~ ZHPDiag v2017.1.12.11 Par Nicolas Coolman (2017/01/12)

~ Démarré par theob (Administrator) (2017/01/13 21:19:08)

~ Web: https://www.nicolascoolman.com

~ Blog: https://www.anti-malware.top

~ Facebook: https://www.facebook.com/nicolascoolman1

~ Etat de la version:

~ Mode: Scanner

~ Rapport: C:\Users\theob\Desktop\ZHPDiag.txt

~ Rapport: C:\Users\theob\AppData\Roaming\ZHP\ZHPDiag.txt

~ UAC: Activate

~ Démarrage du système: Normal (Normal boot)

Windows 10 Home, 64-bit (Build 14393) =>.Microsoft Corporation

---\\ Navigateurs Internet (1) - 0s

~ MSIE: Internet Explorer v11.576.14393.0

---\\ Informations sur les produits Windows (8) - 0s

~ Windows Server License Manager Script : OK

~ Licence Script File Génération : OK

~ Windows(R) Operating System, OEM\_DM channel

Windows ID Activation : OK

~ Windows Partial Key : RGDDQ

Windows License : OK

~ Windows Remaining Initializations Number : 1001

Windows Automatic Updates : OK

---\\ Logiciels de protection (1) - 7s

Windows Defender (Activate) (Protection)

---\\ Informations sur le système (6) - 0s

~ Operating System: Intel64 Family 6 Model 76 Stepping 4, GenuineIntel

~ Operating System: 64-bit

~ Boot mode: Normal (Normal boot)

Total RAM: 4043.82 MB (57% free) : OK =>.RAM Value

System Restore: Activé (Enable)

System drive C: has 138 GB (63%) free of 217 GB : OK =>.Disk Space

---\\ Mode de connexion au système (3) - 0s

~ Computer Name: LAPTOP-0P6GFP5C

~ User Name: theob

~ Logged in as Administrator

---\\ Enumération des unités disques (2) - 0s

~ Drive C: has 138 GB free of 217 GB (System)

~ Drive D: has 24 GB free of 25 GB

---\\ Etat du Centre de Sécurité Windows (7) - 0s

[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: Modified

[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

---\\ Recherche particulière de fichiers génériques (25) - 2s

[MD5.4E10FB1A015B49AC68F76C1A3F4D9C0F] - 11/11/2016 - (.Microsoft Corporation - Explorateur Windows.) -- C:\WINDOWS\Explorer.exe [4673304] =>.Microsoft Windows®

[MD5.C7645D43451C6D94D87F4D07BDE59C89] - 16/07/2016 - (.Microsoft Corporation - Processus hôte Windows (Rundll32).) -- C:\WINDOWS\System32\rundll32.exe [69632] =>.Microsoft Corporation

[MD5.99A19C9A74E2F9820E501DCE77F84F70] - 16/07/2016 - (.Microsoft Corporation - Application de démarrage de Windows.) -- C:\WINDOWS\System32\Wininit.exe [304240] =>.Microsoft Windows Publisher®

[MD5.E584CDC70F694F9A984A060A8291EB04] - 11/11/2016 - (.Microsoft Corporation - Extensions Internet pour Win32.) -- C:\WINDOWS\System32\wininet.dll [2669056] =>.Microsoft Corporation

[MD5.917F081E2AB667C44F7D96DE1D16DFAE] - 14/12/2016 - (.Microsoft Corporation - Application d’ouverture de session Windows.) -- C:\WINDOWS\System32\Winlogon.exe [673792] =>.Microsoft Corporation

[MD5.9600B7F2F89DE60A80D13DE42F672834] - 16/07/2016 - (.Microsoft Corporation - Bibliothèque de licences.) -- C:\WINDOWS\System32\sppcomapi.dll [402432] =>.Microsoft Corporation

[MD5.96B8A433F6407DE34850927C96C6CE9B] - 15/09/2016 - (.Microsoft Corporation - DNS DLL de l’API Client.) -- C:\WINDOWS\System32\dnsapi.dll [646136] =>.Microsoft Windows®

[MD5.227CFE3EDA82029AAC1C088A16297CD7] - 15/09/2016 - (.Microsoft Corporation - DNS DLL de l’API Client.) -- C:\WINDOWS\Syswow64\dnsapi.dll [496872] =>.Microsoft Windows®

[MD5.7ABD5430F75A7FDDE5323B354C77514F] - 16/07/2016 - (.Microsoft Corporation - DLL client de l’API uilisateur de Windows m.) -- C:\WINDOWS\System32\fr-FR\user32.dll.mui [19968] =>.Microsoft Corporation

[MD5.323AA1953ED9C01E23F740FA891FE064] - 15/10/2016 - (.Microsoft Corporation - Pilote de fonction connexe pour WinSock.) -- C:\WINDOWS\System32\drivers\AFD.sys [584032] =>.Microsoft Windows®

[MD5.A10F989A812B57B9695F6C305907C9C6] - 16/07/2016 - (.Microsoft Corporation - ATAPI IDE Miniport Driver.) -- C:\WINDOWS\System32\drivers\atapi.sys [28512] =>.Microsoft Windows®

[MD5.F8FB51B9EF6372610E9B31A1D86B62FC] - 16/07/2016 - (.Microsoft Corporation - CD-ROM File System Driver.) -- C:\WINDOWS\System32\drivers\Cdfs.sys [92160] =>.Microsoft Corporation

[MD5.613D0137C269187FA298A157E3D14A18] - 16/07/2016 - (.Microsoft Corporation - SCSI CD-ROM Driver.) -- C:\WINDOWS\System32\drivers\Cdrom.sys [173056] =>.Microsoft Corporation

[MD5.0D1D392ED2597F295956D058D33BD7C3] - 05/10/2016 - (.Microsoft Corporation - DFS Namespace Client Driver.) -- C:\WINDOWS\System32\drivers\DfsC.sys [144896] =>.Microsoft Corporation

[MD5.10E3515FE5DBA6656FA62C29342EC4A1] - 16/07/2016 - (.Microsoft Corporation - High Definition Audio Bus Driver.) -- C:\WINDOWS\System32\drivers\HDAudBus.sys [83456] =>.Microsoft Corporation

[MD5.B54B30992620C97230013A74461C8517] - 16/07/2016 - (.Microsoft Corporation - Pilote de port i8042.) -- C:\WINDOWS\System32\drivers\i8042prt.sys [114176] =>.Microsoft Corporation

[MD5.F1DAECC3B3D6399875D4F10529D6A77C] - 16/07/2016 - (.Microsoft Corporation - IP Network Address Translator.) -- C:\WINDOWS\System32\drivers\IpNat.sys [212480] =>.Microsoft Corporation

[MD5.E671EDAB0726E05ECEF4058B4CD73C4D] - 07/09/2016 - (.Microsoft Corporation - Minirdr SMB Windows NT.) -- C:\WINDOWS\System32\drivers\MRxSmb.sys [450392] =>.Microsoft Windows®

[MD5.6FEBB0A847FFD5F057B9AC8889F1B9A7] - 16/07/2016 - (.Microsoft Corporation - MBT Transport driver.) -- C:\WINDOWS\System32\drivers\netBT.sys [279040] =>.Microsoft Corporation

[MD5.DB69C6DA8B3DDFDC547D455CA23A8250] - 02/11/2016 - (.Microsoft Corporation - Pilote du système de fichiers NT.) -- C:\WINDOWS\System32\drivers\ntfs.sys [2255712] =>.Microsoft Windows®

[MD5.6B81BF7853D161DB8AC62CD8B9C2DE6B] - 16/07/2016 - (.Microsoft Corporation - Pilote de port parallèle.) -- C:\WINDOWS\System32\drivers\Parport.sys [96768] =>.Microsoft Corporation

[MD5.17E565710172ED71B8531D8822E1C5D1] - 16/07/2016 - (.Microsoft Corporation - RAS L2TP mini-port/call-manager driver.) -- C:\WINDOWS\System32\drivers\Rasl2tp.sys [104960] =>.Microsoft Corporation

[MD5.7135785C21CA79D270D11037C43D3F19] - 16/07/2016 - (.Microsoft Corporation - Redirecteur de périphérique de Microsoft RD.) -- C:\WINDOWS\System32\drivers\rdpdr.sys [177152] =>.Microsoft Corporation

[MD5.9D2DD64A0B51C56285512DC9454340F6] - 16/07/2016 - (.Microsoft Corporation - TDI Translation Driver.) -- C:\WINDOWS\System32\drivers\tdx.sys [118112] =>.Microsoft Windows®

[MD5.BF2546583BB75F01DDA60A7921DFB230] - 16/07/2016 - (.Microsoft Corporation - Volume Shadow Copy driver.) -- C:\WINDOWS\System32\drivers\volsnap.sys [391520] =>.Microsoft Windows®

---\\ Liste des services NT non Microsoft et non désactivés (11) - 2s

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 =>.Adobe Systems, Incorporated®

O23 - Service: Adobe Genuine Software Integrity Service (AGSService) . (.Adobe Systems, Incorporated - Adobe Genuine Software Integrity Service.) - C:\Program Files (x86)\Common Files\Adobe\AdobeGCClient\AGSService.exe =>.Adobe Systems Incorporated®

O23 - Service: @oem21.inf,%ServiceDisplayName%;ESIF Upper Framework Service (esifsvc) . (.Intel Corporation - Intel(R) Dynamic Platform and Thermal Frame.) - C:\Windows\SysWOW64\esif\_uf.exe =>.Intel(R) Software®

O23 - Service: Elan Service (ETDService) . (.ELAN Microelectronics Corp. - Elan Service.) - C:\Program Files\Elantech\ETDService.exe =>.ELAN Microelectronics Corporation®

O23 - Service: Intel(R) PROSet/Wireless Event Log (EvtEng) . (.Intel(R) Corporation - Intel(R) PROSet/Wireless Event Log Service.) - C:\Program Files\Intel\WiFi\bin\EvtEng.exe =>.Intel Corporation-Wireless Connectivity Solutions®

O23 - Service: Intel Bluetooth Service (ibtsiva) . (.Intel Corporation - Intel(R) Wireless Bluetooth(R) iBtSiva Serv.) - C:\Program Files (x86)\Intel\Bluetooth\utilities\ibtsiva.exe =>.Intel Corporation-Wireless Connectivity Solutions®

O23 - Service: Intel(R) HD Graphics Control Panel Service (igfxCUIService2.0.0.0) . (.Intel Corporation - igfxCUIService Module.) - C:\WINDOWS\system32\igfxCUIService.exe =>.Intel Corporation

O23 - Service: Intel(R) Security Assist Helper (isaHelperSvc) . (...) - C:\Program Files (x86)\Intel\Intel(R) Security Assist\isaHelperService.exe =>.Intel Corporation

O23 - Service: Intel(R) Dynamic Application Loader Host Interface (jhi\_service) . (.Intel Corporation - Intel(R) Dynamic Application Loader Host In.) - C:\Program Files (x86)\Intel\TXE Components\DAL\jhi\_service.exe =>.Intel Corporation - Embedded Subsystems and IP Blocks Group®

O23 - Service: Intel(R) PROSet/Wireless Registry Service (RegSrvc) . (.Intel(R) Corporation - Intel(R) PROSet/Wireless Registry Service.) - C:\Program Files\Common Files\Intel\WirelessCommon\RegSrvc.exe =>.Intel Corporation-Wireless Connectivity Solutions®

O23 - Service: Intel(R) PROSet/Wireless Zero Configuration Service (ZeroConfigService) . (.Intel® Corporation - Intel® PROSet/Wireless Zero Configure Servi.) - C:\Program Files\Intel\WiFi\bin\ZeroConfigService.exe =>.Intel Corporation-Wireless Connectivity Solutions®

---\\ Services non Microsoft (SR=Démarré,SS=Stoppé) (15) - 32s

SR - Auto [01/10/2016] [ 82128] Adobe Acrobat Update Service (AdobeARMservice) . (.Adobe Systems Incorporated.) - C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe =>.Adobe Systems, Incorporated®

SR - Auto [26/09/2016] [ 2207960] Adobe Genuine Software Integrity Service (AGSService) . (.Adobe Systems, Incorporated.) - C:\Program Files (x86)\Common Files\Adobe\AdobeGCClient\AGSService.exe =>.Adobe Systems Incorporated®

SS - Demand [26/01/2016] [ 282744] Intel(R) Content Protection HECI Service (cphs) . (.Intel Corporation.) - C:\Windows\SysWOW64\IntelCpHeciSvc.exe =>.Intel Corporation - pGFX®

SR - Auto [07/08/2015] [ 1385640] @oem21.inf,%ServiceDisplayName%;ESIF Upper Framework Service (esifsvc) . (.Intel Corporation.) - C:\Windows\SysWOW64\esif\_uf.exe =>.Intel(R) Software®

SR - Auto [08/01/2016] [ 134880] Elan Service (ETDService) . (.ELAN Microelectronics Corp..) - C:\Program Files\Elantech\ETDService.exe =>.ELAN Microelectronics Corporation®

SR - Auto [09/07/2015] [ 640928] Intel(R) PROSet/Wireless Event Log (EvtEng) . (.Intel(R) Corporation.) - C:\Program Files\Intel\WiFi\bin\EvtEng.exe =>.Intel Corporation-Wireless Connectivity Solutions®

SR - Auto [31/07/2015] [ 150256] Intel Bluetooth Service (ibtsiva) . (.Intel Corporation.) - C:\Program Files (x86)\Intel\Bluetooth\utilities\ibtsiva.exe =>.Intel Corporation-Wireless Connectivity Solutions®

SR - Auto [26/01/2016] [ 354936] Intel(R) HD Graphics Control Panel Service (igfxCUIService2.0.0.0) . (.Intel Corporation.) - C:\WINDOWS\system32\igfxCUIService.exe =>.Intel Corporation - pGFX®

SS - Demand [03/09/2015] [ 887784] Intel(R) Capability Licensing Service TCP IP Interface (Intel(R) Capability Licensing Service TCP IP Interface) . (.Intel(R) Corporation.) - C:\Program Files\Intel\TXE Components\TCS\SocketHeciServer.exe =>.Intel® Trusted Connect Service®

SS - Demand [19/05/2015] [ 335872] Intel(R) Security Assist (Intel(R) Security Assist) . (.Intel Corporation.) - C:\Program Files (x86)\Intel\Intel(R) Security Assist\isa.exe =>.Intel Corporation

SR - Auto [19/05/2015] [ 7680] Intel(R) Security Assist Helper (isaHelperSvc) . (...) - C:\Program Files (x86)\Intel\Intel(R) Security Assist\isaHelperService.exe =>.Intel Corporation

SR - Auto [21/04/2015] [ 174368] Intel(R) Dynamic Application Loader Host Interface (jhi\_service) . (.Intel Corporation.) - C:\Program Files (x86)\Intel\TXE Components\DAL\jhi\_service.exe =>.Intel Corporation - Embedded Subsystems and IP Blocks Group®

SS - Demand [09/07/2015] [ 268192] Wireless PAN DHCP Server (MyWiFiDHCPDNS) . (.Copyright (C) 2005-2010 by Achal Dhir.) - C:\Program Files\Intel\WiFi\bin\PanDhcpDns.exe =>.Intel Corporation-Wireless Connectivity Solutions®

SR - Auto [09/07/2015] [ 157088] Intel(R) PROSet/Wireless Registry Service (RegSrvc) . (.Intel(R) Corporation.) - C:\Program Files\Common Files\Intel\WirelessCommon\RegSrvc.exe =>.Intel Corporation-Wireless Connectivity Solutions®

SR - Auto [09/07/2015] [ 3831712] Intel(R) PROSet/Wireless Zero Configuration Service (ZeroConfigService) . (.Intel® Corporation.) - C:\Program Files\Intel\WiFi\bin\ZeroConfigService.exe =>.Intel Corporation-Wireless Connectivity Solutions®

---\\ Tâches planifiées en automatique (4) - 4s

[MD5.48515EEA1608ECD83FE26C7490460F59] [APT] [AdobeAAMUpdater-1.0-MicrosoftAccount-theo.bastide@gmail.com] (.Adobe Systems Incorporated.) -- C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\UWA\UpdaterStartupUtility.exe [508128] (.Activate.) =>.Adobe Systems Incorporated®

[MD5.00000000000000000000000000000000] [APT] [Microsoft\Office\Office 15 Subscription Heartbeat] (...) -- C:\Program Files\Common Files\Microsoft Shared\Office15\OLicenseHeartbeat.exe (.not file.) [0] (.Activate.) =>.Superfluous.Empty

O39 - APT: AdobeAAMUpdater-1.0-MicrosoftAccount-theo.bastide@gmail.com - (.Adobe Systems Incorporated.) -- C:\WINDOWS\System32\Tasks\AdobeAAMUpdater-1.0-MicrosoftAccount-theo.bastide@gmail.com [2806] =>.Adobe Systems Incorporated®

O39 - APT: Unknown - (.Microsoft Corporation.) -- C:\WINDOWS\System32\Tasks\OneDrive Standalone Update Task v2 [2768] =>.Microsoft Corporation

---\\ Applications lancées au démarrage du système (11) - 0s

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\_LENOVO\_DOLBYDRAGON] . (.Realtek Semiconductor - HD Audio Background Process.) -- C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe =>.Realtek Semiconductor Corp.®

O4 - HKLM\..\Run: [RtHDVBg\_LENOVO\_MICPKEY] . (.Realtek Semiconductor - HD Audio Background Process.) -- C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe =>.Realtek Semiconductor Corp.®

O4 - HKLM\..\Run: [LenovoUtility] . (.Copyright 2014 - Lenovo Utility.) -- C:\Program Files\Lenovo\LenovoUtility\utility.exe =>.LENOVO®

O4 - HKLM\..\Run: [AdobeAAMUpdater-1.0] . (.Adobe Systems Incorporated - Adobe Updater Startup Utility.) -- C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\UWA\UpdaterStartupUtility.exe =>.Adobe Systems Incorporated®

O4 - HKLM\..\Run: [WindowsDefender] . (.Microsoft Corporation - Windows Defender notification icon.) -- C:\Program Files\Windows Defender\MSASCuiL.exe =>.Microsoft Corporation

O4 - HKCU\..\Run: [OneDrive] . (.Microsoft Corporation - Microsoft OneDrive.) -- C:\Users\theob\AppData\Local\Microsoft\OneDrive\OneDrive.exe =>.Microsoft Corporation®

O4 - HKLM\..\Wow6432Node\Run: [Adobe ARM] . (.Adobe Systems Incorporated - Adobe Reader and Acrobat Manager.) -- C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe =>.Adobe Systems, Incorporated®

O4 - HKUS\S-1-5-19\..\Run: [OneDriveSetup] . (.Microsoft Corporation - Microsoft OneDrive Setup.) -- C:\Windows\SysWOW64\OneDriveSetup.exe =>.Microsoft Corporation®

O4 - HKUS\S-1-5-20\..\Run: [OneDriveSetup] . (.Microsoft Corporation - Microsoft OneDrive Setup.) -- C:\Windows\SysWOW64\OneDriveSetup.exe =>.Microsoft Corporation®

O4 - HKUS\S-1-5-21-3289622345-69416996-2806818222-1001\..\Run: [OneDrive] . (.Microsoft Corporation - Microsoft OneDrive.) -- C:\Users\theob\AppData\Local\Microsoft\OneDrive\OneDrive.exe =>.Microsoft Corporation®

---\\ Processus lancés (26) - 3s

[MD5.00000000000000000000000000000000] - (.Intel Corporation - igfxCUIService Module.) -- C:\WINDOWS\system32\igfxCUIService.exe [0] [PID.1532] =>.Intel Corporation

[MD5.DC00FD73505DAEDD99CAF4533B0C05BD] - (.Adobe Systems Incorporated - Adobe Acrobat Update Service.) -- C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe [82128] [PID.2464] =>.Adobe Systems, Incorporated®

[MD5.8A00CC653B8F02503C250FC1B9475807] - (.Intel Corporation - Intel(R) Dynamic Platform and Thermal Frame.) -- C:\Windows\SysWOW64\esif\_uf.exe [1385640] [PID.2476] =>.Intel(R) Software®

[MD5.E03BE7755C3883A2287575570DA92289] - (.Intel(R) Corporation - Intel(R) PROSet/Wireless Event Log Service.) -- C:\Program Files\Intel\WiFi\bin\EvtEng.exe [640928] [PID.2484] =>.Intel Corporation-Wireless Connectivity Solutions®

[MD5.1DFC3CCA51785254C5604238BB1A5467] - (...) -- C:\Program Files (x86)\Intel\Intel(R) Security Assist\isaHelperService.exe [7680] [PID.2488] =>.Intel Corporation

[MD5.69025F25D2269AB5E5268286999B3C8A] - (.Intel Corporation - Intel(R) Wireless Bluetooth(R) iBtSiva Serv.) -- C:\Program Files (x86)\Intel\Bluetooth\utilities\ibtsiva.exe [150256] [PID.2500] =>.Intel Corporation-Wireless Connectivity Solutions®

[MD5.021D06851E7AFF5C314039DF813608F3] - (.Adobe Systems, Incorporated - Adobe Genuine Software Integrity Service.) -- C:\Program Files (x86)\Common Files\Adobe\AdobeGCClient\AGSService.exe [2207960] [PID.2512] =>.Adobe Systems Incorporated®

[MD5.193026DD0B72B560A798F8DA9A38679A] - (.Intel(R) Corporation - Intel(R) PROSet/Wireless Registry Service.) -- C:\Program Files\Common Files\Intel\WirelessCommon\RegSrvc.exe [157088] [PID.2532] =>.Intel Corporation-Wireless Connectivity Solutions®

[MD5.17D8BC702D933BC83DE5894547412179] - (.ELAN Microelectronics Corp. - Elan Service.) -- C:\Program Files\Elantech\ETDService.exe [134880] [PID.2540] =>.ELAN Microelectronics Corporation®

[MD5.A2859A7B82A1B840AF33E68455E058D9] - (.Intel® Corporation - Intel® PROSet/Wireless Zero Configure Servi.) -- C:\Program Files\Intel\WiFi\bin\ZeroConfigService.exe [3831712] [PID.2680] =>.Intel Corporation-Wireless Connectivity Solutions®

[MD5.CEBBD45985EB8D30A37B6E8D22DCAB11] - (.Intel Corporation - Intel(R) Dynamic Platform and Thermal Frame.) -- C:\Windows\Temp\DPTF\esif\_assist\_64.exe [257192] [PID.3612] =>.Intel(R) Software®

[MD5.17F80F313159160B2A98E2D32AF8574A] - (.ELAN Microelectronics Corp. - ETD Control Center.) -- C:\Program Files\Elantech\ETDCtrl.exe [3763432] [PID.3644] =>.ELAN Microelectronics Corporation®

[MD5.00000000000000000000000000000000] - (.Intel Corporation - igfxEM Module.) -- C:\WINDOWS\system32\igfxEM.exe [0] [PID.4568] =>.Intel Corporation

[MD5.00000000000000000000000000000000] - (.Intel Corporation - igfxHK Module.) -- C:\WINDOWS\system32\igfxHK.exe [0] [PID.4600] =>.Intel Corporation

[MD5.00000000000000000000000000000000] - (.Auteurs - .) -- C:\WINDOWS\system32\igfxTray.exe [0] [PID.4652] =>.Intel Corporation

[MD5.814C8768A991D458268CFBC9E70030E8] - (.ELAN Microelectronics Corp. - ETD Control Center Helper.) -- C:\Program Files\Elantech\ETDCtrlHelper.exe [2654440] [PID.4720] =>.ELAN Microelectronics Corporation®

[MD5.C1ED6E34FC5206C34BA09A899F22A7F3] - (.ELAN Microelectronics Corp. - ETDIntelligent.) -- C:\Program Files\Elantech\ETDIntelligent.exe [2267360] [PID.4796] =>.ELAN Microelectronics Corporation®

[MD5.D5A2D371E4704137CD41A912232B0BBA] - (...) -- C:\Program Files\WindowsApps\Microsoft.SkypeApp\_11.10.145.0\_x64\_\_kzf8qxf38zg5c\SkypeHost.exe [72192] [PID.5212] =>.Skype Technologies

[MD5.03D9717B58D67F0B321DD413952F712E] - (.Realtek Semiconductor - Gestionnaire audio HD Realtek.) -- C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe [16418560] [PID.5668] =>.Realtek Semiconductor Corp®

[MD5.80FF74C2D410B7DDFAF7A6F9D33CEACB] - (.Realtek Semiconductor - HD Audio Background Process.) -- C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe [1410168] [PID.2580] =>.Realtek Semiconductor Corp.®

[MD5.80FF74C2D410B7DDFAF7A6F9D33CEACB] - (.Realtek Semiconductor - HD Audio Background Process.) -- C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe [1410168] [PID.3184] =>.Realtek Semiconductor Corp.®

[MD5.772123B2276B94C797659AEDC0D49943] - (.Copyright 2014 - Lenovo Utility.) -- C:\Program Files\Lenovo\LenovoUtility\utility.exe [791848] [PID.5912] =>.LENOVO®

[MD5.959F100D1BC00D7BCDE44BF1D9A835C7] - (.Adobe Systems Incorporated - Adobe Reader and Acrobat Manager.) -- C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe [1156824] [PID.5616] =>.Adobe Systems, Incorporated®

[MD5.B85D41C1FA947398D253F7D4C74EE517] - (.Adobe Systems Inc. - AcroTray.) -- C:\Program Files (x86)\Adobe\Acrobat 11.0\Acrobat\acrotray.exe [3498720] [PID.6160] =>.Adobe Systems, Incorporated®

[MD5.DCEABCDB2EAF57CEDEF5FD5D017ABE1D] - (.Intel Corporation - Intel(R) Dynamic Application Loader Host In.) -- C:\Program Files (x86)\Intel\TXE Components\DAL\jhi\_service.exe [174368] [PID.7768] =>.Intel Corporation - Embedded Subsystems and IP Blocks Group®

[MD5.3CCD57D9CB41AC322B161654E5DA14F8] - (.Nicolas Coolman - ZHPDiag.) -- C:\Users\theob\AppData\Roaming\ZHP\ZHPDiag3.exe [2642944] [PID.7968] =>.Nicolas Coolman

---\\ Firefox, Plugins,Demarrage,Recherche,Extensions (1) - 1s

P2 - EXT: (.Microsoft Corporation - The plugin allows you to have a better expe.) -- C:\Program Files (x86)\Mozilla Firefox\Plugins\npMeetingJoinPluginOC.dll =>.Microsoft Corporation®

---\\ Internet Explorer,Démarrage,Recherche,URLSearchHook (19) - 0s

R0 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = http://go.microsoft.com/ =>.Microsoft Corporation

R0 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = http://go.microsoft.com/ =>.Microsoft Corporation

R0 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main,Start Page = http://go.microsoft.com/ =>.Microsoft Corporation

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

R1 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Default\_Page\_URL = http://lenovo15.msn.com/ =>.Microsoft Corporation

R1 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Default\_Secondary\_Page\_URL = http://www.lenovo.com =>.Lenovo Group Limited

R1 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Search Bar = preserve =>.Microsoft Corporation

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

R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Default\_Page\_URL = http://go.microsoft.com/ =>.Microsoft Corporation

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

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

R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Default\_Search\_URL = http://go.microsoft.com/ =>.Microsoft Corporation

R1 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft.com/ =>.Microsoft Corporation

R1 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main,Default\_Page\_URL = http://go.microsoft.com/ =>.Microsoft Corporation

R1 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main,Default\_Search\_URL = http://go.microsoft.com/ =>.Microsoft Corporation

R1 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main,Extensions Off Page = about:noadd-ons =>.Microsoft Corporation

R1 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main,Security Risk Page = about:securityrisk =>.Microsoft Corporation

R1 - HKEY\_USERS\S-1-5-21-3289622345-69416996-2806818222-1001\SOFTWARE\Microsoft\Internet Explorer\Main,Search Bar = preserve =>.Microsoft Corporation

R3 - URLSearchHook: (no name) - {CFBFAE00-17A6-11D0-99CB-00C04FD64497} Orphan =>.Microsoft Internet Explorer

---\\ Internet Explorer,Proxy Management (10) - 0s

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,ProxyHttp1.1 = 0

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

R5 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyOverride = <-loopback>

R5 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyServer = http=127.0.0.1:8080;https=127.0.0.1:8080

R5 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyEnable = 1

R5 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings,MigrateProxy = 1

R5 - HKLM\SYSTEM\CurrentControlSet\services\NlaSvc\Parameters\Internet\ManualProxies [1http=127.0.0.1:8080;https=127.0.0.1:8080]

---\\ Internet Explorer,IniFiles, Autoloading programs (3) - 0s

F2 - REG:system.ini: UserInit=

F2 - REG:system.ini: Shell=C:\WINDOWS\explorer.exe (.Microsoft Corporation.) =>.Microsoft Corporation

F2 - REG:system.ini: VMApplet=

---\\ Etude du fichier hosts (1) - 0s

~ Le fichier hôte est sain (The hosts file is clean) (32)

---\\ Browser Helper Object de navigateur (BHO) (4) - 0s

O2 - BHO: Skype for Business Click to Call BHO [64Bits] - {31D09BA0-12F5-4CCE-BE8A-2923E76605DA} . (.Microsoft Corporation - Skype for Business.) -- C:\Program Files (x86)\Microsoft Office\Office15\OCHelper.dll =>.Microsoft Corporation®

O2 - BHO: Adobe Acrobat Create PDF Helper [64Bits] - {AE7CD045-E861-484f-8273-0445EE161910} . (.Adobe Systems Incorporated - Adobe PDF Toolbar for Internet Explorer.) -- C:\Program Files (x86)\Common Files\Adobe\Acrobat\WCIEActiveX\AcroIEFavClient.dll =>.Adobe Systems, Incorporated®

O2 - BHO: Microsoft SkyDrive Pro Browser Helper [64Bits] - {D0498E0A-45B7-42AE-A9AA-ABA463DBD3BF} . (.Microsoft Corporation - Microsoft OneDrive for Business Extensions.) -- C:\Program Files (x86)\Microsoft Office\Office15\GROOVEEX.DLL =>.Microsoft Corporation®

O2 - BHO: SmartSelect [64Bits] - {F4971EE7-DAA0-4053-9964-665D8EE6A077} . (.Adobe Systems Incorporated - Adobe PDF Toolbar for Internet Explorer.) -- C:\Program Files (x86)\Common Files\Adobe\Acrobat\WCIEActiveX\AcroIEFavClient.dll =>.Adobe Systems, Incorporated®

---\\ Raccourcis Global Startup (41) - 4s

O4 - GS\Desktop [Administrateur]: ZHPCleaner.lnk . (.Nicolas Coolman - ZHPCleane.) C:\Users\theob\AppData\Roaming\ZHP\ZHPCleaner.exe =>.Nicolas Coolman

O4 - GS\Desktop [Administrateur]: ZHPDiag.lnk . (.Nicolas Coolman - ZHPDiag.) C:\Users\theob\AppData\Roaming\ZHP\ZHPDiag3.exe =>.Nicolas Coolman

O4 - GS\Quicklaunch [Administrateur]: Microsoft Outlook.lnk . (.Microsoft Corporation - Microsoft Outlook.) C:\Program Files (x86)\Microsoft Office\Office15\OUTLOOK.EXE /recycle =>.Microsoft Corporation®

O4 - GS\sendTo [Administrateur]: Destinataire de télécopie.lnk . (.Microsoft Corporation - Microsoft Windows Fax and Scan.) C:\Windows\System32\WFS.exe /SendTo =>.Microsoft Corporation

O4 - GS\sendTo [Administrateur]: Fax Recipient.lnk . (.Microsoft Corporation - Microsoft Windows Fax and Scan.) C:\WINDOWS\system32\WFS.exe /SendTo =>.Microsoft Corporation

O4 - GS\sendTo [Administrateur]: Transfert de fichiers Bluetooth.LNK . (.Microsoft Corporation - .) C:\Windows\System32\fsquirt.exe =>.Microsoft Corporation

O4 - GS\TaskBar [Administrateur]: Outlook 2013.lnk . (...) C:\Windows\Installer\{90150000-0011-0000-0000-0000000FF1CE}\outicon.exe =>.Microsoft Corporation®

O4 - GS\Programs [Administrateur]: OneDrive.lnk . (.Microsoft Corporation - Microsoft OneDrive.) C:\Users\theob\AppData\Local\Microsoft\OneDrive\OneDrive.exe =>.Microsoft Corporation®

O4 - GS\Desktop [theob]: ZHPCleaner.lnk . (.Nicolas Coolman - ZHPCleane.) C:\Users\theob\AppData\Roaming\ZHP\ZHPCleaner.exe =>.Nicolas Coolman

O4 - GS\Desktop [theob]: ZHPDiag.lnk . (.Nicolas Coolman - ZHPDiag.) C:\Users\theob\AppData\Roaming\ZHP\ZHPDiag3.exe =>.Nicolas Coolman

O4 - GS\Quicklaunch [theob]: Microsoft Outlook.lnk . (.Microsoft Corporation - Microsoft Outlook.) C:\Program Files (x86)\Microsoft Office\Office15\OUTLOOK.EXE /recycle =>.Microsoft Corporation®

O4 - GS\sendTo [theob]: Destinataire de télécopie.lnk . (.Microsoft Corporation - Microsoft Windows Fax and Scan.) C:\Windows\System32\WFS.exe /SendTo =>.Microsoft Corporation

O4 - GS\sendTo [theob]: Fax Recipient.lnk . (.Microsoft Corporation - Microsoft Windows Fax and Scan.) C:\WINDOWS\system32\WFS.exe /SendTo =>.Microsoft Corporation

O4 - GS\sendTo [theob]: Transfert de fichiers Bluetooth.LNK . (.Microsoft Corporation - .) C:\Windows\System32\fsquirt.exe =>.Microsoft Corporation

O4 - GS\TaskBar [theob]: Outlook 2013.lnk . (...) C:\Windows\Installer\{90150000-0011-0000-0000-0000000FF1CE}\outicon.exe =>.Microsoft Corporation®

O4 - GS\Programs [theob]: OneDrive.lnk . (.Microsoft Corporation - Microsoft OneDrive.) C:\Users\theob\AppData\Local\Microsoft\OneDrive\OneDrive.exe =>.Microsoft Corporation®

O4 - GS\CommonDesktop [Public]: Adobe Acrobat XI Pro.lnk . (.Adobe Systems Incorporated - Adobe Acrobat.) C:\Program Files (x86)\Adobe\Acrobat 11.0\Acrobat\Acrobat.exe =>.Adobe Systems, Incorporated®

O4 - GS\CommonDesktop [Public]: Adobe FormsCentral.lnk . (...) C:\Program Files (x86)\Adobe\Acrobat 11.0\FormsCentral\FormsCentralForAcrobat.exe =>.Adobe Systems, Incorporated®

O4 - GS\Programs [Public]: OneDrive.lnk . (.Microsoft Corporation - Microsoft OneDrive.) C:\Users\theob\AppData\Local\Microsoft\OneDrive\OneDrive.exe =>.Microsoft Corporation®

O4 - GS\Accessories [Public]: Internet Explorer.lnk . (.Microsoft Corporation - Internet Explorer.) C:\Program Files (x86)\Internet Explorer\iexplore.exe =>.Microsoft Corporation®

O4 - GS\Accessories [Public]: Notepad.lnk . (.Microsoft Corporation - Bloc-notes.) C:\WINDOWS\system32\notepad.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Math Input Panel.lnk . (.Microsoft Corporation - .) C:\Program Files (x86)\Common Files\Microsoft Shared\Ink\mip.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Paint.lnk . (.Microsoft Corporation - Paint.) C:\WINDOWS\system32\mspaint.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Quick Assist.lnk . (.Microsoft Corporation - Quick Assist.) C:\WINDOWS\system32\quickassist.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Remote Desktop Connection.lnk . (.Microsoft Corporation - Connexion Bureau à distance.) C:\WINDOWS\system32\mstsc.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Snipping Tool.lnk . (.Microsoft Corporation - Outil Capture d’écran.) C:\WINDOWS\system32\SnippingTool.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Steps Recorder.lnk . (.Microsoft Corporation - Enregistreur d’actions.) C:\WINDOWS\system32\psr.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Windows Fax and Scan.lnk . (.Microsoft Corporation - Microsoft Windows Fax and Scan.) C:\WINDOWS\system32\WFS.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Windows Media Player.lnk . (.Microsoft Corporation - Lecteur Windows Media.) C:\Program Files (x86)\Windows Media Player\wmplayer.exe /prefetch:1 =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Wordpad.lnk . (.Microsoft Corporation - Application Windows Wordpad.) C:\Program Files (x86)\Windows NT\Accessories\wordpad.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: XPS Viewer.lnk . (.Microsoft Corporation - Visionneuse XPS.) C:\WINDOWS\system32\xpsrchvw.exe =>.Microsoft Corporation

O4 - GS\SystemTools [Public]: Character Map.lnk . (.Microsoft Corporation - Table des caractères.) C:\WINDOWS\system32\charmap.exe =>.Microsoft Corporation

O4 - GS\ProgramsCommon [Public]: Adobe Acrobat Distiller XI.lnk . (.Adobe Systems Incorporated. - Acrobat Distiller.) C:\Program Files (x86)\Adobe\Acrobat 11.0\Acrobat\acrodist.exe =>.Adobe Systems, Incorporated®

O4 - GS\ProgramsCommon [Public]: Adobe Acrobat XI Pro.lnk . (...) C:\Windows\Installer\{AC76BA86-1033-FFFF-7760-000000000006}\\_SC\_Acrobat.ico

O4 - GS\ProgramsCommon [Public]: Adobe FormsCentral.lnk . (...) C:\Program Files (x86)\Adobe\Acrobat 11.0\FormsCentral\FormsCentralForAcrobat.exe =>.Adobe Systems, Incorporated®

O4 - GS\ProgramsCommon [Public]: Adobe Photoshop CC 2015 (32 Bit).lnk . (.Adobe Systems, Incorporated - Adobe Photoshop CC 2015.) C:\Program Files (x86)\Adobe\Adobe Photoshop CC 2015 (32 Bit)\Photoshop.exe =>.Adobe Systems Incorporated®

O4 - GS\ProgramsCommon [Public]: Immersive Control Panel.lnk . (.Microsoft Corporation - Windows Control Panel.) C:\WINDOWS\System32\Control.exe =>.Microsoft Corporation

O4 - GS\ProgramsCommon [Public]: Intel(R) HD Graphics Control Panel.lnk . (.Intel Corporation - GFXUIEX Module.) C:\Windows\system32\GfxUIEx.exe =>.Intel Corporation

O4 - GS\ProgramsCommon [Public]: MiracastView.lnk . (.Microsoft Corporation - MiracastView.) C:\WINDOWS\MiracastView\MiracastView.exe =>.Microsoft Windows®

O4 - GS\ProgramsCommon [Public]: PrintDialog.lnk . (.Microsoft Corporation - Print Dialog.) C:\WINDOWS\PrintDialog\PrintDialog.exe =>.Microsoft Windows®

O4 - GS\ProgramsCommon [Public]: Windows Media Player.lnk . (.Microsoft Corporation - Lecteur Windows Media.) C:\Program Files (x86)\Windows Media Player\wmplayer.exe /prefetch:1 =>.Microsoft Corporation

---\\ Modification Domaine/Adresses DNS (2) - 0s

O17 - HKLM\System\CCS\Services\Tcpip\Parameters: DhcpNameServer = 192.168.0.254 =>.Local IP Adress

O17 - HKLM\System\CCS\Services\Tcpip\..\{8b67c681-3e4c-4bab-9cbb-8d8b8a1d2e49}: DhcpNameServer = 192.168.0.254 =>.Local IP Adress

---\\ Protocole additionnel (25) - 0s

O18 - Handler: about [64Bits] - {3050F406-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Visionneuse HTML Microsoft (R).) -- C:\Windows\SysWOW64\mshtml.dll =>.Microsoft Corporation

O18 - Handler: cdl [64Bits] - {3dd53d40-7b8b-11D0-b013-00aa0059ce02} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\SysWOW64\urlmon.dll =>.Microsoft Corporation

O18 - Handler: dvd [64Bits] - {12D51199-0DB5-46FE-A120-47A3D7D937CC} . (.Microsoft Corporation - Contrôle ActiveX pour le flux vidéo.) -- C:\Windows\SysWOW64\MSVidCtl.dll =>.Microsoft Corporation

O18 - Handler: file [64Bits] - {79eac9e7-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\SysWOW64\urlmon.dll =>.Microsoft Corporation

O18 - Handler: ftp [64Bits] - {79eac9e3-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\SysWOW64\urlmon.dll =>.Microsoft Corporation

O18 - Handler: http [64Bits] - {79eac9e2-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\SysWOW64\urlmon.dll =>.Microsoft Corporation

O18 - Handler: https [64Bits] - {79eac9e5-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\SysWOW64\urlmon.dll =>.Microsoft Corporation

O18 - Handler: its [64Bits] - {9D148291-B9C8-11D0-A4CC-0000F80149F6} . (.Microsoft Corporation - Microsoft® InfoTech Storage System Library.) -- C:\Windows\SysWOW64\itss.dll =>.Microsoft Corporation

O18 - Handler: javascript [64Bits] - {3050F3B2-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Visionneuse HTML Microsoft (R).) -- C:\Windows\SysWOW64\mshtml.dll =>.Microsoft Corporation

O18 - Handler: local [64Bits] - {79eac9e7-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\SysWOW64\urlmon.dll =>.Microsoft Corporation

O18 - Handler: mailto [64Bits] - {3050f3DA-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Visionneuse HTML Microsoft (R).) -- C:\Windows\SysWOW64\mshtml.dll =>.Microsoft Corporation

O18 - Handler: mhtml [64Bits] - {05300401-BCBC-11d0-85E3-00C04FD85AB4} . (.Microsoft Corporation - Microsoft Internet Messaging API Resources.) -- C:\Windows\SysWOW64\inetcomm.dll =>.Microsoft Corporation

O18 - Handler: mk [64Bits] - {79eac9e6-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\SysWOW64\urlmon.dll =>.Microsoft Corporation

O18 - Handler: ms-help [64Bits] - {314111c7-a502-11d2-bbca-00c04f8ec294} . (.Microsoft Corporation - Microsoft® Help Data Services Module.) -- C:\Program Files (x86)\Common Files\Microsoft Shared\Help\hxds.dll =>.Microsoft Corporation®

O18 - Handler: ms-its [64Bits] - {9D148291-B9C8-11D0-A4CC-0000F80149F6} . (.Microsoft Corporation - Microsoft® InfoTech Storage System Library.) -- C:\Windows\SysWOW64\itss.dll =>.Microsoft Corporation

O18 - Handler: osf [64Bits] - {D924BDC6-C83A-4BD5-90D0-095128A113D1} . (.Microsoft Corporation - Microsoft Office 2013 component.) -- C:\Program Files (x86)\Microsoft Office\Office15\MSOSB.DLL =>.Microsoft Corporation®

O18 - Handler: res [64Bits] - {3050F3BC-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Visionneuse HTML Microsoft (R).) -- C:\Windows\SysWOW64\mshtml.dll =>.Microsoft Corporation

O18 - Handler: tbauth [64Bits] - {14654CA6-5711-491D-B89A-58E571679951} . (.Microsoft Corporation - TBAuth protocol handler.) -- C:\Windows\SysWOW64\tbauth.dll =>.Microsoft Corporation

O18 - Handler: tv [64Bits] - {CBD30858-AF45-11D2-B6D6-00C04FBBDE6E} . (.Microsoft Corporation - Contrôle ActiveX pour le flux vidéo.) -- C:\Windows\SysWOW64\MSVidCtl.dll =>.Microsoft Corporation

O18 - Handler: vbscript [64Bits] - {3050F3B2-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Visionneuse HTML Microsoft (R).) -- C:\Windows\SysWOW64\mshtml.dll =>.Microsoft Corporation

O18 - Handler: windows.tbauth [64Bits] - {14654CA6-5711-491D-B89A-58E571679951} . (.Microsoft Corporation - TBAuth protocol handler.) -- C:\Windows\SysWOW64\tbauth.dll =>.Microsoft Corporation

O18 - Filter: application/octet-stream [64Bits] - {1E66F26B-79EE-11D2-8710-00C04F79ED0D} . (.Microsoft Corporation - Microsoft .NET Runtime Execution Engine.) -- C:\Windows\SysWOW64\mscoree.dll =>.Microsoft Corporation

O18 - Filter: application/x-complus [64Bits] - {1E66F26B-79EE-11D2-8710-00C04F79ED0D} . (.Microsoft Corporation - Microsoft .NET Runtime Execution Engine.) -- C:\Windows\SysWOW64\mscoree.dll =>.Microsoft Corporation

O18 - Filter: application/x-msdownload [64Bits] - {1E66F26B-79EE-11D2-8710-00C04F79ED0D} . (.Microsoft Corporation - Microsoft .NET Runtime Execution Engine.) -- C:\Windows\SysWOW64\mscoree.dll =>.Microsoft Corporation

O18 - Filter: text/xml [64Bits] - {807583E5-5146-11D5-A672-00B0D022E945} . (.Microsoft Corporation - Microsoft Office XML MIME Filter.) -- C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE15\MSOXMLMF.DLL =>.Microsoft Corporation®

---\\ Logiciels installés (38) - 13s

O42 - Logiciel: Adobe Acrobat XI Pro - (.Adobe Systems.) [HKLM][64Bits] -- {AC76BA86-1033-FFFF-7760-000000000006} =>.Adobe Systems

O42 - Logiciel: Adobe Photoshop CC 2015 (32 Bit) - (.Adobe Systems Incorporated.) [HKLM][64Bits] -- {2614BC86-757D-4293-9E25-E4E16F370A9E} =>.Adobe Systems Incorporated®

O42 - Logiciel: ELAN pointing device - (.ELAN Microelectronic Corp..) [HKLM][64Bits] -- Elantech =>.ELAN Microelectronics Corporation®

O42 - Logiciel: Intel(R) Chipset Device Software - (.Intel Corporation.) [HKLM][64Bits] -- {8E2CA9DC-9975-468F-90CF-C740109DD2B8} =>.Intel Corporation

O42 - Logiciel: Intel(R) Dynamic Platform and Thermal Framework - (.Intel Corporation.) [HKLM][64Bits] -- {654EE65D-FAA4-4EA6-8C07-DC94E6A304D4} =>.Intel Corporation

O42 - Logiciel: Intel(R) PRO/Wireless Driver - (.Intel Corporation.) [HKLM][64Bits] -- {4d4a045b-9761-43d2-811c-1c29cbdb7459} =>.Intel Corporation

O42 - Logiciel: Intel(R) Processor Graphics - (.Intel Corporation.) [HKLM][64Bits] -- {F0E3AD40-2BBD-4360-9C76-B9AC9A5886EA} =>.Intel Corporation - pGFX®

O42 - Logiciel: Intel(R) Trusted Execution Engine - (.Intel Corporation.) [HKLM][64Bits] -- {176E2755-0A17-42C6-88E2-192AB2131278} =>.Intel Corporation

O42 - Logiciel: Intel(R) Trusted Execution Engine - (.Intel Corporation.) [HKLM][64Bits] -- {57FDCE53-64B7-48F3-AD5B-302A46C3080B} =>.Intel Corporation

O42 - Logiciel: Intel(R) Trusted Execution Engine Driver - (.Intel Corporation.) [HKLM][64Bits] -- {BAAE2AA9-513A-4658-A44F-9D6D607A9BC7} =>.Intel Corporation

O42 - Logiciel: Intel(R) Wireless Bluetooth(R) - (.Intel Corporation.) [HKLM][64Bits] -- {240E5DBF-63FA-4331-BC9D-1705B3C33E38} =>.Intel Corporation

O42 - Logiciel: Intel® PROSet/Wireless WiFi Software - (.Intel Corporation.) [HKLM][64Bits] -- {C8ADA4FE-F8E7-4A57-8F6C-083195DF78BF} =>.Intel Corporation

O42 - Logiciel: Intel® Security Assist - (.Intel Corporation.) [HKLM][64Bits] -- {4B230374-6475-4A73-BA6E-41015E9C5013} =>.Intel Corporation

O42 - Logiciel: Lenovo EasyCamera - (.Realtek Semiconductor Corp..) [HKLM][64Bits] -- {E399A5B3-ED53-4DEA-AF04-8011E1EB1EAC} =>.Realtek Semiconductor Corp®

O42 - Logiciel: LenovoUtility - (.Lenovo.) [HKLM][64Bits] -- {6ADA7E88-8D16-4D0D-BC90-2B93AC5E56DA} =>.Lenovo

O42 - Logiciel: LenovoUtility - (.Lenovo.) [HKLM][64Bits] -- InstallShield\_{6ADA7E88-8D16-4D0D-BC90-2B93AC5E56DA} =>.Lenovo

O42 - Logiciel: Logiciel Intel® PROSet/Wireless - (.Intel Corporation.) [HKLM][64Bits] -- {795ee3a0-97fa-489a-9543-7564ccc43be4} =>.Intel Corporation-Wireless Connectivity Solutions®

O42 - Logiciel: Logiciel pour périphérique à chipset Intel® - (.Intel(R) Corporation.) [HKLM][64Bits] -- {a2d9fda8-65eb-4c06-81ef-31e0a4daa335} =>.Intel Corporation - Software and Firmware Products®

O42 - Logiciel: Manuels d'utilisateur - (.Lenovo.) [HKLM][64Bits] -- {7042D952-EE42-4C09-A23D-E7AE4D047007} =>.Lenovo

O42 - Logiciel: Microsoft Access MUI (French) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-0015-040C-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft DCF MUI (French) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-0090-040C-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft Excel MUI (French) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-0016-040C-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft Groove MUI (French) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-00BA-040C-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft InfoPath MUI (French) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-0044-040C-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft Lync MUI (French) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-012B-040C-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft OneDrive - (.Microsoft Corporation.) [HKCU][64Bits] -- OneDriveSetup.exe =>.Microsoft Corporation®

O42 - Logiciel: Microsoft OneNote MUI (French) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-00A1-040C-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft Outlook MUI (French) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-001A-040C-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft PowerPoint MUI (French) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-0018-040C-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft Publisher MUI (French) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-0019-040C-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft Word MUI (French) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-001B-040C-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Realtek High Definition Audio Driver - (.Realtek Semiconductor Corp..) [HKLM][64Bits] -- {F132AF7F-7BCA-4EDE-8A7C-958108FE7DBC} =>.Realtek Semiconductor Corp®

O42 - Logiciel: Security Update for Skype for Business 2015 (KB3118348) 32-Bit Edition - (.Microsoft.) [HKLM][64Bits] -- {90150000-0011-0000-0000-0000000FF1CE}\_Office15.PROPLUS\_{73613498-F76D-41A6-B1A6-49E24436C671} =>.Microsoft Corporation®

O42 - Logiciel: Security Update for Skype for Business 2015 (KB3118348) 32-Bit Edition - (.Microsoft.) [HKLM][64Bits] -- {90150000-002A-0000-1000-0000000FF1CE}\_Office15.PROPLUS\_{73613498-F76D-41A6-B1A6-49E24436C671} =>.Microsoft Corporation®

O42 - Logiciel: Security Update for Skype for Business 2015 (KB3118348) 32-Bit Edition - (.Microsoft.) [HKLM][64Bits] -- {90150000-012B-040C-0000-0000000FF1CE}\_Office15.PROPLUS\_{73613498-F76D-41A6-B1A6-49E24436C671} =>.Microsoft Corporation®

O42 - Logiciel: Update for Skype for Business 2015 (KB3039776) 32-Bit Edition - (.Microsoft.) [HKLM][64Bits] -- {90150000-012B-040C-0000-0000000FF1CE}\_Office15.PROPLUS\_{8D97B9A2-D73D-4CB6-9D1F-D25178AC4EDE} =>.Microsoft Corporation®

O42 - Logiciel: User Manuals - (.Lenovo.) [HKLM][64Bits] -- InstallShield\_{7042D952-EE42-4C09-A23D-E7AE4D047007} =>.Lenovo

O42 - Logiciel: WinZip 16.5 - (.WinZip Computing, S.L..) [HKLM][64Bits] -- {CD95F661-A5C4-44F5-A6AA-ECDD91C240D2} =>.WinZip Computing, S.L.

---\\ HKCU & HKLM Software Keys (34) - 13s

HKLM\SOFTWARE\Wow6432Node\Adobe =>.Adobe

HKLM\SOFTWARE\Wow6432Node\Caphyon =>.Caphyon

HKLM\SOFTWARE\Wow6432Node\Google =>.Google

HKLM\SOFTWARE\Wow6432Node\IM Providers =>.IM Providers

HKLM\SOFTWARE\Wow6432Node\Intel =>.Intel

HKLM\SOFTWARE\Wow6432Node\Khronos =>.Khronos

HKLM\SOFTWARE\Wow6432Node\Lenovo =>.Lenovo

HKLM\SOFTWARE\Wow6432Node\Macromedia =>.Macromedia

HKLM\SOFTWARE\Wow6432Node\MAXSOFT-OCRON =>.Maxsoft-Ocron, Inc

HKLM\SOFTWARE\Wow6432Node\Mozilla =>.Mozilla

HKLM\SOFTWARE\Wow6432Node\MozillaPlugins =>.MozillaPlugins

HKLM\SOFTWARE\Wow6432Node\Nico Mak Computing =>.Nico Mak Computing

HKLM\SOFTWARE\Wow6432Node\Nuance =>.Nuance

HKLM\SOFTWARE\Wow6432Node\ODBC =>.DB Connectivity Solutions

HKLM\SOFTWARE\Wow6432Node\Realtek =>.Realtek

HKLM\SOFTWARE\Wow6432Node\Realtek Semiconductor Corp. =>.Realtek Semiconductor Corp.

HKLM\SOFTWARE\Wow6432Node\SRS Labs =>.SRS Labs

HKLM\SOFTWARE\Wow6432Node\WOW6432Node =>.Microsoft Corporation

HKLM\SOFTWARE\Wow6432Node\RegisteredApplications =>.Microsoft Corporation

HKCU\SOFTWARE\Adobe =>.Adobe

HKCU\SOFTWARE\AppDataLow =>.Microsoft Corporation

HKCU\SOFTWARE\Elantech =>.Elantech Inc.

HKCU\SOFTWARE\IM Providers =>.IM Providers

HKCU\SOFTWARE\Intel =>.Intel

HKCU\SOFTWARE\Netscape =>.Netscape

HKCU\SOFTWARE\Nico Mak Computing =>.Nico Mak Computing

HKCU\SOFTWARE\ODBC =>.DB Connectivity Solutions

HKCU\SOFTWARE\Realtek =>.Realtek

HKCU\SOFTWARE\RegisteredApplications =>.Microsoft Corporation

HKCU\SOFTWARE\SYNCJM =>.SYNCJM

HKCU\SOFTWARE\WinZip Computing =>.WinZip Computing

HKCU\SOFTWARE\Wow6432Node =>.Microsoft Corporation

HKCU\SOFTWARE\ZHP =>.Nicolas Coolman

HKCU\SOFTWARE\AppDataLow\Software =>.Microsoft Corporation

---\\ Contenu des dossiers Programmes (131) - 3s

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files\Common Files =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files\Elantech =>.ELAN Microelectronics Corporation®

O43 - CFD: 31/12/2016 - [0] SHD -- C:\Program Files\Fichiers communs =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files\Intel =>.Intel Corporation

O43 - CFD: 13/01/2017 - [] D -- C:\Program Files\Internet Explorer =>.Microsoft Corporation

O43 - CFD: 10/09/2016 - [] D -- C:\Program Files\Lenovo =>.Lenovo

O43 - CFD: 06/01/2017 - [] D -- C:\Program Files\Microsoft Office =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files\MSBuild =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files\Realtek =>.Realtek

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files\Reference Assemblies =>.Microsoft Corporation

O43 - CFD: 03/11/2015 - [0] HD -- C:\Program Files\Uninstall Information =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] RD -- C:\Program Files\Windows Defender =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files\Windows Mail =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files\Windows Media Player =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [] D -- C:\Program Files\Windows Multimedia Platform =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files\Windows NT =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files\Windows Photo Viewer =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [] D -- C:\Program Files\Windows Portable Devices =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [] SHD -- C:\Program Files\Windows Sidebar =>.Microsoft Corporation

O43 - CFD: 13/01/2017 - [] HD -- C:\Program Files\WindowsApps =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [] D -- C:\Program Files\WindowsPowerShell =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] AD -- C:\Program Files (x86)\Adobe =>.Adobe Systems Incorporated®

O43 - CFD: 10/09/2016 - [] AD -- C:\Program Files (x86)\Cisco =>.Cisco

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files (x86)\Common Files =>.Microsoft Corporation

O43 - CFD: 10/09/2016 - [] HD -- C:\Program Files (x86)\InstallShield Installation Information =>.InstallShield Software

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files (x86)\Intel =>.Intel Corporation

O43 - CFD: 13/01/2017 - [] D -- C:\Program Files (x86)\Internet Explorer =>.Microsoft Corporation

O43 - CFD: 10/09/2016 - [] D -- C:\Program Files (x86)\Lenovo =>.Lenovo

O43 - CFD: 06/01/2017 - [] D -- C:\Program Files (x86)\Microsoft Analysis Services =>.Microsoft Corporation

O43 - CFD: 06/01/2017 - [] AD -- C:\Program Files (x86)\Microsoft Office =>.Microsoft Corporation

O43 - CFD: 06/01/2017 - [] D -- C:\Program Files (x86)\Microsoft SQL Server =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] AD -- C:\Program Files (x86)\Microsoft.NET =>.Microsoft Corporation

O43 - CFD: 13/01/2017 - [] D -- C:\Program Files (x86)\Mozilla Firefox =>.Mozilla

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files (x86)\MSBuild =>.Microsoft Corporation

O43 - CFD: 10/09/2016 - [] D -- C:\Program Files (x86)\Realtek =>.Realtek

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files (x86)\Reference Assemblies =>.Microsoft Corporation

O43 - CFD: 10/09/2016 - [0] HD -- C:\Program Files (x86)\Temp =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files (x86)\Windows Defender =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files (x86)\Windows Mail =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files (x86)\Windows Media Player =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [] D -- C:\Program Files (x86)\Windows Multimedia Platform =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [] D -- C:\Program Files (x86)\Windows NT =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files (x86)\Windows Photo Viewer =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [] D -- C:\Program Files (x86)\Windows Portable Devices =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [] SHD -- C:\Program Files (x86)\Windows Sidebar =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [] D -- C:\Program Files (x86)\WindowsPowerShell =>.Microsoft Corporation

O43 - CFD: 05/01/2017 - [] AD -- C:\Program Files (x86)\WinZip =>.WinZip Computing®

O43 - CFD: 16/07/2016 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessibility =>.Microsoft Corporation

O43 - CFD: 13/01/2017 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools =>.Administrative Tools

O43 - CFD: 08/01/2017 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Lenovo =>.Lenovo

O43 - CFD: 16/07/2016 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Maintenance =>.Microsoft Corporation

O43 - CFD: 13/01/2017 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Office 2013 =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Realtek =>.Realtek

O43 - CFD: 16/07/2016 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\System Tools =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\WinZip =>.WinZip

O43 - CFD: 08/01/2017 - [] D -- C:\ProgramData\Adobe =>.Adobe

O43 - CFD: 08/01/2017 - [0] SHD -- C:\ProgramData\Application Data =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\ProgramData\boost\_interprocess =>.boost.org

O43 - CFD: 31/12/2016 - [0] SHD -- C:\ProgramData\Bureau =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [0] D -- C:\ProgramData\Comms =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [0] SHD -- C:\ProgramData\Documents =>.Microsoft Corporation

O43 - CFD: 10/09/2016 - [] D -- C:\ProgramData\Intel =>.Intel Corporation

O43 - CFD: 10/09/2016 - [] D -- C:\ProgramData\Intel.sav =>.Intel Corporation

O43 - CFD: 31/12/2016 - [0] SHD -- C:\ProgramData\Menu Démarrer =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] SD -- C:\ProgramData\Microsoft =>.Microsoft Corporation

O43 - CFD: 13/01/2017 - [] D -- C:\ProgramData\Microsoft Help =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\ProgramData\Microsoft OneDrive =>.Microsoft Corporation

O43 - CFD: 31/12/2016 - [0] SHD -- C:\ProgramData\Modèles =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\ProgramData\Package Cache =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\ProgramData\regid.1986-12.com.adobe =>.Adobe Inc.

O43 - CFD: 08/01/2017 - [] AD -- C:\ProgramData\regid.1991-06.com.microsoft =>.Microsoft Corporation

O43 - CFD: 10/09/2016 - [] D -- C:\ProgramData\Roaming =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [0] D -- C:\ProgramData\SoftwareDistribution =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\ProgramData\USOPrivate =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\ProgramData\USOShared =>.Microsoft Corporation

O43 - CFD: 05/01/2017 - [] D -- C:\ProgramData\WinZip =>.WinZip

O43 - CFD: 08/01/2017 - [] AD -- C:\Program Files (x86)\Common Files\Adobe =>.Adobe

O43 - CFD: 06/01/2017 - [] AD -- C:\Program Files (x86)\Common Files\DESIGNER =>.Designer

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files (x86)\Common Files\Intel =>.Intel Corporation

O43 - CFD: 08/01/2017 - [] AD -- C:\Program Files (x86)\Common Files\Microsoft Shared =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [] D -- C:\Program Files (x86)\Common Files\Services =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\Program Files (x86)\Common Files\System =>.Microsoft Corporation

O43 - CFD: 09/01/2017 - [] D -- C:\Users\theob\AppData\Roaming\Adobe =>.Adobe

O43 - CFD: 09/01/2017 - [] D -- C:\Users\theob\AppData\Roaming\com.adobe.formscentral.FormsCentralForAcrobat =>.Adobe Inc.

O43 - CFD: 31/12/2016 - [] D -- C:\Users\theob\AppData\Roaming\Intel =>.Intel Corporation

O43 - CFD: 31/12/2016 - [] D -- C:\Users\theob\AppData\Roaming\Macromedia =>.Macromedia

O43 - CFD: 13/01/2017 - [] SD -- C:\Users\theob\AppData\Roaming\Microsoft =>.Microsoft Corporation

O43 - CFD: 31/12/2016 - [] D -- C:\Users\theob\AppData\Roaming\Skype =>.Skype

O43 - CFD: 13/01/2017 - [] D -- C:\Users\theob\AppData\Roaming\ZHP =>.Nicolas Coolman

O43 - CFD: 31/12/2016 - [0] D -- C:\Users\theob\AppData\Local\ActiveSync =>.Microsoft Corporation

O43 - CFD: 13/01/2017 - [] D -- C:\Users\theob\AppData\Local\Adobe =>.Adobe

O43 - CFD: 08/01/2017 - [0] SHD -- C:\Users\theob\AppData\Local\Application Data =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\Users\theob\AppData\Local\CEF =>.CEF

O43 - CFD: 31/12/2016 - [] D -- C:\Users\theob\AppData\Local\Comms =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\Users\theob\AppData\Local\ConnectedDevicesPlatform =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\Users\theob\AppData\Local\Diagnostics =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [0] SHD -- C:\Users\theob\AppData\Local\Historique =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\Users\theob\AppData\Local\Microsoft =>.Microsoft Corporation

O43 - CFD: 09/01/2017 - [] D -- C:\Users\theob\AppData\Local\Microsoft Help =>.Microsoft Corporation

O43 - CFD: 31/12/2016 - [] D -- C:\Users\theob\AppData\Local\MicrosoftEdge =>.Microsoft Corporation

O43 - CFD: 31/12/2016 - [0] D -- C:\Users\theob\AppData\Local\NetworkTiles =>.NetworkTiles

O43 - CFD: 08/01/2017 - [] D -- C:\Users\theob\AppData\Local\Packages =>.Microsoft Corporation

O43 - CFD: 06/01/2017 - [] D -- C:\Users\theob\AppData\Local\Programs =>.Microsoft Corporation

O43 - CFD: 31/12/2016 - [] D -- C:\Users\theob\AppData\Local\Publishers =>.Microsoft Corporation

O43 - CFD: 13/01/2017 - [] D -- C:\Users\theob\AppData\Local\Temp =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [0] SHD -- C:\Users\theob\AppData\Local\Temporary Internet Files =>.Microsoft Corporation

O43 - CFD: 31/12/2016 - [] D -- C:\Users\theob\AppData\Local\TileDataLayer =>.Microsoft Corporation

O43 - CFD: 31/12/2016 - [0] D -- C:\Users\theob\AppData\Local\VirtualStore =>.Microsoft Corporation

O43 - CFD: 06/01/2017 - [0] D -- C:\Users\theob\AppData\Local\Programs\Common =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [] RD -- C:\Users\theob\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] RD -- C:\Users\theob\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories =>.Microsoft Corporation

O43 - CFD: 13/01/2017 - [] RD -- C:\Users\theob\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools =>.Administrative Tools

O43 - CFD: 16/07/2016 - [] D -- C:\Users\theob\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance =>.Microsoft Corporation

O43 - CFD: 13/01/2017 - [] RD -- C:\Users\theob\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [] RD -- C:\Users\theob\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [] RD -- C:\Users\theob\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Windows PowerShell =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [0] SHD -- C:\Users\Default\AppData\Local\Application Data =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [0] SHD -- C:\Users\Default\AppData\Local\Historique =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [] D -- C:\Users\Default\AppData\Local\Microsoft =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [0] D -- C:\Users\Default\AppData\Local\Microsoft Help =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [0] D -- C:\Users\Default\AppData\Local\Temp =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [0] SHD -- C:\Users\Default\AppData\Local\Temporary Internet Files =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [0] SHD -- C:\Users\Default User\AppData\Local\Application Data =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [0] SHD -- C:\Users\Default User\AppData\Local\Historique =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [] D -- C:\Users\Default User\AppData\Local\Microsoft =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [0] D -- C:\Users\Default User\AppData\Local\Microsoft Help =>.Microsoft Corporation

O43 - CFD: 16/07/2016 - [0] D -- C:\Users\Default User\AppData\Local\Temp =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [0] SHD -- C:\Users\Default User\AppData\Local\Temporary Internet Files =>.Microsoft Corporation

O43 - CFD: 08/01/2017 - [] D -- C:\WINDOWS\System32\Config\systemprofile\AppData\Local\Microsoft =>.Microsoft Corporation

---\\ ShellIconOverlayIdentifiers (SIOI) (8) - 1s

O106 - SIOI: ErrorOverlayHandler Class [ OneDrive1] - {BBACC218-34EA-4666-9D7A-C78F2274A524}. (.Microsoft Corporation - Microsoft OneDrive Shell Extension.) -- C:\Users\theob\AppData\Local\Microsoft\OneDrive\17.3.6720.1207\_1\FileSyncShell.dll =>.Microsoft Corporation®

O106 - SIOI: SharedOverlayHandler Class [ OneDrive2] - {5AB7172C-9C11-405C-8DD5-AF20F3606282}. (.Microsoft Corporation - Microsoft OneDrive Shell Extension.) -- C:\Users\theob\AppData\Local\Microsoft\OneDrive\17.3.6720.1207\_1\FileSyncShell.dll =>.Microsoft Corporation®

O106 - SIOI: SharedSyncingOverlayHandler Class [ OneDrive3] - {A78ED123-AB77-406B-9962-2A5D9D2F7F30}. (.Microsoft Corporation - Microsoft OneDrive Shell Extension.) -- C:\Users\theob\AppData\Local\Microsoft\OneDrive\17.3.6720.1207\_1\FileSyncShell.dll =>.Microsoft Corporation®

O106 - SIOI: UpToDateOverlayHandler Class [ OneDrive4] - {F241C880-6982-4CE5-8CF7-7085BA96DA5A}. (.Microsoft Corporation - Microsoft OneDrive Shell Extension.) -- C:\Users\theob\AppData\Local\Microsoft\OneDrive\17.3.6720.1207\_1\FileSyncShell.dll =>.Microsoft Corporation®

O106 - SIOI: SyncingOverlayHandler Class [ OneDrive5] - {A0396A93-DC06-4AEF-BEE9-95FFCCAEF20E}. (.Microsoft Corporation - Microsoft OneDrive Shell Extension.) -- C:\Users\theob\AppData\Local\Microsoft\OneDrive\17.3.6720.1207\_1\FileSyncShell.dll =>.Microsoft Corporation®

O106 - SIOI: Microsoft SkyDrive Pro Icon Overlay 1 (ErrorConflict) [ SkyDrivePro1 (ErrorConflict)] - {8BA85C75-763B-4103-94EB-9470F12FE0F7}. (.Microsoft Corporation - Microsoft OneDrive for Business Extensions.) -- C:\Program Files (x86)\Microsoft Office\Office15\GROOVEEX.DLL =>.Microsoft Corporation®

O106 - SIOI: Microsoft SkyDrive Pro Icon Overlay 2 (SyncInProgress) [ SkyDrivePro2 (SyncInProgress)] - {CD55129A-B1A1-438E-A425-CEBC7DC684EE}. (.Microsoft Corporation - Microsoft OneDrive for Business Extensions.) -- C:\Program Files (x86)\Microsoft Office\Office15\GROOVEEX.DLL =>.Microsoft Corporation®

O106 - SIOI: Microsoft SkyDrive Pro Icon Overlay 3 (InSync) [ SkyDrivePro3 (InSync)] - {E768CD3B-BDDC-436D-9C13-E1B39CA257B1}. (.Microsoft Corporation - Microsoft OneDrive for Business Extensions.) -- C:\Program Files (x86)\Microsoft Office\Office15\GROOVEEX.DLL =>.Microsoft Corporation®

---\\ Liste des pilotes du système (58) - 13s

O58 - SDL:2016/07/16 12:41:53 A . (.LSI - LSI 3ware SCSI Storport Driver.) -- C:\WINDOWS\System32\drivers\3ware.sys [107360] =>.Microsoft Windows®

O58 - SDL:2015/07/29 12:20:50 A . (.Lenovo Corporation - ACPI Virtual Power Controller Driver.) -- C:\WINDOWS\System32\drivers\AcpiVpc.sys [42328] =>.LENOVO®

O58 - SDL:2016/07/16 12:41:53 A . (.PMC-Sierra - PMC-Sierra Storport Driver For SPC8x6G SAS.) -- C:\WINDOWS\System32\drivers\adp80xx.sys [1135456] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Advanced Micro Devices - AHCI 1.3 Device Driver.) -- C:\WINDOWS\System32\drivers\amdsata.sys [83296] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.AMD Technologies Inc. - AMD Technology AHCI Compatible Controller D.) -- C:\WINDOWS\System32\drivers\amdsbs.sys [259424] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Advanced Micro Devices - Storage Filter Driver.) -- C:\WINDOWS\System32\drivers\amdxata.sys [26976] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.PMC-Sierra, Inc. - Adaptec SAS RAID WS03 Driver.) -- C:\WINDOWS\System32\drivers\arcsas.sys [131936] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Windows (R) Win 7 DDK provider - BCM Function 2 Device Driver.) -- C:\WINDOWS\System32\drivers\bcmfn.sys [9728] =>.Windows (R) Win 7 DDK provider

O58 - SDL:2016/07/16 12:41:53 A . (.Windows (R) Win 7 DDK provider - BCM Function 2 Device Driver.) -- C:\WINDOWS\System32\drivers\bcmfn2.sys [9728] =>.Windows (R) Win 7 DDK provider

O58 - SDL:2016/07/16 12:41:52 A . (.QLogic Corporation - QLogic Gigabit Ethernet VBD.) -- C:\WINDOWS\System32\drivers\bxvbda.sys [533856] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Chelsio Communications - Chelsio iSCSI Crash Dump Driver.) -- C:\WINDOWS\System32\drivers\cht4dx64.sys [102752] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Chelsio Communications - Chelsio iSCSI VMiniport Driver.) -- C:\WINDOWS\System32\drivers\cht4sx64.sys [346976] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Chelsio Communications - Virtual Bus Driver for Chelsio ® T4 Chipset.) -- C:\WINDOWS\System32\drivers\cht4vx64.sys [2104160] =>.Microsoft Windows®

O58 - SDL:2015/08/13 00:54:44 A . (.Intel Corporation - DPTF ACPI Device (64-Bit).) -- C:\WINDOWS\System32\drivers\dptf\_acpi.sys [55816] =>.Intel(R) Software®

O58 - SDL:2015/08/13 00:54:44 A . (.Intel Corporation - DPTF CPU Device (64-Bit).) -- C:\WINDOWS\System32\drivers\dptf\_cpu.sys [53752] =>.Intel(R) Software®

O58 - SDL:2015/08/13 00:54:44 A . (.Intel Corporation - DPTF Zone (64-Bit).) -- C:\WINDOWS\System32\drivers\esif\_lf.sys [261624] =>.Intel(R) Software®

O58 - SDL:2016/01/08 09:48:34 A . (.ELAN Microelectronics Corp. - ETD Kernel Center.) -- C:\WINDOWS\System32\drivers\ETD.sys [470104] =>.ELAN MICROELECTRONICS CORPORATION®

O58 - SDL:2016/07/16 12:41:52 A . (.QLogic Corporation - QLogic 10 GigE VBD.) -- C:\WINDOWS\System32\drivers\evbda.sys [3418976] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Hewlett-Packard Company - Smart Array SAS/SATA Controller Media Drive.) -- C:\WINDOWS\System32\drivers\HpSAMD.sys [64352] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:54 A . (.Intel(R) Corporation - Intel(R) Serial IO GPIO Controller Driver.) -- C:\WINDOWS\System32\drivers\iagpio.sys [33280] =>.Intel(R) Corporation

O58 - SDL:2016/07/16 12:41:54 A . (.Intel(R) Corporation - Intel(R) Serial IO I2C Driver.) -- C:\WINDOWS\System32\drivers\iai2c.sys [81408] =>.Intel(R) Corporation

O58 - SDL:2016/07/16 12:41:54 A . (.Intel Corporation - Intel(R) Serial IO GPIO Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i\_GPIO2.sys [64512] =>.Intel Corporation

O58 - SDL:2016/07/16 12:41:54 A . (.Intel Corporation - Intel(R) Serial IO I2C Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i\_I2C.sys [176384] =>.Intel Corporation - Embedded Subsystems and IP Blocks Group®

O58 - SDL:2016/07/16 12:41:52 A . (.Intel Corporation - Intel(R) Serial IO GPIO Controller Driver.) -- C:\WINDOWS\System32\drivers\iaLPSSi\_GPIO.sys [38128] =>.Intel Corporation - Client Components Group®

O58 - SDL:2016/07/16 12:41:50 A . (.Intel Corporation - Intel(R) Serial IO I2C Controller Driver.) -- C:\WINDOWS\System32\drivers\iaLPSSi\_I2C.sys [113152] =>.Intel Corporation

O58 - SDL:2016/07/16 12:41:53 A . (.Intel Corporation - Intel(R) Rapid Storage Technology driver (i.) -- C:\WINDOWS\System32\drivers\iaStorAV.sys [673120] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Intel Corporation - Intel Matrix Storage Manager driver - x64.) -- C:\WINDOWS\System32\drivers\iaStorV.sys [412000] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Mellanox - InfiniBand Fabric Bus Driver.) -- C:\WINDOWS\System32\drivers\ibbus.sys [526176] =>.Microsoft Windows®

O58 - SDL:2015/07/31 12:56:08 A . (.Intel Corporation - Intel(R) Wireless Bluetooth(R) USB Driver.) -- C:\WINDOWS\System32\drivers\ibtusb.sys [259312] =>.Intel Corporation-Wireless Connectivity Solutions®

O58 - SDL:2016/01/26 16:21:38 A . (.Intel Corporation - Intel Graphics Kernel Mode Driver.) -- C:\WINDOWS\System32\drivers\igdkmd64lp.sys [7329744] =>.Intel(R) pGFX®

O58 - SDL:2016/01/26 16:21:22 A . (.Intel(R) Corporation - Intel(R) Display Audio Driver.) -- C:\WINDOWS\System32\drivers\IntcDAud.sys [481032] =>.Intel Corporation - Client Components Group®

O58 - SDL:2016/07/16 12:41:53 A . (.LSI Corporation - LSI Fusion-MPT SAS Driver (StorPort).) -- C:\WINDOWS\System32\drivers\lsi\_sas.sys [108896] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.LSI Corporation - LSI SAS Gen2 Driver (StorPort).) -- C:\WINDOWS\System32\drivers\lsi\_sas2i.sys [105824] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Avago Technologies - Avago SAS Gen3 Driver (StorPort).) -- C:\WINDOWS\System32\drivers\lsi\_sas3i.sys [101216] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.LSI Corporation - LSI SSS PCIe/Flash Driver (StorPort).) -- C:\WINDOWS\System32\drivers\lsi\_sss.sys [82776] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Avago Technologies - MEGASAS RAID Controller Driver for Windows.) -- C:\WINDOWS\System32\drivers\megasas.sys [59744] =>.Microsoft Windows®

O58 - SDL:2016/10/05 11:09:07 A . (.Avago Technologies - MEGASAS RAID Controller Driver for Windows.) -- C:\WINDOWS\System32\drivers\MegaSas2i.sys [64352] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.LSI Corporation, Inc. - LSI MegaRAID Software RAID Driver.) -- C:\WINDOWS\System32\drivers\megasr.sys [575840] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Mellanox - MLX4 Bus Driver.) -- C:\WINDOWS\System32\drivers\mlx4\_bus.sys [842584] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Marvell Semiconductor, Inc. - Marvell Flash Controller Driver.) -- C:\WINDOWS\System32\drivers\mvumis.sys [63840] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Mellanox - NetworkDirect Support Filter Driver.) -- C:\WINDOWS\System32\drivers\ndfltr.sys [108896] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:42:03 A . (.Auteurs - .) -- C:\WINDOWS\System32\drivers\NetAdapterCx.sys [90624] =>.Microsoft Corporation

O58 - SDL:2015/07/16 11:55:18 A . (.Intel Corporation - Intel® Wireless WiFi Link Driver.) -- C:\WINDOWS\System32\drivers\Netwbw02.sys [4043544] =>.Intel Corporation-Wireless Connectivity Solutions®

O58 - SDL:2015/10/30 08:17:19 A . (.Intel Corporation - Intel® Wireless WiFi Link Driver.) -- C:\WINDOWS\System32\drivers\NETwew01.sys [3343872] =>.Intel Corporation

O58 - SDL:2016/07/16 12:41:53 A . (.NVIDIA Corporation - NVIDIA® nForce(TM) RAID Driver.) -- C:\WINDOWS\System32\drivers\nvraid.sys [150368] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.NVIDIA Corporation - NVIDIA® nForce(TM) Sata Performance Driver.) -- C:\WINDOWS\System32\drivers\nvstor.sys [166240] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Avago Technologies - MEGASAS RAID Controller Driver for Windows.) -- C:\WINDOWS\System32\drivers\percsas2i.sys [58720] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Avago Technologies - MEGASAS RAID Controller Driver for Windows.) -- C:\WINDOWS\System32\drivers\percsas3i.sys [61792] =>.Microsoft Windows®

O58 - SDL:2016/01/13 11:55:26 A . (.Realtek Semiconductor Corp. - Realtek(r) High Definition Audio Function D.) -- C:\WINDOWS\System32\drivers\RTKVHD64.sys [4739328] =>.Realtek Semiconductor Corp®

O58 - SDL:2015/10/08 08:34:48 A . (.Realtek Semiconductor Corp. - Realtek UVC Driver for Vista/Win7/Win8/Win8.) -- C:\WINDOWS\System32\drivers\rtsuvc.sys [3057920] =>.Realtek Semiconductor Corp®

O58 - SDL:2016/07/16 12:41:53 A . (.Silicon Integrated Systems Corp. - SiS RAID Stor Miniport Driver.) -- C:\WINDOWS\System32\drivers\sisraid2.sys [44896] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Silicon Integrated Systems - SiS AHCI Stor-Miniport Driver.) -- C:\WINDOWS\System32\drivers\sisraid4.sys [81760] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Promise Technology, Inc. - Promise SuperTrak EX Series Driver for Wind.) -- C:\WINDOWS\System32\drivers\stexstor.sys [31072] =>.Microsoft Windows®

O58 - SDL:2015/10/15 00:12:40 A . (.Intel Corporation - Intel(R) Trusted Execution Engine Interface.) -- C:\WINDOWS\System32\drivers\TXEIx64.sys [146200] =>.Intel Corporation - Embedded Subsystems and IP Blocks Group®

O58 - SDL:2016/07/16 12:41:53 A . (.VIA Technologies Inc.,Ltd - VIA RAID DRIVER FOR AMD-X86-64.) -- C:\WINDOWS\System32\drivers\vsmraid.sys [166752] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.VIA Corporation - VIA StorX RAID Controller Driver.) -- C:\WINDOWS\System32\drivers\VSTXRAID.SYS [305504] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Mellanox - Kernel WinMad.) -- C:\WINDOWS\System32\drivers\winmad.sys [32096] =>.Microsoft Windows®

O58 - SDL:2016/07/16 12:41:53 A . (.Mellanox - Kernel WinVerbs.) -- C:\WINDOWS\System32\drivers\winverbs.sys [64864] =>.Microsoft Windows®

---\\ Associations Shell Spawning (10) - 1s

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 Ob.) -- C:\Windows\System32\eventvwr.exe =>.Microsoft Corporation

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 =>.Microsoft Corporation®

O67 - Shell Spawning: <.js> <JSFile>[HKLM\..\open\Command] (.Microsoft Corporation - Microsoft ® Windows Based Script Host.) -- C:\Windows\System32\wscript.exe =>.Microsoft Corporation

O67 - Shell Spawning: <.reg> <regfile>[HKLM\..\open\Command] (.Microsoft Corporation - Éditeur du Registre.) -- C:\Windows\regedit.exe =>.Microsoft Corporation

O67 - Shell Spawning: <.scr> <scrfile>[HKLM\..\open\Command] (...) -- "%1" /S

---\\ Menu de démarrage Internet (4) - 0s

O68 - StartMenuInternet: <IEXPLORE.EXE> <Internet Explorer>[HKLM\..\Shell\open\Command] (.Microsoft Corporation - Internet Explorer.) -- C:\Program Files\Internet Explorer\iexplore.exe =>.Microsoft Corporation®

O68 - StartMenuInternet: <IEXPLORE.EXE> <Internet Explorer>[HKLM\..\InstallInfo\ShowIconsCommand] (.Microsoft Corporation - Utilitaire d'initialisation d'Internet Expl.) -- C:\Windows\System32\ie4uinit.exe =>.Microsoft Corporation

O68 - StartMenuInternet: <IEXPLORE.EXE> <Internet Explorer>[HKLM\..\InstallInfo\ReinstallCommand] (.Microsoft Corporation - Utilitaire d'initialisation d'Internet Expl.) -- C:\Windows\System32\ie4uinit.exe =>.Microsoft Corporation

O68 - StartMenuInternet: <IEXPLORE.EXE> <Internet Explorer>[HKLM\..\InstallInfo\HideIconsCommand] (.Microsoft Corporation - Utilitaire d'initialisation d'Internet Expl.) -- C:\Windows\System32\ie4uinit.exe =>.Microsoft Corporation

---\\ Recherche d'infection sur les navigateurs (3) - 0s

O69 - SBI: SearchScopes [HKCU] {0633EE93-D776-472f-A0FF-E1416B8B2E3A} [DefaultScope] - (Bing) - http://www.bing.com/ =>.Bing.com

O69 - SBI: SearchScopes [HKLM] {0633EE93-D776-472f-A0FF-E1416B8B2E3A} - (@ieframe.dll,-12512) - http://www.bing.com/ =>.Bing.com

O69 - SBI: SearchScopes [HKLM] {F27AC6AA-382A-445D-9A33-193F754F57E9} [DefaultScope] - (Bing) - http://www.bing.com/ =>.Bing.com

---\\ Enumère les services démarrés par Svchost (45) - 1s

O83 - Search Svchost Services: CertPropSvc (CertPropSvc) . (.Microsoft Corporation - Service de propagation de certificats de ca.) -- C:\WINDOWS\System32\certprop.dll [193536] =>.Microsoft Corporation

O83 - Search Svchost Services: SCPolicySvc (SCPolicySvc) . (.Microsoft Corporation - Service de propagation de certificats de ca.) -- C:\WINDOWS\System32\certprop.dll [193536] =>.Microsoft Corporation

O83 - Search Svchost Services: lanmanserver (lanmanserver) . (.Microsoft Corporation - DLL du service Serveur.) -- C:\WINDOWS\system32\srvsvc.dll [305152] =>.Microsoft Corporation

O83 - Search Svchost Services: gpsvc (gpsvc) . (.Microsoft Corporation - Client de stratégie de groupe.) -- C:\WINDOWS\System32\gpsvc.dll [1227264] =>.Microsoft Corporation

O83 - Search Svchost Services: IKEEXT (IKEEXT) . (.Microsoft Corporation - Extension IKE.) -- C:\WINDOWS\System32\ikeext.dll [932352] =>.Microsoft Corporation

O83 - Search Svchost Services: iphlpsvc (iphlpsvc) . (.Microsoft Corporation - Service offrant une connectivité IPv6 sur u.) -- C:\WINDOWS\System32\iphlpsvc.dll [945664] =>.Microsoft Corporation

O83 - Search Svchost Services: seclogon (seclogon) . (.Microsoft Corporation - DLL de service d’ouverture de session secon.) -- C:\WINDOWS\system32\seclogon.dll [31232] =>.Microsoft Corporation

O83 - Search Svchost Services: AppInfo (AppInfo) . (.Microsoft Corporation - Service Informations d’application.) -- C:\WINDOWS\System32\appinfo.dll [125952] =>.Microsoft Corporation

O83 - Search Svchost Services: msiscsi (msiscsi) . (.Microsoft Corporation - Service de découverte iSCSI.) -- C:\WINDOWS\system32\iscsiexe.dll [151552] =>.Microsoft Corporation

O83 - Search Svchost Services: EapHost (EapHost) . (.Microsoft Corporation - Service EAPHost Microsoft.) -- C:\WINDOWS\System32\eapsvc.dll [112128] =>.Microsoft Corporation

O83 - Search Svchost Services: schedule (schedule) . (.Microsoft Corporation - Service du Planificateur de tâches.) -- C:\WINDOWS\system32\schedsvc.dll [948224] =>.Microsoft Corporation

O83 - Search Svchost Services: winmgmt (winmgmt) . (.Microsoft Corporation - WMI.) -- C:\WINDOWS\system32\wbem\WMIsvc.dll [222720] =>.Microsoft Corporation

O83 - Search Svchost Services: browser (browser) . (.Microsoft Corporation - DLL du service Explorateur d’ordinateurs.) -- C:\WINDOWS\System32\browser.dll [134656] =>.Microsoft Corporation

O83 - Search Svchost Services: SessionEnv (SessionEnv) . (.Microsoft Corporation - Service Configuration des services Bureau à.) -- C:\Windows\System32\SessEnv.dll [387072] =>.Microsoft Corporation

O83 - Search Svchost Services: wercplsupport (wercplsupport) . (.Microsoft Corporation - Rapports et solutions aux problèmes.) -- C:\WINDOWS\System32\wercplsupport.dll [94208] =>.Microsoft Corporation

O83 - Search Svchost Services: shpamsvc (shpamsvc) . (.Microsoft Corporation - SharedPC.AccountManager.) -- C:\WINDOWS\system32\Windows.SharedPC.AccountManager.dll [161792] =>.Microsoft Corporation

O83 - Search Svchost Services: Themes (Themes) . (.Microsoft Corporation - DLL du service des thèmes Windows Shell.) -- C:\WINDOWS\system32\themeservice.dll [70656] =>.Microsoft Corporation

O83 - Search Svchost Services: lfsvc (lfsvc) . (.Microsoft Corporation - Service de géolocalisation.) -- C:\WINDOWS\System32\lfsvc.dll [37376] =>.Microsoft Corporation

O83 - Search Svchost Services: DmEnrollmentSvc (DmEnrollmentSvc) . (.Microsoft Corporation - DLL Windows Management Service.) -- C:\Windows\System32\Windows.Internal.Management.dll [407552] =>.Microsoft Corporation

O83 - Search Svchost Services: Irmon (Irmon) . (.Microsoft Corporation - Moniteur infrarouge.) -- C:\WINDOWS\System32\irmon.dll [25088] =>.Microsoft Corporation

O83 - Search Svchost Services: Rasauto (Rasauto) . (.Microsoft Corporation - Gestionnaire de numérotation automatique d’.) -- C:\WINDOWS\System32\rasauto.dll [105472] =>.Microsoft Corporation

O83 - Search Svchost Services: Rasman (Rasman) . (.Microsoft Corporation - Gestionnaire des connexions d’accès à dista.) -- C:\WINDOWS\System32\rasmans.dll [657920] =>.Microsoft Corporation

O83 - Search Svchost Services: Remoteaccess (Remoteaccess) . (.Microsoft Corporation - Gestionnaire d’interface dynamique.) -- C:\Windows\System32\mprdim.dll [496128] =>.Microsoft Corporation

O83 - Search Svchost Services: SENS (SENS) . (.Microsoft Corporation - Service de notification d’événements systèm.) -- C:\WINDOWS\System32\sens.dll [70656] =>.Microsoft Corporation

O83 - Search Svchost Services: Sharedaccess (Sharedaccess) . (.Microsoft Corporation - Composants de l’application d’assistance à.) -- C:\WINDOWS\System32\ipnathlp.dll [541696] =>.Microsoft Corporation

O83 - Search Svchost Services: Tapisrv (Tapisrv) . (.Microsoft Corporation - Serveur de téléphonie Microsoft® Windows(TM.) -- C:\Windows\System32\tapisrv.dll [309248] =>.Microsoft Corporation

O83 - Search Svchost Services: wuauserv (wuauserv) . (.Microsoft Corporation - Agent de mise à jour automatique Windows Up.) -- C:\WINDOWS\system32\wuaueng.dll [2317824] =>.Microsoft Corporation

O83 - Search Svchost Services: BITS (BITS) . (.Microsoft Corporation - Service de transfert intelligent en arrière.) -- C:\WINDOWS\System32\qmgr.dll [1054208] =>.Microsoft Corporation

O83 - Search Svchost Services: ShellHWDetection (ShellHWDetection) . (.Microsoft Corporation - Dll des services Windows Shell.) -- C:\Windows\System32\shsvcs.dll [617472] =>.Microsoft Corporation

O83 - Search Svchost Services: dmwappushservice (dmwappushservice) . (.Microsoft Corporation - dmwappushsvc.) -- C:\WINDOWS\system32\dmwappushsvc.dll [57344] =>.Microsoft Corporation

O83 - Search Svchost Services: WpnService (WpnService) . (.Microsoft Corporation - Service du système de notifications Push Wi.) -- C:\WINDOWS\system32\WpnService.dll [234496] =>.Microsoft Corporation

O83 - Search Svchost Services: XboxNetApiSvc (XboxNetApiSvc) . (.Microsoft Corporation - Xbox Live Networking Service.) -- C:\WINDOWS\system32\XboxNetApiSvc.dll [1025536] =>.Microsoft Corporation

O83 - Search Svchost Services: DcpSvc (DcpSvc) . (.Microsoft Corporation - dcpsvc Task.) -- C:\WINDOWS\system32\dcpsvc.dll [183808] =>.Microsoft Corporation

O83 - Search Svchost Services: RetailDemo (RetailDemo) . (.Microsoft Corporation - RDXService.) -- C:\WINDOWS\system32\RDXService.dll [650752] =>.Microsoft Corporation

O83 - Search Svchost Services: BDESVC (BDESVC) . (.Microsoft Corporation - Service BDE.) -- C:\WINDOWS\System32\bdesvc.dll [361472] =>.Microsoft Corporation

O83 - Search Svchost Services: DsmSvc (DsmSvc) . (.Microsoft Corporation - Gestionnaire d’installation de périphérique.) -- C:\WINDOWS\System32\DeviceSetupManager.dll [197632] =>.Microsoft Corporation

O83 - Search Svchost Services: NcaSvc (NcaSvc) . (.Microsoft Corporation - Service Assistant Connectivité réseau Micro.) -- C:\WINDOWS\System32\ncasvc.dll [167936] =>.Microsoft Corporation

O83 - Search Svchost Services: ProfSvc (ProfSvc) . (.Microsoft Corporation - ProfSvc.) -- C:\WINDOWS\system32\profsvc.dll [358400] =>.Microsoft Corporation

O83 - Search Svchost Services: wlidsvc (wlidsvc) . (.Microsoft Corporation - Service de compte Microsoft®.) -- C:\WINDOWS\system32\wlidsvc.dll [2104320] =>.Microsoft Corporation

O83 - Search Svchost Services: UsoSvc (UsoSvc) . (.Microsoft Corporation - Mettre à jour la session Orchestrator Core.) -- C:\WINDOWS\system32\usocore.dll [539648] =>.Microsoft Corporation

O83 - Search Svchost Services: wisvc (wisvc) . (.Microsoft Corporation - Paramètres de vol.) -- C:\WINDOWS\system32\flightsettings.dll [635904] =>.Microsoft Corporation

O83 - Search Svchost Services: UserManager (UserManager) . (.Microsoft Corporation - UserMgr.) -- C:\WINDOWS\System32\usermgr.dll [1020928] =>.Microsoft Corporation

O83 - Search Svchost Services: XblAuthManager (XblAuthManager) . (.Microsoft Corporation - Xbox Live Auth Manager.) -- C:\WINDOWS\System32\XblAuthManager.dll [1013248] =>.Microsoft Corporation

O83 - Search Svchost Services: XblGameSave (XblGameSave) . (.Microsoft Corporation - Xbox Live Game Save Service.) -- C:\WINDOWS\System32\XblGameSave.dll [1159680] =>.Microsoft Corporation

O83 - Search Svchost Services: NetSetupSvc (NetSetupSvc) . (.Microsoft Corporation - Service Configuration du réseau.) -- C:\WINDOWS\System32\NetSetupSvc.dll [265728] =>.Microsoft Corporation

---\\ Liste des exceptions du parefeu Windows (2) - 1s

O87 - FAEL: "{8AEDB33B-D36F-4549-A6D7-528DE09F9848}" [In-None-P17-TRUE] .(...) -- C:\Program Files (x86)\Microsoft Office\root\Office16\UcMapi.exe (.not file.)

O87 - FAEL: "{B3DE615F-7676-463E-B1D3-43A762F538A9}" [In-None-P17-TRUE] .(...) -- C:\Program Files (x86)\Microsoft Office\root\Office16\Lync.exe (.not file.)

---\\ Scan Additionnel (1) - 0s

~ Aucun élément malicieux ou superflu trouvé.

---\\ Récapitulatif des éléments trouvés sur votre station (1) - 0s

https://www.anti-malware.top/2016/06/09/pirate-de-serveur-proxy-hijacker-proxy/ =>Hijacker.Proxy

~ Unselected Options: O82,

~ End of the scan, 62407 items in 03mn41s (644)(0)