ï»¿Logfile of random's system information tool 1.10 (written by random/random)
Run by Riekie at 2014-09-27 16:20:28
Microsoft Windows 8.1
System drive C: has 381 GB (84%) free of 454 GB
Total RAM: 3912 MB (47% free)

Logfile of Trend Micro HijackThis v2.0.4
Scan saved at 16:20:36, on 27-9-2014
Platform: Unknown Windows (WinNT 6.02.1008)
MSIE: Internet Explorer v11.0 (11.00.9600.17278)
Boot mode: Normal

Running processes:
C:\Program Files (x86)\TeamViewer\Version8\TeamViewer.exe
C:\Program Files (x86)\Launch Manager\LManager.exe
C:\Program Files\Microsoft Office 15\Root\VFS\ProgramFilesCommonX86\Microsoft Shared\OFFICE15\CSISYNCCLIENT.EXE
C:\Program Files (x86)\Skype\Phone\Skype.exe
C:\Program Files (x86)\AVG\AVG2014\avgui.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files\Microsoft Office 15\Root\Office15\MsoSync.exe
C:\WINDOWS\SysWOW64\ctfmon.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files\Acer\Acer Instant Service\InstantUpdate\iuEmailOutlookAgent.exe
C:\Program Files\Acer\Acer Instant Service\InstantUpdate\iuBrowserIEAgent.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files\trend micro\Riekie.exe

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = http://acer13.msn.com
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://acer13.msn.com/
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = http://go.microsoft.com/fwlink/p/?LinkId=255141
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/p/?LinkId=255141
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
R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName =
F2 - REG:system.ini: UserInit=userinit.exe,
O2 - BHO: SkypeIEPluginBHO - {AE805869-2E5C-4ED4-8F7B-F1F7851A4497} - C:\Program Files (x86)\Skype\Toolbars\Internet Explorer\SkypeIEPlugin.dll
O4 - HKLM\..\Run: [Dolby Home Theater v4] "C:\Dolby PCEE4\pcee4.exe" -autostart
O4 - HKLM\..\Run: [APSDaemon] "C:\Program Files (x86)\Common Files\Apple\Apple Application Support\APSDaemon.exe"
O4 - HKLM\..\Run: [Adobe ARM] "C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe"
O4 - HKLM\..\Run: [AVG_UI] "C:\Program Files (x86)\AVG\AVG2014\avgui.exe" /TRAYONLY
O4 - HKCU\..\Run: [StartMenuX] C:\Program Files\Start Menu X\StartMenuX.exe
O4 - HKCU\..\Run: [GarminExpressTrayApp] "C:\Program Files (x86)\Garmin\Express Tray\ExpressTray.exe"
O4 - HKCU\..\Run: [Skype] "C:\Program Files (x86)\Skype\Phone\Skype.exe" /minimized /regrun
O4 - HKLM\..\Policies\Explorer\Run: [BtvStack] "C:\Program Files (x86)\Qualcomm Atheros\Bluetooth Suite\BtvStack.exe"
O4 - HKUS\S-1-5-18\..\Run: [GarminExpressTrayApp] "C:\Program Files (x86)\Garmin\Express Tray\ExpressTray.exe" (User 'SYSTEM')
O4 - HKUS\.DEFAULT\..\Run: [GarminExpressTrayApp] "C:\Program Files (x86)\Garmin\Express Tray\ExpressTray.exe" (User 'Default user')
O4 - Startup: Verzenden naar OneNote.lnk = C:\Program Files\Microsoft Office 15\root\office15\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: E&xport to Microsoft Excel - res://C:\Program Files\Microsoft Office

15\Root\Office15\EXCEL.EXE/3000
O8 - Extra context menu item: Se&nd to OneNote - res://C:\Program Files\Microsoft Office 15\Root\Office15\ONBttnIE.dll/105
O9 - Extra button: Send to OneNote - {2670000A-7350-4f3c-8081-5663EE0C6C49} - C:\Program Files\Microsoft Office 15\root\Office15\ONBttnIE.dll
O9 - Extra 'Tools' menuitem: Se&nd to OneNote - {2670000A-7350-4f3c-8081-5663EE0C6C49} - C:\Program Files\Microsoft Office 15\root\Office15\ONBttnIE.dll
O9 - Extra button: OneNote Lin&ked Notes - {789FE86F-6FC4-46A1-9849-EDE0DB0C95CA} - C:\Program Files\Microsoft Office 15\root\Office15\ONBttnIELinkedNotes.dll
O9 - Extra 'Tools' menuitem: OneNote Lin&ked Notes - {789FE86F-6FC4-46A1-9849-EDE0DB0C95CA} - C:\Program Files\Microsoft Office 15\root\Office15\ONBttnIELinkedNotes.dll
O9 - Extra button: Skype Click to Call settings - {898EA8C8-E7FF-479B-8935-AEC46303B9E5} - C:\Program Files (x86)\Skype\Toolbars\Internet Explorer\SkypeIEPlugin.dll
O11 - Options group: [ACCELERATED_GRAPHICS] Accelerated graphics
O18 - Protocol: osf - {D924BDC6-C83A-4BD5-90D0-095128A113D1} - C:\Program Files\Microsoft Office 15\root\Office15\MSOSB.DLL
O18 - Protocol: skypec2c - {91774881-D725-4E58-B298-07617B9B86A8} - C:\Program Files (x86)\Skype\Toolbars\Internet Explorer\SkypeIEPlugin.dll
O23 - Service: Adobe Acrobat Update Service (AdobeARMservice) - Adobe Systems Incorporated - C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe
O23 - Service: Adobe Flash Player Update Service (AdobeFlashPlayerUpdateSvc) - Adobe Systems Incorporated - C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe
O23 - Service: @%SystemRoot%\system32\Alg.exe,-112 (ALG) - Unknown owner - C:\WINDOWS\System32\alg.exe (file missing)
O23 - Service: AtherosSvc - Qualcomm Atheros Commnucations - C:\Program Files (x86)\Qualcomm Atheros\Bluetooth Suite\adminservice.exe
O23 - Service: AVGIDSAgent - AVG Technologies CZ, s.r.o. - C:\Program Files (x86)\AVG\AVG2014\avgidsagent.exe
O23 - Service: AVG WatchDog (avgwd) - AVG Technologies CZ, s.r.o. - C:\Program Files (x86)\AVG\AVG2014\avgwdsvc.exe
O23 - Service: CCDMonitorService - Acer Incorporated - C:\Program Files (x86)\Acer\Acer Cloud\CCDMonitorService.exe
O23 - Service: Intel(R) Content Protection HECI Service (cphs) - Intel Corporation - C:\WINDOWS\SysWow64\IntelCpHeciSvc.exe
O23 - Service: Device Fast-lane Service (DeviceFastLaneService) - Acer Incorporated - C:\Program Files\Acer\Acer Device Fast-lane\DeviceFastLaneSvc.exe
O23 - Service: Dritek WMI Service (DsiWMIService) - Dritek System Inc. - C:\Program Files (x86)\Launch Manager\dsiwmis.exe
O23 - Service: @%SystemRoot%\system32\efssvc.dll,-100 (EFS) - Unknown owner - C:\WINDOWS\System32\lsass.exe (file missing)
O23 - Service: ePower Service (ePowerSvc) - Acer Incorporated - C:\Program Files\Acer\Acer Power Management\ePowerSvc.exe
O23 - Service: @%systemroot%\system32\fxsresm.dll,-118 (Fax) - Unknown owner - C:\WINDOWS\system32\fxssvc.exe (file missing)
O23 - Service: FLEXnet Licensing Service - Acresso Software Inc. - C:\Program Files (x86)\Common Files\Macrovision Shared\FLEXnet Publisher\FNPLicensingService.exe
O23 - Service: Garmin Core Update Service - Garmin Ltd or its subsidiaries - C:\Program Files (x86)\Garmin\Core Update Service\Garmin.Cartography.MapUpdate.CoreService.exe
O23 - Service: Google Update-service (gupdate) (gupdate) - Google Inc. - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
O23 - Service: Google Update-service (gupdatem) (gupdatem) - Google Inc. - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
O23 - Service: Google Updater Service (gusvc) - Google - C:\Program Files (x86)\Google\Common\Google Updater\GoogleUpdaterService.exe
O23 - Service: IconMan_R - Realsil Microelectronics Inc. - C:\Program Files (x86)\Realtek\Realtek PCIE Card Reader\RIconMan.exe
O23 - Service: @%SystemRoot%\system32\ieetwcollectorres.dll,-1000 (IEEtwCollectorService) - Unknown owner - C:\WINDOWS\system32\IEEtwCollector.exe (file missing)
O23 - Service: Intel(R) Capability Licensing Service Interface - Intel(R) Corporation - C:\Program Files\Intel\iCLS Client\HeciServer.exe
O23 - Service: Intel(R) Dynamic Application Loader Host Interface Service (jhi_service) - Intel Corporation - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\DAL\jhi_service.exe
O23 - Service: @keyiso.dll,-100 (KeyIso) - Unknown owner - C:\WINDOWS\system32\lsass.exe (file missing)

O23 - Service: LiveUpdate (LiveUpdateSvc) - IObit - C:\Program Files (x86)\IObit\LiveUpdate\LiveUpdate.exe
O23 - Service: Intel(R) Management and Security Application Local Management Service (LMS) - Intel Corporation - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe
O23 - Service: McAfee SiteAdvisor Service - McAfee, Inc. - C:\Program Files\Common Files\McAfee\McSvcHost\McSvHost.exe
O23 - Service: @comres.dll,-2797 (MSDTC) - Unknown owner - C:\WINDOWS\System32\msdtc.exe (file missing)
O23 - Service: NTI IScheduleSvc - NTI Corporation - C:\Program Files (x86)\NTI\Acer Backup Manager\IScheduleSvc.exe
O23 - Service: Dritek RF Button Command Service (RfButtonDriverService) - Dritek System INC. - C:\Windows\RfBtnSvc64.exe
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: Skype Updater (SkypeUpdate) - Skype Technologies - C:\Program Files (x86)\Skype\Updater\Updater.exe
O23 - Service: @%systemroot%\system32\spoolsv.exe,-1 (Spooler) - Unknown owner - C:\WINDOWS\System32\spoolsv.exe (file missing)
O23 - Service: @%SystemRoot%\system32\sppsvc.exe,-101 (sppsvc) - Unknown owner - C:\WINDOWS\system32\sppsvc.exe (file missing)
O23 - Service: TeamViewer 8 (TeamViewer8) - TeamViewer GmbH - C:\Program Files (x86)\TeamViewer\Version8\TeamViewer_Service.exe
O23 - Service: AVG PC TuneUp Service (TuneUp.UtilitiesSvc) - AVG Technologies - C:\Program Files (x86)\AVG\AVG PC TuneUp\TuneUpUtilitiesService64.exe
O23 - Service: @%SystemRoot%\system32\ui0detect.exe,-101 (UI0Detect) - Unknown owner - C:\WINDOWS\system32\UI0Detect.exe (file missing)
O23 - Service: Intel(R) Management and Security Application User Notification Service (UNS) - Intel Corporation - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\UNS\UNS.exe
O23 - Service: @%SystemRoot%\system32\vaultsvc.dll,-1003 (VaultSvc) - Unknown owner - C:\WINDOWS\system32\lsass.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: @%systemroot%\system32\wbengine.exe,-104 (wbengine) - Unknown owner - C:\WINDOWS\system32\wbengine.exe (file missing)
O23 - Service: @%ProgramFiles%\Windows Defender\MpAsDesc.dll,-320 (WdNisSvc) - Unknown owner - C:\Program Files (x86)\Windows Defender\NisSrv.exe (file missing)
O23 - Service: @%ProgramFiles%\Windows Defender\MpAsDesc.dll,-310 (WinDefend) - Unknown owner - C:\Program Files (x86)\Windows Defender\MsMpEng.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 - 11395 bytes

======Listing Processes======

c:\PROGRA~2\AVG\AVG2014\avgrsa.exe /boot
C:\Program Files (x86)\AVG\AVG2014\avgcsrva.exe /pipeName=b988067d-5bb1-496c-9aae-876c5a03e604 /coreSdkOptions=4382 /logConfFile="C:\WINDOWS\system32\config\systemprofile\AppData\Local\Avg2014\temp\9ded496c-01ce-434f-8821-893d2c4c8738-1fc-oopp.tmp" /loggerName=AVG.RS.Core /binaryPath="C:\Program Files (x86)\AVG\AVG2014\" /tempPath="C:\WINDOWS\system32\config\systemprofile\AppData\Local\Avg2014\temp\" /logPath="C:\WINDOWS\system32\config\systemprofile\AppData\Local\Avg2014\log\"

wininit.exe

C:\WINDOWS\system32\lsass.exe
C:\WINDOWS\system32\svchost.exe -k DcomLaunch
C:\WINDOWS\system32\svchost.exe -k RPCSS
C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted
C:\WINDOWS\system32\svchost.exe -k netsvcs
C:\WINDOWS\system32\svchost.exe -k LocalService
C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted
C:\WINDOWS\system32\svchost.exe -k NetworkService
C:\WINDOWS\System32\spoolsv.exe
C:\WINDOWS\system32\svchost.exe -k LocalServiceNoNetwork
"C:\Program Files (x86)\Qualcomm Atheros\Bluetooth Suite\adminservice.exe"
"C:\Program Files (x86)\AVG\AVG2014\avgidsagent.exe"
"C:\Program Files (x86)\AVG\AVG2014\avgwdsvc.exe"
"C:\Program Files (x86)\Acer\Acer Cloud\CCDMonitorService.exe"
dashost.exe {dea29287-78a8-4aac-b94c51d4ae513fb6}
"C:\Program Files (x86)\Launch Manager\dsiwmis.exe"
C:\WINDOWS\system32\svchost.exe -k LocalServiceAndNoImpersonation
"C:\Program Files (x86)\Garmin\Core Update Service\Garmin.Cartography.MapUpdate.CoreService.exe"
"C:\Program Files (x86)\AVG\AVG2014\avgnsa.exe"
"C:\Program Files (x86)\AVG\AVG2014\avgemca.exe"
"C:\Program Files\Intel\iCLS Client\HeciServer.exe"
"C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\DAL\jhi_service.exe"
"C:\Program Files (x86)\NTI\Acer Backup Manager\IScheduleSvc.exe"
C:\Windows\RfBtnSvc64.exe
"C:\Program Files (x86)\TeamViewer\Version8\TeamViewer_Service.exe"
"C:\Program Files (x86)\AVG\AVG PC TuneUp\TuneUpUtilitiesService64.exe"
C:\WINDOWS\System32\svchost.exe -k LocalServicePeerNet
C:\WINDOWS\system32\DllHost.exe /Processid:{30D49246-D217-465F-B00B-AC9DDD652EB7}
"C:\Program Files (x86)\Realtek\Realtek PCIE Card Reader\RIconMan.exe"
"C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe"
"C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\UNS\UNS.exe"
"C:\Program Files\Acer\Acer Power Management\ePowerSvc.exe"
"C:\Windows\System32\WUDFHost.exe" -HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa}
-IoEventPortName:HostProcess-bf8374cd-f1e7-4c44-b4a9-b80ceaa3991b -SystemEventPortName:HostProcess-
e9333b1f-70c8-490f-ab61-53fd5899b6aa -IoCancelEventPortName:HostProcess-0debbc25-d159-41e1-a23a-
725fa1c164c3 -NonStateChangingEventPortName:HostProcess-0d1b4151-4015-46b7-ac55-f966f5f2ce0c
-ServiceSID:S-1-5-80-2652678385-582572993-1835434367-1344795993-749280709 -LifetimeId:f7103744-0659-
4ac4-a5da-9e5b7dae92fa -DeviceGroupId:WpdFsGroup
"C:\Program Files\Microsoft Office 15\ClientX64\OfficeClickToRun.exe" /service
C:\WINDOWS\system32\wbem\wmiprvse.exe
C:\WINDOWS\system32\svchost.exe -k imgsvc
"C:\Program Files (x86)\Skype\Toolbars\AutoUpdate\SkypeC2CAutoUpdateSvc.exe" /service
"C:\Program Files (x86)\Skype\Toolbars\PNRSvc\SkypeC2CPNRSvc.exe" /service
"C:\Windows\System32\WUDFHost.exe" -HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa}
-IoEventPortName:HostProcess-9eff2008-ee02-439d-873f-5191d5d57b69 -SystemEventPortName:HostProcess-
0d60861d-7ddf-4589-8606-90d0c38c996e -IoCancelEventPortName:HostProcess-1d42792c-c5da-4bb3-848c-
00ce956a3ad4 -NonStateChangingEventPortName:HostProcess-39b05952-aacb-4db6-b350-3d0cb8a90e55
-ServiceSID:S-1-5-80-2652678385-582572993-1835434367-1344795993-749280709 -LifetimeId:af60a974-9edf-4ea8-
ba41-834c9d989a2a -DeviceGroupId:WudfDefaultDevicePool
C:\WINDOWS\system32\SearchIndexer.exe /Embedding
"C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe"

C:\WINDOWS\System32\WinLogon.exe -SpecialSession
-hiberboot
"C:\Program Files (x86)\Launch Manager\LMutilps32.exe" --system-level --system-level-mutex="Local\{B904A927-
FE6B-48fd-8C83-6B807BED1F9C}" --enable-wmi-window --enable-setforeground-window --enable-kbhook-window
taskhostex.exe
"C:\Program Files (x86)\TeamViewer\Version8\TeamViewer.exe"
C:\WINDOWS\Explorer.EXE
"C:\Program Files (x86)\TeamViewer\Version8\tv_w32.exe" --action hooks --log C:\Program Files
(x86)\TeamViewer\Version8\TeamViewer8_Logfile.log
"C:\Program Files (x86)\TeamViewer\Version8\tv_x64.exe" --action hooks --log C:\Program Files
(x86)\TeamViewer\Version8\TeamViewer8_Logfile.log

"C:\Program Files (x86)\Launch Manager\LManager.exe"
C:\WINDOWS\system32\wbem\unsecapp.exe -Embedding
C:\Windows\System32\skydrive.exe -Embedding
"C:\Program Files (x86)\Launch Manager\MMDx64Fx.exe"
"C:\WINDOWS\system32\igfxext.exe" -Embedding
"C:\Program Files (x86)\Qualcomm Atheros\Bluetooth Suite\BtvStack.exe"
"C:\Program Files\Microsoft Office 15\Root\VFS\ProgramFilesCommonX86\Microsoft Shared\OFFICE15\CSISYNCCLIENT.EXE" "C:\Program Files\Microsoft Office 15\Root\VFS\ProgramFilesCommonX86\Microsoft Shared\OFFICE15\CSISYNCCLIENT.EXE" -Embedding
"C:\Windows\System32\igfxtray.exe"
"C:\Program Files (x86)\Qualcomm Atheros\Bluetooth Suite\ActivateDesktop.exe"
"C:\Windows\System32\hkcmd.exe"
"C:\Windows\System32\igfxpers.exe"
"C:\Program Files\Apoint2K\Apoint.exe"
"C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe" -s
"C:\Program Files\Apoint2K\ApMsgFwd.exe" -s{05FA8492-C047-4207-BE65-780D8591C113}
"C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe" /FORPCEE4
"C:\Program Files\Apoint2K\HidFind.exe"
"Apntex.exe"
\??\C:\WINDOWS\system32\conhost.exe 0x4
"C:\Program Files (x86)\Qualcomm Atheros\Bluetooth Suite\BtTray.exe"
"C:\Program Files\Start Menu X\StartMenuX.exe"
"C:\Program Files (x86)\Skype\Phone\Skype.exe" /minimized /regrun
"C:\Dolby PCEE4\pcee4.exe" -autostart
"C:\Program Files (x86)\AVG\AVG2014\avgui.exe" /TRAYONLY
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"
"C:\Program Files\Acer\Acer Power Management\ePowerTray.exe"
"C:\Program Files\Microsoft Office 15\Root\Office15\MsoSync.exe"
ctfmon.exe
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=gpu-process --channel="19796.0.1841595302\2025284246" --disable-d3d11 --supports-dual-gpus=false --gpu-driver-bug-workarounds=1,6,17 --gpu-vendor-id=0x8086 --gpu-device-id=0x0116 --gpu-driver-vendor="Intel Corporation" --gpu-driver-version=9.17.10.3347 --ignored=" --type=renderer " /prefetch:822062411
C:\WINDOWS\system32\wbem\unsecapp.exe -Embedding
"C:\Program Files\Acer\Acer Power Management\ePowerEvent.exe"
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --lang=nl --force-fieldtrials="AutoReloadExperiment/Enabled/AutoReloadVisibleOnlyExperiment/Enabled/BrowserBlacklist/Enabled/ChromeSuggestions/Most Likely with Kodachrome/EmbeddedSearch/Group2 pct:10b stable:pp2 prefetch_results:1 reuse_instant_search_base_page:1/ExtensionInstallVerification/Enforce/GoogleNow/Enable/OmniboxBundledExperimentV1/StandardR4/Prerender/PrerenderEnabled/PrerenderLocalPredictorSpec/LocalPredictor=Disabled/QUIC/Disabled/SafeBrowsingIncidentReportingService/Default/SettingsEnforcement/enforce_always_with_extensions_and_dse/ShowAppLauncherPromo/ShowPromoUntilDismissed/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Dynamic-Uniformity-Trial/Group6/UMA-New-Install-Uniformity-Trial/Control/UMA-Population-Restrict/normal/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_06/UMA-Uniformity-Trial-1-Percent/group_08/UMA-Uniformity-Trial-10-Percent/group_02/UMA-Uniformity-Trial-100-Percent/group_01/UMA-Uniformity-Trial-20-Percent/group_04/UMA-Uniformity-Trial-5-Percent/group_03/UMA-Uniformity-Trial-50-Percent/group_01/VoiceTrigger/Install/" --renderer-print-preview --enable-offline-auto-reload --enable-offline-auto-reload-visible-only --enable-pinch --device-scale-factor=1 --enable-threaded-compositing --enable-delegated-renderer --channel="19796.4.1409155898\609347752" /prefetch:673131151
"C:\Program Files\Acer\Acer Instant Service\InstantUpdate\iuEmailOutlookAgent.exe"
"C:\Program Files\Acer\Acer Instant Service\InstantUpdate\iuBrowserIEAgent.exe"
"C:\Windows\System32\SettingSyncHost.exe" -Embedding
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --lang=nl --force-fieldtrials="AutoReloadExperiment/Enabled/AutoReloadVisibleOnlyExperiment/Enabled/BrowserBlacklist/Enabled/ChromeSuggestions/Most Likely with Kodachrome/EmbeddedSearch/Group2 pct:10b stable:pp2 prefetch_results:1 reuse_instant_search_base_page:1/ExtensionInstallVerification/Enforce/GoogleNow/Enable/OmniboxBundledExperimentV1/StandardR4/Prerender/PrerenderEnabled/PrerenderLocalPredictorSpec/LocalPredictor=Disabled/QUIC/Disabled/SafeBrowsingIncidentReportingService/Default/SettingsEnforcement/enforce_always_with_extensions_and_dse/ShowAppLauncherPromo/ShowPromoUntilDismissed/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Dynamic-Uniformity-Trial/Group6/UMA-New-Install-Uniformity-Trial/Control/UMA-Population-Restrict/normal/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_06/UMA-Uniformity-Trial-1-Percent/group_08/UMA-Uniformity-Trial-10-Percent/group_02/UMA-Uniformity-Trial-100-Percent/group_01/UMA-Uniformity-Trial-20-Percent/group_04/UMA-Uniformity-Trial-5-Percent/group_03/UMA-Uniformity-Trial-50-

Percent/group_01/VoiceTrigger/Install/" --renderer-print-preview --enable-offline-auto-reload --enable-offline-auto-reload-visible-only --enable-pinch --device-scale-factor=1 --enable-threaded-compositing --enable-delegated-renderer --channel="19796.6.1098494346\1462276078" /prefetch:673131151
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --lang=nl --force-fieldtrials="AutoReloadExperiment/Enabled/AutoReloadVisibleOnlyExperiment/Enabled/BrowserBlacklist/Enabled/ChromeSuggestions/Most Likely with Kodachrome/EmbeddedSearch/Group2 pct:10b stable:pp2 prefetch_results:1 reuse_instant_search_base_page:1/ExtensionInstallVerification/Enforce/GoogleNow/Enable/OmniboxBundledExperimentV1/StandardR4/Prerender/PrerenderEnabled/PrerenderFromOmnibox/OmniboxPrerenderEnabled/PrerenderLocalPredictorSpec/LocalPredictor=Disabled/QUIC/Disabled/SafeBrowsingIncidentReportingService/Default/SettingsEnforcement/enforce_always_with_extensions_and_dse/ShowAppLauncherPromo/ShowPromoUntilDismissed/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Dynamic-Uniformity-Trial/Group6/UMA-New-Install-Uniformity-Trial/Control/UMA-Population-Restrict/normal/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_06/UMA-Uniformity-Trial-1-Percent/group_08/UMA-Uniformity-Trial-10-Percent/group_02/UMA-Uniformity-Trial-100-Percent/group_01/UMA-Uniformity-Trial-20-Percent/group_04/UMA-Uniformity-Trial-5-Percent/group_03/UMA-Uniformity-Trial-50-Percent/group_01/VoiceTrigger/Install/" --renderer-print-preview --enable-offline-auto-reload --enable-offline-auto-reload-visible-only --enable-pinch --device-scale-factor=1 --enable-threaded-compositing --enable-delegated-renderer --channel="19796.10.1963923890\976961714" /prefetch:673131151
C:\WINDOWS\splwow64.exe 12288
C:\WINDOWS\System32\svchost.exe -k WerSvcGroup
"C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.5.9600.20605_x64__8wekyb3d8bbwe\LiveComm.exe" -ServerName:Microsoft.WindowsLive.Platform.Server
C:\Windows\System32\RuntimeBroker.exe -Embedding
"C:\WINDOWS\system32\SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe23_ Global\UsGthrCtrlFltPipeMssGthrPipe23 1 -2147483646 "Software\Microsoft\Windows Search" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT; MS Search 4.0 Robot)"
"C:\ProgramData\Microsoft\Search\Data\Temp\usgthrsvc" "DownLevelDaemon"
"C:\WINDOWS\system32\SearchFilterHost.exe" 0 576 580 588 65536 584

"C:\Users\Riekie\Favorites\Downloads\RSITx64.exe"
C:\WINDOWS\system32\wbem\wmiprvse.exe

======Scheduled tasks folder======

C:\WINDOWS\tasks\Adobe Flash Player Updater.job - C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe#
C:\WINDOWS\tasks\GoogleUpdateTaskMachineCore.job - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe# /c#
C:\WINDOWS\tasks\GoogleUpdateTaskMachineUA.job - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe# /ua /installsource scheduler#

======Registry dump======

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{31D09BA0-12F5-4CCE-BE8A-2923E76605DA}]
Lync Browser Helper - C:\Program Files\Microsoft Office 15\root\VFS\ProgramFilesX64\Microsoft Office\Office15\OCHelper.dll [2014-09-23 218776]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{8D10F6C4-0E01-4BD4-8601-11AC1FDF8126}]
CIESpeechBHO Class - C:\Program Files (x86)\Qualcomm Atheros\Bluetooth Suite\IEPlugIn.dll [2013-01-28 66688]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{AE805869-2E5C-4ED4-8F7B-F1F7851A4497}]
Skype Click to Call for Internet Explorer - C:\Program Files (x86)\Skype\Toolbars\Internet Explorer x64\skypeieplugin.dll [2014-07-14 2117216]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{D0498E0A-45B7-42AE-A9AA-ABA463DBD3BF}]
Microsoft SkyDrive Pro Browser Helper - C:\Program Files\Microsoft Office 15\root\VFS\ProgramFilesX64\Microsoft Office\Office15\GROOVEEX.DLL [2014-09-23 2334416]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser

Helper Objects\{AE805869-2E5C-4ED4-8F7B-F1F7851A4497}]
Skype Click to Call for Internet Explorer - C:\Program Files (x86)\Skype\Toolbars\Internet Explorer\SkypeIEPlugin.dll [2014-07-14 1709152]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Toolbar]
{318A227B-5E9F-45bd-8999-7F8F10CA4CF5}
{CC1A175A-E45B-41ED-A30C-C9B1D7A0C02F}

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
"IgfxTray"=C:\WINDOWS\system32\igfxtray.exe [2014-01-29 171992]
"HotKeysCmds"=C:\WINDOWS\system32\hkcmd.exe [2014-01-29 399832]
"Persistence"=C:\WINDOWS\system32\igfxpers.exe [2014-01-29 442328]
"Apoint"=C:\Program Files\Apoint2K\Apoint.exe [2012-11-09 661400]
"RtHDVCpl"=C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe [2012-07-27 12937872]
"RtHDVBg_Dolby"=C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe [2012-07-10 1214608]
"BtPreLoad"=C:\Program Files (x86)\Qualcomm Atheros\Bluetooth Suite\BtPreLoad.exe [2013-01-28 64640]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run]
"BtvStack"=C:\Program Files (x86)\Qualcomm Atheros\Bluetooth Suite\BtvStack.exe [2013-01-28 132736]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"StartMenuX"=C:\Program Files\Start Menu X\StartMenuX.exe [2013-11-17 7674176]
"GarminExpressTrayApp"=C:\Program Files (x86)\Garmin\Express Tray\ExpressTray.exe [2014-07-23 688984]
"Skype"=C:\Program Files (x86)\Skype\Phone\Skype.exe [2014-08-27 22038120]

[HKEY_LOCAL_MACHINE\Software\wow6432node\Microsoft\Windows\CurrentVersion\Run]
"Dolby Home Theater v4"=C:\Dolby PCEE4\pcee4.exe [2012-07-26 508656]
"APSDaemon"=C:\Program Files (x86)\Common Files\Apple\Apple Application Support\APSDaemon.exe [2013-09-13 59720]
"Adobe ARM"=C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe [2014-08-21 959176]
"AVG_UI"=C:\Program Files (x86)\AVG\AVG2014\avgui.exe [2014-08-25 5188112]

[HKEY_LOCAL_MACHINE\Software\wow6432node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run]
"BtvStack"=C:\Program Files (x86)\Qualcomm Atheros\Bluetooth Suite\BtvStack.exe [2013-01-28 132736]

C:\Users\Riekie\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
Verzenden naar OneNote.lnk - C:\Program Files\Microsoft Office 15\root\office15\ONENOTEM.EXE

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\igfxcui]
C:\WINDOWS\system32\igfxdev.dll [2014-01-29 442880]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\41505288.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\41505288.sys]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"DisableCAD"=1

[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\sharedaccess\parameters\firewallpolicy\standardprofile\authorizedapplications\list]

[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\sharedaccess\parameters\firewallpolicy\domainprofile\authorizedapplications\list]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32]
"msacm.l3acm"=C:\Windows\System32\l3codeca.acm
"VIDC.YUY2"=msyuv.dll
"vidc.i420"=iyuv_32.dll
"msacm.msgsm610"=msgsm32.acm
"msacm.msg711"=msg711.acm
"VIDC.YVYU"=msyuv.dll
"VIDC.YVU9"=tsbyuv.dll
"wavemapper"=msacm32.drv

"midimapper"=midimap.dll
"VIDC.UYVY"=msyuv.dll
"VIDC.IYUV"=iyuv_32.dll
"vidc.mrle"=msrle32.dll
"msacm.imaadpcm"=imaadp32.acm
"msacm.msadpcm"=msadp32.acm
"vidc.msvc"=msvidc32.dll
"wave"=wdmaud.drv
"midi"=wdmaud.drv
"mixer"=wdmaud.drv
"aux"=wdmaud.drv
"wave1"=wdmaud.drv
"midi1"=wdmaud.drv
"mixer1"=wdmaud.drv
"aux1"=wdmaud.drv
"MSVideo8"=VfWWDM32.dll
"wave2"=wdmaud.drv
"mixer2"=wdmaud.drv
"midi2"=wdmaud.drv

======File associations======

.js - edit - C:\Windows\System32\Notepad.exe %1
.js - open - C:\Windows\System32\WScript.exe "%1" %*

======List of files/folders created in the last 1 month======

2014-09-27 16:14:51 ----D---- C:\rsit
2014-09-27 09:46:33 ----SHD---- C:\Config.Msi
2014-09-24 16:17:04 ----D---- C:\Users\Riekie\AppData\Roaming\Skype
2014-09-24 16:16:10 ----RD---- C:\Program Files (x86)\Skype
2014-09-24 16:13:59 ----D---- C:\ProgramData\Skype
2014-09-24 16:10:22 ----D---- C:\Program Files (x86)\SkypeWebPlugin
2014-09-18 15:16:59 ----D---- C:\b60a214a62ad504ba0910cc2a9973f
2014-09-18 14:34:33 ----D---- C:\ProgramData\Babylon
2014-09-18 14:34:32 ----D---- C:\Users\Riekie\AppData\Roaming\Babylon
2014-09-17 14:36:42 ----A---- C:\WINDOWS\system32\TURegOpt.exe
2014-09-17 14:36:41 ----A---- C:\WINDOWS\system32\authuitu.dll
2014-09-17 14:36:40 ----A---- C:\WINDOWS\SYSWOW64\authuitu.dll
2014-09-15 22:11:19 ----A---- C:\WINDOWS\SYSWOW64\FlashPlayerApp.exe
2014-09-15 15:00:46 ----A---- C:\WINDOWS\system32\WSDMon.dll
2014-09-15 15:00:45 ----A---- C:\WINDOWS\system32\tcpmon.dll
2014-09-15 15:00:39 ----A---- C:\WINDOWS\SYSWOW64\explorer.exe
2014-09-15 15:00:39 ----A---- C:\WINDOWS\system32\uDWM.dll
2014-09-15 15:00:37 ----A---- C:\WINDOWS\explorer.exe
2014-09-15 15:00:33 ----A---- C:\WINDOWS\system32\twinui.dll
2014-09-15 14:59:33 ----A---- C:\WINDOWS\SYSWOW64\twinui.dll
2014-09-15 14:57:30 ----A---- C:\WINDOWS\SYSWOW64\UXInit.dll
2014-09-15 14:57:30 ----A---- C:\WINDOWS\SYSWOW64\actxprxy.dll
2014-09-15 14:57:30 ----A---- C:\WINDOWS\system32\actxprxy.dll
2014-09-15 14:57:29 ----A---- C:\WINDOWS\system32\UXInit.dll
2014-09-15 14:55:41 ----A---- C:\WINDOWS\system32\Windows.UI.Xaml.dll
2014-09-15 14:55:37 ----A---- C:\WINDOWS\SYSWOW64\authui.dll
2014-09-15 14:55:36 ----A---- C:\WINDOWS\system32\authui.dll
2014-09-15 14:55:31 ----A---- C:\WINDOWS\system32\shell32.dll
2014-09-15 14:55:29 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.Xaml.dll
2014-09-15 14:55:26 ----A---- C:\WINDOWS\SYSWOW64\shell32.dll
2014-09-15 14:55:22 ----A---- C:\WINDOWS\system32\mstscax.dll
2014-09-15 14:55:19 ----A---- C:\WINDOWS\system32\Windows.UI.Search.dll
2014-09-15 14:55:18 ----A---- C:\WINDOWS\system32\ntoskrnl.exe
2014-09-15 14:55:17 ----A---- C:\WINDOWS\SYSWOW64\mstscax.dll
2014-09-15 14:55:16 ----A---- C:\WINDOWS\system32\d3d10warp.dll
2014-09-15 14:55:15 ----A---- C:\WINDOWS\system32\SettingsHandlers.dll

2014-09-15 14:55:03 ----A---- C:\WINDOWS\system32\mfcore.dll
2014-09-15 14:55:02 ----A---- C:\WINDOWS\system32\drivers\tcpip.sys
2014-09-15 14:55:00 ----A---- C:\WINDOWS\SYSWOW64\mfcore.dll
2014-09-15 14:54:59 ----A---- C:\WINDOWS\SYSWOW64\d3d10warp.dll
2014-09-15 14:54:58 ----A---- C:\WINDOWS\system32\gpsvc.dll
2014-09-15 14:54:57 ----A---- C:\WINDOWS\system32\wlansvc.dll
2014-09-15 14:54:56 ----A---- C:\WINDOWS\system32\workfolderssvc.dll
2014-09-15 14:54:52 ----A---- C:\WINDOWS\system32\Windows.Media.dll
2014-09-15 14:54:49 ----A---- C:\WINDOWS\system32\iphlpsvc.dll
2014-09-15 14:54:46 ----A---- C:\WINDOWS\system32\mfmp4srcsnk.dll
2014-09-15 14:54:46 ----A---- C:\WINDOWS\system32\localspl.dll
2014-09-15 14:54:45 ----A---- C:\WINDOWS\SYSWOW64\Windows.Media.dll
2014-09-15 14:54:45 ----A---- C:\WINDOWS\SYSWOW64\mfmp4srcsnk.dll
2014-09-15 14:54:44 ----A---- C:\WINDOWS\system32\drivers\srv.sys
2014-09-15 14:54:43 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.Search.dll
2014-09-15 14:54:43 ----A---- C:\WINDOWS\system32\WMVDECOD.DLL
2014-09-15 14:54:42 ----A---- C:\WINDOWS\SYSWOW64\mfplat.dll
2014-09-15 14:54:42 ----A---- C:\WINDOWS\system32\mfplat.dll
2014-09-15 14:54:41 ----A---- C:\WINDOWS\system32\SRH.dll
2014-09-15 14:54:41 ----A---- C:\WINDOWS\system32\printui.dll
2014-09-15 14:54:41 ----A---- C:\WINDOWS\system32\drivers\ntfs.sys
2014-09-15 14:54:40 ----A---- C:\WINDOWS\system32\wuaueng.dll
2014-09-15 14:54:39 ----A---- C:\WINDOWS\SYSWOW64\WMVDECOD.DLL
2014-09-15 14:54:38 ----A---- C:\WINDOWS\system32\drivers\srv2.sys
2014-09-15 14:54:37 ----A---- C:\WINDOWS\system32\mispace.dll
2014-09-15 14:54:36 ----A---- C:\WINDOWS\system32\drivers\netio.sys
2014-09-15 14:54:35 ----A---- C:\WINDOWS\system32\XpsPrint.dll
2014-09-15 14:54:33 ----AC---- C:\WINDOWS\system32\drivers\bthport.sys
2014-09-15 14:54:33 ----A---- C:\WINDOWS\system32\WorkfoldersControl.dll
2014-09-15 14:54:33 ----A---- C:\WINDOWS\system32\netcfgx.dll
2014-09-15 14:54:32 ----A---- C:\WINDOWS\SYSWOW64\mispace.dll
2014-09-15 14:54:32 ----A---- C:\WINDOWS\system32\AppxPackaging.dll
2014-09-15 14:54:31 ----A---- C:\WINDOWS\SYSWOW64\printui.dll
2014-09-15 14:54:31 ----A---- C:\WINDOWS\SYSWOW64\netcfgx.dll
2014-09-15 14:54:30 ----A---- C:\WINDOWS\system32\aclui.dll
2014-09-15 14:54:29 ----A---- C:\WINDOWS\SYSWOW64\SRH.dll
2014-09-15 14:54:28 ----AC---- C:\WINDOWS\system32\drivers\spaceport.sys
2014-09-15 14:54:27 ----A---- C:\WINDOWS\system32\wlanmsm.dll
2014-09-15 14:54:27 ----A---- C:\WINDOWS\system32\srvsvc.dll
2014-09-15 14:54:25 ----A---- C:\WINDOWS\system32\spoolsv.exe
2014-09-15 14:54:25 ----A---- C:\WINDOWS\system32\mfreadwrite.dll
2014-09-15 14:54:24 ----A---- C:\WINDOWS\SYSWOW64\aclui.dll
2014-09-15 14:54:23 ----AC---- C:\WINDOWS\system32\drivers\usbccgp.sys
2014-09-15 14:54:23 ----A---- C:\WINDOWS\SYSWOW64\mfreadwrite.dll
2014-09-15 14:54:23 ----A---- C:\WINDOWS\SYSWOW64\AppxPackaging.dll
2014-09-15 14:54:22 ----A---- C:\WINDOWS\SYSWOW64\wlanmsm.dll
2014-09-15 14:54:22 ----A---- C:\WINDOWS\system32\SHCore.dll
2014-09-15 14:54:21 ----AC---- C:\WINDOWS\system32\drivers\volsnap.sys
2014-09-15 14:54:20 ----A---- C:\WINDOWS\SYSWOW64\Windows.Devices.Bluetooth.dll
2014-09-15 14:54:20 ----A---- C:\WINDOWS\system32\puiobj.dll
2014-09-15 14:54:18 ----A---- C:\WINDOWS\SYSWOW64\mftranscode.dll
2014-09-15 14:54:18 ----A---- C:\WINDOWS\system32\storagewmi.dll
2014-09-15 14:54:17 ----A---- C:\WINDOWS\SYSWOW64\SHCore.dll
2014-09-15 14:54:17 ----A---- C:\WINDOWS\system32\wuapi.dll
2014-09-15 14:54:17 ----A---- C:\WINDOWS\system32\usbmon.dll
2014-09-15 14:54:17 ----A---- C:\WINDOWS\system32\mftranscode.dll
2014-09-15 14:54:17 ----A---- C:\WINDOWS\system32\comdlg32.dll
2014-09-15 14:54:17 ----A---- C:\WINDOWS\system32\clusapi.dll
2014-09-15 14:54:16 ----AC---- C:\WINDOWS\system32\drivers\USBHUB3.SYS
2014-09-15 14:54:16 ----A---- C:\WINDOWS\system32\winload.exe
2014-09-15 14:54:16 ----A---- C:\WINDOWS\system32\WebClnt.dll
2014-09-15 14:54:14 ----A---- C:\WINDOWS\system32\wisp.dll
2014-09-15 14:54:14 ----A---- C:\WINDOWS\system32\defragsvc.dll

2014-09-15 14:54:12 ----A---- C:\WINDOWS\system32\lsasrv.dll
2014-09-15 14:54:11 ----A---- C:\WINDOWS\SYSWOW64\comdlg32.dll
2014-09-15 14:54:11 ----A---- C:\WINDOWS\system32\winresume.exe
2014-09-15 14:54:10 ----A---- C:\WINDOWS\system32\wsecedit.dll
2014-09-15 14:54:09 ----A---- C:\WINDOWS\system32\drivers\srvnet.sys
2014-09-15 14:54:08 ----A---- C:\WINDOWS\SYSWOW64\WebClnt.dll
2014-09-15 14:54:08 ----A---- C:\WINDOWS\system32\profsvc.dll
2014-09-15 14:54:08 ----A---- C:\WINDOWS\system32\drivers\nwifi.sys
2014-09-15 14:54:07 ----A---- C:\WINDOWS\SYSWOW64\clusapi.dll
2014-09-15 14:54:07 ----A---- C:\WINDOWS\system32\user32.dll
2014-09-15 14:54:06 ----A---- C:\WINDOWS\system32\wpdbusenum.dll
2014-09-15 14:54:06 ----A---- C:\WINDOWS\system32\winmmbase.dll
2014-09-15 14:54:06 ----A---- C:\WINDOWS\system32\WiFiDisplay.dll
2014-09-15 14:54:05 ----A---- C:\WINDOWS\SYSWOW64\puiobj.dll
2014-09-15 14:54:05 ----A---- C:\WINDOWS\system32\win32spl.dll
2014-09-15 14:54:05 ----A---- C:\WINDOWS\system32\rdpcorets.dll
2014-09-15 14:54:05 ----A---- C:\WINDOWS\system32\conhost.exe
2014-09-15 14:54:04 ----A---- C:\WINDOWS\SYSWOW64\wlanapi.dll
2014-09-15 14:54:04 ----A---- C:\WINDOWS\SYSWOW64\Display.dll
2014-09-15 14:54:04 ----A---- C:\WINDOWS\system32\VAN.dll
2014-09-15 14:54:04 ----A---- C:\WINDOWS\system32\SettingSync.dll
2014-09-15 14:54:04 ----A---- C:\WINDOWS\system32\rdvidcrl.dll
2014-09-15 14:54:03 ----A---- C:\WINDOWS\SYSWOW64\storagewmi.dll
2014-09-15 14:54:03 ----A---- C:\WINDOWS\system32\WUSettingsProvider.dll
2014-09-15 14:54:03 ----A---- C:\WINDOWS\system32\WorkFoldersGPExt.dll
2014-09-15 14:54:03 ----A---- C:\WINDOWS\system32\Display.dll
2014-09-15 14:54:03 ----A---- C:\WINDOWS\system32\AppxSip.dll
2014-09-15 14:54:02 ----A---- C:\WINDOWS\SYSWOW64\winmmbase.dll
2014-09-15 14:54:02 ----A---- C:\WINDOWS\system32\SndVol.exe
2014-09-15 14:54:02 ----A---- C:\WINDOWS\system32\osk.exe
2014-09-15 14:54:01 ----A---- C:\WINDOWS\SYSWOW64\wuapi.dll
2014-09-15 14:54:01 ----A---- C:\WINDOWS\SYSWOW64\wisp.dll
2014-09-15 14:54:01 ----A---- C:\WINDOWS\system32\drivers\IPMIDrv.sys
2014-09-15 14:54:00 ----A---- C:\WINDOWS\system32\DafPrintProvider.dll
2014-09-15 14:54:00 ----A---- C:\WINDOWS\system32\bcryptprimitives.dll
2014-09-15 14:53:59 ----A---- C:\WINDOWS\system32\mfps.dll
2014-09-15 14:53:59 ----A---- C:\WINDOWS\system32\drivers\ndis.sys
2014-09-15 14:53:58 ----AC---- C:\WINDOWS\system32\drivers\hdaudbus.sys
2014-09-15 14:53:58 ----A---- C:\WINDOWS\SYSWOW64\bcryptprimitives.dll
2014-09-15 14:53:58 ----A---- C:\WINDOWS\system32\winmm.dll
2014-09-15 14:53:58 ----A---- C:\WINDOWS\system32\Windows.Networking.dll
2014-09-15 14:53:58 ----A---- C:\WINDOWS\system32\httpprxm.dll
2014-09-15 14:53:58 ----A---- C:\WINDOWS\system32\drivers\NdisImPlatform.sys
2014-09-15 14:53:58 ----A---- C:\WINDOWS\system32\drivers\mrxsmb20.sys
2014-09-15 14:53:57 ----A---- C:\WINDOWS\SYSWOW64\AppxSip.dll
2014-09-15 14:53:57 ----A---- C:\WINDOWS\system32\twinapi.dll
2014-09-15 14:53:57 ----A---- C:\WINDOWS\system32\dwmapi.dll
2014-09-15 14:53:56 ----A---- C:\WINDOWS\SYSWOW64\wsecedit.dll
2014-09-15 14:53:56 ----A---- C:\WINDOWS\system32\wucltux.dll
2014-09-15 14:53:56 ----A---- C:\WINDOWS\system32\WSShared.dll
2014-09-15 14:53:56 ----A---- C:\WINDOWS\system32\prnntfy.dll
2014-09-15 14:53:56 ----A---- C:\WINDOWS\system32\GdiPlus.dll
2014-09-15 14:53:56 ----A---- C:\WINDOWS\system32\drivers\bridge.sys
2014-09-15 14:53:55 ----A---- C:\WINDOWS\SYSWOW64\prnntfy.dll
2014-09-15 14:53:55 ----A---- C:\WINDOWS\system32\WorkFoldersShell.dll
2014-09-15 14:53:55 ----A---- C:\WINDOWS\system32\gpedit.dll
2014-09-15 14:53:54 ----A---- C:\WINDOWS\SYSWOW64\XpsPrint.dll
2014-09-15 14:53:54 ----A---- C:\WINDOWS\SYSWOW64\winmm.dll
2014-09-15 14:53:54 ----A---- C:\WINDOWS\system32\puiapi.dll
2014-09-15 14:53:53 ----A---- C:\WINDOWS\SYSWOW64\puiapi.dll
2014-09-15 14:53:53 ----A---- C:\WINDOWS\system32\iasnap.dll
2014-09-15 14:53:52 ----A---- C:\WINDOWS\SYSWOW64\VAN.dll
2014-09-15 14:53:52 ----A---- C:\WINDOWS\SYSWOW64\SndVol.exe

2014-09-15 14:53:52 ----A---- C:\WINDOWS\SYSWOW64\dwmapi.dll
2014-09-15 14:53:52 ----A---- C:\WINDOWS\system32\wups.dll
2014-09-15 14:53:52 ----A---- C:\WINDOWS\system32\adhsvc.dll
2014-09-15 14:53:51 ----AC---- C:\WINDOWS\system32\drivers\pci.sys
2014-09-15 14:53:51 ----A---- C:\WINDOWS\SYSWOW64\WSShared.dll
2014-09-15 14:53:51 ----A---- C:\WINDOWS\system32\drivers\ks.sys
2014-09-15 14:53:50 ----A---- C:\WINDOWS\system32\SystemSettingsAdminFlows.exe
2014-09-15 14:53:50 ----A---- C:\WINDOWS\system32\stobject.dll
2014-09-15 14:53:49 ----A---- C:\WINDOWS\SYSWOW64\rdvidcrl.dll
2014-09-15 14:53:49 ----A---- C:\WINDOWS\system32\wcmcsp.dll
2014-09-15 14:53:49 ----A---- C:\WINDOWS\system32\dab.dll
2014-09-15 14:53:49 ----A---- C:\WINDOWS\system32\AppxSysprep.dll
2014-09-15 14:53:48 ----A---- C:\WINDOWS\SYSWOW64\iasnap.dll
2014-09-15 14:53:48 ----A---- C:\WINDOWS\system32\wwanconn.dll
2014-09-15 14:53:48 ----A---- C:\WINDOWS\system32\wuauclt.exe
2014-09-15 14:53:47 ----A---- C:\WINDOWS\SYSWOW64\rsaenh.dll
2014-09-15 14:53:47 ----A---- C:\WINDOWS\SYSWOW64\gpedit.dll
2014-09-15 14:53:47 ----A---- C:\WINDOWS\system32\ActionCenter.dll
2014-09-15 14:53:46 ----A---- C:\WINDOWS\system32\wlanapi.dll
2014-09-15 14:53:46 ----A---- C:\WINDOWS\system32\rsaenh.dll
2014-09-15 14:53:45 ----A---- C:\WINDOWS\SYSWOW64\osk.exe
2014-09-15 14:53:45 ----A---- C:\WINDOWS\system32\wups2.dll
2014-09-15 14:53:45 ----A---- C:\WINDOWS\system32\schannel.dll
2014-09-15 14:53:44 ----A---- C:\WINDOWS\SYSWOW64\Windows.Networking.dll
2014-09-15 14:53:44 ----A---- C:\WINDOWS\SYSWOW64\SettingSync.dll
2014-09-15 14:53:44 ----A---- C:\WINDOWS\system32\wshbth.dll
2014-09-15 14:53:43 ----A---- C:\WINDOWS\SYSWOW64\DafPrintProvider.dll
2014-09-15 14:53:43 ----A---- C:\WINDOWS\system32\PrintDialogs.dll
2014-09-15 14:53:42 ----A---- C:\WINDOWS\system32\wlansvcpal.dll
2014-09-15 14:53:42 ----A---- C:\WINDOWS\system32\Windows.Devices.Bluetooth.dll
2014-09-15 14:53:42 ----A---- C:\WINDOWS\system32\SearchFolder.dll
2014-09-15 14:53:42 ----A---- C:\WINDOWS\system32\browser.dll
2014-09-15 14:53:41 ----A---- C:\WINDOWS\SYSWOW64\wshbth.dll
2014-09-15 14:53:40 ----A---- C:\WINDOWS\SYSWOW64\stobject.dll
2014-09-15 14:53:39 ----A---- C:\WINDOWS\SYSWOW64\ActionCenter.dll
2014-09-15 14:53:39 ----A---- C:\WINDOWS\system32\Defrag.exe
2014-09-15 14:53:38 ----A---- C:\WINDOWS\SYSWOW64\wups.dll
2014-09-15 14:53:38 ----A---- C:\WINDOWS\SYSWOW64\KBDRUM.DLL
2014-09-15 14:53:38 ----A---- C:\WINDOWS\system32\KBDRUM.DLL
2014-09-15 14:53:37 ----A---- C:\WINDOWS\SYSWOW64\schannel.dll
2014-09-15 14:53:37 ----A---- C:\WINDOWS\SYSWOW64\GdiPlus.dll
2014-09-15 14:53:36 ----A---- C:\WINDOWS\SYSWOW64\user32.dll
2014-09-15 14:53:36 ----A---- C:\WINDOWS\system32\KBDYAK.DLL
2014-09-15 14:53:36 ----A---- C:\WINDOWS\system32\KBDRU1.DLL
2014-09-15 14:53:36 ----A---- C:\WINDOWS\system32\KBDRU.DLL
2014-09-15 14:53:36 ----A---- C:\WINDOWS\system32\KBDBASH.DLL
2014-09-15 14:53:35 ----A---- C:\WINDOWS\SYSWOW64\KBDYAK.DLL
2014-09-15 14:53:35 ----A---- C:\WINDOWS\SYSWOW64\KBDRU1.DLL
2014-09-15 14:53:35 ----A---- C:\WINDOWS\SYSWOW64\KBDRU.DLL
2014-09-15 14:53:35 ----A---- C:\WINDOWS\SYSWOW64\KBDBASH.DLL
2014-09-15 14:53:35 ----A---- C:\WINDOWS\system32\BluetoothApis.dll
2014-09-15 14:53:30 ----AC---- C:\WINDOWS\system32\drivers\bthpan.sys
2014-09-15 14:53:30 ----A---- C:\WINDOWS\system32\certcli.dll
2014-09-15 14:53:29 ----A---- C:\WINDOWS\SYSWOW64\PrintDialogs.dll
2014-09-15 14:53:29 ----A---- C:\WINDOWS\SYSWOW64\KBDTAT.DLL
2014-09-15 14:53:29 ----A---- C:\WINDOWS\SYSWOW64\certcli.dll
2014-09-15 14:53:29 ----A---- C:\WINDOWS\system32\wwanmm.dll
2014-09-15 14:53:29 ----A---- C:\WINDOWS\system32\SndVolSSO.dll
2014-09-15 14:53:29 ----A---- C:\WINDOWS\system32\KBDTAT.DLL
2014-09-15 14:53:29 ----A---- C:\WINDOWS\system32\compstui.dll
2014-09-15 14:53:28 ----A---- C:\WINDOWS\SYSWOW64\BluetoothApis.dll
2014-09-15 14:53:28 ----A---- C:\WINDOWS\system32\rdpudd.dll
2014-09-15 14:53:27 ----A---- C:\WINDOWS\system32\wlansec.dll

2014-09-15 14:53:26 ----A---- C:\WINDOWS\SYSWOW64\wudriver.dll
2014-09-15 14:53:26 ----A---- C:\WINDOWS\SYSWOW64\Windows.ApplicationModel.Store.TestingFramework.dll
2014-09-15 14:53:26 ----A---- C:\WINDOWS\system32\wudriver.dll
2014-09-15 14:53:26 ----A---- C:\WINDOWS\system32\Windows.ApplicationModel.Store.TestingFramework.dll
2014-09-15 14:53:26 ----A---- C:\WINDOWS\system32\SystemSettingsAdminFlowUI.dll
2014-09-15 14:53:25 ----A---- C:\WINDOWS\SYSWOW64\KBDTT102.DLL
2014-09-15 14:53:25 ----A---- C:\WINDOWS\system32\KBDTT102.DLL
2014-09-15 14:43:27 ----A---- C:\WINDOWS\system32\drivers\msgpioclx.sys
2014-09-15 13:46:33 ----A---- C:\WINDOWS\SYSWOW64\msrating.dll
2014-09-15 13:46:31 ----A---- C:\WINDOWS\SYSWOW64\jsproxy.dll
2014-09-15 13:46:11 ----A---- C:\WINDOWS\system32\ieetwproxystub.dll
2014-09-15 13:46:11 ----A---- C:\WINDOWS\system32\ieetwcollectorres.dll
2014-09-15 13:46:11 ----A---- C:\WINDOWS\system32\ieetwcollector.exe
2014-09-15 13:46:10 ----A---- C:\WINDOWS\SYSWOW64\ieetwproxystub.dll
2014-09-15 13:46:09 ----A---- C:\WINDOWS\system32\ieUnatt.exe
2014-09-15 13:46:08 ----A---- C:\WINDOWS\SYSWOW64\ieUnatt.exe
2014-09-15 13:46:07 ----A---- C:\WINDOWS\SYSWOW64\iesetup.dll
2014-09-15 13:46:07 ----A---- C:\WINDOWS\SYSWOW64\iernonce.dll
2014-09-15 13:46:06 ----A---- C:\WINDOWS\system32\iernonce.dll
2014-09-15 13:46:05 ----A---- C:\WINDOWS\system32\iesetup.dll
2014-09-15 13:45:59 ----A---- C:\WINDOWS\system32\msrating.dll
2014-09-15 13:45:57 ----A---- C:\WINDOWS\system32\jsproxy.dll
2014-09-15 13:45:16 ----A---- C:\WINDOWS\SYSWOW64\MshtmlDac.dll
2014-09-15 13:45:16 ----A---- C:\WINDOWS\system32\MshtmlDac.dll
2014-09-15 13:45:12 ----A---- C:\WINDOWS\SYSWOW64\mshtmled.dll
2014-09-15 13:45:12 ----A---- C:\WINDOWS\system32\mshtmled.dll
2014-09-15 13:45:10 ----A---- C:\WINDOWS\system32\jscript9diag.dll
2014-09-15 13:45:10 ----A---- C:\WINDOWS\system32\JavaScriptCollectionAgent.dll
2014-09-15 13:45:09 ----A---- C:\WINDOWS\SYSWOW64\vbscript.dll
2014-09-15 13:45:09 ----A---- C:\WINDOWS\system32\vbscript.dll
2014-09-15 13:45:04 ----A---- C:\WINDOWS\SYSWOW64\dxtmsft.dll
2014-09-15 13:45:04 ----A---- C:\WINDOWS\system32\dxtrans.dll
2014-09-15 13:45:04 ----A---- C:\WINDOWS\system32\dxtmsft.dll
2014-09-15 13:45:03 ----A---- C:\WINDOWS\SYSWOW64\dxtrans.dll
2014-09-15 13:45:02 ----A---- C:\WINDOWS\system32\msfeeds.dll
2014-09-15 13:45:01 ----A---- C:\WINDOWS\SYSWOW64\msfeeds.dll
2014-09-15 13:45:01 ----A---- C:\WINDOWS\SYSWOW64\iedkcs32.dll
2014-09-15 13:45:01 ----A---- C:\WINDOWS\system32\iedkcs32.dll
2014-09-15 13:45:01 ----A---- C:\WINDOWS\system32\ie4uinit.exe
2014-09-15 13:44:59 ----A---- C:\WINDOWS\SYSWOW64\jscript9diag.dll
2014-09-15 13:44:59 ----A---- C:\WINDOWS\SYSWOW64\JavaScriptCollectionAgent.dll
2014-09-15 13:44:59 ----A---- C:\WINDOWS\SYSWOW64\ieapfltr.dll
2014-09-15 13:44:58 ----A---- C:\WINDOWS\system32\ieapfltr.dll
2014-09-15 13:44:55 ----A---- C:\WINDOWS\system32\mshtml.dll
2014-09-15 13:44:48 ----A---- C:\WINDOWS\system32\wininet.dll
2014-09-15 13:44:47 ----A---- C:\WINDOWS\SYSWOW64\wininet.dll
2014-09-15 13:44:47 ----A---- C:\WINDOWS\SYSWOW64\iertutil.dll
2014-09-15 13:44:46 ----A---- C:\WINDOWS\SYSWOW64\urlmon.dll
2014-09-15 13:44:46 ----A---- C:\WINDOWS\system32\urlmon.dll
2014-09-15 13:44:46 ----A---- C:\WINDOWS\system32\iertutil.dll
2014-09-15 13:44:43 ----A---- C:\WINDOWS\system32\ieframe.dll
2014-09-15 13:44:41 ----A---- C:\WINDOWS\SYSWOW64\ieframe.dll
2014-09-15 13:44:39 ----A---- C:\WINDOWS\SYSWOW64\mshtml.dll
2014-09-15 13:44:38 ----A---- C:\WINDOWS\system32\jscript9.dll
2014-09-15 13:44:37 ----A---- C:\WINDOWS\SYSWOW64\jscript9.dll
2014-09-15 13:36:00 ----A---- C:\WINDOWS\system32\schedsvc.dll
2014-09-15 13:34:51 ----A---- C:\WINDOWS\SYSWOW64\msvcr120_clr0400.dll
2014-09-15 13:34:50 ----A---- C:\WINDOWS\system32\msvcr120_clr0400.dll
2014-08-28 08:23:57 ----A---- C:\WINDOWS\system32\win32k.sys

======List of files/folders modified in the last 1 month======

2014-09-27 16:20:32 ----D---- C:\Program Files\trend micro

2014-09-27 16:19:04 ----D---- C:\WINDOWS\Temp
2014-09-27 16:18:12 ----D---- C:\WINDOWS\Prefetch
2014-09-27 16:13:25 ----D---- C:\WINDOWS\AppReadiness
2014-09-27 16:13:09 ----HD---- C:\Program Files\WindowsApps
2014-09-27 16:05:58 ----D---- C:\WINDOWS\system32\sru
2014-09-27 13:42:12 ----D---- C:\ProgramData\MFAData
2014-09-27 13:40:48 ----D---- C:\WINDOWS\debug
2014-09-27 13:16:23 ----D---- C:\WINDOWS\Inf
2014-09-27 13:16:08 ----D---- C:\Windows
2014-09-27 09:46:45 ----SHD---- C:\WINDOWS\Installer
2014-09-27 09:46:37 ----D---- C:\Program Files (x86)\AVG
2014-09-26 17:53:47 ----D---- C:\WINDOWS\SysWOW64
2014-09-26 16:58:39 ----D---- C:\WINDOWS\system32\config
2014-09-26 16:56:32 ----D---- C:\WINDOWS\system32\DriverStore
2014-09-26 16:56:29 ----D---- C:\Program Files\Common Files
2014-09-26 16:55:39 ----SHD---- C:\System Volume Information
2014-09-25 16:38:52 ----D---- C:\WINDOWS\Microsoft.NET
2014-09-25 16:30:11 ----RD---- C:\WINDOWS\assembly
2014-09-24 18:49:55 ----D---- C:\WINDOWS\CbsTemp
2014-09-24 18:49:54 ----D---- C:\WINDOWS\WinSxS
2014-09-24 18:49:37 ----D---- C:\WINDOWS\SYSWOW64\nl-NL
2014-09-24 18:49:37 ----D---- C:\WINDOWS\system32\nl-NL
2014-09-24 18:49:17 ----D---- C:\WINDOWS\system32\MRT
2014-09-24 18:37:42 ----A---- C:\WINDOWS\system32\MRT.exe
2014-09-24 16:16:10 ----RD---- C:\Program Files (x86)
2014-09-24 16:16:10 ----D---- C:\Program Files (x86)\Common Files
2014-09-24 16:14:03 ----D---- C:\WINDOWS\system32\Tasks
2014-09-24 16:13:59 ----HD---- C:\ProgramData
2014-09-23 22:02:18 ----D---- C:\WINDOWS\SoftwareDistribution
2014-09-23 14:49:02 ----D---- C:\ProgramData\regid.1991-06.com.microsoft
2014-09-23 14:46:41 ----D---- C:\Program Files\Microsoft Office 15
2014-09-18 20:43:36 ----D---- C:\WINDOWS\rescache
2014-09-18 14:36:14 ----D---- C:\Program Files\Unlocker
2014-09-18 14:13:35 ----RD---- C:\WINDOWS\System32
2014-09-18 14:13:35 ----A---- C:\WINDOWS\system32\PerfStringBackup.INI
2014-09-18 14:11:20 ----SD---- C:\Users\Riekie\AppData\Roaming\Microsoft
2014-09-18 14:10:29 ----RSD---- C:\WINDOWS\Fonts
2014-09-18 14:10:29 ----D---- C:\Program Files (x86)\OpenOffice 4
2014-09-17 18:44:31 ----A---- C:\WINDOWS\SYSWOW64\log.txt
2014-09-17 15:09:12 ----SHD---- C:\ProgramData\{01BD4FC9-2F86-4706-A62E-774BB7E9D308}
2014-09-17 14:36:07 ----D---- C:\Users\Riekie\AppData\Roaming\AVG
2014-09-17 14:29:24 ----D---- C:\ProgramData\AVG
2014-09-15 22:09:45 ----D---- C:\WINDOWS\system32\drivers
2014-09-15 22:03:41 ----RD---- C:\WINDOWS\ToastData
2014-09-15 22:03:30 ----D---- C:\WINDOWS\WinStore
2014-09-15 22:03:30 ----D---- C:\WINDOWS\SYSWOW64\wbem
2014-09-15 22:03:30 ----D---- C:\WINDOWS\SYSWOW64\setup
2014-09-15 22:03:30 ----D---- C:\Program Files\Windows Journal
2014-09-15 22:03:29 ----RD---- C:\WINDOWS\ImmersiveControlPanel
2014-09-15 22:03:29 ----D---- C:\WINDOWS\system32\drivers\nl-NL
2014-09-15 22:03:28 ----D---- C:\WINDOWS\system32\wbem
2014-09-15 22:03:28 ----D---- C:\WINDOWS\system32\setup
2014-09-15 22:03:28 ----D---- C:\WINDOWS\system32\oobe
2014-09-15 22:03:28 ----D---- C:\WINDOWS\system32\Boot
2014-09-15 22:03:24 ----D---- C:\WINDOWS\apppatch
2014-09-15 22:03:23 ----D---- C:\WINDOWS\SYSWOW64\migration
2014-09-15 22:03:23 ----D---- C:\WINDOWS\SYSWOW64\InputMethod
2014-09-15 22:03:23 ----D---- C:\WINDOWS\system32\migration
2014-09-15 22:03:21 ----D---- C:\Program Files\Internet Explorer
2014-09-15 22:03:21 ----D---- C:\Program Files (x86)\Internet Explorer
2014-09-15 14:39:53 ----D---- C:\WINDOWS\system32\catroot2
2014-09-04 19:44:00 ----D---- C:\WINDOWS\system32\NDF
2014-09-01 14:49:06 ----D---- C:\Program Files\CCleaner

2014-08-29 18:18:26 ----D---- C:\WINDOWS\Tasks

======List of drivers (R=Running, S=Stopped, 0=Boot, 1=System, 2=Auto, 3=Demand, 4=Disabled)======

R0 AVGIDSHA;AVGIDSHA; C:\WINDOWS\system32\DRIVERS\avgidsha.sys [2014-06-17 190744]
R0 Avgloga;AVG Logging Driver; C:\WINDOWS\system32\DRIVERS\avgloga.sys [2014-06-17 328984]
R0 Avgmfx64;AVG Mini-Filter Resident Anti-Virus Shield; C:\WINDOWS\system32\DRIVERS\avgmfx64.sys [2014-08-06 123672]
R0 Avgrkx64;AVG Anti-Rootkit Driver; C:\WINDOWS\system32\DRIVERS\avgrkx64.sys [2014-06-17 31512]
R0 iaStorA;iaStorA; C:\WINDOWS\System32\drivers\iaStorA.sys [2012-08-16 645952]
R0 RapportHades64;RapportHades64; C:\WINDOWS\System32\Drivers\RapportHades64.sys [2013-10-25 275056]
R0 RapportKE64;RapportKE64; C:\WINDOWS\System32\Drivers\RapportKE64.sys [2013-10-25 317808]
R1 Avgdiska;AVG Disk Driver; C:\WINDOWS\system32\DRIVERS\avgdiska.sys [2014-06-30 152344]
R1 AVGIDSDriver;AVGIDSDriver; C:\WINDOWS\system32\DRIVERS\avgidsdrivera.sys [2014-07-21 244504]
R1 Avgldx64;AVG AVI Loader Driver; C:\WINDOWS\system32\DRIVERS\avgldx64.sys [2014-06-17 235800]
R1 Avgwfpa;AVG Firewall Driver; C:\WINDOWS\system32\DRIVERS\avgwfpa.sys [2014-06-30 270104]
R1 RapportCerberus_59849;RapportCerberus_59849; \??\C:\ProgramData\Trusteer\Rapport\store\exts\RapportCerberus\baseline\RapportCerberus64_59849.sys [2013-12-08 606672]
R1 RapportEI64;RapportEI64; \??\C:\Program Files (x86)\Trusteer\Rapport\bin\x64\RapportEI64.sys [2013-12-21 282648]
R1 RapportPG64;RapportPG64; \??\C:\Program Files (x86)\Trusteer\Rapport\bin\x64\RapportPG64.sys [2013-12-21 397784]
R1 vwififlt;@%SystemRoot%\System32\drivers\vwififlt.sys,-259; C:\WINDOWS\system32\DRIVERS\vwififlt.sys [2014-04-30 71680]
R2 aswHwid;avast! HardwareID; C:\WINDOWS\system32\drivers\aswHwid.sys [2014-07-19 29208]
R2 SSPORT;SSPORT; \??\C:\WINDOWS\system32\Drivers\SSPORT.sys [2011-03-21 11576]
R3 ApfiltrService;@oem27.inf,%Filter.SvcDesc%;Alps Pointing-device Filter Driver; C:\WINDOWS\system32\DRIVERS\Apfiltr.sys [2012-11-13 452472]
R3 AthBTPort;@oem9.inf,%BTHSUPPORT.SvcDesc%;Qualcomm Atheros Virtual Bluetooth Class; C:\WINDOWS\system32\DRIVERS\btath_flt.sys [2013-01-28 89168]
R3 athr;@athw8x.inf,%ATHR.Service.DispName%;Qualcomm Atheros Extensible Wireless LAN device driver; C:\WINDOWS\system32\DRIVERS\athw8x.sys [2013-06-18 3680256]
R3 BTATH_A2DP;@oem8.inf,%BTATH_A2DP.SvcDesc%;Bluetooth A2DP Audio Driver; C:\WINDOWS\system32\drivers\btath_a2dp.sys [2013-01-28 346192]
R3 btath_avdt;@oem8.inf,%btath_avdt.SvcDesc%;Qualcomm Atheros Bluetooth AVDT Service; C:\WINDOWS\system32\drivers\btath_avdt.sys [2013-01-28 115280]
R3 BTATH_BUS;@oem5.inf,%BTATH_BUS.SVCDESC%;Qualcomm Atheros Bluetooth Bus; C:\WINDOWS\System32\drivers\btath_bus.sys [2013-01-28 34384]
R3 BTATH_HCRP;@oem12.inf,%BTATH_HCRP.SvcDesc%;Bluetooth HCRP Server driver; C:\WINDOWS\System32\drivers\btath_hcrp.sys [2013-01-28 179432]
R3 BTATH_LWFLT;@oem21.inf,%BTATH_LWFLT%;Bluetooth LWFLT Device; C:\WINDOWS\system32\DRIVERS\btath_lwflt.sys [2013-01-28 77464]
R3 BTATH_RCP;@oem17.inf,%BTATH_RCP%;Bluetooth AVRCP Device; C:\WINDOWS\System32\drivers\btath_rcp.sys [2013-01-28 136424]
R3 BtFilter;BtFilter; C:\WINDOWS\system32\DRIVERS\btfilter.sys [2014-04-28 599240]
R3 BthEnum;@bth.inf,%BthEnum.SVCDESC%;Bluetooth Enumerator-service; C:\WINDOWS\System32\drivers\BthEnum.sys [2013-08-22 53248]
R3 BthLEEnum;@bthleenum.inf,%BthLEEnum.SVCDESC%;Bluetooth Low Energy-stuurprogramma; C:\WINDOWS\system32\DRIVERS\BthLEEnum.sys [2014-03-18 226304]
R3 BthPan;@bthpan.inf,%BthPan.DisplayName%;Bluetooth Device (Personal Area Network); C:\WINDOWS\System32\drivers\bthpan.sys [2014-07-24 118272]
R3 BTHUSB;@bth.inf,%BTHUSB.SvcDesc%;USB-stuurprogramma voor Bluetooth-radio; C:\WINDOWS\System32\Drivers\BTHUSB.sys [2014-03-18 81920]
R3 igfx;igfx; C:\WINDOWS\system32\DRIVERS\igdkmd64.sys [2014-01-29 5363200]
R3 IntcAzAudAddService;Service for Realtek HD Audio (WDM); C:\WINDOWS\system32\drivers\RTKVHD64.sys [2012-07-31 4102928]
R3 IntcDAud;@oem22.inf,%IntcDAud.SvcDesc%;Intel(R) Display Audio; C:\WINDOWS\system32\DRIVERS\IntcDAud.sys [2012-06-19 342528]
R3 L1C;@netl1c63x64.inf,%L1C.Service.DispName%;NDIS-minipoortstuurprogramma voor Qualcomm Atheros AR81xx PCI-E Ethernet-controller; C:\WINDOWS\system32\DRIVERS\L1C63x64.sys [2013-06-18 129224]
R3 MEIx64;@oem25.inf,%HECI_SvcDesc%;Intel(R) Management Engine Interface ; C:\WINDOWS\System32\drivers\HECIx64.sys [2012-07-02 62784]

R3 NTIDrvr;NTIDrvr; \??\C:\Windows\system32\drivers\NTIDrvr.sys [2010-04-20 18432]
R3 Ps2Kb2Hid;@oem26.inf,%Ps2Kb2Hid.SVCDESC%;PS/2 Keyboard to HID Driver;
C:\WINDOWS\System32\drivers\aPs2Kb2Hid.sys [2013-03-22 26736]
R3 RFCOMM;@tdibth.inf,%RFCOMM.DisplayName%;Bluetooth Device (RFCOMM Protocol TDI);
C:\WINDOWS\System32\drivers\rfcomm.sys [2014-03-18 167424]
R3 TuneUpUtilitiesDrv;TuneUpUtilitiesDrv; \??\C:\Program Files (x86)\AVG\AVG PC
TuneUp\TuneUpUtilitiesDriver64.sys [2014-08-28 14112]
R3 UBHelper;UBHelper; \??\C:\Windows\system32\drivers\UBHelper.sys [2010-07-09 17408]
R3 usbvideo;@usbvideo.inf,%USBVideo.SvcDesc%;USB-videoapparaat (WDM);
C:\WINDOWS\System32\Drivers\usbvideo.sys [2013-08-22 212224]
R3 vwifimp;@%SystemRoot%\System32\drivers\vwifimp.sys,-261; C:\WINDOWS\system32\DRIVERS\vwifimp.sys
[2014-04-30 38912]
S0 Avgboota;AVG Early Launch Anti-Malware Driver; C:\WINDOWS\system32\DRIVERS\avgboota.sys [2013-09-04
20496]
S3 BTHPORT;@bth.inf,%BTHPORT.SvcDesc%;Stuurprogramma voor Bluetooth-poort;
C:\WINDOWS\System32\Drivers\BTHport.sys [2014-07-24 1200640]
S3 RSPCIESTOR;@oem2.inf,%Rts5208%;Realtek PCIE CardReader Driver;
C:\WINDOWS\system32\DRIVERS\RtsPStor.sys [2012-08-03 340112]
S3 usbscan;@sti.inf,%usbscan.SvcDesc%;Stuurprogramma voor USB-scanner;
C:\WINDOWS\system32\DRIVERS\usbscan.sys [2013-08-22 44544]

======List of services (R=Running, S=Stopped, 0=Boot, 1=System, 2=Auto, 3=Demand, 4=Disabled)======

R2 AdobeARMservice;Adobe Acrobat Update Service; C:\Program Files (x86)\Common
Files\Adobe\ARM\1.0\armsvc.exe [2014-09-12 64704]
R2 AtherosSvc;AtherosSvc; C:\Program Files (x86)\Qualcomm Atheros\Bluetooth Suite\adminservice.exe [2013-01-28
227456]
R2 AVGIDSAgent;AVGIDSAgent; C:\Program Files (x86)\AVG\AVG2014\avgidsagent.exe [2014-08-25 3242000]
R2 avgwd;AVG WatchDog; C:\Program Files (x86)\AVG\AVG2014\avgwdsvc.exe [2014-08-25 289328]
R2 c2cautoupdatesvc;Skype Click to Call Updater; C:\Program Files
(x86)\Skype\Toolbars\AutoUpdate\SkypeC2CAutoUpdateSvc.exe [2014-07-14 1390176]
R2 c2cpnrsvc;Skype Click to Call PNR Service; C:\Program Files
(x86)\Skype\Toolbars\PNRSvc\SkypeC2CPNRSvc.exe [2014-07-14 1767520]
R2 CCDMonitorService;CCDMonitorService; C:\Program Files (x86)\Acer\Acer Cloud\CCDMonitorService.exe
[2012-10-26 2449552]
R2 ClickToRunSvc;Microsoft Office ClickToRun Service; C:\Program Files\Microsoft Office
15\ClientX64\OfficeClickToRun.exe [2014-08-12 2428088]
R2 DsiWMIService;Dritek WMI Service; C:\Program Files (x86)\Launch Manager\dsiwmis.exe [2012-12-10 350544]
R2 Garmin Core Update Service;Garmin Core Update Service; C:\Program Files (x86)\Garmin\Core Update
Service\Garmin.Cartography.MapUpdate.CoreService.exe [2014-07-23 438616]
R2 IconMan_R;IconMan_R; C:\Program Files (x86)\Realtek\Realtek PCIE Card Reader\RIconMan.exe [2012-07-24
2457232]
R2 Intel(R) Capability Licensing Service Interface;Intel(R) Capability Licensing Service Interface; C:\Program
Files\Intel\iCLS Client\HeciServer.exe [2012-04-20 635104]
R2 jhi_service;Intel(R) Dynamic Application Loader Host Interface Service; C:\Program Files (x86)\Intel\Intel(R)
Management Engine Components\DAL\jhi_service.exe [2012-07-17 165760]
R2 LMS;Intel(R) Management and Security Application Local Management Service; C:\Program Files
(x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe [2012-07-17 276864]
R2 NTI IScheduleSvc;NTI IScheduleSvc; C:\Program Files (x86)\NTI\Acer Backup Manager\IScheduleSvc.exe [2012-
11-03 259136]
R2 RfButtonDriverService;Dritek RF Button Command Service; C:\Windows\RfBtnSvc64.exe [2013-03-22 93296]
R2 TeamViewer8;TeamViewer 8; C:\Program Files (x86)\TeamViewer\Version8\TeamViewer_Service.exe [2014-08-
04 5095264]
R2 UNS;Intel(R) Management and Security Application User Notification Service; C:\Program Files
(x86)\Intel\Intel(R) Management Engine Components\UNS\UNS.exe [2012-07-17 364416]
R3 ePowerSvc;ePower Service; C:\Program Files\Acer\Acer Power Management\ePowerSvc.exe [2012-10-23 658064]
S2 gupdate;Google Update-service (gupdate); C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [2013-11-19
116648]
S2 LiveUpdateSvc;LiveUpdate; C:\Program Files (x86)\IObit\LiveUpdate\LiveUpdate.exe [2013-12-03 2151200]
S2 McAfee SiteAdvisor Service;McAfee SiteAdvisor Service; C:\Program Files\Common
Files\McAfee\McSvcHost\McSvHost.exe [2012-05-11 200728]
S2 SkypeUpdate;Skype Updater; C:\Program Files (x86)\Skype\Updater\Updater.exe [2014-04-03 315008]
S2 TuneUp.UtilitiesSvc;AVG PC TuneUp Service; C:\Program Files (x86)\AVG\AVG PC

TuneUp\TuneUpUtilitiesService64.exe [2014-09-04 2538808]
S3 AdobeFlashPlayerUpdateSvc;Adobe Flash Player Update Service;
C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe [2014-09-15 267440]
S3 cphs;Intel(R) Content Protection HECI Service; C:\WINDOWS\SysWow64\IntelCpHeciSvc.exe [2014-01-29
279000]
S3 DeviceFastLaneService;Device Fast-lane Service; C:\Program Files\Acer\Acer Device Fast-
lane\DeviceFastLaneSvc.exe [2012-11-17 469648]
S3 FLEXnet Licensing Service;FLEXnet Licensing Service; C:\Program Files (x86)\Common Files\Macrovision
Shared\FLEXnet Publisher\FNPLicensingService.exe [2013-03-22 655624]
S3 FontCache3.0.0.0;@%SystemRoot%\system32\PresentationHost.exe,-3309;
C:\WINDOWS\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe [2013-08-03 43696]
S3 gupdatem;Google Update-service (gupdatem); C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [2013-11-
19 116648]
S3 gusvc;Google Updater Service; C:\Program Files (x86)\Google\Common\Google
Updater\GoogleUpdaterService.exe [2014-03-11 136120]
S3 ose;Office Source Engine; C:\Program Files (x86)\Common Files\Microsoft Shared\Source Engine\OSE.EXE
[2013-10-17 150600]

----------EOF----------