~ Rapport de ZHPDiag v2014.3.2.6 - Nicolas Coolman (03/03/2014)

~ Lancé par RONDEAU (03/03/2014 21:05:31)

~ Adresse du Site Web http://nicolascoolman.webs.com

~ Forums gratuits d'Assistance à la désinfection : http://nicolascoolman.webs.com/apps/links/

~ Traduit par Nicolas Coolman

~ Etat de la version :

~ Liste blanche : Désactivée par l'utilisateur

~ Elévation des Privilèges : OK

~ User Account Control (UAC): Deactivate by program

---\\ Navigateurs Internet

MSIE: Internet Explorer v8.0.6001.19499

GCIE: Google Chrome v33.0.1750.117 (Defaut)

---\\ Informations sur les produits Windows

~ Langage: Français

Windows Vista (TM) Home Premium, 32-bit Service Pack 2 (Build 6002)

Windows Server License Manager Script : OK

~ Vista, OEM\_SLP channel

System Locked Preinstallation (OEM\_SLP) : OK

Windows ID Activation : OK

~ Windows Partial Key : RPFFV

Windows License : OK

Windows Automatic Updates : OK

---\\ Logiciels de protection du système

Avira Free Antivirus v14.0.2.286

Malwarebytes Anti-Malware version 1.75.0.1300

---\\ Logiciels d'optimisation du système

---\\ Logiciels de partage PeerToPeer

---\\ Surveillance de Logiciels

Adobe Flash Player 12 Plugin

Adobe Reader 8.1.2 - Français

Java 7 Update 17

---\\ Informations sur le système

~ Processor: x86 Family 6 Model 23 Stepping 6, GenuineIntel

~ Operating System: 32 Bits

Boot mode: Normal (Normal boot)

Total RAM: 3070 MB (59% free)

System Restore: Activé (Enable)

System drive C: has 27 GB (23%) free of 116 GB

---\\ Mode de connexion au système

~ Computer Name: PC-DE-RONDEAU

~ User Name: RONDEAU

~ All Users Names: RONDEAU, Administrateur,

~ Unselected Option: None

Logged in as Administrator

---\\ Variables d'environnement

~ System Unit : C:\

~ %AppZHP% : C:\Users\RONDEAU\AppData\Roaming\ZHP\

~ %AppData% : C:\Users\RONDEAU\AppData\Roaming\

~ %Desktop% : C:\Users\RONDEAU\Desktop\

~ %Favorites% : C:\Users\RONDEAU\Favorites\

~ %LocalAppData% : C:\Users\RONDEAU\AppData\Local\

~ %StartMenu% : C:\Users\RONDEAU\AppData\Roaming\Microsoft\Windows\Start Menu\

~ %Windir% : C:\Windows\

~ %System% : C:\Windows\System32\

---\\ Enumération des unités disques

C: Hard drive, Flash drive, Thumb drive (Free 27 Go of 116 Go)

D: Hard drive, Flash drive, Thumb drive (Free 107 Go of 107 Go)

E: CD-ROM drive (Not Inserted)

F: Hard drive, Flash drive, Thumb drive (Free 116 Go of 116 Go)

G: Hard drive, Flash drive, Thumb drive (Free 116 Go of 116 Go)

---\\ Etat du Centre de Sécurité Windows

[HKLM\SOFTWARE\Microsoft\Security Center] UacDisableNotify: OK

[HKLM\SOFTWARE\Microsoft\Security Center\Svc] AntiSpywareOverride: OK

[HKLM\SOFTWARE\Microsoft\Security Center\Svc] AntiVirusOverride: OK

[HKLM\SOFTWARE\Microsoft\Security Center\Svc] FirewallOverride: OK

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system] EnableLUA: OK

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\NOHIDDEN] CheckedValue: OK

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL] CheckedValue: OK

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Associations] Application: OK

[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] Shell: OK

[HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows] Load: OK

[HKLM\SYSTEM\CurrentControlSet\Services\COMSysApp] Type: OK

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\Results\Install] LastSuccessTime : OK

~ Security Center: 50 Scanned in 00mn 00s

---\\ Recherche particulière de fichiers génériques

[MD5.D07D4C3038F3578FFCE1C0237F2A1253] - (.Microsoft Corporation - Explorateur Windows.) (.11/04/2009 - 07:27:36.) -- C:\Windows\Explorer.exe [2926592]

[MD5.101BA3EA053480BB5D957EF37C06B5ED] - (.Microsoft Corporation - Application de démarrage de Windows.) (.21/01/2008 - 03:23:42.) -- C:\Windows\System32\Wininit.exe [96768]

[MD5.5CE024AD2C4AA64F1589AC39109F07F8] - (.Microsoft Corporation - Extensions Internet pour Win32.) (.02/02/2014 - 21:10:57.) -- C:\Windows\System32\wininet.dll [916992]

[MD5.898E7C06A350D4A1A64A9EA264D55452] - (.Microsoft Corporation - Application d'ouverture de session Windows.) (.11/04/2009 - 07:28:13.) -- C:\Windows\System32\Winlogon.exe [314368]

[MD5.3911B972B55FEA0478476B2E777B29FA] - (.Microsoft Corporation - Ancillary Function Driver for WinSock.) (.21/04/2011 - 14:58:27.) -- C:\Windows\system32\Drivers\AFD.sys [273408]

[MD5.1F05B78AB91C9075565A9D8A4B880BC4] - (.Microsoft Corporation - ATAPI IDE Miniport Driver.) (.11/04/2009 - 07:32:26.) -- C:\Windows\system32\Drivers\atapi.sys [19944]

[MD5.7ADD03E75BEB9E6DD102C3081D29840A] - (.Microsoft Corporation - CD-ROM File System Driver.) (.21/01/2008 - 03:23:51.) -- C:\Windows\system32\Drivers\Cdfs.sys [70144]

[MD5.6B4BFFB9BECD728097024276430DB314] - (.Microsoft Corporation - SCSI CD-ROM Driver.) (.11/04/2009 - 05:39:17.) -- C:\Windows\system32\Drivers\Cdrom.sys [67072]

[MD5.622C41A07CA7E6DD91770F50D532CB6C] - (.Microsoft Corporation - DFS Namespace Client Driver.) (.14/04/2011 - 15:59:03.) -- C:\Windows\system32\Drivers\DfsC.sys [75264]

[MD5.062452B7FFD68C8C042A6261FE8DFF4A] - (.Microsoft Corporation - High Definition Audio Bus Driver.) (.11/04/2009 - 05:42:42.) -- C:\Windows\system32\Drivers\HDAudBus.sys [561152]

[MD5.22D56C8184586B7A1F6FA60BE5F5A2BD] - (.Microsoft Corporation - Pilote de port i8042.) (.21/01/2008 - 03:23:20.) -- C:\Windows\system32\Drivers\i8042prt.sys [54784]

[MD5.8793643A67B42CEC66490B2A0CF92D68] - (.Microsoft Corporation - IP Network Address Translator.) (.21/01/2008 - 03:24:25.) -- C:\Windows\system32\Drivers\IpNat.sys [100864]

[MD5.1E94971C4B446AB2290DEB71D01CF0C2] - (.Microsoft Corporation - Windows NT SMB Minirdr.) (.29/04/2011 - 14:24:40.) -- C:\Windows\system32\Drivers\MRxSmb.sys [106496]

[MD5.ECD64230A59CBD93C85F1CD1CAB9F3F6] - (.Microsoft Corporation - MBT Transport driver.) (.11/04/2009 - 05:45:37.) -- C:\Windows\system32\Drivers\netBT.sys [185856]

[MD5.2C1121F2B87E9A6B12485DF53CD848C7] - (.Microsoft Corporation - Pilote du système de fichiers NT.) (.03/03/2013 - 20:07:52.) -- C:\Windows\system32\Drivers\ntfs.sys [1082232]

[MD5.0FA9B5055484649D63C303FE404E5F4D] - (.Microsoft Corporation - Pilote de port parallèle.) (.02/11/2006 - 09:51:30.) -- C:\Windows\system32\Drivers\Parport.sys [79360]

[MD5.A214ADBAF4CB47DD2728859EF31F26B0] - (.Microsoft Corporation - RAS L2TP mini-port/call-manager driver.) (.21/01/2008 - 03:24:55.) -- C:\Windows\system32\Drivers\Rasl2tp.sys [76288]

[MD5.FBC0BACD9C3D7F6956853F64A66E252D] - (.Microsoft Corporation - Microsoft RDP Device redirector.) (.21/01/2008 - 03:23:01.) -- C:\Windows\system32\Drivers\rdpdr.sys [248832]

[MD5.7B75299A4D201D6A6533603D6914AB04] - (.Microsoft Corporation - SMB Transport driver.) (.11/04/2009 - 05:45:22.) -- C:\Windows\system32\Drivers\smb.sys [66560]

[MD5.76B06EB8A01FC8624D699E7045303E54] - (.Microsoft Corporation - TDI Translation Driver.) (.11/04/2009 - 05:45:56.) -- C:\Windows\system32\Drivers\tdx.sys [72192]

[MD5.786DB5771F05EF300390399F626BF30A] - (.Microsoft Corporation - Pilote de cliché instantané du volume.) (.21/08/2012 - 12:47:42.) -- C:\Windows\system32\Drivers\volsnap.sys [224640]

~ Generic Processes: Scanned in 00mn 00s

---\\ Etat des fichiers cachés (Caché/Total)

~ Mes images (My Pictures) : 2/7

~ Mes musiques (My Musics) : 9/65

~ Mes Videos (My Videos) : 1/6

~ Mes Favoris (My Favorites) : 1/78

~ Mes Documents (My Documents) : 2/156

~ Mon Bureau (My Desktop) : 3/20427

~ Menu demarrer (Programs) : 1/38

~ Hidden Files: Scanned in 00mn 18s

---\\ Processus lancés

[MD5.0D392EDE3B97E0B3131B2F63EF1DB94E] - (.Microsoft Corporation - Windows Defender User Interface.) -- C:\Program Files\Windows Defender\MSASCui.exe [1008184] [PID.2360]

[MD5.550EA4A351D7E15F75A99185269BC906] - (.CyberLink - CyberLink MediaLibray Service.) -- C:\Program Files\ASUS\AI TouchMedia\AI TouchMedia\Kernel\CLML\CLMLSvc.exe [196608] [PID.2384]

[MD5.16F147D3A57DA6278C1E3CEC06F7FA55] - (.CyberLink Corp. - CyberLink PowerCinema Resident Program.) -- C:\Program Files\ASUS\AI TouchMedia\AI TouchMedia\PCMAgent.exe [212992] [PID.2508]

[MD5.3ED91B805AE2AE2E219D03137213300A] - (.CyberLink Corp. - CyberLink PlayMovie Resident ProgramPlayMov.) -- C:\Program Files\ASUS\AI TouchMedia\PlayMovie\PMVService.exe [172032] [PID.2552]

[MD5.9F5F2F0FB0A7F5AA9F16B9A7B6DAD89F] - (.Google - Google Desktop.) -- C:\Program Files\Google\Google Desktop Search\GoogleDesktop.exe [30192] [PID.2584]

[MD5.A6001C8CF042D31AB1377CC7626A1046] - (.Pas de propriétaire - HControlUser.) -- C:\Program Files\ASUS\ATK Hotkey\HControlUser.exe [98304] [PID.2624]

[MD5.6F3C6E627C038373237C25AC8F54E8F0] - (.ASUS - ATKOSD2.) -- C:\Program Files\ASUS\ATKOSD2\ATKOSD2.exe [7651328] [PID.900]

[MD5.4B555106290BD117334E9A08761C035A] - (...) -- ystem32\rundll32.exe [0] [PID.2180]

[MD5.86171114D84AFBD3DFCE930E320C1BBF] - (.Realtek Semiconductor - HD Audio Control Panel.) -- C:\Windows\RtHDVCpl.exe [6183456] [PID.2764]

[MD5.18A713EFF246F3C1293AD1D921B44396] - (.ASUS - ATK Media.) -- C:\Program Files\ASUS\ATK Media\DMedia.exe [159744] [PID.2568]

[MD5.2B2F678CC761AFC91E4085A519B33D75] - (.ASUS - AsScrPro.) -- C:\Windows\AsScrPro.exe [3054136] [PID.2784]

[MD5.D6F8DE039BED647B02697CC2885B8367] - (.Synaptics, Inc. - Synaptics TouchPad Enhancements.) -- C:\Program Files\Synaptics\SynTP\SynTPEnh.exe [1328424] [PID.2948]

[MD5.7D58C9BDF9C0A3955BDCDE7387AD12AC] - (.Macrovision Corporation - InstallShield Update Service Scheduler.) -- C:\Program Files\Common Files\InstallShield\UpdateService\issch.exe [81920] [PID.2420]

[MD5.DD231039B13EC2ABDE315D76E658EF0E] - (.Avira Operations GmbH & Co. KG - Antivirus System Tray Tool (Desktop).) -- C:\Program Files\Avira\AntiVir Desktop\avgnt.exe [684600] [PID.3032]

[MD5.F4DCD4912B185C3AAEB92A7040832AD1] - (.Pas de propriétaire - ALU.) -- C:\Program Files\ASUS\ASUS Live Update\ALU.exe [51768] [PID.3308]

[MD5.F6158734F1E24C6C510155CF0D363911] - (.RealNetworks, Inc. - RealNetworks Scheduler.) -- C:\Program Files\Real\RealPlayer\Update\realsched.exe [295512] [PID.3388]

[MD5.CE5C9977DA751DDC30952AC4DCBCA788] - (.Hewlett-Packard - hpwuSchd Application.) -- C:\Program Files\HP\HP Software Update\hpwuschd2.exe [49208] [PID.3672]

[MD5.4A9295C9BE22739D030AB072E9A0B169] - (.Hewlett-Packard Company - Pas de description.) -- C:\Program Files\Common Files\LightScribe\LightScribeControlPanel.exe [2363392] [PID.3268]

[MD5.BF08674925F151BD4537B89A493E3E0C] - (.Microsoft Corporation - Media Center Tray Applet.) -- C:\Windows\ehome\ehtray.exe [125952] [PID.3884]

[MD5.483FBD92DC106092D30CF2866F3E68E6] - (.Sony Ericsson Mobile Communications AB - Sony Ericsson PC Companion.) -- C:\Program Files\Sony Ericsson\Sony Ericsson PC Companion\PCCompanion.exe [774144] [PID.3948]

[MD5.C98EF7E083579C0D588D0E909F48A90A] - (.TomTom - System Tray application for TomTom HOME.) -- C:\Program Files\TomTom HOME 2\TomTomHOMERunner.exe [247728] [PID.3060]

[MD5.395BCC9122E705F6586217E32CD01CC9] - (.Hewlett-Packard Co. - ScanToPCActivationApp.) -- C:\Program Files\HP\HP Photosmart 5520 series\Bin\ScanToPCActivationApp.exe [1837672] [PID.2756]

[MD5.B614F11CB487FB97BC5FEBA24B884CBA] - (.Broadcom Corporation. - Bluetooth Tray Application.) -- C:\Program Files\WIDCOMM\Bluetooth Software\BTTray.exe [752168] [PID.4068]

[MD5.38595C19227D211B5A0932F6609A6C32] - (.ASUS - SmartLogon Application.) -- C:\Program Files\ASUS\SmartLogon\sensorsrv.exe [297528] [PID.2936]

[MD5.0F4195B9B348DE5CF9B822F81704B20E] - (.Microsoft Corporation - Media Center Media Status Aggregator Servic.) -- C:\Windows\ehome\ehmsas.exe [37376] [PID.4532]

[MD5.0826F139E35EDBE6064797A68564812E] - (.Flexera Software LLC. - FLEXnet Connect Agent.) -- C:\ProgramData\FLEXnet\Connect\11\agent.exe [1446264] [PID.2508]

[MD5.6F5C9785C05D23DABE407653C12B8A05] - (.Flexera Software LLC. - Common Software Manager.) -- C:\ProgramData\FLEXnet\Connect\11\ISUSPM.exe [2068856] [PID.4656]

[MD5.135724D3F79E261B63628D75A6DD0817] - (.Hewlett-Packard Co. - HPNetworkCommunicator.) -- C:\Program Files\HP\HP Photosmart 5520 series\Bin\HPNetworkCommunicator.exe [673384] [PID.5560]

[MD5.5A3F602D80B9E36E71DACFBF62982970] - (.eInstruction Corporation - Launcher Application.) -- C:\Program Files\eInstruction\Device Manager\Launch.exe [4912184] [PID.4476]

[MD5.FC987A45D8DC7AB320383A1418D1DC3C] - (.Synaptics, Inc. - Synaptics Pointing Device Helper.) -- C:\Program Files\Synaptics\SynTP\SynTPHelper.exe [103720] [PID.5636]

[MD5.B9E350C3EEE748E332251274DEC33829] - (.Microsoft Corporation - Internet Explorer.) -- C:\Program Files\Internet Explorer\IELowutil.exe [115712] [PID.5064]

[MD5.66EA3B698F9A7EA2DBF0E4B246B6C958] - (.Nicolas Coolman - ZHPDiag.) -- C:\ZHPDiag\ZHPDiag.exe [8349696] [PID.2688]

[MD5.6080A176D09435FC8E6E800996656E18] - (.Microsoft Corporation - Console IME.) -- C:\Windows\system32\conime.exe [69120] [PID.4608]

[MD5.16DAEB9301135432916D1DAE3FED0B88] - (.NVIDIA Corporation - NVIDIA Driver Helper Service, Version 176.0.) -- C:\Windows\system32\nvvsvc.exe [196608] [PID.1016]

[MD5.862BB4CBC05D80C5B45BE430E5EF872F] - (.Microsoft Corporation - Service de gestion des licences Microsoft.) -- C:\Windows\system32\SLsvc.exe [3408896] [PID.1328]

[MD5.5A055A4777CBBC8845DD598CB2EEBF69] - (.Pas de propriétaire - ASLDR Service.) -- C:\Program Files\ASUS\ATK Hotkey\ASLDRSrv.exe [94208] [PID.1688]

[MD5.7C157574A181B19B9DCF5F339E25337E] - (.Pas de propriétaire - GFNEXSrv.) -- C:\Program Files\ATKGFNEX\GFNEXSrv.exe [94208] [PID.1712]

[MD5.23C3A0680042C0D1DE1F360F8B62BC57] - (.Microsoft Corporation - Infrastructure d'extensibilité pour les ser.) -- C:\Windows\system32\WLANExt.exe [74240] [PID.1740]

[MD5.FE79366FECD444A16CCA9979134DBEA8] - (.Avira Operations GmbH & Co. KG - Antivirus Host Framework Service.) -- C:\Program Files\Avira\AntiVir Desktop\sched.exe [440376] [PID.1920]

[MD5.FDE9C7030FB1E9E2715E113EE6A10F90] - (.Avira Operations GmbH & Co. KG - Antivirus Host Framework Service.) -- C:\Program Files\Avira\AntiVir Desktop\avguard.exe [440376] [PID.1028]

[MD5.F2E8CEFC8CF4D6454F4121C5FF93136A] - (.Microsoft Corporation. - BingBar Service.) -- C:\Program Files\Microsoft\BingBar\7.3.124.0\BBSvc.exe [193696] [PID.1280]

[MD5.09CB316DB9D61ED9FC9A7B07A1A301F6] - (.Broadcom Corporation. - Bluetooth Support Server.) -- C:\Program Files\WIDCOMM\Bluetooth Software\bin\btwdins.exe [518696] [PID.1520]

[MD5.3A107B2215EFC62A2283FA0C661480AC] - (.Nuance Communications, Inc. - Dragon NaturallySpeaking Service.) -- C:\Program Files\Common Files\Nuance\dgnsvc.exe [311184] [PID.2008]

[MD5.ABF90FC5A127F481219B873C1B8DFC1C] - (.Hewlett-Packard Company - LightScribe Service.) -- C:\Program Files\Common Files\LightScribe\LSSrvc.exe [73728] [PID.1440]

[MD5.837608240884733792DDAE81E50B802A] - (.Microsoft Corporation - SQL Server Windows NT.) -- C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\sqlservr.exe [29293408] [PID.2132]

[MD5.837608240884733792DDAE81E50B802A] - (.Microsoft Corporation - SQL Server Windows NT.) -- C:\Program Files\Microsoft SQL Server\MSSQL.2\MSSQL\Binn\sqlservr.exe [29293408] [PID.2132]

[MD5.96EFEC24346A8EB1157E80523079ADDC] - (...) -- C:\Program Files\RealNetworks\RealDownloader\rndlresolversvc.exe [39056] [PID.2524]

[MD5.739DB668DBD812285ECC553E64A5E212] - (.Pas de propriétaire - spmgr Module.) -- C:\Program Files\ASUS\NB Probe\SPM\spmgr.exe [125496] [PID.2592]

[MD5.86EBD8B1F23E743AAD21F4D5B4D40985] - (.Microsoft Corporation - SQL Browser Service EXE.) -- C:\Program Files\Microsoft SQL Server\90\Shared\sqlbrowser.exe [238944] [PID.2632]

[MD5.D89083C4EB02DACA8F944B0E05E57F9D] - (.Microsoft Corporation - SQL Server VSS Writer.) -- C:\Program Files\Microsoft SQL Server\90\Shared\sqlwriter.exe [86880] [PID.2660]

[MD5.3199A477F0F06EEDE41BD55179F8EB05] - (.TomTom - Windows Service for TomTom HOME.) -- C:\Program Files\TomTom HOME 2\TomTomHOMEService.exe [92592] [PID.2788]

[MD5.8192CC6303ACA5BE84CBB7E7B323A0E9] - (.Pas de propriétaire - MsgTranAgt.) -- C:\Program Files\ASUS\ATK Hotkey\MsgTranAgt.exe [106496] [PID.1356]

[MD5.5EF3A73AAEBC91AA43C144E931A15746] - (.ASUS - HControl.) -- C:\Program Files\ASUS\ATK Hotkey\HControl.exe [217088] [PID.2516]

[MD5.BADBC0E13D7BD5B5E09324587041D8C9] - (.Pas de propriétaire - Wireless Console 2.) -- C:\Program Files\Wireless Console 2\wcourier.exe [1040384] [PID.3440]

[MD5.303582DFC8A2C474A78F9738FB857E82] - (.ATK - Power4Gear eXtreme.) -- C:\Program Files\P4G\BatteryLife.exe [191032] [PID.3452]

[MD5.8060AABB3722E360BDF17867A7BF7CEA] - (.ATK - ACMON.) -- C:\Program Files\ASUS\Splendid\ACMON.exe [851968] [PID.3460]

[MD5.D142CB37F10ACF08E68D9A4A21E29059] - (.ASUS - ASPG application.) -- C:\Program Files\ASUS\ASUS CopyProtect\aspg.exe [154168] [PID.3328]

[MD5.A391896CD406E6377F5CEF31FDC12019] - (.ASUSTeK - ACEngSvr Module.) -- C:\Windows\System32\ACEngSvr.exe [155648] [PID.1964]

[MD5.B289E3C5C7E74E49E076BBD05A2D94CC] - (.ASUS - ATKOSD.) -- C:\Program Files\ASUS\ATK Hotkey\ATKOSD.exe [2482176] [PID.4332]

[MD5.7BBC817DDC46A9D5413CB91764E889E8] - (.Pas de propriétaire - KBFiltr Application.) -- C:\Program Files\ASUS\ATK Hotkey\KBFiltr.exe [106496] [PID.4348]

[MD5.D3917821614CF44F8658B74DAFC59520] - (.Pas de propriétaire - WDC Application.) -- C:\Program Files\ASUS\ATK Hotkey\WDC.exe [151552] [PID.4376]

[MD5.6F1E9AB820B3DD8BD38C0190A206205D] - (.Avira Operations GmbH & Co. KG - AntiVir shadow copy service.) -- C:\Program Files\Avira\AntiVir Desktop\avshadow.exe [431672] [PID.5420]

[MD5.29D956C8CB67222D678FAF20D485B25B] - (.Avira Operations GmbH & Co. KG - AntiVir WebGuard Service.) -- C:\Program Files\Avira\AntiVir Desktop\AVWEBGRD.exe [1011768] [PID.5692]

[MD5.97D9D6A04E3AD9B6C626B9931DB78DBA] - (.Microsoft Corporation - Programme d’installation de modules Windows.) -- C:\Windows\servicing\TrustedInstaller.exe [39424] [PID.5748]

~ Processes Running: Scanned in 00mn 02s

---\\ Google Chrome, Démarrage,Recherche,Extensions (G0,G1,G2)

C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Preferences

G1 - GCS: Preference [User Data\Default] http://www.awesomehp.com =>PUP.Awesomehp

G0 - GCSP: Preference [User Data\Default][HomePage] http://www.google.com

G2 - GCE: Preference [User Data\Default] [ahfgeienlihckogmohjhadlkjgocpleb] GoogleÂ Store v.0.2 (Activé)

G2 - GCE: Preference [User Data\Default] [aohghmighlieiainnegkcijnfilokake] Documents Google v.0.5 (Activé)

G2 - GCE: Preference [User Data\Default] [apdfllckaahabafndbhieahigkjlhalf] GoogleÂ Drive v.6.3 (Activé)

G2 - GCE: Preference [User Data\Default] [blpcfgokakmgnkcojhhkbfbldkacnbeo] YouTube v.4.2.6 (Activé)

G2 - GCE: Preference [User Data\Default] [coobgpohoikkiipiblmjeljniedjpjpf] Recherche Google v.0.0.0.20 (Activé)

G2 - GCE: Preference [User Data\Default] [eemcgdkfndhakfknompkggombfjjjeno] Bookmark Manager v.0.1 (Activé)

G2 - GCE: Preference [User Data\Default] [ennkphjdgehloodpbhlhldgbnhmacadg] Settings v.0.2 (Activé)

G2 - GCE: Preference [User Data\Default] [gfdkimpbcpahaombhbimeihdjnejgicl] Feedback v.1.0 (Activé)

G2 - GCE: Preference [User Data\Default] [idhngdhcfkoamngbedgpaokgjbnpdiji] RealDownloader v.1.3.3 (Désactivé)

G2 - GCE: Preference [User Data\Default] [mfehgcgbbipciphmccgaenjidiccnmng] Cloud Print v.0.1 (Activé)

G2 - GCE: Preference [User Data\Default] [mgndgikekgjfcpckkfioiadnlibdjbkf] Chrome v.0.1 (Activé)

G2 - GCE: Preference [User Data\Default] [mikhcaiakabeeokmenglcdebplfdjicn] Dragon NaturallySpeaking Rich Internet Application Support v.1.0 (Désactivé)

G2 - GCE: Preference [User Data\Default] [neajdppkdcdipfabeoofebfddakdcjhd] Google Network Speech v.1.0 (Activé)

G2 - GCE: Preference [User Data\Default] [nkeimhogjdpnpccoofpliimaahmaaome] Hangout Services v.1.0 (Activé)

G2 - GCE: Preference [User Data\Default] [nmmhkkegccagdldgiimedpiccmgmieda] GoogleÂ Wallet v.0.0.6.1 (Activé)

G2 - GCE: Preference [User Data\Default] [pjkljhegncpnkpknbcohdijeoejaedia] Gmail v.7 (Activé)

~ Google Browser: 18 Scanned in 00mn 01s

---\\ Mozilla Firefox, Plugins,Demarrage,Recherche,Extensions (P2,M0,M1,M2,M3)

C:\Users\RONDEAU\AppData\Roaming\Mozilla\Firefox\Profiles\o9c59crw.default\prefs.js

M2 - MFEP: prefs.js [RONDEAU - o9c59crw.default\2020Player\_IKEA@2020Technologies.com] [] Visualisateur 3D de 20-20 v5.0.94.0 (..)

M2 - MFEP: prefs.js [RONDEAU - o9c59crw.default\quick\_start@gmail.com] [] Quick Start v5.0.94.0 (..)

P2 - FPN: [HKLM] [@adobe.com/FlashPlayer] - (...) -- C:\Windows\system32\Macromed\Flash\NPSWF32\_12\_0\_0\_70.dll

P2 - FPN: [HKLM] [@adobe.com/ShockwavePlayer] - (.Adobe Systems, Inc. - Adobe Shockwave for Director Netscape plug-in, version 11.5.9.615.) -- C:\Windows\system32\Adobe\Director\np32dsw.dll

P2 - FPN: [HKLM] [@Google.com/GoogleEarthPlugin] - (.Google - GEPlugin.) -- C:\Program Files\Google\Google Earth\plugin\npgeplugin.dll =>.Google Inc

P2 - FPN: [HKLM] [@google.com/npPicasa2,version=2.0.0] - (.Google, Inc. - Picasa plugin.) -- C:\Program Files\Picasa2\npPicasa2.dll

P2 - FPN: [HKLM] [@java.com/DTPlugin,version=10.17.2] - (.Oracle Corporation - NPRuntime Script Plug-in Library for Java(TM) Deploy.) -- C:\Windows\system32\npDeployJava1.dll

P2 - FPN: [HKLM] [@java.com/JavaPlugin,version=10.17.2] - (.Oracle Corporation - Next Generation Java Plug-in 10.17.2 for Mozilla browsers.) -- C:\Program Files\Java\jre7\bin\plugin2\npjp2.dll

P2 - FPN: [HKLM] [@Microsoft.com/NpCtrl,version=1.0] - (. Microsoft Corporation - 5.1.20913.0.) -- C:\Program Files\Microsoft Silverlight\5.1.20913.0\npctrl.dll

P2 - FPN: [HKLM] [@microsoft.com/WPF,version=3.5] - (.Microsoft Corporation - Windows Presentation Foundation (WPF) plug-in for Mozilla browsers.) -- C:\Windows\Microsoft.NET\Framework\v3.5\Windows Presentation Foundation\NPWPF.dll

P2 - FPN: [HKLM] [@real.com/nppl3260;version=16.0.3.51] - (.RealNetworks, Inc. - RealPlayer(tm) LiveConnect-Enabled Plug-In.) -- C:\Program Files\Real\RealPlayer\Netscape6\nppl3260.dll

P2 - FPN: [HKLM] [@real.com/nprndlchromebrowserrecordext;version=1.3.3] - (.RealNetworks, Inc. - RealNetworks(tm) RealDownloader Chrome Background Extension Plug-In.) -- C:\ProgramData\RealNetworks\RealDownloader\BrowserPlugins\MozillaPlugins\nprndlchromebrowserrecordext.dll

P2 - FPN: [HKLM] [@real.com/nprndlhtml5videoshim;version=1.3.3] - (.RealNetworks, Inc. - RealNetworks(tm) RealDownloader HTML5VideoShim Plug-In.) -- C:\ProgramData\RealNetworks\RealDownloader\BrowserPlugins\MozillaPlugins\nprndlhtml5videoshim.dll

P2 - FPN: [HKLM] [@real.com/nprndlpepperflashvideoshim;version=1.3.3] - (.RealNetworks, Inc. - RealNetworks(tm) RealDownloader PepperFlashVideoShim Plug-In.) -- C:\ProgramData\RealNetworks\RealDownloader\BrowserPlugins\MozillaPlugins\nprndlpepperflashvideoshim.dll

P2 - FPN: [HKLM] [@real.com/nprpplugin;version=16.0.3.51] - (.RealPlayer - RealPlayer Download Plugin.) -- C:\Program Files\Real\RealPlayer\Netscape6\nprpplugin.dll

P2 - FPN: [HKLM] [@realnetworks.com/npdlplugin;version=1] - (.RealDownloader - RealDownloader Plugin.) -- C:\ProgramData\RealNetworks\RealDownloader\BrowserPlugins\npdlplugin.dll

P2 - FPN: [HKLM] [nuance.com/DragonRIAPlugin] - (.Nuance Communications Inc. - Dragon NaturallySpeaking Rich Internet Application Support - Plugin.) -- C:\Program Files\Nuance\NaturallySpeaking12\Program\npDgnRia.dll

P2 - FPN: [HKCU] [@unity3d.com/UnityPlayer,version=1.0] - (.Unity Technologies ApS - Unity Player 3.3.0f4.) -- C:\Users\RONDEAU\AppData\LocalLow\Unity\WebPlayer\loader\npUnity3D32.dll

~ Firefox Browser: 18 Scanned in 00mn 00s

---\\ Internet Explorer, Démarrage,Recherche,URLSearchHook, Phishing (R0,R1,R3,R4)

R0 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = http://www.google.com

R0 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = http://www.google.com

R1 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Search Page = http://www.google.com

R1 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Default\_Page\_URL = http://www.google.com

R1 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Default\_Search\_URL = http://www.google.com

R1 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Search Bar = http://www.google.com

R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Search Page = http://www.google.com

R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Default\_Page\_URL = http://www.google.com

R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Extensions Off Page = about:noadd-ons

R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Security Risk Page = about:securityrisk

R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Default\_Search\_URL = http://www.google.com

R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\AboutURLs,Tabs = about:home

R3 - URLSearchHook: UrlSearchHook Class - {00000000-6E41-4FD3-8538-502F5495E5FC} . (.Unity Technologies ApS - Unity Player 3.3.0f4.) (No version) -- (.not file.)

R3 - URLSearchHook: Microsoft Url Search Hook - {CFBFAE00-17A6-11D0-99CB-00C04FD64497} . (.Unity Technologies ApS - Unity Player 3.3.0f4.) (No version) -- (.not file.)

~ IE Browser: 14 Scanned in 00mn 00s

---\\ Internet Explorer, Proxy Management (R5)

R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyOverride = <-loopback> =>Hijacker.Proxy

R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyServer = http=127.0.0.1:49207;https=127.0.0.1:49207 =>Hijacker.Proxy

R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyEnable = 0

R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,MigrateProxy = 1

R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,EnableHttp1\_1 = 0

R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyHttp1.1 = 1

R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,AutoConfigProxy = wininet.dll

~ Proxy management: Scanned in 00mn 00s

---\\ Analyse des lignes F0, F1, F2, F3 - IniFiles, Autoloading programs

F2 - REG:system.ini: USERINIT=C:\Windows\system32\userinit.exe,

F2 - REG:system.ini: Shell=C:\Windows\explorer.exe

F2 - REG:system.ini: VMApplet=rundll32 shell32,Control\_RunDLL "sysdm.cpl"

~ Keys: Scanned in 00mn 00s

---\\ Hosts file redirection (O1)

~ Le fichier hosts est sain (The hosts file is clean).

~ Hosts File: Scanned in 00mn 00s

~ Nombre de lignes (Lines number): 20

---\\ Browser Helper Objects de navigateur (O2)

O2 - BHO: Aide pour le lien d'Adobe PDF Reader - {06849E9F-C8D7-4D59-B87D-784B7D6BE0B3} . (.Adobe Systems Incorporated - Adobe PDF Helper for Internet Explorer.) -- C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll

O2 - BHO: Bing Bar Helper - {1dad3af3-ef2f-4f64-ac4b-11789189fcb6} . (.Microsoft Corporation. - Extensions du client Bing.) -- C:\Program Files\Microsoft\BingBar\7.3.124.0\BingExt.dll =>Toolbar.Bing

O2 - BHO: RealNetworks Download and Record Plugin for Internet Explorer - {3049C3E9-B461-4BC5-8870-4C09146192CA} . (.RealDownloader - RealPlayer Download and Record Plugin.) -- C:\ProgramData\RealNetworks\RealDownloader\BrowserPlugins\IE\rndlbrowserrecordplugin.dll

O2 - BHO: Java(tm) Plug-In SSV Helper - {761497BB-D6F0-462C-B6EB-D4DAF1D92D43} . (.Oracle Corporation - Java(TM) Platform SE binary.) -- C:\Program Files\Java\jre7\bin\ssv.dll

O2 - BHO: Windows Live ID Sign-in Helper - {9030D464-4C02-4ABF-8ECC-5164760863C6} . (.Microsoft Corp. - Microsoft® Windows Live ID Login Helper.) -- C:\Program Files\Common Files\Microsoft Shared\Windows Live\WindowsLiveLogin.dll

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

O2 - BHO: Java(tm) Plug-In 2 SSV Helper - {DBC80044-A445-435b-BC74-9C25C1C588A9} . (.Oracle Corporation - Java(TM) Platform SE binary.) -- C:\Program Files\Java\jre7\bin\jp2ssv.dll

O2 - BHO: ASUS Security Protect Manager - {DF21F1DB-80C6-11D3-9483-B03D0EC10000} . (.Bioscrypt Inc. - SSO IE Listener.) -- C:\Program Files\ASUS Security Center\ASUS Security Protect Manager\Bin\ItIEAddIn.dll

~ BHO: 16 Scanned in 00mn 00s

---\\ Internet Explorer Toolbars (O3)

O3 - Toolbar: Bing Bar - [HKLM]{eec0f710-38b5-4aba-99bf-ec87564a4e13} . (.Microsoft Corporation. - Extensions du client Bing.) -- C:\Program Files\Microsoft\BingBar\7.3.124.0\BingExt.dll =>Toolbar.Bing

O3 - Toolbar\WebBrowser: (no name) - [HKCU]{2318C2B1-4965-11D4-9B18-009027A5CD4F} Clé orpheline

~ Toolbar: Scanned in 00mn 00s

---\\ Autres liens utilisateurs (O4)

O4 - GS\Desktop [Public]: Achat de consommables - HP Photosmart 5520 series.lnk . (.Hewlett-Packard Co. - DesktopSureSupply.) -- C:\Program Files\HP\HP Photosmart 5520 series\Bin\hpqDTSS.exe =>.Hewlett-Packard Co

O4 - GS\Desktop [Public]: AI TouchMedia.lnk . (.CyberLink Corp. - ASUS AI TouchMedia Main Program.) -- C:\Program Files\ASUS\AI TouchMedia\AI TouchMedia\AI TouchMedia.exe

O4 - GS\Desktop [Public]: ASUS Camera ScreenSaver.lnk . (.Macromedia, Inc. - Macromedia Flash Player 6.0 r21.) -- C:\Windows\ASUS Camera ScreenSaver.exe

O4 - GS\Desktop [Public]: ASUS CopyProtect.lnk . (...) -- C:\Windows\Installer\{6B77A7F6-DD63-4F13-A6FF-83137A5AC354}\\_D0026486DB7A90E371F8D3.exe

O4 - GS\Desktop [Public]: Avira Control Center.lnk . (.Avira Operations GmbH & Co. KG - Antivirus Control Center (Desktop).) -- C:\Program Files\Avira\AntiVir Desktop\avcenter.exe

O4 - GS\Desktop [Public]: Dragon NaturallySpeaking 12.5.lnk . (.Acresso Software Inc. - InstallShield.) -- C:\Windows\Installer\{D5D422B9-6976-4E98-8DDF-9632CB515D7E}\NatSpeakD\_Shortcut\_D5D422B969764E988DDF9632CB515D7E.exe

O4 - GS\Desktop [Public]: Google Earth.lnk . (.Google - Google Earth.) -- C:\Program Files\Google\Google Earth\client\googleearth.exe =>.Google Inc

O4 - GS\Desktop [Public]: HP Photo Creations.lnk . (.Visan / RocketLife - PhotoProduct.exe.) -- C:\Program Files\HP Photo Creations\PhotoProduct.exe

O4 - GS\Desktop [Public]: HP Photosmart 5520 series.lnk . (.Hewlett-Packard Co. - HP Printer Assistant.) -- C:\Program Files\HP\HP Photosmart 5520 series\Bin\HP Photosmart 5520 series.exe =>.Hewlett-Packard Co

O4 - GS\Desktop [Public]: MAGIX Photo Manager.lnk . (.MAGIX - MAGIX Foto Manager.) -- C:\MAGIX\Photo\_Manager\PhotoManager.exe

O4 - GS\Desktop [Public]: Malwarebytes Anti-Malware.lnk . (.Malwarebytes Corporation - Malwarebytes Anti-Malware.) -- C:\Program Files\Malwarebytes' Anti-Malware\mbam.exe

O4 - GS\Desktop [Public]: SmartLogon Manager.lnk . (.ASUS - SmartLogon Application.) -- C:\Program Files\ASUS\SmartLogon\logonmgr.exe

O4 - GS\Desktop [Public]: Splendid Utility.Lnk . (...) -- C:\Program Files\ASUS\Splendid\Backbone.exe

O4 - GS\Desktop [Public]: WorkSpace.lnk . (.GTCO CalComp, Inc. - Interwrite WorkSpace.) -- C:\Program Files\eInstruction\Workspace\IW.exe

O4 - GS\Program [Public]: Adobe Reader 8.lnk . (...) -- C:\Windows\Installer\{AC76BA86-7AD7-1036-7B44-A81200000003}\SC\_Reader.exe

O4 - GS\Program [Public]: Apple Software Update.lnk . (...) -- C:\Windows\Installer\{789A5B64-9DD9-4BA5-915A-F0FC0A1B7BFE}\AppleSoftwareUpdateIco.exe =>.Apple Inc

O4 - GS\Program [Public]: Classification.Lnk . (.Jeulin - Classification.) -- C:\Program Files\Classification\Classif.exe

O4 - GS\Program [Public]: Dolby Control Center.lnk . (...) -- C:\Windows\Installer\{DE66EFAD-B9CC-4FD4-9157-6C18E5100161}\\_324FCE11D5E253F82AF837.exe

O4 - GS\Program [Public]: La respiration.lnk . (.Studio PEREZ - Programme de seconde.) -- C:\Program Files\Pulmo\pulmo.exe

O4 - GS\Program [Public]: Media Center.lnk . (.Microsoft Corporation - Media Center.) -- C:\Windows\ehome\ehshell.exe

O4 - GS\Program [Public]: Oxygene.lnk . (...) -- C:\Program Files\Oxygene\Oxygene.exe (.not file.)

O4 - GS\Program [Public]: svt2.lnk . (...) -- C:\Program Files\svt2\svt2.exe

O4 - GS\Program [Public]: Vostok.lnk . (.Vostok paléoclimats - Vostok.) -- C:\Program Files\Vostok\Vostok.exe

O4 - GS\Program [Public]: Windows Calendar.lnk . (.Microsoft Corporation - Calendrier Windows.) -- C:\Program Files\Windows Calendar\WinCal.exe =>.Microsoft Corporation

O4 - GS\Program [Public]: Windows Collaboration.lnk . (.Microsoft Corporation - Windows Meeting Space.) -- C:\Program Files\Windows Collaboration\WinCollab.exe =>.Microsoft Corporation

O4 - GS\Program [Public]: Windows Contacts.lnk . (.Microsoft Corporation - Windows Contacts.) -- C:\Program Files\Windows Mail\wab.exe =>.Microsoft Corporation

O4 - GS\Program [Public]: Windows Defender.lnk . (.Microsoft Corporation - Windows Defender User Interface.) -- C:\Program Files\Windows Defender\MSASCui.exe

O4 - GS\Program [Public]: Windows DVD Maker.lnk . (.Microsoft Corporation - Création de DVD Windows.) -- C:\Program Files\Movie Maker\DVDMaker.exe =>.Microsoft Corporation

O4 - GS\Program [Public]: Windows Live Mail.lnk . (.Microsoft Corporation - Windows Live Mail.) -- C:\Program Files\Windows Live\Mail\wlmail.exe =>.Microsoft Corporation

O4 - GS\Program [Public]: Windows Movie Maker.lnk . (.Microsoft Corporation - Windows Movie Maker.) -- C:\Program Files\Movie Maker\MOVIEMK.exe =>.Microsoft Corporation

O4 - GS\Program [Public]: Windows Photo Gallery.lnk . (.Microsoft Corporation - Galerie de photos Windows.) -- C:\Program Files\Windows Photo Gallery\WindowsPhotoGallery.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Bluetooth File Transfer Wizard.lnk . (.Microsoft Corporation - Pas de description.) -- C:\Windows\System32\fsquirt.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Calculator.lnk . (.Microsoft Corporation - Calculatrice de Windows.) -- C:\Windows\System32\calc.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Mobility Center.lnk . (.Microsoft Corporation - Centre de mobilité Windows.) -- C:\Windows\System32\mblctr.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: NetworkProjection.lnk . (.Microsoft Corporation - Connect to a Network Projector.) -- C:\Windows\System32\NetProj.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Paint.lnk . (.Microsoft Corporation - Paint.) -- C:\Windows\System32\mspaint.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Remote Desktop Connection.lnk . (.Microsoft Corporation - Connexion Bureau à distance.) -- C:\Windows\System32\mstsc.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Sidebar.lnk . (.Microsoft Corporation - Volet Windows.) -- C:\Program Files\Windows Sidebar\sidebar.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Snipping Tool.lnk . (.Microsoft Corporation - Outil Capture.) -- C:\Windows\System32\SnippingTool.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Sound Recorder.lnk . (.Microsoft Corporation - Magnétophone Windows.) -- C:\Windows\System32\SoundRecorder.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Sync Center.lnk . (.Microsoft Corporation - Microsoft Sync Center.) -- C:\Windows\System32\mobsync.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Welcome Center.lnk . (.Microsoft Corporation - Windows Control Panel.) -- C:\Windows\System32\control.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Wordpad.lnk . (.Microsoft Corporation - Application Windows Wordpad.) -- C:\Program Files\Windows NT\Accessories\wordpad.exe =>.Microsoft Corporation

O4 - GS\SystemTools [Public]: Backup.lnk . (.Microsoft Corporation - Sauvegarde Microsoft® Windows.) -- C:\Windows\System32\sdclt.exe =>.Microsoft Corporation

O4 - GS\SystemTools [Public]: Character Map.lnk . (.Microsoft Corporation - Table des caractères.) -- C:\Windows\System32\charmap.exe =>.Microsoft Corporation

O4 - GS\SystemTools [Public]: dfrgui.lnk . (.Microsoft Corporation - Défragmenteur de disque Microsoft®.) -- C:\Windows\System32\dfrgui.exe =>.Microsoft Corporation

O4 - GS\SystemTools [Public]: Disk Cleanup.lnk . (.Microsoft Corporation - Gestionnaire de nettoyage de disque pour Wi.) -- C:\Windows\System32\cleanmgr.exe =>.Microsoft Corporation

O4 - GS\SystemTools [Public]: migwiz.lnk . (.Microsoft Corporation - Transfert de fichiers et paramètres Windows.) -- C:\Windows\System32\migwiz\migwiz.exe =>.Microsoft Corporation

O4 - GS\SystemTools [Public]: System Information.lnk . (.Microsoft Corporation - Informations système.) -- C:\Windows\System32\msinfo32.exe =>.Microsoft Corporation

O4 - GS\SystemTools [Public]: System Restore.lnk . (.Microsoft Corporation - Restauration du système de Microsoft® Windo.) -- C:\Windows\System32\rstrui.exe =>.Microsoft Corporation

O4 - GS\SystemTools [Public]: Task Scheduler.lnk . (...) -- C:\Windows\System32\taskschd.msc

O4 - GS\QuickLaunch [RONDEAU]: Classification.Lnk . (.Jeulin - Classification.) -- C:\Program Files\Classification\Classif.exe

O4 - GS\QuickLaunch [RONDEAU]: Dragon NaturallySpeaking 12.5.lnk . (.Acresso Software Inc. - InstallShield.) -- C:\Windows\Installer\{D5D422B9-6976-4E98-8DDF-9632CB515D7E}\NatSpeakD\_Shortcut\_D5D422B969764E988DDF9632CB515D7E.exe

O4 - GS\QuickLaunch [RONDEAU]: Google Chrome.lnk . (.Google Inc. - Google Chrome.) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\Application\chrome.exe

O4 - GS\QuickLaunch [RONDEAU]: HP Scan.lnk . (.Hewlett-Packard Co. - HPScan.) -- C:\Program Files\HP\HP Photosmart 5520 series\Bin\HPScan.exe =>.Hewlett-Packard Co

O4 - GS\QuickLaunch [RONDEAU]: Microsoft Office Outlook.lnk . (.Microsoft Corporation - Microsoft Office Outlook.) -- C:\Program Files\Microsoft Office\Office12\OUTLOOK.exe =>.Microsoft Corporation

O4 - GS\QuickLaunch [RONDEAU]: monAlbumPhoto.lnk . (.monAlbumPhoto - monAlbumPhoto.) -- C:\Program Files\monAlbumPhoto\monAlbumphoto.exe

O4 - GS\QuickLaunch [RONDEAU]: Snipping Tool.lnk . (.Microsoft Corporation - Outil Capture.) -- C:\Windows\System32\SnippingTool.exe =>.Microsoft Corporation

O4 - GS\QuickLaunch [RONDEAU]: Windows Media Player.lnk . (.Microsoft Corporation - Windows Media Player.) -- C:\Program Files\Windows Media Player\wmplayer.exe =>.Microsoft Corporation

O4 - GS\Program [RONDEAU]: Nutri Pro 7.lnk . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Installer\{7D7B1BA1-8914-43E5-B4EB-F53BC111AA9D}\\_229BCD31D3F80BADF181D0.exe

O4 - GS\Program [RONDEAU]: puissance.LNK . (.MEN - Pas de description.) -- C:\Program Files\puissance\puissance.exe

O4 - GS\Program [RONDEAU]: Windows Media Player.lnk . (.Microsoft Corporation - Windows Media Player.) -- C:\Program Files\Windows Media Player\wmplayer.exe =>.Microsoft Corporation

O4 - GS\Accessories [RONDEAU]: Command Prompt.lnk . (.Microsoft Corporation - Interpréteur de commandes Windows.) -- C:\Windows\System32\cmd.exe =>.Microsoft Corporation

O4 - GS\Accessories [RONDEAU]: Notepad.lnk . (.Microsoft Corporation - Bloc-notes.) -- C:\Windows\System32\notepad.exe =>.Microsoft Corporation

O4 - GS\Accessories [RONDEAU]: Run.lnk - Clé orpheline

O4 - GS\Accessories [RONDEAU]: Windows Explorer.lnk . (.Microsoft Corporation - Explorateur Windows.) -- C:\Windows\explorer.exe =>.Microsoft Corporation

O4 - GS\SendTo [RONDEAU]: Assistant Transfert de fichiers Bluetooth.LNK . (.Microsoft Corporation - Pas de description.) -- C:\Windows\System32\fsquirt.exe

O4 - GS\SendTo [RONDEAU]: AVS Mobile Uploader.lnk . (.Online Media Technologies Ltd. - AVS Mobile Uploader.) -- C:\Program Files\Common Files\AVSMedia\MobileUploader\AVSMobileUploader.exe

O4 - GS\SendTo [RONDEAU]: AVS Video Burner.lnk . (.Online Media Technologies Ltd. - AVS Video Burner.) -- C:\Program Files\Common Files\AVSMedia\BurnerService\AVSVideoBurner.exe

O4 - GS\SendTo [RONDEAU]: AVS Video Uploader.lnk . (.Online Media Technologies Ltd. - AVS Video Uploader.) -- C:\Program Files\Common Files\AVSMedia\VideoUploader\AVSVideoUploader.exe

O4 - GS\Desktop [RONDEAU]: AVS Video Editor.lnk . (.Online Media Technologies Ltd. - Video Editor.) -- C:\Program Files\AVS4YOU\AVSVideoEditor\AVSVideoEditor.exe

O4 - GS\Desktop [RONDEAU]: AVS4YOU Software Navigator.lnk . (.Online Media Technologies Ltd. - Pas de description.) -- C:\Program Files\AVS4YOU\AVSSoftwareNavigator\AVS4YOUSoftwareNavigator.exe

O4 - GS\Desktop [RONDEAU]: Description Cave et Caisses - Raccourci.lnk . (...) -- C:\Users\RONDEAU\Documents\Description Cave et Caisses.docx

O4 - GS\Desktop [RONDEAU]: Google Chrome.lnk . (.Google Inc. - Google Chrome.) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\Application\chrome.exe

O4 - GS\Desktop [RONDEAU]: La respiration.lnk . (.Studio PEREZ - Programme de seconde.) -- C:\Program Files\Pulmo\pulmo.exe

O4 - GS\Desktop [RONDEAU]: MAGIX Video deLuxe 2006.lnk . (.MAGIX AG - MAGIX Video deLuxe 2006.) -- C:\MAGIX\Video\_deLuxe\_2006\VideodeLuxe.exe

O4 - GS\Desktop [RONDEAU]: Nutri Pro7.lnk . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Installer\{7D7B1BA1-8914-43E5-B4EB-F53BC111AA9D}\\_F996BA2C3E5AC3484BE28B.exe

O4 - GS\Desktop [RONDEAU]: Sweet Home 3D.lnk . (.eTeks - Sweet Home 3D.) -- C:\Program Files\Sweet Home 3D\SweetHome3D.exe

O4 - GS\Desktop [RONDEAU]: ZHPDiag.lnk . (.Nicolas Coolman - ZHPDiag Setup.) -- C:\ZHPDiag\ZHPhep.exe =>.Nicolas Coolman

O4 - GS\Desktop [RONDEAU]: ZHPFix.lnk . (.Nicolas Coolman - ZHPDiag Setup.) -- C:\ZHPDiag\ZHPFix\ZHPhep.exe =>.Nicolas Coolman

~ Global Startup: 82 Scanned in 00mn 03s

---\\ Applications lancées au démarrage du sytème (O4)

O4 - GS\Startup [Public]: Bluetooth.lnk . (.Broadcom Corporation. - Bluetooth Tray Application.) -- C:\Program Files\WIDCOMM\Bluetooth Software\BTTray.exe

O4 - GS\Startup [Public]: eInstruction Device Manager.lnk . (.eInstruction Corporation - Launcher Application.) -- C:\Program Files\eInstruction\Device Manager\Launch.exe

O4 - HKLM\..\Run: [Windows Defender] . (.Microsoft Corporation - Windows Defender User Interface.) -- C:\Program Files\Windows Defender\MSASCui.exe

O4 - HKLM\..\Run: [CLMLServer] . (.CyberLink - CyberLink MediaLibray Service.) -- C:\Program Files\ASUS\AI TouchMedia\AI TouchMedia\Kernel\CLML\CLMLSvc.exe

O4 - HKLM\..\Run: [P2Go\_Menu] . (.CyberLink Corp. - StartMen Application.) -- C:\Program Files\CyberLink\Power2Go\MUITransfer\MUIStartMenu.exe

O4 - HKLM\..\Run: [PCMAgent] . (.CyberLink Corp. - CyberLink PowerCinema Resident Program.) -- C:\Program Files\ASUS\AI TouchMedia\AI TouchMedia\PCMAgent.exe

O4 - HKLM\..\Run: [PlayMovie] . (.CyberLink Corp. - CyberLink PlayMovie Resident ProgramPlayMov.) -- C:\Program Files\ASUS\AI TouchMedia\PlayMovie\PMVService.exe

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

O4 - HKLM\..\Run: [HControlUser] . (.Pas de propriétaire - HControlUser.) -- C:\Program Files\ASUS\ATK Hotkey\HControlUser.exe

O4 - HKLM\..\Run: [ATKOSD2] . (.ASUS - ATKOSD2.) -- C:\Program Files\ASUS\ATKOSD2\ATKOSD2.exe

O4 - HKLM\..\Run: [NvCplDaemon] . (.NVIDIA Corporation - NVIDIA Display Properties Extension.) -- C:\Windows\system32\NvCpl.dll =>.NVIDIA Corporation

O4 - HKLM\..\Run: [NvMediaCenter] . (.NVIDIA Corporation - NVIDIA Media Center Library.) -- C:\Windows\system32\NvMcTray.dll

O4 - HKLM\..\Run: [RtHDVCpl] . (.Realtek Semiconductor - HD Audio Control Panel.) -- C:\Windows\RtHDVCpl.exe =>.Realtek Semiconductor Corp

O4 - HKLM\..\Run: [CognizanceTS] . (.Cognizance Corporation - Terminal Services Virtual Channel Client.) -- C:\Program Files\ASUS Security Center\ASUS Security Protect Manager\Bin\ASTSVCC.dll

O4 - HKLM\..\Run: [ATKMEDIA] . (.ASUS - ATK Media.) -- C:\Program Files\ASUS\ATK Media\DMedia.exe

O4 - HKLM\..\Run: [ASUS Screen Saver Protector] . (.ASUS - AsScrPro.) -- C:\Windows\AsScrPro.exe

O4 - HKLM\..\Run: [ASUS Camera ScreenSaver] . (...) -- C:\Windows\AsScrProlog.exe

O4 - HKLM\..\Run: [SynTPEnh] . (.Synaptics, Inc. - Synaptics TouchPad Enhancements.) -- C:\Program Files\Synaptics\SynTP\SynTPEnh.exe

O4 - HKLM\..\Run: [Adobe Reader Speed Launcher] . (.Adobe Systems Incorporated - Adobe Acrobat SpeedLauncher.) -- C:\Program Files\Adobe\Reader 8.0\Reader\Reader\_sl.exe

O4 - HKLM\..\Run: [Skytel] . (.Realtek Semiconductor Corp. - Realtek Voice Manager.) -- C:\Windows\Skytel.exe =>.Realtek Semiconductor Corp

O4 - HKLM\..\Run: [APSDaemon] . (.Apple Inc. - Apple Push.) -- C:\Program Files\Common Files\Apple\Apple Application Support\APSDaemon.exe

O4 - HKLM\..\Run: [ISUSScheduler] . (.Macrovision Corporation - InstallShield Update Service Scheduler.) -- C:\Program Files\Common Files\InstallShield\UpdateService\issch.exe

O4 - HKLM\..\Run: [avgnt] . (.Avira Operations GmbH & Co. KG - Antivirus System Tray Tool (Desktop).) -- C:\Program Files\Avira\AntiVir Desktop\avgnt.exe

O4 - HKLM\..\Run: [QuickTime Task] . (.Apple Inc. - QuickTime Task.) -- C:\Program Files\QuickTime\QTTask.exe

O4 - HKLM\..\Run: [TkBellExe] . (.RealNetworks, Inc. - RealNetworks Scheduler.) -- C:\Program Files\Real\RealPlayer\Update\realsched.exe =>.RealNetworks, Inc

O4 - HKLM\..\Run: [HP Software Update] . (.Hewlett-Packard - hpwuSchd Application.) -- C:\Program Files\Hp\HP Software Update\HPWuSchd2.exe =>.Hewlett-Packard Co

O4 - HKLM\..\Run: [ISUSPM] . (.Flexera Software LLC. - Common Software Manager.) -- C:\ProgramData\FLEXnet\Connect\11\isuspm.exe

O4 - HKLM\..\Run: [DNS7reminder] . (.Nuance Communications, Inc. - Ereg.) -- C:\Program Files\Nuance\NaturallySpeaking12\Ereg\Ereg.exe

O4 - HKCU\..\Run: [Sidebar] . (.Microsoft Corporation - Volet Windows.) -- C:\Program Files\Windows Sidebar\sidebar.exe =>.Microsoft Corporation

O4 - HKCU\..\Run: [LightScribe Control Panel] . (.Hewlett-Packard Company - Pas de description.) -- C:\Program Files\Common Files\LightScribe\LightScribeControlPanel.exe

O4 - HKCU\..\Run: [ehTray.exe] . (.Microsoft Corporation - Media Center Tray Applet.) -- C:\Windows\ehome\ehTray.exe

O4 - HKCU\..\Run: [Sony Ericsson PC Companion] . (.Sony Ericsson Mobile Communications AB - Sony Ericsson PC Companion.) -- C:\Program Files\Sony Ericsson\Sony Ericsson PC Companion\PCCompanion.exe

O4 - HKCU\..\Run: [TomTomHOME.exe] . (.TomTom - System Tray application for TomTom HOME.) -- C:\Program Files\TomTom HOME 2\TomTomHOMERunner.exe

O4 - HKCU\..\Run: [Disulupefi] C:\Users\RONDEAU\AppData\Roaming\Ocugba\erza.exe (.not file.)

O4 - HKCU\..\Run: [ISUSPM Startup] C:\Program Files\Common Files\InstallShield\UpdateService\ISUSPM.exe (.not file.)

O4 - HKCU\..\Run: [HP Photosmart 5520 series (NET)] . (.Hewlett-Packard Co. - ScanToPCActivationApp.) -- C:\Program Files\HP\HP Photosmart 5520 series\Bin\ScanToPCActivationApp.exe =>.Hewlett-Packard Co

O4 - HKCU\..\Run: [HP Photosmart 5520 series (NET) #2] . (.Hewlett-Packard Co. - ScanToPCActivationApp.) -- C:\Program Files\HP\HP Photosmart 5520 series\Bin\ScanToPCActivationApp.exe =>.Hewlett-Packard Co

O4 - HKCU\..\Run: [ISUSPM] . (.Flexera Software LLC. - Common Software Manager.) -- C:\ProgramData\FLEXnet\Connect\11\ISUSPM.exe

O4 - HKUS\S-1-5-19\..\Run: [Sidebar] . (.Microsoft Corporation - Volet Windows.) -- C:\Program Files\Windows Sidebar\Sidebar.exe =>.Microsoft Corporation

O4 - HKUS\S-1-5-19\..\Run: [WindowsWelcomeCenter] Clé orpheline

O4 - HKUS\S-1-5-20\..\Run: [Sidebar] . (.Microsoft Corporation - Volet Windows.) -- C:\Program Files\Windows Sidebar\Sidebar.exe =>.Microsoft Corporation

O4 - HKUS\S-1-5-20\..\Run: [WindowsWelcomeCenter] Clé orpheline

O4 - HKUS\S-1-5-21-1479064021-3229367824-3524447455-1000\..\Run: [Sidebar] . (.Microsoft Corporation - Volet Windows.) -- C:\Program Files\Windows Sidebar\sidebar.exe =>.Microsoft Corporation

O4 - HKUS\S-1-5-21-1479064021-3229367824-3524447455-1000\..\Run: [LightScribe Control Panel] . (.Hewlett-Packard Company - Pas de description.) -- C:\Program Files\Common Files\LightScribe\LightScribeControlPanel.exe

O4 - HKUS\S-1-5-21-1479064021-3229367824-3524447455-1000\..\Run: [ehTray.exe] . (.Microsoft Corporation - Media Center Tray Applet.) -- C:\Windows\ehome\ehTray.exe

O4 - HKUS\S-1-5-21-1479064021-3229367824-3524447455-1000\..\Run: [Sony Ericsson PC Companion] . (.Sony Ericsson Mobile Communications AB - Sony Ericsson PC Companion.) -- C:\Program Files\Sony Ericsson\Sony Ericsson PC Companion\PCCompanion.exe

O4 - HKUS\S-1-5-21-1479064021-3229367824-3524447455-1000\..\Run: [TomTomHOME.exe] . (.TomTom - System Tray application for TomTom HOME.) -- C:\Program Files\TomTom HOME 2\TomTomHOMERunner.exe

O4 - HKUS\S-1-5-21-1479064021-3229367824-3524447455-1000\..\Run: [Disulupefi] C:\Users\RONDEAU\AppData\Roaming\Ocugba\erza.exe (.not file.)

O4 - HKUS\S-1-5-21-1479064021-3229367824-3524447455-1000\..\Run: [ISUSPM Startup] C:\Program Files\Common Files\InstallShield\UpdateService\ISUSPM.exe (.not file.)

O4 - HKUS\S-1-5-21-1479064021-3229367824-3524447455-1000\..\Run: [HP Photosmart 5520 series (NET)] . (.Hewlett-Packard Co. - ScanToPCActivationApp.) -- C:\Program Files\HP\HP Photosmart 5520 series\Bin\ScanToPCActivationApp.exe =>.Hewlett-Packard Co

O4 - HKUS\S-1-5-21-1479064021-3229367824-3524447455-1000\..\Run: [HP Photosmart 5520 series (NET) #2] . (.Hewlett-Packard Co. - ScanToPCActivationApp.) -- C:\Program Files\HP\HP Photosmart 5520 series\Bin\ScanToPCActivationApp.exe =>.Hewlett-Packard Co

O4 - HKUS\S-1-5-21-1479064021-3229367824-3524447455-1000\..\Run: [ISUSPM] . (.Flexera Software LLC. - Common Software Manager.) -- C:\ProgramData\FLEXnet\Connect\11\ISUSPM.exe

~ Application: Scanned in 00mn 00s

---\\ Boutons situés sur la barre d'outils principale d'Internet Explorer (O9)

O9 - Extra button: @C:\Program Files\Windows Live\Companion\companionlang.dll,-600 - {0000036B-C524-4050-81A0-243669A86B9F} . (.Microsoft Corporation - Windows Live Messenger Companion core resources.) -- C:\Program Files\Windows Live\Companion\companionres.dll

O9 - Extra button: @C:\Program Files\Windows Live\Writer\WindowsLiveWriterShortcuts.dll,-1003 - {219C3416-8CB2-491a-A3C7-D9FCDDC9D600} . (.Microsoft Corporation - Windows Live Writer Blog This Extension.) -- C:\Program Files\Windows Live\Writer\WriterBrowserExtension.dll

O9 - Extra button: HP Smart Print - {22CC3EBD-C286-43aa-B8E6-06B115F74162} . (...) -- C:\Program Files\Hewlett-Packard\Smart Print 2.0\smartprint.ico

O9 - Extra button: Research - {92780B25-18CC-41C8-B9BE-3C9C571A8263} . (...) -- C:\Program Files\Microsoft Office\Office12\REFBARH.ICO

~ IE Extra Buttons: Scanned in 00mn 00s

---\\ Winsock hijacker (Layered Service Provider) (O10)

O10 - WLSP:\000000000001\Winsock LSP File . (.Microsoft Corporation - Network Location Awareness 2.) -- C:\Windows\system32\NLAapi.dll

O10 - WLSP:\000000000002\Winsock LSP File . (.Microsoft Corporation - Fournisseur Shim d'affectation de noms de messagerie.) -- C:\Windows\system32\napinsp.dll

O10 - WLSP:\000000000003\Winsock LSP File . (.Microsoft Corporation - Fournisseur d’espace de noms PNRP.) -- C:\Windows\system32\pnrpnsp.dll

O10 - WLSP:\000000000004\Winsock LSP File . (.Microsoft Corporation - Fournisseur d’espace de noms PNRP.) -- C:\Windows\system32\pnrpnsp.dll

O10 - WLSP:\000000000005\Winsock LSP File . (.Microsoft Corporation - Fournisseur de service Sockets 2.0 de Microsoft Windows.) -- C:\Windows\system32\mswsock.dll =>.Microsoft Corporation

O10 - WLSP:\000000000006\Winsock LSP File . (.Microsoft Corporation - LDAP RnR Provider DLL.) -- C:\Windows\system32\winrnr.dll

O10 - WLSP:\000000000007\Winsock LSP File . (.Microsoft Corporation - Windows Sockets Helper DLL.) -- C:\Windows\system32\wshbth.dll

~ Winsock: 7 Scanned in 00mn 00s

---\\ Objets ActiveX (Downloaded Program Files)(O16)

O16 - DPF: {166B1BCA-3F9C-11CF-8075-444553540000} ((no name)) - http://download.macromedia.com/pub/shockwave/cabs/director/sw.cab

O16 - DPF: {1ABA5FAC-1417-422B-BA82-45C35E2C908B} ((no name)) - http://kitchenplanner.ikea.com/FR/Core/Player/2020PlayerAX\_IKEA\_Win32.cab

O16 - DPF: {233C1507-6A77-46A4-9443-F871F945D258} ((no name)) - http://download.macromedia.com/pub/shockwave/cabs/director/sw.cab

O16 - DPF: {784797A8-342D-4072-9486-03C8D0F2F0A1} ((no name)) - https://www.battlefieldheroes.com/static/updater/BFHUpdater\_5.0.67.0.cab

O16 - DPF: {E2883E8F-472F-4FB0-9522-AC9BF37916A7} ((no name)) - http://platformdl.adobe.com/NOS/getPlusPlus/1.6/gp.cab

~ Objets ActiveX: Scanned in 00mn 00s

---\\ Modification Domaine/Adresses DNS (O17)

O17 - HKLM\System\CCS\Services\Tcpip\..\{D3E003F8-9F17-4BE8-AB81-D9613E00775C}: DhcpNameServer = 212.27.40.240 212.27.40.241

O17 - HKLM\System\CCS\Services\Tcpip\..\{ECF2F5E4-63E6-4E57-9EFC-23AF4BF2110F}: DhcpNameServer = 10.2.100.50

O17 - HKLM\System\CCS\Services\Tcpip\..\{ECF2F5E4-63E6-4E57-9EFC-23AF4BF2110F}: DhcpDomain = interne.collegejy

O17 - HKLM\System\CS1\Services\Tcpip\..\{D3E003F8-9F17-4BE8-AB81-D9613E00775C}: DhcpNameServer = 212.27.40.240 212.27.40.241

O17 - HKLM\System\CS1\Services\Tcpip\..\{ECF2F5E4-63E6-4E57-9EFC-23AF4BF2110F}: DhcpNameServer = 10.2.100.50

O17 - HKLM\System\CS1\Services\Tcpip\..\{ECF2F5E4-63E6-4E57-9EFC-23AF4BF2110F}: DhcpDomain = interne.collegejy

O17 - HKLM\System\CS2\Services\Tcpip\..\{D3E003F8-9F17-4BE8-AB81-D9613E00775C}: DhcpNameServer = 212.27.40.240 212.27.40.241

O17 - HKLM\System\CS2\Services\Tcpip\..\{ECF2F5E4-63E6-4E57-9EFC-23AF4BF2110F}: DhcpNameServer = 10.2.100.50

O17 - HKLM\System\CS2\Services\Tcpip\..\{ECF2F5E4-63E6-4E57-9EFC-23AF4BF2110F}: DhcpDomain = interne.collegejy

O17 - HKLM\System\CCS\Services\Tcpip\Parameters: DhcpNameServer = 212.27.40.240 212.27.40.241

~ Domain: Scanned in 00mn 00s

---\\ Protocole additionnel (O18)

O18 - Handler: wlmailhtml - {03C514A3-1EFB-4856-9F99-10D7BE1653C0} . (.Microsoft Corporation - Windows Live Mail.) -- C:\Program Files\Windows Live\Mail\mailcomm.dll =>.Microsoft Corporation

O18 - Filter: text/xml - {807563E5-5146-11D5-A672-00B0D022E945} . (.Microsoft Corporation - Microsoft Office XML MIME Filter.) -- C:\Program Files\Common Files\microsoft shared\OFFICE12\MSOXMLMF.dll =>.Microsoft Corporation

~ Protocole Additionnel: Scanned in 00mn 00s

---\\ Valeur de Registre AppInit\_DLLs et sous-clés Winlogon Notify (autorun) (O20)

O20 - AppInit\_DLLs: . (.Google - Google Desktop.) - C:\Program Files\google\google~1\goec62~1.dll

~ AppInit DLL: Scanned in 00mn 00s

---\\ Clé de Registre autorun ShellServiceObjectDelayLoad (SSO/SSODL) (O21)

O21 - SSODL: WebCheck - {E6FB5E20-DE35-11CF-9C87-00AA005127ED} . (.Microsoft Corporation - Contrôleur de site Web.) -- C:\Windows\System32\webcheck.dll

~ SSODL: 1 Scanned in 00mn 00s

---\\ Clé de Registre autorun SharedTaskScheduler (STS) (O22)

O22 - SharedTaskScheduler: Component Categories cache daemon - {8C7461EF-2B13-11d2-BE35-3078302C2030} . (.Microsoft Corporation - Bibliothèque de l'interface utilisateur du.) -- C:\Windows\System32\browseui.dll

~ STS/SSO: Scanned in 00mn 00s

---\\ Liste des services NT non Microsoft et non désactivés (O23)

O23 - Service: Avira Planificateur (AntiVirSchedulerService) . (.Avira Operations GmbH & Co. KG - Antivirus Host Framework Service.) - C:\Program Files\Avira\AntiVir Desktop\sched.exe

O23 - Service: Avira Protection temps réel (AntiVirService) . (.Avira Operations GmbH & Co. KG - Antivirus Host Framework Service.) - C:\Program Files\Avira\AntiVir Desktop\avguard.exe

O23 - Service: Avira Protection Web (AntiVirWebService) . (.Avira Operations GmbH & Co. KG - AntiVir WebGuard Service.) - C:\Program Files\Avira\AntiVir Desktop\AVWEBGRD.exe

O23 - Service: ASLDR Service (ASLDRService) . (.Pas de propriétaire - ASLDR Service.) - C:\Program Files\ASUS\ATK Hotkey\ASLDRSrv.exe

O23 - Service: ATKGFNEX Service (ATKGFNEXSrv) . (.Pas de propriétaire - GFNEXSrv.) - C:\Program Files\ATKGFNEX\GFNEXSrv.exe

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

O23 - Service: Dragon Service (DragonSvc) . (.Nuance Communications, Inc. - Dragon NaturallySpeaking Service.) - C:\Program Files\Common Files\Nuance\dgnsvc.exe

O23 - Service: LightScribeService Direct Disc Labeling Service (LightScribeService) . (.Hewlett-Packard Company - LightScribe Service.) - C:\Program Files\Common Files\LightScribe\LSSrvc.exe

O23 - Service: NVIDIA Display Driver Service (nvsvc) . (.NVIDIA Corporation - NVIDIA Driver Helper Service, Version 176.0.) - C:\Windows\System32\nvvsvc.exe

O23 - Service: RealNetworks Downloader Resolver Service (RealNetworks Downloader Resolver Service) . (...) - C:\Program Files\RealNetworks\RealDownloader\rndlresolversvc.exe

O23 - Service: spmgr (spmgr) . (.Pas de propriétaire - spmgr Module.) - C:\Program Files\ASUS\NB Probe\SPM\spmgr.exe

O23 - Service: TomTomHOMEService (TomTomHOMEService) . (.TomTom - Windows Service for TomTom HOME.) - C:\Program Files\TomTom HOME 2\TomTomHOMEService.exe

O23 - Service: {49DE1C67-83F8-4102-99E0-C16DCC7EEC796} ({49DE1C67-83F8-4102-99E0-C16DCC7EEC796}) . (.Cyberlink Corp. - FCL Driver.) - C:\Program Files\ASUS\AI TouchMedia\PlayMovie\000.fcl

~ Services: 13 Scanned in 00mn 05s

---\\ Enumération Active Desktop & MHTML Editor (O24)

O24 - Default MHTML Editor: Last - .(.Microsoft Corporation - Microsoft Office Word.) - C:\Program Files\Microsoft Office\Office12\WINWORD.exe

O24 - Desktop General: BackupWallPaper - .(...) - C:\Windows\Web\Wallpaper\img11.jpg

O24 - Desktop General: WallPaper - .(...) - C:\Windows\Web\Wallpaper\img11.jpg

~ Desktop Component: 4 Scanned in 00mn 00s

---\\ Enumère les données de BootExecute (BEX) (O34)

O34 - HKLM BootExecute: (autocheck autochk \*) - File not found

~ BEX: 1 Scanned in 00mn 00s

---\\ Tâches planifiées en automatique (O39)

O39 - APT:Automatic Planified Task - C:\Windows\Tasks\Ad-Aware Update (Weekly).job [370]

O39 - APT:Automatic Planified Task - C:\Windows\Tasks\Adobe Flash Player Updater.job [1002]

O39 - APT:Automatic Planified Task - C:\Windows\Tasks\User\_Feed\_Synchronization-{793C64DF-F4F5-4CD3-9443-304F915C9135}.job [422]

[MD5.00000000000000000000000000000000] [APT] [Ad-Aware Update (Weekly)] (...) -- C:\Program Files\Lavasoft\Ad-Aware\Ad-AwareAdmin.exe (.not file.) [0]

[MD5.F7AB315A4D400CA876381D1E188A2E20] [APT] [Adobe Flash Player Updater] (.Adobe Systems Incorporated.) -- C:\Windows\system32\Macromed\Flash\FlashPlayerUpdateService.exe [257928]

[MD5.F4DCD4912B185C3AAEB92A7040832AD1] [APT] [ASUS Live Update] (...) -- C:\Program Files\ASUS\ASUS Live Update\ALU.exe [51768]

[MD5.38595C19227D211B5A0932F6609A6C32] [APT] [ASUS SmartLogon Console Sensor] (.ASUS.) -- C:\Program Files\ASUS\SmartLogon\sensorsrv.exe [297528]

[MD5.00000000000000000000000000000000] [APT] [GoogleUpdateTaskMachineCore] (...) -- C:\Program Files\Google\Update\GoogleUpdate.exe (.not file.) [0]

[MD5.6D51713A36C0733A4BDD94EAD5A33AD9] [APT] [HPCustParticipation HP Photosmart 5520 series] (.Hewlett-Packard Co..) -- C:\Program Files\HP\HP Photosmart 5520 series\Bin\HPCustPartic.exe [2938984]

[MD5.DDBE89226D55D694F1B7B3DD0C324640] [APT] [RealDownloaderDownloaderScheduledTaskS-1-5-21-1479064021-3229367824-3524447455-1000] (.RealNetworks, Inc..) -- C:\Program Files\RealNetworks\RealDownloader\recordingmanager.exe [233048]

[MD5.675DE4EC2D88A6D68C39C662A3204596] [APT] [RealDownloaderRealUpgradeLogonTaskS-1-5-21-1479064021-3229367824-3524447455-1000] (.RealNetworks, Inc..) -- C:\Program Files\RealNetworks\RealDownloader\realupgrade.exe [187984]

[MD5.675DE4EC2D88A6D68C39C662A3204596] [APT] [RealDownloaderRealUpgradeScheduledTaskS-1-5-21-1479064021-3229367824-3524447455-1000] (.RealNetworks, Inc..) -- C:\Program Files\RealNetworks\RealDownloader\realupgrade.exe [187984]

[MD5.2A356FA2650E30E139F0476979548BF6] [APT] [RealPlayerRealUpgradeLogonTaskS-1-5-21-1479064021-3229367824-3524447455-1000] (.RealNetworks, Inc..) -- C:\Program Files\Real\RealUpgrade\RealUpgrade.exe [187984]

[MD5.2A356FA2650E30E139F0476979548BF6] [APT] [RealPlayerRealUpgradeScheduledTaskS-1-5-21-1479064021-3229367824-3524447455-1000] (.RealNetworks, Inc..) -- C:\Program Files\Real\RealUpgrade\RealUpgrade.exe [187984]

[MD5.00000000000000000000000000000000] [APT] [{D2D22519-C1FA-4B3F-8B78-33CB68BA9808}] (...) -- E:\SETUP.exe (.not file.) [0]

[MD5.34EBD4FF6A24D86BB4716D6AFCC1A89B] [APT] [AppleSoftwareUpdate] (.Apple Inc..) -- C:\Program Files\Apple Software Update\SoftwareUpdate.exe [561984]

~ Scheduled Task: 17 Scanned in 00mn 04s

---\\ Composants installés (ActiveSetup Installed Components) (O40)

O40 - ASIC: Microsoft Windows Media Player - >{22d6f312-b0f6-11d0-94ab-0080c74c7e95} . (.Microsoft Corporation - Ressources du Lecteur Windows Media.) -- C:\Windows\System32\wmploc.dll =>.Microsoft Corporation

O40 - ASIC: Internet Explorer - >{26923b43-4d38-484f-9b9e-de460746276c} . (.Microsoft Corporation - Utilitaire d’initialisation d’Internet Explorer par utilisateur.) -- C:\Windows\system32\ie4uinit.exe

O40 - ASIC: Browser Customizations - >{60B49E34-C7CC-11D0-8953-00A0C90347FF} . (.Microsoft Corporation - Personnalisation d’IEAK.) -- C:\Windows\system32\iedkcs32.dll

O40 - ASIC: LightScribe Control Panel - {10880D85-AAD9-4558-ABDC-2AB1552D831F} . (.Hewlett-Packard Company - Pas de description.) -- C:\Program Files\Common Files\LightScribe\LSRunOnce.exe

O40 - ASIC: (no name) - {2179C5D3-EBFF-11CF-B6FD-00AA00B4E220} . (.Microsoft Corporation - Microsoft Windows Media Component Removal File..) -- C:\Windows\system32\msdxm.ocx

O40 - ASIC: Windows Media Player 5.2 - {22d6f312-b0f6-11d0-94ab-0080c74c7e95} . (...) -- C:\Windows\INF\mswmp.inf =>.Microsoft Corporation

O40 - ASIC: Themes Setup - {2C7339CF-2B09-4501-B3F3-F3508C9228ED} . (.Microsoft Corporation - API Windows Theme.) -- C:\Windows\System32\themeui.dll

O40 - ASIC: Microsoft Windows Mail 7 - {44BBA840-CC51-11CF-AAFA-00AA00B6015C} . (.Microsoft Corporation - Windows Mail.) -- C:\Program Files\Windows Mail\WinMail.exe =>.Microsoft Corporation

O40 - ASIC: Browsing Enhancements - {630b1da0-b465-11d1-9948-00c04f98bbc9} . (.Microsoft Corporation - Extension Shell dossier FTP Microsoft Internet Explorer..) -- C:\Windows\System32\msieftp.dll

O40 - ASIC: Microsoft Windows Media Player - {6BF52A52-394A-11d3-B153-00C04F79FAA6} . (.Microsoft Corporation - Ressources du Lecteur Windows Media.) -- C:\Windows\System32\wmploc.dll =>.Microsoft Corporation

O40 - ASIC: Windows Desktop Update - {89820200-ECBD-11cf-8B85-00AA005B4340} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\Windows\System32\shell32.dll

O40 - ASIC: Internet Explorer - {89820200-ECBD-11cf-8B85-00AA005B4383} . (.Microsoft Corporation - Utilitaire d’initialisation d’Internet Explorer par utilisateur.) -- C:\Windows\system32\ie4uinit.exe

O40 - ASIC: (no name) - {89B4C1CD-B018-4511-B0A1-5476DBF70820} . (.Microsoft Corporation - Microsoft .NET IE SECURITY REGISTRATION.) -- C:\Windows\system32\mscories.dll

O40 - ASIC: Adobe Flash Player - {D27CDB6E-AE6D-11CF-96B8-444553540000} . (.Adobe Systems, Inc. - Adobe Flash Player 12.0 r0.) -- C:\Windows\system32\Macromed\Flash\Flash32\_12\_0\_0\_70.ocx

~ Active Setup: 14 Scanned in 00mn 00s

---\\ Pilotes lancés au démarrage du système (O41)

O41 - Driver: (AFD) . (.Microsoft Corporation - Ancillary Function Driver for WinSock.) - C:\Windows\system32\drivers\afd.sys

O41 - Driver: (avipbb) . (.Avira Operations GmbH & Co. KG - Avira Driver for Security Enhancement.) - C:\Windows\System32\DRIVERS\avipbb.sys

O41 - Driver: (avkmgr) . (.Avira Operations GmbH & Co. KG - Avira Manager Driver.) - C:\Windows\System32\DRIVERS\avkmgr.sys

O41 - Driver: (cdrom) . (.Microsoft Corporation - SCSI CD-ROM Driver.) - C:\Windows\System32\DRIVERS\cdrom.sys

O41 - Driver: C:\Windows\System32\drivers\dfsc.sys (DfsC) . (.Microsoft Corporation - DFS Namespace Client Driver.) - C:\Windows\System32\Drivers\dfsc.sys

O41 - Driver: (i8042prt) . (.Microsoft Corporation - Pilote de port i8042.) - C:\Windows\System32\DRIVERS\i8042prt.sys

O41 - Driver: (kbdclass) . (.Microsoft Corporation - Pilote de la classe Clavier.) - C:\Windows\System32\DRIVERS\kbdclass.sys

O41 - Driver: (kbdhid) . (.Microsoft Corporation - Pilote de filtre clavier HID.) - C:\Windows\System32\DRIVERS\kbdhid.sys

O41 - Driver: (mouclass) . (.Microsoft Corporation - Pilote de la classe Souris.) - C:\Windows\System32\DRIVERS\mouclass.sys

O41 - Driver: (NetBIOS) . (.Microsoft Corporation - NetBIOS interface driver.) - C:\Windows\System32\DRIVERS\netbios.sys

O41 - Driver: (netbt) . (.Microsoft Corporation - MBT Transport driver.) - C:\Windows\System32\DRIVERS\netbt.sys

O41 - Driver: (nsiproxy) . (.Microsoft Corporation - NSI Proxy.) - C:\Windows\System32\drivers\nsiproxy.sys

O41 - Driver: C:\Windows\System32\drivers\pacer.sys (PSched) . (.Microsoft Corporation - Planificateur de paquets QoS.) - C:\Windows\System32\DRIVERS\pacer.sys

O41 - Driver: (RasAcd) . (.Microsoft Corporation - RAS Automatic Connection Driver.) - C:\Windows\System32\DRIVERS\rasacd.sys

O41 - Driver: (rdbss) . (.Microsoft Corporation - Redirected Drive Buffering SubSystem Driver.) - C:\Windows\System32\DRIVERS\rdbss.sys

O41 - Driver: (RDPCDD) . (.Microsoft Corporation - RDP Miniport.) - C:\Windows\System32\DRIVERS\RDPCDD.sys

O41 - Driver: (RDPENCDD) . (.Microsoft Corporation - RDP Miniport.) - C:\Windows\System32\drivers\rdpencdd.sys

O41 - Driver: C:\Windows\System32\tcpipcfg.dll (Smb) . (.Microsoft Corporation - SMB Transport driver.) - C:\Windows\System32\DRIVERS\smb.sys

O41 - Driver: (ssmdrv) . (.Avira GmbH - AVIRA SnapShot Driver.) - C:\Windows\System32\DRIVERS\ssmdrv.sys

O41 - Driver: C:\Windows\System32\tcpipcfg.dll (tdx) . (.Microsoft Corporation - TDI Translation Driver.) - C:\Windows\System32\DRIVERS\tdx.sys

O41 - Driver: (TermDD) . (.Microsoft Corporation - Terminal Server Driver.) - C:\Windows\System32\DRIVERS\termdd.sys

O41 - Driver: (VgaSave) . (.Microsoft Corporation - VGA/Super VGA Video Driver.) - C:\Windows\system32\drivers\vga.sys

O41 - Driver: (Wanarpv6) . (.Microsoft Corporation - MS Remote Access and Routing ARP Driver.) - C:\Windows\System32\DRIVERS\wanarp.sys

~ Drivers: 69 Scanned in 00mn 00s

---\\ Logiciels installés (O42)

O42 - Logiciel: "La respiration" version 1.2a - (...) [HKLM] -- La respiration\_is1

O42 - Logiciel: 7-Zip 9.20 - (...) [HKLM] -- 7-Zip

O42 - Logiciel: AI TouchMedia - (.CyberLink Corp..) [HKLM] -- InstallShield\_{2637C347-9DAD-11D6-9EA2-00055D0CA761}

O42 - Logiciel: AI TouchMedia - (.CyberLink Corp..) [HKLM] -- {2637C347-9DAD-11D6-9EA2-00055D0CA761}

O42 - Logiciel: ASUS CopyProtect - (.ASUS.) [HKLM] -- {6B77A7F6-DD63-4F13-A6FF-83137A5AC354}

O42 - Logiciel: ASUS LifeFrame3 - (.ASUS.) [HKLM] -- {1DBD1F12-ED93-49C0-A7CC-56CBDE488158}

O42 - Logiciel: ASUS Live Update - (.ASUS.) [HKLM] -- {E657B243-9AD4-4ECC-BE81-4CCF8D667FD0}

O42 - Logiciel: ASUS Power4Gear eXtreme - (.ASUS.) [HKLM] -- {9B6239BF-4E85-4590-8D72-51E30DB1A9AA}

O42 - Logiciel: ASUS Security Protect Manager - (.ASUSTeK Computer Inc..) [HKLM] -- {D8D4AF9A-6ADE-4B14-A7F5-BA858792729E}

O42 - Logiciel: ASUS SmartLogon - (.ASUS.) [HKLM] -- {64452561-169F-4A36-A2FF-B5E118EC65F5}

O42 - Logiciel: ASUS Splendid Video Enhancement Technology - (.ASUS.) [HKLM] -- {0969AF05-4FF6-4C00-9406-43599238DE0D}

O42 - Logiciel: ASUS Virtual Camera - (.ASUS.) [HKLM] -- {EC8BD21F-0CA0-4BBF-97D9-4A52B30041A1}

O42 - Logiciel: ATK Generic Function Service - (.ATK.) [HKLM] -- {D3D54F3E-C5C3-443D-978F-87A72E5616E8}

O42 - Logiciel: ATK Hotkey - (.ASUS.) [HKLM] -- {7C05592D-424B-46CB-B505-E0013E8E75C9}

O42 - Logiciel: ATK Media - (.ASUS.) [HKLM] -- {D1E5870E-E3E5-4475-98A6-ADD614524ADF}

O42 - Logiciel: ATKOSD2 - (.ASUS.) [HKLM] -- {3B05F2FB-745B-4012-ADF2-439F36B2E70B}

O42 - Logiciel: AVS Screen Capture version 2.0.2 - (.Online Media Technologies Ltd..) [HKLM] -- AVS Screen Capture\_is1

O42 - Logiciel: AVS Update Manager 1.0 - (.Online Media Technologies Ltd..) [HKLM] -- AVS Update Manager\_is1

O42 - Logiciel: AVS Video Editor 6 - (.Online Media Technologies Ltd..) [HKLM] -- AVS Video Editor\_is1

O42 - Logiciel: AVS Video Recorder 2.5 - (.Online Media Technologies Ltd..) [HKLM] -- AVS Video Recorder\_is1

O42 - Logiciel: AVS4YOU Software Navigator 1.4 - (.Online Media Technologies Ltd..) [HKLM] -- AVS4YOU Software Navigator\_is1

O42 - Logiciel: Adobe AIR - (.Adobe Systems Inc..) [HKLM] -- Adobe AIR

O42 - Logiciel: Adobe AIR - (.Adobe Systems Inc..) [HKLM] -- {A2BCA9F1-566C-4805-97D1-7FDC93386723}

O42 - Logiciel: Adobe Flash Player 12 ActiveX - (.Adobe Systems Incorporated.) [HKLM] -- Adobe Flash Player ActiveX

O42 - Logiciel: Adobe Flash Player 12 Plugin - (.Adobe Systems Incorporated.) [HKLM] -- Adobe Flash Player Plugin

O42 - Logiciel: Adobe Reader 8.1.2 - Français - (.Adobe Systems Incorporated.) [HKLM] -- {AC76BA86-7AD7-1036-7B44-A81200000003}

O42 - Logiciel: Adobe Shockwave Player 11.5 - (.Adobe Systems, Inc..) [HKLM] -- Adobe Shockwave Player

O42 - Logiciel: Apple Application Support - (.Apple Inc..) [HKLM] -- {5D09C772-ECB3-442B-9CC6-B4341C78FDC2}

O42 - Logiciel: Apple Software Update - (.Apple Inc..) [HKLM] -- {789A5B64-9DD9-4BA5-915A-F0FC0A1B7BFE} =>.Apple Inc

O42 - Logiciel: Asus\_Camera\_ScreenSaver - (.ASUS.) [HKLM] -- Asus\_Camera\_ScreenSaver

O42 - Logiciel: Atheros Client Installation Program - (.Atheros.) [HKLM] -- {28006915-2739-4EBE-B5E8-49B25D32EB33}

O42 - Logiciel: AuthenTec Fingerprint Sensor Minimum Install - (.AuthenTec, Inc..) [HKLM] -- {EB4DF30B-102B-4F0C-927A-D50E037A325D}

O42 - Logiciel: Avira Free Antivirus v14.0.2.286 - (.Avira.) [HKLM] -- Avira AntiVir Desktop

O42 - Logiciel: Bing Bar - (.Microsoft Corporation.) [HKLM] -- {FF6DD716-7B10-4269-9F19-FFB07AC4CD95} =>Toolbar.Bing

O42 - Logiciel: BrowserSafeguard - (.Browsersafeguard.) [HKCU] -- Browsersafeguard =>PUP.BrowserSafeguard

O42 - Logiciel: Chinese Traditional Fonts Support For Adobe Reader 8 - (.Adobe Systems.) [HKLM] -- {AC76BA86-7AD7-2448-0000-800000000003}

O42 - Logiciel: Cisco EAP-FAST Module - (.Cisco Systems, Inc..) [HKLM] -- {415B2719-AD3A-4944-B404-C472DB6085B3}

O42 - Logiciel: Cisco LEAP Module - (.Cisco Systems, Inc..) [HKLM] -- {83770D14-21B9-44B3-8689-F7B523F94560}

O42 - Logiciel: Cisco PEAP Module - (.Cisco Systems, Inc..) [HKLM] -- {669C7BD8-DAA2-49B6-966C-F1E2AAE6B17E}

O42 - Logiciel: Classification - (...) [HKLM] -- Classification-1

O42 - Logiciel: Complément Messenger - (.Microsoft Corporation.) [HKLM] -- {6E5324C1-84FC-4F76-9A3A-C65E07F80EE6}

O42 - Logiciel: CyberLink LabelPrint - (.CyberLink Corp..) [HKLM] -- {C59C179C-668D-49A9-B6EA-0121CCFC1243}

O42 - Logiciel: CyberLink Power2Go - (.CyberLink Corp..) [HKLM] -- InstallShield\_{40BF1E83-20EB-11D8-97C5-0009C5020658}

O42 - Logiciel: CyberLink Power2Go - (.CyberLink Corp..) [HKLM] -- {40BF1E83-20EB-11D8-97C5-0009C5020658}

O42 - Logiciel: D3DX10 - (.Microsoft.) [HKLM] -- {E09C4DB7-630C-4F06-A631-8EA7239923AF}

O42 - Logiciel: DeviceManager - (.eInstruction.) [HKLM] -- DeviceManager

O42 - Logiciel: Dolby Control Center - (.Dolby.) [HKLM] -- {DE66EFAD-B9CC-4FD4-9157-6C18E5100161}

O42 - Logiciel: Dragon NaturallySpeaking 12 - (.Nuance Communications Inc..) [HKLM] -- {D5D422B9-6976-4E98-8DDF-9632CB515D7E}

O42 - Logiciel: Evolution allélique - (...) [HKLM] -- Evolution allélique

O42 - Logiciel: Express Gate - (.devicevm.) [HKLM] -- {27D51A76-371D-48B6-B06E-4137A15B7583}

O42 - Logiciel: FreeMind - (...) [HKLM] -- B991B020-2968-11D8-AF23-444553540000\_is1

O42 - Logiciel: Google Chrome - (.Google Inc..) [HKCU] -- Google Chrome

O42 - Logiciel: Google Desktop - (.Google.) [HKLM] -- Google Desktop

O42 - Logiciel: Google Earth - (.Google.) [HKLM] -- {A2264E8F-1649-11E3-8BED-B8AC6F98CCE3}

O42 - Logiciel: HP Photo Creations - (.HP Photo Creations Powered by RocketLife.) [HKLM] -- HP Photo Creations

O42 - Logiciel: HP Update - (.Hewlett-Packard.) [HKLM] -- {6F1C00D2-25C2-4CBA-8126-AE9A6E2E9CD5}

O42 - Logiciel: ITECIR - (.ITE.) [HKLM] -- {40580068-9B10-40B5-9548-536CE88AB23C}

O42 - Logiciel: Java 7 Update 17 - (.Oracle.) [HKLM] -- {26A24AE4-039D-4CA4-87B4-2F83217017FF}

O42 - Logiciel: Java Runtime Environment 1.1 - (...) [HKLM] -- JRE 1.1

O42 - Logiciel: Junk Mail filter update - (.Microsoft Corporation.) [HKLM] -- {1F6AB0E7-8CDD-4B93-8A23-AA9EB2FEFCE4}

O42 - Logiciel: LightScribe System Software 1.14.17.1 - (.LightScribe.) [HKLM] -- {0E7DBD52-B097-4F2B-A7C7-F105B0D20FDB}

O42 - Logiciel: Logiciel de base du périphérique HP Photosmart 5520 series - (.Hewlett-Packard Co..) [HKLM] -- {0FCD946D-1C6E-4476-A441-88B9ADE88ACA} =>.Hewlett-Packard Co

O42 - Logiciel: MAGIX Music Manager - (.MAGIX AG.) [HKLM] -- MAGIX Music Manager

O42 - Logiciel: MAGIX Photo Manager - (.MAGIX AG.) [HKLM] -- MAGIX Photo Manager

O42 - Logiciel: MAGIX Video deLuxe 2006 - (.MAGIX AG.) [HKLM] -- MAGIX Video deLuxe 2006

O42 - Logiciel: MSVCRT - (.Microsoft.) [HKLM] -- {8DD46C6A-0056-4FEC-B70A-28BB16A1F11F}

O42 - Logiciel: MSXML 4.0 SP2 (KB954430) - (.Microsoft Corporation.) [HKLM] -- {86493ADD-824D-4B8E-BD72-8C5DCDC52A71}

O42 - Logiciel: MSXML 4.0 SP2 (KB973688) - (.Microsoft Corporation.) [HKLM] -- {F662A8E6-F4DC-41A2-901E-8C11F044BDEC}

O42 - Logiciel: Malwarebytes Anti-Malware version 1.75.0.1300 - (.Malwarebytes Corporation.) [HKLM] -- Malwarebytes' Anti-Malware\_is1

O42 - Logiciel: Microsoft Silverlight - (.Microsoft Corporation.) [HKLM] -- {89F4137D-6C26-4A84-BDB8-2E5A4BB71E00}

O42 - Logiciel: NB Probe - (...) [HKLM] -- {6324A1EF-CEF4-43E3-8BCD-9EF3F67317FD}

O42 - Logiciel: NVIDIA Drivers - (...) [HKLM] -- NVIDIA Drivers

O42 - Logiciel: Nutri Pro 7 édition familiale - (.JM.) [HKLM] -- {7D7B1BA1-8914-43E5-B4EB-F53BC111AA9D}

O42 - Logiciel: Oxygène18/ Oxygène16 version 2.0.0.a - (...) [HKLM] -- Oxygène18/ Oxygène16\_is1

O42 - Logiciel: PhotoFiltre Studio X - (...) [HKCU] -- PhotoFiltre Studio X

O42 - Logiciel: Picasa 2 - (.Google, Inc..) [HKLM] -- Picasa2

O42 - Logiciel: QuickTime - (.Apple Inc..) [HKLM] -- {B67BAFBA-4C9F-48FA-9496-933E3B255044}

O42 - Logiciel: RICOH R5C83x/84x Flash Media Controller Driver Ver.3.55.01 - (...) [HKLM] -- {59F6A514-9813-47A3-948C-8A155460CC2A}

O42 - Logiciel: RealDownloader - (.RealNetworks, Inc..) [HKLM] -- {C8E8D2E3-EF6A-4B1D-A09E-7B27EBE2F3CE}

O42 - Logiciel: RealPlayer - (.RealNetworks.) [HKLM] -- RealPlayer 16.0

O42 - Logiciel: RealUpgrade 1.1 - (.RealNetworks, Inc..) [HKLM] -- {28C2DED6-325B-4CC7-983A-1777C8F7FBAB}

O42 - Logiciel: Realtek 8169 8168 8101E 8102E Ethernet Driver - (.Realtek.) [HKLM] -- {8833FFB6-5B0C-4764-81AA-06DFEED9A476}

O42 - Logiciel: Realtek High Definition Audio Driver - (.Realtek Semiconductor Corp..) [HKLM] -- {F132AF7F-7BCA-4EDE-8A7C-958108FE7DBC}

O42 - Logiciel: Segoe UI - (.Microsoft Corp.) [HKLM] -- {5DD4FCBD-A3C1-4155-9E17-4161C70AAABA}

O42 - Logiciel: Sony Ericsson PC Companion 1.60.13 - (.Sony Ericsson.) [HKLM] -- {F09EF8F2-0976-42C1-8D9D-8DF78337C6E3}

O42 - Logiciel: Sweet Home 3D version 3.6 - (.eTeks.) [HKLM] -- Sweet Home 3D\_is1

O42 - Logiciel: Synaptics Pointing Device Driver - (.Synaptics.) [HKLM] -- SynTPDeinstKey

O42 - Logiciel: THE SETTLERS - Bâtisseurs d'Empire - (.Ubisoft.) [HKLM] -- {D3F80A98-05AB-4D8C-9272-766CCFA6A48D}

O42 - Logiciel: TomTom HOME 2.8.3.2499 - (.TomTom.) [HKLM] -- TomTom HOME

O42 - Logiciel: TomTom HOME Visual Studio Merge Modules - (.TomTom International B.V..) [HKLM] -- {8F3C31C5-9C3A-4AA8-8EFA-71290A7AD533}

O42 - Logiciel: USB2.0 1.3M UVC WebCam - (...) [HKLM] -- USB2.0 1.3M UVC WebCam

O42 - Logiciel: Unity Web Player - (.Unity Technologies ApS.) [HKCU] -- UnityWebPlayer

O42 - Logiciel: VLC media player 1.1.9 - (.VideoLAN.) [HKLM] -- VLC media player =>.VideoLAN

O42 - Logiciel: Visual C++ 2008 x86 Runtime - (v9.0.30729) - (.Microsoft Corporation.) [HKLM] -- {F333A33D-125C-32A2-8DCE-5C5D14231E27}

O42 - Logiciel: Visual C++ 2008 x86 Runtime - v9.0.30729.01 - (.Microsoft Corporation.) [HKLM] -- {F333A33D-125C-32A2-8DCE-5C5D14231E27}.vc\_x86runtime\_30729\_01

O42 - Logiciel: Vostok version 1.3.0a - (...) [HKLM] -- Vostok\_is1

O42 - Logiciel: WIDCOMM Bluetooth Software - (.Broadcom Corporation.) [HKLM] -- {03D1988F-469F-4843-8E6E-E5FE9D17889D}

O42 - Logiciel: WinFlash - (...) [HKLM] -- {DE10AB76-4756-4913-BE25-55D1C1051F9A}

O42 - Logiciel: Wireless Console 2 - (.ATK.) [HKLM] -- {83F73CB1-7705-49D1-9852-84D839CA2A45}

O42 - Logiciel: WorkSpace - (.eInstruction.) [HKLM] -- {4EEA8A8A-6532-4A3E-8B00-DCC090FE902E}

O42 - Logiciel: WorkSpace Content - (.Nom de votre société.) [HKLM] -- {CDE317AB-13D1-47A1-929A-018603072780}

O42 - Logiciel: WorkSpaceLanguagePack-French - (.eInstruction.) [HKLM] -- WorkSpaceLanguagePack-French

O42 - Logiciel: monAlbumPhoto 6.3.0.8 - (.monAlbumPhoto.) [HKLM] -- monAlbumPhoto\_is1

O42 - Logiciel: puissance - (...) [HKLM] -- ST4UNST #1

O42 - Logiciel: svt2 - (.Les Editions Hatier.) [HKLM] -- svt2.3CF329FC7EF006D94C1AC4C34744208D3C373211.1

O42 - Logiciel: svt2 - (.Les Editions Hatier.) [HKLM] -- {ABC48E26-08F5-5E48-C173-F0CB8D029C19}

O42 - Logiciel: Étude pour l'amélioration du produit HP Photosmart 5520 series - (.Hewlett-Packard Co..) [HKLM] -- {E1786986-C7FB-45E3-A1D1-3A0B899B9E27} =>.Hewlett-Packard Co

~ Logic: 64 Scanned in 00mn 00s

---\\ HKCU & HKLM Software Keys

[HKCU\Software\3rd Eye Solutions]

[HKCU\Software\7-Zip]

[HKCU\Software\APN]

[HKCU\Software\ASUS]

[HKCU\Software\AVS4YOU]

[HKCU\Software\Adobe]

[HKCU\Software\AppDataLow\Software\Adobe]

[HKCU\Software\AppDataLow\Software\AppDataLow]

[HKCU\Software\AppDataLow\Software\CallingID]

[HKCU\Software\AppDataLow\Software\Google]

[HKCU\Software\AppDataLow\Software\Macromedia]

[HKCU\Software\AppDataLow\Software\RealNetworks]

[HKCU\Software\AppDataLow\Software\Unity]

[HKCU\Software\AppDataLow]

[HKCU\Software\Apple Computer, Inc.]

[HKCU\Software\Apple Inc.]

[HKCU\Software\Avira]

[HKCU\Software\BrowsersafeguardInstalled] =>PUP.BrowserSafeguard

[HKCU\Software\CDDB]

[HKCU\Software\CallingID]

[HKCU\Software\Classes]

[HKCU\Software\Clients]

[HKCU\Software\CyberLink]

[HKCU\Software\DivXNetworks]

[HKCU\Software\Dragon Systems]

[HKCU\Software\FLEXnet]

[HKCU\Software\GSpot Appliance Corp]

[HKCU\Software\GTCO CalComp]

[HKCU\Software\Google]

[HKCU\Software\HP]

[HKCU\Software\Hermitech Laboratory]

[HKCU\Software\Hewlett-Packard]

[HKCU\Software\IM Providers]

[HKCU\Software\ITConcepts]

[HKCU\Software\InstallShield]

[HKCU\Software\JavaSoft]

[HKCU\Software\KasperskyLab]

[HKCU\Software\Lavasoft]

[HKCU\Software\LightScribe]

[HKCU\Software\Ligos]

[HKCU\Software\Local AppWizard-Generated Applications]

[HKCU\Software\Logiciels Jeulin]

[HKCU\Software\MAGIX AG]

[HKCU\Software\MAP-DN]

[HKCU\Software\Macromedia]

[HKCU\Software\Magix]

[HKCU\Software\Malwarebytes' Anti-Malware]

[HKCU\Software\MatchWare]

[HKCU\Software\MozillaPlugins]

[HKCU\Software\Mozilla]

[HKCU\Software\NVIDIA Corporation]

[HKCU\Software\Netscape]

[HKCU\Software\Northcode Inc]

[HKCU\Software\ODBC]

[HKCU\Software\Policies]

[HKCU\Software\RealNetworks]

[HKCU\Software\Realtek]

[HKCU\Software\ScanSoft]

[HKCU\Software\SecuROM]

[HKCU\Software\Software]

[HKCU\Software\Sony Ericsson]

[HKCU\Software\Symantec]

[HKCU\Software\Synaptics]

[HKCU\Software\Sysinternals]

[HKCU\Software\TomTom]

[HKCU\Software\Trolltech]

[HKCU\Software\Ubisoft]

[HKCU\Software\Unity]

[HKCU\Software\Visan]

[HKCU\Software\Widcomm]

[HKCU\Software\Wow6432Node]

[HKCU\Software\ZebHelpProcess Helper]

[HKCU\Software\monAlbumPhoto]

[HKLM\Software\APN]

[HKLM\Software\ASPG]

[HKLM\Software\ASUS]

[HKLM\Software\ATK0100]

[HKLM\Software\ATK]

[HKLM\Software\AVS4YOU]

[HKLM\Software\Adobe]

[HKLM\Software\AdwCleaner]

[HKLM\Software\AppDataLow]

[HKLM\Software\Apple Computer, Inc.]

[HKLM\Software\Apple Inc.]

[HKLM\Software\AsLdr]

[HKLM\Software\Atheros]

[HKLM\Software\AuthenTec]

[HKLM\Software\Avira]

[HKLM\Software\BrowserChoice]

[HKLM\Software\CDDB]

[HKLM\Software\CallingID]

[HKLM\Software\Classes]

[HKLM\Software\Clients]

[HKLM\Software\Corel]

[HKLM\Software\CyberLink]

[HKLM\Software\DivXNetworks]

[HKLM\Software\Dolby]

[HKLM\Software\Dragon Systems]

[HKLM\Software\EnigmaSoftwareGroup]

[HKLM\Software\GTCO CalComp]

[HKLM\Software\Google]

[HKLM\Software\HP]

[HKLM\Software\Hewlett-Packard]

[HKLM\Software\ITConcepts]

[HKLM\Software\ITE]

[HKLM\Software\InstallShield]

[HKLM\Software\InstalledOptions]

[HKLM\Software\Intel]

[HKLM\Software\JavaSoft]

[HKLM\Software\JreMetrics]

[HKLM\Software\KasperskyLab]

[HKLM\Software\Lavasoft]

[HKLM\Software\Licenses]

[HKLM\Software\LightScribe]

[HKLM\Software\Logiciels Jeulin]

[HKLM\Software\MAP-DN]

[HKLM\Software\Macromedia]

[HKLM\Software\Magix]

[HKLM\Software\Malwarebytes' Anti-Malware]

[HKLM\Software\MimarSinan]

[HKLM\Software\Motorola]

[HKLM\Software\MozillaPlugins]

[HKLM\Software\Mozilla]

[HKLM\Software\NVIDIA Corporation]

[HKLM\Software\Norton]

[HKLM\Software\Nuance]

[HKLM\Software\ODBC]

[HKLM\Software\Policies]

[HKLM\Software\RTLSetup]

[HKLM\Software\RealNetworks]

[HKLM\Software\Realtek Semiconductor Corp.]

[HKLM\Software\Realtek]

[HKLM\Software\RegisteredApplications]

[HKLM\Software\RocketLife]

[HKLM\Software\SRS Labs]

[HKLM\Software\ScanSoft]

[HKLM\Software\Siemens]

[HKLM\Software\Software]

[HKLM\Software\Sonic]

[HKLM\Software\Sony Ericsson]

[HKLM\Software\SuppHelpDir]

[HKLM\Software\SymDebug]

[HKLM\Software\Symantec]

[HKLM\Software\Synaptics]

[HKLM\Software\TomTom]

[HKLM\Software\USB2800]

[HKLM\Software\Ubisoft]

[HKLM\Software\VB2S360]

[HKLM\Software\VideoLAN]

[HKLM\Software\Visan]

[HKLM\Software\Voice]

[HKLM\Software\Volatile]

[HKLM\Software\WOW6432Node]

[HKLM\Software\Waves Audio]

[HKLM\Software\WebSupergoo]

[HKLM\Software\WholeSecurity]

[HKLM\Software\Widcomm]

[HKLM\Software\Windows]

[HKLM\Software\X-AVCSD]

[HKLM\Software\Xing Technology Corp.]

[HKLM\Software\eInstruction]

[HKLM\Software\mozilla.org]

~ Key Software: 338 Scanned in 00mn 00s

---\\ Contenu des dossiers Programs/ProgramFiles/ProgramData/AppData (O43)

O43 - CFD: 14/09/2011 - 20:57:11 - [3,348] ----D C:\Program Files\7-Zip

O43 - CFD: 04/12/2008 - 02:14:44 - [11,601] ----D C:\Program Files\Activation Assistant for the 2007 Microsoft Office suites

O43 - CFD: 26/12/2008 - 14:25:21 - [211,240] ----D C:\Program Files\Adobe

O43 - CFD: 02/11/2011 - 18:36:28 - [2,316] ----D C:\Program Files\Apple Software Update =>.Apple Inc

O43 - CFD: 09/03/2011 - 09:31:49 - [201,499] ----D C:\Program Files\ASUS

O43 - CFD: 04/12/2008 - 04:07:24 - [18,243] ----D C:\Program Files\ASUS Security Center

O43 - CFD: 04/12/2008 - 03:58:53 - [9,837] ----D C:\Program Files\Atheros

O43 - CFD: 04/12/2008 - 03:51:16 - [0,443] ----D C:\Program Files\ATKGFNEX

O43 - CFD: 20/11/2012 - 13:41:15 - [286,702] ----D C:\Program Files\Avira

O43 - CFD: 23/01/2013 - 15:23:31 - [181,807] ----D C:\Program Files\AVS4YOU

O43 - CFD: 04/12/2008 - 04:27:47 - [0] ----D C:\Program Files\ChkMail

O43 - CFD: 04/12/2008 - 03:58:41 - [3,739] ----D C:\Program Files\Cisco

O43 - CFD: 09/01/2014 - 22:19:26 - [12,056] ----D C:\Program Files\Classification

O43 - CFD: 02/03/2014 - 22:59:57 - [849,755] ----D C:\Program Files\Common Files

O43 - CFD: 04/12/2008 - 02:22:09 - [215,297] ----D C:\Program Files\CyberLink

O43 - CFD: 02/03/2014 - 20:12:55 - [1,170] ----D C:\Program Files\DivX

O43 - CFD: 04/12/2008 - 03:57:50 - [35,322] ----D C:\Program Files\Dolby

O43 - CFD: 01/06/2011 - 21:27:21 - [2,753] ----D C:\Program Files\EA Games

O43 - CFD: 04/02/2014 - 19:17:03 - [1123,161] ----D C:\Program Files\eInstruction

O43 - CFD: 27/03/2011 - 18:41:26 - [9,018] ----D C:\Program Files\Enigma Software Group

O43 - CFD: 24/12/2013 - 12:10:43 - [0,180] ----D C:\Program Files\EVF

O43 - CFD: 15/01/2011 - 17:16:34 - [0,701] ----D C:\Program Files\Evolution

O43 - CFD: 04/12/2008 - 04:06:24 - [0,621] ----D C:\Program Files\Fingerprint Sensor

O43 - CFD: 18/08/2011 - 20:36:17 - [10,118] ----D C:\Program Files\FreeMind

O43 - CFD: 02/03/2014 - 20:14:20 - [248,206] ----D C:\Program Files\Google

O43 - CFD: 04/02/2014 - 18:54:23 - [44,242] ----D C:\Program Files\Hermitech Laboratory

O43 - CFD: 17/11/2013 - 18:16:36 - [0,996] ----D C:\Program Files\Hewlett-Packard

O43 - CFD: 28/11/2013 - 14:00:57 - [91,407] ----D C:\Program Files\HP

O43 - CFD: 02/11/2011 - 16:51:38 - [0,352] ----D C:\Program Files\HP Photo Creations

O43 - CFD: 02/03/2014 - 20:11:30 - [90,318] --H-D C:\Program Files\InstallShield Installation Information

O43 - CFD: 04/12/2008 - 03:42:14 - [0,049] ----D C:\Program Files\Intel

O43 - CFD: 13/02/2014 - 13:38:10 - [5,236] ----D C:\Program Files\Internet Explorer

O43 - CFD: 07/03/2013 - 11:10:28 - [122,862] ----D C:\Program Files\Java

O43 - CFD: 23/12/2013 - 14:29:18 - [5,445] ----D C:\Program Files\JavaSoft

O43 - CFD: 28/02/2014 - 23:36:09 - [13,449] ----D C:\Program Files\Malwarebytes' Anti-Malware

O43 - CFD: 24/04/2012 - 21:35:18 - [64,839] ----D C:\Program Files\Microsoft

O43 - CFD: 30/03/2010 - 19:25:20 - [91,840] ----D C:\Program Files\Microsoft Games

O43 - CFD: 07/07/2011 - 10:29:30 - [1123,483] ----D C:\Program Files\Microsoft Office

O43 - CFD: 12/10/2013 - 15:26:42 - [40,851] ----D C:\Program Files\Microsoft Silverlight

O43 - CFD: 14/11/2012 - 21:41:22 - [390,258] ----D C:\Program Files\Microsoft SQL Server

O43 - CFD: 04/12/2008 - 02:12:43 - [0,014] ----D C:\Program Files\Microsoft Visual Studio

O43 - CFD: 12/03/2010 - 17:31:35 - [3,554] ----D C:\Program Files\Microsoft Works

O43 - CFD: 15/01/2011 - 12:40:00 - [8,790] ----D C:\Program Files\Microsoft.NET

O43 - CFD: 09/10/2011 - 17:18:39 - [87,493] ----D C:\Program Files\monAlbumPhoto

O43 - CFD: 04/11/2010 - 17:31:31 - [94,740] ----D C:\Program Files\Movie Maker

O43 - CFD: 01/03/2014 - 17:39:58 - [5,137] ----D C:\Program Files\Mozilla Firefox

O43 - CFD: 02/11/2006 - 13:37:34 - [0,025] ----D C:\Program Files\MSBuild

O43 - CFD: 03/03/2009 - 07:47:48 - [0] ----D C:\Program Files\MSXML 4.0

O43 - CFD: 03/01/2014 - 20:57:44 - [1608,821] ----D C:\Program Files\Nuance

O43 - CFD: 15/01/2011 - 12:44:42 - [0,500] ----D C:\Program Files\Nutri Pro 7 édition familiale

O43 - CFD: 04/01/2010 - 14:59:57 - [427,943] ----D C:\Program Files\office 2007-2

O43 - CFD: 04/12/2008 - 04:29:24 - [7,199] ----D C:\Program Files\P4G

O43 - CFD: 04/12/2008 - 03:11:36 - [34,621] ----D C:\Program Files\Picasa2

O43 - CFD: 29/01/2011 - 22:14:14 - [0,018] ----D C:\Program Files\puissance

O43 - CFD: 11/12/2011 - 18:15:57 - [2,266] ----D C:\Program Files\Pulmo

O43 - CFD: 02/08/2013 - 14:01:03 - [73,545] ----D C:\Program Files\QuickTime

O43 - CFD: 07/10/2013 - 18:02:16 - [111,738] ----D C:\Program Files\Real

O43 - CFD: 07/10/2013 - 18:02:41 - [18,245] ----D C:\Program Files\RealNetworks

O43 - CFD: 04/12/2008 - 03:56:01 - [116,826] ----D C:\Program Files\Realtek

O43 - CFD: 02/11/2006 - 13:37:34 - [40,729] ----D C:\Program Files\Reference Assemblies

O43 - CFD: 01/06/2012 - 18:00:48 - [0] ----D C:\Program Files\Sapphire\_N Updater

O43 - CFD: 08/08/2011 - 18:30:18 - [5,413] ----D C:\Program Files\Sony Ericsson

O43 - CFD: 30/01/2011 - 15:53:12 - [146,401] ----D C:\Program Files\svt2

O43 - CFD: 12/10/2012 - 19:52:30 - [99,758] ----D C:\Program Files\Sweet Home 3D

O43 - CFD: 04/12/2008 - 04:31:54 - [14,600] ----D C:\Program Files\Synaptics

O43 - CFD: 15/07/2011 - 19:45:06 - [48,338] ----D C:\Program Files\TomTom HOME 2

O43 - CFD: 15/07/2011 - 19:45:18 - [0,021] ----D C:\Program Files\TomTom International B.V

O43 - CFD: 30/03/2011 - 15:51:47 - [0,378] ----D C:\Program Files\Trend Micro

O43 - CFD: 14/05/2010 - 10:44:16 - [-1314,674] ----D C:\Program Files\Ubisoft

O43 - CFD: 02/11/2006 - 14:01:55 - [0] --H-D C:\Program Files\Uninstall Information

O43 - CFD: 24/05/2011 - 17:10:37 - [78,472] ----D C:\Program Files\VideoLAN

O43 - CFD: 12/05/2011 - 21:27:40 - [0,951] ----D C:\Program Files\Vostok

O43 - CFD: 04/12/2008 - 04:09:12 - [4,479] ----D C:\Program Files\WIDCOMM

O43 - CFD: 17/10/2009 - 10:22:09 - [0,970] ----D C:\Program Files\Windows Calendar

O43 - CFD: 17/10/2009 - 10:22:06 - [2,610] ----D C:\Program Files\Windows Collaboration

O43 - CFD: 17/10/2009 - 10:21:58 - [4,283] ----D C:\Program Files\Windows Defender

O43 - CFD: 12/07/2013 - 10:22:59 - [6,757] ----D C:\Program Files\Windows Journal

O43 - CFD: 10/08/2011 - 16:07:35 - [105,532] ----D C:\Program Files\Windows Live

O43 - CFD: 24/04/2012 - 18:10:25 - [8,694] ----D C:\Program Files\Windows Mail =>.Microsoft Corporation

O43 - CFD: 06/11/2010 - 07:21:52 - [4,394] ----D C:\Program Files\Windows Media Player =>.Microsoft Corporation

O43 - CFD: 02/11/2006 - 13:37:34 - [7,589] ----D C:\Program Files\Windows NT

O43 - CFD: 17/10/2009 - 10:22:03 - [12,902] ----D C:\Program Files\Windows Photo Gallery

O43 - CFD: 07/01/2010 - 11:06:49 - [0,128] ----D C:\Program Files\Windows Portable Devices

O43 - CFD: 17/10/2009 - 10:22:07 - [9,944] ----D C:\Program Files\Windows Sidebar

O43 - CFD: 04/12/2008 - 04:02:32 - [2,115] ----D C:\Program Files\Wireless Console 2

O43 - CFD: 04/02/2014 - 19:11:27 - [0,002] --H-D C:\Program Files\Zero G Registry

O43 - CFD: 26/12/2008 - 14:25:30 - [14,115] ----D C:\Program Files\Common Files\Adobe

O43 - CFD: 28/11/2010 - 21:41:01 - [30,668] ----D C:\Program Files\Common Files\Adobe AIR

O43 - CFD: 08/02/2012 - 13:29:05 - [63,872] ----D C:\Program Files\Common Files\Apple

O43 - CFD: 23/01/2013 - 15:23:25 - [94,410] ----D C:\Program Files\Common Files\AVSMedia

O43 - CFD: 30/12/2012 - 13:19:01 - [0,704] ----D C:\Program Files\Common Files\DESIGNER

O43 - CFD: 01/06/2012 - 15:54:45 - [6,035] ----D C:\Program Files\Common Files\InstallShield

O43 - CFD: 03/01/2014 - 21:03:51 - [1,440] ----D C:\Program Files\Common Files\IVA

O43 - CFD: 04/12/2008 - 02:20:58 - [28,832] ----D C:\Program Files\Common Files\LightScribe

O43 - CFD: 10/01/2009 - 11:38:32 - [0,567] ----D C:\Program Files\Common Files\MAGIX Shared

O43 - CFD: 08/03/2012 - 19:00:09 - [494,027] ----D C:\Program Files\Common Files\microsoft shared

O43 - CFD: 03/01/2014 - 21:03:16 - [11,200] ----D C:\Program Files\Common Files\Nuance

O43 - CFD: 02/11/2006 - 12:18:33 - [0,003] ----D C:\Program Files\Common Files\Services

O43 - CFD: 02/11/2006 - 12:18:33 - [39,198] ----D C:\Program Files\Common Files\SpeechEngines

O43 - CFD: 27/03/2011 - 16:20:07 - [1,027] ----D C:\Program Files\Common Files\Symantec Shared

O43 - CFD: 11/11/2011 - 14:46:13 - [43,146] ----D C:\Program Files\Common Files\System

O43 - CFD: 16/01/2010 - 12:20:22 - [0] ----D C:\Program Files\Common Files\Windows Live

O43 - CFD: 27/03/2011 - 18:40:30 - [20,033] ----D C:\Program Files\Common Files\Wise Installation Wizard

O43 - CFD: 07/10/2013 - 18:02:13 - [0,336] ----D C:\Program Files\Common Files\xing shared

O43 - CFD: 03/12/2012 - 23:26:44 - [0,001] ----D C:\ProgramData\Adobe

O43 - CFD: 03/03/2014 - 13:11:52 - [172,822] ----D C:\ProgramData\albumphoto

O43 - CFD: 02/11/2011 - 18:36:27 - [61,578] ----D C:\ProgramData\Apple

O43 - CFD: 02/08/2013 - 14:00:22 - [26,332] ----D C:\ProgramData\Apple Computer

O43 - CFD: 02/11/2006 - 14:02:03 - [0] -SH-D C:\ProgramData\Application Data

O43 - CFD: 26/12/2008 - 15:21:56 - [0,579] ----D C:\ProgramData\ASUS

O43 - CFD: 04/12/2008 - 03:58:18 - [0,011] ----D C:\ProgramData\Atheros

O43 - CFD: 20/11/2012 - 13:41:15 - [270,719] ----D C:\ProgramData\Avira

O43 - CFD: 23/01/2013 - 15:24:10 - [0] ----D C:\ProgramData\AVS4YOU

O43 - CFD: 23/11/2012 - 17:00:34 - [0,123] ----D C:\ProgramData\CyberLink

O43 - CFD: 02/11/2006 - 14:02:03 - [0] -SH-D C:\ProgramData\Desktop

O43 - CFD: 02/11/2006 - 14:02:03 - [0] -SH-D C:\ProgramData\Documents

O43 - CFD: 02/11/2006 - 14:02:03 - [0] -SH-D C:\ProgramData\Favorites

O43 - CFD: 03/01/2014 - 20:57:45 - [5,031] ----D C:\ProgramData\FLEXnet

O43 - CFD: 21/11/2012 - 21:11:14 - [0,502] ----D C:\ProgramData\Google

O43 - CFD: 17/11/2013 - 18:12:13 - [1,342] ----D C:\ProgramData\HP

O43 - CFD: 02/11/2011 - 16:57:29 - [2,487] ----D C:\ProgramData\HP Photo Creations

O43 - CFD: 01/06/2012 - 15:54:53 - [0] ----D C:\ProgramData\InstallShield

O43 - CFD: 02/03/2014 - 20:02:16 - [0,049] ----D C:\ProgramData\Kaspersky Lab Setup Files

O43 - CFD: 30/03/2011 - 20:36:27 - [0] ----D C:\ProgramData\Lavasoft

O43 - CFD: 03/01/2014 - 20:57:45 - [2,248] ----D C:\ProgramData\Macrovision

O43 - CFD: 27/03/2011 - 19:10:33 - [16,855] ----D C:\ProgramData\Malwarebytes

O43 - CFD: 15/01/2010 - 18:43:44 - [0,001] ----D C:\ProgramData\McAfee

O43 - CFD: 15/01/2010 - 18:42:15 - [0] ----D C:\ProgramData\McAfee Security Scan

O43 - CFD: 14/05/2010 - 10:52:04 - [0,002] ----D C:\ProgramData\Media Center Programs

O43 - CFD: 26/02/2014 - 10:09:57 - [553,449] -S--D C:\ProgramData\Microsoft

O43 - CFD: 16/01/2014 - 11:23:58 - [0,159] ----D C:\ProgramData\Microsoft Help

O43 - CFD: 28/11/2012 - 16:25:14 - [0,036] ----D C:\ProgramData\Mozilla

O43 - CFD: 30/03/2011 - 14:49:56 - [0] ----D C:\ProgramData\nJkKhBoEcIh28604

O43 - CFD: 25/02/2010 - 15:12:47 - [0] ----D C:\ProgramData\Norton

O43 - CFD: 03/01/2014 - 20:57:44 - [-1093,502] ----D C:\ProgramData\Nuance

O43 - CFD: 17/10/2009 - 10:13:14 - [0,181] ----D C:\ProgramData\NVIDIA

O43 - CFD: 04/07/2011 - 04:40:12 - [0,002] ----D C:\ProgramData\P4G

O43 - CFD: 07/10/2013 - 18:04:07 - [2,467] ----D C:\ProgramData\Real

O43 - CFD: 07/10/2013 - 18:02:24 - [3,335] ----D C:\ProgramData\RealNetworks

O43 - CFD: 01/03/2011 - 19:37:44 - [0,024] ----D C:\ProgramData\Sony Ericsson

O43 - CFD: 02/11/2006 - 14:02:03 - [0] -SH-D C:\ProgramData\Start Menu

O43 - CFD: 05/12/2010 - 22:10:28 - [0] ----D C:\ProgramData\Sun

O43 - CFD: 27/03/2011 - 14:50:56 - [0,204] ----D C:\ProgramData\Symantec

O43 - CFD: 03/03/2014 - 10:01:03 - [0,086] ---AD C:\ProgramData\Temp

O43 - CFD: 02/11/2006 - 14:02:04 - [0] -SH-D C:\ProgramData\Templates

O43 - CFD: 15/07/2011 - 19:48:34 - [0] ----D C:\ProgramData\TomTom

O43 - CFD: 01/03/2014 - 11:25:00 - [0] ----D C:\ProgramData\WindowsSearch

O43 - CFD: 04/12/2008 - 02:14:44 - [5,041] ----D C:\ProgramData\{623D32E9-0C62-4453-AD44-98B31F52A5E1}

O43 - CFD: 28/11/2010 - 21:41:05 - [31,423] ----D C:\Users\RONDEAU\AppData\Roaming\Adobe

O43 - CFD: 08/02/2012 - 16:16:03 - [0,021] ----D C:\Users\RONDEAU\AppData\Roaming\Apple Computer

O43 - CFD: 20/11/2012 - 13:48:33 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\Avira

O43 - CFD: 23/01/2013 - 15:23:52 - [12,418] ----D C:\Users\RONDEAU\AppData\Roaming\AVS4YOU

O43 - CFD: 01/06/2012 - 14:56:15 - [0,027] ----D C:\Users\RONDEAU\AppData\Roaming\Azocbo

O43 - CFD: 17/06/2011 - 21:32:09 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\CyberLink

O43 - CFD: 13/06/2011 - 08:55:52 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\Delivery

O43 - CFD: 26/05/2012 - 16:37:28 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\Dipaec

O43 - CFD: 16/01/2010 - 17:59:48 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\DivX

O43 - CFD: 04/02/2014 - 18:51:20 - [0,004] ----D C:\Users\RONDEAU\AppData\Roaming\eInstruction

O43 - CFD: 12/10/2012 - 20:03:58 - [28,617] ----D C:\Users\RONDEAU\AppData\Roaming\eTeks

O43 - CFD: 03/01/2014 - 21:09:55 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\FLEXnet

O43 - CFD: 28/02/2009 - 12:36:32 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\Google

O43 - CFD: 04/02/2014 - 19:20:57 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\GTCO CalComp

O43 - CFD: 04/02/2014 - 18:54:32 - [0,002] ----D C:\Users\RONDEAU\AppData\Roaming\Hermitech Laboratory

O43 - CFD: 28/11/2013 - 12:27:03 - [0,007] ----D C:\Users\RONDEAU\AppData\Roaming\HpUpdate

O43 - CFD: 04/06/2012 - 10:51:24 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\Huup

O43 - CFD: 07/02/2011 - 17:45:37 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\Identities

O43 - CFD: 01/06/2012 - 15:25:56 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\Iwazeg

O43 - CFD: 26/12/2008 - 14:27:57 - [0,040] ----D C:\Users\RONDEAU\AppData\Roaming\Macromedia

O43 - CFD: 08/03/2009 - 16:38:11 - [0,004] ----D C:\Users\RONDEAU\AppData\Roaming\MAGIX

O43 - CFD: 27/03/2011 - 19:10:50 - [0,497] ----D C:\Users\RONDEAU\AppData\Roaming\Malwarebytes

O43 - CFD: 02/11/2006 - 13:37:34 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\Media Center Programs

O43 - CFD: 23/12/2013 - 15:21:41 - [39,209] -S--D C:\Users\RONDEAU\AppData\Roaming\Microsoft

O43 - CFD: 26/05/2012 - 18:38:57 - [0,040] ----D C:\Users\RONDEAU\AppData\Roaming\Milas

O43 - CFD: 28/11/2012 - 16:25:20 - [50,928] ----D C:\Users\RONDEAU\AppData\Roaming\Mozilla

O43 - CFD: 06/01/2014 - 09:08:58 - [1,900] ----D C:\Users\RONDEAU\AppData\Roaming\Nuance

O43 - CFD: 15/01/2011 - 16:20:39 - [0,001] ----D C:\Users\RONDEAU\AppData\Roaming\Nutri Pro 7

O43 - CFD: 01/06/2012 - 15:59:38 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\Ocugba

O43 - CFD: 01/06/2012 - 14:56:15 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\Ohir

O43 - CFD: 30/05/2012 - 21:33:20 - [0,041] ----D C:\Users\RONDEAU\AppData\Roaming\Omsup

O43 - CFD: 18/08/2013 - 18:24:24 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\Orange

O43 - CFD: 02/03/2014 - 23:44:29 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\PeerNetworking

O43 - CFD: 07/02/2011 - 17:45:45 - [0,001] ----D C:\Users\RONDEAU\AppData\Roaming\PhotoFiltre Studio X

O43 - CFD: 21/12/2013 - 17:46:04 - [2,256] ----D C:\Users\RONDEAU\AppData\Roaming\Real

O43 - CFD: 07/10/2013 - 18:03:45 - [0,027] ----D C:\Users\RONDEAU\AppData\Roaming\RealNetworks

O43 - CFD: 25/02/2010 - 13:04:29 - [0] R-H-D C:\Users\RONDEAU\AppData\Roaming\SecuROM

O43 - CFD: 30/01/2011 - 15:55:12 - [0,005] ----D C:\Users\RONDEAU\AppData\Roaming\svt2.3CF329FC7EF006D94C1AC4C34744208D3C373211.1

O43 - CFD: 26/12/2008 - 14:28:12 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\Symantec

O43 - CFD: 15/07/2011 - 19:45:27 - [3,492] ----D C:\Users\RONDEAU\AppData\Roaming\TomTom

O43 - CFD: 30/05/2012 - 21:33:20 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\Ulik

O43 - CFD: 26/05/2012 - 18:38:57 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\Usxai

O43 - CFD: 09/12/2013 - 10:43:58 - [1,379] ----D C:\Users\RONDEAU\AppData\Roaming\vlc

O43 - CFD: 01/06/2012 - 16:21:23 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\Vyva

O43 - CFD: 03/03/2014 - 21:06:21 - [0,365] ----D C:\Users\RONDEAU\AppData\Roaming\ZHP =>.Nicolas Coolman

O43 - CFD: 04/06/2012 - 10:57:16 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\Zyekho

O43 - CFD: 06/04/2011 - 14:57:21 - [38,061] ----D C:\Users\RONDEAU\AppData\Local\Adobe

O43 - CFD: 20/11/2012 - 13:42:19 - [0,159] ----D C:\Users\RONDEAU\AppData\Local\APN

O43 - CFD: 21/06/2009 - 20:00:04 - [0] ----D C:\Users\RONDEAU\AppData\Local\Apple

O43 - CFD: 21/06/2009 - 20:08:21 - [0,003] ----D C:\Users\RONDEAU\AppData\Local\Apple Computer

O43 - CFD: 26/12/2008 - 14:22:12 - [0] -SH-D C:\Users\RONDEAU\AppData\Local\Application Data

O43 - CFD: 26/12/2008 - 15:21:54 - [1,763] ----D C:\Users\RONDEAU\AppData\Local\ASUS

O43 - CFD: 24/11/2010 - 14:33:53 - [0] ----D C:\Users\RONDEAU\AppData\Local\Chat Republic Games

O43 - CFD: 02/03/2014 - 19:07:23 - [0,085] ----D C:\Users\RONDEAU\AppData\Local\DoNotTrackPlus

O43 - CFD: 31/12/2012 - 14:05:22 - [802,558] ----D C:\Users\RONDEAU\AppData\Local\Google

O43 - CFD: 26/12/2008 - 14:22:12 - [0] -SH-D C:\Users\RONDEAU\AppData\Local\Historique

O43 - CFD: 17/11/2013 - 18:17:59 - [0,150] ----D C:\Users\RONDEAU\AppData\Local\HP

O43 - CFD: 03/12/2012 - 23:27:04 - [0] ----D C:\Users\RONDEAU\AppData\Local\Macromedia

O43 - CFD: 03/12/2012 - 23:27:04 - [1154,494] ----D C:\Users\RONDEAU\AppData\Local\Microsoft

O43 - CFD: 16/01/2010 - 11:43:59 - [1,649] ----D C:\Users\RONDEAU\AppData\Local\Microsoft Games

O43 - CFD: 12/09/2012 - 17:18:26 - [0,324] ----D C:\Users\RONDEAU\AppData\Local\Microsoft Help

O43 - CFD: 28/11/2012 - 16:25:20 - [30,167] ----D C:\Users\RONDEAU\AppData\Local\Mozilla

O43 - CFD: 22/06/2009 - 14:49:02 - [0,010] ----D C:\Users\RONDEAU\AppData\Local\PlayMovie

O43 - CFD: 03/01/2009 - 20:42:50 - [24,871] ----D C:\Users\RONDEAU\AppData\Local\PowerCinema

O43 - CFD: 28/02/2014 - 22:48:43 - [0] ----D C:\Users\RONDEAU\AppData\Local\Software

O43 - CFD: 08/08/2011 - 18:30:38 - [0] ----D C:\Users\RONDEAU\AppData\Local\Sony Ericsson

O43 - CFD: 30/03/2011 - 16:48:35 - [0] ----D C:\Users\RONDEAU\AppData\Local\Sunbelt Software

O43 - CFD: 03/03/2014 - 21:05:11 - [636,467] ----D C:\Users\RONDEAU\AppData\Local\Temp

O43 - CFD: 26/12/2008 - 14:22:12 - [0] -SH-D C:\Users\RONDEAU\AppData\Local\Temporary Internet Files

O43 - CFD: 15/07/2011 - 19:45:27 - [1,683] ----D C:\Users\RONDEAU\AppData\Local\TomTom

O43 - CFD: 15/07/2011 - 15:25:36 - [0,200] ----D C:\Users\RONDEAU\AppData\Local\Unity

O43 - CFD: 01/02/2009 - 15:22:16 - [7,075] ----D C:\Users\RONDEAU\AppData\Local\VirtualStore

O43 - CFD: 02/03/2014 - 19:08:41 - [0,168] ----D C:\Users\RONDEAU\AppData\Local\Windows Live

O43 - CFD: 21/01/2008 - 03:42:46 - [0,014] R---D C:\Users\RONDEAU\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories

O43 - CFD: 26/12/2008 - 14:27:41 - [0] R---D C:\Users\RONDEAU\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools

O43 - CFD: 23/01/2013 - 15:23:27 - [0,001] ----D C:\Users\RONDEAU\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\AVS4YOU

O43 - CFD: 04/12/2008 - 02:22:05 - [0,013] ----D C:\Users\RONDEAU\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\CyberLink DVD Suite

O43 - CFD: 15/01/2011 - 17:16:34 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Evolution allélique

O43 - CFD: 02/03/2014 - 23:38:57 - [0,002] ----D C:\Users\RONDEAU\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Google Chrome

O43 - CFD: 26/12/2008 - 14:28:17 - [0,005] ----D C:\Users\RONDEAU\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Google Desktop

O43 - CFD: 03/03/2014 - 00:04:09 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Hachette Multimédia

O43 - CFD: 21/01/2008 - 03:42:46 - [0,001] R---D C:\Users\RONDEAU\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance

O43 - CFD: 07/02/2011 - 17:44:14 - [0] ----D C:\Users\RONDEAU\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\PhotoFiltre Studio X

O43 - CFD: 02/03/2014 - 19:11:16 - [0] R---D C:\Users\RONDEAU\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

~ 290 Dossiers CLSID vides (CLSID Empty Folders)

~ Program Folder: 522 Scanned in 01mn 14s

---\\ Derniers fichiers modifiés ou crées sous Windows et System32 (O44)

O44 - LFC:[MD5.1BC5FDDC172AA00A0A656CE3B214FB6D] - 02/03/2014 - 23:19:05 ---A- . (...) -- C:\PhysicalDisk0\_MBR.bin [512]

O44 - LFC:[MD5.CE7C6A70BC32F0997BBDDE9F824B7538] - 03/03/2014 - 00:09:20 ---A- . (...) -- C:\Windows\System32\PerfStringBackup.INI [276830]

O44 - LFC:[MD5.01E8342A7847029B3C8F77C80DE095A2] - 03/03/2014 - 00:09:20 ---A- . (...) -- C:\Windows\System32\perfc009.dat [4401832]

O44 - LFC:[MD5.D59D09677F6365F5AD0D22A07AC73553] - 03/03/2014 - 00:09:20 ---A- . (...) -- C:\Windows\System32\perfc00C.dat [70234]

O44 - LFC:[MD5.2BDB5488A4DEF5CB9B57069CB6CB8373] - 03/03/2014 - 00:09:20 ---A- . (...) -- C:\Windows\System32\perfh009.dat [5562672]

O44 - LFC:[MD5.2A2CC594AB53619E12F29FBD6AFCCD0E] - 03/03/2014 - 00:09:20 ---A- . (...) -- C:\Windows\System32\perfh00C.dat [198604]

O44 - LFC:[MD5.58404A4FDEA0C530FDD9663051357B11] - 03/03/2014 - 09:36:16 ---A- . (...) -- C:\Windows\PFRO.log [500582]

O44 - LFC:[MD5.6BCAF46E2B7FA9ACE92B4D39F3037C5C] - 03/03/2014 - 09:36:43 ---A- . (...) -- C:\Windows\System32\acovcnt.exe [45056]

O44 - LFC:[MD5.258231CEFCDB44AB52F56F8FE2C6C34C] - 03/03/2014 - 21:00:24 -S-A- . (...) -- C:\Windows\bootstat.dat [67584]

O44 - LFC:[MD5.E5043A38F3A9C30F123D0F1B8A0A7CAC] - 03/03/2014 - 21:04:35 ---A- . (...) -- C:\Windows\WindowsUpdate.log [1117980]

O44 - LFC:[MD5.72F76B12C09B36F26219920D0B2E7EF3] - 21/02/2014 - 18:46:33 ---A- . (.Adobe Systems Incorporated - Adobe Flash Player Control Panel Applet.) -- C:\Windows\System32\FlashPlayerApp.exe [692616]

O44 - LFC:[MD5.FD38EBD137378FE594E7EFEBB5B3E096] - 21/02/2014 - 18:46:33 ---A- . (.Adobe Systems Incorporated - Adobe Flash Player Control Panel Applet.) -- C:\Windows\System32\FlashPlayerCPLApp.cpl [71048]

~ Files: 12 Scanned in 01mn 10s

---\\ Derniers fichiers créés dans Windows Prefetcher (O45)

O45 - LFCP:[MD5.5FA1AA1E5BCF6808F921C92E6CA71FD9] - 01/03/2014 - 03:32:32 ---A- - C:\Windows\Prefetch\RUNDLL32.EXE-230FC512.pf

O45 - LFCP:[MD5.FDD010DF415F7B42EEB6C949DDB8EF0F] - 01/03/2014 - 08:53:06 ---A- - C:\Windows\Prefetch\Layout.ini

O45 - LFCP:[MD5.C09A4B45A35191AA7DDD1364AB970C7A] - 01/03/2014 - 12:03:30 ---A- - C:\Windows\Prefetch\MBAMGUI.EXE-4FE652ED.pf

O45 - LFCP:[MD5.0231AC51CD588B03BC3F652A95D6330E] - 01/03/2014 - 12:04:05 ---A- - C:\Windows\Prefetch\CLMLSVC.EXE-256FA05D.pf

O45 - LFCP:[MD5.527A0512E5B512F63E1234821484948C] - 01/03/2014 - 12:04:17 ---A- - C:\Windows\Prefetch\PMVSERVICE.EXE-A6E94A0D.pf

O45 - LFCP:[MD5.AAC409774295337756B33F6D2007C550] - 01/03/2014 - 12:38:36 ---A- - C:\Windows\Prefetch\REGEDIT.EXE-90FEEA06.pf

O45 - LFCP:[MD5.50E5263EF5012A69F4F100369E78907A] - 01/03/2014 - 13:02:04 ---A- - C:\Windows\Prefetch\KBFILTR.EXE-5630B608.pf

O45 - LFCP:[MD5.D4F3E229323EC73C9AB28365F98C8982] - 01/03/2014 - 13:02:04 ---A- - C:\Windows\Prefetch\WDC.EXE-CD48EA20.pf

O45 - LFCP:[MD5.AEAF0D5F36BD22ABC634F72B552BBAB7] - 01/03/2014 - 17:11:33 ---A- - C:\Windows\Prefetch\RUNDLL32.EXE-9AC4CDDB.pf

O45 - LFCP:[MD5.28546B6A9EE313D5B4D31519D2B2D31E] - 01/03/2014 - 17:13:52 ---A- - C:\Windows\Prefetch\CERTUTIL.EXE-F3874186.pf

O45 - LFCP:[MD5.C968561BA8755B8D95481BAAF2FF6FDC] - 01/03/2014 - 17:13:53 ---A- - C:\Windows\Prefetch\RUNDLL32.EXE-53F681E6.pf

O45 - LFCP:[MD5.44CA5A8646CED8A429638675E14F72AD] - 01/03/2014 - 17:14:30 ---A- - C:\Windows\Prefetch\FIREFOX.EXE-A606B53C.pf

O45 - LFCP:[MD5.FAA882D0894F9926211C5EF6276621E5] - 01/03/2014 - 17:15:58 ---A- - C:\Windows\Prefetch\LPKSETUP.EXE-90F505D8.pf

O45 - LFCP:[MD5.511C5AD83E8E477A96467390EDEBC600] - 01/03/2014 - 17:21:41 ---A- - C:\Windows\Prefetch\FLASHPLAYERPLUGIN\_12\_0\_0\_70.E-A8E9B96E.pf

O45 - LFCP:[MD5.05DC478C175441EC0616A843EEBB9E6D] - 01/03/2014 - 17:21:41 ---A- - C:\Windows\Prefetch\PLUGIN-CONTAINER.EXE-7226D1F8.pf

O45 - LFCP:[MD5.FC91FC6A93F4ECFEF28A532059A1B593] - 01/03/2014 - 17:25:52 ---A- - C:\Windows\Prefetch\WUDFHOST.EXE-AFFEF87C.pf

O45 - LFCP:[MD5.5EFB1A27A700F32AE5C4B0647F2D231F] - 01/03/2014 - 17:27:18 ---A- - C:\Windows\Prefetch\1820319.EXE-EDC9BB96.pf

O45 - LFCP:[MD5.8506FC919DFD0038A6D1A9E0279CDD8C] - 01/03/2014 - 17:39:52 ---A- - C:\Windows\Prefetch\HELPER.EXE-8AEDE3E3.pf

O45 - LFCP:[MD5.4826C70D2365AF4840CF4F0CFC0A694A] - 01/03/2014 - 17:39:52 ---A- - C:\Windows\Prefetch\UNINSTALLER.EXE-FB9CC9A0.pf

O45 - LFCP:[MD5.58BFBD2C3DFA7EA2DFD47BD06A327404] - 01/03/2014 - 17:39:59 ---A- - C:\Windows\Prefetch\NS5E97.TMP-5576301A.pf

O45 - LFCP:[MD5.1A548C33A1AC434A46690D1E0E026815] - 01/03/2014 - 17:39:59 ---A- - C:\Windows\Prefetch\UNINSTALL.EXE-2D621464.pf

O45 - LFCP:[MD5.D69649A85C92FB6D5E69A7298CF94010] - 01/03/2014 - 17:40:01 ---A- - C:\Windows\Prefetch\BU\_.EXE-6A3245F0.pf

O45 - LFCP:[MD5.5D3635D4822E0BBA8006027F0B8FC968] - 01/03/2014 - 17:40:01 ---A- - C:\Windows\Prefetch\MAINTENANCESERVICE.EXE-28D2775E.pf

O45 - LFCP:[MD5.0A1B22F8A57B524B51B24B5F1E3A7FE0] - 01/03/2014 - 17:40:01 ---A- - C:\Windows\Prefetch\NS66DF.TMP-70DB70AC.pf

O45 - LFCP:[MD5.010DDCF48EC3C0E0F52BE0B72A74D52F] - 01/03/2014 - 17:49:29 ---A- - C:\Windows\Prefetch\RUNDLL32.EXE-E8AC3089.pf

O45 - LFCP:[MD5.A1F296793B03C98BD31555D978744B22] - 01/03/2014 - 17:49:53 ---A- - C:\Windows\Prefetch\RUNDLL32.EXE-A98BDBDF.pf

O45 - LFCP:[MD5.8AFADF37AC91EE42A4C616FDBAF81640] - 01/03/2014 - 17:55:53 ---A- - C:\Windows\Prefetch\RUNDLL32.EXE-D083B3CE.pf

O45 - LFCP:[MD5.9BCAAF9DF4786C3B42EB4FCEAC70F14B] - 01/03/2014 - 18:02:16 ---A- - C:\Windows\Prefetch\SETUP\_11.0.1.1245.X01\_2013\_12-E5648D2F.pf

O45 - LFCP:[MD5.F5A0EF7639D0502D7CCE07C11A76A08C] - 01/03/2014 - 18:02:18 ---A- - C:\Windows\Prefetch\1820319.EXE-B26CC43B.pf

O45 - LFCP:[MD5.0DAE34B27629B2F5879D117B719B300A] - 01/03/2014 - 18:02:19 ---A- - C:\Windows\Prefetch\NET.EXE-DF44F913.pf

O45 - LFCP:[MD5.B03986BC0A7B26C11CA8D4DE18AEDF5F] - 01/03/2014 - 18:02:19 ---A- - C:\Windows\Prefetch\NET1.EXE-849DA590.pf

O45 - LFCP:[MD5.CD18131FB221914D1BECBDA34A3E551B] - 01/03/2014 - 18:02:34 ---A- - C:\Windows\Prefetch\1820319RAR.EXE-CE8FBEE4.pf

O45 - LFCP:[MD5.FA9B1CA8E65AF6B2A8140B1263459970] - 01/03/2014 - 18:02:53 ---A- - C:\Windows\Prefetch\1820319.EXE-C8E0F58F.pf

O45 - LFCP:[MD5.CA5C65ECBBB0AF04B0083E46619878EF] - 01/03/2014 - 18:04:23 ---A- - C:\Windows\Prefetch\RUNDLL32.EXE-829BCF11.pf

O45 - LFCP:[MD5.86B53FFA8FB93881FBDE2DD8342A3E86] - 02/03/2014 - 18:45:34 ---A- - C:\Windows\Prefetch\ASGHOST.EXE-AB5DBB79.pf

O45 - LFCP:[MD5.76B2388F8CCE1C7C923FDED8C6982024] - 02/03/2014 - 18:46:19 ---A- - C:\Windows\Prefetch\AgCx\_SC2.db

O45 - LFCP:[MD5.CED23D5C3ACA22673EC8E064211BC2BE] - 02/03/2014 - 19:07:07 ---A- - C:\Windows\Prefetch\RUNDLL32.EXE-917D4EF2.pf

O45 - LFCP:[MD5.7863DED31778B1C8B2A39EA0064D8773] - 02/03/2014 - 19:08:07 ---A- - C:\Windows\Prefetch\BBSVC.EXE-8D35CC14.pf

O45 - LFCP:[MD5.0F3B7A3940A83947B2512A6B2D56BAFB] - 02/03/2014 - 19:08:34 ---A- - C:\Windows\Prefetch\RUNDLL32.EXE-09EDA3F1.pf

O45 - LFCP:[MD5.E7F64B4A33468B89341C8E9AFF2C1F23] - 02/03/2014 - 19:11:12 ---A- - C:\Windows\Prefetch\GRPCONV.EXE-B823222B.pf

O45 - LFCP:[MD5.C4798D3C8C922A939EEA1A71DDE64090] - 02/03/2014 - 19:11:12 ---A- - C:\Windows\Prefetch\RUNONCE.EXE-D0649312.pf

O45 - LFCP:[MD5.3253DEBE71D2BDFB0FBA394390B8C558] - 02/03/2014 - 19:12:25 ---A- - C:\Windows\Prefetch\DNTPSERVICE.EXE-BE9A7B90.pf

O45 - LFCP:[MD5.404304EE4CE2BE9A4F29ED0B12832B8B] - 02/03/2014 - 19:12:27 ---A- - C:\Windows\Prefetch\BINGSURROGATE.EXE-19032050.pf

O45 - LFCP:[MD5.525CD143C1A086F27277C3DD60D8B087] - 02/03/2014 - 19:13:22 ---A- - C:\Windows\Prefetch\BINGAPP.EXE-00A26B79.pf

O45 - LFCP:[MD5.7C7F90B620C4DE79F4A25C0FEA910F19] - 02/03/2014 - 19:13:22 ---A- - C:\Windows\Prefetch\BINGBAR.EXE-B698CD25.pf

O45 - LFCP:[MD5.E95C4D18E96AE297D0F41ABAFC822F9E] - 02/03/2014 - 19:19:20 ---A- - C:\Windows\Prefetch\DLLHOST.EXE-EEE13F6D.pf

O45 - LFCP:[MD5.82B930635A2F5DC6EC0D58FACA9245AA] - 02/03/2014 - 19:39:20 ---A- - C:\Windows\Prefetch\TEST\_WPF.EXE-1EB487B9.pf

O45 - LFCP:[MD5.1F9AC5D01C6C52A6A749F3A66E112FD5] - 02/03/2014 - 19:41:00 ---A- - C:\Windows\Prefetch\UPDATETASK.EXE-7C757890.pf

O45 - LFCP:[MD5.484FD627C48B6AE711818D924C74481C] - 02/03/2014 - 19:52:34 ---A- - C:\Windows\Prefetch\REALPLAY.EXE-A09C7945.pf

O45 - LFCP:[MD5.10788EFBC407F11E4360A3A61EC4AE5B] - 02/03/2014 - 20:02:09 ---A- - C:\Windows\Prefetch\KIS14.0.0.4651ABCFR\_5546\_TRIA-0A55D39F.pf

O45 - LFCP:[MD5.8382507A147BD7B5A1D88ABA9EA8CD42] - 02/03/2014 - 20:05:49 ---A- - C:\Windows\Prefetch\REALSCHED.EXE-DDDCD145.pf

O45 - LFCP:[MD5.44BB40CAF8246413313D846D93E95868] - 02/03/2014 - 20:12:58 ---A- - C:\Windows\Prefetch\AU\_.EXE-E932B6BB.pf

O45 - LFCP:[MD5.CA61334C8140FEFD805B1725AF8DE252] - 02/03/2014 - 20:13:29 ---A- - C:\Windows\Prefetch\CHROME.EXE-5A1054AF.pf

O45 - LFCP:[MD5.4FA76232C520AFF23F1A663223EA10DB] - 02/03/2014 - 20:13:55 ---A- - C:\Windows\Prefetch\GOOGLEUPDATE.EXE-FE771DDA.pf

O45 - LFCP:[MD5.15B0D63B16F166865A01281494CA4572] - 02/03/2014 - 20:29:48 ---A- - C:\Windows\Prefetch\DLLHOST.EXE-7FAA2E4C.pf

O45 - LFCP:[MD5.F87BE5682F870D7699678F86C30EDCA7] - 02/03/2014 - 22:14:51 ---A- - C:\Windows\Prefetch\SAUPDATE.EXE-AEB00BE5.pf

O45 - LFCP:[MD5.BB7020309E3BE27204FBCA4B89498794] - 02/03/2014 - 22:53:52 ---A- - C:\Windows\Prefetch\CIDGLOBALLIGHT.EXE-29BA72E8.pf

O45 - LFCP:[MD5.87DC9CF1DD75F7FDBEFBFF5BB21BA45E] - 02/03/2014 - 22:54:37 ---A- - C:\Windows\Prefetch\FLASHUTIL32\_12\_0\_0\_70\_ACTIVEX-0F9E2908.pf

O45 - LFCP:[MD5.CF6E68D0F4BE2BEB5625F1AD413BDAA7] - 02/03/2014 - 22:56:59 ---A- - C:\Windows\Prefetch\MAKECERT.EXE-5E166383.pf

O45 - LFCP:[MD5.59CADFF1B2951A46B51703DABE683F8D] - 02/03/2014 - 23:05:55 ---A- - C:\Windows\Prefetch\AVPUI.EXE-AD6FD2E2.pf

O45 - LFCP:[MD5.49CE422842C9C940C72A9EB5043E3BC7] - 02/03/2014 - 23:12:44 ---A- - C:\Windows\Prefetch\WPFFONTCACHE\_V0400.EXE-3A5005E3.pf

O45 - LFCP:[MD5.EDDD0E4BAE1291265D449083BEE91BE7] - 02/03/2014 - 23:40:56 ---A- - C:\Windows\Prefetch\RUNDLL32.EXE-5541CA5D.pf

O45 - LFCP:[MD5.BE49F4E9B60A272B7990FD7057FC5FAE] - 02/03/2014 - 23:45:27 ---A- - C:\Windows\Prefetch\GOOGLEDESKTOP.EXE-C9B032BF.pf

O45 - LFCP:[MD5.6E6D286F46D35D0D1B80FD536E5463E6] - 02/03/2014 - 23:45:38 ---A- - C:\Windows\Prefetch\COMPANIONUSER.EXE-B600D0B4.pf

O45 - LFCP:[MD5.29D825F3374C3EEA9DBE0CF76D270AB2] - 02/03/2014 - 23:45:38 ---A- - C:\Windows\Prefetch\RECORDINGMANAGER.EXE-A711D8FE.pf

O45 - LFCP:[MD5.998F4CE3E595871D869B01DA4426EA9F] - 02/03/2014 - 23:45:41 ---A- - C:\Windows\Prefetch\IEXPLORE.EXE-908C99F8.pf

O45 - LFCP:[MD5.C8F65ABB118CF5625D13B61062EB1BD7] - 02/03/2014 - 23:46:13 ---A- - C:\Windows\Prefetch\RUNDLL32.EXE-EF0DD113.pf

O45 - LFCP:[MD5.C6D7F1F96113FD4B1BC48926CE7B4FE6] - 02/03/2014 - 23:47:12 ---A- - C:\Windows\Prefetch\VSSVC.EXE-B8AFC319.pf

O45 - LFCP:[MD5.0BE7A8D735DD3F530489246856480926] - 02/03/2014 - 23:47:30 ---A- - C:\Windows\Prefetch\SVCHOST.EXE-7CFEDEA3.pf

O45 - LFCP:[MD5.49AEC2AFD65550BBA0733C1C1EA58FAA] - 02/03/2014 - 23:49:55 ---A- - C:\Windows\Prefetch\AVP.EXE-13DFE9F4.pf

O45 - LFCP:[MD5.78CF7E9C772FF321727C1302EB235DF3] - 02/03/2014 - 23:49:55 ---A- - C:\Windows\Prefetch\WMI32.EXE-E7CCFA3B.pf

O45 - LFCP:[MD5.EE5A8A2B6FF95E9C3FE891D9ED0CC414] - 02/03/2014 - 23:49:59 ---A- - C:\Windows\Prefetch\KLWTBLFS.EXE-9050CA16.pf

O45 - LFCP:[MD5.2894468FB584362DD2C30AFBC4C36BE7] - 02/03/2014 - 23:49:59 ---A- - C:\Windows\Prefetch\KLWTBWS.EXE-88E89DAF.pf

O45 - LFCP:[MD5.0D274FE3A5402EDB01BC144B169E3016] - 02/03/2014 - 23:50:46 ---A- - C:\Windows\Prefetch\DRVINST.EXE-4CB4314A.pf

O45 - LFCP:[MD5.2BB4F6028FEA8155AC6EF79EED33157B] - 03/03/2014 - 00:04:26 ---A- - C:\Windows\Prefetch\DLLHOST.EXE-6A473D35.pf

O45 - LFCP:[MD5.2060250318E12B485A8F0582609FFA9D] - 03/03/2014 - 00:09:37 ---A- - C:\Windows\Prefetch\MSIEXEC.EXE-A2D55CB6.pf

O45 - LFCP:[MD5.DF351E33DCA358776EB5EBE23B55A9AC] - 03/03/2014 - 00:23:06 ---A- - C:\Windows\Prefetch\DLLHOST.EXE-C2B8534F.pf

O45 - LFCP:[MD5.BBDBAA1A26E9138866773412FA153B8A] - 03/03/2014 - 00:24:35 ---A- - C:\Windows\Prefetch\RUNDLL32.EXE-F4579822.pf

O45 - LFCP:[MD5.C0F0BF7C32C4DEB786753522F15BCB39] - 03/03/2014 - 00:26:03 ---A- - C:\Windows\Prefetch\RUNDLL32.EXE-1304AE86.pf

O45 - LFCP:[MD5.51DFFFAD20786F62038CC48A41073AF7] - 03/03/2014 - 09:37:10 ---A- - C:\Windows\Prefetch\PRESENTATIONSETTINGS.EXE-2F4708C9.pf

O45 - LFCP:[MD5.6435CE6F3837AEF94731BCF67B203054] - 03/03/2014 - 09:37:23 ---A- - C:\Windows\Prefetch\EHMSAS.EXE-2D3B2F21.pf

O45 - LFCP:[MD5.50180AA4EA58E56A2554AFB7CE41D6DB] - 03/03/2014 - 09:42:31 ---A- - C:\Windows\Prefetch\AVSCAN.EXE-E289CD20.pf

O45 - LFCP:[MD5.758C8A45B9A48EFBDA173128E1B4F9AC] - 03/03/2014 - 09:46:38 ---A- - C:\Windows\Prefetch\WSQMCONS.EXE-118B52B7.pf

O45 - LFCP:[MD5.57436F1763D99C043AD20085DA95B21E] - 03/03/2014 - 09:50:13 ---A- - C:\Windows\Prefetch\REGSVR32.EXE-8461DBEE.pf

O45 - LFCP:[MD5.3341DF07A0C5103A51441C510C2AE95C] - 03/03/2014 - 09:50:23 ---A- - C:\Windows\Prefetch\MBAM.EXE-305FF92C.pf

O45 - LFCP:[MD5.E0FA5B1977B7180794588FD56AA145BB] - 03/03/2014 - 11:59:14 ---A- - C:\Windows\Prefetch\NOTEPAD.EXE-86E0E9B9.pf

O45 - LFCP:[MD5.80F92F94ABC60D0AF0DB0330B0764401] - 03/03/2014 - 12:20:32 ---A- - C:\Windows\Prefetch\WMPLAYER.EXE-BAD6BD53.pf

O45 - LFCP:[MD5.CD951186D24ECC88BC25B572A3E9A07C] - 03/03/2014 - 12:20:39 ---A- - C:\Windows\Prefetch\MOBSYNC.EXE-C5E2284F.pf

O45 - LFCP:[MD5.4148B10CB09010AEA54EB2B4DA7C70F9] - 03/03/2014 - 12:46:15 ---A- - C:\Windows\Prefetch\RUNDLL32.EXE-095C481F.pf

O45 - LFCP:[MD5.3B3EF149EC10001CA10208BD5F706064] - 03/03/2014 - 12:49:50 ---A- - C:\Windows\Prefetch\FLASHPLAYERUPDATESERVICE.EXE-ECAD9571.pf

O45 - LFCP:[MD5.DAF2DAB483243E82876BE0D74E50C5A4] - 03/03/2014 - 13:03:01 ---A- - C:\Windows\Prefetch\CONTROL.EXE-817F8F1D.pf

O45 - LFCP:[MD5.756F58E435DF5E272FDB17BDED698923] - 03/03/2014 - 13:16:09 ---A- - C:\Windows\Prefetch\HPCUSTPARTIC.EXE-731280AD.pf

O45 - LFCP:[MD5.D360B8074DA1B6FCE86E5431C0252492] - 03/03/2014 - 13:16:47 ---A- - C:\Windows\Prefetch\LOGONUI.EXE-09140401.pf

O45 - LFCP:[MD5.126DE6E02C0A64E89CD8483C6096722A] - 03/03/2014 - 14:58:39 ---A- - C:\Windows\Prefetch\LIVEUPDT.EXE-A23FB7E2.pf

O45 - LFCP:[MD5.5C53C986709B734449313B2FEB0CE3DE] - 03/03/2014 - 14:59:32 ---A- - C:\Windows\Prefetch\SEAPORT.EXE-A7BA8D92.pf

O45 - LFCP:[MD5.5D87D56F83DFF366D9CBFE5828934F59] - 03/03/2014 - 15:00:50 ---A- - C:\Windows\Prefetch\LOGON.SCR-30601369.pf

O45 - LFCP:[MD5.0DF58E4B7BF18377ABC998C1F147B3F3] - 03/03/2014 - 15:01:30 ---A- - C:\Windows\Prefetch\WERMGR.EXE-0F2AC88C.pf

O45 - LFCP:[MD5.87262157168959555CE5BB4904842131] - 03/03/2014 - 15:03:30 ---A- - C:\Windows\Prefetch\TASKENG.EXE-48D4E289.pf

O45 - LFCP:[MD5.D2F9462CDDC1181742F83ACBEABADCEE] - 03/03/2014 - 15:03:35 ---A- - C:\Windows\Prefetch\DLLHOST.EXE-CF2B07FC.pf

O45 - LFCP:[MD5.F57289218F73284CA584056A6958D6D9] - 03/03/2014 - 15:08:37 ---A- - C:\Windows\Prefetch\AgGlUAD\_P\_S-1-5-21-1479064021-3229367824-3524447455-1000.db

O45 - LFCP:[MD5.4BC3E3F740F031E11BC4769BCB204E33] - 03/03/2014 - 15:08:37 ---A- - C:\Windows\Prefetch\AgGlUAD\_S-1-5-21-1479064021-3229367824-3524447455-1000.db

O45 - LFCP:[MD5.3F9F71C007F9F6D22F7736DC504DEF46] - 03/03/2014 - 15:11:33 ---A- - C:\Windows\Prefetch\VERCLSID.EXE-7C52E31C.pf

O45 - LFCP:[MD5.7DB2B628FE253CF34EDE4F4157093F2C] - 03/03/2014 - 15:13:51 ---A- - C:\Windows\Prefetch\WERFAULT.EXE-E69F695A.pf

O45 - LFCP:[MD5.603703B051B9B4D91D61606F9C95192E] - 03/03/2014 - 15:13:55 ---A- - C:\Windows\Prefetch\PfSvPerfStats.bin

O45 - LFCP:[MD5.1E2FFCF09EFDEE3ADEA44550C64772D9] - 03/03/2014 - 15:13:56 ---A- - C:\Windows\Prefetch\AgRobust.db

O45 - LFCP:[MD5.35EBFE5E3C1B4A92ABED260B4E800B35] - 03/03/2014 - 15:13:59 ---A- - C:\Windows\Prefetch\AgGlGlobalHistory.db

O45 - LFCP:[MD5.07ED36309181B55586E039CDBF315C69] - 03/03/2014 - 15:14:00 ---A- - C:\Windows\Prefetch\AgGlFaultHistory.db

O45 - LFCP:[MD5.FFEC8E7E13971573783ABE8C827D8DB0] - 03/03/2014 - 15:14:01 ---A- - C:\Windows\Prefetch\AgGlFgAppHistory.db

O45 - LFCP:[MD5.B9D23BC409CC624005D44D61D68D042A] - 03/03/2014 - 21:01:16 ---A- - C:\Windows\Prefetch\AGENT.EXE-D5774666.pf

O45 - LFCP:[MD5.145D06E7627D6C8C9778CC43B8D33CBF] - 03/03/2014 - 21:01:16 ---A- - C:\Windows\Prefetch\AVSHADOW.EXE-CC252F8D.pf

O45 - LFCP:[MD5.BFAD057D441BC1BA6CA0AEF28DA67052] - 03/03/2014 - 21:01:16 ---A- - C:\Windows\Prefetch\ISUSPM.EXE-37A4AA80.pf

O45 - LFCP:[MD5.9801CF8473D217DA32B4FE38DC73330B] - 03/03/2014 - 21:01:16 ---A- - C:\Windows\Prefetch\NTOSBOOT-B00DFAAD.pf

O45 - LFCP:[MD5.21878BBE86F587997B4279853C5926BC] - 03/03/2014 - 21:01:19 ---A- - C:\Windows\Prefetch\WMPNSCFG.EXE-FC0D39BF.pf

O45 - LFCP:[MD5.1C1B53E35860F66429E42E84B1A0242C] - 03/03/2014 - 21:01:24 ---A- - C:\Windows\Prefetch\AVWEBGRD.EXE-28A29336.pf

O45 - LFCP:[MD5.46E65A462DE61F4E7F42F33CE48DD72D] - 03/03/2014 - 21:01:26 ---A- - C:\Windows\Prefetch\TRUSTEDINSTALLER.EXE-3CC531E5.pf

O45 - LFCP:[MD5.2CA95138AB5CAAB24D82F2F130F48CCC] - 03/03/2014 - 21:01:36 ---A- - C:\Windows\Prefetch\UNSECAPP.EXE-A02905A6.pf

O45 - LFCP:[MD5.4125FD99FA6E2BB7809AB135A3B38A42] - 03/03/2014 - 21:01:47 ---A- - C:\Windows\Prefetch\LAUNCH.EXE-CF4228A3.pf

O45 - LFCP:[MD5.8868AF4A581E17EA5001FB28F9CE924A] - 03/03/2014 - 21:02:12 ---A- - C:\Windows\Prefetch\AVCENTER.EXE-C4AEDCEC.pf

O45 - LFCP:[MD5.D5C01DCDB572EE077AF06ABB66A63E1F] - 03/03/2014 - 21:02:19 ---A- - C:\Windows\Prefetch\SEARCHPROTOCOLHOST.EXE-0CB8CADE.pf

O45 - LFCP:[MD5.1B0665BF941376860B5DB930747FC9F1] - 03/03/2014 - 21:02:26 ---A- - C:\Windows\Prefetch\IPMGUI.EXE-EEAE1F1B.pf

O45 - LFCP:[MD5.761262F4EE90B720348921112C90B9CA] - 03/03/2014 - 21:02:36 ---A- - C:\Windows\Prefetch\SYNTPHELPER.EXE-0A20AAC4.pf

O45 - LFCP:[MD5.8570356D1C696D38793B14E8916C3BD4] - 03/03/2014 - 21:03:10 ---A- - C:\Windows\Prefetch\MSFEEDSSYNC.EXE-6E6FBDF4.pf

O45 - LFCP:[MD5.C741E40AE044065FE629EB05EC9D9DEB] - 03/03/2014 - 21:03:20 ---A- - C:\Windows\Prefetch\MSCORSVW.EXE-C3C515BD.pf

O45 - LFCP:[MD5.DB404DC279FE8F40DEAF369E83CBB156] - 03/03/2014 - 21:03:31 ---A- - C:\Windows\Prefetch\SVCHOST.EXE-007FEA55.pf

O45 - LFCP:[MD5.DDFF8FC3CE9DA8BCC8DEE11433CD0BD0] - 03/03/2014 - 21:03:34 ---A- - C:\Windows\Prefetch\WMPNETWK.EXE-D9F2A96F.pf

O45 - LFCP:[MD5.1A4AF6ECEE966F955B845CF955712C78] - 03/03/2014 - 21:03:55 ---A- - C:\Windows\Prefetch\IELOWUTIL.EXE-3885C25E.pf

O45 - LFCP:[MD5.87B4D5BE36AF05C10A785C35D83D7204] - 03/03/2014 - 21:04:02 ---A- - C:\Windows\Prefetch\CONSENT.EXE-531BD9EA.pf

O45 - LFCP:[MD5.96529B390D10CBD280C3D7E15BFEB36C] - 03/03/2014 - 21:04:33 ---A- - C:\Windows\Prefetch\DLLHOST.EXE-766398D2.pf

O45 - LFCP:[MD5.097DEC71903B65A0FB0E4492F944FD98] - 03/03/2014 - 21:04:33 ---A- - C:\Windows\Prefetch\WMIADAP.EXE-F8DFDFA2.pf

O45 - LFCP:[MD5.24F0E231D3B2A44C954DF68BBA462A58] - 03/03/2014 - 21:04:36 ---A- - C:\Windows\Prefetch\WMIPRVSE.EXE-1628051C.pf

O45 - LFCP:[MD5.C1BDC9A20AA6EEB63A549BC15393FE2B] - 03/03/2014 - 21:05:14 ---A- - C:\Windows\Prefetch\DLLHOST.EXE-5E46FA0D.pf

O45 - LFCP:[MD5.61EE945A7D9D52DBD544838F4CA96494] - 03/03/2014 - 21:05:42 ---A- - C:\Windows\Prefetch\CONIME.EXE-9781FD5F.pf

O45 - LFCP:[MD5.ADD2DBF453965CAB1D4ABD97FFD32CCB] - 03/03/2014 - 21:06:18 ---A- - C:\Windows\Prefetch\AVWSC.EXE-4630B658.pf

O45 - LFCP:[MD5.9F73F5F8788A9E8DE3F93351AFB86705] - 03/03/2014 - 21:06:21 ---A- - C:\Windows\Prefetch\SEARCHFILTERHOST.EXE-77482212.pf

O45 - LFCP:[MD5.5DD4F501ABDACD59B23801C4DE73CBC2] - 03/03/2014 - 21:06:22 ---A- - C:\Windows\Prefetch\UPDATE.EXE-026DCA13.pf

O45 - LFCP:[MD5.4D0E0407490A5828859F6C390B1F4CA6] - 03/03/2014 - 21:06:27 ---A- - C:\Windows\Prefetch\UPDRGUI.EXE-650B9264.pf

O45 - LFCP:[MD5.9B93C48A369A5B328BB2BE8F6A18FEB9] - 03/03/2014 - 21:07:09 ---A- - C:\Windows\Prefetch\HPNETWORKCOMMUNICATOR.EXE-ADCA4C6A.pf

O45 - LFCP:[MD5.D41D8CD98F00B204E9800998ECF8427E] - 30/08/2110 - 07:30:32 ----D - C:\Windows\Prefetch\ReadyBoot

~ Prefetcher: 138 Scanned in 00mn 02s

---\\ Déni du service (Local Security Authority) (O48)

O48 - LSA:Local Security Authority Authentication Packages . (.Microsoft Corporation - Microsoft Authentication Package v1.0.) -- C:\Windows\System32\msv1\_0.dll

O48 - LSA:Local Security Authority Notification Packages . (.Microsoft Corporation - Moteur du client de l'Éditeur de configuration de sécurité Windows.) -- C:\Windows\System32\scecli.dll

O48 - LSA:Local Security Authority Notification Packages . (...) -- C:\Windows\System32\ASWLNPkg.dll

O48 - LSA:Local Security Authority Security Packages . (.Microsoft Corporation - Package de sécurité Kerberos.) -- C:\Windows\System32\kerberos.dll

O48 - LSA:Local Security Authority Security Packages . (.Microsoft Corporation - Microsoft Authentication Package v1.0.) -- C:\Windows\System32\msv1\_0.dll

O48 - LSA:Local Security Authority Security Packages . (.Microsoft Corporation - TLS / SSL Security Provider.) -- C:\Windows\System32\schannel.dll

O48 - LSA:Local Security Authority Security Packages . (.Microsoft Corporation - Microsoft Digest Access.) -- C:\Windows\System32\wdigest.dll

O48 - LSA:Local Security Authority Security Packages . (.Microsoft Corporation - Web Service Security Package.) -- C:\Windows\System32\tspkg.dll

~ LSA: 8 Scanned in 00mn 00s

---\\ Contrôle du Safe Boot (CSB) (O49)

O49 - CSB:Control Safe Boot HKLM\...\CCS\Minimal\sermouse.sys . (.Microsoft Corporation - Pilote de filtre souris série.) -- C:\Windows\System32\Drivers\sermouse.sys

O49 - CSB:Control Safe Boot HKLM\...\CCS\Minimal\vga.sys . (.Microsoft Corporation - VGA/Super VGA Video Driver.) -- C:\Windows\System32\Drivers\vga.sys

O49 - CSB:Control Safe Boot HKLM\...\CCS\Minimal\vgasave.sys . (...) -- C:\Windows\System32\Drivers\vgasave.sys (.not file.)

O49 - CSB:Control Safe Boot HKLM\...\CCS\Minimal\volmgr.sys . (.Microsoft Corporation - Volume Manager Driver.) -- C:\Windows\System32\Drivers\volmgr.sys

O49 - CSB:Control Safe Boot HKLM\...\CCS\Minimal\volmgrx.sys . (.Microsoft Corporation - Volume Manager Extension Driver.) -- C:\Windows\System32\Drivers\volmgrx.sys

O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\ipnat.sys . (.Microsoft Corporation - IP Network Address Translator.) -- C:\Windows\System32\Drivers\ipnat.sys

O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\nsiproxy.sys . (.Microsoft Corporation - NSI Proxy.) -- C:\Windows\System32\Drivers\nsiproxy.sys

O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\rdpencdd.sys . (.Microsoft Corporation - RDP Miniport.) -- C:\Windows\System32\Drivers\rdpencdd.sys

O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\sermouse.sys . (.Microsoft Corporation - Pilote de filtre souris série.) -- C:\Windows\System32\Drivers\sermouse.sys

O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\vga.sys . (.Microsoft Corporation - VGA/Super VGA Video Driver.) -- C:\Windows\System32\Drivers\vga.sys

O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\vgasave.sys . (...) -- C:\Windows\System32\Drivers\vgasave.sys (.not file.)

O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\volmgr.sys . (.Microsoft Corporation - Volume Manager Driver.) -- C:\Windows\System32\Drivers\volmgr.sys

O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\volmgrx.sys . (.Microsoft Corporation - Volume Manager Extension Driver.) -- C:\Windows\System32\Drivers\volmgrx.sys

~ CSB: 13 Scanned in 00mn 00s

---\\ Clé de registre Shell MountPoints2 (MPKS) (O51)

O51 - MPSK:{510c7ca2-882b-11df-b6dd-002354a12c83}\AutoRun\command. (...) -- H:\U3ROM\flyhigh.exe (.not file.)

O51 - MPSK:{813edea7-442e-11e0-994f-002354a12c83}\AutoRun\command. (...) -- H:\Startme.exe (.not file.)

O51 - MPSK:{b7e8140b-0031-11e3-8b4b-002354a12c83}\AutoRun\command. (...) -- H:\Setup.exe (.not file.)

O51 - MPSK:{bbe7ca54-567b-11df-8f3f-002354a12c83}\AutoRun\command - Clé orpheline

O51 - MPSK:{bbe7ca63-567b-11df-8f3f-002354a12c83}\AutoRun\command - Clé orpheline

O51 - MPSK:{bbe7ca6b-567b-11df-8f3f-002354a12c83}\AutoRun\command. (.Microsoft Corporation - Microsoft (R) Windows Based Script Host.) -- C:\Windows\system32\wscript.exe

~ Keys: Scanned in 00mn 00s

---\\ Recherche d'infection sur les pilotes (HKLM)(TDSD) (O52)

O52 - TDSD: \Drivers32\"msacm.l3acm"="C:\Windows\System32\l3codeca.acm" . (.Fraunhofer Institut Integrierte Schaltungen - MPEG Layer-3 Audio Codec for MSACM.) -- C:\Windows\System32\l3codeca.acm

O52 - TDSD: \Drivers32\"vidc.cvid"="iccvid.dll" . (.Radius Inc. - Codec Cinepak®.) -- C:\Windows\System32\iccvid.dll

O52 - TDSD: \Drivers32\"msacm.l3codecp"="l3codecp.acm" . (.Fraunhofer Institut Integrierte Schaltungen - MPEG Audio Layer-3 Codec for MSACM.) -- C:\Windows\System32\l3codecp.acm

O52 - TDSD: \Drivers32\"VIDC.IV41"="IR41\_32.AX" . (.Intel Corporation - Intel Indeo® Video 4.5.) -- C:\Windows\System32\IR41\_32.AX

O52 - TDSD: \Drivers32\"msacm.pspgru"="pspgru.acm" . (.Philips Austria GmbH - Speech Processing - PSPGRU.) -- C:\Windows\System32\pspgru.acm

O52 - TDSD: \Drivers32\"vidc.tscc"="tsccvid.dll" . (.TechSmith Corporation - TechSmith Screen Capture Codec.) -- C:\Windows\System32\tsccvid.dll

O52 - TDSD: \drivers.desc\"C:\Windows\System32\l3codeca.acm"="Fraunhofer IIS MPEG Layer-3 Codec" . (.Fraunhofer Institut Integrierte Schaltungen - MPEG Layer-3 Audio Codec for MSACM.) -- C:\Windows\System32\l3codeca.acm

O52 - TDSD: \drivers.desc\"pspgru.acm"="Philips StandardPlay Audio CODEC" . (.Philips Austria GmbH - Speech Processing - PSPGRU.) -- C:\Windows\System32\pspgru.acm

O52 - TDSD: \drivers.desc\"tsccvid.dll"="TechSmith Screen Capture Codec" . (.TechSmith Corporation - TechSmith Screen Capture Codec.) -- C:\Windows\System32\tsccvid.dll

~ TDSD: 9 Scanned in 00mn 00s

---\\ Enumération des clés de registre SecurityProviders (MCSP) (O54)

O54 - MCSP:[HKLM\...\CurrentControlSet\Control] - (SecurityProviders) - (.Microsoft Corporation - TS Single Sign On Security Package.) -- C:\Windows\System32\credssp.dll

O54 - MCSP:[HKLM\...\ControlSet001\Control] - (SecurityProviders) - (.Microsoft Corporation - TS Single Sign On Security Package.) -- C:\Windows\System32\credssp.dll

~ MSCP: 2 Scanned in 00mn 00s

---\\ Enumération des clés de registre PoliciesSystem (MWPS) (O55)

O55 - MWPS:[HKLM\...\Policies\System] - "ConsentPromptBehaviorAdmin"=2

O55 - MWPS:[HKLM\...\Policies\System] - "ConsentPromptBehaviorUser"=1

O55 - MWPS:[HKLM\...\Policies\System] - "EnableInstallerDetection"=1

O55 - MWPS:[HKLM\...\Policies\System] - "EnableLUA"=1

O55 - MWPS:[HKLM\...\Policies\System] - "EnableSecureUIAPaths"=1

O55 - MWPS:[HKLM\...\Policies\System] - "EnableVirtualization"=1

O55 - MWPS:[HKLM\...\Policies\System] - "PromptOnSecureDesktop"=1

O55 - MWPS:[HKLM\...\Policies\System] - "ValidateAdminCodeSignatures"=0

O55 - MWPS:[HKLM\...\Policies\System] - "dontdisplaylastusername"=0

O55 - MWPS:[HKLM\...\Policies\System] - "legalnoticecaption"=0

O55 - MWPS:[HKLM\...\Policies\System] - "legalnoticetext"=0

O55 - MWPS:[HKLM\...\Policies\System] - "scforceoption"=0

O55 - MWPS:[HKLM\...\Policies\System] - "shutdownwithoutlogon"=1

O55 - MWPS:[HKLM\...\Policies\System] - "undockwithoutlogon"=1

O55 - MWPS:[HKLM\...\Policies\System] - "FilterAdministratorToken"=0

O55 - MWPS:[HKLM\...\Policies\System] - "EnableUIADesktopToggle"=0

~ MWPS: 16 Scanned in 00mn 00s

---\\ Enumération des clés de registre PoliciesExplorer (MWPE) (O56)

O56 - MWPE:[HKLM\...\policies\Explorer] - "BindDirectlyToPropertySetStorage"=0

~ MWPE Keys: 1 Scanned in 00mn 00s

---\\ Liste des pilotes du système (SDL) (O58)

O58 - SDL:[MD5.0349BE02F329F4F48F1D48097FD65974] - 21/01/2008 - 03:23:21 ---A- . (.Microsoft Corporation - 1394 Bus Device Driver.) -- C:\Windows\System32\Drivers\1394bus.sys [53376]

O58 - SDL:[MD5.82B296AE1892FE3DBEE00C9CF92F8AC7] - 11/04/2009 - 07:32:46 ---A- . (.Microsoft Corporation - Pilote ACPI pour NT.) -- C:\Windows\System32\Drivers\acpi.sys [265688]

O58 - SDL:[MD5.04F0FCAC69C7C71A3AC4EB97FAFC8303] - 21/01/2008 - 03:23:21 ---A- . (.Adaptec, Inc. - Adaptec Windows SAS/SATA Storport Driver.) -- C:\Windows\System32\Drivers\adp94xx.sys [422968]

O58 - SDL:[MD5.60505E0041F7751BDBB80F88BF45C2CE] - 21/01/2008 - 03:23:25 ---A- . (.Adaptec, Inc. - Adaptec Windows SATA Storport Driver.) -- C:\Windows\System32\Drivers\adpahci.sys [300600]

O58 - SDL:[MD5.8A42779B02AEC986EAB64ECFC98F8BD7] - 21/01/2008 - 03:23:26 ---A- . (.Adaptec, Inc. - Adaptec LH Ultra160 Driver (x86).) -- C:\Windows\System32\Drivers\adpu160m.sys [101432]

O58 - SDL:[MD5.241C9E37F8CE45EF51C3DE27515CA4E5] - 21/01/2008 - 03:23:27 ---A- . (.Adaptec, Inc. - Adaptec StorPort Ultra320 SCSI Driver.) -- C:\Windows\System32\Drivers\adpu320.sys [149560]

O58 - SDL:[MD5.3911B972B55FEA0478476B2E777B29FA] - 21/04/2011 - 14:58:27 ---A- . (.Microsoft Corporation - Ancillary Function Driver for WinSock.) -- C:\Windows\System32\Drivers\afd.sys [273408]

O58 - SDL:[MD5.13F9E33747E6B41A3FF305C37DB0D360] - 21/01/2008 - 03:23:01 ---A- . (.Microsoft Corporation - Filtre AGP 440 NT.) -- C:\Windows\System32\Drivers\AGP440.sys [56376]

O58 - SDL:[MD5.9EAEF5FC9B8E351AFA7E78A6FAE91F91] - 21/01/2008 - 03:23:00 ---A- . (.Acer Laboratories Inc. - ALi mini IDE Driver.) -- C:\Windows\System32\Drivers\aliide.sys [17464]

O58 - SDL:[MD5.C47344BC706E5F0B9DCE369516661578] - 21/01/2008 - 03:23:01 ---A- . (.Microsoft Corporation - Filtre AGP AMD NT.) -- C:\Windows\System32\Drivers\AMDAGP.SYS [57400]

O58 - SDL:[MD5.9B78A39A4C173FDBC1321E0DD659B34C] - 21/01/2008 - 03:23:00 ---A- . (.Microsoft Corporation - Pilote IDE AMD.) -- C:\Windows\System32\Drivers\amdide.sys [17976]

O58 - SDL:[MD5.18F29B49AD23ECEE3D2A826C725C8D48] - 21/01/2008 - 03:23:00 ---A- . (.Microsoft Corporation - Processor Device Driver.) -- C:\Windows\System32\Drivers\amdk7.sys [41472]

O58 - SDL:[MD5.93AE7F7DD54AB986A6F1A1B37BE7442D] - 21/01/2008 - 03:23:00 ---A- . (.Microsoft Corporation - Processor Device Driver.) -- C:\Windows\System32\Drivers\amdk8.sys [44032]

O58 - SDL:[MD5.5D2888182FB46632511ACEE92FDAD522] - 21/01/2008 - 03:23:23 ---A- . (.Adaptec, Inc. - Adaptec RAID Storport Driver.) -- C:\Windows\System32\Drivers\arc.sys [79416]

O58 - SDL:[MD5.5E2A321BD7C8B3624E41FDEC3E244945] - 21/01/2008 - 03:23:24 ---A- . (.Adaptec, Inc. - Adaptec SAS RAID WS03 Driver.) -- C:\Windows\System32\Drivers\arcsas.sys [79928]

O58 - SDL:[MD5.53B202ABEE6455406254444303E87BE1] - 21/01/2008 - 03:24:04 ---A- . (.Microsoft Corporation - MS Remote Access serial network driver.) -- C:\Windows\System32\Drivers\asyncmac.sys [17408]

O58 - SDL:[MD5.1F05B78AB91C9075565A9D8A4B880BC4] - 11/04/2009 - 07:32:26 ---A- . (.Microsoft Corporation - ATAPI IDE Miniport Driver.) -- C:\Windows\System32\Drivers\atapi.sys [19944]

O58 - SDL:[MD5.64B0052340B8EC28FA8A56B708AE71CC] - 11/04/2009 - 07:32:42 ---A- . (.Microsoft Corporation - ATAPI Driver Extension.) -- C:\Windows\System32\Drivers\ataport.sys [109032]

O58 - SDL:[MD5.2846F5EE802889D500FCF5CC48B28381] - 05/09/2009 - 13:25:36 ---A- . (.Atheros Communications, Inc. - Atheros Extensible Wireless LAN device driver.) -- C:\Windows\System32\Drivers\athr.sys [1183744]

O58 - SDL:[MD5.97AFFA9D95FFE20EEE6229BC6BE166CF] - 14/12/2006 - 08:11:57 ---A- . (.ATK0100 - ATK0100 ACPI Utility.) -- C:\Windows\System32\Drivers\ATKACPI.sys [7680]

O58 - SDL:[MD5.72BC628AF75C4C3250F2A3BAC260265A] - 15/01/2010 - 19:15:00 ---A- . (...) -- C:\Windows\System32\Drivers\atksgt.sys [278728]

O58 - SDL:[MD5.F70D2392158CB68E775F8C4CD3D12FBB] - 17/06/2007 - 06:29:08 ---A- . (.AuthenTec, Inc. - Slide Fingerprint USB Driver.) -- C:\Windows\System32\Drivers\atswpdrv.sys [146824]

O58 - SDL:[MD5.B8C10FF9369394EB84993F331810CF29] - 19/12/2013 - 19:37:46 ---A- . (.Avira Operations GmbH & Co. KG - Avira Minifilter Driver.) -- C:\Windows\System32\Drivers\avgntflt.sys [90400]

O58 - SDL:[MD5.4189E5AB2CAD6F395D87DAAE73EB090F] - 19/12/2013 - 19:37:46 ---A- . (.Avira Operations GmbH & Co. KG - Avira Driver for Security Enhancement.) -- C:\Windows\System32\Drivers\avipbb.sys [135648]

O58 - SDL:[MD5.D8C712305F73CD34D1B344810E522728] - 27/11/2013 - 15:55:51 ---A- . (.Avira Operations GmbH & Co. KG - Avira Manager Driver.) -- C:\Windows\System32\Drivers\avkmgr.sys [37352]

O58 - SDL:[MD5.2B8A5A8879238C3BA9A89A8E3AC4E45D] - 21/01/2008 - 03:23:00 ---A- . (.Microsoft Corporation - Battery Class Driver.) -- C:\Windows\System32\Drivers\battc.sys [28216]

O58 - SDL:[MD5.9F5F8F2318DFA3974A6F6A5602733929] - 21/01/2008 - 03:23:31 ---A- . (.Microsoft Corporation - Microsoft BDA Driver Support Library.) -- C:\Windows\System32\Drivers\bdasup.sys [12288]

O58 - SDL:[MD5.67E506B75BD5326A3EC7B70BD014DFB6] - 21/01/2008 - 03:23:44 ---A- . (.Microsoft Corporation - BEEP Driver.) -- C:\Windows\System32\Drivers\beep.sys [6144]

O58 - SDL:[MD5.D4DF28447741FD3D953526E33A617397] - 21/01/2008 - 03:23:01 ---A- . (.Microsoft Corporation - BLB Drive Driver.) -- C:\Windows\System32\Drivers\blbdrive.sys [45568]

O58 - SDL:[MD5.35F376253F687BDE63976CCB3F2108CA] - 22/02/2011 - 14:23:55 ---A- . (.Microsoft Corporation - NT Lan Manager Datagram Receiver Driver.) -- C:\Windows\System32\Drivers\bowser.sys [69632]

O58 - SDL:[MD5.9F9ACC7F7CCDE8A15C282D3F88B43309] - 02/11/2006 - 09:24:45 ---A- . (.Brother Industries, Ltd. - Windows ME USB Mass-Storage Bulk-Only Lower Filter Driver.) -- C:\Windows\System32\Drivers\BrFiltLo.sys [13568]

O58 - SDL:[MD5.56801AD62213A41F6497F96DEE83755A] - 02/11/2006 - 09:24:46 ---A- . (.Brother Industries, Ltd. - Windows ME USB Mass-Storage Bulk-Only Upper Filter Driver.) -- C:\Windows\System32\Drivers\BrFiltUp.sys [5248]

O58 - SDL:[MD5.B1564976D98E91FC764D5DC28A0297DA] - 11/04/2009 - 06:42:55 ---A- . (.Microsoft Corporation - MAC Bridge Driver.) -- C:\Windows\System32\Drivers\bridge.sys [93696]

O58 - SDL:[MD5.B304E75CFF293029EDDF094246747113] - 02/11/2006 - 09:25:24 ---A- . (.Brother Industries Ltd. - Pilote Brother Série I/F (WDM).) -- C:\Windows\System32\Drivers\BrSerId.sys [71808]

O58 - SDL:[MD5.203F0B1E73ADADBBB7B7B1FABD901F6B] - 02/11/2006 - 09:24:44 ---A- . (.Brother Industries Ltd. - Brother Serial driver (WDM version).) -- C:\Windows\System32\Drivers\BrSerWdm.sys [62336]

O58 - SDL:[MD5.BD456606156BA17E60A04E18016AE54B] - 02/11/2006 - 09:24:44 ---A- . (.Brother Industries Ltd. - Brother USB MDM Driver.) -- C:\Windows\System32\Drivers\BrUsbMdm.sys [12160]

O58 - SDL:[MD5.AF72ED54503F717A43268B3CC5FAEC2E] - 02/11/2006 - 09:24:47 ---A- . (.Brother Industries Ltd. - Brother USB Serial Driver.) -- C:\Windows\System32\Drivers\BrUsbSer.sys [11904]

O58 - SDL:[MD5.6D39C954799B63BA866910234CF7D726] - 11/04/2009 - 05:43:10 ---A- . (.Microsoft Corporation - Bluetooth Bus Extender.) -- C:\Windows\System32\Drivers\bthenum.sys [22528]

O58 - SDL:[MD5.9A966A8E86D1771911AE34A20D11BFF3] - 11/04/2009 - 05:43:10 ---A- . (.Microsoft Corporation - Bluetooth Communications Driver.) -- C:\Windows\System32\Drivers\bthmodem.sys [41472]

O58 - SDL:[MD5.5904EFA25F829BF84EA6FB045134A1D8] - 21/01/2008 - 03:23:20 ---A- . (.Microsoft Corporation - Bluetooth Personal Area Networking.) -- C:\Windows\System32\Drivers\bthpan.sys [92160]

O58 - SDL:[MD5.611FF3F2F095C8D4A6D4CFD9DCC09793] - 21/04/2011 - 14:55:05 ---A- . (.Microsoft Corporation - Bluetooth Bus Driver.) -- C:\Windows\System32\Drivers\bthport.sys [508416]

O58 - SDL:[MD5.D330803EAB2A15CAEC7F011F1D4CB30E] - 17/06/2009 - 14:23:23 ---A- . (.Microsoft Corporation - Bluetooth Miniport Driver.) -- C:\Windows\System32\Drivers\BTHUSB.SYS [30208]

O58 - SDL:[MD5.F2F7342742180D5060285499DEE50F99] - 17/03/2008 - 01:42:21 ---A- . (.Broadcom Corporation. - Bluetooth Audio Device.) -- C:\Windows\System32\Drivers\btwaudio.sys [81960]

O58 - SDL:[MD5.32F59F26A30CFC508DA11DB3EA0F8B77] - 17/03/2008 - 01:42:19 ---A- . (.Broadcom Corporation. - Broadcom Bluetooth AVDT Service.) -- C:\Windows\System32\Drivers\btwavdt.sys [100392]

O58 - SDL:[MD5.ECB98391C756A7B9CFBAE89D9D1235E1] - 29/01/2008 - 03:46:57 ---A- . (.Broadcom Corporation. - Broadcom Bluetooth L2CAP Service.) -- C:\Windows\System32\Drivers\btwl2cap.sys [29736]

O58 - SDL:[MD5.03658734EF7D0F3B3F4636D3E8A38964] - 17/03/2008 - 01:42:15 ---A- . (.Broadcom Corporation. - Bluetooth Remote Control HID Minidriver.) -- C:\Windows\System32\Drivers\btwrchid.sys [17320]

O58 - SDL:[MD5.7ADD03E75BEB9E6DD102C3081D29840A] - 21/01/2008 - 03:23:51 ---A- . (.Microsoft Corporation - CD-ROM File System Driver.) -- C:\Windows\System32\Drivers\cdfs.sys [70144]

O58 - SDL:[MD5.BF79E659C506674C0497CC9C61F1A165] - 05/10/2006 - 03:42:42 ---A- . (.Sonic Solutions - CDR4 CD and DVD Place Holder Driver (see PxHelp).) -- C:\Windows\System32\Drivers\cdr4\_xp.sys [2432]

O58 - SDL:[MD5.2C41CD49D82D5FD85C72D57B6CA25471] - 05/10/2006 - 03:42:42 ---A- . (.Sonic Solutions - CDRAL Place Holder Driver (see PxHelp).) -- C:\Windows\System32\Drivers\cdralw2k.sys [2560]

O58 - SDL:[MD5.6B4BFFB9BECD728097024276430DB314] - 11/04/2009 - 05:39:17 ---A- . (.Microsoft Corporation - SCSI CD-ROM Driver.) -- C:\Windows\System32\Drivers\cdrom.sys [67072]

O58 - SDL:[MD5.E5D4133F37219DBCFE102BC61072589D] - 21/01/2008 - 03:23:26 ---A- . (.Microsoft Corporation - Consumer IR Class Driver for eHome.) -- C:\Windows\System32\Drivers\circlass.sys [35328]

O58 - SDL:[MD5.0767B09C74D935A590B4879D14463B64] - 11/04/2009 - 07:32:43 ---A- . (.Microsoft Corporation - SCSI Class System Dll.) -- C:\Windows\System32\Drivers\Classpnp.sys [125928]

O58 - SDL:[MD5.99AFC3795B58CC478FBBBCDC658FCB56] - 21/01/2008 - 03:23:26 ---A- . (.Microsoft Corporation - Control Method Battery Driver.) -- C:\Windows\System32\Drivers\CmBatt.sys [14208]

O58 - SDL:[MD5.0CA25E686A4928484E9FDABD168AB629] - 21/01/2008 - 03:23:00 ---A- . (.CMD Technology, Inc. - CMD PCI IDE Bus Driver.) -- C:\Windows\System32\Drivers\cmdide.sys [19000]

O58 - SDL:[MD5.6AFEF0B60FA25DE07C0968983EE4F60A] - 21/01/2008 - 03:23:00 ---A- . (.Microsoft Corporation - Composite Battery Driver.) -- C:\Windows\System32\Drivers\compbatt.sys [20792]

O58 - SDL:[MD5.36975327EF03949CC378AB01E316B574] - 11/04/2009 - 07:32:30 ---A- . (.Microsoft Corporation - Crash Dump Driver.) -- C:\Windows\System32\Drivers\crashdmp.sys [35304]

O58 - SDL:[MD5.741E9DFF4F42D2D8477D0FC1DC0DF871] - 21/01/2008 - 03:23:22 ---A- . (.Microsoft Corporation - Disk Block Verification Filter Driver.) -- C:\Windows\System32\Drivers\crcdisk.sys [24632]

O58 - SDL:[MD5.1F07BECDCA750766A96CDA811BA86410] - 21/01/2008 - 03:23:00 ---A- . (.Microsoft Corporation - Processor Device Driver.) -- C:\Windows\System32\Drivers\crusoe.sys [40960]

O58 - SDL:[MD5.622C41A07CA7E6DD91770F50D532CB6C] - 14/04/2011 - 15:59:03 ---A- . (.Microsoft Corporation - DFS Namespace Client Driver.) -- C:\Windows\System32\Drivers\dfsc.sys [75264]

O58 - SDL:[MD5.5D4AEFC3386920236A548271F8F1AF6A] - 11/04/2009 - 07:32:31 ---A- . (.Microsoft Corporation - PnP Disk Driver.) -- C:\Windows\System32\Drivers\disk.sys [53736]

O58 - SDL:[MD5.494075282E23D838F43A4C9FB7143959] - 11/04/2009 - 05:39:11 ---A- . (.Microsoft Corporation - Crash Dump Disk Driver.) -- C:\Windows\System32\Drivers\Diskdump.sys [19456]

O58 - SDL:[MD5.AE1FDF7BF7BB6C6A70F67699D880592A] - 02/11/2006 - 10:50:11 ---A- . (.Adaptec, Inc. - Adaptec Ultra SCSI miniport.) -- C:\Windows\System32\Drivers\djsvs.sys [71272]

O58 - SDL:[MD5.2A63675F6FA8EF0FF9F5C72695584CAA] - 30/10/2013 - 02:43:04 ---A- . (.Microsoft Corporation - Microsoft Kernel DRM Descrambler Filter.) -- C:\Windows\System32\Drivers\drmk.sys [130048]

O58 - SDL:[MD5.97FEF831AB90BEE128C9AF390E243F80] - 21/01/2008 - 03:23:21 ---A- . (.Microsoft Corporation - Microsoft Kernel DRM Audio Descrambler Filter.) -- C:\Windows\System32\Drivers\drmkaud.sys [5632]

O58 - SDL:[MD5.C67EBF9C05531C406E1E079FF669A2E6] - 11/04/2009 - 07:32:29 ---A- . (.Microsoft Corporation - ATAPI Dump Driver.) -- C:\Windows\System32\Drivers\Dumpata.sys [27624]

O58 - SDL:[MD5.EAAAFEF04FBB45665C9576E525D45A12] - 21/01/2008 - 03:24:21 ---A- . (.Microsoft Corporation - DirectX API Driver.) -- C:\Windows\System32\Drivers\dxapi.sys [13312]

O58 - SDL:[MD5.C8D5369BFE193B5FB53337DCE77CE314] - 11/04/2009 - 05:23:23 ---A- . (.Microsoft Corporation - DirectX Graphics Driver.) -- C:\Windows\System32\Drivers\dxg.sys [76288]

O58 - SDL:[MD5.988670D8343EF9835FB3659DB71B2EFA] - 01/08/2013 - 04:16:32 ---A- . (.Microsoft Corporation - DirectX Graphics Kernel.) -- C:\Windows\System32\Drivers\dxgkrnl.sys [638400]

O58 - SDL:[MD5.5425F74AC0C1DBD96A1E04F17D63F94C] - 21/01/2008 - 03:23:24 ---A- . (.Intel Corporation - Pilote désérialisé NDIS 6 de la carte Intel(R) PRO/1000.) -- C:\Windows\System32\Drivers\E1G60I32.sys [118784]

O58 - SDL:[MD5.7F64EA048DCFAC7ACF8B4D7B4E6FE371] - 11/04/2009 - 07:32:43 ---A- . (.Microsoft Corporation - Special Memory Device Cache.) -- C:\Windows\System32\Drivers\ecache.sys [141288]

O58 - SDL:[MD5.23B62471681A124889978F6295B3F4C6] - 21/01/2008 - 03:23:22 ---A- . (.Emulex - Storport Miniport Driver for LightPulse HBAs.) -- C:\Windows\System32\Drivers\elxstor.sys [342584]

O58 - SDL:[MD5.3DB974F3935483555D7148663F726C61] - 21/01/2008 - 03:23:00 ---A- . (.Microsoft Corporation - Error Device Driver.) -- C:\Windows\System32\Drivers\errdev.sys [6656]

O58 - SDL:[MD5.699CE24FE6B5120AF709A0B91582A02D] - 06/09/2007 - 09:43:49 ---A- . (.eMPIA Technology, Inc. - USB 27xx WDM Driver.) -- C:\Windows\System32\Drivers\etDevice.sys [474624]

O58 - SDL:[MD5.FD7CB14845A7F91BE11F80635B2CD8A6] - 05/02/2008 - 08:52:23 ---A- . (.eMPIA Technology Inc. - EM27xx / EM28xx Filter Driver.) -- C:\Windows\System32\Drivers\etFilter.sys [206464]

O58 - SDL:[MD5.2393ED056AE02F5DBB3A7D6E40A5FDC2] - 31/01/2008 - 12:18:57 ---A- . (.eMPIA Technology, Inc. - USB 27xx WDM Upper Filter.) -- C:\Windows\System32\Drivers\etScan.sys [6528]

O58 - SDL:[MD5.1D4D6D24256F61E6B08A3CF8184A78B8] - 12/08/2010 - 13:52:48 ---A- . (.Huawei Technologies Co., Ltd. - USB Modem/Serial Device Driver.) -- C:\Windows\System32\Drivers\ewusbfake.sys [103040]

O58 - SDL:[MD5.92CA47DA32009CCC00A5ADED04ABBD78] - 12/08/2010 - 13:52:48 ---A- . (.Huawei Technologies Co., Ltd. - USB Modem/Serial Device Driver.) -- C:\Windows\System32\Drivers\ewusbmdm.sys [102784]

O58 - SDL:[MD5.22B408651F9123527BCEE54B4F6C5CAE] - 11/04/2009 - 05:13:53 ---A- . (.Microsoft Corporation - Microsoft Extended FAT File System.) -- C:\Windows\System32\Drivers\exfat.sys [136704]

O58 - SDL:[MD5.1E9B9A70D332103C52995E957DC09EF8] - 11/04/2009 - 05:13:52 ---A- . (.Microsoft Corporation - Fast FAT File System Driver.) -- C:\Windows\System32\Drivers\fastfat.sys [142848]

O58 - SDL:[MD5.AFE1E8B9782A0DD7FB46BBD88E43F89A] - 21/01/2008 - 03:23:20 ---A- . (.Microsoft Corporation - Floppy Disk Controller Driver.) -- C:\Windows\System32\Drivers\fdc.sys [25088]

O58 - SDL:[MD5.A8C0139A884861E3AAE9CFE73B208A9F] - 21/01/2008 - 03:24:04 ---A- . (.Microsoft Corporation - FileInfo Filter Driver.) -- C:\Windows\System32\Drivers\fileinfo.sys [58936]

O58 - SDL:[MD5.0AE429A696AECBC5970E3CF2C62635AE] - 21/01/2008 - 03:24:21 ---A- . (.Microsoft Corporation - File Trace Filter Driver.) -- C:\Windows\System32\Drivers\filetrace.sys [27648]

O58 - SDL:[MD5.85B7CF99D532820495D68D747FDA9EBD] - 21/01/2008 - 03:23:20 ---A- . (.Microsoft Corporation - Floppy Driver.) -- C:\Windows\System32\Drivers\flpydisk.sys [20480]

O58 - SDL:[MD5.01334F9EA68E6877C4EF05D3EA8ABB05] - 11/04/2009 - 07:32:46 ---A- . (.Microsoft Corporation - Gestionnaire de filtres de système de fichiers Microsoft.) -- C:\Windows\System32\Drivers\fltMgr.sys [190424]

O58 - SDL:[MD5.D909075FA72C090F27AA926C32CB4612] - 23/09/2010 - 00:21:24 ---A- . (.Microsoft Corporation - Family Safety Filter Driver (WFP Callout).) -- C:\Windows\System32\Drivers\fssfltr.sys [39272]

O58 - SDL:[MD5.B972A66758577E0BFD1DE0F91AAA27B5] - 29/02/2012 - 14:32:37 ---A- . (.Microsoft Corporation - File System Recognizer Driver.) -- C:\Windows\System32\Drivers\fs\_rec.sys [12800]

O58 - SDL:[MD5.73594DBC99E22958150192EE99BC48CE] - 11/04/2009 - 07:32:43 ---A- . (.Microsoft Corporation - FWP/IPsec Kernel-Mode API.) -- C:\Windows\System32\Drivers\FWPKCLNT.SYS [99816]

O58 - SDL:[MD5.34582A6E6573D54A07ECE5FE24A126B5] - 21/01/2008 - 03:23:22 ---A- . (.Microsoft Corporation - Filtre AGPv3.0 générique Microsoft pour plateformes de processe.) -- C:\Windows\System32\Drivers\GAGP30KX.SYS [61496]

O58 - SDL:[MD5.062452B7FFD68C8C042A6261FE8DFF4A] - 11/04/2009 - 05:42:42 ---A- . (.Microsoft Corporation - High Definition Audio Bus Driver.) -- C:\Windows\System32\Drivers\hdaudbus.sys [561152]

O58 - SDL:[MD5.CB04C744BE0A61B1D648FAED182C3B59] - 02/11/2006 - 08:36:49 ---A- . (.Microsoft Corporation - High Definition Audio Function Driver.) -- C:\Windows\System32\Drivers\HdAudio.sys [235520]

O58 - SDL:[MD5.1338520E78D90154ED6BE8F84DE5FCEB] - 02/11/2006 - 09:55:22 ---A- . (.Microsoft Corporation - Pilote de miniport Bluetooth pour les périphériques HID.) -- C:\Windows\System32\Drivers\hidbth.sys [29184]

O58 - SDL:[MD5.5961CADB7CAD938368D2028725EF771D] - 11/04/2009 - 05:42:48 ---A- . (.Microsoft Corporation - Hid Class Library.) -- C:\Windows\System32\Drivers\hidclass.sys [39424]

O58 - SDL:[MD5.D8DF3722D5E961BAA1292AA2F12827E2] - 21/01/2008 - 03:23:26 ---A- . (.Microsoft Corporation - Infrared Miniport Driver for Input Devices.) -- C:\Windows\System32\Drivers\hidir.sys [21504]

O58 - SDL:[MD5.BE4AD4045D7A6C6AF4ECCBD5F6B7F8D8] - 03/07/2013 - 03:10:50 ---A- . (.Microsoft Corporation - Hid Parsing Library.) -- C:\Windows\System32\Drivers\hidparse.sys [25472]

O58 - SDL:[MD5.CCA4B519B17E23A00B826C55716809CC] - 11/04/2009 - 05:42:48 ---A- . (.Microsoft Corporation - USB Miniport Driver for Input Devices.) -- C:\Windows\System32\Drivers\hidusb.sys [12800]

O58 - SDL:[MD5.16EE7B23A009E00D835CDB79574A91A6] - 21/01/2008 - 03:23:26 ---A- . (.Hewlett-Packard Company - Smart Array Storport Driver.) -- C:\Windows\System32\Drivers\HpCISSs.sys [40504]

O58 - SDL:[MD5.F870AA3E254628EBEAFE754108D664DE] - 20/02/2010 - 21:53:34 ---A- . (.Microsoft Corporation - HTTP Pile du protocole.) -- C:\Windows\System32\Drivers\http.sys [411648]

O58 - SDL:[MD5.95BD3EA81EBE6B8CACAFDB6CDAB3586C] - 21/01/2008 - 03:23:02 ---A- . (.Microsoft Corporation - I2O Utility Filter.) -- C:\Windows\System32\Drivers\i2omgmt.sys [19000]

O58 - SDL:[MD5.C6B032D69650985468160FC9937CF5B4] - 21/01/2008 - 03:23:02 ---A- . (.Microsoft Corporation - I2O Miniport Driver.) -- C:\Windows\System32\Drivers\i2omp.sys [30264]

O58 - SDL:[MD5.22D56C8184586B7A1F6FA60BE5F5A2BD] - 21/01/2008 - 03:23:20 ---A- . (.Microsoft Corporation - Pilote de port i8042.) -- C:\Windows\System32\Drivers\i8042prt.sys [54784]

O58 - SDL:[MD5.80C633722DA72E97F3F5B3B11325696D] - 07/05/2008 - 10:40:01 ---A- . (.Intel Corporation - Intel Matrix Storage Manager driver - ia32.) -- C:\Windows\System32\Drivers\iaStor.sys [317976]

O58 - SDL:[MD5.54155EA1B0DF185878E0FC9EC3AC3A14] - 21/01/2008 - 03:23:23 ---A- . (.Intel Corporation - Intel Matrix Storage Manager driver (base).) -- C:\Windows\System32\Drivers\iaStorV.sys [235064]

O58 - SDL:[MD5.2D077BF86E843F901D8DB709C95B49A5] - 02/11/2006 - 10:50:17 ---A- . (.Intel Corp./ICP vortex GmbH - Intel/ICP Raid Storport Driver.) -- C:\Windows\System32\Drivers\iirsp.sys [41576]

O58 - SDL:[MD5.83AA759F3189E6370C30DE5DC5590718] - 21/01/2008 - 03:23:00 ---A- . (.Microsoft Corporation - Intel PCI IDE Driver.) -- C:\Windows\System32\Drivers\intelide.sys [17976]

O58 - SDL:[MD5.224191001E78C89DFA78924C3EA595FF] - 21/01/2008 - 03:23:00 ---A- . (.Microsoft Corporation - Processor Device Driver.) -- C:\Windows\System32\Drivers\intelppm.sys [41472]

O58 - SDL:[MD5.62C265C38769B864CB25B4BCF62DF6C3] - 21/01/2008 - 03:24:45 ---A- . (.Microsoft Corporation - IP FILTER DRIVER.) -- C:\Windows\System32\Drivers\ipfltdrv.sys [47616]

O58 - SDL:[MD5.B25AAF203552B7B3491139D582B39AD1] - 21/01/2008 - 03:23:22 ---A- . (.Microsoft Corporation - PILOT IPMI WMI.) -- C:\Windows\System32\Drivers\IPMIDrv.sys [64512]

O58 - SDL:[MD5.8793643A67B42CEC66490B2A0CF92D68] - 21/01/2008 - 03:24:25 ---A- . (.Microsoft Corporation - IP Network Address Translator.) -- C:\Windows\System32\Drivers\ipnat.sys [100864]

O58 - SDL:[MD5.E50A95179211B12946F7E035D60AF560] - 21/01/2008 - 03:24:31 ---A- . (.Microsoft Corporation - IRDA Protocol Driver.) -- C:\Windows\System32\Drivers\irda.sys [95744]

O58 - SDL:[MD5.109C0DFB82C3632FBD11949B73AEEAC9] - 21/01/2008 - 03:23:54 ---A- . (.Microsoft Corporation - Infra-Red Bus Enumerator.) -- C:\Windows\System32\Drivers\irenum.sys [13312]

O58 - SDL:[MD5.6C70698A3E5C4376C6AB5C7C17FB0614] - 21/01/2008 - 03:23:01 ---A- . (.Microsoft Corporation - Pilote de bus PNP ISA.) -- C:\Windows\System32\Drivers\isapnp.sys [49720]

O58 - SDL:[MD5.BCED60D16156E428F8DF8CF27B0DF150] - 02/11/2006 - 10:50:07 ---A- . (.Integrated Technology Express, Inc. - ITE IT8211 ATA/ATAPI SCSI miniport.) -- C:\Windows\System32\Drivers\iteatapi.sys [35944]

O58 - SDL:[MD5.8BCD857C7932AD005D5F9C89329DA2E1] - 19/12/2007 - 02:12:12 ---A- . (.ITE Tech. Inc. - ITE Consumer IR Driver for eHome.) -- C:\Windows\System32\Drivers\itecir.sys [54784]

O58 - SDL:[MD5.06FA654504A498C30ADCA8BEC4E87E7E] - 02/11/2006 - 10:50:09 ---A- . (.Integrated Technology Express, Inc. - ITE IT8212 ATA RAID SCSI miniport.) -- C:\Windows\System32\Drivers\iteraid.sys [35944]

O58 - SDL:[MD5.37605E0A8CF00CBBA538E753E4344C6E] - 21/01/2008 - 03:23:23 ---A- . (.Microsoft Corporation - Pilote de la classe Clavier.) -- C:\Windows\System32\Drivers\kbdclass.sys [35384]

O58 - SDL:[MD5.EDE59EC70E25C24581ADD1FBEC7325F7] - 11/04/2009 - 05:38:40 ---A- . (.Microsoft Corporation - Pilote de filtre clavier HID.) -- C:\Windows\System32\Drivers\kbdhid.sys [17408]

O58 - SDL:[MD5.27BD4AC228EF6C0D490617C32E86A672] - 03/06/2008 - 07:41:51 ---A- . (.Pas de propriétaire - Keyboard Filter Driver.) -- C:\Windows\System32\Drivers\kbfiltr.sys [15928]

O58 - SDL:[MD5.EF73C1E29FBE7B0FD0274BF4394E346A] - 11/04/2009 - 05:38:49 ---A- . (.Microsoft Corporation - Kernel CSA Library.) -- C:\Windows\System32\Drivers\ks.sys [149504]

O58 - SDL:[MD5.4A1445EFA932A3BAF5BDB02D7131EE20] - 04/06/2012 - 16:26:04 ---A- . (.Microsoft Corporation - Kernel Security Support Provider Interface.) -- C:\Windows\System32\Drivers\ksecdd.sys [440704]

O58 - SDL:[MD5.4127E8B6DDB4090E815C1F8852C277D3] - 15/01/2010 - 19:14:59 ---A- . (...) -- C:\Windows\System32\Drivers\lirsgt.sys [25416]

O58 - SDL:[MD5.D1C5883087A0C3F1344D9D55A44901F6] - 21/01/2008 - 03:24:37 ---A- . (.Microsoft Corporation - Link-Layer Topology Mapper I/O Driver.) -- C:\Windows\System32\Drivers\lltdio.sys [47104]

O58 - SDL:[MD5.C7E15E82879BF3235B559563D4185365] - 21/01/2008 - 03:23:23 ---A- . (.LSI Logic - LSI Logic Fusion-MPT FC Driver (StorPort).) -- C:\Windows\System32\Drivers\lsi\_fc.sys [96312]

O58 - SDL:[MD5.EE01EBAE8C9BF0FA072E0FF68718920A] - 21/01/2008 - 03:23:25 ---A- . (.LSI Logic - LSI Logic Fusion-MPT SAS Driver (StorPort).) -- C:\Windows\System32\Drivers\lsi\_sas.sys [89656]

O58 - SDL:[MD5.912A04696E9CA30146A62AFA1463DD5C] - 21/01/2008 - 03:23:23 ---A- . (.LSI Logic - LSI Logic Fusion-MPT SCSI Driver (StorPort).) -- C:\Windows\System32\Drivers\lsi\_scsi.sys [96312]

O58 - SDL:[MD5.8F5C7426567798E62A3B3614965D62CC] - 21/01/2008 - 03:24:37 ---A- . (.Microsoft Corporation - Pilote de filtre de virtualisation de fichier LUA.) -- C:\Windows\System32\Drivers\luafv.sys [84480]

O58 - SDL:[MD5.8039F480C192DD99FED4EBC71FFBF795] - 29/05/2008 - 19:21:02 ---A- . (.Windows (R) Codename Longhorn DDK provider - ASUS CopyProtect driver.) -- C:\Windows\System32\Drivers\lullaby.sys [15416]

O58 - SDL:[MD5.4470E3C1E0C3378E4CAB137893C12C3A] - 04/04/2013 - 14:50:32 ---A- . (.Malwarebytes Corporation - Malwarebytes Anti-Malware.) -- C:\Windows\System32\Drivers\mbam.sys [22856]

O58 - SDL:[MD5.B271EC02E71271A2DA28B3B7BC4E4F15] - 21/01/2008 - 03:24:47 ---A- . (.Microsoft Corporation - Medium changer class driver.) -- C:\Windows\System32\Drivers\mcd.sys [18944]

O58 - SDL:[MD5.0001CE609D66632FA17B84705F658879] - 21/01/2008 - 03:23:27 ---A- . (.LSI Corporation - MEGASAS RAID Controller Driver for Windows Vista/Longhorn for x.) -- C:\Windows\System32\Drivers\megasas.sys [31288]

O58 - SDL:[MD5.C252F32CD9A49DBFC25ECF26EBD51A99] - 21/01/2008 - 03:23:27 ---A- . (.LSI Corporation, Inc. - LSI MegaRAID Software RAID Driver.) -- C:\Windows\System32\Drivers\MegaSR.sys [386616]

O58 - SDL:[MD5.E13B5EA0F51BA5B1512EC671393D09BA] - 21/01/2008 - 03:24:57 ---A- . (.Microsoft Corporation - Pilote de périphérique modem.) -- C:\Windows\System32\Drivers\modem.sys [31744]

O58 - SDL:[MD5.0A9BB33B56E294F686ABB7C1E4E2D8A8] - 21/01/2008 - 03:23:22 ---A- . (.Microsoft Corporation - Monitor Driver.) -- C:\Windows\System32\Drivers\monitor.sys [41984]

O58 - SDL:[MD5.5BF6A1326A335C5298477754A506D263] - 21/01/2008 - 03:23:20 ---A- . (.Microsoft Corporation - Pilote de la classe Souris.) -- C:\Windows\System32\Drivers\mouclass.sys [34360]

O58 - SDL:[MD5.93B8D4869E12CFBE663915502900876F] - 21/01/2008 - 03:23:20 ---A- . (.Microsoft Corporation - Pilote de filtre souris HID.) -- C:\Windows\System32\Drivers\mouhid.sys [15872]

O58 - SDL:[MD5.BDAFC88AA6B92F7842416EA6A48E1600] - 21/01/2008 - 03:23:43 ---A- . (.Microsoft Corporation - Mount Point Manager.) -- C:\Windows\System32\Drivers\mountmgr.sys [57400]

O58 - SDL:[MD5.511D011289755DD9F9A7579FB0B064E6] - 21/01/2008 - 03:23:20 ---A- . (.Microsoft Corporation - Pilote du bus de prise en charge des chemins d’accès multiples.) -- C:\Windows\System32\Drivers\mpio.sys [105016]

O58 - SDL:[MD5.22241FEBA9B2DEFA669C8CB0A8DD7D2E] - 21/01/2008 - 03:24:47 ---A- . (.Microsoft Corporation - Microsoft Protection Service Driver.) -- C:\Windows\System32\Drivers\mpsdrv.sys [64000]

O58 - SDL:[MD5.4FBBB70D30FD20EC51F80061703B001E] - 02/11/2006 - 10:49:59 ---A- . (.LSI Logic Corporation - MegaRAID RAID Controller Driver for Windows Vista/Longhorn for.) -- C:\Windows\System32\Drivers\Mraid35x.sys [33384]

O58 - SDL:[MD5.82CEA0395524AACFEB58BA1448E8325C] - 11/04/2009 - 05:14:40 ---A- . (.Microsoft Corporation - Windows NT WebDav Minirdr.) -- C:\Windows\System32\Drivers\mrxdav.sys [114688]

O58 - SDL:[MD5.1E94971C4B446AB2290DEB71D01CF0C2] - 29/04/2011 - 14:24:40 ---A- . (.Microsoft Corporation - Windows NT SMB Minirdr.) -- C:\Windows\System32\Drivers\mrxsmb.sys [106496]

O58 - SDL:[MD5.4FCCB34D793B116423209C0F8B7A3B03] - 06/07/2011 - 16:31:47 ---A- . (.Microsoft Corporation - Longhorn SMB Downlevel SubRdr.) -- C:\Windows\System32\Drivers\mrxsmb10.sys [214016]

O58 - SDL:[MD5.C3CB1B40AD4A0124D617A1199B0B9D7C] - 29/04/2011 - 14:24:42 ---A- . (.Microsoft Corporation - Longhorn SMB 2.0 Redirector.) -- C:\Windows\System32\Drivers\mrxsmb20.sys [79872]

O58 - SDL:[MD5.DE77526BDE93142BDC90CFA9F5CEAD36] - 22/02/2008 - 06:04:00 ---A- . (.Microsoft Corporation - MS AHCI 1.0 Standard Driver.) -- C:\Windows\System32\Drivers\msahci.sys [28728]

O58 - SDL:[MD5.4468B0F385A86ECDDAF8D3CA662EC0E7] - 21/01/2008 - 03:23:21 ---A- . (.Microsoft Corporation - Microsoft Device Specific Module.) -- C:\Windows\System32\Drivers\msdsm.sys [94776]

O58 - SDL:[MD5.A9927F4A46B816C92F461ACB90CF8515] - 21/01/2008 - 03:23:51 ---A- . (.Microsoft Corporation - Mailslot driver.) -- C:\Windows\System32\Drivers\msfs.sys [22528]

O58 - SDL:[MD5.0F400E306F385C56317357D6DEA56F62] - 21/01/2008 - 03:23:01 ---A- . (.Microsoft Corporation - ISA Driver.) -- C:\Windows\System32\Drivers\msisadrv.sys [16440]

O58 - SDL:[MD5.232FA340531D940AAC623B121A595034] - 11/04/2009 - 07:32:46 ---A- . (.Microsoft Corporation - Microsoft iSCSI Initiator Driver.) -- C:\Windows\System32\Drivers\msiscsi.sys [180712]

O58 - SDL:[MD5.D8C63D34D9C9E56C059E24EC7185CC07] - 21/01/2008 - 03:24:50 ---A- . (.Microsoft Corporation - MS KS Server.) -- C:\Windows\System32\Drivers\mskssrv.sys [8192]

O58 - SDL:[MD5.1D373C90D62DDB641D50E55B9E78D65E] - 21/01/2008 - 03:24:51 ---A- . (.Microsoft Corporation - MS Proxy Clock.) -- C:\Windows\System32\Drivers\mspclock.sys [5888]

O58 - SDL:[MD5.B572DA05BF4E098D4BBA3A4734FB505B] - 21/01/2008 - 03:24:51 ---A- . (.Microsoft Corporation - MS Proxy Quality Manager.) -- C:\Windows\System32\Drivers\mspqm.sys [5504]

O58 - SDL:[MD5.B49456D70555DE905C311BCDA6EC6ADB] - 11/04/2009 - 07:32:46 ---A- . (.Microsoft Corporation - Kernel Remote Procedure Call Provider.) -- C:\Windows\System32\Drivers\msrpc.sys [161752]

O58 - SDL:[MD5.E384487CB84BE41D09711C30CA79646C] - 21/01/2008 - 03:23:01 ---A- . (.Microsoft Corporation - System Management BIOS Driver.) -- C:\Windows\System32\Drivers\mssmbios.sys [31288]

O58 - SDL:[MD5.7199C1EEC1E4993CAF96B8C0A26BD58A] - 21/01/2008 - 03:24:51 ---A- . (.Microsoft Corporation - WDM Tee/Communication Transform Filter.) -- C:\Windows\System32\Drivers\mstee.sys [6016]

O58 - SDL:[MD5.6A57B5733D4CB702C8EA4542E836B96C] - 11/04/2009 - 07:32:31 ---A- . (.Microsoft Corporation - Multiple UNC Provider driver.) -- C:\Windows\System32\Drivers\mup.sys [48104]

O58 - SDL:[MD5.1357274D1883F68300AEADD15D7BBB42] - 11/04/2009 - 07:32:49 ---A- . (.Microsoft Corporation - NDIS 6.0 wrapper driver.) -- C:\Windows\System32\Drivers\ndis.sys [527848]

O58 - SDL:[MD5.0E186E90404980569FB449BA7519AE61] - 21/01/2008 - 03:24:25 ---A- . (.Microsoft Corporation - NDIS 3.0 connection wrapper driver.) -- C:\Windows\System32\Drivers\ndistapi.sys [20992]

O58 - SDL:[MD5.D6973AA34C4D5D76C0430B181C3CD389] - 21/01/2008 - 03:24:55 ---A- . (.Microsoft Corporation - NDIS User mode I/O driver.) -- C:\Windows\System32\Drivers\ndisuio.sys [16896]

O58 - SDL:[MD5.818F648618AE34F729FDB47EC68345C3] - 11/04/2009 - 05:46:32 ---A- . (.Microsoft Corporation - MS PPP Framing Driver (Strong Encryption).) -- C:\Windows\System32\Drivers\ndiswan.sys [121344]

O58 - SDL:[MD5.71DAB552B41936358F3B541AE5997FB3] - 21/01/2008 - 03:24:25 ---A- . (.Microsoft Corporation - NDIS Proxy.) -- C:\Windows\System32\Drivers\ndproxy.sys [49664]

O58 - SDL:[MD5.BCD093A5A6777CF626434568DC7DBA78] - 21/01/2008 - 03:24:20 ---A- . (.Microsoft Corporation - NetBIOS interface driver.) -- C:\Windows\System32\Drivers\netbios.sys [35840]

O58 - SDL:[MD5.ECD64230A59CBD93C85F1CD1CAB9F3F6] - 11/04/2009 - 05:45:37 ---A- . (.Microsoft Corporation - MBT Transport driver.) -- C:\Windows\System32\Drivers\netbt.sys [185856]

O58 - SDL:[MD5.063EE4D3CB88A14EAB9901875CEE98B1] - 11/04/2009 - 07:32:46 ---A- . (.Microsoft Corporation - Network I/O Subsystem.) -- C:\Windows\System32\Drivers\netio.sys [223208]

O58 - SDL:[MD5.2E7FB731D4790A1BC6270ACCEFACB36E] - 02/11/2006 - 10:50:19 ---A- . (.IBM Corporation - IBM ServeRAID Controller Driver.) -- C:\Windows\System32\Drivers\nfrd960.sys [45160]

O58 - SDL:[MD5.D36F239D7CCE1931598E8FB90A0DBC26] - 11/04/2009 - 05:14:01 ---A- . (.Microsoft Corporation - NPFS Driver.) -- C:\Windows\System32\Drivers\npfs.sys [35328]

O58 - SDL:[MD5.609773E344A97410CE4EBF74A8914FCF] - 21/01/2008 - 03:24:47 ---A- . (.Microsoft Corporation - NSI Proxy.) -- C:\Windows\System32\Drivers\nsiproxy.sys [16384]

O58 - SDL:[MD5.2C1121F2B87E9A6B12485DF53CD848C7] - 03/03/2013 - 20:07:52 ---A- . (.Microsoft Corporation - Pilote du système de fichiers NT.) -- C:\Windows\System32\Drivers\ntfs.sys [1082232]

O58 - SDL:[MD5.E875C093AEC0C978A90F30C9E0DFBB72] - 02/11/2006 - 08:36:50 ---A- . (.N-trig Innovative Technologies - Pilote intégré de digitalisateur de tablette N-trig.) -- C:\Windows\System32\Drivers\ntrigdigi.sys [20608]

O58 - SDL:[MD5.C5DBBCDA07D780BDA9B685DF333BB41E] - 21/01/2008 - 03:23:50 ---A- . (.Microsoft Corporation - NULL Driver.) -- C:\Windows\System32\Drivers\null.sys [4608]

O58 - SDL:[MD5.11BE4B269549173CFF542591E4BE2C08] - 25/06/2008 - 15:58:59 ---A- . (.NVIDIA Corporation - NVIDIA HDMI Audio Driver.) -- C:\Windows\System32\Drivers\nvhda32v.sys [43040]

O58 - SDL:[MD5.7DB332F85AB7894C69DFB934EEE23EB9] - 25/06/2008 - 15:58:59 ---A- . (.NVIDIA Corporation - NVIDIA Compatible Windows Vista Kernel Mode Driver, Version 176.) -- C:\Windows\System32\Drivers\nvlddmkm.sys [7534720]

O58 - SDL:[MD5.2EDF9E7751554B42CBB60116DE727101] - 21/01/2008 - 03:23:21 ---A- . (.NVIDIA Corporation - NVIDIA® nForce(TM) RAID Driver.) -- C:\Windows\System32\Drivers\nvraid.sys [102968]

O58 - SDL:[MD5.ABED0C09758D1D97DB0042DBB2688177] - 21/01/2008 - 03:23:21 ---A- . (.NVIDIA Corporation - NVIDIA® nForce(TM) Sata Performance Driver.) -- C:\Windows\System32\Drivers\nvstor.sys [45112]

O58 - SDL:[MD5.18BBDF913916B71BD54575BDB6EEAC0B] - 21/01/2008 - 03:23:01 ---A- . (.Microsoft Corporation - Filtre AGP NForce NT.) -- C:\Windows\System32\Drivers\NV\_AGP.SYS [109112]

O58 - SDL:[MD5.85C44FDFF9CF7E72A40DCB7EC06A4416] - 11/04/2009 - 05:43:28 ---A- . (.Microsoft Corporation - NativeWiFi Miniport Driver.) -- C:\Windows\System32\Drivers\nwifi.sys [148480]

O58 - SDL:[MD5.6F310E890D46E246E0E261A63D9B36B4] - 11/04/2009 - 05:43:04 ---A- . (.Microsoft Corporation - 1394 OpenHCI Port Driver.) -- C:\Windows\System32\Drivers\ohci1394.sys [62208]

O58 - SDL:[MD5.99514FAA8DF93D34B5589187DB3AA0BA] - 11/04/2009 - 05:45:51 ---A- . (.Microsoft Corporation - Planificateur de paquets QoS.) -- C:\Windows\System32\Drivers\pacer.sys [72192]

O58 - SDL:[MD5.0FA9B5055484649D63C303FE404E5F4D] - 02/11/2006 - 09:51:30 ---A- . (.Microsoft Corporation - Pilote de port parallèle.) -- C:\Windows\System32\Drivers\parport.sys [79360]

O58 - SDL:[MD5.B9C2B89F08670E159F7181891E449CD9] - 21/03/2012 - 00:28:50 ---A- . (.Microsoft Corporation - Partition Management Driver.) -- C:\Windows\System32\Drivers\partmgr.sys [53120]

O58 - SDL:[MD5.4F9A6A8A31413180D0FCB279AD5D8112] - 02/11/2006 - 09:51:23 ---A- . (.Microsoft Corporation - Pilote parallèle VDM.) -- C:\Windows\System32\Drivers\parvdm.sys [8704]

O58 - SDL:[MD5.941DC1D19E7E8620F40BBC206981EFDB] - 11/04/2009 - 07:32:55 ---A- . (.Microsoft Corporation - Énumérateur Plug-and-Play PCI pour NT.) -- C:\Windows\System32\Drivers\pci.sys [149480]

O58 - SDL:[MD5.FC175F5DDAB666D7F4D17449A547626F] - 21/01/2008 - 03:23:00 ---A- . (.Microsoft Corporation - Generic PCI IDE Bus Driver.) -- C:\Windows\System32\Drivers\pciide.sys [16440]

O58 - SDL:[MD5.99F62C34332223251D4D5E9D25FE276B] - 22/02/2008 - 06:04:39 ---A- . (.Microsoft Corporation - PCI IDE Bus Driver Extension.) -- C:\Windows\System32\Drivers\pciidex.sys [45112]

O58 - SDL:[MD5.E6F3FB1B86AA519E7698AD05E58B04E5] - 02/11/2006 - 10:51:12 ---A- . (.Microsoft Corporation - Pilote de bus PCMCIA.) -- C:\Windows\System32\Drivers\pcmcia.sys [167528]

O58 - SDL:[MD5.6349F6ED9C623B44B52EA3C63C831A92] - 02/11/2006 - 10:04:35 ---A- . (.Microsoft Corporation - Protected Environment Authentication and Authorization Export D.) -- C:\Windows\System32\Drivers\PEAuth.sys [878080]

O58 - SDL:[MD5.6DBA75306DD9B242B6F1C343179AD201] - 30/10/2013 - 01:43:06 ---A- . (.Microsoft Corporation - Port Class (Class Driver for Port/Miniport Devices).) -- C:\Windows\System32\Drivers\portcls.sys [167936]

O58 - SDL:[MD5.2027293619DD0F047C584CF2E7DF4FFD] - 21/01/2008 - 03:23:00 ---A- . (.Microsoft Corporation - Processor Device Driver.) -- C:\Windows\System32\Drivers\processr.sys [40960]

O58 - SDL:[MD5.49452BFCEC22F36A7A9B9C2181BC3042] - 23/02/2008 - 03:38:33 ---A- . (.Sonic Solutions - Px Engine Device Driver for Windows 2000/XP.) -- C:\Windows\System32\Drivers\pxhelp20.sys [43872]

O58 - SDL:[MD5.0A6DB55AFB7820C99AA1F3A1D270F4F6] - 21/01/2008 - 03:23:24 ---A- . (.QLogic Corporation - QLogic Fibre Channel Stor Miniport Driver.) -- C:\Windows\System32\Drivers\ql2300.sys [1122360]

O58 - SDL:[MD5.81A7E5C076E59995D54BC1ED3A16E60B] - 02/11/2006 - 10:50:35 ---A- . (.QLogic Corporation - QLogic iSCSI Storport Miniport Driver.) -- C:\Windows\System32\Drivers\ql40xx.sys [106088]

O58 - SDL:[MD5.9F5E0E1926014D17486901C88ECA2DB7] - 21/01/2008 - 03:23:31 ---A- . (.Microsoft Corporation - Pilote du support de Microsoft Quality Windows Audio Video Expe.) -- C:\Windows\System32\Drivers\qwavedrv.sys [31232]

O58 - SDL:[MD5.147D7F9C556D259924351FEB0DE606C3] - 21/01/2008 - 03:24:19 ---A- . (.Microsoft Corporation - RAS Automatic Connection Driver.) -- C:\Windows\System32\Drivers\rasacd.sys [11776]

O58 - SDL:[MD5.A214ADBAF4CB47DD2728859EF31F26B0] - 21/01/2008 - 03:24:55 ---A- . (.Microsoft Corporation - RAS L2TP mini-port/call-manager driver.) -- C:\Windows\System32\Drivers\rasl2tp.sys [76288]

O58 - SDL:[MD5.509A98DD18AF4375E1FC40BC175F1DEF] - 11/04/2009 - 05:46:30 ---A- . (.Microsoft Corporation - RAS PPPoE mini-port/call-manager driver.) -- C:\Windows\System32\Drivers\raspppoe.sys [41472]

O58 - SDL:[MD5.ECFFFAEC0C1ECD8DBC77F39070EA1DB1] - 21/01/2008 - 03:24:55 ---A- . (.Microsoft Corporation - Peer-to-Peer Tunneling Protocol.) -- C:\Windows\System32\Drivers\raspptp.sys [62976]

O58 - SDL:[MD5.2005F4A1E05FA09389AC85840F0A9E4D] - 11/04/2009 - 05:46:40 ---A- . (.Microsoft Corporation - RAS SSTP Miniport Call Manager.) -- C:\Windows\System32\Drivers\rassstp.sys [69120]

O58 - SDL:[MD5.B14C9D5B9ADD2F84F70570BBBFAA7935] - 11/04/2009 - 05:14:29 ---A- . (.Microsoft Corporation - Redirected Drive Buffering SubSystem Driver.) -- C:\Windows\System32\Drivers\rdbss.sys [225280]

O58 - SDL:[MD5.89E59BE9A564262A3FB6C4F4F1CD9899] - 21/01/2008 - 03:24:06 ---A- . (.Microsoft Corporation - RDP Miniport.) -- C:\Windows\System32\Drivers\RDPCDD.sys [6144]

O58 - SDL:[MD5.FBC0BACD9C3D7F6956853F64A66E252D] - 21/01/2008 - 03:23:01 ---A- . (.Microsoft Corporation - Microsoft RDP Device redirector.) -- C:\Windows\System32\Drivers\rdpdr.sys [248832]

O58 - SDL:[MD5.9D91FE5286F748862ECFFA05F8A0710C] - 21/01/2008 - 03:24:50 ---A- . (.Microsoft Corporation - RDP Miniport.) -- C:\Windows\System32\Drivers\RDPENCDD.sys [6144]

O58 - SDL:[MD5.C127EBD5AFAB31524662C48DFCEB773A] - 01/05/2012 - 15:03:49 ---A- . (.Microsoft Corporation - RDP Terminal Stack Driver.) -- C:\Windows\System32\Drivers\rdpwd.sys [180736]

O58 - SDL:[MD5.6482707F9F4DA0ECBAB43B2E0398A101] - 11/04/2009 - 05:43:12 ---A- . (.Microsoft Corporation - Bluetooth RFCOMM Driver.) -- C:\Windows\System32\Drivers\rfcomm.sys [148992]

O58 - SDL:[MD5.A5B12A4B3B774432DB9B9FA221190E59] - 16/02/2008 - 02:42:42 ---A- . (.REDC - RICOH SD Driver.) -- C:\Windows\System32\Drivers\rimmptsk.sys [46592]

O58 - SDL:[MD5.C398BCA91216755B098679A8DA8A2300] - 30/07/2007 - 19:42:58 ---A- . (.REDC - RICOH MS Driver.) -- C:\Windows\System32\Drivers\rimsptsk.sys [43008]

O58 - SDL:[MD5.2A2554CB24506E0A0508FC395C4A1B42] - 30/07/2007 - 20:54:02 ---A- . (.REDC - RICOH XD SM Driver.) -- C:\Windows\System32\Drivers\rixdptsk.sys [38400]

O58 - SDL:[MD5.EEC7EE5675294B03E88AA868540007C1] - 11/04/2009 - 05:45:24 ---A- . (.Microsoft Corporation - Reliable Multicast Transport.) -- C:\Windows\System32\Drivers\rmcast.sys [113664]

O58 - SDL:[MD5.D9225D107E40D0FA5C5069446759C8E9] - 11/04/2009 - 05:46:07 ---A- . (.Microsoft Corporation - Remote NDIS Miniport.) -- C:\Windows\System32\Drivers\RNDISMP.sys [33280]

O58 - SDL:[MD5.75E8A6BFA7374ABA833AE92BF41AE4E6] - 21/01/2008 - 03:24:49 ---A- . (.Microsoft Corporation - Legacy Non-Pnp Modem Device Driver.) -- C:\Windows\System32\Drivers\rootmdm.sys [8192]

O58 - SDL:[MD5.9C508F4074A39E8B4B31D27198146FAD] - 21/01/2008 - 03:24:37 ---A- . (.Microsoft Corporation - Link-Layer Topology Responder Driver for NDIS 6.) -- C:\Windows\System32\Drivers\rspndr.sys [60416]

O58 - SDL:[MD5.58072F5FD95ECE78F9FA7BDA1210A9E7] - 17/06/2008 - 09:49:51 ---A- . (.Realtek Semiconductor Corp. - Realtek(r) High Definition Audio Function Driver.) -- C:\Windows\System32\Drivers\RTKVHDA.sys [2153688]

O58 - SDL:[MD5.2FC33077F85D7DC0D03678C06D43898C] - 02/05/2008 - 06:59:39 ---A- . (.Realtek Corporation - Realtek 8101E/8168/8169 NDIS6 32-bit Driver.) -- C:\Windows\System32\Drivers\Rtlh86.sys [122368]

O58 - SDL:[MD5.B587F7FFBF6B61523B7C9127F9D999CF] - 25/05/2009 - 10:49:10 ---A- . (.MCCI Corporation - Sony Ericsson Device 1029 Driver.) -- C:\Windows\System32\Drivers\s1029bus.sys [86568]

O58 - SDL:[MD5.71170F6990B271C0BAFE36F22455C532] - 25/05/2009 - 10:49:08 ---A- . (.MCCI Corporation - Windows 2000/XP support functions.) -- C:\Windows\System32\Drivers\s1029cm.sys [12200]

O58 - SDL:[MD5.71170F6990B271C0BAFE36F22455C532] - 25/05/2009 - 10:49:08 ---A- . (.MCCI Corporation - Windows 2000/XP support functions.) -- C:\Windows\System32\Drivers\s1029cmnt.sys [12200]

O58 - SDL:[MD5.EEF53F82914FE1C5DEB5AAFA6D310C4C] - 25/05/2009 - 10:49:10 ---A- . (.MCCI Corporation - Sony Ericsson Device 1029 USB Ethernet Emulation (WDM class reg.) -- C:\Windows\System32\Drivers\s1029cr.sys [10792]

O58 - SDL:[MD5.03899AD24893F066C94534978CBE87E6] - 25/05/2009 - 10:49:08 ---A- . (.MCCI Corporation - Sony Ericsson Device 1029 USB WMC Modem Filter Driver.) -- C:\Windows\System32\Drivers\s1029mdfl.sys [15016]

O58 - SDL:[MD5.548E8C91F0FDC2858E5DC498A723C87C] - 25/05/2009 - 10:49:08 ---A- . (.MCCI Corporation - Sony Ericsson Device 1029 USB WMC Modem WDM Driver.) -- C:\Windows\System32\Drivers\s1029mdm.sys [114472]

O58 - SDL:[MD5.C6B7870127821B6DB1B6897AD80AC9D0] - 25/05/2009 - 10:49:08 ---A- . (.MCCI Corporation - Sony Ericsson Device 1029 USB WMC Device Management Driver.) -- C:\Windows\System32\Drivers\s1029mgmt.sys [108200]

O58 - SDL:[MD5.41271C04631A66B023B347943ECF3446] - 25/05/2009 - 10:49:08 ---A- . (.MCCI Corporation - Sony Ericsson Device 1029 USB Ethernet Emulation (NDIS 5 Minipo.) -- C:\Windows\System32\Drivers\s1029nd5.sys [26024]

O58 - SDL:[MD5.D1FE6656C9AE3E26DC299A0929B48BDE] - 25/05/2009 - 10:49:08 ---A- . (.MCCI Corporation - Sony Ericsson Device 1029 USB WMC OBEX Interface Device Driver.) -- C:\Windows\System32\Drivers\s1029obex.sys [104488]

O58 - SDL:[MD5.B59912EC19DB1534ECC28D22DD179D91] - 25/05/2009 - 10:49:08 ---A- . (.MCCI Corporation - Sony Ericsson Device 1029 USB Ethernet Emulation.) -- C:\Windows\System32\Drivers\s1029unic.sys [109480]

O58 - SDL:[MD5.E42B6142DB7C8313F93256C4811BB19B] - 25/05/2009 - 10:49:10 ---A- . (.MCCI Corporation - Windows 2000/XP support functions.) -- C:\Windows\System32\Drivers\s1029wh.sys [12200]

O58 - SDL:[MD5.E42B6142DB7C8313F93256C4811BB19B] - 25/05/2009 - 10:49:10 ---A- . (.MCCI Corporation - Windows 2000/XP support functions.) -- C:\Windows\System32\Drivers\s1029whnt.sys [12200]

O58 - SDL:[MD5.3CE8F073A557E172B330109436984E30] - 02/11/2006 - 10:50:16 ---A- . (.Microsoft Corporation - SBP-2 Protocol Driver.) -- C:\Windows\System32\Drivers\sbp2port.sys [76392]

O58 - SDL:[MD5.C1AE5D1F53285D79A0B73A62AF20734F] - 30/03/2011 - 16:59:03 ---A- . (.Sunbelt Software - Anti-Rootkit Engine.) -- C:\Windows\System32\Drivers\SBREDrv.sys [98392]

O58 - SDL:[MD5.6F5CA34AE885645ACF8A20D564DB976C] - 21/01/2008 - 03:23:54 ---A- . (.Microsoft Corporation - SCSI Port Driver.) -- C:\Windows\System32\Drivers\scsiport.sys [142904]

O58 - SDL:[MD5.8F36B54688C31EED4580129040C6A3D3] - 11/04/2009 - 05:19:14 ---A- . (.Microsoft Corporation - SecureDigital Bus Driver.) -- C:\Windows\System32\Drivers\sdbus.sys [89088]

O58 - SDL:[MD5.68E44E331D46F0FB38F0863A84CD1A31] - 02/11/2006 - 09:51:25 ---A- . (.Microsoft Corporation - Serial Port Enumerator.) -- C:\Windows\System32\Drivers\serenum.sys [17920]

O58 - SDL:[MD5.C70D69A918B178D3C3B06339B40C2E1B] - 02/11/2006 - 09:51:30 ---A- . (.Microsoft Corporation - Pilote de périphérique série.) -- C:\Windows\System32\Drivers\serial.sys [83456]

O58 - SDL:[MD5.8AF3D28A879BF75DB53A0EE7A4289624] - 21/01/2008 - 03:23:20 ---A- . (.Microsoft Corporation - Pilote de filtre souris série.) -- C:\Windows\System32\Drivers\sermouse.sys [19968]

O58 - SDL:[MD5.EF70B3D22B4BFFDA6EA851ECB063EFAA] - 21/01/2008 - 03:23:27 ---A- . (.Microsoft Corporation - Pilote de périphérique Serial Imaging.) -- C:\Windows\System32\Drivers\serscan.sys [9216]

O58 - SDL:[MD5.3EFA810BDCA87F6ECC24F9832243FE86] - 21/01/2008 - 03:23:23 ---A- . (.Microsoft Corporation - Small Form Factor Disk Driver.) -- C:\Windows\System32\Drivers\sffdisk.sys [13312]

O58 - SDL:[MD5.E95D451F7EA3E583AEC75F3B3EE42DC5] - 21/01/2008 - 03:23:23 ---A- . (.Microsoft Corporation - Small Form Factor MMC Protocol Driver.) -- C:\Windows\System32\Drivers\sffp\_mmc.sys [12288]

O58 - SDL:[MD5.9F66A46C55D6F1CCABC79BB7AFCCC545] - 11/04/2009 - 05:39:13 ---A- . (.Microsoft Corporation - Small Form Factor SD Protocol Driver.) -- C:\Windows\System32\Drivers\sffp\_sd.sys [11776]

O58 - SDL:[MD5.C33BFBD6E9E41FCD9FFEF9729E9FAED6] - 21/01/2008 - 03:23:20 ---A- . (.Microsoft Corporation - SCSI Floppy Driver.) -- C:\Windows\System32\Drivers\sfloppy.sys [13312]

O58 - SDL:[MD5.1D76624A09A054F682D746B924E2DBC3] - 21/01/2008 - 03:23:01 ---A- . (.Microsoft Corporation - Filtre SIS NT AGP.) -- C:\Windows\System32\Drivers\SISAGP.SYS [55864]

O58 - SDL:[MD5.43CB7AA756C7DB280D01DA9B676CFDE2] - 21/01/2008 - 03:23:26 ---A- . (.Microsoft Corporation - SiS RAID Stor Miniport Driver.) -- C:\Windows\System32\Drivers\sisraid2.sys [41016]

O58 - SDL:[MD5.A99C6C8B0BAA970D8AA59DDC50B57F94] - 21/01/2008 - 03:23:26 ---A- . (.Silicon Integrated Systems - SiS AHCI Stor-Miniport Driver.) -- C:\Windows\System32\Drivers\sisraid4.sys [74808]

O58 - SDL:[MD5.7B75299A4D201D6A6533603D6914AB04] - 11/04/2009 - 05:45:22 ---A- . (.Microsoft Corporation - SMB Transport driver.) -- C:\Windows\System32\Drivers\smb.sys [66560]

O58 - SDL:[MD5.A7D7EA1771D2ED6F39A8063E79B6C3E8] - 21/01/2008 - 03:24:55 ---A- . (.Microsoft Corporation - Smard Card Driver Library.) -- C:\Windows\System32\Drivers\smclib.sys [17408]

O58 - SDL:[MD5.C8A58FC905C9184FA70E37F71060C64D] - 02/11/2006 - 08:41:49 ---A- . (.Motorola Inc. - Motorola SM56 Modem WDM Driver.) -- C:\Windows\System32\Drivers\smserial.sys [1010560]

O58 - SDL:[MD5.7AEBDEEF071FE28B0EEF2CDD69102BFF] - 21/01/2008 - 03:24:11 ---A- . (.Microsoft Corporation - loader for security processor.) -- C:\Windows\System32\Drivers\spldr.sys [21048]

O58 - SDL:[MD5.A7F8BAD9590ADDC425B4003E94780DFA] - 11/04/2009 - 03:52:40 ---A- . (.Microsoft Corporation - security processor.) -- C:\Windows\System32\Drivers\spsys.sys [684032]

O58 - SDL:[MD5.41987F9FC0E61ADF54F581E15029AD91] - 18/02/2011 - 15:03:32 ---A- . (.Microsoft Corporation - Server driver.) -- C:\Windows\System32\Drivers\srv.sys [305152]

O58 - SDL:[MD5.FF33AFF99564B1AA534F58868CBE41EF] - 29/04/2011 - 14:25:10 ---A- . (.Microsoft Corporation - Smb 2.0 Server driver.) -- C:\Windows\System32\Drivers\srv2.sys [146432]

O58 - SDL:[MD5.7605C0E1D01A08F3ECD743F38B834A44] - 29/04/2011 - 14:25:09 ---A- . (.Microsoft Corporation - Server Network driver.) -- C:\Windows\System32\Drivers\srvnet.sys [102400]

O58 - SDL:[MD5.A36EE93698802CD899F98BFD553D8185] - 27/08/2012 - 14:50:24 ---A- . (.Avira GmbH - AVIRA SnapShot Driver.) -- C:\Windows\System32\Drivers\ssmdrv.sys [28520]

O58 - SDL:[MD5.47E55AFE1ED1D5AFF09690DB226F4A7A] - 11/04/2009 - 07:32:54 ---A- . (.Microsoft Corporation - Microsoft Storage Port Driver.) -- C:\Windows\System32\Drivers\Storport.sys [122344]

O58 - SDL:[MD5.70A92E46A2F459CDEDE3CA558CB26B6A] - 11/04/2009 - 05:42:47 ---A- . (.Microsoft Corporation - WDM CODEC Class Device Driver 2.0.) -- C:\Windows\System32\Drivers\stream.sys [52992]

O58 - SDL:[MD5.7BA58ECF0C0A9A69D44B3DCA62BECF56] - 21/01/2008 - 03:23:01 ---A- . (.Microsoft Corporation - Plug and Play Software Device Enumerator.) -- C:\Windows\System32\Drivers\swenum.sys [15288]

O58 - SDL:[MD5.192AA3AC01DF071B541094F251DEED10] - 02/11/2006 - 10:50:05 ---A- . (.LSI Logic - LSI Logic 8XX SCSI Miniport Driver.) -- C:\Windows\System32\Drivers\symc8xx.sys [35944]

O58 - SDL:[MD5.8C8EB8C76736EBAF3B13B633B2E64125] - 02/11/2006 - 10:49:56 ---A- . (.LSI Logic - LSI Logic Hi-Perf SCSI Miniport Driver.) -- C:\Windows\System32\Drivers\sym\_hi.sys [31848]

O58 - SDL:[MD5.8072AF52B5FD103BBBA387A1E49F62CB] - 02/11/2006 - 10:50:03 ---A- . (.LSI Logic - LSI Logic Ultra160 SCSI Miniport Driver.) -- C:\Windows\System32\Drivers\sym\_u3.sys [34920]

O58 - SDL:[MD5.BE78198C69135EF1FA157E08FD5C90FF] - 03/07/2008 - 09:30:13 ---A- . (.Synaptics, Inc. - Synaptics Touchpad Driver.) -- C:\Windows\System32\Drivers\SynTP.sys [200112]

O58 - SDL:[MD5.1239FD18895040D97B7CDBC19BC2075E] - 21/01/2008 - 03:24:44 ---A- . (.Microsoft Corporation - SCSI Tape Class Driver.) -- C:\Windows\System32\Drivers\tape.sys [24576]

O58 - SDL:[MD5.D18D53974FD715D50FC76F9FFE1C830D] - 05/07/2013 - 05:53:33 ---A- . (.Microsoft Corporation - TCP/IP Driver.) -- C:\Windows\System32\Drivers\tcpip.sys [905664]

O58 - SDL:[MD5.608C345A255D82A6289C2D468EB41FD7] - 08/12/2009 - 18:26:18 ---A- . (.Microsoft Corporation - TCP/IP Registry Compatibility Driver.) -- C:\Windows\System32\Drivers\tcpipreg.sys [30720]

O58 - SDL:[MD5.77937EFF009AC696B90E09F671F9D0A4] - 21/01/2008 - 03:24:05 ---A- . (.Microsoft Corporation - TDI Wrapper.) -- C:\Windows\System32\Drivers\tdi.sys [20992]

O58 - SDL:[MD5.5DCF5E267BE67A1AE926F2DF77FBCC56] - 21/01/2008 - 03:24:08 ---A- . (.Microsoft Corporation - Named Pipe Transport Driver.) -- C:\Windows\System32\Drivers\tdpipe.sys [17920]

O58 - SDL:[MD5.389C63E32B3CEFED425B61ED92D3F021] - 21/01/2008 - 03:24:08 ---A- . (.Microsoft Corporation - TCP Transport Driver.) -- C:\Windows\System32\Drivers\tdtcp.sys [29184]

O58 - SDL:[MD5.76B06EB8A01FC8624D699E7045303E54] - 11/04/2009 - 05:45:56 ---A- . (.Microsoft Corporation - TDI Translation Driver.) -- C:\Windows\System32\Drivers\tdx.sys [72192]

O58 - SDL:[MD5.3CAD38910468EAB9A6479E2F01DB43C7] - 11/04/2009 - 07:32:52 ---A- . (.Microsoft Corporation - Terminal Server Driver.) -- C:\Windows\System32\Drivers\termdd.sys [53224]

O58 - SDL:[MD5.F4EAA7ECBCB25DE901C9B7F2CDCDA0B3] - 15/06/2013 - 12:23:33 ---A- . (.Microsoft Corporation - TS Security Filter Driver.) -- C:\Windows\System32\Drivers\tssecsrv.sys [24064]

O58 - SDL:[MD5.CAECC0120AC49E3D2F758B9169872D38] - 21/01/2008 - 03:24:25 ---A- . (.Microsoft Corporation - Microsoft Tunnel Interface Driver.) -- C:\Windows\System32\Drivers\TUNMP.SYS [15360]

O58 - SDL:[MD5.300DB877AC094FEAB0BE7688C3454A9C] - 18/02/2010 - 12:28:13 ---A- . (.Microsoft Corporation - Microsoft Tunnel Interface Driver.) -- C:\Windows\System32\Drivers\tunnel.sys [25088]

O58 - SDL:[MD5.7D33C4DB2CE363C8518D2DFCF533941F] - 21/01/2008 - 03:23:22 ---A- . (.Microsoft Corporation - Filtre MS AGPv3.5.) -- C:\Windows\System32\Drivers\UAGP35.SYS [59448]

O58 - SDL:[MD5.D9728AF68C4C7693CB100B8441CBDEC6] - 11/04/2009 - 05:13:59 ---A- . (.Microsoft Corporation - UDF File System Driver.) -- C:\Windows\System32\Drivers\udfs.sys [226816]

O58 - SDL:[MD5.B0ACFDC9E4AF279E9116C03E014B2B27] - 21/01/2008 - 03:23:01 ---A- . (.Microsoft Corporation - Filtre ULi AGPv3.0 pour plateformes à processeur K8/9.) -- C:\Windows\System32\Drivers\ULIAGPKX.SYS [60984]

O58 - SDL:[MD5.9224BB254F591DE4CA8D572A5F0D635C] - 21/01/2008 - 03:23:20 ---A- . (.ULi Electronics Inc. - ULi SATA Controller Driver.) -- C:\Windows\System32\Drivers\uliahci.sys [238648]

O58 - SDL:[MD5.8514D0E5CD0534467C5FC61BE94A569F] - 02/11/2006 - 10:50:35 ---A- . (.Promise Technology, Inc. - Promise Ultra/Sata Series Driver for Win2003.) -- C:\Windows\System32\Drivers\ulsata.sys [98408]

O58 - SDL:[MD5.38C3C6E62B157A6BC46594FADA45C62B] - 21/01/2008 - 03:23:23 ---A- . (.Promise Technology, Inc. - Promise SATAII150 Series Windows Drivers.) -- C:\Windows\System32\Drivers\ulsata2.sys [115816]

O58 - SDL:[MD5.32CFF9F809AE9AED85464492BF3E32D2] - 21/01/2008 - 03:23:22 ---A- . (.Microsoft Corporation - User-Mode Bus Enumerator.) -- C:\Windows\System32\Drivers\umbus.sys [34816]

O58 - SDL:[MD5.88BD96A1BAEED33EE8BDF9499C07A841] - 21/01/2008 - 03:23:49 ---A- . (.Microsoft Corporation - Generic pass-through driver.) -- C:\Windows\System32\Drivers\umpass.sys [7680]

O58 - SDL:[MD5.8D31A140B55021BBD3A608F5A7AA2E18] - 12/02/2013 - 02:57:27 ---A- . (.Microsoft Corporation - Remote NDIS USB Driver.) -- C:\Windows\System32\Drivers\usb8023.sys [15872]

O58 - SDL:[MD5.D06F193F3E9CC3B356DF97F6A43C054A] - 11/04/2009 - 05:42:56 ---A- . (.Microsoft Corporation - Universal Serial Bus Camera Driver.) -- C:\Windows\System32\Drivers\USBCAMD.sys [25856]

O58 - SDL:[MD5.EAE017D3AA298374A1967B96C379C5AB] - 11/04/2009 - 05:42:56 ---A- . (.Microsoft Corporation - Universal Serial Bus Camera Driver.) -- C:\Windows\System32\Drivers\USBCAMD2.sys [25856]

O58 - SDL:[MD5.AAB0B5F72D2D726FBFDC895A2902DE1D] - 29/06/2013 - 03:07:04 ---A- . (.Microsoft Corporation - USB Common Class Generic Parent Driver.) -- C:\Windows\System32\Drivers\usbccgp.sys [73216]

O58 - SDL:[MD5.E9476E6C486E76BC4898074768FB7131] - 02/11/2006 - 09:55:09 ---A- . (.Microsoft Corporation - USB Consumer IR Driver for eHome.) -- C:\Windows\System32\Drivers\usbcir.sys [68608]

O58 - SDL:[MD5.FE619ED13CE12F5B43C04E3EA061BBD6] - 29/06/2013 - 03:06:53 ---A- . (.Microsoft Corporation - Universal Serial Bus Driver.) -- C:\Windows\System32\Drivers\usbd.sys [6016]

O58 - SDL:[MD5.153E8515CB86F8BB5D1A8B478EBF4BB2] - 05/05/2011 - 14:54:07 ---A- . (.Microsoft Corporation - EHCI eUSB Miniport Driver.) -- C:\Windows\System32\Drivers\usbehci.sys [39936]

O58 - SDL:[MD5.2AE6BCEBD85D31317E433733DAF25888] - 29/06/2013 - 03:07:15 ---A- . (.Microsoft Corporation - Default Hub Driver for USB.) -- C:\Windows\System32\Drivers\usbhub.sys [197632]

O58 - SDL:[MD5.38DBC7DD6CC5A72011F187425384388B] - 02/11/2006 - 09:55:05 ---A- . (.Microsoft Corporation - OHCI USB Miniport Driver.) -- C:\Windows\System32\Drivers\usbohci.sys [19456]

O58 - SDL:[MD5.B09C74A41F26B08149707EA5E7F956C2] - 29/06/2013 - 03:07:01 ---A- . (.Microsoft Corporation - USB 1.1 & 2.0 Port Driver.) -- C:\Windows\System32\Drivers\usbport.sys [226304]

O58 - SDL:[MD5.B51E52ACF758BE00EF3A58EA452FE360] - 02/11/2006 - 10:14:58 ---A- . (.Microsoft Corporation - USB Printer driver.) -- C:\Windows\System32\Drivers\usbprint.sys [18944]

O58 - SDL:[MD5.BE3DA31C191BC222D9AD503C5224F2AD] - 11/04/2009 - 05:42:55 ---A- . (.Microsoft Corporation - USB Mass Storage Class Driver.) -- C:\Windows\System32\Drivers\USBSTOR.SYS [65536]

O58 - SDL:[MD5.44056325428A8E4C755830426E29878F] - 05/05/2011 - 14:54:07 ---A- . (.Microsoft Corporation - UHCI USB Miniport Driver.) -- C:\Windows\System32\Drivers\usbuhci.sys [23552]

O58 - SDL:[MD5.E67998E8F14CB0627A769F6530BCB352] - 21/01/2008 - 03:23:26 ---A- . (.Microsoft Corporation - USB Video Class Driver.) -- C:\Windows\System32\Drivers\usbvideo.sys [134016]

O58 - SDL:[MD5.2E93AC0A1D8C79D019DB6C51F036636C] - 21/01/2008 - 03:24:50 ---A- . (.Microsoft Corporation - VGA/Super VGA Video Driver.) -- C:\Windows\System32\Drivers\vga.sys [25088]

O58 - SDL:[MD5.87B06E1F30B749A114F74622D013F8D4] - 21/01/2008 - 03:23:02 ---A- . (.Microsoft Corporation - VGA/Super VGA Video Driver.) -- C:\Windows\System32\Drivers\vgapnp.sys [26112]

O58 - SDL:[MD5.5D7159DEF58A800D5781BA3A879627BC] - 21/01/2008 - 03:23:01 ---A- . (.Microsoft Corporation - Filtre VIA NT AGP.) -- C:\Windows\System32\Drivers\VIAAGP.SYS [56888]

O58 - SDL:[MD5.C4F3A691B5BAD343E6249BD8C2D45DEE] - 21/01/2008 - 03:23:00 ---A- . (.Microsoft Corporation - Processor Device Driver.) -- C:\Windows\System32\Drivers\viac7.sys [41472]

O58 - SDL:[MD5.AADF5587A4063F52C2C3FED7887426FC] - 21/01/2008 - 03:23:00 ---A- . (.VIA Technologies, Inc. - VIA Generic PCI IDE Bus Driver.) -- C:\Windows\System32\Drivers\viaide.sys [20024]

O58 - SDL:[MD5.C048D2C33D27441A0CDCAAE2651EB03D] - 21/01/2008 - 03:23:42 ---A- . (.Microsoft Corporation - Video Port Driver.) -- C:\Windows\System32\Drivers\videoprt.sys [110080]

O58 - SDL:[MD5.69503668AC66C77C6CD7AF86FBDF8C43] - 21/01/2008 - 03:23:01 ---A- . (.Microsoft Corporation - Volume Manager Driver.) -- C:\Windows\System32\Drivers\volmgr.sys [52792]

O58 - SDL:[MD5.23E41B834759917BFD6B9A0D625D0C28] - 11/04/2009 - 07:33:03 ---A- . (.Microsoft Corporation - Volume Manager Extension Driver.) -- C:\Windows\System32\Drivers\volmgrx.sys [292840]

O58 - SDL:[MD5.786DB5771F05EF300390399F626BF30A] - 21/08/2012 - 12:47:42 ---A- . (.Microsoft Corporation - Pilote de cliché instantané du volume.) -- C:\Windows\System32\Drivers\volsnap.sys [224640]

O58 - SDL:[MD5.587253E09325E6BF226B299774B728A9] - 21/01/2008 - 03:23:23 ---A- . (.VIA Technologies Inc.,Ltd - VIA RAID DRIVER FOR AMD-X86-64.) -- C:\Windows\System32\Drivers\vsmraid.sys [130616]

O58 - SDL:[MD5.48DFEE8F1AF7C8235D4E626F0C4FE031] - 02/11/2006 - 09:52:52 ---A- . (.Microsoft Corporation - Wacom Serial Pen Tablet HID Driver.) -- C:\Windows\System32\Drivers\wacompen.sys [20608]

O58 - SDL:[MD5.55201897378CCA7AF8B5EFD874374A26] - 21/01/2008 - 03:24:25 ---A- . (.Microsoft Corporation - MS Remote Access and Routing ARP Driver.) -- C:\Windows\System32\Drivers\wanarp.sys [62464]

O58 - SDL:[MD5.4A5C31E2C1646034E6A60EBA4C747FF6] - 11/04/2009 - 05:22:46 ---A- . (.Microsoft Corporation - Watchdog Driver.) -- C:\Windows\System32\Drivers\watchdog.sys [33280]

O58 - SDL:[MD5.78FE9542363F297B18C027B2D7E7C07F] - 21/01/2008 - 03:23:24 ---A- . (.Microsoft Corporation - Microsoft Watchdog Timer Driver.) -- C:\Windows\System32\Drivers\wd.sys [22072]

O58 - SDL:[MD5.25944D2CC49E0A6C581D02A74B7D6645] - 27/06/2013 - 00:01:59 ---A- . (.Microsoft Corporation - Runtime de l’infrastructure de pilotes en mode noyau.) -- C:\Windows\System32\Drivers\Wdf01000.sys [527064]

O58 - SDL:[MD5.48704647CD2E9DAA2EB81BDE6D029EDB] - 26/07/2012 - 04:39:21 ---A- . (.Microsoft Corporation - Kernel Mode Driver Framework Loader.) -- C:\Windows\System32\Drivers\WdfLdr.sys [47720]

O58 - SDL:[MD5.2E7255D172DF0B8283CDFB7B433B864E] - 21/01/2008 - 03:23:00 ---A- . (.Microsoft Corporation - Windows Management Interface for ACPI.) -- C:\Windows\System32\Drivers\wmiacpi.sys [11264]

O58 - SDL:[MD5.C546864EED786304762D030FEBF6B411] - 21/01/2008 - 03:23:42 ---A- . (.Microsoft Corporation - WMILIB WMI support library Dll.) -- C:\Windows\System32\Drivers\wmilib.sys [17976]

O58 - SDL:[MD5.DE9D36F91A4DF3D911626643DEBF11EA] - 01/10/2009 - 02:01:54 ---A- . (.Microsoft Corporation - WPD USB Driver.) -- C:\Windows\System32\Drivers\WpdUsb.sys [40448]

O58 - SDL:[MD5.E3A3CB253C0EC2494D4A61F5E43A389C] - 21/01/2008 - 03:24:47 ---A- . (.Microsoft Corporation - Winsock2 IFS Layer.) -- C:\Windows\System32\Drivers\ws2ifsl.sys [15872]

O58 - SDL:[MD5.06E6F32C8D0A3F66D956F57B43A2E070] - 26/07/2012 - 03:33:43 ---A- . (.Microsoft Corporation - Windows Driver Foundation - User-mode Driver Framework Platform.) -- C:\Windows\System32\Drivers\WUDFPf.sys [66560]

O58 - SDL:[MD5.867C301E8B790040AE9CF6486E8041DF] - 26/07/2012 - 03:32:51 ---A- . (.Microsoft Corporation - Windows Driver Foundation - User-mode Driver Framework Reflecto.) -- C:\Windows\System32\Drivers\WUDFRd.sys [155136]

O58 - SDL:[MD5.7D1F3B131D503EF43EE594B5A2B9B427] - 02/11/2006 - 08:30:56 ---A- . (.Marvell - Pilote miniport NDIS6.0 pour contrôleur Ethernet Marvell Yukon.) -- C:\Windows\System32\Drivers\yk60x86.sys [194048]

O58 - SDL:[MD5.8AAD333C876590293F72B315E162BCC7] - 02/11/2006 - 08:09:42 ---A- . (...) -- C:\Windows\System32\ANSI.SYS [9029]

O58 - SDL:[MD5.4DF523F49694B2884F8E5D870BF3E253] - 06/04/2008 - 03:56:08 ---A- . (.Atheros Communications, Inc. - Atheros Extensible Wireless LAN device driver.) -- C:\Windows\System32\athr.sys [908800]

O58 - SDL:[MD5.D7659D3B5B92C31E84E53C1431F35132] - 11/04/2009 - 07:32:46 ---A- . (.Microsoft Corporation - Common Log File System Driver.) -- C:\Windows\System32\clfs.sys [245736]

O58 - SDL:[MD5.0FE9F16075C9ACB941C957B7C649176E] - 02/11/2006 - 08:09:45 ---A- . (...) -- C:\Windows\System32\country.sys [27097]

O58 - SDL:[MD5.E6BC0F98FECEF245A0010D350C1A0B9B] - 02/11/2006 - 08:09:41 ---A- . (...) -- C:\Windows\System32\HIMEM.SYS [4768]

O58 - SDL:[MD5.492090267B9608C62B956CD29BE3AFB7] - 02/11/2006 - 08:09:44 ---A- . (...) -- C:\Windows\System32\KEY01.SYS [42809]

O58 - SDL:[MD5.FBBCFEC1379C5C02D88A361993EDF1B8] - 02/11/2006 - 08:09:44 ---A- . (...) -- C:\Windows\System32\KEYBOARD.SYS [42537]

O58 - SDL:[MD5.FFFF296A08DBF2AC0126C62E3778AC0D] - 02/11/2006 - 08:09:29 ---A- . (...) -- C:\Windows\System32\NTDOS.SYS [27866]

O58 - SDL:[MD5.CF9ED169FF86D935E47999E82359E898] - 02/11/2006 - 08:09:35 ---A- . (...) -- C:\Windows\System32\NTDOS404.SYS [29146]

O58 - SDL:[MD5.03B945AC0481CD8BB161C3569D8ED1C3] - 02/11/2006 - 08:09:38 ---A- . (...) -- C:\Windows\System32\NTDOS411.SYS [29370]

O58 - SDL:[MD5.BBC957DC18C17CC027EB80B7C77F2AEA] - 02/11/2006 - 08:09:40 ---A- . (...) -- C:\Windows\System32\NTDOS412.SYS [29274]

O58 - SDL:[MD5.3CFFAEFFF23B0D208214A6D3061A5B1B] - 02/11/2006 - 08:09:31 ---A- . (...) -- C:\Windows\System32\NTDOS804.SYS [29146]

O58 - SDL:[MD5.2E4112FB7D1B76E11ADFD7487B5D0E95] - 02/11/2006 - 08:09:20 ---A- . (...) -- C:\Windows\System32\NTIO.SYS [33952]

O58 - SDL:[MD5.A98EBD4C2DF983665BF2D1AF49949974] - 02/11/2006 - 08:09:23 ---A- . (...) -- C:\Windows\System32\NTIO404.SYS [34672]

O58 - SDL:[MD5.3F7E6406EDEF197C5CAAB2240EEF6F48] - 02/11/2006 - 08:09:24 ---A- . (...) -- C:\Windows\System32\NTIO411.SYS [35776]

O58 - SDL:[MD5.3E64D681B776CC57BDC38A46D881F85B] - 02/11/2006 - 08:09:26 ---A- . (...) -- C:\Windows\System32\NTIO412.SYS [35536]

O58 - SDL:[MD5.D86B6435729231C171432B4E77801BDB] - 02/11/2006 - 08:09:22 ---A- . (...) -- C:\Windows\System32\NTIO804.SYS [34672]

O58 - SDL:[MD5.A6E18756EA7B6E971184B57B86251FC5] - 30/10/2013 - 01:35:24 ---A- . (.Microsoft Corporation - Pilote Win32 multi-utilisateurs.) -- C:\Windows\System32\win32k.sys [2050560]

~ Drivers: 16 Scanned in 04mn 08s

---\\ Derniers fichiers modifiés ou crées (Utilisateur) (O61)

O61 - LFC: 01/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor [18432]

O61 - LFC: 01/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor-journal [15992]

O61 - LFC: 01/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Pepper Data\Shockwave Flash\WritableRoot\#SharedObjects\W5LB55NC\live.sekindo.com\##78CC5CD70E98ABF3\00000001.sol [175]

O61 - LFC: 01/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Pepper Data\Shockwave Flash\WritableRoot\#SharedObjects\W5LB55NC\macromedia.com\support\flashplayer\sys\#live.sekindo.com\settings.sol [86]

O61 - LFC: 01/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Pepper Data\Shockwave Flash\WritableRoot\#SharedObjects\W5LB55NC\macromedia.com\support\flashplayer\sys\settings.sol [437]

O61 - LFC: 01/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Shortcuts [12288]

O61 - LFC: 01/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Shortcuts-journal [12824]

O61 - LFC: 01/03/2014 - 21:13:48 ---A- . (.Robert Simpson, et al..) -- C:\Users\RONDEAU\AppData\Local\Temp\System.Data.SQLite12565.dll [1053184]

O61 - LFC: 01/03/2014 - 21:13:48 ---A- . (.Robert Simpson, et al..) -- C:\Users\RONDEAU\AppData\Local\Temp\System.Data.SQLite55689.dll [1053184]

O61 - LFC: 01/03/2014 - 21:13:48 ---A- . (.Robert Simpson, et al..) -- C:\Users\RONDEAU\AppData\Local\Temp\System.Data.SQLite93419.dll [1053184]

O61 - LFC: 01/03/2014 - 21:13:54 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Malwarebytes\Malwarebytes' Anti-Malware\Logs\mbam-log-2014-03-01 (13-24-30).txt [2348]

O61 - LFC: 01/03/2014 - 21:13:54 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Malwarebytes\Malwarebytes' Anti-Malware\Logs\mbam-log-2014-03-01 (17-23-32).txt [2198]

O61 - LFC: 02/03/2014 - 21:13:04 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\DoNotTrackPlus\dntp-optout.bin [9883]

O61 - LFC: 02/03/2014 - 21:13:04 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\DoNotTrackPlus\optout.json [13066]

O61 - LFC: 02/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\Application\First Run [0]

O61 - LFC: 02/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\Application\VisualElementsManifest.xml [399]

O61 - LFC: 02/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies [6144]

O61 - LFC: 02/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies-journal [3608]

O61 - LFC: 02/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extension State\000081.ldb [196]

O61 - LFC: 02/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\idhngdhcfkoamngbedgpaokgjbnpdiji\1.3.3\_1\background.html [231]

O61 - LFC: 02/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\idhngdhcfkoamngbedgpaokgjbnpdiji\1.3.3\_1\contentscript.js [7999]

O61 - LFC: 02/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\idhngdhcfkoamngbedgpaokgjbnpdiji\1.3.3\_1\manifest.json [644]

O61 - LFC: 02/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\mikhcaiakabeeokmenglcdebplfdjicn\1.0\_1\background.js [274]

O61 - LFC: 02/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\mikhcaiakabeeokmenglcdebplfdjicn\1.0\_1\manifest.json [717]

O61 - LFC: 02/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\mikhcaiakabeeokmenglcdebplfdjicn\1.0\_1\script.js [2905]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\128.png [5920]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\ar\messages.json [312]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\bg\messages.json [292]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\ca\messages.json [254]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\cs\messages.json [249]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\da\messages.json [236]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\de\messages.json [239]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\el\messages.json [332]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\en\messages.json [215]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\es\messages.json [269]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\fi\messages.json [256]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\fil\messages.json [234]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\fr\messages.json [268]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\hi\messages.json [289]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\hr\messages.json [230]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\hu\messages.json [226]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\id\messages.json [242]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\it\messages.json [256]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\ja\messages.json [271]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\ko\messages.json [256]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\lt\messages.json [253]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\lv\messages.json [238]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\nl\messages.json [232]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\no\messages.json [210]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\pl\messages.json [264]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\pt\_BR\messages.json [222]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\pt\_PT\messages.json [223]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\ro\messages.json [265]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\ru\messages.json [286]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\se\messages.json [210]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\sk\messages.json [222]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\sl\messages.json [234]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\sr\messages.json [295]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\th\messages.json [324]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\tr\messages.json [234]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\uk\messages.json [304]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\vi\messages.json [232]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\zh\_CN\messages.json [258]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\\_locales\zh\_TW\messages.json [249]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\7\_0\manifest.json [755]

O61 - LFC: 02/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Google Profile.ico [181623]

O61 - LFC: 02/03/2014 - 21:13:19 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\AviraLog.txt [2916]

O61 - LFC: 02/03/2014 - 21:13:19 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\kl-install-2014-03-02-19-42-07.log.enc1 [7286708]

O61 - LFC: 02/03/2014 - 21:13:19 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\kl-preinstall-2014-03-02-19-39-27.log.enc1 [528122]

O61 - LFC: 02/03/2014 - 21:13:19 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\kl-setup-2014-03-02-19-38-27.log.enc1 [2382956]

O61 - LFC: 02/03/2014 - 21:13:19 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\kl-setup-2014-03-02-20-02-00.log.enc1 [42420]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo000.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo001.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo002.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo003.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo004.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo005.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo006.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo007.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo008.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo009.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo010.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo011.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo012.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo013.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo014.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo015.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo016.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo017.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo018.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo019.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo020.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo021.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo022.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo023.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo024.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo025.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo026.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo027.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\Messenger Companion\compo028.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:42 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Low\iexplore.exe\_\_611cb8ad5bb741e52033d5b7bac64fe5.dmp [198642]

O61 - LFC: 02/03/2014 - 21:13:43 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Messenger Companion\compo000.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:43 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Messenger Companion\compo001.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:43 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Messenger Companion\compo002.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:43 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Messenger Companion\compo003.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:43 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Messenger Companion\compo004.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:43 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Messenger Companion\compo005.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:43 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Messenger Companion\compo006.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:43 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Messenger Companion\compo007.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:43 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Messenger Companion\compo008.sqm [380]

O61 - LFC: 02/03/2014 - 21:13:51 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\wmplog07.sqm [1858]

O61 - LFC: 02/03/2014 - 21:13:51 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\wmplog08.sqm [1594]

O61 - LFC: 02/03/2014 - 21:13:52 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Windows Live\uxcore\_iexplore\_00.etl [8192]

O61 - LFC: 02/03/2014 - 21:13:52 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Windows Live\uxcore\_iexplore\_01.etl [8192]

O61 - LFC: 02/03/2014 - 21:13:52 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Windows Live\uxcore\_iexplore\_02.etl [8192]

O61 - LFC: 02/03/2014 - 21:13:52 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Windows Live\uxcore\_iexplore\_03.etl [8192]

O61 - LFC: 02/03/2014 - 21:13:52 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Windows Live\uxcore\_iexplore\_04.etl [8192]

O61 - LFC: 02/03/2014 - 21:13:55 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Network\Connections\Pbk\rasphone.pbk [0]

O61 - LFC: 02/03/2014 - 21:13:56 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\UserTile.png [24206]

O61 - LFC: 02/03/2014 - 21:13:56 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\ZHP\ZHPADSReport.txt [351] =>.Nicolas Coolman

O61 - LFC: 02/03/2014 - 21:13:56 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\ZHP\ZHPDiag.txt [310203] =>.Nicolas Coolman

O61 - LFC: 02/03/2014 - 21:14:30 ---A- . (...) -- C:\Users\RONDEAU\Contacts\RONDEAU.contact [45960]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\Application\Dictionaries\fr-FR-3-0.bdic [1074744]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Certificate Revocation Lists [270670]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Bookmarks [1153]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Bookmarks.bak [1153]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Cookies [152576]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal [16384]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Current Session [23489]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Current Tabs [7843]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extension State\000124.ldb [245]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extension State\000126.ldb [259]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extension State\CURRENT [16]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG [269]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old [777]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extension State\MANIFEST-000125 [490] =>.Google Inc

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\ar\messages.json [246]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\bg\messages.json [264]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\ca\messages.json [207]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\cs\messages.json [222]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\da\messages.json [216]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\de\messages.json [217]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\el\messages.json [260]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\en\_GB\messages.json [208]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\en\_US\messages.json [209]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\es\messages.json [206]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\es\_419\messages.json [206]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\et\messages.json [216]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\fi\messages.json [216]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\fil\messages.json [219]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\fr\messages.json [220]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\he\messages.json [221]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\hi\messages.json [279]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\hu\messages.json [235]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\id\messages.json [209]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\it\messages.json [213]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\ja\messages.json [221]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\icon\_128.png [3009]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\icon\_16.png [143]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\main.html [92]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\main.js [98]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\manifest.json [724]

O61 - LFC: 03/03/2014 - 21:13:05 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\chrome\_shutdown\_ms.txt [4]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\ko\messages.json [218]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\lt\messages.json [228]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\lv\messages.json [224]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\ms\messages.json [207]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\nl\messages.json [217]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\no\messages.json [195]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\pl\messages.json [213]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\pt\_BR\messages.json [206]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\pt\_PT\messages.json [208]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\ro\messages.json [213]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\ru\messages.json [266]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\sk\messages.json [221]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\sl\messages.json [218]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\sr\messages.json [248]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\sv\messages.json [214]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\th\messages.json [254]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\tr\messages.json [227]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\uk\messages.json [264]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\vi\messages.json [225]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\zh\_CN\messages.json [206]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.5\_0\\_locales\zh\_TW\messages.json [206]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\128.png [7654]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\ar\messages.json [278]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\bg\messages.json [319]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\ca\messages.json [265]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\cs\messages.json [259]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\da\messages.json [243]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\de\messages.json [256]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\el\messages.json [329]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\en\_GB\messages.json [249]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\en\_US\messages.json [249]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\es\messages.json [259]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\es\_419\messages.json [259]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\et\messages.json [251]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\eu\messages.json [243]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\fi\messages.json [257]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\fil\messages.json [260]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\fr\messages.json [252]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\he\messages.json [278]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\hi\messages.json [345]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\hr\messages.json [263]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\hu\messages.json [264]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\id\messages.json [261]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\it\messages.json [258]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\ja\messages.json [293]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\ko\messages.json [281]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\lt\messages.json [285]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\lv\messages.json [258]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\ms\messages.json [254]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\nl\messages.json [242]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\no\messages.json [218]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\pl\messages.json [257]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\pt\_BR\messages.json [246]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\pt\_PT\messages.json [264]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\ro\messages.json [281]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\ru\messages.json [338]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\sk\messages.json [274]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\sl\messages.json [268]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\sr\messages.json [287]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\sv\messages.json [253]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\th\messages.json [356]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\tr\messages.json [270]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\uk\messages.json [353]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\vi\messages.json [279]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\zh\_CN\messages.json [273]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\\_locales\zh\_TW\messages.json [267]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf\6.3\_0\manifest.json [996]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\128.png [3524]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\ar\messages.json [257]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\bg\messages.json [267]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\ca\messages.json [234]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\cs\messages.json [231]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\da\messages.json [230]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\de\messages.json [226]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\el\messages.json [283]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\en\messages.json [227]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\es\messages.json [232]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\fi\messages.json [218]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\fil\messages.json [236]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\fr\messages.json [241]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\he\messages.json [263]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\hi\messages.json [297]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\hr\messages.json [220]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\hu\messages.json [229]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\id\messages.json [231]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\it\messages.json [220]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\ja\messages.json [268]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\ko\messages.json [254]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\lt\messages.json [246]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\lv\messages.json [229]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\nl\messages.json [225]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\no\messages.json [216]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\pl\messages.json [250]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\pt\_BR\messages.json [233]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\pt\_PT\messages.json [232]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\ro\messages.json [240]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\ru\messages.json [254]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\sk\messages.json [229]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\sl\messages.json [245]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\sr\messages.json [269]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\sv\messages.json [226]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\th\messages.json [272]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\tr\messages.json [231]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\uk\messages.json [270]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\vi\messages.json [263]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\zh\_CN\messages.json [218]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\\_locales\zh\_TW\messages.json [224]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo\4.2.6\_0\manifest.json [785]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\128.png [5367]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\16.png [499]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\32.png [1154]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\48.png [1872]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\ar\messages.json [327]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\bg\messages.json [359]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\ca\messages.json [322]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\cs\messages.json [331]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\da\messages.json [316]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\de\messages.json [307]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\el\messages.json [377]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\en\messages.json [314]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\en\_GB\messages.json [314]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\en\_US\messages.json [314]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\es\messages.json [328]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\es\_419\messages.json [329]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\et\messages.json [314]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\fi\messages.json [305]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\fil\messages.json [337]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\fr\messages.json [325]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\he\messages.json [343]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\hi\messages.json [317]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\hr\messages.json [324]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\hu\messages.json [324]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\id\messages.json [319]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\it\messages.json [320]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\ja\messages.json [331]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\ko\messages.json [329]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\lt\messages.json [333]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\lv\messages.json [328]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\nl\messages.json [323]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\no\messages.json [300]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\pl\messages.json [328]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\pt\_BR\messages.json [328]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\pt\_PT\messages.json [327]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\ro\messages.json [324]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\ru\messages.json [343]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\sk\messages.json [318]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\sl\messages.json [321]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\sr\messages.json [347]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\sv\messages.json [317]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\th\messages.json [373]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\tr\messages.json [318]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\uk\messages.json [353]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\vi\messages.json [331]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\zh\_CN\messages.json [310]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\\_locales\zh\_TW\messages.json [310]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\coobgpohoikkiipiblmjeljniedjpjpf\0.0.0.20\_0\manifest.json [817]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\craw\_background.js [126613]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\craw\_window.js [156903]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\css\craw\_window.css [1741]

O61 - LFC: 03/03/2014 - 21:13:06 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\html\craw\_window.html [810]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\bg\messages.json [833]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\ca\messages.json [658]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\cs\messages.json [651]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\da\messages.json [633]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\de\messages.json [698]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\el\messages.json [884]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\en\messages.json [611]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\en\_GB\messages.json [611]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\es\messages.json [685]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\es\_419\messages.json [647]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\et\messages.json [603]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\fi\messages.json [666]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\fil\messages.json [672]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\fr\messages.json [693]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\hi\messages.json [929]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\hr\messages.json [626]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\hu\messages.json [674]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\id\messages.json [612]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\it\messages.json [618]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\ja\messages.json [794]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\ko\messages.json [664]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\lt\messages.json [648]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\lv\messages.json [655]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\nb\messages.json [633]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\nl\messages.json [630]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\pl\messages.json [637]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\pt\_BR\messages.json [665]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\pt\_PT\messages.json [650]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\ro\messages.json [640]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\ru\messages.json [716]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\sk\messages.json [659]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\sl\messages.json [627]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\sr\messages.json [791]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\sv\messages.json [635]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\th\messages.json [1023]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\tr\messages.json [636]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\uk\messages.json [764]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\vi\messages.json [677]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\zh\_CN\messages.json [583]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\\_locales\zh\_TW\messages.json [610]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\images\icon\_128.png [9460]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\images\icon\_16.png [702]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\images\topbar\_floating\_button.png [160]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\images\topbar\_floating\_button\_close.png [252]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\images\topbar\_floating\_button\_hover.png [160]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\images\topbar\_floating\_button\_maximize.png [166]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\images\topbar\_floating\_button\_pressed.png [160]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\0.0.6.1\_1\manifest.json [1275]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Favicons [59392]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal [16384]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\File System\000\t\.usage [24]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\File System\000\t\00\00000000 [211]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\File System\000\t\00\00000001 [15027084]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\File System\000\t\Paths\000005.ldb [622]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\File System\000\t\Paths\CURRENT [16]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\File System\000\t\Paths\LOCK [0]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\File System\000\t\Paths\LOG [145]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\File System\000\t\Paths\LOG.old [142]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\File System\000\t\Paths\MANIFEST-000015 [86]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\000005.ldb [180]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\CURRENT [16]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\LOCK [0]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\LOG [145]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\LOG.old [145]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\MANIFEST-000015 [112]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\History [163840]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache [23779]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\History-journal [16384]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Last Session [91226]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Last Tabs [25748]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Local Storage\http\_c.betrad.com\_0.localstorage [74752]

O61 - LFC: 03/03/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Local Storage\http\_c.betrad.com\_0.localstorage-journal [3608]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Login Data [12288]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Login Data-journal [8736]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Origin Bound Certs [14336]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Origin Bound Certs-journal [3608]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Preferences [60732]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\QuotaManager [13312]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\QuotaManager-journal [8768]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000159.ldb [145]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Session Storage\CURRENT [16]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG [771]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old [271]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Session Storage\MANIFEST-000156 [472] =>.Google Inc

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Top Sites [69632]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Top Sites-journal [16384]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity [325]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Visited Links [131072]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Web Data [83968]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Web Data-journal [16384]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Local State [71028]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Safe Browsing Bloom [16599408]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Safe Browsing Bloom Prefix Set [2618202]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Safe Browsing Cookies [6144]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Safe Browsing Cookies-journal [4640]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Safe Browsing Csd Whitelist [135548]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Safe Browsing Download [1336740]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Safe Browsing Download Whitelist [30068]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\pnacl\0.1.0.12332\\_platform\_specific\x86\_32\pnacl\_public\_pnacl\_json [439]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\pnacl\0.1.0.12332\\_platform\_specific\x86\_32\pnacl\_public\_x86\_32\_crtbegin\_for\_eh\_o [1476]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\pnacl\0.1.0.12332\\_platform\_specific\x86\_32\pnacl\_public\_x86\_32\_crtbegin\_o [1564]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\pnacl\0.1.0.12332\\_platform\_specific\x86\_32\pnacl\_public\_x86\_32\_crtend\_o [981]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\pnacl\0.1.0.12332\\_platform\_specific\x86\_32\pnacl\_public\_x86\_32\_ld\_nexe [1854128]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\pnacl\0.1.0.12332\\_platform\_specific\x86\_32\pnacl\_public\_x86\_32\_libcrt\_platform\_a [4064]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\pnacl\0.1.0.12332\\_platform\_specific\x86\_32\pnacl\_public\_x86\_32\_libgcc\_a [37712]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\pnacl\0.1.0.12332\\_platform\_specific\x86\_32\pnacl\_public\_x86\_32\_libgcc\_eh\_a [148206]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\pnacl\0.1.0.12332\\_platform\_specific\x86\_32\pnacl\_public\_x86\_32\_libpnacl\_irt\_shim\_a [147672]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\pnacl\0.1.0.12332\\_platform\_specific\x86\_32\pnacl\_public\_x86\_32\_libpnacl\_irt\_shim\_dummy\_a [1310]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\pnacl\0.1.0.12332\\_platform\_specific\x86\_32\pnacl\_public\_x86\_32\_pnacl\_llc\_nexe [8163600]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\pnacl\0.1.0.12332\manifest.fingerprint [66]

O61 - LFC: 03/03/2014 - 21:13:08 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\pnacl\0.1.0.12332\manifest.json [572]

O61 - LFC: 03/03/2014 - 21:13:09 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Safe Browsing Extension Blacklist [24040]

O61 - LFC: 03/03/2014 - 21:13:09 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Safe Browsing IP Blacklist [1348]

O61 - LFC: 03/03/2014 - 21:13:09 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\SwiftShader\1.0.5.0\libEGL.dll [112128]

O61 - LFC: 03/03/2014 - 21:13:09 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\SwiftShader\1.0.5.0\libGLESv2.dll [4591616]

O61 - LFC: 03/03/2014 - 21:13:09 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\SwiftShader\1.0.5.0\manifest.fingerprint [9]

O61 - LFC: 03/03/2014 - 21:13:09 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\SwiftShader\1.0.5.0\manifest.json [202]

O61 - LFC: 03/03/2014 - 21:13:09 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Google Desktop\e45b5b5819ba\sites.txt [2418]

O61 - LFC: 03/03/2014 - 21:13:10 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Google Desktop\e45b5b5819ba\uinfo.dat [424960]

O61 - LFC: 03/03/2014 - 21:13:10 --HA- . (...) -- C:\Users\RONDEAU\AppData\Local\IconCache.db [3921940]

O61 - LFC: 03/03/2014 - 21:13:11 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\PowerCinema\CLML\CLDB\_SUB\_INFO.db [20182016]

O61 - LFC: 03/03/2014 - 21:13:17 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\12\_17910\crl-set [270670]

O61 - LFC: 03/03/2014 - 21:13:17 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\12\_17910\manifest.fingerprint [12]

O61 - LFC: 03/03/2014 - 21:13:17 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\12\_17910\manifest.json [34]

O61 - LFC: 03/03/2014 - 21:13:17 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Administrateur.bmp [32848]

O61 - LFC: 03/03/2014 - 21:13:19 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\Invité.bmp [49208]

O61 - LFC: 03/03/2014 - 21:13:45 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\msohtmlclip1\01\clip\_colorschememapping.xml [314]

O61 - LFC: 03/03/2014 - 21:13:45 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\msohtmlclip1\01\clip\_themedata.thmx [3086]

O61 - LFC: 03/03/2014 - 21:13:47 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\RONDEAU.bmp [31832]

O61 - LFC: 03/03/2014 - 21:13:51 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\wmplog09.sqm [1594]

O61 - LFC: 03/03/2014 - 21:13:51 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\wmplog10.sqm [1858]

O61 - LFC: 03/03/2014 - 21:13:54 ----- . (...) -- C:\Users\RONDEAU\AppData\Roaming\eTeks\Sweet Home 3D\work\3600-86accdef-51e8-4159-825a-7b428cddf98c\open6177981679888572975.sweethome3d [2259920]

O61 - LFC: 03/03/2014 - 21:13:54 ----- . (...) -- C:\Users\RONDEAU\AppData\Roaming\eTeks\Sweet Home 3D\work\3600-a065eaa8-a17b-4490-b7ac-2e3712c1a8ff\open2840696192332543988.sweethome3d [2259920]

O61 - LFC: 03/03/2014 - 21:13:54 ----- . (...) -- C:\Users\RONDEAU\AppData\Roaming\eTeks\Sweet Home 3D\work\3600-ededa4de-d334-4c2d-892b-4720e4e12074\open4680313487043266116.sweethome3d [2259920]

O61 - LFC: 03/03/2014 - 21:13:54 ----- . (...) -- C:\Users\RONDEAU\AppData\Roaming\eTeks\Sweet Home 3D\work\3600-fd85ce80-ac55-4c1f-bc5f-80d7cbb6aeb6\open5717819418774463939.sweethome3d [2297477]

O61 - LFC: 03/03/2014 - 21:13:54 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\FLEXnet\Connect\Database\{D5D422B9-6976-4E98-8DDF-9632CB515D7E}.sch [132]

O61 - LFC: 03/03/2014 - 21:13:54 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Malwarebytes\Malwarebytes' Anti-Malware\Logs\mbam-log-2014-03-03 (09-50-34).txt [2218]

O61 - LFC: 03/03/2014 - 21:13:54 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\eInstruction\Device Manager\.eInstructionDeviceManagerPreferences.xml [627]

O61 - LFC: 03/03/2014 - 21:13:54 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\eInstruction\Device Manager\DeviceManagerState.properties [248]

O61 - LFC: 03/03/2014 - 21:13:54 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\eInstruction\Device Manager\DeviceManager\_0.log.lck [0]

O61 - LFC: 03/03/2014 - 21:13:54 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\eTeks\Sweet Home 3D\preferences.xml [2167]

O61 - LFC: 03/03/2014 - 21:13:55 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Office\MSOut12.pip [1724]

O61 - LFC: 03/03/2014 - 21:13:55 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Office\Recent\AdwCleaner v3.LNK [843]

O61 - LFC: 03/03/2014 - 21:13:55 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Office\Recent\Bureau.LNK [685]

O61 - LFC: 03/03/2014 - 21:13:55 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Office\Recent\Difficulté.LNK [828]

O61 - LFC: 03/03/2014 - 21:13:55 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Office\Recent\Identifiant.LNK [833]

O61 - LFC: 03/03/2014 - 21:13:55 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Office\Recent\LISTE DES LOGICIELS DES CAHIERS DE LA CYPRIOLETTE.LNK [1138]

O61 - LFC: 03/03/2014 - 21:13:55 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Office\Recent\Malwarebytes Anti diagnostic.LNK [918]

O61 - LFC: 03/03/2014 - 21:13:55 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Office\Recent\Semaine paire.LNK [843]

O61 - LFC: 03/03/2014 - 21:13:55 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Office\Recent\radiateurs (mail de commande) (2).LNK [943]

O61 - LFC: 03/03/2014 - 21:13:55 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Office\Recent\radiateurs (mail de commande).LNK [923]

O61 - LFC: 03/03/2014 - 21:13:55 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Office\Recent\ticket paiement radiateurs blanc habitat.LNK [983]

O61 - LFC: 03/03/2014 - 21:13:55 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Office\Word12.pip [1764]

O61 - LFC: 03/03/2014 - 21:13:55 --HA- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Office\Recent\index.dat [1658]

O61 - LFC: 03/03/2014 - 21:13:56 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Nuance\NaturallySpeaking12\dd10enum.dat [928]

O61 - LFC: 03/03/2014 - 21:13:56 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\ZHP\Log.txt [73094] =>.Nicolas Coolman

O61 - LFC: 03/03/2014 - 21:13:56 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\ZHP\TestsZHPDiag.txt [2837] =>.Nicolas Coolman

O61 - LFC: 03/03/2014 - 21:14:32 ---A- . (...) -- C:\Users\RONDEAU\Documents\monAlbumPhoto\monAlbumPhoto\_backup\_file.dat [25935872]

O61 - LFC: 28/02/2014 - 21:13:07 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\User Data\Default\Local Storage\chrome-extension\_pelmeidfhdlhlbjimpabfcbnnojbboma\_0.localstorage [3072]

O61 - LFC: 28/02/2014 - 21:13:17 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\BackupSetup.exe [10365728]

O61 - LFC: 28/02/2014 - 21:13:18 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\fullpackage\_temp1393624047\tmp\package2.zip [5854162]

O61 - LFC: 28/02/2014 - 21:13:18 ---A- . (.Cherished Technololgy LIMITED.) -- C:\Users\RONDEAU\AppData\Local\Temp\fullpackage\_temp1393624047\tmp\wpm.exe [501904] =>PUP.WpManager

O61 - LFC: 28/02/2014 - 21:13:48 ---A- . (.Robert Simpson, et al..) -- C:\Users\RONDEAU\AppData\Local\Temp\System.Data.SQLite.dll [1053184]

O61 - LFC: 28/02/2014 - 21:13:48 ---A- . (.Robert Simpson, et al..) -- C:\Users\RONDEAU\AppData\Local\Temp\System.Data.SQLite40028.dll [1053184]

O61 - LFC: 28/02/2014 - 21:13:52 ---A- . (...) -- C:\Users\RONDEAU\AppData\Local\Temp\㩃啜敳獲剜乏䕄啁䅜灰慄慴䱜捯污呜浥屰潬⹧硴t [246]

O61 - LFC: 28/02/2014 - 21:13:55 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Office\Recent\3ème.LNK [268]

O61 - LFC: 28/02/2014 - 21:13:55 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Office\Recent\6ème.LNK [268]

O61 - LFC: 28/02/2014 - 21:13:55 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Office\Recent\Chapitre 8.LNK [365]

O61 - LFC: 28/02/2014 - 21:13:55 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Office\Recent\Partie 4 chapitres 14, 15, 16.LNK [438]

O61 - LFC: 28/02/2014 - 21:13:55 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Office\Recent\résumé ch.12.LNK [496]

O61 - LFC: 28/02/2014 - 21:13:55 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Microsoft\Office\Recent\tableau 4 colonnes-3lignes.LNK [432]

O61 - LFC: 28/02/2014 - 21:13:56 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Real\RealMediaSDK\c0a80000.txt [131]

O61 - LFC: 28/02/2014 - 21:13:56 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Real\RealPlayer\Temp\rn\_tmpsb.ivr [0]

O61 - LFC: 28/02/2014 - 21:13:56 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Real\RealPlayer\Temp\rn\_tmpsb2.ivr [0]

O61 - LFC: 28/02/2014 - 21:13:56 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Real\RealPlayer\Temp\rn\_tmpsb3.ivr [0]

O61 - LFC: 28/02/2014 - 21:13:56 ---A- . (...) -- C:\Users\RONDEAU\AppData\Roaming\Real\RealPlayer\Temp\rn\_tmpsb4.ivr [0]

O61 - LFC: 28/02/2014 - 21:14:33 ---A- . (...) -- C:\Users\RONDEAU\Downloads\2038\_RealPlayer(1).exe [2240896]

O61 - LFC: 28/02/2014 - 21:14:33 ---A- . (...) -- C:\Users\RONDEAU\Downloads\2038\_RealPlayer.exe [2240896]

~ 65 Fichiers temporaires (Temporary files)

~ Files: 501 Scanned in 01mn 41s

---\\ Liste des outils de désinfection (LATC) (O63)

O63 - Logiciel: ZHPDiag 2014 - (.Nicolas Coolman.) [HKLM] -- ZHPDiag\_is1 =>.Nicolas Coolman

~ ADS: Scanned in 00mn 00s

---\\ Liste les services legacy du registre (LALS) (O64)

O64 - Services: CurCS - 21/04/2011 - C:\Windows\system32\drivers\afd.sys (AFD) .(.Microsoft Corporation - Ancillary Function Driver for WinSock.) - LEGACY\_AFD

O64 - Services: CurCS - 24/07/2007 - C:\Program Files\ATKGFNEX\ASMMAP.sys (ASMMAP) .(...) - LEGACY\_ASMMAP

O64 - Services: CurCS - 11/04/2009 - C:\Windows\System32\drivers\atapi.sys (atapi) .(.Microsoft Corporation - ATAPI IDE Miniport Driver.) - LEGACY\_ATAPI

O64 - Services: CurCS - 15/01/2010 - C:\Windows\System32\DRIVERS\atksgt.sys (atksgt) .(...) - LEGACY\_ATKSGT

O64 - Services: CurCS - 19/12/2013 - C:\Windows\System32\DRIVERS\avgntflt.sys (avgntflt) .(.Avira Operations GmbH & Co. KG - Avira Minifilter Driver.) - LEGACY\_AVGNTFLT

O64 - Services: CurCS - 19/12/2013 - C:\Windows\System32\DRIVERS\avipbb.sys (avipbb) .(.Avira Operations GmbH & Co. KG - Avira Driver for Security Enhancement.) - LEGACY\_AVIPBB

O64 - Services: CurCS - 27/11/2013 - C:\Windows\System32\DRIVERS\avkmgr.sys (avkmgr) .(.Avira Operations GmbH & Co. KG - Avira Manager Driver.) - LEGACY\_AVKMGR

O64 - Services: CurCS - 21/01/2008 - C:\Windows\System32\Drivers\Beep.sys (Beep) .(.Microsoft Corporation - BEEP Driver.) - LEGACY\_BEEP

O64 - Services: CurCS - 22/02/2011 - C:\Windows\System32\DRIVERS\bowser.sys (bowser) .(.Microsoft Corporation - NT Lan Manager Datagram Receiver Driver.) - LEGACY\_BOWSER

O64 - Services: CurCS - 21/01/2008 - C:\Windows\System32\DRIVERS\cdfs.sys (cdfs) .(.Microsoft Corporation - CD-ROM File System Driver.) - LEGACY\_CDFS

O64 - Services: CurCS - 11/04/2009 - C:\Windows\System32\CLFS.sys (CLFS) .(.Microsoft Corporation - Common Log File System Driver.) - LEGACY\_CLFS

O64 - Services: CurCS - 21/01/2008 - C:\Windows\System32\drivers\crcdisk.sys (crcdisk) .(.Microsoft Corporation - Disk Block Verification Filter Driver.) - LEGACY\_CRCDISK

O64 - Services: CurCS - 14/04/2011 - C:\Windows\system32\drivers\dfsc.sys (DfsC) .(.Microsoft Corporation - DFS Namespace Client Driver.) - LEGACY\_DFSC

O64 - Services: CurCS - 01/08/2013 - C:\Windows\system32\drivers\dxgkrnl.sys (DXGKrnl) .(.Microsoft Corporation - DirectX Graphics Kernel.) - LEGACY\_DXGKRNL

O64 - Services: CurCS - 11/04/2009 - C:\Windows\System32\Drivers\fastfat.sys (fastfat) .(.Microsoft Corporation - Fast FAT File System Driver.) - LEGACY\_FASTFAT

O64 - Services: CurCS - 21/01/2008 - C:\Windows\System32\drivers\fileinfo.sys (FileInfo) .(.Microsoft Corporation - FileInfo Filter Driver.) - LEGACY\_FILEINFO

O64 - Services: CurCS - 11/04/2009 - C:\Windows\System32\drivers\fltmgr.sys (FltMgr) .(.Microsoft Corporation - Gestionnaire de filtres de système de fichi.) - LEGACY\_FLTMGR

O64 - Services: CurCS - 03/08/2007 - C:\Program Files\ASUS\NB Probe\SPM\ghaio.sys (ghaio) .(...) - LEGACY\_GHAIO

O64 - Services: CurCS - 20/02/2010 - C:\Windows\System32\drivers\HTTP.sys (HTTP) .(.Microsoft Corporation - HTTP Pile du protocole.) - LEGACY\_HTTP

O64 - Services: CurCS - 04/06/2012 - C:\Windows\System32\Drivers\ksecdd.sys (KSecDD) .(.Microsoft Corporation - Kernel Security Support Provider Interface.) - LEGACY\_KSECDD

O64 - Services: CurCS - 15/01/2010 - C:\Windows\System32\DRIVERS\lirsgt.sys (lirsgt) .(...) - LEGACY\_LIRSGT

O64 - Services: CurCS - 21/01/2008 - C:\Windows\System32\DRIVERS\lltdio.sys (lltdio) .(.Microsoft Corporation - Link-Layer Topology Mapper I/O Driver.) - LEGACY\_LLTDIO

O64 - Services: CurCS - 21/01/2008 - C:\Windows\system32\drivers\luafv.sys (luafv) .(.Microsoft Corporation - Pilote de filtre de virtualisation de fichi.) - LEGACY\_LUAFV

O64 - Services: CurCS - 29/05/2008 - C:\Windows\System32\DRIVERS\lullaby.sys (lullaby) .(.Windows (R) Codename Longhorn DDK provider - ASUS CopyProtect driver.) - LEGACY\_LULLABY

O64 - Services: CurCS - 21/01/2008 - C:\Windows\System32\drivers\mountmgr.sys (MountMgr) .(.Microsoft Corporation - Mount Point Manager.) - LEGACY\_MOUNTMGR

O64 - Services: CurCS - 21/01/2008 - C:\Windows\system32\FirewallAPI.dll (mpsdrv) .(.Microsoft Corporation - API du Pare-feu Windows.) - LEGACY\_MPSDRV

O64 - Services: CurCS - 11/04/2009 - C:\Windows\system32\drivers\mrxdav.sys (MRxDAV) .(.Microsoft Corporation - Windows NT WebDav Minirdr.) - LEGACY\_MRXDAV

O64 - Services: CurCS - 29/04/2011 - C:\Windows\System32\DRIVERS\mrxsmb.sys (mrxsmb) .(.Microsoft Corporation - Windows NT SMB Minirdr.) - LEGACY\_MRXSMB

O64 - Services: CurCS - 06/07/2011 - C:\Windows\System32\DRIVERS\mrxsmb10.sys (mrxsmb10) .(.Microsoft Corporation - Longhorn SMB Downlevel SubRdr.) - LEGACY\_MRXSMB10

O64 - Services: CurCS - 29/04/2011 - C:\Windows\System32\DRIVERS\mrxsmb20.sys (mrxsmb20) .(.Microsoft Corporation - Longhorn SMB 2.0 Redirector.) - LEGACY\_MRXSMB20

O64 - Services: CurCS - 22/02/2008 - C:\Windows\System32\drivers\msahci.sys (msahci) .(.Microsoft Corporation - MS AHCI 1.0 Standard Driver.) - LEGACY\_MSAHCI

O64 - Services: CurCS - 21/01/2008 - C:\Windows\System32\drivers\msisadrv.sys (msisadrv) .(.Microsoft Corporation - ISA Driver.) - LEGACY\_MSISADRV

O64 - Services: CurCS - 11/04/2009 - C:\Windows\System32\Drivers\mup.sys (Mup) .(.Microsoft Corporation - Multiple UNC Provider driver.) - LEGACY\_MUP

O64 - Services: CurCS - 11/04/2009 - C:\Windows\System32\DRIVERS\nwifi.sys (NativeWifiP) .(.Microsoft Corporation - NativeWiFi Miniport Driver.) - LEGACY\_NATIVEWIFIP

O64 - Services: CurCS - 11/04/2009 - C:\Windows\System32\drivers\ndis.sys (NDIS) .(.Microsoft Corporation - NDIS 6.0 wrapper driver.) - LEGACY\_NDIS

O64 - Services: CurCS - 21/01/2008 - C:\Windows\System32\DRIVERS\ndisuio.sys (Ndisuio) .(.Microsoft Corporation - NDIS User mode I/O driver.) - LEGACY\_NDISUIO

O64 - Services: CurCS - 21/01/2008 - C:\Windows\System32\DRIVERS\netbios.sys (NetBIOS) .(.Microsoft Corporation - NetBIOS interface driver.) - LEGACY\_NETBIOS

O64 - Services: CurCS - 11/04/2009 - C:\Windows\System32\DRIVERS\netbt.sys (netbt) .(.Microsoft Corporation - MBT Transport driver.) - LEGACY\_NETBT

O64 - Services: CurCS - 21/01/2008 - C:\Windows\System32\drivers\nsiproxy.sys (nsiproxy) .(.Microsoft Corporation - NSI Proxy.) - LEGACY\_NSIPROXY

O64 - Services: CurCS - 02/11/2006 - C:\Windows\System32\drivers\peauth.sys (PEAUTH) .(.Microsoft Corporation - Protected Environment Authentication and Au.) - LEGACY\_PEAUTH

O64 - Services: CurCS - 11/04/2009 - C:\Windows\System32\drivers\pacer.sys (PSched) .(.Microsoft Corporation - Planificateur de paquets QoS.) - LEGACY\_PSCHED

O64 - Services: CurCS - 21/01/2008 - C:\Windows\System32\DRIVERS\rasacd.sys (RasAcd) .(.Microsoft Corporation - RAS Automatic Connection Driver.) - LEGACY\_RASACD

O64 - Services: CurCS - 11/04/2009 - C:\Windows\System32\DRIVERS\rdbss.sys (rdbss) .(.Microsoft Corporation - Redirected Drive Buffering SubSystem Driver.) - LEGACY\_RDBSS

O64 - Services: CurCS - 21/01/2008 - C:\Windows\System32\DRIVERS\RDPCDD.sys (RDPCDD) .(.Microsoft Corporation - RDP Miniport.) - LEGACY\_RDPCDD

O64 - Services: CurCS - 21/01/2008 - C:\Windows\System32\drivers\rdpencdd.sys (RDPENCDD) .(.Microsoft Corporation - RDP Miniport.) - LEGACY\_RDPENCDD

O64 - Services: CurCS - 21/01/2008 - C:\Windows\System32\DRIVERS\rspndr.sys (rspndr) .(.Microsoft Corporation - Link-Layer Topology Responder Driver for ND.) - LEGACY\_RSPNDR

O64 - Services: CurCS - 11/04/2009 - C:\Windows\system32\tcpipcfg.dll (Smb) .(.Microsoft Corporation - Objets de configuration du réseau.) - LEGACY\_SMB

O64 - Services: CurCS - 21/01/2008 - C:\Windows\System32\Drivers\spldr.sys (spldr) .(.Microsoft Corporation - loader for security processor.) - LEGACY\_SPLDR

O64 - Services: CurCS - 18/02/2011 - C:\Windows\System32\DRIVERS\srv.sys (srv) .(.Microsoft Corporation - Server driver.) - LEGACY\_SRV

O64 - Services: CurCS - 29/04/2011 - C:\Windows\System32\DRIVERS\srv2.sys (srv2) .(.Microsoft Corporation - Smb 2.0 Server driver.) - LEGACY\_SRV2

O64 - Services: CurCS - 29/04/2011 - C:\Windows\System32\DRIVERS\srvnet.sys (srvnet) .(.Microsoft Corporation - Server Network driver.) - LEGACY\_SRVNET

O64 - Services: CurCS - 27/08/2012 - C:\Windows\System32\DRIVERS\ssmdrv.sys (ssmdrv) .(.Avira GmbH - AVIRA SnapShot Driver.) - LEGACY\_SSMDRV

O64 - Services: CurCS - 11/04/2009 - C:\Windows\system32\tcpipcfg.dll (Tcpip) .(.Microsoft Corporation - Objets de configuration du réseau.) - LEGACY\_TCPIP

O64 - Services: CurCS - 08/12/2009 - C:\Windows\System32\drivers\tcpipreg.sys (tcpipreg) .(.Microsoft Corporation - TCP/IP Registry Compatibility Driver.) - LEGACY\_TCPIPREG

O64 - Services: CurCS - 11/04/2009 - C:\Windows\system32\tcpipcfg.dll (tdx) .(.Microsoft Corporation - Objets de configuration du réseau.) - LEGACY\_TDX

O64 - Services: CurCS - 21/01/2008 - C:\Windows\system32\drivers\vga.sys (VgaSave) .(.Microsoft Corporation - VGA/Super VGA Video Driver.) - LEGACY\_VGASAVE

O64 - Services: CurCS - 11/04/2009 - C:\Windows\System32\drivers\volmgrx.sys (volmgrx) .(.Microsoft Corporation - Volume Manager Extension Driver.) - LEGACY\_VOLMGRX

O64 - Services: CurCS - 21/08/2012 - C:\Windows\System32\drivers\volsnap.sys (volsnap) .(.Microsoft Corporation - Pilote de cliché instantané du volume.) - LEGACY\_VOLSNAP

O64 - Services: CurCS - 21/01/2008 - C:\Windows\System32\DRIVERS\wanarp.sys (Wanarpv6) .(.Microsoft Corporation - MS Remote Access and Routing ARP Driver.) - LEGACY\_WANARPV6

O64 - Services: CurCS - 27/06/2013 - C:\Windows\System32\drivers\Wdf01000.sys (Wdf01000) .(.Microsoft Corporation - Runtime de l’infrastructure de pilotes en m.) - LEGACY\_WDF01000

O64 - Services: CurCS - 26/07/2012 - C:\Windows\system32\drivers\Wudfpf.sys (WudfPf) .(.Microsoft Corporation - Windows Driver Foundation - User-mode Drive.) - LEGACY\_WUDFPF

O64 - Services: CurCS - 20/05/2008 - C:\Program Files\ASUS\AI TouchMedia\PlayMovie\000.fcl ({49DE1C67-83F8-4102-99E0-C16DCC7EEC796}) .(.Cyberlink Corp. - FCL Driver.) - LEGACY\_{49DE1C67-83F8-4102-99E0-C16DCC7EEC796}

~ Legacy: 87 Scanned in 00mn 00s

---\\ Associations Shell Spawning (O67)

O67 - Shell Spawning: <.bat> <batfile>[HKLM\..\open\Command] (...) -- "%1" %\*

O67 - Shell Spawning: <.cpl> <cplfile>[HKLM\..\cplopen\Command] (.Microsoft Corporation - Windows Control Panel.) -- C:\Windows\System32\control.exe =>.Microsoft Corporation

O67 - Shell Spawning: <.cmd> <cmdfile>[HKLM\..\open\Command] (...) -- "%1" %\*

O67 - Shell Spawning: <.com> <comfile>[HKLM\..\open\Command] (...) -- "%1" %\*

O67 - Shell Spawning: <.evt> <evtfile>[HKLM\..\open\Command] (.Microsoft Corporation - Lanceur du composant logiciel enfichable Observateur d'événements.) -- C:\Windows\System32\eventvwr.exe

O67 - Shell Spawning: <.exe> <exefile>[HKLM\..\open\Command] (...) -- "%1" %\*

O67 - Shell Spawning: <.html> <htmlfile>[HKLM\..\open\Command] (.Microsoft Corporation - Internet Explorer.) -- C:\Program Files\Internet Explorer\iexplore.exe

O67 - Shell Spawning: <.js> <JSFile>[HKLM\..\open\Command] (.Microsoft Corporation - Microsoft (R) Windows Based Script Host.) -- C:\Windows\System32\WScript.exe

O67 - Shell Spawning: <.reg> <regfile>[HKLM\..\open\Command] (.Microsoft Corporation - Éditeur du Registre.) -- C:\Windows\regedit.exe

O67 - Shell Spawning: <.scr> <scrfile>[HKLM\..\open\Command] (...) -- "%1" /S

O67 - Shell Spawning: <.html> <ChromeHTML.URQ6AVB5AGAEI2IJIBE2BESMCQ>[HKCU\..\open\Command] (.Google Inc. - Google Chrome.) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\Application\chrome.exe

~ FASS Keys: 11 Scanned in 00mn 00s

---\\ Menu de démarrage Internet (SMI) (O68)

O68 - StartMenuInternet: <Google Chrome.URQ6AVB5AGAEI2IJIBE2BESMCQ> <Google Chrome>[HKLM\..\Shell\open\Command] (.Google Inc. - Google Chrome.) -- C:\Users\RONDEAU\AppData\Local\Google\Chrome\Application\chrome.exe

O68 - StartMenuInternet: <IEXPLORE.EXE> <Internet Explorer>[HKLM\..\Shell\open\Command] (.Microsoft Corporation - Internet Explorer.) -- c:\program files\internet explorer\iexplore.exe

~ Keys: Scanned in 00mn 00s

---\\ Recherche d'infection sur les navigateurs internet (SBI) (O69)

O69 - SBI: SearchScopes [HKCU] {6A1806CD-94D4-4689-BA73-E35EA1EA9990} [DefaultScope] - (Google) - http://www.google.com

O69 - SBI: SearchScopes [HKCU] {92A37C44-992F-40DF-A428-90965F4D401A} - (Ask Search) - http://websearch.ask.com =>Toolbar.Ask

~ Keys: Scanned in 00mn 00s

---\\ Enumère les service demarrés par Svchost (SSS) (O83)

O83 - Search Svchost Services: AeLookupSvc (AeLookupSvc) . (.Microsoft Corporation - Service Expérience d’application.) -- C:\Windows\System32\aelupsvc.dll [24576]

O83 - Search Svchost Services: wercplsupport (wercplsupport) . (.Microsoft Corporation - Rapports et solutions aux problèmes.) -- C:\Windows\System32\wercplsupport.dll [62976]

O83 - Search Svchost Services: Themes (Themes) . (.Microsoft Corporation - Dll des services Windows Shell.) -- C:\Windows\System32\shsvcs.dll [247808]

O83 - Search Svchost Services: CertPropSvc (CertPropSvc) . (.Microsoft Corporation - Service de propagation de certificats de cartes à puce Microsoft.) -- C:\Windows\System32\certprop.dll [40448]

O83 - Search Svchost Services: SCPolicySvc (SCPolicySvc) . (.Microsoft Corporation - Service de propagation de certificats de cartes à puce Microsoft.) -- C:\Windows\System32\certprop.dll [40448]

O83 - Search Svchost Services: lanmanserver (lanmanserver) . (.Microsoft Corporation - DLL du service Serveur.) -- C:\Windows\System32\srvsvc.dll [125952]

O83 - Search Svchost Services: gpsvc (gpsvc) . (.Microsoft Corporation - Client de stratégie de groupe.) -- C:\Windows\System32\gpsvc.dll [576512]

O83 - Search Svchost Services: IKEEXT (IKEEXT) . (.Microsoft Corporation - Extension IKE.) -- C:\Windows\System32\ikeext.dll [444928]

O83 - Search Svchost Services: AudioSrv (AudioSrv) . (.Microsoft Corporation - Service Audio Windows.) -- C:\Windows\System32\Audiosrv.dll [315392]

O83 - Search Svchost Services: Rasauto (Rasauto) . (.Microsoft Corporation - Gestionnaire de numérotation automatique d’accès distant.) -- C:\Windows\System32\rasauto.dll [90624]

O83 - Search Svchost Services: Rasman (Rasman) . (.Microsoft Corporation - Gestionnaire de connexions d'accès distant.) -- C:\Windows\System32\rasmans.dll [262144]

O83 - Search Svchost Services: Remoteaccess (Remoteaccess) . (.Microsoft Corporation - Gestionnaire d’interface dynamique.) -- C:\Windows\System32\mprdim.dll [68608]

O83 - Search Svchost Services: SENS (SENS) . (.Microsoft Corporation - Service de notification d’événements système (SENS).) -- C:\Windows\System32\sens.dll [47104]

O83 - Search Svchost Services: Sharedaccess (Sharedaccess) . (.Microsoft Corporation - Composants de l'application d'assistance à Microsoft NAT.) -- C:\Windows\System32\ipnathlp.dll [288256]

O83 - Search Svchost Services: Tapisrv (Tapisrv) . (.Microsoft Corporation - Serveur de téléphonie Microsoft® Windows(TM).) -- C:\Windows\System32\tapisrv.dll [242688]

O83 - Search Svchost Services: TermService (TermService) . (.Microsoft Corporation - Gestionnaire des connexions distantes Terminal Server.) -- C:\Windows\System32\termsrv.dll [449024]

O83 - Search Svchost Services: wuauserv (wuauserv) . (.Microsoft Corporation - Agent de mise à jour automatique Windows Update.) -- C:\Windows\System32\wuaueng.dll [1933848]

O83 - Search Svchost Services: BITS (BITS) . (.Microsoft Corporation - Service de transfert intelligent en arrière-plan.) -- C:\Windows\System32\qmgr.dll [758784]

O83 - Search Svchost Services: ShellHWDetection (ShellHWDetection) . (.Microsoft Corporation - Dll des services Windows Shell.) -- C:\Windows\System32\shsvcs.dll [247808]

O83 - Search Svchost Services: iphlpsvc (iphlpsvc) . (.Microsoft Corporation - Service offrant une connectivité IPv6 sur un réseau IPv4..) -- C:\Windows\System32\iphlpsvc.dll [200704]

O83 - Search Svchost Services: seclogon (seclogon) . (.Microsoft Corporation - DLL de service d'ouverture de session secondaire.) -- C:\Windows\system32\seclogon.dll [19968]

O83 - Search Svchost Services: AppInfo (AppInfo) . (.Microsoft Corporation - Service Informations d’application.) -- C:\Windows\System32\appinfo.dll [33280]

O83 - Search Svchost Services: msiscsi (msiscsi) . (.Microsoft Corporation - Service de découverte iSCSI.) -- C:\Windows\System32\iscsiexe.dll [111616]

O83 - Search Svchost Services: MMCSS (MMCSS) . (.Microsoft Corporation - Service Planificateur de classes multimédias.) -- C:\Windows\System32\mmcss.dll [45056]

O83 - Search Svchost Services: ProfSvc (ProfSvc) . (.Microsoft Corporation - ProfSvc.) -- C:\Windows\System32\profsvc.dll [153088]

O83 - Search Svchost Services: EapHost (EapHost) . (.Microsoft Corporation - Service EAPHost Microsoft.) -- C:\Windows\System32\eapsvc.dll [57344]

O83 - Search Svchost Services: winmgmt (winmgmt) . (.Microsoft Corporation - WMI.) -- C:\Windows\System32\wbem\WMIsvc.dll [162304]

O83 - Search Svchost Services: schedule (schedule) . (.Microsoft Corporation - Service du Planificateur de tâches.) -- C:\Windows\System32\schedsvc.dll [601600]

O83 - Search Svchost Services: SessionEnv (SessionEnv) . (.Microsoft Corporation - Service de configuration des services Terminal Server.) -- C:\Windows\System32\sessenv.dll [84992]

O83 - Search Svchost Services: browser (browser) . (.Microsoft Corporation - DLL du service Explorateur d’ordinateurs.) -- C:\Windows\System32\browser.dll [81920]

O83 - Search Svchost Services: hkmsvc (hkmsvc) . (.Microsoft Corporation - Service Gestion des clés.) -- C:\Windows\System32\kmsvc.dll [68096]

~ Services: 31 Scanned in 00mn 00s

---\\ Recherche particulière à la racine du système (SPRF) (O84)

[MD5.8F6EAB69886EA7676613AB2584EF5A08] [SPRF][12/02/2014] (...) -- C:\ProgramData\nvModes.dat [55487]

[MD5.90E3FFA51DDCDB07C482FCE962E56E99] [SPRF][15/07/2011] (.TomTom International B.V. - WinLatest.exe.) -- C:\Users\RONDEAU\Desktop\TomTomHOME2winlatest.exe [20398464]

[MD5.159DA8539E1A4ECBC33CC9A556C0F6A2] [SPRF][03/03/2011] (.EA Digital Illusions CE AB - EA Battlefield Heroes Updater.) -- C:\Windows\Downloaded Program Files\BFHUpdater.dll [222584]

[MD5.14583C9FB1D6970745DC92AD8EC0F5E0] [SPRF][03/03/2011] (.EA Digital Illusions CE AB - EA Battlefield Heroes Updater.) -- C:\Windows\Downloaded Program Files\BFHUpdater.exe [1312120]

[MD5.3FEA9D2EDF23B0283C7A66C8DEA380BD] [SPRF][25/07/2002] (.InstallShield Software Corporation - InstallShield Update Service Setup Player Module.) -- C:\Windows\Downloaded Program Files\dwusplay.dll [24576]

[MD5.CDBE35EA59BC9223E4F800BD1DB82D27] [SPRF][25/07/2002] (.InstallShield Software Corporation - InstallShield Update Service Setup Player.) -- C:\Windows\Downloaded Program Files\dwusplay.exe [196608]

[MD5.B8F39C9E0F0B71E454DBA431CF3B99C9] [SPRF][11/08/2005] (.Macrovision Corporation - InstallShield Update Service Web Agent.) -- C:\Windows\Downloaded Program Files\isusweb.dll [417792]

~ Files: 7 Scanned in 00mn 00s

---\\ Liste des exceptions du parefeu (FirewallRules) (O87)

O87 - FAEL: "CoreNet-GP-LSASS-Out-TCP" | Out - Domain - P6 - TRUE | .(.Microsoft Corporation - Processus de l’autorité de sécurité locale.) -- C:\Windows\system32\lsass.exe

O87 - FAEL: "CoreNet-DNS-Out-UDP" | Out - None - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "CoreNet-GP-Out-TCP" | Out - Domain - P6 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "CoreNet-Teredo-Out" | Out - None - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "CoreNet-Teredo-In" | In - None - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "CoreNet-DHCP-Out" | Out - None - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "CoreNet-DHCP-In" | In - None - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "FPS-SpoolSvc-In-TCP" | In - Public - P6 - TRUE | .(.Microsoft Corporation - Application sous-système spouleur.) -- C:\Windows\system32\spoolsv.exe

O87 - FAEL: "FPS-SpoolSvc-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Application sous-système spouleur.) -- C:\Windows\system32\spoolsv.exe

O87 - FAEL: "NETDIS-FDRESPUB-WSD-Out-UDP" | Out - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "NETDIS-FDRESPUB-WSD-In-UDP" | In - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "NETDIS-LLMNR-Out-UDP" | Out - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "NETDIS-LLMNR-In-UDP" | In - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "NETDIS-FDPHOST-Out-UDP" | Out - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "NETDIS-FDPHOST-In-UDP" | In - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "NETDIS-UPnP-Out-TCP" | Out - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "NETDIS-SSDPSrv-Out-UDP" | Out - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "NETDIS-SSDPSrv-In-UDP" | In - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "NETDIS-FDRESPUB-WSD-Out-UDP-Active" | Out - Private - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "NETDIS-FDRESPUB-WSD-In-UDP-Active" | In - Private - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "NETDIS-LLMNR-Out-UDP-Active" | Out - Private - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "NETDIS-LLMNR-In-UDP-Active" | In - Private - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "NETDIS-FDPHOST-Out-UDP-Active" | Out - Private - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "NETDIS-FDPHOST-In-UDP-Active" | In - Private - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "NETDIS-UPnP-Out-TCP-Active" | Out - Private - P6 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "NETDIS-SSDPSrv-Out-UDP-Active" | Out - Private - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "NETDIS-SSDPSrv-In-UDP-Active" | In - Private - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "SNMPTRAP-In-UDP-NoScope" | In - Domain - P17 - FALSE | .(.Microsoft Corporation - Interruption SNMP.) -- C:\Windows\system32\snmptrap.exe

O87 - FAEL: "SNMPTRAP-In-UDP" | In - Public - P17 - FALSE | .(.Microsoft Corporation - Interruption SNMP.) -- C:\Windows\system32\snmptrap.exe

O87 - FAEL: "NetPres-Out-TCP" | Out - Public - P6 - FALSE | .(.Microsoft Corporation - Connect to a Network Projector.) -- C:\Windows\system32\netproj.exe =>.Microsoft Corporation

O87 - FAEL: "NetPres-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Connect to a Network Projector.) -- C:\Windows\system32\netproj.exe =>.Microsoft Corporation

O87 - FAEL: "NetPres-WSD-Out-UDP" | Out - Domain - P17 - FALSE | .(.Microsoft Corporation - Connect to a Network Projector.) -- C:\Windows\system32\netproj.exe =>.Microsoft Corporation

O87 - FAEL: "NetPres-WSD-In-UDP" | In - Domain - P17 - FALSE | .(.Microsoft Corporation - Connect to a Network Projector.) -- C:\Windows\system32\netproj.exe =>.Microsoft Corporation

O87 - FAEL: "NetPres-Out-TCP-NoScope" | Out - Domain - P6 - FALSE | .(.Microsoft Corporation - Connect to a Network Projector.) -- C:\Windows\system32\netproj.exe =>.Microsoft Corporation

O87 - FAEL: "NetPres-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Connect to a Network Projector.) -- C:\Windows\system32\netproj.exe =>.Microsoft Corporation

O87 - FAEL: "WPDMTP-UPnP-Out-TCP" | Out - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WPDMTP-SSDPSrv-Out-UDP" | Out - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WPDMTP-SSDPSrv-In-UDP" | In - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WPDMTP-Out-TCP" | Out - Public - P6 - FALSE | .(.Microsoft Corporation - Windows Driver Foundation - Processus hôte de l’infrastructure de pilotes.) -- C:\Windows\system32\wudfhost.exe

O87 - FAEL: "WPDMTP-Out-TCP-NoScope" | Out - Domain - P6 - FALSE | .(.Microsoft Corporation - Windows Driver Foundation - Processus hôte de l’infrastructure de pilotes.) -- C:\Windows\system32\wudfhost.exe

O87 - FAEL: "RemoteAssistance-UPnP-Out-TCP-Active" | Out - Private - P6 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteAssistance-SSDPSrv-Out-UDP-Active" | Out - Private - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteAssistance-SSDPSrv-In-UDP-Active" | In - Private - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteAssistance-Out-TCP-Active" | Out - Private - P6 - TRUE | .(.Microsoft Corporation - Assistance à distance Windows.) -- C:\Windows\system32\msra.exe

O87 - FAEL: "RemoteAssistance-In-TCP-EdgeScope-Active" | In - Private - P6 - TRUE | .(.Microsoft Corporation - Assistance à distance Windows.) -- C:\Windows\system32\msra.exe

O87 - FAEL: "RemoteAssistance-UPnP-Out-TCP" | Out - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteAssistance-SSDPSrv-Out-UDP" | Out - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteAssistance-SSDPSrv-In-UDP" | In - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteAssistance-Out-TCP" | Out - Domain - P6 - FALSE | .(.Microsoft Corporation - Assistance à distance Windows.) -- C:\Windows\system32\msra.exe

O87 - FAEL: "RemoteAssistance-In-TCP-EdgeScope" | In - Domain - P6 - TRUE | .(.Microsoft Corporation - Assistance à distance Windows.) -- C:\Windows\system32\msra.exe

O87 - FAEL: "RemoteAssistance-DCOM-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteAssistance-RAServer-Out-TCP-NoScope" | Out - Domain - P6 - FALSE | .(.Microsoft Corporation - Serveur COM d’assistance à distance Windows.) -- C:\Windows\system32\raserver.exe

O87 - FAEL: "RemoteAssistance-RAServer-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Serveur COM d’assistance à distance Windows.) -- C:\Windows\system32\raserver.exe

O87 - FAEL: "MSDTC-RPCSS-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "MSDTC-KTMRM-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "MSDTC-Out-TCP" | Out - Public - P6 - FALSE | .(.Microsoft Corporation - Programme DTCconsole MS.) -- C:\Windows\system32\msdtc.exe

O87 - FAEL: "MSDTC-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Programme DTCconsole MS.) -- C:\Windows\system32\msdtc.exe

O87 - FAEL: "MSDTC-RPCSS-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "MSDTC-KTMRM-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "MSDTC-Out-TCP-NoScope" | Out - Domain - P6 - FALSE | .(.Microsoft Corporation - Programme DTCconsole MS.) -- C:\Windows\system32\msdtc.exe

O87 - FAEL: "MSDTC-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Programme DTCconsole MS.) -- C:\Windows\system32\msdtc.exe

O87 - FAEL: "RemoteTask-RPCSS-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteTask-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteTask-RPCSS-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteTask-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "BITSSVC-RPCSS-In-TCP" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "BITSSVC-RPC-In-TCP" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "BITSSVC-WSD-Out-UDP" | Out - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "BITSSVC-WSD-In-UDP" | In - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteFwAdmin-RPCSS-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteFwAdmin-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteFwAdmin-RPCSS-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteFwAdmin-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteSvcAdmin-RPCSS-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteSvcAdmin-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Applications Services et Contrôleur.) -- C:\Windows\system32\services.exe

O87 - FAEL: "RemoteSvcAdmin-RPCSS-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteSvcAdmin-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Applications Services et Contrôleur.) -- C:\Windows\system32\services.exe

O87 - FAEL: "RemoteEventLogSvc-RPCSS-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteEventLogSvc-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteEventLogSvc-RPCSS-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteEventLogSvc-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "PNRPMNRS-SSDPSrv-Out-UDP" | Out - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "PNRPMNRS-SSDPSrv-In-UDP" | In - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "PNRPMNRS-PNRP-Out-UDP" | Out - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "PNRPMNRS-PNRP-In-UDP" | In - Domain - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WMI-ASYNC-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Sink to receive asynchronous callbacks for WMI client application.) -- C:\Windows\system32\wbem\unsecapp.exe

O87 - FAEL: "WMI-WINMGMT-Out-TCP" | Out - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WMI-WINMGMT-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WMI-RPCSS-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WMI-ASYNC-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Sink to receive asynchronous callbacks for WMI client application.) -- C:\Windows\system32\wbem\unsecapp.exe

O87 - FAEL: "WMI-WINMGMT-Out-TCP-NoScope" | Out - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WMI-WINMGMT-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WMI-RPCSS-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RVM-RPCSS-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RVM-VDSLDR-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Virtual Disk Service Loader.) -- C:\Windows\system32\vdsldr.exe

O87 - FAEL: "RVM-VDS-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Service de disque virtuel.) -- C:\Windows\system32\vds.exe

O87 - FAEL: "RVM-RPCSS-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RVM-VDSLDR-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Virtual Disk Service Loader.) -- C:\Windows\system32\vdsldr.exe

O87 - FAEL: "RVM-VDS-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Service de disque virtuel.) -- C:\Windows\system32\vds.exe

O87 - FAEL: "Collab-PNRP-SSDPSrv-Out-UDP" | Out - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "Collab-PNRP-SSDPSrv-In-UDP" | In - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "Collab-PNRP-Out-UDP" | Out - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "Collab-PNRP-In-UDP" | In - Domain - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "Collab-P2PHost-WSD-Out-UDP" | Out - Domain - P17 - FALSE | .(.Microsoft Corporation - Voisinage immédiat.) -- C:\Windows\system32\p2phost.exe

O87 - FAEL: "Collab-P2PHost-WSD-In-UDP" | In - Domain - P17 - FALSE | .(.Microsoft Corporation - Voisinage immédiat.) -- C:\Windows\system32\p2phost.exe

O87 - FAEL: "Collab-P2PHost-Out-TCP" | Out - Domain - P6 - FALSE | .(.Microsoft Corporation - Voisinage immédiat.) -- C:\Windows\system32\p2phost.exe

O87 - FAEL: "Collab-P2PHost-In-TCP" | In - Domain - P6 - TRUE | .(.Microsoft Corporation - Voisinage immédiat.) -- C:\Windows\system32\p2phost.exe

O87 - FAEL: "MsiScsi-Out-TCP" | Out - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "MsiScsi-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "MsiScsi-Out-TCP-NoScope" | Out - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "MsiScsi-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteAdmin-RPCSS-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteAdmin-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteAdmin-RPCSS-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "RemoteAdmin-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WinCollab-P2P-Out-TCP" | Out - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WinCollab-P2P-In-TCP" | In - Domain - P6 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WinCollab-Out-UDP" | Out - Domain - P17 - FALSE | .(.Microsoft Corporation - Windows Meeting Space.) -- C:\Program Files\Windows Collaboration\WinCollab.exe =>.Microsoft Corporation

O87 - FAEL: "WinCollab-In-UDP" | In - Domain - P17 - TRUE | .(.Microsoft Corporation - Windows Meeting Space.) -- C:\Program Files\Windows Collaboration\WinCollab.exe =>.Microsoft Corporation

O87 - FAEL: "WinCollab-Out-TCP" | Out - Domain - P6 - FALSE | .(.Microsoft Corporation - Windows Meeting Space.) -- C:\Program Files\Windows Collaboration\WinCollab.exe =>.Microsoft Corporation

O87 - FAEL: "WinCollab-In-TCP" | In - Domain - P6 - TRUE | .(.Microsoft Corporation - Windows Meeting Space.) -- C:\Program Files\Windows Collaboration\WinCollab.exe =>.Microsoft Corporation

O87 - FAEL: "WinCollab-DFSR-Out-TCP" | Out - Domain - P6 - FALSE | .(.Microsoft Corporation - Réplication DFS.) -- C:\Windows\system32\dfsr.exe

O87 - FAEL: "WinCollab-DFSR-In-TCP" | In - Domain - P6 - TRUE | .(.Microsoft Corporation - Réplication DFS.) -- C:\Windows\system32\dfsr.exe

O87 - FAEL: "MCX-Prov-Out-TCP" | Out - Domain - P6 - FALSE | .(.Microsoft Corporation - MCX2 Provisioning library.) -- C:\Windows\ehome\mcx2prov.exe

O87 - FAEL: "MCX-MCX2SVC-Out-TCP" | Out - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "MCX-Out-UDP" | Out - Domain - P17 - FALSE | .(.Microsoft Corporation - Media Center.) -- C:\Windows\ehome\ehshell.exe

O87 - FAEL: "MCX-In-UDP" | In - Domain - P17 - FALSE | .(.Microsoft Corporation - Media Center.) -- C:\Windows\ehome\ehshell.exe

O87 - FAEL: "MCX-QWave-Out-TCP" | Out - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "MCX-QWave-In-TCP" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "MCX-QWave-Out-UDP" | Out - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "MCX-QWave-In-UDP" | In - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "MCX-Out-TCP" | Out - Domain - P6 - FALSE | .(.Microsoft Corporation - Media Center.) -- C:\Windows\ehome\ehshell.exe

O87 - FAEL: "MCX-In-TCP" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Media Center.) -- C:\Windows\ehome\ehshell.exe

O87 - FAEL: "MCX-SSDPSrv-Out-UDP" | Out - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "MCX-SSDPSrv-In-UDP" | In - Domain - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-UPnP-Out-TCP" | Out - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-Out-TCP" | Out - Public - P6 - FALSE | .(.Microsoft Corporation - Service Partage réseau du Lecteur Windows Media.) -- C:\Program Files\Windows Media Player\wmpnetwk.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Service Partage réseau du Lecteur Windows Media.) -- C:\Program Files\Windows Media Player\wmpnetwk.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-Out-UDP" | Out - Public - P17 - FALSE | .(.Microsoft Corporation - Service Partage réseau du Lecteur Windows Media.) -- C:\Program Files\Windows Media Player\wmpnetwk.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-In-UDP" | In - Public - P17 - FALSE | .(.Microsoft Corporation - Service Partage réseau du Lecteur Windows Media.) -- C:\Program Files\Windows Media Player\wmpnetwk.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-WMP-Out-TCP" | Out - Public - P6 - FALSE | .(.Microsoft Corporation - Windows Media Player.) -- C:\Program Files\Windows Media Player\wmplayer.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-WMP-Out-UDP" | Out - Public - P17 - FALSE | .(.Microsoft Corporation - Windows Media Player.) -- C:\Program Files\Windows Media Player\wmplayer.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-WMP-In-UDP" | In - Public - P17 - FALSE | .(.Microsoft Corporation - Windows Media Player.) -- C:\Program Files\Windows Media Player\wmplayer.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-SSDPSrv-Out-UDP" | Out - Public - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-SSDPSrv-In-UDP" | In - Public - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-QWave-Out-TCP" | Out - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-QWave-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-QWave-Out-UDP" | Out - Public - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-QWave-In-UDP" | In - Public - P17 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-Out-TCP-NoScope" | Out - Domain - P6 - TRUE | .(.Microsoft Corporation - Service Partage réseau du Lecteur Windows Media.) -- C:\Program Files\Windows Media Player\wmpnetwk.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-In-TCP-NoScope" | In - Domain - P6 - TRUE | .(.Microsoft Corporation - Service Partage réseau du Lecteur Windows Media.) -- C:\Program Files\Windows Media Player\wmpnetwk.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-Out-UDP-NoScope" | Out - Domain - P17 - TRUE | .(.Microsoft Corporation - Service Partage réseau du Lecteur Windows Media.) -- C:\Program Files\Windows Media Player\wmpnetwk.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-In-UDP-NoScope" | In - Domain - P17 - TRUE | .(.Microsoft Corporation - Service Partage réseau du Lecteur Windows Media.) -- C:\Program Files\Windows Media Player\wmpnetwk.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-WMP-Out-TCP-NoScope" | Out - Domain - P6 - TRUE | .(.Microsoft Corporation - Windows Media Player.) -- C:\Program Files\Windows Media Player\wmplayer.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-WMP-Out-UDP-NoScope" | Out - Domain - P17 - TRUE | .(.Microsoft Corporation - Windows Media Player.) -- C:\Program Files\Windows Media Player\wmplayer.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-WMP-In-UDP-NoScope" | In - Domain - P17 - TRUE | .(.Microsoft Corporation - Windows Media Player.) -- C:\Program Files\Windows Media Player\wmplayer.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-QWave-Out-TCP-NoScope" | Out - Domain - P6 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-QWave-In-TCP-NoScope" | In - Domain - P6 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-QWave-Out-UDP-NoScope" | Out - Domain - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WMPNSS-QWave-In-UDP-NoScope" | In - Domain - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "WMP-Out-TCP" | Out - Public - P6 - FALSE | .(.Microsoft Corporation - Windows Media Player.) -- C:\Program Files\Windows Media Player\wmplayer.exe =>.Microsoft Corporation

O87 - FAEL: "WMP-Out-UDP" | Out - Public - P17 - FALSE | .(.Microsoft Corporation - Windows Media Player.) -- C:\Program Files\Windows Media Player\wmplayer.exe =>.Microsoft Corporation

O87 - FAEL: "WMP-In-UDP" | In - Public - P17 - FALSE | .(.Microsoft Corporation - Windows Media Player.) -- C:\Program Files\Windows Media Player\wmplayer.exe =>.Microsoft Corporation

O87 - FAEL: "PerfLogsAlerts-DCOM-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "PerfLogsAlerts-PLASrv-In-TCP-NoScope" | In - Domain - P6 - FALSE | .(.Microsoft Corporation - Serveur DCOM des journaux et alertes de performance.) -- C:\Windows\system32\plasrv.exe

O87 - FAEL: "PerfLogsAlerts-DCOM-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "PerfLogsAlerts-PLASrv-In-TCP" | In - Public - P6 - FALSE | .(.Microsoft Corporation - Serveur DCOM des journaux et alertes de performance.) -- C:\Windows\system32\plasrv.exe

O87 - FAEL: "{151CFD79-6126-4AF1-84A4-F7D890D81642}" | In - Public - P17 - TRUE | .(.Microsoft Corporation - Microsoft Office Outlook.) -- C:\Program Files\Microsoft Office\Office12\outlook.exe =>.Microsoft Corporation

O87 - FAEL: "{19645F40-75E3-499C-A6C4-DB320256C617}" |In - None - P17 - TRUE | .(...) -- C:\Program Files\ASUS\AI TouchMedia\AI TouchMedia\PowerCinema.exe (.not file.)

O87 - FAEL: "{9705FA53-FF89-4CE3-9A95-62353CDA12F0}" |In - None - P17 - TRUE | .(...) -- C:\Program Files\ASUS\AI TouchMedia\AI TouchMedia\PCMService.exe (.not file.)

O87 - FAEL: "{4164D363-360B-49D7-BBAC-59B2655F1A37}" |In - None - P17 - TRUE | .(...) -- C:\Program Files\ASUS\AI TouchMedia\AI TouchMedia\Kernel\DMP\CLBrowserEngine.exe (.not file.)

O87 - FAEL: "{FCF09EB1-7B7C-40B3-A19F-2919FAA33656}" |In - None - P17 - TRUE | .(...) -- C:\Program Files\ASUS\AI TouchMedia\AI TouchMedia\Kernel\DMS\CLMSService.exe (.not file.)

O87 - FAEL: "{F3CC8A41-A95C-40E6-95E3-64B570ED5666}" | In - None - P17 - TRUE | .(.CyberLink Corp. - PlayMovie.) -- C:\Program Files\ASUS\AI TouchMedia\PlayMovie\PlayMovie.exe

O87 - FAEL: "{3F9D7D36-97A8-476D-946A-67E477AEEF48}" | In - None - P17 - TRUE | .(.CyberLink Corp. - CyberLink PlayMovie Resident ProgramPlayMovie Resident Program.) -- C:\Program Files\ASUS\AI TouchMedia\PlayMovie\PMVService.exe

O87 - FAEL: "{115DCD57-FBA4-400E-AE38-0F004B44D61C}" | In - Public - P6 - TRUE | .(.Blue Byte GmbH - THE SETTLERS - Rise of an Empire.) -- C:\Program Files\Ubisoft\THE SETTLERS - Bâtisseurs d'Empire\base\bin\Settlers6.exe

O87 - FAEL: "{2AA79B87-B663-44DE-AC7C-37B84C992E30}" | In - Public - P17 - TRUE | .(.Blue Byte GmbH - THE SETTLERS - Rise of an Empire.) -- C:\Program Files\Ubisoft\THE SETTLERS - Bâtisseurs d'Empire\base\bin\Settlers6.exe

O87 - FAEL: "{AD635E25-C230-4A06-9E48-7B6D920827C9}" | In - None - P17 - TRUE | .(.Microsoft Corporation - Windows Live Communications Platform.) -- C:\Program Files\Windows Live\Contacts\wlcomm.exe

O87 - FAEL: "{01BD9FB2-E14F-4A65-BC56-AE1E9BE995EB}" | In - None - P17 - TRUE | .(.Microsoft Corporation - Windows Live Messenger.) -- C:\Program Files\Windows Live\Messenger\msnmsgr.exe

O87 - FAEL: "TCP Query User{A86D9944-5CDD-431A-9390-C180673699EE}C:\program files\microsoft office\office12\winword.exe" | In - Private - P6 - TRUE | .(.Microsoft Corporation - Microsoft Office Word.) -- C:\program files\microsoft office\office12\winword.exe

O87 - FAEL: "UDP Query User{296A28A9-3975-4993-B339-69F2931CB242}C:\program files\microsoft office\office12\winword.exe" | In - Private - P17 - TRUE | .(.Microsoft Corporation - Microsoft Office Word.) -- C:\program files\microsoft office\office12\winword.exe

O87 - FAEL: "TCP Query User{7CFA16F4-395C-41CB-9D64-DA103F143BF6}C:\program files\ubisoft\the settlers - bâtisseurs d'empire\base\bin\settlers6.exe" | In - Private - P6 - TRUE | .(.Blue Byte GmbH - THE SETTLERS - Rise of an Empire.) -- C:\program files\ubisoft\the settlers - bâtisseurs d'empire\base\bin\settlers6.exe

O87 - FAEL: "UDP Query User{B0796E40-4E5C-4B32-825B-D27565CAB082}C:\program files\ubisoft\the settlers - bâtisseurs d'empire\base\bin\settlers6.exe" | In - Private - P17 - TRUE | .(.Blue Byte GmbH - THE SETTLERS - Rise of an Empire.) -- C:\program files\ubisoft\the settlers - bâtisseurs d'empire\base\bin\settlers6.exe

O87 - FAEL: "{48DDC70B-852D-41E7-A36C-083851B72D03}" | In - Private - P6 - TRUE | .(.Microsoft Corporation - Application sous-système spouleur.) -- C:\Windows\system32\spoolsv.exe

O87 - FAEL: "{741478D2-841D-4EDE-AF11-72DE457C7A1B}" | Out - Private - P6 - TRUE | .(.Microsoft Corporation - Windows Driver Foundation - Processus hôte de l’infrastructure de pilotes.) -- C:\Windows\system32\wudfhost.exe

O87 - FAEL: "{B6F67ECA-BDD7-488E-8B0A-BB9632827B43}" | In - Private - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "{7B137425-2710-4563-A9E9-4C6DFDEE572C}" | Out - Private - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "{A3A93B5D-3314-48B4-9C2C-37ECBF1E9E11}" | Out - Private - P6 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "TCP Query User{1C6B26A1-05CF-4F84-847E-1038977A8C8F}C:\program files\hp\hp photosmart plus b210 series\bin\hpnetworkcommunicator.exe" |In - Public - P6 - TRUE | .(...) -- C:\program files\hp\hp photosmart plus b210 series\bin\hpnetworkcommunicator.exe (.not file.) =>.Hewlett-Packard Co

O87 - FAEL: "UDP Query User{B14CDEFC-9720-46B4-92AB-5A6491E819B6}C:\program files\hp\hp photosmart plus b210 series\bin\hpnetworkcommunicator.exe" |In - Public - P17 - TRUE | .(...) -- C:\program files\hp\hp photosmart plus b210 series\bin\hpnetworkcommunicator.exe (.not file.) =>.Hewlett-Packard Co

O87 - FAEL: "{9163A27A-FD43-4891-BD7C-64010101FDC8}" | In - None - P17 - TRUE | .(.Apple Inc. - WebKit2WebProcess.exe.) -- C:\Program Files\Common Files\Apple\Apple Application Support\WebKit2WebProcess.exe

O87 - FAEL: "TCP Query User{8DEBDB16-8942-4B12-A832-E09C8654C57E}C:\windows\explorer.exe" | In - Private - P6 - TRUE | .(.Microsoft Corporation - Explorateur Windows.) -- C:\windows\explorer.exe =>.Microsoft Corporation

O87 - FAEL: "UDP Query User{76797F2B-310D-4CA2-8234-60371814785E}C:\windows\explorer.exe" | In - Private - P17 - TRUE | .(.Microsoft Corporation - Explorateur Windows.) -- C:\windows\explorer.exe =>.Microsoft Corporation

O87 - FAEL: "TCP Query User{D49FA888-8216-4C6D-B18C-8C980596545A}C:\windows\system32\taskeng.exe" | In - Private - P6 - TRUE | .(.Microsoft Corporation - Moteur du Planificateur de tâches.) -- C:\windows\system32\taskeng.exe

O87 - FAEL: "UDP Query User{99B71F50-E1F9-4C6C-98D6-BEA928714222}C:\windows\system32\taskeng.exe" | In - Private - P17 - TRUE | .(.Microsoft Corporation - Moteur du Planificateur de tâches.) -- C:\windows\system32\taskeng.exe

O87 - FAEL: "TCP Query User{44162226-50FD-4083-80FE-4569EE08C01C}C:\windows\explorer.exe" | In - Public - P6 - TRUE | .(.Microsoft Corporation - Explorateur Windows.) -- C:\windows\explorer.exe =>.Microsoft Corporation

O87 - FAEL: "UDP Query User{C1812C44-6282-4219-9196-103882CCB7BD}C:\windows\explorer.exe" | In - Public - P17 - TRUE | .(.Microsoft Corporation - Explorateur Windows.) -- C:\windows\explorer.exe =>.Microsoft Corporation

O87 - FAEL: "{C40653C9-016E-4EAD-B9BA-8F43C387CBE6}" | In - Domain - P17 - TRUE | .(.Microsoft Corporation - Windows Media Player.) -- C:\Program Files\Windows Media Player\wmplayer.exe =>.Microsoft Corporation

O87 - FAEL: "{E26D8695-AE13-49C5-96E6-DC9EEDF895AD}" | Out - Domain - P17 - TRUE | .(.Microsoft Corporation - Windows Media Player.) -- C:\Program Files\Windows Media Player\wmplayer.exe =>.Microsoft Corporation

O87 - FAEL: "{C8B4518A-601C-4AEE-8269-DF593C70F33C}" | Out - Domain - P6 - TRUE | .(.Microsoft Corporation - Windows Media Player.) -- C:\Program Files\Windows Media Player\wmplayer.exe =>.Microsoft Corporation

O87 - FAEL: "{282FC624-7AF5-44AB-B3B5-836AA6F3E2B5}" | In - Private - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "{E30207C0-6819-4775-BB13-E5F059E8CAAD}" | Out - Private - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "{6734A08D-FCE8-480A-AB32-4882BB9097AB}" | In - Private - P6 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "{1E98149C-19A1-40F6-873E-1B4518C1A3C3}" | Out - Private - P6 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "{5183B837-8262-4C3A-9D22-31CE9EB3D7F6}" | In - Domain - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "{EA23533D-586B-43A1-8554-C45B86A3D009}" | Out - Domain - P17 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "{3E2499DF-41D9-4E27-AEF6-5A5FEE3A9770}" | In - Private - P17 - TRUE | .(.Microsoft Corporation - Windows Media Player.) -- C:\Program Files\Windows Media Player\wmplayer.exe =>.Microsoft Corporation

O87 - FAEL: "{C29363C8-33BD-4D70-9635-1CBC3A22AA96}" | Out - Private - P17 - TRUE | .(.Microsoft Corporation - Windows Media Player.) -- C:\Program Files\Windows Media Player\wmplayer.exe =>.Microsoft Corporation

O87 - FAEL: "{58F77693-8DF1-44A6-9A25-51E2406D98F0}" | Out - Private - P6 - TRUE | .(.Microsoft Corporation - Windows Media Player.) -- C:\Program Files\Windows Media Player\wmplayer.exe =>.Microsoft Corporation

O87 - FAEL: "{A7BEE2BB-DC51-4E24-B1EC-BAD479620923}" | In - Private - P17 - TRUE | .(.Microsoft Corporation - Service Partage réseau du Lecteur Windows Media.) -- C:\Program Files\Windows Media Player\wmpnetwk.exe =>.Microsoft Corporation

O87 - FAEL: "{D03156AD-79F0-420A-BCAA-CE660ACEB71A}" | Out - Private - P17 - TRUE | .(.Microsoft Corporation - Service Partage réseau du Lecteur Windows Media.) -- C:\Program Files\Windows Media Player\wmpnetwk.exe =>.Microsoft Corporation

O87 - FAEL: "{BEED6C56-6AA2-4909-87DB-9DC7D0EC45E2}" | In - Private - P6 - TRUE | .(.Microsoft Corporation - Service Partage réseau du Lecteur Windows Media.) -- C:\Program Files\Windows Media Player\wmpnetwk.exe =>.Microsoft Corporation

O87 - FAEL: "{791E8158-7928-44EB-8267-541C94321B60}" | Out - Private - P6 - TRUE | .(.Microsoft Corporation - Service Partage réseau du Lecteur Windows Media.) -- C:\Program Files\Windows Media Player\wmpnetwk.exe =>.Microsoft Corporation

O87 - FAEL: "{2B95639E-CC9F-40D2-A0E8-BA49A683DECE}" | Out - Domain - P6 - TRUE | .(.Microsoft Corporation - Processus hôte pour les services Windows.) -- C:\Windows\system32\svchost.exe =>.Microsoft Corporation

O87 - FAEL: "TCP Query User{BBD55FA1-354E-47B5-BE25-91C8DBAEFC3F}C:\users\rondeau\appdata\roaming\cacaoweb\cacaoweb.exe" |In - Private - P6 - TRUE | .(...) -- C:\users\rondeau\appdata\roaming\cacaoweb\cacaoweb.exe (.not file.) =>PUP.CacaoWeb

O87 - FAEL: "UDP Query User{76FB117C-C286-47AA-B18F-5E70541509C5}C:\users\rondeau\appdata\roaming\cacaoweb\cacaoweb.exe" |In - Private - P17 - TRUE | .(...) -- C:\users\rondeau\appdata\roaming\cacaoweb\cacaoweb.exe (.not file.) =>PUP.CacaoWeb

O87 - FAEL: "{3C5BF7D7-4BED-4FD8-9A69-81B374723CC7}" | In - None - P17 - TRUE | .(.Hewlett-Packard Co. - DeviceSetup.exe.) -- C:\Program Files\HP\HP Photosmart 5520 series\Bin\DeviceSetup.exe =>.Hewlett-Packard Co

O87 - FAEL: "{DBFC0762-BA52-475E-AC31-D1AED322EE10}" | In - None - P17 - TRUE | .(.Hewlett-Packard Co. - HPNetworkCommunicator.) -- C:\Program Files\HP\HP Photosmart 5520 series\Bin\HPNetworkCommunicator.exe =>.Hewlett-Packard Co

O87 - FAEL: "{21685ECC-BA3A-4626-8B18-D5CBEE4853AD}" | In - None - P17 - TRUE | .(.Hewlett-Packard Co. - HPNetworkCommunicatorCom.) -- C:\Program Files\HP\HP Photosmart 5520 series\Bin\HPNetworkCommunicatorCom.exe =>.Hewlett-Packard Co

O87 - FAEL: "TCP Query User{9D664E94-3FB3-4BD0-A78F-AE1795958AA8}C:\users\rondeau\appdata\roaming\cacaoweb\cacaoweb.exe" |In - Public - P6 - TRUE | .(...) -- C:\users\rondeau\appdata\roaming\cacaoweb\cacaoweb.exe (.not file.) =>PUP.CacaoWeb

O87 - FAEL: "UDP Query User{6C7DB1F0-8C81-4FD4-9F01-CE0AEDC89D91}C:\users\rondeau\appdata\roaming\cacaoweb\cacaoweb.exe" |In - Public - P17 - TRUE | .(...) -- C:\users\rondeau\appdata\roaming\cacaoweb\cacaoweb.exe (.not file.) =>PUP.CacaoWeb

O87 - FAEL: "{D3A771EB-7535-4FDF-8A7E-E3EA4188B7A8}" | In - None - P6 - FALSE | .(.Microsoft Corporation - SMSvcHost.exe.) -- C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMSvcHost.exe

O87 - FAEL: "{5B0F0AF6-C742-4069-B91C-DE91D48148F6}" | In - Private - P6 - TRUE | .(.eInstruction Corporation - Launcher Application.) -- C:\Program Files\eInstruction\Device Manager\Launch.exe

O87 - FAEL: "{AEB27AF4-6CAF-4213-A550-5BC42C109FDF}" | In - Private - P17 - TRUE | .(.eInstruction Corporation - Launcher Application.) -- C:\Program Files\eInstruction\Device Manager\Launch.exe

O87 - FAEL: "{0191F038-3CCC-47EE-B54A-1720CC53A07E}" | In - Private - P6 - TRUE | .(.Sun Microsystems, Inc. - Java(TM) Platform SE binary.) -- C:\Program Files\eInstruction\Device Manager\jre\bin\java.exe

O87 - FAEL: "{9288FC0C-8080-4FBA-A0D9-E173D51F4825}" | In - Private - P17 - TRUE | .(.Sun Microsystems, Inc. - Java(TM) Platform SE binary.) -- C:\Program Files\eInstruction\Device Manager\jre\bin\java.exe

O87 - FAEL: "{A147F762-D033-42B3-AF51-4D7C9B9CB2DA}" | In - Private - P6 - TRUE | .(.Sun Microsystems, Inc. - Java(TM) Platform SE binary.) -- C:\Program Files\eInstruction\Device Manager\jre\bin\javaw.exe

O87 - FAEL: "{40DA8149-6215-4639-A0A2-C7AE7BBD6EE1}" | In - Private - P17 - TRUE | .(.Sun Microsystems, Inc. - Java(TM) Platform SE binary.) -- C:\Program Files\eInstruction\Device Manager\jre\bin\javaw.exe

O87 - FAEL: "TCP Query User{8C48B63B-B969-457B-AF8D-1BE4C4F514CC}C:\program files\einstruction\device manager\launch.exe" | In - Public - P6 - TRUE | .(.eInstruction Corporation - Launcher Application.) -- C:\program files\einstruction\device manager\launch.exe

O87 - FAEL: "UDP Query User{F8E531F6-E0E5-47FC-B1D7-920E9FA77220}C:\program files\einstruction\device manager\launch.exe" | In - Public - P17 - TRUE | .(.eInstruction Corporation - Launcher Application.) -- C:\program files\einstruction\device manager\launch.exe

O87 - FAEL: "TCP Query User{3492DE3E-CADF-49A4-8000-29870A3317BD}C:\program files\einstruction\workspace\iw.exe" | In - Private - P6 - TRUE | .(.GTCO CalComp, Inc. - Interwrite WorkSpace.) -- C:\program files\einstruction\workspace\iw.exe

O87 - FAEL: "UDP Query User{01BA427A-6267-4BDC-A708-8BAB7D15336D}C:\program files\einstruction\workspace\iw.exe" | In - Private - P17 - TRUE | .(.GTCO CalComp, Inc. - Interwrite WorkSpace.) -- C:\program files\einstruction\workspace\iw.exe

~ Firewall: 231 Scanned in 00mn 03s

---\\ Enumère les codes produits des logiciels (PUC) (O90)

O90 - PUC: "076CFAAAB965F2A4284B2449E5D03EFE" . (.Windows Live Writer.) -- C:\Windows\Installer\{AAAFC670-569B-4A2F-82B4-42945E0DE3EF}\ApplicationIcon.ico

O90 - PUC: "0C11FED6FF5306145A34DF3D634CAD5E" . (.Microsoft SQL Server 2005 Express Edition.) -- C:\Windows\Installer\{6DEF11C0-35FF-4160-A543-FDD336C4DAE5}\ARPIcon.ico

O90 - PUC: "11F12B5E3396B0E42AC597363E0CD711" . (.Windows Live Messenger.) -- C:\Windows\Installer\{E5B21F11-6933-4E0B-A25C-7963E3C07D11}\MsblIco.Exe

O90 - PUC: "16525446F96163A42AFF5B1E81CE565F" . (.ASUS SmartLogon.) -- C:\Windows\Installer\{64452561-169F-4A36-A2FF-B5E118EC65F5}\\_294823.exe

O90 - PUC: "1C4235E6CF4867F4A9A36CE5708FE06E" . (.Complément Messenger.) -- C:\Windows\Installer\{6E5324C1-84FC-4F76-9A3A-C65E07F80EE6}\CompanionIcon

O90 - PUC: "21F1DBD139DE0C947ACC65BCED841885" . (.ASUS LifeFrame3.) -- C:\Windows\Installer\{1DBD1F12-ED93-49C0-A7CC-56CBDE488158}\\_6FEFF9B68218417F98F549.exe

O90 - PUC: "25DBD7E0790BB2F47A7C1F500B2DF0BD" . (.LightScribe System Software 1.14.17.1.) -- C:\Windows\Installer\{0E7DBD52-B097-4F2B-A7C7-F105B0D20FDB}\ARPPRODUCTICON.exe

O90 - PUC: "277C90D53BCEB244C96C4B43C187DF2C" . (.Apple Application Support.) -- C:\Windows\Installer\{5D09C772-ECB3-442B-9CC6-B4341C78FDC2}\WinInstall.ico

O90 - PUC: "2D00C1F62C52ABC41862EAA9E6E2C95D" . (.HP Update.) -- C:\Windows\Installer\{6F1C00D2-25C2-4CBA-8126-AE9A6E2E9CD5}\ARPPRODUCTICON.exe

O90 - PUC: "38E1FB04BE028D11795C00905C206085" . (.Power2Go.) -- C:\Windows\Installer\{40BF1E83-20EB-11D8-97C5-0009C5020658}\ARPPRODUCTICON.exe

O90 - PUC: "3E2D8E8CA6FED1B40AE9B772BE2E3FEC" . (.RealDownloader.) -- C:\Windows\Installer\{C8E8D2E3-EF6A-4B1D-A09E-7B27EBE2F3CE}\AddRemoveProgramsIcon

O90 - PUC: "46B5A9879DD95AB419A50FCFA0B1B7EF" . (.Apple Software Update.) -- C:\Windows\Installer\{789A5B64-9DD9-4BA5-915A-F0FC0A1B7BFE}\Installer.ico =>.Apple Inc

O90 - PUC: "617DD6FF01B79624F991FF0BA74CDC59" . (.Bing Bar.) -- C:\Windows\Installer\{FF6DD716-7B10-4269-9F19-FFB07AC4CD95}\icon\_installer\_ico =>Toolbar.Bing

O90 - PUC: "61F61FCBE0CAEBA49AFE14C24F48AB15" . (.Windows Live Family Safety.) -- C:\Windows\Installer\{BCF16F16-AC0E-4ABE-A9EF-412CF484BA51}\fssicon.ico

O90 - PUC: "67A15D72D1736B840BE614731AB55738" . (.Express Gate.) -- C:\Windows\Installer\{27D51A76-371D-48B6-B06E-4137A15B7583}\ARPPRODUCTICON.exe

O90 - PUC: "6896871EBF7C3E541A1DA3B098B9E972" . (.Étude pour l'amélioration du produit HP Photosmart 5520 series.) -- C:\Windows\Installer\{E1786986-C7FB-45E3-A1D1-3A0B899B9E27}\ARP\_Icon =>.Hewlett-Packard Co

O90 - PUC: "68AB67CA7DA76301B7448A2100000030" . (.Adobe Reader 8.1.2 - Français.) -- C:\Windows\Installer\{AC76BA86-7AD7-1036-7B44-A81200000003}\SC\_Reader.exe

O90 - PUC: "68AB67CA7DA784420000080000000030" . (.Chinese Traditional Fonts Support For Adobe Reader 8.) -- C:\Windows\Installer\{AC76BA86-7AD7-2448-0000-800000000003}\ARPPRODUCTICON.exe

O90 - PUC: "6F7A77B636DD31F46AFF3831A7A53C45" . (.ASUS CopyProtect.) -- C:\Windows\Installer\{6B77A7F6-DD63-4F13-A6FF-83137A5AC354}\\_6FEFF9B68218417F98F549.exe

O90 - PUC: "743C7362DAD96D11E92A0050D5C07A16" . (.PowerCinema.) -- C:\Windows\Installer\{2637C347-9DAD-11D6-9EA2-00055D0CA761}\ARPPRODUCTICON.exe

O90 - PUC: "7DDFFFA258DE09A4C825D59ABECDB9F8" . (.Microsoft SQL Server 2005 Express Edition (SQLEXPRESS).) -- C:\Windows\Installer\{2AFFFDD7-ED85-4A90-8C52-5DA9EBDC9B8F}\ARPIcon.ico

O90 - PUC: "98B4807E0E963B641A81F8990D9688DC" . (.Microsoft SQL Server VSS Writer.) -- C:\Windows\Installer\{E7084B89-69E0-46B3-A118-8F99D06988CD}\ARPIco

O90 - PUC: "9B224D5D679689E4D8FD6923BC15D5E7" . (.Dragon NaturallySpeaking 12.5.) -- C:\Windows\Installer\{D5D422B9-6976-4E98-8DDF-9632CB515D7E}\ARPPRODUCTICON.exe

O90 - PUC: "A8A8AEE42356E3A4B800CD0C09EF09E2" . (.WorkSpace.) -- C:\Windows\Installer\{4EEA8A8A-6532-4A3E-8B00-DCC090FE902E}\ARPPRODUCTICON.exe

O90 - PUC: "A9FA4D8DEDA641B47A5FAB58782927E9" . (.ASUS Security Protect Manager.) -- C:\Windows\Installer\{D8D4AF9A-6ADE-4B14-A7F5-BA858792729E}\ARPPRODUCTICON.exe

O90 - PUC: "ABFAB76BF9C4AF84496939E3B3520544" . (.QuickTime.) -- C:\Windows\Installer\{B67BAFBA-4C9F-48FA-9496-933E3B255044}\Installer.ico

O90 - PUC: "B03FD4BEB201C0F429A75DE030A723D5" . (.AuthenTec Fingerprint Sensor Minimum Install.) -- C:\Windows\Installer\{EB4DF30B-102B-4F0C-927A-D50E037A325D}\ARPPRODUCTICON.exe

O90 - PUC: "BF2F50B3B5472104DA2F34F9632B7EB0" . (.ATKOSD2.) -- C:\Windows\Installer\{3B05F2FB-745B-4012-ADF2-439F36B2E70B}\\_294823.exe

O90 - PUC: "D29550C7B424BC645B500E10E3E8579C" . (.ATK Hotkey.) -- C:\Windows\Installer\{7C05592D-424B-46CB-B505-E0013E8E75C9}\\_294823.exe

O90 - PUC: "D649DCF0E6C167444A14889BDA8EA8AC" . (.Logiciel de base du périphérique HP Photosmart 5520 series.) -- C:\Windows\Installer\{0FCD946D-1C6E-4476-A441-88B9ADE88ACA}\ARP\_Icon =>.Hewlett-Packard Co

O90 - PUC: "D7314F9862C648A4DB8BE2A5B47BE100" . (.Microsoft Silverlight.) -- C:\Windows\Installer\{89F4137D-6C26-4A84-BDB8-2E5A4BB71E00}\ARPIcon

O90 - PUC: "DAFE66EDCC9B4DF41975C6815E011016" . (.Dolby Control Center.) -- C:\Windows\Installer\{DE66EFAD-B9CC-4FD4-9157-6C18E5100161}\\_6FEFF9B68218417F98F549.exe

O90 - PUC: "E0785E1D5E3E5744896ADA6D4125A4FD" . (.ATK Media.) -- C:\Windows\Installer\{D1E5870E-E3E5-4475-98A6-ADD614524ADF}\\_18be6784.exe

O90 - PUC: "EE3C5F35DE50038499B4052B0F5DF0EC" . (.Microsoft SQL Server Setup Support Files (English).) -- C:\Windows\Installer\{53F5C3EE-05ED-4830-994B-50B2F0D50FCE}\ARPIcon.ico

O90 - PUC: "F23D07676EAD94E4C8B83B0FB8B56168" . (.Microsoft SQL Server Native Client.) -- C:\Windows\Installer\{7670D32F-DAE6-4E49-8C8B-B3F08B5B1686}\ARPIco

O90 - PUC: "F8891D30F9643484E8E65EEFD97188D9" . (.WIDCOMM Bluetooth Software.) -- C:\Windows\Installer\{03D1988F-469F-4843-8E6E-E5FE9D17889D}\ARPPRODUCTICON.exe

O90 - PUC: "F8E4622A94613E11B8DE8BCAF689CC3E" . (.Google Earth.) -- C:\Windows\Installer\{A2264E8F-1649-11E3-8BED-B8AC6F98CCE3}\ARPPRODUCTICON.exe

O90 - PUC: "FB9326B958E40954D827153ED01B9AAA" . (.ASUS Power4Gear eXtreme.) -- C:\Windows\Installer\{9B6239BF-4E85-4590-8D72-51E30DB1A9AA}\\_6FEFF9B68218417F98F549.exe

~ Update Products: 141 Scanned in 00mn 00s

---\\ Recherche des packages WindowsInstaller (WIS) (O93) (NTFS)

[MD5.220F8CFDE0D78DF96A2FF7ADDE4EA490] [WIS][04/12/2008] (.devicevm - Blank Project Template.) -- C:\Windows\Installer\2fd1c.msi [4288512]

[MD5.9DD5657F71D1797B36F244FD8A9EF679] [WIS][04/02/2014] (.eInstruction - WorkSpace.) -- C:\Windows\Installer\5ba3e.msi [46919168]

[MD5.1C73AB401206E88D705E97558DECA813] [WIS][30/01/2011] (.Les Editions Hatier - svt2.) -- C:\Windows\Installer\9bfb49.msi [212480]

[MD5.02D33D80DCC8CC594B3AFC03196BFD61] [WIS][04/12/2008] (.Cognizance Corporation - Cognizance Identity Manager.) -- C:\Windows\Installer\a88e0.msi [465920]

[MD5.1BC14532F27BAB53191210B86B1E6AF1] [WIS][04/12/2008] (.Broadcom Corp. - WIDCOMM Bluetooth Profile Pack.) -- C:\Windows\Installer\a88f5.msi [3501568]

[MD5.89856DE6CB7FF7AE080E10A9E7161D69] [WIS][04/02/2014] (.eInstruction - WorkSpace Content.) -- C:\Windows\Installer\b3d71.msi [6352384]

[MD5.157FE39C329134AFCB1AA152F46892EA] [WIS][29/01/2014] (.Ask.com - Blank Project Template.) -- C:\Windows\Installer\b64fc.msi [2426880]

~ WIS: 148 Scanned in 00mn 20s

---\\ Etat général des services non Microsoft (EGS) (SR=Running, SS=Stopped)

SS - | Demand 21/02/2014 257928 | (AdobeFlashPlayerUpdateSvc) . (.Adobe Systems Incorporated.) - C:\Windows\system32\Macromed\Flash\FlashPlayerUpdateService.exe

SS - | Demand 05/11/2010 30192 | (GoogleDesktopManager-051210-111108) . (.Google.) - C:\Program Files\Google\Google Desktop Search\GoogleDesktop.exe

SS - | Demand 16/09/2012 194032 | (gusvc) . (.Google.) - C:\Program Files\Google\Common\Google Updater\GoogleUpdaterService.exe

SR - | Auto 19/12/2013 440376 | (AntiVirSchedulerService) . (.Avira Operations GmbH & Co. KG.) - C:\Program Files\Avira\AntiVir Desktop\sched.exe

SR - | Auto 27/11/2013 440376 | (AntiVirService) . (.Avira Operations GmbH & Co. KG.) - C:\Program Files\Avira\AntiVir Desktop\avguard.exe

SR - | Auto 19/12/2013 1011768 | (AntiVirWebService) . (.Avira Operations GmbH & Co. KG.) - C:\Program Files\Avira\AntiVir Desktop\AVWEBGRD.exe

SR - | Auto 21/01/2008 21504 | C:\Program Files\ASUS Security Center\ASUS Security Protect Manager\Bin\ASWLNPkg.dll (ASBroker) . (.Cognizance Corporation.) - C:\Windows\System32\svchost.exe

SR - | Auto 21/01/2008 21504 | C:\Program Files\ASUS Security Center\ASUS Security Protect Manager\Bin\AsChnl.dll (ASChannel) . (.Cognizance Corporation.) - C:\Windows\System32\svchost.exe

SR - | Auto 03/10/2007 94208 | (ASLDRService) . (...) - C:\Program Files\ASUS\ATK Hotkey\ASLDRSrv.exe

SR - | Auto 08/08/2007 94208 | (ATKGFNEXSrv) . (...) - C:\Program Files\ATKGFNEX\GFNEXSrv.exe

SR - | Auto 16/12/2013 193696 | (BBSvc) . (.Microsoft Corporation..) - C:\Program Files\Microsoft\BingBar\7.3.124.0\BBSvc.exe

SR - | Demand 16/12/2013 247968 | (BBUpdate) . (.Microsoft Corporation..) - C:\Program Files\Microsoft\BingBar\7.3.124.0\SeaPort.exe

SR - | Auto 10/04/2008 518696 | (btwdins) . (.Broadcom Corporation..) - C:\Program Files\WIDCOMM\Bluetooth Software\bin\btwdins.exe

SR - | Auto 08/03/2013 311184 | (DragonSvc) . (.Nuance Communications, Inc..) - C:\Program Files\Common Files\Nuance\dgnsvc.exe

SR - | Auto 09/06/2008 73728 | (LightScribeService) . (.Hewlett-Packard Company.) - C:\Program Files\Common Files\LightScribe\LSSrvc.exe

SR - | Auto 25/06/2008 196608 | (nvsvc) . (.NVIDIA Corporation.) - C:\Windows\System32\nvvsvc.exe

SR - | Auto 14/08/2013 39056 | (RealNetworks Downloader Resolver Service) . (...) - C:\Program Files\RealNetworks\RealDownloader\rndlresolversvc.exe

SR - | Auto 03/08/2007 125496 | (spmgr) . (...) - C:\Program Files\ASUS\NB Probe\SPM\spmgr.exe

SR - | Auto 23/01/2012 92592 | (TomTomHOMEService) . (.TomTom.) - C:\Program Files\TomTom HOME 2\TomTomHOMEService.exe

SR - | Auto 21/01/2008 21504 | C:\Program Files\Windows Defender\mpsvc.dll (WinDefend) . (.Microsoft Corporation.) - C:\Windows\System32\svchost.exe

SR - | Auto 21/01/2008 21504 | C:\Windows\System32\wuaueng.dll (wuauserv) . (.Microsoft Corporation.) - C:\Windows\System32\svchost.exe

SR - | Auto 20/05/2008 61424 | ({49DE1C67-83F8-4102-99E0-C16DCC7EEC796}) . (.Cyberlink Corp..) - C:\Program Files\ASUS\AI TouchMedia\PlayMovie\000.fcl

~ Services: Scanned in 00mn 22s

---\\ Recherche d'infection sur le Master Boot Record (MBR)(O80)

Stealth MBR rootkit/Mebroot/Sinowal/TDL4 detector 0.4.2 by Gmer, http://www.gmer.net

Run by RONDEAU at 03/03/2014 21:15:34

device: opened successfully

user: MBR read successfully

Disk trace:

called modules: ntkrnlpa.exe CLASSPNP.SYS disk.sys acpi.sys hal.dll iaStor.sys

C:\Windows\system32\DRIVERS\iaStor.sys Intel Corporation Intel Matrix Storage Manager driver

1 ntkrnlpa!IofCallDriver[0x82688916] >> \Device\Harddisk0\DR0[0x86B2B1D8]

3 CLASSPNP[0x8ADA58B3] >> ntkrnlpa!IofCallDriver[0x82688916] >> [0x8594ACB8]

5 acpi[0x8069A6BC] >> ntkrnlpa!IofCallDriver[0x82688916] >> \Device\Ide\IAAStorageDevice-1[0x85986028]

kernel: MBR read successfully

user & kernel MBR OK

~ MBR: 14 Scanned in 00mn 02s

---\\ Recherche d'infection sur le Master Boot Record (MBRCheck)(O80)

Written by ad13, http://ad13.geekstog

Run by RONDEAU at 03/03/2014 21:15:36

\*\*\*\*\*\*\*\*\* Dump file Name \*\*\*\*\*\*\*\*\*

C:\PhysicalDisk0\_MBR.bin

~ MBR: Scanned in 00mn 04s

---\\ Scan Additionnel (O88)

Database Version : 13031 - (03/03/2014)

Clés trouvées (Keys found) : 7

Valeurs trouvées (Values found) : 2

Dossiers trouvés (Folders found) : 1

Fichiers trouvés (Files found) : 1

[HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{1DAD3AF3-EF2F-4F64-AC4B-11789189FCB6}] =>Toolbar.Bing^

[HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\{FF6DD716-7B10-4269-9F19-FFB07AC4CD95}] =>Toolbar.Bing^

[HKCU\Software\Microsoft\Windows\CurrentVersion\Uninstall\Browsersafeguard] =>PUP.BrowserSafeguard^

[HKLM\Software\Classes\CLSID\{00000000-6E41-4FD3-8538-502F5495E5FC}] =>Toolbar.AskTBar

[HKCU\Software\Microsoft\Internet Explorer\Low Rights\ElevationPolicy\{A5AA24EA-11B8-4113-95AE-9ED71DEAF12A}] =>Toolbar.Ask

[HKCU\Software\APN] =>Toolbar.Ask

[HKLM\Software\APN] =>Toolbar.Ask

[HKLM\Software\Microsoft\Internet Explorer\Toolbar]:{eec0f710-38b5-4aba-99bf-ec87564a4e13} =>Toolbar.Bing^

[HKCU\Software\Microsoft\Internet Explorer\URLSearchHooks]:{00000000-6E41-4FD3-8538-502F5495E5FC} =>Adware.ShopperReports

C:\Users\RONDEAU\AppData\Local\Software =>Adware.Boxore

[HKCU\Software\BrowsersafeguardInstalled] =>PUP.BrowserSafeguard^

~ Additionnel Scan: 376641 Items scanned in 00mn 28s

---\\ Récapitulatif des détections trouvées sur votre station

~ http://nicolascoolman.webs.com/apps/blog/show/41011964-pup-awesomehp =>PUP.Awesomehp

~ http://nicolascoolman.webs.com/apps/blog/show/27232411-hijacker-proxy =>Hijacker.Proxy

~ http://nicolascoolman.webs.com/apps/blog/show/32799788-pup-browsersafeguard =>PUP.BrowserSafeguard

~ http://nicolascoolman.webs.com/apps/blog/show/38737316-pup-wpmanager =>PUP.WpManager

~ http://nicolascoolman.webs.com/apps/blog/show/28927746-toolbar-ask =>Toolbar.Ask

~ http://nicolascoolman.webs.com/apps/blog/show/27566847-pup-cacaoweb =>PUP.CacaoWeb

~ http://nicolascoolman.webs.com/apps/blog/show/26626977-adware-boxore =>Adware.Boxore

~ MSI: 7 link(s) detected in 00mn 29s

End of the scan (2768 lines in 10mn 39s)(0)