ï»¿Logfile of random's system information tool 1.10 (written by random/random)
Run by Riekie at 2014-08-07 22:21:36
Microsoft Windows 8.1
System drive C: has 382 GB (84%) free of 454 GB
Total RAM: 3912 MB (42% free)

Logfile of Trend Micro HijackThis v2.0.4
Scan saved at 22:21:47, on 7-8-2014
Platform: Unknown Windows (WinNT 6.02.1008)
MSIE: Internet Explorer v11.0 (11.00.9600.17126)
Boot mode: Normal

Running processes:
C:\Program Files (x86)\Launch Manager\LManager.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files\AVAST Software\Avast\avastui.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files\Microsoft Office 15\Root\VFS\ProgramFilesCommonX86\Microsoft Shared\OFFICE15\CSISYNCCLIENT.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)\TeamViewer\Version8\TeamViewer.exe
C:\Program Files\WindowsApps\Microsoft.MicrosoftSolitaireCollection_2.3.1407.252_x86__8wekyb3d8bbwe\Solitaire.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: avast! Online Security - {8E5E2654-AD2D-48bf-AC2D-D17F00898D06} - C:\Program Files\AVAST Software\Avast\aswWebRepIE.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: [AvastUI.exe] "C:\Program Files\AVAST Software\Avast\AvastUI.exe" /nogui
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 - 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
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
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: Apple Mobile Device - Apple Inc. - C:\Program Files (x86)\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe
O23 - Service: AtherosSvc - Qualcomm Atheros Commnucations - C:\Program Files (x86)\Qualcomm Atheros\Bluetooth Suite\adminservice.exe
O23 - Service: avast! Antivirus - AVAST Software - C:\Program Files\AVAST Software\Avast\AvastSvc.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: Rapport Management Service (RapportMgmtService) - Unknown owner - C:\Program Files (x86)\Trusteer\Rapport\bin\RapportMgmtService.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: @%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: @%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 - 10925 bytes

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

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:\Program Files\AVAST Software\Avast\AvastSvc.exe"
C:\WINDOWS\System32\spoolsv.exe
C:\WINDOWS\system32\svchost.exe -k LocalServiceNoNetwork
"C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe"
"C:\Program Files (x86)\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe"
"C:\Program Files (x86)\Qualcomm Atheros\Bluetooth Suite\adminservice.exe"
"C:\Program Files (x86)\Acer\Acer Cloud\CCDMonitorService.exe"

"C:\Program Files\Microsoft Office 15\ClientX64\OfficeClickToRun.exe" /service
"C:\Program Files (x86)\Launch Manager\dsiwmis.exe"
dashost.exe {3df42083-788e-4100-ae870d48dbf9a1cd}
C:\WINDOWS\system32\svchost.exe -k LocalServiceAndNoImpersonation
"C:\Program Files (x86)\Garmin\Core Update Service\Garmin.Cartography.MapUpdate.CoreService.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:\WINDOWS\system32\svchost.exe -k imgsvc
C:\WINDOWS\System32\svchost.exe -k LocalServicePeerNet
C:\WINDOWS\system32\DllHost.exe /Processid:{30D49246-D217-465F-B00B-AC9DDD652EB7}
C:\WINDOWS\system32\SearchIndexer.exe /Embedding
"C:\Program Files\Acer\Acer Power Management\ePowerSvc.exe"
"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\Windows Media Player\wmpnetwk.exe"
C:\WINDOWS\system32\wbem\wmiprvse.exe
C:\WINDOWS\system32\wbem\wmiprvse.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:\WINDOWS\Explorer.EXE
"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 (x86)\Google\Chrome\Application\chrome.exe"
"C:\Windows\System32\igfxtray.exe"
"C:\Program Files (x86)\Qualcomm Atheros\Bluetooth Suite\ActivateDesktop.exe"
"C:\Windows\System32\hkcmd.exe"
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=gpu-process --channel="1768.0.804702737\1789270716" --disable-d3d11 --supports-dual-gpus=false --gpu-driver-bug-workarounds=1,5,16 --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\igfxpers.exe"
"C:\Program Files\Apoint2K\Apoint.exe"
"C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe" -s
"C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe" /FORPCEE4
"C:\Program Files (x86)\Qualcomm Atheros\Bluetooth Suite\BtTray.exe"
"C:\Program Files\Common Files\Common Desktop Agent\CDASrv.exe"
"C:\Program Files\Apoint2K\ApMsgFwd.exe" -s{05FA8492-C047-4207-BE65-780D8591C113}
"C:\Program Files\Apoint2K\HidFind.exe"
"C:\Program Files\Start Menu X\StartMenuX.exe"
"Apntex.exe"
\??\C:\WINDOWS\system32\conhost.exe 0x4
"C:\Dolby PCEE4\pcee4.exe" -autostart
"C:\Program Files\AVAST Software\Avast\avastui.exe" /nogui
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --lang=nl --force-fieldtrials="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/SettingsEnforcement/no_enforcement/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_09/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/" --extension-process --renderer-print-preview --enable-pinch --enable-threaded-compositing --enable-delegated-renderer --channel="1768.3.353854818\719436768" /prefetch:673131151
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --lang=nl --force-fieldtrials="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/SettingsEnforcement/no_enforcement/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_09/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/" --extension-process --renderer-print-preview --enable-pinch --enable-threaded-compositing --enable-delegated-renderer --channel="1768.4.363254741\207153239" /prefetch:673131151
C:\WINDOWS\system32\wbem\unsecapp.exe -Embedding
"C:\Program Files\Acer\Acer Power Management\ePowerTray.exe"
"C:\Windows\System32\SettingSyncHost.exe" -Embedding
"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:\Program Files\Acer\Acer Power Management\ePowerEvent.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)\TeamViewer\Version8\TeamViewer_Service.exe"
"C:\Program Files (x86)\TeamViewer\Version8\TeamViewer.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:\Windows\System32\RuntimeBroker.exe -Embedding
"C:\Program Files\WindowsApps\Microsoft.MicrosoftSolitaireCollection_2.3.1407.252_x86__8wekyb3d8bbwe\Solitaire.exe" -ServerName:App.AppXx8xn0rs58sab7mvbtxgdhw97cpm1dzhb.mca

"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --lang=nl --force-fieldtrials="BrowserBlacklist/Enabled/ChromeSuggestions/Most Likely with Kodachrome/EmbeddedSearch/Group2 pct:10b stable:pp2 prefetch_results:1 reuse_instant_search_base_page:1/ExtensionInstallVerification/Enforce/FlashHardwareVideoDecode/HwVideo/GoogleNow/Enable/OmniboxBundledExperimentV1/StandardR4/Prerender/PrerenderEnabled/PrerenderFromOmnibox/OmniboxPrerenderEnabled/PrerenderLocalPredictorSpec/LocalPredictor=Disabled/QUIC/Disabled/SettingsEnforcement/no_enforcement/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_09/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/" --extension-process --renderer-print-preview --enable-pinch --enable-threaded-compositing --enable-delegated-renderer --channel="1768.61.582757477\70239813" /prefetch:673131151
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --lang=nl --force-fieldtrials="BrowserBlacklist/Enabled/ChromeSuggestions/Most Likely with Kodachrome/EmbeddedSearch/Group2 pct:10b stable:pp2 prefetch_results:1 reuse_instant_search_base_page:1/ExtensionInstallVerification/Enforce/FlashHardwareVideoDecode/HwVideo/GoogleNow/Enable/OmniboxBundledExperimentV1/StandardR4/Prerender/PrerenderEnabled/PrerenderFromOmnibox/OmniboxPrerenderEnabled/PrerenderLocalPredictorSpec/LocalPredictor=Disabled/QUIC/Disabled/SettingsEnforcement/no_enforcement/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_09/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-pinch --enable-threaded-compositing --enable-delegated-renderer
--channel="1768.64.503861876\1634453581" /prefetch:673131151
"C:\WINDOWS\system32\SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe116_
Global\UsGthrCtrlFltPipeMssGthrPipe116 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" 0 580 584 592 65536 588
taskeng.exe {C87B099D-1A75-46CB-888D-9AD6BBA6E636}
"C:\Users\Riekie\Desktop\RSITx64.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#
C:\WINDOWS\tasks\Uninstaller_SkipUac_Administrator.job - C:\Program Files (x86)\IObit\IObit
Uninstaller\IObitUninstaler.exe# /UninstallExplorer#

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

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\
{10921475-03CE-4E04-90CE-E2E7EF20C814}]
ExplorerWnd Helper - C:\Program Files (x86)\IObit\IObit Uninstaller\UninstallExplorer64.dll [2014-05-18 2471744]

[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 [2014-07-12 218784]

[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\
{8E5E2654-AD2D-48bf-AC2D-D17F00898D06}]
avast! Online Security - C:\Program Files\AVAST Software\Avast\aswWebRepIE64.dll [2014-07-19 612248]

[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 [2014-07-12 2335960]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser
Helper Objects\{8E5E2654-AD2D-48bf-AC2D-D17F00898D06}]
avast! Online Security - C:\Program Files\AVAST Software\Avast\aswWebRepIE.dll [2014-07-19 457712]

[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]
"CDAServer"=C:\Program Files\Common Files\Common Desktop Agent\CDASrv.exe [2012-02-20 456704]

[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]

[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 [2013-11-21 959904]
"AvastUI.exe"=C:\Program Files\AVAST Software\Avast\AvastUI.exe [2014-07-29 4085896]

[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\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======

2014-08-03 09:09:15 ----D---- C:\WINDOWS\Minidump
2014-08-03 09:09:06 ----ASH---- C:\pagefile.sys
2014-08-02 22:13:42 ----A---- C:\WINDOWS\system32\SyncEngine.dll
2014-08-02 22:13:40 ----A---- C:\WINDOWS\system32\SkyDrive.exe
2014-08-02 22:13:39 ----A---- C:\WINDOWS\system32\SkyDriveTelemetry.dll
2014-08-01 18:40:59 ----D---- C:\Program Files\Common Files\Atheros
2014-08-01 18:35:32 ----A---- C:\WINDOWS\SYSWOW64\mfcore.dll
2014-08-01 18:35:31 ----A---- C:\WINDOWS\SYSWOW64\d3d9.dll
2014-08-01 18:35:31 ----A---- C:\WINDOWS\system32\d3d9.dll
2014-08-01 18:35:31 ----A---- C:\WINDOWS\system32\authui.dll
2014-08-01 18:35:28 ----A---- C:\WINDOWS\SYSWOW64\authui.dll
2014-08-01 18:35:28 ----A---- C:\WINDOWS\system32\mfcore.dll
2014-08-01 18:35:27 ----A---- C:\WINDOWS\system32\localspl.dll
2014-08-01 18:35:26 ----A---- C:\WINDOWS\system32\vpnike.dll
2014-08-01 18:35:26 ----A---- C:\WINDOWS\system32\fveapi.dll
2014-08-01 18:35:26 ----A---- C:\WINDOWS\system32\dhcpcore.dll
2014-08-01 18:35:25 ----A---- C:\WINDOWS\system32\ntdll.dll
2014-08-01 18:35:24 ----A---- C:\WINDOWS\SYSWOW64\ntdll.dll
2014-08-01 18:35:24 ----A---- C:\WINDOWS\SYSWOW64\dhcpcore.dll
2014-08-01 18:35:24 ----A---- C:\WINDOWS\system32\actxprxy.dll
2014-08-01 18:35:23 ----A---- C:\WINDOWS\system32\SkyDriveShell.dll
2014-08-01 18:35:23 ----A---- C:\WINDOWS\system32\framedynos.dll
2014-08-01 18:35:23 ----A---- C:\WINDOWS\system32\drivers\mrxsmb.sys
2014-08-01 18:35:22 ----A---- C:\WINDOWS\SYSWOW64\SkyDriveShell.dll
2014-08-01 18:35:20 ----A---- C:\WINDOWS\system32\dhcpcore6.dll
2014-08-01 18:35:19 ----A---- C:\WINDOWS\system32\bdesvc.dll
2014-08-01 18:35:18 ----A---- C:\WINDOWS\SYSWOW64\framedynos.dll
2014-08-01 18:35:18 ----A---- C:\WINDOWS\SYSWOW64\dhcpcore6.dll
2014-08-01 18:35:17 ----A---- C:\WINDOWS\system32\drivers\agilevpn.sys
2014-08-01 18:35:17 ----A---- C:\WINDOWS\system32\BFE.DLL
2014-08-01 18:35:16 ----A---- C:\WINDOWS\system32\ncobjapi.dll
2014-08-01 18:35:14 ----A---- C:\WINDOWS\system32\winbici.dll
2014-08-01 18:35:14 ----A---- C:\WINDOWS\system32\framedyn.dll
2014-08-01 18:35:13 ----A---- C:\WINDOWS\SYSWOW64\ncobjapi.dll
2014-08-01 18:35:12 ----A---- C:\WINDOWS\SYSWOW64\WebClnt.dll
2014-08-01 18:35:12 ----A---- C:\WINDOWS\system32\WebClnt.dll
2014-08-01 18:35:12 ----A---- C:\WINDOWS\system32\Robocopy.exe
2014-08-01 18:35:12 ----A---- C:\WINDOWS\system32\drivers\vwifimp.sys
2014-08-01 18:35:11 ----A---- C:\WINDOWS\system32\dhcpcsvc.dll
2014-08-01 18:35:10 ----A---- C:\WINDOWS\SYSWOW64\Robocopy.exe
2014-08-01 18:35:10 ----A---- C:\WINDOWS\system32\IKEEXT.DLL
2014-08-01 18:35:10 ----A---- C:\WINDOWS\system32\dhcpcsvc6.dll
2014-08-01 18:35:09 ----A---- C:\WINDOWS\SYSWOW64\framedyn.dll
2014-08-01 18:35:09 ----A---- C:\WINDOWS\SYSWOW64\dhcpcsvc.dll
2014-08-01 18:35:09 ----A---- C:\WINDOWS\SYSWOW64\actxprxy.dll
2014-08-01 18:35:09 ----A---- C:\WINDOWS\system32\drivers\vwififlt.sys
2014-08-01 18:35:09 ----A---- C:\WINDOWS\system32\BulkOperationHost.exe
2014-08-01 18:35:08 ----A---- C:\WINDOWS\SYSWOW64\dhcpcsvc6.dll
2014-08-01 18:35:07 ----A---- C:\WINDOWS\SYSWOW64\d3d8thk.dll
2014-08-01 18:35:07 ----A---- C:\WINDOWS\system32\srms.dat
2014-08-01 18:35:07 ----A---- C:\WINDOWS\system32\reseteng.dll
2014-08-01 18:34:33 ----A---- C:\WINDOWS\system32\drivers\mrxsmb20.sys
2014-08-01 18:34:18 ----A---- C:\WINDOWS\system32\Windows.UI.Xaml.dll
2014-08-01 18:34:15 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.Xaml.dll
2014-08-01 18:34:12 ----A---- C:\WINDOWS\system32\drivers\tcpip.sys
2014-08-01 18:34:11 ----AC---- C:\WINDOWS\system32\drivers\usbport.sys
2014-08-01 18:34:11 ----AC---- C:\WINDOWS\system32\drivers\usbhub.sys
2014-08-01 18:34:10 ----A---- C:\WINDOWS\system32\rsaenh.dll

2014-08-01 18:34:10 ----A---- C:\WINDOWS\system32\drivers\WUDFRd.sys
2014-08-01 18:34:09 ----AC---- C:\WINDOWS\system32\drivers\USBHUB3.SYS
2014-08-01 18:34:09 ----A---- C:\WINDOWS\SYSWOW64\rsaenh.dll
2014-08-01 18:34:09 ----A---- C:\WINDOWS\system32\WUDFSvc.dll
2014-08-01 18:34:09 ----A---- C:\WINDOWS\system32\WUDFHost.exe
2014-08-01 18:34:09 ----A---- C:\WINDOWS\system32\drivers\WUDFPf.sys
2014-08-01 18:34:08 ----AC---- C:\WINDOWS\system32\drivers\usbuhci.sys
2014-08-01 18:34:08 ----AC---- C:\WINDOWS\system32\drivers\usbehci.sys
2014-08-01 18:34:08 ----A---- C:\WINDOWS\system32\WUDFPlatform.dll
2014-08-01 18:34:08 ----A---- C:\WINDOWS\system32\DaOtpCredentialProvider.dll
2014-08-01 18:34:07 ----AC---- C:\WINDOWS\system32\drivers\usbd.sys
2014-08-01 18:34:07 ----A---- C:\WINDOWS\SYSWOW64\DaOtpCredentialProvider.dll
2014-08-01 18:34:07 ----A---- C:\WINDOWS\system32\hal.dll
2014-08-01 18:32:09 ----A---- C:\WINDOWS\system32\mfps.dll
2014-08-01 18:28:02 ----A---- C:\WINDOWS\system32\drivers\FWPKCLNT.SYS
2014-07-30 13:23:50 ----D---- C:\rsit
2014-07-25 08:14:08 ----D---- C:\ProgramData\Package Cache
2014-07-19 09:52:01 ----D---- C:\Users\Riekie\AppData\Roaming\AVAST Software
2014-07-19 09:50:34 ----A---- C:\WINDOWS\system32\drivers\aswsp.sys
2014-07-19 09:50:22 ----A---- C:\WINDOWS\system32\drivers\aswVmm.sys
2014-07-19 09:50:22 ----A---- C:\WINDOWS\system32\drivers\aswStm.sys
2014-07-19 09:50:22 ----A---- C:\WINDOWS\system32\drivers\aswSnx.sys
2014-07-19 09:50:22 ----A---- C:\WINDOWS\system32\drivers\aswRvrt.sys
2014-07-19 09:50:22 ----A---- C:\WINDOWS\system32\drivers\aswRdr2.sys
2014-07-19 09:50:22 ----A---- C:\WINDOWS\system32\drivers\aswMonFlt.sys
2014-07-19 09:50:22 ----A---- C:\WINDOWS\system32\drivers\aswKbd.sys
2014-07-19 09:50:22 ----A---- C:\WINDOWS\system32\drivers\aswHwid.sys
2014-07-19 09:50:20 ----A---- C:\WINDOWS\system32\aswBoot.exe
2014-07-19 09:50:10 ----A---- C:\WINDOWS\avastSS.scr
2014-07-19 09:44:46 ----D---- C:\Program Files\AVAST Software
2014-07-15 21:34:15 ----A---- C:\WINDOWS\SYSWOW64\FlashPlayerApp.exe
2014-07-15 16:47:50 ----A---- C:\WINDOWS\system32\termsrv.dll
2014-07-10 13:29:24 ----A---- C:\WINDOWS\system32\win32k.sys
2014-07-10 13:29:23 ----A---- C:\WINDOWS\system32\osk.exe
2014-07-10 13:29:22 ----A---- C:\WINDOWS\SYSWOW64\osk.exe
2014-07-10 13:29:19 ----A---- C:\WINDOWS\system32\drivers\afd.sys
2014-07-10 13:29:08 ----A---- C:\WINDOWS\system32\lsasrv.dll
2014-07-10 13:29:08 ----A---- C:\WINDOWS\system32\drivers\cng.sys
2014-07-10 13:29:08 ----A---- C:\WINDOWS\system32\certcli.dll
2014-07-10 13:29:08 ----A---- C:\WINDOWS\system32\adtschema.dll
2014-07-10 13:29:07 ----A---- C:\WINDOWS\SYSWOW64\certcli.dll
2014-07-10 13:29:07 ----A---- C:\WINDOWS\SYSWOW64\adtschema.dll
2014-07-10 13:27:58 ----A---- C:\WINDOWS\SYSWOW64\iedkcs32.dll
2014-07-10 13:27:57 ----A---- C:\WINDOWS\system32\mshtml.dll
2014-07-10 13:27:57 ----A---- C:\WINDOWS\system32\iedkcs32.dll
2014-07-10 13:27:54 ----A---- C:\WINDOWS\SYSWOW64\mshtml.dll
2014-07-10 13:27:28 ----A---- C:\WINDOWS\system32\jscript9.dll
2014-07-10 13:27:22 ----A---- C:\WINDOWS\system32\ieframe.dll
2014-07-10 13:27:17 ----A---- C:\WINDOWS\SYSWOW64\jscript9.dll
2014-07-10 13:27:15 ----A---- C:\WINDOWS\SYSWOW64\ieframe.dll
2014-07-10 13:27:12 ----A---- C:\WINDOWS\system32\urlmon.dll
2014-07-10 13:27:11 ----A---- C:\WINDOWS\SYSWOW64\urlmon.dll
2014-07-10 13:27:11 ----A---- C:\WINDOWS\system32\wininet.dll
2014-07-10 13:27:11 ----A---- C:\WINDOWS\system32\iertutil.dll
2014-07-10 13:27:10 ----A---- C:\WINDOWS\SYSWOW64\wininet.dll
2014-07-10 13:27:10 ----A---- C:\WINDOWS\SYSWOW64\iertutil.dll
2014-07-10 13:27:10 ----A---- C:\WINDOWS\SYSWOW64\dxtrans.dll
2014-07-10 13:27:10 ----A---- C:\WINDOWS\SYSWOW64\dxtmsft.dll
2014-07-10 13:27:10 ----A---- C:\WINDOWS\system32\dxtrans.dll
2014-07-10 13:27:10 ----A---- C:\WINDOWS\system32\dxtmsft.dll
2014-07-10 13:27:09 ----A---- C:\WINDOWS\SYSWOW64\mshtmled.dll
2014-07-10 13:27:09 ----A---- C:\WINDOWS\SYSWOW64\msfeeds.dll
2014-07-10 13:27:09 ----A---- C:\WINDOWS\system32\mshtmled.dll

2014-07-10 13:27:09 ----A---- C:\WINDOWS\system32\msfeeds.dll
2014-07-10 13:27:08 ----A---- C:\WINDOWS\SYSWOW64\ieapfltr.dll
2014-07-10 13:27:08 ----A---- C:\WINDOWS\system32\ieapfltr.dll
2014-07-10 13:27:08 ----A---- C:\WINDOWS\system32\ie4uinit.exe
2014-07-10 13:27:00 ----A---- C:\WINDOWS\system32\qedit.dll
2014-07-10 13:26:59 ----A---- C:\WINDOWS\SYSWOW64\qedit.dll
2014-07-10 13:26:48 ----A---- C:\WINDOWS\SYSWOW64\WSShared.dll
2014-07-10 13:26:47 ----A---- C:\WINDOWS\system32\WSShared.dll
2014-07-10 13:26:47 ----A---- C:\WINDOWS\system32\twinui.dll
2014-07-10 13:26:45 ----A---- C:\WINDOWS\SYSWOW64\Windows.ApplicationModel.Store.TestingFramework.dll
2014-07-10 13:26:45 ----A---- C:\WINDOWS\system32\wuaueng.dll
2014-07-10 13:26:45 ----A---- C:\WINDOWS\system32\Windows.ApplicationModel.Store.TestingFramework.dll
2014-07-10 13:26:44 ----A---- C:\WINDOWS\SYSWOW64\twinui.dll
2014-07-10 13:26:43 ----A---- C:\WINDOWS\SYSWOW64\twinui.appcore.dll
2014-07-10 13:26:43 ----A---- C:\WINDOWS\system32\wuauclt.exe
2014-07-10 13:26:43 ----A---- C:\WINDOWS\system32\twinui.appcore.dll
2014-07-10 13:26:43 ----A---- C:\WINDOWS\system32\twinapi.appcore.dll
2014-07-10 13:26:42 ----A---- C:\WINDOWS\SYSWOW64\wudriver.dll
2014-07-10 13:26:42 ----A---- C:\WINDOWS\SYSWOW64\wuapi.dll
2014-07-10 13:26:42 ----A---- C:\WINDOWS\system32\wudriver.dll
2014-07-10 13:26:42 ----A---- C:\WINDOWS\system32\wuapi.dll
2014-07-10 13:08:16 ----A---- C:\WINDOWS\system32\WSReset.exe

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

2014-08-07 22:21:40 ----D---- C:\Program Files\trend micro
2014-08-07 22:19:34 ----D---- C:\WINDOWS\Prefetch
2014-08-07 22:10:07 ----D---- C:\WINDOWS\Temp
2014-08-07 22:00:01 ----D---- C:\WINDOWS\system32\sru
2014-08-07 13:49:58 ----D---- C:\WINDOWS\system32\Tasks
2014-08-07 13:46:45 ----D---- C:\WINDOWS\Microsoft.NET
2014-08-07 13:45:52 ----D---- C:\WINDOWS\debug
2014-08-07 12:31:42 ----D---- C:\WINDOWS\AppReadiness
2014-08-07 12:31:26 ----D---- C:\WINDOWS\SoftwareDistribution
2014-08-07 12:31:26 ----D---- C:\Windows
2014-08-06 23:37:20 ----D---- C:\WINDOWS\Inf
2014-08-05 13:40:49 ----HD---- C:\Program Files\WindowsApps
2014-08-03 20:38:14 ----D---- C:\WINDOWS\rescache
2014-08-03 20:36:57 ----D---- C:\WINDOWS\system32\config
2014-08-03 20:33:48 ----SHD---- C:\System Volume Information
2014-08-03 20:16:49 ----D---- C:\WINDOWS\system32\DriverStore
2014-08-03 20:16:43 ----RD---- C:\WINDOWS\assembly
2014-08-03 09:12:58 ----A---- C:\WINDOWS\SYSWOW64\log.txt
2014-08-03 08:55:25 ----D---- C:\ProgramData\ProductData
2014-08-03 08:55:03 ----D---- C:\WINDOWS\WinSxS
2014-08-03 08:53:37 ----D---- C:\Program Files\Microsoft Silverlight
2014-08-03 08:53:36 ----D---- C:\Program Files (x86)\Microsoft Silverlight
2014-08-03 08:53:35 ----SHD---- C:\Config.Msi
2014-08-03 08:53:35 ----RD---- C:\Program Files (x86)
2014-08-03 08:53:35 ----D---- C:\ProgramData\MFAData
2014-08-03 08:53:35 ----D---- C:\ProgramData\AVG2014
2014-08-03 08:52:55 ----D---- C:\WINDOWS\system32\drivers
2014-08-03 08:51:52 ----RD---- C:\WINDOWS\System32
2014-08-03 08:51:51 ----D---- C:\WINDOWS\MediaViewer
2014-08-03 08:51:50 ----D---- C:\WINDOWS\SYSWOW64\wbem
2014-08-03 08:51:50 ----D---- C:\WINDOWS\SYSWOW64\nl-NL
2014-08-03 08:51:50 ----D---- C:\WINDOWS\SYSWOW64\migration
2014-08-03 08:51:50 ----D---- C:\WINDOWS\SysWOW64
2014-08-03 08:51:50 ----D---- C:\WINDOWS\system32\wbem
2014-08-03 08:51:50 ----D---- C:\WINDOWS\system32\nl-NL
2014-08-03 08:51:50 ----D---- C:\WINDOWS\system32\en-US
2014-08-03 08:51:48 ----D---- C:\WINDOWS\FileManager
2014-08-03 08:51:48 ----D---- C:\WINDOWS\Camera

2014-08-03 08:51:07 ----D---- C:\WINDOWS\CbsTemp
2014-08-02 15:42:45 ----A---- C:\WINDOWS\system32\PerfStringBackup.INI
2014-08-02 15:39:31 ----SHD---- C:\WINDOWS\Installer
2014-08-02 15:38:02 ----D---- C:\ProgramData\regid.1991-06.com.microsoft
2014-08-02 15:33:44 ----D---- C:\Program Files\Microsoft Office 15
2014-08-01 18:40:59 ----D---- C:\Program Files\Common Files
2014-08-01 18:32:43 ----D---- C:\WINDOWS\system32\catroot2
2014-07-31 11:06:53 ----D---- C:\Program Files\CCleaner
2014-07-25 08:15:34 ----D---- C:\ProgramData\Garmin
2014-07-25 08:15:16 ----D---- C:\Program Files (x86)\Garmin
2014-07-25 08:14:08 ----HD---- C:\ProgramData
2014-07-19 09:49:28 ----HD---- C:\$AVG
2014-07-19 09:48:53 ----HD---- C:\WINDOWS\ELAMBKUP
2014-07-19 09:44:46 ----RD---- C:\Program Files
2014-07-19 09:44:46 ----D---- C:\ProgramData\AVAST Software
2014-07-15 21:29:10 ----RD---- C:\WINDOWS\ToastData
2014-07-15 21:29:09 ----D---- C:\WINDOWS\WinStore
2014-07-15 21:29:06 ----D---- C:\Program Files\Internet Explorer
2014-07-15 21:29:06 ----D---- C:\Program Files (x86)\Internet Explorer
2014-07-15 16:55:12 ----D---- C:\WINDOWS\system32\MRT
2014-07-15 16:50:18 ----A---- C:\WINDOWS\system32\MRT.exe
2014-07-15 16:46:23 ----D---- C:\Program Files\Windows Journal

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

R0 aswRvrt;avast! Revert; C:\WINDOWS\system32\drivers\aswRvrt.sys [2014-07-19 65776]
R0 aswVmm;avast! VM Monitor; C:\WINDOWS\system32\drivers\aswVmm.sys [2014-07-19 224896]
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 aswKbd;aswKbd; C:\WINDOWS\system32\drivers\aswKbd.sys [2014-07-19 28184]
R1 aswRdr;aswRdr; C:\WINDOWS\system32\drivers\aswRdr2.sys [2014-07-19 93568]
R1 aswSnx;aswSnx; C:\WINDOWS\system32\drivers\aswSnx.sys [2014-07-19 1041168]
R1 aswSP;aswSP; C:\WINDOWS\system32\drivers\aswSP.sys [2014-07-19 427360]
R1
RapportCerberus_59849;RapportCerberus_59849; \??\C:\ProgramData\Trusteer\Rapport\store\exts\RapportCerberus\ba
seline\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 aswMonFlt;aswMonFlt; C:\WINDOWS\system32\drivers\aswMonFlt.sys [2014-07-19 79184]
R2 aswStm;aswStm; C:\WINDOWS\system32\drivers\aswStm.sys [2014-07-19 92008]
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-apparaat (Personal Area Network);
C:\WINDOWS\system32\DRIVERS\bthpan.sys [2013-08-22 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-apparaat (RFCOMM Protocol TDI);
C:\WINDOWS\system32\DRIVERS\rfcomm.sys [2014-03-18 167424]
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]
S3 BTHPORT;@bth.inf,%BTHPORT.SvcDesc%;Stuurprogramma voor Bluetooth-poort;
C:\WINDOWS\System32\Drivers\BTHport.sys [2014-05-18 1200128]
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 [2013-12-21 65432]
R2 Apple Mobile Device;Apple Mobile Device; C:\Program Files (x86)\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe [2013-09-07 55624]
R2 AtherosSvc;AtherosSvc; C:\Program Files (x86)\Qualcomm Atheros\Bluetooth Suite\adminservice.exe [2013-01-28 227456]
R2 avast! Antivirus;avast! Antivirus; C:\Program Files\AVAST Software\Avast\AvastSvc.exe [2014-07-19 50344]
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 [2014-07-19 2356912]
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 RapportMgmtService;Rapport Management Service; C:\Program Files (x86)\Trusteer\Rapport\bin\RapportMgmtService.exe [2013-12-21 1444120]
S3 AdobeFlashPlayerUpdateSvc;Adobe Flash Player Update Service; C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe [2014-07-08 262320]
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----------