~ Rapport de ZHPDiag v2015.2.2.15 - Nicolas Coolman (02/02/2015)
~ Lancé par Lucie (05/02/2015 18:00:30)
~ Facebook : https://www.facebook.com/nicolascoolman1
~ Adresse du Forum http://forum.nicolascoolman.fr
~ Traduit par Nicolas Coolman
~ Etat de la version : Version à jour.
~ Liste blanche : Désactivée par l'utilisateur
~ Elévation des Privilèges : OK
~ User Account Control (UAC): Activate by user

---\\ Navigateurs Internet
MSIE: Internet Explorer v11.0.9600.17498
MFIE: Mozilla Firefox 28.0
GCIE: Google Chrome v40.0.2214.94 (Defaut)

---\\ Informations sur les produits Windows
~ Langage: Français
Windows Server License Manager Script : OK
~ Windows(R) Operating System, OEM_DM channel
Windows ID Activation : OK
~ Windows Partial Key : 7CBQ6
Windows License : OK
~ Windows Remaining Initializations Number : 1000
Software Protection Service (Protection logicielle) : OK
Windows Automatic Updates : OK
Windows Activation Technologies : OK
Windows 8.1, 64-bit (Build 9600)

---\\ Logiciels de protection du système
avast! Free Antivirus v9.0.2021
Malwarebytes Anti-Malware version 2.0.4.1028
Windows Defender W8 (Deactivate)

---\\ Logiciels d'optimisation du système
CCleaner v4.19

---\\ Logiciels de partage PeerToPeer

---\\ Surveillance de Logiciels
Adobe Flash Player 16 NPAPI
Adobe Reader XI

---\\ Informations sur le système
~ Processor: Intel64 Family 6 Model 58 Stepping 9, GenuineIntel
~ Operating System: 64 Bits
Boot mode: Normal (Normal boot)
Total RAM: 3891 MB (51% free)
System Restore: Activé (Enable)
System drive C: has 587 GB (86%) free of 682 GB

---\\ Mode de connexion au système
~ Computer Name: LUCIE
~ User Name: Lucie

~ All Users Names: Lucie, Administrateur,
~ Unselected Option: None
Logged in as Administrator

---\\ Variables d'environnement
~ System Unit : C:\
~ %AppZHP% : C:\Users\Lucie\AppData\Roaming\ZHP\
~ %AppData% : C:\Users\Lucie\AppData\Roaming\
~ %Desktop% : C:\Users\Lucie\Desktop\
~ %Favorites% : C:\Users\Lucie\Favorites\
~ %LocalAppData% : C:\Users\Lucie\AppData\Local\
~ %StartMenu% : C:\Users\Lucie\AppData\Roaming\Microsoft\Windows\Start Menu\
~ %Windir% : C:\Windows\
~ %System% : C:\Windows\System32\

---\\ Enumération des unités disques
C: Hard drive, Flash drive, Thumb drive (Free 587 Go of 682 Go)
D: CD-ROM drive (Free 0 Go of 0 Go)

---\\ Etat du Centre de Sécurité Windows
[HKLM\SOFTWARE\Microsoft\Security Center\Svc] AntiSpywareOverride: OK
[HKLM\SOFTWARE\Microsoft\Security Center\Svc] AntiVirusOverride: OK
[HKLM\SOFTWARE\Microsoft\Security Center\Svc] FirewallOverride: OK
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer] NoActiveDesktopChanges: Modified
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system] EnableLUA: OK
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\NOHIDDEN] CheckedValue: OK
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL] CheckedValue: OK
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Associations] Application: OK
[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] Shell: OK
[HKLM\SYSTEM\CurrentControlSet\Services\COMSysApp] Type: OK
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\Results\Install] LastSuccessTime : OK
~ Security Center: 49 Scanned in 00mn 00s

---\\ Recherche particulière de fichiers génériques
[MD5.ACDBE1ED38167C8B01B8F63161BB2CEA] - (.Microsoft Corporation - Explorateur Windows.) (.23/08/2014 - 08:48:28.) -- C:\Windows\Explorer.exe [2374784]
[MD5.48CFA7BE561A7BE144C29BB912055016] - (.Microsoft Corporation - Application de démarrage de Windows.) (.22/08/2013 - 10:58:29.) -- C:\Windows\System32\Wininit.exe [144384]
[MD5.4AF089160FE082E5EA5C4AA72782DCA2] - (.Microsoft Corporation - Extensions Internet pour Win32.) (.22/11/2014 - 02:28:21.) -- C:\Windows\System32\wininet.dll [2358272]

[MD5.306EB21E5B480AE9065EA55AC8C35936] - (.Microsoft Corporation - Application d'ouverture de session Windows.) (.24/09/2014 - 16:34:56.) -- C:\Windows\System32\Winlogon.exe [562176]
[MD5.AFCAB4DC692CCE37E283B00E2D7B438F] - (.Microsoft Corporation - Bibliothèque de licences.) (.24/09/2014 - 16:34:58.) -- C:\Windows\System32\sppcomapi.dll [447488]
[MD5.374E27295F0A9DCAA8FC96370F9BEEA5] - (.Microsoft Corporation - Pilote de fonction connexe pour WinSock.) (.24/09/2014 - 17:48:38.) -- C:\Windows\system32\Drivers\AFD.sys [563200]
[MD5.74B14192CF79A72F7536B27CB8814FBD] - (.Microsoft Corporation - ATAPI IDE Miniport Driver.) (.22/08/2013 - 13:43:41.) -- C:\Windows\system32\Drivers\atapi.sys [26464]
[MD5.2FA6510E33F7DEFEC03658B74101A9B9] - (.Microsoft Corporation - CD-ROM File System Driver.) (.22/08/2013 - 12:40:15.) -- C:\Windows\system32\Drivers\Cdfs.sys [88576]
[MD5.C6796EA22B513E3457514D92DCDB1A3D] - (.Microsoft Corporation - SCSI CD-ROM Driver.) (.22/08/2013 - 09:46:35.) -- C:\Windows\system32\Drivers\Cdrom.sys [164352]
[MD5.A03F362C5557E238CBFA914689C77248] - (.Microsoft Corporation - DFS Namespace Client Driver.) (.24/09/2014 - 17:03:07.) -- C:\Windows\system32\Drivers\DfsC.sys [134144]
[MD5.D4B7ED39C7900384D9E5C1283F1E7926] - (.Microsoft Corporation - High Definition Audio Bus Driver.) (.24/09/2014 - 16:44:42.) -- C:\Windows\system32\Drivers\HDAudBus.sys [76800]
[MD5.84CFC5EFA97D0C965EDE1D56F116A541] - (.Microsoft Corporation - Pilote de port i8042.) (.22/08/2013 - 12:39:15.) -- C:\Windows\system32\Drivers\i8042prt.sys [107520]
[MD5.B7342B3C58E91107F6E946A93D9D4EFD] - (.Microsoft Corporation - IP Network Address Translator.) (.24/09/2014 - 16:35:02.) -- C:\Windows\system32\Drivers\IpNat.sys [142848]
[MD5.7A1A3F213CDB3363D179D5014272025D] - (.Microsoft Corporation - Minirdr SMB Windows NT.) (.30/04/2014 - 07:41:46.) -- C:\Windows\system32\Drivers\MRxSmb.sys [402432]
[MD5.0217532E19A748F0E5D569307363D5FD] - (.Microsoft Corporation - MBT Transport driver.) (.22/08/2013 - 12:37:02.) -- C:\Windows\system32\Drivers\netBT.sys [282624]
[MD5.038C77D577900EE39410662478BB0D50] - (.Microsoft Corporation - Pilote du système de fichiers NT.) (.24/09/2014 - 16:44:43.) -- C:\Windows\system32\Drivers\ntfs.sys [2009920]
[MD5.764B1121867B2D9B31C491668AC72B2B] - (.Microsoft Corporation - Pilote de port parallèle.) (.22/08/2013 - 12:40:02.) -- C:\Windows\system32\Drivers\Parport.sys [94208]
[MD5.BBB6272B7F46C4640A8CDB8A70C3450F] - (.Microsoft Corporation - RAS L2TP mini-port/call-manager driver.) (.22/08/2013 - 12:35:51.) -- C:\Windows\system32\Drivers\Rasl2tp.sys [120832]
[MD5.680C1DAE268B6FB67FA21B389A8B79EF] - (.Microsoft Corporation - Redirecteur de périphérique de Microsoft RDP.) (.24/09/2014 - 16:03:44.) -- C:\Windows\system32\Drivers\rdpdr.sys [195584]
[MD5.FFF28F9F6823EB1756C60F1649560BBF] - (.Microsoft Corporation - TDI Translation Driver.) (.22/08/2013 - 14:25:35.) -- C:\Windows\system32\Drivers\tdx.sys [107520]
[MD5.64CA2B4A49A8EAF495E435623ECCE7DB] - (.Microsoft Corporation - Pilote de cliché instantané du volume.) (.24/09/2014 - 16:44:42.) -- C:\Windows\system32\Drivers\volsnap.sys [310080]

~ Generic Processes: Scanned in 00mn 00s

---\\ Etat des fichiers cachés (Caché/Total)
~ Mes images (My Pictures) : 1/187
~ Mes musiques (My Musics) : 1/8
~ Mes Videos (My Videos) : 1/76
~ Mes Favoris (My Favorites) : 1/7
~ Mes Documents (My Documents) : 6/2489
~ Mon Bureau (My Desktop) : 1/46
~ Menu demarrer (Programs) : 1/30
~ Hidden Files: Scanned in 00mn 05s

---\\ Processus lancés
[MD5.0EFF23C3D910380746D4F56BA5C746C4] - (.Dritek System Inc. - Launch Manager.) -- C:\Program Files (x86)\Launch Manager\LManager.exe [1192784] [PID.2200]
[MD5.3C13F26A4766752314A5413038BD86B4] - (.Malwarebytes Corporation - Malwarebytes Anti-Malware.) -- C:\Program Files (x86)\Malwarebytes Anti-Malware\mbam.exe   [7229752] [PID.2724]
[MD5.8BE1C89BD0C6F659C3AE3A2C8D0955C4] - (.Microsoft Corporation - Run Once Wrapper.) -- C:\WINDOWS\SysWOW64\runonce.exe   [36864] [PID.3644]
[MD5.54B3866E6741B34F3FB1BA6B18F607EB] - (.Microsoft Corporation - Microsoft ® Windows Based Script Host.) -- C:\Windows\SysWOW64\wscript.exe   [133120] [PID.3920]
[MD5.E659E38D2D51DF5817C91D7386920C7E] - (.CyberLink - MediaEspresso DeviceDetector.) -- C:\Program Files (x86)\CyberLink\MediaEspresso\DeviceDetector\DeviceDetector.exe [995856] [PID.2056]
[MD5.749E4BF1FA6DB8C3F9C2B7F29A544F95] - (.Google Inc. - Google Chrome.) -- C:\Program Files (x86)\Google\Chrome\Application\chrome.exe   [843592] [PID.1756]
[MD5.BE52EDAADE29AC59681B6CD60E257C92] - (.Nicolas Coolman - ZHPDiag.) -- C:\Program Files (x86)\ZHPDiag\ZHPDiag.exe   [8158720] [PID.748]
~ Processes Running: Scanned in 00mn 01s

---\\ Google Chrome, Démarrage,Recherche,Extensions (G0,G1,G2)
C:\Users\Lucie\AppData\Local\Google\Chrome\User Data\Default\Preferences

---\\ Liste des dossiers d'extension Google Chrome
~ Google Lines Browser: 0 Scanned in 00mn 04s

---\\ Mozilla Firefox, Plugins,Demarrage,Recherche,Extensions (P2,M0,M1,M2,M3)
C:\Users\Lucie\AppData\Roaming\Mozilla\Firefox\Profiles\1rsinrsv.default\prefs.js

```
M3 - MFPP: Plugins - [Lucie] --
C:\Users\Lucie\AppData\Roaming\Mozilla\Firefox\Profiles\1rsinrsv.default\
searchplugins\Binkiland.xml
M3 - MFPP: Plugins - [Lucie] --
C:\Users\Lucie\AppData\Roaming\Mozilla\Firefox\Profiles\1rsinrsv.default\
searchplugins\yahoo-msd.xml
M0 - MFSP: prefs.js [Lucie - 1rsinrsv.default] http://binkiland.com
M2 - MFEP: prefs.js [Lucie - 1rsinrsv.default\{b9db16a4-6edc-47ec-a1f4-
b86292ed211d}] [dwhelper] DownloadHelper v4.9.24 (..)
P2 - FPN: [HKLM] [@adobe.com/FlashPlayer] - (...) --
C:\WINDOWS\system32\Macromed\Flash\NPSWF64_16_0_0_305.dll
P2 - FPN: [HKLM] [@mcafee.com/MSC,version=10] - (...) -- C:\Program
Files\mcafee\msc\npMcSnFFPl64.dll (.not file.)
P2 - FPN: [HKLM] [@Microsoft.com/NpCtrl,version=1.0] - (. Microsoft
Corporation - 5.1.30514.0.) -- c:\Program Files\Microsoft
Silverlight\5.1.30514.0\npctrl.dll
~ Firefox Browser: 7 Scanned in 00mn 00s



---\\ Internet Explorer, Démarrage,Recherche,URLSearchHook, Phishing
(R0,R1,R3,R4)
R0 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page =
http://binkiland.com
R0 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page =
http://www.google.com
R0 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main,Start
Page = http://go.microsoft.com
R1 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Search Page =
http://go.microsoft.com
R1 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Default_Page_URL =
http://acer13.msn.com
R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Search Page =
http://go.microsoft.com
R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Default_Page_URL =
http://go.microsoft.com
R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Extensions Off Page =
about:noadd-ons
R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Security Risk Page =
about:securityrisk
R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Default_Search_URL =
http://go.microsoft.com
R1 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main,Search
Page = http://go.microsoft.com
R1 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet
Explorer\Main,Default_Page_URL = http://go.microsoft.com
R1 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet
Explorer\Main,Default_Search_URL = http://go.microsoft.com
R1 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet
Explorer\Main,Extensions Off Page = about:noadd-ons
R1 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main,Security
Risk Page = about:securityrisk
R3 - URLSearchHook: Microsoft Url Search Hook [64Bits] - {CFBFAE00-17A6-
11D0-99CB-00C04FD64497} . (.Microsoft Corporation - Navigateur Internet.)
```

(11.00.9600.17496 (winblue_r5.141121-1500)) --
C:\Windows\SysWOW64\ieframe.dll
~ IE Browser: 16 Scanned in 00mn 00s

---\\ Internet Explorer, Proxy Management (R5)
R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings,ProxyServer = no key
R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings,ProxyEnable = 0
R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings,MigrateProxy = 1
R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings,EnableHttp1_1 = 1
R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings,AutoConfigProxy = wininet.dll
~ Proxy management: Scanned in 00mn 00s

---\\ Analyse des lignes F0, F1, F2, F3 - IniFiles, Autoloading programs
F2 - REG:system.ini: USERINIT=C:\Windows\system32\userinit.exe,
F2 - REG:system.ini: Shell=C:\Windows\explorer.exe
F2 - REG:system.ini:
VMApplet=C:\Windows\System32\SystemPropertiesPerformance.exe
~ Keys: Scanned in 00mn 00s

---\\ Hosts file redirection (O1)
~ Le fichier hôte est sain (The hosts file is clean) (21)
~ Hosts File: Scanned in 00mn 00s

---\\ Browser Helper Objects de navigateur (O2)
O2 - BHO: avast! Online Security [64Bits] - {8E5E2654-AD2D-48bf-AC2D-
D17F00898D06} . (.AVAST Software - IE Webrep plugin.) -- C:\Program
Files\AVAST Software\Avast\aswWebRepIE.dll
O2 - BHO: IESpeakDoc [64Bits] - {8D10F6C4-0E01-4BD4-8601-11AC1FDF8126}
Clé orpheline
~ BHO: 3 Scanned in 00mn 00s

---\\ Internet Explorer Toolbars (O3)
O3 - Toolbar: (no name) - [HKLM]{318A227B-5E9F-45bd-8999-7F8F10CA4CF5}
Clé orpheline
~ Toolbar: Scanned in 00mn 00s

---\\ Autres liens utilisateurs (O4)

O4 - GS\Desktop [Public]: Acheter en ligne.lnk . (...) -- C:\Program Files (x86)\Accessory Store\StartUrl.exe (.not file.)
O4 - GS\Desktop [Public]: Configuration de la Livebox.lnk . (.SAGEM - Pas de description.) -- C:\Program Files (x86)\SAGEM\SAGEM F@st 3202\RunHttpCfg.exe C:\Program Files (x86)\SAGEM\SAGEM F@st 3202\RunHttpCfg.exe -I -L040C
~ Global Startup: 2 Scanned in 00mn 03s

---\\ Applications lancées au démarrage du système (O4)
O4 - HKLM\..\Run: [RtHDVCpl] . (.Realtek Semiconductor - Gestionnaire audio HD Realtek.) -- C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe =>.Realtek Semiconductor Corp
O4 - HKLM\..\Run: [RtHDVBg_Dolby] . (.Realtek Semiconductor - HD Audio Background Process.) -- C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe
O4 - HKLM\..\Run: [HotKeysCmds] C:\Windows\system32\hkcmd.exe (.not file.)
O4 - HKLM\..\Run: [Persistence] C:\Windows\system32\igfxpers.exe (.not file.)
O4 - HKLM\..\Run: [BtPreLoad] . (...) -- C:\Program Files (x86)\Bluetooth Suite\BtPreLoad.exe
O4 - HKLM\..\Run: [SynTPEnh] C:\Program Files (x86)\Synaptics\SynTP\SynTPEnh.exe (.not file.)
O4 - HKCU\..\Run: [Spotify Web Helper] . (.Spotify Ltd - SpotifyWebHelper.) -- C:\Users\Lucie\AppData\Roaming\Spotify\Data\SpotifyWebHelper.exe
O4 - HKCU\..\Run: [CCleaner Monitoring] . (.Piriform Ltd - CCleaner.) -- C:\Program Files\CCleaner\CCleaner64.exe   =>.Piriform Ltd
O4 - HKCU\..\Run: [GarminExpressTrayApp] . (.Garmin Ltd or its subsidiaries - Express Tray.) -- C:\Program Files (x86)\Garmin\Express Tray\ExpressTray.exe
O4 - HKCU\..\Run: [GoogleChromeAutoLaunch_9752FD91EC81386F8187715A319E4BE7] . (.Google Inc. - Google Chrome.) -- C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
O4 - HKLM\..\Wow6432Node\Run: [mcui_exe] C:\Program Files\McAfee.com\Agent\mcagent.exe (.not file.)
O4 - HKLM\..\Wow6432Node\Run: [LManager] Clé orpheline
O4 - HKLM\..\Wow6432Node\Run: [RadioController] . (.Dritek System Inc. - RF Button Helper.) -- C:\Program Files (x86)\RadioController\RfBtnHelper.exe
O4 - HKLM\..\Wow6432Node\Run: [Dolby Advanced Audio v2] . (.Dolby Laboratories Inc. - Dolby Profile Selector.) -- C:\Dolby PCEE4\pcee4.exe
O4 - HKLM\..\Wow6432Node\Run: [Norton Online Backup] . (.Symantec Corporation - Norton Online Backup Service.) -- C:\Program Files (x86)\Symantec\Norton Online Backup\NOBuClient.exe   =>.Symantec Corporation
O4 - HKLM\..\Wow6432Node\Run: [AvastUI.exe] . (.AVAST Software - avast! Antivirus.) -- C:\Program Files\AVAST Software\Avast\AvastUI.exe
O4 - HKLM\..\Wow6432Node\Run: [iTunesHelper] . (.Apple Inc. - iTunesHelper.) -- C:\Program Files (x86)\iTunes\iTunesHelper.exe

```
O4 - HKLM\..\Wow6432Node\RunOnce: [Malwarebytes Anti-Malware (cleanup)] .
(.Malwarebytes Corporation - Malwarebytes Anti-Malware.) --
C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\mbamdor.exe
O4 - HKUS\S-1-5-21-432611429-936888870-1252711551-1001\..\Run: [Spotify
Web Helper] . (.Spotify Ltd - SpotifyWebHelper.) --
C:\Users\Lucie\AppData\Roaming\Spotify\Data\SpotifyWebHelper.exe
O4 - HKUS\S-1-5-21-432611429-936888870-1252711551-1001\..\Run: [CCleaner
Monitoring] . (.Piriform Ltd - CCleaner.) -- C:\Program
Files\CCleaner\CCleaner64.exe   =>.Piriform Ltd
O4 - HKUS\S-1-5-21-432611429-936888870-1252711551-1001\..\Run:
[GarminExpressTrayApp] . (.Garmin Ltd or its subsidiaries - Express
Tray.) -- C:\Program Files (x86)\Garmin\Express Tray\ExpressTray.exe
O4 - HKUS\S-1-5-21-432611429-936888870-1252711551-1001\..\Run:
[GoogleChromeAutoLaunch_9752FD91EC81386F8187715A319E4BE7] . (.Google Inc.
- Google Chrome.) -- C:\Program Files
(x86)\Google\Chrome\Application\chrome.exe
~ Application:  Scanned in 00mn 00s



---\\ Invisibilité de l'icône d'options IE dans le panneau de
Configuration (O5)
O5 - control.ini: [HKLM\..\Control Panel] inetcpl.cpl=no
~ IE Control Panel: 1 Scanned in 00mn 00s



---\\ Boutons situés sur la barre d'outils principale d'Internet Explorer
(O9)
O9 - Extra button: Send by Bluetooth to [64Bits] - {7815BE26-237D-41A8-
A98F-F7BD75F71086} -- Clé orpheline
~ IE Extra Buttons:  Scanned in 00mn 00s



---\\ Winsock hijacker (Layered Service Provider) (O10)
O10 - WLSP:\000000000001\Winsock LSP File . (.Microsoft Corporation -
Fournisseur Shim d’affectation de noms de messagerie.) --
C:\WINDOWS\system32\napinsp.dll
O10 - WLSP:\000000000002\Winsock LSP File . (.Microsoft Corporation -
Fournisseur d’espace de noms PNRP.) -- C:\WINDOWS\system32\pnrpnsp.dll
O10 - WLSP:\000000000003\Winsock LSP File . (.Microsoft Corporation -
Fournisseur d’espace de noms PNRP.) -- C:\WINDOWS\system32\pnrpnsp.dll
O10 - WLSP:\000000000004\Winsock LSP File . (.Microsoft Corporation -
Network Location Awareness 2.) -- C:\WINDOWS\system32\NLAapi.dll
O10 - WLSP:\000000000005\Winsock LSP File . (.Microsoft Corporation -
Fournisseur de service Sockets 2.0 de Microsoft Windows.) --
C:\WINDOWS\system32\mswsock.dll  =>.Microsoft Corporation
O10 - WLSP:\000000000006\Winsock LSP File . (.Microsoft Corporation -
LDAP RnR Provider DLL.) -- C:\WINDOWS\system32\winrnr.dll
O10 - WLSP:\000000000007\Winsock LSP File . (.Microsoft Corporation -
Windows Sockets Helper DLL.) -- C:\WINDOWS\system32\wshbth.dll
O10 - WLSP:\000000000008\Winsock LSP File . (.Apple Inc. - Bonjour
Namespace Provider.) -- C:\Program Files (x86)\Bonjour\mdnsNSP.dll
```

~ Winsock: 8 Scanned in 00mn 00s

---\\ Modification Domaine/Adresses DNS (O17)
O17 - HKLM\System\CCS\Services\Tcpip\..\{3AB67817-4829-41F0-AAA6-F3A8341B7167}: DhcpNameServer = 192.168.1.1
O17 - HKLM\System\CS1\Services\Tcpip\..\{3AB67817-4829-41F0-AAA6-F3A8341B7167}: DhcpNameServer = 192.168.1.1
O17 - HKLM\System\CCS\Services\Tcpip\Parameters: DhcpNameServer = 192.168.1.1
~ Domain: Scanned in 00mn 00s

---\\ Protocole additionnel (O18)
O18 - Handler: wlpg [64Bits] - {E43EF6CD-A37A-4A9B-9E6F-83F89B8E6324} . (...) --
O18 - Filter: application/x-msdownload [64Bits] - {1E66F26B-79EE-11D2-8710-00C04F79ED0D} . (.Microsoft Corporation - Microsoft .NET Runtime Execution Engine.) -- C:\Windows\System32\mscoree.dll =>.Microsoft Corporation
~ Protocole Additionnel: Scanned in 00mn 00s

---\\ Clé de Registre autorun ShellServiceObjectDelayLoad (SSO/SSODL) (O21)
O21 - SSODL: WebCheck - {E6FB5E20-DE35-11CF-9C87-00AA005127ED} - CLSID or File not found.
~ SSODL: 1 Scanned in 00mn 00s

---\\ Liste des services NT non Microsoft et non désactivés (O23)
O23 - Service: Adobe Acrobat Update Service (AdobeARMservice) . (.Adobe Systems Incorporated - Adobe Acrobat Update Service.) - C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe
O23 - Service: Apple Mobile Device (Apple Mobile Device) . (.Apple Inc. - YSLoader.exe.) - C:\Program Files (x86)\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe
O23 - Service: AtherosSvc (AtherosSvc) . (.Qualcomm Atheros Commnucations - AdminService Application.) - C:\Program Files (x86)\Bluetooth Suite\adminservice.exe
O23 - Service: avast! Antivirus (avast! Antivirus) . (.AVAST Software - avast! Service.) - C:\Program Files\AVAST Software\Avast\AvastSvc.exe
O23 - Service: Service Bonjour (Bonjour Service) . (.Apple Inc. - Bonjour Service.) - C:\Program Files\Bonjour\mDNSResponder.exe
O23 - Service: CCDMonitorService (CCDMonitorService) . (.Acer Incorporated - CCD Monitor Service.) - C:\Program Files (x86)\Acer\Acer Cloud\CCDMonitorService.exe
O23 - Service: Dritek WMI Service (DsiWMIService) . (.Dritek System Inc. - Dritek WMI Service.) - C:\Program Files (x86)\Launch Manager\dsiwmis.exe

```
O23 - Service: GamesAppIntegrationService (GamesAppIntegrationService) .
(.WildTangent - WildTangent Games App Integration Service.) - C:\Program
Files (x86)\WildTangent Games\App\GamesAppIntegrationService.exe
O23 - Service: Garmin Core Update Service (Garmin Core Update Service) .
(.Garmin Ltd or its subsidiaries - Garmin Core Update Service.) -
C:\Program Files (x86)\Garmin\Core Update
Service\Garmin.Cartography.MapUpdate.CoreService.exe
O23 - Service: Service Google Update (gupdate) (gupdate) . (.Google Inc.
- Programme d'installation de Google.) - C:\Program Files
(x86)\Google\Update\GoogleUpdate.exe  =>.Google Inc
O23 - Service: IconMan_R (IconMan_R) . (.Realsil Microelectronics Inc. -
Realtek Card Reader Patch Tool..) - C:\Program Files
(x86)\Realtek\Realtek PCIE Card Reader\RIconMan.exe
O23 - Service: Intel(R) HD Graphics Control Panel Service
(igfxCUIService1.0.0.0) . (.Intel Corporation - igfxCUIService Module.) -
C:\Windows\System32\igfxCUIService.exe
O23 - Service: Intel(R) Capability Licensing Service Interface (Intel(R)
Capability Licensing Service Interface) . (.Intel(R) Corporation -
Intel(R) Capability Licensing Service Inter.) - C:\Program
Files\Intel\iCLS Client\HeciServer.exe
O23 - Service: Intel(R) Dynamic Application Loader Host Interface Service
(jhi_service) . (.Intel Corporation - Intel(R) Dynamic Application Loader
Host In.) - C:\Program Files (x86)\Intel\Intel(R) Management Engine
Components\DAL\jhi_service.exe
O23 - Service: Intel(R) Management and Security Application Local
Manageme (LMS) . (.Intel Corporation - Local Manageability Service.) -
C:\Program Files (x86)\Intel\Intel(R) Management Engine
Components\LMS\LMS.exe
O23 - Service:  (MBAMScheduler) . (.Malwarebytes Corporation -
Malwarebytes Anti-Malware.) - C:\Program Files (x86)\Malwarebytes Anti-
Malware\mbamscheduler.exe
O23 - Service:  (MBAMService) . (.Malwarebytes Corporation - Malwarebytes
Anti-Malware.) - C:\Program Files (x86)\Malwarebytes Anti-
Malware\mbamservice.exe
O23 - Service: Nero Update (NAUpdate) . (.Nero AG - NeroUpdate.) -
C:\Program Files (x86)\Nero\Update\NASvc.exe
O23 - Service: Norton Online Backup (NOBU) . (.Symantec Corporation -
Norton Online Backup Service.) - C:\Program Files (x86)\Symantec\Norton
Online Backup\NOBuAgent.exe  =>.Symantec Corporation
O23 - Service: NTI IScheduleSvc (NTI IScheduleSvc) . (.NTI Corporation -
Backup Manager Module.) - C:\Program Files (x86)\NTI\Acer Backup
Manager\IScheduleSvc.exe
O23 - Service: Dritek RF Button Command Service (RfButtonDriverService) .
(.Dritek System INC. - RfBtnSvc Application.) - C:\Windows\RfBtnSvc64.exe
O23 - Service: Intel(R) Management and Security Application User
Notificat (UNS) . (.Intel Corporation - User Notification Service.) -
C:\Program Files (x86)\Intel\Intel(R) Management Engine
Components\UNS\UNS.exe
~ Services: 22 Scanned in 00mn 22s


---\\ Enumération Active Desktop & MHTML Editor (O24)
O24 - Default MHTML Editor: Last - .(...) -  (.not file.)
```

~ Desktop Component: 4 Scanned in 00mn 00s

---\\ Enumère les données de BootExecute (BEX) (O34)
O34 - HKLM BootExecute: (autocheck autochk *) - File not found
~ BEX: 1 Scanned in 00mn 00s

---\\ Tâches planifiées en automatique (O39)
[MD5.3E04F1E482357B1FC8B088197C3D9FF8] [APT] [Adobe Acrobat Update Task] (.Adobe Systems Incorporated.) -- C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe [1022152]
[MD5.080255CDCB878813B481B8C348D47D8E] [APT] [Adobe Flash Player Updater] (.Adobe Systems Incorporated.) -- C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe [267440]
[MD5.1E1324A5D695E8A8268D7D253282C761] [APT] [ALU] (...) -- C:\Program Files (x86)\Acer\Live Updater\updater.exe [3356816]
[MD5.BD0BA490E0300E859DB99DA3AB024371] [APT] [ALUAgent] (...) -- C:\Program Files (x86)\Acer\Live Updater\liveupdater_agent.exe [39568]
[MD5.1AD8512A5C40AD1A0558498D8E0AC2AA] [APT] [avast! Emergency Update] (.AVAST Software.) -- C:\Program Files\AVAST Software\Avast\AvastEmUpdate.exe [808448]
[MD5.E659E38D2D51DF5817C91D7386920C7E] [APT] [DeviceDetector] (.CyberLink.) -- C:\Program Files (x86)\CyberLink\MediaEspresso\DeviceDetector\DeviceDetector.exe [995856]
[MD5.4942FBE3BA93C1536EC775A0104C11E9] [APT] [EgisUpdate] (.Egis Technology Inc..) -- C:\Program Files\EgisTec IPS\EgisUpdate.exe [202832]
[MD5.1F43C67FE77AB9299D41D86066C0C732] [APT] [GarminUpdaterTask] (...) -- C:\Program Files (x86)\Garmin\Express Self Updater\ExpressSelfUpdater.exe [24920]
[MD5.506708142BC63DABA64F2D3AD1DCD5BF] [APT] [GoogleUpdateTaskMachineCore] (.Google Inc..) -- C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [116648]
[MD5.506708142BC63DABA64F2D3AD1DCD5BF] [APT] [GoogleUpdateTaskMachineUA] (.Google Inc..) -- C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [116648]
[MD5.773C84EA68CF5359A6B4C82D6A96A938] [APT] [PMMUpdate] (.Egis Technology Inc..) -- C:\Program Files\EgisTec IPS\PMMUpdate.exe [467024]
[MD5.CFDF0015D4DC1EE66B395054EB330B06] [APT] [Power Management] (.Acer Incorporated.) -- C:\Program Files\Acer\Acer Power Management\ePowerTray.exe [5314192]
[MD5.00000000000000000000000000000000] [APT] [{E11DADF4-CE16-4FD5-B5A8-D3BFD9276500}] (...) -- D:\start.exe (.not file.) [0]
[MD5.34EBD4FF6A24D86BB4716D6AFCC1A89B] [APT] [AppleSoftwareUpdate] (.Apple Inc..) -- C:\Program Files (x86)\Apple Software Update\SoftwareUpdate.exe [561984]
O39 - APT: Adobe Flash Player Updater - (.Adobe Systems Incorporated.) -- C:\Windows\Tasks\Adobe Flash Player Updater.job [1002]

O39 - APT: Adobe Flash Player Updater - (.Adobe Systems Incorporated.) -- C:\Windows\System32\Tasks\Adobe Flash Player Updater [1002]
O39 - APT: - (..) -- C:\Windows\Tasks\Binkiland tidi.job [776]
O39 - APT: GoogleUpdateTaskMachineCore - (.Google Inc..) -- C:\Windows\Tasks\GoogleUpdateTaskMachineCore.job [1084]
O39 - APT: GoogleUpdateTaskMachineCore - (.Google Inc..) -- C:\Windows\System32\Tasks\GoogleUpdateTaskMachineCore [1084]
O39 - APT: GoogleUpdateTaskMachineUA - (.Google Inc..) -- C:\Windows\Tasks\GoogleUpdateTaskMachineUA.job [1088]
O39 - APT: GoogleUpdateTaskMachineUA - (.Google Inc..) -- C:\Windows\System32\Tasks\GoogleUpdateTaskMachineUA [1088]
O39 - APT: - (..) -- C:\Windows\Tasks\Synaptics TouchPad Enhancements.job [264]
O39 - APT: - (..) -- C:\Windows\System32\Tasks\Synaptics TouchPad Enhancements [264]
~ Scheduled Task: 22 Scanned in 00mn 07s

---\\ Composants installés (ActiveSetup Installed Components) (O40)
O40 - ASIC: Microsoft Windows Media Player [64Bits] - >{22d6f312-b0f6-11d0-94ab-0080c74c7e95} . (.Microsoft Corporation - Ressources du Lecteur Windows Media.) -- C:\Windows\System32\wmploc.dll =>.Microsoft Corporation
O40 - ASIC: Microsoft Windows Media Player 12.0 [64Bits] - {22d6f312-b0f6-11d0-94ab-0080c74c7e95} . (.Microsoft Corporation - Windows Media Player Extension.) -- C:\Windows\SysWOW64\wmpdxm.dll =>.Microsoft Corporation
O40 - ASIC: Themes Setup [64Bits] - {2C7339CF-2B09-4501-B3F3-F3508C9228ED} . (.Microsoft Corporation - API Windows Theme.) -- C:\Windows\System32\themeui.dll
O40 - ASIC: Microsoft Windows [64Bits] - {44BBA840-CC51-11CF-AAFA-00AA00B6015C} . (.Microsoft Corporation - Windows Mail.) -- C:\Program Files (x86)\Windows Mail\WinMail.exe =>.Microsoft Corporation
O40 - ASIC: Browsing Enhancements [64Bits] - {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 [64Bits] - {6BF52A52-394A-11d3-B153-00C04F79FAA6} . (.Microsoft Corporation - Ressources du Lecteur Windows Media.) -- C:\Windows\System32\wmploc.dll =>.Microsoft Corporation
O40 - ASIC: Windows Desktop Update [64Bits] - {89820200-ECBD-11cf-8B85-00AA005B4340} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\Windows\System32\shell32.dll
O40 - ASIC: Web Platform Customizations [64Bits] - {89820200-ECBD-11cf-8B85-00AA005B4383} . (.Microsoft Corporation - Utilitaire d'initialisation d'Internet Explorer par utilisateur.) -- C:\Windows\System32\ie4uinit.exe
O40 - ASIC: (no name) [64Bits] - {89B4C1CD-B018-4511-B0A1-5476DBF70820} . (.Microsoft Corporation - Microsoft .NET IE SECURITY REGISTRATION.) -- C:\Windows\System32\mscories.dll
~ Active Setup: 9 Scanned in 00mn 00s

---\\ Pilotes lancés au démarrage du système (O41)
O41 - Driver: C:\Windows\System32\drivers\afd.sys (AFD) . (.Microsoft Corporation - Pilote de fonction connexe pour WinSock.) - C:\Windows\system32\drivers\afd.sys
O41 - Driver: C:\Windows\System32\drivers\ahcache.sys (ahcache) . (.Microsoft Corporation - Application Compatibility Cache.) - C:\Windows\System32\DRIVERS\ahcache.sys
O41 - Driver: (aswRdr) . (.AVAST Software - avast! WFP Redirect Driver.) - C:\Windows\system32\drivers\aswRdr2.sys
O41 - Driver: (aswSnx) . (.AVAST Software - avast! Virtualization Driver.) - C:\Windows\system32\drivers\aswSnx.sys
O41 - Driver: (aswSP) . (.AVAST Software - avast! self protection module.) - C:\Windows\system32\drivers\aswSP.sys
O41 - Driver: (BasicDisplay) . (.Microsoft Corporation - Microsoft Basic Display Driver.) - C:\Windows\system32\drivers\BasicDisplay.sys
O41 - Driver: (BasicRender) . (.Microsoft Corporation - Microsoft Basic Render Driver.) - C:\Windows\system32\drivers\BasicRender.sys
O41 - Driver: (ccSet_NARA) . (.Symantec Corporation - Common Client Settings Driver.) - C:\Windows\system32\drivers\NARAx64\0401000.00E\ccSetx64.sys
O41 - Driver: cdrom.inf (cdrom) . (.Microsoft Corporation - SCSI CD-ROM Driver.) - C:\Windows\system32\drivers\cdrom.sys
O41 - Driver: C:\Windows\System32\drivers\dam.sys (dam) . (.Microsoft Corporation - DAM Kernel Driver.) - C:\Windows\System32\drivers\dam.sys
O41 - Driver: C:\Windows\System32\wkssvc.dll (Dfsc) . (.Microsoft Corporation - DFS Namespace Client Driver.) - C:\Windows\System32\Drivers\dfsc.sys
O41 - Driver: mssmbios.inf (mssmbios) . (.Microsoft Corporation - System Management BIOS Driver.) - C:\Windows\system32\drivers\mssmbios.sys
O41 - Driver: (mwlPSDFilter) . (.Egis Technology Inc. - PSD Mini Filter Driver.) - C:\Windows\System32\DRIVERS\mwlPSDFilter.sys
O41 - Driver: (mwlPSDNServ) . (.Egis Technology Inc. - MyWinLocker PSD Named Pipe Driver.) - C:\Windows\system32\DRIVERS\mwlPSDNServ.sys
O41 - Driver: (mwlPSDVDisk) . (.Egis Technology Inc. - MyWinLocker PSD Virtual Disk Driver.) - C:\Windows\system32\DRIVERS\mwlPSDVDisk.sys
O41 - Driver: netnb.inf (NetBIOS) . (.Microsoft Corporation - NetBIOS interface driver.) - C:\Windows\System32\DRIVERS\netbios.sys
O41 - Driver: C:\Windows\System32\drivers\netbt.sys (NetBT) . (.Microsoft Corporation - MBT Transport driver.) - C:\Windows\System32\DRIVERS\netbt.sys
O41 - Driver: npsvctrig.inf (npsvctrig) . (.Microsoft Corporation - Named pipe service triggers.) - C:\Windows\system32\drivers\npsvctrig.sys
O41 - Driver: C:\Windows\System32\drivers\nsiproxy.sys (nsiproxy) . (.Microsoft Corporation - NSI Proxy.) - C:\Windows\System32\drivers\nsiproxy.sys
O41 - Driver: C:\Windows\System32\drivers\pacer.sys (Psched) . (.Microsoft Corporation - Planificateur de paquets QoS.) - C:\Windows\system32\DRIVERS\pacer.sys
O41 - Driver: C:\Windows\System32\wkssvc.dll (rdbss) . (.Microsoft Corporation - Pilote du sous-système de mise en mémoire t.) - C:\Windows\System32\DRIVERS\rdbss.sys

```
O41 - Driver: C:\Windows\System32\tcpipcfg.dll (tdx) . (.Microsoft
Corporation - TDI Translation Driver.) -
C:\Windows\system32\DRIVERS\tdx.sys
O41 - Driver: C:\Windows\System32\drivers\vwififlt.sys (vwififlt) .
(.Microsoft Corporation - Virtual WiFi Filter Driver.) -
C:\Windows\system32\DRIVERS\vwififlt.sys
~ Drivers: 46 Scanned in 00mn 00s



---\\ Logiciels installés (O42)
O42 - Logiciel: 7-Zip 9.20 - (...) [HKLM][64Bits] -- 7-Zip
O42 - Logiciel: ANT Drivers Installer x64 - (.Garmin Ltd or its
subsidiaries.) [HKLM][64Bits] -- {ABB006B0-2E10-4B85-8E6B-A6C9109B0893}
O42 - Logiciel: Acer Backup Manager - (.NTI Corporation.) [HKLM][64Bits]
-- InstallShield_{9DDDF20E-9FD1-4434-A43E-E7889DBC9420}
O42 - Logiciel: Acer Device Fast-lane - (.Acer Incorporated.)
[HKLM][64Bits] -- {3F62D2FD-13C1-49A2-8B5D-47623D9460D7}
O42 - Logiciel: Acer Power Management - (.Acer Incorporated.)
[HKLM][64Bits] -- {91F52DE4-B789-42B0-9311-A349F10E5479}
O42 - Logiciel: Acer Recovery Management - (.Acer Incorporated.)
[HKLM][64Bits] -- {07F2005A-8CAC-4A4B-83A2-DA98A722CA61}
O42 - Logiciel: AcerCloud - (.Acer Incorporated.) [HKLM][64Bits] --
{A5AD0B17-F34D-49BE-A157-C8B3D52ACD13}
O42 - Logiciel: AcerCloud Docs - (.Acer Incorporated.) [HKLM][64Bits] --
{CA4FE8B0-298C-4E5D-A486-F33B126D6A0A}
O42 - Logiciel: Adobe Flash Player 16 NPAPI - (.Adobe Systems
Incorporated.) [HKLM][64Bits] -- Adobe Flash Player NPAPI
O42 - Logiciel: Adobe Reader XI (11.0.10) - Français - (.Adobe Systems
Incorporated.) [HKLM][64Bits] -- {AC76BA86-7AD7-1036-7B44-AB0000000001}
O42 - Logiciel: Adobe Refresh Manager - (.Adobe Systems Incorporated.)
[HKLM][64Bits] -- {AC76BA86-0804-1033-1959-001802114130}
O42 - Logiciel: Agatha Christie - Death on the Nile - (.WildTangent.)
[HKLM][64Bits] -- WTA-0cd0315b-1033-4917-b5d1-9018d53bc488
=>.WildTangent
O42 - Logiciel: Aloha TriPeaks - (.WildTangent.) [HKLM][64Bits] -- WTA-
e110a565-aaac-48b7-b4ec-e57dd940a448  =>.WildTangent
O42 - Logiciel: Apple Application Support - (.Apple Inc..) [HKLM][64Bits]
-- {A922C4B7-50E0-4787-A94C-59DBF3C65DBE}
O42 - Logiciel: Apple Mobile Device Support - (.Apple Inc..)
[HKLM][64Bits] -- {FE86CB0C-FCB3-4358-B4B0-B0A41E33B3DD}
O42 - Logiciel: Apple Software Update - (.Apple Inc..) [HKLM][64Bits] --
{789A5B64-9DD9-4BA5-915A-F0FC0A1B7BFE}  =>.Apple Inc
O42 - Logiciel: Audacity 2.0.6 - (.Audacity Team.) [HKLM][64Bits] --
Audacity_is1
O42 - Logiciel: Backup Manager v4 - (.NTI Corporation.) [HKLM][64Bits] --
{9DDDF20E-9FD1-4434-A43E-E7889DBC9420}
O42 - Logiciel: Bejeweled 3 - (.WildTangent.) [HKLM][64Bits] -- WTA-
918780a1-8719-43c2-99e9-7e0352136ecf  =>.WildTangent
O42 - Logiciel: Bonjour - (.Apple Inc..) [HKLM][64Bits] -- {6E3610B2-
430D-4EB0-81E3-2B57E8B9DE8D}
O42 - Logiciel: CCleaner - (.Piriform.) [HKLM][64Bits] -- CCleaner
O42 - Logiciel: CDBurnerXP - (.CDBurnerXP.) [HKLM][64Bits] -- {7E265513-
8CDA-4631-B696-F40D983F3B07}_is1
```

```
O42 - Logiciel: CyberLink MediaEspresso 6.5 - (.CyberLink Corp..)
[HKLM][64Bits] -- InstallShield_{E3739848-5329-48E3-8D28-5BBD6E8BE384}
O42 - Logiciel: CyberLink MediaEspresso 6.5 - (.CyberLink Corp..)
[HKLM][64Bits] -- {E3739848-5329-48E3-8D28-5BBD6E8BE384}
O42 - Logiciel: D3DX10 - (.Microsoft.) [HKLM][64Bits] -- {E09C4DB7-630C-
4F06-A631-8EA7239923AF}
O42 - Logiciel: Delicious: Emily's True Love Premium Edition -
(.WildTangent.) [HKLM][64Bits] -- WTA-0e52c30b-7996-4bdc-8831-
c8d37d11e689  =>.WildTangent
O42 - Logiciel: Dolby Advanced Audio v2 - (.Dolby Laboratories Inc.)
[HKLM][64Bits] -- {B9E70C7A-9F85-4A39-A4A3-BFA3C3BF7613}
O42 - Logiciel: Elevated Installer - (.Garmin Ltd or its subsidiaries.)
[HKLM][64Bits] -- {C0ED5561-F673-47B4-B31A-7DC07651B7FD}
O42 - Logiciel: Galerie de photos - (.Microsoft Corporation.)
[HKLM][64Bits] -- {439B34FF-F74E-4807-B5E2-4B758551DA6B}
O42 - Logiciel: Garmin Express - (.Garmin Ltd or its subsidiaries.)
[HKLM][64Bits] -- {045320b6-c340-4960-aefd-57bf08a9b425}  =>.Garmin
Corporation
O42 - Logiciel: Garmin Express - (.Garmin Ltd or its subsidiaries.)
[HKLM][64Bits] -- {0FF2E7C6-D80F-4E9A-AA97-599E1CA26BED}  =>.Garmin
Corporation
O42 - Logiciel: Garmin Express Tray - (.Garmin Ltd or its subsidiaries.)
[HKLM][64Bits] -- {AE7D09D2-FA96-4CCE-8C74-F0A0DBD557EB}  =>.Garmin
Corporation
O42 - Logiciel: Google Chrome - (.Google Inc..) [HKLM][64Bits] -- Google
Chrome
O42 - Logiciel: Google Update Helper - (.Google Inc..) [HKLM][64Bits] --
{A92DAB39-4E2C-4304-9AB6-BC44E68B55E2}
O42 - Logiciel: Governor of Poker 2 Premium Edition - (.WildTangent.)
[HKLM][64Bits] -- WTA-90efde6f-ed63-40d0-aac6-376805b57f96
=>.WildTangent
O42 - Logiciel: Identity Card - (.Acer Incorporated.) [HKLM][64Bits] --
{3D9CB654-99AD-4301-89C6-0D12A790767C}
O42 - Logiciel: Intel(R) Management Engine Components - (.Intel
Corporation.) [HKLM][64Bits] -- {65153EA5-8B6E-43B6-857B-C6E4FC25798A}
O42 - Logiciel: Intel(R) Processor Graphics - (.Intel Corporation.)
[HKLM][64Bits] -- {F0E3AD40-2BBD-4360-9C76-B9AC9A5886EA}
O42 - Logiciel: Intel(R) Rapid Storage Technology - (.Intel Corporation.)
[HKLM][64Bits] -- {3E29EE6C-963A-4aae-86C1-DC237C4A49FC}
O42 - Logiciel: Intel(R) SDK for OpenCL - CPU Only Runtime Package -
(.Intel Corporation.) [HKLM][64Bits] -- {FCB3772C-B7D0-4933-B1A9-
3707EBACC573}
O42 - Logiciel: Intel® Trusted Connect Service Client - (.Intel
Corporation.) [HKLM][64Bits] -- {F4404AFD-2EF3-40C1-8C09-29E5F3B6972B}
O42 - Logiciel: Island Tribe - (.WildTangent.) [HKLM][64Bits] -- WTA-
e913efbb-add0-4e87-ada6-11f50360b2a5  =>.WildTangent
O42 - Logiciel: JDownloader 0.9 - (.AppWork GmbH.) [HKLM][64Bits] --
5513-1208-7298-9440
O42 - Logiciel: Jewel Match 3 - (.WildTangent.) [HKLM][64Bits] -- WTA-
02ff0ddf-5fc5-4574-91ec-101857655e74  =>.WildTangent
O42 - Logiciel: John Deere Drive Green - (.WildTangent.) [HKLM][64Bits] -
- WTA-c896539a-924a-4caa-b263-2a3893da23a6  =>.WildTangent
O42 - Logiciel: La boite a couleurs version 1.6.15 - (...) [HKLM][64Bits]
-- La boite a couleurs_is1
```

O42 - Logiciel: Launch Manager - (.Acer Inc..) [HKLM][64Bits] -- LManager
O42 - Logiciel: LibreOffice 4.1.0.4 - (.The Document Foundation.) [HKLM][64Bits] -- {F8478020-D98E-49FB-BA14-07A534AED99C}
O42 - Logiciel: Live Updater - (.Acer Incorporated.) [HKLM][64Bits] -- {EE26E302-876A-48D9-9058-3129E5B99999}
O42 - Logiciel: MSVCRT - (.Microsoft.) [HKLM][64Bits] -- {8DD46C6A-0056-4FEC-B70A-28BB16A1F11F}
O42 - Logiciel: MSVCRT110 - (.Microsoft.) [HKLM][64Bits] -- {8E14DDC8-EA60-4E18-B3E3-1937104D5BDA}
O42 - Logiciel: MSVCRT110_amd64 - (.Microsoft.) [HKLM][64Bits] -- {E9FA781F-3E80-4399-825A-AD3E11C28C77}
O42 - Logiciel: Magic Academy - (.WildTangent.) [HKLM][64Bits] -- WTA-a5058af1-d603-48b7-a37c-67b4c27eb8f5 =>.WildTangent
O42 - Logiciel: Malwarebytes Anti-Malware version 2.0.4.1028 - (.Malwarebytes Corporation.) [HKLM][64Bits] -- Malwarebytes Anti-Malware_is1
O42 - Logiciel: McAfee SiteAdvisor - (.McAfee, Inc..) [HKLM][64Bits] -- {35ED3F83-4BDC-4c44-8EC6-6A8301C7413A}
O42 - Logiciel: Microsoft Silverlight - (.Microsoft Corporation.) [HKLM][64Bits] -- {89F4137D-6C26-4A84-BDB8-2E5A4BB71E00}
O42 - Logiciel: Mozilla Firefox 28.0 (x86 fr) - (.Mozilla.) [HKLM][64Bits] -- Mozilla Firefox 28.0 (x86 fr)
O42 - Logiciel: Mozilla Maintenance Service - (.Mozilla.) [HKLM][64Bits] -- MozillaMaintenanceService
O42 - Logiciel: MyWinLocker - (.Egis Technology Inc..) [HKLM][64Bits] -- {0B78ECB0-1A6B-4E6D-89D7-0E7CE77F0427}
O42 - Logiciel: MyWinLocker 4 - (.Egis Technology Inc..) [HKLM][64Bits] -- {39F15B50-A977-4CA6-B1C3-6A8724CDA025}
O42 - Logiciel: MyWinLocker Suite - (.Egis Technology Inc..) [HKLM][64Bits] -- InstallShield_{17DF9714-60C9-43C9-A9C2-32BCAED44CBE}
O42 - Logiciel: MyWinLocker Suite - (.Egis Technology Inc..) [HKLM][64Bits] -- {17DF9714-60C9-43C9-A9C2-32BCAED44CBE}
O42 - Logiciel: NTI Media Maker 9 - (.NTI Corporation.) [HKLM][64Bits] -- InstallShield_{D3D5C4E8-040F-4C6F-8105-41D43CF94F44}
O42 - Logiciel: NTI Media Maker 9 - (.NTI Corporation.) [HKLM][64Bits] -- {D3D5C4E8-040F-4C6F-8105-41D43CF94F44}
O42 - Logiciel: Nero 7.10.1.0 - (.Nero AG.) [HKLM][64Bits] -- Nero7_is1
O42 - Logiciel: Nero BurnLite 10 - (.Nero AG.) [HKLM][64Bits] -- {842BEE12-CCCB-43F4-ABAF-CBA6DFE2583D}
O42 - Logiciel: Nero BurnLite 10 - (.Nero AG.) [HKLM][64Bits] -- {AB627AF2-9C7E-4DBD-816B-3B2646B81E89}
O42 - Logiciel: Nero Burning Core - (.Nero AG.) [HKLM][64Bits] -- {B166374C-105E-445E-8E5D-A86CA5742645}
O42 - Logiciel: Nero Burning ROM - (.Nero AG.) [HKLM][64Bits] -- {F2B9C8D6-C69C-4BA7-95D2-66F1C68D15DA}
O42 - Logiciel: Nero Burning ROM 2014 - (.Nero AG.) [HKLM][64Bits] -- {64187E83-9CCE-4496-8068-DF1E8415970D}
O42 - Logiciel: Nero Burning ROM Help (CHM) - (.Nero AG.) [HKLM][64Bits] -- {FA78CC15-9F90-443B-BA61-A66595F06432}
O42 - Logiciel: Nero Control Center 10 - (.Nero AG.) [HKLM][64Bits] -- {6DFB899F-17A2-48F0-A533-ED8D6866CF38}
O42 - Logiciel: Nero ControlCenter - (.Nero AG.) [HKLM][64Bits] -- {ABC88553-8770-4B97-B43E-5A90647A5B63}

O42 - Logiciel: Nero ControlCenter 10 Help (CHM) - (.Nero AG.) [HKLM][64Bits] -- {523B2B1B-D8DB-4B41-90FF-C4D799E2758A}
O42 - Logiciel: Nero ControlCenter Help (CHM) - (.Nero AG.) [HKLM][64Bits] -- {CDFE8F95-F80F-4115-9C3F-0E1FD8F9F58C}
O42 - Logiciel: Nero Core Components - (.Nero AG.) [HKLM][64Bits] -- {BEBEE34D-84A2-4EDD-8BEA-96CC54371263}
O42 - Logiciel: Nero Core Components 10 - (.Nero AG.) [HKLM][64Bits] -- {2436F2A8-4B7E-4B6C-AE4E-604C84AA6A4F}
O42 - Logiciel: Nero SharedVideoCodecs - (.Nero AG.) [HKLM][64Bits] -- {2432E589-6256-4513-B0BF-EFA8E325D5F0}
O42 - Logiciel: Nero Update - (.Nero AG.) [HKLM][64Bits] -- {65BB0407-4CC8-4DC7-952E-3EEFDF05602A}
O42 - Logiciel: Norton Online Backup - (.Symantec Corporation.) [HKLM][64Bits] -- {40A66DF6-22D3-44B5-A7D3-83B118A2C0DC} =>.Symantec Corporation
O42 - Logiciel: Norton Online Backup ARA - (.Symantec Corporation.) [HKLM][64Bits] -- NARA =>.Symantec Corporation
O42 - Logiciel: Office Addin - (.Acer.) [HKLM][64Bits] -- {6D2BBE1D-E600-4695-BA37-0B0E605542CC}
O42 - Logiciel: Package de pilotes Windows - Dynastream Innovations, Inc. ANT LibUSB Driver - (.Dynastream Innovations, Inc..) [HKLM][64Bits] -- F9D2A789F9CFF8CEC36B544F53877C80F1F73C46
O42 - Logiciel: Package de pilotes Windows - Silicon Labs Software (DSI_SiUSBXp_3_1) USB (- (.Silicon Labs Software.) [HKLM][64Bits] -- D1506E0025B5A3F9EB8270FE81C1EEDD9388B8A2
O42 - Logiciel: Penguins! - (.WildTangent.) [HKLM][64Bits] -- WTA-245c9a0b-0524-44af-a8a1-49f702957451 =>.WildTangent
O42 - Logiciel: Plants vs. Zombies - Game of the Year - (.WildTangent.) [HKLM][64Bits] -- WTA-a3136c86-9d78-4e60-b512-13c528b623e9 =>.WildTangent
O42 - Logiciel: Polar Bowler - (.WildTangent.) [HKLM][64Bits] -- WTA-da5528b0-7846-4520-9178-9b59102dfaf1 =>.WildTangent
O42 - Logiciel: Qualcomm Atheros Bluetooth Suite (64) - (.Qualcomm Atheros Communications.) [HKLM][64Bits] -- {A84A4FB1-D703-48DB-89E0-68B6499D2801}
O42 - Logiciel: Qualcomm Atheros WiFi Driver Installation - (.Qualcomm Atheros.) [HKLM][64Bits] -- {28006915-2739-4EBE-B5E8-49B25D32EB33}
O42 - Logiciel: Realtek Ethernet Controller Driver - (.Realtek.) [HKLM][64Bits] -- {8833FFB6-5B0C-4764-81AA-06DFEED9A476}
O42 - Logiciel: Realtek High Definition Audio Driver - (.Realtek Semiconductor Corp..) [HKLM][64Bits] -- {F132AF7F-7BCA-4EDE-8A7C-958108FE7DBC}
O42 - Logiciel: Realtek PCIE Card Reader - (.Realtek Semiconductor Corp..) [HKLM][64Bits] -- {C1594429-8296-4652-BF54-9DBE4932A44C}
O42 - Logiciel: Shared C Run-time for x64 - (.McAfee.) [HKLM][64Bits] -- {EF79C448-6946-4D71-8134-03407888C054}
O42 - Logiciel: Shredder - (.Egis Technology Inc..) [HKLM][64Bits] -- {C2695E83-CF1D-43D1-84FE-B3BEC561012A}
O42 - Logiciel: Spotify - (.Spotify AB.) [HKLM][64Bits] -- Spotify
O42 - Logiciel: Synaptics Pointing Device Driver - (.Synaptics Incorporated.) [HKLM][64Bits] -- SynTPDeinstKey
O42 - Logiciel: Tales of Lagoona - (.WildTangent.) [HKLM][64Bits] -- WTA-4cee26fb-cfa3-4282-ac30-79ac337e5599 =>.WildTangent

```
O42 - Logiciel: Update Installer for WildTangent Games App -
(.WildTangent.) [HKLM][64Bits] -- {2FA94A64-C84E-49d1-97DD-
7BF06C7BBFB2}.WildTangent Games App  =>.WildTangent
O42 - Logiciel: VLC media player 2.0.8 - (.VideoLAN.) [HKLM][64Bits] --
VLC media player  =>.VideoLAN
O42 - Logiciel: Visionneuse Microsoft PowerPoint - (.Microsoft
Corporation.) [HKLM][64Bits] -- {95140000-00AF-040C-0000-0000000FF1CE}
O42 - Logiciel: Visual Studio 2005 Tools pour Office Second Edition
Runtime - (.Microsoft Corporation.) [HKLM][64Bits] -- Microsoft Visual
Studio 2005 Tools for Office Runtime
O42 - Logiciel: Visual Studio Tools for the Office system 3.0 Runtime -
(.Microsoft Corporation.) [HKLM][64Bits] -- Visual Studio Tools for the
Office system 3.0 Runtime
O42 - Logiciel: Visual Studio Tools for the Office system 3.0 Runtime -
(.Microsoft Corporation.) [HKLM][64Bits] -- {8FB53850-246A-3507-8ADE-
0060093FFEA6}
O42 - Logiciel: Visual Studio Tools for the Office system 3.0 Runtime
Service Pack 1 (KB949 - (.Microsoft Corporation.) [HKLM][64Bits] --
{8FB53850-246A-3507-8ADE-0060093FFEA6}.KB949258
O42 - Logiciel: VoiceOver Kit - (.Apple Inc..) [HKLM][64Bits] --
{6B4AD1A9-E73A-4184-9D6B-072F8A3C5EBA}
O42 - Logiciel: WSE_Binkiland - (.WSE_Binkiland.) [HKLM][64Bits] --
WSE_Binkiland
O42 - Logiciel: WildTangent Games - (.WildTangent.) [HKLM][64Bits] --
WildTangent wildgames Master Uninstall  =>.WildTangent
O42 - Logiciel: WildTangent Games App - (.WildTangent.) [HKLM][64Bits] --
{70B446D1-E03B-4ab0-9B3C-0832142C9AA8}.WildTangent Games App-acer
=>.WildTangent
O42 - Logiciel: WinRAR 5.01 (32-bit) - (.win.rar GmbH.) [HKLM][64Bits] --
WinRAR archiver
O42 - Logiciel: Woonoz SKY 3.4d - (.Woonoz SAs.) [HKLM][64Bits] -- 0313-
7094-4803-8388
O42 - Logiciel: Zuma's Revenge - (.WildTangent.) [HKLM][64Bits] -- WTA-
dec892c1-310c-4528-9f25-f15a63106e45  =>.WildTangent
O42 - Logiciel: avast! Free Antivirus v9.0.2021 - (.AVAST Software.)
[HKLM][64Bits] -- avast
O42 - Logiciel: clear.fi Media - (.Acer Incorporated.) [HKLM][64Bits] --
{E9AF1707-3F3A-49E2-8345-4F2D629D0876}
O42 - Logiciel: clear.fi Photo - (.Acer Incorporated.) [HKLM][64Bits] --
{B5AD89F2-03D3-4206-8487-018298007DD0}
O42 - Logiciel: clear.fi SDK - Video 2 - (.CyberLink Corp..)
[HKLM][64Bits] -- {EBA33CAD-E071-48d5-A168-FBA4EEB42E93}
O42 - Logiciel: clear.fi SDK- Movie 2 - (.CyberLink Corp..)
[HKLM][64Bits] -- {35DA427D-BB23-49B8-9AFD-CFFCFE3B708D}
O42 - Logiciel: iTunes - (.Apple Inc..) [HKLM][64Bits] -- {0D924CB2-2EA4-
4044-BAF7-770202D6BD0D}
O42 - Logiciel: livebox - (.SAGEM.) [HKLM][64Bits] -- {17342E3B-0818-
4A6F-BFF8-99476605ADD6}
~ Logic: 71 Scanned in 00mn 00s


---\\ HKCU & HKLM Software Keys
[HKCU\Software\7-Zip]
```

[HKCU\Software\AVAST Software]
[HKCU\Software\Adobe]
[HKCU\Software\Ahead]
[HKCU\Software\AppDataLow]
[HKCU\Software\Apple Computer, Inc.]
[HKCU\Software\Apple Inc.]
[HKCU\Software\Atheros]
[HKCU\Software\Audacity]
[HKCU\Software\BCCP]
[HKCU\Software\Binkiland Browser]
[HKCU\Software\Canneverbe Limited]
[HKCU\Software\CanonBJ]
[HKCU\Software\Canon]
[HKCU\Software\Chromium]
[HKCU\Software\Classes]
[HKCU\Software\Clients]
[HKCU\Software\Cyberlink]
[HKCU\Software\Dritek]
[HKCU\Software\Emulators]
[HKCU\Software\Garmin]
[HKCU\Software\Google]
[HKCU\Software\Intel]
[HKCU\Software\JavaSoft]
[HKCU\Software\Licenses]
[HKCU\Software\Lightworks]
[HKCU\Software\Local AppWizard-Generated Applications]
[HKCU\Software\Macromedia]
[HKCU\Software\Malwarebytes' Anti-Malware]
[HKCU\Software\McAfee]
[HKCU\Software\Mine]
[HKCU\Software\MozillaPlugins]
[HKCU\Software\Nero]
[HKCU\Software\Netscape]
[HKCU\Software\OEM]
[HKCU\Software\Piriform]
[HKCU\Software\Policies]
[HKCU\Software\Realtek]
[HKCU\Software\RegisteredApplications]
[HKCU\Software\Synaptics]
[HKCU\Software\TeleCharger]
[HKCU\Software\Trolltech]
[HKCU\Software\TuneUp]
[HKCU\Software\WinRAR SFX]
[HKCU\Software\WinRAR]
[HKCU\Software\Wow6432Node]
[HKCU\Software\ZebHelpProcess Helper]
[HKCU\Software\ej-technologies]
[HKCU\Software\malavida]
[HKCU\Software\mozilla]
[HKCU\Software\wse_binkiland]
[HKLM\Software\ATI Technologies]
[HKLM\Software\Apple Computer, Inc.]
[HKLM\Software\Apple Inc.]
[HKLM\Software\Atheros]

[HKLM\Software\Canon]
[HKLM\Software\Classes]
[HKLM\Software\Clients]
[HKLM\Software\Cyberlink]
[HKLM\Software\DTS]
[HKLM\Software\Dolby]
[HKLM\Software\EgisTec IPS]
[HKLM\Software\EgisTec Shredder]
[HKLM\Software\EnigmaSoftwareGroup] =>PUP.EnigmaSoftware
[HKLM\Software\GEAR Software]
[HKLM\Software\Google]
[HKLM\Software\InstalledOptions]
[HKLM\Software\Intel]
[HKLM\Software\Khronos]
[HKLM\Software\Macromedia]
[HKLM\Software\MozillaPlugins]
[HKLM\Software\Mozilla]
[HKLM\Software\ODBC]
[HKLM\Software\OEM]
[HKLM\Software\Piriform]
[HKLM\Software\Policies]
[HKLM\Software\RTLSetup]
[HKLM\Software\Realtek Semiconductor Corp.]
[HKLM\Software\Realtek]
[HKLM\Software\RegisteredApplications]
[HKLM\Software\SRS Labs]
[HKLM\Software\SonicFocus]
[HKLM\Software\Symantec]
[HKLM\Software\Synaptics]
[HKLM\Software\TuneUp]
[HKLM\Software\Waves Audio]
[HKLM\Software\Wow6432Node\AVAST Software]
[HKLM\Software\Wow6432Node\Adobe]
[HKLM\Software\Wow6432Node\AdwCleaner]
[HKLM\Software\Wow6432Node\Ahead]
[HKLM\Software\Wow6432Node\Apple Computer, Inc.]
[HKLM\Software\Wow6432Node\Apple Inc.]
[HKLM\Software\Wow6432Node\Brother]
[HKLM\Software\Wow6432Node\Canneverbe Limited]
[HKLM\Software\Wow6432Node\Canon]
[HKLM\Software\Wow6432Node\Classes]
[HKLM\Software\Wow6432Node\Clients]
[HKLM\Software\Wow6432Node\CyberLink]
[HKLM\Software\Wow6432Node\Dritek]
[HKLM\Software\Wow6432Node\EgisTec IPS]
[HKLM\Software\Wow6432Node\EgisTec MyWinLockerSuite]
[HKLM\Software\Wow6432Node\EgisTec MyWinLocker]
[HKLM\Software\Wow6432Node\EgisTec Shredder]
[HKLM\Software\Wow6432Node\Garmin]
[HKLM\Software\Wow6432Node\Google]
[HKLM\Software\Wow6432Node\InstallShield]
[HKLM\Software\Wow6432Node\Intel]
[HKLM\Software\Wow6432Node\JavaSoft]
[HKLM\Software\Wow6432Node\Khronos]

```
[HKLM\Software\Wow6432Node\LibreOffice]
[HKLM\Software\Wow6432Node\Licenses]
[HKLM\Software\Wow6432Node\Lightworks]
[HKLM\Software\Wow6432Node\Macromedia]
[HKLM\Software\Wow6432Node\Macrovision]
[HKLM\Software\Wow6432Node\Malwarebytes' Anti-Malware (Trial)]
[HKLM\Software\Wow6432Node\Malwarebytes' Anti-Malware]
[HKLM\Software\Wow6432Node\MozillaPlugins]
[HKLM\Software\Wow6432Node\Mozilla]
[HKLM\Software\Wow6432Node\Nero]
[HKLM\Software\Wow6432Node\NewTech Infosystems]
[HKLM\Software\Wow6432Node\Norton]
[HKLM\Software\Wow6432Node\ODBC]
[HKLM\Software\Wow6432Node\OEM]
[HKLM\Software\Wow6432Node\Policies]
[HKLM\Software\Wow6432Node\Qualcomm Atheros WiFi Driver Installation]
[HKLM\Software\Wow6432Node\Realtek Semiconductor Corp.]
[HKLM\Software\Wow6432Node\Realtek]
[HKLM\Software\Wow6432Node\RegisteredApplications]
[HKLM\Software\Wow6432Node\Sagem]
[HKLM\Software\Wow6432Node\ScanSoft]
[HKLM\Software\Wow6432Node\SiteAdvisor]
[HKLM\Software\Wow6432Node\Symantec]
[HKLM\Software\Wow6432Node\The Document Foundation]
[HKLM\Software\Wow6432Node\TuneUp]
[HKLM\Software\Wow6432Node\VideoLAN]
[HKLM\Software\Wow6432Node\VirualDiskRedist]
[HKLM\Software\Wow6432Node\Volatile]
[HKLM\Software\Wow6432Node\WildTangent]
[HKLM\Software\Wow6432Node\WinRAR]
[HKLM\Software\Wow6432Node\Zeon]
[HKLM\Software\Wow6432Node\ej-technologies]
[HKLM\Software\Wow6432Node\mozilla.org]
[HKLM\Software\Wow6432Node]
~ Key Software: 335 Scanned in 00mn 00s


---\\ Contenu des dossiers Programs/ProgramFiles/ProgramData/AppData
(O43)
O43 - CFD: 02/08/2013 - 19:07:51 - [] ----D C:\Program Files (x86)\7-Zip
O43 - CFD: 09/03/2013 - 06:56:53 - [] ----D C:\Program Files (x86)\Acer
O43 - CFD: 03/11/2014 - 17:47:46 - [] ----D C:\Program Files (x86)\Adobe
O43 - CFD: 31/01/2014 - 17:16:37 - [] ----D C:\Program Files (x86)\Apple
Software Update  =>.Apple Inc
O43 - CFD: 06/01/2015 - 14:33:27 - [] ----D C:\Program Files
(x86)\Audacity
O43 - CFD: 09/03/2013 - 06:17:48 - [] ----D C:\Program Files
(x86)\Bluetooth Suite
O43 - CFD: 31/01/2014 - 17:15:00 - [] ----D C:\Program Files
(x86)\Bonjour
O43 - CFD: 21/02/2014 - 21:24:11 - [] ----D C:\Program Files
(x86)\CDBurnerXP
```

```
O43 - CFD: 31/01/2015 - 16:52:52 - [] ----D C:\Program Files (x86)\Common
Files
O43 - CFD: 17/12/2012 - 13:32:01 - [] ----D C:\Program Files
(x86)\CyberLink
O43 - CFD: 17/12/2012 - 13:27:45 - [] ----D C:\Program Files
(x86)\EgisTec IPS
O43 - CFD: 17/12/2012 - 13:27:54 - [] ----D C:\Program Files
(x86)\EgisTec MyWinLocker
O43 - CFD: 17/12/2012 - 13:26:32 - [] ----D C:\Program Files
(x86)\EgisTec MyWinLockerSuite
O43 - CFD: 17/12/2012 - 13:28:18 - [] ----D C:\Program Files
(x86)\EgisTec Shredder
O43 - CFD: 03/12/2014 - 16:55:14 - [] ----D C:\Program Files (x86)\Garmin
O43 - CFD: 16/06/2013 - 20:14:35 - [] ----D C:\Program Files (x86)\Google
O43 - CFD: 03/08/2013 - 20:33:12 - [] --H-D C:\Program Files
(x86)\InstallShield Installation Information
O43 - CFD: 27/12/2014 - 16:39:34 - [] ----D C:\Program Files (x86)\Intel
O43 - CFD: 31/12/2014 - 17:58:04 - [] ----D C:\Program Files
(x86)\Internet Explorer
O43 - CFD: 31/01/2014 - 17:24:29 - [] ----D C:\Program Files (x86)\iTunes
O43 - CFD: 04/12/2014 - 19:45:42 - [] ----D C:\Program Files
(x86)\JDownloader
O43 - CFD: 07/01/2015 - 10:05:29 - [] ----D C:\Program Files
(x86)\LaBoiteACouleurs
O43 - CFD: 09/03/2013 - 06:06:16 - [] ----D C:\Program Files (x86)\Launch
Manager
O43 - CFD: 02/08/2013 - 15:17:12 - [] ----D C:\Program Files
(x86)\LibreOffice 4
O43 - CFD: 05/02/2015 - 17:24:40 - [] ----D C:\Program Files
(x86)\Lightworks
O43 - CFD: 03/07/2013 - 17:32:19 - [] ----D C:\Program Files
(x86)\Malware Eraser
O43 - CFD: 05/02/2015 - 16:50:25 - [] ----D C:\Program Files
(x86)\Malwarebytes Anti-Malware
O43 - CFD: 06/02/2014 - 15:29:38 - [] ----D C:\Program Files
(x86)\Microsoft Office
O43 - CFD: 15/08/2014 - 16:22:22 - [] ----D C:\Program Files
(x86)\Microsoft Silverlight
O43 - CFD: 31/01/2015 - 16:59:13 - [] ----D C:\Program Files
(x86)\Microsoft SQL Server Compact Edition
O43 - CFD: 22/08/2013 - 16:36:30 - [] ----D C:\Program Files
(x86)\Microsoft.NET
O43 - CFD: 18/08/2014 - 11:11:03 - [] ----D C:\Program Files
(x86)\Mozilla Firefox
O43 - CFD: 26/08/2014 - 19:29:05 - [] ----D C:\Program Files
(x86)\Mozilla Maintenance Service
O43 - CFD: 27/12/2014 - 16:04:39 - [] ----D C:\Program Files
(x86)\MSBuild
O43 - CFD: 06/02/2014 - 15:24:28 - [] ----D C:\Program Files
(x86)\MSECache
O43 - CFD: 22/02/2014 - 12:43:18 - [] ----D C:\Program Files (x86)\Nero
O43 - CFD: 09/03/2013 - 06:44:28 - [] ----D C:\Program Files (x86)\Norton
Online Backup ARA  =>.Symantec Corporation
```

```
O43 - CFD: 09/03/2013 - 06:44:20 - [] ----D C:\Program Files
(x86)\NortonInstaller
O43 - CFD: 09/03/2013 - 06:43:21 - [] ----D C:\Program Files (x86)\NTI
O43 - CFD: 09/03/2013 - 06:25:39 - [] ----D C:\Program Files
(x86)\Qualcomm Atheros
O43 - CFD: 09/03/2013 - 06:08:25 - [] ----D C:\Program Files
(x86)\RadioController
O43 - CFD: 09/03/2013 - 06:23:12 - [] ----D C:\Program Files
(x86)\Realtek
O43 - CFD: 27/12/2014 - 16:04:39 - [] ----D C:\Program Files
(x86)\Reference Assemblies
O43 - CFD: 03/08/2013 - 20:33:14 - [] ----D C:\Program Files (x86)\SAGEM
O43 - CFD: 24/06/2013 - 16:08:55 - [] ----D C:\Program Files
(x86)\ScanSoft
O43 - CFD: 03/08/2013 - 20:32:05 - [] ----D C:\Program Files
(x86)\Securitoo
O43 - CFD: 09/03/2013 - 06:30:26 - [] ----D C:\Program Files
(x86)\Spotify
O43 - CFD: 30/10/2014 - 00:33:47 - [] ----D C:\Program Files
(x86)\Studio-Scrap
O43 - CFD: 09/03/2013 - 06:45:02 - [] ----D C:\Program Files
(x86)\Symantec
O43 - CFD: 09/03/2013 - 06:14:41 - [0] --H-D C:\Program Files (x86)\Temp
O43 - CFD: 02/08/2013 - 15:34:22 - [] ----D C:\Program Files
(x86)\VideoLAN
O43 - CFD: 17/12/2012 - 13:22:24 - [] ----D C:\Program Files
(x86)\WildGames
O43 - CFD: 01/12/2013 - 11:37:12 - [] ----D C:\Program Files
(x86)\WildTangent Games
O43 - CFD: 27/12/2014 - 16:14:54 - [] ----D C:\Program Files
(x86)\Windows Defender
O43 - CFD: 31/01/2015 - 16:59:08 - [] ----D C:\Program Files
(x86)\Windows Live
O43 - CFD: 24/09/2014 - 15:41:38 - [] ----D C:\Program Files
(x86)\Windows Mail  =>.Microsoft Corporation
O43 - CFD: 27/12/2014 - 16:39:40 - [] ----D C:\Program Files
(x86)\Windows Media Player  =>.Microsoft Corporation
O43 - CFD: 24/09/2014 - 19:10:22 - [] ----D C:\Program Files
(x86)\Windows Multimedia Platform
O43 - CFD: 22/08/2013 - 16:36:30 - [] ----D C:\Program Files
(x86)\Windows NT
O43 - CFD: 24/09/2014 - 15:41:38 - [] ----D C:\Program Files
(x86)\Windows Photo Viewer
O43 - CFD: 24/09/2014 - 19:10:22 - [] ----D C:\Program Files
(x86)\Windows Portable Devices
O43 - CFD: 27/12/2014 - 16:39:41 - [] -SH-D C:\Program Files
(x86)\Windows Sidebar
O43 - CFD: 22/08/2013 - 16:36:30 - [] ----D C:\Program Files
(x86)\WindowsPowerShell
O43 - CFD: 03/02/2014 - 20:17:59 - [] ----D C:\Program Files (x86)\WinRAR
O43 - CFD: 08/01/2015 - 21:02:13 - [] ----D C:\Program Files (x86)\Woonoz
O43 - CFD: 05/02/2015 - 18:00:14 - [] ----D C:\Program Files
(x86)\ZHPDiag  =>.Nicolas Coolman
```

```
O43 - CFD: 03/11/2014 - 17:48:15 - [] ----D C:\Program Files (x86)\Common
Files\Adobe
O43 - CFD: 22/02/2014 - 12:38:10 - [] ----D C:\Program Files (x86)\Common
Files\Ahead
O43 - CFD: 31/01/2014 - 17:18:14 - [] ----D C:\Program Files (x86)\Common
Files\Apple
O43 - CFD: 09/03/2013 - 06:18:11 - [] ----D C:\Program Files (x86)\Common
Files\Atheros
O43 - CFD: 17/12/2012 - 13:27:42 - [] ----D C:\Program Files (x86)\Common
Files\EgisTec
O43 - CFD: 24/06/2013 - 16:09:32 - [] ----D C:\Program Files (x86)\Common
Files\InstallShield
O43 - CFD: 27/12/2014 - 16:22:44 - [] ----D C:\Program Files (x86)\Common
Files\Intel
O43 - CFD: 09/03/2013 - 06:43:03 - [] ----D C:\Program Files (x86)\Common
Files\Macrovision Shared
O43 - CFD: 27/12/2014 - 16:39:33 - [] ----D C:\Program Files (x86)\Common
Files\Microsoft Shared
O43 - CFD: 21/02/2014 - 21:03:39 - [] ----D C:\Program Files (x86)\Common
Files\Nero
O43 - CFD: 09/03/2013 - 06:09:14 - [] ----D C:\Program Files (x86)\Common
Files\postureAgent
O43 - CFD: 09/03/2013 - 06:18:58 - [] ----D C:\Program Files (x86)\Common
Files\QCA_Bluetooth
O43 - CFD: 22/08/2013 - 16:36:33 - [] ----D C:\Program Files (x86)\Common
Files\Services
O43 - CFD: 24/09/2014 - 15:41:38 - [] ----D C:\Program Files (x86)\Common
Files\System
O43 - CFD: 31/01/2015 - 16:52:52 - [] ----D C:\Program Files (x86)\Common
Files\Windows Live
O43 - CFD: 26/06/2013 - 14:14:26 - [] ----D C:\Program Files (x86)\Common
Files\Wise Installation Wizard
O43 - CFD: 31/01/2014 - 17:19:52 - [] ----D C:\ProgramData\34BE82C4-E596-
4e99-A191-52C6199EBF69
O43 - CFD: 09/03/2013 - 06:52:58 - [] ----D C:\ProgramData\Acer
O43 - CFD: 30/10/2014 - 11:55:26 - [] ----D C:\ProgramData\Adobe
O43 - CFD: 31/01/2014 - 17:16:20 - [] ----D C:\ProgramData\Apple
O43 - CFD: 31/01/2014 - 17:18:14 - [] ----D C:\ProgramData\Apple Computer
O43 - CFD: 22/08/2013 - 15:45:52 - [] -SH-D C:\ProgramData\Application
Data
O43 - CFD: 04/08/2013 - 19:56:15 - [] ----D C:\ProgramData\Applications
O43 - CFD: 27/12/2014 - 17:20:26 - [] ----D C:\ProgramData\Atheros
O43 - CFD: 08/12/2013 - 18:52:11 - [] ----D C:\ProgramData\AVAST Software
O43 - CFD: 17/12/2012 - 13:29:18 - [] ----D C:\ProgramData\BackupManager
O43 - CFD: 08/01/2014 - 20:28:47 - [] ----D C:\ProgramData\BlueStacks
O43 - CFD: 03/07/2013 - 11:04:27 - [] ----D
C:\ProgramData\BlueStacksSetup
O43 - CFD: 01/11/2013 - 19:04:32 - [] ----D
C:\ProgramData\boost_interprocess
O43 - CFD: 24/06/2013 - 16:02:56 - [] ----D C:\ProgramData\Brother
O43 - CFD: 15/06/2013 - 18:54:31 - [] -SH-D C:\ProgramData\Bureau
O43 - CFD: 21/02/2014 - 21:24:30 - [] ----D C:\ProgramData\Canneverbe
Limited
O43 - CFD: 01/12/2013 - 19:00:35 - [] --H-D C:\ProgramData\CanonBJ
```

```
O43 - CFD: 09/03/2013 - 06:49:10 - [] ----D C:\ProgramData\CLSK
O43 - CFD: 21/02/2014 - 21:08:40 - [] --H-D C:\ProgramData\Common Files
O43 - CFD: 28/06/2013 - 17:58:23 - [] ----D C:\ProgramData\CyberLink
O43 - CFD: 22/08/2013 - 15:45:52 - [] -SH-D C:\ProgramData\Desktop
O43 - CFD: 22/08/2013 - 15:45:52 - [] -SH-D C:\ProgramData\Documents
O43 - CFD: 09/03/2013 - 06:39:01 - [] ----D C:\ProgramData\EgisTec
O43 - CFD: 16/06/2013 - 20:15:19 - [] ----D C:\ProgramData\EgisTec IPS
O43 - CFD: 09/03/2013 - 06:43:04 - [] ----D C:\ProgramData\FLEXnet
O43 - CFD: 03/12/2014 - 16:56:08 - [] ----D C:\ProgramData\Garmin
O43 - CFD: 28/01/2015 - 19:05:35 - [] ----D C:\ProgramData\Geevs
O43 - CFD: 11/11/2014 - 13:36:30 - [] ----D C:\ProgramData\HP
O43 - CFD: 03/07/2013 - 12:54:11 - [] ----D C:\ProgramData\InstallMate
=>PUP.Tarma
O43 - CFD: 24/06/2013 - 16:12:47 - [] ----D C:\ProgramData\InstallShield
O43 - CFD: 09/03/2013 - 06:48:46 - [] ----D C:\ProgramData\install_clap
O43 - CFD: 09/03/2013 - 06:10:41 - [] ----D C:\ProgramData\Intel
O43 - CFD: 05/02/2015 - 16:50:18 - [] ----D C:\ProgramData\Malwarebytes
O43 - CFD: 27/12/2014 - 16:39:45 - [] ----D C:\ProgramData\McAfee
O43 - CFD: 15/06/2013 - 18:54:31 - [] -SH-D C:\ProgramData\Menu Démarrer
O43 - CFD: 31/01/2015 - 16:52:47 - [] -S--D C:\ProgramData\Microsoft
O43 - CFD: 15/06/2013 - 18:54:31 - [] -SH-D C:\ProgramData\Modèles
O43 - CFD: 25/06/2013 - 22:20:23 - [] ----D C:\ProgramData\Mozilla
O43 - CFD: 21/02/2014 - 21:03:37 - [] ----D C:\ProgramData\Nero
O43 - CFD: 25/06/2013 - 12:08:40 - [] ----D C:\ProgramData\Norton
O43 - CFD: 09/03/2013 - 06:44:20 - [] ----D
C:\ProgramData\NortonInstaller
O43 - CFD: 09/03/2013 - 06:44:01 - [] ----D C:\ProgramData\NTI Launcher
O43 - CFD: 15/06/2013 - 12:02:25 - [] ----D C:\ProgramData\OEM
O43 - CFD: 03/12/2014 - 16:55:24 - [] ----D C:\ProgramData\Package Cache
O43 - CFD: 27/12/2014 - 16:39:51 - [] ----D C:\ProgramData\PRICache
O43 - CFD: 09/03/2013 - 06:25:34 - [] ----D C:\ProgramData\Qualcomm
Atheros
O43 - CFD: 27/12/2014 - 16:45:23 - [] ----D C:\ProgramData\regid.1991-
06.com.microsoft
O43 - CFD: 22/08/2013 - 15:45:52 - [] -SH-D C:\ProgramData\Start Menu
O43 - CFD: 09/03/2013 - 06:45:02 - [] ----D C:\ProgramData\Symantec
O43 - CFD: 09/03/2013 - 06:29:20 - [] ----D C:\ProgramData\Synaptics
O43 - CFD: 21/06/2013 - 05:47:07 - [] ---AD C:\ProgramData\Temp
O43 - CFD: 22/08/2013 - 15:45:52 - [] -SH-D C:\ProgramData\Templates
O43 - CFD: 23/02/2014 - 12:52:18 - [] ----D C:\ProgramData\TuneUp
Software
O43 - CFD: 01/12/2013 - 11:37:09 - [] ----D C:\ProgramData\WildTangent
O43 - CFD: 04/02/2015 - 18:31:23 - [] ----D C:\ProgramData\{462EAEED-
16AC-7F6B-A72A-0FE977A8DC67}
O43 - CFD: 21/02/2014 - 21:08:40 - [] -SH-D C:\ProgramData\{FE8D473A-
6F06-4F99-B5F4-BED72B2A038C}
O43 - CFD: 27/12/2014 - 16:45:23 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\7-Zip
O43 - CFD: 22/08/2013 - 16:36:33 - [] R---D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessibility
O43 - CFD: 24/09/2014 - 16:03:54 - [] R---D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories
O43 - CFD: 27/12/2014 - 16:45:23 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Acer
```

```
O43 - CFD: 24/09/2014 - 19:10:43 - [] R---D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools
O43 - CFD: 27/12/2014 - 16:45:23 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Avast
O43 - CFD: 27/12/2014 - 16:45:23 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\CCleaner
O43 - CFD: 27/12/2014 - 16:45:23 - [] R---D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\CyberLink
MediaEspresso 6.5
O43 - CFD: 27/12/2014 - 16:45:23 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Dolby
O43 - CFD: 27/12/2014 - 16:45:23 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\EgisTec
O43 - CFD: 24/09/2014 - 19:10:43 - [] R---D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Embedded Lockdown
Manager
O43 - CFD: 27/12/2014 - 16:45:23 - [] R---D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Games
O43 - CFD: 27/12/2014 - 16:45:23 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Garmin
O43 - CFD: 04/02/2015 - 21:23:17 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Google Chrome
O43 - CFD: 27/12/2014 - 16:45:23 - [] R---D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Intel
O43 - CFD: 27/12/2014 - 16:45:23 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\iTunes
O43 - CFD: 07/01/2015 - 10:05:29 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\La boite a couleurs
O43 - CFD: 27/12/2014 - 16:45:23 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\LibreOffice 4.1
O43 - CFD: 28/01/2015 - 19:05:45 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Lightworks
O43 - CFD: 27/12/2014 - 16:45:23 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Livebox
O43 - CFD: 22/08/2013 - 16:36:33 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Maintenance
O43 - CFD: 05/02/2015 - 16:50:26 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Malwarebytes Anti-
Malware
O43 - CFD: 27/12/2014 - 16:45:23 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft
Silverlight
O43 - CFD: 27/12/2014 - 16:45:23 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Nero
O43 - CFD: 27/12/2014 - 16:45:23 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\NTI Media Maker 9
O43 - CFD: 27/12/2014 - 16:45:23 - [] R---D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp
O43 - CFD: 24/09/2014 - 19:10:28 - [] R---D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\System Tools
O43 - CFD: 24/09/2014 - 16:03:53 - [0] R-H-D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Tablet PC
O43 - CFD: 27/12/2014 - 16:45:23 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\VideoLAN
```

```
O43 - CFD: 27/12/2014 - 16:45:23 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\WinRAR
O43 - CFD: 27/12/2014 - 16:45:23 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Woonoz
O43 - CFD: 05/02/2015 - 18:00:14 - [] ----D
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\ZHP  =>.Nicolas
Coolman
O43 - CFD: 03/11/2014 - 17:47:44 - [] ----D
C:\Users\Lucie\AppData\Roaming\Adobe
O43 - CFD: 22/02/2014 - 12:46:43 - [] ----D
C:\Users\Lucie\AppData\Roaming\Ahead
O43 - CFD: 31/01/2014 - 17:20:30 - [] ----D
C:\Users\Lucie\AppData\Roaming\Apple Computer
O43 - CFD: 15/06/2013 - 12:03:25 - [] ----D
C:\Users\Lucie\AppData\Roaming\Atheros
O43 - CFD: 31/01/2015 - 17:27:29 - [] ----D
C:\Users\Lucie\AppData\Roaming\Audacity
O43 - CFD: 12/12/2013 - 17:33:44 - [] ----D
C:\Users\Lucie\AppData\Roaming\AVAST Software
O43 - CFD: 04/02/2015 - 18:31:49 - [] ----D
C:\Users\Lucie\AppData\Roaming\Binkiland
O43 - CFD: 21/02/2014 - 21:24:11 - [] ----D
C:\Users\Lucie\AppData\Roaming\Canneverbe Limited
O43 - CFD: 28/06/2013 - 17:59:23 - [] ----D
C:\Users\Lucie\AppData\Roaming\CyberLink
O43 - CFD: 03/12/2014 - 16:57:22 - [] ----D
C:\Users\Lucie\AppData\Roaming\Garmin
O43 - CFD: 07/07/2014 - 12:31:04 - [] ----D
C:\Users\Lucie\AppData\Roaming\gtk-2.0
O43 - CFD: 27/12/2014 - 17:15:30 - [] ----D
C:\Users\Lucie\AppData\Roaming\Identities
O43 - CFD: 03/08/2013 - 20:32:35 - [] ----D
C:\Users\Lucie\AppData\Roaming\InstallShield
O43 - CFD: 21/10/2013 - 16:36:11 - [] ----D
C:\Users\Lucie\AppData\Roaming\LibreOffice
O43 - CFD: 15/06/2013 - 12:01:40 - [] ----D
C:\Users\Lucie\AppData\Roaming\lm
O43 - CFD: 15/06/2013 - 12:01:34 - [] ----D
C:\Users\Lucie\AppData\Roaming\Macromedia
O43 - CFD: 27/06/2013 - 08:36:05 - [] ----D
C:\Users\Lucie\AppData\Roaming\Malwarebytes
O43 - CFD: 27/12/2014 - 17:17:55 - [] -S--D
C:\Users\Lucie\AppData\Roaming\Microsoft
O43 - CFD: 25/06/2013 - 22:58:20 - [] ----D
C:\Users\Lucie\AppData\Roaming\Mozilla
O43 - CFD: 21/02/2014 - 21:05:08 - [] ----D
C:\Users\Lucie\AppData\Roaming\Nero
O43 - CFD: 04/02/2015 - 20:52:16 - [0] ----D
C:\Users\Lucie\AppData\Roaming\Samsung
O43 - CFD: 31/01/2015 - 15:18:38 - [] ----D
C:\Users\Lucie\AppData\Roaming\Spotify
O43 - CFD: 15/06/2013 - 12:01:15 - [] ----D
C:\Users\Lucie\AppData\Roaming\Synaptics
```

```
O43 - CFD: 21/02/2014 - 21:11:03 - [] ----D
C:\Users\Lucie\AppData\Roaming\TuneUp Software
O43 - CFD: 05/12/2014 - 18:05:26 - [] ----D
C:\Users\Lucie\AppData\Roaming\vlc
O43 - CFD: 01/12/2013 - 11:36:28 - [] ----D
C:\Users\Lucie\AppData\Roaming\WildTangent
O43 - CFD: 04/02/2014 - 18:07:10 - [] ----D
C:\Users\Lucie\AppData\Roaming\WinRAR
O43 - CFD: 05/02/2015 - 18:01:24 - [] ----D
C:\Users\Lucie\AppData\Roaming\ZHP  =>.Nicolas Coolman
O43 - CFD: 30/10/2014 - 13:13:33 - [] ----D
C:\Users\Lucie\AppData\Local\Adobe
O43 - CFD: 31/01/2014 - 17:16:43 - [] ----D
C:\Users\Lucie\AppData\Local\Apple
O43 - CFD: 31/01/2014 - 17:20:09 - [] ----D
C:\Users\Lucie\AppData\Local\Apple Computer
O43 - CFD: 27/12/2014 - 16:34:10 - [] -SH-D
C:\Users\Lucie\AppData\Local\Application Data
O43 - CFD: 16/06/2013 - 20:08:35 - [] ----D
C:\Users\Lucie\AppData\Local\Apps
O43 - CFD: 05/02/2015 - 17:17:32 - [] ----D
C:\Users\Lucie\AppData\Local\Binkiland
O43 - CFD: 27/12/2014 - 17:20:28 - [] ----D
C:\Users\Lucie\AppData\Local\BMExplorer
O43 - CFD: 17/07/2013 - 13:32:58 - [] ----D
C:\Users\Lucie\AppData\Local\clear.fi
O43 - CFD: 05/02/2015 - 17:23:20 - [0] ----D
C:\Users\Lucie\AppData\Local\CrashDumps
O43 - CFD: 28/06/2013 - 17:57:43 - [] ----D
C:\Users\Lucie\AppData\Local\Cyberlink
O43 - CFD: 20/02/2014 - 07:24:00 - [0] ----D
C:\Users\Lucie\AppData\Local\Diagnostics
O43 - CFD: 04/02/2015 - 18:33:35 - [] ----D
C:\Users\Lucie\AppData\Local\Downloaded Installations
O43 - CFD: 16/06/2013 - 20:15:19 - [] ----D
C:\Users\Lucie\AppData\Local\EgisTec IPS
O43 - CFD: 03/12/2014 - 16:56:07 - [] ----D
C:\Users\Lucie\AppData\Local\Garmin
O43 - CFD: 16/06/2013 - 20:14:48 - [] ----D
C:\Users\Lucie\AppData\Local\Google
O43 - CFD: 27/12/2014 - 16:34:10 - [] -SH-D
C:\Users\Lucie\AppData\Local\Historique
O43 - CFD: 13/01/2014 - 18:19:42 - [] ----D
C:\Users\Lucie\AppData\Local\Macromedia
O43 - CFD: 31/01/2015 - 17:01:44 - [] ----D
C:\Users\Lucie\AppData\Local\Microsoft
O43 - CFD: 28/11/2013 - 18:54:19 - [] ----D
C:\Users\Lucie\AppData\Local\Mozilla
O43 - CFD: 07/09/2013 - 17:28:55 - [0] ----D
C:\Users\Lucie\AppData\Local\MusicPlayer
O43 - CFD: 02/02/2015 - 20:25:21 - [] ----D
C:\Users\Lucie\AppData\Local\Packages
O43 - CFD: 17/06/2013 - 10:33:43 - [] ----D
C:\Users\Lucie\AppData\Local\Programs
```

```
O43 - CFD: 25/06/2013 - 07:11:24 - [] ----D
C:\Users\Lucie\AppData\Local\Scansoft
O43 - CFD: 31/01/2015 - 10:10:01 - [] ----D
C:\Users\Lucie\AppData\Local\Spotify
O43 - CFD: 05/02/2015 - 18:01:01 - [] ----D
C:\Users\Lucie\AppData\Local\Temp
O43 - CFD: 27/12/2014 - 16:34:10 - [] -SH-D
C:\Users\Lucie\AppData\Local\Temporary Internet Files
O43 - CFD: 07/01/2015 - 10:06:14 - [] ----D
C:\Users\Lucie\AppData\Local\VirtualStore
O43 - CFD: 03/02/2015 - 07:10:59 - [] ----D
C:\Users\Lucie\AppData\Local\Windows Live
O43 - CFD: 27/12/2014 - 16:35:38 - [] R---D
C:\Users\Lucie\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Accessibility
O43 - CFD: 22/08/2013 - 16:36:32 - [] R---D
C:\Users\Lucie\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Accessories
O43 - CFD: 27/12/2014 - 16:45:23 - [] ----D
C:\Users\Lucie\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Acer
O43 - CFD: 27/12/2014 - 17:15:46 - [] R---D
C:\Users\Lucie\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Administrative Tools
O43 - CFD: 22/08/2013 - 16:36:32 - [] ----D
C:\Users\Lucie\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Maintenance
O43 - CFD: 27/12/2014 - 17:15:46 - [] R---D
C:\Users\Lucie\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup
O43 - CFD: 27/12/2014 - 16:35:38 - [] R---D
C:\Users\Lucie\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\System Tools
O43 - CFD: 27/12/2014 - 16:45:23 - [] ----D
C:\Users\Lucie\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\WinRAR
~ Program Folder: 234 Scanned in 00mn 00s


---\\ Derniers fichiers modifiés ou crées sous Windows et System32 (O44)
O44 - LFC:[MD5.DD596F70D5A4D959E1FCD50C4102FA62] - 05/02/2015 - 16:16:56
---A- . (...) -- C:\Windows\System32\PerfStringBackup.INI   [1824010]
O44 - LFC:[MD5.F16F8412B2A5FE9FF278F9F7F8CAE5AC] - 05/02/2015 - 16:16:56
---A- . (...) -- C:\Windows\System32\perfc009.dat   [135592]
O44 - LFC:[MD5.E1901A3676D849FE8A005C7202C57B8C] - 05/02/2015 - 16:16:56
---A- . (...) -- C:\Windows\System32\perfc00C.dat   [159412]
O44 - LFC:[MD5.994B663E830AD6955C25EED1A9E554DA] - 05/02/2015 - 16:16:56
---A- . (...) -- C:\Windows\System32\perfh009.dat   [722476]
O44 - LFC:[MD5.DB926B438CF346C26460EB73F1AEE027] - 05/02/2015 - 16:16:56
---A- . (...) -- C:\Windows\System32\perfh00C.dat   [812350]
O44 - LFC:[MD5.CA43F8904E24BBE49982E4C0B29E6579] - 05/02/2015 - 16:50:18
---A- . (.Malwarebytes Corporation - Malwarebytes Anti-Malware.) --
C:\Windows\System32\Drivers\mbam.sys   [25816]
```

```
O44 - LFC:[MD5.478CC94C937D235CB0A96AB8F2359D81] - 05/02/2015 - 16:50:18
---A- . (.Malwarebytes Corporation - Malwarebytes Chameleon Protection
Driver.) -- C:\Windows\System32\Drivers\mbamchameleon.sys   [93400]
O44 - LFC:[MD5.9D7BFFDB5FA62B600DF1FCB4919D9D79] - 05/02/2015 - 16:50:18
---A- . (.Malwarebytes Corporation - Malwarebytes Web Access Control.) --
C:\Windows\System32\Drivers\mwac.sys   [64216]
O44 - LFC:[MD5.5BA4AD184D1B0830CFA267E9D48F617A] - 05/02/2015 - 17:12:43
---A- . (...) -- C:\Windows\System32\wpbbin.exe   [53284]
O44 - LFC:[MD5.26C43960C99EE861A5D0EDC4DCF3B1C3] - 05/02/2015 - 17:14:02
---A- . (.Malwarebytes Corporation - Malwarebytes Anti-Malware.) --
C:\Windows\System32\Drivers\MBAMSwissArmy.sys   [129752]
O44 - LFC:[MD5.6CB1DC9343BDAA79C9043F35AE621E90] - 05/02/2015 - 17:15:02
-S-A- . (...) -- C:\Windows\bootstat.dat   [67584]
O44 - LFC:[MD5.D66211FA91C0AB9B4A5C7B8F7CDF0198] - 05/02/2015 - 17:34:36
---A- . (...) -- C:\Windows\WindowsUpdate.log   [32713]
O44 - LFC:[MD5.7160FC226391C0B50C85571FA1A546E5] - 28/01/2015 - 19:04:08
---A- . (.Microsoft Corporation - Direct3D 9 Extensions.) --
C:\Windows\System32\D3DX9_43.dll   [2401112]
O44 - LFC:[MD5.AD7FA9485059F4DC53C98B49CAB13F0B] - 28/01/2015 - 19:04:10
---A- . (.Microsoft Corporation - Direct3D 10.1 Extensions.) --
C:\Windows\System32\d3dx10_43.dll   [511328]
O44 - LFC:[MD5.5F1DA86286A2DFB01C4FED55C2DD1D61] - 28/01/2015 - 19:04:11
---A- . (.Microsoft Corporation - Direct3D 10.1 Extensions.) --
C:\Windows\System32\d3dcsx_43.dll   [1907552]
O44 - LFC:[MD5.9D6429F410597750B2DC2579B2347303] - 28/01/2015 - 19:04:11
---A- . (.Microsoft Corporation - Direct3D 10.1 Extensions.) --
C:\Windows\System32\d3dx11_43.dll   [276832]
O44 - LFC:[MD5.ADA0C39D4EACDC81FD84163A95D62079] - 28/01/2015 - 19:04:12
---A- . (.Microsoft Corporation - Direct3D HLSL Compiler.) --
C:\Windows\System32\D3DCompiler_43.dll   [2526056]
O44 - LFC:[MD5.BDEC09A032DB44D9CDB3A0D97224D64E] - 28/01/2015 - 19:04:13
---A- . (.Microsoft Corporation - XACT Engine API.) --
C:\Windows\System32\xactengine3_7.dll   [176984]
O44 - LFC:[MD5.E9739AE8B2FA28DCD6F2EF5525DA8827] - 28/01/2015 - 19:04:16
---A- . (.Microsoft Corporation - Audio Effect Library.) --
C:\Windows\System32\XAPOFX1_5.dll   [77656]
O44 - LFC:[MD5.4F7513FF4DE6303088DB28DCBCEF372C] - 28/01/2015 - 19:04:16
---A- . (.Microsoft Corporation - XAudio2 Game Audio API.) --
C:\Windows\System32\XAudio2_7.dll   [518488]
O44 - LFC:[MD5.93B0550500D1BD86CBAB9C4CC6B6A356] - 31/01/2015 - 11:49:12
---A- . (.Microsoft Corporation - Outil de suppression de logiciels
malveilla.) -- C:\Windows\System32\MRT.exe   [113365784]
O44 - LFC:[MD5.A4DDFE5DC4E73D1FED9B1B3A3D885612] - 31/01/2015 - 16:57:37
---A- . (.Microsoft Corporation - Pas de description.) --
C:\Windows\System32\d3dx9_32.dll   [4398360]
O44 - LFC:[MD5.B739C423276AE62D7AC91773226EC13B] - 31/01/2015 - 16:58:11
---A- . (.Microsoft Corporation - Direct3D 10.1 Extensions.) --
C:\Windows\System32\d3dx10_42.dll   [523088]
~ Files: 23 Scanned in 00mn 10s


---\\ Déni du service (Local Security Authority) (O48)
```

```
O48 - LSA:Local Security Authority Authentication Packages . (.Microsoft
Corporation - Microsoft Authentication Package v1.0.) --
C:\Windows\System32\msv1_0.dll
O48 - LSA:Local Security Authority Notification Packages . (.Microsoft
Corporation - Moteur du client de l'Éditeur de configuration de sécurité
Windows.) -- C:\Windows\System32\scecli.dll
O48 - LSA:Local Security Authority Security Packages . (.Microsoft
Corporation - Package de sécurité Kerberos.) --
C:\Windows\System32\kerberos.dll
O48 - LSA:Local Security Authority Security Packages . (.Microsoft
Corporation - Microsoft Authentication Package v1.0.) --
C:\Windows\System32\msv1_0.dll
O48 - LSA:Local Security Authority Security Packages . (.Microsoft
Corporation - Fournisseur de sécurité TLS/SSL.) --
C:\Windows\System32\schannel.dll
O48 - LSA:Local Security Authority Security Packages . (.Microsoft
Corporation - Microsoft Digest Access.) --
C:\Windows\System32\wdigest.dll
O48 - LSA:Local Security Authority Security Packages . (.Microsoft
Corporation - Web Service Security Package.) --
C:\Windows\System32\tspkg.dll
O48 - LSA:Local Security Authority Security Packages . (.Microsoft
Corporation - Pku2u Security Package.) -- C:\Windows\System32\pku2u.dll
O48 - LSA:Local Security Authority Security Packages . (.Microsoft
Corporation - Live Security Package.) -- C:\Windows\System32\livessp.dll
~ LSA: 9 Scanned in 00mn 00s



---\\ Contrôle du Safe Boot (CSB) (O49)
O49 - CSB:Control Safe Boot HKLM\...\CCS\Minimal\BasicDisplay.sys .
(.Microsoft Corporation - Microsoft Basic Display Driver.) --
C:\Windows\System32\Drivers\BasicDisplay.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Minimal\BasicRender.sys .
(.Microsoft Corporation - Microsoft Basic Render Driver.) --
C:\Windows\System32\Drivers\BasicRender.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Minimal\dxgkrnl.sys .
(.Microsoft Corporation - DirectX Graphics Kernel.) --
C:\Windows\System32\Drivers\dxgkrnl.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Minimal\FsDepends.sys .
(.Microsoft Corporation - File System Dependency Manager Mini Filter
Driver.) -- C:\Windows\System32\Drivers\FsDepends.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Minimal\sermouse.sys .
(.Microsoft Corporation - Pilote de filtre souris série.) --
C:\Windows\System32\Drivers\sermouse.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Minimal\volmgr.sys . (.Microsoft
Corporation - Volume Manager Driver.) --
C:\Windows\System32\Drivers\volmgr.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Minimal\volmgrx.sys .
(.Microsoft Corporation - Pilote d'extension du gestionnaire de volumes.)
-- C:\Windows\System32\Drivers\volmgrx.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\BasicDisplay.sys .
(.Microsoft Corporation - Microsoft Basic Display Driver.) --
C:\Windows\System32\Drivers\BasicDisplay.sys
```

```
O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\BasicRender.sys .
(.Microsoft Corporation - Microsoft Basic Render Driver.) --
C:\Windows\System32\Drivers\BasicRender.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\dxgkrnl.sys .
(.Microsoft Corporation - DirectX Graphics Kernel.) --
C:\Windows\System32\Drivers\dxgkrnl.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\FsDepends.sys .
(.Microsoft Corporation - File System Dependency Manager Mini Filter
Driver.) -- C:\Windows\System32\Drivers\FsDepends.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\ipnat.sys . (.Microsoft
Corporation - IP Network Address Translator.) --
C:\Windows\System32\Drivers\ipnat.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\nsiproxy.sys .
(.Microsoft Corporation - NSI Proxy.) --
C:\Windows\System32\Drivers\nsiproxy.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\rdpencdd.sys . (...) --
C:\Windows\System32\Drivers\rdpencdd.sys (.not file.)
O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\sermouse.sys .
(.Microsoft Corporation - Pilote de filtre souris série.) --
C:\Windows\System32\Drivers\sermouse.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\volmgr.sys . (.Microsoft
Corporation - Volume Manager Driver.) --
C:\Windows\System32\Drivers\volmgr.sys
O49 - CSB:Control Safe Boot HKLM\...\CCS\Network\volmgrx.sys .
(.Microsoft Corporation - Pilote d’extension du gestionnaire de volumes.)
-- C:\Windows\System32\Drivers\volmgrx.sys
~ CSB: 17 Scanned in 00mn 00s


---\\ Clé de registre Shell MountPoints2 (MPSK) (O51)
O51 - MPSK:{007761f5-8875-11e2-be6a-806e6f6e6963}\AutoRun\command.
(.Woonoz SAs - Woonoz.) -- D:\install.exe
~ Keys:  Scanned in 00mn 02s


---\\ Recherche d'infection sur les pilotes (HKLM)(TDSD) (O52)
O52 - TDSD: \Drivers32\"msacm.l3acm"="C:\Windows\System32\l3codeca.acm" .
(.Fraunhofer Institut Integrierte Schaltungen - MPEG Layer-3 Audio Codec
for MSACM.) -- C:\Windows\System32\l3codeca.acm
O52 - TDSD: \drivers.desc\"C:\Windows\System32\l3codeca.acm"="Fraunhofer
IIS MPEG Layer-3 Codec" . (.Fraunhofer Institut Integrierte Schaltungen -
MPEG Layer-3 Audio Codec for MSACM.) -- C:\Windows\System32\l3codeca.acm
~ TDSD: 2 Scanned in 00mn 00s


---\\ Enumération des clés de registre SecurityProviders (MCSP) (O54)
O54 - MCSP:[HKLM\...\CurrentControlSet\Control] - (SecurityProviders) -
(.Microsoft Corporation - Credential Delegation Security Package.) --
C:\Windows\System32\credssp.dll
```

```
O54 - MCSP:[HKLM\...\ControlSet001\Control] - (SecurityProviders) -
(.Microsoft Corporation - Credential Delegation Security Package.) --
C:\Windows\System32\credssp.dll
~ MSCP: 2 Scanned in 00mn 00s


---\\ Enumération des clés de registre PoliciesSystem (MWPS) (O55)
O55 - MWPS:[HKLM\...\Policies\System] - "EnableVirtualization"=1
O55 - MWPS:[HKLM\...\Policies\System] - "EnableInstallerDetection"=1
O55 - MWPS:[HKLM\...\Policies\System] - "EnableLUA"=1
O55 - MWPS:[HKLM\...\Policies\System] - "EnableSecureUIAPaths"=1
O55 - MWPS:[HKLM\...\Policies\System] - "ConsentPromptBehaviorAdmin"=5
O55 - MWPS:[HKLM\...\Policies\System] - "ValidateAdminCodeSignatures"=0
O55 - MWPS:[HKLM\...\Policies\System] - "EnableUIADesktopToggle"=0
O55 - MWPS:[HKLM\...\Policies\System] - "EnableCursorSuppression"=1
O55 - MWPS:[HKLM\...\Policies\System] - "ConsentPromptBehaviorUser"=3
O55 - MWPS:[HKLM\...\Policies\System] - "dontdisplaylastusername"=0
O55 - MWPS:[HKLM\...\Policies\System] - "legalnoticecaption"=0
O55 - MWPS:[HKLM\...\Policies\System] - "legalnoticetext"=0
O55 - MWPS:[HKLM\...\Policies\System] - "scforceoption"=0
O55 - MWPS:[HKLM\...\Policies\System] - "shutdownwithoutlogon"=1
O55 - MWPS:[HKLM\...\Policies\System] - "undockwithoutlogon"=1
O55 - MWPS:[HKLM\...\Policies\System] - "FilterAdministratorToken"=0
O55 - MWPS:[HKLM\...\Policies\System] - "DisableCAD"=1
O55 - MWPS:[HKLM\...\Policies\System] - "DisableTaskMgr"=0
O55 - MWPS:[HKLM\...\Policies\System] - "DisableRegistryTools"=0
O55 - MWPS:[HKLM\...\Policies\System] - "PromptOnSecureDesktop"=0
~ MWPS: 20 Scanned in 00mn 00s


---\\ Enumération des clés de registre PoliciesExplorer (MWPE) (O56)
O56 - MWPE:[HKLM\...\policies\Explorer] - "ForceActiveDesktopOn"=0
O56 - MWPE:[HKLM\...\policies\Explorer] - "NoActiveDesktopChanges"=1
O56 - MWPE:[HKLM\...\policies\Explorer] - "NoActiveDesktop"=1
O56 - MWPE:[HKLM\...\policies\Explorer] - "NoRun"=0
O56 - MWPE:[HKLM\...\policies\Explorer] - "NoControlPanel"=0
~ MWPE Keys: 5 Scanned in 00mn 00s


---\\ Liste des pilotes du système (SDL) (O58)
O58 - SDL:22/08/2013 - 13:43:41 ---A- . (.LSI - LSI 3ware SCSI Storport
Driver.) -- C:\Windows\System32\Drivers\3ware.sys   [108896]
O58 - SDL:22/08/2013 - 13:43:41 ---A- . (.PMC-Sierra - PMC-Sierra
Storport  Driver For SPC8x6G SAS/SATA controller.) --
C:\Windows\System32\Drivers\adp80xx.sys   [782176]
O58 - SDL:22/08/2013 - 13:43:41 ---A- . (.Advanced Micro Devices - AHCI
1.3 Device Driver.) -- C:\Windows\System32\Drivers\amdsata.sys   [79200]
O58 - SDL:22/08/2013 - 13:43:41 ---A- . (.AMD Technologies Inc. - AMD
Technology AHCI Compatible Controller Driver for Windows -.) --
C:\Windows\System32\Drivers\amdsbs.sys   [259424]
```

```
O58 - SDL:22/08/2013 - 13:43:40 ---A- . (.Advanced Micro Devices -
Storage Filter Driver.) -- C:\Windows\System32\Drivers\amdxata.sys
[25952]
O58 - SDL:09/03/2013 - 06:08:22 ---A- . (.Dritek System Inc. - PS/2 KB to
HID Device Driver.) -- C:\Windows\System32\Drivers\aPs2Kb2Hid.sys
[26736]
O58 - SDL:22/08/2013 - 13:43:41 ---A- . (.PMC-Sierra, Inc. - Adaptec SAS
RAID WS03 Driver.) -- C:\Windows\System32\Drivers\arcsas.sys   [114016]
O58 - SDL:02/08/2014 - 16:17:39 ---A- . (...) --
C:\Windows\System32\Drivers\aswHwid.sys   [29208]  =>.ALWIL Software
O58 - SDL:02/08/2014 - 16:17:39 ---A- . (.AVAST Software - avast! File
System Minifilter for Windows 2003/Vista.) --
C:\Windows\System32\Drivers\aswMonFlt.sys   [79184]
O58 - SDL:02/08/2014 - 16:17:38 ---A- . (.AVAST Software - avast! WFP
Redirect Driver.) -- C:\Windows\System32\Drivers\aswRdr2.sys   [93568]
O58 - SDL:02/08/2014 - 16:17:39 ---A- . (...) --
C:\Windows\System32\Drivers\aswRvrt.sys   [65776]  =>.ALWIL Software
O58 - SDL:29/11/2014 - 16:20:08 ---A- . (.AVAST Software - avast!
Virtualization Driver.) -- C:\Windows\System32\Drivers\aswsnx.sys
[1041168]
O58 - SDL:02/08/2014 - 16:18:23 ---A- . (.AVAST Software - avast! self
protection module.) -- C:\Windows\System32\Drivers\aswsp.sys   [427360]
O58 - SDL:02/08/2014 - 16:17:42 ---A- . (.AVAST Software - Stream
Filter.) -- C:\Windows\System32\Drivers\aswStm.sys   [92008]
O58 - SDL:02/08/2014 - 16:17:41 ---A- . (...) --
C:\Windows\System32\Drivers\aswVmm.sys   [224896]  =>.ALWIL Software
O58 - SDL:18/06/2013 - 15:45:02 ---A- . (.Qualcomm Atheros
Communications, Inc. - Qualcomm Atheros Extensible Wireless LAN device
driver.) -- C:\Windows\System32\Drivers\athw8x.sys   [3680256]
O58 - SDL:13/08/2013 - 00:25:46 ---A- . (.Windows (R) Win 7 DDK provider
- BCM Function 2  Device Driver.) --
C:\Windows\System32\Drivers\bcmfn2.sys   [17624]
O58 - SDL:05/12/2012 - 20:25:14 ---A- . (.Qualcomm Atheros - Qualcomm
Atheros A2DP driver.) -- C:\Windows\System32\Drivers\btath_a2dp.sys
[344216]
O58 - SDL:05/12/2012 - 20:25:14 ---A- . (.Qualcomm Atheros - Qualcomm
Atheros Bluetooth AVDT driver.) --
C:\Windows\System32\Drivers\btath_avdt.sys   [114840]
O58 - SDL:05/12/2012 - 20:25:14 ---A- . (.Qualcomm Atheros - Qualcomm
Atheros FILTER driver.) -- C:\Windows\System32\Drivers\btath_flt.sys
[88728]
O58 - SDL:05/12/2012 - 20:25:16 ---A- . (.Qualcomm Atheros - Qualcomm
Atheros HCRP driver.) -- C:\Windows\System32\Drivers\btath_hcrp.sys
[178840]
O58 - SDL:05/12/2012 - 20:25:16 ---A- . (.Qualcomm Atheros - Qualcomm
Atheros FILTER driver.) -- C:\Windows\System32\Drivers\btath_lwflt.sys
[77464]
O58 - SDL:05/12/2012 - 20:25:18 ---A- . (.Qualcomm Atheros - Qualcomm
Atheros AVRCP driver.) -- C:\Windows\System32\Drivers\btath_rcp.sys
[135832]
O58 - SDL:05/12/2012 - 20:25:20 ---A- . (.Qualcomm Atheros - Qualcomm
Atheros BtFilter Driver.) -- C:\Windows\System32\Drivers\btfilter.sys
[576152]
```

O58 - SDL:22/08/2013 - 13:43:41 ---A- . (.Broadcom Corporation - Broadcom NetXtreme II GigE VBD.) -- C:\Windows\System32\Drivers\bxvbda.sys [531296]
O58 - SDL:22/08/2013 - 13:43:45 ---A- . (.Broadcom Corporation - Broadcom NetXtreme II 10 GigE VBD.) -- C:\Windows\System32\Drivers\evbda.sys [3357024]
O58 - SDL:21/08/2012 - 13:01:20 ---A- . (.GEAR Software Inc. - CD DVD Filter.) -- C:\Windows\System32\Drivers\GEARAspiWDM.sys [33240]
O58 - SDL:02/07/2012 - 15:16:02 ---A- . (.Intel Corporation - Intel(R) Management Engine Interface.) -- C:\Windows\System32\Drivers\HECIx64.sys [62784]
O58 - SDL:20/04/2012 - 15:40:58 ---A- . (.McAfee, Inc. - McAfee HIP IPS Driver.) -- C:\Windows\System32\Drivers\HipShieldK.sys [196440]
O58 - SDL:22/08/2013 - 13:43:45 ---A- . (.Hewlett-Packard Company - Smart Array SAS/SATA Controller Media Driver.) -- C:\Windows\System32\Drivers\HpSAMD.sys [64352]
O58 - SDL:30/07/2013 - 19:47:35 ---A- . (.Intel Corporation - Intel(R) Serial IO GPIO Controller Driver.) -- C:\Windows\System32\Drivers\iaLPSSi_GPIO.sys [24568]
O58 - SDL:25/07/2013 - 20:05:39 ---A- . (.Intel Corporation - Intel(R) Serial IO I2C Controller Driver.) -- C:\Windows\System32\Drivers\iaLPSSi_I2C.sys [99320]
O58 - SDL:16/08/2012 - 13:33:42 ---A- . (.Intel Corporation - Intel Rapid Storage Technology driver - x64.) -- C:\Windows\System32\Drivers\iaStorA.sys [645952]
O58 - SDL:10/08/2013 - 01:39:30 ---A- . (.Intel Corporation - Intel Rapid Storage Technology driver (inbox) - x64.) -- C:\Windows\System32\Drivers\iaStorAV.sys [651248]
O58 - SDL:22/08/2013 - 13:43:45 ---A- . (.Intel Corporation - Intel Matrix Storage Manager driver - x64.) -- C:\Windows\System32\Drivers\iaStorV.sys [412000]
O58 - SDL:01/10/2014 - 19:54:16 ---A- . (.Intel Corporation - Intel Graphics Kernel Mode Driver.) -- C:\Windows\System32\Drivers\igdkmd64.sys [3828152]
O58 - SDL:19/06/2012 - 15:40:51 ---A- . (.Intel(R) Corporation - Intel(R) Display Audio Driver.) -- C:\Windows\System32\Drivers\IntcDAud.sys [342528]
O58 - SDL:01/08/2014 - 21:18:33 ---A- . (.Intel Corporation - Intel® WiDi Solution.) -- C:\Windows\System32\Drivers\intelaud.sys [38296]
O58 - SDL:01/08/2014 - 21:18:33 ---A- . (.Intel Corporation - Intel® WiDi Solution.) -- C:\Windows\System32\Drivers\iwdbus.sys [27032]
O58 - SDL:22/08/2013 - 13:43:44 ---A- . (.LSI Corporation - LSI Fusion-MPT SAS Driver (StorPort).) -- C:\Windows\System32\Drivers\lsi_sas.sys [109408]
O58 - SDL:22/08/2013 - 13:43:45 ---A- . (.LSI Corporation - LSI SAS Gen2 Driver (StorPort).) -- C:\Windows\System32\Drivers\lsi_sas2.sys [93536]
O58 - SDL:22/08/2013 - 13:43:44 ---A- . (.LSI Corporation - LSI SAS Gen3 Driver (StorPort).) -- C:\Windows\System32\Drivers\lsi_sas3.sys [81760]
O58 - SDL:22/08/2013 - 13:43:45 ---A- . (.LSI Corporation - LSI SSS PCIe/Flash Driver (StorPort).) -- C:\Windows\System32\Drivers\lsi_sss.sys [82784]
O58 - SDL:21/11/2014 - 06:14:08 ---A- . (.Malwarebytes Corporation - Malwarebytes Anti-Malware.) -- C:\Windows\System32\Drivers\mbam.sys [25816]

```
O58 - SDL:21/11/2014 - 06:14:12 ---A- . (.Malwarebytes Corporation -
Malwarebytes Chameleon Protection Driver.) --
C:\Windows\System32\Drivers\mbamchameleon.sys   [93400]
O58 - SDL:05/02/2015 - 17:14:02 ---A- . (.Malwarebytes Corporation -
Malwarebytes Anti-Malware.) --
C:\Windows\System32\Drivers\MBAMSwissArmy.sys   [129752]
O58 - SDL:22/08/2013 - 13:43:45 ---A- . (.LSI Corporation - MEGASAS RAID
Controller Driver for Windows.) --
C:\Windows\System32\Drivers\megasas.sys   [56672]
O58 - SDL:22/08/2013 - 13:43:45 ---A- . (.LSI Corporation, Inc. - LSI
MegaRAID Software RAID Driver.) -- C:\Windows\System32\Drivers\megasr.sys
[575840]
O58 - SDL:19/02/2013 - 12:55:26 ---A- . (.McAfee, Inc. - McAfee Driver
Cleaning Driver.) -- C:\Windows\System32\Drivers\mfeclnk.sys   [10728]
O58 - SDL:19/02/2013 - 12:55:14 ---A- . (.McAfee, Inc. - McAfee Code
Analysis Driver.) -- C:\Windows\System32\Drivers\mferkdet.sys   [106552]
O58 - SDL:22/08/2013 - 13:43:49 ---A- . (.Marvell Semiconductor, Inc. -
Marvell Flash Controller Driver.) --
C:\Windows\System32\Drivers\mvumis.sys   [63840]
O58 - SDL:21/11/2014 - 06:14:26 ---A- . (.Malwarebytes Corporation -
Malwarebytes Web Access Control.) -- C:\Windows\System32\Drivers\mwac.sys
[64216]
O58 - SDL:17/12/2012 - 13:27:53 ---A- . (.Egis Technology Inc. - PSD Mini
Filter Driver.) -- C:\Windows\System32\Drivers\mwlPSDFilter.sys   [22648]
O58 - SDL:17/12/2012 - 13:27:53 ---A- . (.Egis Technology Inc. -
MyWinLocker PSD Named Pipe Driver.) --
C:\Windows\System32\Drivers\mwlPSDNserv.sys   [20520]
O58 - SDL:17/12/2012 - 13:27:53 ---A- . (.Egis Technology Inc. -
MyWinLocker PSD Virtual Disk Driver.) --
C:\Windows\System32\Drivers\mwlPSDVDisk.sys   [62776]
O58 - SDL:20/04/2010 - 03:35:14 ---A- . (.NTI Corporation - NTI CD-ROM
Filter Driver.) -- C:\Windows\System32\Drivers\NTIDrvr.sys   [18432]
O58 - SDL:22/08/2013 - 13:43:31 ---A- . (.NVIDIA Corporation - NVIDIA®
nForce(TM) RAID Driver.) -- C:\Windows\System32\Drivers\nvraid.sys
[150368]
O58 - SDL:22/08/2013 - 13:43:32 ---A- . (.NVIDIA Corporation - NVIDIA®
nForce(TM) Sata Performance Driver.) --
C:\Windows\System32\Drivers\nvstor.sys   [168288]
O58 - SDL:18/06/2013 - 15:46:17 ---A- . (.Realtek - Realtek
8101E/8168/8169 NDIS 6.30 64-bit Driver.) --
C:\Windows\System32\Drivers\Rt630x64.sys   [591360]
O58 - SDL:03/09/2012 - 01:42:04 ---A- . (.Realtek Semiconductor Corp. -
Realtek(r) High Definition Audio Function Driver.) --
C:\Windows\System32\Drivers\RTKVHD64.sys   [4124176]
O58 - SDL:17/08/2012 - 06:55:26 ---A- . (.Realtek Semiconductor Corp. -
Realtek Pcie CardReader Driver for 2K/XP/Vista/Win7/Win8.) --
C:\Windows\System32\Drivers\RtsBaStor.sys   [288256]
O58 - SDL:22/08/2013 - 16:35:09 ---A- . (.Macrovision Corporation,
Macrovision Europe - Macrovision SECURITY Driver.) --
C:\Windows\System32\Drivers\secdrv.sys   [23040]
O58 - SDL:22/08/2013 - 13:43:31 ---A- . (.Silicon Integrated Systems
Corp. - SiS RAID Stor Miniport Driver.) --
C:\Windows\System32\Drivers\sisraid2.sys   [44896]
```

```
O58 - SDL:22/08/2013 - 13:43:32 ---A- . (.Silicon Integrated Systems -
SiS AHCI Stor-Miniport Driver.) --
C:\Windows\System32\Drivers\sisraid4.sys   [81760]
O58 - SDL:29/11/2012 - 18:05:38 ---A- . (.Synaptics Incorporated -
Synaptics SMBus Driver.) --
C:\Windows\System32\Drivers\Smb_driver_Intel.sys   [31032]
O58 - SDL:22/08/2013 - 13:43:32 ---A- . (.Promise Technology, Inc. -
Promise SuperTrak EX Series Driver for Windows x64.) --
C:\Windows\System32\Drivers\stexstor.sys   [31072]
O58 - SDL:29/11/2012 - 18:05:40 ---A- . (.Synaptics Incorporated -
Synaptics Touchpad Driver.) -- C:\Windows\System32\Drivers\SynTP.sys
[464184]
O58 - SDL:09/07/2010 - 04:51:50 ---A- . (.NTI Corporation - NTI CD-ROM
Filter Driver.) -- C:\Windows\System32\Drivers\UBHelper.sys   [17408]
O58 - SDL:22/08/2013 - 13:43:34 ---A- . (.VIA Technologies, Inc. - VIA
Generic PCI IDE Bus Driver.) -- C:\Windows\System32\Drivers\viaide.sys
[19808]
O58 - SDL:22/08/2013 - 13:43:34 ---A- . (.VIA Technologies Inc.,Ltd - VIA
RAID DRIVER FOR AMD-X86-64.) -- C:\Windows\System32\Drivers\vsmraid.sys
[168800]
O58 - SDL:22/08/2013 - 13:43:34 ---A- . (.VIA Corporation - VIA StorX
RAID Controller Driver.) -- C:\Windows\System32\Drivers\VSTXRAID.SYS
[305504]
~ Drivers: 71 Scanned in 00mn 07s


---\\ Derniers fichiers modifiés ou crées (Utilisateur) (O61)
O61 - LFC: 03/02/2015 - 18:02:06 ---A- . (...) --
C:\Users\Lucie\AppData\Local\Google\Chrome\User
Data\nacl_validation_cache.bin   [272]
O61 - LFC: 04/02/2015 - 18:02:30 ---A- . (...) --
C:\Users\Lucie\AppData\Local\Temp\0004.exe   [30861312]
O61 - LFC: 04/02/2015 - 18:02:30 ---A- . (...) --
C:\Users\Lucie\AppData\Local\Temp\BNKStubSetup.exe   [415672]
O61 - LFC: 04/02/2015 - 18:02:30 ---A- . (...) --
C:\Users\Lucie\AppData\Local\Temp\{91127860-9DA2-44DF-8E36-
87D32B3B24AA}\BrowseFolderDll.dll   [8704]
O61 - LFC: 04/02/2015 - 18:02:30 ---A- . (...) --
C:\Users\Lucie\AppData\Local\Temp\{91127860-9DA2-44DF-8E36-
87D32B3B24AA}\Execute2App.exe   [65536]
O61 - LFC: 04/02/2015 - 18:02:30 ---A- . (...) --
C:\Users\Lucie\AppData\Local\Temp\{91127860-9DA2-44DF-8E36-
87D32B3B24AA}\WiselinkPro.exe   [7381504]
O61 - LFC: 04/02/2015 - 18:02:30 ---A- . (...) --
C:\Users\Lucie\AppData\Local\Temp\{91127860-9DA2-44DF-8E36-
87D32B3B24AA}\WriteDescExecuteFileName.exe   [208896]
O61 - LFC: 04/02/2015 - 18:02:30 ---A- . (...) --
C:\Users\Lucie\AppData\Local\Temp\{91127860-9DA2-44DF-8E36-
87D32B3B24AA}\_isuser_0x040c.dll   [258048]
O61 - LFC: 04/02/2015 - 18:02:30 ---A- . (...) --
C:\Users\Lucie\AppData\Local\Temp\{91127860-9DA2-44DF-8E36-
87D32B3B24AA}\lang.dll   [57856]
```

```
O61 - LFC: 04/02/2015 - 18:02:30 ---A- . (.Acresso Software Inc..) --
C:\Users\Lucie\AppData\Local\Temp\{5D1AA4FA-2BAE-4DAD-86E0-
381342331848}\ISSetup.dll   [9550192]
O61 - LFC: 04/02/2015 - 18:02:30 ---A- . (.Acresso Software Inc..) --
C:\Users\Lucie\AppData\Local\Temp\{91127860-9DA2-44DF-8E36-
87D32B3B24AA}\ISBEW64.exe   [107320]
O61 - LFC: 04/02/2015 - 18:02:30 ---A- . (.Acresso Software Inc..) --
C:\Users\Lucie\AppData\Local\Temp\{91127860-9DA2-44DF-8E36-
87D32B3B24AA}\ISRT.dll   [261424]
O61 - LFC: 04/02/2015 - 18:02:30 ---A- . (.Acresso Software Inc..) --
C:\Users\Lucie\AppData\Local\Temp\{91127860-9DA2-44DF-8E36-
87D32B3B24AA}\_isres_0x040c.dll   [339968]
O61 - LFC: 04/02/2015 - 18:02:30 ---A- . (.Microsoft Corporation.) --
C:\Users\Lucie\AppData\Local\Temp\{91127860-9DA2-44DF-8E36-
87D32B3B24AA}\msvcr90.dll   [655872]
O61 - LFC: 04/02/2015 - 18:02:30 ---A- . (.Samsung Electronics Co.,
Ltd..) -- C:\Users\Lucie\AppData\Local\Temp\{91127860-9DA2-44DF-8E36-
87D32B3B24AA}\setup.exe   [993784]
O61 - LFC: 04/02/2015 - 18:02:30 ---A- . (.TODO: <Company name>.) --
C:\Users\Lucie\AppData\Local\Temp\{91127860-9DA2-44DF-8E36-
87D32B3B24AA}\KiesProgressDialog.dll   [1434624]
O61 - LFC: 04/02/2015 - 18:02:30 ---A- . (.TODO: <회사 이름>.) --
C:\Users\Lucie\AppData\Local\Temp\{91127860-9DA2-44DF-8E36-
87D32B3B24AA}\MSSetupAddinDll.dll   [264704]
O61 - LFC: 04/02/2015 - 18:02:30 ---A- . (.TODO: <회사 이름>.) --
C:\Users\Lucie\AppData\Local\Temp\{91127860-9DA2-44DF-8E36-
87D32B3B24AA}\MSSetupAddinDllForVista.dll   [207360]
O61 - LFC: 05/02/2015 - 18:02:32 ---A- . (...) --
C:\Users\Lucie\Downloads\adwcleaner_4.109.exe   [2194432]
O61 - LFC: 05/02/2015 - 18:02:33 ---A- . (.Malwarebytes Corporation.) --
C:\Users\Lucie\Downloads\mbam-setup-2.0.4.1028.exe   [20447072]
O61 - LFC: 05/02/2015 - 18:02:33 ---A- . (.Nicolas Coolman.) --
C:\Users\Lucie\Downloads\ZHPDiag2-2015.2.2.15.exe   [6870007]  =>.Nicolas
Coolman
O61 - LFC: 31/01/2015 - 18:02:33 ---A- . (.Microsoft Corporation.) --
C:\Users\Lucie\Downloads\wlsetup-web.exe   [1244360]
~ 79 Fichiers temporaires (Temporary files)
~ 3 Fichiers cookies (Cookies files)
~ Files: 22 Scanned in 00mn 38s



---\\ Liste des outils de désinfection (LATC) (O63)
O63 - Logiciel: ZHPDiag 2015 - (.Nicolas Coolman.) [HKLM] -- ZHPDiag_is1
=>.Nicolas Coolman
~ ADS:  Scanned in 00mn 00s



---\\ Associations Shell Spawning (O67)
O67 - Shell Spawning: <.bat> <batfile>[HKLM\..\open\Command] (...) --
"%1" %*
```

```
O67 - Shell Spawning: <.cpl> <cplfile>[HKLM\..\cplopen\Command]
(.Microsoft Corporation - Windows Control Panel.) --
C:\Windows\System32\control.exe  =>.Microsoft Corporation
O67 - Shell Spawning: <.cmd> <cmdfile>[HKLM\..\open\Command] (...) --
"%1" %*
O67 - Shell Spawning: <.com> <comfile>[HKLM\..\open\Command] (...) --
"%1" %*
O67 - Shell Spawning: <.evt> <evtfile>[HKLM\..\open\Command] (.Microsoft
Corporation - Lanceur du composant logiciel enfichable Observateur
d'événements.) -- C:\Windows\System32\eventvwr.exe
O67 - Shell Spawning: <.exe> <exefile>[HKLM\..\open\Command] (...) --
"%1" %*
O67 - Shell Spawning: <.html> <htmlfile>[HKLM\..\open\Command]
(.Microsoft Corporation - Internet Explorer.) -- C:\Program
Files\Internet Explorer\IEXPLORE.exe
O67 - Shell Spawning: <.js> <JSFile>[HKLM\..\open\Command] (.Microsoft
Corporation - Microsoft ® Windows Based Script Host.) --
C:\Windows\System32\WScript.exe
O67 - Shell Spawning: <.reg> <regfile>[HKLM\..\open\Command] (.Microsoft
Corporation - Éditeur du Registre.) -- C:\Windows\regedit.exe
O67 - Shell Spawning: <.scr> <scrfile>[HKLM\..\open\Command] (...) --
"%1" /S
O67 - Shell Spawning: <.html> <ChromeHTML>[HKCU\..\open\Command] (.Not
Key.)
~ FASS Keys: 11 Scanned in 00mn 00s


---\\ Menu de démarrage Internet (SMI) (O68)
O68 - StartMenuInternet: <FIREFOX.EXE> <Mozilla
Firefox>[HKLM\..\Shell\open\Command] (...) -- firefox.exe (.not file.)
O68 - StartMenuInternet: <Google Chrome> <Google
Chrome>[HKLM\..\Shell\open\Command] (.Google Inc. - Google Chrome.) --
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
O68 - StartMenuInternet: <IEXPLORE.EXE> <Internet
Explorer>[HKLM\..\Shell\open\Command] (...) -- C:\Program Files
(x86)\Internet Explorer\iexplore.exe
~ Keys:  Scanned in 00mn 00s


---\\ Recherche d'infection sur les navigateurs internet (SBI) (O69)
O69 - SBI: SearchScopes [HKCU] {0633EE93-D776-472f-A0FF-E1416B8B2E3A}
[DefaultScope] - (Bing) - http://www.bing.com
O69 - SBI: SearchScopes [HKCU] {0b4d26f6-61a8-4463-99dd-5f2fe0400fa6} -
(Recherche sécurisée) - http://fr.search.yahoo.com
O69 - SBI: SearchScopes [HKCU] {B274DC08-D7BC-48C8-9114-80045E2C7272} -
(Binkiland) - http://binkiland.com
~ Keys:  Scanned in 00mn 00s


---\\ Enumère les service demarrés par Svchost (SSS) (O83)
```

O83 - Search Svchost Services: AeLookupSvc (AeLookupSvc) . (.Microsoft Corporation - Service Expérience d'application.) -- C:\Windows\System32\aelupsvc.dll [208896]
O83 - Search Svchost Services: CertPropSvc (CertPropSvc) . (.Microsoft Corporation - Service de propagation de certificats de cartes à puce Microsoft.) -- C:\Windows\System32\certprop.dll [155136]
O83 - Search Svchost Services: SCPolicySvc (SCPolicySvc) . (.Microsoft Corporation - Service de propagation de certificats de cartes à puce Microsoft.) -- C:\Windows\System32\certprop.dll [155136]
O83 - Search Svchost Services: lanmanserver (lanmanserver) . (.Microsoft Corporation - DLL du service Serveur.) -- C:\Windows\System32\srvsvc.dll [324096]
O83 - Search Svchost Services: gpsvc (gpsvc) . (.Microsoft Corporation - Client de stratégie de groupe.) -- C:\Windows\System32\gpsvc.dll [1261056]
O83 - Search Svchost Services: IKEEXT (IKEEXT) . (.Microsoft Corporation - Extension IKE.) -- C:\Windows\System32\ikeext.dll [1063424]
O83 - Search Svchost Services: iphlpsvc (iphlpsvc) . (.Microsoft Corporation - Service offrant une connectivité IPv6 sur un réseau IPv4..) -- C:\Windows\System32\iphlpsvc.dll [914432]
O83 - Search Svchost Services: seclogon (seclogon) . (.Microsoft Corporation - DLL de service d'ouverture de session secondaire.) -- C:\Windows\system32\seclogon.dll [30720]
O83 - Search Svchost Services: AppInfo (AppInfo) . (.Microsoft Corporation - Service Informations d'application.) -- C:\Windows\System32\appinfo.dll [110080]
O83 - Search Svchost Services: msiscsi (msiscsi) . (.Microsoft Corporation - Service de découverte iSCSI.) -- C:\Windows\System32\iscsiexe.dll [150528]
O83 - Search Svchost Services: EapHost (EapHost) . (.Microsoft Corporation - Service EAPHost Microsoft.) -- C:\Windows\System32\eapsvc.dll [107008]
O83 - Search Svchost Services: schedule (schedule) . (.Microsoft Corporation - Service du Planificateur de tâches.) -- C:\Windows\System32\schedsvc.dll [1212928]
O83 - Search Svchost Services: winmgmt (winmgmt) . (.Microsoft Corporation - WMI.) -- C:\Windows\System32\wbem\WMIsvc.dll [220672]
O83 - Search Svchost Services: MMCSS (MMCSS) . (.Microsoft Corporation - Service Planificateur de classes multimédias.) -- C:\Windows\System32\mmcss.dll [70656]
O83 - Search Svchost Services: browser (browser) . (.Microsoft Corporation - DLL du service Explorateur d'ordinateurs.) -- C:\Windows\System32\browser.dll [134144]
O83 - Search Svchost Services: ProfSvc (ProfSvc) . (.Microsoft Corporation - ProfSvc.) -- C:\Windows\System32\profsvc.dll [225280]
O83 - Search Svchost Services: SessionEnv (SessionEnv) . (.Microsoft Corporation - Service Configuration des services Bureau à distance.) -- C:\Windows\System32\sessenv.dll [324096]
O83 - Search Svchost Services: wercplsupport (wercplsupport) . (.Microsoft Corporation - Rapports et solutions aux problèmes.) -- C:\Windows\System32\wercplsupport.dll [81408]
O83 - Search Svchost Services: hkmsvc (hkmsvc) . (.Microsoft Corporation - Service Gestion des clés.) -- C:\Windows\System32\kmsvc.dll [97792]

O83 - Search Svchost Services: BDESVC (BDESVC) . (.Microsoft Corporation - Service BDE.) -- C:\Windows\System32\bdesvc.dll [339456]
O83 - Search Svchost Services: lfsvc (lfsvc) . (.Microsoft Corporation - Service d'infrastructure de localisation Windows.) -- C:\Windows\System32\GeofenceMonitorService.dll [491520]
O83 - Search Svchost Services: wlidsvc (wlidsvc) . (.Microsoft Corporation - Service de compte Microsoft®.) -- C:\Windows\System32\wlidsvc.dll [1576960]
O83 - Search Svchost Services: Themes (Themes) . (.Microsoft Corporation - DLL du service des thèmes Windows Shell.) -- C:\Windows\System32\themeservice.dll [50688]
O83 - Search Svchost Services: DsmSvc (DsmSvc) . (.Microsoft Corporation - Gestionnaire d'installation de périphérique.) -- C:\Windows\System32\DeviceSetupManager.dll [201728]
O83 - Search Svchost Services: NcaSvc (NcaSvc) . (.Microsoft Corporation - Service Assistant Connectivité réseau Microsoft.) -- C:\Windows\System32\ncasvc.dll [164352]
O83 - Search Svchost Services: Rasauto (Rasauto) . (.Microsoft Corporation - Gestionnaire de numérotation automatique d'accès distant.) -- C:\Windows\System32\rasauto.dll [101376]
O83 - Search Svchost Services: Rasman (Rasman) . (.Microsoft Corporation - Gestionnaire des connexions d'accès à distance.) -- C:\Windows\System32\rasmans.dll [534528]
O83 - Search Svchost Services: Remoteaccess (Remoteaccess) . (.Microsoft Corporation - Gestionnaire d'interface dynamique.) -- C:\Windows\System32\mprdim.dll [223744]
O83 - Search Svchost Services: SENS (SENS) . (.Microsoft Corporation - Service de notification d'événements système (SENS).) -- C:\Windows\System32\sens.dll [71680]
O83 - Search Svchost Services: Sharedaccess (Sharedaccess) . (.Microsoft Corporation - Composants de l'application d'assistance à Microsoft NAT.) -- C:\Windows\System32\ipnathlp.dll [433664]
O83 - Search Svchost Services: Tapisrv (Tapisrv) . (.Microsoft Corporation - Serveur de téléphonie Microsoft® Windows(TM).) -- C:\Windows\System32\tapisrv.dll [306688]
O83 - Search Svchost Services: wuauserv (wuauserv) . (.Microsoft Corporation - Agent de mise à jour automatique Windows Update.) -- C:\Windows\System32\wuaueng.dll [3557376]
O83 - Search Svchost Services: BITS (BITS) . (.Microsoft Corporation - Service de transfert intelligent en arrière-plan.) -- C:\Windows\System32\qmgr.dll [1017856]
O83 - Search Svchost Services: ShellHWDetection (ShellHWDetection) . (.Microsoft Corporation - Dll des services Windows Shell.) -- C:\Windows\System32\shsvcs.dll [629760]
~ Services: 34 Scanned in 00mn 01s

---\\ Recherche particulière à la racine du système (SPRF) (O84)
[MD5.C30FF2A7F0CE3A717585A8EC1E751417] [SPRF][02/08/2013] (.Spotify Ltd - Spotify Installer.) -- C:\Users\Lucie\Desktop\SpotifySetup.exe [92776]
[MD5.A75BD3433E4447A609AF0411D68F5261] [SPRF][02/08/2013] (.None - VisualBoyAdvance emulator.) -- C:\Users\Lucie\Desktop\VisualBoyAdvance.exe [1757264]

[MD5.B22198403FFEAF57BE49FF5A08DA1EF4] [SPRF][02/08/2013] (...) -- C:\Users\Lucie\Desktop\vlc-2-0-8-win32.exe [23003252]
[MD5.3FEA9D2EDF23B0283C7A66C8DEA380BD] [SPRF][25/07/2002] (.InstallShield Software Corporation - InstallShield Update Service Setup Player Module.) -- C:\Windows\Downloaded Program Files\dwusplay.dll [24576]
[MD5.CDBE35EA59BC9223E4F800BD1DB82D27] [SPRF][25/07/2002] (.InstallShield Software Corporation - InstallShield Update Service Setup Player.) -- C:\Windows\Downloaded Program Files\dwusplay.exe [196608]
[MD5.3F4413DCD8D3BBABF08F68F25E6D60E1] [SPRF][16/02/2005] (.InstallShield Software Corporation - InstallShield Update Service Web Agent.) -- C:\Windows\Downloaded Program Files\isusweb.dll [401408]
~ Files: 6 Scanned in 00mn 00s

---\\ Enumère les données de la clé NameSpace (MNS) (O92)
O92 - MNS: - {1CF1260C-4DD0-4ebb-811F-33C572699FDE}
O92 - MNS: - {374DE290-123F-4565-9164-39C4925E467B}
O92 - MNS: - {3ADD1653-EB32-4cb0-BBD7-DFA0ABB5ACCA}
O92 - MNS: - {A0953C92-50DC-43bf-BE83-3742FED03C9C}
O92 - MNS: - {A8CDFF1C-4878-43be-B5FD-F8091C1C60D0}
O92 - MNS: - {B4BFCC3A-DB2C-424C-B029-7FE99A87C641}
~ MNS: 6 Scanned in 00mn 00s

---\\ Etat général des services non Microsoft (EGS) (SR=Running, SS=Stopped)
SS - | Demand 05/02/2015 267440 | (AdobeFlashPlayerUpdateSvc) . (.Adobe Systems Incorporated.) - C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe
SS - | Demand 01/10/2014 281488 | (cphs) . (.Intel Corporation.) - C:\Windows\SysWow64\IntelCpHeciSvc.exe
SS - | Demand 16/11/2012 469648 | (DeviceFastLaneService) . (.Acer Incorporated.) - C:\Program Files\Acer\Acer Device Fast-lane\DeviceFastLaneSvc.exe
SS - | Demand 12/07/2012 174160 | (EgisTec Ticket Service) . (.Egis Technology Inc..) - C:\Program Files (x86)\Common Files\EgisTec\Services\EgisTicketService.exe
SS - | Demand 09/03/2013 655624 | (FLEXnet Licensing Service) . (.Acresso Software Inc..) - C:\Program Files (x86)\Common Files\Macrovision Shared\FLEXnet Publisher\FNPLicensingService.exe
SS - | Demand 12/10/2010 206072 | (GamesAppService) . (.WildTangent, Inc..) - C:\Program Files (x86)\WildTangent Games\App\GamesAppService.exe
SS - | Auto 16/06/2013 116648 | (gupdate) . (.Google Inc..) - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
SS - | Demand 16/06/2013 116648 | (gupdatem) . (.Google Inc..) - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
SS - | Demand 20/01/2014 641352 | (iPod Service) . (.Apple Inc..) - C:\Program Files\iPod\bin\iPodService.exe
SS - | Demand 18/08/2014 119408 | (MozillaMaintenance) . (.Mozilla Foundation.) - C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe

SS - | Demand 22/07/1658 0 | (WMPNetworkSvc) . (...) - C:\Program Files (x86)\Windows Media Player\wmpnetwk.exe =>.Microsoft Corporation
SR - | Auto 19/12/2014 81088 | (AdobeARMservice) . (.Adobe Systems Incorporated.) - C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe
SR - | Auto 07/01/2014 43336 | (Apple Mobile Device) . (.Apple Inc..) - C:\Program Files (x86)\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe
SR - | Auto 05/12/2012 231552 | (AtherosSvc) . (.Qualcomm Atheros Commnucations.) - C:\Program Files (x86)\Bluetooth Suite\adminservice.exe
SR - | Auto 02/08/2014 50344 | (avast! Antivirus) . (.AVAST Software.) - C:\Program Files\AVAST Software\Avast\AvastSvc.exe
SR - | Auto 30/08/2011 462184 | (Bonjour Service) . (.Apple Inc..) - C:\Program Files\Bonjour\mDNSResponder.exe
SR - | Auto 25/10/2012 2449552 | (CCDMonitorService) . (.Acer Incorporated.) - C:\Program Files (x86)\Acer\Acer Cloud\CCDMonitorService.exe
SR - | Auto 10/12/2012 350544 | (DsiWMIService) . (.Dritek System Inc..) - C:\Program Files (x86)\Launch Manager\dsiwmis.exe
SR - | Demand 23/10/2012 658064 | (ePowerSvc) . (.Acer Incorporated.) - C:\Program Files\Acer\Acer Power Management\ePowerSvc.exe
SR - | Auto 09/11/2013 227936 | (GamesAppIntegrationService) . (.WildTangent.) - C:\Program Files (x86)\WildTangent Games\App\GamesAppIntegrationService.exe
SR - | Auto 21/10/2014 451416 | (Garmin Core Update Service) . (.Garmin Ltd or its subsidiaries.) - C:\Program Files (x86)\Garmin\Core Update Service\Garmin.Cartography.MapUpdate.CoreService.exe
SR - | Auto 24/07/2012 2457232 | (IconMan_R) . (.Realsil Microelectronics Inc..) - C:\Program Files (x86)\Realtek\Realtek PCIE Card Reader\RIconMan.exe
SR - | Auto 01/10/2014 319376 | (igfxCUIService1.0.0.0) . (.Intel Corporation.) - C:\Windows\System32\igfxCUIService.exe
SR - | Auto 20/04/2012 635104 | (Intel(R) Capability Licensing Service Interface) . (.Intel(R) Corporation.) - C:\Program Files\Intel\iCLS Client\HeciServer.exe
SR - | Auto 25/06/2012 166720 | (jhi_service) . (.Intel Corporation.) - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\DAL\jhi_service.exe
SR - | Auto 17/07/2012 277824 | (LMS) . (.Intel Corporation.) - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe
SR - | Auto 21/11/2014 1871160 | (MBAMScheduler) . (.Malwarebytes Corporation.) - C:\Program Files (x86)\Malwarebytes Anti-Malware\mbamscheduler.exe
SR - | Auto 21/11/2014 969016 | (MBAMService) . (.Malwarebytes Corporation.) - C:\Program Files (x86)\Malwarebytes Anti-Malware\mbamservice.exe
SR - | Auto 18/07/2013 762192 | (NAUpdate) . (.Nero AG.) - C:\Program Files (x86)\Nero\Update\NASvc.exe
SR - | Auto 15/08/2012 3943104 | (NOBU) . (.Symantec Corporation.) - C:\Program Files (x86)\Symantec\Norton Online Backup\NOBuAgent.exe =>.Symantec Corporation
SR - | Auto 03/11/2012 259136 | (NTI IScheduleSvc) . (.NTI Corporation.) - C:\Program Files (x86)\NTI\Acer Backup Manager\IScheduleSvc.exe

SR - | Auto 09/03/2013 96880 | (RfButtonDriverService) . (.Dritek System INC..) - C:\Windows\RfBtnSvc64.exe
SR - | Auto 17/07/2012 365376 | (UNS) . (.Intel Corporation.) - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\UNS\UNS.exe
SR - | Demand 22/07/1658 0 | (WdNisSvc) . (...) - C:\Program Files (x86)\Windows Defender\NisSrv.exe
SR - | Demand 22/07/1658 0 | (WinDefend) . (...) - C:\Program Files (x86)\Windows Defender\MsMpEng.exe
SR - | Demand 22/08/2013 37768 | C:\Windows\System32\wuaueng.dll (wuauserv) . (.Microsoft Corporation.) - C:\Windows\System32\svchost.exe
~ Services: Scanned in 00mn 16s

---\\ Recherche d'infection sur le Master Boot Record (MBR)(O80)
Run by Lucie at 05/02/2015 18:04:30
~ OS 64 not supported by MBR tool
~ MBR: 0 Scanned in 00mn 00s

---\\ Recherche d'infection sur le Master Boot Record (MBRCheck)(O80)
Written by ad13, http://ad13.geekstog
Run by Lucie at 05/02/2015 18:04:32
********* Dump file Name *********
C:\PhysicalDisk0_MBR.bin
~ MBR: Scanned in 00mn 02s

---\\ Scan Additionnel (O88)
Database Version : 13008 - (02/02/2015)
Clés trouvées (Keys found) : 0
Valeurs trouvées (Values found) : 0
Dossiers trouvés (Folders found) : 1
Fichiers trouvés (Files found) : 1

C:\ProgramData\InstallMate   =>PUP.Tarma^
[HKLM\Software\EnigmaSoftwareGroup]   =>PUP.EnigmaSoftware^
~ Additionnel Scan: 307721 Items scanned in 00mn 49s

---\\ Informations complémentaires sur les modules
~ http://nicolascoolman.fr/r5-internet-explorer-proxy-management-iepm/ =>.Internet Explorer, Proxy Management (R5)
~ http://nicolascoolman.fr/o2-browser-helper-objects-de-navigateur/ =>.Browser Helper Objects de navigateur (O2)
~ http://nicolascoolman.fr/o3-internet-explorer-toolbars/ =>.Internet Explorer Toolbars (O3)
~ http://nicolascoolman.fr/o4-applications-demarrees-par-le-registre/ =>.Applications lancées au démarrage du système (O4)

~ http://nicolascoolman.fr/o51-mountpoints2-shell-key-mpsk/ =>.Clé de registre Shell MountPoints2 (MPSK) (O51)
~ AMI: 5 Scanned in 00mn 00s

---\\ Récapitulatif des détections trouvées sur votre station
http://www.nicolascoolman.fr/blog/ =>PUP.EnigmaSoftware
http://nicolascoolman.fr/pup-tarma =>PUP.Tarma
~ MSI: 2 link(s) detected in 00mn 00s

End of the scan (1329 lines in 04mn 57s)(0.11)