~ Rapport de ZHPDiag v2014.7.6.102 - Nicolas Coolman (06/07/2014)

~ Lancé par manu (07/07/2014 16:05:19)

~ Adresse du Site Web http://nicolascoolman.fr

~ Adresse du Forum http://forum.nicolascoolman.fr

~ Traduit par Nicolas Coolman

~ Etat de la version : Version à jour.

~ Liste blanche : Désactivée par l'utilisateur

~ Elévation des Privilèges : OK

~ User Account Control (UAC): Activate by user

---\\ Navigateurs Internet

MSIE: Internet Explorer v9.0.8112.16421 (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

~ Windows Operating System - Vista, OEM\_SLP channel

System Locked Preinstallation (OEM\_SLP) : OK

Windows ID Activation : OK

~ Windows Partial Key : G6MF9

Windows License : OK

Windows Automatic Updates : OK

---\\ Logiciels de protection du système

avast! Internet Security v9.0.2021

Malwarebytes Anti-Malware version 2.0.2.1012

---\\ Logiciels d'optimisation du système

CCleaner v4.15

---\\ Logiciels de partage PeerToPeer

---\\ Surveillance de Logiciels

Adobe Flash Player 14 ActiveX

Adobe Reader XI

---\\ Informations sur le système

~ Processor: x86 Family 6 Model 15 Stepping 13, GenuineIntel

~ Operating System: 32 Bits

Boot mode: Normal (Normal boot)

Total RAM: 2045 MB (55% free)

System Restore: Activé (Enable)

System drive C: has 20 GB (13%) free of 140 GB

---\\ Mode de connexion au système

~ Computer Name: PC-DE-MANU

~ User Name: manu

~ All Users Names: Manu Internet, manu, Administrateur,

~ Unselected Option: None

Logged in as Administrator

---\\ Variables d'environnement

~ System Unit : C:\

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

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

~ %Desktop% : C:\Users\manu\Desktop\

~ %Favorites% : C:\Users\manu\Favorites\

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

~ %StartMenu% : C:\Users\manu\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 20 Go of 140 Go)

D: Floppy drive, Flash card reader, USB Key (Not Inserted)

E: Floppy drive, Flash card reader, USB Key (Not Inserted)

F: CD-ROM drive (Not Inserted)

---\\ Etat du Centre de Sécurité Windows

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

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

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

[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] DisableTaskMgr: OK

[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] DisableRegistryTools: 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.) (.19/01/2008 - 08:33:37.) -- C:\Windows\System32\Wininit.exe [96768]

[MD5.CFD26829131439B71D0109F9D5345573] - (.Microsoft Corporation - Extensions Internet pour Win32.) (.28/05/2014 - 17:32:59.) -- C:\Windows\System32\wininet.dll [1129472]

[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.) (.19/01/2008 - 06:28:02.) -- 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.) (.19/01/2008 - 06:49:18.) -- C:\Windows\system32\Drivers\i8042prt.sys [54784]

[MD5.8793643A67B42CEC66490B2A0CF92D68] - (.Microsoft Corporation - IP Network Address Translator.) (.19/01/2008 - 06:56:28.) -- 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.) (.19/01/2008 - 06:56:34.) -- C:\Windows\system32\Drivers\Rasl2tp.sys [76288]

[MD5.E8BD98D46F2ED77132BA927FCCB47D8B] - (.Microsoft Corporation - Microsoft RDP Device redirector.) (.02/11/2006 - 10:03:00.) -- C:\Windows\system32\Drivers\rdpdr.sys [242688]

[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) : 1/2

~ Mes musiques (My Musics) : 1/2

~ Mes Videos (My Videos) : 1/5

~ Mes Favoris (My Favorites) : 1/189

~ Mes Documents (My Documents) : 1/732

~ Mon Bureau (My Desktop) : 1/177

~ Menu demarrer (Programs) : 1/23

~ Hidden Files: Scanned in 00mn 01s

---\\ Processus lancés

[MD5.349AB4F70E2AC44970894E7F03E1576E] - (.Huawei Technologies Co., Ltd. - DataCardMonitor MFC Application.) -- C:\ProgramData\DatacardService\DCSHelper.exe [236384] [PID.3728]

[MD5.0D392EDE3B97E0B3131B2F63EF1DB94E] - (.Microsoft Corporation - Windows Defender User Interface.) -- C:\Program Files\Windows Defender\MSASCui.exe [1008184] [PID.3912]

[MD5.82EAD5A5804BB2937416254A45B6C3C0] - (.Realtek Semiconductor - HD Audio Control Panel.) -- C:\Windows\RtHDVCpl.exe [4489216] [PID.3940]

[MD5.5CE6D96C5210D5B0145EE39C0B8E7C8A] - (.Synaptics, Inc. - Synaptics TouchPad Enhancements.) -- C:\Program Files\Synaptics\SynTP\SynTPEnh.exe [835584] [PID.4016]

[MD5.DC068189910FCC0375B8A9CC9C3D179D] - (.Sony Corporation - Pas de description.) -- C:\Program Files\Sony\ISB Utility\ISBMgr.exe [317560] [PID.2080]

[MD5.D3804513FC9C11A4637392B4F0F43BC5] - (.Intel Corporation - Event Monitor User Notification Tool.) -- C:\Program Files\Intel\Intel Matrix Storage Manager\IAAnotif.exe [182808] [PID.2068]

[MD5.4B555106290BD117334E9A08761C035A] - (...) -- ystem32\rundll32.exe [0] [PID.2672]

[MD5.26AFC1F16494FFE66F2197153B342A27] - (.AVAST Software - avast! Antivirus.) -- C:\Program Files\AVAST Software\Avast\AvastUI.exe [4086432] [PID.2948]

[MD5.D658AB1B55127D18DCFBCAC8CAAEA522] - (.Hewlett-Packard - hpwuSchd Application.) -- C:\Program Files\HP\HP Software Update\hpwuschd2.exe [49208] [PID.2964]

[MD5.882539219B40107D5BC0557E0088DD79] - (.ScanSoft, Inc. - OCR Aware (32-bit).) -- C:\Program Files\ScanSoft\OmniPageSE2.0\opwareSE2.exe [49152] [PID.3068]

[MD5.F7AD0BD4A944A97C13B196215981346C] - (.Oracle Corporation - Java Update Scheduler.) -- C:\Program Files\Common Files\Java\Java Update\jusched.exe [224128] [PID.1340]

[MD5.7E6ACA6B6C89B7CD098944A9159DAED3] - (.TomTom - System Tray application for TomTom HOME.) -- C:\Program Files\TomTom HOME 2\TomTomHOMERunner.exe [248208] [PID.3228]

[MD5.BF08674925F151BD4537B89A493E3E0C] - (.Microsoft Corporation - Media Center Tray Applet.) -- C:\Windows\ehome\ehtray.exe [125952] [PID.3348]

[MD5.DF2D45B134120E0A35EC1FEF343E74F6] - (.Broadcom Corporation. - Bluetooth Tray Application.) -- C:\Program Files\WIDCOMM\Bluetooth Software\BTTray.exe [739880] [PID.3428]

[MD5.2D821AFA5A1A9CA7F9F997A1AAD09E72] - (.Microsoft Corporation - Windows Media Player.) -- C:\Program Files\Windows Media Player\wmplayer.exe [168960] [PID.3388]

[MD5.9C63BAEE102BB99BC10D6E56F3AED7BC] - (.Trusteer Ltd. - RapportService.) -- C:\Users\Manu Internet\AppData\Roaming\Trusteer\Rapport\app\bin\RapportService.exe [2640152] [PID.4136]

[MD5.D0E2BE311D8F0608D90A8FD1369BADD9] - (.Sony Corporation - VAIOUpdt.) -- C:\Program Files\Sony\VAIO Update\VAIOUpdt.exe [753200] [PID.4524]

[MD5.7E0EBC6933621F994BF6C4232548CDA7] - (.Nicolas Coolman - ZHPDiag.) -- C:\Program Files\ZHPDiag\ZHPDiag.exe [8074240] [PID.5736]

[MD5.6080A176D09435FC8E6E800996656E18] - (.Microsoft Corporation - Console IME.) -- C:\Windows\system32\conime.exe [69120] [PID.4444]

[MD5.862BB4CBC05D80C5B45BE430E5EF872F] - (.Microsoft Corporation - Service de gestion des licences Microsoft.) -- C:\Windows\system32\SLsvc.exe [3408896] [PID.1388]

[MD5.73F5C13B431915BAE35254B4E95DFB71] - (.AVAST Software - avast! Service.) -- C:\Program Files\AVAST Software\Avast\AvastSvc.exe [50344] [PID.1720]

[MD5.D386D51B1839E208EF7CCFBFA964638E] - (.AVAST Software - avast! firewall service.) -- C:\Program Files\AVAST Software\Avast\afwServ.exe [106488] [PID.1784]

[MD5.B362181ED3771DC03B4141927C80F801] - (.Adobe Systems Incorporated - Adobe Acrobat Update Service.) -- C:\Program Files\Common Files\Adobe\ARM\1.0\armsvc.exe [65432] [PID.604]

[MD5.5EF3427AE503B5C03A48F7C9FF458B69] - (.Pas de propriétaire - DCSHOST.) -- C:\ProgramData\DatacardService\HWDeviceService.exe [271712] [PID.928]

[MD5.3E42C4691AAD4B1E8D0466F9CBF05CBE] - (.Intel Corporation - RAID Monitor.) -- C:\Program Files\Intel\Intel Matrix Storage Manager\Iaantmon.exe [354840] [PID.1068]

[MD5.213822072085B5BBAD9AF30AB577D817] - (.InterVideo - RegMgr Module.) -- C:\Program Files\Common Files\InterVideo\RegMgr\iviRegMgr.exe [112152] [PID.1008]

[MD5.7E6DD4B34ACD36AF6C711D2BDE91B040] - (.IDT, Inc. - STacSV Module.) -- C:\Windows\system32\stacsv.exe [102400] [PID.2148]

[MD5.E4FAD21646088D79F8889B6531396ACF] - (.TomTom - Windows Service for TomTom HOME.) -- C:\Program Files\TomTom HOME 2\TomTomHOMEService.exe [93072] [PID.2288]

[MD5.8A9F18ADAD471402236CA931553BF79B] - (.Sony Corporation - VAIO Event Service (Service Module).) -- C:\Program Files\Sony\VAIO Event Service\VESMgr.exe [182392] [PID.2360]

[MD5.4D6644132F26EF055A1F754B1C38C084] - (.Sony Corporation - VAIO Entertainment UPnP Client Adapter.) -- C:\Program Files\Common Files\Sony Shared\VAIO Entertainment Platform\VCSW\VCSW.exe [274432] [PID.2400]

[MD5.2E785F4F92C4C67CEBB61DD55ED1F6A1] - (.Sony Corporation - VAIO Entertainment Database Service.) -- C:\Program Files\Common Files\Sony Shared\VAIO Entertainment Platform\VzCdb\VzCdbSvc.exe [192512] [PID.2720]

[MD5.2D876CAD8C7FFB08179DFF361FF851E6] - (.Sony Corporation - VAIO Entertainment File Import Service.) -- C:\Program Files\Common Files\Sony Shared\VAIO Entertainment Platform\VzCdb\VzFw.exe [131072] [PID.3220]

[MD5.B0C84CEA4FE07231BA87A054AF95984D] - (.Sony Corporation - VAIO Event Service(Service Sub Module).) -- C:\Program Files\Sony\VAIO Event Service\VESMgrSub.exe [100472] [PID.3268]

[MD5.EFBF07671FF832FE03437665C03CE41A] - (.Sony Corporation - SPM Module.) -- C:\Program Files\Sony\VAIO Power Management\SPMgr.exe [921600] [PID.4064]

[MD5.0F4195B9B348DE5CF9B822F81704B20E] - (.Microsoft Corporation - Media Center Media Status Aggregator Servic.) -- C:\Windows\ehome\ehmsas.exe [37376] [PID.3508]

[MD5.7942F3D689E5F08D3EC7EDBF3CF9116F] - (.Sony Corporation - VUAgent.) -- C:\Program Files\Sony\VAIO Update\VUAgent.exe [1020976] [PID.5916]

~ Processes Running: Scanned in 00mn 03s

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

P2 - FPN: [HKLM] [@divx.com/DivX Player Plugin,version=1.0.0] - (...) -- C:\Program Files\DivX\DivX Player\npDivxPlayerPlugin.dll (.not file.)

P2 - FPN: [HKLM] [@java.com/DTPlugin,version=11.5.2] - (.Oracle Corporation - NPRuntime Script Plug-in Library for Java(TM) Deploy.) -- C:\Program Files\Java\jre8\bin\dtplugin\npDeployJava1.dll

P2 - FPN: [HKLM] [@java.com/JavaPlugin,version=11.5.2] - (.Oracle Corporation - Next Generation Java Plug-in 11.5.2 for Mozilla browsers.) -- C:\Program Files\Java\jre8\bin\plugin2\npjp2.dll

P2 - FPN: [HKLM] [@ma-config.com/HardwareDetection] - (.Cybelsoft - Plugin NPAPI Ma-Config.com.) -- C:\Program Files\ma-config.com\nphardwaredetection.dll

P2 - FPN: [HKLM] [@Microsoft.com/NpCtrl,version=1.0] - (. Microsoft Corporation - 5.1.30214.0.) -- c:\Program Files\Microsoft Silverlight\5.1.30214.0\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] [Adobe Reader] - (.Adobe Systems Inc. - Adobe PDF Plug-In For Firefox and Netscape 11.0.07.) -- C:\Program Files\Adobe\Reader 11.0\Reader\AIR\nppdf32.dll

~ Firefox Browser: 7 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.bing.com

R0 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = about:blank

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

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

R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft.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

R3 - URLSearchHook: Microsoft Url Search Hook - {CFBFAE00-17A6-11D0-99CB-00C04FD64497} . (.Adobe Systems Inc. - Adobe PDF Plug-In For Firefox and Netscape 11.0.07.) (No version) -- (.not file.)

~ IE Browser: 8 Scanned in 00mn 00s

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

R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyServer = no key

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

O2 - BHO: avast! Online Security - {8E5E2654-AD2D-48bf-AC2D-D17F00898D06} . (.AVAST Software - IE Webrep plugin.) -- C:\Program Files\AVAST Software\Avast\aswWebRepIE.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: Java(tm) Plug-In 2 SSV Helper - {DBC80044-A445-435b-BC74-9C25C1C588A9} . (.Oracle Corporation - Java(TM) Platform SE binary.) -- C:\Program Files\Java\jre8\bin\jp2ssv.dll

~ BHO: 8 Scanned in 00mn 00s

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

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

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

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

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

O4 - HKLM\..\Run: [ISBMgr.exe] . (.Sony Corporation - Pas de description.) -- C:\Program Files\Sony\ISB Utility\ISBMgr.exe

O4 - HKLM\..\Run: [IAAnotif] . (.Intel Corporation - Event Monitor User Notification Tool.) -- C:\Program Files\Intel\Intel Matrix Storage Manager\iaanotif.exe

O4 - HKLM\..\Run: [AppMon Utility] . (.Sony Corporation - App Monitor Utility.) -- C:\Program Files\Sony\AppMonUtil\AppMonUtility.exe

O4 - HKLM\..\Run: [NvSvc] . (.NVIDIA Corporation - NVIDIA Driver Helper Service, Version 101.2.) -- C:\Windows\system32\nvsvc.dll

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

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

O4 - HKLM\..\Run: [OpwareSE2] . (.ScanSoft, Inc. - OCR Aware (32-bit).) -- C:\Program Files\ScanSoft\OmniPageSE2.0\OpwareSE2.exe =>.ScanSoft, Inc

O4 - HKLM\..\Run: [Adobe ARM] . (.Adobe Systems Incorporated - Adobe Reader and Acrobat Manager.) -- C:\Program Files\Common Files\Adobe\ARM\1.0\AdobeARM.exe =>.Adobe Systems Incorporated

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

O4 - HKCU\..\Run: [WMPNSCFG] . (.Microsoft Corporation - Application de configuration du service Par.) -- C:\Program Files\Windows Media Player\WMPNSCFG.exe =>.Microsoft Corporation

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

O4 - HKCU\..\Run: [Skype] . (.Skype Technologies S.A. - Skype.) -- C:\Program Files\Skype\Phone\Skype.exe =>.Skype Technologies S.A.

O4 - HKCU\..\Run: [Mobile Partner] Clé orpheline

O4 - HKUS\.DEFAULT\..\Run: [TELEPHONESURPCAGENT] C:\Program Files\Orange\Telephone sur PC\TelephoneSurPCAgent.exe (.not file.)

O4 - HKUS\S-1-5-18\..\Run: [TELEPHONESURPCAGENT] C:\Program Files\Orange\Telephone sur PC\TelephoneSurPCAgent.exe (.not file.)

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-1-5-19\..\Run: [TELEPHONESURPCAGENT] C:\Program Files\Orange\Telephone sur PC\TelephoneSurPCAgent.exe (.not file.)

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-1-5-20\..\Run: [TELEPHONESURPCAGENT] C:\Program Files\Orange\Telephone sur PC\TelephoneSurPCAgent.exe (.not file.)

O4 - HKUS\S-1-5-21-1182382394-3354541472-2524611106-1000\..\Run: [Sidebar] . (.Microsoft Corporation - Volet Windows.) -- C:\Program Files\Windows Sidebar\sidebar.exe =>.Microsoft Corporation

O4 - HKUS\S-1-5-21-1182382394-3354541472-2524611106-1000\..\Run: [WMPNSCFG] . (.Microsoft Corporation - Application de configuration du service Par.) -- C:\Program Files\Windows Media Player\WMPNSCFG.exe =>.Microsoft Corporation

O4 - HKUS\S-1-5-21-1182382394-3354541472-2524611106-1000\..\Run: [TomTomHOME.exe] . (.TomTom - System Tray application for TomTom HOME.) -- C:\Program Files\TomTom HOME 2\TomTomHOMERunner.exe

O4 - HKUS\S-1-5-21-1182382394-3354541472-2524611106-1000\..\Run: [Skype] . (.Skype Technologies S.A. - Skype.) -- C:\Program Files\Skype\Phone\Skype.exe =>.Skype Technologies S.A.

O4 - HKUS\S-1-5-21-1182382394-3354541472-2524611106-1000\..\Run: [Mobile Partner] Clé orpheline

~ 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\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: &Envoyer à OneNote - {2670000A-7350-4f3c-8081-5663EE0C6C49} . (.Microsoft Corporation - Microsoft Office OneNote Internet Explorer Add-in.) -- C:\Program Files\MICROS~2\Office12\ONBttnIE.dll

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

O9 - Extra button: @btrez.dll,-12650 - {CCA281CA-C863-46ef-9331-5C8D4460577F} . (...) -- C:\Program Files\WIDCOMM\Bluetooth Software\bt\_hot\_icon.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 - Windows Sockets Helper DLL.) -- C:\Windows\system32\wshbth.dll

O10 - WLSP:\000000000006\Winsock LSP File . (.Microsoft Corporation - Fournisseur de service Sockets 2.0 de Microsoft Windows.) -- C:\Windows\system32\mswsock.dll =>.Microsoft Corporation

O10 - WLSP:\000000000007\Winsock LSP File . (.Microsoft Corporation - LDAP RnR Provider DLL.) -- C:\Windows\system32\winrnr.dll

~ Winsock: 7 Scanned in 00mn 00s

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

O17 - HKLM\System\CCS\Services\Tcpip\..\{F7DB4C84-F0EC-40BD-A9DD-38A2611A670C}: DhcpNameServer = 192.168.1.1

O17 - HKLM\System\CS1\Services\Tcpip\..\{F7DB4C84-F0EC-40BD-A9DD-38A2611A670C}: DhcpNameServer = 192.168.1.1

O17 - HKLM\System\CS2\Services\Tcpip\..\{F7DB4C84-F0EC-40BD-A9DD-38A2611A670C}: DhcpNameServer = 192.168.1.1

O17 - HKLM\System\CS3\Services\Tcpip\..\{F7DB4C84-F0EC-40BD-A9DD-38A2611A670C}: DhcpNameServer = 192.168.1.1

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

~ 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 - Winlogon Notify: VESWinlogon . (.Sony Corporation - VAIO Event Service (Winlogon Notification M.) -- C:\Windows\System32\VESWinlogon.dll

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

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

O23 - Service: avast! Firewall (avast! Firewall) . (.AVAST Software - avast! firewall service.) - C:\Program Files\AVAST Software\Avast\afwServ.exe

O23 - Service: HWDeviceService.exe (HWDeviceService.exe) . (.Pas de propriétaire - DCSHOST.) - C:\ProgramData\DatacardService\HWDeviceService.exe

O23 - Service: Intel(R) Matrix Storage Event Monitor (IAANTMON) . (.Intel Corporation - RAID Monitor.) - C:\Program Files\Intel\Intel Matrix Storage Manager\Iaantmon.exe

O23 - Service: IviRegMgr (IviRegMgr) . (.InterVideo - RegMgr Module.) - C:\Program Files\Common Files\InterVideo\RegMgr\iviRegMgr.exe

O23 - Service: Skype Updater (SkypeUpdate) . (.Skype Technologies - Skype Updater Service.) - C:\Program Files\Skype\Updater\Updater.exe

O23 - Service: SigmaTel Audio Service (STacSV) . (.IDT, Inc. - STacSV Module.) - C:\Windows\system32\stacsv.exe

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

O23 - Service: VAIO Event Service (VAIO Event Service) . (.Sony Corporation - VAIO Event Service (Service Module).) - C:\Program Files\Sony\VAIO Event Service\VESMgr.exe

O23 - Service: VAIO Entertainment Database Service (VzCdbSvc) . (.Sony Corporation - VAIO Entertainment Database Service.) - C:\Program Files\Common Files\Sony Shared\VAIO Entertainment Platform\VzCdb\VzCdbSvc.exe

O23 - Service: VAIO Entertainment File Import Service (VzFw) . (.Sony Corporation - VAIO Entertainment File Import Service.) - C:\Program Files\Common Files\Sony Shared\VAIO Entertainment Platform\VzCdb\VzFw.exe

~ Services: 12 Scanned in 00mn 06s

---\\ 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\img21.jpg

O24 - Desktop General: WallPaper - .(...) - C:\Windows\Web\Wallpaper\img21.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)

[MD5.B5D8DE922237CEDDC7992297654A4BE4] [APT] [Adobe Flash Player Updater] (.Adobe Systems Incorporated.) -- C:\Windows\system32\Macromed\Flash\FlashPlayerUpdateService.exe [262320]

[MD5.1AD8512A5C40AD1A0558498D8E0AC2AA] [APT] [avast! Emergency Update] (.AVAST Software.) -- C:\Program Files\AVAST Software\Avast\AvastEmUpdate.exe [808448]

[MD5.11543DEB4316B9DBB42999C83495838F] [APT] [CCleanerSkipUAC] (.Piriform Ltd.) -- C:\Program Files\CCleaner\CCleaner.exe [4624152]

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

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

[MD5.F37774719A5E1B26F57BC1C4B7575E4C] [APT] [HP Deskjet 1050 J410 series.exe] (.Hewlett-Packard Co..) -- C:\Program Files\HP\HP Deskjet 1050 J410 series\Bin\HP Deskjet 1050 J410 series.exe [518504]

[MD5.C39790BA091F3F9EC7DFE5C2E4598DF0] [APT] [HPCustParticipation HP Deskjet 1050 J410 series] (.Hewlett-Packard Co..) -- C:\Program Files\HP\HP Deskjet 1050 J410 series\Bin\HPCustPartic.exe [2551656]

[MD5.7C0E303EB9A6B6E9A659C95EA0D7497F] [APT] [hpUtility.exe] (.Hewlett-Packard Co..) -- C:\Program Files\HP\HP Deskjet 1050 J410 series\Bin\utils\hpUtility.exe [47976]

[MD5.2EFF6334A2BD29E404F6809C37658FCD] [APT] [HpWebReg.exe] (.Hewlett-Packard Co..) -- C:\Program Files\HP\HP Deskjet 1050 J410 series\Bin\HpWebReg.exe [302440]

[MD5.00000000000000000000000000000000] [APT] [ParetoLogic Update Version3] (...) -- C:\Program Files\Common Files\ParetoLogic\UUS3\Pareto\_Update3.exe (.not file.) [0] =>PUP.Paretologic

[MD5.D6417E3EE99744EDECC5978CAC82A1B0] [APT] [PC Health Advisor] (.ParetoLogic, Inc..) -- C:\Program Files\ParetoLogic\PCHA\PCHA.exe [4830512] =>Rogue.PCHealthAdvisor

[MD5.D6417E3EE99744EDECC5978CAC82A1B0] [APT] [PC Health Advisor Defrag] (.ParetoLogic, Inc..) -- C:\Program Files\ParetoLogic\PCHA\PCHA.exe [4830512] =>Rogue.PCHealthAdvisor

[MD5.00000000000000000000000000000000] [APT] [PhotoProduct.exe] (...) -- C:\Program Files\HP Photo Creations\PhotoProduct.exe (.not file.) [0]

[MD5.AF334CA84536E743D6AEF32548223403] [APT] [WSSU] (.Sony Corporation.) -- C:\Program Files\Sony\Wireless Switch Setting Utility\Switcher.exe [469112]

[MD5.D0E2BE311D8F0608D90A8FD1369BADD9] [APT] [VAIO Update] (.Sony Corporation.) -- C:\Program Files\Sony\VAIO Update\VAIOUpdt.exe [753200]

[MD5.8DA7CA826867B626468476657FDEA9C3] [APT] [VAIO Update Self Repair] (.Sony Corporation.) -- C:\Program Files\Sony\VAIO Update\VUSR.exe [281648]

O39 - APT: Adobe Flash Player Updater - (.Adobe Systems Incorporated.) -- C:\Windows\Tasks\Adobe Flash Player Updater.job [1002]

O39 - APT: Adobe Flash Player Updater - (.Adobe Systems Incorporated.) -- C:\Windows\System32\Tasks\Adobe Flash Player Updater [1002]

~ Scheduled Task: 21 Scanned in 00mn 06s

---\\ 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: Java (Sun) - {08B0E5C0-4FCB-11CF-AAA5-00401C608500} . (...) -- C:\Program Files\Java\jre1.6.0\_01\bin\regutils.dll

O40 - ASIC: Microsoft Windows Media Player 11.0 - {22d6f312-b0f6-11d0-94ab-0080c74c7e95} . (.Microsoft Corporation - Windows Media Player Extension.) -- C:\Windows\System32\wmpdxm.dll =>.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: Web Platform Customizations - {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 14.0 r0.) -- C:\Windows\system32\Macromed\Flash\Flash32\_14\_0\_0\_125.ocx

~ Active Setup: 13 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: (aswKbd) . (.AVAST Software - avast! Keyboard Filter Driver.) - C:\Windows\system32\drivers\aswKbd.sys

O41 - Driver: (AswRdr) . (.AVAST Software - avast! TDI Redirect Driver.) - C:\Windows\system32\drivers\aswRdr.sys

O41 - Driver: (aswSnx) . (.AVAST Software - avast! Virtualization Driver.) - C:\Windows\system32\drivers\aswSnx.sys

O41 - Driver: (aswSP) . (.AVAST Software - avast! self protection module.) - C:\Windows\system32\drivers\aswSP.sys

O41 - Driver: (aswTdi) . (.AVAST Software - avast! TDI Filter Driver.) - C:\Windows\system32\drivers\aswTdi.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: (DMICall) . (.Sony Corporation - Windows 2000 DMI Call Kernel Driver.) - C:\Windows\System32\DRIVERS\DMICall.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: 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: 102 Scanned in 00mn 00s

---\\ Logiciels installés (O42)

O42 - Logiciel: Adobe Flash Player 14 ActiveX - (.Adobe Systems Incorporated.) [HKLM] -- Adobe Flash Player ActiveX

O42 - Logiciel: Adobe Reader XI (11.0.07) - Français - (.Adobe Systems Incorporated.) [HKLM] -- {AC76BA86-7AD7-1036-7B44-AB0000000001}

O42 - Logiciel: ArcSoft Magic-i Visual Effects Installer - (.ArcSoft.) [HKLM] -- {9AB83A3C-604D-4B4F-AA25-A23A3FC39844}

O42 - Logiciel: ArcSoft PhotoStudio 5.5 - (.ArcSoft.) [HKLM] -- {D2261C4B-4D9B-4149-8472-31B7A2FEAB91}

O42 - Logiciel: CCleaner - (.Piriform.) [HKLM] -- CCleaner

O42 - Logiciel: CDBurnerXP - (.CDBurnerXP.) [HKLM] -- {7E265513-8CDA-4631-B696-F40D983F3B07}\_is1

O42 - Logiciel: CanoScan Toolbox Ver4.6 - (...) [HKLM] -- {088A077A-8028-408C-AE7B-4512AE2A65A0}

O42 - Logiciel: Click to DVD 2.0.05 Menu Data - (.Sony Corporation.) [HKLM] -- {9E407618-D9CD-4F39-9490-9ED45294073D}

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

O42 - Logiciel: DSD Direct - (.Sony Corporation.) [HKLM] -- {82D5BACA-3619-4D34-99DB-3A65CFB4DA33}

O42 - Logiciel: DSD Playback Plug-in - (.Sony Corporation.) [HKLM] -- {009E7FB7-1775-4D89-8956-F5C9A1C019FC}

O42 - Logiciel: GearDrvs - (.Symantec Corporation.) [HKLM] -- {206FD69B-F9FE-4164-81BD-D52552BC9C23}

O42 - Logiciel: HP Deskjet 1050 J410 series - Enquête sur l'amélioration du produit - (.Hewlett-Packard Co..) [HKLM] -- {0B461C2C-29AC-4FBB-B925-CF7641D370BE}

O42 - Logiciel: HP Deskjet 1050 J410 series Aide - (.Hewlett Packard.) [HKLM] -- {5C90D8CF-F12A-41C6-9007-3B651A1F0D78}

O42 - Logiciel: HP Update - (.Hewlett-Packard.) [HKLM] -- {B0069CFA-5BB9-4C03-B1C6-89CE290E5AFE}

O42 - Logiciel: IDT Audio - (.IDT.) [HKLM] -- {07D8511D-C9FE-4A93-933F-EAA5C8F20095}

O42 - Logiciel: Intel® Matrix Storage Manager - (.Intel Corporation.) [HKLM] -- {9068B2BE-D93A-4C0A-861C-5E35E2C0E09E}

O42 - Logiciel: Java 8 Update 5 - (.Oracle Corporation.) [HKLM] -- {26A24AE4-039D-4CA4-87B4-2F83218005FF}

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

O42 - Logiciel: Logiciel de base du périphérique HP Deskjet 1050 J410 series - (.Hewlett-Packard Co..) [HKLM] -- {21D2DB5B-C7C1-4BFD-B74A-C85A5A1B0184} =>.Hewlett-Packard Co

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

O42 - Logiciel: MSXML 4.0 SP2 (KB927978) - (.Microsoft Corporation.) [HKLM] -- {37477865-A3F1-4772-AD43-AAFC6BCFF99F}

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: Ma-Config.com - (.Cybelsoft.) [HKLM] -- {7EA6E8DF-37B3-4533-B1A4-45E490C77537}

O42 - Logiciel: Malwarebytes Anti-Malware version 2.0.2.1012 - (.Malwarebytes Corporation.) [HKLM] -- Malwarebytes Anti-Malware\_is1

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

O42 - Logiciel: Microsoft Works - (.Microsoft Corporation.) [HKLM] -- {6B1CB38D-E2E4-4a30-933D-EFDEBA76AD9C}

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

O42 - Logiciel: OmniPage SE 2.0 - (.ScanSoft, Inc..) [HKLM] -- {79D5997E-BF79-48BB-8B41-9BE59C15C2D7}

O42 - Logiciel: OpenOffice 4.0.1 - (.Apache Software Foundation.) [HKLM] -- {8D5D54B8-3D29-4AB4-8DA8-1868DAF941D8}

O42 - Logiciel: Outil de restauration de données VAIO - (.Sony Corporation.) [HKLM] -- {57B955CE-B5D3-495D-AF1B-FAEE0540BFEF}

O42 - Logiciel: Paramètres des fonctions d'origine VAIO - (.Sony Corporation.) [HKLM] -- {7C404084-C5A6-42FF-B731-0BAC79A6E134}

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

O42 - Logiciel: Rapport - (.Trusteer.) [HKLM] -- {1DD81E7D-0D28-4CEB-87B2-C041A4FCB215}

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

O42 - Logiciel: Roxio Easy Media Creator Home - (.Roxio.) [HKLM] -- {B7FB0C86-41A4-4402-9A33-912C462042A0} =>.Roxio

O42 - Logiciel: Roxio Easy Media Creator Home - (.Roxio.) [HKLM] -- {C8B0680B-CDAE-4809-9F91-387B6DE00F7C} =>.Roxio

O42 - Logiciel: Security Update for CAPICOM (KB931906) - (.Microsoft Corporation.) [HKLM] -- KB931906

O42 - Logiciel: Security Update for CAPICOM (KB931906) - (.Microsoft Corporation.) [HKLM] -- {0EFDF2F9-836D-4EB7-A32D-038BD3F1FB2A}

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

O42 - Logiciel: Skype™ 6.11 - (.Skype Technologies S.A..) [HKLM] -- {4E76FF7E-AEBA-4C87-B788-CD47E5425B9D}

O42 - Logiciel: SonicStage Mastering Studio - (.Sony Corporation.) [HKLM] -- {6332AFF1-9D9A-429C-AA03-F82749FA4F49}

O42 - Logiciel: SonicStage Mastering Studio Audio Filter - (.Sony Corporation.) [HKLM] -- {DF7DB916-90E5-40F2-9010-B8125EB5FD6F}

O42 - Logiciel: SonicStage Mastering Studio Audio Filter Custom Preset - (.Sony Corporation.) [HKLM] -- {EC37A846-53AC-4DA7-98FA-76A4E74AA900}

O42 - Logiciel: SonicStage Mastering Studio Plugins - (.Sony Corporation.) [HKLM] -- {9C1C8A04-F8CA-4472-A92D-4288CE32DE86}

O42 - Logiciel: Sony Video Shared Library - (.Sony Corporation.) [HKLM] -- {01FDC9FC-4D4F-4DB0-ACD1-D3E8E1D52902}

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

O42 - Logiciel: TomTom HOME - (.Nom de votre société.) [HKLM] -- {99072AB4-D795-44D5-9D65-E3C9F8322C97}

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

O42 - Logiciel: VAIO Content Importer / VAIO Content Exporter - (.Sony Corporation.) [HKLM] -- {68A69CFF-130D-4CDE-AB0E-7374ECB144C8}

O42 - Logiciel: VAIO Content Metadata Intelligent Analyzing Manager - (.Sony Corporation.) [HKLM] -- {FAA6B94E-78A7-489C-B2DB-050D9FEBFADA}

O42 - Logiciel: VAIO Content Metadata Manager Settings - (.Sony Corporation.) [HKLM] -- {12D0BE8D-538C-4AB1-86DE-C540308F50DA}

O42 - Logiciel: VAIO Content Metadata XML Interface Library - (.Sony Corporation.) [HKLM] -- {B5E2DF30-1061-4DB4-AF28-08996C8E5680}

O42 - Logiciel: VAIO Entertainment Platform - (.Sony Corporation.) [HKLM] -- {6B1F20F2-6321-4669-A58C-33DF8E7517FF}

O42 - Logiciel: VAIO Media AC3 Decoder 1.0 - (...) [HKLM] -- {2063C2E8-3812-4BBD-9998-6610F80C1DD4}

O42 - Logiciel: VAIO Movie Story - (.Sony Corporation.) [HKLM] -- {B25563A0-41F4-4A81-A6C1-6DBC0911B1F3}

O42 - Logiciel: VAIO Movie Story Template Data - (.Sony Corporation.) [HKLM] -- {6FA8BA2C-052B-4072-B8E2-2302C268BE9E}

O42 - Logiciel: VAIO MusicBox - (.Sony Corporation.) [HKLM] -- {4EA55D20-27FB-45D7-8726-147E8A5F6C62}

O42 - Logiciel: VAIO Original Screen Saver - (...) [HKLM] -- {1BEF9285-5530-426B-A5F1-5836B95C7EB1}

O42 - Logiciel: VAIO Update - (.Sony Corporation.) [HKLM] -- {9FF95DA2-7DA1-4228-93B7-DED7EC02B6B2}

O42 - Logiciel: VAIO Xblack Contents - (...) [HKLM] -- VAIO Xblack Contents

O42 - Logiciel: VLC media player 2.1.3 - (.VideoLAN.) [HKLM] -- VLC media player =>.VideoLAN

O42 - Logiciel: VU5x86 - (.Sony Corporation .) [HKLM] -- {9D12A8B5-9D41-4465-BF11-70719EB0CD02}

O42 - Logiciel: WIDCOMM Bluetooth Software 6.1.0.1205 - (.Broadcom Corporation.) [HKLM] -- {03D1988F-469F-4843-8E6E-E5FE9D17889D}

O42 - Logiciel: Wi-Fi Modem - (.Huawei Technologies Co.,Ltd.) [HKLM] -- Wi-Fi Modem

O42 - Logiciel: WinDVD for VAIO - (.InterVideo Inc..) [HKLM] -- InstallShield\_{20471B27-D702-4FE8-8DEC-0702CC8C0A85}

O42 - Logiciel: avast! Internet Security v9.0.2021 - (.AVAST Software.) [HKLM] -- avast

~ Logic: 33 Scanned in 00mn 00s

---\\ HKCU & HKLM Software Keys

[HKCU\Software\AVAST Software]

[HKCU\Software\Adobe]

[HKCU\Software\AppDataLow\Software\Google]

[HKCU\Software\AppDataLow\Software\JavaSoft]

[HKCU\Software\AppDataLow]

[HKCU\Software\AsioStHd]

[HKCU\Software\BAE]

[HKCU\Software\Canneverbe Limited]

[HKCU\Software\Canon]

[HKCU\Software\Classes]

[HKCU\Software\Clients]

[HKCU\Software\Conduit] =>Toolbar.Conduit

[HKCU\Software\Corel]

[HKCU\Software\DivXNetworks]

[HKCU\Software\Google]

[HKCU\Software\HP]

[HKCU\Software\IDT]

[HKCU\Software\IM Providers]

[HKCU\Software\InterVideo]

[HKCU\Software\JEDI-VCL]

[HKCU\Software\JavaSoft]

[HKCU\Software\Lake]

[HKCU\Software\Local AppWizard-Generated Applications]

[HKCU\Software\Macromedia]

[HKCU\Software\Malwarebytes' Anti-Malware]

[HKCU\Software\MimarSinan]

[HKCU\Software\MozillaPlugins]

[HKCU\Software\NVIDIA Corporation]

[HKCU\Software\Netscape]

[HKCU\Software\ODBC]

[HKCU\Software\OpenOffice]

[HKCU\Software\ParetoLogic] =>PUP.Paretologic

[HKCU\Software\Piriform]

[HKCU\Software\Policies]

[HKCU\Software\Realtek]

[HKCU\Software\Roxio]

[HKCU\Software\S3R521]

[HKCU\Software\ScanSoft]

[HKCU\Software\Secunia]

[HKCU\Software\Skype]

[HKCU\Software\Sonic]

[HKCU\Software\Sony Corporation]

[HKCU\Software\Synaptics]

[HKCU\Software\TomTom]

[HKCU\Software\Trolltech]

[HKCU\Software\Visan]

[HKCU\Software\Widcomm]

[HKCU\Software\ZebHelpProcess Helper]

[HKCU\Software\cybelsoft]

[HKCU\Software\kde.org]

[HKLM\Software\ASIO]

[HKLM\Software\AVAST Software]

[HKLM\Software\Adobe]

[HKLM\Software\ArcSoft]

[HKLM\Software\BrowserChoice]

[HKLM\Software\Bytemobile]

[HKLM\Software\CDDB]

[HKLM\Software\CXT]

[HKLM\Software\Canal+ Active]

[HKLM\Software\Canon]

[HKLM\Software\Classes]

[HKLM\Software\Clients]

[HKLM\Software\Conexant]

[HKLM\Software\Data Fellows]

[HKLM\Software\Debug]

[HKLM\Software\DivXNetworks]

[HKLM\Software\Google]

[HKLM\Software\HP]

[HKLM\Software\Hewlett-Packard]

[HKLM\Software\Huawei technologies]

[HKLM\Software\IDT]

[HKLM\Software\IM Providers]

[HKLM\Software\InstallShield]

[HKLM\Software\InstalledOptions]

[HKLM\Software\Intel]

[HKLM\Software\InterVideo]

[HKLM\Software\JavaSoft]

[HKLM\Software\JreMetrics]

[HKLM\Software\Lake]

[HKLM\Software\Macromedia]

[HKLM\Software\Malwarebytes' Anti-Malware]

[HKLM\Software\MimarSinan]

[HKLM\Software\MozillaPlugins]

[HKLM\Software\Mozilla]

[HKLM\Software\NVIDIA Corporation]

[HKLM\Software\ODBC]

[HKLM\Software\OpenOffice]

[HKLM\Software\ParetoLogic] =>PUP.Paretologic

[HKLM\Software\Piriform]

[HKLM\Software\Policies]

[HKLM\Software\Realtek Semiconductor Corp.]

[HKLM\Software\Realtek]

[HKLM\Software\RegisteredApplications]

[HKLM\Software\Roxio]

[HKLM\Software\S3R521]

[HKLM\Software\SRS Labs]

[HKLM\Software\ScanSoft]

[HKLM\Software\Secunia]

[HKLM\Software\Sigmatel]

[HKLM\Software\Skype]

[HKLM\Software\Sonic]

[HKLM\Software\Sony Corporation]

[HKLM\Software\Sony]

[HKLM\Software\SymNRT]

[HKLM\Software\Synaptics]

[HKLM\Software\TomTom]

[HKLM\Software\Trymedia Systems] =>Adware.Trymedia

[HKLM\Software\VideoLAN]

[HKLM\Software\Volatile]

[HKLM\Software\Widcomm]

[HKLM\Software\Windows]

[HKLM\Software\cybelsoft]

[HKLM\Software\illiminable]

~ Key Software: 216 Scanned in 00mn 00s

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

O43 - CFD: 21/02/2010 - 12:10:42 - [] ----D C:\Program Files\Activation Assistant for the 2007 Microsoft Office suites

O43 - CFD: 18/01/2014 - 22:00:32 - [] ----D C:\Program Files\Adobe

O43 - CFD: 30/12/2013 - 16:43:38 - [] ----D C:\Program Files\ArcSoft

O43 - CFD: 01/05/2013 - 19:05:12 - [] ----D C:\Program Files\AVAST Software

O43 - CFD: 01/05/2013 - 18:49:09 - [] ----D C:\Program Files\Barre de Confiance

O43 - CFD: 17/08/2007 - 15:40:00 - [] ----D C:\Program Files\BFG

O43 - CFD: 30/12/2013 - 19:24:41 - [] ----D C:\Program Files\Canon

O43 - CFD: 05/07/2014 - 10:48:31 - [] ----D C:\Program Files\CCleaner

O43 - CFD: 10/11/2011 - 20:27:13 - [] ----D C:\Program Files\CDBurnerXP

O43 - CFD: 14/06/2014 - 16:45:10 - [] ----D C:\Program Files\Common Files

O43 - CFD: 24/02/2010 - 09:57:15 - [] ----D C:\Program Files\DivX

O43 - CFD: 17/08/2007 - 12:10:25 - [] -SH-D C:\Program Files\Fichiers communs

O43 - CFD: 07/07/2014 - 11:29:12 - [] ----D C:\Program Files\Google

O43 - CFD: 17/08/2007 - 15:42:32 - [] ----D C:\Program Files\Google BAE

O43 - CFD: 27/12/2013 - 19:24:55 - [] ----D C:\Program Files\HP

O43 - CFD: 23/02/2010 - 23:04:08 - [] ----D C:\Program Files\IDT

O43 - CFD: 30/12/2013 - 19:24:41 - [] --H-D C:\Program Files\InstallShield Installation Information

O43 - CFD: 17/08/2007 - 15:43:17 - [] ----D C:\Program Files\Intel

O43 - CFD: 14/06/2014 - 15:12:38 - [] ----D C:\Program Files\Internet Explorer

O43 - CFD: 20/02/2010 - 11:32:49 - [] ----D C:\Program Files\InterVideo

O43 - CFD: 14/06/2014 - 16:40:20 - [] ----D C:\Program Files\Java

O43 - CFD: 23/02/2010 - 21:40:46 - [] ----D C:\Program Files\Lecteur CANALPLAY

O43 - CFD: 22/12/2010 - 14:02:21 - [] ----D C:\Program Files\ma-config.com

O43 - CFD: 04/06/2014 - 14:00:46 - [] ----D C:\Program Files\Malwarebytes Anti-Malware

O43 - CFD: 17/05/2014 - 10:38:10 - [0] ----D C:\Program Files\Malwarebytes' Anti-Malware

O43 - CFD: 27/12/2013 - 20:26:24 - [0] ----D C:\Program Files\Microsoft

O43 - CFD: 21/02/2010 - 11:46:20 - [] ----D C:\Program Files\Microsoft CAPICOM 2.1.0.2

O43 - CFD: 02/11/2006 - 14:37:34 - [] ----D C:\Program Files\Microsoft Games

O43 - CFD: 06/11/2013 - 15:16:40 - [] ----D C:\Program Files\Microsoft Office

O43 - CFD: 17/03/2014 - 13:02:31 - [] ----D C:\Program Files\Microsoft Silverlight

O43 - CFD: 06/11/2013 - 15:17:13 - [] ----D C:\Program Files\Microsoft Visual Studio

O43 - CFD: 06/11/2013 - 15:12:28 - [] ----D C:\Program Files\Microsoft Visual Studio 8

O43 - CFD: 21/02/2010 - 13:09:27 - [] ----D C:\Program Files\Microsoft Works

O43 - CFD: 30/06/2010 - 19:16:05 - [] ----D C:\Program Files\Microsoft.NET

O43 - CFD: 18/08/2010 - 09:11:17 - [] ----D C:\Program Files\Movie Maker

O43 - CFD: 06/11/2013 - 15:17:49 - [] ----D C:\Program Files\MSBuild

O43 - CFD: 17/08/2007 - 13:55:00 - [0] ----D C:\Program Files\MSXML 4.0

O43 - CFD: 11/11/2013 - 19:01:32 - [] ----D C:\Program Files\OpenOffice 4

O43 - CFD: 19/12/2012 - 10:09:20 - [] ----D C:\Program Files\Orange

O43 - CFD: 17/01/2014 - 11:01:26 - [] ----D C:\Program Files\ParetoLogic =>PUP.Paretologic

O43 - CFD: 17/08/2007 - 15:42:55 - [] ----D C:\Program Files\Picasa2

O43 - CFD: 17/08/2007 - 14:21:10 - [] ----D C:\Program Files\Realtek

O43 - CFD: 02/11/2006 - 14:37:34 - [] ----D C:\Program Files\Reference Assemblies

O43 - CFD: 20/02/2010 - 11:13:08 - [] ----D C:\Program Files\Roxio

O43 - CFD: 30/12/2013 - 16:49:47 - [] ----D C:\Program Files\ScanSoft

O43 - CFD: 07/12/2012 - 16:27:30 - [] ----D C:\Program Files\Secunia

O43 - CFD: 23/02/2010 - 23:03:47 - [] ----D C:\Program Files\Sigmatel

O43 - CFD: 19/02/2014 - 10:41:33 - [] R---D C:\Program Files\Skype

O43 - CFD: 11/11/2013 - 18:33:55 - [] ----D C:\Program Files\Sony

O43 - CFD: 23/02/2010 - 22:37:09 - [] ----D C:\Program Files\Sony Corporation

O43 - CFD: 17/08/2007 - 14:41:35 - [] ----D C:\Program Files\Synaptics

O43 - CFD: 04/04/2010 - 17:28:58 - [0] ----D C:\Program Files\TomTom DesktopSuite

O43 - CFD: 23/11/2013 - 17:33:23 - [] ----D C:\Program Files\TomTom HOME 2

O43 - CFD: 04/04/2010 - 18:42:47 - [] ----D C:\Program Files\TomTom International B.V

O43 - CFD: 03/08/2012 - 15:21:17 - [] ----D C:\Program Files\Tomtomax Maxi-Box

O43 - CFD: 14/06/2014 - 16:21:08 - [] ----D C:\Program Files\Tomtomax Maxi-Box V3

O43 - CFD: 02/11/2006 - 15:01:55 - [0] --H-D C:\Program Files\Uninstall Information

O43 - CFD: 02/09/2010 - 15:27:01 - [] ----D C:\Program Files\VideoLAN

O43 - CFD: 07/10/2012 - 11:31:47 - [0] ----D C:\Program Files\VS Revo Group

O43 - CFD: 27/09/2013 - 10:52:43 - [] ----D C:\Program Files\Wi-Fi Modem

O43 - CFD: 17/08/2007 - 14:34:19 - [] ----D C:\Program Files\WIDCOMM

O43 - CFD: 20/02/2010 - 22:40:54 - [] ----D C:\Program Files\Windows Calendar

O43 - CFD: 20/02/2010 - 22:40:53 - [] ----D C:\Program Files\Windows Collaboration

O43 - CFD: 20/02/2010 - 22:40:53 - [] ----D C:\Program Files\Windows Defender

O43 - CFD: 11/07/2013 - 17:16:46 - [] ----D C:\Program Files\Windows Journal

O43 - CFD: 31/03/2011 - 07:30:23 - [] ----D C:\Program Files\Windows Live

O43 - CFD: 12/04/2012 - 16:43:05 - [] ----D C:\Program Files\Windows Mail =>.Microsoft Corporation

O43 - CFD: 16/10/2010 - 11:34:48 - [] ----D C:\Program Files\Windows Media Player =>.Microsoft Corporation

O43 - CFD: 17/08/2007 - 12:10:25 - [] ----D C:\Program Files\Windows NT

O43 - CFD: 20/02/2010 - 22:40:53 - [] ----D C:\Program Files\Windows Photo Gallery

O43 - CFD: 20/02/2010 - 23:01:18 - [] ----D C:\Program Files\Windows Portable Devices

O43 - CFD: 10/03/2012 - 12:04:36 - [] ----D C:\Program Files\Windows Sidebar

O43 - CFD: 07/07/2014 - 16:00:27 - [] ----D C:\Program Files\ZHPDiag =>.Nicolas Coolman

O43 - CFD: 18/01/2014 - 22:00:32 - [] ----D C:\Program Files\Common Files\Adobe

O43 - CFD: 29/12/2010 - 17:34:54 - [] ----D C:\Program Files\Common Files\BitDefender

O43 - CFD: 17/05/2014 - 10:11:03 - [] ----D C:\Program Files\Common Files\DESIGNER

O43 - CFD: 20/02/2010 - 11:11:12 - [] ----D C:\Program Files\Common Files\InstallShield

O43 - CFD: 20/02/2010 - 11:32:49 - [] ----D C:\Program Files\Common Files\InterVideo

O43 - CFD: 14/06/2014 - 16:45:10 - [] ----D C:\Program Files\Common Files\Java

O43 - CFD: 06/11/2013 - 17:01:29 - [] ----D C:\Program Files\Common Files\microsoft shared

O43 - CFD: 23/02/2010 - 23:33:29 - [0] ----D C:\Program Files\Common Files\PX Storage Engine

O43 - CFD: 20/02/2010 - 11:13:20 - [] ----D C:\Program Files\Common Files\Roxio Shared

O43 - CFD: 30/12/2013 - 16:50:20 - [] ----D C:\Program Files\Common Files\ScanSoft Shared

O43 - CFD: 02/11/2006 - 13:18:33 - [] ----D C:\Program Files\Common Files\Services

O43 - CFD: 01/05/2013 - 15:14:52 - [] ----D C:\Program Files\Common Files\Skype

O43 - CFD: 20/02/2010 - 11:13:20 - [] ----D C:\Program Files\Common Files\Sonic Shared

O43 - CFD: 23/02/2010 - 22:20:22 - [] ----D C:\Program Files\Common Files\Sony Shared

O43 - CFD: 02/11/2006 - 13:18:33 - [] ----D C:\Program Files\Common Files\SpeechEngines

O43 - CFD: 11/11/2011 - 11:17:47 - [] ----D C:\Program Files\Common Files\System

O43 - CFD: 26/02/2010 - 11:23:03 - [] ----D C:\Program Files\Common Files\Windows Live

O43 - CFD: 18/01/2014 - 22:00:34 - [] ----D C:\ProgramData\Adobe

O43 - CFD: 02/11/2006 - 15:02:03 - [] -SH-D C:\ProgramData\Application Data

O43 - CFD: 06/11/2013 - 18:46:11 - [] ----D C:\ProgramData\AVAST Software

O43 - CFD: 17/08/2007 - 12:10:25 - [] -SH-D C:\ProgramData\Bureau

O43 - CFD: 10/11/2011 - 20:27:54 - [] ----D C:\ProgramData\Canneverbe Limited

O43 - CFD: 27/09/2013 - 10:55:00 - [] ----D C:\ProgramData\DatacardService

O43 - CFD: 02/11/2006 - 15:02:03 - [] -SH-D C:\ProgramData\Desktop

O43 - CFD: 02/11/2006 - 15:02:03 - [] -SH-D C:\ProgramData\Documents

O43 - CFD: 10/11/2010 - 19:27:09 - [] ----D C:\ProgramData\Downloaded Installations

O43 - CFD: 19/12/2011 - 14:28:19 - [] ----D C:\ProgramData\Dumps

O43 - CFD: 26/02/2013 - 11:11:02 - [] ----D C:\ProgramData\f-secure

O43 - CFD: 17/08/2007 - 12:10:25 - [] -SH-D C:\ProgramData\Favoris

O43 - CFD: 02/11/2006 - 15:02:03 - [] -SH-D C:\ProgramData\Favorites

O43 - CFD: 19/12/2012 - 10:08:06 - [] ----D C:\ProgramData\fssg

O43 - CFD: 05/07/2014 - 10:49:05 - [] ----D C:\ProgramData\Google

O43 - CFD: 27/12/2013 - 19:23:13 - [] ----D C:\ProgramData\HP

O43 - CFD: 22/12/2010 - 14:02:06 - [] ----D C:\ProgramData\ma-config.com

O43 - CFD: 17/05/2014 - 10:38:10 - [] ----D C:\ProgramData\Malwarebytes

O43 - CFD: 17/08/2007 - 12:10:25 - [] -SH-D C:\ProgramData\Menu Démarrer

O43 - CFD: 27/11/2013 - 10:29:56 - [] -S--D C:\ProgramData\Microsoft

O43 - CFD: 14/06/2014 - 15:10:34 - [] ----D C:\ProgramData\Microsoft Help

O43 - CFD: 17/08/2007 - 12:10:25 - [] -SH-D C:\ProgramData\Modèles

O43 - CFD: 14/06/2014 - 16:45:02 - [0] ----D C:\ProgramData\Oracle

O43 - CFD: 23/09/2012 - 21:25:51 - [] ----D C:\ProgramData\Orange

O43 - CFD: 17/05/2014 - 11:11:43 - [] ----D C:\ProgramData\ParetoLogic =>PUP.Paretologic

O43 - CFD: 23/08/2012 - 18:03:30 - [0] ----D C:\ProgramData\Roxio

O43 - CFD: 19/02/2014 - 10:41:48 - [] ----D C:\ProgramData\Skype

O43 - CFD: 21/05/2011 - 10:01:01 - [] ----D C:\ProgramData\Skype Extras

O43 - CFD: 20/02/2010 - 11:13:25 - [] ----D C:\ProgramData\Sonic

O43 - CFD: 17/08/2007 - 15:40:29 - [] ----D C:\ProgramData\Sony

O43 - CFD: 22/06/2014 - 11:40:20 - [] ----D C:\ProgramData\Sony Corporation

O43 - CFD: 30/12/2013 - 16:50:20 - [0] ----D C:\ProgramData\SSScanAppDataDir

O43 - CFD: 30/12/2013 - 16:50:20 - [0] ----D C:\ProgramData\SSScanWizard

O43 - CFD: 02/11/2006 - 15:02:03 - [] -SH-D C:\ProgramData\Start Menu

O43 - CFD: 27/03/2010 - 10:37:40 - [] ----D C:\ProgramData\Sun

O43 - CFD: 02/11/2006 - 15:02:04 - [] -SH-D C:\ProgramData\Templates

O43 - CFD: 09/04/2010 - 19:03:34 - [] ----D C:\ProgramData\TomTom

O43 - CFD: 02/12/2010 - 10:34:03 - [] ----D C:\ProgramData\Trusteer

O43 - CFD: 20/02/2010 - 11:24:02 - [0] ----D C:\ProgramData\VAIO Media Platform

O43 - CFD: 31/07/2010 - 09:06:01 - [] ----D C:\ProgramData\WindowsSearch

O43 - CFD: 18/09/2011 - 16:34:26 - [] ----D C:\Users\manu\AppData\Roaming\Adobe

O43 - CFD: 06/11/2013 - 19:38:46 - [] ----D C:\Users\manu\AppData\Roaming\AVAST Software

O43 - CFD: 21/02/2010 - 18:20:01 - [] ----D C:\Users\manu\AppData\Roaming\DivX

O43 - CFD: 17/01/2014 - 11:01:54 - [] ----D C:\Users\manu\AppData\Roaming\DriverCure

O43 - CFD: 23/08/2012 - 18:27:34 - [] ----D C:\Users\manu\AppData\Roaming\dvdcss

O43 - CFD: 21/02/2010 - 16:09:31 - [] ----D C:\Users\manu\AppData\Roaming\Google

O43 - CFD: 27/12/2013 - 19:24:54 - [0] ----D C:\Users\manu\AppData\Roaming\HpUpdate

O43 - CFD: 17/08/2007 - 12:12:46 - [] ----D C:\Users\manu\AppData\Roaming\Identities

O43 - CFD: 17/08/2007 - 15:43:11 - [] ----D C:\Users\manu\AppData\Roaming\InstallShield

O43 - CFD: 23/08/2012 - 17:20:17 - [] ----D C:\Users\manu\AppData\Roaming\InterVideo

O43 - CFD: 21/02/2010 - 15:58:01 - [] ----D C:\Users\manu\AppData\Roaming\Macromedia

O43 - CFD: 17/05/2014 - 10:38:31 - [0] ----D C:\Users\manu\AppData\Roaming\Malwarebytes

O43 - CFD: 02/11/2006 - 14:37:34 - [0] ----D C:\Users\manu\AppData\Roaming\Media Center Programs

O43 - CFD: 19/04/2014 - 16:16:19 - [] -S--D C:\Users\manu\AppData\Roaming\Microsoft

O43 - CFD: 11/09/2010 - 14:28:15 - [] ----D C:\Users\manu\AppData\Roaming\Mozilla

O43 - CFD: 07/11/2013 - 11:00:30 - [] ----D C:\Users\manu\AppData\Roaming\OpenOffice

O43 - CFD: 17/01/2014 - 11:01:53 - [] ----D C:\Users\manu\AppData\Roaming\ParetoLogic =>PUP.Paretologic

O43 - CFD: 29/12/2010 - 17:29:42 - [0] ----D C:\Users\manu\AppData\Roaming\QuickScan

O43 - CFD: 23/08/2012 - 17:49:03 - [] ----D C:\Users\manu\AppData\Roaming\Roxio

O43 - CFD: 30/12/2013 - 16:50:43 - [] ----D C:\Users\manu\AppData\Roaming\ScanSoft

O43 - CFD: 05/07/2014 - 10:17:00 - [] ----D C:\Users\manu\AppData\Roaming\Skype

O43 - CFD: 21/05/2011 - 09:54:02 - [] ----D C:\Users\manu\AppData\Roaming\skypePM

O43 - CFD: 23/02/2010 - 21:27:46 - [] ----D C:\Users\manu\AppData\Roaming\Sony Corporation

O43 - CFD: 23/09/2012 - 21:34:41 - [] ----D C:\Users\manu\AppData\Roaming\Telephone sur PC

O43 - CFD: 11/09/2010 - 14:28:10 - [] ----D C:\Users\manu\AppData\Roaming\TomTom

O43 - CFD: 25/11/2013 - 10:06:19 - [] ----D C:\Users\manu\AppData\Roaming\vlc

O43 - CFD: 07/07/2014 - 16:06:05 - [] ----D C:\Users\manu\AppData\Roaming\ZHP =>.Nicolas Coolman

O43 - CFD: 20/02/2010 - 21:06:25 - [] -SH-D C:\Users\manu\AppData\Local\Application Data

O43 - CFD: 05/07/2014 - 10:49:05 - [] ----D C:\Users\manu\AppData\Local\Google

O43 - CFD: 20/02/2010 - 21:06:25 - [] -SH-D C:\Users\manu\AppData\Local\Historique

O43 - CFD: 04/11/2011 - 13:11:52 - [] ----D C:\Users\manu\AppData\Local\HP

O43 - CFD: 27/12/2013 - 19:25:37 - [] ----D C:\Users\manu\AppData\Local\Microsoft

O43 - CFD: 17/08/2007 - 15:33:55 - [0] ----D C:\Users\manu\AppData\Local\Microsoft Help

O43 - CFD: 07/12/2012 - 16:27:47 - [0] ----D C:\Users\manu\AppData\Local\Secunia PSI

O43 - CFD: 17/08/2007 - 15:37:11 - [] ----D C:\Users\manu\AppData\Local\Seven Zip

O43 - CFD: 07/07/2014 - 16:00:46 - [] ----D C:\Users\manu\AppData\Local\Temp

O43 - CFD: 20/02/2010 - 21:06:25 - [] -SH-D C:\Users\manu\AppData\Local\Temporary Internet Files

O43 - CFD: 11/09/2010 - 14:28:10 - [] ----D C:\Users\manu\AppData\Local\TomTom

O43 - CFD: 20/02/2010 - 18:54:41 - [] ----D C:\Users\manu\AppData\Local\VirtualStore

O43 - CFD: 29/12/2010 - 13:26:39 - [] ----D C:\Users\manu\AppData\Local\Windows Live

O43 - CFD: 21/02/2010 - 10:26:21 - [] ----D C:\Users\manu\AppData\Local\WindowsUpdate

O43 - CFD: 02/11/2006 - 14:54:36 - [] R---D C:\Users\manu\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories

O43 - CFD: 17/08/2007 - 12:12:54 - [] R---D C:\Users\manu\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools

O43 - CFD: 02/11/2006 - 14:50:41 - [] R---D C:\Users\manu\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance

O43 - CFD: 17/08/2007 - 12:12:54 - [] R---D C:\Users\manu\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

~ Program Folder: 175 Scanned in 00mn 00s

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

O44 - LFC:[MD5.8807767A4C1137A131A26546ED9EBDCB] - 05/07/2014 - 08:53:55 ---A- . (.AVAST Software - avast! Filtering NDIS driver.) -- C:\Windows\System32\Drivers\aswndis2.sys [252872]

O44 - LFC:[MD5.4E39E113E8F5FEE3C49160A0D657A4D5] - 05/07/2014 - 08:54:35 ---A- . (.AVAST Software - avast! Keyboard Filter Driver.) -- C:\Windows\System32\Drivers\aswKbd.sys [26136]

O44 - LFC:[MD5.588C2C48CB267E1C4B5A9EB5ACFF0116] - 05/07/2014 - 08:55:22 ---A- . (.AVAST Software - avast! start-up scanner.) -- C:\Windows\System32\aswBoot.exe [276432]

O44 - LFC:[MD5.357CEBBCD99C8928A2D1A61A6CACC168] - 05/07/2014 - 08:55:23 ---A- . (.AVAST Software - avast! Screen Saver stub.) -- C:\Windows\avastSS.scr [43152]

O44 - LFC:[MD5.3BFBB5DAE801CB893B8B46345FED6437] - 05/07/2014 - 08:55:27 ---A- . (...) -- C:\Windows\System32\Drivers\aswHwid.sys [24184]

O44 - LFC:[MD5.B7750AF7EDFD95674EB7CA92BCDD3358] - 05/07/2014 - 08:55:27 ---A- . (...) -- C:\Windows\System32\Drivers\aswRvrt.sys [49944]

O44 - LFC:[MD5.C3014C735F450FE822C97FFBB0627113] - 05/07/2014 - 08:55:27 ---A- . (.AVAST Software - avast! File System Minifilter for Windows 2.) -- C:\Windows\System32\Drivers\aswMonFlt.sys [67824]

O44 - LFC:[MD5.D6C9024F5D14843D33ADA8A6A10A1BE1] - 05/07/2014 - 08:55:27 ---A- . (.AVAST Software - avast! TDI Redirect Driver.) -- C:\Windows\System32\Drivers\aswrdr.sys [55112]

O44 - LFC:[MD5.90BEE0170D70D6744CEF2355EEAF8086] - 05/07/2014 - 08:55:28 ---A- . (...) -- C:\Windows\System32\Drivers\aswVmm.sys [192352]

O44 - LFC:[MD5.26C51C289E39E8EE0F12B8B06B71E436] - 05/07/2014 - 08:55:28 ---A- . (.AVAST Software - avast! TDI Filter Driver.) -- C:\Windows\System32\Drivers\aswTdi.sys [57800]

O44 - LFC:[MD5.51FDE588D860857A97E4C4B560E40C9B] - 05/07/2014 - 08:55:28 ---A- . (.AVAST Software - avast! Virtualization Driver.) -- C:\Windows\System32\Drivers\aswsnx.sys [779536]

O44 - LFC:[MD5.1AEB8CDB797666AF709A291B47AE81E0] - 05/07/2014 - 08:56:32 ---A- . (.AVAST Software - avast! self protection module.) -- C:\Windows\System32\Drivers\aswsp.sys [414520]

O44 - LFC:[MD5.D41D8CD98F00B204E9800998ECF8427E] - 05/07/2014 - 09:40:13 ---A- . (...) -- C:\Windows\setupact.log [0]

O44 - LFC:[MD5.D41D8CD98F00B204E9800998ECF8427E] - 05/07/2014 - 09:40:13 ---A- . (...) -- C:\Windows\setuperr.log [0]

O44 - LFC:[MD5.12E71DA845D76665B56753AD149E32B3] - 05/07/2014 - 10:28:47 ---A- . (.Malwarebytes Corporation - Malwarebytes Anti-Malware.) -- C:\Windows\System32\Drivers\MBAMSwissArmy.sys [110296]

O44 - LFC:[MD5.BF4821F1A76EF939253330106195AFAA] - 07/07/2014 - 10:29:12 ---A- . (...) -- C:\Windows\PFRO.log [2318]

O44 - LFC:[MD5.EB7BD40336C0D70F99FD84E7F6CB679F] - 07/07/2014 - 14:35:33 -S-A- . (...) -- C:\Windows\bootstat.dat [67584]

O44 - LFC:[MD5.8F6FA328CB88B2242CA1F229630F4932] - 07/07/2014 - 14:55:54 ---A- . (...) -- C:\Windows\WindowsUpdate.log [1366534]

~ Files: 18 Scanned in 00mn 09s

---\\ 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 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: 7 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

---\\ 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: \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

~ TDSD: 3 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

O55 - MWPS:[HKCU\...\Policies\System] - "DisableRegistryTools"=0

O55 - MWPS:[HKCU\...\Policies\System] - "DisableTaskMgr"=0

~ MWPS: 18 Scanned in 00mn 00s

---\\ Enumération des clés de registre PoliciesExplorer (MWPE) (O56)

O56 - MWPE:[HKCU\...\policies\Explorer] - "NoDriveTypeAutoRun"=145

O56 - MWPE:[HKLM\...\policies\Explorer] - "BindDirectlyToPropertySetStorage"=0

~ MWPE Keys: 2 Scanned in 00mn 00s

---\\ Liste des pilotes du système (SDL) (O58)

O58 - SDL:02/11/2006 - 10:51:38 ---A- . (.Adaptec, Inc. - Adaptec Windows SAS/SATA Storport Driver.) -- C:\Windows\System32\Drivers\adp94xx.sys [420968]

O58 - SDL:02/11/2006 - 10:51:32 ---A- . (.Adaptec, Inc. - Adaptec Windows SATA Storport Driver.) -- C:\Windows\System32\Drivers\adpahci.sys [297576]

O58 - SDL:02/11/2006 - 10:50:35 ---A- . (.Adaptec, Inc. - Adaptec LH Ultra160 Driver (x86).) -- C:\Windows\System32\Drivers\adpu160m.sys [98408]

O58 - SDL:02/11/2006 - 10:51:00 ---A- . (.Adaptec, Inc. - Adaptec StorPort Ultra320 SCSI Driver.) -- C:\Windows\System32\Drivers\adpu320.sys [147048]

O58 - SDL:02/11/2006 - 10:49:20 ---A- . (.Acer Laboratories Inc. - ALi mini IDE Driver.) -- C:\Windows\System32\Drivers\aliide.sys [14952]

O58 - SDL:02/11/2006 - 10:50:09 ---A- . (.Adaptec, Inc. - Adaptec RAID Storport Driver.) -- C:\Windows\System32\Drivers\arc.sys [67688]

O58 - SDL:02/11/2006 - 10:50:10 ---A- . (.Adaptec, Inc. - Adaptec SAS RAID WS03 Driver.) -- C:\Windows\System32\Drivers\arcsas.sys [67688]

O58 - SDL:05/07/2014 - 08:55:27 ---A- . (...) -- C:\Windows\System32\Drivers\aswHwid.sys [24184] =>.ALWIL Software

O58 - SDL:05/07/2014 - 08:54:35 ---A- . (.AVAST Software - avast! Keyboard Filter Driver.) -- C:\Windows\System32\Drivers\aswKbd.sys [26136]

O58 - SDL:05/07/2014 - 08:55:27 ---A- . (.AVAST Software - avast! File System Minifilter for Windows 2003/Vista.) -- C:\Windows\System32\Drivers\aswMonFlt.sys [67824]

O58 - SDL:03/12/2013 - 07:39:07 ---A- . (.ALWIL Software - avast! Filtering NDIS driver.) -- C:\Windows\System32\Drivers\aswNdis.sys [12112]

O58 - SDL:05/07/2014 - 08:53:55 ---A- . (.AVAST Software - avast! Filtering NDIS driver.) -- C:\Windows\System32\Drivers\aswndis2.sys [252872]

O58 - SDL:05/07/2014 - 08:55:27 ---A- . (.AVAST Software - avast! TDI Redirect Driver.) -- C:\Windows\System32\Drivers\aswrdr.sys [55112]

O58 - SDL:18/04/2014 - 08:32:15 ---A- . (.AVAST Software - avast! TDI Redirect Driver.) -- C:\Windows\System32\Drivers\aswrdr.sys.1400310269654 [54832]

O58 - SDL:05/07/2014 - 08:55:27 ---A- . (...) -- C:\Windows\System32\Drivers\aswRvrt.sys [49944] =>.ALWIL Software

O58 - SDL:05/07/2014 - 08:55:28 ---A- . (.AVAST Software - avast! Virtualization Driver.) -- C:\Windows\System32\Drivers\aswsnx.sys [779536]

O58 - SDL:18/04/2014 - 08:32:17 ---A- . (.AVAST Software - avast! Virtualization Driver.) -- C:\Windows\System32\Drivers\aswsnx.sys.1400310269654 [776976]

O58 - SDL:05/07/2014 - 08:56:32 ---A- . (.AVAST Software - avast! self protection module.) -- C:\Windows\System32\Drivers\aswsp.sys [414520]

O58 - SDL:05/07/2014 - 08:55:28 ---A- . (.AVAST Software - avast! TDI Filter Driver.) -- C:\Windows\System32\Drivers\aswTdi.sys [57800]

O58 - SDL:05/07/2014 - 08:55:28 ---A- . (...) -- C:\Windows\System32\Drivers\aswVmm.sys [192352] =>.ALWIL Software

O58 - SDL: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: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: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:02/11/2006 - 09:24:44 ---A- . (.Brother Industries Ltd. - Brother Serial driver (WDM version).) -- C:\Windows\System32\Drivers\BrSerWdm.sys [62336]

O58 - SDL:02/11/2006 - 09:24:44 ---A- . (.Brother Industries Ltd. - Brother USB MDM Driver.) -- C:\Windows\System32\Drivers\BrUsbMdm.sys [12160]

O58 - SDL:02/11/2006 - 09:24:47 ---A- . (.Brother Industries Ltd. - Brother USB Serial Driver.) -- C:\Windows\System32\Drivers\BrUsbSer.sys [11904]

O58 - SDL:24/07/2007 - 01:56:12 ---A- . (.Broadcom Corporation. - Bluetooth Audio Device.) -- C:\Windows\System32\Drivers\btwaudio.sys [80936]

O58 - SDL:24/07/2007 - 01:56:12 ---A- . (.Broadcom Corporation. - Broadcom Bluetooth AVDT Service.) -- C:\Windows\System32\Drivers\btwavdt.sys [98608]

O58 - SDL:24/07/2007 - 01:55:39 ---A- . (.Broadcom Corporation. - Broadcom Bluetooth L2CAP Service.) -- C:\Windows\System32\Drivers\btwl2cap.sys [28464]

O58 - SDL:24/07/2007 - 01:56:14 ---A- . (.Broadcom Corporation. - Bluetooth Remote Control HID Minidriver.) -- C:\Windows\System32\Drivers\btwrchid.sys [17712]

O58 - SDL:11/06/2007 - 12:09:46 ---A- . (.Sonic Solutions - CDR4 CD and DVD Place Holder Driver (see PxHelp).) -- C:\Windows\System32\Drivers\cdr4\_xp.sys [9336]

O58 - SDL:11/06/2007 - 12:09:46 ---A- . (.Sonic Solutions - CDRAL Place Holder Driver (see PxHelp).) -- C:\Windows\System32\Drivers\cdralw2k.sys [9464]

O58 - SDL:02/11/2006 - 10:49:28 ---A- . (.CMD Technology, Inc. - CMD PCI IDE Bus Driver.) -- C:\Windows\System32\Drivers\cmdide.sys [16488]

O58 - SDL:02/11/2006 - 10:50:11 ---A- . (.Adaptec, Inc. - Adaptec Ultra SCSI miniport.) -- C:\Windows\System32\Drivers\djsvs.sys [71272]

O58 - SDL:27/06/2007 - 18:29:58 ---A- . (.Sony Corporation - Windows 2000 DMI Call Kernel Driver.) -- C:\Windows\System32\Drivers\DMICall.sys [10216]

O58 - SDL:02/11/2006 - 08:30:54 ---A- . (.Intel Corporation - Intel(R) PRO/1000 Adapter NDIS 6 deserialized driver.) -- C:\Windows\System32\Drivers\E1G60I32.sys [117760]

O58 - SDL:02/11/2006 - 10:51:34 ---A- . (.Emulex - Storport Miniport Driver for LightPulse HBAs.) -- C:\Windows\System32\Drivers\elxstor.sys [316520]

O58 - SDL:08/10/2010 - 15:55:06 ---A- . (.Huawei Tech. Co., Ltd. - HUAWEI USB Smart Card Driver.) -- C:\Windows\System32\Drivers\ewdcsc.sys [25856]

O58 - SDL:03/05/2011 - 14:42:30 ---A- . (.Huawei Technologies Co., Ltd. - USB Modem/Serial Device Driver.) -- C:\Windows\System32\Drivers\ewusbmdm.sys [194816]

O58 - SDL:24/12/2010 - 10:55:58 ---A- . (.Huawei Technologies Co., Ltd. - USB NDIS Miniport Driver.) -- C:\Windows\System32\Drivers\ewusbnet.sys [235392]

O58 - SDL:26/09/2010 - 17:09:22 ---A- . (.Huawei Technologies Co., Ltd. - ew\_hwupgrade Driver.) -- C:\Windows\System32\Drivers\ew\_hwupgrade.sys [19200]

O58 - SDL:27/07/2010 - 08:52:02 ---A- . (.Huawei Technologies Co., Ltd. - USB Modem/Serial Device Driver.) -- C:\Windows\System32\Drivers\ew\_hwusbdev.sys [102784]

O58 - SDL:30/01/2011 - 17:19:00 ---A- . (.Huawei Technologies Co., Ltd. - ew\_jubusenum Driver.) -- C:\Windows\System32\Drivers\ew\_jubusenum.sys [73216]

O58 - SDL:25/02/2011 - 17:02:26 ---A- . (.Huawei Technologies Co., Ltd. - ew\_jucdcacm Driver.) -- C:\Windows\System32\Drivers\ew\_jucdcacm.sys [90368]

O58 - SDL:30/01/2011 - 17:19:00 ---A- . (.Huawei Technologies Co., Ltd. - ew\_jucdcndis Driver.) -- C:\Windows\System32\Drivers\ew\_jucdcecm.sys [64384]

O58 - SDL:30/01/2011 - 17:19:00 ---A- . (.Huawei Technologies Co., Ltd. - ew\_juextctrl Driver.) -- C:\Windows\System32\Drivers\ew\_juextctrl.sys [26624]

O58 - SDL:20/03/2010 - 11:06:58 ---A- . (.Huawei Technologies Co., Ltd. - Filter Driver.) -- C:\Windows\System32\Drivers\ew\_usbenumfilter.sys [11136]

O58 - SDL:19/09/2006 - 14:44:04 ---A- . (.GEAR Software Inc. - CD/DVD Class Filter Driver.) -- C:\Windows\System32\Drivers\GEARAspiWDM.sys [15664]

O58 - SDL:02/11/2006 - 10:50:10 ---A- . (.Hewlett-Packard Company - Smart Array Storport Driver.) -- C:\Windows\System32\Drivers\HpCISSs.sys [37480]

O58 - SDL:20/07/2008 - 17:44:44 ---A- . (.Intel Corporation - Intel Matrix Storage Manager driver - ia32.) -- C:\Windows\System32\Drivers\iaStor.sys [324120]

O58 - SDL:02/11/2006 - 10:51:25 ---A- . (.Intel Corporation - Intel Matrix Storage Manager driver (base).) -- C:\Windows\System32\Drivers\iaStorV.sys [232040]

O58 - SDL: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: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: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:02/11/2006 - 10:50:04 ---A- . (.LSI Logic - LSI Logic Fusion-MPT FC Driver (StorPort).) -- C:\Windows\System32\Drivers\lsi\_fc.sys [65640]

O58 - SDL:02/11/2006 - 10:50:05 ---A- . (.LSI Logic - LSI Logic Fusion-MPT SAS Driver (StorPort).) -- C:\Windows\System32\Drivers\lsi\_sas.sys [65640]

O58 - SDL:02/11/2006 - 10:50:10 ---A- . (.LSI Logic - LSI Logic Fusion-MPT SCSI Driver (StorPort).) -- C:\Windows\System32\Drivers\lsi\_scsi.sys [65640]

O58 - SDL:12/05/2014 - 06:25:54 ---A- . (.Malwarebytes Corporation - Malwarebytes Anti-Malware.) -- C:\Windows\System32\Drivers\mbam.sys [23256]

O58 - SDL:12/05/2014 - 06:25:58 ---A- . (.Malwarebytes Corporation - Malwarebytes Chameleon Protection Driver.) -- C:\Windows\System32\Drivers\mbamchameleon.sys [74456]

O58 - SDL:05/07/2014 - 10:28:47 ---A- . (.Malwarebytes Corporation - Malwarebytes Anti-Malware.) -- C:\Windows\System32\Drivers\MBAMSwissArmy.sys [110296]

O58 - SDL:02/11/2006 - 10:49:53 ---A- . (.LSI Logic Corporation - MEGASAS RAID Controller Driver for Windows Vista/Longhorn for x.) -- C:\Windows\System32\Drivers\megasas.sys [28776]

O58 - SDL: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:12/05/2014 - 06:26:04 ---A- . (.Malwarebytes Corporation - Malwarebytes Web Access Control.) -- C:\Windows\System32\Drivers\mwac.sys [51928]

O58 - SDL:30/06/2007 - 12:04:34 ---A- . (.Intel Corporation - Intel® Wireless WiFi Link Driver.) -- C:\Windows\System32\Drivers\NETw4v32.sys [2222080]

O58 - SDL:02/11/2006 - 10:50:19 ---A- . (.IBM Corporation - IBM ServeRAID Controller Driver.) -- C:\Windows\System32\Drivers\nfrd960.sys [45160]

O58 - SDL: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:01/08/2007 - 01:18:30 ---A- . (.NVIDIA Corporation - NVIDIA Compatible Windows 2000 Miniport Driver, Version 101.28.) -- C:\Windows\System32\Drivers\nvlddmkm.sys [7115072]

O58 - SDL:02/11/2006 - 10:50:24 ---A- . (.NVIDIA Corporation - NVIDIA® nForce(TM) RAID Driver.) -- C:\Windows\System32\Drivers\nvraid.sys [88680]

O58 - SDL:02/11/2006 - 10:50:13 ---A- . (.NVIDIA Corporation - NVIDIA® nForce(TM) Sata Performance Driver.) -- C:\Windows\System32\Drivers\nvstor.sys [40040]

O58 - SDL:02/11/2006 - 10:51:45 ---A- . (.QLogic Corporation - QLogic Fibre Channel Stor Miniport Driver.) -- C:\Windows\System32\Drivers\ql2300.sys [900712]

O58 - SDL:02/11/2006 - 10:50:35 ---A- . (.QLogic Corporation - QLogic iSCSI Storport Miniport Driver.) -- C:\Windows\System32\Drivers\ql40xx.sys [106088]

O58 - SDL:20/04/2007 - 01:00:55 ---A- . (.Ricoh - Description string for UvcFilter driver.) -- C:\Windows\System32\Drivers\R5U870FLx86.sys [73472]

O58 - SDL:20/04/2007 - 01:00:55 ---A- . (.Ricoh - Description string for UvcUpperFilter driver.) -- C:\Windows\System32\Drivers\R5U870FUx86.sys [43904]

O58 - SDL:17/04/2007 - 20:09:28 ---A- . (.InterVideo - regi driver.) -- C:\Windows\System32\Drivers\regi.sys [11032]

O58 - SDL:26/06/2007 - 01:39:35 ---A- . (.Realtek Semiconductor Corp. - Realtek(r) High Definition Audio Function Driver.) -- C:\Windows\System32\Drivers\RTKVHDA.sys [1787816]

O58 - SDL:02/11/2006 - 07:37:21 ---A- . (.Macrovision Corporation, Macrovision Europe - Macrovision SECURITY Driver.) -- C:\Windows\System32\Drivers\secdrv.sys [20480]

O58 - SDL:02/11/2006 - 10:50:10 ---A- . (.Silicon Integrated Systems Corp. - SiS RAID Stor Miniport Driver.) -- C:\Windows\System32\Drivers\sisraid2.sys [38504]

O58 - SDL:02/11/2006 - 10:50:16 ---A- . (.Silicon Integrated Systems - SiS AHCI Stor-Miniport Driver.) -- C:\Windows\System32\Drivers\sisraid4.sys [71784]

O58 - SDL:06/11/2006 - 09:29:32 ---A- . (.Sony Corporation - Sony Firmware Extension Parser driver.) -- C:\Windows\System32\Drivers\SonyNC.sys [27520]

O58 - SDL:13/09/2007 - 15:46:06 ---A- . (.IDT, Inc. - NDHF.) -- C:\Windows\System32\Drivers\stwrt.sys [330240]

O58 - SDL:02/11/2006 - 10:50:05 ---A- . (.LSI Logic - LSI Logic 8XX SCSI Miniport Driver.) -- C:\Windows\System32\Drivers\symc8xx.sys [35944]

O58 - SDL: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: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:10/03/2007 - 02:58:05 ---A- . (.Synaptics, Inc. - Synaptics Touchpad Driver.) -- C:\Windows\System32\Drivers\SynTP.sys [181560]

O58 - SDL:06/06/2007 - 01:00:39 ---A- . (.Texas Instruments - ti21sony.sys.) -- C:\Windows\System32\Drivers\ti21sony.sys [812544]

O58 - SDL:02/11/2006 - 10:51:25 ---A- . (.ULi Electronics Inc. - ULi SATA Controller Driver.) -- C:\Windows\System32\Drivers\uliahci.sys [235112]

O58 - SDL: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:02/11/2006 - 10:50:45 ---A- . (.Promise Technology, Inc. - Promise SATAII150 Series Windows Drivers.) -- C:\Windows\System32\Drivers\ulsata2.sys [115816]

O58 - SDL:02/11/2006 - 10:49:30 ---A- . (.VIA Technologies, Inc. - VIA Generic PCI IDE Bus Driver.) -- C:\Windows\System32\Drivers\viaide.sys [17512]

O58 - SDL:02/11/2006 - 10:50:41 ---A- . (.VIA Technologies Inc.,Ltd - VIA RAID DRIVER FOR X86-32.) -- C:\Windows\System32\Drivers\vsmraid.sys [112232]

O58 - SDL:02/11/2006 - 08:41:49 ---A- . (.Conexant Systems, Inc. - HSF\_HWAZL WDM driver.) -- C:\Windows\System32\Drivers\VSTAZL3.SYS [200704]

O58 - SDL:02/11/2006 - 08:41:48 ---A- . (.Conexant Systems, Inc. - HSF\_CNXT driver.) -- C:\Windows\System32\Drivers\VSTCNXT3.SYS [654336]

O58 - SDL:02/11/2006 - 08:41:50 ---A- . (.Conexant Systems, Inc. - HSF\_DP driver.) -- C:\Windows\System32\Drivers\VSTDPV3.SYS [987648]

O58 - SDL:13/07/2007 - 07:15:17 ---A- . (.Marvell - NDIS6.0 Miniport Driver for Marvell Yukon Ethernet Controller.) -- C:\Windows\System32\Drivers\yk60x86.sys [246784]

O58 - SDL:02/11/2006 - 08:09:42 ---A- . (...) -- C:\Windows\System32\ANSI.SYS [9029]

O58 - SDL:02/11/2006 - 08:09:45 ---A- . (...) -- C:\Windows\System32\country.sys [27097]

O58 - SDL:02/11/2006 - 08:09:41 ---A- . (...) -- C:\Windows\System32\HIMEM.SYS [4768]

O58 - SDL:02/11/2006 - 08:09:44 ---A- . (...) -- C:\Windows\System32\KEY01.SYS [42809]

O58 - SDL:02/11/2006 - 08:09:44 ---A- . (...) -- C:\Windows\System32\KEYBOARD.SYS [42537]

O58 - SDL:02/11/2006 - 08:09:29 ---A- . (...) -- C:\Windows\System32\NTDOS.SYS [27866]

O58 - SDL:02/11/2006 - 08:09:35 ---A- . (...) -- C:\Windows\System32\NTDOS404.SYS [29146]

O58 - SDL:02/11/2006 - 08:09:38 ---A- . (...) -- C:\Windows\System32\NTDOS411.SYS [29370]

O58 - SDL:02/11/2006 - 08:09:40 ---A- . (...) -- C:\Windows\System32\NTDOS412.SYS [29274]

O58 - SDL:02/11/2006 - 08:09:31 ---A- . (...) -- C:\Windows\System32\NTDOS804.SYS [29146]

O58 - SDL:02/11/2006 - 08:09:20 ---A- . (...) -- C:\Windows\System32\NTIO.SYS [33952]

O58 - SDL:02/11/2006 - 08:09:23 ---A- . (...) -- C:\Windows\System32\NTIO404.SYS [34672]

O58 - SDL:02/11/2006 - 08:09:24 ---A- . (...) -- C:\Windows\System32\NTIO411.SYS [35776]

O58 - SDL:02/11/2006 - 08:09:26 ---A- . (...) -- C:\Windows\System32\NTIO412.SYS [35536]

O58 - SDL:02/11/2006 - 08:09:22 ---A- . (...) -- C:\Windows\System32\NTIO804.SYS [34672]

~ Drivers: 109 Scanned in 00mn 23s

---\\ 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 - 05/07/2014 - C:\Windows\system32\drivers\aswHwid.sys (aswHwid) .(...) - LEGACY\_ASWHWID

O64 - Services: CurCS - 05/07/2014 - C:\Windows\system32\drivers\aswMonFlt.sys (aswMonFlt) .(.AVAST Software - avast! File System Minifilter for Windows 2.) - LEGACY\_ASWMONFLT

O64 - Services: CurCS - 05/07/2014 - C:\Windows\System32\Drivers\aswNdis2.sys (aswNdis2) .(.AVAST Software - avast! Filtering NDIS driver.) - LEGACY\_ASWNDIS2

O64 - Services: CurCS - 05/07/2014 - C:\Windows\system32\drivers\aswRdr.sys (AswRdr) .(.AVAST Software - avast! TDI Redirect Driver.) - LEGACY\_ASWRDR

O64 - Services: CurCS - 05/07/2014 - C:\Windows\System32\Drivers\aswRvrt.sys (aswRvrt) .(...) - LEGACY\_ASWRVRT

O64 - Services: CurCS - 05/07/2014 - C:\Windows\system32\drivers\aswSnx.sys (aswSnx) .(.AVAST Software - avast! Virtualization Driver.) - LEGACY\_ASWSNX

O64 - Services: CurCS - 05/07/2014 - C:\Windows\system32\drivers\aswSP.sys (aswSP) .(.AVAST Software - avast! self protection module.) - LEGACY\_ASWSP

O64 - Services: CurCS - 05/07/2014 - C:\Windows\system32\drivers\aswTdi.sys (aswTdi) .(.AVAST Software - avast! TDI Filter Driver.) - LEGACY\_ASWTDI

O64 - Services: CurCS - 05/07/2014 - C:\Windows\System32\Drivers\aswVmm.sys (aswVmm) .(...) - LEGACY\_ASWVMM

O64 - Services: CurCS - 27/06/2007 - C:\Windows\System32\DRIVERS\DMICall.sys (DMICall) .(.Sony Corporation - Windows 2000 DMI Call Kernel Driver.) - LEGACY\_DMICALL

O64 - Services: CurCS - 02/11/2006 - C:\Windows\System32\drivers\iastorv.sys (iaStorV) .(.Intel Corporation - Intel Matrix Storage Manager driver (base).) - LEGACY\_IASTORV

O64 - Services: CurCS - 17/04/2007 - C:\Windows\System32\drivers\regi.sys (regi) .(.InterVideo - regi driver.) - LEGACY\_REGI

O64 - Services: CurCS - 02/11/2006 - C:\Windows\System32\Drivers\secdrv.sys (secdrv) .(.Macrovision Corporation, Macrovision Europe - Macrovision SECURITY Driver.) - LEGACY\_SECDRV

~ Legacy: 144 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

~ FASS Keys: 10 Scanned in 00mn 00s

---\\ Menu de démarrage Internet (SMI) (O68)

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] {0633EE93-D776-472f-A0FF-E1416B8B2E3A} - (@ieframe.dll,-12512) - http://www.bing.com

O69 - SBI: SearchScopes [HKCU] {1DC840A1-8C42-4CE7-A7BB-D1C235FA26B0} [DefaultScope] - (Google) - http://www.google.com

O69 - SBI: SearchScopes [HKCU] {6A1806CD-94D4-4689-BA73-E35EA1EA9990} - (@ieframe.dll,-12512) - http://www.bing.com

~ 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)

[MD5.6C0312E7C844A56E06DEDBBDF8153AA3] [SPRF][10/03/2012] (...) -- C:\ProgramData\bdinstall.bin [976159]

[MD5.09EA6D58EC572FB3463DB49AF60D4FAF] [SPRF][04/06/2010] (...) -- C:\ProgramData\ezsidmv.dat [56]

[MD5.5E10CBC67A2B9A17B7CE88E4FEAEE0EE] [SPRF][14/06/2014] (...) -- C:\Users\manu\AppData\Roaming\nvModes.dat [48872]

[MD5.D9DE89F0FAF18019BC9595F0F47BCA61] [SPRF][24/07/2009] (.Atribune.org - ATF Cleaner.exe.) -- C:\Users\manu\Desktop\ATF-Cleaner.exe [50688]

[MD5.0FD74B173541AF82A4FAF7A40292CA2C] [SPRF][03/05/2014] (...) -- C:\Users\manu\Desktop\cc\_20140503\_111245.reg [34608]

[MD5.B211F62DD50509086940ED09E9D868F5] [SPRF][14/06/2014] (.Oracle Corporation - Java Platform SE binary.) -- C:\Users\manu\Desktop\java-runtime-environment\_8u5\_fr\_121472\_32.exe [31112616]

[MD5.2C1A57069523D230E90CF76757A3795C] [SPRF][14/06/2014] (.Pas de propriétaire - Désinstallation et mise à jour Java.) -- C:\Users\manu\Desktop\JavaUpdate\_Rapport.exe [856523]

[MD5.DB93D6671398CEB31359D4C587776BB3] [SPRF][03/08/2012] (.Tomtomax et KoakDesign - Tomtomax Maxi-Box Setup.) -- C:\Users\manu\Desktop\tomtomax\_maxibox\_v3.1.2.exe [1533038]

~ Files: 8 Scanned in 00mn 01s

---\\ Etat général des services non Microsoft (EGS) (SR=Running, SS=Stopped)

SS - | Demand 14/06/2014 262320 | (AdobeFlashPlayerUpdateSvc) . (.Adobe Systems Incorporated.) - C:\Windows\system32\Macromed\Flash\FlashPlayerUpdateService.exe

SS - | Demand 01/05/2013 194032 | (gusvc) . (.Google.) - C:\Program Files\Google\Common\Google Updater\GoogleUpdaterService.exe

SS - | Demand 14/11/2005 69632 | (IDriverT) . (.Macrovision Corporation.) - C:\Program Files\Common Files\InstallShield\Driver\1150\Intel 32\IDriverT.exe

SS - | Demand 20/12/2010 251760 | (maconfservice) . (.CybelSoft.) - C:\Program Files\ma-config.com\maconfservice.exe

SS - | Auto 23/10/2013 172192 | (SkypeUpdate) . (.Skype Technologies.) - C:\Program Files\Skype\Updater\Updater.exe

SS - | Demand 28/06/2007 73728 | (VAIO Entertainment TV Device Arbitration Service) . (.Sony Corporation.) - C:\Program Files\Common Files\Sony Shared\VAIO Entertainment Platform\VzCs\VzHardwareResourceManager\VzHardwareResourceManager.exe

SS - | Demand 20/06/2007 2523136 | (VAIOMediaPlatform-IntegratedServer-AppServer) . (.Sony Corporation.) - C:\Program Files\Sony\VAIO Media Integrated Server\VMISrv.exe

SS - | Demand 20/06/2007 397312 | (VAIOMediaPlatform-IntegratedServer-HTTP) . (.Sony Corporation.) - C:\Program Files\Sony\VAIO Media Integrated Server\Platform\SV\_Httpd.exe

SS - | Demand 20/06/2007 1089536 | (VAIOMediaPlatform-IntegratedServer-UPnP) . (.Sony Corporation.) - C:\Program Files\Sony\VAIO Media Integrated Server\Platform\UPnPFramework.exe

SS - | Demand 20/06/2007 499712 | (VAIOMediaPlatform-Mobile-Gateway) . (.Sony Corporation.) - C:\Program Files\Sony\VAIO Media Integrated Server\Platform\VmGateway.exe

SS - | Demand 10/01/2007 745472 | (VAIOMediaPlatform-UCLS-AppServer) . (.Sony Corporation.) - C:\Program Files\Sony\VAIO Media Integrated Server\UCLS.exe

SS - | Demand 20/06/2007 397312 | (VAIOMediaPlatform-UCLS-HTTP) . (.Sony Corporation.) - C:\Program Files\Sony\VAIO Media Integrated Server\Platform\SV\_Httpd.exe

SS - | Demand 20/06/2007 1089536 | (VAIOMediaPlatform-UCLS-UPnP) . (.Sony Corporation.) - C:\Program Files\Sony\VAIO Media Integrated Server\Platform\UPnPFramework.exe

SS - | Demand 05/07/2007 292152 | (VcmIAlzMgr) . (.Sony Corporation.) - C:\Program Files\Sony\VCM Intelligent Analyzing Manager\VcmIAlzMgr.exe

SR - | Auto 21/12/2013 65432 | (AdobeARMservice) . (.Adobe Systems Incorporated.) - C:\Program Files\Common Files\Adobe\ARM\1.0\armsvc.exe

SR - | Auto 05/07/2014 50344 | (avast! Antivirus) . (.AVAST Software.) - C:\Program Files\AVAST Software\Avast\AvastSvc.exe

SR - | Auto 05/07/2014 106488 | (avast! Firewall) . (.AVAST Software.) - C:\Program Files\AVAST Software\Avast\afwServ.exe

SR - | Auto 14/03/2011 271712 | (HWDeviceService.exe) . (...) - C:\ProgramData\DatacardService\HWDeviceService.exe

SR - | Auto 20/07/2008 354840 | (IAANTMON) . (.Intel Corporation.) - C:\Program Files\Intel\Intel Matrix Storage Manager\Iaantmon.exe

SR - | Auto 04/01/2007 112152 | (IviRegMgr) . (.InterVideo.) - C:\Program Files\Common Files\InterVideo\RegMgr\iviRegMgr.exe

SR - | Auto 13/09/2007 102400 | (STacSV) . (.IDT, Inc..) - C:\Windows\system32\stacsv.exe

SR - | Auto 27/08/2013 93072 | (TomTomHOMEService) . (.TomTom.) - C:\Program Files\TomTom HOME 2\TomTomHOMEService.exe

SR - | Auto 24/07/2007 182392 | (VAIO Event Service) . (.Sony Corporation.) - C:\Program Files\Sony\VAIO Event Service\VESMgr.exe

SR - | Demand 28/06/2007 274432 | (Vcsw) . (.Sony Corporation.) - C:\Program Files\Common Files\Sony Shared\VAIO Entertainment Platform\VCSW\VCSW.exe

SR - | Demand 25/09/2013 1020976 | (VUAgent) . (.Sony Corporation.) - C:\Program Files\Sony\VAIO Update\VUAgent.exe

SR - | Auto 28/08/2007 192512 | (VzCdbSvc) . (.Sony Corporation.) - C:\Program Files\Common Files\Sony Shared\VAIO Entertainment Platform\VzCdb\VzCdbSvc.exe

SR - | Auto 28/08/2007 131072 | (VzFw) . (.Sony Corporation.) - C:\Program Files\Common Files\Sony Shared\VAIO Entertainment Platform\VzCdb\VzFw.exe

SR - | Auto 19/01/2008 21504 | C:\Program Files\Windows Defender\mpsvc.dll (WinDefend) . (.Microsoft Corporation.) - C:\Windows\System32\svchost.exe

SR - | Auto 19/01/2008 21504 | C:\Windows\System32\wuaueng.dll (wuauserv) . (.Microsoft Corporation.) - C:\Windows\System32\svchost.exe

~ Services: Scanned in 00mn 14s

---\\ 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 manu at 07/07/2014 16:08:25

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[0x84062916] >> \Device\Harddisk0\DR0[0x880051F8]

3 CLASSPNP[0x8A5A18B3] >> ntkrnlpa!IofCallDriver[0x84062916] >> [0x87564330]

5 acpi[0x846996BC] >> ntkrnlpa!IofCallDriver[0x84062916] >> \Device\Ide\IAAStorageDevice-0[0x86FDF028]

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 manu at 07/07/2014 16:08:27

\*\*\*\*\*\*\*\*\* Dump file Name \*\*\*\*\*\*\*\*\*

C:\PhysicalDisk0\_MBR.bin

~ MBR: Scanned in 00mn 04s

---\\ Scan Additionnel (O88)

Database Version : 13026 - (06/07/2014)

Clés trouvées (Keys found) : 4

Valeurs trouvées (Values found) : 0

Dossiers trouvés (Folders found) : 3

Fichiers trouvés (Files found) : 5

[HKCU\Software\ParetoLogic] =>PUP.Paretologic

[HKLM\Software\ParetoLogic] =>PUP.Paretologic

[HKLM\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\0FF2AEFF45EEA0A48A4B33C1973B6094] =>PUP.SweetIM^

[HKLM\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\305B09CE8C53A214DB58887F62F25536] =>PUP.SweetIM^

C:\Program Files\ParetoLogic =>PUP.Paretologic^

C:\ProgramData\ParetoLogic =>PUP.Paretologic^

C:\Users\manu\AppData\Roaming\ParetoLogic =>PUP.Paretologic^

C:\Program Files\ParetoLogic\PCHA\PCHA.exe =>Rogue.PCHealthAdvisor^

[HKCU\Software\Conduit] =>Toolbar.Conduit^

[HKLM\Software\Trymedia Systems] =>Adware.Trymedia^

C:\Users\manu\AppData\Local\Temp\GoogleToolbarInstaller1.log =>PUP.Babylon

C:\Users\manu\AppData\Local\Temp\GoogleToolbarInstaller2.log =>PUP.Babylon

~ Additionnel Scan: 280434 Items scanned in 00mn 33s

---\\ Informations complémentaires sur les modules

~ http://nicolascoolman.fr/r5-internet-explorer-proxy-management-iepm/ =>.Internet Explorer, Proxy Management (R5)

~ http://nicolascoolman.fr/o2-browser-helper-objects-de-navigateur/ =>.Browser Helper Objects de navigateur (O2)

~ http://nicolascoolman.fr/o4-applications-demarrees-par-le-registre/ =>.Applications lancées au démarrage du système (O4)

~ AMI: 3 Scanned in 00mn 00s

---\\ Récapitulatif des détections trouvées sur votre station

http://nicolascoolman.fr/30068076-pup-paretologic =>PUP.Paretologic

http://nicolascoolman.fr/toolbar-conduit =>Toolbar.Conduit

http://nicolascoolman.fr/adware-trymedia =>Adware.Trymedia

http://nicolascoolman.fr/pup-sweetim =>PUP.SweetIM

http://nicolascoolman.fr/pup-babylon =>PUP.Babylon

~ MSI: 5 link(s) detected in 00mn 00s

End of the scan (1208 lines in 03mn 44s)(0)