ï»¿Logfile of random's system information tool 1.10 (written by random/random)
Run by computer at 2016-01-29 19:20:27
Microsoft Windows 10 Home
System drive C: has 389 GB (86%) free of 454 GB
Total RAM: 3912 MB (45% free)

Logfile of Trend Micro HijackThis v2.0.4
Scan saved at 19:20:34, on 29-1-2016
Platform: Unknown Windows (WinNT 6.02.1008)
MSIE: Internet Explorer v11.0 (11.00.10586.0020)
Boot mode: Normal

Running processes:
C:\Program Files (x86)\Launch Manager\LManager.exe
C:\Program Files (x86)\Trusteer\Rapport\bin\RapportService.exe
C:\Users\computer\AppData\Local\Microsoft\OneDrive\OneDrive.exe
C:\Program Files (x86)\NTI\Acer Backup Manager\BackupManagerTray.exe
C:\Program Files (x86)\Adobe\Acrobat DC\Acrobat\acrotray.exe
C:\Program Files (x86)\CyberLink\MediaEspresso\DeviceDetector\DeviceDetector.exe
C:\Program Files\WindowsApps\Microsoft.Messaging_2.13.20000.0_x86__8wekyb3d8bbwe\SkypeHost.exe
C:\Program Files (x86)\McAfee\SiteAdvisor\McChHost.exe
C:\Program Files\trend micro\computer.exe

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = http://acer13.msn.com
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Default_Search_URL = http://go.microsoft.com/fwlink/?LinkId=54896
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar = http://go.microsoft.com/fwlink/?LinkId=54896
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft.com/fwlink/?LinkId=54896
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
R1 - HKCU\Software\Microsoft\Internet Explorer\Search,Default_Search_URL = http://go.microsoft.com/fwlink/?LinkId=54896
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 =
R3 - URLSearchHook: McAfee SiteAdvisor Toolbar - {0EBBBE48-BAD4-4B4C-8E5A-516ABECAE064} - c:\PROGRA~2\mcafee\SITEAD~1\mcieplg.dll
F2 - REG:system.ini: UserInit=
O2 - BHO: Google Toolbar Helper - {AA58ED58-01DD-4d91-8333-CF10577473F7} - C:\Program Files (x86)\Google\Google Toolbar\GoogleToolbar_32.dll
O2 - BHO: Adobe Acrobat Create PDF Helper - {AE7CD045-E861-484f-8273-0445EE161910} - C:\Program Files (x86)\Common Files\Adobe\Acrobat\WCIEActiveX\DC\AcroIEFavStub.dll
O2 - BHO: SkypeIEPluginBHO - {AE805869-2E5C-4ED4-8F7B-F1F7851A4497} - C:\Program Files (x86)\Skype\Toolbars\Internet Explorer\SkypeIEPlugin.dll
O2 - BHO: SmartSelect - {F4971EE7-DAA0-4053-9964-665D8EE6A077} - C:\Program Files (x86)\Common Files\Adobe\Acrobat\WCIEActiveX\DC\AcroIEFavStub.dll
O3 - Toolbar: Google Toolbar - {2318C2B1-4965-11d4-9B18-009027A5CD4F} - C:\Program Files (x86)\Google\Google Toolbar\GoogleToolbar_32.dll
O3 - Toolbar: Adobe Acrobat Create PDF Toolbar - {47833539-D0C5-4125-9FA8-0819E2EAAC93} - C:\Program Files (x86)\Common Files\Adobe\Acrobat\WCIEActiveX\DC\AcroIEFavStub.dll
O4 - HKLM\..\Run: [Norton Online Backup] C:\Program Files (x86)\Symantec\Norton Online Backup\NOBuClient.exe
O4 - HKLM\..\Run: [Acrobat Assistant 8.0] "C:\Program Files (x86)\Adobe\Acrobat DC\Acrobat\Acrotray.exe"
O4 - HKCU\..\Run: [Google Update] "C:\Users\computer\AppData\Local\Google\Update\GoogleUpdate.exe" /c
O4 - HKCU\..\Run: [OneDrive] "C:\Users\computer\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
O4 - HKCU\..\Run: [Skype] "C:\Program Files (x86)\Skype\Phone\Skype.exe" /minimized /regrun
O4 - HKCU\..\Run: [Adobe Acrobat Synchronizer] "C:\Program Files (x86)\Adobe\Acrobat DC\Acrobat\AdobeCollabSync.exe"
O4 - HKCU\..\Run: [CCleaner Monitoring] "C:\Program Files\CCleaner\CCleaner64.exe" /MONITOR

O4 - HKCU\..\RunOnce: [Uninstall C:\Users\computer\AppData\Local\Microsoft\OneDrive\17.3.6201.1019_1\amd64] C:\WINDOWS\system32\cmd.exe /q /c rmdir /s /q "C:\Users\computer\AppData\Local\Microsoft\OneDrive\17.3.6201.1019_1\amd64"
O4 - HKUS\S-1-5-19\..\Run: [OneDriveSetup] C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup (User 'LOCAL SERVICE')
O4 - HKUS\S-1-5-20\..\Run: [OneDriveSetup] C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup (User 'NETWORK SERVICE')
O4 - Global Startup: Acer Backup Manager Tray.lnk = C:\Program Files (x86)\NTI\Acer Backup Manager\BackupManagerTray.exe
O8 - Extra context menu item: Add to Google Photos Screensa&ver - res://C:\WINDOWS\system32\GPhotos.scr/200
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: dssrequest - {5513F07E-936B-4E52-9B00-067394E91CC5} - c:\PROGRA~2\mcafee\SITEAD~1\mcieplg.dll
O18 - Protocol: sacore - {5513F07E-936B-4E52-9B00-067394E91CC5} - c:\PROGRA~2\mcafee\SITEAD~1\mcieplg.dll
O18 - Protocol: skypec2c - {91774881-D725-4E58-B298-07617B9B86A8} - C:\Program Files (x86)\Skype\Toolbars\Internet Explorer\SkypeIEPlugin.dll
O18 - Protocol: tbauth - {14654CA6-5711-491D-B89A-58E571679951} - C:\Windows\SysWOW64\tbauth.dll
O18 - Protocol: windows.tbauth - {14654CA6-5711-491D-B89A-58E571679951} - C:\Windows\SysWOW64\tbauth.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: Adobe Genuine Software Integrity Service (AGSService) - Adobe Systems, Incorporated - C:\Program Files (x86)\Common Files\Adobe\AdobeGCClient\AGSService.exe
O23 - Service: @%SystemRoot%\system32\Alg.exe,-112 (ALG) - Unknown owner - C:\WINDOWS\System32\alg.exe (file missing)
O23 - Service: @oem1.inf,%HidMonitor.SvcDisp%;Alps HID Monitor Service (ApHidMonitorService) - Alps Electric Co., Ltd. - C:\Program Files\Apoint2K\HidMonitorSvc.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: @%SystemRoot%\system32\DiagSvcs\DiagnosticsHub.StandardCollector.ServiceRes.dll,-1000 (diagnosticshub.standardcollector.service) - Unknown owner - C:\WINDOWS\system32\DiagSvcs\DiagnosticsHub.StandardCollector.Service.exe (file missing)
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: EgisTec Ticket Service - Egis Technology Inc. - C:\Program Files (x86)\Common Files\EgisTec\Services\EgisTicketService.exe
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: GamesAppService - WildTangent, Inc. - C:\Program Files (x86)\WildTangent Games\App\GamesAppService.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 Software Updater (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: MBAMService - Malwarebytes - C:\Program Files (x86)\Malwarebytes Anti-Malware\mbamservice.exe
O23 - Service: McAfee SiteAdvisor Service - McAfee, Inc. - C:\Program Files (x86)\McAfee\SiteAdvisor\McSACore.exe
O23 - Service: Mozilla Maintenance Service (MozillaMaintenance) - Mozilla Foundation - C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe
O23 - Service: @comres.dll,-2797 (MSDTC) - Unknown owner - C:\WINDOWS\System32\msdtc.exe (file missing)
O23 - Service: @%SystemRoot%\System32\netlogon.dll,-102 (Netlogon) - Unknown owner - C:\WINDOWS\system32\lsass.exe (file missing)
O23 - Service: Norton Online Backup (NOBU) - Symantec Corporation - C:\Program Files (x86)\Symantec\Norton Online Backup\NOBuAgent.exe
O23 - Service: NTI IScheduleSvc - NTI Corporation - C:\Program Files (x86)\NTI\Acer Backup Manager\IScheduleSvc.exe
O23 - Service: Rapport Management Service (RapportMgmtService) - IBM Corp. - 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: Samsung UPD Utility Service (SamsungUPDUtilSvc) - Unknown owner - C:\WINDOWS\SysWOW64\SecUPDUtilSvc.exe
O23 - Service: @%SystemRoot%\system32\SensorDataService.exe,-101 (SensorDataService) - Unknown owner - C:\WINDOWS\System32\SensorDataService.exe (file missing)
O23 - Service: Skype Updater (SkypeUpdate) - Skype Technologies - C:\Program Files (x86)\Skype\Updater\Updater.exe
O23 - Service: @%SystemRoot%\system32\snmptrap.exe,-3 (SNMPTRAP) - Unknown owner - C:\WINDOWS\System32\snmptrap.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 10 (TeamViewer) - TeamViewer GmbH - C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe
O23 - Service: @%SystemRoot%\system32\TieringEngineService.exe,-702 (TieringEngineService) - Unknown owner - C:\WINDOWS\system32\TieringEngineService.exe (file missing)
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 - 13235 bytes

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

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 LocalSystemNetworkRestricted
C:\WINDOWS\system32\svchost.exe -k LocalServiceAndNoImpersonation
C:\WINDOWS\system32\svchost.exe -k LocalService
"C:\Program Files (x86)\Trusteer\Rapport\bin\RapportMgmtService.exe"
C:\WINDOWS\system32\svchost.exe -k LocalServiceNoNetwork
C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted
C:\WINDOWS\system32\svchost.exe -k netsvcs
C:\WINDOWS\system32\svchost.exe -k NetworkService
C:\WINDOWS\System32\spoolsv.exe
C:\WINDOWS\System32\svchost.exe -k utcsvc
"C:\Program Files\Apoint2K\HidMonitorSvc.exe"
"C:\Program Files (x86)\Launch Manager\dsiwmis.exe"
"C:\Program Files (x86)\Acer\Acer Cloud\CCDMonitorService.exe"
"C:\Program Files (x86)\Skype\Toolbars\AutoUpdate\SkypeC2CAutoUpdateSvc.exe" /service
"C:\Program Files (x86)\Skype\Toolbars\PNRSvc\SkypeC2CPNRSvc.exe" /service
"C:\Program Files\Intel\iCLS Client\HeciServer.exe"
"C:\Program Files (x86)\IObit\LiveUpdate\LiveUpdate.exe"
"C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe"
"C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\DAL\jhi_service.exe"
"C:\Program Files (x86)\McAfee\SiteAdvisor\McSACore.exe"
"C:\Program Files (x86)\Symantec\Norton Online Backup\NOBuAgent.exe" SERVICE
C:\Windows\RfBtnSvc64.exe
C:\WINDOWS\SysWOW64\SecUPDUtilSvc.exe
"C:\Program Files (x86)\NTI\Acer Backup Manager\IScheduleSvc.exe"
"C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe"

C:\WINDOWS\system32\svchost.exe -k imgsvc
"C:\Program Files (x86)\Common Files\Adobe\AdobeGCClient\AGSService.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)\Google\Update\1.3.29.1\GoogleCrashHandler.exe"
"C:\Program Files (x86)\Google\Update\1.3.29.1\GoogleCrashHandler64.exe"
C:\WINDOWS\system32\SearchIndexer.exe /Embedding
"C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\UNS\UNS.exe"
C:\WINDOWS\system32\svchost.exe -k appmodel
C:\WINDOWS\system32\wbem\wmiprvse.exe
"C:\Program Files\Acer\Acer Power Management\ePowerSvc.exe"
dashost.exe {a035abbd-f7a8-4901-9e19dd220e7559b3}

C:\WINDOWS\System32\WinLogon.exe -SpecialSession
"dwm.exe"
C:\WINDOWS\system32\wbem\wmiprvse.exe
"C:\Program Files\Apoint2K\Apoint.exe"
"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
sihost.exe
taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}
C:\WINDOWS\Explorer.EXE
"C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\RemindersServer.exe"
-ServerName:RemindersServer
"C:\Program Files\Apoint2K\ApMsgFwd.exe" -s{05FA8492-C047-4207-BE65-780D8591C113}
"Apntex.exe"
"C:\Program Files\Apoint2K\HidFind.exe"
C:\Windows\System32\RuntimeBroker.exe -Embedding
\??\C:\WINDOWS\system32\conhost.exe 0x4
"C:\Program Files (x86)\Launch Manager\LManager.exe"
"C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe"
-ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca
C:\WINDOWS\system32\wbem\unsecapp.exe -Embedding
"C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe"
-ServerName:CortanaUI.AppXa50dqqa5gqv4a428c9y1jjw7m3btvepj.mca
"C:\Program Files (x86)\Launch Manager\MMDx64Fx.exe"
"C:\Program Files (x86)\Trusteer\Rapport\bin\RapportService.exe" -servicelaunch=true
"C:\WINDOWS\system32\igfxext.exe" -Embedding
C:\WINDOWS\system32\ApplicationFrameHost.exe -Embedding
C:\WINDOWS\system32\SettingSyncHost.exe -Embedding
"C:\Windows\System32\igfxtray.exe"
"C:\Windows\System32\hkcmd.exe"
"C:\Windows\System32\igfxpers.exe"
"C:\Program Files\Common Files\Common Desktop Agent\CDASrv.exe"
"C:\Users\computer\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
"C:\Program Files (x86)\NTI\Acer Backup Manager\BackupManagerTray.exe" -h -k
"C:\Program Files (x86)\Adobe\Acrobat DC\Acrobat\acrotray.exe"
"C:\Program Files\Acer\Acer Power Management\ePowerTray.exe"
C:\WINDOWS\system32\wbem\unsecapp.exe -Embedding
"C:\Program Files\Acer\Acer Power Management\ePowerEvent.exe"
"C:\Program Files\CCleaner\CCleaner.exe" /MONITOR /uac
C:\WINDOWS\system32\wbem\unsecapp.exe -Embedding
"C:\Program Files (x86)\CyberLink\MediaEspresso\DeviceDetector\DeviceDetector.exe"
C:\WINDOWS\System32\svchost.exe -k UnistackSvcGroup
"C:\Program Files\WindowsApps\Microsoft.Messaging_2.13.20000.0_x86__8wekyb3d8bbwe\SkypeHost.exe"
-ServerName:SkypeHost.ServerServer
"C:\Program Files\EgisTec IPS\PMMUpdate.exe"
"C:\Program Files\EgisTec IPS\EgisUpdate.exe"
taskhostw.exe

C:\Windows\System32\InstallAgent.exe -Embedding
"C:\Program Files\Windows Defender\MpCmdRun.exe" SpyNetService -RestrictPrivileges -AccessKey C2C985D3-
8F25-36F1-FD01-4D34D2528F69 -Reinvoke
C:\WINDOWS\System32\svchost.exe -k swprv
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=watcher --main-thread-id=9816 --on-
initialized-event-handle=940 --parent-handle=944
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=gpu-process
--channel="6360.0.1775150793\892330409" --supports-dual-gpus=false --gpu-driver-bug-workarounds=2,24,52 --gpu-
vendor-id=0x8086 --gpu-device-id=0x0116 --gpu-driver-vendor="Intel Corporation" --gpu-driver-
version=9.17.10.4229 --ignored=" --type=renderer " /prefetch:822062411
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --lang=nl --force-
fieldtrials=AffiliationBasedMatching/EnabledThroughFieldTrial/AppBannerTriggering/Aggressive/*AsyncSetAsDefau
lt/EnabledFull/AutomaticTabDiscarding/Default/CaptivePortalInterstitial/Enabled/ChildAccountDetection/Disabled/*C
hromeSuggestions/Default/*ClientSideDetectionModel/Model0/*CrossDevicePromo/14DaySingleProfile/ExtensionDe
veloperModeWarning/Enabled/*ExtensionInstallVerification/Enforce/*GFE/Default/InstanceID/Enabled/*IntelligentSe
ssionRestore/Enabled2/*NetworkQualityEstimator/Enabled/*OmniboxBundledExperimentV1/Unused_2/PasswordBran
ding/Disabled/*PasswordGeneration/Disabled/*QUIC/EnabledNoId/ReportCertificateErrors/ShowAndPossiblySend/*R
esourcePriorities/Disabled/SHA1IdentityUIWarning/Enabled/SHA1ToolbarUIJanuary2016/Warning/SHA1ToolbarUIJ
anuary2017/Error/*SRTPromptFieldTrial/On/*SafeBrowsingIncidentReportingService/Default/SafeBrowsingReportPhi
shingErrorLink/Enabled/SafeBrowsingSocialEngineeringStrings/Enabled/SafeBrowsingUnverifiedDownloads/Disable

ByParameterMostSbTypes/SafeBrowsingUpdateFrequency/Default/SlimmingPaint/EnableSlimmingPaint/*TriggeredResetFieldTrial/On/*UMA-Dynamic-Uniformity-Trial/Group3/*UMA-Population-Restrict/normal/*UMA-Uniformity-Trial-100-Percent/group_01/*UMA-Uniformity-Trial-20-Percent/default/*UMA-Uniformity-Trial-50-Percent/group_01/*UseDelayAgnosticAEC/DefaultEnabled/*VarationsServiceControl/Interval_30min/WebRTC-LocalIPPermissionCheck/Default/WebRTC-PeerConnectionDTLS1.2/Enabled/ --extension-process --enable-webrtc-hw-h264-encoding --enable-offline-auto-reload --enable-offline-auto-reload-visible-only --enable-pinch --device-scale-factor=1 --num-raster-threads=2 --content-image-texture-target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553 --video-image-texture-target=3553 --channel="6360.2.1409881576\1292978760" --font-cache-shared-handle=3052 /prefetch:673131151
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --lang=nl --force-fieldtrials=AffiliationBasedMatching/EnabledThroughFieldTrial/AppBannerTriggering/Aggressive/*AsyncSetAsDefault/EnabledFull/AutomaticTabDiscarding/Default/CaptivePortalInterstitial/Enabled/ChildAccountDetection/Disabled/*ChromeSuggestions/Default/*ClientSideDetectionModel/Model0/*CrossDevicePromo/14DaySingleProfile/ExtensionDeveloperModeWarning/Enabled/*ExtensionInstallVerification/Enforce/*GFE/Default/InstanceID/Enabled/*IntelligentSessionRestore/Enabled2/*NetworkQualityEstimator/Enabled/*OmniboxBundledExperimentV1/Unused_2/PasswordBranding/Disabled/*PasswordGeneration/Disabled/*QUIC/EnabledNoId/ReportCertificateErrors/ShowAndPossiblySend/*ResourcePriorities/Disabled/SHA1IdentityUIWarning/Enabled/SHA1ToolbarUIJanuary2016/Warning/SHA1ToolbarUIJanuary2017/Error/*SRTPromptFieldTrial/On/*SafeBrowsingIncidentReportingService/Default/SafeBrowsingReportPhishingErrorLink/Enabled/SafeBrowsingSocialEngineeringStrings/Enabled/SafeBrowsingUnverifiedDownloads/Disable
ByParameterMostSbTypes/SafeBrowsingUpdateFrequency/Default/SlimmingPaint/EnableSlimmingPaint/*TriggeredResetFieldTrial/On/*UMA-Dynamic-Uniformity-Trial/Group3/*UMA-Population-Restrict/normal/*UMA-Uniformity-Trial-100-Percent/group_01/*UMA-Uniformity-Trial-20-Percent/default/*UMA-Uniformity-Trial-50-Percent/group_01/*UseDelayAgnosticAEC/DefaultEnabled/*VarationsServiceControl/Interval_30min/WebRTC-LocalIPPermissionCheck/Default/WebRTC-PeerConnectionDTLS1.2/Enabled/ --extension-process --enable-webrtc-hw-h264-encoding --enable-offline-auto-reload --enable-offline-auto-reload-visible-only --enable-pinch --device-scale-factor=1 --num-raster-threads=2 --content-image-texture-target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553 --video-image-texture-target=3553 --channel="6360.3.1481778925\1758865085" --font-cache-shared-handle=2952 /prefetch:673131151
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --lang=nl --force-fieldtrials=AffiliationBasedMatching/EnabledThroughFieldTrial/AppBannerTriggering/Aggressive/*AsyncSetAsDefault/EnabledFull/AutomaticTabDiscarding/Default/CaptivePortalInterstitial/Enabled/ChildAccountDetection/Disabled/*ChromeSuggestions/Default/*ClientSideDetectionModel/Model0/*CrossDevicePromo/14DaySingleProfile/ExtensionDeveloperModeWarning/Enabled/*ExtensionInstallVerification/Enforce/*GFE/Default/InstanceID/Enabled/*IntelligentSessionRestore/Enabled2/*NetworkQualityEstimator/Enabled/*OmniboxBundledExperimentV1/Unused_2/PasswordBranding/Disabled/*PasswordGeneration/Disabled/*QUIC/EnabledNoId/ReportCertificateErrors/ShowAndPossiblySend/*ResourcePriorities/Disabled/SHA1IdentityUIWarning/Enabled/SHA1ToolbarUIJanuary2016/Warning/SHA1ToolbarUIJanuary2017/Error/*SRTPromptFieldTrial/On/*SafeBrowsingIncidentReportingService/Default/SafeBrowsingReportPhishingErrorLink/Enabled/SafeBrowsingSocialEngineeringStrings/Enabled/SafeBrowsingUnverifiedDownloads/Disable
ByParameterMostSbTypes/SafeBrowsingUpdateFrequency/Default/SlimmingPaint/EnableSlimmingPaint/*TriggeredResetFieldTrial/On/*UMA-Dynamic-Uniformity-Trial/Group3/*UMA-Population-Restrict/normal/*UMA-Uniformity-Trial-100-Percent/group_01/*UMA-Uniformity-Trial-20-Percent/default/*UMA-Uniformity-Trial-50-Percent/group_01/*UseDelayAgnosticAEC/DefaultEnabled/*VarationsServiceControl/Interval_30min/WebRTC-LocalIPPermissionCheck/Default/WebRTC-PeerConnectionDTLS1.2/Enabled/ --extension-process --enable-webrtc-hw-h264-encoding --enable-offline-auto-reload --enable-offline-auto-reload-visible-only --enable-pinch --device-scale-factor=1 --num-raster-threads=2 --content-image-texture-target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553 --video-image-texture-target=3553 --channel="6360.4.1689463104\1415962907" --font-cache-shared-handle=3112 /prefetch:673131151
C:\WINDOWS\system32\cmd.exe /c "C:\Program Files (x86)\McAfee\SiteAdvisor\McChHost.exe" --parent-window=0 chrome-extension://fheoggkfdfchfphceeifdbepaooicaho/ < \\.\pipe\chrome.nativeMessaging.in.34570926c6889e54 > \\.\pipe\chrome.nativeMessaging.out.34570926c6889e54
\??\C:\WINDOWS\system32\conhost.exe 0x4
"C:\Program Files (x86)\McAfee\SiteAdvisor\McChHost.exe" --parent-window=0 chrome-extension://fheoggkfdfchfphceeifdbepaooicaho/
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --lang=nl --force-fieldtrials=AffiliationBasedMatching/EnabledThroughFieldTrial/AppBannerTriggering/Aggressive/*AsyncSetAsDefault/EnabledFull/AutomaticTabDiscarding/Default/CaptivePortalInterstitial/Enabled/ChildAccountDetection/Disabled/*ChromeSuggestions/Default/*ClientSideDetectionModel/Model0/*CrossDevicePromo/14DaySingleProfile/ExtensionDeveloperModeWarning/Enabled/*ExtensionInstallVerification/Enforce/*GFE/Default/InstanceID/Enabled/*IntelligentSessionRestore/Enabled2/*NetworkQualityEstimator/Enabled/*OmniboxBundledExperimentV1/Unused_2/PasswordBranding/Disabled/*PasswordGeneration/Disabled/*QUIC/EnabledNoId/ReportCertificateErrors/ShowAndPossiblySend/*ResourcePriorities/Disabled/SHA1IdentityUIWarning/Enabled/SHA1ToolbarUIJanuary2016/Warning/SHA1ToolbarUIJanuary2017/Error/*SRTPromptFieldTrial/On/*SafeBrowsingIncidentReportingService/Default/SafeBrowsingReportPhishingErrorLink/Enabled/SafeBrowsingSocialEngineeringStrings/Enabled/SafeBrowsingUnverifiedDownloads/Disable

ByParameterMostSbTypes/SafeBrowsingUpdateFrequency/Default/SlimmingPaint/EnableSlimmingPaint/*TriggeredResetFieldTrial/On/*UMA-Dynamic-Uniformity-Trial/Group3/*UMA-Population-Restrict/normal/*UMA-Uniformity-Trial-100-Percent/group_01/*UMA-Uniformity-Trial-20-Percent/default/*UMA-Uniformity-Trial-50-Percent/group_01/*UseDelayAgnosticAEC/DefaultEnabled/*VarationsServiceControl/Interval_30min/WebRTC-LocalIPPermissionCheck/Default/WebRTC-PeerConnectionDTLS1.2/Enabled/ --enable-offline-auto-reload --enable-offline-auto-reload-visible-only --enable-pinch --device-scale-factor=1 --num-raster-threads=2 --content-image-texture-target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553 --video-image-texture-target=3553 --channel="6360.5.926902612\790714753" --font-cache-shared-handle=5596 /prefetch:673131151

C:\WINDOWS\splwow64.exe 12288
"C:\Users\computer\Downloads\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\GoogleUpdateTaskUserS-1-5-21-2871391618-1465616402-3070090435-1001Core.job -
C:\Users\computer\AppData\Local\Google\Update\GoogleUpdate.exe# /c#
C:\WINDOWS\tasks\GoogleUpdateTaskUserS-1-5-21-2871391618-1465616402-3070090435-1001UA.job -
C:\Users\computer\AppData\Local\Google\Update\GoogleUpdate.exe# /ua /installsource scheduler#

=========Mozilla firefox=========

ProfilePath - C:\Users\computer\AppData\Roaming\Mozilla\Firefox\Profiles\212uzxmh.default

"{4ED1F68A-5463-4931-9384-8FFF5ED91D92}"=C:\Program Files (x86)\McAfee\SiteAdvisor\saffplg.xpi

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@adobe.com/FlashPlayer]
"Description"=AdobeÂ® FlashÂ® Player 20.0.0.286 Plugin
"Path"=C:\WINDOWS\SysWOW64\Macromed\Flash\NPSWF32_20_0_0_286.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@google.com/npPicasa3,version=3.0.0]
"Description"=Picasa3 plugin
"Path"=C:\Program Files (x86)\Google\Picasa3\npPicasa3.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@intel-webapi.intel.com/Intel WebAPI ipt;version=2.1.42]
"Description"=Intel IPT WebApi plugin
"Path"=C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\IPT\npIntelWebAPIIPT.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@intel-webapi.intel.com/Intel WebAPI updater]
"Description"=This plugin updates Intel WebAPI component
"Path"=C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\IPT\npIntelWebAPIUpdater.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@tools.google.com/Google Update;version=3]
"Description"=Google Update
"Path"=C:\Program Files (x86)\Google\Update\1.3.29.1\npGoogleUpdate3.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@tools.google.com/Google Update;version=9]
"Description"=Google Update
"Path"=C:\Program Files (x86)\Google\Update\1.3.29.1\npGoogleUpdate3.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@WildTangent.com/GamesAppPresence Detector,Version=1.0]
"Description"=WildTangent Games App V2 Presence Detector Plugin

"Path"=C:\Program Files (x86)\WildTangent Games\App\BrowserIntegration\Registered\0\NP_wtapp.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\Adobe Acrobat]
"Description"=Handles PDFs in-place in Firefox
"Path"=C:\Program Files (x86)\Adobe\Acrobat DC\Acrobat\Air\nppdf32.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\Adobe Reader]
"Description"=Handles PDFs in-place in Firefox
"Path"=C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AIR\nppdf32.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\adobe.com/AdobeAAMDetect]
"Description"=
"Path"=C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\CCM\Utilities\npAdobeAAMDetect32.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\MozillaPlugins\@adobe.com/FlashPlayer]
"Description"=AdobeÂ® FlashÂ® Player 20.0.0.286 Plugin
"Path"=C:\WINDOWS\system32\Macromed\Flash\NPSWF64_20_0_0_286.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\MozillaPlugins\adobe.com/AdobeAAMDetect]
"Description"=
"Path"=C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\CCM\Utilities\npAdobeAAMDetect64.dll

C:\Users\computer\AppData\Roaming\Mozilla\Firefox\Profiles\212uzxmh.default\extensions\
staged
{5384767E-00D9-40E9-B72F-9CC39D655D6F}

C:\Users\computer\AppData\Roaming\Mozilla\Firefox\Profiles\212uzxmh.default\searchplugins\
McSiteAdvisor.xml

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

[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 [2012-11-10 64640]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\
{AA58ED58-01DD-4d91-8333-CF10577473F7}]
Google Toolbar Helper - C:\Program Files (x86)\Google\Google Toolbar\GoogleToolbar_64.dll [2015-12-25 256456]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\
{AE7CD045-E861-484f-8273-0445EE161910}]
Adobe Acrobat Create PDF Helper - C:\Program Files (x86)\Common
Files\Adobe\Acrobat\WCIEActiveX\DC\x64\AcroIEFavStub.dll [2015-09-30 171704]

[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 [2016-01-08 2134656]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\
{F4971EE7-DAA0-4053-9964-665D8EE6A077}]
Adobe Acrobat Create PDF from Selection - C:\Program Files (x86)\Common
Files\Adobe\Acrobat\WCIEActiveX\DC\x64\AcroIEFavStub.dll [2015-09-30 171704]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser
Helper Objects\{AA58ED58-01DD-4d91-8333-CF10577473F7}]
Google Toolbar Helper - C:\Program Files (x86)\Google\Google Toolbar\GoogleToolbar_32.dll [2015-12-25 194504]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser
Helper Objects\{AE7CD045-E861-484f-8273-0445EE161910}]
Adobe Acrobat Create PDF Helper - C:\Program Files (x86)\Common

Files\Adobe\Acrobat\WCIEActiveX\DC\AcroIEFavStub.dll [2015-09-30 141496]

[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 [2016-01-08 1725056]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{F4971EE7-DAA0-4053-9964-665D8EE6A077}]
Adobe Acrobat Create PDF from Selection - C:\Program Files (x86)\Common Files\Adobe\Acrobat\WCIEActiveX\DC\AcroIEFavStub.dll [2015-09-30 141496]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Toolbar]
{2318C2B1-4965-11d4-9B18-009027A5CD4F} - Google Toolbar - C:\Program Files (x86)\Google\Google Toolbar\GoogleToolbar_64.dll [2015-12-25 256456]
{47833539-D0C5-4125-9FA8-0819E2EAAC93} - Adobe Acrobat Create PDF Toolbar - C:\Program Files (x86)\Common Files\Adobe\Acrobat\WCIEActiveX\DC\x64\AcroIEFavStub.dll [2015-09-30 171704]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Internet Explorer\Toolbar]
{2318C2B1-4965-11d4-9B18-009027A5CD4F} - Google Toolbar - C:\Program Files (x86)\Google\Google Toolbar\GoogleToolbar_32.dll [2015-12-25 194504]
{47833539-D0C5-4125-9FA8-0819E2EAAC93} - Adobe Acrobat Create PDF Toolbar - C:\Program Files (x86)\Common Files\Adobe\Acrobat\WCIEActiveX\DC\AcroIEFavStub.dll [2015-09-30 141496]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
"IgfxTray"=C:\WINDOWS\system32\igfxtray.exe [2015-06-01 183216]
"HotKeysCmds"=C:\WINDOWS\system32\hkcmd.exe [2015-06-01 411056]
"Persistence"=C:\WINDOWS\system32\igfxpers.exe [2015-06-01 453552]
"Apoint"=C:\Program Files\Apoint2K\Apoint.exe [2015-10-04 706440]
"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]
"CDAServer"=C:\Program Files\Common Files\Common Desktop Agent\CDASrv.exe [2014-09-08 464608]
"AdobeAAMUpdater-1.0"=C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\UWA\UpdaterStartupUtility.exe [2015-10-30 508104]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"Google Update"=C:\Users\computer\AppData\Local\Google\Update\GoogleUpdate.exe [2015-09-13 144200]
"OneDrive"=C:\Users\computer\AppData\Local\Microsoft\OneDrive\OneDrive.exe [2016-01-27 551112]
"Skype"=C:\Program Files (x86)\Skype\Phone\Skype.exe [2015-11-17 50137728]
"Adobe Acrobat Synchronizer"=C:\Program Files (x86)\Adobe\Acrobat DC\Acrobat\AdobeCollabSync.exe [2015-12-18 881336]
"CCleaner Monitoring"=C:\Program Files\CCleaner\CCleaner64.exe [2015-12-08 8590760]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
"Uninstall C:\Users\computer\AppData\Local\Microsoft\OneDrive\17.3.6201.1019_1\amd64"=C:\WINDOWS\system32\cmd.exe [2015-10-30 233984]

[HKEY_LOCAL_MACHINE\Software\wow6432node\Microsoft\Windows\CurrentVersion\Run]
"LManager"= []
"Norton Online Backup"=C:\Program Files (x86)\Symantec\Norton Online Backup\NOBuClient.exe [2012-08-15 2994880]
"Acrobat Assistant 8.0"=C:\Program Files (x86)\Adobe\Acrobat DC\Acrobat\Acrotray.exe [2015-12-18 1867448]
""= []

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Acer Backup Manager Tray.lnk - C:\Program Files (x86)\NTI\Acer Backup Manager\BackupManagerTray.exe

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\igfxcui]
C:\WINDOWS\system32\igfxdev.dll [2015-06-01 451584]

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\CoreMessagingRegistrar]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\iai2c.sys]

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\StateRepository]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\TileDataModelSvc]

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\UserManager]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\Wdf01000.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{F2E7DD72-6468-4E36-B6F1-6488F42C1B52}]

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\CoreMessagingRegistrar]

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\StateRepository]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\TileDataModelSvc]

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\UserManager]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\Wdf01000.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{F2E7DD72-6468-4E36-B6F1-6488F42C1B52}]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"DSCAutomationHostEnabled"=2
"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]
"midimapper"=midimap.dll
"msacm.imaadpcm"=imaadp32.acm
"msacm.l3acm"=C:\Windows\System32\l3codeca.acm
"msacm.msadpcm"=msadp32.acm
"msacm.msg711"=msg711.acm
"msacm.msgsm610"=msgsm32.acm
"vidc.i420"=iyuv_32.dll
"vidc.iyuv"=iyuv_32.dll
"vidc.mrle"=msrle32.dll
"vidc.msvc"=msvidc32.dll
"vidc.uyvy"=msyuv.dll
"vidc.yuy2"=msyuv.dll
"vidc.yvu9"=tsbyuv.dll
"vidc.yvyu"=msyuv.dll

"wavemapper"=msacm32.drv
"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

======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======

2016-01-29 19:18:50 ----D---- C:\rsit
2016-01-29 14:28:35 ----HD---- C:\OneDriveTemp
2016-01-28 09:27:54 ----A---- C:\WINDOWS\SYSWOW64\Windows.Media.Protection.PlayReady.dll
2016-01-28 09:27:52 ----A---- C:\WINDOWS\system32\Windows.Media.Protection.PlayReady.dll
2016-01-28 09:27:32 ----A---- C:\WINDOWS\system32\edgehtml.dll
2016-01-28 09:27:29 ----A---- C:\WINDOWS\SYSWOW64\edgehtml.dll
2016-01-28 09:27:26 ----A---- C:\WINDOWS\SYSWOW64\mshtml.dll
2016-01-28 09:27:24 ----A---- C:\WINDOWS\system32\mshtml.dll
2016-01-28 09:27:21 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.Xaml.dll
2016-01-28 09:27:17 ----A---- C:\WINDOWS\system32\Windows.UI.Xaml.dll
2016-01-28 09:27:16 ----A---- C:\WINDOWS\system32\windows.storage.dll
2016-01-28 09:27:15 ----A---- C:\WINDOWS\system32\twinui.dll
2016-01-28 09:27:14 ----A---- C:\WINDOWS\system32\ieframe.dll
2016-01-28 09:27:13 ----A---- C:\WINDOWS\SYSWOW64\windows.storage.dll
2016-01-28 09:27:12 ----A---- C:\WINDOWS\SYSWOW64\ieframe.dll
2016-01-28 09:27:10 ----A---- C:\WINDOWS\SYSWOW64\twinui.dll
2016-01-28 09:27:06 ----A---- C:\WINDOWS\system32\shell32.dll
2016-01-28 09:27:04 ----A---- C:\WINDOWS\SYSWOW64\mos.dll
2016-01-28 09:27:03 ----A---- C:\WINDOWS\system32\d2d1.dll
2016-01-28 09:27:02 ----A---- C:\WINDOWS\system32\mos.dll
2016-01-28 09:27:00 ----A---- C:\WINDOWS\SYSWOW64\shell32.dll
2016-01-28 09:26:53 ----A---- C:\WINDOWS\SYSWOW64\BingMaps.dll
2016-01-28 09:26:51 ----A---- C:\WINDOWS\SYSWOW64\d2d1.dll
2016-01-28 09:26:50 ----A---- C:\WINDOWS\system32\dwmcore.dll
2016-01-28 09:26:50 ----A---- C:\WINDOWS\system32\audiosrv.dll
2016-01-28 09:26:49 ----A---- C:\WINDOWS\system32\InputService.dll
2016-01-28 09:26:48 ----A---- C:\WINDOWS\system32\WpcMon.exe
2016-01-28 09:26:46 ----A---- C:\WINDOWS\SYSWOW64\InputService.dll
2016-01-28 09:26:46 ----A---- C:\WINDOWS\system32\BingMaps.dll
2016-01-28 09:26:45 ----A---- C:\WINDOWS\SYSWOW64\dwmcore.dll
2016-01-28 09:26:45 ----A---- C:\WINDOWS\system32\drivers\dxgkrnl.sys
2016-01-28 09:26:44 ----A---- C:\WINDOWS\system32\wlidsvc.dll
2016-01-28 09:26:44 ----A---- C:\WINDOWS\system32\NetworkMobileSettings.dll
2016-01-28 09:26:43 ----A---- C:\WINDOWS\system32\winhttp.dll
2016-01-28 09:26:42 ----A---- C:\WINDOWS\system32\RecoveryDrive.exe
2016-01-28 09:26:41 ----A---- C:\WINDOWS\SYSWOW64\winhttp.dll
2016-01-28 09:26:41 ----A---- C:\WINDOWS\SYSWOW64\msctf.dll
2016-01-28 09:26:41 ----A---- C:\WINDOWS\system32\aeinv.dll
2016-01-28 09:26:40 ----A---- C:\WINDOWS\SYSWOW64\mfsvr.dll
2016-01-28 09:26:40 ----A---- C:\WINDOWS\system32\msctf.dll
2016-01-28 09:26:40 ----A---- C:\WINDOWS\system32\MapsStore.dll
2016-01-28 09:26:40 ----A---- C:\WINDOWS\system32\AudioSes.dll
2016-01-28 09:26:39 ----A---- C:\WINDOWS\SYSWOW64\quartz.dll
2016-01-28 09:26:39 ----A---- C:\WINDOWS\SYSWOW64\AudioSes.dll
2016-01-28 09:26:38 ----A---- C:\WINDOWS\system32\wifinetworkmanager.dll

2016-01-28 09:26:38 ----A---- C:\WINDOWS\system32\mfsvr.dll
2016-01-28 09:26:37 ----A---- C:\WINDOWS\system32\SmsRouterSvc.dll
2016-01-28 09:26:37 ----A---- C:\WINDOWS\system32\SensorsApi.dll
2016-01-28 09:26:37 ----A---- C:\WINDOWS\system32\msfeeds.dll
2016-01-28 09:26:36 ----A---- C:\WINDOWS\system32\wscsvc.dll
2016-01-28 09:26:36 ----A---- C:\WINDOWS\system32\quartz.dll
2016-01-28 09:26:36 ----A---- C:\WINDOWS\system32\CredProvDataModel.dll
2016-01-28 09:26:35 ----A---- C:\WINDOWS\SYSWOW64\SensorsApi.dll
2016-01-28 09:26:35 ----A---- C:\WINDOWS\SYSWOW64\msfeeds.dll
2016-01-28 09:26:35 ----A---- C:\WINDOWS\system32\MTFServer.dll
2016-01-28 09:26:35 ----A---- C:\WINDOWS\system32\drivers\http.sys
2016-01-28 09:26:35 ----A---- C:\WINDOWS\system32\audiodg.exe
2016-01-28 09:26:34 ----A---- C:\WINDOWS\system32\wbiosrvc.dll
2016-01-28 09:26:34 ----A---- C:\WINDOWS\system32\MTF.dll
2016-01-28 09:26:33 ----A---- C:\WINDOWS\SYSWOW64\MTF.dll
2016-01-28 09:26:33 ----A---- C:\WINDOWS\SYSWOW64\CredProvDataModel.dll
2016-01-28 09:26:33 ----A---- C:\WINDOWS\system32\WWanAPI.dll
2016-01-28 09:26:32 ----A---- C:\WINDOWS\SYSWOW64\iedkcs32.dll
2016-01-28 09:26:32 ----A---- C:\WINDOWS\SYSWOW64\evr.dll
2016-01-28 09:26:31 ----A---- C:\WINDOWS\SYSWOW64\WWanAPI.dll
2016-01-28 09:26:31 ----A---- C:\WINDOWS\SYSWOW64\DisplayManager.dll
2016-01-28 09:26:31 ----A---- C:\WINDOWS\system32\StorSvc.dll
2016-01-28 09:26:31 ----A---- C:\WINDOWS\system32\srcore.dll
2016-01-28 09:26:31 ----A---- C:\WINDOWS\system32\drivers\dxgmms2.sys
2016-01-28 09:26:30 ----A---- C:\WINDOWS\SYSWOW64\SimCfg.dll
2016-01-28 09:26:30 ----A---- C:\WINDOWS\SYSWOW64\rastls.dll
2016-01-28 09:26:30 ----A---- C:\WINDOWS\SYSWOW64\rasdlg.dll
2016-01-28 09:26:30 ----A---- C:\WINDOWS\system32\SimCfg.dll
2016-01-28 09:26:29 ----A---- C:\WINDOWS\system32\Windows.Networking.UX.EapRequestHandler.dll
2016-01-28 09:26:29 ----A---- C:\WINDOWS\system32\services.exe
2016-01-28 09:26:28 ----A---- C:\WINDOWS\SYSWOW64\SimAuth.dll
2016-01-28 09:26:28 ----A---- C:\WINDOWS\system32\SimAuth.dll
2016-01-28 09:26:28 ----A---- C:\WINDOWS\system32\rasapi32.dll
2016-01-28 09:26:28 ----A---- C:\WINDOWS\system32\iedkcs32.dll
2016-01-28 09:26:27 ----A---- C:\WINDOWS\SYSWOW64\TextInputFramework.dll
2016-01-28 09:26:27 ----A---- C:\WINDOWS\system32\wscapi.dll
2016-01-28 09:26:27 ----A---- C:\WINDOWS\system32\SMSRouter.dll
2016-01-28 09:26:27 ----A---- C:\WINDOWS\system32\rasdlg.dll
2016-01-28 09:26:27 ----A---- C:\WINDOWS\system32\ie4uinit.exe
2016-01-28 09:26:27 ----A---- C:\WINDOWS\system32\AudioEndpointBuilder.dll
2016-01-28 09:26:26 ----A---- C:\WINDOWS\system32\enterprisecsps.dll
2016-01-28 09:26:25 ----A---- C:\WINDOWS\SYSWOW64\rasapi32.dll
2016-01-28 09:26:25 ----A---- C:\WINDOWS\SYSWOW64\MapsBtSvc.dll
2016-01-28 09:26:25 ----A---- C:\WINDOWS\system32\DDDS.dll
2016-01-28 09:26:25 ----A---- C:\WINDOWS\system32\AUDIOKSE.dll
2016-01-28 09:26:24 ----A---- C:\WINDOWS\system32\wlidcli.dll
2016-01-28 09:26:24 ----A---- C:\WINDOWS\system32\MusUpdateHandlers.dll
2016-01-28 09:26:24 ----A---- C:\WINDOWS\system32\MapsBtSvc.dll
2016-01-28 09:26:24 ----A---- C:\WINDOWS\system32\ipnathlp.dll
2016-01-28 09:26:23 ----A---- C:\WINDOWS\SYSWOW64\AUDIOKSE.dll
2016-01-28 09:26:23 ----A---- C:\WINDOWS\system32\DisplayManager.dll
2016-01-28 09:26:22 ----A---- C:\WINDOWS\system32\win32kfull.sys
2016-01-28 09:26:21 ----A---- C:\WINDOWS\system32\rastls.dll
2016-01-28 09:26:21 ----A---- C:\WINDOWS\system32\evr.dll
2016-01-28 09:26:20 ----A---- C:\WINDOWS\system32\MusNotificationUx.exe
2016-01-28 09:26:20 ----A---- C:\WINDOWS\system32\MusNotification.exe
2016-01-28 09:26:20 ----A---- C:\WINDOWS\system32\invagent.dll
2016-01-28 09:26:20 ----A---- C:\WINDOWS\system32\devinv.dll
2016-01-28 09:26:19 ----A---- C:\WINDOWS\SYSWOW64\pcaui.exe
2016-01-28 09:26:19 ----A---- C:\WINDOWS\system32\TextInputFramework.dll
2016-01-28 09:26:19 ----A---- C:\WINDOWS\system32\pcaui.exe
2016-01-28 09:26:19 ----A---- C:\WINDOWS\system32\FilterDS.dll
2016-01-28 09:26:17 ----A---- C:\WINDOWS\system32\Windows.UI.Core.TextInput.dll

2016-01-28 09:26:17 ----A---- C:\WINDOWS\system32\rasautou.exe
2016-01-28 09:26:17 ----A---- C:\WINDOWS\system32\drivers\usbser.sys
2016-01-28 09:26:16 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.Core.TextInput.dll
2016-01-28 09:26:16 ----A---- C:\WINDOWS\SYSWOW64\rasautou.exe
2016-01-28 09:26:15 ----A---- C:\WINDOWS\SYSWOW64\wlidcli.dll
2016-01-28 09:26:15 ----A---- C:\WINDOWS\system32\sscoreext.dll
2016-01-28 09:26:15 ----A---- C:\WINDOWS\system32\rasadhlp.dll
2016-01-28 09:26:14 ----A---- C:\WINDOWS\SYSWOW64\winhttpcom.dll
2016-01-28 09:26:14 ----A---- C:\WINDOWS\system32\winhttpcom.dll
2016-01-28 09:26:14 ----A---- C:\WINDOWS\system32\winbio.dll
2016-01-28 09:26:14 ----A---- C:\WINDOWS\system32\reseteng.dll
2016-01-28 09:26:14 ----A---- C:\WINDOWS\system32\rasauto.dll
2016-01-28 09:26:13 ----A---- C:\WINDOWS\SYSWOW64\winbio.dll
2016-01-28 09:26:13 ----A---- C:\WINDOWS\SYSWOW64\rastlsext.dll
2016-01-28 09:26:13 ----A---- C:\WINDOWS\SYSWOW64\rasadhlp.dll
2016-01-28 09:26:13 ----A---- C:\WINDOWS\system32\rastlsext.dll
2016-01-26 10:32:35 ----D---- C:\SanDisk
2016-01-14 16:54:22 ----AD---- C:\Program Files\CCleaner
2016-01-13 17:25:32 ----SHD---- C:\Config.Msi
2016-01-13 11:19:40 ----D---- C:\Users\computer\AppData\Roaming\SolidDocuments
2016-01-13 11:09:20 ----D---- C:\ProgramData\regid.1986-12.com.adobe
2016-01-13 10:19:47 ----A---- C:\WINDOWS\SYSWOW64\mfcore.dll
2016-01-13 10:19:47 ----A---- C:\WINDOWS\system32\Windows.Media.dll
2016-01-13 10:19:47 ----A---- C:\WINDOWS\system32\mfcore.dll
2016-01-13 10:19:45 ----A---- C:\WINDOWS\SYSWOW64\Windows.Media.dll
2016-01-13 10:19:42 ----A---- C:\WINDOWS\SYSWOW64\mfnetsrc.dll
2016-01-13 10:19:42 ----A---- C:\WINDOWS\system32\ntoskrnl.exe
2016-01-13 10:19:42 ----A---- C:\WINDOWS\system32\mfnetsrc.dll
2016-01-13 10:19:41 ----A---- C:\WINDOWS\SYSWOW64\qdvd.dll
2016-01-13 10:19:41 ----A---- C:\WINDOWS\system32\qdvd.dll
2016-01-13 10:19:41 ----A---- C:\WINDOWS\system32\Chakra.dll
2016-01-13 10:19:40 ----A---- C:\WINDOWS\SYSWOW64\WWAHost.exe
2016-01-13 10:19:40 ----A---- C:\WINDOWS\SYSWOW64\mfps.dll
2016-01-13 10:19:40 ----A---- C:\WINDOWS\SYSWOW64\Chakra.dll
2016-01-13 10:19:40 ----A---- C:\WINDOWS\system32\WWAHost.exe
2016-01-13 10:19:40 ----A---- C:\WINDOWS\system32\wuaueng.dll
2016-01-13 10:19:40 ----A---- C:\WINDOWS\system32\usermgr.dll
2016-01-13 10:19:40 ----A---- C:\WINDOWS\system32\msxml6.dll
2016-01-13 10:19:40 ----A---- C:\WINDOWS\system32\mfps.dll
2016-01-13 10:19:39 ----A---- C:\WINDOWS\SYSWOW64\msxml6.dll
2016-01-13 10:19:39 ----A---- C:\WINDOWS\SYSWOW64\mfnetcore.dll
2016-01-13 10:19:39 ----A---- C:\WINDOWS\system32\WMADMOD.DLL
2016-01-13 10:19:39 ----A---- C:\WINDOWS\system32\mfnetcore.dll
2016-01-13 10:19:39 ----A---- C:\WINDOWS\system32\jscript9.dll
2016-01-13 10:19:39 ----A---- C:\WINDOWS\system32\generaltel.dll
2016-01-13 10:19:38 ----A---- C:\WINDOWS\SYSWOW64\WMADMOD.DLL
2016-01-13 10:19:38 ----A---- C:\WINDOWS\SYSWOW64\jscript9.dll
2016-01-13 10:19:38 ----A---- C:\WINDOWS\system32\WMSPDMOD.DLL
2016-01-13 10:19:38 ----A---- C:\WINDOWS\system32\facecredentialprovider.dll
2016-01-13 10:19:37 ----A---- C:\WINDOWS\SYSWOW64\WMSPDMOD.DLL
2016-01-13 10:19:37 ----A---- C:\WINDOWS\SYSWOW64\schannel.dll
2016-01-13 10:19:37 ----A---- C:\WINDOWS\SYSWOW64\gdi32.dll
2016-01-13 10:19:37 ----A---- C:\WINDOWS\system32\gdi32.dll
2016-01-13 10:19:37 ----A---- C:\WINDOWS\system32\DeviceCensus.exe
2016-01-13 10:19:36 ----A---- C:\WINDOWS\SYSWOW64\mftranscode.dll
2016-01-13 10:19:36 ----A---- C:\WINDOWS\SYSWOW64\MessagingDataModel2.dll
2016-01-13 10:19:36 ----A---- C:\WINDOWS\SYSWOW64\advapi32.dll
2016-01-13 10:19:36 ----A---- C:\WINDOWS\system32\WMALFXGFXDSP.dll
2016-01-13 10:19:36 ----A---- C:\WINDOWS\system32\winlogon.exe
2016-01-13 10:19:36 ----A---- C:\WINDOWS\system32\uReFS.dll
2016-01-13 10:19:36 ----A---- C:\WINDOWS\system32\schannel.dll
2016-01-13 10:19:36 ----A---- C:\WINDOWS\system32\PhoneService.dll
2016-01-13 10:19:36 ----A---- C:\WINDOWS\system32\MessagingDataModel2.dll

2016-01-13 10:19:36 ----A---- C:\WINDOWS\system32\appraiser.dll
2016-01-13 10:19:36 ----A---- C:\WINDOWS\system32\advapi32.dll
2016-01-13 10:19:35 ----A---- C:\WINDOWS\SYSWOW64\uReFS.dll
2016-01-13 10:19:35 ----A---- C:\WINDOWS\SYSWOW64\qedit.dll
2016-01-13 10:19:35 ----A---- C:\WINDOWS\SYSWOW64\MP3DMOD.DLL
2016-01-13 10:19:35 ----A---- C:\WINDOWS\system32\WMSPDMOE.DLL
2016-01-13 10:19:35 ----A---- C:\WINDOWS\system32\winload.exe
2016-01-13 10:19:35 ----A---- C:\WINDOWS\system32\usermgrcli.dll
2016-01-13 10:19:35 ----A---- C:\WINDOWS\system32\storewuauth.dll
2016-01-13 10:19:35 ----A---- C:\WINDOWS\system32\qedit.dll
2016-01-13 10:19:35 ----A---- C:\WINDOWS\system32\ProximityCommon.dll
2016-01-13 10:19:35 ----A---- C:\WINDOWS\system32\MP3DMOD.DLL
2016-01-13 10:19:35 ----A---- C:\WINDOWS\system32\mftranscode.dll
2016-01-13 10:19:35 ----A---- C:\WINDOWS\system32\drivers\bthport.sys
2016-01-13 10:19:34 ----A---- C:\WINDOWS\SYSWOW64\WMSPDMOE.DLL
2016-01-13 10:19:34 ----A---- C:\WINDOWS\SYSWOW64\vbscript.dll
2016-01-13 10:19:34 ----A---- C:\WINDOWS\SYSWOW64\UserMgrProxy.dll
2016-01-13 10:19:34 ----A---- C:\WINDOWS\SYSWOW64\usermgrcli.dll
2016-01-13 10:19:34 ----A---- C:\WINDOWS\SYSWOW64\ProximityCommon.dll
2016-01-13 10:19:34 ----A---- C:\WINDOWS\system32\vbscript.dll
2016-01-13 10:19:34 ----A---- C:\WINDOWS\system32\UserMgrProxy.dll
2016-01-13 10:19:34 ----A---- C:\WINDOWS\system32\RMSRoamingSecurity.dll
2016-01-13 10:19:34 ----A---- C:\WINDOWS\system32\omadmclient.exe
2016-01-13 10:19:34 ----A---- C:\WINDOWS\system32\DscCore.dll
2016-01-13 10:19:34 ----A---- C:\WINDOWS\system32\drivers\BthLEEnum.sys
2016-01-13 10:19:34 ----A---- C:\WINDOWS\system32\Chakradiag.dll
2016-01-13 10:19:34 ----A---- C:\WINDOWS\system32\aitstatic.exe
2016-01-13 10:19:34 ----A---- C:\WINDOWS\system32\aepic.dll

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

2016-01-29 19:20:30 ----D---- C:\Program Files\trend micro
2016-01-29 19:18:57 ----D---- C:\WINDOWS\Prefetch
2016-01-29 19:18:41 ----D---- C:\WINDOWS\Temp
2016-01-29 18:21:00 ----D---- C:\WINDOWS\system32\sru
2016-01-29 17:48:14 ----D---- C:\WINDOWS\system32\config
2016-01-29 17:45:26 ----D---- C:\WINDOWS\system32\DriverStore
2016-01-29 16:53:44 ----D---- C:\WINDOWS\Microsoft.NET
2016-01-29 16:16:45 ----D---- C:\ProgramData\boost_interprocess
2016-01-29 14:29:13 ----D---- C:\WINDOWS\AppReadiness
2016-01-29 14:17:42 ----HD---- C:\Program Files\WindowsApps
2016-01-28 14:00:35 ----D---- C:\WINDOWS\INF
2016-01-28 13:56:12 ----A---- C:\WINDOWS\SYSWOW64\log.txt
2016-01-28 13:54:25 ----D---- C:\WINDOWS\WinSxS
2016-01-28 13:52:50 ----D---- C:\Windows
2016-01-28 12:19:01 ----D---- C:\WINDOWS\SYSWOW64\migration
2016-01-28 12:19:01 ----AD---- C:\WINDOWS\SysWOW64
2016-01-28 12:19:00 ----D---- C:\WINDOWS\system32\WinBioPlugIns
2016-01-28 12:19:00 ----D---- C:\WINDOWS\system32\oobe
2016-01-28 12:19:00 ----D---- C:\WINDOWS\system32\migration
2016-01-28 12:18:59 ----SD---- C:\WINDOWS\system32\F12
2016-01-28 12:18:59 ----D---- C:\WINDOWS\system32\drivers
2016-01-28 12:18:59 ----D---- C:\WINDOWS\system32\appraiser
2016-01-28 12:18:59 ----D---- C:\WINDOWS\System32
2016-01-28 12:18:57 ----RD---- C:\WINDOWS\PurchaseDialog
2016-01-28 12:18:57 ----RD---- C:\WINDOWS\ImmersiveControlPanel
2016-01-28 12:18:56 ----D---- C:\WINDOWS\bcastdvr
2016-01-28 12:18:56 ----D---- C:\WINDOWS\AppPatch
2016-01-28 10:43:46 ----D---- C:\WINDOWS\CbsTemp
2016-01-28 09:14:20 ----D---- C:\WINDOWS\system32\catroot2
2016-01-26 10:33:46 ----A---- C:\WINDOWS\system32\PerfStringBackup.INI
2016-01-26 10:29:43 ----D---- C:\WINDOWS\system32\drivers\UMDF
2016-01-25 16:00:59 ----SHD---- C:\System Volume Information

2016-01-23 12:47:47 ----D---- C:\ProgramData\ProductData
2016-01-22 08:35:13 ----D---- C:\WINDOWS\debug
2016-01-21 08:37:52 ----D---- C:\WINDOWS\system32\LogFiles
2016-01-17 21:28:26 ----SHD---- C:\WINDOWS\Installer
2016-01-17 21:28:20 ----RD---- C:\Program Files (x86)\Skype
2016-01-16 15:16:30 ----RD---- C:\WINDOWS\assembly
2016-01-16 15:15:32 ----RSD---- C:\WINDOWS\Fonts
2016-01-16 15:15:32 ----AD---- C:\Program Files (x86)\OpenOffice 4
2016-01-15 13:46:51 ----D---- C:\WINDOWS\system32\Tasks
2016-01-14 17:03:55 ----DC---- C:\WINDOWS\Panther
2016-01-14 16:54:22 ----RD---- C:\Program Files
2016-01-14 12:05:43 ----SD---- C:\Users\computer\AppData\Roaming\Microsoft
2016-01-13 17:23:55 ----D---- C:\Program Files (x86)\McAfee
2016-01-13 13:02:42 ----D---- C:\WINDOWS\system32\Boot
2016-01-13 11:58:50 ----D---- C:\WINDOWS\system32\MRT
2016-01-13 11:49:03 ----A---- C:\WINDOWS\system32\MRT.exe
2016-01-13 11:17:15 ----D---- C:\Users\computer\AppData\Roaming\Adobe
2016-01-13 11:10:37 ----D---- C:\ProgramData\Adobe
2016-01-13 11:09:20 ----HD---- C:\ProgramData
2016-01-13 11:03:55 ----D---- C:\Program Files (x86)\Adobe
2016-01-06 08:08:10 ----D---- C:\WINDOWS\LiveKernelReports
2016-01-03 02:40:25 ----A---- C:\WINDOWS\SYSWOW64\FlashPlayerApp.exe

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

R0 iaStorA;iaStorA; C:\WINDOWS\System32\drivers\iaStorA.sys [2012-08-16 645952]
R0 RapportHades64;RapportHades64; C:\WINDOWS\System32\Drivers\RapportHades64.sys [2016-01-03 141304]
R0 RapportKE64;RapportKE64; C:\WINDOWS\System32\Drivers\RapportKE64.sys [2016-01-03 396152]
R1 ccSet_NARA;NARA Settings Manager; C:\WINDOWS\system32\drivers\NARAx64\0401000.00E\ccSetx64.sys [2012-05-26 168608]
R1 FileCrypt;@%systemroot%\system32\drivers\filecrypt.sys,-100; C:\WINDOWS\system32\drivers\filecrypt.sys [2015-10-30 87040]
R1 GpuEnergyDrv;@%SystemRoot%\system32\drivers\gpuenergydrv.sys,-100; C:\WINDOWS\System32\drivers\gpuenergydrv.sys [2015-10-30 8192]
R1 mwlPSDFilter;mwlPSDFilter; C:\WINDOWS\system32\DRIVERS\mwlPSDFilter.sys [2012-12-20 22648]
R1 mwlPSDNServ;mwlPSDNServ; C:\WINDOWS\system32\DRIVERS\mwlPSDNServ.sys [2012-12-20 20520]
R1 mwlPSDVDisk;mwlPSDVDisk; C:\WINDOWS\system32\DRIVERS\mwlPSDVDisk.sys [2012-12-20 62776]
R1 RapportCerberus_1507079;RapportCerberus_1507079; \??\C:\ProgramData\Trusteer\Rapport\store\exts\RapportCerberus\baseline\RapportCerberus64_1507079.sys [2015-12-09 961880]
R1 RapportEI64;RapportEI64; \??\C:\Program Files (x86)\Trusteer\Rapport\bin\x64\RapportEI64.sys [2016-01-03 503320]
R1 RapportPG64;RapportPG64; \??\C:\Program Files (x86)\Trusteer\Rapport\bin\x64\RapportPG64.sys [2016-01-03 496408]
R2 MMCSS;@%systemroot%\system32\drivers\mmcss.sys,-100; C:\WINDOWS\system32\drivers\mmcss.sys [2015-10-30 47616]
R2 SSPORT;SSPORT; \??\C:\WINDOWS\system32\Drivers\SSPORT.sys [2015-06-15 20336]
R2 storqosflt;@%SystemRoot%\System32\drivers\storqosflt.sys,-101; C:\WINDOWS\system32\drivers\storqosflt.sys [2015-10-30 78848]
R3 ApfiltrService;@oem1.inf,%Filter.SvcDesc%;Alps Pointing-device Filter Driver; C:\WINDOWS\system32\DRIVERS\Apfiltr.sys [2015-10-04 517992]
R3 athr;@athw8x.inf,%ATHR.Service.DispName%;Qualcomm Atheros Extensible Wireless LAN device driver; C:\WINDOWS\System32\drivers\athw8x.sys [2015-10-30 4207104]
R3 BTATH_BUS;@oem10.inf,%BTATH_BUS.SVCDESC%;Qualcomm Atheros Bluetooth Bus; C:\WINDOWS\System32\drivers\btath_bus.sys [2012-11-09 33944]
R3 BtFilter;BtFilter; C:\WINDOWS\system32\DRIVERS\btfilter.sys [2015-03-09 599240]
R3 BthEnum;@bth.inf,%BthEnum.SVCDESC%;Bluetooth Enumerator-service; C:\WINDOWS\System32\drivers\BthEnum.sys [2015-10-30 112640]
R3 BthLEEnum;@bthleenum.inf,%BthLEEnum.SVCDESC%;Bluetooth Low Energy Driver; C:\WINDOWS\System32\drivers\BthLEEnum.sys [2016-01-05 245760]
R3 BthPan;@bthpan.inf,%BthPan.DisplayName%;Bluetooth Device (Personal Area Network); C:\WINDOWS\System32\drivers\bthpan.sys [2015-10-30 128512]
R3 BTHUSB;@bth.inf,%BTHUSB.SvcDesc%;USB-stuurprogramma voor Bluetooth-radio;

C:\WINDOWS\System32\drivers\BTHUSB.sys [2015-10-30 84992]
R3 igfx;igfx; C:\WINDOWS\system32\DRIVERS\igdkmd64.sys [2015-06-01 5384176]
R3 IntcAzAudAddService;Service for Realtek HD Audio (WDM); C:\WINDOWS\system32\drivers\RTKVHD64.sys [2012-07-31 4102928]
R3 IntcDAud;@oem28.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 Miniport Driver for Qualcomm Atheros AR81xx PCI-E Ethernet Controller; C:\WINDOWS\System32\drivers\L1C63x64.sys [2015-10-30 121344]
R3 MBAMProtector;MBAMProtector; \??\C:\WINDOWS\system32\drivers\mbam.sys [2015-10-05 25816]
R3 MEIx64;@oem24.inf,%HECI_SvcDesc%;Intel(R) Management Engine Interface ;
C:\WINDOWS\System32\drivers\HECIx64.sys [2012-07-02 62784]
R3 mfesapsn;McAfee Process Start Notification Service; \??\C:\Program Files (x86)\McAfee\SiteAdvisor\x64\mfesapsn.sys [2015-12-29 37448]
R3 NTIDrvr;NTIDrvr; \??\C:\Windows\system32\drivers\NTIDrvr.sys [2010-04-20 18432]
R3 Ps2Kb2Hid;@oem12.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 [2015-10-30 175104]
R3 StillCam;@sti.inf,%StillCam.SvcDesc%;Stuurprogramma voor seriÃ«le digitale fotocamera;
C:\WINDOWS\system32\DRIVERS\serscan.sys [2015-10-30 12800]
R3 UBHelper;UBHelper; \??\C:\Windows\system32\drivers\UBHelper.sys [2010-07-09 17408]
S0 LSI_SAS2i;LSI_SAS2i; C:\WINDOWS\System32\drivers\lsi_sas2i.sys [2015-10-30 104800]
S0 LSI_SAS3i;LSI_SAS3i; C:\WINDOWS\System32\drivers\lsi_sas3i.sys [2015-10-30 99168]
S0 percsas2i;percsas2i; C:\WINDOWS\System32\drivers\percsas2i.sys [2015-10-30 58208]
S0 percsas3i;percsas3i; C:\WINDOWS\System32\drivers\percsas3i.sys [2015-10-30 58720]
S0 storufs;@storufs.inf,%UfsServiceDesc%;Microsoft Universal Flash Storage (UFS) Driver;
C:\WINDOWS\System32\drivers\storufs.sys [2015-10-30 34144]
S3 bcmfn;@bcmfn.inf,%bcmfn.SVCDESC%;bcmfn Service; C:\WINDOWS\System32\drivers\bcmfn.sys [2015-10-30 9728]
S3 BTHPORT;@bth.inf,%BTHPORT.SvcDesc%;Stuurprogramma voor Bluetooth-poort;
C:\WINDOWS\System32\drivers\BTHport.sys [2016-01-05 953856]
S3 buttonconverter;@buttonconverter.inf,%btnconv.SvcDesc%;Service for Portable Device Control devices;
C:\WINDOWS\System32\drivers\buttonconverter.sys [2015-10-30 37376]
S3 CapImg;@capimg.inf,%CapImgHid_Service%;HID driver for CapImg touch screen;
C:\WINDOWS\System32\drivers\capimg.sys [2015-11-22 117248]
S3 genericusbfn;@genericusbfn.inf,%genericusbfn.ServiceName%;Generic USB Function Class;
C:\WINDOWS\System32\drivers\genericusbfn.sys [2015-10-30 20992]
S3 hidinterrupt;@hidinterrupt.inf,%HID_Interrupt.SvcDesc%;Common Driver for HID Buttons implemented with interrupts; C:\WINDOWS\System32\drivers\hidinterrupt.sys [2015-10-30 50016]
S3 iai2c;@iai2c.inf,%iai2c.SVCDESC%;Intel(R) Serial IO I2C Host Controller;
C:\WINDOWS\System32\drivers\iai2c.sys [2015-10-30 81408]
S3 iaLPSS2i_I2C;@iaLPSS2i_I2C_SKL.inf,%iaLPSS2i_I2C.SVCDESC%;Intel(R) Serial IO I2C Driver v2;
C:\WINDOWS\System32\drivers\iaLPSS2i_I2C.sys [2015-10-30 165888]
S3 ibbus;@mlx4_bus.inf,%Ibbus.ServiceDesc%;Mellanox InfiniBand Bus/AL (Filter Driver);
C:\WINDOWS\System32\drivers\ibbus.sys [2015-10-30 424800]
S3 IoQos;@%SystemRoot%\system32\drivers\ioqos.sys,-100; C:\WINDOWS\system32\drivers\ioqos.sys [2015-10-30 26624]
S3 MBAMWebAccessControl;MBAMWebAccessControl; \??\C:\WINDOWS\system32\drivers\mwac.sys [2015-10-05 64216]
S3 mlx4_bus;@mlx4_bus.inf,%MLX4BUS.ServiceDesc%;Mellanox ConnectX Bus Enumerator;
C:\WINDOWS\System32\drivers\mlx4_bus.sys [2015-10-30 705376]
S3 ndfltr;@mlx4_bus.inf,%ndfltr.ServiceDesc%;NetworkDirect Service; C:\WINDOWS\System32\drivers\ndfltr.sys [2015-10-30 76128]
S3 ReFSv1;ReFSv1; C:\WINDOWS\system32\drivers\ReFSv1.sys [2015-10-30 930656]
S3 RSPCIESTOR;@oem13.inf,%Rts5208%;Realtek PCIE CardReader Driver;
C:\WINDOWS\system32\DRIVERS\RtsPStor.sys [2015-06-03 374016]
S3 UcmCx0101;USB Connector Manager KMDF Class Extension; C:\WINDOWS\System32\Drivers\UcmCx.sys [2015-10-30 61952]
S3 UcmUcsi;@UcmUcsi.inf,%UcmUcsi.ServiceName%;USB Connector Manager UCSI Client;
C:\WINDOWS\System32\drivers\UcmUcsi.sys [2015-10-30 46592]
S3 UdeCx;USB Device Emulation Support Library; C:\WINDOWS\system32\drivers\udecx.sys [2015-10-30 45056]
S3 Ufx01000;USB Function Class Extension; C:\WINDOWS\system32\drivers\ufx01000.sys [2015-10-30 254816]
S3 UfxChipidea;@ufxchipidea.inf,%UfxChipidea.ServiceName%;USB Chipidea Controller;

C:\WINDOWS\System32\drivers\UfxChipidea.sys [2015-10-30 94048]
S3 ufxsynopsys;@ufxsynopsys.inf,%ufxsynopsys.ServiceName%;USB Synopsys Controller;
C:\WINDOWS\System32\drivers\ufxsynopsys.sys [2015-10-30 131424]

======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 [2015-12-13 82128]
R2 AGSService;Adobe Genuine Software Integrity Service; C:\Program Files (x86)\Common Files\Adobe\AdobeGCClient\AGSService.exe [2015-11-25 2016448]
R2 ApHidMonitorService;@oem1.inf,%HidMonitor.SvcDisp%;Alps HID Monitor Service; C:\Program Files\Apoint2K\HidMonitorSvc.exe [2015-10-04 104840]
R2 c2cautoupdatesvc;Skype Click to Call Updater; C:\Program Files (x86)\Skype\Toolbars\AutoUpdate\SkypeC2CAutoUpdateSvc.exe [2016-01-08 1433216]
R2 c2cpnrsvc;Skype Click to Call PNR Service; C:\Program Files (x86)\Skype\Toolbars\PNRSvc\SkypeC2CPNRSvc.exe [2016-01-08 1773696]
R2 CCDMonitorService;CCDMonitorService; C:\Program Files (x86)\Acer\Acer Cloud\CCDMonitorService.exe [2012-10-26 2449552]
R2 CoreMessagingRegistrar;@%SystemRoot%\system32\coremessaging.dll,-1; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
R2 DiagTrack;@%SystemRoot%\system32\diagtrack.dll,-3001; C:\WINDOWS\System32\svchost.exe [2015-10-30 43944]
R2 DsiWMIService;Dritek WMI Service; C:\Program Files (x86)\Launch Manager\dsiwmis.exe [2012-12-10 350544]
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 LiveUpdateSvc;LiveUpdate; C:\Program Files (x86)\IObit\LiveUpdate\LiveUpdate.exe [2015-07-30 2909472]
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 McAfee SiteAdvisor Service;McAfee SiteAdvisor Service; C:\Program Files (x86)\McAfee\SiteAdvisor\McSACore.exe [2015-12-29 158952]
R2 NOBU;Norton Online Backup; C:\Program Files (x86)\Symantec\Norton Online Backup\NOBuAgent.exe [2012-08-15 3943104]
R2 NTI IScheduleSvc;NTI IScheduleSvc; C:\Program Files (x86)\NTI\Acer Backup Manager\IScheduleSvc.exe [2012-11-03 259136]
R2 OneSyncSvc_2ec3f37;Host synchroniseren_2ec3f37; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
R2 RapportMgmtService;Rapport Management Service; C:\Program Files (x86)\Trusteer\Rapport\bin\RapportMgmtService.exe [2016-01-03 2259224]
R2 RfButtonDriverService;Dritek RF Button Command Service; C:\Windows\RfBtnSvc64.exe [2013-03-22 93296]
R2 SamsungUPDUtilSvc;Samsung UPD Utility Service; C:\WINDOWS\SysWOW64\SecUPDUtilSvc.exe [2014-11-26 118576]
R2 TeamViewer;TeamViewer 10; C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe [2015-09-11 5702416]
R2 tiledatamodelsvc;@%SystemRoot%\system32\tileobjserver.dll,-1; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
R3 DsSvc;@%SystemRoot%\system32\dssvc.dll,-10003; C:\WINDOWS\System32\svchost.exe [2015-10-30 43944]
R3 ePowerSvc;ePower Service; C:\Program Files\Acer\Acer Power Management\ePowerSvc.exe [2012-10-23 658064]
R3 LicenseManager;@%SystemRoot%\system32\licensemanagersvc.dll,-200; C:\WINDOWS\System32\svchost.exe [2015-10-30 43944]
R3 PimIndexMaintenanceSvc_2ec3f37;Contact Data_2ec3f37; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
R3 StateRepository;@%SystemRoot%\system32\windows.staterepository.dll,-1; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S2 DoSvc;@%systemroot%\system32\dosvc.dll,-100; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S2 gupdate;Google Update-service (gupdate); C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [2015-09-13 144200]
S2 MapsBroker;@%SystemRoot%\System32\moshost.dll,-100; C:\WINDOWS\System32\svchost.exe [2015-10-30 43944]
S2 MBAMService;MBAMService; C:\Program Files (x86)\Malwarebytes Anti-Malware\mbamservice.exe [2015-10-05 1135416]

S2 OneSyncSvc;@%SystemRoot%\system32\APHostRes.dll,-10002; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S2 OneSyncSvc_62a5d8b;Host synchroniseren_62a5d8b; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S2 SkypeUpdate;Skype Updater; C:\Program Files (x86)\Skype\Updater\Updater.exe [2015-07-09 327296]
S3 AdobeFlashPlayerUpdateSvc;Adobe Flash Player Update Service; C:\WINDOWS\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe [2016-01-20 269504]
S3 AJRouter;@%SystemRoot%\system32\AJRouter.dll,-2; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S3 BthHFSrv;@%SystemRoot%\System32\BthHFSrv.dll,-103; C:\WINDOWS\System32\svchost.exe [2015-10-30 43944]
S3 ClipSVC;@%SystemRoot%\system32\ClipSVC.dll,-103; C:\WINDOWS\System32\svchost.exe [2015-10-30 43944]
S3 cphs;Intel(R) Content Protection HECI Service; C:\WINDOWS\SysWow64\IntelCpHeciSvc.exe [2015-06-01 290224]
S3 DcpSvc;@%SystemRoot%\system32\dcpsvc.dll,-3001; C:\WINDOWS\System32\svchost.exe [2015-10-30 43944]
S3 DeviceFastLaneService;Device Fast-lane Service; C:\Program Files\Acer\Acer Device Fast-lane\DeviceFastLaneSvc.exe [2012-11-16 469648]
S3 DevQueryBroker;@%SystemRoot%\system32\DevQueryBroker.dll,-100; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S3 diagnosticshub.standardcollector.service;@%SystemRoot%\system32\DiagSvcs\DiagnosticsHub.StandardCollector.ServiceRes.dll,-1000; C:\WINDOWS\system32\DiagSvcs\DiagnosticsHub.StandardCollector.Service.exe [2015-10-30 31744]
S3 DmEnrollmentSvc;@%systemroot%\system32\Windows.Internal.Management.dll,-100; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S3 dmwappushservice;@%SystemRoot%\system32\dmwappushsvc.dll,-200; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S3 EgisTec Ticket Service;EgisTec Ticket Service; C:\Program Files (x86)\Common Files\EgisTec\Services\EgisTicketService.exe [2012-07-12 174160]
S3 embeddedmode;@%SystemRoot%\system32\embeddedmodesvc.dll,-200; C:\WINDOWS\System32\svchost.exe [2015-10-30 43944]
S3 EntAppSvc;@EnterpriseAppMgmtSvc.dll,-1; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
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 [2015-10-23 43696]
S3 GamesAppService;GamesAppService; C:\Program Files (x86)\WildTangent Games\App\GamesAppService.exe [2010-10-12 206072]
S3 gupdatem;Google Update-service (gupdatem); C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [2015-09-13 144200]
S3 gusvc;Google Software Updater; C:\Program Files (x86)\Google\Common\Google Updater\GoogleUpdaterService.exe [2015-06-30 194032]
S3 icssvc;@%SystemRoot%\System32\tetheringservice.dll,-4097; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S3 MessagingService;@%SystemRoot%\system32\MessagingService.dll,-100; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S3 MessagingService_2ec3f37;MessagingService_2ec3f37; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S3 MessagingService_62a5d8b;MessagingService_62a5d8b; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S3 MozillaMaintenance;Mozilla Maintenance Service; C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe [2015-11-11 147624]
S3 NetSetupSvc;@%SystemRoot%\system32\NetSetupSvc.dll,-3; C:\WINDOWS\System32\svchost.exe [2015-10-30 43944]
S3 NgcCtnrSvc;@%SystemRoot%\System32\NgcCtnrSvc.dll,-1; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S3 NgcSvc;@%SystemRoot%\System32\ngcsvc.dll,-100; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S3 PhoneSvc;@%SystemRoot%\system32\PhoneserviceRes.dll,-10000; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S3 PimIndexMaintenanceSvc;@%SystemRoot%\system32\UserDataAccessRes.dll,-15001; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S3 PimIndexMaintenanceSvc_62a5d8b;Contact Data_62a5d8b; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S3 RetailDemo;@%SystemRoot%\System32\RDXService.dll,-256; C:\WINDOWS\System32\svchost.exe [2015-10-30 43944]
S3 SensorDataService;@%SystemRoot%\system32\SensorDataService.exe,-101; C:\WINDOWS\System32\SensorDataService.exe [2015-10-30 1297408]

S3 SensorService;@%SystemRoot%\System32\sensorservice.dll,-1000; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S3 SmsRouter;@%SystemRoot%\System32\SmsRouterSvc.dll,-10001; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S3 TieringEngineService;@%SystemRoot%\system32\TieringEngineService.exe,-702; C:\WINDOWS\system32\TieringEngineService.exe [2015-10-30 290304]
S4 CDPSvc;@%SystemRoot%\system32\cdpsvc.dll,-100; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]
S4 tzautoupdate;@%SystemRoot%\system32\tzautoupdate.dll,-200; C:\WINDOWS\system32\svchost.exe [2015-10-30 43944]

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