OTL txt

OTL logfile created on: 23/02/2013 17:28:09 - Run 1

OTL by OldTimer - Version 3.2.69.0 Folder = C:\Users\serge-corinne\Downloads

64bit- Home Premium Edition Service Pack 1 (Version = 6.1.7601) - Type = NTWorkstation

Internet Explorer (Version = 9.0.8112.16421)

Locale: 0000040C | Country: France | Language: FRA | Date Format: dd/MM/yyyy

3,68 Gb Total Physical Memory | 2,31 Gb Available Physical Memory | 62,84% Memory free

7,35 Gb Paging File | 5,79 Gb Available in Paging File | 78,76% Paging File free

Paging file location(s): ?:\pagefile.sys [binary data]

%SystemDrive% = C: | %SystemRoot% = C:\Windows | %ProgramFiles% = C:\Program Files (x86)

Drive C: | 452,16 Gb Total Space | 305,50 Gb Free Space | 67,56% Space Free | Partition Type: NTFS

Computer Name: SG | User Name: serge-corinne | Logged in as Administrator.

Boot Mode: Normal | Scan Mode: Current user | Include 64bit Scans

Company Name Whitelist: Off | Skip Microsoft Files: Off | No Company Name Whitelist: On | File Age = 30 Days

[color=#E56717]========== Processes (SafeList) ==========[/color]

PRC - C:\Users\serge-corinne\Downloads\OTL.exe (OldTimer Tools)

PRC - C:\Windows\SysWOW64\Macromed\Flash\FlashUtil32\_11\_5\_502\_149\_ActiveX.exe (Adobe Systems Incorporated)

PRC - C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe (Adobe Systems Incorporated)

PRC - C:\Program Files (x86)\TomTom HOME 2\TomTomHOMEService.exe (TomTom)

PRC - C:\Program Files\AVAST Software\Avast\AvastUI.exe (AVAST Software)

PRC - C:\Program Files\AVAST Software\Avast\AvastSvc.exe (AVAST Software)

PRC - C:\Program Files\Acer\Acer Updater\UpdaterService.exe (Acer Incorporated)

PRC - C:\Program Files (x86)\NVIDIA Corporation\NVIDIA Updatus\daemonu.exe (NVIDIA Corporation)

PRC - C:\Program Files (x86)\Acer\clear.fi\MVP\clear.fiAgent.exe (CyberLink Corp.)

PRC - C:\Program Files (x86)\Acer\clear.fi\MVP\.\Kernel\DMR\DMREngine.exe ()

PRC - C:\Program Files (x86)\Launch Manager\LMutilps32.exe (Dritek System Inc.)

PRC - C:\Program Files (x86)\Launch Manager\dsiwmis.exe (Dritek System Inc.)

PRC - C:\Program Files (x86)\Acer\Registration\GREGsvc.exe (Acer Incorporated)

PRC - C:\Program Files (x86)\NTI\Acer Backup Manager\IScheduleSvc.exe (NTI Corporation)

PRC - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\UNS\UNS.exe (Intel Corporation)

PRC - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe (Intel Corporation)

PRC - C:\Program Files (x86)\Sony Ericsson\Sony Ericsson PC Suite\SupServ.exe ()

[color=#E56717]========== Modules (No Company Name) ==========[/color]

MOD - C:\Program Files (x86)\Acer\clear.fi\MVP\Kernel\DMR\CLNetMediaDMA.dll ()

MOD - C:\Program Files (x86)\Acer\clear.fi\MVP\.\Kernel\DMR\DMREngine.exe ()

[color=#E56717]========== Services (SafeList) ==========[/color]

SRV:[b]64bit:[/b] - (avast! Antivirus) -- C:\Program Files\AVAST Software\Avast\AvastSvc.exe (AVAST Software)

SRV:[b]64bit:[/b] - (Live Updater Service) -- C:\Program Files\Acer\Acer Updater\UpdaterService.exe (Acer Incorporated)

SRV:[b]64bit:[/b] - (ePowerSvc) -- C:\Program Files\Acer\Acer ePower Management\ePowerSvc.exe (Acer Incorporated)

SRV:[b]64bit:[/b] - (wlcrasvc) -- C:\Program Files\Windows Live\Mesh\wlcrasvc.exe (Microsoft Corporation)

SRV:[b]64bit:[/b] - (WinDefend) -- C:\Program Files\Windows Defender\mpsvc.dll (Microsoft Corporation)

SRV - (AdobeFlashPlayerUpdateSvc) -- C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe (Adobe Systems Incorporated)

SRV - (AdobeARMservice) -- C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe (Adobe Systems Incorporated)

SRV - (TomTomHOMEService) -- C:\Program Files (x86)\TomTom HOME 2\TomTomHOMEService.exe (TomTom)

SRV - (SkypeUpdate) -- C:\Program Files (x86)\Skype\Updater\Updater.exe (Skype Technologies)

SRV - (FLEXnet Licensing Service) -- C:\Program Files (x86)\Common Files\Macrovision Shared\FLEXnet Publisher\FNPLicensingService.exe (Acresso Software Inc.)

SRV - (nvUpdatusService) -- C:\Program Files (x86)\NVIDIA Corporation\NVIDIA Updatus\daemonu.exe (NVIDIA Corporation)

SRV - (DsiWMIService) -- C:\Program Files (x86)\Launch Manager\dsiwmis.exe (Dritek System Inc.)

SRV - (EgisTec Ticket Service) -- C:\Program Files (x86)\Common Files\EgisTec\Services\EgisTicketService.exe (Egis Technology Inc. )

SRV - (GREGService) -- C:\Program Files (x86)\Acer\Registration\GREGsvc.exe (Acer Incorporated)

SRV - (NTI IScheduleSvc) -- C:\Program Files (x86)\NTI\Acer Backup Manager\IScheduleSvc.exe (NTI Corporation)

SRV - (GamesAppService) -- C:\Program Files (x86)\WildTangent Games\App\GamesAppService.exe (WildTangent, Inc.)

SRV - (UNS) -- C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\UNS\UNS.exe (Intel Corporation)

SRV - (LMS) -- C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe (Intel Corporation)

SRV - (NOBU) -- C:\Program Files (x86)\Symantec\Norton Online Backup\NOBuAgent.exe (Symantec Corporation)

SRV - (clr\_optimization\_v4.0.30319\_32) -- C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe (Microsoft Corporation)

SRV - (clr\_optimization\_v2.0.50727\_32) -- C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe (Microsoft Corporation)

SRV - (OMSI download service) -- C:\Program Files (x86)\Sony Ericsson\Sony Ericsson PC Suite\SupServ.exe ()

[color=#E56717]========== Driver Services (SafeList) ==========[/color]

DRV:[b]64bit:[/b] - (aswSnx) -- C:\Windows\SysNative\drivers\aswSnx.sys (AVAST Software)

DRV:[b]64bit:[/b] - (aswSP) -- C:\Windows\SysNative\drivers\aswSP.sys (AVAST Software)

DRV:[b]64bit:[/b] - (aswTdi) -- C:\Windows\SysNative\drivers\aswTdi.sys (AVAST Software)

DRV:[b]64bit:[/b] - (aswMonFlt) -- C:\Windows\SysNative\drivers\aswMonFlt.sys (AVAST Software)

DRV:[b]64bit:[/b] - (aswRdr) -- C:\Windows\SysNative\drivers\aswRdr2.sys (AVAST Software)

DRV:[b]64bit:[/b] - (aswFsBlk) -- C:\Windows\SysNative\drivers\aswFsBlk.sys (AVAST Software)

DRV:[b]64bit:[/b] - (Fs\_Rec) -- C:\Windows\SysNative\drivers\fs\_rec.sys (Microsoft Corporation)

DRV:[b]64bit:[/b] - (mwlPSDVDisk) -- C:\Windows\SysNative\drivers\mwlPSDVDisk.sys (Egis Technology Inc.)

DRV:[b]64bit:[/b] - (mwlPSDFilter) -- C:\Windows\SysNative\drivers\mwlPSDFilter.sys (Egis Technology Inc.)

DRV:[b]64bit:[/b] - (mwlPSDNServ) -- C:\Windows\SysNative\drivers\mwlPSDNserv.sys (Egis Technology Inc.)

DRV:[b]64bit:[/b] - (nvpciflt) -- C:\Windows\SysNative\drivers\nvpciflt.sys (NVIDIA Corporation)

DRV:[b]64bit:[/b] - (NTIDrvr) -- C:\Windows\SysNative\drivers\NTIDrvr.sys (NTI Corporation)

DRV:[b]64bit:[/b] - (UBHelper) -- C:\Windows\SysNative\drivers\UBHelper.sys (NTI Corporation)

DRV:[b]64bit:[/b] - (igfx) -- C:\Windows\SysNative\drivers\igdkmd64.sys (Intel Corporation)

DRV:[b]64bit:[/b] - (amdsata) -- C:\Windows\SysNative\drivers\amdsata.sys (Advanced Micro Devices)

DRV:[b]64bit:[/b] - (amdxata) -- C:\Windows\SysNative\drivers\amdxata.sys (Advanced Micro Devices)

DRV:[b]64bit:[/b] - (athr) -- C:\Windows\SysNative\drivers\athrx.sys (Atheros Communications, Inc.)

DRV:[b]64bit:[/b] - (SynTP) -- C:\Windows\SysNative\drivers\SynTP.sys (Synaptics Incorporated)

DRV:[b]64bit:[/b] - (L1C) -- C:\Windows\SysNative\drivers\L1C62x64.sys (Atheros Communications, Inc.)

DRV:[b]64bit:[/b] - (RSUSBSTOR) -- C:\Windows\SysNative\drivers\RtsUStor.sys (Realtek Semiconductor Corp.)

DRV:[b]64bit:[/b] - (TsUsbFlt) -- C:\Windows\SysNative\drivers\TsUsbFlt.sys (Microsoft Corporation)

DRV:[b]64bit:[/b] - (HpSAMD) -- C:\Windows\SysNative\drivers\HpSAMD.sys (Hewlett-Packard Company)

DRV:[b]64bit:[/b] - (TsUsbGD) -- C:\Windows\SysNative\drivers\TsUsbGD.sys (Microsoft Corporation)

DRV:[b]64bit:[/b] - (iaStor) -- C:\Windows\SysNative\drivers\iaStor.sys (Intel Corporation)

DRV:[b]64bit:[/b] - (IntcDAud) -- C:\Windows\SysNative\drivers\IntcDAud.sys (Intel(R) Corporation)

DRV:[b]64bit:[/b] - (Impcd) -- C:\Windows\SysNative\drivers\Impcd.sys (Intel Corporation)

DRV:[b]64bit:[/b] - (BR\_MCU) -- C:\Windows\SysNative\drivers\br\_mcu2usb.sys (Windows (R) Win 7 DDK provider)

DRV:[b]64bit:[/b] - (HECIx64) -- C:\Windows\SysNative\drivers\HECIx64.sys (Intel Corporation)

DRV:[b]64bit:[/b] - (amdsbs) -- C:\Windows\SysNative\drivers\amdsbs.sys (AMD Technologies Inc.)

DRV:[b]64bit:[/b] - (LSI\_SAS2) -- C:\Windows\SysNative\drivers\lsi\_sas2.sys (LSI Corporation)

DRV:[b]64bit:[/b] - (stexstor) -- C:\Windows\SysNative\drivers\stexstor.sys (Promise Technology)

DRV:[b]64bit:[/b] - (ebdrv) -- C:\Windows\SysNative\drivers\evbda.sys (Broadcom Corporation)

DRV:[b]64bit:[/b] - (b06bdrv) -- C:\Windows\SysNative\drivers\bxvbda.sys (Broadcom Corporation)

DRV:[b]64bit:[/b] - (b57nd60a) -- C:\Windows\SysNative\drivers\b57nd60a.sys (Broadcom Corporation)

DRV:[b]64bit:[/b] - (hcw85cir) -- C:\Windows\SysNative\drivers\hcw85cir.sys (Hauppauge Computer Works, Inc.)

DRV:[b]64bit:[/b] - (s1018mdm) -- C:\Windows\SysNative\drivers\s1018mdm.sys (MCCI Corporation)

DRV:[b]64bit:[/b] - (s1018unic) -- C:\Windows\SysNative\drivers\s1018unic.sys (MCCI Corporation)

DRV:[b]64bit:[/b] - (s1018mgmt) -- C:\Windows\SysNative\drivers\s1018mgmt.sys (MCCI Corporation)

DRV:[b]64bit:[/b] - (s1018obex) -- C:\Windows\SysNative\drivers\s1018obex.sys (MCCI Corporation)

DRV:[b]64bit:[/b] - (s1018bus) -- C:\Windows\SysNative\drivers\s1018bus.sys (MCCI Corporation)

DRV:[b]64bit:[/b] - (s1018nd5) -- C:\Windows\SysNative\drivers\s1018nd5.sys (MCCI Corporation)

DRV:[b]64bit:[/b] - (s1018mdfl) -- C:\Windows\SysNative\drivers\s1018mdfl.sys (MCCI Corporation)

DRV - (WIMMount) -- C:\Windows\SysWOW64\drivers\wimmount.sys (Microsoft Corporation)

[color=#E56717]========== Standard Registry (SafeList) ==========[/color]

[color=#E56717]========== Internet Explorer ==========[/color]

IE:[b]64bit:[/b] - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Default\_Page\_URL = http://acer.msn.com

IE:[b]64bit:[/b] - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = http://acer.msn.com

IE:[b]64bit:[/b] - HKLM\..\SearchScopes,DefaultScope =

IE:[b]64bit:[/b] - HKLM\..\SearchScopes\{0633EE93-D776-472f-A0FF-E1416B8B2E3A}: "URL" = http://www.bing.com/search?q={searchTerms}&form=AARTDF&pc=MAAR&src=IE-SearchBox

IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Default\_Page\_URL = http://acer.msn.com

IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Local Page = C:\Windows\SysWOW64\blank.htm

IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = http://www.google.fr

IE - HKLM\..\SearchScopes,DefaultScope =

IE - HKLM\..\SearchScopes\{0633EE93-D776-472f-A0FF-E1416B8B2E3A}: "URL" = http://www.bing.com/search?q={searchTerms}&form=AARTDF&pc=MAAR&src=IE-SearchBox

IE - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Default\_Page\_URL = http://acer.msn.com

IE - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = http://www.google.fr/

IE - HKCU\..\URLSearchHook: {8e5025c2-8ea3-430d-80b8-a14151068a6d} - No CLSID value found

IE - HKCU\..\SearchScopes,DefaultScope = {0633EE93-D776-472f-A0FF-E1416B8B2E3A}

IE - HKCU\..\SearchScopes\{A531D99C-5A22-449b-83DA-872725C6D0ED}: "URL" = http://search.alot.com/web?q={searchTerms}&pr=prov&client\_id=6C1194A001CDDF5800466E5D&install\_time=2012-12-21T08:52:01Z&src\_id=30159&camp\_id=3334&tb\_version=1.3.0001.0(B)

IE - HKCU\..\SearchScopes\{C5A0D89E-A282-462A-A362-560F09B24FE9}: "URL" = http://search.conduit.com/ResultsExt.aspx?q={searchTerms}&SearchSource=4&ctid=CT3128284

IE - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings: "ProxyEnable" = 0

IE - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings: "ProxyOverride" = <local>

[color=#E56717]========== FireFox ==========[/color]

FF - user.js - File not found

FF:[b]64bit:[/b] - HKLM\Software\MozillaPlugins\@adobe.com/FlashPlayer: C:\Windows\system32\Macromed\Flash\NPSWF64\_11\_5\_502\_149.dll File not found

FF:[b]64bit:[/b] - HKLM\Software\MozillaPlugins\@microsoft.com/GENUINE: disabled File not found

FF:[b]64bit:[/b] - HKLM\Software\MozillaPlugins\@microsoft.com/OfficeAuthz,version=14.0: C:\PROGRA~1\MICROS~2\Office14\NPAUTHZ.DLL (Microsoft Corporation)

FF - HKLM\Software\MozillaPlugins\@adobe.com/FlashPlayer: C:\Windows\SysWOW64\Macromed\Flash\NPSWF32\_11\_5\_502\_149.dll ()

FF - HKLM\Software\MozillaPlugins\@canon.com/EPPEX: C:\Program Files\Canon\Easy-PhotoPrint EX\NPEZFFPI.DLL (CANON INC.)

FF - HKLM\Software\MozillaPlugins\@google.com/npPicasa3,version=3.0.0: C:\Program Files (x86)\Google\Picasa3\npPicasa3.dll (Google, Inc.)

FF - HKLM\Software\MozillaPlugins\@microsoft.com/GENUINE: disabled File not found

FF - HKLM\Software\MozillaPlugins\@Microsoft.com/NpCtrl,version=1.0: c:\Program Files (x86)\Microsoft Silverlight\4.1.10329.0\npctrl.dll ( Microsoft Corporation)

FF - HKLM\Software\MozillaPlugins\@microsoft.com/OfficeAuthz,version=14.0: C:\PROGRA~2\MICROS~4\Office14\NPAUTHZ.DLL (Microsoft Corporation)

FF - HKLM\Software\MozillaPlugins\@microsoft.com/SharePoint,version=14.0: C:\PROGRA~2\MICROS~4\Office14\NPSPWRAP.DLL (Microsoft Corporation)

FF - HKLM\Software\MozillaPlugins\@microsoft.com/WLPG,version=15.4.3502.0922: C:\Program Files (x86)\Windows Live\Photo Gallery\NPWLPG.dll (Microsoft Corporation)

FF - HKLM\Software\MozillaPlugins\@microsoft.com/WLPG,version=15.4.3538.0513: C:\Program Files (x86)\Windows Live\Photo Gallery\NPWLPG.dll (Microsoft Corporation)

FF - HKLM\Software\MozillaPlugins\@microsoft.com/WLPG,version=15.4.3555.0308: C:\Program Files (x86)\Windows Live\Photo Gallery\NPWLPG.dll (Microsoft Corporation)

FF - HKLM\Software\MozillaPlugins\@tools.google.com/Google Update;version=3: C:\Program Files (x86)\Google\Update\1.3.21.135\npGoogleUpdate3.dll (Google Inc.)

FF - HKLM\Software\MozillaPlugins\@tools.google.com/Google Update;version=9: C:\Program Files (x86)\Google\Update\1.3.21.135\npGoogleUpdate3.dll (Google Inc.)

FF - HKLM\Software\MozillaPlugins\@WildTangent.com/GamesAppPresenceDetector,Version=1.0: C:\Program Files (x86)\WildTangent Games\App\BrowserIntegration\Registered\1\NP\_wtapp.dll ()

FF - HKLM\Software\MozillaPlugins\Adobe Reader: C:\Program Files (x86)\Adobe\Reader 10.0\Reader\AIR\nppdf32.dll (Adobe Systems Inc.)

FF - HKCU\Software\MozillaPlugins\@squareclock.com/SQ3DPlayer\_Production\_Castorama\_Internet: C:\Users\serge-corinne\AppData\Local\SquareClock.Production\_Castorama\_Internet\NPSQ3D.dll (SquareClock SAS)

FF - HKEY\_LOCAL\_MACHINE\software\mozilla\Firefox\Extensions\\wrc@avast.com: C:\Program Files\AVAST Software\Avast\WebRep\FF [2012/09/23 10:59:12 | 000,000,000 | ---D | M]

[2012/08/10 08:47:34 | 000,000,000 | ---D | M] (No name found) -- C:\Users\serge-corinne\AppData\Roaming\mozilla\Extensions

[2012/08/10 08:47:34 | 000,000,000 | ---D | M] (No name found) -- C:\Users\serge-corinne\AppData\Roaming\mozilla\Extensions\home2@tomtom.com

[2013/02/23 17:11:55 | 000,000,000 | ---D | M] (No name found) -- C:\Users\serge-corinne\AppData\Roaming\mozilla\Firefox\Profiles\2bzjiisr.default\extensions

[color=#E56717]========== Chrome ==========[/color]

CHR - homepage: http://www.google.com/

CHR - default\_search\_provider: Conduit (Enabled)

CHR - default\_search\_provider: search\_url = {google:baseURL}search?q={searchTerms}&{google:RLZ}{google:acceptedSuggestion}{google:originalQueryForSuggestion}{google:searchFieldtrialParameter}sourceid=chrome&ie={inputEncoding}

CHR - default\_search\_provider: suggest\_url =

CHR - homepage: http://www.google.com/

CHR - plugin: Remoting Viewer (Enabled) = internal-remoting-viewer

CHR - plugin: Native Client (Enabled) = C:\Program Files (x86)\Google\Chrome\Application\24.0.1312.57\ppGoogleNaClPluginChrome.dll

CHR - plugin: Chrome PDF Viewer (Enabled) = C:\Program Files (x86)\Google\Chrome\Application\24.0.1312.57\pdf.dll

CHR - plugin: Shockwave Flash (Enabled) = C:\Program Files (x86)\Google\Chrome\Application\24.0.1312.57\gcswf32.dll

CHR - plugin: Adobe Acrobat (Enabled) = C:\Program Files (x86)\Adobe\Reader 10.0\Reader\Browser\nppdf32.dll

CHR - plugin: Microsoft Office 2010 (Enabled) = C:\PROGRA~2\MICROS~4\Office14\NPAUTHZ.DLL

CHR - plugin: Microsoft Office 2010 (Enabled) = C:\PROGRA~2\MICROS~4\Office14\NPSPWRAP.DLL

CHR - plugin: Google Earth Plugin (Enabled) = C:\Program Files (x86)\Google\Google Earth\plugin\npgeplugin.dll

CHR - plugin: Google Update (Enabled) = C:\Program Files (x86)\Google\Update\1.3.21.111\npGoogleUpdate3.dll

CHR - plugin: Windows Live\u0099 Photo Gallery (Enabled) = C:\Program Files (x86)\Windows Live\Photo Gallery\NPWLPG.dll

CHR - plugin: CANON iMAGE GATEWAY Album Plugin Utility (Enabled) = C:\Program Files\Canon\Easy-PhotoPrint EX\NPEZFFPI.DLL

CHR - plugin: Silverlight Plug-In (Enabled) = c:\Program Files (x86)\Microsoft Silverlight\4.1.10329.0\npctrl.dll

CHR - Extension: YouTube = C:\Users\serge-corinne\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.5\_1\

CHR - Extension: Recherche Google = C:\Users\serge-corinne\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.19\_1\

CHR - Extension: avast! WebRep = C:\Users\serge-corinne\AppData\Local\Google\Chrome\User Data\Default\Extensions\icmlaeflemplmjndnaapfdbbnpncnbda\7.0.1466\_0\

CHR - Extension: Gmail = C:\Users\serge-corinne\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_1\

O1 HOSTS File: ([2009/06/10 22:00:26 | 000,000,824 | ---- | M]) - C:\Windows\SysNative\drivers\etc\hosts

O2:[b]64bit:[/b] - BHO: (avast! WebRep) - {318A227B-5E9F-45bd-8999-7F8F10CA4CF5} - C:\Program Files\AVAST Software\Avast\aswWebRepIE64.dll (AVAST Software)

O2:[b]64bit:[/b] - BHO: (Google Toolbar Helper) - {AA58ED58-01DD-4d91-8333-CF10577473F7} - C:\Program Files (x86)\Google\Google Toolbar\GoogleToolbar\_64.dll (Google Inc.)

O2:[b]64bit:[/b] - BHO: (Office Document Cache Handler) - {B4F3A835-0E21-4959-BA22-42B3008E02FF} - C:\PROGRA~1\MICROS~2\Office14\URLREDIR.DLL (Microsoft Corporation)

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

O3:[b]64bit:[/b] - HKLM\..\Toolbar: (Google Toolbar) - {2318C2B1-4965-11d4-9B18-009027A5CD4F} - C:\Program Files (x86)\Google\Google Toolbar\GoogleToolbar\_64.dll (Google Inc.)

O3:[b]64bit:[/b] - HKLM\..\Toolbar: (avast! WebRep) - {318A227B-5E9F-45bd-8999-7F8F10CA4CF5} - C:\Program Files\AVAST Software\Avast\aswWebRepIE64.dll (AVAST Software)

O3:[b]64bit:[/b] - HKLM\..\Toolbar: (no name) - Locked - No CLSID value found.

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

O3 - HKLM\..\Toolbar: (no name) - Locked - No CLSID value found.

O3 - HKCU\..\Toolbar\WebBrowser: (no name) - {8E5025C2-8EA3-430D-80B8-A14151068A6D} - No CLSID value found.

O4:[b]64bit:[/b] - HKLM..\Run: [HotKeysCmds] C:\Windows\SysNative\hkcmd.exe (Intel Corporation)

O4:[b]64bit:[/b] - HKLM..\Run: [IgfxTray] C:\Windows\SysNative\igfxtray.exe (Intel Corporation)

O4:[b]64bit:[/b] - HKLM..\Run: [Persistence] C:\Windows\SysNative\igfxpers.exe (Intel Corporation)

O4 - HKLM..\Run: [avast] C:\Program Files\AVAST Software\Avast\avastUI.exe (AVAST Software)

O6 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer: NoActiveDesktop = 1

O6 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer: NoActiveDesktopChanges = 1

O6 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\System: ConsentPromptBehaviorAdmin = 5

O6 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\System: ConsentPromptBehaviorUser = 3

O8:[b]64bit:[/b] - Extra context menu item: Add to Google Photos Screensa&ver - res://C:\Windows\system32\GPhotos.scr/200 File not found

O8 - Extra context menu item: Add to Google Photos Screensa&ver - C:\Windows\SysWow64\GPhotos.scr (Google Inc.)

O9 - Extra Button: @C:\Program Files (x86)\Evernote\Evernote\Resource.dll,-101 - {A95fe080-8f5d-11d2-a20b-00aa003c157a} - C:\Program Files (x86)\Evernote\Evernote\EvernoteIE.dll (Evernote Corp., 333 W Evelyn Ave. Mountain View, CA 94041)

O9 - Extra 'Tools' menuitem : @C:\Program Files (x86)\Evernote\Evernote\Resource.dll,-101 - {A95fe080-8f5d-11d2-a20b-00aa003c157a} - C:\Program Files (x86)\Evernote\Evernote\EvernoteIE.dll (Evernote Corp., 333 W Evelyn Ave. Mountain View, CA 94041)

O13[b]64bit:[/b] - gopher Prefix: missing

O13 - gopher Prefix: missing

O16 - DPF: {1ABA5FAC-1417-422B-BA82-45C35E2C908B} http://kitchenplanner.ikea.com/fr/Core/Player/2020PlayerAX\_IKEA\_Win32.cab (20-20 3D Viewer for IKEA)

O16 - DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000} http://fpdownload2.macromedia.com/get/shockwave/cabs/flash/swflash.cab (Shockwave Flash Object)

O17 - HKLM\System\CCS\Services\Tcpip\Parameters: DhcpNameServer = 192.168.1.1 192.168.1.1

O17 - HKLM\System\CCS\Services\Tcpip\Parameters\Interfaces\{99E70B42-4F6E-46F6-BD16-5AC32E76E895}: DhcpNameServer = 192.168.1.1 192.168.1.1

O18:[b]64bit:[/b] - Protocol\Handler\livecall - No CLSID value found

O18:[b]64bit:[/b] - Protocol\Handler\ms-help - No CLSID value found

O18:[b]64bit:[/b] - Protocol\Handler\msnim - No CLSID value found

O18:[b]64bit:[/b] - Protocol\Handler\skype4com - No CLSID value found

O18:[b]64bit:[/b] - Protocol\Handler\wlmailhtml - No CLSID value found

O18:[b]64bit:[/b] - Protocol\Handler\wlpg - No CLSID value found

O18 - Protocol\Handler\skype4com {FFC8B962-9B40-4DFF-9458-1830C7DD7F5D} - C:\Program Files (x86)\Common Files\Skype\Skype4COM.dll (Skype Technologies)

O20:[b]64bit:[/b] - AppInit\_DLLs: (C:\Windows\system32\nvinitx.dll) - C:\Windows\SysNative\nvinitx.dll (NVIDIA Corporation)

O20 - AppInit\_DLLs: (C:\Windows\SysWOW64\nvinit.dll) - C:\Windows\SysWOW64\nvinit.dll (NVIDIA Corporation)

O20:[b]64bit:[/b] - HKLM Winlogon: Shell - (explorer.exe) - C:\Windows\explorer.exe (Microsoft Corporation)

O20:[b]64bit:[/b] - HKLM Winlogon: UserInit - (C:\Windows\system32\userinit.exe) - C:\Windows\SysNative\userinit.exe (Microsoft Corporation)

O20 - HKLM Winlogon: Shell - (explorer.exe) - C:\Windows\SysWow64\explorer.exe (Microsoft Corporation)

O20 - HKLM Winlogon: UserInit - (userinit.exe) - C:\Windows\SysWow64\userinit.exe (Microsoft Corporation)

O20:[b]64bit:[/b] - Winlogon\Notify\igfxcui: DllName - (igfxdev.dll) - C:\Windows\SysNative\igfxdev.dll (Intel Corporation)

O21:[b]64bit:[/b] - SSODL: WebCheck - {E6FB5E20-DE35-11CF-9C87-00AA005127ED} - No CLSID value found.

O21 - SSODL: WebCheck - {E6FB5E20-DE35-11CF-9C87-00AA005127ED} - No CLSID value found.

O32 - HKLM CDRom: AutoRun - 1

O33 - MountPoints2\{d2e0bcd7-9b5e-11e1-a0aa-e840f231b1c4}\Shell - "" = AutoRun

O33 - MountPoints2\{d2e0bcd7-9b5e-11e1-a0aa-e840f231b1c4}\Shell\AutoRun\command - "" = E:\Startme.exe

O34 - HKLM BootExecute: (autocheck autochk \*)

O35:[b]64bit:[/b] - HKLM\..comfile [open] -- "%1" %\*

O35:[b]64bit:[/b] - HKLM\..exefile [open] -- "%1" %\*

O35 - HKLM\..comfile [open] -- "%1" %\*

O35 - HKLM\..exefile [open] -- "%1" %\*

O37:[b]64bit:[/b] - HKLM\...com [@ = comfile] -- "%1" %\*

O37:[b]64bit:[/b] - HKLM\...exe [@ = exefile] -- "%1" %\*

O37 - HKLM\...com [@ = comfile] -- "%1" %\*

O37 - HKLM\...exe [@ = exefile] -- "%1" %\*

O38 - SubSystems\\Windows: (ServerDll=winsrv:UserServerDllInitialization,3)

O38 - SubSystems\\Windows: (ServerDll=winsrv:ConServerDllInitialization,2)

O38 - SubSystems\\Windows: (ServerDll=sxssrv,4)

MsConfig:64bit - StartUpReg: [b]ArcadeMovieService[/b] - hkey= - key= - C:\Program Files (x86)\Acer\clear.fi\Movie\clear.fiMovieService.exe (CyberLink Corp.)

MsConfig:64bit - StartUpReg: [b]BackupManagerTray[/b] - hkey= - key= - C:\Program Files (x86)\NTI\Acer Backup Manager\BackupManagerTray.exe (NTI Corporation)

MsConfig:64bit - StartUpReg: [b]CanonMyPrinter[/b] - hkey= - key= - C:\Program Files\Canon\MyPrinter\BJMyPrt.exe (CANON INC.)

MsConfig:64bit - StartUpReg: [b]CanonSolutionMenu[/b] - hkey= - key= - C:\Program Files (x86)\Canon\SolutionMenu\CNSLMAIN.exe (CANON INC.)

MsConfig:64bit - StartUpReg: [b]LManager[/b] - hkey= - key= - C:\Program Files (x86)\Launch Manager\LManager.exe (Dritek System Inc.)

MsConfig:64bit - StartUpReg: [b]msnmsgr[/b] - hkey= - key= - C:\Program Files (x86)\Windows Live\Messenger\msnmsgr.exe (Microsoft Corporation)

MsConfig:64bit - StartUpReg: [b]Norton Online Backup[/b] - hkey= - key= - C:\Program Files (x86)\Symantec\Norton Online Backup\NOBuClient.exe (Symantec Corporation)

MsConfig:64bit - StartUpReg: [b]Power Management[/b] - hkey= - key= - C:\Program Files\Acer\Acer ePower Management\ePowerTray.exe (Acer Incorporated)

MsConfig:64bit - StartUpReg: [b]RTHDVCPL[/b] - hkey= - key= - C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe (Realtek Semiconductor)

MsConfig:64bit - StartUpReg: [b]SuiteTray[/b] - hkey= - key= - C:\Program Files (x86)\EgisTec MyWinLockerSuite\x86\SuiteTray.exe (Egis Technology Inc.)

MsConfig:64bit - StartUpReg: [b]SynTPEnh[/b] - hkey= - key= - C:\Program Files\Synaptics\SynTP\SynTPEnh.exe (Synaptics Incorporated)

MsConfig:64bit - StartUpReg: [b]TomTomHOME.exe[/b] - hkey= - key= - C:\Program Files (x86)\TomTom HOME 2\TomTomHOMERunner.exe (TomTom)

MsConfig:64bit - State: "startup" - Reg Error: Key error.

ActiveX:[b]64bit:[/b] {22d6f312-b0f6-11d0-94ab-0080c74c7e95} - Microsoft Windows Media Player 12.0

ActiveX:[b]64bit:[/b] {2C7339CF-2B09-4501-B3F3-F3508C9228ED} - %SystemRoot%\system32\regsvr32.exe /s /n /i:/UserInstall %SystemRoot%\system32\themeui.dll

ActiveX:[b]64bit:[/b] {3af36230-a269-11d1-b5bf-0000f8051515} - Offline Browsing Pack

ActiveX:[b]64bit:[/b] {44BBA840-CC51-11CF-AAFA-00AA00B6015C} - "%ProgramFiles%\Windows Mail\WinMail.exe" OCInstallUserConfigOE

ActiveX:[b]64bit:[/b] {44BBA855-CC51-11CF-AAFA-00AA00B6015F} - DirectDrawEx

ActiveX:[b]64bit:[/b] {45ea75a0-a269-11d1-b5bf-0000f8051515} - Internet Explorer Help

ActiveX:[b]64bit:[/b] {4f645220-306d-11d2-995d-00c04f98bbc9} - Microsoft Windows Script 5.6

ActiveX:[b]64bit:[/b] {5fd399c0-a70a-11d1-9948-00c04f98bbc9} - Internet Explorer Setup Tools

ActiveX:[b]64bit:[/b] {630b1da0-b465-11d1-9948-00c04f98bbc9} - Browsing Enhancements

ActiveX:[b]64bit:[/b] {6BF52A52-394A-11d3-B153-00C04F79FAA6} - Microsoft Windows Media Player

ActiveX:[b]64bit:[/b] {6fab99d0-bab8-11d1-994a-00c04f98bbc9} - MSN Site Access

ActiveX:[b]64bit:[/b] {7790769C-0471-11d2-AF11-00C04FA35D02} - Address Book 7

ActiveX:[b]64bit:[/b] {89820200-ECBD-11cf-8B85-00AA005B4340} - regsvr32.exe /s /n /i:U shell32.dll

ActiveX:[b]64bit:[/b] {89820200-ECBD-11cf-8B85-00AA005B4383} - C:\Windows\System32\ie4uinit.exe -BaseSettings

ActiveX:[b]64bit:[/b] {89B4C1CD-B018-4511-B0A1-5476DBF70820} - C:\Windows\system32\Rundll32.exe C:\Windows\system32\mscories.dll,Install

ActiveX:[b]64bit:[/b] {9381D8F2-0288-11D0-9501-00AA00B911A5} - Dynamic HTML Data Binding

ActiveX:[b]64bit:[/b] {C9E9A340-D1F1-11D0-821E-444553540600} - Internet Explorer Core Fonts

ActiveX:[b]64bit:[/b] {de5aed00-a4bf-11d1-9948-00c04f98bbc9} - HTML Help

ActiveX:[b]64bit:[/b] {E92B03AB-B707-11d2-9CBD-0000F87A369E} - Active Directory Service Interface

ActiveX:[b]64bit:[/b] {F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4} - .NET Framework

ActiveX:[b]64bit:[/b] {FEBEF00C-046D-438D-8A88-BF94A6C9E703} - .NET Framework

ActiveX:[b]64bit:[/b] >{22d6f312-b0f6-11d0-94ab-0080c74c7e95} - %SystemRoot%\system32\unregmp2.exe /ShowWMP

ActiveX:[b]64bit:[/b] >{26923b43-4d38-484f-9b9e-de460746276c} - C:\Windows\System32\ie4uinit.exe -UserIconConfig

ActiveX:[b]64bit:[/b] >{60B49E34-C7CC-11D0-8953-00A0C90347FF} - "C:\Windows\System32\rundll32.exe" "C:\Windows\System32\iedkcs32.dll",BrandIEActiveSetup SIGNUP

ActiveX: {22d6f312-b0f6-11d0-94ab-0080c74c7e95} - Microsoft Windows Media Player 12.0

ActiveX: {2C7339CF-2B09-4501-B3F3-F3508C9228ED} - %SystemRoot%\system32\regsvr32.exe /s /n /i:/UserInstall %SystemRoot%\system32\themeui.dll

ActiveX: {3af36230-a269-11d1-b5bf-0000f8051515} - Offline Browsing Pack

ActiveX: {44BBA840-CC51-11CF-AAFA-00AA00B6015C} - "%ProgramFiles(x86)%\Windows Mail\WinMail.exe" OCInstallUserConfigOE

ActiveX: {44BBA855-CC51-11CF-AAFA-00AA00B6015F} - DirectDrawEx

ActiveX: {45ea75a0-a269-11d1-b5bf-0000f8051515} - Internet Explorer Help

ActiveX: {4f645220-306d-11d2-995d-00c04f98bbc9} - Microsoft Windows Script 5.6

ActiveX: {5fd399c0-a70a-11d1-9948-00c04f98bbc9} - Internet Explorer Setup Tools

ActiveX: {630b1da0-b465-11d1-9948-00c04f98bbc9} - Browsing Enhancements

ActiveX: {6BF52A52-394A-11d3-B153-00C04F79FAA6} - Microsoft Windows Media Player

ActiveX: {6fab99d0-bab8-11d1-994a-00c04f98bbc9} - MSN Site Access

ActiveX: {7790769C-0471-11d2-AF11-00C04FA35D02} - Address Book 7

ActiveX: {7C028AF8-F614-47B3-82DA-BA94E41B1089} - .NET Framework

ActiveX: {89820200-ECBD-11cf-8B85-00AA005B4340} - regsvr32.exe /s /n /i:U shell32.dll

ActiveX: {89820200-ECBD-11cf-8B85-00AA005B4383} - C:\Windows\SysWOW64\ie4uinit.exe -BaseSettings

ActiveX: {89B4C1CD-B018-4511-B0A1-5476DBF70820} - C:\Windows\SysWOW64\Rundll32.exe C:\Windows\SysWOW64\mscories.dll,Install

ActiveX: {8A69D345-D564-463c-AFF1-A69D9E530F96} - "C:\Program Files (x86)\Google\Chrome\Application\24.0.1312.57\Installer\chrmstp.exe" --configure-user-settings --verbose-logging --system-level --multi-install --chrome

ActiveX: {9381D8F2-0288-11D0-9501-00AA00B911A5} - Dynamic HTML Data Binding

ActiveX: {C6BAF60B-6E91-453F-BFF9-D3789CFEFCDD} - .NET Framework

ActiveX: {C9E9A340-D1F1-11D0-821E-444553540600} - Internet Explorer Core Fonts

ActiveX: {de5aed00-a4bf-11d1-9948-00c04f98bbc9} - HTML Help

ActiveX: {E92B03AB-B707-11d2-9CBD-0000F87A369E} - Active Directory Service Interface

ActiveX: {F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4} - .NET Framework

ActiveX: >{22d6f312-b0f6-11d0-94ab-0080c74c7e95} - %SystemRoot%\system32\unregmp2.exe /ShowWMP

ActiveX: >{26923b43-4d38-484f-9b9e-de460746276c} - C:\Windows\SysWOW64\ie4uinit.exe -UserIconConfig

ActiveX: >{60B49E34-C7CC-11D0-8953-00A0C90347FF} - "C:\Windows\SysWOW64\rundll32.exe" "C:\Windows\SysWOW64\iedkcs32.dll",BrandIEActiveSetup SIGNUP

Drivers32:[b]64bit:[/b] msacm.l3acm - C:\Windows\System32\l3codeca.acm (Fraunhofer Institut Integrierte Schaltungen IIS)

Drivers32: msacm.l3acm - C:\Windows\SysWow64\l3codecp.acm (Fraunhofer Institut Integrierte Schaltungen IIS)

Drivers32: msacm.l3codecp - C:\Windows\SysWow64\l3codecp.acm (Fraunhofer Institut Integrierte Schaltungen IIS)

Drivers32: vidc.cvid - C:\Windows\SysWow64\iccvid.dll (Radius Inc.)

PhysicalDisk0 MBR saved to C:\PhysicalMBR.bin

CREATERESTOREPOINT

Restore point Set: OTL Restore Point

[color=#E56717]========== Files/Folders - Created Within 30 Days ==========[/color]

[2013/02/23 08:36:33 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{469C861D-6693-41CA-8FC9-A83690A8D8F0}

[2013/02/22 16:48:58 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Roaming\NVIDIA

[2013/02/22 08:53:09 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{DA6D546C-32F3-4165-B6D0-2AF918FFC702}

[2013/02/21 20:52:43 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{0C941D59-9E39-4252-A0BB-B9FAE13B5EA1}

[2013/02/21 08:40:32 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{A276DD7A-9AC2-4967-96D9-C9919326572E}

[2013/02/20 09:52:09 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\Desktop\La Réunion

[2013/02/20 08:38:31 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{82C8BDFA-D477-44BE-9A91-AE0DCC89044B}

[2013/02/19 10:45:11 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{7787B189-A9C2-42F6-B6E6-770F174A1A05}

[2013/02/18 22:08:47 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{7533615E-7B79-4474-A22C-FE09E416EDC5}

[2013/02/18 08:34:19 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{48306BA1-D9E0-4F67-B5B4-15AAB2AB0B18}

[2013/02/17 11:47:03 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\Documents\Ambarès

[2013/02/17 09:07:44 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{E9EFCE55-83E6-427E-AAE0-E16DDF737657}

[2013/02/16 11:42:37 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{EB7586BE-58D4-4320-A591-36F735D84728}

[2013/02/15 23:04:23 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{5B8D0E65-93F1-4B4C-9472-BE2EDCCD2623}

[2013/02/15 09:38:53 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{FEAB8C02-3E36-41E9-9E70-4CB160B6A8D2}

[2013/02/14 21:38:29 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{5CEBFB96-25A1-4744-8EB2-5DA2A5BE3F96}

[2013/02/14 09:11:44 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{B0A6C4D4-80F0-400A-A0CC-30E95AC73D54}

[2013/02/13 22:51:34 | 000,096,768 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysNative\mshtmled.dll

[2013/02/13 22:51:34 | 000,073,216 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysWow64\mshtmled.dll

[2013/02/13 22:51:32 | 000,248,320 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysNative\ieui.dll

[2013/02/13 22:51:32 | 000,237,056 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysNative\url.dll

[2013/02/13 22:51:32 | 000,231,936 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysWow64\url.dll

[2013/02/13 22:51:32 | 000,176,640 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysWow64\ieui.dll

[2013/02/13 22:51:32 | 000,173,056 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysNative\ieUnatt.exe

[2013/02/13 22:51:32 | 000,142,848 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysWow64\ieUnatt.exe

[2013/02/13 22:51:31 | 001,427,968 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysWow64\inetcpl.cpl

[2013/02/13 22:51:30 | 002,312,704 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysNative\jscript9.dll

[2013/02/13 22:51:30 | 001,494,528 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysNative\inetcpl.cpl

[2013/02/13 22:51:30 | 000,729,088 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysNative\msfeeds.dll

[2013/02/13 22:51:28 | 000,816,640 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysNative\jscript.dll

[2013/02/13 22:51:28 | 000,717,824 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysWow64\jscript.dll

[2013/02/13 22:51:28 | 000,599,040 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysNative\vbscript.dll

[2013/02/13 21:08:54 | 005,553,512 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysNative\ntoskrnl.exe

[2013/02/13 21:08:53 | 003,967,848 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysWow64\ntkrnlpa.exe

[2013/02/13 21:08:50 | 003,913,064 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysWow64\ntoskrnl.exe

[2013/02/13 21:08:44 | 000,215,040 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysNative\winsrv.dll

[2013/02/13 21:08:44 | 000,025,600 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysWow64\setup16.exe

[2013/02/13 21:08:44 | 000,014,336 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysWow64\ntvdm64.dll

[2013/02/13 21:08:44 | 000,007,680 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysWow64\instnm.exe

[2013/02/13 21:08:44 | 000,005,120 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysWow64\wow32.dll

[2013/02/13 21:08:43 | 000,002,048 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysWow64\user.exe

[2013/02/13 21:08:42 | 000,288,088 | ---- | C] (Microsoft Corporation) -- C:\Windows\SysNative\drivers\FWPKCLNT.SYS

[2013/02/13 14:31:00 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{81BD414C-C6D0-4895-A952-67EFCB7F50A7}

[2013/02/11 16:23:52 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{CB95506C-D482-4CB2-B769-A609F990EE6D}

[2013/02/10 20:53:47 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{CEF98526-6B23-4D90-962A-17B34F379328}

[2013/02/10 08:48:39 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{C2CF797A-B4DD-4161-A509-21C243603F15}

[2013/02/09 20:40:04 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{3474DE9A-6239-4DF2-AF26-E5AA6AC39407}

[2013/02/09 08:39:40 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{7033487E-6E72-4A06-BDA1-8FF39AF3AB34}

[2013/02/08 08:40:48 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{00857C87-8D3A-475F-A5E1-00D072D995F4}

[2013/02/07 10:42:19 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{3C965B11-82D1-4240-B862-F85389B49B71}

[2013/02/07 09:43:00 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{0A7EC71E-94C6-4D04-99C0-07DB38EEBC9C}

[2013/02/06 21:42:36 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{371E3A49-B23F-4EB2-A5DD-343067083368}

[2013/02/06 17:16:24 | 000,000,000 | -HSD | C] -- C:\Config.Msi

[2013/02/06 09:22:53 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{AA7F4CD7-6F60-4537-B3C8-59F9D5CD7B24}

[2013/02/05 08:47:54 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{63DD3961-3073-4D16-9511-585D68481024}

[2013/02/04 22:19:26 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{4EA5DFF5-009B-4C8E-B0B1-BF0431BD21D0}

[2013/02/04 08:44:33 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{968FD762-64E2-4F11-A7A9-629448376AAE}

[2013/02/03 11:20:56 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{884CEB24-2131-461A-B486-76F9A1AE517C}

[2013/02/02 22:06:03 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{6C6353D3-FF6A-4AEC-8FC8-28C7D1F54D20}

[2013/02/02 09:31:40 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{5DE6C9E9-3A5B-4D40-B7FA-1EEA3C25C932}

[2013/02/01 20:40:57 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{BCBA8A14-7A2D-46DF-B6D6-B8ED9A1E683E}

[2013/02/01 08:40:34 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{7CDF23BD-2BF8-4AEE-9E2E-3F6A548D9167}

[2013/01/31 10:17:03 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\ElevatedDiagnostics

[2013/01/31 09:17:18 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{A701FDF2-2578-4FE3-9F5C-31A18025D643}

[2013/01/30 11:06:49 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{9C9E7DA5-B16B-497D-9C9D-E62D366FAE32}

[2013/01/29 23:02:22 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{BAD1F703-7F82-4996-A6CF-FBF5A43B1CB6}

[2013/01/29 09:39:54 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{A0536613-BC19-43DA-A981-D129CE771321}

[2013/01/28 22:03:52 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{5F7EE993-EACE-4E9F-AC17-13A2AB8C9783}

[2013/01/28 08:50:08 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{FC9B0FB9-29EC-4EC7-BCFF-9226B7DE1CCA}

[2013/01/27 09:49:01 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{14E5A181-B966-49A6-B8DD-00A494E150FD}

[2013/01/26 10:24:21 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{9DA6EDA6-7AD2-4A4D-B350-C34FDC5CE7EC}

[2013/01/25 22:12:29 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{61EB6696-32FC-43D6-ADF6-40986D5517F7}

[2013/01/25 09:17:49 | 000,000,000 | ---D | C] -- C:\Users\serge-corinne\AppData\Local\{3E900FDB-BC39-4AA6-96C0-733CEBF6B805}

[2012/05/11 14:13:59 | 000,148,736 | ---- | C] (Avanquest Software) -- C:\ProgramData\hpeEE07.dll

[2 C:\Program Files (x86)\\*.tmp files -> C:\Program Files (x86)\\*.tmp -> ]

[color=#E56717]========== Files - Modified Within 30 Days ==========[/color]

[2013/02/23 17:33:00 | 000,001,082 | ---- | M] () -- C:\Windows\tasks\GoogleUpdateTaskMachineUA.job

[2013/02/23 17:29:25 | 000,000,512 | ---- | M] () -- C:\PhysicalMBR.bin

[2013/02/23 17:20:52 | 000,016,976 | -H-- | M] () -- C:\Windows\SysNative\7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0

[2013/02/23 17:20:52 | 000,016,976 | -H-- | M] () -- C:\Windows\SysNative\7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0

[2013/02/23 17:13:36 | 000,001,078 | ---- | M] () -- C:\Windows\tasks\GoogleUpdateTaskMachineCore.job

[2013/02/23 17:13:03 | 000,067,584 | -H-- | M] () -- C:\Windows\bootstat.dat

[2013/02/23 17:12:58 | 2960,805,888 | -HS- | M] () -- C:\hiberfil.sys

[2013/02/23 16:41:00 | 000,001,002 | ---- | M] () -- C:\Windows\tasks\Adobe Flash Player Updater.job

[2013/02/20 16:44:09 | 001,549,700 | ---- | M] () -- C:\Windows\SysNative\PerfStringBackup.INI

[2013/02/20 16:44:09 | 000,704,480 | ---- | M] () -- C:\Windows\SysNative\perfh00C.dat

[2013/02/20 16:44:09 | 000,616,008 | ---- | M] () -- C:\Windows\SysNative\perfh009.dat

[2013/02/20 16:44:09 | 000,130,754 | ---- | M] () -- C:\Windows\SysNative\perfc00C.dat

[2013/02/20 16:44:09 | 000,106,388 | ---- | M] () -- C:\Windows\SysNative\perfc009.dat

[2013/02/15 17:36:49 | 000,001,961 | ---- | M] () -- C:\Users\Public\Desktop\CDBurnerXP.lnk

[2013/02/14 09:10:28 | 000,381,800 | ---- | M] () -- C:\Windows\SysNative\FNTCACHE.DAT

[2013/02/10 09:41:19 | 000,697,712 | ---- | M] (Adobe Systems Incorporated) -- C:\Windows\SysWow64\FlashPlayerApp.exe

[2013/02/10 09:41:19 | 000,074,096 | ---- | M] (Adobe Systems Incorporated) -- C:\Windows\SysWow64\FlashPlayerCPLApp.cpl

[2 C:\Program Files (x86)\\*.tmp files -> C:\Program Files (x86)\\*.tmp -> ]

[color=#E56717]========== Files Created - No Company Name ==========[/color]

[2013/02/23 17:29:25 | 000,000,512 | ---- | C] () -- C:\PhysicalMBR.bin

[2013/02/15 17:36:49 | 000,001,961 | ---- | C] () -- C:\Users\Public\Desktop\CDBurnerXP.lnk

[2012/08/04 13:38:36 | 000,000,112 | ---- | C] () -- C:\Windows\ActiveSkin.INI

[2012/05/11 13:57:15 | 000,000,053 | ---- | C] () -- C:\Windows\B51a\_Down.INI

[2011/10/27 13:08:23 | 000,066,856 | ---- | C] () -- C:\Windows\SysWow64\SynTPEnhPS.dll

[2011/10/27 13:06:58 | 000,867,020 | ---- | C] () -- C:\Windows\SysWow64\igkrng575.bin

[2011/10/27 13:06:58 | 000,105,608 | ---- | C] () -- C:\Windows\SysWow64\igfcg575m.bin

[2011/10/27 13:06:56 | 000,128,204 | ---- | C] () -- C:\Windows\SysWow64\igcompkrng575.bin

[2011/10/27 13:06:53 | 013,903,872 | ---- | C] () -- C:\Windows\SysWow64\ig4icd32.dll

[color=#E56717]========== ZeroAccess Check ==========[/color]

[2009/07/14 05:55:00 | 000,000,227 | RHS- | M] () -- C:\Windows\assembly\Desktop.ini

[HKEY\_CURRENT\_USER\Software\Classes\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1}\InProcServer32] /64

[HKEY\_CURRENT\_USER\Software\Classes\Wow6432node\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1}\InProcServer32]

[HKEY\_CURRENT\_USER\Software\Classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\InProcServer32] /64

[HKEY\_CURRENT\_USER\Software\Classes\Wow6432node\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\InProcServer32]

[HKEY\_LOCAL\_MACHINE\Software\Classes\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1}\InProcServer32] /64

"" = C:\Windows\SysNative\shell32.dll -- [2012/06/09 06:43:10 | 014,172,672 | ---- | M] (Microsoft Corporation)

"ThreadingModel" = Apartment

[HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Classes\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1}\InProcServer32]

"" = %SystemRoot%\system32\shell32.dll -- [2012/06/09 05:41:00 | 012,873,728 | ---- | M] (Microsoft Corporation)

"ThreadingModel" = Apartment

[HKEY\_LOCAL\_MACHINE\Software\Classes\clsid\{5839FCA9-774D-42A1-ACDA-D6A79037F57F}\InProcServer32] /64

"" = C:\Windows\SysNative\wbem\fastprox.dll -- [2009/07/14 02:40:51 | 000,909,312 | ---- | M] (Microsoft Corporation)

"ThreadingModel" = Free

[HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Classes\clsid\{5839FCA9-774D-42A1-ACDA-D6A79037F57F}\InProcServer32]

"" = %systemroot%\system32\wbem\fastprox.dll -- [2010/11/21 04:24:25 | 000,606,208 | ---- | M] (Microsoft Corporation)

"ThreadingModel" = Free

[HKEY\_LOCAL\_MACHINE\Software\Classes\clsid\{F3130CDB-AA52-4C3A-AB32-85FFC23AF9C1}\InProcServer32] /64

"" = C:\Windows\SysNative\wbem\wbemess.dll -- [2009/07/14 02:41:56 | 000,505,856 | ---- | M] (Microsoft Corporation)

"ThreadingModel" = Both

[HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Classes\clsid\{F3130CDB-AA52-4C3A-AB32-85FFC23AF9C1}\InProcServer32]

[color=#E56717]========== Custom Scans ==========[/color]

[color=#A23BEC]< >[/color]

[color=#A23BEC]< %systemroot%\\*. /mp /s >[/color]

[color=#A23BEC]< %systemroot%\system32\\*.dll /lockedfiles >[/color]

[2013/01/08 23:09:18 | 009,738,240 | ---- | M] (Microsoft Corporation)[b] Unable to obtain MD5[/b] -- C:\Windows\system32\ieframe.dll

[2011/09/21 10:28:13 | 000,118,784 | ---- | M] (Microsoft Corporation)[b] Unable to obtain MD5[/b] -- C:\Windows\system32\iepeers.dll

[color=#A23BEC]< %systemroot%\system32\drivers\\*.sys /lockedfiles >[/color]

[color=#A23BEC]< %systemroot%\Tasks\\*.job /lockedfiles >[/color]

Invalid Environment Variable: alluserprofile

Invalid Environment Variable: alluserprofile

[color=#A23BEC]< %appdata%\\*. >[/color]

[2012/05/10 15:25:47 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\Adobe

[2012/08/24 10:16:21 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\AVS4YOU

[2012/11/02 18:09:13 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\Canneverbe Limited

[2012/05/29 08:11:36 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\Canon

[2012/11/02 20:32:27 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\CyberLink

[2013/01/05 15:27:22 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\dvdcss

[2012/05/12 21:22:46 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\GetRightToGo

[2012/05/09 18:34:12 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\Identities

[2012/09/19 15:31:12 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\KC Softwares

[2011/10/27 13:18:58 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\Macromedia

[2012/05/11 17:32:37 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\Malwarebytes

[2010/11/21 08:16:41 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\Media Center Programs

[2012/11/02 18:09:41 | 000,000,000 | --SD | M] -- C:\Users\serge-corinne\AppData\Roaming\Microsoft

[2012/10/03 13:18:28 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\Mozilla

[2013/02/22 16:48:58 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\NVIDIA

[2012/08/01 17:59:46 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\OpenOffice.org

[2012/05/29 18:26:20 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\PhotoFiltre

[2012/09/20 15:33:37 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\PowerCinema

[2012/11/02 20:31:45 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\Skype

[2012/05/11 14:14:56 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\Sony

[2012/05/11 14:10:02 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\Sony Setup

[2012/08/10 08:47:33 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\TomTom

[2013/02/21 15:48:12 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\vlc

[2012/05/10 09:36:40 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\WildTangent

[2012/05/10 09:48:56 | 000,000,000 | ---D | M] -- C:\Users\serge-corinne\AppData\Roaming\Windows Live Writer

[color=#A23BEC]< %appdata%\\*.exe /s >[/color]

[2011/10/27 13:18:13 | 000,053,632 | ---- | M] (Adobe Systems Inc.) -- C:\Users\serge-corinne\AppData\Roaming\Macromedia\Flash Player\www.macromedia.com\bin\airappinstaller\airappinstaller.exe

[2012/05/11 14:12:46 | 000,010,134 | R--- | M] () -- C:\Users\serge-corinne\AppData\Roaming\Microsoft\Installer\{0E532C84-4275-41B3-9D81-D4A1A20D8EE7}\ARPPRODUCTICON.exe

[2012/11/12 17:57:31 | 000,388,096 | R--- | M] (Trend Micro Inc.) -- C:\Users\serge-corinne\AppData\Roaming\Microsoft\Installer\{45A66726-69BC-466B-A7A4-12FCBA4883D7}\HiJackThis.exe

[2012/05/11 14:10:39 | 033,850,672 | ---- | M] (Apple Inc.) -- C:\Users\serge-corinne\AppData\Roaming\Sony Setup\9234765D-29DF-48d0-93FB-284B7B6009B9\QuickTimeInstaller.exe

[color=#A23BEC]< %systemdrive%\\*. >[/color]

[2012/07/21 14:00:36 | 000,000,000 | -HSD | M] -- C:\$Recycle.Bin

[2012/09/15 10:21:21 | 000,000,000 | ---D | M] -- C:\5fb5eb973b959045286e319bd26e0c40

[2012/01/28 23:59:17 | 000,000,000 | -H-D | M] -- C:\book

[2013/02/23 10:19:29 | 000,000,000 | -HSD | M] -- C:\Config.Msi

[2009/07/14 06:08:56 | 000,000,000 | -HSD | M] -- C:\Documents and Settings

[2012/01/29 00:00:58 | 000,000,000 | -H-D | M] -- C:\Intel

[2012/05/10 15:02:43 | 000,000,000 | RH-D | M] -- C:\MSOCache

[2012/05/09 18:33:35 | 000,000,000 | -H-D | M] -- C:\OEM

[2009/07/14 04:20:08 | 000,000,000 | ---D | M] -- C:\PerfLogs

[2012/11/03 18:51:37 | 000,000,000 | R--D | M] -- C:\Program Files

[2013/02/23 17:11:43 | 000,000,000 | R--D | M] -- C:\Program Files (x86)

[2012/12/07 20:06:23 | 000,000,000 | -H-D | M] -- C:\ProgramData

[2012/05/09 18:31:46 | 000,000,000 | -HSD | M] -- C:\Recovery

[2013/02/23 17:29:54 | 000,000,000 | -HSD | M] -- C:\System Volume Information

[2012/07/21 14:00:11 | 000,000,000 | R--D | M] -- C:\Users

[2013/02/23 17:14:00 | 000,000,000 | ---D | M] -- C:\Windows

[color=#A23BEC]< %systemdrive%\\*.exe >[/color]

[2008/04/11 08:03:48 | 000,562,688 | ---- | M] (Microsoft Corporation) -- C:\install.exe

[2001/05/24 11:59:30 | 000,162,304 | ---- | M] () -- C:\UNWISE.EXE

[color=#A23BEC]< %programfiles%\\*. >[/color]

[2012/12/07 20:07:01 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Acer

[2011/10/27 12:40:57 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Acer Games

[2011/10/27 13:18:58 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Adobe

[2012/05/11 13:54:26 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\AlerteGPS

[2012/08/24 17:27:28 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\AVS4YOU

[2012/05/11 13:30:24 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\BooRee-USB

[2012/05/31 15:28:30 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Canon

[2013/02/16 08:52:19 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\CDBurnerXP

[2013/02/07 10:34:38 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Common Files

[2012/01/29 00:19:48 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Cyberlink

[2011/10/27 13:08:42 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\EgisTec IPS

[2011/10/27 13:08:56 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\EgisTec MyWinLocker

[2011/10/27 13:07:30 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\EgisTec MyWinLockerSuite

[2011/10/27 13:09:28 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\EgisTec Shredder

[2011/10/27 12:41:27 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Evernote

[2011/10/27 13:18:59 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Fooz Kids

[2013/02/23 10:19:29 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Google

[2013/02/16 19:28:56 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\GUMF1D8.tmp

[2012/12/08 22:45:24 | 000,000,000 | -H-D | M] -- C:\Program Files (x86)\InstallShield Installation Information

[2012/01/29 00:01:33 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Intel

[2013/02/14 09:08:14 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Internet Explorer

[2012/09/19 15:29:32 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\KC Softwares

[2012/01/29 00:06:17 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Launch Manager

[2013/01/29 21:49:41 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Malwarebytes' Anti-Malware

[2012/05/13 09:40:54 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Microsoft

[2012/05/10 15:03:30 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Microsoft Analysis Services

[2012/05/10 15:16:37 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Microsoft Office

[2012/05/11 21:41:25 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Microsoft Silverlight

[2011/10/27 12:59:54 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Microsoft SQL Server Compact Edition

[2012/05/20 21:25:46 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Microsoft.NET

[2012/11/12 09:11:05 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Mozilla Firefox

[2009/07/14 06:32:38 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\MSBuild

[2012/01/29 00:15:21 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\NTI

[2012/01/29 00:09:50 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\NVIDIA Corporation

[2012/11/27 17:22:56 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\OpenOffice.org 3

[2012/11/17 14:32:50 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\PDFCreator

[2012/05/29 18:21:39 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\PhotoFiltre

[2012/01/29 00:07:39 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Realtek

[2009/07/14 06:32:38 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Reference Assemblies

[2012/09/18 21:45:16 | 000,000,000 | R--D | M] -- C:\Program Files (x86)\Skype

[2012/05/11 17:18:10 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Sony

[2012/05/11 17:20:09 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Sony Ericsson

[2011/10/27 13:10:02 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Symantec

[2012/01/29 00:07:59 | 000,000,000 | -H-D | M] -- C:\Program Files (x86)\Temp

[2013/01/26 18:56:11 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\TomTom HOME 2

[2012/08/10 08:46:24 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\TomTom International B.V

[2012/11/12 11:18:46 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Trend Micro

[2009/07/14 05:57:06 | 000,000,000 | -H-D | M] -- C:\Program Files (x86)\Uninstall Information

[2012/05/29 15:08:30 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\VideoLAN

[2011/10/27 12:36:46 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\WildTangent Games

[2012/01/29 08:50:24 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Windows Defender

[2012/06/20 18:58:09 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Windows Live

[2012/01/29 08:50:24 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Windows Mail

[2012/01/29 08:50:24 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Windows Media Player

[2009/07/14 06:32:38 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Windows NT

[2012/01/29 08:50:24 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Windows Photo Viewer

[2010/11/21 04:31:38 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Windows Portable Devices

[2012/01/29 08:50:24 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\Windows Sidebar

[2012/08/01 17:52:57 | 000,000,000 | ---D | M] -- C:\Program Files (x86)\WiseConvert

[color=#A23BEC]< MD5 for: EXPLORER.EXE >[/color]

[2011/07/14 06:30:29 | 002,616,320 | ---- | M] (Microsoft Corporation) MD5=0FB9C74046656D1579A64660AD67B746 -- C:\Windows\winsxs\wow64\_microsoft-windows-explorer\_31bf3856ad364e35\_6.1.7601.21669\_none\_ba87e574ddfe652d\explorer.exe

[2011/07/14 06:30:29 | 002,871,808 | ---- | M] (Microsoft Corporation) MD5=332FEAB1435662FC6C672E25BEB37BE3 -- C:\Windows\explorer.exe

[2011/07/14 06:30:29 | 002,871,808 | ---- | M] (Microsoft Corporation) MD5=332FEAB1435662FC6C672E25BEB37BE3 -- C:\Windows\winsxs\amd64\_microsoft-windows-explorer\_31bf3856ad364e35\_6.1.7601.17567\_none\_afa79dc39081d0ba\explorer.exe

[2011/07/14 06:30:29 | 002,871,808 | ---- | M] (Microsoft Corporation) MD5=3B69712041F3D63605529BD66DC00C48 -- C:\Windows\winsxs\amd64\_microsoft-windows-explorer\_31bf3856ad364e35\_6.1.7601.21669\_none\_b0333b22a99da332\explorer.exe

[2010/11/21 04:24:25 | 002,616,320 | ---- | M] (Microsoft Corporation) MD5=40D777B7A95E00593EB1568C68514493 -- C:\Windows\winsxs\wow64\_microsoft-windows-explorer\_31bf3856ad364e35\_6.1.7601.17514\_none\_ba2f56d3c4bcbafb\explorer.exe

[2011/07/14 06:30:29 | 002,616,320 | ---- | M] (Microsoft Corporation) MD5=8B88EBBB05A0E56B7DCC708498C02B3E -- C:\Windows\SysWOW64\explorer.exe

[2011/07/14 06:30:29 | 002,616,320 | ---- | M] (Microsoft Corporation) MD5=8B88EBBB05A0E56B7DCC708498C02B3E -- C:\Windows\winsxs\wow64\_microsoft-windows-explorer\_31bf3856ad364e35\_6.1.7601.17567\_none\_b9fc4815c4e292b5\explorer.exe

[2010/11/21 04:24:11 | 002,872,320 | ---- | M] (Microsoft Corporation) MD5=AC4C51EB24AA95B77F705AB159189E24 -- C:\Windows\winsxs\amd64\_microsoft-windows-explorer\_31bf3856ad364e35\_6.1.7601.17514\_none\_afdaac81905bf900\explorer.exe

[color=#A23BEC]< MD5 for: NETLOGON.DLL >[/color]

[2010/11/21 04:24:01 | 000,695,808 | ---- | M] (Microsoft Corporation) MD5=AA339DD8BB128EF66660DFBBB59043D3 -- C:\Windows\SysNative\netlogon.dll

[2010/11/21 04:24:01 | 000,695,808 | ---- | M] (Microsoft Corporation) MD5=AA339DD8BB128EF66660DFBBB59043D3 -- C:\Windows\winsxs\amd64\_microsoft-windows-security-netlogon\_31bf3856ad364e35\_6.1.7601.17514\_none\_5bddbcb24e997298\netlogon.dll

[2010/11/21 04:24:09 | 000,563,712 | ---- | M] (Microsoft Corporation) MD5=C1809B9907ADEDAF16F50C894100883B -- C:\Windows\SysWOW64\netlogon.dll

[2010/11/21 04:24:09 | 000,563,712 | ---- | M] (Microsoft Corporation) MD5=C1809B9907ADEDAF16F50C894100883B -- C:\Windows\winsxs\wow64\_microsoft-windows-security-netlogon\_31bf3856ad364e35\_6.1.7601.17514\_none\_6632670482fa3493\netlogon.dll

[color=#A23BEC]< MD5 for: USERINIT.EXE >[/color]

[2010/11/21 04:23:55 | 000,026,624 | ---- | M] (Microsoft Corporation) MD5=61AC3EFDFACFDD3F0F11DD4FD4044223 -- C:\Windows\SysWOW64\userinit.exe

[2010/11/21 04:23:55 | 000,026,624 | ---- | M] (Microsoft Corporation) MD5=61AC3EFDFACFDD3F0F11DD4FD4044223 -- C:\Windows\winsxs\x86\_microsoft-windows-userinit\_31bf3856ad364e35\_6.1.7601.17514\_none\_de3024012ff21116\userinit.exe

[2010/11/21 04:24:28 | 000,030,720 | ---- | M] (Microsoft Corporation) MD5=BAFE84E637BF7388C96EF48D4D3FDD53 -- C:\Windows\SysNative\userinit.exe

[2010/11/21 04:24:28 | 000,030,720 | ---- | M] (Microsoft Corporation) MD5=BAFE84E637BF7388C96EF48D4D3FDD53 -- C:\Windows\winsxs\amd64\_microsoft-windows-userinit\_31bf3856ad364e35\_6.1.7601.17514\_none\_3a4ebf84e84f824c\userinit.exe

[color=#A23BEC]< MD5 for: WINLOGON.EXE >[/color]

[2010/11/21 04:24:29 | 000,390,656 | ---- | M] (Microsoft Corporation) MD5=1151B1BAA6F350B1DB6598E0FEA7C457 -- C:\Windows\SysNative\winlogon.exe

[2010/11/21 04:24:29 | 000,390,656 | ---- | M] (Microsoft Corporation) MD5=1151B1BAA6F350B1DB6598E0FEA7C457 -- C:\Windows\winsxs\amd64\_microsoft-windows-winlogon\_31bf3856ad364e35\_6.1.7601.17514\_none\_cde90685eb910636\winlogon.exe

[2012/12/14 16:49:28 | 000,216,424 | ---- | M] () MD5=22101A85B3CA2FE2BE05FE9A61A7A83D -- C:\Program Files (x86)\Malwarebytes' Anti-Malware\Chameleon\winlogon.exe

< End of report >