Logfile of random's system information tool 1.09 (written by random/random)

Run by David at 2012-12-21 01:21:57

Microsoft Windows 7 Home Premium Service Pack 1

System drive C: has 40 GB (14%) free of 292 GB

Total RAM: 4063 MB (32% free)

Logfile of Trend Micro HijackThis v2.0.4

Scan saved at 1:22:06, on 21.12.2012

Platform: Windows 7 SP1 (WinNT 6.00.3505)

MSIE: Internet Explorer v9.00 (9.00.8112.16457)

Boot mode: Normal

Running processes:

C:\Windows\SysWOW64\rundll32.exe

C:\Users\David\AppData\Local\Google\Update\1.3.21.123\GoogleCrashHandler.exe

C:\Program Files (x86)\SugarSync\SugarSyncManager.exe

c:\Program Files (x86)\Hewlett-Packard\Media\DVD\DVDAgent.exe

c:\Program Files (x86)\Hewlett-Packard\Media\Live TV\TVAgent.exe

c:\Program Files (x86)\Hewlett-Packard\TouchSmart\Media\Kernel\CLML\CLMLSvc.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Program Files (x86)\Gmail Notifier\Gmail Notifier.exe

C:\Users\David\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\NBSTAT.EXE

C:\Users\David\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\pomocnik.exe

C:\Program Files (x86)\DigitalPersona\Bin\DpAgent.exe

C:\Program Files (x86)\Hewlett-Packard\HP Quick Launch Buttons\QLBCTRL.exe

C:\Program Files (x86)\Google\Google Desktop Search\GoogleDesktop.exe

C:\Program Files (x86)\Hp\HP Software Update\hpwuschd2.exe

C:\Program Files\AVAST Software\Avast\AvastUI.exe

C:\Program Files (x86)\real\realplayer\Update\realsched.exe

C:\Program Files (x86)\Hewlett-Packard\Shared\hpqToaster.exe

C:\Program Files (x86)\The KMPlayer\KMPlayer.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Google Talk Plugin\googletalkplugin.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Program Files\trend micro\David.exe

C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe

R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = http://go.microsoft.com/fwlink/?LinkId=69157

R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL = http://go.microsoft.com/fwlink/?LinkId=54896

R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft.com/fwlink/?LinkId=54896

R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName =

O2 - BHO: HP Print Enhancer - {0347C33E-8762-4905-BF09-768834316C61} - C:\Program Files (x86)\HP\Digital Imaging\Smart Web Printing\hpswp_printenhancer.dll

O2 - BHO: AcroIEHelperStub - {18DF081C-E8AD-4283-A596-FA578C2EBDC3} - C:\Program Files (x86)\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll

O2 - BHO: RealPlayer Download and Record Plugin for Internet Explorer - {3049C3E9-B461-4BC5-8870-4C09146192CA} - C:\ProgramData\Real\RealPlayer\BrowserRecordPlugin\IE\rpbrowserrecordplugin.dll

O2 - BHO: DigitalPersona Personal Extension - {395610AE-C624-4f58-B89E-23733EA00F9A} - C:\Program Files (x86)\DigitalPersona\Bin\DpOtsPluginIe8.dll

O2 - BHO: Groove GFS Browser Helper - {72853161-30C5-4D22-B7F9-0BBC1D38A37E} - C:\Program Files (x86)\Microsoft Office\Office12\GrooveShellExtensions.dll

O2 - BHO: Java(tm) Plug-In SSV Helper - {761497BB-D6F0-462C-B6EB-D4DAF1D92D43} - C:\Program Files (x86)\Oracle\JavaFX 2.1 Runtime\bin\ssv.dll

O2 - BHO: avast! WebRep - {8E5E2654-AD2D-48bf-AC2D-D17F00898D06} - C:\Program Files\AVAST Software\Avast\aswWebRepIE.dll

O2 - BHO: Pomocná služba pro přihlášení ke službě Windows Live ID - {9030D464-4C02-4ABF-8ECC-5164760863C6} - C:\Program Files (x86)\Common Files\Microsoft Shared\Windows Live\WindowsLiveLogin.dll

O2 - BHO: Free-Ebook-Download.net - {90d375c8-2b3c-46db-bdb5-58e30d998a54} - C:\Program Files (x86)\Free-Ebook-Download.net\prxtbFre2.dll

O2 - BHO: Windows Live Messenger Companion Helper - {9FDDE16B-836F-4806-AB1F-1455CBEFF289} - C:\Program Files (x86)\Windows Live\Companion\companioncore.dll

O2 - BHO: Google Toolbar Helper - {AA58ED58-01DD-4d91-8333-CF10577473F7} - C:\Program Files (x86)\Google\Google Toolbar\GoogleToolbar_32.dll

O2 - BHO: NCH Toolbar - {c2db4fe6-8409-45ce-8010-189a7b5cce86} - C:\Program Files (x86)\NCH\tbNCH.dll

O2 - BHO: Java(tm) Plug-In 2 SSV Helper - {DBC80044-A445-435b-BC74-9C25C1C588A9} - C:\Program Files (x86)\Oracle\JavaFX 2.1 Runtime\bin\jp2ssv.dll

O2 - BHO: HP Network Check Helper - {E76FD755-C1BA-4DCB-9F13-99BD91223ADE} - C:\Program Files (x86)\Hewlett-Packard\HP Support Framework\Resources\HPNetworkCheck\HPNetworkCheckPlugin.dll

O2 - BHO: HP Smart BHO Class - {FFFFFFFF-CF4E-4F2B-BDC2-0E72E116A856} - C:\Program Files (x86)\HP\Digital Imaging\Smart Web Printing\hpswp_BHO.dll

O3 - Toolbar: avast! WebRep - {8E5E2654-AD2D-48bf-AC2D-D17F00898D06} - C:\Program Files\AVAST Software\Avast\aswWebRepIE.dll

O3 - Toolbar: Google Toolbar - {2318C2B1-4965-11d4-9B18-009027A5CD4F} - C:\Program Files (x86)\Google\Google Toolbar\GoogleToolbar_32.dll

O4 - HKLM\..\Run: [StartCCC] "C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLIStart.exe" MSRun

O4 - HKLM\..\Run: [HPCam_Menu] "c:\Program Files (x86)\Hewlett-Packard\Media\Webcam\MUITransfer\MUIStartMenu.exe" "c:\Program Files (x86)\Hewlett-Packard\Media\Webcam" UpdateWithCreateOnce "Software\Hewlett-Packard\Media\Webcam"

O4 - HKLM\..\Run: [DpAgent] C:\Program Files (x86)\DigitalPersona\Bin\dpagent.exe

O4 - HKLM\..\Run: [QlbCtrl.exe] C:\Program Files (x86)\Hewlett-Packard\HP Quick Launch Buttons\QlbCtrl.exe /Start

O4 - HKLM\..\Run: [UpdatePRCShortCut] "C:\Program Files (x86)\Hewlett-Packard\Recovery\MUITransfer\MUIStartMenu.exe" "C:\Program Files (x86)\Hewlett-Packard\Recovery" UpdateWithCreateOnce "Software\CyberLink\PowerRecover"

O4 - HKLM\..\Run: [WirelessAssistant] C:\Program Files (x86)\Hewlett-Packard\HP Wireless Assistant\HPWAMain.exe

O4 - HKLM\..\Run: [Google Desktop Search] "C:\Program Files (x86)\Google\Google Desktop Search\GoogleDesktop.exe" /startup

O4 - HKLM\..\Run: [TrayServer] C:\Program Files (x86)\MAGIX\Movie_Edit_Pro_15_Plus_Download_version\TrayServer.exe

O4 - HKLM\..\Run: [HP Software Update] C:\Program Files (x86)\Hp\HP Software Update\HPWuSchd2.exe

O4 - HKLM\..\Run: [avast] "C:\Program Files\AVAST Software\Avast\avastUI.exe" /nogui

O4 - HKLM\..\Run: [Adobe ARM] "C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe"

O4 - HKLM\..\Run: [TkBellExe] "C:\Program Files (x86)\real\realplayer\update\realsched.exe" -osboot

O4 - HKCU\..\Run: [swg] "C:\Program Files (x86)\Google\GoogleToolbarNotifier\GoogleToolbarNotifier.exe"

O4 - HKCU\..\Run: [Sidebar] C:\Program Files\Windows Sidebar\sidebar.exe /autoRun

O4 - HKCU\..\Run: [Google Update] "C:\Users\David\AppData\Local\Google\Update\GoogleUpdate.exe" /c

O4 - HKCU\..\Run: [SugarSync] "C:\Program Files (x86)\SugarSync\SugarSyncManager.exe" -startInTray -usedelay=true

O4 - HKCU\..\Run: [3DFE07AAA0B32A309ED9547B543D5CA16227B004._service_run] "C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=service

O4 - HKCU\..\Run: [Gmail Notifier.exe] C:\Program Files (x86)\Gmail Notifier\Gmail Notifier.exe /startup

O4 - Startup: Adobe Gamma.lnk = C:\Program Files (x86)\Common Files\Adobe\Calibration\Adobe Gamma Loader.exe

O4 - Startup: bateriedata.sav

O4 - Startup: NBSTAT.EXE

O4 - Startup: nbstat_varovani.log

O4 - Startup: pomocnik.exe

O4 - Startup: pomocnik.ini

O8 - Extra context menu item: E&xportovat do aplikace Microsoft Excel - res://C:\PROGRA~2\MICROS~1\Office12\EXCEL.EXE/3000

O8 - Extra context menu item: Hledání panelu &AOL Toolbar - C:\ProgramData\AOL\ieToolbar\resources\cs-CZ\local\search.html

O8 - Extra context menu item: Odeslat obrázek do zařízení &Bluetooth... - C:\Program Files\WIDCOMM\Bluetooth Software\btsendto_ie_ctx.htm

O8 - Extra context menu item: Odeslat stránku do zařízení &Bluetooth... - C:\Program Files\WIDCOMM\Bluetooth Software\btsendto_ie.htm

O9 - Extra button: @C:\Program Files (x86)\Windows Live\Companion\companionlang.dll,-600 - {0000036B-C524-4050-81A0-243669A86B9F} - C:\Program Files (x86)\Windows Live\Companion\companioncore.dll

O9 - Extra button: @C:\Program Files (x86)\Windows Live\Writer\WindowsLiveWriterShortcuts.dll,-1004 - {219C3416-8CB2-491a-A3C7-D9FCDDC9D600} - C:\Program Files (x86)\Windows Live\Writer\WriterBrowserExtension.dll

O9 - Extra 'Tools' menuitem: @C:\Program Files (x86)\Windows Live\Writer\WindowsLiveWriterShortcuts.dll,-1003 - {219C3416-8CB2-491a-A3C7-D9FCDDC9D600} - C:\Program Files (x86)\Windows Live\Writer\WriterBrowserExtension.dll

O9 - Extra button: @C:\Program Files (x86)\Hewlett-Packard\HP Support Framework\Resources\HPNetworkCheck\HPNetworkCheckPlugin.dll,-103 - {25510184-5A38-4A99-B273-DCA8EEF6CD08} - C:\Program Files (x86)\Hewlett-Packard\HP Support Framework\Resources\HPNetworkCheck\NCLauncherFromIE.exe

O9 - Extra 'Tools' menuitem: @C:\Program Files (x86)\Hewlett-Packard\HP Support Framework\Resources\HPNetworkCheck\HPNetworkCheckPlugin.dll,-102 - {25510184-5A38-4A99-B273-DCA8EEF6CD08} - C:\Program Files (x86)\Hewlett-Packard\HP Support Framework\Resources\HPNetworkCheck\NCLauncherFromIE.exe

O9 - Extra button: Odeslat do aplikace OneNote - {2670000A-7350-4f3c-8081-5663EE0C6C49} - C:\PROGRA~2\MICROS~1\Office12\ONBttnIE.dll

O9 - Extra 'Tools' menuitem: Od&eslat do aplikace OneNote - {2670000A-7350-4f3c-8081-5663EE0C6C49} - C:\PROGRA~2\MICROS~1\Office12\ONBttnIE.dll

O9 - Extra button: ICQ7M - {781B39EC-2E18-41FC-9B00-B84E4FFCA85F} - C:\Program Files (x86)\ICQ7M\ICQ.exe

O9 - Extra 'Tools' menuitem: ICQ7M - {781B39EC-2E18-41FC-9B00-B84E4FFCA85F} - C:\Program Files (x86)\ICQ7M\ICQ.exe

O9 - Extra button: Research - {92780B25-18CC-41C8-B9BE-3C9C571A8263} - C:\PROGRA~2\MICROS~1\Office12\REFIEBAR.DLL

O9 - Extra button: Odeslat do zařízení Bluetooth - {CCA281CA-C863-46ef-9331-5C8D4460577F} - C:\Program Files\WIDCOMM\Bluetooth Software\btsendto_ie.htm

O9 - Extra 'Tools' menuitem: Odeslat do zařízení &Bluetooth... - {CCA281CA-C863-46ef-9331-5C8D4460577F} - C:\Program Files\WIDCOMM\Bluetooth Software\btsendto_ie.htm

O9 - Extra button: Zobrazit nebo skrýt HP Smart Web Printing - {DDE87865-83C5-48c4-8357-2F5B1AA84522} - C:\Program Files (x86)\HP\Digital Imaging\Smart Web Printing\hpswp_BHO.dll

O9 - Extra button: QIP 2005 - {1EF681F7-A04B-4D6D-9012-A307CCA55610} - C:\Program Files (x86)\QIP\qip.exe (file missing) (HKCU)

O10 - Unknown file in Winsock LSP: c:\program files (x86)\common files\microsoft shared\windows live\wlidnsp.dll

O10 - Unknown file in Winsock LSP: c:\program files (x86)\common files\microsoft shared\windows live\wlidnsp.dll

O11 - Options group: [ACCELERATED_GRAPHICS] Accelerated graphics

O18 - Protocol: grooveLocalGWS - {88FED34C-F0CA-4636-A375-3CB6248B04CD} - C:\Program Files (x86)\Microsoft Office\Office12\GrooveSystemServices.dll

O18 - Protocol: skype4com - {FFC8B962-9B40-4DFF-9458-1830C7DD7F5D} - C:\PROGRA~2\COMMON~1\Skype\SKYPE4~1.DLL

O18 - Protocol: wlpg - {E43EF6CD-A37A-4A9B-9E6F-83F89B8E6324} - C:\Program Files (x86)\Windows Live\Photo Gallery\AlbumDownloadProtocolHandler.dll

O20 - AppInit_DLLs: C:\PROGRA~2\Google\GOOGLE~3\GoogleDesktopNetwork3.dll C:\PROGRA~2\Google\GOOGLE~3\GoogleDesktopNetwork3.dll C:\PROGRA~2\Google\GOOGLE~3\GO36F4~1.DLL

O23 - Service: Adobe LM Service - Adobe Systems - C:\Program Files (x86)\Common Files\Adobe Systems Shared\Service\Adobelmsvc.exe

O23 - Service: Adobe Acrobat Update Service (AdobeARMservice) - Adobe Systems Incorporated - C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe

O23 - Service: Andrea ST Filters Service (AESTFilters) - Andrea Electronics Corporation - C:\Windows\System32\DriverStore\FileRepository\stwrt64.inf_amd64_neutral_70dacb64382a61a7\AESTSr64.exe

O23 - Service: @%SystemRoot%\system32\Alg.exe,-112 (ALG) - Unknown owner - C:\Windows\System32\alg.exe (file missing)

O23 - Service: AMD External Events Utility - Unknown owner - C:\Windows\system32\atiesrxx.exe (file missing)

O23 - Service: avast! Antivirus - AVAST Software - C:\Program Files\AVAST Software\Avast\AvastSvc.exe

O23 - Service: Bonjour Service - Apple Inc. - C:\Program Files (x86)\Bonjour\mDNSResponder.exe

O23 - Service: Bluetooth Service (btwdins) - Broadcom Corporation. - C:\Program Files\WIDCOMM\Bluetooth Software\btwdins.exe

O23 - Service: Com4QLBEx - Hewlett-Packard Development Company, L.P. - C:\Program Files (x86)\Hewlett-Packard\HP Quick Launch Buttons\Com4QLBEx.exe

O23 - Service: @C:\Program Files (x86)\DigitalPersona\Bin\DpHostW.exe,-128 (DpHost) - DigitalPersona, Inc. - C:\Program Files (x86)\DigitalPersona\Bin\DpHostW.exe

O23 - Service: @%SystemRoot%\system32\efssvc.dll,-100 (EFS) - Unknown owner - C:\Windows\System32\lsass.exe (file missing)

O23 - Service: @%systemroot%\system32\fxsresm.dll,-118 (Fax) - Unknown owner - C:\Windows\system32\fxssvc.exe (file missing)

O23 - Service: Firebird Server - MAGIX Instance (FirebirdServerMAGIXInstance) - MAGIX® - C:\Program Files (x86)\MAGIX\Common\Database\bin\fbserver.exe

O23 - Service: GameConsoleService - WildTangent, Inc. - C:\Program Files (x86)\HP Games\HP Game Console\GameConsoleService.exe

O23 - Service: Google Desktop Manager 5.9.1005.12335 (GoogleDesktopManager-051210-111108) - Google - C:\Program Files (x86)\Google\Google Desktop Search\GoogleDesktop.exe

O23 - Service: Služba Google Update (gupdate) (gupdate) - Google Inc. - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe

O23 - Service: Služba Google Update (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: HP Support Assistant Service - Hewlett-Packard Company - C:\Program Files (x86)\Hewlett-Packard\HP Support Framework\hpsa_service.exe

O23 - Service: HP Software Framework Service (hpqwmiex) - Hewlett-Packard Company - C:\Program Files (x86)\Hewlett-Packard\Shared\hpqWmiEx.exe

O23 - Service: HP Service (hpsrv) - Unknown owner - C:\Windows\system32\Hpservice.exe (file missing)

O23 - Service: @keyiso.dll,-100 (KeyIso) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)

O23 - Service: LightScribeService Direct Disc Labeling Service (LightScribeService) - Hewlett-Packard Company - C:\Program Files (x86)\Common Files\LightScribe\LSSrvc.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: @%systemroot%\system32\psbase.dll,-300 (ProtectedStorage) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)

O23 - Service: Cyberlink RichVideo Service(CRVS) (RichVideo) - Unknown owner - C:\Program Files (x86)\CyberLink\Shared files\RichVideo.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: SolidConverterPDFReadSpool (SCPDFReadSpool) - Solid Documents, LLC - C:\Program Files (x86)\SolidDocuments\Solid Converter PDF\SCPDFV6\SolidConverterPDFServicex64.exe

O23 - Service: ServiceLayer - Nokia. - C:\Program Files (x86)\PC Connectivity Solution\ServiceLayer.exe

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: Audio Service (STacSV) - IDT, Inc. - C:\Windows\System32\DriverStore\FileRepository\stwrt64.inf_amd64_neutral_70dacb64382a61a7\STacSV64.exe

O23 - Service: TV Background Capture Service (TVBCS) (TVCapSvc) - Unknown owner - c:\Program Files (x86)\Hewlett-Packard\Media\Live TV\Kernel\TV\TVCapSvc.exe

O23 - Service: TV Task Scheduler (TVTS) (TVSched) - Unknown owner - c:\Program Files (x86)\Hewlett-Packard\Media\Live TV\Kernel\TV\TVSched.exe

O23 - Service: @%SystemRoot%\system32\ui0detect.exe,-101 (UI0Detect) - Unknown owner - C:\Windows\system32\UI0Detect.exe (file missing)

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: Validity Fingerprint Service (vfsFPService) - Validity Sensors, Inc. - C:\Windows\system32\vfsFPService.exe

O23 - Service: @%systemroot%\system32\vssvc.exe,-102 (VSS) - Unknown owner - C:\Windows\system32\vssvc.exe (file missing)

O23 - Service: @%SystemRoot%\system32\Wat\WatUX.exe,-601 (WatAdminSvc) - Unknown owner - C:\Windows\system32\Wat\WatAdminSvc.exe (file missing)

O23 - Service: @%systemroot%\system32\wbengine.exe,-104 (wbengine) - Unknown owner - C:\Windows\system32\wbengine.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 - 19704 bytes

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

\SystemRoot\System32\smss.exe

%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16

wininit.exe

%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16

C:\Windows\system32\services.exe

C:\Windows\system32\lsass.exe

winlogon.exe

C:\Windows\system32\lsm.exe

C:\Windows\system32\svchost.exe -k DcomLaunch

C:\Windows\system32\svchost.exe -k RPCSS

C:\Windows\system32\atiesrxx.exe

C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted

C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted

C:\Windows\system32\svchost.exe -k netsvcs

C:\Windows\System32\DriverStore\FileRepository\stwrt64.inf_amd64_neutral_70dacb64382a61a7\STacSV64.exe

C:\Windows\system32\svchost.exe -k GPSvcGroup

C:\Windows\system32\svchost.exe -k LocalService

C:\Windows\system32\Hpservice.exe

atieclxx

C:\Windows\system32\vfsFPService.exe

C:\Windows\system32\svchost.exe -k NetworkService

"C:\Program Files\AVAST Software\Avast\AvastSvc.exe"

C:\Windows\System32\spoolsv.exe

"C:\Program Files (x86)\DigitalPersona\Bin\DpHostW.exe"

C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork

"C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe"

C:\Windows\System32\DriverStore\FileRepository\stwrt64.inf_amd64_neutral_70dacb64382a61a7\AESTSr64.exe

"C:\Program Files (x86)\Bonjour\mDNSResponder.exe"

"taskhost.exe"

"C:\Windows\system32\Dwm.exe"

taskeng.exe {7CAD884B-38BB-43ED-B83A-50CC44F32959}

C:\Windows\Explorer.EXE

"C:\Program Files\WIDCOMM\Bluetooth Software\btwdins.exe"

C:\Windows\SysWOW64\svchost.exe -k hpdevmgmt

"C:\Program Files (x86)\Common Files\LightScribe\LSSrvc.exe"

C:\Windows\System32\svchost.exe -k HPZ12

C:\Windows\System32\svchost.exe -k HPZ12

"C:\Program Files (x86)\CyberLink\Shared files\RichVideo.exe"

"C:\Program Files (x86)\SolidDocuments\Solid Converter PDF\SCPDFV6\SolidConverterPDFServicex64.exe"

C:\Windows\system32\svchost.exe -k imgsvc

"c:\Program Files (x86)\Hewlett-Packard\Media\Live TV\Kernel\TV\TVCapSvc.exe"

"c:\Program Files (x86)\Hewlett-Packard\Media\Live TV\Kernel\TV\TVSched.exe"

"C:\Program Files\Common Files\Microsoft Shared\Windows Live\WLIDSVC.EXE"

WLIDSvcM.exe 2076

"C:\Program Files\Synaptics\SynTP\SynTPEnh.exe"

"C:\Program Files\Hewlett-Packard\HP MediaSmart\SmartMenu.exe" /background

"C:\Program Files\Java\jre6\bin\jusched.exe"

"C:\Program Files\IDT\WDM\sttray64.exe"

"C:\Windows\SysWOW64\rundll32.exe" C:\Windows\Syswow64\cm108.dll,CMICtrlWnd

"C:\Program Files\BOINC\boinctray.exe"

"C:\Program Files\Windows Sidebar\sidebar.exe" /autoRun

C:\Users\David\AppData\Local\Google\Update\1.3.21.123\GoogleCrashHandler.exe

C:\Users\David\AppData\Local\Google\Update\1.3.21.123\GoogleCrashHandler64.exe

"C:\Program Files (x86)\SugarSync\SugarSyncManager.exe" -startInTray -usedelay=true

"c:\Program Files (x86)\Hewlett-Packard\Media\DVD\DVDAgent.exe"

"c:\Program Files (x86)\Hewlett-Packard\Media\Live TV\TVAgent.exe"

"c:\Program Files (x86)\Hewlett-Packard\TouchSmart\Media\Kernel\CLML\CLMLSvc.exe"

"C:\PROGRAM FILES\SYNAPTICS\SYNTP\SYNTPHELPER.EXE"

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=service

"C:\Program Files (x86)\Gmail Notifier\Gmail Notifier.exe" /startup

"C:\Users\David\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\NBSTAT.EXE"

"C:\Users\David\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\pomocnik.exe"

"C:\Program Files (x86)\DigitalPersona\Bin\DpAgent.exe"

"C:\Program Files (x86)\Hewlett-Packard\HP Quick Launch Buttons\QLBCTRL.exe" /Start

"C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\MOM"

"C:\Program Files (x86)\Hewlett-Packard\HP Wireless Assistant\HPWAMain.exe"

"C:\Program Files (x86)\Google\Google Desktop Search\GoogleDesktop.exe" /startup

"C:\Program Files (x86)\Hp\HP Software Update\hpwuschd2.exe"

"C:\Program Files\AVAST Software\Avast\AvastUI.exe" /nogui

"C:\Program Files\DigitalPersona\Bin\DPAgent.exe"

"C:\Program Files (x86)\real\realplayer\Update\realsched.exe" -osboot

"C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CCC.exe" 0

C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation

"C:\Program Files (x86)\Hewlett-Packard\Shared\hpqWmiEx.exe"

C:\Windows\system32\wbem\wmiprvse.exe

C:\Windows\system32\SearchIndexer.exe /Embedding

C:\Windows\system32\svchost.exe -k HPService

C:\Windows\System32\alg.exe

C:\Windows\system32\svchost.exe -k bthsvcs

"C:\Program Files (x86)\Hewlett-Packard\HP Quick Launch Buttons\Com4QLBEx.exe"

"C:\Program Files (x86)\Hewlett-Packard\Shared\hpqToaster.exe" -Embedding

"C:\Program Files (x86)\Hewlett-Packard\HP Support Framework\hpsa_service.exe"

C:\Windows\System32\svchost.exe -k secsvcs

"C:\Program Files\Windows Media Player\wmpnetwk.exe"

"C:\Program Files (x86)\The KMPlayer\KMPlayer.exe"

C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe"

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --extension-process --renderer-print-preview --channel="2496.0.817812238\1128984384" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --extension-process --renderer-print-preview --channel="2496.1.819185353\642906445" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBacku

pJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --renderer-print-preview --channel="2496.2.1854407108\431790385" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --renderer-print-preview --channel="2496.3.630352345\236249688" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=gpu-process --channel="2496.4.240420485\384172889" --reduce-gpu-sandbox --disable-image-transport-surface --gpu-vendor-id=0x1002 --gpu-device-id=0x9480 --gpu-driver-vendor="ATI Technologies Inc." --gpu-driver-version=8.632.0.0 --ignored=" --type=renderer " /prefetch:12

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --extension-process --renderer-print-preview --channel="2496.5.950863794\1620874220" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --extension-process --renderer-print-preview --channel="2496.6.1345706791\503469152" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --extension-process --renderer-print-preview --channel="2496.7.619437341\1039452849" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --renderer-print-preview --channel="2496.8.187932101\29278892" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --extension-process --renderer-print-preview --channel="2496.9.889154824\1752337996" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --extension-process --renderer-print-preview --channel="2496.10.1210346990\1278712850" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --extension-process --renderer-print-preview --channel="2496.11.1882762609\1761963044" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --extension-process --renderer-print-preview --channel="2496.12.434469065\1432886896" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --extension-process --renderer-print-preview --channel="2496.13.484494283\1820587587" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --extension-process --renderer-print-preview --channel="2496.14.2075796294\301241980" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --extension-process --renderer-print-preview --channel="2496.16.490253106\1448071054" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --extension-process --renderer-print-preview --channel="2496.17.2022121726\1528335803" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --extension-process --renderer-print-preview --channel="2496.18.184135416\1688804012" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --renderer-print-preview --channel="2496.19.2051556182\1911635770" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --extension-process --renderer-print-preview --channel="2496.20.1641502449\680968854" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --renderer-print-preview --channel="2496.21.769320230\1319677350" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --renderer-print-preview --channel="2496.22.1350376508\593482258" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --renderer-print-preview --channel="2496.24.103585911\1520382195" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --renderer-print-preview --channel="2496.29.1818610100\1110236518" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --renderer-print-preview --channel="2496.30.1099778455\715360380" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=plugin --plugin-path="C:\Users\David\AppData\Roaming\Mozilla\plugins\npgoogletalk.dll" --lang=cs --channel="2496.31.1141880413\1269281936" /prefetch:4

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --renderer-print-preview --channel="2496.32.60869280\115648831" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-

Percent/default/WarmSocketImpact/warmest_socket/ --renderer-print-preview --channel="2496.33.1510895098\207440484" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --renderer-print-preview --channel="2496.35.1069360201\631272510" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --renderer-print-preview --channel="2496.36.790257928\1773990930" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=ppapi --channel="2496.37.1876416904\1396628935" --lang=cs --ignored=" --type=renderer " /prefetch:13

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-

Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --renderer-print-preview --channel="2496.38.1870465967\190027275" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --renderer-print-preview --channel="2496.39.257552465\318108355" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --renderer-print-preview --channel="2496.40.1968995172\1249136074" /prefetch:3

"C:\Users\David\AppData\Local\Google\Google Talk Plugin\googletalkplugin.exe"

C:\Windows\sysWOW64\wbem\wmiprvse.exe -Embedding

C:\Windows\system32\wbem\WmiApSrv.exe

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/HttpPipeliningCompatibility/disable_test/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NetworkConnectivity/disable_network_stats/NewTabB

utton/default/OmniboxDisallowInlineHQP/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --renderer-print-preview --channel="2496.46.1117762141\1269019643" /prefetch:3

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/HttpPipeliningCompatibility/disable_test/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NetworkConnectivity/disable_network_stats/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxHQPNewScoring/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/PrerenderFromOmnibox/OmniboxPrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --renderer-print-preview --channel="2496.54.620896242\701641012" /prefetch:3

"C:\Users\David\Documents\plocha3\RSITx64.exe"

C:\Windows\system32\wbem\wmiprvse.exe

"C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe" --type=renderer --lang=cs --force-fieldtrials=AsyncDns/disabled/ConnCountImpact/conn_count_6/ConnnectBackupJobs/ConnectBackupJobsEnabled/DnsImpact/default_enabled_prefetch/EnableStage3D/enabled_default/ForceCompositingMode/disable/GlobalSdch/global_enable_sdch/HttpPipeliningCompatibility/disable_test/IdleSktToImpact/idle_timeout_10/InfiniteCache/Yes/NetworkConnectivity/disable_network_stats/NewTabButton/default/OmniboxDisallowInlineHQP/Standard/OmniboxHQPNewScoring/Standard/OmniboxSearchSuggest/2/OneClickSignIn/Standard/Prerender/PrerenderEnabled/PrerenderFromOmnibox/OmniboxPrerenderEnabled/ProxyConnectionImpact/proxy_connections_32/SBInterstitial/V2/SpdyCwnd/cwndMin16/SpeculativePrefetchingLearning/SpeculativePrefetchingDisabled/Test0PercentDefault/group_01/UMA-Dynamic-Binary-Uniformity-Trial/default/UMA-Session-Randomized-Uniformity-Trial-5-Percent/group_12/UMA-Uniformity-Trial-1-Percent/group_51/UMA-Uniformity-Trial-10-Percent/group_09/UMA-Uniformity-Trial-20-Percent/group_03/UMA-Uniformity-Trial-5-Percent/group_04/UMA-Uniformity-Trial-50-Percent/default/WarmSocketImpact/warmest_socket/ --extension-process --renderer-print-preview --channel="2496.55.1072387248\1199368917" /prefetch:3

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

C:\Windows\tasks\GoogleUpdateTaskMachineCore.job

C:\Windows\tasks\GoogleUpdateTaskMachineUA.job

C:\Windows\tasks\GoogleUpdateTaskUserS-1-5-21-3673342490-4105428771-1027504696-1000Core.job

C:\Windows\tasks\GoogleUpdateTaskUserS-1-5-21-3673342490-4105428771-1027504696-1000UA.job

C:\Windows\tasks\HPCeeScheduleForDavid.job

C:\Windows\tasks\ReclaimerUpdateFiles_David.job

C:\Windows\tasks\ReclaimerUpdateXML_David.job

C:\Windows\tasks\RNUpgradeHelperLogonPrompt_David.job

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

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{318A227B-5E9F-45bd-8999-7F8F10CA4CF5}]

avast! WebRep - C:\Program Files\AVAST Software\Avast\aswWebRepIE64.dll [2012-10-30 1502288]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{395610AE-C624-4f58-B89E-23733EA00F9A}]

DigitalPersona Personal Extension - C:\Program Files\DigitalPersona\Bin\DpOtsPluginIe8.dll [2009-07-17 1889856]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{9030D464-4C02-4ABF-8ECC-5164760863C6}]

Windows Live ID Sign-in Helper - C:\Program Files\Common Files\Microsoft Shared\Windows Live\WindowsLiveLogin.dll [2010-09-21 529280]

[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 [2012-12-15 253584]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{DBC80044-A445-435b-BC74-9C25C1C588A9}]

Java(tm) Plug-In 2 SSV Helper - C:\Program Files\Java\jre6\bin\jp2ssv.dll [2009-09-18 43520]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{0347C33E-8762-4905-BF09-768834316C61}]

HP Print Enhancer - C:\Program Files (x86)\HP\Digital Imaging\Smart Web Printing\hpswp_printenhancer.dll [2009-10-22 328248]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}]

Adobe PDF Link Helper - C:\Program Files (x86)\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll [2012-07-27 63944]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{3049C3E9-B461-4BC5-8870-4C09146192CA}]

RealPlayer Download and Record Plugin for Internet Explorer - C:\ProgramData\Real\RealPlayer\BrowserRecordPlugin\IE\rpbrowserrecordplugin.dll [2012-06-27 425680]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{395610AE-C624-4f58-B89E-23733EA00F9A}]

DigitalPersona Personal Extension - C:\Program Files (x86)\DigitalPersona\Bin\DpOtsPluginIe8.dll [2009-07-17 1256512]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{72853161-30C5-4D22-B7F9-0BBC1D38A37E}]

Groove GFS Browser Helper - C:\Program Files (x86)\Microsoft Office\Office12\GrooveShellExtensions.dll [2009-02-26 2217832]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}]

Java(tm) Plug-In SSV Helper - C:\Program Files (x86)\Oracle\JavaFX 2.1 Runtime\bin\ssv.dll [2012-07-05 453544]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{8E5E2654-AD2D-48bf-AC2D-D17F00898D06}]

avast! WebRep - C:\Program Files\AVAST Software\Avast\aswWebRepIE.dll [2012-10-30 1227736]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{9030D464-4C02-4ABF-8ECC-5164760863C6}]

Pomocná služba pro přihlášení ke službě Windows Live ID - C:\Program Files (x86)\Common Files\Microsoft Shared\Windows Live\WindowsLiveLogin.dll [2010-09-21 439168]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{90d375c8-2b3c-46db-bdb5-58e30d998a54}]

Free-Ebook-Download.net Toolbar - C:\Program Files (x86)\Free-Ebook-Download.net\prxtbFre2.dll [2011-05-09 176936]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{9FDDE16B-836F-4806-AB1F-1455CBEFF289}]

Windows Live Messenger Companion Helper - C:\Program Files (x86)\Windows Live\Companion\companioncore.dll [2010-11-10 393600]

[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 [2012-12-15 192144]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{c2db4fe6-8409-45ce-8010-189a7b5cce86}]

NCH Toolbar - C:\Program Files (x86)\NCH\tbNCH.dll [2009-12-31 2349080]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{DBC80044-A445-435b-BC74-9C25C1C588A9}]

Java(tm) Plug-In 2 SSV Helper - C:\Program Files (x86)\Oracle\JavaFX 2.1 Runtime\bin\jp2ssv.dll [2012-07-05 157616]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{E76FD755-C1BA-4DCB-9F13-99BD91223ADE}]

HP Network Check Helper - C:\Program Files (x86)\Hewlett-Packard\HP Support Framework\Resources\HPNetworkCheck\HPNetworkCheckPlugin.dll [2012-07-09 351136]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{FFFFFFFF-CF4E-4F2B-BDC2-0E72E116A856}]

HP Smart BHO Class - C:\Program Files (x86)\HP\Digital Imaging\Smart Web Printing\hpswp_BHO.dll [2009-10-22 517688]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Toolbar]

{32099AAC-C132-4136-9E9A-4E364A424E17} - DAEMON Tools Toolbar - C:\Program Files (x86)\DAEMON Tools Toolbar\DTToolbar64.dll [2011-01-20 1581376]

{318A227B-5E9F-45bd-8999-7F8F10CA4CF5} - avast! WebRep - C:\Program Files\AVAST Software\Avast\aswWebRepIE64.dll [2012-10-30 1502288]

{2318C2B1-4965-11d4-9B18-009027A5CD4F} - Google Toolbar - C:\Program Files (x86)\Google\Google Toolbar\GoogleToolbar_64.dll [2012-12-15 253584]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Internet Explorer\Toolbar]

{8E5E2654-AD2D-48bf-AC2D-D17F00898D06} - avast! WebRep - C:\Program Files\AVAST Software\Avast\aswWebRepIE.dll [2012-10-30 1227736]

{2318C2B1-4965-11d4-9B18-009027A5CD4F} - Google Toolbar - C:\Program Files (x86)\Google\Google Toolbar\GoogleToolbar_32.dll [2012-12-15 192144]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]

"SynTPEnh"=C:\Program Files\Synaptics\SynTP\SynTPEnh.exe [2011-10-14 2837288]

"SmartMenu"=C:\Program Files\Hewlett-Packard\HP MediaSmart\SmartMenu.exe [2009-07-21 610872]

"SunJavaUpdateSched"=C:\Program Files\Java\jre6\bin\jusched.exe [2009-09-18 171520]

"SysTrayApp"=C:\Program Files\IDT\WDM\sttray64.exe [2010-03-23 487424]

"Cm108Sound"=C:\Windows\syswow64\RunDll32.exe [2009-07-14 44544]

"boincmgr"=C:\Program Files\BOINC\boincmgr.exe [2012-04-04 5853872]

"boinctray"=C:\Program Files\BOINC\boinctray.exe [2012-04-04 70832]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]

"swg"=C:\Program Files (x86)\Google\GoogleToolbarNotifier\GoogleToolbarNotifier.exe [2010-01-09 39408]

"Sidebar"=C:\Program Files\Windows Sidebar\sidebar.exe [2010-11-20 1475584]

"Google Update"=C:\Users\David\AppData\Local\Google\Update\GoogleUpdate.exe [2010-01-14 135664]

"SugarSync"=C:\Program Files (x86)\SugarSync\SugarSyncManager.exe [2012-12-13 11179720]

"3DFE07AAA0B32A309ED9547B543D5CA16227B004._service_run"=C:\Users\David\AppData\Local\Google\Chrome\Application\chrome.exe [2012-12-05 1242728]

"Gmail Notifier.exe"=C:\Program Files (x86)\Gmail Notifier\Gmail Notifier.exe [2011-04-07 2155008]

[HKEY_LOCAL_MACHINE\Software\wow6432node\Microsoft\Windows\CurrentVersion\Run]

"StartCCC"=C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLIStart.exe [2009-07-02 98304]

"HPCam_Menu"=c:\Program Files (x86)\Hewlett-Packard\Media\Webcam\MUITransfer\MUIStartMenu.exe [2009-02-25 218408]

"DpAgent"=C:\Program Files (x86)\DigitalPersona\Bin\dpagent.exe [2009-07-17 842816]

"QlbCtrl.exe"=C:\Program Files (x86)\Hewlett-Packard\HP Quick Launch Buttons\QlbCtrl.exe [2009-06-24 320056]

"UpdatePRCShortCut"=C:\Program Files (x86)\Hewlett-Packard\Recovery\MUITransfer\MUIStartMenu.exe [2009-05-19 222504]

"WirelessAssistant"=C:\Program Files (x86)\Hewlett-Packard\HP Wireless Assistant\HPWAMain.exe [2009-07-23 498744]

"Google Desktop Search"=C:\Program Files (x86)\Google\Google Desktop Search\GoogleDesktop.exe [2010-07-14 30192]

"TrayServer"=C:\Program Files (x86)\MAGIX\Movie_Edit_Pro_15_Plus_Download_version\TrayServer.exe [2008-11-13 90112]

"HP Software Update"=C:\Program Files (x86)\Hp\HP Software Update\HPWuSchd2.exe [2009-11-18 54576]

"avast"=C:\Program Files\AVAST Software\Avast\avastUI.exe [2012-10-30 4297136]

"Adobe ARM"=C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe [2012-07-27 919008]

"TkBellExe"=C:\Program Files (x86)\real\realplayer\update\realsched.exe [2012-06-27 296056]

C:\Users\David\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

Adobe Gamma.lnk - C:\Program Files (x86)\Common Files\Adobe\Calibration\Adobe Gamma Loader.exe

bateriedata.sav

NBSTAT.EXE

nbstat_varovani.log

pomocnik.exe

pomocnik.ini

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad]

WebCheck - {E6FB5E20-DE35-11CF-9C87-00AA005127ED} - C:\Windows\system32\webcheck.dll [2012-04-12 249344]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks]

"{AEB6717E-7E19-11d0-97EE-00C04FD91972}"= []

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks]

"{B5A7F190-DDA6-4420-B3BA-52453494E6CD}"=C:\Program Files (x86)\Microsoft Office\Office12\GrooveShellExtensions.dll [2009-02-26 2217832]

"{AEB6717E-7E19-11d0-97EE-00C04FD91972}"= []

[HKEY_LOCAL_MACHINE\system\currentcontrolset\control\securityproviders]

"SecurityProviders"=credssp.dll

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

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

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

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System]

"ConsentPromptBehaviorAdmin"=0

"ConsentPromptBehaviorUser"=3

"EnableLUA"=0

"EnableUIADesktopToggle"=0

"PromptOnSecureDesktop"=0

"dontdisplaylastusername"=0

"legalnoticecaption"=

"legalnoticetext"=

"shutdownwithoutlogon"=1

"undockwithoutlogon"=1

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\explorer]

"NoDriveAutorun"=0

"NoDriveTypeAutoRun"=145

[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]

"vidc.mrle"=msrle32.dll

"vidc.msvc"=msvidc32.dll

"msacm.imaadpcm"=imaadp32.acm

"msacm.msg711"=msg711.acm

"msacm.msgsm610"=msgsm32.acm

"msacm.msadpcm"=msadp32.acm

"midimapper"=midimap.dll

"wavemapper"=msacm32.drv

"VIDC.UYVY"=msyuv.dll

"VIDC.YUY2"=msyuv.dll

"VIDC.YVYU"=msyuv.dll

"VIDC.IYUV"=iyuv_32.dll

"vidc.i420"=iyuv_32.dll

"VIDC.YVU9"=tsbyuv.dll

"msacm.l3acm"=C:\Windows\System32\l3codeca.acm

"MSVideo8"=VfWWDM32.dll

"wave1"=wdmaud.drv

"midi1"=wdmaud.drv

"mixer1"=wdmaud.drv

"aux1"=wdmaud.drv

"wave2"=wdmaud.drv

"midi2"=wdmaud.drv

"mixer2"=wdmaud.drv

"msacm.ac3filter"=ac3filter64.acm

"wave"=wdmaud.drv

"midi"=wdmaud.drv

"mixer"=wdmaud.drv

"wave3"=wdmaud.drv

"midi3"=wdmaud.drv

"mixer3"=wdmaud.drv

"wave4"=wdmaud.drv

"midi4"=wdmaud.drv

"mixer4"=wdmaud.drv

"aux"=wdmaud.drv

"wave5"=wdmaud.drv

"midi5"=wdmaud.drv

"mixer5"=wdmaud.drv

"wave6"=wdmaud.drv

"midi6"=wdmaud.drv

"mixer6"=wdmaud.drv

"wave7"=wdmaud.drv

"midi7"=wdmaud.drv

"mixer7"=wdmaud.drv

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

.js - edit - C:\Windows\System32\Notepad.exe %1

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

2012-12-13 14:42:58 ----D---- C:\Windows\Migration

2012-12-13 13:04:40 ----D---- C:\Program Files\HP

2012-12-13 13:01:29 ----D---- C:\Users\David\AppData\Roaming\GetRightToGo

2012-12-13 12:47:58 ----A---- C:\Windows\SYSWOW64\ncobjapi.dll

2012-12-13 12:47:58 ----A---- C:\Windows\system32\ncobjapi.dll

2012-12-13 12:47:38 ----A---- C:\Windows\system32\Register-CimProvider.exe

2012-12-13 12:47:37 ----A---- C:\Windows\SYSWOW64\Register-CimProvider.exe

2012-12-13 12:47:29 ----A---- C:\Windows\SYSWOW64\winrm.vbs

2012-12-13 12:47:29 ----A---- C:\Windows\system32\winrshost.exe

2012-12-13 12:47:28 ----A---- C:\Windows\SYSWOW64\winrsmgr.dll

2012-12-13 12:47:28 ----A---- C:\Windows\system32\winrsmgr.dll

2012-12-13 12:47:20 ----A---- C:\Windows\SYSWOW64\winrshost.exe

2012-12-13 12:47:19 ----A---- C:\Windows\SYSWOW64\winrs.exe

2012-12-13 12:47:19 ----A---- C:\Windows\SYSWOW64\wecutil.exe

2012-12-13 12:47:19 ----A---- C:\Windows\SYSWOW64\wecapi.dll

2012-12-13 12:47:19 ----A---- C:\Windows\system32\winrs.exe

2012-12-13 12:47:18 ----A---- C:\Windows\SYSWOW64\wevtfwd.dll

2012-12-13 12:47:18 ----A---- C:\Windows\system32\wsmplpxy.dll

2012-12-13 12:47:18 ----A---- C:\Windows\system32\winrssrv.dll

2012-12-13 12:47:18 ----A---- C:\Windows\system32\wevtfwd.dll

2012-12-13 12:47:18 ----A---- C:\Windows\system32\wecutil.exe

2012-12-13 12:47:18 ----A---- C:\Windows\system32\wecsvc.dll

2012-12-13 12:47:18 ----A---- C:\Windows\system32\wecapi.dll

2012-12-13 12:47:13 ----A---- C:\Windows\system32\winrscmd.dll

2012-12-13 12:47:04 ----A---- C:\Windows\SYSWOW64\WsmRes.dll

2012-12-13 12:47:04 ----A---- C:\Windows\system32\WsmRes.dll

2012-12-13 12:47:04 ----A---- C:\Windows\system32\WsmAgent.dll

2012-12-13 12:47:04 ----A---- C:\Windows\system32\PSModuleDiscoveryProvider.dll

2012-12-13 12:47:04 ----A---- C:\Windows\system32\prvdmofcomp.dll

2012-12-13 12:47:03 ----A---- C:\Windows\SYSWOW64\wsmplpxy.dll

2012-12-13 12:47:03 ----A---- C:\Windows\SYSWOW64\WsmAgent.dll

2012-12-13 12:47:03 ----A---- C:\Windows\SYSWOW64\winrssrv.dll

2012-12-13 12:47:03 ----A---- C:\Windows\SYSWOW64\PSModuleDiscoveryProvider.dll

2012-12-13 12:47:03 ----A---- C:\Windows\SYSWOW64\prvdmofcomp.dll

2012-12-13 12:47:00 ----A---- C:\Windows\SYSWOW64\wsmprovhost.exe

2012-12-13 12:47:00 ----A---- C:\Windows\SYSWOW64\WSManHTTPConfig.exe

2012-12-13 12:47:00 ----A---- C:\Windows\SYSWOW64\winrscmd.dll

2012-12-13 12:47:00 ----A---- C:\Windows\system32\wsmprovhost.exe

2012-12-13 12:47:00 ----A---- C:\Windows\system32\WSManHTTPConfig.exe

2012-12-13 12:46:59 ----A---- C:\Windows\SYSWOW64\pwrshplugin.dll

2012-12-13 12:46:59 ----A---- C:\Windows\SYSWOW64\mi.dll

2012-12-13 12:46:59 ----A---- C:\Windows\system32\mi.dll

2012-12-13 12:46:57 ----A---- C:\Windows\system32\pwrshplugin.dll

2012-12-13 12:46:49 ----A---- C:\Windows\SYSWOW64\wmitomi.dll

2012-12-13 12:46:49 ----A---- C:\Windows\SYSWOW64\wmidcom.dll

2012-12-13 12:46:49 ----A---- C:\Windows\system32\wmidcom.dll

2012-12-13 12:46:49 ----A---- C:\Windows\system32\winrm.vbs

2012-12-13 12:46:48 ----A---- C:\Windows\SYSWOW64\WSManMigrationPlugin.dll

2012-12-13 12:46:48 ----A---- C:\Windows\SYSWOW64\miutils.dll

2012-12-13 12:46:48 ----A---- C:\Windows\SYSWOW64\framedyn.dll

2012-12-13 12:46:48 ----A---- C:\Windows\system32\WSManMigrationPlugin.dll

2012-12-13 12:46:48 ----A---- C:\Windows\system32\wmitomi.dll

2012-12-13 12:46:48 ----A---- C:\Windows\system32\miutils.dll

2012-12-13 12:46:48 ----A---- C:\Windows\system32\framedynos.dll

2012-12-13 12:46:48 ----A---- C:\Windows\system32\framedyn.dll

2012-12-13 12:46:47 ----A---- C:\Windows\SYSWOW64\WsmWmiPl.dll

2012-12-13 12:46:47 ----A---- C:\Windows\SYSWOW64\framedynos.dll

2012-12-13 12:46:46 ----A---- C:\Windows\system32\WsmWmiPl.dll

2012-12-13 12:46:45 ----A---- C:\Windows\SYSWOW64\wbemcomn2.dll

2012-12-13 12:46:45 ----A---- C:\Windows\system32\wbemcomn2.dll

2012-12-13 12:46:44 ----A---- C:\Windows\SYSWOW64\WsmGCDeps.dll

2012-12-13 12:46:44 ----A---- C:\Windows\SYSWOW64\WsmAuto.dll

2012-12-13 12:46:44 ----A---- C:\Windows\system32\WsmAuto.dll

2012-12-13 12:46:43 ----A---- C:\Windows\SYSWOW64\WsmSvc.dll

2012-12-13 12:46:43 ----A---- C:\Windows\system32\WsmSvc.dll

2012-12-13 12:46:43 ----A---- C:\Windows\system32\WsmGCDeps.dll

2012-12-13 12:40:15 ----A---- C:\Windows\SYSWOW64\mshtmled.dll

2012-12-13 12:40:15 ----A---- C:\Windows\system32\mshtmled.dll

2012-12-13 12:40:14 ----A---- C:\Windows\SYSWOW64\vbscript.dll

2012-12-13 12:40:13 ----A---- C:\Windows\SYSWOW64\ieUnatt.exe

2012-12-13 12:40:13 ----A---- C:\Windows\SYSWOW64\ieui.dll

2012-12-13 12:40:13 ----A---- C:\Windows\system32\ieUnatt.exe

2012-12-13 12:40:13 ----A---- C:\Windows\system32\ieui.dll

2012-12-13 12:40:12 ----A---- C:\Windows\SYSWOW64\url.dll

2012-12-13 12:40:12 ----A---- C:\Windows\system32\url.dll

2012-12-13 12:40:11 ----A---- C:\Windows\SYSWOW64\urlmon.dll

2012-12-13 12:40:10 ----A---- C:\Windows\system32\urlmon.dll

2012-12-13 12:40:09 ----A---- C:\Windows\SYSWOW64\msfeeds.dll

2012-12-13 12:40:09 ----A---- C:\Windows\system32\msfeeds.dll

2012-12-13 12:40:09 ----A---- C:\Windows\system32\jscript9.dll

2012-12-13 12:40:08 ----A---- C:\Windows\SYSWOW64\wininet.dll

2012-12-13 12:40:08 ----A---- C:\Windows\system32\wininet.dll

2012-12-13 12:40:07 ----A---- C:\Windows\SYSWOW64\jscript9.dll

2012-12-13 12:40:07 ----A---- C:\Windows\system32\jsproxy.dll

2012-12-13 12:40:06 ----A---- C:\Windows\SYSWOW64\jscript.dll

2012-12-13 12:40:06 ----A---- C:\Windows\system32\vbscript.dll

2012-12-13 12:40:06 ----A---- C:\Windows\system32\jscript.dll

2012-12-13 12:40:05 ----A---- C:\Windows\SYSWOW64\jsproxy.dll

2012-12-13 12:40:05 ----A---- C:\Windows\SYSWOW64\iertutil.dll

2012-12-13 12:40:05 ----A---- C:\Windows\system32\iertutil.dll

2012-12-13 12:40:02 ----A---- C:\Windows\SYSWOW64\mshtml.dll

2012-12-13 12:40:00 ----A---- C:\Windows\system32\mshtml.dll

2012-12-13 12:39:58 ----A---- C:\Windows\system32\ieframe.dll

2012-12-13 12:39:57 ----A---- C:\Windows\SYSWOW64\ieframe.dll

2012-12-13 12:35:15 ----A---- C:\Windows\system32\KernelBase.dll

2012-12-13 12:35:14 ----A---- C:\Windows\SYSWOW64\kernel32.dll

2012-12-13 12:35:14 ----A---- C:\Windows\system32\winsrv.dll

2012-12-13 12:35:14 ----A---- C:\Windows\system32\kernel32.dll

2012-12-13 12:35:14 ----A---- C:\Windows\system32\conhost.exe

2012-12-13 12:35:13 ----A---- C:\Windows\SYSWOW64\KernelBase.dll

2012-12-13 12:35:12 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-sysinfo-l1-1-0.dll

2012-12-13 12:35:12 ----A---- C:\Windows\SYSWOW64\wow32.dll

2012-12-13 12:35:12 ----A---- C:\Windows\SYSWOW64\setup16.exe

2012-12-13 12:35:12 ----A---- C:\Windows\SYSWOW64\ntvdm64.dll

2012-12-13 12:35:12 ----A---- C:\Windows\SYSWOW64\instnm.exe

2012-12-13 12:35:12 ----A---- C:\Windows\system32\wow64win.dll

2012-12-13 12:35:12 ----A---- C:\Windows\system32\wow64cpu.dll

2012-12-13 12:35:12 ----A---- C:\Windows\system32\wow64.dll

2012-12-13 12:35:12 ----A---- C:\Windows\system32\ntvdm64.dll

2012-12-13 12:35:11 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-processthreads-l1-1-0.dll

2012-12-13 12:35:11 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-file-l1-1-0.dll

2012-12-13 12:35:11 ----AH---- C:\Windows\system32\api-ms-win-security-base-l1-1-0.dll

2012-12-13 12:35:11 ----AH---- C:\Windows\system32\api-ms-win-core-xstate-l1-1-0.dll

2012-12-13 12:35:11 ----AH---- C:\Windows\system32\api-ms-win-core-util-l1-1-0.dll

2012-12-13 12:35:11 ----AH---- C:\Windows\system32\api-ms-win-core-threadpool-l1-1-0.dll

2012-12-13 12:35:11 ----AH---- C:\Windows\system32\api-ms-win-core-sysinfo-l1-1-0.dll

2012-12-13 12:35:11 ----AH---- C:\Windows\system32\api-ms-win-core-heap-l1-1-0.dll

2012-12-13 12:35:11 ----AH---- C:\Windows\system32\api-ms-win-core-file-l1-1-0.dll

2012-12-13 12:35:10 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-synch-l1-1-0.dll

2012-12-13 12:35:10 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-string-l1-1-0.dll

2012-12-13 12:35:10 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-rtlsupport-l1-1-0.dll

2012-12-13 12:35:10 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-profile-l1-1-0.dll

2012-12-13 12:35:10 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-processenvironment-l1-1-0.dll

2012-12-13 12:35:10 ----AH---- C:\Windows\system32\api-ms-win-core-string-l1-1-0.dll

2012-12-13 12:35:10 ----AH---- C:\Windows\system32\api-ms-win-core-rtlsupport-l1-1-0.dll

2012-12-13 12:35:10 ----AH---- C:\Windows\system32\api-ms-win-core-profile-l1-1-0.dll

2012-12-13 12:35:10 ----AH---- C:\Windows\system32\api-ms-win-core-processthreads-l1-1-0.dll

2012-12-13 12:35:10 ----AH---- C:\Windows\system32\api-ms-win-core-processenvironment-l1-1-0.dll

2012-12-13 12:35:09 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-namedpipe-l1-1-0.dll

2012-12-13 12:35:09 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-misc-l1-1-0.dll

2012-12-13 12:35:09 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-memory-l1-1-0.dll

2012-12-13 12:35:09 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-localregistry-l1-1-0.dll

2012-12-13 12:35:09 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-libraryloader-l1-1-0.dll

2012-12-13 12:35:09 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-io-l1-1-0.dll

2012-12-13 12:35:09 ----AH---- C:\Windows\system32\api-ms-win-core-namedpipe-l1-1-0.dll

2012-12-13 12:35:09 ----AH---- C:\Windows\system32\api-ms-win-core-misc-l1-1-0.dll

2012-12-13 12:35:09 ----AH---- C:\Windows\system32\api-ms-win-core-memory-l1-1-0.dll

2012-12-13 12:35:09 ----AH---- C:\Windows\system32\api-ms-win-core-localregistry-l1-1-0.dll

2012-12-13 12:35:09 ----AH---- C:\Windows\system32\api-ms-win-core-libraryloader-l1-1-0.dll

2012-12-13 12:35:08 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-interlocked-l1-1-0.dll

2012-12-13 12:35:08 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-handle-l1-1-0.dll

2012-12-13 12:35:08 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-fibers-l1-1-0.dll

2012-12-13 12:35:08 ----AH---- C:\Windows\system32\api-ms-win-core-io-l1-1-0.dll

2012-12-13 12:35:08 ----AH---- C:\Windows\system32\api-ms-win-core-interlocked-l1-1-0.dll

2012-12-13 12:35:08 ----AH---- C:\Windows\system32\api-ms-win-core-handle-l1-1-0.dll

2012-12-13 12:35:08 ----AH---- C:\Windows\system32\api-ms-win-core-fibers-l1-1-0.dll

2012-12-13 12:35:07 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-errorhandling-l1-1-0.dll

2012-12-13 12:35:07 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-delayload-l1-1-0.dll

2012-12-13 12:35:07 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-debug-l1-1-0.dll

2012-12-13 12:35:07 ----AH---- C:\Windows\system32\api-ms-win-core-errorhandling-l1-1-0.dll

2012-12-13 12:35:07 ----AH---- C:\Windows\system32\api-ms-win-core-delayload-l1-1-0.dll

2012-12-13 12:35:07 ----AH---- C:\Windows\system32\api-ms-win-core-debug-l1-1-0.dll

2012-12-13 12:35:06 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-datetime-l1-1-0.dll

2012-12-13 12:35:06 ----AH---- C:\Windows\system32\api-ms-win-core-datetime-l1-1-0.dll

2012-12-13 12:35:01 ----AH---- C:\Windows\system32\api-ms-win-core-synch-l1-1-0.dll

2012-12-13 12:35:00 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-heap-l1-1-0.dll

2012-12-13 12:34:59 ----AH---- C:\Windows\SYSWOW64\api-ms-win-security-base-l1-1-0.dll

2012-12-13 12:34:57 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-xstate-l1-1-0.dll

2012-12-13 12:34:53 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-util-l1-1-0.dll

2012-12-13 12:34:53 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-threadpool-l1-1-0.dll

2012-12-13 12:34:53 ----AH---- C:\Windows\system32\api-ms-win-core-localization-l1-1-0.dll

2012-12-13 12:34:52 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-localization-l1-1-0.dll

2012-12-13 12:34:49 ----AH---- C:\Windows\SYSWOW64\api-ms-win-core-console-l1-1-0.dll

2012-12-13 12:34:48 ----AH---- C:\Windows\system32\api-ms-win-core-console-l1-1-0.dll

2012-12-13 12:34:45 ----A---- C:\Windows\SYSWOW64\user.exe

2012-12-13 12:33:43 ----A---- C:\Windows\system32\win32k.sys

2012-12-13 12:33:15 ----A---- C:\Windows\system32\tzres.dll

2012-12-13 12:33:14 ----A---- C:\Windows\SYSWOW64\tzres.dll

2012-12-13 12:32:08 ----A---- C:\Windows\system32\atmfd.dll

2012-12-13 12:32:07 ----A---- C:\Windows\SYSWOW64\atmlib.dll

2012-12-13 12:32:07 ----A---- C:\Windows\SYSWOW64\atmfd.dll

2012-12-13 12:32:07 ----A---- C:\Windows\system32\atmlib.dll

2012-12-13 12:29:09 ----A---- C:\Windows\SYSWOW64\dpnet.dll

2012-12-13 12:29:09 ----A---- C:\Windows\system32\dpnet.dll

2012-11-26 14:17:40 ----D---- C:\ProgramData\{9BF4D58B-C6D6-467B-BC5A-FD0C1278F4AF}

2012-11-26 13:21:21 ----A---- C:\Windows\SYSWOW64\javaws.exe

2012-11-26 13:21:21 ----A---- C:\Windows\SYSWOW64\javaw.exe

2012-11-26 13:21:21 ----A---- C:\Windows\SYSWOW64\java.exe

2012-11-26 11:35:51 ----A---- C:\Windows\system32\TsUsbRedirectionGroupPolicyExtension.dll

2012-11-26 11:35:51 ----A---- C:\Windows\system32\TsUsbRedirectionGroupPolicyControl.exe

2012-11-26 11:35:50 ----A---- C:\Windows\system32\RdpGroupPolicyExtension.dll

2012-11-26 11:35:33 ----A---- C:\Windows\system32\drivers\rdpvideominiport.sys

2012-11-26 11:35:32 ----A---- C:\Windows\system32\drivers\TsUsbFlt.sys

2012-11-26 11:35:16 ----A---- C:\Windows\system32\wksprtPS.dll

2012-11-26 11:35:15 ----A---- C:\Windows\system32\TsUsbGDCoInstaller.dll

2012-11-26 11:35:15 ----A---- C:\Windows\system32\tsgqec.dll

2012-11-26 11:35:14 ----A---- C:\Windows\SYSWOW64\wksprtPS.dll

2012-11-26 11:35:14 ----A---- C:\Windows\SYSWOW64\rdpendp_winip.dll

2012-11-26 11:35:13 ----A---- C:\Windows\SYSWOW64\tsgqec.dll

2012-11-26 11:35:13 ----A---- C:\Windows\SYSWOW64\aaclient.dll

2012-11-26 11:35:12 ----A---- C:\Windows\SYSWOW64\MsRdpWebAccess.dll

2012-11-26 11:35:09 ----A---- C:\Windows\system32\rdpudd.dll

2012-11-26 11:35:09 ----A---- C:\Windows\system32\MsRdpWebAccess.dll

2012-11-26 11:35:09 ----A---- C:\Windows\system32\aaclient.dll

2012-11-26 11:35:08 ----A---- C:\Windows\SYSWOW64\mstsc.exe

2012-11-26 11:35:08 ----A---- C:\Windows\system32\wksprt.exe

2012-11-26 11:35:08 ----A---- C:\Windows\system32\TSWbPrxy.exe

2012-11-26 11:35:08 ----A---- C:\Windows\system32\rdpendp_winip.dll

2012-11-26 11:35:07 ----A---- C:\Windows\system32\rdpcorets.dll

2012-11-26 11:35:07 ----A---- C:\Windows\system32\mstsc.exe

2012-11-26 11:35:06 ----A---- C:\Windows\SYSWOW64\mstscax.dll

2012-11-26 11:35:05 ----A---- C:\Windows\system32\mstscax.dll

2012-11-26 11:33:44 ----A---- C:\Windows\SYSWOW64\schannel.dll

2012-11-26 11:33:44 ----A---- C:\Windows\system32\schannel.dll

2012-11-26 11:33:44 ----A---- C:\Windows\system32\ncrypt.dll

2012-11-26 11:33:44 ----A---- C:\Windows\system32\drivers\cng.sys

2012-11-26 11:33:43 ----A---- C:\Windows\SYSWOW64\ncrypt.dll

2012-11-26 11:33:43 ----A---- C:\Windows\system32\lsasrv.dll

2012-11-26 11:33:43 ----A---- C:\Windows\system32\drivers\ksecpkg.sys

2012-11-26 11:33:42 ----A---- C:\Windows\SYSWOW64\sspicli.dll

2012-11-26 11:33:42 ----A---- C:\Windows\SYSWOW64\secur32.dll

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

2012-12-21 01:22:06 ----D---- C:\Windows\Prefetch

2012-12-21 01:22:03 ----D---- C:\Program Files\trend micro

2012-12-21 01:21:56 ----D---- C:\Windows\Temp

2012-12-21 01:11:16 ----D---- C:\Users\David\AppData\Roaming\SolidDocuments

2012-12-21 01:11:13 ----D---- C:\Windows\system32\FxsTmp

2012-12-21 00:45:59 ----D---- C:\Windows

2012-12-21 00:42:34 ----D---- C:\Users\David\AppData\Roaming\Media Player Classic

2012-12-21 00:42:31 ----D---- C:\Windows\Minidump

2012-12-21 00:40:31 ----D---- C:\Program Files (x86)

2012-12-21 00:40:20 ----D---- C:\Windows\system32\config

2012-12-21 00:39:35 ----D---- C:\ProgramData

2012-12-21 00:39:35 ----A---- C:\ProgramData\HPWALog.txt

2012-12-21 00:39:18 ----D---- C:\Users\David\AppData\Roaming\Gmail Notifier

2012-12-20 12:03:01 ----D---- C:\Program Files (x86)\Zotero Standalone

2012-12-19 09:05:30 ----D---- C:\Program Files (x86)\SugarSync

2012-12-19 08:00:01 ----D---- C:\Windows\Tasks

2012-12-18 19:59:01 ----D---- C:\Windows\System32

2012-12-18 19:59:01 ----A---- C:\Windows\system32\PerfStringBackup.INI

2012-12-16 17:26:29 ----D---- C:\Windows\rescache

2012-12-16 02:44:06 ----D---- C:\Windows\system32\Tasks

2012-12-15 18:13:38 ----D---- C:\Windows\Microsoft.NET

2012-12-15 18:13:36 ----RSD---- C:\Windows\assembly

2012-12-15 17:34:26 ----SHD---- C:\Windows\Installer

2012-12-15 16:45:56 ----D---- C:\Users\David\AppData\Roaming\Winamp

2012-12-15 16:45:52 ----D---- C:\Windows\debug

2012-12-14 20:53:32 ----D---- C:\Windows\winsxs

2012-12-13 14:43:00 ----D---- C:\Windows\SYSWOW64\cs-CZ

2012-12-13 14:43:00 ----D---- C:\Windows\SysWOW64

2012-12-13 14:43:00 ----D---- C:\Windows\system32\cs-CZ

2012-12-13 14:42:58 ----D---- C:\Windows\SYSWOW64\wbem

2012-12-13 14:42:58 ----D---- C:\Windows\SYSWOW64\migration

2012-12-13 14:42:58 ----D---- C:\Windows\SYSWOW64\en-US

2012-12-13 14:42:58 ----D---- C:\Windows\PolicyDefinitions

2012-12-13 14:42:56 ----D---- C:\Windows\system32\wbem

2012-12-13 14:42:56 ----D---- C:\Windows\system32\migration

2012-12-13 14:42:55 ----D---- C:\Windows\system32\en-US

2012-12-13 14:42:53 ----D---- C:\Windows\AppPatch

2012-12-13 14:42:53 ----D---- C:\Program Files (x86)\Internet Explorer

2012-12-13 14:42:52 ----D---- C:\Program Files\Internet Explorer

2012-12-13 13:04:40 ----D---- C:\Program Files

2012-12-13 12:49:49 ----D---- C:\Windows\system32\catroot

2012-12-13 12:49:48 ----D---- C:\Windows\system32\catroot2

2012-12-13 12:42:21 ----A---- C:\Windows\system32\MRT.exe

2012-12-13 12:42:11 ----D---- C:\ProgramData\Microsoft Help

2012-12-13 12:42:11 ----D---- C:\Config.Msi

2012-12-13 12:36:36 ----SHD---- C:\System Volume Information

2012-12-09 21:44:05 ----D---- C:\Users\David\AppData\Roaming\Skype

2012-12-05 09:38:52 ----D---- C:\VNTI Database

2012-12-05 09:38:16 ----A---- C:\Windows\Vnti40.ini

2012-12-04 19:50:18 ----D---- C:\Windows\twain_32

2012-12-04 19:41:52 ----A---- C:\Windows\win.ini

2012-11-27 08:33:35 ----D---- C:\Users\David\AppData\Roaming\gtk-2.0

2012-11-26 14:25:45 ----HD---- C:\Program Files (x86)\InstallShield Installation Information

2012-11-26 14:25:38 ----D---- C:\Windows\Help

2012-11-26 14:21:03 ----D---- C:\Program Files (x86)\Hewlett-Packard

2012-11-26 14:18:47 ----D---- C:\Users\David\AppData\Roaming\hpqlog

2012-11-26 14:15:26 ----D---- C:\SwSetup

2012-11-26 12:18:21 ----D---- C:\Windows\system32\drivers\en-US

2012-11-26 12:18:21 ----D---- C:\Windows\system32\drivers

2012-11-26 12:18:19 ----D---- C:\Windows\system32\DriverStore

2012-11-26 12:18:17 ----D---- C:\Windows\inf

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

R0 hpdskflt;HP Filter; C:\Windows\system32\DRIVERS\hpdskflt.sys [2011-05-13 30008]

R0 pciide;pciide; C:\Windows\system32\drivers\pciide.sys [2009-07-14 12352]

R0 rdyboost;ReadyBoost; C:\Windows\System32\drivers\rdyboost.sys [2010-11-20 213888]

R0 sptd;sptd; C:\Windows\System32\Drivers\sptd.sys [2011-02-28 513080]

R1 aswKbd;aswKbd; C:\Windows\system32\drivers\aswKbd.sys [2012-02-23 28504]

R1 aswRdr;aswRdr; C:\Windows\System32\Drivers\aswrdr2.sys [2012-10-15 54072]

R1 aswSnx;aswSnx; C:\Windows\system32\drivers\aswSnx.sys [2012-10-30 984144]

R1 aswSP;aswSP; C:\Windows\system32\drivers\aswSP.sys [2012-10-30 370288]

R1 aswTdi;avast! Network Shield Support; C:\Windows\system32\drivers\aswTdi.sys [2012-10-30 59728]

R1 VWiFiFlt;Virtual WiFi Filter Driver; C:\Windows\system32\DRIVERS\vwififlt.sys [2009-07-14 59904]

R2 aswFsBlk;aswFsBlk; C:\Windows\system32\drivers\aswFsBlk.sys [2012-10-30 25232]

R2 aswMonFlt;aswMonFlt; \??\C:\Windows\system32\drivers\aswMonFlt.sys [2012-10-30 71600]

R3 Accelerometer;HP Mobile Data Protection Sensor; C:\Windows\system32\DRIVERS\Accelerometer.sys [2011-05-13 43320]

R3 AtiHdmiService;ATI Service for HD Audio Codec; C:\Windows\system32\drivers\AtiHdmi.sys [2009-06-29 116752]

R3 atikmdag;atikmdag; C:\Windows\system32\DRIVERS\atikmdag.sys [2009-07-02 6036480]

R3 AVerAF15;HP DVB-T TV Tuner; C:\Windows\System32\Drivers\AVerAF15.sys [2009-05-22 311424]

R3 BthEnum;Ovladač pro Bluetooth Request Block; C:\Windows\system32\drivers\BthEnum.sys [2009-07-14 41984]

R3 BthPan;Zařízení Bluetooth (síť PAN); C:\Windows\system32\DRIVERS\bthpan.sys [2009-07-14 118784]

R3 BTHUSB;Ovladač rozhraní USB radiostanice Bluetooth; C:\Windows\System32\Drivers\BTHUSB.sys [2011-04-28 80384]

R3 btwaudio;Bluetooth Audio Device Service; C:\Windows\system32\drivers\btwaudio.sys [2009-07-01 98344]

R3 btwavdt;Bluetooth AVDT; C:\Windows\system32\DRIVERS\btwavdt.sys [2009-07-01 132648]

R3 btwl2cap;Bluetooth L2CAP Service; C:\Windows\system32\DRIVERS\btwl2cap.sys [2009-04-08 35104]

R3 btwrchid;btwrchid; C:\Windows\system32\DRIVERS\btwrchid.sys [2009-07-01 21160]

R3 enecir;ENE CIR Receiver; C:\Windows\system32\DRIVERS\enecir.sys [2009-06-29 70656]

R3 HpqKbFiltr;HpqKbFilter Driver; C:\Windows\system32\DRIVERS\HpqKbFiltr.sys [2009-04-29 18432]

R3 mcdbus;Driver for MagicISO SCSI Host Controller; C:\Windows\system32\DRIVERS\mcdbus.sys [2009-02-24 255552]

R3 NETw5s64;Ovladač adaptéru Intel(R) Wireless WiFi Link pro systém Windows 7 64 Bit; C:\Windows\system32\DRIVERS\NETw5s64.sys [2010-01-13 7675392]

R3 pcouffin;VSO Software pcouffin; C:\Windows\System32\Drivers\pcouffin.sys [2010-11-15 82816]

R3 RFCOMM;Zařízení Bluetooth (RFCOMM protokol TDI); C:\Windows\system32\DRIVERS\rfcomm.sys [2009-07-14 158720]

R3 RTL8167;Realtek 8167 NT Driver; C:\Windows\system32\DRIVERS\Rt64win7.sys [2009-07-13 233472]

R3 STHDA;IDT High Definition Audio CODEC; C:\Windows\system32\DRIVERS\stwrt64.sys [2010-03-23 505344]

R3 SynTP;Synaptics TouchPad Driver; C:\Windows\system32\DRIVERS\SynTP.sys [2011-10-14 396848]

R3 USBPNPA;USB PnP Sound Device Interface; C:\Windows\system32\drivers\CM10864.sys [2009-12-22 1308160]

R3 vwifimp;Microsoft Virtual WiFi Miniport Service; C:\Windows\system32\DRIVERS\vwifimp.sys [2009-07-14 17920]

S3 AgereSoftModem;Agere Systems Soft Modem; C:\Windows\system32\DRIVERS\agrsm64.sys [2009-06-10 1146880]

S3 BTHPORT;Ovladač portu Bluetooth; C:\Windows\System32\Drivers\BTHport.sys [2012-07-06 552960]

S3 catchme;catchme; \??\C:\ComboFix\catchme.sys []

S3 DIRECTIO;DIRECTIO; \??\C:\windows\temp\FCT\crosse-FCT\FCT\DirectIo.sys []

S3 Dot4;MS IEEE-1284.4 Driver; C:\Windows\system32\DRIVERS\Dot4.sys [2009-07-14 145920]

S3 Dot4Print;Print Class Driver for IEEE-1284.4; C:\Windows\system32\DRIVERS\Dot4Prt.sys [2010-11-20 19968]

S3 dot4usb;MS Dot4USB Filter Dot4USB Filter; C:\Windows\system32\DRIVERS\dot4usb.sys [2009-07-14 43008]

S3 fssfltr;FssFltr; C:\Windows\system32\DRIVERS\fssfltr.sys [2010-09-22 48488]

S3 igfx;igfx; C:\Windows\system32\DRIVERS\igdkmd64.sys [2009-06-10 6108416]

S3 JMCR;JMCR; C:\Windows\system32\DRIVERS\jmcr.sys [2009-07-21 140712]

S3 NETw1v64;Intel(R) Wireless WiFi Link 1000 Series Adapter Driver for Windows Vista 64 Bit; C:\Windows\system32\DRIVERS\NETw1v64.sys [2009-07-21 7058432]

S3 netw5v64;Intel(R) Wireless WiFi Link 5000 Series Adapter Driver for Windows Vista 64 Bit; C:\Windows\system32\DRIVERS\netw5v64.sys [2009-06-10 5434368]

S3 pccsmcfd;PCCS Mode Change Filter Driver; C:\Windows\system32\DRIVERS\pccsmcfdx64.sys [2008-08-28 25600]

S3 RdpVideoMiniport;Remote Desktop Video Miniport Driver; C:\Windows\System32\drivers\rdpvideominiport.sys [2012-08-23 19456]

S3 RivaTuner64;RivaTuner64; \??\C:\Program Files (x86)\RivaTuner v2.24 MSI Master Overclocking Arena 2009 edition\RivaTuner64.sys []

S3 sdbus;sdbus; C:\Windows\system32\drivers\sdbus.sys [2010-11-20 109056]

S3 SrvHsfHDA;SrvHsfHDA; C:\Windows\system32\DRIVERS\VSTAZL6.SYS [2009-06-10 292864]

S3 SrvHsfV92;SrvHsfV92; C:\Windows\system32\DRIVERS\VSTDPV6.SYS [2009-06-10 1485312]

S3 SrvHsfWinac;SrvHsfWinac; C:\Windows\system32\DRIVERS\VSTCNXT6.SYS [2009-06-10 740864]

S3 TsUsbFlt;TsUsbFlt; C:\Windows\system32\drivers\tsusbflt.sys [2012-08-23 57856]

S3 usbscan;Ovladač skeneru USB; C:\Windows\system32\DRIVERS\usbscan.sys [2009-07-14 41984]

S3 VCSVADHWSer;Avnex Virtual Audio Device (WDM); C:\Windows\system32\DRIVERS\vcsvad.sys [2008-12-26 21504]

======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 [2012-07-27 63960]

R2 AESTFilters;Andrea ST Filters Service; C:\Windows\System32\DriverStore\FileRepository\stwrt64.inf_amd64_neutral_70dacb64382a61a7\AESTSr64.exe [2009-03-02 89600]

R2 AMD External Events Utility;AMD External Events Utility; C:\Windows\system32\atiesrxx.exe [2009-07-02 203264]

R2 avast! Antivirus;avast! Antivirus; C:\Program Files\AVAST Software\Avast\AvastSvc.exe [2012-10-30 44808]

R2 Bonjour Service;Bonjour Service; C:\Program Files (x86)\Bonjour\mDNSResponder.exe [2010-10-07 345376]

R2 btwdins;Bluetooth Service; C:\Program Files\WIDCOMM\Bluetooth Software\btwdins.exe [2009-07-30 864032]

R2 DpHost;@C:\Program Files (x86)\DigitalPersona\Bin\DpHostW.exe,-128; C:\Program Files (x86)\DigitalPersona\Bin\DpHostW.exe [2009-07-17 322624]

R2 HP Support Assistant Service;HP Support Assistant Service; C:\Program Files (x86)\Hewlett-Packard\HP Support Framework\hpsa_service.exe [2012-09-27 86528]

R2 hpqddsvc;Služba HP CUE DeviceDiscovery; C:\Windows\system32\svchost.exe [2009-07-14 27136]

R2 HPSLPSVC;HP Network Devices Support; C:\Windows\system32\svchost.exe [2009-07-14 27136]

R2 hpsrv;HP Service; C:\Windows\system32\Hpservice.exe [2011-05-13 30520]

R2 LightScribeService;LightScribeService Direct Disc Labeling Service; C:\Program Files (x86)\Common Files\LightScribe\LSSrvc.exe [2009-06-17 73728]

R2 Net Driver HPZ12;Net Driver HPZ12; C:\Windows\System32\svchost.exe [2009-07-14 27136]

R2 Pml Driver HPZ12;Pml Driver HPZ12; C:\Windows\System32\svchost.exe [2009-07-14 27136]

R2 RichVideo;Cyberlink RichVideo Service(CRVS); C:\Program Files (x86)\CyberLink\Shared files\RichVideo.exe [2009-01-21 247152]

R2 SCPDFReadSpool;SolidConverterPDFReadSpool; C:\Program Files (x86)\SolidDocuments\Solid Converter PDF\SCPDFV6\SolidConverterPDFServicex64.exe [2009-09-10 320512]

R2 STacSV;Audio Service; C:\Windows\System32\DriverStore\FileRepository\stwrt64.inf_amd64_neutral_70dacb64382a61a7\STacSV64.exe [2010-03-23 247808]

R2 TVCapSvc;TV Background Capture Service (TVBCS); c:\Program Files (x86)\Hewlett-Packard\Media\Live TV\Kernel\TV\TVCapSvc.exe [2009-07-24 275840]

R2 TVSched;TV Task Scheduler (TVTS); c:\Program Files (x86)\Hewlett-Packard\Media\Live TV\Kernel\TV\TVSched.exe [2009-07-24 157056]

R2 vfsFPService;Validity Fingerprint Service; C:\Windows\system32\vfsFPService.exe [2009-06-03 721712]

R3 Com4QLBEx;Com4QLBEx; C:\Program Files (x86)\Hewlett-Packard\HP Quick Launch Buttons\Com4QLBEx.exe [2009-05-05 228408]

R3 hpqcxs08;hpqcxs08; C:\Windows\system32\svchost.exe [2009-07-14 27136]

R3 hpqwmiex;HP Software Framework Service; C:\Program Files (x86)\Hewlett-Packard\Shared\hpqWmiEx.exe [2012-08-10 1001376]

S2 clr_optimization_v4.0.30319_32;Microsoft .NET Framework NGEN v4.0.30319_X86; C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe [2010-03-18 130384]

S2 clr_optimization_v4.0.30319_64;Microsoft .NET Framework NGEN v4.0.30319_X64; C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe [2010-03-18 138576]

S2 gupdate;Služba Google Update (gupdate); C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [2010-01-14 135664]

S2 SkypeUpdate;Skype Updater; C:\Program Files (x86)\Skype\Updater\Updater.exe [2012-07-13 160944]

S3 Adobe LM Service;Adobe LM Service; C:\Program Files (x86)\Common Files\Adobe Systems Shared\Service\Adobelmsvc.exe [2010-06-01 72704]

S3 aspnet_state;Stavová služba ASP.NET; C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe [2010-03-18 44376]

S3 FirebirdServerMAGIXInstance;Firebird Server - MAGIX Instance; C:\Program Files (x86)\MAGIX\Common\Database\bin\fbserver.exe [2005-11-17 1527900]

S3 fsssvc;Windows Live Family Safety Service; C:\Program Files (x86)\Windows Live\Family Safety\fsssvc.exe [2010-09-22 1493352]

S3 GameConsoleService;GameConsoleService; C:\Program Files (x86)\HP Games\HP Game Console\GameConsoleService.exe [2009-05-22 250616]

S3 GoogleDesktopManager-051210-111108;Google Desktop Manager 5.9.1005.12335; C:\Program Files (x86)\Google\Google Desktop Search\GoogleDesktop.exe [2010-07-14 30192]

S3 gupdatem;Služba Google Update (gupdatem); C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [2010-01-14 135664]

S3 gusvc;Google Software Updater; C:\Program Files (x86)\Google\Common\Google Updater\GoogleUpdaterService.exe [2012-08-14 194032]

S3 Microsoft Office Groove Audit Service;Microsoft Office Groove Audit Service; C:\Program Files (x86)\Microsoft Office\Office12\GrooveAuditService.exe [2009-02-26 64856]

S3 odserv;Microsoft Office Diagnostics Service; C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\ODSERV.EXE [2011-07-20 440696]

S3 ose;Office Source Engine; C:\Program Files (x86)\Common Files\Microsoft Shared\Source Engine\OSE.EXE [2006-10-26 145184]

S3 ServiceLayer;ServiceLayer; C:\Program Files (x86)\PC Connectivity Solution\ServiceLayer.exe [2009-03-04 621056]

S3 WatAdminSvc;@%SystemRoot%\system32\Wat\WatUX.exe,-601; C:\Windows\system32\Wat\WatAdminSvc.exe [2010-05-18 1255736]

S4 avast! Firewall;avast! Firewall; C:\Program Files\AVAST Software\Avast\afwServ.exe []

S4 NetMsmqActivator;@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelInstallRC.dll,-8195; C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe [2010-03-18 124240]

S4 NetPipeActivator;@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelInstallRC.dll,-8197; C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe [2010-03-18 124240]

S4 NetTcpActivator;@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelInstallRC.dll,-8199; C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe [2010-03-18 124240]

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