Rapport de ZHPDiag v1.31.28 par Nicolas Coolman, Update du 30/09/2012
Run by user at 04/10/2012 03:04:48
Web site : http://nicolascoolman.skyrock.com/
State : Problème connexion internet
UAC :

---\\ Web Browser
MSIE: Internet Explorer v8.0.6001.18702
GCIE: Google Chrome v22.0.1229.79 (Defaut)

---\\ Windows Product Information
~ Langage: Français
Windows XP Home Edition Service Pack 3 (Build 2600)
Windows Automatic Updates : OK
Windows Genuine Advantage : OK

---\\ System Information
~ Processor: x86 Family 15 Model 4 Stepping 1, GenuineIntel
~ Operating System: 32 Bits
Boot mode: Normal (Normal boot)
Total RAM: 2038 MB (52% free)
System Restore: Activé (Enable)
System drive C: has 677 GB (96%) free of 699 GB

---\\ Logged in mode
~ Computer Name: MAISON-A579729E
~ User Name: user
~ All Users Names: user, tf, SUPPORT_388945a0, HelpAssistant, Administrateur,
~ Unselected Option: O45,O61,O62,O65,O66,O80,O82,O89
Logged in as Administrator

---\\ Environnement Variables
~ System Unit : C:\
~ %AppData% : C:\Documents and Settings\user\Application Data\
~ %Desktop% : C:\Documents and Settings\user\Bureau\
~ %Favorites% : C:\Documents and Settings\user\Favoris\
~ %LocalAppData% : C:\Documents and Settings\user\Local Settings\Application Data\
~ %StartMenu% : C:\Documents and Settings\user\Menu Démarrer\
~ %Windir% : C:\WINDOWS\
~ %System% : C:\WINDOWS\system32\

---\\ DOS/Devices
A:\ Floppy drive, Flash card reader, USB Key (Not Inserted)
C:\ Hard drive, Flash drive, Thumb drive (Free 677 Go of 699 Go)
D:\ CD-ROM drive (Not Inserted)
E:\ Floppy drive, Flash card reader, USB Key (Not Inserted)

---\\ Security Center & Tools Informations
~ UAC deactivate by user

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Associations] Application: OK
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Associations] Intl: OK
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Associations] XMLLookup: OK
[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] Shell: OK
[HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows] Load: OK
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\Results\Install] LastSuccessTime : OK
~ Scan Security Center in 00mn 00s

---\\ Recherche particulière de fichiers génériques
[MD5.F2317622D29F9FF0F88AEECD5F60F0DD] - (.Microsoft Corporation - Explorateur Windows.) (.13/04/2008 - 19:34:04.) -- C:\WINDOWS\Explorer.exe [1037824]
[MD5.D0E5BB7F1F2B2A86CE809CC8EA9CB5B5] - (.Microsoft Corporation - Internet Extensions for Win32.) (.28/08/2012 - 16:04:59.) -- C:\WINDOWS\system32\wininet.dll [916992]
[MD5.DD73D6B9F6B4CB630CF35B438B540174] - (.Microsoft Corporation - Application d'ouverture de session Windows NT.) (.13/04/2008 - 19:34:30.) -- C:\WINDOWS\system32\Winlogon.exe [512000]
[MD5.1E44BC1E83D8FD2305F8D452DB109CF9] - (.Microsoft Corporation - Ancillary Function Driver for WinSock.) (.17/08/2011 - 14:49:54.) -- C:\WINDOWS\system32\Drivers\AFD.sys [138496]
[MD5.9F3A2F5AA6875C72BF062C712CFA2674] - (.Microsoft Corporation - IDE/ATAPI Port Driver.) (.13/04/2008 - 11:40:32.) -- C:\WINDOWS\system32\Drivers\atapi.sys [96512]
[MD5.C885B02847F5D2FD45A24E219ED93B32] - (.Microsoft Corporation - CD-ROM File System Driver.) (.13/04/2008 - 12:14:22.) -- C:\WINDOWS\system32\Drivers\Cdfs.sys [63744]
[MD5.1F4260CC5B42272D71F79E570A27A4FE] - (.Microsoft Corporation - SCSI CD-ROM Driver.) (.13/04/2008 - 11:40:48.) -- C:\WINDOWS\system32\Drivers\Cdrom.sys [62976]
[MD5.31F923EB2170FC172C81ABDA0045D18C] - (.Microsoft Corporation - Pilote de cryptographie FIPS.) (.13/04/2008 - 18:57:40.) -- C:\WINDOWS\system32\Drivers\Fips.sys [44672]
[MD5.573C7D0A32852B48F3058CFD8026F511] - (.Windows (R) Server 2003 DDK provider - High Definition Audio Bus Driver v1.0a.) (.13/04/2008 - 09:36:06.) -- C:\WINDOWS\system32\Drivers\HDAudBus.sys [144384]
[MD5.A09BDC4ED10E3B2E0EC27BB94AF32516] - (.Microsoft Corporation - Pilote de port i8042.) (.13/04/2008 - 19:00:54.) -- C:\WINDOWS\system32\Drivers\i8042prt.sys [54144]
[MD5.083A052659F5310DD8B6A6CB05EDCF8E] - (.Microsoft Corporation - IMAPI Kernel Driver.) (.13/04/2008 - 11:41:00.) -- C:\WINDOWS\system32\Drivers\Imapi.sys [42112]
[MD5.CC748EA12C6EFFDE940EE98098BF96BB] - (.Microsoft Corporation - IP Network Address Translator.) (.13/04/2008 - 11:57:16.) -- C:\WINDOWS\system32\Drivers\IpNat.sys [152832]
[MD5.23C74D75E36E7158768DD63D92789A91] - (.Microsoft Corporation - IPSec Driver.) (.13/04/2008 - 12:19:44.) -- C:\WINDOWS\system32\Drivers\IPSec.sys [75264]
[MD5.7D304A5EB4344EBEEAB53A2FE3FFB9F0] - (.Microsoft Corporation - Windows NT SMB Minirdr.) (.15/07/2011 - 14:29:31.) -- C:\WINDOWS\system32\Drivers\MRxSmb.sys [456320]
[MD5.74B2B2F5BEA5E9A3DC021D685551BD3D] - (.Microsoft Corporation - MBT Transport driver.) (.13/04/2008 - 12:21:02.) -- C:\WINDOWS\system32\Drivers\netBT.sys [162816]
[MD5.78A08DD6A8D65E697C18E1DB01C5CDCA] - (.Microsoft Corporation - NT File System Driver.) (.13/04/2008 - 12:15:54.) -- C:\WINDOWS\system32\Drivers\ntfs.sys [574976]
[MD5.8FD0BDBEA875D06CCF6C945CA9ABAF75] - (.Microsoft Corporation - Pilote de port

parallèle.) (.13/04/2008 - 19:47:24.) -- C:\WINDOWS\system32\Drivers\Parport.sys [80384] [MD5.11B4A627BC9614B885C4969BFA5FF8A6] - (.Microsoft Corporation - RAS L2TP mini-port/call-manager driver.) (.13/04/2008 - 12:19:44.) -- C:\WINDOWS\system32\Drivers\Rasl2tp.sys [51328]
[MD5.15CABD0F7C00C47C70124907916AF3F1] - (.Microsoft Corporation - Microsoft RDP Device redirector.) (.13/04/2008 - 10:32:52.) -- C:\WINDOWS\system32\Drivers\rdpdr.sys [196224]
[MD5.D8EB2A7904DB6C916EB5361878DDCBAE] - (.Microsoft Corporation - Pilote de filtre audio Livre rouge.) (.13/04/2008 - 19:57:36.) -- C:\WINDOWS\system32\Drivers\redbook.sys [58752]
[MD5.46DE1126684369BACE4849E4FC8C43CA] - (.Microsoft Corporation - Pilote de cliché instantané du volume.) (.13/04/2008 - 18:56:06.) -- C:\WINDOWS\system32\Drivers\volsnap.sys [53376]
~ Scan Generic Processes in 00mn 00s

---\\ Etat des fichiers cachés (Caché/Total)
~ Mes images (My Pictures) : 2/104
~ Mes musiques (My Musics) : 1/9
~ Mes Videos (My Videos) : 1/5
~ Mes Favoris (My Favorites) : 1/14
~ Mes Documents (My Documents) : 1/2091
~ Mon Bureau (My Desktop) : 0/642
~ Menu demarrer (Programs) : 1/25
~ Scan Hidden Files in 00mn 01s

---\\ Processus lancés
[MD5.04AC21E821F259845BD7367CEE057290] - (.AVAST Software - avast! Service.) -- C:\Program Files\Alwil Software\Avast5\AvastSvc.exe [44808] [PID.]
[MD5.28E8A9984BA1297EFE44B6138D2CA51E] - (.Sun Microsystems, Inc. - Java(TM) Quick Starter Service.) -- C:\Program Files\Java\jre6\bin\jqs.exe [153392] [PID.]
[MD5.C52C9D43108E8DB947DCF053356843A7] - (.Pas de propriétaire - Printer Communication System.) -- C:\WINDOWS\system32\lxctcoms.exe [537520] [PID.]
[MD5.F036CFB275D0C55F4E45FBBF5F98B3C8] - (.Protexis Inc. - PsiService PsiService.) -- C:\Program Files\Fichiers communs\Protexis\License Service\PsiService_2.exe [193824] [PID.]
[MD5.F4A9476AA49B69D28BE439C64F96C714] - (...) -- C:\Program Files\Web Assistant\ExtensionUpdaterService.exe [188760] [PID.]
[MD5.52C18A4B4AC4778B6980CF8284893FB8] - (...) -- C:\WINDOWS\system32\dmwu.exe [1006448] [PID.]
[MD5.6194CC4A71F51CF3E815252BB43AAC28] - (.Google Inc. - Google Chrome.) -- C:\Documents and Settings\user\Local Settings\Application Data\Google\Chrome\Application\chrome.exe [1239064] [PID.]
[MD5.41D0F8FD52CA4B98D21F9D137F0F5FF9] - (...) -- C:\Program Files\ZHPDiag\ZHPDiag.exe [3769856] [PID.]
[MD5.5E9A6658A2A69AE7EB195113B7A2E7A9] - (.Microsoft Corporation - Application Layer Gateway Service.) -- C:\WINDOWS\System32\alg.exe [44544] [PID.]
~ Scan Processes Running in 00mn 00s

---\\ Google Chrome, Démarrage,Recherche,Extensions (G0,G1,G2)
C:\Documents and Settings\user\Local Settings\Application Data\Google\Chrome\User Data\Default\Preferences
G0 - GCSP: Preference [User Data\Default][HomePage] http://www.google.fr
G0 - GCSP: Preference [User Data\Default] http://www.google.fr
G1 - GCS: Preference [User Data\Default] None
~ Scan Google Browser in 00mn 00s

---\\ Mozilla Firefox, Plugins,Demarrage,Recherche,Extensions (P2,M0,M1,M2,M3)
P2 - FPN: [HKLM] [@java.com/DTPlugin,version=1.6.0_33] - (.Sun Microsystems, Inc. - NPRuntime Script Plug-in Library for Java(TM) Deploy.) -- C:\WINDOWS\system32\npdeployJava1.dll
P2 - FPN: [HKLM] [@java.com/JavaPlugin] - (.Sun Microsystems, Inc. - Next Generation Java Plug-in 1.6.0_33 for Mozilla browsers.) -- C:\Program Files\Java\jre6\bin\plugin2\npjp2.dll
P2 - FPN: [HKLM] [@Microsoft.com/NpCtrl,version=1.0] - (. Microsoft Corporation - 5.1.10411.0.) -- c:\Program Files\Microsoft Silverlight\5.1.10411.0\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] [@tools.google.com/Google Update;version=3] - (.Google Inc. - Google Update.) -- C:\Program Files\Google\Update\1.3.21.123\npGoogleUpdate3.dll
P2 - FPN: [HKLM] [@tools.google.com/Google Update;version=9] - (.Google Inc. - Google Update.) -- C:\Program Files\Google\Update\1.3.21.123\npGoogleUpdate3.dll
P2 - FPN: [HKLM] [Adobe Reader] - (.Adobe Systems Inc. - Adobe PDF Plug-In For Firefox and Netscape 10.1.4.) -- C:\Program Files\Adobe\Reader 10.0\Reader\AIR\nppdf32.dll
P2 - FPN: [HKCU] [@tools.google.com/Google Update;version=3] - (.Google Inc. - Google Update.) -- C:\Documents and Settings\user\Local Settings\Application Data\Google\Update\1.3.21.123\npGoogleUpdate3.dll
P2 - FPN: [HKCU] [@tools.google.com/Google Update;version=9] - (.Google Inc. - Google Update.) -- C:\Documents and Settings\user\Local Settings\Application Data\Google\Update\1.3.21.123\npGoogleUpdate3.dll
~ Scan Firefox Browser in 00mn 00s

---\\ Internet Explorer, Démarrage,Recherche,URLSearchHook, Phishing (R0,R1,R3,R4)
R0 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = http://google.fr
R0 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = http://start.funmoods.com
R1 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Search Page = http://www.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
R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\AboutURLs,Tabs = http://start.funmoods.com
R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Search,SearchAssistant = http://ie.search.msn.com
R3 - URLSearchHook: (no name) - {EEE6C35D-6118-11DC-9C72-001320C79847} . (.Google Inc.

- Google Update.) (No version) -- (.not file.)
~ Scan IE Browser 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
~ Scan Proxy management in 00mn 00s

---\\ Modification d'une valeur Ini (Changed inifile value, mapped to Registry) (F2)
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"
~ Scan Keys in 00mn 00s

---\\ Redirection du fichier Hosts (O1)
~ Le fichier hosts est sain (The hosts file is clean).
~ Scan Hosts File in 00mn 00s
~ Nombre de lignes (Lines number): 22

---\\ Browser Helper Objects de navigateur (O2)
O2 - BHO: (no name) - {0F6E720A-1A6B-40E1-A294-1D4D19F156C8} Clé orpheline
O2 - BHO: (no name) - {0FB6A909-6086-458F-BD92-1F8EE10042A0} Clé orpheline
O2 - BHO: (no name) - {1017A80C-6F09-4548-A84D-EDD6AC9525F0} Clé orpheline
O2 - BHO: (no name) - {18DF081C-E8AD-4283-A596-FA578C2EBDC3} Clé orpheline
O2 - BHO: (no name) - {336D0C35-8A85-403a-B9D2-65C292C39087} Clé orpheline
O2 - BHO: (no name) - {75EBB0AA-4214-4CB4-90EC-E3E07ECD04F7} Clé orpheline
O2 - BHO: (no name) - {761497BB-D6F0-462C-B6EB-D4DAF1D92D43} Clé orpheline
O2 - BHO: (no name) - {8E5E2654-AD2D-48bf-AC2D-D17F00898D06} Clé orpheline
O2 - BHO: (no name) - {DBC80044-A445-435b-BC74-9C25C1C588A9} Clé orpheline
O2 - BHO: (no name) - {E7E6F031-17CE-4C07-BC86-EABFE594F69C} Clé orpheline
O2 - BHO: (no name) - {EEE6C35C-6118-11DC-9C72-001320C79847} Clé orpheline
~ Scan BHO in 00mn 00s

---\\ Internet Explorer Toolbars (O3)
O3 - Toolbar: (no name) - [HKLM]{EEE6C35B-6118-11DC-9C72-001320C79847} . (...) -- (.not file.)
O3 - Toolbar: (no name) - [HKLM]{1017A80C-6F09-4548-A84D-EDD6AC9525F0} . (...) -- (.not file.)

O3 - Toolbar: (no name) - [HKLM]{A4C272EC-ED9E-4ACE-A6F2-9558C7F29EF3} . (...) -- (.not file.)
O3 - Toolbar: (no name) - [HKLM]{8E5E2654-AD2D-48bf-AC2D-D17F00898D06} . (...) -- (.not file.)
~ Scan Toolbar in 00mn 00s

---\\ Applications démarrées par registre & par dossier (O4)
O4 - HKLM\..\Run: [IgfxTray] . (.Intel Corporation - igfxTray Module.) -- C:\WINDOWS\system32\igfxtray.exe
O4 - HKLM\..\Run: [HotKeysCmds] . (.Intel Corporation - hkcmd Module.) -- C:\WINDOWS\system32\hkcmd.exe
O4 - HKLM\..\Run: [Persistence] . (.Intel Corporation - persistence Module.) -- C:\WINDOWS\system32\igfxpers.exe
O4 - HKLM\..\Run: [avast5] . (.AVAST Software - avast! Antivirus.) -- C:\Program Files\Alwil Software\Avast5\avastUI.exe
O4 - HKLM\..\Run: [Adobe ARM] . (.Adobe Systems Incorporated - Adobe Reader and Acrobat Manager.) -- C:\Program Files\Fichiers communs\Adobe\ARM\1.0\AdobeARM.exe
O4 - HKLM\..\Run: [SoundMAXPnP] . (.Analog Devices, Inc. - SMax4PNP MFC Application.) -- C:\Program Files\Analog Devices\Core\smax4pnp.exe
O4 - HKLM\..\Run: [APSDaemon] . (.Apple Inc. - Apple Push.) -- C:\Program Files\Fichiers communs\Apple\Apple Application Support\APSDaemon.exe
O4 - HKLM\..\Run: [SweetIM] . (.SweetIM Technologies Ltd. - SweetIM Instant Messenger Enhancer.) -- C:\Program Files\SweetIM\Messenger\SweetIM.exe
O4 - HKLM\..\Run: [QuickTime Task] . (.Apple Inc. - QuickTime Task.) -- C:\Program Files\QuickTime\QTTask.exe
O4 - HKLM\..\Run: [lxctmon.exe] . (.Pas de propriétaire - Device Monitor.) -- C:\Program Files\Lexmark 5400 Series\lxctmon.exe
O4 - HKLM\..\Run: [Lexmark 5400 Series Fax Server] . (.Pas de propriétaire - Fax Man Server.) -- C:\Program Files\Lexmark 5400 Series\fm3032.exe
O4 - HKLM\..\Run: [EzPrint] . (.Lexmark International Inc. - Lexmark Fast Pics Application.) -- C:\Program Files\Lexmark 5400 Series\ezprint.exe
O4 - HKLM\..\Run: [LXCTCATS] rundll32 C:\WINDOWS\System32\spool\DRIVERS\W32X86\3\LXCTtime.dll (.not file.)
O4 - HKLM\..\Run: [KernelFaultCheck] Clé orpheline
O4 - HKLM\..\Run: [SunJavaUpdateSched] . (.Sun Microsystems, Inc. - Java(TM) Update Scheduler.) -- C:\Program Files\Fichiers communs\Java\Java Update\jusched.exe
O4 - HKCU\..\Run: [CTFMON.EXE] . (.Microsoft Corporation - CTF Loader.) -- C:\WINDOWS\system32\ctfmon.exe
O4 - HKCU\..\Run: [MSMSGS] . (.Microsoft Corporation - Windows Messenger.) -- C:\Program Files\Messenger\msmsgs.exe
O4 - HKCU\..\Run: [ares] C:\Program Files\Ares\Ares.exe (.not file.)
O4 - HKCU\..\Run: [Google Update] . (.Google Inc. - Programme d'installation de Google.) -- C:\Documents and Settings\user\Local Settings\Application Data\Google\Update\GoogleUpdate.exe
O4 - HKCU\..\Run: [Badoo Desktop] C:\Documents and Settings\All Users\Application Data\Badoo\Badoo desktop\1.6.55.1183\Badoo.desktop.exe (.not file.)
O4 - HKUS\S-1-5-18\..\Run: [CTFMON.EXE] . (.Microsoft Corporation - CTF Loader.) -- C:\WINDOWS\system32\CTFMON.exe
O4 - HKUS\S-1-5-18\..\Run: [CTFMON.EXE] . (.Microsoft Corporation - CTF Loader.) -- C:\WINDOWS\system32\CTFMON.exe

O4 - HKUS\S-1-5-19\..\Run: [CTFMON.EXE] . (.Microsoft Corporation - CTF Loader.) -- C:\WINDOWS\system32\CTFMON.exe
O4 - HKUS\S-1-5-20\..\Run: [CTFMON.EXE] . (.Microsoft Corporation - CTF Loader.) -- C:\WINDOWS\system32\CTFMON.exe
O4 - HKUS\S-1-5-21-2851534266-985727058-2256982857-1004\..\Run: [CTFMON.EXE] . (.Microsoft Corporation - CTF Loader.) -- C:\WINDOWS\system32\ctfmon.exe
O4 - HKUS\S-1-5-21-2851534266-985727058-2256982857-1004\..\Run: [MSMSGS] . (.Microsoft Corporation - Windows Messenger.) -- C:\Program Files\Messenger\msmsgs.exe
O4 - HKUS\S-1-5-21-2851534266-985727058-2256982857-1004\..\Run: [ares] C:\Program Files\Ares\Ares.exe (.not file.)
O4 - HKUS\S-1-5-21-2851534266-985727058-2256982857-1004\..\Run: [Google Update] . (.Google Inc. - Programme d'installation de Google.) -- C:\Documents and Settings\user\Local Settings\Application Data\Google\Update\GoogleUpdate.exe
O4 - HKUS\S-1-5-21-2851534266-985727058-2256982857-1004\..\Run: [Badoo Desktop] C:\Documents and Settings\All Users\Application Data\Badoo\Badoo desktop\1.6.55.1183\Badoo.desktop.exe (.not file.)
~ Scan Application in 00mn 00s

---\\ Autres liens utilisateurs (O4)
O4 - Global Startup: C:\Documents And Settings\All Users\Menu Démarrer\Programmes\Adobe Reader X.lnk . (...) -- C:\WINDOWS\Installer\{AC76BA86-7AD7-1036-7B44-AA1000000001}\SC_Reader.ico
O4 - Global Startup: C:\Documents And Settings\All Users\Menu Démarrer\Programmes\Apple Software Update.lnk . (...) -- C:\WINDOWS\Installer\{789A5B64-9DD9-4BA5-915A-F0FC0A1B7BFE}\AppleSoftwareUpdateIco.exe
O4 - Global Startup: C:\Documents And Settings\All Users\Menu Démarrer\Programmes\Corel WinDVD 2010.lnk . (.Corel Corporation.) -- C:\Program Files\Corel\CorelWinDVD2010\WinDVD.exe
O4 - Global Startup: C:\Documents And Settings\All Users\Menu Démarrer\Programmes\Serif DrawPlus X2.lnk . (...) -- C:\WINDOWS\Installer\{4D9DD45B-E79A-4F04-898E-B2C3769AB729}\DrawPlus.ico
O4 - Global Startup: C:\Documents And Settings\All Users\Menu Démarrer\Programmes\Windows Movie Maker.lnk . (.Microsoft Corporation.) -- C:\Program Files\Movie Maker\moviemk.exe
O4 - Global Startup: C:\Documents And Settings\user\Menu Démarrer\Programmes\Assistance à distance.lnk . (.Microsoft Corporation.) -- C:\WINDOWS\system32\rcimlby.exe
O4 - Global Startup: C:\Documents And Settings\user\Menu Démarrer\Programmes\Outlook Express.lnk . (.Microsoft Corporation.) -- C:\Program Files\Outlook Express\msimn.exe
O4 - Global Startup: C:\Documents And Settings\user\Menu Démarrer\Programmes\Windows Media Player.lnk . (.Microsoft Corporation.) -- C:\Program Files\Windows Media Player\wmplayer.exe
O4 - Global Startup: C:\Documents And Settings\tf\Menu Démarrer\Programmes\Assistance à distance.lnk . (.Microsoft Corporation.) -- C:\WINDOWS\system32\rcimlby.exe
O4 - Global Startup: C:\Documents And Settings\tf\Menu Démarrer\Programmes\Internet Explorer.lnk . (.Microsoft Corporation.) -- C:\Program Files\Internet Explorer\iexplore.exe
O4 - Global Startup: C:\Documents And Settings\tf\Menu Démarrer\Programmes\Lecteur Windows Media.lnk . (.Microsoft Corporation.) -- C:\Program Files\Windows Media Player\wmplayer.exe
O4 - Global Startup: C:\Documents And Settings\tf\Menu Démarrer\Programmes\Outlook Express.lnk . (.Microsoft Corporation.) -- C:\Program Files\Outlook Express\msimn.exe
O4 - Global Startup: C:\Documents And Settings\All Users\Menu Démarrer\Programmes\Adobe Reader X.lnk . (...) -- C:\WINDOWS\Installer\{AC76BA86-7AD7-1036-7B44-

AA1000000001}\SC_Reader.ico
O4 - Global Startup: C:\Documents And Settings\All Users\Menu Démarrer\Programmes\Apple Software Update.lnk . (...) -- C:\WINDOWS\Installer\{789A5B64-9DD9-4BA5-915A-F0FC0A1B7BFE}\AppleSoftwareUpdateIco.exe
O4 - Global Startup: C:\Documents And Settings\All Users\Menu Démarrer\Programmes\Corel WinDVD 2010.lnk . (.Corel Corporation.) -- C:\Program Files\Corel\CorelWinDVD2010\WinDVD.exe
O4 - Global Startup: C:\Documents And Settings\All Users\Menu Démarrer\Programmes\Serif DrawPlus X2.lnk . (...) -- C:\WINDOWS\Installer\{4D9DD45B-E79A-4F04-898E-B2C3769AB729}\DrawPlus.ico
O4 - Global Startup: C:\Documents And Settings\All Users\Menu Démarrer\Programmes\Windows Movie Maker.lnk . (.Microsoft Corporation.) -- C:\Program Files\Movie Maker\moviemk.exe
O4 - Global Startup: C:\Documents And Settings\user\Menu Démarrer\Programmes\Assistance à distance.lnk . (.Microsoft Corporation.) -- C:\WINDOWS\system32\rcimlby.exe
O4 - Global Startup: C:\Documents And Settings\user\Menu Démarrer\Programmes\Outlook Express.lnk . (.Microsoft Corporation.) -- C:\Program Files\Outlook Express\msimn.exe
O4 - Global Startup: C:\Documents And Settings\user\Menu Démarrer\Programmes\Windows Media Player.lnk . (.Microsoft Corporation.) -- C:\Program Files\Windows Media Player\wmplayer.exe
O4 - Global Startup: C:\Documents And Settings\tf\Menu Démarrer\Programmes\Assistance à distance.lnk . (.Microsoft Corporation.) -- C:\WINDOWS\system32\rcimlby.exe
O4 - Global Startup: C:\Documents And Settings\tf\Menu Démarrer\Programmes\Internet Explorer.lnk . (.Microsoft Corporation.) -- C:\Program Files\Internet Explorer\iexplore.exe
O4 - Global Startup: C:\Documents And Settings\tf\Menu Démarrer\Programmes\Lecteur Windows Media.lnk . (.Microsoft Corporation.) -- C:\Program Files\Windows Media Player\wmplayer.exe
O4 - Global Startup: C:\Documents And Settings\tf\Menu Démarrer\Programmes\Outlook Express.lnk . (.Microsoft Corporation.) -- C:\Program Files\Outlook Express\msimn.exe
~ Scan Global Startup in 00mn 00s

---\\ Boutons situés sur la barre d'outils principale d'Internet Explorer (O9)
O9 - Extra button: @xpsp3res.dll,-20001 - {e2e2dd38-d088-4134-82b7-f2ba38496583} -- Clé orpheline
O9 - Extra button: Windows Messenger - {FB5F1910-F110-11d2-BB9E-00C04F795683} . (.Microsoft Corporation - Windows Messenger.) -- C:\Program Files\Messenger\msmsgs.exe
~ Scan IE Extra Buttons in 00mn 00s

---\\ Winsock hijacker (Layered Service Provider) (O10)
O10 - WLSP:\000000000001\Winsock LSP File . (.Microsoft Corporation - Fournisseur de service Sockets 2.0 de Microsoft Windows.) -- C:\WINDOWS\system32\mswsock.dll
O10 - WLSP:\000000000002\Winsock LSP File . (.Microsoft Corporation - LDAP RnR Provider DLL.) -- C:\WINDOWS\system32\winrnr.dll
O10 - WLSP:\000000000003\Winsock LSP File . (.Microsoft Corporation - Fournisseur de service Sockets 2.0 de Microsoft Windows.) -- C:\WINDOWS\system32\mswsock.dll
~ Scan Winsock in 00mn 00s

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

O16 - DPF: {17492023-C23A-453E-A040-C7C580BBF700} (Windows Genuine Advantage Validation Tool) - http://go.microsoft.com/fwlink/?linkid=39204
~ Scan Objets ActiveX in 00mn 00s

---\\ Modification Domaine/Adresses DNS (O17)
O17 - HKLM\System\CCS\Services\Tcpip\..\{15DBBA58-4838-4CDE-9046-8A9F5BD78F53}: DhcpNameServer = 192.168.1.1
O17 - HKLM\System\CCS\Services\Tcpip\..\{2A51258E-86C7-4366-92FC-5600FD9197A8}: DhcpNameServer = 0.0.0.0
O17 - HKLM\System\CCS\Services\Tcpip\..\{F365305E-D797-4C8A-AD33-C045E5D31540}: DhcpNameServer = 192.168.1.1
O17 - HKLM\System\CS1\Services\Tcpip\..\{15DBBA58-4838-4CDE-9046-8A9F5BD78F53}: DhcpNameServer = 192.168.1.1
O17 - HKLM\System\CS1\Services\Tcpip\..\{2A51258E-86C7-4366-92FC-5600FD9197A8}: DhcpNameServer = 0.0.0.0
O17 - HKLM\System\CS1\Services\Tcpip\..\{78123132-BE6F-4B48-B21B-783388FEADD0}: DhcpNameServer = 192.168.1.254
O17 - HKLM\System\CS1\Services\Tcpip\..\{78123132-BE6F-4B48-B21B-783388FEADD0}: DhcpDomain = lan
O17 - HKLM\System\CS2\Services\Tcpip\..\{15DBBA58-4838-4CDE-9046-8A9F5BD78F53}: DhcpNameServer = 192.168.1.1
O17 - HKLM\System\CS2\Services\Tcpip\..\{2A51258E-86C7-4366-92FC-5600FD9197A8}: DhcpNameServer = 0.0.0.0
O17 - HKLM\System\CS2\Services\Tcpip\..\{F365305E-D797-4C8A-AD33-C045E5D31540}: DhcpNameServer = 192.168.1.1
O17 - HKLM\System\CS3\Services\Tcpip\..\{15DBBA58-4838-4CDE-9046-8A9F5BD78F53}: DhcpNameServer = 192.168.1.1
O17 - HKLM\System\CS3\Services\Tcpip\..\{2A51258E-86C7-4366-92FC-5600FD9197A8}: DhcpNameServer = 0.0.0.0
O17 - HKLM\System\CS3\Services\Tcpip\..\{F365305E-D797-4C8A-AD33-C045E5D31540}: DhcpNameServer = 192.168.1.1
~ Scan Domain in 00mn 00s

---\\ Protocole additionnel (O18)
O18 - Handler: about - {3050F406-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Microsoft (R) HTML Viewer.) -- C:\WINDOWS\system32\mshtml.dll
O18 - Handler: cdl - {3dd53d40-7b8b-11D0-b013-00aa0059ce02} . (.Microsoft Corporation - OLE32 Extensions for Win32.) -- C:\WINDOWS\system32\urlmon.dll
O18 - Handler: dvd - {12D51199-0DB5-46FE-A120-47A3D7D937CC} . (.Microsoft Corporation - Contrôle ActiveX pour le flux vidéo.) -- C:\WINDOWS\system32\msvidctl.dll
O18 - Handler: file - {79eac9e7-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - OLE32 Extensions for Win32.) -- C:\WINDOWS\system32\urlmon.dll
O18 - Handler: ftp - {79eac9e3-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - OLE32 Extensions for Win32.) -- C:\WINDOWS\system32\urlmon.dll
O18 - Handler: gopher - {79eac9e4-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - OLE32 Extensions for Win32.) -- C:\WINDOWS\system32\urlmon.dll
O18 - Handler: http - {79eac9e2-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - OLE32 Extensions for Win32.) -- C:\WINDOWS\system32\urlmon.dll

O18 - Handler: https - {79eac9e5-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - OLE32 Extensions for Win32.) -- C:\WINDOWS\system32\urlmon.dll
O18 - Handler: its - {9D148291-B9C8-11D0-A4CC-0000F80149F6} . (.Microsoft Corporation - Microsoft® InfoTech Storage System Library.) -- C:\WINDOWS\system32\itss.dll
O18 - Handler: javascript - {3050F3B2-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Microsoft (R) HTML Viewer.) -- C:\WINDOWS\system32\mshtml.dll
O18 - Handler: local - {79eac9e7-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - OLE32 Extensions for Win32.) -- C:\WINDOWS\system32\urlmon.dll
O18 - Handler: mailto - {3050f3DA-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Microsoft (R) HTML Viewer.) -- C:\WINDOWS\system32\mshtml.dll
O18 - Handler: mhtml - {05300401-BCBC-11d0-85E3-00C04FD85AB4} . (.Microsoft Corporation - Microsoft Internet Messaging API.) -- C:\WINDOWS\system32\inetcomm.dll
O18 - Handler: mk - {79eac9e6-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - OLE32 Extensions for Win32.) -- C:\WINDOWS\system32\urlmon.dll
O18 - Handler: ms-its - {9D148291-B9C8-11D0-A4CC-0000F80149F6} . (.Microsoft Corporation - Microsoft® InfoTech Storage System Library.) -- C:\WINDOWS\system32\itss.dll
O18 - Handler: res - {3050F3BC-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Microsoft (R) HTML Viewer.) -- C:\WINDOWS\system32\mshtml.dll
O18 - Handler: sysimage - {76E67A63-06E9-11D2-A840-006008059382} . (.Microsoft Corporation - Microsoft (R) HTML Viewer.) -- C:\WINDOWS\system32\mshtml.dll
O18 - Handler: tv - {CBD30858-AF45-11D2-B6D6-00C04FBBDE6E} . (.Microsoft Corporation - Contrôle ActiveX pour le flux vidéo.) -- C:\WINDOWS\system32\msvidctl.dll
O18 - Handler: vbscript - {3050F3B2-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Microsoft (R) HTML Viewer.) -- C:\WINDOWS\system32\mshtml.dll
O18 - Handler: wia - {13F3EA8B-91D7-4F0A-AD76-D2853AC8BECE} . (.Microsoft Corporation - WIA Scripting Layer.) -- C:\WINDOWS\system32\wiascr.dll
O18 - Filter: application/octet-stream - {1E66F26B-79EE-11D2-8710-00C04F79ED0D} . (.Microsoft Corporation - Microsoft .NET Runtime Execution Engine.) -- C:\WINDOWS\system32\mscoree.dll
O18 - Filter: application/x-complus - {1E66F26B-79EE-11D2-8710-00C04F79ED0D} . (.Microsoft Corporation - Microsoft .NET Runtime Execution Engine.) -- C:\WINDOWS\system32\mscoree.dll
O18 - Filter: application/x-msdownload - {1E66F26B-79EE-11D2-8710-00C04F79ED0D} . (.Microsoft Corporation - Microsoft .NET Runtime Execution Engine.) -- C:\WINDOWS\system32\mscoree.dll
O18 - Filter: Class Install Handler - {32B533BB-EDAE-11d0-BD5A-00AA00B92AF1} . (.Microsoft Corporation - OLE32 Extensions for Win32.) -- C:\WINDOWS\system32\urlmon.dll
O18 - Filter: deflate - {8f6b0360-b80d-11d0-a9b3-006097942311} . (.Microsoft Corporation - OLE32 Extensions for Win32.) -- C:\WINDOWS\system32\urlmon.dll
O18 - Filter: gzip - {8f6b0360-b80d-11d0-a9b3-006097942311} . (.Microsoft Corporation - OLE32 Extensions for Win32.) -- C:\WINDOWS\system32\urlmon.dll
O18 - Filter: lzdhtml - {8f6b0360-b80d-11d0-a9b3-006097942311} . (.Microsoft Corporation - OLE32 Extensions for Win32.) -- C:\WINDOWS\system32\urlmon.dll
O18 - Filter: text/webviewhtml - {733AC4CB-F1A4-11d0-B951-00A0C90312E1} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\WINDOWS\system32\SHELL32.dll
~ Scan Protocole Additionnel in 00mn 00s

---\\ Valeur de Registre AppInit_DLLs et sous-clés Winlogon Notify (autorun) (O20)
O20 - Winlogon Notify: crypt32chain . (.Microsoft Corporation - Crypto API32.) -- C:\WINDOWS\system32\crypt32.dll
O20 - Winlogon Notify: cryptnet . (.Microsoft Corporation - Crypto Network Related API.) --

C:\WINDOWS\system32\cryptnet.dll
O20 - Winlogon Notify: cscdll . (.Microsoft Corporation - Agent réseau hors connexion.) -- C:\WINDOWS\system32\cscdll.dll
O20 - Winlogon Notify: dimsntfy . (.Microsoft Corporation - DIMS Notification Handler.) -- C:\WINDOWS\system32\dimsntfy.dll
O20 - Winlogon Notify: igfxcui . (.Intel Corporation - igfxsrvc Module.) -- C:\WINDOWS\system32\igfxsrvc.dll
O20 - Winlogon Notify: ScCertProp . (.Microsoft Corporation - DLL commune de réception des notifications.) -- C:\WINDOWS\system32\wlnotify.dll
O20 - Winlogon Notify: Schedule . (.Microsoft Corporation - DLL commune de réception des notifications.) -- C:\WINDOWS\system32\wlnotify.dll
O20 - Winlogon Notify: sclgntfy . (.Microsoft Corporation - DLL secondaire de notification de service d.) -- C:\WINDOWS\system32\sclgntfy.dll
O20 - Winlogon Notify: SensLogn . (.Microsoft Corporation - DLL commune de réception des notifications.) -- C:\WINDOWS\system32\WlNotify.dll
O20 - Winlogon Notify: termsrv . (.Microsoft Corporation - DLL commune de réception des notifications.) -- C:\WINDOWS\system32\wlnotify.dll
O20 - Winlogon Notify: wlballoon . (.Microsoft Corporation - DLL commune de réception des notifications.) -- C:\WINDOWS\system32\wlnotify.dll
~ Scan Winlogon in 00mn 00s

---\\ Clé de Registre autorun ShellServiceObjectDelayLoad (SSO/SSODL) (O21)
O21 - SSODL: PostBootReminder - {7849596a-48ea-486e-8937-a2a3009f31a9} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\WINDOWS\system32\SHELL32.dll
O21 - SSODL: CDBurn - {fbeb8a05-beee-4442-804e-409d6c4515e9} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\WINDOWS\system32\SHELL32.dll
O21 - SSODL: WebCheck - {E6FB5E20-DE35-11CF-9C87-00AA005127ED} . (.Microsoft Corporation - Web Site Monitor.) -- C:\WINDOWS\system32\webcheck.dll
O21 - SSODL: SysTray - {35CEC8A3-2BE6-11D2-8773-92E220524153} . (.Microsoft Corporation - Objet du service d'environnement Systray.) -- C:\WINDOWS\system32\stobject.dll
O21 - SSODL: WPDShServiceObj - {AAA288BA-9A4C-45B0-95D7-94D524869DB5} . (.Microsoft Corporation - Windows Portable Device Shell Service Objec.) -- C:\WINDOWS\system32\WPDShServiceObj.dll
~ Scan SSODL in 00mn 00s

---\\ Liste des services NT non Microsoft et non désactivés (O23)
O23 - Service: avast! Antivirus (avast! Antivirus) . (.AVAST Software - avast! Service.) - C:\Program Files\Alwil Software\Avast5\AvastSvc.exe
O23 - Service: Service Google Update (gupdate) (gupdate) . (.Google Inc. - Programme d'installation de Google.) - C:\Program Files\Google\Update\GoogleUpdate.exe
O23 - Service: Java Quick Starter (JavaQuickStarterService) . (.Sun Microsystems, Inc. - Java(TM) Quick Starter Service.) - C:\Program Files\Java\jre6\bin\jqs.exe
O23 - Service: lxct_device (lxct_device) . (.Pas de propriétaire - Printer Communication System.) - C:\WINDOWS\system32\lxctcoms.exe
O23 - Service: Protexis Licensing V2 (PSI_SVC_2) . (.Protexis Inc. - PsiService PsiService.) - C:\Program Files\Fichiers communs\Protexis\License Service\PsiService_2.exe
O23 - Service: Web Assistant Updater (Web Assistant Updater) . (...) - C:\Program Files\Web Assistant\ExtensionUpdaterService.exe

O23 - Service: (WebOptimizer) . (...) - C:\WINDOWS\system32\dmwu.exe
~ Scan Services in 00mn 00s

---\\ Enumération Active Desktop & MHTML Editor (O24)
O24 - Default MHTML Editor: Last - .(...) - (.not file.)
O24 - Desktop General: BackupWallPaper - .(...) - C:\Documents and Settings\user\Local Settings\Application Data\Microsoft\Wallpaper1.bmp
O24 - Desktop General: WallPaper - .(...) - C:\Documents and Settings\user\Local Settings\Application Data\Microsoft\Wallpaper1.bmp
~ Scan Desktop Component in 00mn 00s

---\\ BootExecute (O34)
O34 - HKLM BootExecute: (autocheck autochk *) - File not found
~ Scan Keys in 00mn 00s

---\\ Tâches planifiées en automatique (O39)
O39 - APT:Automatic Planified Task - C:\WINDOWS\Tasks\Adobe Flash Player Updater.job
O39 - APT:Automatic Planified Task - C:\WINDOWS\Tasks\AppleSoftwareUpdate.job
O39 - APT:Automatic Planified Task - C:\WINDOWS\Tasks\avast! Emergency Update.job
O39 - APT:Automatic Planified Task - C:\WINDOWS\Tasks\GoogleUpdateTaskMachineCore.job
O39 - APT:Automatic Planified Task - C:\WINDOWS\Tasks\GoogleUpdateTaskMachineUA.job
O39 - APT:Automatic Planified Task - C:\WINDOWS\Tasks\GoogleUpdateTaskUserS-1-5-21-2851534266-985727058-2256982857-1004Core.job
O39 - APT:Automatic Planified Task - C:\WINDOWS\Tasks\GoogleUpdateTaskUserS-1-5-21-2851534266-985727058-2256982857-1004UA.job
O39 - APT:Automatic Planified Task - C:\WINDOWS\Tasks\User_Feed_Synchronization-{1EA88599-23D3-4401-8DA6-0720497452A8}.job
~ Scan Scheduled Task in 00mn 00s

---\\ Composants installés (ActiveSetup Installed Components) (O40)
O40 - ASIC: Mise à jour de la version d’Internet Explorer - <{12d0ed0d-0ee0-4f90-8827-78cefb8f4988} . (.Microsoft Corporation - IE Per User Active Setup Uninstall Utility.) -- C:\WINDOWS\system32\ieudinit.exe
O40 - ASIC: Microsoft Windows Media Player - >{22d6f312-b0f6-11d0-94ab-0080c74c7e95} . (.Microsoft Corporation - Utilitaire d'installation du Lecteur Windows Media de Microsoft.) -- C:\WINDOWS\inf\unregmp2.exe
O40 - ASIC: Internet Explorer - >{26923b43-4d38-484f-9b9e-de460746276c} . (.Microsoft Corporation - Utilitaire d’initialisation d’Internet Explorer par utilisateur.) -- C:\WINDOWS\system32\ie4uinit.exe.mui
O40 - ASIC: Browser Customizations - >{60B49E34-C7CC-11D0-8953-00A0C90347FF} . (.Microsoft Corporation - IEAK branding.) -- C:\WINDOWS\system32\iedkcs32.dll
O40 - ASIC: Outlook Express - >{881dd1c5-3dcf-431b-b061-f3f88e8be88a} . (.Microsoft Corporation - Windows NT User Data Migration Tool.) -- C:\WINDOWS\system32\shmgrate.exe
O40 - ASIC: Java (Sun) - {08B0E5C0-4FCB-11CF-AAA5-00401C608500} . (.Sun Microsystems,

Inc. - Java(TM) Platform SE binary.) -- C:\Program Files\Java\jre6\bin\regutils.dll
O40 - ASIC: Microsoft NetShow Player - {2179C5D3-EBFF-11CF-B6FD-00AA00B4E220} . (.Microsoft Corporation - Windows Media Player Extension.) -- C:\WINDOWS\system32\wmpdxm.dll
O40 - ASIC: Microsoft Windows Media Player 6.4 - {22d6f312-b0f6-11d0-94ab-0080c74c7e95} . (.Microsoft Corporation - Windows Media Player Extension.) -- C:\WINDOWS\system32\wmpdxm.dll
O40 - ASIC: Themes Setup - {2C7339CF-2B09-4501-B3F3-F3508C9228ED} . (.Microsoft Corporation - API Windows Theme.) -- C:\WINDOWS\system32\themeui.dll
O40 - ASIC: Microsoft Outlook Express 6 - {44BBA840-CC51-11CF-AAFA-00AA00B6015C} . (.Microsoft Corporation - Bibliothèque d'installation Outlook Express.) -- C:\Program Files\Outlook Express\setup50.exe
O40 - ASIC: NetMeeting 3.01 - {44BBA842-CC51-11CF-AAFA-00AA00B6015B} . (...) -- C:\WINDOWS\INF\msnetmtg.inf
O40 - ASIC: Windows Messenger 4.7 - {5945c046-1e7d-11d1-bc44-00c04fd912be} . (...) -- C:\WINDOWS\INF\msmsgs.inf
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} . (...) -- C:\WINDOWS\INF\wmp11.inf
O40 - ASIC: Carnet d'adresses 6 - {7790769C-0471-11d2-AF11-00C04FA35D02} . (.Microsoft Corporation - Bibliothèque d'installation Outlook Express.) -- C:\Program Files\Outlook Express\setup50.exe
O40 - ASIC: Mise à jour du Bureau Windows - {89820200-ECBD-11cf-8B85-00AA005B4340} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\WINDOWS\system32\shell32.dll
O40 - ASIC: Internet Explorer - {89820200-ECBD-11cf-8B85-00AA005B4383} . (.Microsoft Corporation - Utilitaire d’initialisation d’Internet Explorer par utilisateur.) -- C:\WINDOWS\system32\ie4uinit.exe.mui
O40 - ASIC: (no name) - {89B4C1CD-B018-4511-B0A1-5476DBF70820} . (.Microsoft Corporation - Microsoft .NET IE SECURITY REGISTRATION.) -- c:\WINDOWS\system32\mscories.dll
O40 - ASIC: Shockwave Flash - {D27CDB6E-AE6D-11cf-96B8-444553540000} . (.Adobe Systems, Inc. - Adobe Flash Player 11.4 r402.) -- C:\WINDOWS\system32\Macromed\Flash\Flash32_11_4_402_278.ocx
O40 - ASIC: Installed Component - S-1-5-21-2851534266-985727058-2256982857-1004 - <{12d0ed0d-0ee0-4f90-8827-78cefb8f4988} -- Not Hexadécimal CLSID
O40 - ASIC: Installed Component - S-1-5-21-2851534266-985727058-2256982857-1004 - >{60B49E34-C7CC-11D0-8953-00A0C90347FF}MICROS -- Not Hexadécimal CLSID
~ Scan Active Setup in 00mn 00s

---\\ Pilotes lancés au démarrage (O41)
O41 - Driver: (AFD) . (.Microsoft Corporation - Ancillary Function Driver for WinSock.) - C:\WINDOWS\system32\drivers\afd.sys
O41 - Driver: (Cdrom) . (.Microsoft Corporation - SCSI CD-ROM Driver.) - C:\WINDOWS\system32\DRIVERS\cdrom.sys
O41 - Driver: (i8042prt) . (.Microsoft Corporation - Pilote de port i8042.) - C:\WINDOWS\system32\DRIVERS\i8042prt.sys
O41 - Driver: (Imapi) . (.Microsoft Corporation - IMAPI Kernel Driver.) -

C:\WINDOWS\system32\DRIVERS\imapi.sys
O41 - Driver: (intelppm) . (.Microsoft Corporation - Pilote de périphérique processeur.) - C:\WINDOWS\system32\DRIVERS\intelppm.sys
O41 - Driver: (IPSec) . (.Microsoft Corporation - IPSec Driver.) - C:\WINDOWS\system32\DRIVERS\ipsec.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 souris 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: (MRxSmb) . (.Microsoft Corporation - Windows NT SMB Minirdr.) - C:\WINDOWS\system32\DRIVERS\mrxsmb.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: (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: (redbook) . (.Microsoft Corporation - Pilote de filtre audio Livre rouge.) - C:\WINDOWS\system32\DRIVERS\redbook.sys
O41 - Driver: (Serial) . (.Microsoft Corporation - Pilote de périphérique série.) - C:\WINDOWS\system32\DRIVERS\serial.sys
O41 - Driver: (Tcpip) . (.Microsoft Corporation - TCP/IP Protocol Driver.) - C:\WINDOWS\system32\DRIVERS\tcpip.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
~ Scan Drivers in 00mn 00s

---\\ Logiciels installés (O42)
O42 - Logiciel: 802.11 USB Wireless LAN Adapter - (.Pas de propriétaire.) [HKLM] -- sis163u
O42 - Logiciel: ABBYY FineReader 6.0 Sprint - (.ABBYY Software House.) [HKLM] -- {ACF60000-22B9-4CE9-98D6-2CCF359BAC07}
O42 - Logiciel: Adobe AIR - (.Adobe Systems Incorporated.) [HKLM] -- Adobe AIR
O42 - Logiciel: Adobe AIR - (.Adobe Systems Incorporated.) [HKLM] -- {65CB4C08-C47B-4A7E-A6A4-50C06ADA5FC6}
O42 - Logiciel: Adobe Flash Player 11 ActiveX - (.Adobe Systems Incorporated.) [HKLM] -- Adobe Flash Player ActiveX
O42 - Logiciel: Adobe Reader X (10.1.4) - Français - (.Adobe Systems Incorporated.) [HKLM] -- {AC76BA86-7AD7-1036-7B44-AA1000000001}
O42 - Logiciel: Apple Application Support - (.Apple Inc..) [HKLM] -- {EB879750-CCBD-4013-BFD5-0294D4DA5BD0}
O42 - Logiciel: Apple Software Update - (.Apple Inc..) [HKLM] -- {789A5B64-9DD9-4BA5-915A-F0FC0A1B7BFE}

O42 - Logiciel: CCleaner - (.Piriform.) [HKLM] -- CCleaner
O42 - Logiciel: Complitly - (.Complitly.) [HKLM] -- {4FFBB818-B13C-11E0-931D-B2664824019B}_is1
O42 - Logiciel: Corel WinDVD 2010 - (.Corel Inc..) [HKLM] -- {5C1F18D2-F6B7-4242-B803-B5A78648185D}
O42 - Logiciel: DVD Decoder Pak for Windows XP - (.roddy2000@hotbox.ru.) [HKLM] -- {92C5DB3D-9D6F-4324-BB11-57825F4C2635}
O42 - Logiciel: FreeMind - (.Pas de propriétaire.) [HKLM] -- B991B020-2968-11D8-AF23-444553540000_is1
O42 - Logiciel: Funmoods Web Search - (.Pas de propriétaire.) [HKCU] -- Funmoods Web Search
O42 - Logiciel: Google Chrome - (.Google Inc..) [HKCU] -- Google Chrome
O42 - Logiciel: Google Update Helper - (.Google Inc..) [HKLM] -- {A92DAB39-4E2C-4304-9AB6-BC44E68B55E2}
O42 - Logiciel: Hotfix for Microsoft .NET Framework 3.5 SP1 (KB953595) - (.Microsoft Corporation.) [HKLM] -- {CE2CDD62-0124-36CA-84D3-9F4DCF5C5BD9}.KB953595
O42 - Logiciel: Hotfix for Microsoft .NET Framework 3.5 SP1 (KB958484) - (.Microsoft Corporation.) [HKLM] -- {CE2CDD62-0124-36CA-84D3-9F4DCF5C5BD9}.KB958484
O42 - Logiciel: Hotfix for Windows Media Format 11 SDK (KB929399) - (.Microsoft Corporation.) [HKLM] -- KB929399
O42 - Logiciel: Hotfix for Windows XP (KB954550-v5) - (.Microsoft Corporation.) [HKLM] -- KB954550-v5
O42 - Logiciel: Hotfix for Windows XP (KB976002-v5) - (.Microsoft Corporation.) [HKLM] -- KB976002-v5
O42 - Logiciel: Intel(R) Graphics Media Accelerator Driver - (.Pas de propriétaire.) [HKLM] -- HDMI
O42 - Logiciel: Intel(R) Graphics Media Accelerator Driver - (.Pas de propriétaire.) [HKLM] -- {8A708DD8-A5E6-11D4-A706-000629E95E20}
O42 - Logiciel: Java(TM) 6 Update 33 - (.Oracle.) [HKLM] -- {26A24AE4-039D-4CA4-87B4-2F83216033FF}
O42 - Logiciel: Lecteur Windows Media 11 - (.Pas de propriétaire.) [HKLM] -- Windows Media Player
O42 - Logiciel: Lexmark 5400 Series - (.Lexmark International, Inc..) [HKLM] -- Lexmark 5400 Series
O42 - Logiciel: Lexmark Barre d'outils - (.Pas de propriétaire.) [HKLM] -- {1017A80C-6F09-4548-A84D-EDD6AC9525F0}
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: McAfee Security Scan Plus - (.McAfee, Inc..) [HKLM] -- McAfee Security Scan
O42 - Logiciel: Microsoft .NET Framework 2.0 Client Service Pack 2 - Language Pack (FRA) - (.Microsoft.) [HKLM] -- {30F71986-F2F2-33C8-89AA-99E566B04FD2}
O42 - Logiciel: Microsoft .NET Framework 2.0 Service Pack 2 - (.Microsoft Corporation.) [HKLM] -- {C09FB3CD-3D0C-3F2D-899A-6A1D67F2073F}
O42 - Logiciel: Microsoft .NET Framework 3.0 Client Profile - Language Pack (FRA) - (.Microsoft Corporation.) [HKLM] -- {0089CA27-3E85-3E64-9814-A7B1A1756CE3}
O42 - Logiciel: Microsoft .NET Framework 3.0 Service Pack 2 - (.Microsoft Corporation.) [HKLM] -- {A3051CD0-2F64-3813-A88D-B8DCCDE8F8C7}
O42 - Logiciel: Microsoft .NET Framework 3.5 Client Profile - Language Pack (FRA) - (.Microsoft Corporation.) [HKLM] -- {25EDB0C9-A32C-35AB-9AA3-6D74BBE16813}
O42 - Logiciel: Microsoft .NET Framework 3.5 SP1 - (.Microsoft Corporation.) [HKLM] -- Microsoft .NET Framework 3.5 SP1

O42 - Logiciel: Microsoft .NET Framework 3.5 SP1 - (.Microsoft Corporation.) [HKLM] -- {CE2CDD62-0124-36CA-84D3-9F4DCF5C5BD9}
O42 - Logiciel: Microsoft .NET Framework Client Profile - (.Pas de propriétaire.) [HKLM] -- Microsoft.Net.Client.3.5
O42 - Logiciel: Microsoft Compression Client Pack 1.0 for Windows XP - (.Microsoft Corporation.) [HKLM] -- MSCompPackV1
O42 - Logiciel: Microsoft Silverlight - (.Microsoft Corporation.) [HKLM] -- {89F4137D-6C26-4A84-BDB8-2E5A4BB71E00}
O42 - Logiciel: Microsoft User-Mode Driver Framework Feature Pack 1.0 - (.Microsoft Corporation.) [HKLM] -- Wudf01000
O42 - Logiciel: Microsoft Visual C++ 2005 ATL Update kb973923 - x86 8.0.50727.4053 - (.Microsoft Corporation.) [HKLM] -- {770657D0-A123-3C07-8E44-1C83EC895118}
O42 - Logiciel: Microsoft Visual C++ 2005 Redistributable - (.Microsoft Corporation.) [HKLM] -- {710f4c1c-cc18-4c49-8cbf-51240c89a1a2}
O42 - Logiciel: Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 - (.Microsoft Corporation.) [HKLM] -- {1F1C2DFC-2D24-3E06-BCB8-725134ADF989}
O42 - Logiciel: Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 - (.Microsoft Corporation.) [HKLM] -- {9BE518E6-ECC6-35A9-88E4-87755C07200F}
O42 - Logiciel: Module linguistique Microsoft .NET Framework Client Profile - FRA - (.Pas de propriétaire.) [HKLM] -- Microsoft.Net.Client.3.5.LangPack.fra
O42 - Logiciel: Notepad++ - (.Pas de propriétaire.) [HKLM] -- Notepad++
O42 - Logiciel: OpenOffice.org 3.2 - (.OpenOffice.org.) [HKLM] -- {266517E6-D866-439D-919C-B8B1A52E6080}
O42 - Logiciel: QuickTime - (.Apple Inc..) [HKLM] -- {0E64B098-8018-4256-BA23-C316A43AD9B0}
O42 - Logiciel: REALTEK Wireless LAN Driver and Utility - (.REALTEK Semiconductor Corp..) [HKLM] -- {9C049499-055C-4a0c-A916-1D8CA1FF45EB}
O42 - Logiciel: SFR - Kit de connexion - (.SFR.) [HKLM] -- SFR_Kit
O42 - Logiciel: Security Update for Microsoft .NET Framework 3.5 SP1 (KB2604111) - (.Microsoft Corporation.) [HKLM] -- {CE2CDD62-0124-36CA-84D3-9F4DCF5C5BD9}.KB2604111
O42 - Logiciel: Security Update for Microsoft .NET Framework 3.5 SP1 (KB2657424) - (.Microsoft Corporation.) [HKLM] -- {CE2CDD62-0124-36CA-84D3-9F4DCF5C5BD9}.KB2657424
O42 - Logiciel: Serif DrawPlus X2 - (.Serif (Europe) Ltd.) [HKLM] -- {4D9DD45B-E79A-4F04-898E-B2C3769AB729}
O42 - Logiciel: Serif DrawPlus X2 Ressources - (.Serif (Europe) Ltd.) [HKLM] -- {946383CC-B47D-4817-A4D9-03F4E76A9003}
O42 - Logiciel: SoundMAX - (.Analog Devices.) [HKLM] -- {F0A37341-D692-11D4-A984-009027EC0A9C}
O42 - Logiciel: Squeeze Page Pro - (.Pas de propriétaire.) [HKLM] -- Squeeze Page Pro_is1
O42 - Logiciel: SweetIM for Messenger 3.6 - (.SweetIM Technologies Ltd..) [HKLM] -- {B85C4CB2-B352-4BD8-818C-BCE353599107}
O42 - Logiciel: SweetPacks Toolbar for Internet Explorer 4.4 - (.SweetIM Technologies Ltd..) [HKLM] -- {2F603A45-D956-496B-81B5-50D782424976}
O42 - Logiciel: Update for Microsoft .NET Framework 3.5 SP1 (KB963707) - (.Microsoft Corporation.) [HKLM] -- {CE2CDD62-0124-36CA-84D3-9F4DCF5C5BD9}.KB963707
O42 - Logiciel: WampServer 2.2 - (.Hervé Leclerc (HeL).) [HKLM] -- WampServer 2_is1
O42 - Logiciel: Web Assistant 2.0.0.478 - (.IncrediBar.) [HKLM] -- {336D0C35-8A85-403a-B9D2-65C292C39087}_is1
O42 - Logiciel: Web Optimizer - (.Pas de propriétaire.) [HKLM] -- WNLT
O42 - Logiciel: Windows Genuine Advantage Validation Tool (KB892130) - (.Microsoft

Corporation.) [HKLM] -- KB892130
O42 - Logiciel: Windows Internet Explorer 8 - (.Microsoft Corporation.) [HKLM] -- ie8
O42 - Logiciel: Windows Media Format 11 runtime - (.Microsoft Corporation.) [HKLM] -- WMFDist11
O42 - Logiciel: Windows Media Format 11 runtime - (.Pas de propriétaire.) [HKLM] -- Windows Media Format Runtime
O42 - Logiciel: Windows Media Player 11 - (.Microsoft Corporation.) [HKLM] -- wmp11
O42 - Logiciel: Wireless LAN Utility - (.Pas de propriétaire.) [HKLM] -- Wireless LAN Utility
O42 - Logiciel: avast! Free Antivirus v7.0.1466.0 - (.AVAST Software.) [HKLM] -- avast

---\\ HKCU & HKLM Software Keys
[HKCU\Software\ABBYY]
[HKCU\Software\ALWIL Software]
[HKCU\Software\AVAST Software]
[HKCU\Software\Adobe]
[HKCU\Software\AlterGeo]
[HKCU\Software\Analog Devices]
[HKCU\Software\AppDataLow\Software\Microsoft]
[HKCU\Software\AppDataLow\Software]
[HKCU\Software\AppDataLow]
[HKCU\Software\Apple Computer, Inc.]
[HKCU\Software\Apple Inc.]
[HKCU\Software\Badoo]
[HKCU\Software\BrowserTemp]
[HKCU\Software\Citrix]
[HKCU\Software\Classes]
[HKCU\Software\Clients]
[HKCU\Software\Complitly]
[HKCU\Software\Corel]
[HKCU\Software\Evoclic]
[HKCU\Software\Google]
[HKCU\Software\IM]
[HKCU\Software\ImInstaller]
[HKCU\Software\IncrediMail]
[HKCU\Software\Intel]
[HKCU\Software\JavaSoft]
[HKCU\Software\Lexmark 5400 Series]
[HKCU\Software\LexmarkPhoto]
[HKCU\Software\Lexmark]
[HKCU\Software\Local AppWizard-Generated Applications]
[HKCU\Software\MAP-DN]
[HKCU\Software\Macromedia]
[HKCU\Software\MozillaPlugins]
[HKCU\Software\Netscape]
[HKCU\Software\OfferBox]
[HKCU\Software\PC SOFT]
[HKCU\Software\Piriform]
[HKCU\Software\Policies]
[HKCU\Software\RegisteredApplications]
[HKCU\Software\Serif]
[HKCU\Software\SiS]
[HKCU\Software\SweetIM]

[HKCU\Software\SysInternals]
[HKCU\Software\Trolltech]
[HKCU\Software\VidSoft]
[HKCU\Software\WNLT]
[HKCU\Software\Web Assistant]
[HKCU\Software\WhiteKnightProtector]
[HKCU\Software\WinRAR SFX]
[HKCU\Software\Wow6432Node]
[HKCU\Software\freeTVRadio]
[HKCU\Software\monAlbumPhoto]
[HKLM\Software\ABBYY]
[HKLM\Software\ALWIL Software]
[HKLM\Software\AVAST Software]
[HKLM\Software\Adobe]
[HKLM\Software\AedgePerformanceBCN]
[HKLM\Software\Analog Devices]
[HKLM\Software\Apple Computer, Inc.]
[HKLM\Software\Apple Inc.]
[HKLM\Software\Babylon]
[HKLM\Software\BrowserChoice]
[HKLM\Software\C07ft5Y]
[HKLM\Software\Citrix]
[HKLM\Software\Classes]
[HKLM\Software\Clients]
[HKLM\Software\Conduit]
[HKLM\Software\Corel]
[HKLM\Software\Dofus2]
[HKLM\Software\FaxMan5400SeriesPorts]
[HKLM\Software\Gemplus]
[HKLM\Software\Global IP Solutions]
[HKLM\Software\Google]
[HKLM\Software\INTEL]
[HKLM\Software\IncrediMail]
[HKLM\Software\InstalledOptions]
[HKLM\Software\JavaSoft]
[HKLM\Software\JreMetrics]
[HKLM\Software\LexmarkInkjet]
[HKLM\Software\Lexmark]
[HKLM\Software\MAP-DN]
[HKLM\Software\MDC]
[HKLM\Software\Macromedia]
[HKLM\Software\McAfee.com]
[HKLM\Software\MozillaPlugins]
[HKLM\Software\Mozilla]
[HKLM\Software\Neuf]
[HKLM\Software\ODBC]
[HKLM\Software\OEM]
[HKLM\Software\OfferBox]
[HKLM\Software\OpenOffice.org]
[HKLM\Software\Piriform]
[HKLM\Software\Policies]
[HKLM\Software\Program Groups]

[HKLM\Software\REALTEK Semiconductor Corp.]
[HKLM\Software\Realtek]
[HKLM\Software\RegisteredApplications]
[HKLM\Software\RtWLan]
[HKLM\Software\Schlumberger]
[HKLM\Software\Secure]
[HKLM\Software\Sensaura]
[HKLM\Software\Serif]
[HKLM\Software\Set8188SU]
[HKLM\Software\Set8191SU]
[HKLM\Software\Set8192GU]
[HKLM\Software\Set8192SU]
[HKLM\Software\Set8712]
[HKLM\Software\SiS]
[HKLM\Software\SimplyGen]
[HKLM\Software\Staccato]
[HKLM\Software\Sun Microsystems]
[HKLM\Software\SweetIM]
[HKLM\Software\Techcity]
[HKLM\Software\Web Assistant]
[HKLM\Software\WebSupergoo]
[HKLM\Software\Windows 3.1 Migration Status]
[HKLM\Software\Windows]
[HKLM\Software\Wow6432Node]
[HKLM\Software\mcafeeupdater]
~ Scan Softwares in 00mn 00s

---\\ Contenu des dossiers Programs/ProgramFiles/ProgramData/AppData (O43)
O43 - CFD: 24/05/2012 - 12:18:11 - [115,559] ----D C:\Program Files\Abbyy FineReader 6.0 Sprint
O43 - CFD: 26/10/2011 - 19:59:11 - [113,274] ----D C:\Program Files\Adobe
O43 - CFD: 16/12/2010 - 11:39:27 - [255,714] ----D C:\Program Files\Alwil Software
O43 - CFD: 16/12/2010 - 11:37:12 - [2,493] ----D C:\Program Files\Analog Devices
O43 - CFD: 26/11/2011 - 07:51:22 - [2,316] ----D C:\Program Files\Apple Software Update
O43 - CFD: 06/10/2011 - 19:24:21 - [3,981] ----D C:\Program Files\CCleaner
O43 - CFD: 10/06/2012 - 12:11:54 - [0] ----D C:\Program Files\Citrix
O43 - CFD: 02/03/2012 - 23:37:04 - [1,597] ----D C:\Program Files\Complitly
O43 - CFD: 28/04/2010 - 13:58:11 - [0] ----D C:\Program Files\ComPlus Applications
O43 - CFD: 16/12/2010 - 11:42:42 - [230,619] ----D C:\Program Files\Corel
O43 - CFD: 21/08/2012 - 13:45:43 - [127,702] ----D C:\Program Files\Fichiers communs
O43 - CFD: 02/11/2011 - 18:41:04 - [16,071] ----D C:\Program Files\FreeMind
O43 - CFD: 10/06/2012 - 12:52:04 - [0,352] ----D C:\Program Files\freeTVRadio
O43 - CFD: 27/06/2012 - 20:40:15 - [2,012] ----D C:\Program Files\Funmoods
O43 - CFD: 16/12/2010 - 11:39:48 - [6,024] ----D C:\Program Files\Google
O43 - CFD: 18/02/2005 - 04:38:55 - [25,750] --H-D C:\Program Files\InstallShield Installation Information
O43 - CFD: 23/09/2012 - 02:00:03 - [5,729] ----D C:\Program Files\Internet Explorer
O43 - CFD: 23/10/2011 - 12:54:22 - [78,424] ----D C:\Program Files\Java
O43 - CFD: 16/12/2010 - 11:50:02 - [15,541] ----D C:\Program Files\JRE
O43 - CFD: 24/05/2012 - 12:23:40 - [105,847] ----D C:\Program Files\Lexmark 5400 Series
O43 - CFD: 24/05/2012 - 12:24:55 - [0,337] ----D C:\Program Files\Lexmark Toolbar

O43 - CFD: 04/10/2012 - 01:18:19 - [0,021] ----D C:\Program Files\Lx_cats
O43 - CFD: 10/12/2011 - 21:33:04 - [9,481] ----D C:\Program Files\McAfee Security Scan
O43 - CFD: 24/06/2011 - 15:59:41 - [2,073] ----D C:\Program Files\Messenger
O43 - CFD: 28/04/2010 - 14:02:44 - [0] ----D C:\Program Files\microsoft frontpage
O43 - CFD: 12/05/2012 - 10:31:38 - [40,838] ----D C:\Program Files\Microsoft Silverlight
O43 - CFD: 24/06/2011 - 15:37:35 - [9,894] ----D C:\Program Files\Movie Maker
O43 - CFD: 27/06/2012 - 20:27:38 - [0,000] ----D C:\Program Files\Mozilla Firefox
O43 - CFD: 09/11/2011 - 13:37:24 - [0,025] ----D C:\Program Files\MSBuild
O43 - CFD: 28/04/2010 - 13:56:10 - [18,385] ----D C:\Program Files\MSN
O43 - CFD: 28/04/2010 - 13:57:17 - [8,341] ----D C:\Program Files\MSN Gaming Zone
O43 - CFD: 24/06/2011 - 15:37:08 - [0] ----D C:\Program Files\MSXML 4.0
O43 - CFD: 28/04/2010 - 13:59:54 - [3,133] ----D C:\Program Files\NetMeeting
O43 - CFD: 20/04/2012 - 21:26:21 - [11,196] ----D C:\Program Files\Notepad++
O43 - CFD: 28/04/2010 - 13:57:28 - [0,002] ----D C:\Program Files\Online Services
O43 - CFD: 16/12/2010 - 11:50:01 - [368,596] ----D C:\Program Files\OpenOffice.org 3
O43 - CFD: 24/06/2011 - 15:36:26 - [4,176] ----D C:\Program Files\Outlook Express
O43 - CFD: 17/05/2012 - 22:34:45 - [72,431] ----D C:\Program Files\QuickTime
O43 - CFD: 18/02/2005 - 04:38:59 - [5,270] ----D C:\Program Files\REALTEK
O43 - CFD: 06/11/2011 - 21:06:00 - [35,390] ----D C:\Program Files\Reference Assemblies
O43 - CFD: 23/10/2011 - 12:24:15 - [533,225] ----D C:\Program Files\Serif
O43 - CFD: 28/04/2010 - 14:00:51 - [0,001] ----D C:\Program Files\Services en ligne
O43 - CFD: 20/02/2012 - 23:08:41 - [17,874] ----D C:\Program Files\SFR
O43 - CFD: 14/05/2010 - 10:02:56 - [0,288] ----D C:\Program Files\SiSWLAN
O43 - CFD: 28/05/2012 - 18:51:42 - [4,436] ----D C:\Program Files\Squeeze Page Pro
O43 - CFD: 18/03/2012 - 23:02:11 - [8,487] ----D C:\Program Files\SweetIM
O43 - CFD: 15/02/2005 - 02:50:03 - [0] ----D C:\Program Files\Techcity
O43 - CFD: 02/03/2012 - 23:40:22 - [2,121] ---AD C:\Program Files\TelevisionFanaticEI
O43 - CFD: 28/04/2010 - 14:17:06 - [0] --H-D C:\Program Files\Uninstall Information
O43 - CFD: 18/03/2012 - 23:02:18 - [0] ----D C:\Program Files\Video Codec
O43 - CFD: 29/08/2012 - 07:22:14 - [1,929] ----D C:\Program Files\Web Assistant
O43 - CFD: 15/09/2012 - 11:22:42 - [3,415] ----D C:\Program Files\Windows Media Connect 2
O43 - CFD: 15/09/2012 - 11:23:05 - [7,956] ----D C:\Program Files\Windows Media Player
O43 - CFD: 28/04/2010 - 13:56:51 - [3,760] ----D C:\Program Files\Windows NT
O43 - CFD: 28/04/2010 - 14:00:55 - [0] --H-D C:\Program Files\WindowsUpdate
O43 - CFD: 14/05/2010 - 10:03:05 - [3,106] ----D C:\Program Files\Wireless LAN Utility
O43 - CFD: 28/04/2010 - 14:02:44 - [0] ----D C:\Program Files\xerox
O43 - CFD: 04/10/2012 - 03:04:51 - [10,014] ----D C:\Program Files\ZHPDiag
O43 - CFD: 26/10/2011 - 19:59:19 - [3,661] ----D C:\Program Files\Fichiers communs\Adobe
O43 - CFD: 21/08/2012 - 13:45:43 - [39,326] ----D C:\Program Files\Fichiers communs\Adobe AIR
O43 - CFD: 16/12/2010 - 11:46:56 - [60,278] ----D C:\Program Files\Fichiers communs\Apple
O43 - CFD: 14/05/2010 - 10:02:46 - [2,106] ----D C:\Program Files\Fichiers communs\InstallShield
O43 - CFD: 01/04/2012 - 17:56:08 - [1,201] ----D C:\Program Files\Fichiers communs\Java
O43 - CFD: 06/11/2011 - 21:04:20 - [8,521] ----D C:\Program Files\Fichiers communs\Microsoft Shared
O43 - CFD: 28/04/2010 - 13:59:46 - [0,893] ----D C:\Program Files\Fichiers communs\MSSoap
O43 - CFD: 28/04/2010 - 15:50:55 - [0] ----D C:\Program Files\Fichiers communs\ODBC
O43 - CFD: 16/12/2010 - 11:43:13 - [1,600] ----D C:\Program Files\Fichiers communs\Protexis
O43 - CFD: 28/04/2010 - 13:59:53 - [0,008] ----D C:\Program Files\Fichiers communs\Services
O43 - CFD: 28/04/2010 - 15:50:51 - [3,612] ----D C:\Program Files\Fichiers communs\SpeechEngines
O43 - CFD: 28/04/2010 - 13:58:42 - [6,496] ----D C:\Program Files\Fichiers communs\System
O43 - CFD: 03/10/2012 - 23:08:39 - [425,647] R-H-D C:\Documents and Settings\All

Users\Application Data
O43 - CFD: 04/10/2012 - 02:44:13 - [0,006] ----D C:\Documents and Settings\All Users\Bureau
O43 - CFD: 18/02/2005 - 11:26:54 - [1,660] R---D C:\Documents and Settings\All Users\Documents
O43 - CFD: 15/09/2012 - 11:21:38 - [0,146] -SH-D C:\Documents and Settings\All Users\DRM
O43 - CFD: 28/04/2010 - 15:50:10 - [0] ----D C:\Documents and Settings\All Users\Favoris
O43 - CFD: 29/10/2011 - 21:59:59 - [0,121] R---D C:\Documents and Settings\All Users\Menu Démarrer
O43 - CFD: 16/12/2010 - 11:50:44 - [0,030] --H-D C:\Documents and Settings\All Users\Modèles
O43 - CFD: 24/05/2012 - 12:20:42 - [0,042] ----D C:\Documents and Settings\user\Application Data\5400 Series
O43 - CFD: 21/08/2012 - 13:45:46 - [14,919] ----D C:\Documents and Settings\user\Application Data\Adobe
O43 - CFD: 21/08/2012 - 14:03:16 - [0,004] ----D C:\Documents and Settings\user\Application Data\app
O43 - CFD: 26/11/2011 - 20:22:16 - [0,019] ----D C:\Documents and Settings\user\Application Data\Apple Computer
O43 - CFD: 29/10/2011 - 21:54:29 - [0,024] ----D C:\Documents and Settings\user\Application Data\Babylon
O43 - CFD: 02/03/2012 - 23:37:03 - [0,467] ----D C:\Documents and Settings\user\Application Data\Complitly
O43 - CFD: 15/02/2005 - 18:27:37 - [0,000] ----D C:\Documents and Settings\user\Application Data\Corel
O43 - CFD: 21/08/2012 - 14:03:11 - [0] ----D C:\Documents and Settings\user\Application Data\Dofus-2.C9ECCBDBA4E09304DEEFB106465BC17F6D6749B9.1
O43 - CFD: 21/08/2012 - 14:33:18 - [0,405] ----D C:\Documents and Settings\user\Application Data\Dofus2
O43 - CFD: 10/06/2012 - 12:42:38 - [0,001] ----D C:\Documents and Settings\user\Application Data\freeTVRadio
O43 - CFD: 28/04/2010 - 14:17:08 - [0] ----D C:\Documents and Settings\user\Application Data\Identities
O43 - CFD: 21/03/2012 - 21:24:29 - [0] ----D C:\Documents and Settings\user\Application Data\kujytuo
O43 - CFD: 15/02/2005 - 02:46:10 - [0,076] ----D C:\Documents and Settings\user\Application Data\Macromedia
O43 - CFD: 02/10/2012 - 21:04:05 - [12,391] -S--D C:\Documents and Settings\user\Application Data\Microsoft
O43 - CFD: 20/04/2012 - 21:27:16 - [0,397] ----D C:\Documents and Settings\user\Application Data\Notepad++
O43 - CFD: 11/06/2012 - 09:48:42 - [0,342] ----D C:\Documents and Settings\user\Application Data\OfferBox
O43 - CFD: 15/02/2005 - 18:24:46 - [4,735] ----D C:\Documents and Settings\user\Application Data\OpenOffice.org
O43 - CFD: 21/08/2012 - 14:03:16 - [0] ----D C:\Documents and Settings\user\Application Data\Reg.C9ECCBDBA4E09304DEEFB106465BC17F6D6749B9.1
O43 - CFD: 23/10/2011 - 12:58:36 - [4,575] ----D C:\Documents and Settings\user\Application Data\Serif
O43 - CFD: 21/02/2005 - 05:27:49 - [1,053] ----D C:\Documents and Settings\user\Application Data\Sun
O43 - CFD: 21/08/2012 - 13:45:39 - [14,561] ----D C:\Documents and Settings\user\Local Settings\Application Data\Adobe
O43 - CFD: 26/11/2011 - 07:51:17 - [0] ----D C:\Documents and Settings\user\Local

Settings\Application Data\Apple
O43 - CFD: 15/02/2005 - 18:36:40 - [0,010] ----D C:\Documents and Settings\user\Local Settings\Application Data\Apple Computer
O43 - CFD: 29/10/2011 - 21:55:10 - [0,028] ----D C:\Documents and Settings\user\Local Settings\Application Data\Ares
O43 - CFD: 10/06/2012 - 12:51:12 - [0,247] ----D C:\Documents and Settings\user\Local Settings\Application Data\freetvradio Air
O43 - CFD: 28/06/2012 - 07:05:02 - [1250,400] ----D C:\Documents and Settings\user\Local Settings\Application Data\Google
O43 - CFD: 15/02/2005 - 18:30:34 - [0,289] ----D C:\Documents and Settings\user\Local Settings\Application Data\Identities
O43 - CFD: 17/09/2012 - 21:28:41 - [3,830] ----D C:\Documents and Settings\user\Local Settings\Application Data\Microsoft
O43 - CFD: 25/04/2012 - 19:41:00 - [0,000] ----D C:\Documents and Settings\user\Local Settings\Application Data\rencontreshard
O43 - CFD: 26/10/2011 - 20:00:10 - [0] ----D C:\Documents and Settings\user\Local Settings\Application Data\Temp
O43 - CFD: 23/11/2011 - 16:54:34 - [0] ----D C:\Documents and Settings\user\Local Settings\Application Data\WDSetup
O43 - CFD: 18/02/2005 - 11:27:11 - [0] ----D C:\Documents and Settings\user\Local Settings\Application Data\WMTools Downloaded Files
O43 - CFD: 15/02/2005 - 02:32:36 - [0,015] R---D C:\Documents and Settings\user\Menu Démarrer\Programmes\Accessoires
O43 - CFD: 15/02/2005 - 18:25:48 - [0,001] R---D C:\Documents and Settings\user\Menu Démarrer\Programmes\Démarrage
O43 - CFD: 28/06/2012 - 07:05:39 - [0,004] ----D C:\Documents and Settings\user\Menu Démarrer\Programmes\Google Chrome
O43 - CFD: 20/04/2012 - 21:26:18 - [0] ----D C:\Documents and Settings\user\Menu Démarrer\Programmes\Notepad++
~ Scan Program Folder in 00mn 03s

---\\ Derniers fichiers modifiés ou crées sous Windows et System32 (O44)
O44 - LFC:[MD5.20689D3C5B2132C10E07692971A3C662] - 04/10/2012 - 01:22:42 ---A- . (...) -- C:\WINDOWS\WindowsUpdate.log [1355857]
O44 - LFC:[MD5.D41D8CD98F00B204E9800998ECF8427E] - 03/10/2012 - 22:29:00 ---A- . (...) -- C:\WINDOWS\0.log [0]
O44 - LFC:[MD5.6E7899BCB8C143C13198160BE4BB3A68] - 03/10/2012 - 22:28:46 ---A- . (...) -- C:\WINDOWS\wiadebug.log [159]
O44 - LFC:[MD5.3ADBC22F08573FD6DFAA29F4AF342978] - 03/10/2012 - 22:28:42 ---A- . (...) -- C:\WINDOWS\wiaservc.log [50]
O44 - LFC:[MD5.6A2CB42966136854F4464516FBB4AE72] - 03/10/2012 - 22:28:22 -S-A- . (...) -- C:\WINDOWS\bootstat.dat [2048]
O44 - LFC:[MD5.6E507289469B5D8DF6673EF6FD2DAD59] - 03/10/2012 - 22:27:49 ---A- . (...) -- C:\WINDOWS\SchedLgU.Txt [32294]
O44 - LFC:[MD5.876E9D3BF52B3096945640093FE23DE6] - 03/10/2012 - 22:10:01 ---A- . (...) -- C:\INSTALLHELPER.LOG [19125]
O44 - LFC:[MD5.8FC5EE6FC46F9C5DD20F8BF77359FC79] - 03/10/2012 - 22:09:59 ---A- . (...) -- C:\alotserviceruntime.log [16841312]
O44 - LFC:[MD5.78C1299EC87162ABA65FAB1B0C7E3341] - 30/09/2012 - 15:02:18 ---A- . (...) -- C:\WINDOWS\system32\wpa.dbl [1374]

O44 - LFC:[MD5.6A2DC3BB2188E958E9B33382E22380BB] - 23/09/2012 - 01:00:13 ---A- . (...) -- C:\WINDOWS\FaxSetup.log [123662]
O44 - LFC:[MD5.6A2CC437F9C3C205A992252173E6D1F9] - 23/09/2012 - 01:00:13 ---A- . (...) -- C:\WINDOWS\KB2744842-IE8.log [16563]
O44 - LFC:[MD5.47F440594D2995A1299B5513F6D8A15E] - 23/09/2012 - 01:00:13 ---A- . (...) -- C:\WINDOWS\comsetup.log [41534]
O44 - LFC:[MD5.A74D786FC43CB5BE49205CC8E158E81F] - 23/09/2012 - 01:00:13 ---A- . (...) -- C:\WINDOWS\iis6.log [19689]
O44 - LFC:[MD5.1B5DB0FBC7626432C2280DB3470475F9] - 23/09/2012 - 01:00:13 ---A- . (...) -- C:\WINDOWS\imsins.log [1374]
O44 - LFC:[MD5.26C2B8F0314F721C3EAB26477BE24DB5] - 23/09/2012 - 01:00:13 ---A- . (...) -- C:\WINDOWS\msgsocm.log [6180]
O44 - LFC:[MD5.7BC2AE3DD800D6E3C0359AE7EFBB094F] - 23/09/2012 - 01:00:13 ---A- . (...) -- C:\WINDOWS\ntdtcsetup.log [25102]
O44 - LFC:[MD5.4252F0673877C5F0A8A412FB4B5C7256] - 23/09/2012 - 01:00:13 ---A- . (...) -- C:\WINDOWS\ocgen.log [59120]
O44 - LFC:[MD5.9C759D1739A798EEE5B02A5DA4B8C147] - 23/09/2012 - 01:00:13 ---A- . (...) -- C:\WINDOWS\ocmsn.log [6840]
O44 - LFC:[MD5.CB3434442FC1D4EEAA3FA7DC81CDC8AE] - 23/09/2012 - 01:00:13 ---A- . (...) -- C:\WINDOWS\setupapi.log [98322]
O44 - LFC:[MD5.8E7135DC810DAC8606661488103242D8] - 23/09/2012 - 01:00:13 ---A- . (...) -- C:\WINDOWS\tsoc.log [47185]
O44 - LFC:[MD5.BEE90F7D52BF26E981727D1AF19A459F] - 23/09/2012 - 01:00:02 ---A- . (...) -- C:\WINDOWS\updspapi.log [10762]
O44 - LFC:[MD5.3B6F0E8EC254686E4382390B4C49EF59] - 22/09/2012 - 22:13:13 ---A- . (.Adobe Systems Incorporated - Adobe Flash Player Control Panel Applet.) -- C:\WINDOWS\system32\FlashPlayerApp.exe [696240]
O44 - LFC:[MD5.51911756C61CF1437DA21E82EC4BA1A7] - 22/09/2012 - 22:13:13 ---A- . (.Adobe Systems Incorporated - Adobe Flash Player Control Panel Applet.) -- C:\WINDOWS\system32\FlashPlayerCPLApp.cpl [73136]
O44 - LFC:[MD5.72901D62C40FDF29A1A2AE58756FB146] - 22/09/2012 - 21:38:27 ---A- . (...) -- C:\WINDOWS\spupdsvc.log [49825]
O44 - LFC:[MD5.12C159ED04033EBC98346D103F048B2A] - 17/09/2012 - 22:19:36 ---A- . (...) -- C:\WINDOWS\KB975558.log [5663]
O44 - LFC:[MD5.7300BC04462FC157AD4A8767880780BB] - 17/09/2012 - 22:19:33 ---A- . (...) -- C:\WINDOWS\KB2378111.log [5368]
O44 - LFC:[MD5.EB7543316FE92B5DA08BD6E70F722195] - 17/09/2012 - 22:19:32 ---A- . (...) -- C:\WINDOWS\wmsetup.log [8613]
O44 - LFC:[MD5.0E6F0824648F80ACE4ABF9375B0E7C00] - 17/09/2012 - 22:19:28 ---A- . (...) -- C:\WINDOWS\KB954155.log [5756]
O44 - LFC:[MD5.6979902D7DAC24E188D075D6BAC29932] - 17/09/2012 - 22:19:25 ---A- . (...) -- C:\WINDOWS\KB941569.log [6400]
O44 - LFC:[MD5.2610984398859979ED5964C413476A4A] - 17/09/2012 - 22:19:25 ---A- . (...) -- C:\WINDOWS\imsins.BAK [1374]
O44 - LFC:[MD5.EF358470E72F693D69A91F7FFC611FB5] - 17/09/2012 - 22:18:57 ---A- . (...) -- C:\WINDOWS\KB978695.log [5721]
O44 - LFC:[MD5.EEC07314B6F3129CA999B53B89A042B3] - 17/09/2012 - 22:18:54 ---A- . (...) -- C:\WINDOWS\KB973540.log [6514]
O44 - LFC:[MD5.23926E1B58EE71B7E93E5EF68E0AFB7F] - 17/09/2012 - 22:18:47 ---A- . (...) -- C:\WINDOWS\KB929399.log [4795]
O44 - LFC:[MD5.7D112FDDF8C294502DD176F881F4A5A8] - 17/09/2012 - 22:18:18 ---A- . (...) -- C:\WINDOWS\KB939683.log [4520]

O44 - LFC:[MD5.36B816DE0031428AF2941DB8486023EE] - 17/09/2012 - 22:17:46 ---A- . (...) -- C:\WINDOWS\KB952069.log [10739]
O44 - LFC:[MD5.DDC75A66F1AD11A92CA192ABB4C21A25] - 17/09/2012 - 22:17:42 ---A- . (...) -- C:\WINDOWS\KB954154.log [4172]
O44 - LFC:[MD5.7D91D429A364B720E21DC204FDE25EA0] - 17/09/2012 - 20:29:11 ---A- . (...) -- C:\WINDOWS\wmsetup10.log [1211]
O44 - LFC:[MD5.6D6F4B1886E91EB37ABCCAD19C561EE0] - 17/09/2012 - 20:28:40 ---A- . (...) -- C:\WINDOWS\system32\amcompat.tlb [16832]
O44 - LFC:[MD5.A32B14BE5EDAE794FCE1A9E970827509] - 17/09/2012 - 20:28:40 ---A- . (...) -- C:\WINDOWS\system32\nscompat.tlb [23392]
O44 - LFC:[MD5.71CC93A189E9B696AE5DE6ED3E46E691] - 15/09/2012 - 10:23:15 ---A- . (...) -- C:\WINDOWS\MSCompPackV1.log [3324]
O44 - LFC:[MD5.942991F66DF71D2495E6FAB9F05BD65F] - 15/09/2012 - 10:23:05 ---A- . (...) -- C:\WINDOWS\wmp11.log [14427]
O44 - LFC:[MD5.F5C397BEFBE878EBBAA17055D06359C7] - 15/09/2012 - 10:22:53 ---A- . (...) -- C:\WINDOWS\win.ini [507]
O44 - LFC:[MD5.DE1C5C921C6D9AC6208DBE54A4EE05A7] - 15/09/2012 - 10:21:35 ---A- . (...) -- C:\WINDOWS\WMFDist11.log [22165]
O44 - LFC:[MD5.DC17DD0189B0C36D863B4DD0A036C10F] - 15/09/2012 - 10:21:28 ---A- . (...) -- C:\WINDOWS\WMSysPr9.prx [316640]
O44 - LFC:[MD5.D69A336BED772975B1BA01EEC3D84AD7] - 15/09/2012 - 10:20:22 ---A- . (...) -- C:\WINDOWS\Wudf01000Inst.log [7196]
O44 - LFC:[MD5.52C18A4B4AC4778B6980CF8284893FB8] - 13/09/2012 - 14:26:52 ---A- . (...) -- C:\WINDOWS\system32\dmwu.exe [1006448]
O44 - LFC:[MD5.D76BF9E2E3F6E64DE663037D70722D9A] - 13/09/2012 - 14:24:48 ---A- . (...) -- C:\WINDOWS\system32\ImHttpComm.dll [28160]
O44 - LFC:[MD5.7ACE05D782798D3E3667CD6C632F278B] - 12/09/2012 - 23:26:26 ---A- . (...) -- C:\WINDOWS\KB2736233.log [6377]
~ Scan Files in 00mn 01s

---\\ Opérations et fonctions au démarrage de Windows Explorer (O46)
O46 - SEH:ShellExecuteHooks - URL Exec Hook - {AEB6717E-7E19-11d0-97EE-00C04FD91972} - shell32.dll
~ Scan ShellExecuteHooks in 00mn 00s

---\\ Export de clé d'application autorisée (O47)
O47 - AAKE:Key Export SP - "%windir%\Network Diagnostic\xpnetdiag.exe" [Enabled] . (.Microsoft Corporation - Network Diagnostic for Windows XP.) -- C:\WINDOWS\Network Diagnostic\xpnetdiag.exe
O47 - AAKE:Key Export SP - "%windir%\system32\sessmgr.exe" [Enabled] .(.Microsoft Corporation - Gestionnaire de session de l'aide sur le Bureau à distance de Microsoft®.) -- C:\WINDOWS\system32\sessmgr.exe
O47 - AAKE:Key Export SP - "D:\data\eSKernel.exe" [Enabled] .(...) -- D:\data\eSKernel.exe (.not file.)
O47 - AAKE:Key Export SP - "C:\Program Files\REALTEK\11n USB Wireless LAN Utility\RtWLan.exe" [Enabled] .(.Realtek Semiconductor Corp. - RtWLan (For XP/2003) Application.) -- C:\Program Files\REALTEK\11n USB Wireless LAN Utility\RtWLan.exe
O47 - AAKE:Key Export SP - "C:\Program Files\Ares\Ares.exe" [Enabled] .(...) -- C:\Program

Files\Ares\Ares.exe (.not file.)
O47 - AAKE:Key Export SP - "C:\Documents and Settings\user\Application Data\Spotify\spotify.exe" [Enabled] .(...) -- C:\Documents and Settings\user\Application Data\Spotify\spotify.exe (.not file.)
O47 - AAKE:Key Export SP - "C:\wamp\bin\apache\Apache2.2.21\bin\httpd.exe" [Enabled] . (.Apache Software Foundation - Apache HTTP Server.) -- C:\wamp\bin\apache\Apache2.2.21\bin\httpd.exe
O47 - AAKE:Key Export SP - "C:\Program Files\Fichiers communs\Apple\Apple Application Support\WebKit2WebProcess.exe" [Enabled] .(.Apple Inc..) -- C:\Program Files\Fichiers communs\Apple\Apple Application Support\WebKit2WebProcess.exe
O47 - AAKE:Key Export SP - "C:\WINDOWS\system32\lxctcoms.exe" [Enabled] .(.Pas de propriétaire - Printer Communication System.) -- C:\WINDOWS\system32\lxctcoms.exe
O47 - AAKE:Key Export SP - "C:\WINDOWS\system32\dmwu.exe" [Enabled] .(...) -- C:\WINDOWS\system32\dmwu.exe
O47 - AAKE:Key Export SP - "C:\WINDOWS\system32\ARFC\wrtc.exe" [Enabled] .(...) -- C:\WINDOWS\system32\ARFC\wrtc.exe
O47 - AAKE:Key Export DP - "%windir%\Network Diagnostic\xpnetdiag.exe" [Enabled] . (.Microsoft Corporation - Network Diagnostic for Windows XP.) -- C:\WINDOWS\Network Diagnostic\xpnetdiag.exe
O47 - AAKE:Key Export DP - "%windir%\system32\sessmgr.exe" [Enabled] .(.Microsoft Corporation - Gestionnaire de session de l'aide sur le Bureau à distance de Microsoft®.) -- C:\WINDOWS\system32\sessmgr.exe
~ Scan Keys in 00mn 01s

---\\ 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 - Kerberos Security Package.) -- 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
~ Scan Keys in 00mn 00s

---\\ Contrôle du Safe Boot (CSB) (O49)
O49 - CSB:Control Safe Boot HKLM\...\CCS\Minimal\dmboot.sys . (.Microsoft Corp., Veritas Software - Pilote de démarrage du gestionnaire de disque NT.) -- C:\WINDOWS\system32\Drivers\dmboot.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Minimal\dmio.sys . (.Microsoft Corp., Veritas Software - Pilote E/S du Gestionnaire de disques NT.) -- C:\WINDOWS\system32\Drivers\dmio.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Minimal\dmload.sys . (.Microsoft Corp., Veritas Software. - NT Disk Manager Startup Driver.) -- C:\WINDOWS\system32\Drivers\dmload.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Minimal\sermouse.sys . (...) --

C:\WINDOWS\system32\Drivers\sermouse.sys (.not file.)
O49 - CSB:Control Safe Boot HKLM\...\CCS\Minimal\sr.sys . (.Microsoft Corporation - Pilote de filtre de système de fichiers pour la restauration du système.) --
C:\WINDOWS\system32\Drivers\sr.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\Network\dmboot.sys . (.Microsoft Corp., Veritas Software - Pilote de démarrage du gestionnaire de disque NT.) --
C:\WINDOWS\system32\Drivers\dmboot.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\dmio.sys . (.Microsoft Corp., Veritas Software - Pilote E/S du Gestionnaire de disques NT.) -- C:\WINDOWS\system32\Drivers\dmio.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\dmload.sys . (.Microsoft Corp., Veritas Software. - NT Disk Manager Startup Driver.) -- C:\WINDOWS\system32\Drivers\dmload.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\ip6fw.sys . (.Microsoft Corporation - IPv6 Windows Firewall Driver.) -- C:\WINDOWS\system32\Drivers\ip6fw.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\rdpcdd.sys . (.Microsoft Corporation - RDP Miniport.) -- C:\WINDOWS\system32\Drivers\rdpcdd.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\rdpdd.sys . (...) --
C:\WINDOWS\system32\Drivers\rdpdd.sys (.not file.)
O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\rdpwd.sys . (.Microsoft Corporation - RDP Terminal Stack Driver (US/Canada Only, Not for Export).) --
C:\WINDOWS\system32\Drivers\rdpwd.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\sermouse.sys . (...) --
C:\WINDOWS\system32\Drivers\sermouse.sys (.not file.)
O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\sr.sys . (.Microsoft Corporation - Pilote de filtre de système de fichiers pour la restauration du système.) --
C:\WINDOWS\system32\Drivers\sr.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\tdpipe.sys . (.Microsoft Corporation - Named Pipe Transport Driver.) -- C:\WINDOWS\system32\Drivers\tdpipe.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\tdtcp.sys . (.Microsoft Corporation - TCP Transport Driver.) -- C:\WINDOWS\system32\Drivers\tdtcp.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.)
~ Scan CSB in 00mn 00s

---\\ Image File Execution Options (IFEO) (O50)
O50 - IFEO:Image File Execution Options - Your Image File Name Here without a path - ntsd -d
~ Scan IFEO in 00mn 00s

---\\ MountPoints2 Shell Key (O51)
O51 - MPSK:{f4303d41-52bf-11df-9ebc-ad23b4d793eb}\AutoRun\command - Clé orpheline
~ Scan Keys in 00mn 00s

---\\ Trojan Driver Search Data (HKLM) (O52)
O52 - TDSD: \Drivers32\"msacm.trspch"="tssoft32.acm" . (.DSP GROUP, INC. - Codec audio TrueSpeech(TM) DSP Group pour MSACM V3.50.) -- C:\WINDOWS\system32\tssoft32.acm
O52 - TDSD: \Drivers32\"vidc.cvid"="iccvid.dll" . (.Radius Inc. - Cinepak® Codec.) -- C:\WINDOWS\system32\iccvid.dll
O52 - TDSD: \Drivers32\"vidc.iv31"="ir32_32.dll" . (...) -- C:\WINDOWS\system32\ir32_32.dll
O52 - TDSD: \Drivers32\"vidc.iv32"="ir32_32.dll" . (...) -- C:\WINDOWS\system32\ir32_32.dll
O52 - TDSD: \Drivers32\"vidc.iv41"="ir41_32.ax" . (.Intel Corporation - Intel Indeo® Video 4.5.) -- C:\WINDOWS\system32\ir41_32.ax
O52 - TDSD: \Drivers32\"msacm.sl_anet"="sl_anet.acm" . (.Sipro Lab Telecom Inc. - Audio codec for MS ACM.) -- C:\WINDOWS\system32\sl_anet.acm
O52 - TDSD: \Drivers32\"msacm.iac2"="C:\WINDOWS\system32\iac25_32.ax" . (.Intel Corporation - Indeo® audio software.) -- C:\WINDOWS\system32\iac25_32.ax
O52 - TDSD: \Drivers32\"vidc.iv50"="ir50_32.dll" . (.Intel Corporation - Intel Indeo® video 5.10.) -- C:\WINDOWS\system32\ir50_32.dll
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: \drivers.desc\"sl_anet.acm"="Sipro Lab Telecom Audio Codec" . (.Sipro Lab Telecom Inc. - Audio codec for MS ACM.) -- C:\WINDOWS\system32\sl_anet.acm
O52 - TDSD: \drivers.desc\"C:\WINDOWS\system32\iac25_32.ax"="Indeo® audio software" . (.Intel Corporation - Indeo® audio software.) -- C:\WINDOWS\system32\iac25_32.ax
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
~ Scan Keys in 00mn 00s

---\\ ShareTools MSconfig StartupReg (O53) (None)

---\\ Microsoft Control Security Providers (O54)
O54 - MCSP:[HKLM\...\CurrentControlSet\Control] - (SecurityProviders) - (.Microsoft Corporation - Client DPA pour plate-forme 32 bit.) -- C:\WINDOWS\system32\msapsspc.dll
O54 - MCSP:[HKLM\...\CurrentControlSet\Control] - (SecurityProviders) - (.Microsoft Corporation - TLS / SSL Security Provider.) -- C:\WINDOWS\system32\schannel.dll
O54 - MCSP:[HKLM\...\CurrentControlSet\Control] - (SecurityProviders) - (.Microsoft Corporation - Package d'authentification Digest SSPI.) -- C:\WINDOWS\system32\digest.dll
O54 - MCSP:[HKLM\...\ControlSet001\Control] - (SecurityProviders) - (.Microsoft Corporation - Client DPA pour plate-forme 32 bit.) -- C:\WINDOWS\system32\msapsspc.dll
O54 - MCSP:[HKLM\...\ControlSet001\Control] - (SecurityProviders) - (.Microsoft Corporation - TLS / SSL Security Provider.) -- C:\WINDOWS\system32\schannel.dll
O54 - MCSP:[HKLM\...\ControlSet001\Control] - (SecurityProviders) - (.Microsoft Corporation - Package d'authentification Digest SSPI.) -- C:\WINDOWS\system32\digest.dll
~ Scan Keys in 00mn 00s

---\\ Microsoft Windows Policies System (O55)

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] - "shutdownwithoutlogon"=1
O55 - MWPS:[HKLM\...\Policies\System] - "undockwithoutlogon"=1
~ Scan Keys in 00mn 00s

---\\ Microsoft Windows Policies Explorer (O56)
O56 - MWPE:[HKCU\...\policies\Explorer] - "NoDriveTypeAutoRun"=145
O56 - MWPE:[HKLM\...\policies\Explorer] - "HonorAutoRunSetting"=1
~ Scan Keys in 00mn 00s

---\\ Liste des Drivers Système (O58)
O58 - SDL:[MD5.0352A73CD6B1782EA3ED7A03A8268F55] - 21/08/2012 - 10:13:13 ---A- . (.AVAST Software - avast! Base Kernel-Mode Device Driver for Windows NT/2000/XP.) -- C:\WINDOWS\system32\Drivers\aavmker4.sys [25256]
O58 - SDL:[MD5.6D3ADA4CE95CECA7BCE527A08C4C474E] - 02/03/2006 - 13:00:00 ---A- . (...) -- C:\WINDOWS\system32\ansi.sys [9037]
~ Scan Drivers in 00mn 00s

---\\ Liste des outils de nettoyage (O63)
O63 - Logiciel: ZHPDiag 1.31 - (.Nicolas Coolman.) [HKLM] -- ZHPDiag_is1
~ Scan ADS in 00mn 00s

---\\ Liste des services Legacy (O64)
O64 - Services: CurCS - ??\??\???? - C:\WINDOWS\system32\Drivers\Aavmker4.sys (Aavmker4) .(.AVAST Software - avast! Base Kernel-Mode Device Driver for W.) - LEGACY_AAVMKER4
O64 - Services: CurCS - 22/09/2012 - C:\WINDOWS\system32\Macromed\Flash\FlashPlayerUpdateService.exe (AdobeFlashPlayerUpdateSvc) .(.Adobe Systems Incorporated - Adobe® Flash® Player Update Service 11.4 r4.) - LEGACY_ADOBEFLASHPLAYERUPDATESVC
O64 - Services: CurCS - 18/02/2005 - C:\WINDOWS\system32\DRIVERS\AegisP.sys (AegisP) . (.Cisco Systems, Inc. - IEEE 802.1X Protocol Driver.) - LEGACY_AEGISP
O64 - Services: CurCS - ??\??\???? - C:\WINDOWS\system32\Drivers\aswFsBlk.sys (aswFsBlk) . (.AVAST Software - avast! File System Access Blocking Driver.) - LEGACY_ASWFSBLK
O64 - Services: CurCS - ??\??\???? - C:\WINDOWS\system32\Drivers\aswMon2.sys (aswMon2) . (.AVAST Software - avast! File System Filter Driver for Window.) - LEGACY_ASWMON2
O64 - Services: CurCS - ??\??\???? - C:\WINDOWS\system32\Drivers\aswRdr.sys (aswRdr) . (.AVAST Software - avast! TDI Redirect Driver.) - LEGACY_ASWRDR
O64 - Services: CurCS - ??\??\???? - C:\WINDOWS\system32\Drivers\aswSnx.sys (aswSnx) . (.AVAST Software - avast! Virtualization Driver.) - LEGACY_ASWSNX
O64 - Services: CurCS - ??\??\???? - C:\WINDOWS\system32\Drivers\aswSP.sys (aswSP) . (.AVAST Software - avast! self protection module.) - LEGACY_ASWSP

O64 - Services: CurCS - ??\??\???? - C:\WINDOWS\system32\Drivers\aswTdi.sys (aswTdi) . (.AVAST Software - avast! TDI Filter Driver.) - LEGACY_ASWTDI
O64 - Services: CurCS - 21/08/2012 - C:\Program Files\Alwil Software\Avast5\AvastSvc.exe (avast! Antivirus) .(.AVAST Software - avast! Service.) - LEGACY_AVAST!_ANTIVIRUS
O64 - Services: CurCS - ??\??\???? - (DcomLaunch) .(. - .) - LEGACY_DCOMLAUNCH
O64 - Services: CurCS - 13/04/2008 - C:\WINDOWS\system32\drivers\dmboot.sys (dmboot) . (.Microsoft Corp., Veritas Software - Pilote de démarrage du gestionnaire de disq.) - LEGACY_DMBOOT
O64 - Services: CurCS - 02/03/2006 - C:\WINDOWS\system32\drivers\dmload.sys (dmload) . (.Microsoft Corp., Veritas Software. - NT Disk Manager Startup Driver.) - LEGACY_DMLOAD
O64 - Services: CurCS - 16/12/2010 - C:\Program Files\Google\Update\GoogleUpdate.exe (gupdate) .(.Google Inc. - Programme d'installation de Google.) - LEGACY_GUPDATE
O64 - Services: CurCS - 16/12/2010 - C:\Program Files\Google\Update\GoogleUpdate.exe (gupdatem) .(.Google Inc. - Programme d'installation de Google.) - LEGACY_GUPDATEM
O64 - Services: CurCS - 13/07/2012 - C:\Program Files\Java\jre6\bin\jqs.exe (JavaQuickStarterService) .(.Sun Microsystems, Inc. - Java(TM) Quick Starter Service.) - LEGACY_JAVAQUICKSTARTERSERVICE
O64 - Services: CurCS - 22/11/2006 - C:\WINDOWS\system32\lxctcoms.exe (lxct_device) .(.Pas de propriétaire - Printer Communication System.) - LEGACY_LXCT_DEVICE
O64 - Services: CurCS - 15/01/2010 - C:\Program Files\McAfee Security Scan\2.0.181\McCHSvc.exe (McComponentHostService) .(.McAfee, Inc. - Component Host Service.) - LEGACY_MCCOMPONENTHOSTSERVICE
O64 - Services: CurCS - 11/03/2010 - C:\Program Files\Fichiers communs\Protexis\License Service\PsiService_2.exe (PSI_SVC_2) .(.Protexis Inc. - PsiService PsiService.) - LEGACY_PSI_SVC_2
O64 - Services: CurCS - 17/04/2007 - C:\WINDOWS\system32\drivers\regi.sys (regi) .(.InterVideo - regi driver.) - LEGACY_REGI
O64 - Services: CurCS - ??\??\???? - (RpcSs) .(. - .) - LEGACY_RPCSS
O64 - Services: CurCS - 13/04/2008 - C:\WINDOWS\system32\svchost.exe (ShellHWDetection) . (.Microsoft Corporation - Generic Host Process for Win32 Services.) - LEGACY_SHELLHWDETECTION
O64 - Services: CurCS - ??\??\???? - (TermService) .(. - .) - LEGACY_TERMSERVICE
O64 - Services: CurCS - 26/09/2011 - c:\wamp\bin\apache\apache2.2.21\bin\httpd.exe (wampapache) .(.Apache Software Foundation - Apache HTTP Server.) - LEGACY_WAMPAPACHE
O64 - Services: CurCS - 25/01/2012 - c:\wamp\bin\mysql\mysql5.5.20\bin\mysqld.exe - wampmysqld (wampmysqld) .(...) - LEGACY_WAMPMYSQLD
O64 - Services: CurCS - 13/09/2012 - C:\WINDOWS\system32\dmwu.exe - WebOptimizer (WebOptimizer) .(...) - LEGACY_WEBOPTIMIZER
O64 - Services: CurCS - 23/08/2012 - C:\Program Files\Web Assistant\ExtensionUpdaterService.exe - Web Assistant Updater (Web Assistant Updater) .(...) - LEGACY_WEB_ASSISTANT_UPDATER
~ Scan Services in 00mn 00s

---\\ File Associations Shell Spawning (O67)
O67 - Shell Spawning: <.bat> <batfile>[HKLM\..\open\Command] (...) -- "%1" %*
O67 - Shell Spawning: <.cpl> <cplfile>[HKLM\..\cplopen\Command] (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\WINDOWS\system32\shell32.dll
O67 - Shell Spawning: <.cmd> <cmdfile>[HKLM\..\open\Command] (...) -- "%1" %*
O67 - Shell Spawning: <.com> <comfile>[HKLM\..\open\Command] (...) -- "%1" %*

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: <.html> <ChromeHTML>[HKCU\..\open\Command] (.Google Inc. - Google Chrome.) -- C:\Documents and Settings\user\Local Settings\Application Data\Google\Chrome\Application\chrome.exe
O67 - Shell Spawning: <.bat> <batfile>[HKCR\..\open\Command] (...) -- "%1" %*
O67 - Shell Spawning: <.cpl> <cplfile>[HKCR\..\cplopen\Command] (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\WINDOWS\system32\shell32.dll
O67 - Shell Spawning: <.cmd> <cmdfile>[HKCR\..\open\Command] (...) -- "%1" %*
O67 - Shell Spawning: <.com> <comfile>[HKCR\..\open\Command] (...) -- "%1" %*
O67 - Shell Spawning: <.exe> <exefile>[HKCR\..\open\Command] (...) -- "%1" %*
O67 - Shell Spawning: <.html> <ChromeHTML>[HKCR\..\open\Command] (.Google Inc. - Google Chrome.) -- C:\Documents and Settings\user\Local Settings\Application Data\Google\Chrome\Application\chrome.exe
O67 - Shell Spawning: <.js> <JSFile>[HKCR\..\open\Command] (.Microsoft Corporation - Microsoft (R) Windows Based Script Host.) -- C:\WINDOWS\system32\WScript.exe
O67 - Shell Spawning: <.reg> <regfile>[HKCR\..\open\Command] (.Microsoft Corporation - Éditeur du Registre.) -- C:\WINDOWS\regedit.exe
~ Scan Keys in 00mn 00s

---\\ Start Menu Internet (O68)
O68 - StartMenuInternet: <chrome.exe> <>[HKLM\..\Shell\open\Command] (.Google Inc. - Google Chrome.) -- C:\Documents and Settings\user\Local Settings\Application Data\Google\Chrome\Application\chrome.exe
O68 - StartMenuInternet: <Google Chrome> <Google Chrome>[HKLM\..\Shell\open\Command] (.Google Inc. - Google Chrome.) -- C:\Documents and Settings\user\Local Settings\Application Data\Google\Chrome\Application\chrome.exe
O68 - StartMenuInternet: <IEXPLORE.EXE> <Internet Explorer>[HKLM\..\Shell\open\Command] (.Microsoft Corporation - Internet Explorer.) -- C:\Program Files\Internet Explorer\iexplore.exe
O68 - StartMenuInternet: <Google Chrome> <Google Chrome>[HKLM\..\InstallInfo\ShowIconsCommand] (...) -- C:\Documents and Settings\user\Local Settings\Application Data\Google\Chrome\Application\chrome.exe (.not file.)
O68 - StartMenuInternet: <IEXPLORE.EXE> <Internet Explorer>[HKLM\..\InstallInfo\ShowIconsCommand] (...) -- C:\WINDOWS\system32\ie4uinit.exe (.not file.)
O68 - StartMenuInternet: <Google Chrome> <Google Chrome>[HKLM\..\InstallInfo\ReinstallCommand] (...) -- C:\Documents and Settings\user\Local Settings\Application Data\Google\Chrome\Application\chrome.exe (.not file.)
O68 - StartMenuInternet: <IEXPLORE.EXE> <Internet Explorer>[HKLM\..\InstallInfo\ReinstallCommand] (...) -- C:\WINDOWS\system32\ie4uinit.exe (.not file.)
O68 - StartMenuInternet: <Google Chrome> <Google Chrome>[HKLM\..\InstallInfo\HideIconsCommand] (...) -- C:\Documents and Settings\user\Local Settings\Application Data\Google\Chrome\Application\chrome.exe (.not file.)

O68 - StartMenuInternet: <IEXPLORE.EXE> <Internet Explorer>[HKLM\..\InstallInfo\HideIconsCommand] (...) -- C:\WINDOWS\system32\ie4uinit.exe (.not file.)
~ Scan Keys in 00mn 00s

---\\ Search Browser Infection (O69)
O69 - SBI: SearchScopes [HKCU] {0ECDF796-C2DC-4d79-A620-CCE0C0A66CC9} - (Search the web (Babylon)) - http://search.babylon.com
O69 - SBI: SearchScopes [HKCU] {14FCC24E-8728-740F-56D2-7C32D5F3EDE7} - (Search the web (Babylon)) - http://search.babylon.com
O69 - SBI: SearchScopes [HKCU] {77764D33-C584-34B0-85D1-5EAFD179C28B} - (MyStart Search) - http://mystart.incredibar.com
O69 - SBI: SearchScopes [HKCU] {8A244612-A1F7-11E0-95C0-E71F4824019B} - (Search) - http://badoo.com
O69 - SBI: SearchScopes [HKCU] {A531D99C-5A22-449b-83DA-872725C6D0ED} - (Recherche alOt) - http://search.alot.com
O69 - SBI: SearchScopes [HKCU] {a5b9c0f5-5616-47cd-a95f-e43b488faccf} - (My Web Search) - http://search.mywebsearch.com
O69 - SBI: SearchScopes [HKCU] {CFF4DB9B-135F-47c0-9269-B4C6572FD61A} [DefaultScope] - (Funmoods) - http://start.funmoods.com
O69 - SBI: SearchScopes [HKCU] {EEE6C360-6118-11DC-9C72-001320C79847} - (SweetIM Search) - http://search.sweetim.com
~ Scan Keys in 00mn 00s

---\\ Recherche des services démarrés par Svchost (O83)
O83 - Search Svchost Services: AppMgmt (AppMgmt) . (...) -- C:\WINDOWS\system32\appmgmts.dll [0]
O83 - Search Svchost Services: AudioSrv (AudioSrv) . (.Microsoft Corporation - Windows Audio Service.) -- C:\WINDOWS\system32\audiosrv.dll [42496]
O83 - Search Svchost Services: Browser (Browser) . (.Microsoft Corporation - Computer Browser Service DLL.) -- C:\WINDOWS\system32\browser.dll [78336]
O83 - Search Svchost Services: CryptSvc (CryptSvc) . (.Microsoft Corporation - Cryptographic Services.) -- C:\WINDOWS\system32\cryptsvc.dll [62464]
O83 - Search Svchost Services: DMServer (DMServer) . (.Microsoft Corp. - DLL Service gestionnaire de disque logique.) -- C:\WINDOWS\system32\dmserver.dll [24576]
O83 - Search Svchost Services: DHCP (DHCP) . (.Microsoft Corporation - Service client DHCP.) -- C:\WINDOWS\system32\dhcpcsvc.dll [127488]
O83 - Search Svchost Services: ERSvc (ERSvc) . (.Microsoft Corporation - Windows Error Reporting Service.) -- C:\WINDOWS\system32\ersvc.dll [23040]
O83 - Search Svchost Services: EventSystem (EventSystem) . (.Microsoft Corporation - Pas de description.) -- C:\WINDOWS\system32\es.dll [253952]
O83 - Search Svchost Services: FastUserSwitchingCompatibility (FastUserSwitchingCompatibility) . (.Microsoft Corporation - Dll des services Windows Shell.) -- C:\WINDOWS\system32\shsvcs.dll [135680]
O83 - Search Svchost Services: HidServ (HidServ) . (.Microsoft Corporation - HID Audio Service.) -- C:\WINDOWS\system32\hidserv.dll [21504]
O83 - Search Svchost Services: LanmanServer (LanmanServer) . (.Microsoft Corporation - Server Service DLL.) -- C:\WINDOWS\system32\srvsvc.dll [99840]

O83 - Search Svchost Services: LanmanWorkstation (LanmanWorkstation) . (.Microsoft Corporation - Workstation Service DLL.) -- C:\WINDOWS\system32\wkssvc.dll [132096]
O83 - Search Svchost Services: Messenger (Messenger) . (.Microsoft Corporation - NT Messenger Service.) -- C:\WINDOWS\system32\msgsvc.dll [33792]
O83 - Search Svchost Services: Netman (Netman) . (.Microsoft Corporation - Gestionnaire de connexions réseau.) -- C:\WINDOWS\system32\netman.dll [198144]
O83 - Search Svchost Services: Nla (Nla) . (.Microsoft Corporation - Fournisseur de service Sockets 2.0 de Microsoft Windows.) -- C:\WINDOWS\system32\mswsock.dll [247808]
O83 - Search Svchost Services: Ntmssvc (Ntmssvc) . (.Microsoft Corporation - Gestionnaire de stockage amovible.) -- C:\WINDOWS\system32\ntmssvc.dll [438272]
O83 - Search Svchost Services: Rasauto (Rasauto) . (.Microsoft Corporation - Remote Access AutoDial Manager.) -- C:\WINDOWS\system32\rasauto.dll [88576]
O83 - Search Svchost Services: Rasman (Rasman) . (.Microsoft Corporation - Remote Access Connection Manager.) -- C:\WINDOWS\system32\rasmans.dll [186368]
O83 - Search Svchost Services: Remoteaccess (Remoteaccess) . (.Microsoft Corporation - Dynamic Interface Manager.) -- C:\WINDOWS\system32\mprdim.dll [53248]
O83 - Search Svchost Services: Schedule (Schedule) . (.Microsoft Corporation - Moteur du Planificateur de tâches.) -- C:\WINDOWS\system32\schedsvc.dll [194560]
O83 - Search Svchost Services: Seclogon (Seclogon) . (.Microsoft Corporation - DLL de service d'ouverture de session secondaire.) -- C:\WINDOWS\system32\seclogon.dll [18944]
O83 - Search Svchost Services: SENS (SENS) . (.Microsoft Corporation - System Event Notification Service (SENS).) -- C:\WINDOWS\system32\sens.dll [39424]
O83 - Search Svchost Services: Sharedaccess (Sharedaccess) . (.Microsoft Corporation - Composants de l'application d'assistance à Microsoft NAT.) -- C:\WINDOWS\system32\ipnathlp.dll [332800]
O83 - Search Svchost Services: SRService (SRService) . (.Microsoft Corporation - Service de restauration du système.) -- C:\WINDOWS\system32\srsvc.dll [171520]
O83 - Search Svchost Services: Tapisrv (Tapisrv) . (.Microsoft Corporation - Serveur de téléphonie Microsoft® Windows(TM).) -- C:\WINDOWS\system32\tapisrv.dll [249856]
O83 - Search Svchost Services: Themes (Themes) . (.Microsoft Corporation - Dll des services Windows Shell.) -- C:\WINDOWS\system32\shsvcs.dll [135680]
O83 - Search Svchost Services: TrkWks (TrkWks) . (.Microsoft Corporation - Distributed Link Tracking Client.) -- C:\WINDOWS\system32\trkwks.dll [90112]
O83 - Search Svchost Services: W32Time (W32Time) . (.Microsoft Corporation - Service de temps Windows.) -- C:\WINDOWS\system32\w32time.dll [178176]
O83 - Search Svchost Services: WZCSVC (WZCSVC) . (.Microsoft Corporation - Service configuration automatique sans fil.) -- C:\WINDOWS\system32\wzcsvc.dll [483840]
O83 - Search Svchost Services: winmgmt (winmgmt) . (.Microsoft Corporation - WMI.) -- C:\WINDOWS\system32\wbem\WMIsvc.dll [145408]
O83 - Search Svchost Services: wscsvc (wscsvc) . (.Microsoft Corporation - Windows Security Center Service.) -- C:\WINDOWS\system32\wscsvc.dll [80896]
O83 - Search Svchost Services: xmlprov (xmlprov) . (.Microsoft Corporation - Network Provisioning Service.) -- C:\WINDOWS\system32\xmlprov.dll [129024]
O83 - Search Svchost Services: napagent (napagent) . (.Microsoft Corporation - Exécution du service Agent de quarantaine.) -- C:\WINDOWS\system32\qagentrt.dll [293376]
O83 - Search Svchost Services: hkmsvc (hkmsvc) . (.Microsoft Corporation - Service Gestion des clés.) -- C:\WINDOWS\system32\kmsvc.dll [61440]
O83 - Search Svchost Services: BITS (BITS) . (.Microsoft Corporation - Service de transfert intelligent en arrière-plan.) -- C:\WINDOWS\system32\qmgr.dll [409088]
O83 - Search Svchost Services: wuauserv (wuauserv) . (.Microsoft Corporation - Windows Update AutoUpdate Service.) -- C:\WINDOWS\system32\wuauserv.dll [6656]
O83 - Search Svchost Services: ShellHWDetection (ShellHWDetection) . (.Microsoft Corporation -

Dll des services Windows Shell.) -- C:\WINDOWS\system32\shsvcs.dll [135680]
O83 - Search Svchost Services: helpsvc (helpsvc) . (.Microsoft Corporation - Microsoft PCHealth Service Holder.) -- C:\WINDOWS\PCHealth\HelpCtr\Binaries\pchsvc.dll [38400]
O83 - Search Svchost Services: WmdmPmSN (WmdmPmSN) . (.Microsoft Corporation - Microsoft Media Device Service Provider.) -- C:\WINDOWS\system32\MsPMSNSv.dll [27136]
~ Scan Services in 00mn 00s

---\\ Recherche particuliere à la racine de certains dossiers (O84)
[MD5.0641A46F1E58529A42EAD4573A3A0861] [SPRF][15/02/2005] (...) -- C:\Documents and Settings\All Users\Application Data\F202D354F4.sys [8]
[MD5.C01EDE9438DFFA4B5D08CFE06B857B79] [SPRF][15/02/2005] (...) -- C:\Documents and Settings\All Users\Application Data\KGyGaAvL.sys [2516]
[MD5.21DC27FFF6928C90A304CAADC41D155A] [SPRF][02/03/2012] (.Pas de propriétaire - MainResource Module.) -- C:\Program Files\64res.dll [174024]
[MD5.77DFC08831C1B275C6D39F4A73F5693B] [SPRF][02/03/2012] (.MindSpark - MindSpark Toolbar Platform.) -- C:\Program Files\64Uninstall TelevisionFanatic.dll [693648]
~ Scan Files in 00mn 00s

---\\ Scan Additionnel (O88)
Database Version : 9199 - (30/09/2012)
Clés trouvées (Keys found) : 61
Valeurs trouvées (Values found) : 0
Dossiers trouvés (Folders found) : 6
Fichiers trouvés (Files found) : 0

[HKLM\Software\Classes\sim-packages] =>Toolbar.Agent
[HKLM\Software\Classes\suggestmeyes.suggestmeyesbho] =>Adware.PredictAd
[HKLM\Software\Classes\suggestmeyes.suggestmeyesbho.1] =>Adware.PredictAd
[HKLM\Software\Classes\sweetie.ietoolbar] =>Toolbar.SweetIM
[HKLM\Software\Classes\sweetie.ietoolbar.1] =>Toolbar.SweetIM
[HKLM\Software\Classes\sweetim_urlsearchhook.toolbarurlsearchhook] =>Toolbar.SweetIM
[HKLM\Software\Classes\sweetim_urlsearchhook.toolbarurlsearchhook.1] =>Toolbar.SweetIM
[HKLM\Software\Classes\Toolbar3.sweetie] =>Toolbar.SweetIM
[HKLM\Software\Classes\Toolbar3.sweetie.1] =>Toolbar.SweetIM
[HKLM\Software\Classes\TypeLib\{01bcb858-2f62-4f06-a8f4-48f927c15333}] =>Adware.PredictAd
[HKCU\Software\Microsoft\Internet Explorer\SearchScopes\{0ecdf796-c2dc-4d79-a620-cce0c0a66cc9}] =>Toolbar.Babylon
[HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{0FB6A909-6086-458F-BD92-1F8EE10042A0}] =>Adware.PredictAd
[HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{0FB6A909-6086-458F-BD92-1F8EE10042A0}] =>Adware.PredictAd
[HKLM\Software\Classes\CLSID\{0FB6A909-6086-458F-BD92-1F8EE10042A0}] =>Adware.PredictAd
[HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{0FB6A909-6086-458F-BD92-1F8EE10042A0}] =>Adware.PredictAd
[HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{2EECD738-5844-4A99-B4B6-146BF802613B}] =>Toolbar.Agent

[HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{2EECD738-5844-4A99-B4B6-146BF802613B}] =>Toolbar.Agent
[HKLM\Software\Classes\CLSID\{2EECD738-5844-4A99-B4B6-146BF802613B}] =>Toolbar.Agent
[HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{2EECD738-5844-4a99-B4B6-146BF802613B}] =>Toolbar.Babylon
[HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{2EECD738-5844-4a99-B4B6-146BF802613B}] =>Toolbar.Babylon
[HKLM\Software\Classes\CLSID\{2EECD738-5844-4a99-B4B6-146BF802613B}] =>Toolbar.Babylon
[HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\{2F603A45-D956-496B-81B5-50D782424976}] =>Toolbar.SweetIM
[HKLM\Software\Classes\AppID\{442f13bc-2031-42d5-9520-437f65271153}] =>Adware.PredictAd
[HKLM\Software\Classes\TypeLib\{4d3b167e-5fd8-4276-8fd7-9df19c1e4d19}] =>Toolbar.SweetIM
[HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{6E13DDE1-2B6E-46CE-8B66-DC8BF36F6B99}] =>Toolbar.Conduit
[HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{6E13DDE1-2B6E-46CE-8B66-DC8BF36F6B99}] =>Toolbar.Conduit
[HKLM\Software\Classes\CLSID\{82ac53b4-164c-4b07-a016-437a8388b81a}] =>Toolbar.SweetIM
[HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{98889811-442D-49dd-99D7-DC866BE87DBC}] =>Toolbar.Babylon
[HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{98889811-442D-49dd-99D7-DC866BE87DBC}] =>Toolbar.Babylon
[HKLM\Software\Classes\Interface\{A439801C-961D-452C-AB42-7848E9CBD289}] =>Toolbar.Babylon
[HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{A6174F27-1FFF-E1D6-A93F-BA48AD5DD448}] =>PUP.DealPly
[HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{A6174F27-1FFF-E1D6-A93F-BA48AD5DD448}] =>PUP.DealPly
[HKLM\Software\Classes\AppID\{BDB69379-802F-4EAF-B541-F8DE92DD98DB}] =>Adware.CDNHelper
[HKLM\Software\Classes\AppID\{BDB69379-802F-4eaf-B541-F8DE92DD98DB}] =>Toolbar.Babylon
[HKLM\Software\Classes\Interface\{c9ae652b-8c99-4ac2-b556-8b501182874e}] =>Adware.PredictAd
[HKLM\Software\Classes\CLSID\{E46C8196-B634-44a1-AF6E-957C64278AB1}] =>Toolbar.Babylon
[HKLM\Software\Classes\Interface\{eee6c358-6118-11dc-9c72-001320c79847}] =>Toolbar.SweetIM
[HKLM\Software\Classes\Interface\{EEE6C35A-6118-11DC-9C72-001320C79847}] =>Adware.BHO
[HKLM\Software\Classes\Interface\{eee6c35a-6118-11dc-9c72-001320c79847}] =>Toolbar.SweetIM
[HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{eee6c35b-6118-11dc-9c72-001320c79847}] =>Toolbar.SweetIM
[HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{eee6c35b-6118-11dc-9c72-001320c79847}] =>Toolbar.SweetIM
[HKLM\Software\Classes\CLSID\{eee6c35b-6118-11dc-9c72-001320c79847}] =>Toolbar.SweetIM

[HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{EEE6C35C-6118-11DC-9C72-001320C79847}] =>Adware.BHO
[HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{EEE6C35C-6118-11DC-9C72-001320C79847}] =>Adware.BHO
[HKLM\Software\Classes\CLSID\{EEE6C35C-6118-11DC-9C72-001320C79847}] =>Adware.BHO
[HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{EEE6C35C-6118-11DC-9C72-001320C79847}] =>Adware.BHO
[HKLM\Software\Classes\CLSID\{EEE6C35D-6118-11DC-9C72-001320C79847}] =>Adware.BHO
[HKLM\Software\Classes\TypeLib\{eee6c35e-6118-11dc-9c72-001320c79847}] =>Toolbar.SweetIM
[HKLM\Software\Classes\TypeLib\{eee6c35f-6118-11dc-9c72-001320c79847}] =>Toolbar.SweetIM
[HKCU\Software\Microsoft\Internet Explorer\SearchScopes\{eee6c360-6118-11dc-9c72-001320c79847}] =>Toolbar.SweetIM
[HKLM\Software\Microsoft\Internet Explorer\SearchScopes\{eee6c360-6118-11dc-9c72-001320c79847}] =>Toolbar.SweetIM
[HKLM\Software\Microsoft\Internet Explorer\Low Rights\ElevationPolicy\{EEE6C367-6118-11DC-9C72-001320C79847}] =>Toolbar.SweetIM
[HKLM\Software\Classes\Interface\{F4EBB1E2-21F3-4786-8CF4-16EC5925867F}] =>Toolbar.Babylon
[HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{F9639E4A-801B-4843-AEE3-03D9DA199E77}] =>Toolbar.Conduit
[HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{F9639E4A-801B-4843-AEE3-03D9DA199E77}] =>Toolbar.Conduit
[HKCU\Software\Microsoft\Internet Explorer\MenuExt\&search] =>Adware.BHO
[HKCU\Software\freetvradio] =>Adware.SPointer
[HKCU\Software\OfferBox] =>PUP.OfferBox
[HKLM\Software\OfferBox] =>PUP.OfferBox
[HKCU\Software\SweetIM] =>Toolbar.SweetIM
[HKLM\Software\SweetIM] =>Toolbar.SweetIM
C:\Program Files\freeTVRadio =>Adware.SPointer
C:\Program Files\SweetIM =>Toolbar.SweetIM
C:\Documents and Settings\user\Application Data\Babylon =>Toolbar.Babylon
C:\Documents and Settings\user\Application Data\freeTVRadio =>Adware.SPointer
C:\Documents and Settings\user\Application Data\OfferBox =>PUP.OfferBox
C:\Documents and Settings\user\Local Settings\Application Data\freetvradio Air =>Adware.SPointer
~ Scan Additionnel in 00mn 10s

---\\ Etat général des services non Microsoft (EGS) (SR=Running, SS=Stopped)
SS - | Demand 22/09/2012 250288 | (AdobeFlashPlayerUpdateSvc) . (.Adobe Systems Incorporated.) - C:\WINDOWS\system32\Macromed\Flash\FlashPlayerUpdateService.exe
SR - | Auto 21/08/2012 44808 | (avast! Antivirus) . (.AVAST Software.) - C:\Program Files\Alwil Software\Avast5\AvastSvc.exe
SS - | Demand 13/04/2008 225280 | (dmadmin) . (.Microsoft Corp., Veritas Software.) - C:\WINDOWS\system32\dmadmin.exe
SS - | Auto 16/12/2010 136176 | (gupdate) . (.Google Inc..) - C:\Program Files\Google\Update\GoogleUpdate.exe

SS - | Demand 16/12/2010 136176 | (gupdatem) . (.Google Inc..) - C:\Program Files\Google\Update\GoogleUpdate.exe
SR - | Auto 13/07/2012 153392 | (JavaQuickStarterService) . (.Sun Microsystems, Inc..) - C:\Program Files\Java\jre6\bin\jqs.exe
SR - | Auto 537520 | (lxct_device) . (...) - C:\WINDOWS\system32\lxctcoms.exe
SS - | Demand 15/01/2010 227232 | (McComponentHostService) . (.McAfee, Inc..) - C:\Program Files\McAfee Security Scan\2.0.181\McCHSvc.exe
SR - | Auto 11/03/2010 193824 | (PSI_SVC_2) . (.Protexis Inc..) - C:\Program Files\Fichiers communs\Protexis\License Service\PsiService_2.exe
SS - | Demand 26/09/2011 18432 | (wampapache) . (.Apache Software Foundation.) - c:\wamp\bin\apache\apache2.2.21\bin\httpd.exe
SS - | Demand 8176640 | (wampmysqld) . (...) - c:\wamp\bin\mysql\mysql5.5.20\bin\mysqld.exe
SR - | Auto 188760 | (Web Assistant Updater) . (...) - C:\Program Files\Web Assistant\ExtensionUpdaterService.exe
SR - | Auto 1006448 | (WebOptimizer) . (...) - C:\WINDOWS\system32\dmwu.exe
~ Scan Services in 00mn 10s

End of the scan (1180 lines in 00mn 25s)(0)