OTL logfile created on: 14/07/2014 11:33:52 - Run 1

OTL by OldTimer - Version 3.2.69.0 Folder = D:\Bibliothèques\Documents\Documents\Desktop

Professional Service Pack 1 (Version = 6.1.7601) - Type = NTWorkstation

Internet Explorer (Version = 9.11.9600.17207)

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

2,00 Gb Total Physical Memory | 0,52 Gb Available Physical Memory | 26,07% Memory free

4,00 Gb Paging File | 2,21 Gb Available in Paging File | 55,26% Paging File free

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

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

Drive C: | 52,57 Gb Total Space | 17,72 Gb Free Space | 33,70% Space Free | Partition Type: NTFS

Drive D: | 180,21 Gb Total Space | 114,26 Gb Free Space | 63,40% Space Free | Partition Type: NTFS

Drive H: | 1863,01 Gb Total Space | 1080,14 Gb Free Space | 57,98% Space Free | Partition Type: NTFS

Computer Name: SERGE-PC | User Name: Serge | Logged in as Administrator.

Boot Mode: Normal | Scan Mode: Current user

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

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

PRC - D:\Bibliothèques\Documents\Documents\Desktop\OTL.exe (OldTimer Tools)

PRC - C:\Program Files\Crowdcores\manager\subsystems\1\crwdcalc.exe (Flexagrid Systems Ltd)

PRC - C:\Program Files\Alwil Software\Avast5\AvastUI.exe (AVAST Software)

PRC - C:\Program Files\Alwil Software\Avast5\AvastSvc.exe (AVAST Software)

PRC - C:\Program Files\Crowdcores\service\1.2.91\crwdsvc.exe (Flexagrid Systems Ltd)

PRC - C:\Users\Serge\AppData\Local\Google\Google Talk Plugin\googletalkplugin.exe (Google)

PRC - C:\Program Files\Google\Chrome\Application\chrome.exe (Google Inc.)

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

PRC - C:\Program Files\Skype\Toolbars\PNRSvc\SkypeC2CPNRSvc.exe (Microsoft Corporation)

PRC - C:\Program Files\Skype\Toolbars\AutoUpdate\SkypeC2CAutoUpdateSvc.exe (Microsoft Corporation)

PRC - C:\Program Files\ma-config.com\MaConfigAgent.exe (CybelSoft)

PRC - C:\Program Files\NVIDIA Corporation\Display\nvxdsync.exe (NVIDIA Corporation)

PRC - C:\Program Files\NVIDIA Corporation\Display\nvtray.exe (NVIDIA Corporation)

PRC - C:\Program Files\NVIDIA Corporation\3D Vision\nvSCPAPISvr.exe (NVIDIA Corporation)

PRC - C:\Program Files\NVIDIA Corporation\Update Core\NvBackend.exe (NVIDIA Corporation)

PRC - C:\Program Files\NVIDIA Corporation\NetService\NvNetworkService.exe (NVIDIA Corporation)

PRC - C:\Program Files\NVIDIA Corporation\NvStreamSrv\nvstreamsvc.exe (NVIDIA Corporation)

PRC - C:\Windows\System32\taskhost.exe (Microsoft Corporation)

PRC - C:\Users\Jacqueline\Downloads\uTorrent-3.3 [1].exe (BitTorrent Inc.)

PRC - C:\Windows\System32\conhost.exe (Microsoft Corporation)

PRC - C:\Windows\System32\TiltWheelMouse.exe (Pixart Imaging Inc)

PRC - C:\Program Files\Ralink\Common\RaUI.exe (Ralink Technology, Corp.)

PRC - C:\ProgramData\MobileBrServ\mbbService.exe ()

PRC - C:\Program Files\Common Files\LogiShrd\LVMVFM\UMVPFSrv.exe (Logitech Inc.)

PRC - C:\Windows\explorer.exe (Microsoft Corporation)

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

MOD - C:\Program Files\Alwil Software\Avast5\libcef.dll ()

MOD - C:\Program Files\Alwil Software\Avast5\aswProperty.dll ()

MOD - C:\Program Files\Folder Colorizer\FolderColorShlExt.dll ()

MOD - C:\Program Files\Google\Chrome\Application\35.0.1916.153\ppgooglenaclpluginchrome.dll ()

MOD - C:\Program Files\Google\Chrome\Application\35.0.1916.153\pdf.dll ()

MOD - C:\Program Files\Google\Chrome\Application\35.0.1916.153\libglesv2.dll ()

MOD - C:\Program Files\Google\Chrome\Application\35.0.1916.153\libegl.dll ()

MOD - C:\Program Files\Google\Chrome\Application\35.0.1916.153\ffmpegsumo.dll ()

MOD - C:\Program Files\Notepad++\NppShell\_06.dll ()

MOD - C:\Program Files\Ralink\Common\RaWLAPI.dll ()

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

SRV - (AdobeFlashPlayerUpdateSvc) -- C:\Windows\System32\Macromed\Flash\FlashPlayerUpdateService.exe (Adobe Systems Incorporated)

SRV - (avast! Antivirus) -- C:\Program Files\Alwil Software\Avast5\AvastSvc.exe (AVAST Software)

SRV - (crwdsvc) -- C:\Program Files\Crowdcores\service\1.2.91\crwdsvc.exe (Flexagrid Systems Ltd)

SRV - (MozillaMaintenance) -- C:\Program Files\Mozilla Maintenance Service\maintenanceservice.exe (Mozilla Foundation)

SRV - (FreemakeVideoCapture) -- C:\Program Files\Freemake\CaptureLib\CaptureLibService.exe (Ellora Assets Corp.)

SRV - (IEEtwCollectorService) -- C:\Windows\System32\IEEtwCollector.exe (Microsoft Corporation)

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

SRV - (c2cpnrsvc) -- C:\Program Files\Skype\Toolbars\PNRSvc\SkypeC2CPNRSvc.exe (Microsoft Corporation)

SRV - (c2cautoupdatesvc) -- C:\Program Files\Skype\Toolbars\AutoUpdate\SkypeC2CAutoUpdateSvc.exe (Microsoft Corporation)

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

SRV - (MaConfigAgent) -- C:\Program Files\ma-config.com\MaConfigAgent.exe (CybelSoft)

SRV - (Stereo Service) -- C:\Program Files\NVIDIA Corporation\3D Vision\nvSCPAPISvr.exe (NVIDIA Corporation)

SRV - (NvNetworkService) -- C:\Program Files\NVIDIA Corporation\NetService\NvNetworkService.exe (NVIDIA Corporation)

SRV - (NvStreamSvc) -- C:\Program Files\NVIDIA Corporation\NvStreamSrv\nvstreamsvc.exe (NVIDIA Corporation)

SRV - (WinDefend) -- C:\Program Files\Windows Defender\MpSvc.dll (Microsoft Corporation)

SRV - (RaMediaServer) -- C:\Program Files\Ralink\Common\RaMediaServer.exe (Ralink)

SRV - (Mobile Broadband HL Service) -- C:\ProgramData\MobileBrServ\mbbService.exe ()

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

SRV - (WatAdminSvc) -- C:\Windows\System32\Wat\WatAdminSvc.exe (Microsoft Corporation)

SRV - (UMVPFSrv) -- C:\Program Files\Common Files\LogiShrd\LVMVFM\UMVPFSrv.exe (Logitech Inc.)

SRV - (HFGService) -- C:\Windows\System32\HFGService.dll (CSR, plc)

SRV - (RalinkRegistryWriter) -- C:\Program Files\Conceptronic\Common\RaRegistry.exe (Ralink Technology, Corp.)

SRV - (StorSvc) -- C:\Windows\System32\StorSvc.dll (Microsoft Corporation)

SRV - (SensrSvc) -- C:\Windows\System32\sensrsvc.dll (Microsoft Corporation)

SRV - (PeerDistSvc) -- C:\Windows\System32\PeerDistSvc.dll (Microsoft Corporation)

SRV - (ServiceLayer) -- C:\Program Files\PC Connectivity Solution\ServiceLayer.exe (Nokia.)

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

DRV - (VcommMgr) -- System32\Drivers\VcommMgr.sys File not found

DRV - (IvtComBusSrv) -- System32\Drivers\btcombus.sys File not found

DRV - (Btcsrusb) -- System32\Drivers\btcusb.sys File not found

DRV - (BTCOM) -- system32\DRIVERS\btcomport.sys File not found

DRV - (BT) -- system32\DRIVERS\btnetdrv.sys File not found

DRV - (BlueletAudio) -- system32\DRIVERS\blueletaudio.sys File not found

DRV - (aswSP) -- C:\Windows\System32\drivers\aswsp.sys (AVAST Software)

DRV - (aswStm) -- C:\Windows\System32\drivers\aswstm.sys (AVAST Software)

DRV - (aswSnx) -- C:\Windows\System32\drivers\aswsnx.sys (AVAST Software)

DRV - (aswVmm) -- C:\Windows\System32\drivers\aswVmm.sys ()

DRV - (aswMonFlt) -- C:\Windows\System32\drivers\aswMonFlt.sys (AVAST Software)

DRV - (aswRvrt) -- C:\Windows\System32\drivers\aswRvrt.sys ()

DRV - (aswRdr) -- C:\Windows\System32\drivers\aswRdr2.sys (AVAST Software)

DRV - (aswHwid) -- C:\Windows\System32\drivers\aswHwid.sys ()

DRV - (ma-config\_x86) -- C:\Program Files\ma-config.com\Drivers\ma-config\_x86.sys (CybelSoft)

DRV - (nvlddmkm) -- C:\Windows\System32\drivers\nvlddmkm.sys (NVIDIA Corporation)

DRV - (nvvad\_WaveExtensible) -- C:\Windows\System32\drivers\nvvad32v.sys (NVIDIA Corporation)

DRV - (NVHDA) -- C:\Windows\System32\drivers\nvhda32v.sys (NVIDIA Corporation)

DRV - (avgtp) -- C:\Windows\System32\drivers\avgtpx86.sys (AVG Technologies)

DRV - (BtHidBus) -- C:\Windows\System32\drivers\BtHidBus.sys (IVT Corporation.)

DRV - (TsUsbFlt) -- C:\Windows\System32\drivers\TsUsbFlt.sys (Microsoft Corporation)

DRV - (Rockusb) -- C:\Windows\System32\drivers\rockusb.sys (Fuzhou Rockchip Electronics Co,Ltd.)

DRV - (IvtBtBUs) -- C:\Windows\System32\drivers\IvtBtBus.sys (IVT Corporation.)

DRV - (IvtAudioBusSrv) -- C:\Windows\System32\drivers\IvtBtBus.sys (IVT Corporation.)

DRV - (IvtPanBusSrv) -- C:\Windows\System32\drivers\btnetBus.sys (IVT Corporation.)

DRV - (btnetBUs) -- C:\Windows\System32\drivers\btnetBus.sys (IVT Corporation.)

DRV - (t\_mouse.sys) -- C:\Windows\System32\drivers\t\_mouse.sys ()

DRV - (RdpVideoMiniport) -- C:\Windows\System32\drivers\rdpvideominiport.sys (Microsoft Corporation)

DRV - (netr28u) -- C:\Windows\System32\drivers\netr28u.sys (Ralink Technology Corp.)

DRV - (cmdHlp) -- C:\Windows\System32\drivers\cmdhlp.sys (COMODO)

DRV - (cmdGuard) -- C:\Windows\System32\drivers\cmdGuard.sys (COMODO)

DRV - (inspect) -- C:\Windows\System32\drivers\inspect.sys (COMODO)

DRV - (LVUVC) -- C:\Windows\System32\drivers\lvuvc.sys (Logitech Inc.)

DRV - (LVRS) -- C:\Windows\System32\drivers\lvrs.sys (Logitech Inc.)

DRV - (WsAudio\_DeviceS(5) -- C:\Windows\System32\drivers\WsAudio\_DeviceS(5).sys (Wondershare)

DRV - (WsAudio\_DeviceS(4) -- C:\Windows\System32\drivers\WsAudio\_DeviceS(4).sys (Wondershare)

DRV - (WsAudio\_DeviceS(3) -- C:\Windows\System32\drivers\WsAudio\_DeviceS(3).sys (Wondershare)

DRV - (WsAudio\_DeviceS(2) -- C:\Windows\System32\drivers\WsAudio\_DeviceS(2).sys (Wondershare)

DRV - (WsAudio\_DeviceS(1) -- C:\Windows\System32\drivers\WsAudio\_DeviceS(1).sys (Wondershare)

DRV - (MxEFUF) -- C:\Windows\System32\drivers\MxEFUF32.sys (Matrox Graphics Inc.)

DRV - (HPub4DE3) -- C:\Windows\System32\drivers\HPub4DE3.sys (TPMX Electronics Ltd.)

DRV - (HPMo4DE3) -- C:\Windows\System32\drivers\HPMo4DE3.sys (TPMX Electronics Ltd.)

DRV - (npf) -- C:\Windows\System32\drivers\npf.sys (CACE Technologies, Inc.)

DRV - (vmbus) -- C:\Windows\System32\drivers\vmbus.sys (Microsoft Corporation)

DRV - (storflt) -- C:\Windows\System32\drivers\vmstorfl.sys (Microsoft Corporation)

DRV - (storvsc) -- C:\Windows\System32\drivers\storvsc.sys (Microsoft Corporation)

DRV - (WinUsb) -- C:\Windows\System32\drivers\winusb.sys (Microsoft Corporation)

DRV - (VMBusHID) -- C:\Windows\System32\drivers\VMBusHID.sys (Microsoft Corporation)

DRV - (s3cap) -- C:\Windows\System32\drivers\vms3cap.sys (Microsoft Corporation)

DRV - (amdide) -- C:\Windows\System32\drivers\amdide.sys (Advanced Micro Devices Inc.)

DRV - (BthAudioHF) -- C:\Windows\System32\drivers\BthAudioHF.sys (CSR, plc)

DRV - (csr\_a2dp) -- C:\Windows\System32\drivers\bthav.sys (CSR, plc)

DRV - (LPCFilter) -- C:\Windows\System32\drivers\LPCFilter.sys (COMPAL ELECTRONIC INC.)

DRV - (RTL8023xp) -- C:\Windows\System32\drivers\Rtnicxp.sys (Realtek Semiconductor Corporation )

DRV - (Serial) -- C:\Windows\System32\drivers\serial.sys (Brother Industries Ltd.)

DRV - (pccsmcfd) -- C:\Windows\System32\drivers\pccsmcfd.sys (Nokia)

DRV - (usbio) -- C:\Windows\System32\drivers\usbio.sys (Thesycon GmbH, Germany)

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

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

IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Search bar = www.google.com

IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Search Page = http://www.google.com/search?q={searchTerms}&rls=com.microsoft:{language}:{referrer:source?}&ie={inputEncoding}&oe={outputEncoding}&sourceid=ie7&rlz=

IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = www.google.com

IE - HKLM\..\SearchScopes,DefaultScope = {6A1806CD-94D4-4689-BA73-E35EA1EA9990}

IE - HKLM\..\SearchScopes\{0633EE93-D776-472f-A0FF-E1416B8B2E3A}: "URL" = http://www.bing.com/search?q={searchTerms}&FORM=IE8SRC

IE - HKLM\..\SearchScopes\{6A1806CD-94D4-4689-BA73-E35EA1EA9990}: "URL" = http://www.google.com/search?q={searchTerms}&rls=com.microsoft:{language}:{referrer:source?}&ie={inputEncoding}&oe={outputEncoding}&sourceid=ie7&rlz=

IE - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Search bar = www.google.com

IE - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Search Page = http://www.google.com/search?q={searchTerms}&rls=com.microsoft:{language}:{referrer:source?}&ie={inputEncoding}&oe={outputEncoding}&sourceid=ie7&rlz=

IE - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = www.google.com

IE - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page Redirect Cache = http://be.msn.com/defaultf.aspx?lang=fr-be&ocid=iehp

IE - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page Redirect Cache AcceptLangs = fr-be

IE - HKCU\SOFTWARE\Microsoft\Internet Explorer\Search,Default\_Search\_URL = http://www.google.com

IE - HKCU\SOFTWARE\Microsoft\Internet Explorer\Search,SearchAssistant = http://www.google.com

IE - HKCU\..\SearchScopes,DefaultScope = {6A1806CD-94D4-4689-BA73-E35EA1EA9990}

IE - HKCU\..\SearchScopes\{0633EE93-D776-472f-A0FF-E1416B8B2E3A}: "URL" = http://www.bing.com/search?q={searchTerms}&src=IE-SearchBox&FORM=IE11SR

IE - HKCU\..\SearchScopes\{6A1806CD-94D4-4689-BA73-E35EA1EA9990}: "URL" = http://www.google.com/search?q={searchTerms}&rls=com.microsoft:{language}:{referrer:source?}&ie={inputEncoding}&oe={outputEncoding}&sourceid=ie7&rlz=

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 - prefs.js..browser.search.defaultengine: "Google"

FF - prefs.js..browser.search.defaultthis.engineName: "Google"

FF - prefs.js..browser.search.defaulturl: "https://www.google.com/search"

FF - prefs.js..browser.search.order.1: "Google"

FF - prefs.js..browser.search.selectedEngine: "Google"

FF - prefs.js..browser.search.useDBForOrder: true

FF - prefs.js..browser.startup.homepage: "www.google.com"

FF - prefs.js..extensions.enabledAddons: %7Bb9db16a4-6edc-47ec-a1f4-b86292ed211d%7D:4.9.22

FF - prefs.js..extensions.enabledAddons: %7Bfeadb648-e7c4-8504-3f5a-80825e575d1b%7D:1.1

FF - prefs.js..extensions.enabledAddons: fmconverter%40gmail.com:1.0.0

FF - prefs.js..extensions.enabledAddons: %7B972ce4c6-7e08-4474-a285-3208198ce6fd%7D:30.0

FF - prefs.js..browser.search.defaultenginename: "Google"

FF - prefs.js..keyword.URL: "https://www.google.com/search"

FF - user.js - File not found

FF - HKLM\Software\MozillaPlugins\@adobe.com/FlashPlayer: C:\Windows\system32\Macromed\Flash\NPSWF32\_14\_0\_0\_145.dll ()

FF - HKLM\Software\MozillaPlugins\@adobe.com/ShockwavePlayer: C:\Windows\system32\Adobe\Director\np32dsw\_1212152.dll (Adobe Systems, Inc.)

FF - HKLM\Software\MozillaPlugins\@java.com/DTPlugin,version=11.5.2: C:\Program Files\Java\jre8\bin\dtplugin\npDeployJava1.dll (Oracle Corporation)

FF - HKLM\Software\MozillaPlugins\@java.com/JavaPlugin,version=11.5.2: C:\Program Files\Java\jre8\bin\plugin2\npjp2.dll (Oracle Corporation)

FF - HKLM\Software\MozillaPlugins\@microsoft.com/GENUINE: C:\Windows\system32\Wat\npWatWeb.dll (Microsoft Corporation)

FF - HKLM\Software\MozillaPlugins\@Microsoft.com/NpCtrl,version=1.0: C:\Program Files\Microsoft Silverlight\5.1.30214.0\npctrl.dll ( Microsoft Corporation)

FF - HKLM\Software\MozillaPlugins\@microsoft.com/WLPG,version=15.4.3502.0922: File not found

FF - HKLM\Software\MozillaPlugins\@microsoft.com/WLPG,version=16.4.3528.0331: C:\Program Files\Windows Live\Photo Gallery\NPWLPG.dll (Microsoft Corporation)

FF - HKLM\Software\MozillaPlugins\@nvidia.com/3DVision: C:\Program Files\NVIDIA Corporation\3D Vision\npnv3dv.dll (NVIDIA Corporation)

FF - HKLM\Software\MozillaPlugins\@nvidia.com/3DVisionStreaming: C:\Program Files\NVIDIA Corporation\3D Vision\npnv3dvstreaming.dll (NVIDIA Corporation)

FF - HKLM\Software\MozillaPlugins\@tools.google.com/Google Update;version=3: C:\Program Files\Google\Update\1.3.24.15\npGoogleUpdate3.dll (Google Inc.)

FF - HKLM\Software\MozillaPlugins\@tools.google.com/Google Update;version=9: C:\Program Files\Google\Update\1.3.24.15\npGoogleUpdate3.dll (Google Inc.)

FF - HKLM\Software\MozillaPlugins\@videolan.org/vlc,version=2.0.8: C:\Program Files\VideoLAN\VLC\npvlc.dll (VideoLAN)

FF - HKLM\Software\MozillaPlugins\@videolan.org/vlc,version=2.1.1: C:\Program Files\VideoLAN\VLC\npvlc.dll (VideoLAN)

FF - HKLM\Software\MozillaPlugins\@videolan.org/vlc,version=2.1.2: C:\Program Files\VideoLAN\VLC\npvlc.dll (VideoLAN)

FF - HKLM\Software\MozillaPlugins\@videolan.org/vlc,version=2.1.3: C:\Program Files\VideoLAN\VLC\npvlc.dll (VideoLAN)

FF - HKLM\Software\MozillaPlugins\Adobe Reader: C:\Program Files\Adobe\Reader 11.0\Reader\AIR\nppdf32.dll (Adobe Systems Inc.)

FF - HKCU\Software\MozillaPlugins\@Skype Limited.com/Facebook Video Calling Plugin: C:\Users\Serge\AppData\Local\Facebook\Video\Skype\npFacebookVideoCalling.dll File not found

FF - HKCU\Software\MozillaPlugins\@talk.google.com/GoogleTalkPlugin: C:\Users\Serge\AppData\Roaming\Mozilla\plugins\npgoogletalk.dll (Google)

FF - HKCU\Software\MozillaPlugins\@talk.google.com/O1DPlugin: C:\Users\Serge\AppData\Roaming\Mozilla\plugins\npo1d.dll (Google)

FF - HKCU\Software\MozillaPlugins\@tools.google.com/Google Update;version=3: C:\Users\Serge\AppData\Local\Google\Update\1.3.24.15\npGoogleUpdate3.dll (Google Inc.)

FF - HKCU\Software\MozillaPlugins\@tools.google.com/Google Update;version=9: C:\Users\Serge\AppData\Local\Google\Update\1.3.24.15\npGoogleUpdate3.dll (Google Inc.)

FF - HKCU\Software\MozillaPlugins\facebook.com/fbDesktopPlugin: C:\Users\Serge\AppData\Local\Facebook\Messenger\2.1.4814.0\npFbDesktopPlugin.dll (Facebook, Inc.)

FF - HKEY\_LOCAL\_MACHINE\software\mozilla\Firefox\extensions\\wrc@avast.com: C:\Program Files\Alwil Software\Avast5\WebRep\FF [2014/07/04 17:02:27 | 000,000,000 | ---D | M]

FF - HKEY\_LOCAL\_MACHINE\software\mozilla\Firefox\extensions\\fmdownloader@gmail.com: C:\Program Files\Freemake\Freemake Video Downloader\BrowserPlugin\Firefox\fmdownloader@gmail.com\ [2014/07/05 11:28:13 | 000,000,000 | ---D | M]

FF - HKEY\_LOCAL\_MACHINE\software\mozilla\Firefox\extensions\\ytfmdownloader@gmail.com: C:\Program Files\Freemake\Freemake Video Downloader\BrowserPlugin\Firefox\ytfmdownloader@gmail.com\ [2014/07/05 11:28:14 | 000,000,000 | ---D | M]

FF - HKEY\_LOCAL\_MACHINE\software\mozilla\Firefox\extensions\\fmconverter@gmail.com: C:\Program Files\Freemake\Freemake Video Converter\BrowserPlugin\Firefox\ [2014/07/05 08:44:23 | 000,000,000 | ---D | M]

FF - HKEY\_LOCAL\_MACHINE\software\mozilla\Mozilla Firefox 16.0.2\extensions\\Components: C:\Program Files\Mozilla Firefox\components

FF - HKEY\_LOCAL\_MACHINE\software\mozilla\Mozilla Firefox 30.0\extensions\\Components: C:\Program Files\Mozilla Firefox\components

FF - HKEY\_LOCAL\_MACHINE\software\mozilla\Mozilla Firefox 30.0\extensions\\Plugins: C:\Program Files\Mozilla Firefox\plugins

FF - HKEY\_CURRENT\_USER\software\mozilla\Mozilla Firefox 16.0.2\extensions\\Components: C:\Program Files\Mozilla Firefox\components

FF - HKEY\_CURRENT\_USER\software\mozilla\Mozilla Firefox 16.0.2\extensions\\Plugins: C:\Program Files\Mozilla Firefox\plugins

FF - HKEY\_CURRENT\_USER\software\mozilla\Mozilla Firefox 30.0\extensions\\Components: C:\Program Files\Mozilla Firefox\components

FF - HKEY\_CURRENT\_USER\software\mozilla\Mozilla Firefox 30.0\extensions\\Plugins: C:\Program Files\Mozilla Firefox\plugins

[2012/01/30 15:35:25 | 000,000,000 | ---D | M] (No name found) -- C:\Users\Serge\AppData\Roaming\mozilla\Extensions

[2014/07/14 11:15:31 | 000,000,000 | ---D | M] (No name found) -- C:\Users\Serge\AppData\Roaming\mozilla\Firefox\Profiles\81m7dc6p.default\extensions

[2014/03/25 10:18:39 | 000,000,000 | ---D | M] (DownloadHelper) -- C:\Users\Serge\AppData\Roaming\mozilla\Firefox\Profiles\81m7dc6p.default\extensions\{b9db16a4-6edc-47ec-a1f4-b86292ed211d}

[2014/07/14 11:15:34 | 000,002,823 | ---- | M] () -- C:\Users\Serge\AppData\Roaming\mozilla\firefox\profiles\81m7dc6p.default\searchplugins\Google.xml

[2014/06/23 17:00:46 | 000,000,000 | ---D | M] (No name found) -- C:\Program Files\Mozilla Firefox\browser\extensions

[2014/06/23 17:01:04 | 000,000,000 | ---D | M] (Default) -- C:\Program Files\Mozilla Firefox\browser\extensions\{972ce4c6-7e08-4474-a285-3208198ce6fd}

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

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

CHR - default\_search\_provider: search\_url = {google:baseURL}search?q={searchTerms}&{google:RLZ}{google:originalQueryForSuggestion}{google:assistedQueryStats}{google:searchFieldtrialParameter}{google:bookmarkBarPinned}{google:searchClient}{google:sourceId}{google:instantExtendedEnabledParameter}{google:omniboxStartMarginParameter}ie={inputEncoding}

CHR - default\_search\_provider: suggest\_url = {google:baseSuggestURL}search?{google:searchFieldtrialParameter}client={google:suggestClient}&gs\_ri={google:suggestRid}&xssi=t&q={searchTerms}&{google:cursorPosition}{google:currentPageUrl}{google:pageClassification}sugkey={google:suggestAPIKeyParameter},

CHR - homepage:

CHR - plugin: Error reading preferences file

CHR - Extension: AddThis - Share & Bookmark (new) = C:\Users\Serge\AppData\Local\Google\Chrome\User Data\Default\Extensions\cgbogdmdefihhljhfeiklfiedefalcde\3.0.3\_0\

CHR - Extension: Autocomplete = on = C:\Users\Serge\AppData\Local\Google\Chrome\User Data\Default\Extensions\ecpgkdflcnofdbbkiggklcfmgbnbabhh\1.0\_0\

CHR - Extension: AdBlock = C:\Users\Serge\AppData\Local\Google\Chrome\User Data\Default\Extensions\gighmmpiobklfepjocnamgkkbiglidom\2.7.7\_0\

CHR - Extension: avast! Online Security = C:\Users\Serge\AppData\Local\Google\Chrome\User Data\Default\Extensions\gomekmidlodglbbmalcneegieacbdmki\9.0.2021.112\_0\

CHR - Extension: GlowModified = C:\Users\Serge\AppData\Local\Google\Chrome\User Data\Default\Extensions\hhabmhnmepifdbcjioefehlfipkhmgnh\2.2\_0\

CHR - Extension: Bookolio = C:\Users\Serge\AppData\Local\Google\Chrome\User Data\Default\Extensions\lbgmbgopjppdjfopndcniomnhpodajba\0.9.6.9\_0\

CHR - Extension: Skype Click to Call = C:\Users\Serge\AppData\Local\Google\Chrome\User Data\Default\Extensions\lifbcibllhkdhoafpjfnlhfpfgnpldfl\7.2.15747.10003\_1\

CHR - Extension: VÃ©rificateur de messages Google = C:\Users\Serge\AppData\Local\Google\Chrome\User Data\Default\Extensions\mihcahmgecmbnbcchbopgniflfhgnkff\4.4.0\_0\

CHR - Extension: GoogleÂ Wallet = C:\Users\Serge\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\

O1 HOSTS File: ([2010/12/23 21:08:04 | 000,000,780 | ---- | M]) - C:\Windows\System32\drivers\etc\hosts

O1 - Hosts: 127.0.0.1 localhost

O1 - Hosts: ::1 localhost

O2 - BHO: (Java(tm) Plug-In SSV Helper) - {761497BB-D6F0-462C-B6EB-D4DAF1D92D43} - C:\Program Files\Java\jre8\bin\ssv.dll (Oracle Corporation)

O2 - BHO: (avast! Online Security) - {8E5E2654-AD2D-48bf-AC2D-D17F00898D06} - C:\Program Files\Alwil Software\Avast5\aswWebRepIE.dll (AVAST Software)

O2 - BHO: (Java(tm) Plug-In 2 SSV Helper) - {DBC80044-A445-435b-BC74-9C25C1C588A9} - C:\Program Files\Java\jre8\bin\jp2ssv.dll (Oracle Corporation)

O4 - HKLM..\Run: [AvastUI.exe] C:\Program Files\Alwil Software\Avast5\AvastUI.exe (AVAST Software)

O4 - HKLM..\Run: [MouseDriver] C:\Windows\System32\TiltWheelMouse.exe (Pixart Imaging Inc)

O4 - HKLM..\Run: [NvBackend] C:\Program Files\NVIDIA Corporation\Update Core\NvBackend.exe (NVIDIA Corporation)

O4 - HKLM..\Run: [ShadowPlay] C:\Windows\System32\nvspcap.dll (NVIDIA Corporation)

O4 - HKCU..\Run: [FileHippo.com] C:\Program Files\FileHippo.com\UpdateChecker.exe (FileHippo.com)

O4 - HKCU..\Run: [Xvid] C:\Program Files\Xvid\CheckUpdate.exe ()

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

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

O9 - Extra Button: Skype Click to Call - {898EA8C8-E7FF-479B-8935-AEC46303B9E5} - C:\Program Files\Skype\Toolbars\Internet Explorer\SkypeIEPlugin.dll (Microsoft Corporation)

O13 - gopher Prefix: missing

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

O17 - HKLM\System\CCS\Services\Tcpip\Parameters\Interfaces\{0D69EC01-7D3F-46D1-B4BF-316F67E45909}: DhcpNameServer = 192.168.1.1

O17 - HKLM\System\CCS\Services\Tcpip\Parameters\Interfaces\{55731959-E232-4E6B-99E1-22AF3ED0741F}: DhcpNameServer = 192.168.1.1 192.168.1.1

O17 - HKLM\System\CCS\Services\Tcpip\Parameters\Interfaces\{710EEEE7-C3D9-430A-9F3F-A1693FB76B2B}: DhcpNameServer = 192.168.1.1 192.168.1.1

O17 - HKLM\System\CCS\Services\Tcpip\Parameters\Interfaces\{B29975AF-17A4-44DC-98E0-09303F96B48E}: DhcpNameServer = 192.168.1.1

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

O18 - Protocol\Handler\skype-ie-addon-data {91774881-D725-4E58-B298-07617B9B86A8} - C:\Program Files\Skype\Toolbars\Internet Explorer\SkypeIEPlugin.dll (Microsoft Corporation)

O20 - AppInit\_DLLs: (c:\windows\system32\guard32.dll) - C:\Windows\System32\guard32.dll (COMODO)

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

O20 - HKLM Winlogon: UserInit - (C:\Windows\system32\userinit.exe) - C:\Windows\System32\userinit.exe (Microsoft Corporation)

O20 - HKLM Winlogon: VMApplet - (SystemPropertiesPerformance.exe) - C:\Windows\System32\SystemPropertiesPerformance.exe (Microsoft Corporation)

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

O32 - HKLM CDRom: AutoRun - 1

O32 - AutoRun File - [2009/06/10 23:42:20 | 000,000,024 | ---- | M] () - C:\autoexec.bat -- [ NTFS ]

O33 - MountPoints2\{8b78dfec-5595-11e3-b7bc-001921ca38f9}\Shell - "" = AutoRun

O33 - MountPoints2\{8b78dfec-5595-11e3-b7bc-001921ca38f9}\Shell\AutoRun\command - "" = F:\AutoRun.exe

O33 - MountPoints2\{8b78dff2-5595-11e3-b7bc-001921ca38f9}\Shell - "" = AutoRun

O33 - MountPoints2\{8b78dff2-5595-11e3-b7bc-001921ca38f9}\Shell\AutoRun\command - "" = F:\AutoRun.exe

O34 - HKLM BootExecute: (autocheck autochk \*)

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

O35 - HKLM\..exefile [open] -- "%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)

NetSvcs: FastUserSwitchingCompatibility - File not found

NetSvcs: Ias - C:\Windows\System32\ias.dll (Microsoft Corporation)

NetSvcs: Nla - File not found

NetSvcs: Ntmssvc - File not found

NetSvcs: NWCWorkstation - File not found

NetSvcs: Nwsapagent - File not found

NetSvcs: SRService - File not found

NetSvcs: WmdmPmSp - File not found

NetSvcs: LogonHours - File not found

NetSvcs: PCAudit - File not found

NetSvcs: helpsvc - File not found

NetSvcs: uploadmgr - File not found

MsConfig - StartUpFolder: C:^ProgramData^Microsoft^Windows^Start Menu^Programs^Startup^Conceptronic Wireless Utility.lnk - C:\Program Files\Conceptronic\Common\RaUI.exe - (Ralink Technology, Corp.)

MsConfig - StartUpFolder: C:^ProgramData^Microsoft^Windows^Start Menu^Programs^Startup^McAfee Security Scan Plus.lnk - - File not found

MsConfig - StartUpFolder: C:^Users^Serge^AppData^Roaming^Microsoft^Windows^Start Menu^Programs^Startup^Dropbox.lnk - C:\Users\Serge\AppData\Roaming\Dropbox\bin\Dropbox.exe - (Dropbox, Inc.)

MsConfig - StartUpFolder: C:^Users^Serge^AppData^Roaming^Microsoft^Windows^Start Menu^Programs^Startup^Facebook Messenger.lnk - C:\Users\Serge\AppData\Local\Facebook\MESSEN~1\214814~1.0\FACEBO~1.EXE - (Facebook)

MsConfig - StartUpFolder: C:^Users^Serge^AppData^Roaming^Microsoft^Windows^Start Menu^Programs^Startup^Logitech . Enregistrement du produit.lnk - - File not found

MsConfig - StartUpReg: [b]Adobe ARM[/b] - hkey= - key= - C:\Program Files\Common Files\Adobe\ARM\1.0\AdobeARM.exe (Adobe Systems Incorporated)

MsConfig - StartUpReg: [b]Adobe Reader Speed Launcher[/b] - hkey= - key= - File not found

MsConfig - StartUpReg: [b]AdobeCS4ServiceManager[/b] - hkey= - key= - C:\Program Files\Common Files\Adobe\CS4ServiceManager\CS4ServiceManager.exe (Adobe Systems Incorporated)

MsConfig - StartUpReg: [b]CPA[/b] - hkey= - key= - File not found

MsConfig - StartUpReg: [b]DriverMax[/b] - hkey= - key= - File not found

MsConfig - StartUpReg: [b]DriverMax\_RESTART[/b] - hkey= - key= - File not found

MsConfig - StartUpReg: [b]Facebook Update[/b] - hkey= - key= - C:\Users\Serge\AppData\Local\Facebook\Update\FacebookUpdate.exe (Facebook Inc.)

MsConfig - StartUpReg: [b]Google Update[/b] - hkey= - key= - C:\Users\Serge\AppData\Local\Google\Update\GoogleUpdate.exe (Google Inc.)

MsConfig - StartUpReg: [b]LogitechQuickCamRibbon[/b] - hkey= - key= - File not found

MsConfig - StartUpReg: [b]Malwarebytes Anti-Malware[/b] - hkey= - key= - File not found

MsConfig - StartUpReg: [b]MarineAquarium3Free\_57 Browser Plugin Loader[/b] - hkey= - key= - File not found

MsConfig - StartUpReg: [b]Messenger (Yahoo!)[/b] - hkey= - key= - File not found

MsConfig - StartUpReg: [b]msnmsgr[/b] - hkey= - key= - File not found

MsConfig - StartUpReg: [b]NBKeyScan[/b] - hkey= - key= - File not found

MsConfig - StartUpReg: [b]{0228e555-4f9c-4e35-a3ec-b109a192b4c2}[/b] - hkey= - key= - File not found

MsConfig - State: "startup" - 2

MsConfig - State: "services" - 2

SafeBootMin: Base - Driver Group

SafeBootMin: Boot Bus Extender - Driver Group

SafeBootMin: Boot file system - Driver Group

SafeBootMin: File system - Driver Group

SafeBootMin: Filter - Driver Group

SafeBootMin: HelpSvc - Service

SafeBootMin: NTDS - File not found

SafeBootMin: PCI Configuration - Driver Group

SafeBootMin: PNP Filter - Driver Group

SafeBootMin: Primary disk - Driver Group

SafeBootMin: sacsvr - Service

SafeBootMin: SCSI Class - Driver Group

SafeBootMin: System Bus Extender - Driver Group

SafeBootMin: vmms - Service

SafeBootMin: WinDefend - C:\Program Files\Windows Defender\MpSvc.dll (Microsoft Corporation)

SafeBootMin: {36FC9E60-C465-11CF-8056-444553540000} - Universal Serial Bus controllers

SafeBootMin: {4D36E965-E325-11CE-BFC1-08002BE10318} - CD-ROM Drive

SafeBootMin: {4D36E967-E325-11CE-BFC1-08002BE10318} - DiskDrive

SafeBootMin: {4D36E969-E325-11CE-BFC1-08002BE10318} - Standard floppy disk controller

SafeBootMin: {4D36E96A-E325-11CE-BFC1-08002BE10318} - Hdc

SafeBootMin: {4D36E96B-E325-11CE-BFC1-08002BE10318} - Keyboard

SafeBootMin: {4D36E96F-E325-11CE-BFC1-08002BE10318} - Mouse

SafeBootMin: {4D36E977-E325-11CE-BFC1-08002BE10318} - PCMCIA Adapters

SafeBootMin: {4D36E97B-E325-11CE-BFC1-08002BE10318} - SCSIAdapter

SafeBootMin: {4D36E97D-E325-11CE-BFC1-08002BE10318} - System

SafeBootMin: {4D36E980-E325-11CE-BFC1-08002BE10318} - Floppy disk drive

SafeBootMin: {533C5B84-EC70-11D2-9505-00C04F79DEAF} - Volume shadow copy

SafeBootMin: {6BDD1FC1-810F-11D0-BEC7-08002BE2092F} - IEEE 1394 Bus host controllers

SafeBootMin: {71A27CDD-812A-11D0-BEC7-08002BE2092F} - Volume

SafeBootMin: {745A17A0-74D3-11D0-B6FE-00A0C90F57DA} - Human Interface Devices

SafeBootMin: {D48179BE-EC20-11D1-B6B8-00C04FA372A7} - SBP2 IEEE 1394 Devices

SafeBootMin: {D94EE5D8-D189-4994-83D2-F68D7D41B0E6} - SecurityDevices

SafeBootNet: Base - Driver Group

SafeBootNet: Boot Bus Extender - Driver Group

SafeBootNet: Boot file system - Driver Group

SafeBootNet: File system - Driver Group

SafeBootNet: Filter - Driver Group

SafeBootNet: HelpSvc - Service

SafeBootNet: Messenger - Service

SafeBootNet: NDIS Wrapper - Driver Group

SafeBootNet: NetBIOSGroup - Driver Group

SafeBootNet: NetDDEGroup - Driver Group

SafeBootNet: Network - Driver Group

SafeBootNet: NetworkProvider - Driver Group

SafeBootNet: NTDS - File not found

SafeBootNet: PCI Configuration - Driver Group

SafeBootNet: PNP Filter - Driver Group

SafeBootNet: PNP\_TDI - Driver Group

SafeBootNet: Primary disk - Driver Group

SafeBootNet: rdsessmgr - Service

SafeBootNet: sacsvr - Service

SafeBootNet: SCSI Class - Driver Group

SafeBootNet: Streams Drivers - Driver Group

SafeBootNet: System Bus Extender - Driver Group

SafeBootNet: TDI - Driver Group

SafeBootNet: vmms - Service

SafeBootNet: WinDefend - C:\Program Files\Windows Defender\MpSvc.dll (Microsoft Corporation)

SafeBootNet: WudfUsbccidDriver - Driver

SafeBootNet: {36FC9E60-C465-11CF-8056-444553540000} - Universal Serial Bus controllers

SafeBootNet: {4D36E965-E325-11CE-BFC1-08002BE10318} - CD-ROM Drive

SafeBootNet: {4D36E967-E325-11CE-BFC1-08002BE10318} - DiskDrive

SafeBootNet: {4D36E969-E325-11CE-BFC1-08002BE10318} - Standard floppy disk controller

SafeBootNet: {4D36E96A-E325-11CE-BFC1-08002BE10318} - Hdc

SafeBootNet: {4D36E96B-E325-11CE-BFC1-08002BE10318} - Keyboard

SafeBootNet: {4D36E96F-E325-11CE-BFC1-08002BE10318} - Mouse

SafeBootNet: {4D36E972-E325-11CE-BFC1-08002BE10318} - Net

SafeBootNet: {4D36E973-E325-11CE-BFC1-08002BE10318} - NetClient

SafeBootNet: {4D36E974-E325-11CE-BFC1-08002BE10318} - NetService

SafeBootNet: {4D36E975-E325-11CE-BFC1-08002BE10318} - NetTrans

SafeBootNet: {4D36E977-E325-11CE-BFC1-08002BE10318} - PCMCIA Adapters

SafeBootNet: {4D36E97B-E325-11CE-BFC1-08002BE10318} - SCSIAdapter

SafeBootNet: {4D36E97D-E325-11CE-BFC1-08002BE10318} - System

SafeBootNet: {4D36E980-E325-11CE-BFC1-08002BE10318} - Floppy disk drive

SafeBootNet: {50DD5230-BA8A-11D1-BF5D-0000F805F530} - Smart card readers

SafeBootNet: {533C5B84-EC70-11D2-9505-00C04F79DEAF} - Volume shadow copy

SafeBootNet: {6BDD1FC1-810F-11D0-BEC7-08002BE2092F} - IEEE 1394 Bus host controllers

SafeBootNet: {71A27CDD-812A-11D0-BEC7-08002BE2092F} - Volume

SafeBootNet: {745A17A0-74D3-11D0-B6FE-00A0C90F57DA} - Human Interface Devices

SafeBootNet: {D48179BE-EC20-11D1-B6B8-00C04FA372A7} - SBP2 IEEE 1394 Devices

SafeBootNet: {D94EE5D8-D189-4994-83D2-F68D7D41B0E6} - SecurityDevices

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: {2D46B6DC-2207-486B-B523-A557E6D54B47} - C:\Windows\system32\cmd.exe /D /C start C:\Windows\system32\ie4uinit.exe -ClearIconCache

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

ActiveX: {3C3901C5-3455-3E0A-A214-0B093A5070A6} - .NET Framework

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

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

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

ActiveX: {4903D172-DCCB-392F-93A3-34CA9D47FE3D} - .NET Framework

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

ActiveX: {5A99D44D-60B7-18B1-7F19-039DC025A995} - Microsoft Windows Media Player 12.0

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: {8060B9BF-F20C-445E-0618-95A20C97C540} - Microsoft Windows Media Player 12.0

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

ActiveX: {89820200-ECBD-11cf-8B85-00AA005B4383} - C:\Windows\System32\ie4uinit.exe -UserConfig

ActiveX: {89B4C1CD-B018-4511-B0A1-5476DBF70820} - C:\Windows\system32\Rundll32.exe C:\Windows\system32\mscories.dll,Install

ActiveX: {8A69D345-D564-463c-AFF1-A69D9E530F96} - "C:\Program Files\Google\Chrome\Application\35.0.1916.153\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: >{22d6f312-b0f6-11d0-94ab-0080c74c7e95} - %SystemRoot%\system32\unregmp2.exe /ShowWMP

Drivers32: msacm.l3acm - C:\Windows\System32\l3codecp.acm (Fraunhofer Institut Integrierte Schaltungen IIS)

Drivers32: msacm.vorbis - C:\Windows\System32\vorbis.acm (HMS http://hp.vector.co.jp/authors/VA012897/)

Drivers32: MSVideo - C:\Windows\System32\vfwwdm32.dll (Microsoft Corporation)

Drivers32: MSVideo8 - C:\Windows\System32\vfwwdm32.dll (Microsoft Corporation)

Drivers32: vidc.cvid - C:\Windows\System32\iccvid.dll (Radius Inc.)

Drivers32: vidc.i420 - i420vfw.dll File not found

Drivers32: vidc.XVID - C:\Windows\System32\xvidvfw.dll ()

Drivers32: vidc.yv12 - yv12vfw.dll File not found

CREATERESTOREPOINT

Restore point Set: OTL Restore Point

PhysicalDisk0 MBR saved to C:\PhysicalMBR.bin

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

[2014/07/14 11:28:23 | 000,602,112 | ---- | C] (OldTimer Tools) -- D:\Bibliothèques\Documents\Documents\Desktop\OTL.exe

[2014/07/10 13:42:11 | 000,110,296 | ---- | C] (Malwarebytes Corporation) -- C:\Windows\System32\drivers\MBAMSwissArmy.sys

[2014/07/10 13:41:53 | 000,000,000 | ---D | C] -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Malwarebytes Anti-Malware

[2014/07/10 13:41:45 | 000,074,456 | ---- | C] (Malwarebytes Corporation) -- C:\Windows\System32\drivers\mbamchameleon.sys

[2014/07/10 13:41:45 | 000,051,928 | ---- | C] (Malwarebytes Corporation) -- C:\Windows\System32\drivers\mwac.sys

[2014/07/10 13:41:45 | 000,023,256 | ---- | C] (Malwarebytes Corporation) -- C:\Windows\System32\drivers\mbam.sys

[2014/07/10 13:41:45 | 000,000,000 | ---D | C] -- C:\Program Files\Malwarebytes Anti-Malware

[2014/07/10 11:58:44 | 000,000,000 | ---D | C] -- D:\Bibliothèques\Documents\Documents\FormatFactory

[2014/07/09 20:04:04 | 000,108,032 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\ieetwcollector.exe

[2014/07/09 20:04:04 | 000,051,200 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\ieetwproxystub.dll

[2014/07/09 20:04:04 | 000,032,256 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\JavaScriptCollectionAgent.dll

[2014/07/09 20:04:03 | 000,646,144 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\MsSpellCheckingFacility.exe

[2014/07/09 20:04:02 | 000,032,768 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\iernonce.dll

[2014/07/09 20:04:01 | 000,240,824 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\iedkcs32.dll

[2014/07/09 20:04:00 | 000,704,512 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\ieapfltr.dll

[2014/07/09 20:04:00 | 000,367,616 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\dxtmsft.dll

[2014/07/09 20:04:00 | 000,112,128 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\ieUnatt.exe

[2014/07/09 20:04:00 | 000,043,008 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\jsproxy.dll

[2014/07/09 20:03:59 | 002,724,864 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\mshtml.tlb

[2014/07/09 20:03:59 | 000,526,336 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\msfeeds.dll

[2014/07/09 20:03:57 | 001,964,544 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\inetcpl.cpl

[2014/07/09 20:03:56 | 000,595,968 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\ie4uinit.exe

[2014/07/09 20:03:56 | 000,164,864 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\msrating.dll

[2014/07/09 20:03:56 | 000,061,952 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\iesetup.dll

[2014/07/09 20:03:54 | 000,004,096 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\ieetwcollectorres.dll

[2014/07/09 20:03:52 | 000,239,616 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\dxtrans.dll

[2014/07/09 20:03:51 | 000,442,368 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\ieui.dll

[2014/07/09 20:03:48 | 001,068,032 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\mshtmlmedia.dll

[2014/07/09 20:03:47 | 000,062,464 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\MshtmlDac.dll

[2014/07/09 20:03:44 | 000,592,896 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\jscript9diag.dll

[2014/07/09 20:03:40 | 004,254,720 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\jscript9.dll

[2014/07/09 20:03:23 | 000,509,440 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\qedit.dll

[2014/07/09 20:03:15 | 002,350,080 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\win32k.sys

[2014/07/09 20:03:14 | 000,646,144 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\osk.exe

[2014/07/09 20:01:49 | 000,404,480 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\aepdu.dll

[2014/07/09 20:01:48 | 000,302,592 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\aeinv.dll

[2014/07/09 20:01:42 | 000,220,160 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\ncrypt.dll

[2014/07/09 14:39:36 | 000,000,000 | ---D | C] -- C:\Users\Serge\AppData\Roaming\DigitalVolcano

[2014/07/09 14:39:08 | 000,000,000 | ---D | C] -- C:\Users\Serge\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Duplicate Cleaner Free

[2014/07/09 14:39:08 | 000,000,000 | ---D | C] -- C:\Program Files\Duplicate Cleaner

[2014/07/09 14:08:16 | 000,000,000 | ---D | C] -- C:\Users\Serge\AppData\Roaming\PhotoFiltre 7

[2014/07/09 14:08:11 | 000,000,000 | ---D | C] -- C:\Users\Serge\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\PhotoFiltre 7

[2014/07/09 14:08:11 | 000,000,000 | ---D | C] -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\PhotoFiltre 7

[2014/07/09 14:08:02 | 000,000,000 | ---D | C] -- C:\Program Files\PhotoFiltre 7

[2014/07/09 11:57:15 | 000,000,000 | ---D | C] -- C:\Users\Serge\AppData\Roaming\FolderColorize

[2014/07/09 11:56:56 | 000,000,000 | ---D | C] -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Folder Colorizer

[2014/07/09 11:56:55 | 000,000,000 | ---D | C] -- C:\Program Files\Folder Colorizer

[2014/07/09 11:17:36 | 000,000,000 | ---D | C] -- C:\Program Files\iColorFolder

[2014/07/09 08:16:16 | 000,000,000 | ---D | C] -- D:\Bibliothèques\Documents\Documents\Desktop\Revenu maman et moi

[2014/07/08 13:31:00 | 000,000,000 | ---D | C] -- C:\PIXresizer

[2014/07/08 10:35:57 | 000,000,000 | ---D | C] -- C:\Users\Serge\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Notepad++

[2014/07/08 10:35:57 | 000,000,000 | ---D | C] -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Notepad++

[2014/07/08 10:35:47 | 000,000,000 | ---D | C] -- C:\Users\Serge\AppData\Roaming\Notepad++

[2014/07/08 10:35:47 | 000,000,000 | ---D | C] -- C:\Program Files\Notepad++

[2014/07/08 08:26:38 | 000,000,000 | ---D | C] -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\VirtualDub

[2014/07/08 08:26:37 | 000,000,000 | ---D | C] -- C:\Program Files\VirtualDub

[2014/07/08 06:59:43 | 000,000,000 | ---D | C] -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Avidemux

[2014/07/06 13:38:26 | 000,000,000 | ---D | C] -- C:\Users\Serge\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\FormatFactory

[2014/07/06 09:44:53 | 000,000,000 | ---D | C] -- C:\Users\Serge\AppData\Roaming\AVI ReComp

[2014/07/06 09:44:32 | 000,000,000 | ---D | C] -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\VobSub

[2014/07/06 09:44:31 | 000,000,000 | ---D | C] -- C:\Program Files\Gabest

[2014/07/06 09:43:52 | 000,000,000 | ---D | C] -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Xvid

[2014/07/06 09:43:48 | 000,000,000 | ---D | C] -- C:\Program Files\Xvid

[2014/07/06 09:42:27 | 000,000,000 | ---D | C] -- C:\Users\Serge\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\AviSynth 2.5

[2014/07/06 09:42:25 | 000,000,000 | ---D | C] -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\AviSynth 2.5

[2014/07/06 09:42:25 | 000,000,000 | ---D | C] -- C:\Program Files\AviSynth 2.5

[2014/07/06 09:42:14 | 000,000,000 | ---D | C] -- C:\Users\Serge\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\AVI ReComp

[2014/07/06 09:42:10 | 000,000,000 | ---D | C] -- C:\Program Files\AVI ReComp

[2014/07/05 11:31:39 | 000,000,000 | ---D | C] -- C:\Users\Serge\AppData\Local\FreemakeVideoDownloader

[2014/07/05 08:54:42 | 000,000,000 | ---D | C] -- C:\Users\Serge\AppData\Local\FreemakeVideoConverter

[2014/07/05 08:21:26 | 000,000,000 | ---D | C] -- C:\Users\Serge\AppData\Roaming\DVDVideoSoft

[2014/07/05 08:03:27 | 000,000,000 | ---D | C] -- C:\Users\Serge\AppData\Roaming\AVS4YOU

[2014/07/05 08:03:27 | 000,000,000 | ---D | C] -- C:\ProgramData\AVS4YOU

[2014/07/05 08:01:33 | 000,000,000 | ---D | C] -- C:\Program Files\Common Files\AVSMedia

[2014/07/05 08:01:32 | 000,024,576 | ---- | C] (Microsoft Corporation) -- C:\Windows\System32\msxml3a.dll

[2014/07/05 08:01:31 | 000,000,000 | ---D | C] -- C:\Program Files\AVS4YOU

[2014/07/05 07:17:35 | 000,264,616 | ---- | C] (Oracle Corporation) -- C:\Windows\System32\javaws.exe

[2014/07/05 07:17:16 | 000,176,040 | ---- | C] (Oracle Corporation) -- C:\Windows\System32\javaw.exe

[2014/07/05 07:17:16 | 000,176,040 | ---- | C] (Oracle Corporation) -- C:\Windows\System32\java.exe

[2014/07/05 07:15:55 | 000,096,680 | ---- | C] (Oracle Corporation) -- C:\Windows\System32\WindowsAccessBridge.dll

[2014/07/04 17:02:18 | 000,043,152 | ---- | C] (AVAST Software) -- C:\Windows\avastSS.scr

[2014/06/29 10:16:17 | 000,000,000 | ---D | C] -- C:\Users\Serge\AppData\Local\com

[2014/06/29 09:59:07 | 000,000,000 | ---D | C] -- C:\Program Files\Crowdcores

[2014/06/26 17:41:41 | 000,000,000 | ---D | C] -- C:\ProgramData\Canneverbe Limited

[2014/06/26 17:40:49 | 000,000,000 | ---D | C] -- C:\Users\Serge\AppData\Roaming\Canneverbe Limited

[2014/06/24 10:26:40 | 000,000,000 | -HSD | C] -- C:\Users\Serge\AppData\Local\EmieUserList

[2014/06/24 10:26:40 | 000,000,000 | -HSD | C] -- C:\Users\Serge\AppData\Local\EmieSiteList

[2014/06/24 09:18:37 | 000,000,000 | ---D | C] -- C:\Program Files\Common Files\Java

[2014/06/24 07:36:11 | 000,000,000 | ---D | C] -- C:\Program Files\FileHippo.com

[2014/06/23 17:00:46 | 000,000,000 | ---D | C] -- C:\Program Files\Mozilla Firefox

[2014/06/22 10:07:32 | 000,000,000 | ---D | C] -- C:\AdwCleaner

[2012/01/28 09:51:01 | 000,047,360 | ---- | C] (VSO Software) -- C:\Users\Serge\AppData\Roaming\pcouffin.sys

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

[2014/07/14 11:39:17 | 000,000,512 | ---- | M] () -- C:\PhysicalMBR.bin

[2014/07/14 11:28:32 | 000,602,112 | ---- | M] (OldTimer Tools) -- D:\Bibliothèques\Documents\Documents\Desktop\OTL.exe

[2014/07/14 11:15:34 | 000,002,115 | ---- | M] () -- C:\Users\Public\Desktop\Google Chrome.lnk

[2014/07/14 11:15:33 | 000,001,145 | ---- | M] () -- D:\Bibliothèques\Documents\Documents\Desktop\Search.lnk

[2014/07/14 11:03:02 | 000,000,928 | ---- | M] () -- C:\Windows\tasks\FacebookUpdateTaskUserS-1-5-21-1184411359-537180760-3068129880-1000UA.job

[2014/07/14 10:53:49 | 000,001,002 | ---- | M] () -- C:\Windows\tasks\Adobe Flash Player Updater.job

[2014/07/14 10:48:23 | 000,001,078 | ---- | M] () -- C:\Windows\tasks\GoogleUpdateTaskUserS-1-5-21-1184411359-537180760-3068129880-1000UA.job

[2014/07/14 06:03:40 | 000,027,232 | -H-- | M] () -- C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0

[2014/07/14 06:03:40 | 000,027,232 | -H-- | M] () -- C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0

[2014/07/14 05:55:55 | 000,000,274 | ---- | M] () -- C:\Windows\tasks\PerfMonitor\_strtp.job

[2014/07/14 05:55:54 | 000,000,346 | ---- | M] () -- C:\Windows\tasks\DriverToolkit Autorun.job

[2014/07/14 05:55:28 | 000,065,536 | ---- | M] () -- C:\Windows\System32\Ikeext.etl

[2014/07/14 05:55:16 | 002,268,120 | ---- | M] () -- C:\Windows\System32\FNTCACHE.DAT

[2014/07/14 05:55:06 | 000,000,000 | ---- | M] () -- C:\Windows\System32\drivers\lvuvc.hs

[2014/07/14 05:55:05 | 000,067,584 | --S- | M] () -- C:\Windows\bootstat.dat

[2014/07/14 05:54:40 | 1610,113,024 | -HS- | M] () -- C:\hiberfil.sys

[2014/07/13 21:48:24 | 000,001,026 | ---- | M] () -- C:\Windows\tasks\GoogleUpdateTaskUserS-1-5-21-1184411359-537180760-3068129880-1000Core.job

[2014/07/13 18:27:46 | 000,110,296 | ---- | M] (Malwarebytes Corporation) -- C:\Windows\System32\drivers\MBAMSwissArmy.sys

[2014/07/13 17:03:07 | 000,000,906 | ---- | M] () -- C:\Windows\tasks\FacebookUpdateTaskUserS-1-5-21-1184411359-537180760-3068129880-1000Core.job

[2014/07/10 19:27:53 | 000,000,061 | ---- | M] () -- D:\Bibliothèques\Documents\Documents\Desktop\Tickets et tarifs - Parc d'attractions Bellewaerde.url

[2014/07/10 13:41:53 | 000,001,020 | ---- | M] () -- C:\Users\Public\Desktop\Malwarebytes Anti-Malware.lnk

[2014/07/10 11:25:35 | 000,000,090 | ---- | M] () -- D:\Bibliothèques\Documents\Documents\Desktop\Tutoriels.url

[2014/07/10 08:13:58 | 000,266,190 | ---- | M] () -- D:\Bibliothèques\Documents\Documents\Desktop\Fuision fichiers.jpg

[2014/07/09 18:14:40 | 000,000,058 | ---- | M] () -- D:\Bibliothèques\Documents\Documents\Desktop\Convertisseur online - Convertir vidéos, images, mp3 et documents.url

[2014/07/09 18:12:40 | 000,000,049 | ---- | M] () -- D:\Bibliothèques\Documents\Documents\Desktop\RedList avec Liens valides sur le nouveau Red-List.tv.url

[2014/07/09 14:39:11 | 000,000,954 | ---- | M] () -- D:\Bibliothèques\Documents\Documents\Desktop\Duplicate Cleaner Free.lnk

[2014/07/09 12:53:22 | 000,699,056 | ---- | M] (Adobe Systems Incorporated) -- C:\Windows\System32\FlashPlayerApp.exe

[2014/07/09 12:53:22 | 000,071,344 | ---- | M] (Adobe Systems Incorporated) -- C:\Windows\System32\FlashPlayerCPLApp.cpl

[2014/07/09 08:33:34 | 000,000,068 | ---- | M] () -- D:\Bibliothèques\Documents\Documents\Desktop\Classement des pays - Duing Business - Le Groupe de la Banque Mondiale.url

[2014/07/08 08:26:38 | 000,000,917 | ---- | M] () -- C:\Users\Serge\Application Data\Microsoft\Internet Explorer\Quick Launch\VirtualDub.lnk

[2014/07/08 08:26:38 | 000,000,795 | ---- | M] () -- D:\Bibliothèques\Documents\Documents\Desktop\VirtualDub.lnk

[2014/07/08 06:59:43 | 000,000,955 | ---- | M] () -- C:\Users\Public\Desktop\Avidemux 2.6 (32-bit).lnk

[2014/07/07 10:21:15 | 000,000,091 | ---- | M] () -- D:\Bibliothèques\Documents\Documents\Desktop\Modifier les options des dossiers.url

[2014/07/06 13:38:26 | 000,000,988 | ---- | M] () -- D:\Bibliothèques\Documents\Documents\Desktop\Format Factory.lnk

[2014/07/06 09:42:14 | 000,001,814 | ---- | M] () -- D:\Bibliothèques\Documents\Documents\Desktop\AVI ReComp.lnk

[2014/07/06 08:42:33 | 000,000,157 | ---- | M] () -- D:\Bibliothèques\Documents\Documents\Desktop\incruster-des-sous-titres-dans-une-video.url

[2014/07/05 11:28:25 | 000,001,250 | ---- | M] () -- C:\Users\Public\Desktop\Freemake Video Downloader.lnk

[2014/07/05 08:44:33 | 000,001,238 | ---- | M] () -- C:\Users\Public\Desktop\Freemake Video Converter.lnk

[2014/07/04 17:03:58 | 000,002,058 | ---- | M] () -- C:\Users\Public\Desktop\avast! Free Antivirus.lnk

[2014/07/04 17:03:41 | 000,414,520 | ---- | M] (AVAST Software) -- C:\Windows\System32\drivers\aswsp.sys

[2014/07/04 17:02:23 | 000,071,944 | ---- | M] (AVAST Software) -- C:\Windows\System32\drivers\aswstm.sys

[2014/07/04 17:02:22 | 000,779,536 | ---- | M] (AVAST Software) -- C:\Windows\System32\drivers\aswsnx.sys

[2014/07/04 17:02:22 | 000,192,352 | ---- | M] () -- C:\Windows\System32\drivers\aswVmm.sys

[2014/07/04 17:02:22 | 000,067,824 | ---- | M] (AVAST Software) -- C:\Windows\System32\drivers\aswMonFlt.sys

[2014/07/04 17:02:22 | 000,049,944 | ---- | M] () -- C:\Windows\System32\drivers\aswRvrt.sys

[2014/07/04 17:02:21 | 000,081,768 | ---- | M] (AVAST Software) -- C:\Windows\System32\drivers\aswRdr2.sys

[2014/07/04 17:02:21 | 000,024,184 | ---- | M] () -- C:\Windows\System32\drivers\aswHwid.sys

[2014/07/04 17:02:19 | 000,043,152 | ---- | M] (AVAST Software) -- C:\Windows\avastSS.scr

[2014/07/04 17:02:18 | 000,276,432 | ---- | M] (AVAST Software) -- C:\Windows\System32\aswBoot.exe

[2014/07/02 13:15:58 | 000,000,965 | ---- | M] () -- C:\Users\Public\Desktop\CCleaner.lnk

[2014/07/02 10:28:36 | 000,000,063 | ---- | M] () -- D:\Bibliothèques\Documents\Documents\Desktop\Retraite en Thaïlande.url

[2014/06/30 03:40:16 | 000,404,480 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\aepdu.dll

[2014/06/30 03:36:00 | 000,302,592 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\aeinv.dll

[2014/06/25 06:35:43 | 000,001,054 | ---- | M] () -- C:\Windows\tasks\GoogleUpdateTaskMachineUA.job

[2014/06/25 06:35:43 | 000,001,050 | ---- | M] () -- C:\Windows\tasks\GoogleUpdateTaskMachineCore.job

[2014/06/24 09:26:24 | 000,001,805 | ---- | M] () -- D:\Bibliothèques\Documents\Documents\Desktop\Update Checker.lnk

[2014/06/24 09:18:05 | 000,001,863 | ---- | M] () -- C:\Users\Public\Desktop\Defraggler.lnk

[2014/06/24 09:12:51 | 000,096,680 | ---- | M] (Oracle Corporation) -- C:\Windows\System32\WindowsAccessBridge.dll

[2014/06/24 09:12:46 | 000,264,616 | ---- | M] (Oracle Corporation) -- C:\Windows\System32\javaws.exe

[2014/06/24 09:12:46 | 000,176,040 | ---- | M] (Oracle Corporation) -- C:\Windows\System32\javaw.exe

[2014/06/24 09:12:46 | 000,176,040 | ---- | M] (Oracle Corporation) -- C:\Windows\System32\java.exe

[2014/06/24 09:10:42 | 000,001,989 | ---- | M] () -- C:\Users\Public\Desktop\Adobe Reader XI.lnk

[2014/06/20 21:39:54 | 000,240,824 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\iedkcs32.dll

[2014/06/20 08:10:18 | 000,000,149 | ---- | M] () -- D:\Bibliothèques\Documents\Documents\Desktop\classement.url

[2014/06/19 06:18:28 | 000,123,423 | ---- | M] () -- D:\Bibliothèques\Documents\Documents\Desktop\capture.jpg

[2014/06/19 01:56:37 | 002,724,864 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\mshtml.tlb

[2014/06/19 01:56:03 | 000,004,096 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\ieetwcollectorres.dll

[2014/06/19 01:37:23 | 000,061,952 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\iesetup.dll

[2014/06/19 01:36:35 | 000,051,200 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\ieetwproxystub.dll

[2014/06/19 01:35:55 | 000,062,464 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\MshtmlDac.dll

[2014/06/19 01:28:45 | 000,043,008 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\jsproxy.dll

[2014/06/19 01:28:16 | 000,032,768 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\iernonce.dll

[2014/06/19 01:25:38 | 000,442,368 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\ieui.dll

[2014/06/19 01:23:27 | 000,112,128 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\ieUnatt.exe

[2014/06/19 01:23:24 | 000,108,032 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\ieetwcollector.exe

[2014/06/19 01:22:40 | 000,592,896 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\jscript9diag.dll

[2014/06/19 01:16:33 | 000,646,144 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\MsSpellCheckingFacility.exe

[2014/06/19 01:12:01 | 000,367,616 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\dxtmsft.dll

[2014/06/19 01:06:10 | 000,032,256 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\JavaScriptCollectionAgent.dll

[2014/06/19 01:01:50 | 000,164,864 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\msrating.dll

[2014/06/19 00:58:08 | 000,239,616 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\dxtrans.dll

[2014/06/19 00:52:58 | 000,595,968 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\ie4uinit.exe

[2014/06/19 00:52:18 | 004,254,720 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\jscript9.dll

[2014/06/19 00:49:52 | 000,526,336 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\msfeeds.dll

[2014/06/19 00:46:23 | 001,068,032 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\mshtmlmedia.dll

[2014/06/19 00:45:59 | 001,964,544 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\inetcpl.cpl

[2014/06/19 00:07:42 | 000,704,512 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\ieapfltr.dll

[2014/06/18 10:50:05 | 000,000,063 | ---- | M] () -- D:\Bibliothèques\Documents\Documents\Desktop\Sous-titres - Téléchargez.url

[2014/06/18 06:41:45 | 000,747,644 | ---- | M] () -- C:\Windows\System32\perfh00C.dat

[2014/06/18 06:41:45 | 000,654,254 | ---- | M] () -- C:\Windows\System32\perfh009.dat

[2014/06/18 06:41:45 | 000,150,168 | ---- | M] () -- C:\Windows\System32\perfc00C.dat

[2014/06/18 06:41:45 | 000,122,126 | ---- | M] () -- C:\Windows\System32\perfc009.dat

[2014/06/18 03:51:32 | 000,646,144 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\osk.exe

[2014/06/18 02:52:00 | 002,350,080 | ---- | M] (Microsoft Corporation) -- C:\Windows\System32\win32k.sys

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

[2014/07/14 11:39:17 | 000,000,512 | ---- | C] () -- C:\PhysicalMBR.bin

[2014/07/14 05:54:44 | 002,268,120 | ---- | C] () -- C:\Windows\System32\FNTCACHE.DAT

[2014/07/10 19:27:53 | 000,000,061 | ---- | C] () -- D:\Bibliothèques\Documents\Documents\Desktop\Tickets et tarifs - Parc d'attractions Bellewaerde.url

[2014/07/10 13:41:53 | 000,001,020 | ---- | C] () -- C:\Users\Public\Desktop\Malwarebytes Anti-Malware.lnk

[2014/07/10 11:25:13 | 000,000,090 | ---- | C] () -- D:\Bibliothèques\Documents\Documents\Desktop\Tutoriels.url

[2014/07/10 08:13:58 | 000,266,190 | ---- | C] () -- D:\Bibliothèques\Documents\Documents\Desktop\Fuision fichiers.jpg

[2014/07/09 18:14:40 | 000,000,058 | ---- | C] () -- D:\Bibliothèques\Documents\Documents\Desktop\Convertisseur online - Convertir vidéos, images, mp3 et documents.url

[2014/07/09 18:12:40 | 000,000,049 | ---- | C] () -- D:\Bibliothèques\Documents\Documents\Desktop\RedList avec Liens valides sur le nouveau Red-List.tv.url

[2014/07/09 14:39:11 | 000,000,954 | ---- | C] () -- D:\Bibliothèques\Documents\Documents\Desktop\Duplicate Cleaner Free.lnk

[2014/07/09 08:33:34 | 000,000,068 | ---- | C] () -- D:\Bibliothèques\Documents\Documents\Desktop\Classement des pays - Duing Business - Le Groupe de la Banque Mondiale.url

[2014/07/08 08:26:38 | 000,000,917 | ---- | C] () -- C:\Users\Serge\Application Data\Microsoft\Internet Explorer\Quick Launch\VirtualDub.lnk

[2014/07/08 08:26:38 | 000,000,795 | ---- | C] () -- D:\Bibliothèques\Documents\Documents\Desktop\VirtualDub.lnk

[2014/07/08 06:59:43 | 000,000,955 | ---- | C] () -- C:\Users\Public\Desktop\Avidemux 2.6 (32-bit).lnk

[2014/07/07 10:21:15 | 000,000,091 | ---- | C] () -- D:\Bibliothèques\Documents\Documents\Desktop\Modifier les options des dossiers.url

[2014/07/06 13:38:26 | 000,000,988 | ---- | C] () -- D:\Bibliothèques\Documents\Documents\Desktop\Format Factory.lnk

[2014/07/06 09:43:52 | 000,153,088 | ---- | C] () -- C:\Windows\System32\xvid.ax

[2014/07/06 09:43:51 | 000,645,632 | ---- | C] () -- C:\Windows\System32\xvidcore.dll

[2014/07/06 09:43:51 | 000,240,640 | ---- | C] () -- C:\Windows\System32\xvidvfw.dll

[2014/07/06 09:42:14 | 000,001,814 | ---- | C] () -- D:\Bibliothèques\Documents\Documents\Desktop\AVI ReComp.lnk

[2014/07/06 08:42:33 | 000,000,157 | ---- | C] () -- D:\Bibliothèques\Documents\Documents\Desktop\incruster-des-sous-titres-dans-une-video.url

[2014/07/05 08:44:30 | 000,001,238 | ---- | C] () -- C:\Users\Public\Desktop\Freemake Video Converter.lnk

[2014/07/02 10:28:36 | 000,000,063 | ---- | C] () -- D:\Bibliothèques\Documents\Documents\Desktop\Retraite en Thaïlande.url

[2014/06/29 10:07:51 | 000,001,312 | ---- | C] () -- C:\Users\Serge\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Search.lnk

[2014/06/29 10:07:51 | 000,001,145 | ---- | C] () -- D:\Bibliothèques\Documents\Documents\Desktop\Search.lnk

[2014/06/29 09:59:50 | 000,000,274 | ---- | C] () -- C:\Windows\tasks\PerfMonitor\_strtp.job

[2014/06/24 09:18:05 | 000,001,863 | ---- | C] () -- C:\Users\Public\Desktop\Defraggler.lnk

[2014/06/24 09:10:42 | 000,001,989 | ---- | C] () -- C:\Users\Public\Desktop\Adobe Reader XI.lnk

[2014/06/24 09:10:41 | 000,002,441 | ---- | C] () -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Adobe Reader XI.lnk

[2014/06/24 07:36:12 | 000,001,945 | ---- | C] () -- C:\Users\Serge\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Update Checker.lnk

[2014/06/24 07:36:12 | 000,001,805 | ---- | C] () -- D:\Bibliothèques\Documents\Documents\Desktop\Update Checker.lnk

[2014/06/20 08:10:18 | 000,000,149 | ---- | C] () -- D:\Bibliothèques\Documents\Documents\Desktop\classement.url

[2014/06/18 18:42:24 | 000,123,423 | ---- | C] () -- D:\Bibliothèques\Documents\Documents\Desktop\capture.jpg

[2014/06/18 10:50:05 | 000,000,063 | ---- | C] () -- D:\Bibliothèques\Documents\Documents\Desktop\Sous-titres - Téléchargez.url

[2014/04/22 06:38:22 | 000,024,184 | ---- | C] () -- C:\Windows\System32\drivers\aswHwid.sys

[2014/02/11 11:12:14 | 000,070,904 | ---- | C] () -- C:\Windows\System32\VMProtectSDK32.dll

[2014/02/11 11:12:00 | 000,311,032 | ---- | C] () -- C:\Windows\System32\IVTCredentialProvider.dll

[2014/02/11 11:11:16 | 000,273,144 | ---- | C] () -- C:\Windows\System32\Adpush.dll

[2013/12/17 13:02:11 | 000,001,024 | ---- | C] () -- C:\Users\Serge\.rnd

[2013/12/17 13:01:44 | 000,000,000 | ---- | C] () -- C:\Windows\Irremote.ini

[2013/10/30 12:30:11 | 000,000,069 | ---- | C] () -- C:\Windows\NeroDigital.ini

[2013/10/01 08:52:20 | 000,003,584 | ---- | C] () -- C:\Users\Serge\AppData\Local\DCBC2A71-70D8-4DAN-EHR8-E0D61DEA3FDF.ini

[2013/08/07 06:57:16 | 000,000,451 | ---- | C] () -- C:\Windows\System32\DiagFunc.ini

[2013/08/07 06:57:15 | 000,480,608 | ---- | C] () -- C:\Windows\System32\DiagFunc.dll

[2013/03/05 08:41:18 | 000,192,352 | ---- | C] () -- C:\Windows\System32\drivers\aswVmm.sys

[2013/03/05 08:41:17 | 000,049,944 | ---- | C] () -- C:\Windows\System32\drivers\aswRvrt.sys

[2012/12/19 09:42:08 | 000,005,120 | ---- | C] () -- C:\Windows\System32\drivers\t\_mouse.sys

[2012/07/30 13:03:04 | 000,014,119 | ---- | C] () -- C:\Windows\System32\RaCoInst.dat

[2012/01/28 09:51:01 | 000,087,608 | ---- | C] () -- C:\Users\Serge\AppData\Roaming\inst.exe

[2012/01/28 09:51:01 | 000,007,887 | ---- | C] () -- C:\Users\Serge\AppData\Roaming\pcouffin.cat

[2012/01/28 09:51:01 | 000,001,144 | ---- | C] () -- C:\Users\Serge\AppData\Roaming\pcouffin.inf

[2012/01/28 09:25:22 | 005,505,024 | -HS- | C] () -- C:\Users\Serge\ntuser.bak

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

[2009/07/14 06:42:31 | 000,000,227 | RHS- | M] () -- C:\Windows\assembly\Desktop.ini

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

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

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

"" = %SystemRoot%\system32\shell32.dll -- [2014/03/25 04:09:54 | 012,874,240 | ---- | M] (Microsoft Corporation)

"ThreadingModel" = Apartment

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

"" = %systemroot%\system32\wbem\fastprox.dll -- [2010/11/20 14:19:02 | 000,606,208 | ---- | M] (Microsoft Corporation)

"ThreadingModel" = Free

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

"" = %systemroot%\system32\wbem\wbemess.dll -- [2009/07/14 03:16:17 | 000,342,528 | ---- | M] (Microsoft Corporation)

"ThreadingModel" = Both

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

[color=#A23BEC]< %ALLUSERSPROFILE%\Application Data\\*. >[/color]

[color=#A23BEC]< %ALLUSERSPROFILE%\Application Data\\*.exe /s >[/color]

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

[2013/05/19 11:09:02 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\4Free

[2013/04/29 10:23:07 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Adobe

[2014/04/21 08:00:50 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Apowersoft

[2013/04/23 11:32:33 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Apple Computer

[2013/12/02 18:30:30 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\AVAST Software

[2014/07/09 14:45:55 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\AVI ReComp

[2014/07/10 08:14:08 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\avidemux

[2014/07/05 08:03:27 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\AVS4YOU

[2013/01/28 07:58:49 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\BirthdayRemember

[2014/06/26 17:40:49 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Canneverbe Limited

[2014/07/09 14:39:36 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\DigitalVolcano

[2013/07/07 22:07:36 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Dropbox

[2013/11/23 13:34:48 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\DVD Flick

[2013/10/20 10:10:23 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\dvdcss

[2012/01/28 10:01:15 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\DVDFab

[2014/07/05 08:21:26 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\DVDVideoSoft

[2014/07/09 12:00:22 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\FolderColorize

[2013/01/02 18:39:23 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Gmail Backup

[2012/02/17 10:35:23 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Gmail Notifier Plus

[2012/01/28 09:25:45 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Identities

[2012/07/30 13:01:10 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\InstallShield

[2013/03/21 12:47:07 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\iolo

[2012/01/30 13:56:06 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Leadertech

[2013/04/29 10:23:10 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Macromedia

[2014/07/10 12:23:46 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Malwarebytes

[2012/07/19 12:02:54 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Marine Aquarium Lite

[2009/07/14 10:46:52 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Media Center Programs

[2013/10/17 06:54:50 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Media Player Classic

[2013/06/26 16:59:02 | 000,000,000 | --SD | M] -- C:\Users\Serge\AppData\Roaming\Microsoft

[2013/10/31 12:46:13 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\MotionDSP

[2014/06/09 11:47:43 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Mozilla

[2013/04/29 10:23:13 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Nero

[2014/07/08 10:56:04 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Notepad++

[2014/07/05 09:00:22 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\NVIDIA

[2012/07/24 12:47:49 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Opera

[2014/07/09 14:27:06 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\PhotoFiltre 7

[2013/12/02 11:33:49 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Real

[2012/03/06 16:12:52 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\RegistryKeys

[2014/07/02 15:47:19 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Skype

[2013/12/17 08:18:23 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\TeamViewer

[2012/02/11 11:36:15 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\TuneUp Software

[2014/07/14 11:49:03 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\uTorrent

[2014/07/14 06:05:46 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\vlc

[2012/09/16 19:04:01 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Vso

[2012/02/03 07:45:58 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Windows Live Writer

[2012/06/26 17:24:06 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\WinRAR

[2013/04/29 10:23:13 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\Yahoo!

[2013/01/09 08:58:11 | 000,000,000 | ---D | M] -- C:\Users\Serge\AppData\Roaming\YoWindow

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

[2012/01/28 09:51:01 | 000,087,608 | ---- | M] () -- C:\Users\Serge\AppData\Roaming\inst.exe

[2013/05/25 02:47:30 | 027,776,968 | ---- | M] (Dropbox, Inc.) -- C:\Users\Serge\AppData\Roaming\Dropbox\bin\Dropbox.exe

[2013/05/25 02:48:34 | 000,229,288 | ---- | M] (Dropbox, Inc.) -- C:\Users\Serge\AppData\Roaming\Dropbox\bin\DropboxUninstaller.exe

[2013/04/10 09:16:00 | 000,919,016 | ---- | M] (Dropbox, Inc.) -- C:\Users\Serge\AppData\Roaming\Dropbox\bin\DropboxUpdateHelper.exe

[2013/12/03 06:25:41 | 000,054,632 | ---- | M] (Adobe Systems Inc.) -- C:\Users\Serge\AppData\Roaming\Macromedia\Flash Player\www.macromedia.com\bin\airappinstaller\airappinstaller.exe

[2014/06/24 10:33:22 | 001,271,376 | ---- | M] (BitTorrent Inc.) -- C:\Users\Serge\AppData\Roaming\uTorrent\uTorrent.exe

[2013/11/22 12:34:45 | 001,122,128 | ---- | M] (BitTorrent Inc.) -- C:\Users\Serge\AppData\Roaming\uTorrent\updates\3.3.1\_29834.exe

[2013/11/22 12:43:47 | 001,141,328 | ---- | M] (BitTorrent Inc.) -- C:\Users\Serge\AppData\Roaming\uTorrent\updates\3.3.2\_30260.exe

[2014/06/24 10:33:22 | 001,271,376 | ---- | M] (BitTorrent Inc.) -- C:\Users\Serge\AppData\Roaming\uTorrent\updates\3.4.1\_31395.exe

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

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

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

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

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

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

[color=#A23BEC]< %systemroot%\System32\config\\*.sav >[/color]

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

[2011/02/26 07:19:21 | 002,616,320 | ---- | M] (Microsoft Corporation) MD5=0FB9C74046656D1579A64660AD67B746 -- C:\Windows\winsxs\x86\_microsoft-windows-explorer\_31bf3856ad364e35\_6.1.7601.21669\_none\_54149f9ef14031fc\explorer.exe

[2009/07/14 03:14:20 | 002,613,248 | ---- | M] (Microsoft Corporation) MD5=15BC38A7492BEFE831966ADB477CF76F -- C:\Windows\winsxs\x86\_microsoft-windows-explorer\_31bf3856ad364e35\_6.1.7600.16385\_none\_518afd35db100430\explorer.exe

[2011/02/26 07:51:13 | 002,614,784 | ---- | M] (Microsoft Corporation) MD5=255CF508D7CFB10E0794D6AC93280BD8 -- C:\Windows\winsxs\x86\_microsoft-windows-explorer\_31bf3856ad364e35\_6.1.7600.20910\_none\_525b5180f3f95373\explorer.exe

[2011/02/26 07:33:07 | 002,614,784 | ---- | M] (Microsoft Corporation) MD5=2AF58D15EDC06EC6FDACCE1F19482BBF -- C:\Windows\winsxs\x86\_microsoft-windows-explorer\_31bf3856ad364e35\_6.1.7600.16768\_none\_51a3a583dafd0cef\explorer.exe

[2010/11/20 14:17:09 | 002,616,320 | ---- | M] (Microsoft Corporation) MD5=40D777B7A95E00593EB1568C68514493 -- C:\Windows\winsxs\x86\_microsoft-windows-explorer\_31bf3856ad364e35\_6.1.7601.17514\_none\_53bc10fdd7fe87ca\explorer.exe

[2011/02/25 07:30:54 | 002,616,320 | ---- | M] (Microsoft Corporation) MD5=8B88EBBB05A0E56B7DCC708498C02B3E -- C:\Windows\explorer.exe

[2011/02/25 07:30:54 | 002,616,320 | ---- | M] (Microsoft Corporation) MD5=8B88EBBB05A0E56B7DCC708498C02B3E -- C:\Windows\winsxs\x86\_microsoft-windows-explorer\_31bf3856ad364e35\_6.1.7601.17567\_none\_5389023fd8245f84\explorer.exe

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

[2009/07/14 03:14:45 | 000,096,256 | ---- | M] (Microsoft Corporation) MD5=B5C5DCAD3899512020D135600129D665 -- C:\Windows\System32\wininit.exe

[2009/07/14 03:14:45 | 000,096,256 | ---- | M] (Microsoft Corporation) MD5=B5C5DCAD3899512020D135600129D665 -- C:\Windows\winsxs\x86\_microsoft-windows-wininit\_31bf3856ad364e35\_6.1.7600.16385\_none\_30c90ef265a43c13\wininit.exe

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

[2014/05/12 07:24:30 | 000,750,392 | ---- | M] (MalwareBytes) MD5=09882E8EDD1144E6EF1AF6D1F98305EE -- C:\Program Files\Malwarebytes Anti-Malware\Chameleon\Windows\winlogon.exe

[2010/11/20 14:17:54 | 000,286,720 | ---- | M] (Microsoft Corporation) MD5=6D13E1406F50C66E2A95D97F22C47560 -- C:\Windows\winsxs\x86\_microsoft-windows-winlogon\_31bf3856ad364e35\_6.1.7601.17514\_none\_71ca6b0233339500\winlogon.exe

[2009/07/14 03:14:45 | 000,285,696 | ---- | M] (Microsoft Corporation) MD5=8EC6A4AB12B8F3759E21F8E3A388F2CF -- C:\Windows\winsxs\x86\_microsoft-windows-winlogon\_31bf3856ad364e35\_6.1.7600.16385\_none\_6f99573a36451166\winlogon.exe

[2014/03/04 11:17:02 | 000,304,128 | ---- | M] (Microsoft Corporation) MD5=998507B046BA314CE8245364C686FA67 -- C:\Windows\System32\winlogon.exe

[2014/03/04 11:17:02 | 000,304,128 | ---- | M] (Microsoft Corporation) MD5=998507B046BA314CE8245364C686FA67 -- C:\Windows\winsxs\x86\_microsoft-windows-winlogon\_31bf3856ad364e35\_6.1.7601.18409\_none\_71da23b23327143c\winlogon.exe

[2014/03/04 12:39:02 | 000,304,640 | ---- | M] (Microsoft Corporation) MD5=D53972F87D850CD2EB4B29B60CAFDD77 -- C:\Windows\winsxs\x86\_microsoft-windows-winlogon\_31bf3856ad364e35\_6.1.7601.22616\_none\_7255f1994c4f8119\winlogon.exe

[color=#A23BEC]< HKEY\_LOCAL\_MACHINE\SYSTEM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters /s >[/color]

[color=#A23BEC]< HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems /s >[/color]

"Debug" =

"" = mnmsrvc

"Kmode" = \SystemRoot\System32\win32k.sys

"Optional" = Posix [binary data]

"Posix" = %SystemRoot%\system32\psxss.exe

"Required" = DebugWindows [binary data]

"Windows" = %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,12288,512 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems\CSRSS]

"CsrSrvSharedSectionBase" = 2137980928

[color=#A23BEC]< nslookup http://www.google.fr /c >[/color]

No captured output from command...

[color=#A23BEC]< hklm\software\clients\startmenuinternet|command /rs >[/color]

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\FIREFOX.EXE\InstallInfo\\HideIconsCommand: "C:\Program Files\Mozilla Firefox\uninstall\helper.exe" /HideShortcuts [2014/06/23 17:00:59 | 000,900,312 | ---- | M] (Mozilla Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\FIREFOX.EXE\InstallInfo\\ShowIconsCommand: "C:\Program Files\Mozilla Firefox\uninstall\helper.exe" /ShowShortcuts [2014/06/23 17:00:59 | 000,900,312 | ---- | M] (Mozilla Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\FIREFOX.EXE\InstallInfo\\ReinstallCommand: "C:\Program Files\Mozilla Firefox\uninstall\helper.exe" /SetAsDefaultAppGlobal [2014/06/23 17:00:59 | 000,900,312 | ---- | M] (Mozilla Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\FIREFOX.EXE\shell\open\command\\: "C:\Program Files\Mozilla Firefox\firefox.exe" [2014/06/23 17:01:04 | 000,275,568 | ---- | M] (Mozilla Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\FIREFOX.EXE\shell\properties\command\\: "C:\Program Files\Mozilla Firefox\firefox.exe" -preferences [2014/06/23 17:01:04 | 000,275,568 | ---- | M] (Mozilla Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\FIREFOX.EXE\shell\safemode\command\\: "C:\Program Files\Mozilla Firefox\firefox.exe" -safe-mode [2014/06/23 17:01:04 | 000,275,568 | ---- | M] (Mozilla Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\Google Chrome\InstallInfo\\ReinstallCommand: "C:\Program Files\Google\Chrome\Application\chrome.exe" --make-default-browser [2014/06/05 15:58:39 | 000,860,488 | ---- | M] (Google Inc.)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\Google Chrome\InstallInfo\\HideIconsCommand: "C:\Program Files\Google\Chrome\Application\chrome.exe" --hide-icons [2014/06/05 15:58:39 | 000,860,488 | ---- | M] (Google Inc.)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\Google Chrome\InstallInfo\\ShowIconsCommand: "C:\Program Files\Google\Chrome\Application\chrome.exe" --show-icons [2014/06/05 15:58:39 | 000,860,488 | ---- | M] (Google Inc.)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\Google Chrome\shell\open\command\\: "C:\Program Files\Google\Chrome\Application\chrome.exe" [2014/06/05 15:58:39 | 000,860,488 | ---- | M] (Google Inc.)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\IEXPLORE.EXE\InstallInfo\\ShowIconsCommand: "C:\Windows\System32\ie4uinit.exe" -show [2014/06/19 00:52:58 | 000,595,968 | ---- | M] (Microsoft Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\IEXPLORE.EXE\InstallInfo\\ReinstallCommand: "C:\Windows\System32\ie4uinit.exe" -reinstall [2014/06/19 00:52:58 | 000,595,968 | ---- | M] (Microsoft Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\IEXPLORE.EXE\InstallInfo\\HideIconsCommand: "C:\Windows\System32\ie4uinit.exe" -hide [2014/06/19 00:52:58 | 000,595,968 | ---- | M] (Microsoft Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\IEXPLORE.EXE\shell\naom\command\\: "C:\Program Files\Internet Explorer\iexplore.exe" -extoff [2014/06/20 21:39:54 | 000,812,216 | ---- | M] (Microsoft Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\IEXPLORE.EXE\shell\open\command\\: C:\Program Files\Internet Explorer\iexplore.exe [2014/06/20 21:39:54 | 000,812,216 | ---- | M] (Microsoft Corporation)

[color=#A23BEC]< hklm\software\clients\startmenuinternet|command /64 /rs >[/color]

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\FIREFOX.EXE\InstallInfo\\HideIconsCommand: "C:\Program Files\Mozilla Firefox\uninstall\helper.exe" /HideShortcuts [2014/06/23 17:00:59 | 000,900,312 | ---- | M] (Mozilla Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\FIREFOX.EXE\InstallInfo\\ShowIconsCommand: "C:\Program Files\Mozilla Firefox\uninstall\helper.exe" /ShowShortcuts [2014/06/23 17:00:59 | 000,900,312 | ---- | M] (Mozilla Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\FIREFOX.EXE\InstallInfo\\ReinstallCommand: "C:\Program Files\Mozilla Firefox\uninstall\helper.exe" /SetAsDefaultAppGlobal [2014/06/23 17:00:59 | 000,900,312 | ---- | M] (Mozilla Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\FIREFOX.EXE\shell\open\command\\: "C:\Program Files\Mozilla Firefox\firefox.exe" [2014/06/23 17:01:04 | 000,275,568 | ---- | M] (Mozilla Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\FIREFOX.EXE\shell\properties\command\\: "C:\Program Files\Mozilla Firefox\firefox.exe" -preferences [2014/06/23 17:01:04 | 000,275,568 | ---- | M] (Mozilla Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\FIREFOX.EXE\shell\safemode\command\\: "C:\Program Files\Mozilla Firefox\firefox.exe" -safe-mode [2014/06/23 17:01:04 | 000,275,568 | ---- | M] (Mozilla Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\Google Chrome\InstallInfo\\ReinstallCommand: "C:\Program Files\Google\Chrome\Application\chrome.exe" --make-default-browser [2014/06/05 15:58:39 | 000,860,488 | ---- | M] (Google Inc.)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\Google Chrome\InstallInfo\\HideIconsCommand: "C:\Program Files\Google\Chrome\Application\chrome.exe" --hide-icons [2014/06/05 15:58:39 | 000,860,488 | ---- | M] (Google Inc.)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\Google Chrome\InstallInfo\\ShowIconsCommand: "C:\Program Files\Google\Chrome\Application\chrome.exe" --show-icons [2014/06/05 15:58:39 | 000,860,488 | ---- | M] (Google Inc.)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\Google Chrome\shell\open\command\\: "C:\Program Files\Google\Chrome\Application\chrome.exe" [2014/06/05 15:58:39 | 000,860,488 | ---- | M] (Google Inc.)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\IEXPLORE.EXE\InstallInfo\\ShowIconsCommand: "C:\Windows\System32\ie4uinit.exe" -show [2014/06/19 00:52:58 | 000,595,968 | ---- | M] (Microsoft Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\IEXPLORE.EXE\InstallInfo\\ReinstallCommand: "C:\Windows\System32\ie4uinit.exe" -reinstall [2014/06/19 00:52:58 | 000,595,968 | ---- | M] (Microsoft Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\IEXPLORE.EXE\InstallInfo\\HideIconsCommand: "C:\Windows\System32\ie4uinit.exe" -hide [2014/06/19 00:52:58 | 000,595,968 | ---- | M] (Microsoft Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\IEXPLORE.EXE\shell\naom\command\\: "C:\Program Files\Internet Explorer\iexplore.exe" -extoff [2014/06/20 21:39:54 | 000,812,216 | ---- | M] (Microsoft Corporation)

HKEY\_LOCAL\_MACHINE\software\clients\startmenuinternet\IEXPLORE.EXE\shell\open\command\\: C:\Program Files\Internet Explorer\iexplore.exe [2014/06/20 21:39:54 | 000,812,216 | ---- | M] (Microsoft Corporation)

[color=#E56717]========== Alternate Data Streams ==========[/color]

@Alternate Data Stream - 132 bytes -> C:\ProgramData\TEMP:DBC416F8

@Alternate Data Stream - 127 bytes -> C:\ProgramData\TEMP:890CC2F3

< End of report >