpip\..\{B8D830FD-0A7D-4497-B34D-ABE56AE33046}: NameServer = 8.8.8.8,8.8.8.4,4.2.2.1,4.2.2.2,208.67.222.222,208.67.220.220,8.26.56.26,8.20.247.20,156.154.70.1,156.154.71.1
O18 - Protocol: viprotocol - {B658800C-F66E-4EF3-AB85-6C0C227862A9} - (no file)
O18 - Filter hijack: text/xml - {807573E5-5146-11D5-A672-00B0D022E945} - C:\Programme\Gemeinsame Dateien\Microsoft Shared\OFFICE14\MSOXMLMF.DLL
O20 - AppInit_DLLs: c:\dokume~1\alluse~1.win\anwend~1\browse~1\23811~1.154\{61d8b~1\browse~1.dll
O22 - SharedTaskScheduler: Browseui preloader - {438755C2-A8BA-11D1-B96B-00A0C90312E1} - C:\WINDOWS\system32\browseui.dll
O22 - SharedTaskScheduler: Component Categories cache daemon - {8C7461EF-2B13-11d2-BE35-3078302C2030} - C:\WINDOWS\system32\browseui.dll
O23 - Service: Acronis Scheduler2 Service (AcrSch2Svc) - Acronis - C:\Programme\Gemeinsame Dateien\Acronis\Schedule2\schedul2.exe
O23 - Service: Adobe Active File Monitor V10 (AdobeActiveFileMonitor10.0) - Adobe Systems Incorporated - C:\Programme\Adobe\Elements 10 Organizer\PhotoshopElementsFileAgent.exe
O23 - Service: Adobe Active File Monitor V11 (AdobeActiveFileMonitor11.0) - Adobe Systems Incorporated - C:\Programme\Adobe\Elements 11 Organizer\PhotoshopElementsFileAgent.exe
O23 - Service: Adobe Active File Monitor V7 (AdobeActiveFileMonitor7.0) - Adobe Systems Incorporated - C:\Programme\Adobe\Photoshop Elements 7.0\PhotoshopElementsFileAgent.exe
O23 - Service: Adobe Flash Player Update Service (AdobeFlashPlayerUpdateSvc) - Adobe Systems Incorporated - C:\WINDOWS\system32\Macromed\Flash\FlashPlayerUpdateService.exe
O23 - Service: Acronis Nonstop Backup-Dienst (afcdpsrv) - Acronis - C:\Programme\Gemeinsame Dateien\Acronis\CDP\afcdpsrv.exe
O23 - Service: G Data AntiVirus Proxy (AVKProxy) - G Data Software AG - C:\Programme\Gemeinsame Dateien\G Data\AVKProxy\AVKProxy.exe

O23 - Service: G Data Scheduler (AVKService) - G Data Software AG - C:\Programme\G Data\InternetSecurity\AVK\AVKService.exe
O23 - Service: G Data Dateisystem Wächter (AVKWCtl) - G Data Software AG - C:\Programme\G Data\InternetSecurity\AVK\AVKWCtl.exe
O23 - Service: Browser Manager - Unknown owner - C:\Dokumente und Einstellungen\All Users.WINDOWS\Anwendungsdaten\Browser Manager\2.3.811.154\{61d8b74e-8d89-46ff-afa6-33382c54ac73}\browsermngr.exe
O23 - Service: Canon Camera Access Library 8 (CCALib8) - Canon Inc. - C:\Programme\Canon\CAL\CALMAIN.exe
O23 - Service: Crypkey License - CrypKey (Canada) Ltd. - C:\WINDOWS\SYSTEM32\crypserv.exe
O23 - Service: DATA BECKER Update Service (DBService) - DATA BECKER GmbH & Co KG - C:\Programme\Gemeinsame Dateien\DATA BECKER Shared\DBService.exe
O23 - Service: FABS - Helping agent for MAGIX media database (Fabs) - MAGIX AG - C:\Programme\Gemeinsame Dateien\MAGIX Services\Database\bin\FABS.exe
O23 - Service: Firebird Server - MAGIX Instance (FirebirdServerMAGIXInstance) - MAGIX® - C:\Programme\Gemeinsame Dateien\MAGIX Services\Database\bin\fbserver.exe
O23 - Service: FLEXnet Licensing Service - Macrovision Europe Ltd. - C:\Programme\Gemeinsame Dateien\Macrovision Shared\FLEXnet Publisher\FNPLicensingService.exe
O23 - Service: G Data Scanner (GDScan) - G Data Software AG - C:\Programme\Gemeinsame Dateien\G Data\GDScan\GDScan.exe
O23 - Service: Google Update-Dienst (gupdate) (gupdate) - Google Inc. - C:\Programme\Google\Update\GoogleUpdate.exe
O23 - Service: Google Update-Dienst (gupdatem) (gupdatem) - Google Inc. - C:\Programme\Google\Update\GoogleUpdate.exe
O23 - Service: Canon Inkjet Printer/Scanner/Fax Extended Survey Program (IJPLMSVC) - Unknown owner - C:\Programme\Canon\IJPLM\IJPLMSVC.EXE
O23 - Service: Java Quick Starter (JavaQuickStarterService) - Oracle Corporation - C:\Programme\Java\jre7\bin\jqs.exe
O23 - Service: MBAMScheduler - Malwarebytes Corporation - C:\Programme\Malwarebytes' Anti-Malware\mbamscheduler.exe
O23 - Service: MBAMService - Malwarebytes Corporation - C:\Programme\Malwarebytes' Anti-Malware\mbamservice.exe
O23 - Service: NVIDIA Driver Helper Service (NVSvc) - NVIDIA Corporation - C:\WINDOWS\system32\nvsvc32.exe
O23 - Service: ProtexisLicensing - Unknown owner - C:\WINDOWS\system32\PSIService.exe
O23 - Service: SpyHunter 4 Service - Enigma Software Group USA, LLC. - C:\PROGRA~1\ENIGMA~1\SPYHUN~1\SH4SER~1.EXE
O23 - Service: TuneUp Utilities Service (TuneUp.UtilitiesSvc) - TuneUp Software - C:\Programme\TuneUp Utilities 2013\TuneUpUtilitiesService32.exe
O23 - Service: UPnPService - Magix AG - C:\Programme\Gemeinsame Dateien\MAGIX Shared\UPnPService\UPnPService.exe
O23 - Service: Web Assistant Updater - Unknown owner - C:\Programme\Web Assistant\ExtensionUpdaterService.exe

--
End of file - 12298 bytes