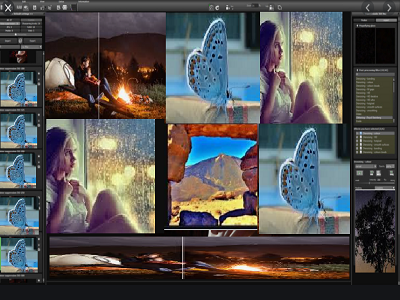
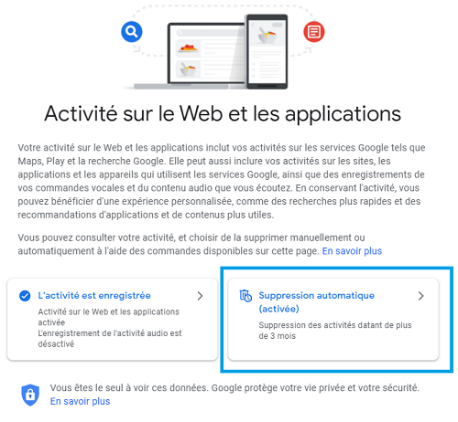
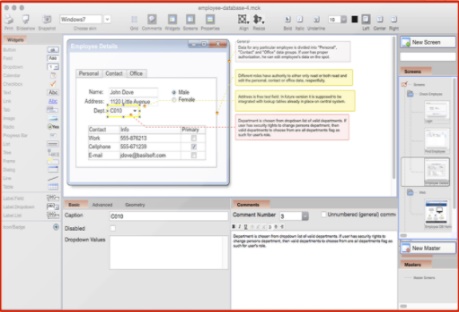
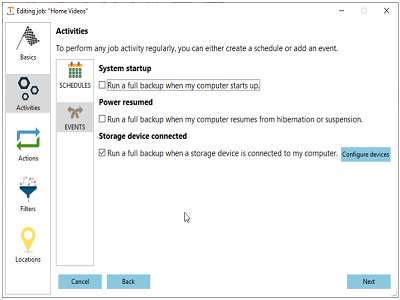
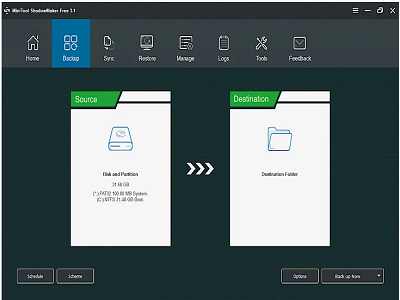
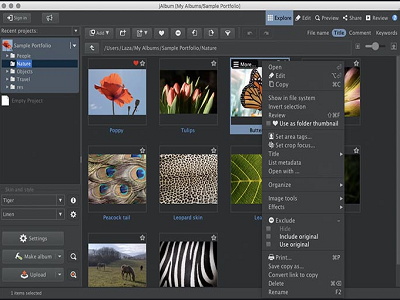
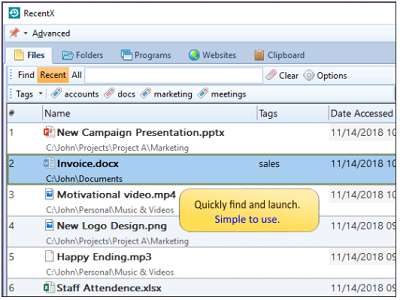
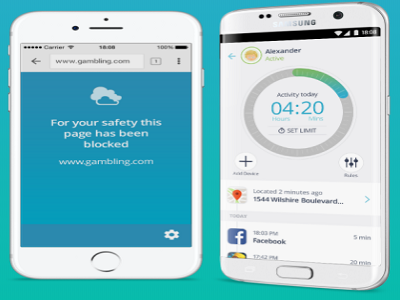
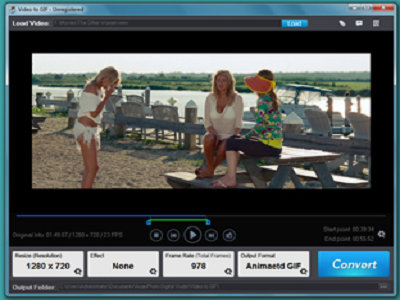
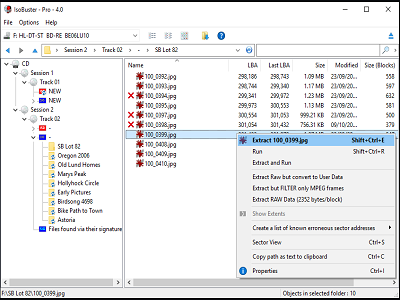
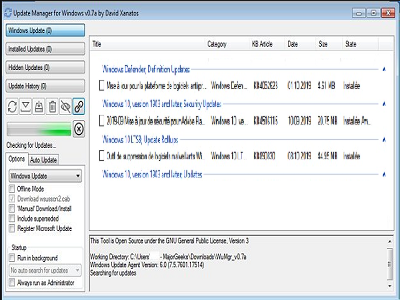
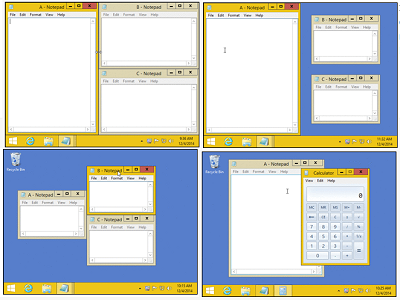
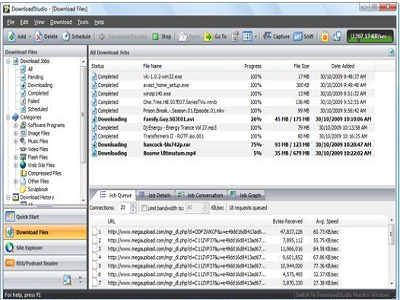
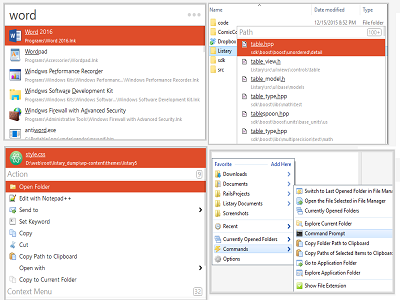
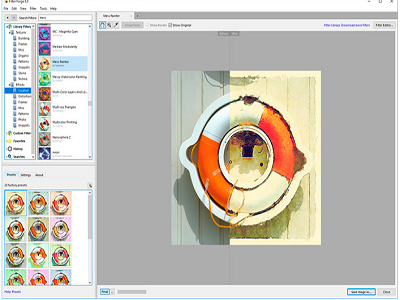
**NEWS ZONE ANTIMALWARE**

[[](https://nicolascoolman.eu/2020/09/25/denoise-projects-logiciel-photo/)](https://nicolascoolman.eu/2020/09/25/denoise-projects-logiciel-photo/)[[](https://nicolascoolman.eu/2020/09/21/comment-effacer-le-suivi-dactivite-de-votre-compte-google/)](https://nicolascoolman.eu/2020/09/21/comment-effacer-le-suivi-dactivite-de-votre-compte-google/)[[](https://nicolascoolman.eu/2020/08/08/telechargement-de-logiciels-gratuits-sur-site-officiel/)](https://nicolascoolman.eu/2020/08/08/telechargement-de-logiciels-gratuits-sur-site-officiel/)[[](https://nicolascoolman.eu/2020/09/15/mockupscreens-logiciel-de-conception/)](https://nicolascoolman.eu/2020/09/15/mockupscreens-logiciel-de-conception/)[[](https://nicolascoolman.eu/2020/09/12/telecharger-ivybackup-logiciel-de-sauvegarde/)](https://nicolascoolman.eu/2020/09/12/telecharger-ivybackup-logiciel-de-sauvegarde/)[[](https://nicolascoolman.eu/2020/09/09/minitool-shadowmaker-logiciel-de-sauvegarde/)](https://nicolascoolman.eu/2020/09/09/minitool-shadowmaker-logiciel-de-sauvegarde/)[[](https://nicolascoolman.eu/2020/09/06/jalbum-gestion-dalbum-photo/)](https://nicolascoolman.eu/2020/09/06/jalbum-gestion-dalbum-photo/)[[](https://nicolascoolman.eu/2020/09/04/minitool-power-data-recovery-gratuit/)](https://nicolascoolman.eu/2020/09/04/minitool-power-data-recovery-gratuit/)[[](https://nicolascoolman.eu/2020/09/03/recentx-gestionnaire-de-fichiers/)](https://nicolascoolman.eu/2020/09/03/recentx-gestionnaire-de-fichiers/)[[](https://nicolascoolman.eu/2020/09/01/qustodio-controle-parental/)](https://nicolascoolman.eu/2020/09/01/qustodio-controle-parental/)[[](https://nicolascoolman.eu/2020/08/30/video-to-gif-convertisseur-video/)](https://nicolascoolman.eu/2020/08/30/video-to-gif-convertisseur-video/)[[](https://nicolascoolman.eu/2020/08/25/isobuster-logiciel-de-recuperation-de-donnees/)](https://nicolascoolman.eu/2020/08/25/isobuster-logiciel-de-recuperation-de-donnees/)[[](https://nicolascoolman.eu/2020/08/24/wumgr-gestion-des-mises-a-jour-windows/)](https://nicolascoolman.eu/2020/08/24/wumgr-gestion-des-mises-a-jour-windows/)[[](https://nicolascoolman.eu/2020/08/23/gestion-fenetres/)](https://nicolascoolman.eu/2020/08/23/gestion-fenetres/)[[](https://nicolascoolman.eu/2020/08/21/downloadstudio-gestionnaire-de-telechargement/)](https://nicolascoolman.eu/2020/08/21/downloadstudio-gestionnaire-de-telechargement/)[[](https://nicolascoolman.eu/2020/08/18/listary-gestion-de-fichier/)](https://nicolascoolman.eu/2020/08/18/listary-gestion-de-fichier/)[[](https://nicolascoolman.eu/2020/08/15/filter-forge-montage-photo/)](https://nicolascoolman.eu/2020/08/15/filter-forge-montage-photo/)[](https://nicolascoolman.eu/2020/08/14/videopad-montage-video-gratuit/)

**RAPPORT DE DIAGNOSTIC DE ZHPDIAG**

~ ZHPDiag v2020.9.30.239 Par Nicolas Coolman (2020/09/30)

~ Démarré par ericl (Administrator) (2020/09/30 16:33:48)

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

~ Blog: https://nicolascoolman.eu/

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

~ Certificate ZHPDiag: Legal

~ Etat de la version: Version OK

~ Mode: Scanner

~ Rapport: D:\OneDrive\Bureau\ZHPDiag.txt

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

~ UAC: Activate

~ Démarrage du système: Normal (Normal boot)

Windows 10 Home, 64-bit (Build 19041)

**---\ NAVIGATEURS INTERNET (2) - 0s**

~ MSIE: Internet Explorer v11.508.19041.0

~ OBIE: Microsoft Edge v85.0.564.63

**---\ INFORMATIONS SUR LES PRODUITS WINDOWS (8) - 3s**

~ 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 : FGDDR

Windows License : OK

~ Windows Remaining Initializations Number : 1001

Windows Automatic Updates : OK

**---\ LOGICIELS DE PROTECTION (2) - 4s**

Windows Defender W10 (Activate) (Protection)

Malwarebytes version 4.2.1.89 v4.2.1.89 (Protection)

**---\ SURVEILLANCE LOGICIEL (1) - 4s**

~ Adobe Acrobat Reader DC - Français (Surveillance)

**---\ LOGICIELS D'OPTIMISATION (2) - 4s**

~ CCleaner Browser v85.0.5824.105 (Optimisation)

~ CCleaner v5.70 (Optimisation)

**---\ INFORMATIONS SUR LE SYSTÈME (6) - 0s**

~ Operating System: Intel64 Family 6 Model 142 Stepping 10, GenuineIntel

~ Operating System: 64-bit

~ Boot mode: Normal (Normal boot)

Total RAM: 8227.556 MB (13% free) : OK =>.RAM Value

System Restore: Activé (Enable)

System drive C: has 19 GB (23%) free of 81 GB : ATTENTION =>Warning Disk Space

**---\ MODE DE CONNEXION AU SYSTÈME (3) - 0s**

~ Computer Name: ELOUTRE\_PC

~ User Name: ericl

~ Logged in as Administrator

**---\ ÉNUMÉRATION DES UNITÉS DE STOCKAGE (2) - 0s**

~ Drive C: has 19 GB free of 81 GB (System)

~ Drive D: has 47 GB free of 146 GB

**---\ ÉTAT DU CENTRE DE SÉCURITÉ WINDOWS (7) - 0s**

[HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer] NoActiveDesktopChanges: Modified

[HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\policies\system] EnableLUA: OK

[HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\NOHIDDEN] CheckedValue: Modified

[HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL] CheckedValue: OK

[HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer\Associations] Application: OK

[HKLM\Software\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon] Shell: OK

[HKLM64\SYSTEM\CurrentControlSet\Services\COMSysApp] Type: OK

**---\ RECHERCHE PARTICULIÈRE DE FICHIERS GÉNÉRIQUES (26) - 1s**

[MD5.C56BF71C18D9CB67F7B9986817A481BE] - 10/09/2020 - (.Microsoft Corporation - Explorateur Windows.) -- C:\WINDOWS\Explorer.exe [4592136] =>.Microsoft®

[MD5.44B041922105E01BFD0D096123F7D312] - 07/12/2019 - (.Microsoft Corporation - Processus hôte Windows (Rundll32).) -- C:\WINDOWS\System32\rundll32.exe [71680] [Unsigned] =>.Microsoft Corporation

[MD5.4BD4AFF6FD90E92043818B79FDE27F09] - 07/12/2019 - (.Microsoft Corporation - Application de démarrage de Windows.) -- C:\WINDOWS\System32\Wininit.exe [418608] [Unsigned] =>.Microsoft Corporation

[MD5.1343F38C6F2F0AD8AE0BAFF08B14EB7D] - 10/09/2020 - (.Microsoft Corporation - Extensions Internet pour Win32.) -- C:\WINDOWS\System32\wininet.dll [5056000] [Unsigned] =>.Microsoft Corporation

[MD5.8B9B35206487D39B2D3D076444485EC2] - 07/12/2019 - (.Microsoft Corporation - Application d’ouverture de session Windows.) -- C:\WINDOWS\System32\Winlogon.exe [907776] [Unsigned] =>.Microsoft Corporation

[MD5.3F910E7BB716BCD9B4C06EE6CF20304A] - 10/09/2020 - (.Microsoft Corporation - Bibliothèque de licences.) -- C:\WINDOWS\System32\sppcomapi.dll [316416] [Unsigned] =>.Microsoft Corporation

[MD5.403BAB9BFBDD33E52451F59FE02629C1] - 10/09/2020 - (.Microsoft Corporation - DNS DLL de l’API Client.) -- C:\WINDOWS\System32\dnsapi.dll [827912] =>.Microsoft®

[MD5.4116BF1EEA2BA39A56C83274AA6D92D8] - 10/09/2020 - (.Microsoft Corporation - DNS DLL de l’API Client.) -- C:\WINDOWS\Syswow64\dnsapi.dll [585696] =>.Microsoft®

[MD5.EFC3573F588989978DC0C1CFDFADA553] - 10/09/2020 - (.Microsoft Corporation - Agent de mise à jour automatique Windows Up.) -- C:\WINDOWS\System32\wuaueng.dll [3384832] [Unsigned] =>.Microsoft Corporation

[MD5.3996E9A5F0CC85E93AA7ADE49A892C5E] - 07/12/2019 - (.Microsoft Corporation - DLL client de l’API uilisateur de Windows m.) -- C:\WINDOWS\System32\fr-FR\user32.dll.mui [19968] [Unsigned] =>.Microsoft Corporation

[MD5.6F082A5EB40F9BFD6873F3796F10F866] - 10/09/2020 - (.Microsoft Corporation - Pilote de fonction connexe pour WinSock.) -- C:\WINDOWS\System32\drivers\AFD.sys [647480] [Unsigned] =>.Microsoft Corporation

[MD5.C394B2347795AB247F4F4FFAB46B8935] - 10/09/2020 - (.Microsoft Corporation - ATAPI IDE Miniport Driver.) -- C:\WINDOWS\System32\drivers\atapi.sys [30024] [Unsigned] =>.Microsoft Corporation

[MD5.764FE2149251A246F6B047A0F09F5F0B] - 07/12/2019 - (.Microsoft Corporation - CD-ROM File System Driver.) -- C:\WINDOWS\System32\drivers\Cdfs.sys [100864] [Unsigned] =>.Microsoft Corporation

[MD5.26255C953A69CCD32EF4491411737904] - 07/12/2019 - (.Microsoft Corporation - SCSI CD-ROM Driver.) -- C:\WINDOWS\System32\drivers\Cdrom.sys [174080] [Unsigned] =>.Microsoft Corporation

[MD5.E958B2741A04DD6442F8AD0FE543D473] - 07/12/2019 - (.Microsoft Corporation - DFS Namespace Client Driver.) -- C:\WINDOWS\System32\drivers\DfsC.sys [152064] [Unsigned] =>.Microsoft Corporation

[MD5.4BFD517F80F247590AB6C03E3FF55E1A] - 07/12/2019 - (.Microsoft Corporation - High Definition Audio Bus Driver.) -- C:\WINDOWS\System32\drivers\HDAudBus.sys [132608] [Unsigned] =>.Microsoft Corporation

[MD5.E4B36C6EAAAB703CBFECB92EE590FB31] - 07/12/2019 - (.Microsoft Corporation - Pilote de port i8042.) -- C:\WINDOWS\System32\drivers\i8042prt.sys [118272] [Unsigned] =>.Microsoft Corporation

[MD5.F63572DF4295C78B3F7036AEDA878176] - 07/12/2019 - (.Microsoft Corporation - IP Network Address Translator.) -- C:\WINDOWS\System32\drivers\IpNat.sys [225280] [Unsigned] =>.Microsoft Corporation

[MD5.6EE28BABC5134E6FBEE8335496C55B39] - 10/09/2020 - (.Microsoft Corporation - Minirdr SMB Windows NT.) -- C:\WINDOWS\System32\drivers\MRxSmb.sys [573752] [Unsigned] =>.Microsoft Corporation

[MD5.F40D4DAFAC8D949AE1738D536D74DD1C] - 07/12/2019 - (.Microsoft Corporation - MBT Transport driver.) -- C:\WINDOWS\System32\drivers\netBT.sys [342016] [Unsigned] =>.Microsoft Corporation

[MD5.CDBB82FE58FB8D8F9423BB9EF3498CF3] - 10/09/2020 - (.Microsoft Corporation - Pilote du système de fichiers NT.) -- C:\WINDOWS\System32\drivers\ntfs.sys [2851128] [Unsigned] =>.Microsoft Corporation

[MD5.138FDB1EBCB61287A645BD3B06DBED5E] - 07/12/2019 - (.Microsoft Corporation - Pilote de port parallèle.) -- C:\WINDOWS\System32\drivers\Parport.sys [109056] [Unsigned] =>.Microsoft Corporation

[MD5.40CBDB4B80284451536C8CA49561E5CD] - 10/09/2020 - (.Microsoft Corporation - RAS L2TP mini-port/call-manager driver.) -- C:\WINDOWS\System32\drivers\Rasl2tp.sys [110080] [Unsigned] =>.Microsoft Corporation

[MD5.5C322D590CEBCAF2F333EBE70E178AB4] - 07/12/2019 - (.Microsoft Corporation - Redirecteur de périphérique de Microsoft RD.) -- C:\WINDOWS\System32\drivers\rdpdr.sys [168448] [Unsigned] =>.Microsoft Corporation

[MD5.9C4C6E0C590F789CECB7A6D437E5A284] - 07/12/2019 - (.Microsoft Corporation - TDI Translation Driver.) -- C:\WINDOWS\System32\drivers\tdx.sys [117560] [Unsigned] =>.Microsoft Corporation

[MD5.988A7A685BB51BAC62F4E176BE5432AC] - 10/09/2020 - (.Microsoft Corporation - Pilote de cliché instantané du volume.) -- C:\WINDOWS\System32\drivers\volsnap.sys [429880] [Unsigned] =>.Microsoft Corporation

**---\ LISTE DES SERVICES (Non désactivés) (88) - 4s**

O23 - Service: Adobe Acrobat Update Service (AdobeARMservice) . (.Adobe Inc. - Adobe Acrobat Update Service.) - C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe =>.Adobe Inc.®

O23 - Service: Intel® SGX AESM (AESMService) . (.Intel Corporation - Intel® SGX Application Enclave Services Man.) - C:\Windows\System32\DriverStore\FileRepository\sgx\_psw.inf\_amd64\_1781f8bae8fdf5c0\aesm\_service.exe =>.Intel(R) pGFX®

O23 - Service: C:\WINDOWS\System32\AudioEndpointBuilder.dll (AudioEndpointBuilder) . (.Microsoft Corporation - Générateur de points de terminaison du serv.) - C:\WINDOWS\System32\AudioEndpointBuilder.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\audiosrv.dll (Audiosrv) . (.Microsoft Corporation - Service Audio Windows.) - C:\WINDOWS\System32\Audiosrv.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\bfe.dll (BFE) . (.Microsoft Corporation - Moteur de filtrage de base.) - C:\WINDOWS\System32\bfe.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\system32\bisrv.dll (BrokerInfrastructure) . (.Microsoft Corporation - Process State Manager (PSM) Service.) - C:\WINDOWS\System32\psmsrv.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: Service CCleaner Browser Update (ccleaner) (ccleaner) . (.Piriform Software - CCleaner Browser.) - C:\Program Files (x86)\CCleaner Browser\Update\CCleanerBrowserUpdate.exe =>.Piriform Software Ltd®

O23 - Service: C:\WINDOWS\System32\cdpusersvc.dll (CDPUserSvc) . (.Microsoft Corporation - Composants utilisateur Microsoft (R) CDP.) - C:\WINDOWS\System32\CDPUserSvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: Service pour utilisateur de plateforme d’appareils connecté (CDPUserSvc\_536f674) . (.Microsoft Corporation - Processus hôte pour les services Windows.) - C:\Windows\System32\svchost.exe =>.Microsoft®

O23 - Service: C:\WINDOWS\System32\certprop.dll (CertPropSvc) . (.Microsoft Corporation - Service de propagation de certificats de ca.) - C:\WINDOWS\System32\certprop.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: Service Microsoft Office « Démarrer en un clic » (ClickToRunSvc) . (.Microsoft Corporation - Microsoft Office Click-to-Run (SxS).) - C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe =>.Microsoft®

O23 - Service: C:\Windows\System32\coremessaging.dll (CoreMessagingRegistrar) . (.Microsoft Corporation - Microsoft CoreMessaging Dll.) - C:\Windows\System32\coremessaging.dll =>.Microsoft®

O23 - Service: Intel(R) Content Protection HDCP Service (cplspcon) . (.Intel Corporation - Intel HD Graphics Drivers for Windows(R).) - C:\Windows\System32\DriverStore\FileRepository\igdlh64.inf\_amd64\_c8634ed19e331cda\IntelCpHDCPSvc.exe =>.Intel(R) pGFX®

O23 - Service: C:\WINDOWS\System32\cryptsvc.dll (CryptSvc) . (.Microsoft Corporation - Services de chiffrement.) - C:\WINDOWS\System32\cryptsvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: Service Mise à jour Dropbox (dbupdate) (dbupdate) . (.Dropbox, Inc. - Dropbox Update.) - C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe =>.Dropbox, Inc®

O23 - Service: DbxSvc (DbxSvc) . (.Dropbox, Inc. - Dropbox Service.) - C:\WINDOWS\System32\DbxSvc.exe [Unsigned] =>.Dropbox, Inc.

O23 - Service: C:\WINDOWS\System32\das.dll (DeviceAssociationService) . (.Microsoft Corporation - Service d’association de périphérique.) - C:\WINDOWS\System32\das.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\Windows\System32\dhcpcore.dll (Dhcp) . (.Microsoft Corporation - Service client DHCP.) - C:\Windows\System32\dhcpcore.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\diagtrack.dll (DiagTrack) . (.Microsoft Corporation - Suivi des diagnostics Microsoft Windows.) - C:\WINDOWS\System32\diagtrack.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\dispbroker.desktop.dll (DispBrokerDesktopSvc) . (.Microsoft Corporation - Courtier d'affichage du bureau.) - C:\WINDOWS\System32\DispBroker.Desktop.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\dmwappushsvc.dll (dmwappushservice) . (.Microsoft Corporation - dmwappushsvc.) - C:\WINDOWS\System32\dmwappushsvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\Windows\System32\dnsapi.dll (Dnscache) . (.Microsoft Corporation - Service de résolution du cache DNS.) - C:\WINDOWS\System32\dnsrslvr.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: Dolby DAX API Service (DolbyDAXAPI) . (...) - C:\WINDOWS\System32\dolbyaposvc\DAX3API.exe [Unsigned]

O23 - Service: C:\WINDOWS\System32\dosvc.dll (DoSvc) . (.Microsoft Corporation - Processus hôte pour les services Windows.) - C:\Windows\System32\svchost.exe =>.Microsoft®

O23 - Service: C:\WINDOWS\System32\dusmsvc.dll (DusmSvc) . (.Microsoft Corporation - Service Consommation des données.) - C:\WINDOWS\System32\dusmsvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: Service Mise à jour de Microsoft Edge (edgeupdate) (edgeupdate) . (.Microsoft Corporation - Microsoft Edge Update.) - C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe =>.Microsoft®

O23 - Service: Intel(R) Dynamic Platform and Thermal Framework service (esifsvc) . (.Intel Corporation - Intel(R) Dynamic Platform and Thermal Frame.) - C:\WINDOWS\System32\Intel\DPTF\esif\_uf.exe [Unsigned] =>.Intel Corporation

O23 - Service: C:\WINDOWS\System32\wevtsvc.dll (EventLog) . (.Microsoft Corporation - Service journal des événements.) - C:\WINDOWS\System32\wevtsvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: @comres.dll,-2450 (EventSystem) . (.Microsoft Corporation - COM+.) - C:\Windows\System32\es.dll [Unsigned] =>.Microsoft 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®

O23 - Service: Fortemedia APO Control Service (FMAPOService) . (.Fortemedia - Fortemedia Service.) - C:\WINDOWS\System32\FMService64.exe [Unsigned] =>.Fortemedia

O23 - Service: C:\WINDOWS\System32\FntCache.dll (FontCache) . (.Microsoft Corporation - Service de cache de police Windows.) - C:\WINDOWS\System32\FntCache.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: @gpapi.dll,-112 (gpsvc) . (.Microsoft Corporation - Client de stratégie de groupe.) - C:\WINDOWS\System32\gpsvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: Service Google Update (gupdate) (gupdate) . (.Google LLC - Programme d'installation de Google.) - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe =>.Google Inc®

O23 - Service: Intel(R) HD Graphics Control Panel Service (igfxCUIService2.0.0.0) . (.Intel Corporation - igfxCUIService Module.) - C:\Windows\System32\DriverStore\FileRepository\igdlh64.inf\_amd64\_c8634ed19e331cda\igfxCUIService.exe =>.Intel(R) pGFX®

O23 - Service: Intel(R) TPM Provisioning Service (Intel(R) TPM Provisioning Service) . (.Intel(R) Corporation - Intel(R) TPM Provisioning Service.) - C:\Program Files\Intel\Intel(R) Management Engine Components\iCLS\TPMProvisioningService.exe =>.Intel(R) Trust Services®

O23 - Service: C:\WINDOWS\System32\iphlpsvc.dll (iphlpsvc) . (.Microsoft Corporation - Service offrant une connectivité IPv6 sur u.) - C:\WINDOWS\System32\iphlpsvc.dll [Unsigned] =>.Microsoft Corporation

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 =>.Intel(R) Embedded Subsystems and IP Blocks Group®

O23 - Service: C:\WINDOWS\System32\srvsvc.dll (LanmanServer) . (.Microsoft Corporation - DLL du service Serveur.) - C:\WINDOWS\System32\srvsvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\wkssvc.dll (LanmanWorkstation) . (.Microsoft Corporation - DLL du service Station de travail.) - C:\WINDOWS\System32\wkssvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: Huawei LCD\_Service (LCD\_Service) . (.Microsoft - LCD\_Service.) - C:\Program Files\Huawei\HwLcdEnhancement\LCD\_Service.exe {6E715E33F17AD55BCBF98C1F14D21F2F}. =>.Microsoft

O23 - Service: Intel(R) Management and Security Application Local Manageme (LMS) . (.Intel Corporation - Intel(R) Local Management Service.) - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe =>.Intel(R) Embedded Subsystems and IP Blocks Group®

O23 - Service: C:\WINDOWS\system32\lsm.dll (LSM) . (.Microsoft Corporation - Service du gestionnaire de session locale.) - C:\WINDOWS\System32\lsm.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\moshost.dll (MapsBroker) . (.Microsoft Corporation - Gestionnaire des cartes téléchargées.) - C:\WINDOWS\System32\moshost.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: Huawei PCManager Windows Service (MBAMainService) . (. {6E715E33F17AD55BCBF98C1F14D21F2F}. - .) - C:\Program Files\Huawei\PCManager\MateBookService.exe {6E715E33F17AD55BCBF98C1F14D21F2F}.

O23 - Service: Malwarebytes Service (MBAMService) . (.Malwarebytes - Malwarebytes Service.) - C:\Program Files\Malwarebytes\Anti-Malware\MBAMService.exe =>.Malwarebytes Inc®

O23 - Service: C:\Windows\System32\FirewallAPI.dll (mpssvc) . (.Microsoft Corporation - Service de protection Microsoft.) - C:\WINDOWS\System32\mpssvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: Net Driver HPZ12 (Net Driver HPZ12) . (.HP Inc. - Dot4Net Module.) - C:\Windows\System32\HPZinw12.dll [Unsigned] =>.HP Inc.

O23 - Service: C:\WINDOWS\System32\nlasvc.dll (NlaSvc) . (.Microsoft Corporation - Connaissance des emplacements réseau 2.) - C:\WINDOWS\System32\nlasvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\nsisvc.dll (nsi) . (.Microsoft Corporation - Serveur RPC de l’interface du magasin résea.) - C:\WINDOWS\System32\nsisvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: NVIDIA Display Container LS (NVDisplay.ContainerLocalSystem) . (.NVIDIA Corporation - NVIDIA Container.) - C:\Program Files\NVIDIA Corporation\Display.NvContainer\NVDisplay.Container.exe =>.NVIDIA Corporation®

O23 - Service: NVIDIA Telemetry Container (NvTelemetryContainer) . (.NVIDIA Corporation - NVIDIA Container.) - C:\Program Files\NVIDIA Corporation\NvTelemetry\NvTelemetryContainer.exe =>.NVIDIA Corporation®

O23 - Service: C:\WINDOWS\System32\APHostRes.dll (OneSyncSvc) . (.Microsoft Corporation - Accounts Host Service.) - C:\WINDOWS\System32\APHostService.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: Hôte de synchronisation\_536f674 (OneSyncSvc\_536f674) . (.Microsoft Corporation - Processus hôte pour les services Windows.) - C:\Windows\System32\svchost.exe =>.Microsoft®

O23 - Service: Huawei OSDMainService Windows Service (OSDMainService) . (. {6E715E33F17AD55BCBF98C1F14D21F2F}. - .) - C:\Program Files\Huawei\HwOsd\OSDMainService.exe {6E715E33F17AD55BCBF98C1F14D21F2F}.

O23 - Service: Pml Driver HPZ12 (Pml Driver HPZ12) . (.HP Inc. - PmlDrv Module.) - C:\Windows\System32\HPZipm12.dll [Unsigned] =>.HP Inc.

O23 - Service: C:\WINDOWS\System32\umpo.dll (Power) . (.Microsoft Corporation - Service d’alimentation en mode utilisateur.) - C:\WINDOWS\System32\umpo.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\profsvc.dll (ProfSvc) . (.Microsoft Corporation - ProfSvc.) - C:\WINDOWS\System32\profsvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\rasmans.dll (RasMan) . (.Microsoft Corporation - Gestionnaire des connexions d’accès à dista.) - C:\WINDOWS\System32\rasmans.dll [Unsigned] =>.Microsoft Corporation

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®

O23 - Service: C:\WINDOWS\system32\RpcEpMap.dll (RpcEptMapper) . (.Microsoft Corporation - Mappeur de point de terminaison RPC.) - C:\WINDOWS\System32\RpcEpMap.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: @combase.dll,-5010 (RpcSs) . (.Microsoft Corporation - Distributed COM Services.) - C:\WINDOWS\System32\rpcss.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: Realtek Audio Universal Service (RtkAudioUniversalService) . (.Realtek Semiconductor - Realtek HD Audio Universal Service.) - C:\WINDOWS\System32\RtkAudUService64.exe [Unsigned] =>.Realtek Semiconductor

O23 - Service: C:\WINDOWS\System32\schedsvc.dll (Schedule) . (.Microsoft Corporation - Service du Planificateur de tâches.) - C:\WINDOWS\System32\schedsvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\Sens.dll (SENS) . (.Microsoft Corporation - Service de notification d’événements systèm.) - C:\WINDOWS\System32\sens.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: Session Detection (SessionSvc) . (...) - C:\WINDOWS\System32\drivers\SessionService.exe [Unsigned]

O23 - Service: C:\WINDOWS\System32\SgrmBroker.exe,-100 (SgrmBroker) . (.Microsoft Corporation - Service Broker du moniteur d'exécution Syst.) - C:\WINDOWS\System32\SgrmBroker.exe [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\Windows\System32\shsvcs.dll (ShellHWDetection) . (.Microsoft Corporation - Dll des services Windows Shell.) - C:\Windows\System32\shsvcs.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\spoolsv.exe,-1 (Spooler) . (.Microsoft Corporation - Application sous-système spouleur.) - C:\WINDOWS\System32\spoolsv.exe [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\sppsvc.exe,-101 (sppsvc) . (.Microsoft Corporation - Service de la plateforme de protection logi.) - C:\WINDOWS\System32\sppsvc.exe [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\wiaservc.dll (stisvc) . (.Microsoft Corporation - Service de périphériques d’images fixes.) - C:\WINDOWS\System32\wiaservc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\StorSvc.dll (StorSvc) . (.Microsoft Corporation - Services de stockage.) - C:\WINDOWS\System32\storsvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\sysmain.dll (SysMain) . (.Microsoft Corporation - Hôte de Service SysMain.) - C:\WINDOWS\System32\sysmain.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\system32\SystemEventsBrokerServer.dll (SystemEventsBroker) . (.Microsoft Corporation - Service Broker pour les événements système.) - C:\WINDOWS\System32\SystemEventsBrokerServer.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\themeservice.dll (Themes) . (.Microsoft Corporation - DLL du service des thèmes Windows Shell.) - C:\WINDOWS\System32\themeservice.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\usermgr.dll (UserManager) . (.Microsoft Corporation - UserMgr.) - C:\WINDOWS\System32\usermgr.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\usosvc.dll (UsoSvc) . (.Microsoft Corporation - Mettre à jour la session du service Orchest.) - C:\WINDOWS\System32\usosvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\wbiosrvc.dll (WbioSrvc) . (.Microsoft Corporation - Service de biométrie Windows.) - C:\WINDOWS\System32\wbiosrvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\wcmsvc.dll (Wcmsvc) . (.Microsoft Corporation - DLL du service de gestion des connexions Wi.) - C:\WINDOWS\System32\wcmsvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: @%ProgramFiles%\Windows Defender\MpAsDesc.dll,-310 (WinDefend) . (.Microsoft Corporation - Antimalware Service Executable.) - C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2009.2-0\MsMpEng.exe =>.Microsoft®

O23 - Service: C:\WINDOWS\System32\wbem\wmisvc.dll (Winmgmt) . (.Microsoft Corporation - WMI.) - C:\WINDOWS\System32\wbem\WMIsvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\wlansvc.dll (WlanSvc) . (.Microsoft Corporation - DLL du service de configuration automatique.) - C:\WINDOWS\System32\wlansvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\wpnservice.dll (WpnService) . (.Microsoft Corporation - Service du système de notifications Push Wi.) - C:\WINDOWS\System32\WpnService.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\WpnUserService.dll (WpnUserService) . (.Microsoft Corporation - Service utilisateur de notifications Push W.) - C:\WINDOWS\System32\WpnUserService.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: Service utilisateur de notifications Push Windows\_536f674 (WpnUserService\_536f674) . (.Microsoft Corporation - Processus hôte pour les services Windows.) - C:\Windows\System32\svchost.exe =>.Microsoft®

O23 - Service: C:\WINDOWS\System32\wscsvc.dll (wscsvc) . (.Microsoft Corporation - Service Centre de sécurité de Windows.) - C:\WINDOWS\System32\wscsvc.dll [Unsigned] =>.Microsoft Corporation

O23 - Service: C:\WINDOWS\System32\SearchIndexer.exe,-103 (WSearch) . (.Microsoft Corporation - Indexeur Microsoft Windows Search.) - C:\Windows\System32\SearchIndexer.exe [Unsigned] =>.Microsoft Corporation

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®

**---\ SERVICES NON MICROSOFT (SR=Démarré,SS=Stoppé) (109) - 16s**

SR - Boot [07/12/2019] [ 107320] (3ware) . (.LSI.) - C:\WINDOWS\System32\drivers\3ware.sys =>.Microsoft®

SR - Auto [06/09/2020] [ 169544] Adobe Acrobat Update Service (AdobeARMservice) . (.Adobe Inc..) - C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe =>.Adobe Inc.®

SR - Boot [07/12/2019] [ 1135416] (ADP80XX) . (.PMC-Sierra.) - C:\WINDOWS\System32\drivers\ADP80XX.SYS =>.Microsoft®

SR - Auto [03/02/2018] [ 3226664] Intel® SGX AESM (AESMService) . (.Intel Corporation.) - C:\Windows\System32\DriverStore\FileRepository\sgx\_psw.inf\_amd64\_1781f8bae8fdf5c0\aesm\_service.exe =>.Intel(R) pGFX®

SR - Demand [07/12/2019] [ 18432] AMD GPIO Client Driver (amdgpio2) . (.Advanced Micro Devices, Inc.) - C:\WINDOWS\System32\drivers\amdgpio2.sys [Unsigned] =>.Advanced Micro Devices, Inc

SR - Demand [07/12/2019] [ 45568] AMD I2C Controller Service (amdi2c) . (.Advanced Micro Devices, Inc.) - C:\WINDOWS\System32\drivers\amdi2c.sys [Unsigned] =>.Advanced Micro Devices, Inc

SR - Boot [07/12/2019] [ 83256] (amdsata) . (.Advanced Micro Devices.) - C:\WINDOWS\System32\drivers\amdsata.sys =>.Microsoft®

SR - Boot [07/12/2019] [ 259384] (amdsbs) . (.AMD Technologies Inc..) - C:\WINDOWS\System32\drivers\amdsbs.sys =>.Microsoft®

SR - Boot [07/12/2019] [ 26936] (amdxata) . (.Advanced Micro Devices.) - C:\WINDOWS\System32\drivers\amdxata.sys =>.Microsoft®

SR - Boot [07/12/2019] [ 131896] Adaptec SAS/SATA-II RAID S (arcsas) . (.PMC-Sierra, Inc..) - C:\WINDOWS\System32\drivers\arcsas.sys =>.Microsoft®

SR - Boot [07/12/2019] [ 533816] QLogic Network Adapter VBD (b06bdrv) . (.QLogic Corporation.) - C:\WINDOWS\System32\drivers\bxvbda.sys =>.Microsoft®

SR - Demand [07/12/2019] [ 9728] bcmfn2 Service (bcmfn2) . (...) - C:\WINDOWS\System32\drivers\bcmfn2.sys [Unsigned] =>.Broadcom Corporation

SR - Auto [03/09/2020] [ 200928] Service CCleaner Browser Update (ccleaner) (ccleaner) . (.Piriform Software.) - C:\Program Files (x86)\CCleaner Browser\Update\CCleanerBrowserUpdate.exe =>.Piriform Software Ltd®

SS - Demand [10/09/2020] [ 1080640] CCleaner Browser Elevation Service (CCleanerBrowserElevationService) . (.Piriform Software.) - C:\Program Files (x86)\CCleaner Browser\Application\85.0.5824.105\elevation\_service.exe =>.Piriform Software Ltd®

SS - Demand [03/09/2020] [ 200928] Service CCleaner Browser Update (ccleanerm) (ccleanerm) . (.Piriform Software.) - C:\Program Files (x86)\CCleaner Browser\Update\CCleanerBrowserUpdate.exe =>.Piriform Software Ltd®

SR - Boot [07/12/2019] [ 319800] (cht4iscsi) . (.Chelsio Communications.) - C:\WINDOWS\System32\drivers\cht4sx64.sys =>.Microsoft®

SR - Demand [07/12/2019] [ 1853752] Chelsio Virtual Bus Driver (cht4vbd) . (.Chelsio Communications.) - C:\WINDOWS\System32\drivers\cht4vx64.sys =>.Microsoft®

SS - Demand [10/10/2018] [ 510240] Intel(R) Content Protection HECI Service (cphs) . (.Intel Corporation.) - C:\Windows\System32\DriverStore\FileRepository\igdlh64.inf\_amd64\_c8634ed19e331cda\IntelCpHeciSvc.exe =>.Intel(R) pGFX®

SR - Auto [10/10/2018] [ 505120] Intel(R) Content Protection HDCP Service (cplspcon) . (.Intel Corporation.) - C:\Windows\System32\DriverStore\FileRepository\igdlh64.inf\_amd64\_c8634ed19e331cda\IntelCpHDCPSvc.exe =>.Intel(R) pGFX®

SR - Auto [26/04/2019] [ 143144] Service Mise à jour Dropbox (dbupdate) (dbupdate) . (.Dropbox, Inc..) - C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe =>.Dropbox, Inc®

SS - Demand [26/04/2019] [ 143144] Service Mise à jour Dropbox (dbupdatem) (dbupdatem) . (.Dropbox, Inc..) - C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe =>.Dropbox, Inc®

SR - Auto [22/09/2020] [ 44552] DbxSvc (DbxSvc) . (.Dropbox, Inc..) - C:\WINDOWS\System32\DbxSvc.exe =>.Dropbox, Inc®

SR - Demand [18/05/2017] [ 131984] SAMSUNG Mobile USB Comp (dg\_ssudbus) . (.Samsung Electronics Co., Ltd..) - C:\WINDOWS\System32\DRIVERS\ssudbus.sys =>.Samsung Electronics Co., Ltd.®

SR - Auto [19/01/2019] [ 598384] Dolby DAX API Service (DolbyDAXAPI) . (.Dolby Laboratories, Inc..) - C:\WINDOWS\System32\dolbyaposvc\DAX3API.exe =>.Dolby Laboratories, Inc.®

SR - Demand [08/11/2017] [ 74144] (dptf\_acpi) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\dptf\_acpi.sys =>.Intel Corporation®

SR - Demand [08/11/2017] [ 69536] (dptf\_cpu) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\dptf\_cpu.sys =>.Intel Corporation®

SR - Boot [07/12/2019] [ 3418936] QLogic 10 Gigabit Ethernet Ada (ebdrv) . (.QLogic Corporation.) - C:\WINDOWS\System32\drivers\evbda.sys =>.Microsoft®

SR - Auto [08/11/2017] [ 1705040] Intel(R) Dynamic Platform a (esifsvc) . (.Intel Corporation.) - C:\WINDOWS\System32\Intel\DPTF\esif\_uf.exe =>.Intel Corporation®

SR - Demand [08/11/2017] [ 382880] (esif\_lf) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\esif\_lf.sys =>.Intel Corporation®

SR - Auto [05/09/2018] [ 670816] Intel(R) PROSet/Wireless Event Log (EvtEng) . (.Intel(R) Corporation.) - C:\Program Files\Intel\WiFi\bin\EvtEng.exe =>.Intel Corporation®

SR - Auto [31/07/2018] [ 306040] Fortemedia APO Control Service (FMAPOService) . (.Fortemedia.) - C:\WINDOWS\System32\FMService64.exe =>.Microsoft Windows Hardware Compatibility Publisher®

SR - Auto [07/11/2019] [ 155432] Service Google Update (gupdate) (gupdate) . (.Google LLC.) - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe =>.Google Inc®

SS - Demand [07/11/2019] [ 155432] Service Google Update (gupdatem) (gupdatem) . (.Google LLC.) - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe =>.Google Inc®

SR - Boot [07/12/2019] [ 64312] (HpSAMD) . (.Hewlett-Packard Company.) - C:\WINDOWS\System32\drivers\HpSAMD.sys =>.Microsoft®

SR - Demand [25/06/2019] [ 30744] hwnetstat (hwnetstat) . (. {6E715E33F17AD55BCBF98C1F14D21F2F}..) - C:\Program Files\Huawei\PCManager\WFPDriver.sys {6E715E33F17AD55BCBF98C1F14D21F2F}.

SR - Auto [25/06/2019] [ 49472] HUAWEI MateBook Os2EC (HwOs2ECx64) . (.Huawei.) - C:\Program Files\Huawei\PCManager\HwOs2EC10x64.sys {6E715E33F17AD55BCBF98C1F14D21F2F}. =>.Huawei

SR - Demand [07/12/2019] [ 36352] Intel Serial IO GPIO Controlle (iagpio) . (.Intel(R) Corporation.) - C:\WINDOWS\System32\drivers\iagpio.sys [Unsigned] =>.Intel(R) Corporation

SR - Demand [07/12/2019] [ 91136] Intel(R) Serial IO I2C Host Cont (iai2c) . (.Intel(R) Corporation.) - C:\WINDOWS\System32\drivers\iai2c.sys [Unsigned] =>.Intel(R) Corporation

SR - Demand [07/12/2019] [ 79360] Intel(R) S (iaLPSS2i\_GPIO2) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i\_GPIO2.sys [Unsigned] =>.Intel Corporation

SR - Demand [07/12/2019] [ 93184] In (iaLPSS2i\_GPIO2\_BXT\_P) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i\_GPIO2\_BXT\_P.sys [Unsigned] =>.Intel Corporation

SR - Demand [07/12/2019] [ 112128] Intel( (iaLPSS2i\_GPIO2\_CNL) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i\_GPIO2\_CNL.sys [Unsigned] =>.Intel Corporation

SR - Demand [07/12/2019] [ 96256] Intel( (iaLPSS2i\_GPIO2\_GLK) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i\_GPIO2\_GLK.sys [Unsigned] =>.Intel Corporation

SR - Demand [07/12/2019] [ 171520] Intel(R) Seria (iaLPSS2i\_I2C) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i\_I2C.sys [Unsigned] =>.Intel Corporation

SR - Demand [07/12/2019] [ 175104] Intel( (iaLPSS2i\_I2C\_BXT\_P) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i\_I2C\_BXT\_P.sys [Unsigned] =>.Intel Corporation

SR - Demand [07/12/2019] [ 177152] Intel(R) S (iaLPSS2i\_I2C\_CNL) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i\_I2C\_CNL.sys [Unsigned] =>.Intel Corporation

SR - Demand [07/12/2019] [ 177664] Intel(R) S (iaLPSS2i\_I2C\_GLK) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i\_I2C\_GLK.sys [Unsigned] =>.Intel Corporation

SR - Demand [14/11/2017] [ 158880] Intel(R) Serial IO SPI Dri (iaLPSS2\_SPI) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2\_SPI.sys =>.Intel(R) Embedded Subsystems and IP Blocks Group®

SR - Demand [14/11/2017] [ 310936] Intel(R) Serial IO UART (iaLPSS2\_UART2) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2\_UART2.sys =>.Intel(R) Embedded Subsystems and IP Blocks Group®

SR - Demand [07/12/2019] [ 38128] Intel(R) Serial IO (iaLPSSi\_GPIO) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSSi\_GPIO.sys =>.Intel Corporation - Client Components Group®

SR - Demand [07/12/2019] [ 113152] Intel(R) Serial IO I (iaLPSSi\_I2C) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSSi\_I2C.sys [Unsigned] =>.Intel Corporation

SR - Boot [07/12/2019] [ 884752] Intel Chipset SATA RAI (iaStorAVC) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaStorAVC.sys =>.Microsoft®

SR - Boot [07/12/2019] [ 412176] Intel RAID Controller Wi (iaStorV) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaStorV.sys =>.Microsoft®

SR - Demand [07/12/2019] [ 558904] Mellanox InfiniBand Bus/A (ibbus) . (.Mellanox.) - C:\WINDOWS\System32\drivers\ibbus.sys =>.Microsoft®

SR - Demand [09/03/2018] [ 197696] Intel(R) Wireless Bluetooth (ibtusb) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\ibtusb.sys =>.Intel(R) Wireless Connectivity Solutions®

SR - Demand [10/10/2018] [14072720] (igfx) . (.Intel Corporation.) - C:\Windows\System32\DriverStore\FileRepository\igdlh64.inf\_amd64\_c8634ed19e331cda\igdkmd64.sys =>.Intel(R) pGFX®

SR - Auto [10/10/2018] [ 413072] Intel(R) HD Graphics Control Panel Service (igfxCUIService2.0.0.0) . (.Intel Corporation.) - C:\Windows\System32\DriverStore\FileRepository\igdlh64.inf\_amd64\_c8634ed19e331cda\igfxCUIService.exe =>.Intel(R) pGFX®

SR - Demand [29/03/2019] [ 6787872] Service for Realtek HD Audio (WDM) (IntcAzAudAddService) . (.Realtek Semiconductor Corp..) - C:\WINDOWS\System32\drivers\RTKVHD64.sys =>.Realtek Semiconductor Corp.®

SR - Demand [10/10/2018] [ 635168] Son Intel(R) pour écrans (IntcDAud) . (.Intel(R) Corporation.) - C:\Windows\System32\DriverStore\FileRepository\intcdaud.inf\_amd64\_3b876fb0bfb3390a\IntcDAud.sys =>.Intel(R) pGFX®

SS - Demand [16/11/2017] [ 743728] Intel(R) Capability Licensing Service TCP IP Interface (Intel(R) Capability Licensing Service TCP IP Interface) . (.Intel(R) Corporation.) - C:\Program Files\Intel\Intel(R) Management Engine Components\iCLS\SocketHeciServer.exe =>.Intel(R) Trust Services®

SR - Auto [16/11/2017] [ 720184] Intel(R) TPM Provisioning Service (Intel(R) TPM Provisioning Service) . (.Intel(R) Corporation.) - C:\Program Files\Intel\Intel(R) Management Engine Components\iCLS\TPMProvisioningService.exe =>.Intel(R) Trust Services®

SR - Boot [07/12/2019] [ 172344] (ItSas35i) . (.Avago Technologies.) - C:\WINDOWS\System32\drivers\ItSas35i.sys =>.Microsoft®

SR - Auto [03/12/2017] [ 205968] Intel(R) Dynamic Application Loader Host Interface Service (jhi\_service) . (.Intel Corporation.) - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\DAL\jhi\_service.exe =>.Intel(R) Embedded Subsystems and IP Blocks Group®

SR - Auto [03/12/2017] [ 419984] Intel(R) Management and Security Application Local Manageme (LMS) . (.Intel Corporation.) - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe =>.Intel(R) Embedded Subsystems and IP Blocks Group®

SR - Boot [07/12/2019] [ 108856] (LSI\_SAS) . (.LSI Corporation.) - C:\WINDOWS\System32\drivers\lsi\_sas.sys =>.Microsoft®

SR - Boot [07/12/2019] [ 124216] (LSI\_SAS2i) . (.LSI Corporation.) - C:\WINDOWS\System32\drivers\lsi\_sas2i.sys =>.Microsoft®

SR - Boot [07/12/2019] [ 135992] (LSI\_SAS3i) . (.Avago Technologies.) - C:\WINDOWS\System32\drivers\lsi\_sas3i.sys =>.Microsoft®

SR - Boot [07/12/2019] [ 82744] (LSI\_SSS) . (.LSI Corporation.) - C:\WINDOWS\System32\drivers\lsi\_sss.sys =>.Microsoft®

SR - Auto [25/06/2019] [ 1034224] Huawei PCManager Windows Service (MBAMainService) . (. {6E715E33F17AD55BCBF98C1F14D21F2F}..) - C:\Program Files\Huawei\PCManager\MateBookService.exe {6E715E33F17AD55BCBF98C1F14D21F2F}.

SR - Auto [18/09/2020] [ 217592] MBAMChameleon (MBAMChameleon) . (.Malwarebytes.) - C:\WINDOWS\System32\Drivers\MbamChameleon.sys =>.Malwarebytes Inc®

SR - Boot [22/09/2020] [ 19912] MbamElam (MbamElam) . (.Malwarebytes.) - C:\WINDOWS\System32\DRIVERS\MbamElam.sys =>.Microsoft®

SR - Auto [22/09/2020] [ 7185288] Malwarebytes Service (MBAMService) . (.Malwarebytes.) - C:\Program Files\Malwarebytes\Anti-Malware\MBAMService.exe =>.Malwarebytes Inc®

SR - Demand [22/09/2020] [ 248968] MBAMSwissArmy (MBAMSwissArmy) . (.Malwarebytes.) - C:\WINDOWS\System32\Drivers\mbamswissarmy.sys =>.Malwarebytes Inc®

SR - Boot [07/12/2019] [ 59704] (megasas) . (.Avago Technologies.) - C:\WINDOWS\System32\drivers\megasas.sys =>.Microsoft®

SR - Boot [07/12/2019] [ 81720] (megasas2i) . (.Avago Technologies.) - C:\WINDOWS\System32\drivers\MegaSas2i.sys =>.Microsoft®

SR - Boot [07/12/2019] [ 105480] (megasas35i) . (.Avago Technologies.) - C:\WINDOWS\System32\drivers\megasas35i.sys =>.Microsoft®

SR - Boot [07/12/2019] [ 575800] (megasr) . (.LSI Corporation, Inc..) - C:\WINDOWS\System32\drivers\megasr.sys =>.Microsoft®

SR - Demand [28/11/2017] [ 206488] Intel(R) Management Engine Interfa (MEIx64) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\TeeDriverW8x64.sys =>.Intel(R) Embedded Subsystems and IP Blocks Group®

SR - Demand [07/12/2019] [ 1131320] Mellanox ConnectX Bus E (mlx4\_bus) . (.Mellanox.) - C:\WINDOWS\System32\drivers\mlx4\_bus.sys =>.Microsoft®

SS - Demand [13/07/2020] [ 244432] Mozilla Maintenance Service (MozillaMaintenance) . (.Mozilla Foundation.) - C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe =>.Mozilla Corporation®

SR - Boot [07/12/2019] [ 63800] (mvumis) . (.Marvell Semiconductor, Inc..) - C:\WINDOWS\System32\drivers\mvumis.sys =>.Microsoft®

SS - Demand [05/09/2018] [ 310880] Wireless PAN DHCP Server (MyWiFiDHCPDNS) . (.by Achal Dhir.) - C:\Program Files\Intel\WiFi\bin\PanDhcpDns.exe =>.Intel Corporation®

SR - Demand [07/12/2019] [ 146232] NetworkDirect Service (ndfltr) . (.Mellanox.) - C:\WINDOWS\System32\drivers\ndfltr.sys =>.Microsoft®

SR - Auto [15/06/2016] [ 50688] Net Driver HPZ12 (Net Driver HPZ12) . (.HP Inc..) - C:\Windows\System32\HPZinw12.dll [Unsigned] =>.HP Inc.

SR - Demand [07/12/2019] [ 8803328] \_\_\_ Intel(R) Wireless Adapter Driver for Windows 10 - 64 Bit (Netwtw06) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\Netwtw06.sys [Unsigned] =>.Intel Corporation

SR - Auto [27/08/2018] [ 767472] NVIDIA Display Container LS (NVDisplay.ContainerLocalSystem) . (.NVIDIA Corporation.) - C:\Program Files\NVIDIA Corporation\Display.NvContainer\NVDisplay.Container.exe =>.NVIDIA Corporation®

SR - Demand [11/09/2018] [17234392] (nvlddmkm) . (.NVIDIA Corporation.) - C:\Windows\System32\DriverStore\FileRepository\nvhw.inf\_amd64\_98eca3702c3cd36e\nvlddmkm.sys =>.NVIDIA Corporation®

SR - Boot [07/12/2019] [ 150328] (nvraid) . (.NVIDIA Corporation.) - C:\WINDOWS\System32\drivers\nvraid.sys =>.Microsoft®

SR - Boot [07/12/2019] [ 166200] (nvstor) . (.NVIDIA Corporation.) - C:\WINDOWS\System32\drivers\nvstor.sys =>.Microsoft®

SR - Auto [18/06/2019] [ 782136] NVIDIA Telemetry Container (NvTelemetryContainer) . (.NVIDIA Corporation.) - C:\Program Files\NVIDIA Corporation\NvTelemetry\NvTelemetryContainer.exe =>.NVIDIA Corporation®

SR - Auto [18/01/2019] [ 665928] Huawei OSDMainService Windows Service (OSDMainService) . (. {6E715E33F17AD55BCBF98C1F14D21F2F}..) - C:\Program Files\Huawei\HwOsd\OSDMainService.exe {6E715E33F17AD55BCBF98C1F14D21F2F}.

SR - Boot [07/12/2019] [ 58680] (percsas2i) . (.Avago Technologies.) - C:\WINDOWS\System32\drivers\percsas2i.sys =>.Microsoft®

SR - Boot [07/12/2019] [ 68408] (percsas3i) . (.Avago Technologies.) - C:\WINDOWS\System32\drivers\percsas3i.sys =>.Microsoft®

SR - Auto [15/06/2016] [ 66048] Pml Driver HPZ12 (Pml Driver HPZ12) . (.HP Inc..) - C:\Windows\System32\HPZipm12.dll [Unsigned] =>.HP Inc.

SR - Auto [05/09/2018] [ 170592] Intel(R) PROSet/Wireless Registry Service (RegSrvc) . (.Intel(R) Corporation.) - C:\Program Files\Common Files\Intel\WirelessCommon\RegSrvc.exe =>.Intel Corporation®

SR - Auto [29/03/2019] [ 838432] Realtek Audio Universal Service (RtkAudioUniversalService) . (.Realtek Semiconductor.) - C:\WINDOWS\System32\RtkAudUService64.exe =>.Realtek Semiconductor Corp.®

SR - Demand [12/02/2020] [ 710232] Realtek USB FE/1 (rtux64w10) . (.Realtek Corporation.) - C:\WINDOWS\System32\drivers\rtux64w10.sys =>.Realtek Semiconductor Corp.®

SR - Auto [20/06/2018] [ 30208] Session Detection (SessionSvc) . (.Microsoft Windows Hardware Compatibility Publisher.) - C:\WINDOWS\System32\drivers\SessionService.exe =>.Microsoft Windows Hardware Compatibility Publisher®

SR - Boot [07/12/2019] [ 44856] (SiSRaid2) . (.Silicon Integrated Systems Corp..) - C:\WINDOWS\System32\drivers\SiSRaid2.sys =>.Microsoft®

SR - Boot [07/12/2019] [ 81720] (SiSRaid4) . (.Silicon Integrated Systems.) - C:\WINDOWS\System32\drivers\sisraid4.sys =>.Microsoft®

SR - Boot [07/12/2019] [ 209720] (SmartSAMD) . (.Microsemi Corportation.) - C:\WINDOWS\System32\drivers\SmartSAMD.sys =>.Microsoft®

SR - Demand [18/05/2017] [ 166288] SAMSUNG Mobile USB Modem Dr (ssudmdm) . (.Samsung Electronics Co., Ltd..) - C:\WINDOWS\System32\DRIVERS\ssudmdm.sys =>.Samsung Electronics Co., Ltd.®

SR - Boot [07/12/2019] [ 31032] (stexstor) . (.Promise Technology, Inc..) - C:\WINDOWS\System32\drivers\stexstor.sys =>.Microsoft®

SS - Demand [26/01/2018] [ 2302184] Thunderbolt(TM) Service (ThunderboltService) . (.Intel Corporation.) - C:\Program Files (x86)\Intel\Thunderbolt Software\tbtsvc.exe =>.Intel(R) Client Connectivity Division SW®

SR - Boot [07/12/2019] [ 166712] (vsmraid) . (.VIA Technologies Inc.,Ltd.) - C:\WINDOWS\System32\drivers\vsmraid.sys =>.Microsoft®

SR - Boot [07/12/2019] [ 305464] VIA StorX Storage RAID Co (VSTXRAID) . (.VIA Corporation.) - C:\WINDOWS\System32\drivers\vstxraid.sys =>.Microsoft®

SR - Demand [30/08/2018] [ 37152] WDTDrv (WDTDrv) . (.Huawei Device.) - C:\WINDOWS\System32\Drivers\WDTDrv.sys {6E715E33F17AD55BCBF98C1F14D21F2F}.

SR - Demand [07/12/2019] [ 36152] WinMad Service (WinMad) . (.Mellanox.) - C:\WINDOWS\System32\drivers\winmad.sys =>.Microsoft®

SR - Demand [07/12/2019] [ 73016] WinVerbs Service (WinVerbs) . (.Mellanox.) - C:\WINDOWS\System32\drivers\winverbs.sys =>.Microsoft®

SR - Auto [05/09/2018] [ 4059744] Intel(R) PROSet/Wireless Zero Configuration Service (ZeroConfigService) . (.Intel® Corporation.) - C:\Program Files\Intel\WiFi\bin\ZeroConfigService.exe =>.Intel Corporation®

**---\ TÂCHES PLANIFIÉES EN AUTOMATIQUE (Registre) (32) - 10s**

O38 - TASK: {05D8DEA8-4317-4B47-99E5-5382F0F47407} [64Bits][\CCleaner Update] - (.Piriform Software Ltd - CCleaner emergency updater.) -- C:\Program Files\CCleaner\CCUpdate.exe [686384] =>.Piriform Software Ltd

O38 - TASK: {0851992B-69F2-42D5-8A7C-B4CED1C8FC44} [64Bits][\CCleaner Browser Heartbeat Task (Logon)] - (.Piriform Software - CCleaner Browser.) -- C:\Program Files (x86)\CCleaner Browser\Application\CCleanerBrowser.exe [1923568] =>.Piriform Software

O38 - TASK: {0E4DC4E9-4EA7-4B43-B2A9-93FE30C11BA4} [64Bits][\DropboxUpdateTaskMachineUA] - (.Dropbox, Inc. - Dropbox Update.) -- C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe [143144] =>.Dropbox, Inc.

O38 - TASK: {117C7B86-3B77-428F-A50D-470CC037ADC1} [64Bits][\NvProfileUpdaterDaily\_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation - NVIDIA driver profile updater.) -- C:\Program Files\NVIDIA Corporation\Update Core\NvProfileUpdater64.exe [897008] =>.NVIDIA Corporation

O38 - TASK: {153A3AA3-503A-433D-A0D1-F1746072FDEC} [64Bits][\GoogleUpdateTaskMachineUA] - (.Google LLC - Programme d'installation de Google.) -- C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [155432] =>.Google LLC

O38 - TASK: {2B27F546-1CB2-47A3-912A-B3DAE980CDF2} [64Bits][\GoogleUpdateTaskMachineCore] - (.Google LLC - Programme d'installation de Google.) -- C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [155432] =>.Google LLC

O38 - TASK: {5627C9B4-57B9-440C-9E24-1AD5AC15F221} [64Bits][\CCleaner Browser Heartbeat Task (Hourly)] - (.Piriform Software - CCleaner Browser.) -- C:\Program Files (x86)\CCleaner Browser\Application\CCleanerBrowser.exe [1923568] =>.Piriform Software

O38 - TASK: {6AB4767B-8F42-471B-87B1-2ADAFFD448B8} [64Bits][\CCleanerUpdateTaskMachineUA] - (.Piriform Software - CCleaner Browser.) -- C:\Program Files (x86)\CCleaner Browser\Update\CCleanerBrowserUpdate.exe [200928] =>.Piriform Software

O38 - TASK: {70F61A0B-B651-41EB-BE82-B21B0FD2FFA8} [64Bits][\DropboxUpdateTaskMachineCore] - (.Dropbox, Inc. - Dropbox Update.) -- C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe [143144] =>.Dropbox, Inc.

O38 - TASK: {8FFA5D62-825C-4E2C-AB9A-DD531A1E49FD} [64Bits][\PremeStartup] - (.Preme for Windows 2010-2018 - Preme for Windows.) -- C:\Users\ericl\AppData\Roaming\Preme for Windows\bin\preme.exe [3540992]

O38 - TASK: {AEA4476E-5AC4-44AF-ABCA-1A66457BE2B7} [64Bits][\NvProfileUpdaterOnLogon\_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation - NVIDIA driver profile updater.) -- C:\Program Files\NVIDIA Corporation\Update Core\NvProfileUpdater64.exe [897008] =>.NVIDIA Corporation

O38 - TASK: {C24228E4-8AA8-4CA4-B29C-997B3495B40D} [64Bits][\CCleanerSkipUAC] - (.Piriform Software Ltd - CCleaner.) -- C:\Program Files\CCleaner\CCleaner.exe [24770744] =>.Piriform Software Ltd

O38 - TASK: {D3BD7DF5-CD90-4B5C-85F6-F83A2B67C5BC} [64Bits][\CCleanerUpdateTaskMachineCore] - (.Piriform Software - CCleaner Browser.) -- C:\Program Files (x86)\CCleaner Browser\Update\CCleanerBrowserUpdate.exe [200928] =>.Piriform Software

O38 - TASK: {D6798F20-5925-4CBC-968E-0D3ACBC534E5} [64Bits][\PremeLogonStart] - (.Preme for Windows 2010-2018 - Preme for Windows.) -- C:\Users\ericl\AppData\Roaming\Preme for Windows\bin\preme.exe [3540992]

O38 - TASK: {D832A6AE-0EF8-4CFA-8223-551F6C4560AB} [64Bits][\Mozilla\Firefox Default Browser Agent 308046B0AF4A39CB] - (.Mozilla Foundation - Firefox Default Browser Agent.) -- C:\Program Files\Mozilla Firefox\default-browser-agent.exe [124112] =>.Mozilla Foundation

O38 - TASK: {DF3D9BF3-15A3-4DCE-8DCF-B66DDF282C5D} [64Bits][\Adobe Acrobat Update Task] - (.Adobe Inc. - Adobe Reader and Acrobat Manager.) -- C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe [1341008] =>.Adobe Inc.

C:\WINDOWS\System32\Tasks\CCleaner Update - (.Piriform Software Ltd.) -- C:\Program Files\CCleaner\CCUpdate.exe [] =>.Piriform Software Ltd

C:\WINDOWS\System32\Tasks\CCleaner Browser Heartbeat Task (Logon) - (.Piriform Software.) -- C:\Program Files (x86)\CCleaner Browser\Application\CCleanerBrowser.exe [--type=heartbeat --logon.--type=heartbeat] =>.Piriform Software

C:\WINDOWS\System32\Tasks\DropboxUpdateTaskMachineUA - (.Dropbox, Inc..) -- C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe [/ua ./ua] =>.Dropbox, Inc.

C:\WINDOWS\System32\Tasks\NvProfileUpdaterDaily\_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files\NVIDIA Corporation\Update Core\NvProfileUpdater64.exe [] =>.NVIDIA Corporation

C:\WINDOWS\System32\Tasks\GoogleUpdateTaskMachineUA - (.Google LLC.) -- C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [/ua ./ua] =>.Google LLC

C:\WINDOWS\System32\Tasks\GoogleUpdateTaskMachineCore - (.Google LLC.) -- C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [/c] =>.Google LLC

C:\WINDOWS\System32\Tasks\CCleaner Browser Heartbeat Task (Hourly) - (.Piriform Software.) -- C:\Program Files (x86)\CCleaner Browser\Application\CCleanerBrowser.exe [--type=heartbeat --hourly.--type=heartbeat] =>.Piriform Software

C:\WINDOWS\System32\Tasks\CCleanerUpdateTaskMachineUA - (.Piriform Software.) -- C:\Program Files (x86)\CCleaner Browser\Update\CCleanerBrowserUpdate.exe [/ua ./ua] =>.Piriform Software

C:\WINDOWS\System32\Tasks\DropboxUpdateTaskMachineCore - (.Dropbox, Inc..) -- C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe [/c] =>.Dropbox, Inc.

C:\WINDOWS\System32\Tasks\PremeStartup - (.Preme for Windows 2010-2018.) -- C:\Users\ericl\AppData\Roaming\Preme for Windows\bin\preme.exe [startup]

C:\WINDOWS\System32\Tasks\NvProfileUpdaterOnLogon\_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files\NVIDIA Corporation\Update Core\NvProfileUpdater64.exe [] =>.NVIDIA Corporation

C:\WINDOWS\System32\Tasks\CCleanerSkipUAC - (.Piriform Software Ltd.) -- C:\Program Files\CCleaner\CCleaner.exe [$(Arg0)] =>.Piriform Software Ltd

C:\WINDOWS\System32\Tasks\CCleanerUpdateTaskMachineCore - (.Piriform Software.) -- C:\Program Files (x86)\CCleaner Browser\Update\CCleanerBrowserUpdate.exe [/c] =>.Piriform Software

C:\WINDOWS\System32\Tasks\PremeLogonStart - (.Preme for Windows 2010-2018.) -- C:\Users\ericl\AppData\Roaming\Preme for Windows\bin\preme.exe [logon]

C:\WINDOWS\System32\Tasks\Mozilla\Firefox Default Browser Agent 308046B0AF4A39CB - (.Mozilla Foundation.) -- C:\Program Files\Mozilla Firefox\default-browser-agent.exe [do-task] =>.Mozilla Foundation

C:\WINDOWS\System32\Tasks\Adobe Acrobat Update Task - (.Adobe Inc..) -- C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe [] =>.Adobe Inc.

**---\ APPLICATIONS LANCÉES AU DÉMARRAGE DU SYSTÈME (17) - 2s**

O4 - HKLM\..\Run: [SecurityHealth] . (.Microsoft Corporation - Windows Security notification icon.) -- C:\WINDOWS\system32\SecurityHealthSystray.exe [Unsigned] =>.Microsoft Corporation

O4 - HKLM\..\Run: [RtkAudUService] . (.Realtek Semiconductor - Realtek HD Audio Universal Service.) -- C:\Windows\System32\RtkAudUService64.exe [Unsigned] =>.Realtek Semiconductor

O4 - HKCU\..\Run: [Google Update] . (. - .) -- C:\Users\ericl\AppData\Local\Google\Update\1.3.35.452\GoogleUpdateCore.exe (.Not File.) =>.SUP.Orphan

O4 - HKCU\..\Run: [CCleaner Smart Cleaning] . (.Piriform Software Ltd - CCleaner.) -- C:\Program Files\CCleaner\CCleaner64.exe =>.Piriform Software Ltd®

O4 - HKCU\..\Run: [GoogleDriveSync] . (...) -- C:\Program Files\Google\Drive\googledrivesync.exe =>.Google LLC®

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

O4 - HKCU\..\Run: [com.squirrel.Teams.Teams] . (. - .) -- Teams.exe =>.SUP.Orphan

O4 - HKCU\..\Run: [CCleanerBrowserAutoLaunch\_593A14077FF47768888263630D5AFAFE] . (.Piriform Software - CCleaner Browser.) -- C:\Program Files (x86)\CCleaner Browser\Application\CCleanerBrowser.exe =>.Piriform Software Ltd®

O4 - HKUS\S-1-5-19\..\Run: [OneDriveSetup] . (.Microsoft Corporation - Microsoft OneDrive (32 bit) Setup.) -- C:\Windows\SysWOW64\OneDriveSetup.exe =>.Microsoft Corporation®

O4 - HKUS\S-1-5-20\..\Run: [OneDriveSetup] . (.Microsoft Corporation - Microsoft OneDrive (32 bit) Setup.) -- C:\Windows\SysWOW64\OneDriveSetup.exe =>.Microsoft Corporation®

O4 - HKLM\..\Wow6432Node\Run: [Dropbox] . (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe =>.Dropbox, Inc®

O4 - HKUS\S-1-5-21-4226646855-4164925663-2316759709-1001\..\Run: [Google Update] . (. - .) -- C:\Users\ericl\AppData\Local\Google\Update\1.3.35.452\GoogleUpdateCore.exe (.Not File.) =>.SUP.Orphan

O4 - HKUS\S-1-5-21-4226646855-4164925663-2316759709-1001\..\Run: [CCleaner Smart Cleaning] . (.Piriform Software Ltd - CCleaner.) -- C:\Program Files\CCleaner\CCleaner64.exe =>.Piriform Software Ltd®

O4 - HKUS\S-1-5-21-4226646855-4164925663-2316759709-1001\..\Run: [GoogleDriveSync] . (...) -- C:\Program Files\Google\Drive\googledrivesync.exe =>.Google LLC®

O4 - HKUS\S-1-5-21-4226646855-4164925663-2316759709-1001\..\Run: [OneDrive] . (.Microsoft Corporation - Microsoft OneDrive.) -- C:\Users\ericl\AppData\Local\Microsoft\OneDrive\OneDrive.exe =>.Microsoft®

O4 - HKUS\S-1-5-21-4226646855-4164925663-2316759709-1001\..\Run: [com.squirrel.Teams.Teams] . (. - .) -- Teams.exe =>.SUP.Orphan

O4 - HKUS\S-1-5-21-4226646855-4164925663-2316759709-1001\..\Run: [CCleanerBrowserAutoLaunch\_593A14077FF47768888263630D5AFAFE] . (.Piriform Software - CCleaner Browser.) -- C:\Program Files (x86)\CCleaner Browser\Application\CCleanerBrowser.exe =>.Piriform Software Ltd®

**---\ PROCESSUS LANCÉS (71) - 13s**

[MD5.476243292AC9B2DD1A2044400A6386F3] - (.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporation\Display.NvContainer\NVDisplay.Container.exe [767472] [PID.2352] =>.NVIDIA Corporation®

[MD5.DF69688686D17D25044ADDC061C27B5F] - (.Intel Corporation - igfxCUIService Module.) -- C:\Windows\System32\DriverStore\FileRepository\igdlh64.inf\_amd64\_c8634ed19e331cda\igfxCUIService.exe [413072] [PID.2980] =>.Intel(R) pGFX®

[MD5.F70A099BC16564F178EDA982377911D5] - (.Intel(R) Corporation - Intel(R) PROSet/Wireless Event Log Service.) -- C:\Program Files\Intel\WiFi\bin\EvtEng.exe [670816] [PID.4832] =>.Intel Corporation®

[MD5.D1FDE804C6572A4ABB5B2F2D61C7FD1A] - (...) -- C:\WINDOWS\system32\dolbyaposvc\DAX3API.exe [598384] [PID.4840] [Unsigned]

[MD5.4030FC99EFAEB625E3F49E7A3C356D14] - (.Fortemedia - Fortemedia Service.) -- C:\Windows\System32\FMService64.exe [306040] [PID.4880] [Unsigned] =>.Fortemedia

[MD5.6F1E5A6AA57F61A2C183A21B291E816D] - (.Intel Corporation - Intel(R) Dynamic Platform and Thermal Frame.) -- C:\WINDOWS\System32\Intel\DPTF\esif\_uf.exe [1705040] [PID.4892] [Unsigned] =>.Intel Corporation

[MD5.6041CCF17D2135D00AE1498107A120EF] - (...) -- C:\Program Files\Huawei\PCManager\MateBookService.exe [1034224] [PID.4900] {6E715E33F17AD55BCBF98C1F14D21F2F}.

[MD5.3F14F133D67231858F3CB3D08762FD42] - (...) -- C:\Windows\System32\drivers\SessionService.exe [30208] [PID.4916] [Unsigned]

[MD5.9277639E4F62E669B08CF3D93FBB6466] - (.Microsoft - LCD\_Service.) -- C:\Program Files\Huawei\HwLcdEnhancement\LCD\_Service.exe [24560] [PID.4940] {6E715E33F17AD55BCBF98C1F14D21F2F}. =>.Microsoft

[MD5.1808E670349B5F45507252715A8728C7] - (.Realtek Semiconductor - Realtek HD Audio Universal Service.) -- C:\WINDOWS\System32\RtkAudUService64.exe [838432] [PID.4948] [Unsigned] =>.Realtek Semiconductor

[MD5.0402ED31C7EF3D5A5BAA110AC3A141D8] - (.Intel(R) Corporation - Intel(R) PROSet/Wireless Registry Service.) -- C:\Program Files\Common Files\Intel\WirelessCommon\RegSrvc.exe [170592] [PID.4964] =>.Intel Corporation®

[MD5.4B68A6743C425EB861C5FEAB6C619B5E] - (...) -- C:\Program Files\Huawei\HwOsd\OSDMainService.exe [665928] [PID.4980] {6E715E33F17AD55BCBF98C1F14D21F2F}.

[MD5.B341929154B45976000166F5F5F48E48] - (.Intel Corporation - Intel HD Graphics Drivers for Windows(R).) -- C:\Windows\System32\DriverStore\FileRepository\igdlh64.inf\_amd64\_c8634ed19e331cda\IntelCpHDCPSvc.exe [505120] [PID.4996] =>.Intel(R) pGFX®

[MD5.E8FFA4ABF3BF3C283A88F0D0E48F572B] - (.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporation\NvTelemetry\NvTelemetryContainer.exe [782136] [PID.5016] =>.NVIDIA Corporation®

[MD5.86DAAF947ED2B8E5C4CCA9749FE25522] - (.Intel® Corporation - Intel® PROSet/Wireless Zero Configure Servi.) -- C:\Program Files\Intel\WiFi\bin\ZeroConfigService.exe [4059744] [PID.5104] =>.Intel Corporation®

[MD5.649EE3A755A5B5AB7E31A4F4FC5C11CE] - (.Intel Corporation - IntelCpHeciSvc Executable.) -- C:\Windows\System32\DriverStore\FileRepository\igdlh64.inf\_amd64\_c8634ed19e331cda\IntelCpHeciSvc.exe [510240] [PID.6136] =>.Intel(R) pGFX®

[MD5.A1F58FFF448E4099297D6EE0641D4D0E] - (.Dropbox, Inc. - Dropbox Update.) -- C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe [143144] [PID.9736] =>.Dropbox, Inc®

[MD5.74CDA8051136B80DC3AE4BF86623003C] - (.Google LLC - Google Crash Handler.) -- C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleCrashHandler.exe [295368] [PID.10896] =>.Google LLC®

[MD5.C92C82D8EF9689330621CA9D79D59ACC] - (.Google LLC - Google Crash Handler.) -- C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleCrashHandler64.exe [376264] [PID.10980] =>.Google LLC®

[MD5.6C034FEB840B8E89C885914C23C9CDEF] - (.Piriform Software - CCleaner Browser Crash Handler.) -- C:\Program Files (x86)\CCleaner Browser\Update\1.8.1067.0\CCleanerBrowserCrashHandler.exe [481360] [PID.11016] =>.Piriform Software Ltd®

[MD5.1FF02EF3D1F76B2825C0201EC8BE6574] - (.Piriform Software - CCleaner Browser Crash Handler.) -- C:\Program Files (x86)\CCleaner Browser\Update\1.8.1067.0\CCleanerBrowserCrashHandler64.exe [623016] [PID.11004] =>.Piriform Software Ltd®

[MD5.151765EAE96274E46995B3DDD1C7DFDC] - (.Intel Corporation - Intel® SGX Application Enclave Services Man.) -- C:\Windows\System32\DriverStore\FileRepository\sgx\_psw.inf\_amd64\_1781f8bae8fdf5c0\aesm\_service.exe [3226664] [PID.2872] =>.Intel(R) pGFX®

[MD5.1ED5A59A7A4A0182FD77F1FDABB8F296] - (.Intel Corporation - Intel(R) Dynamic Application Loader Host In.) -- C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\DAL\jhi\_service.exe [205968] [PID.3020] =>.Intel(R) Embedded Subsystems and IP Blocks Group®

[MD5.1ED6E48252C137E23674AE8FBBE75882] - (.Intel Corporation - Intel(R) Local Management Service.) -- C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe [419984] [PID.13728] =>.Intel(R) Embedded Subsystems and IP Blocks Group®

[MD5.255146C1AB4DCBE753F1240A0C2FAAEE] - (.Dropbox, Inc. - Dropbox Service.) -- C:\Windows\System32\DbxSvc.exe [44552] [PID.1664] [Unsigned] =>.Dropbox, Inc.

[MD5.476243292AC9B2DD1A2044400A6386F3] - (.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporation\Display.NvContainer\NVDisplay.Container.exe [767472] [PID.10644] =>.NVIDIA Corporation®

[MD5.D1FDE804C6572A4ABB5B2F2D61C7FD1A] - (...) -- C:\Windows\System32\dolbyaposvc\DAX3API.exe [598384] [PID.3876] [Unsigned]

[MD5.54A84680391D69D5CF610A03375412AD] - (.Intel Corporation - Intel(R) Dynamic Platform and Thermal Frame.) -- C:\Windows\System32\Intel\DPTF\dptf\_helper.exe [585808] [PID.18008] [Unsigned] =>.Intel Corporation

[MD5.1808E670349B5F45507252715A8728C7] - (.Realtek Semiconductor - Realtek HD Audio Universal Service.) -- C:\WINDOWS\System32\RtkAudUService64.exe [838432] [PID.18296] [Unsigned] =>.Realtek Semiconductor

[MD5.7E437E0435D10EEB918AF48FADEAAF35] - (.Malwarebytes - Malwarebytes Tray Application.) -- C:\Program Files\Malwarebytes\Anti-Malware\mbamtray.exe [5897664] [PID.1620] =>.Malwarebytes Inc®

[MD5.AAED174DEEA5E92DCB486AFC98C0BB0B] - (.Intel Corporation - igfxEM Module.) -- C:\Windows\System32\DriverStore\FileRepository\igdlh64.inf\_amd64\_c8634ed19e331cda\igfxEM.exe [1024800] [PID.18516] =>.Intel(R) pGFX®

[MD5.1A22F5A210423A8BDDBC16102BD49E5D] - (...) -- C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost\_cw5n1h2txyewy\StartMenuExperienceHost.exe [789816] [PID.23148] =>.Microsoft®

[MD5.1808E670349B5F45507252715A8728C7] - (.Realtek Semiconductor - Realtek HD Audio Universal Service.) -- C:\Windows\System32\RtkAudUService64.exe [838432] [PID.19280] [Unsigned] =>.Realtek Semiconductor

[MD5.7DFCCC67990B6DE7F30F553A4E4612A4] - (...) -- C:\Program Files (x86)\RocketDock\RocketDock.exe [495616] [PID.19744] [Unsigned]

[MD5.8B86CFBDD8AA0FCA798090E78677BB16] - (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe [7807488] [PID.19004] =>.Dropbox, Inc®

[MD5.8B86CFBDD8AA0FCA798090E78677BB16] - (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe [7807488] [PID.19388] =>.Dropbox, Inc®

[MD5.8B86CFBDD8AA0FCA798090E78677BB16] - (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe [7807488] [PID.5284] =>.Dropbox, Inc®

[MD5.43E8E6963F42F534C79EF326A949D9F0] - (.The Qt Company Ltd. - Qt Qtwebengineprocess.) -- C:\Program Files (x86)\Dropbox\Client\106.4.368\QtWebEngineProcess.exe [407552] [PID.23404] =>.Dropbox, Inc®

[MD5.43E8E6963F42F534C79EF326A949D9F0] - (.The Qt Company Ltd. - Qt Qtwebengineprocess.) -- C:\Program Files (x86)\Dropbox\Client\106.4.368\QtWebEngineProcess.exe [407552] [PID.5196] =>.Dropbox, Inc®

[MD5.43E8E6963F42F534C79EF326A949D9F0] - (.The Qt Company Ltd. - Qt Qtwebengineprocess.) -- C:\Program Files (x86)\Dropbox\Client\106.4.368\QtWebEngineProcess.exe [407552] [PID.11844] =>.Dropbox, Inc®

[MD5.76E4BE50B2917EA57B62C35344E89E39] - (.Adobe Inc. - Adobe Acrobat Update Service.) -- C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe [169544] [PID.9440] =>.Adobe Inc.®

[MD5.F1477C79D661595A7F9AF3AD85FD7BF2] - (...) -- C:\Program Files\Google\Drive\googledrivesync.exe [48737752] [PID.17792] =>.Google LLC®

[MD5.F1477C79D661595A7F9AF3AD85FD7BF2] - (...) -- C:\Program Files\Google\Drive\googledrivesync.exe [48737752] [PID.14684] =>.Google LLC®

[MD5.7AA4F5416B41A6DFDCAC9D69933A1653] - (...) -- C:\Program Files\WindowsApps\Microsoft.Windows.Photos\_2020.20090.1002.0\_x64\_\_8wekyb3d8bbwe\Microsoft.Photos.exe [484352] [PID.23180] [Unsigned] =>.Microsoft Corporation

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.17128] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.10152] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.14192] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.8028] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.18104] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.7568] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.1028] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.17024] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.3732] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.7440] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.22940] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.8908] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.20768] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.19452] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.18028] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.12984] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.2060] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.18192] =>.Google LLC®

[MD5.29E957AA62506989918E7D660C5A2275] - (...) -- C:\Program Files\Huawei\HwOsd\OSDListener.exe [859464] [PID.2480] {6E715E33F17AD55BCBF98C1F14D21F2F}.

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.3736] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.11088] =>.Google LLC®

[MD5.8A99011C04241E43F6000E1E0718E780] - (.Preme for Windows 2010-2018 - Preme for Windows.) -- C:\Users\ericl\AppData\Roaming\Preme for Windows\bin\premeeng.exe [3540992] [PID.3616] [Unsigned]

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.21664] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.5812] =>.Google LLC®

[MD5.600285F800CC79F078CA66270D4C216B] - (.Nicolas Coolman - ZHPDiag.) -- D:\ToolBox PC\ZHPDiag3.exe [3272064] [PID.1464] [Unsigned] =>.Nicolas Coolman

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.13992] =>.Google LLC®

[MD5.C139654B5C1438A95B321BB01AD63EF6] - (.Google LLC - Google Chrome.) -- C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe [2150896] [PID.11556] =>.Google LLC®

**---\ CHROME, Démarrage, Recherche, Extensions (28) - 1s**

G2 - GCE: Preference [ericl][User Data\Default\Extensions] [aghfnjkcakhmadgdomlmlhhaocbkloab] Just Black =>.Legitimate

G2 - GCE: Preference [ericl][User Data\Default\Extensions] [bbpjcfkgapecndkanjcojnldopjlnmjk] Whereby

G2 - GCE: Preference [ericl][User Data\Default\Extensions] [blpcfgokakmgnkcojhhkbfbldkacnbeo] http://www.youtube.com =>.Youtube {Youtube}

G2 - GCE: Preference [ericl][User Data\Default\Extensions] [cfhdojbkjhnklbpkdaibdccddilifddb] eyeo GmbH =>.Eyeo GmbH

G2 - GCE: Preference [ericl][User Data\Default\Extensions] [efaidnbmnnnibpcajpcglclefindmkaj] =>.Adobe Inc. {Acrobat}

G2 - GCE: Preference [ericl][User Data\Default\Extensions] [elicpjhcidhpjomhibiffojpinpmmpil] Video Downloader professional =>.startpage24.com

G2 - GCE: Preference [ericl][User Data\Default\Extensions] [gojbdfnpnhogfdgjbigejoaolejmgdhk] Clip to OneNote =>.onenote.com

G2 - GCE: Preference [ericl][User Data\Default\Extensions] [himomacamcpodhkahelbnmaddladgjgo] http://google.gantter.com/

G2 - GCE: Preference [ericl][User Data\Default\Extensions] [hmjkmjkepdijhoojdojkdfohbdgmmhki] =>.Google Inc. {Keep}

G2 - GCE: Preference [ericl][User Data\Default\Extensions] [kfokdmfpdnokpmpbjhjbcabgligoelgp] Open Chrome Audio Capture interface

G2 - GCE: Preference [ericl][User Data\Default\Extensions] [lmjegmlicamnimmfhcmpkclmigmmcbeh] Application Launcher for Drive (by Google) =>.Google Inc.

G2 - GCE: Preference [ericl][User Data\Default\Extensions] [lpcaedmchfhocbbapmcbpinfpgnhiddi] Google Keep Chrome Extension =>.Google Inc.

G2 - GCE: Preference [ericl][User Data\Default\Extensions] [nmmhkkegccagdldgiimedpiccmgmieda] =>.Google Inc. {Wallet}

G2 - GCE: Preference [ericl][User Data\Default\Extensions] [pjkljhegncpnkpknbcohdijeoejaedia] http://mail.google.com/ =>.Google Inc. {Gmail}

G2 - GCE: Preference [ericl][User Data\Default\Extensions] [pkedcjkdefgpdelpbcmbmeomcjbeemfm] Chrome Media Router =>.Google Inc.

G2 - GCE: Preference [ericl][User Data\Default\Local Extension Settings] [bbpjcfkgapecndkanjcojnldopjlnmjk]

G2 - GCE: Preference [ericl][User Data\Default\Local Extension Settings] [cfhdojbkjhnklbpkdaibdccddilifddb] =>.eyeo GmbH {AdBlock Plus}

G2 - GCE: Preference [ericl][User Data\Default\Local Extension Settings] [elicpjhcidhpjomhibiffojpinpmmpil] =>.Video Downloader

G2 - GCE: Preference [ericl][User Data\Default\Local Extension Settings] [ghbmnnjooekpmoecnnnilnnbdlolhkhi] =>.Google Inc. {Docs hors connexion}

G2 - GCE: Preference [ericl][User Data\Default\Local Extension Settings] [lpcaedmchfhocbbapmcbpinfpgnhiddi]

G2 - GCE: Preference [ericl][User Data\Default\Local App Settings] [gbchcmhmhahfdphkhkmpfmihenigjmpp] =>.Google Inc. {Bureau à distance}

G2 - GCE: Preference [ericl][User Data\Default\Managed Extension Settings] [cfhdojbkjhnklbpkdaibdccddilifddb] =>.eyeo GmbH {AdBlock Plus}

G2 - GCE: Preference [ericl][User Data\Default\Sync Extension Settings] [dbkchnicaiglcjpgbmpfmoafckkomdcm]

G2 - GCE: Preference [ericl][User Data\Default\Sync Extension Settings] [elicpjhcidhpjomhibiffojpinpmmpil] =>.Video Downloader

G2 - GCE: Preference [ericl][User Data\Default\Sync Extension Settings] [fdpohaocaechififmbbbbbknoalclacl]

G2 - GCE: Preference [ericl][User Data\Default\Sync Extension Settings] [gmlllbghnfkpflemihljekbapjopfjik] =>.Bookmark Manager

G2 - GCE: Preference [ericl][User Data\Default\Sync Extension Settings] [kfokdmfpdnokpmpbjhjbcabgligoelgp]

G2 - GCE: Preference [ericl][User Data\Default\Sync Extension Settings] [pkedcjkdefgpdelpbcmbmeomcjbeemfm] =>.Google Inc. {Chrome Media Router}

**---\ FIREFOX, Plugins,Démarrage,Recherche,Extensions (25) - 3s**

P2 - EXT FILE: (.Avast Software s.r.o.) -- C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\extensions\wrc@avast.com.xpi [Unsigned] =>.Avast Software s.r.o

P2 - EXT FILE: (.Video DownloadHelper - Download Videos from the Web.) -- C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\extensions\{b9db16a4-6edc-47ec-a1f4-b86292ed211d}.xpi [Unsigned] =>.Video DownloadHelper

P2 - EXT FILE: (.Legitimate.) -- C:\Program Files\Mozilla Firefox\browser\features\doh-rollout@mozilla.org.xpi [Unsigned]

P2 - EXT FILE: (.Mozilla Corporation.) -- C:\Program Files\Mozilla Firefox\browser\features\formautofill@mozilla.org.xpi [Unsigned] =>.Mozilla Corporation

P2 - EXT FILE: (.Mozilla Corporation.) -- C:\Program Files\Mozilla Firefox\browser\features\screenshots@mozilla.org.xpi [Unsigned] =>.Mozilla Corporation

P2 - EXT FILE: (.webcompat.com.) -- C:\Program Files\Mozilla Firefox\browser\features\webcompat-reporter@mozilla.org.xpi [Unsigned] =>.webcompat.com

P2 - EXT FILE: (.webcompat.com.) -- C:\Program Files\Mozilla Firefox\browser\features\webcompat@mozilla.org.xpi [Unsigned] =>.webcompat.com

C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\bookmarkbackups =>Mozilla Corporation

C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\browser-extension-data =>Mozilla Corporation

C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\crashes =>Mozilla Corporation

C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\datareporting =>Mozilla Corporation

C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\extensions =>Mozilla Corporation

C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\features =>Mozilla Corporation

C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\gmp =>Mozilla Corporation

C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\gmp-gmpopenh264 =>Mozilla Corporation

C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\gmp-widevinecdm =>Mozilla Corporation

C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\mediacapabilities =>Legitimate

C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\minidumps =>Mozilla Corporation

C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\saved-telemetry-pings =>Mozilla Corporation

C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\security\_state =>Mozilla Corporation

C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\sessionstore-backups =>Mozilla Corporation

C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\storage =>Mozilla Corporation

C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\weave =>Mozilla Corporation

C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\browser-extension-data\doh-rollout@mozilla.org =>Legitimate

C:\Users\ericl\AppData\Roaming\Mozilla\Firefox\Profiles\olaaqvm5.default\browser-extension-data\etp-search-volume-study@shield.mozilla.org =>Hotspot

**---\ INTERNET EXPLORER,Démarrage,Recherche,URLSearchHook (16) - 0s**

R0 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = http://www.google.fr =>.Google Inc.

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://oem17win10.msn.com/ =>.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

R3 - URLSearchHook: (no name)[HKCU] - {CFBFAE00-17A6-11D0-99CB-00C04FD64497} . (.Microsoft Corporation - Navigateur Internet.) (11.00.19041.507 (WinBuild.160101.0800)) -- C:\Windows\System32\ieframe.dll =>.Microsoft Corporation

**---\ INTERNET EXPLORER, Site de confiance et site sensible (2) - 0s**

~ Microsoft Internet Explorer Restricted Site(s) Domains: 0(Good) / 0(Bad)

~ Microsoft Internet Explorer Restricted Site(s) EscDomains: 0(Good) / 0(Bad)

**---\ MICROSOFT EDGE, Plugin,Favoris,Démarrage,Recherche,Extension (15) - 1s**

E2 - GCE: Preference [ericl][User Data\Default\Extensions] [bbpjcfkgapecndkanjcojnldopjlnmjk] Whereby

E2 - GCE: Preference [ericl][User Data\Default\Extensions] [fnmpfimijcopbiaiobinamadmnmhckmp] Browserkit

E2 - GCE: Preference [ericl][User Data\Default\Extensions] [gggmmkjegpiggikcnhidnjjhmicpibll] Microsoft Corporation =>.Microsoft Corporation

E2 - GCE: Preference [ericl][User Data\Default\Extensions] [gmgoamodcdcjnbaobigkjelfplakmdhh] eyeo GmbH =>.Eyeo GmbH

E2 - GCE: Preference [ericl][User Data\Default\Extensions] [kfokdmfpdnokpmpbjhjbcabgligoelgp] Open Chrome Audio Capture interface

E2 - GCE: Preference [ericl][User Data\Default\Extensions] [lpcaedmchfhocbbapmcbpinfpgnhiddi] Google Keep Chrome Extension =>.Google Inc.

E2 - GCE: Preference [ericl][User Data\Default\Extensions] [mbpnbnogejaolbhfpfgagldkeahefbhd] All Video Downloader professional

E2 - GCE: Preference [ericl][User Data\Default\Extensions] [oogbnpmeihfgnccdnmmlgicknopghhma] Clip to OneNote =>.onenote.com

E2 - GCE: Preference [ericl][User Data\Default\Local Extension Settings] [bbpjcfkgapecndkanjcojnldopjlnmjk]

E2 - GCE: Preference [ericl][User Data\Default\Local Extension Settings] [gmgoamodcdcjnbaobigkjelfplakmdhh]

E2 - GCE: Preference [ericl][User Data\Default\Local Extension Settings] [jdiccldimpdaibmpdkjnbmckianbfold] =>.Microsoft Corporation

E2 - GCE: Preference [ericl][User Data\Default\Local Extension Settings] [lpcaedmchfhocbbapmcbpinfpgnhiddi]

E2 - GCE: Preference [ericl][User Data\Default\Local Extension Settings] [mbpnbnogejaolbhfpfgagldkeahefbhd]

E2 - GCE: Preference [ericl][User Data\Default\Managed Extension Settings] [gmgoamodcdcjnbaobigkjelfplakmdhh]

E2 - GCE: Preference [ericl][User Data\Default\Sync Extension Settings] [mbpnbnogejaolbhfpfgagldkeahefbhd]

**---\ INTERNET EXPLORER,Proxy Management (3) - 0s**

R5 - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyEnable = 0 =>.Default.Value

R5 - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings,MigrateProxy = 1 =>.Default.Value

R5 - HKLM\SYSTEM\CurrentControlSet\services\NlaSvc\Parameters\Internet\ManualProxies [] =>.Microsoft

**---\ 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=

**---\ ÉTUDE DU FICHIER HOSTS (1) - 0s**

~ Le fichier hôte est sain (The hosts file is clean) (22)

**---\ BROWSER HELPER OBJECT DE NAVIGATEUR (BHO) (1) - 0s**

O2 - BHO: Lync Click to Call BHO [64Bits] - {31D09BA0-12F5-4CCE-BE8A-2923E76605DA} . (.Microsoft Corporation - Skype for Business.) -- C:\Program Files\Microsoft Office\root\Office16\OCHelper.dll =>.Microsoft®

**---\ RACCOURCIS GLOBAL STARTUP (55) - 4s**

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

O4 - GS\Quicklaunch [ericl]: CCleaner Browser.lnk . (.Piriform Software - CCleaner Browser.) C:\Program Files (x86)\CCleaner Browser\Application\CCleanerBrowser.exe --check-run=src=quicklaunch =>.Piriform Software Ltd®

O4 - GS\Quicklaunch [ericl]: Google Chrome.lnk . (.Google LLC - Google Chrome.) C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe =>.Google LLC®

O4 - GS\Quicklaunch [ericl]: Light Image Resizer 5.lnk . (.ObviousIdea SARL - Light Image Resizer.) C:\Program Files (x86)\ObviousIdea\Light Image Resizer 5\Resize.exe =>.ObviousIdea SARLU®

O4 - GS\Quicklaunch [ericl]: Microsoft Edge.lnk . (.Microsoft Corporation - Microsoft Edge.) C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe =>.Microsoft®

O4 - GS\Quicklaunch [ericl]: Microsoft Outlook.lnk . (.Microsoft Corporation - .) C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.EXE /recycle [Unsigned] =>.Microsoft Corporation

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

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

O4 - GS\sendTo [ericl]: PDFsam Basic.lnk . (.Sober Lemur S.a.s di Vacondio Andrea - .) C:\Program Files (x86)\PDFsam Basic\pdfsam.exe [Unsigned]

O4 - GS\sendTo [ericl]: Transfert de fichiers Bluetooth.LNK . (.Microsoft Corporation - Transfère les fichiers entre l.) C:\Windows\System32\fsquirt.exe [Unsigned] =>.Microsoft Corporation

O4 - GS\TaskBar [ericl]: Google Chrome.lnk . (.Google LLC - Google Chrome.) C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe =>.Google LLC®

O4 - GS\TaskBar [ericl]: Magnify.lnk . (.Microsoft Corporation - Loupe Microsoft.) C:\WINDOWS\system32\magnify.exe [Unsigned] =>.Microsoft Corporation

O4 - GS\TaskBar [ericl]: Microsoft Teams.lnk . (.Microsoft Corporation - Microsoft Teams.) C:\Users\ericl\AppData\Local\Microsoft\Teams\Update.exe --processStart 'Teams.exe' =>.Microsoft®

O4 - GS\TaskBar [ericl]: OneNote 2016.lnk . (.Microsoft Corporation - Prenez des notes et ayez-les s.) C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE [Unsigned] =>.Microsoft Corporation

O4 - GS\TaskBar [ericl]: Outlook.lnk . (.Microsoft Corporation - Manage your email, schedules, .) C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.EXE [Unsigned] =>.Microsoft Corporation

O4 - GS\TaskBar [ericl]: Skype for Business.lnk . (.Microsoft Corporation - Connect with people everywhere.) C:\Program Files (x86)\Microsoft Office\root\Office16\lync.exe [Unsigned] =>.Microsoft Corporation

O4 - GS\Startup [ericl]: Envoyer à OneNote.lnk . (.Microsoft Corporation - Envoyer à OneNote.) C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTEM.EXE /tsr [Unsigned] =>.Microsoft Corporation

O4 - GS\Programs [ericl]: Google Chrome.lnk . (.Google LLC - Google Chrome.) C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe =>.Google LLC®

O4 - GS\Programs [ericl]: Microsoft Teams.lnk . (.Microsoft Corporation - Microsoft Teams.) C:\Users\ericl\AppData\Local\Microsoft\Teams\Update.exe --processStart 'Teams.exe' =>.Microsoft®

O4 - GS\Programs [ericl]: OneDrive (1).lnk . (.Microsoft Corporation - Microsoft OneDrive.) C:\Users\ericl\AppData\Local\Microsoft\OneDrive\OneDrive.exe =>.Microsoft®

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

O4 - GS\Programs [ericl]: Start Tor Browser.lnk . (...) D:\OneDrive\Bureau\Tor Browser\Browser\firefox.exe [Unsigned]

O4 - GS\Programs [Public]: Google Chrome.lnk . (.Google LLC - Google Chrome.) C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe =>.Google LLC®

O4 - GS\Programs [Public]: Microsoft Teams.lnk . (.Microsoft Corporation - Microsoft Teams.) C:\Users\ericl\AppData\Local\Microsoft\Teams\Update.exe --processStart 'Teams.exe' =>.Microsoft®

O4 - GS\Programs [Public]: OneDrive (1).lnk . (.Microsoft Corporation - Microsoft OneDrive.) C:\Users\ericl\AppData\Local\Microsoft\OneDrive\OneDrive.exe =>.Microsoft®

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

O4 - GS\Programs [Public]: Start Tor Browser.lnk . (...) D:\OneDrive\Bureau\Tor Browser\Browser\firefox.exe [Unsigned]

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

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

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

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

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

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

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

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

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

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

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

O4 - GS\ProgramsCommon [Public]: Access.lnk . (.Microsoft Corporation - Build a professional app quick.) C:\Program Files (x86)\Microsoft Office\root\Office16\MSACCESS.EXE [Unsigned] =>.Microsoft Corporation

O4 - GS\ProgramsCommon [Public]: Acrobat Reader DC.lnk . (.Adobe Systems Incorporated - Adobe Acrobat Reader DC.) C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe =>.Adobe Inc.®

O4 - GS\ProgramsCommon [Public]: CCleaner Browser.lnk . (.Piriform Software - CCleaner Browser.) C:\Program Files (x86)\CCleaner Browser\Application\CCleanerBrowser.exe --check-run=src=tile =>.Piriform Software Ltd®

O4 - GS\ProgramsCommon [Public]: Excel.lnk . (.Microsoft Corporation - Easily discover, visualize, an.) C:\Program Files (x86)\Microsoft Office\root\Office16\EXCEL.EXE [Unsigned] =>.Microsoft Corporation

O4 - GS\ProgramsCommon [Public]: Firefox.lnk . (.Mozilla Corporation - Firefox.) C:\Program Files\Mozilla Firefox\firefox.exe =>.Mozilla Corporation®

O4 - GS\ProgramsCommon [Public]: GIMP 2.lnk . (.Spencer Kimball, Peter Mattis and the GIMP Developmen - GNU Image Manipulation Program.) C:\Program Files\GIMP 2\bin\gimp-2.8.exe =>.Jernej Simončič®

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

O4 - GS\ProgramsCommon [Public]: Malwarebytes.lnk . (.Malwarebytes - .) C:\Program Files (x86)\Malwarebytes\Anti-Malware\mbam.exe [Unsigned] =>.Malwarebytes

O4 - GS\ProgramsCommon [Public]: Microsoft Edge.lnk . (.Microsoft Corporation - Microsoft Edge.) C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe =>.Microsoft®

O4 - GS\ProgramsCommon [Public]: OneNote.lnk . (.Microsoft Corporation - Take notes and have them when .) C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE [Unsigned] =>.Microsoft Corporation

O4 - GS\ProgramsCommon [Public]: Outlook.lnk . (.Microsoft Corporation - Manage your email, schedules, .) C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.EXE [Unsigned] =>.Microsoft Corporation

O4 - GS\ProgramsCommon [Public]: PowerPoint.lnk . (.Microsoft Corporation - Design and deliver beautiful p.) C:\Program Files (x86)\Microsoft Office\root\Office16\POWERPNT.EXE [Unsigned] =>.Microsoft Corporation

O4 - GS\ProgramsCommon [Public]: Publisher.lnk . (.Microsoft Corporation - Create professional-grade publ.) C:\Program Files (x86)\Microsoft Office\root\Office16\MSPUB.EXE [Unsigned] =>.Microsoft Corporation

O4 - GS\ProgramsCommon [Public]: Skype for Business.lnk . (.Microsoft Corporation - Connect with people everywhere.) C:\Program Files (x86)\Microsoft Office\root\Office16\lync.exe [Unsigned] =>.Microsoft Corporation

O4 - GS\ProgramsCommon [Public]: SyncToy 2.1(x64).lnk . (...) C:\WINDOWS\Installer\{88DAAF05-5A72-46D2-A7C5-C3759697E943}\\_6FEFF9B68218417F98F549.exe [Unsigned]

O4 - GS\ProgramsCommon [Public]: Word.lnk . (.Microsoft Corporation - Create beautiful documents, ea.) C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE [Unsigned] =>.Microsoft Corporation

**---\ MODIFICATION DOMAINE/ADRESSES (DNS) (8) - 0s**

O17 - HKLM\System\CCS\Services\Tcpip\Parameters: DhcpDomain = lan =>.Local Domain

O17 - HKLM\System\CCS\Services\Tcpip\Parameters: DhcpNameServer = 192.168.1.254 =>.Local IP Adress

O17 - HKLM\System\CCS\Services\Tcpip\..\{3ed21092-3fa8-410c-9ea0-67b69f7e5f71}: DhcpNameServer = 172.16.50.12 172.16.50.14 =>.Hewlett-Packard

O17 - HKLM\System\CCS\Services\Tcpip\..\{b1281357-433b-444a-b452-f7ec5baff419}: DhcpNameServer = 192.168.1.254 =>.Local IP Adress

O17 - HKLM\System\CCS\Services\Tcpip\..\{b8eb653f-66db-4980-8345-52ce392591f7}: DhcpNameServer = 10.31.0.4 =>.Private IP (10.0.0.0 - 10.255.255.255) =>.Private IP

O17 - HKLM\System\CCS\Services\Tcpip\..\{e7d4985d-6423-4b29-b0b4-4b866862a6e8}: DhcpNameServer = 192.168.1.254 =>.Local IP Adress

O17 - HKLM\System\CCS\Services\Tcpip\..\{b8eb653f-66db-4980-8345-52ce392591f7}: DhcpDomain = clients.t31.sncf

O17 - HKLM\System\CCS\Services\Tcpip\..\{e7d4985d-6423-4b29-b0b4-4b866862a6e8}: DhcpDomain = lan =>.Local Domain

**---\ PROTOCOLE ADDITIONNEL (27) - 2s**

O18 - Handler: about [64Bits] - {3050F406-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Visionneuse HTML Microsoft (R).) -- C:\Windows\System32\mshtml.dll [Unsigned] =>.Microsoft Corporation

O18 - Handler: cdl [64Bits] - {3dd53d40-7b8b-11D0-b013-00aa0059ce02} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\System32\urlmon.dll [Unsigned] =>.Microsoft Corporation

O18 - Handler: dvd [64Bits] - {12D51199-0DB5-46FE-A120-47A3D7D937CC} . (.Microsoft Corporation - Contrôle ActiveX pour le flux vidéo.) -- C:\Windows\System32\MSVidCtl.dll [Unsigned] =>.Microsoft Corporation

O18 - Handler: file [64Bits] - {79eac9e7-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\System32\urlmon.dll [Unsigned] =>.Microsoft Corporation

O18 - Handler: ftp [64Bits] - {79eac9e3-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\System32\urlmon.dll [Unsigned] =>.Microsoft Corporation

O18 - Handler: http [64Bits] - {79eac9e2-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\System32\urlmon.dll [Unsigned] =>.Microsoft Corporation

O18 - Handler: https [64Bits] - {79eac9e5-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\System32\urlmon.dll [Unsigned] =>.Microsoft Corporation

O18 - Handler: its [64Bits] - {9D148291-B9C8-11D0-A4CC-0000F80149F6} . (.Microsoft Corporation - Microsoft® InfoTech Storage System Library.) -- C:\Windows\System32\itss.dll [Unsigned] =>.Microsoft Corporation

O18 - Handler: javascript [64Bits] - {3050F3B2-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Visionneuse HTML Microsoft (R).) -- C:\Windows\System32\mshtml.dll [Unsigned] =>.Microsoft Corporation

O18 - Handler: local [64Bits] - {79eac9e7-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\System32\urlmon.dll [Unsigned] =>.Microsoft Corporation

O18 - Handler: mailto [64Bits] - {3050f3DA-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Visionneuse HTML Microsoft (R).) -- C:\Windows\System32\mshtml.dll [Unsigned] =>.Microsoft Corporation

O18 - Handler: mhtml [64Bits] - {05300401-BCBC-11d0-85E3-00C04FD85AB4} . (.Microsoft Corporation - Microsoft Internet Messaging API Resources.) -- C:\Windows\System32\inetcomm.dll [Unsigned] =>.Microsoft Corporation

O18 - Handler: mk [64Bits] - {79eac9e6-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\System32\urlmon.dll [Unsigned] =>.Microsoft Corporation

O18 - Handler: ms-its [64Bits] - {9D148291-B9C8-11D0-A4CC-0000F80149F6} . (.Microsoft Corporation - Microsoft® InfoTech Storage System Library.) -- C:\Windows\System32\itss.dll [Unsigned] =>.Microsoft Corporation

O18 - Handler: mso-minsb-roaming.16 [64Bits] - {83C25742-A9F7-49FB-9138-434302C88D07} . (.Microsoft Corporation - Microsoft Office component.) -- C:\Program Files\Microsoft Office\root\Office16\MSOSB.DLL =>.Microsoft®

O18 - Handler: mso-minsb.16 [64Bits] - {42089D2D-912D-4018-9087-2B87803E93FB} . (.Microsoft Corporation - Microsoft Office component.) -- C:\Program Files\Microsoft Office\root\Office16\MSOSB.DLL =>.Microsoft®

O18 - Handler: osf-roaming.16 [64Bits] - {42089D2D-912D-4018-9087-2B87803E93FB} . (.Microsoft Corporation - Microsoft Office component.) -- C:\Program Files\Microsoft Office\root\Office16\MSOSB.DLL =>.Microsoft®

O18 - Handler: osf.16 [64Bits] - {5504BE45-A83B-4808-900A-3A5C36E7F77A} . (.Microsoft Corporation - Microsoft Office component.) -- C:\Program Files\Microsoft Office\root\Office16\MSOSB.DLL =>.Microsoft®

O18 - Handler: res [64Bits] - {3050F3BC-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Visionneuse HTML Microsoft (R).) -- C:\Windows\System32\mshtml.dll [Unsigned] =>.Microsoft Corporation

O18 - Handler: tbauth [64Bits] - {14654CA6-5711-491D-B89A-58E571679951} . (.Microsoft Corporation - TBAuth protocol handler.) -- C:\Windows\System32\tbauth.dll [Unsigned] =>.Microsoft Corporation

O18 - Handler: tv [64Bits] - {CBD30858-AF45-11D2-B6D6-00C04FBBDE6E} . (.Microsoft Corporation - Contrôle ActiveX pour le flux vidéo.) -- C:\Windows\System32\MSVidCtl.dll [Unsigned] =>.Microsoft Corporation

O18 - Handler: vbscript [64Bits] - {3050F3B2-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Visionneuse HTML Microsoft (R).) -- C:\Windows\System32\mshtml.dll [Unsigned] =>.Microsoft Corporation

O18 - Handler: windows.tbauth [64Bits] - {14654CA6-5711-491D-B89A-58E571679951} . (.Microsoft Corporation - TBAuth protocol handler.) -- C:\Windows\System32\tbauth.dll [Unsigned] =>.Microsoft Corporation

O18 - Filter: application/octet-stream [64Bits] - {1E66F26B-79EE-11D2-8710-00C04F79ED0D} . (.Microsoft Corporation - Microsoft .NET Runtime Execution Engine.) -- C:\Windows\System32\mscoree.dll [Unsigned] =>.Microsoft Corporation

O18 - Filter: application/x-complus [64Bits] - {1E66F26B-79EE-11D2-8710-00C04F79ED0D} . (.Microsoft Corporation - Microsoft .NET Runtime Execution Engine.) -- C:\Windows\System32\mscoree.dll [Unsigned] =>.Microsoft Corporation

O18 - Filter: application/x-msdownload [64Bits] - {1E66F26B-79EE-11D2-8710-00C04F79ED0D} . (.Microsoft Corporation - Microsoft .NET Runtime Execution Engine.) -- C:\Windows\System32\mscoree.dll [Unsigned] =>.Microsoft Corporation

O18 - Filter: text/xml [64Bits] - {807583E5-5146-11D5-A672-00B0D022E945} . (.Microsoft Corporation - Microsoft Office XML MIME Filter.) -- C:\Program Files\Microsoft Office\root\vfs\ProgramFilesCommonX64\Microsoft Shared\OFFICE16\MSOXMLMF.DLL =>.Microsoft®

**---\ REGISTRE AppInit\_DLLs et Winlogon Notify (1) - 0s**

O20 - Winlogon : UserInit . (.Microsoft Corporation - Application d’ouverture de session Userinit.) - C:\windows\system32\userinit.exe =>.Microsoft Corporation

**---\ CLÉ DE REGISTRE EXPLORER StartupApproved (22) - 0s**

[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:CCleaner Smart Cleaning =>.Piriform Ltd

[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:Google Update =>.Google Inc.

[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:OneDrive =>.Microsoft Corporation

[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:RocketDock =>.Punk Software

[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:GoogleDriveSync =>.Google Inc.

[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:com.squirrel.Teams.Teams

[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:CCleanerBrowserAutoLaunch\_593A14077FF47768888263630D5AFAFE

[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:BlueJeans.Detector

[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder]:Envoyer à OneNote.lnk =>.Microsoft Corporation

[HKEY\_USERS\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:CCleaner Smart Cleaning =>.Piriform Ltd

[HKEY\_USERS\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:Google Update =>.Google Inc.

[HKEY\_USERS\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:OneDrive =>.Microsoft Corporation

[HKEY\_USERS\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:RocketDock =>.Punk Software

[HKEY\_USERS\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:GoogleDriveSync =>.Google Inc.

[HKEY\_USERS\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:com.squirrel.Teams.Teams

[HKEY\_USERS\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:CCleanerBrowserAutoLaunch\_593A14077FF47768888263630D5AFAFE

[HKEY\_USERS\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:BlueJeans.Detector

[HKEY\_USERS\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder]:Envoyer à OneNote.lnk =>.Microsoft Corporation

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:SecurityHealth =>.Microsoft Corporation

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:RtkAudUService =>.Realtek Semiconductor Corp.

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run32]:Dropbox =>.Dropbox Inc.

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run32]:WDAppManager =>.Western Digital Technologies

**---\ COMPOSANTS ACTIVESETUP INSTALLÉS (ASIC) (6) - 1s**

O40 - ASIC: Microsoft Windows Media Player [64Bits] - >{22d6f312-b0f6-11d0-94ab-0080c74c7e95} . (.Microsoft Corporation - Utilitaire d’installation du Lecteur Window.) -- C:\Windows\System32\unregmp2.exe [Unsigned] =>.Microsoft Corporation

O40 - ASIC: Microsoft Windows Media Player 12.0 [64Bits] - {22d6f312-b0f6-11d0-94ab-0080c74c7e95} . (.Microsoft Corporation - Windows Media Player Extension.) -- C:\Windows\System32\wmpdxm.dll [Unsigned] =>.Microsoft Corporation

O40 - ASIC: Microsoft Windows Media Player [64Bits] - {6BF52A52-394A-11d3-B153-00C04F79FAA6} . (.Microsoft Corporation - Utilitaire d’installation du Lecteur Window.) -- C:\Windows\System32\unregmp2.exe [Unsigned] =>.Microsoft Corporation

O40 - ASIC: Web Platform Customizations [64Bits] - {89820200-ECBD-11cf-8B85-00AA005B4383} . (.Microsoft Corporation - Utilitaire d'initialisation d'Internet Expl.) -- C:\Windows\System32\ie4uinit.exe [Unsigned] =>.Microsoft Corporation

O40 - ASIC: (no name) [64Bits] - {89B4C1CD-B018-4511-B0A1-5476DBF70820} . (.Microsoft Corporation - Microsoft .NET IE SECURITY REGISTRATION.) -- C:\Windows\System32\mscories.dll =>.Microsoft®

O40 - ASIC: Microsoft Edge [64Bits] - {9459C573-B17A-45AE-9F64-1857B5D58CEE} . (.Microsoft Corporation - Microsoft Edge Installer.) -- C:\Program Files (x86)\Microsoft\Edge\Application\85.0.564.63\Installer\setup.exe =>.Microsoft®

**---\ LOGICIELS INSTALLÉS (89) - 18s**

O42 - Logiciel: 64 Bit HP CIO Components Installer - (.HP Inc..) [HKLM][64Bits] -- {13DA9C7C-EBFB-40D0-94A1-55B42883DF21} [Unsigned] =>.HP Inc. (Hidden)

O42 - Logiciel: Adobe Acrobat Reader DC - Français - (.Adobe Systems Incorporated.) [HKLM][64Bits] -- {AC76BA86-7AD7-1036-7B44-AC0F074E4100} [Unsigned] =>.Adobe Systems Incorporated

O42 - Logiciel: Adobe Refresh Manager - (.Adobe Systems Incorporated.) [HKLM][64Bits] -- {AC76BA86-0804-1033-1959-001824399311} [Unsigned] =>.Adobe Systems Incorporated (Hidden)

O42 - Logiciel: Backup and Sync from Google - (.Google, Inc..) [HKLM][64Bits] -- {B109BD68-709A-485B-97E6-651FEB234AC9} [Unsigned] =>.Google, Inc.

O42 - Logiciel: CCleaner - (.Piriform.) [HKLM][64Bits] -- CCleaner =>.Piriform Software Ltd®

O42 - Logiciel: CCleaner Browser - (.Auteurs de CCleaner Browser.) [HKLM][64Bits] -- CCleaner Browser =>.Piriform Software Ltd®

O42 - Logiciel: Dropbox - (.Dropbox, Inc..) [HKLM][64Bits] -- Dropbox =>.Dropbox, Inc®

O42 - Logiciel: Dropbox Update Helper - (.Dropbox, Inc..) [HKLM][64Bits] -- {099218A5-A723-43DC-8DB5-6173656A1E94} [Unsigned] =>.Dropbox, Inc. (Hidden)

O42 - Logiciel: GIMP 2.8.22 - (.The GIMP Team.) [HKLM][64Bits] -- GIMP-2\_is1 =>.Jernej Simončič®

O42 - Logiciel: Google Update Helper - (.Google LLC.) [HKLM][64Bits] -- {60EC980A-BDA2-4CB6-A427-B07A5498B4CA} [Unsigned] =>.Google LLC (Hidden)

O42 - Logiciel: Google Chrome - (.Google LLC.) [HKCU][64Bits] -- Google Chrome =>.Google LLC®

O42 - Logiciel: HwOsd 9.0.1.66 - (.Huawei Technologies Co., Ltd..) [HKLM][64Bits] -- HwOsd {6E715E33F17AD55BCBF98C1F14D21F2F}. =>.Huawei Technologies Co., Ltd.

O42 - Logiciel: Intel(R) Chipset Device Software - (.Intel Corporation.) [HKLM][64Bits] -- {7FB35D08-C75C-4A18-B593-1D7C3E8970AD} [Unsigned] =>.Intel Corporation (Hidden)

O42 - Logiciel: Intel(R) Chipset Device Software - (.Intel(R) Corporation.) [HKLM][64Bits] -- {44ded3eb-1686-46a6-9770-fd79096c29f7} =>.Intel(R) Software and Firmware Products® (Hidden)

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

O42 - Logiciel: Intel(R) Management Engine Components - (.Intel Corporation.) [HKLM][64Bits] -- {1CEAC85D-2590-4760-800F-8DE5E91F3700} =>.Intel(R) Embedded Subsystems and IP Blocks Group®

O42 - Logiciel: Intel(R) Management Engine Components - (.Intel Corporation.) [HKLM][64Bits] -- {5E21AB91-2EF8-4E8A-BA33-515E667CDC4B} [Unsigned] =>.Intel Corporation (Hidden)

O42 - Logiciel: Intel(R) Management Engine Components - (.Intel Corporation.) [HKLM][64Bits] -- {EB67ED3E-E5CA-4F35-8D2D-F0EF10802DBF} [Unsigned] =>.Intel Corporation (Hidden)

O42 - Logiciel: Intel(R) Management Engine Driver - (.Intel Corporation.) [HKLM][64Bits] -- {42625EDB-9CF1-421C-8540-0E66F1402DEC} [Unsigned] =>.Intel Corporation (Hidden)

O42 - Logiciel: Intel(R) ME UninstallLegacy - (.Intel Corporation.) [HKLM][64Bits] -- {E9B9A1A5-6398-4C99-8FDE-10794F6505C5} [Unsigned] =>.Intel Corporation (Hidden)

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

O42 - Logiciel: Intel(R) Serial IO - (.Intel Corporation.) [HKLM][64Bits] -- {4B4449E2-ABC0-4A51-989C-CB1217D3A433} [Unsigned] =>.Intel Corporation (Hidden)

O42 - Logiciel: Intel(R) Serial IO - (.Intel Corporation.) [HKLM][64Bits] -- {9FD91C5C-44AE-4D9D-85BE-AE52816B0294} =>.Intel(R) Serial IO®

O42 - Logiciel: Intel(R) Trusted Connect Service Client x64 - (.Intel Corporation.) [HKLM][64Bits] -- {C9552825-7BF2-4344-BA91-D3CD46F4C442} [Unsigned] =>.Intel Corporation (Hidden)

O42 - Logiciel: Intel(R) Trusted Connect Service Client x86 - (.Intel Corporation.) [HKLM][64Bits] -- {C9552825-7BF2-4344-BA91-D3CD46F4C441} [Unsigned] =>.Intel Corporation (Hidden)

O42 - Logiciel: Intel(R) Trusted Connect Services Client - (.Intel Corporation.) [HKLM][64Bits] -- {66129f84-d3f0-4884-ac54-369ae6fc2cf6} =>.Intel(R) Trust Services® (Hidden)

O42 - Logiciel: Intel® PROSet/Wireless WiFi Software - (.Intel Corporation.) [HKLM][64Bits] -- {EF71AFFB-85B5-407C-A301-39EA25F98313} [Unsigned] =>.Intel Corporation (Hidden)

O42 - Logiciel: Light Image Resizer 5.1.4.1 - (.ObviousIdea.) [HKLM][64Bits] -- {D5C093E0-D3DF-42D3-AFD6-CAAFB6985CBC}\_is1 =>.ObviousIdea SARLU®

O42 - Logiciel: Logiciel Intel® PROSet/Wireless - (.Intel Corporation.) [HKLM][64Bits] -- {3d609846-847c-46e5-9a23-682bec1569ea} =>.Intel(R) Wireless Connectivity Solutions®

O42 - Logiciel: Malwarebytes version 4.2.1.89 - (.Malwarebytes.) [HKLM][64Bits] -- {35065F43-4BB2-439A-BFF7-0F1014F2E0CD}\_is1 =>.Malwarebytes Inc®

O42 - Logiciel: Microsoft 365 - en-us - (.Microsoft Corporation.) [HKLM][64Bits] -- O365HomePremRetail - en-us =>.Microsoft®

O42 - Logiciel: Microsoft 365 - fr-fr - (.Microsoft Corporation.) [HKLM][64Bits] -- O365HomePremRetail - fr-fr =>.Microsoft®

O42 - Logiciel: Microsoft 365 Apps for enterprise - en-us - (.Microsoft Corporation.) [HKLM][64Bits] -- O365ProPlusRetail - en-us =>.Microsoft®

O42 - Logiciel: Microsoft 365 Apps for enterprise - fr-fr - (.Microsoft Corporation.) [HKLM][64Bits] -- O365ProPlusRetail - fr-fr =>.Microsoft®

O42 - Logiciel: Microsoft Edge - (.Microsoft Corporation.) [HKLM][64Bits] -- Microsoft Edge =>.Microsoft®

O42 - Logiciel: Microsoft Edge Update - (.Microsoft Corporation.) [HKLM][64Bits] -- Microsoft Edge Update [Unsigned] =>.Microsoft Corporation

O42 - Logiciel: Microsoft Lync Web App Plug-in - (.Microsoft Corporation.) [HKLM][64Bits] -- {BE6D5464-0B1F-46CC-8973-F9651FE6A45A} [Unsigned] =>.Microsoft Corporation

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

O42 - Logiciel: Microsoft Sync Framework 2.0 Core Components (x64) ENU - (.Microsoft Corporation.) [HKLM][64Bits] -- {8CCBEC22-D2DB-4DC9-A58A-E1A1F3A38C8A} [Unsigned] =>.Microsoft Corporation

O42 - Logiciel: Microsoft Sync Framework 2.0 Provider Services (x64) ENU - (.Microsoft Corporation.) [HKLM][64Bits] -- {03AC245F-4C64-425C-89CF-7783C1D3AB2C} [Unsigned] =>.Microsoft Corporation

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

O42 - Logiciel: Microsoft VC++ redistributables repacked. - (.Intel Corporation.) [HKLM][64Bits] -- {599ED608-BADF-4C3D-9172-EA5E06386EF6} [Unsigned] =>.Intel Corporation (Hidden)

O42 - Logiciel: Microsoft VC++ redistributables repacked. - (.Intel Corporation.) [HKLM][64Bits] -- {ED4D7D2E-A64D-4C3A-A8B9-B27CE153A2A6} [Unsigned] =>.Intel Corporation (Hidden)

O42 - Logiciel: Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.21005 - (.Microsoft Corporation.) [HKLM][64Bits] -- {7f51bdb9-ee21-49ee-94d6-90afc321780e} =>.Microsoft®

O42 - Logiciel: Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.21005 - (.Microsoft Corporation.) [HKLM][64Bits] -- {ce085a78-074e-4823-8dc1-8a721b94b76d} =>.Microsoft®

O42 - Logiciel: Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 - (.Microsoft Corporation.) [HKLM][64Bits] -- {929FBD26-9020-399B-9A7A-751D61F0B942} [Unsigned] =>.Microsoft Corporation (Hidden)

O42 - Logiciel: Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005 - (.Microsoft Corporation.) [HKLM][64Bits] -- {A749D8E6-B613-3BE3-8F5F-045C84EBA29B} [Unsigned] =>.Microsoft Corporation (Hidden)

O42 - Logiciel: Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 - (.Microsoft Corporation.) [HKLM][64Bits] -- {F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185} [Unsigned] =>.Microsoft Corporation (Hidden)

O42 - Logiciel: Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 - (.Microsoft Corporation.) [HKLM][64Bits] -- {13A4EE12-23EA-3371-91EE-EFB36DDFFF3E} [Unsigned] =>.Microsoft Corporation (Hidden)

O42 - Logiciel: Microsoft Visual C++ 2017 Redistributable (x64) - 14.13.26020 - (.Microsoft Corporation.) [HKLM][64Bits] -- {7474cd6e-76cc-4257-837e-5b9261e526af} =>.Microsoft Corporation®

O42 - Logiciel: Microsoft Visual C++ 2017 Redistributable (x86) - 14.13.26020 - (.Microsoft Corporation.) [HKLM][64Bits] -- {5c045b7f-e561-4794-91f8-c6cda0893107} =>.Microsoft Corporation®

O42 - Logiciel: Microsoft Visual C++ 2017 x64 Additional Runtime - 14.13.26020 - (.Microsoft Corporation.) [HKLM][64Bits] -- {C5ECDB9A-D9B0-3107-BA85-1269998A5B3E} [Unsigned] =>.Microsoft Corporation (Hidden)

O42 - Logiciel: Microsoft Visual C++ 2017 x64 Minimum Runtime - 14.13.26020 - (.Microsoft Corporation.) [HKLM][64Bits] -- {221D6DB4-46E2-333C-B09B-5F49351D0980} [Unsigned] =>.Microsoft Corporation (Hidden)

O42 - Logiciel: Microsoft Visual C++ 2017 x86 Additional Runtime - 14.13.26020 - (.Microsoft Corporation.) [HKLM][64Bits] -- {895D5198-C5DB-375E-86AB-133F4DAA9FE2} [Unsigned] =>.Microsoft Corporation (Hidden)

O42 - Logiciel: Microsoft Visual C++ 2017 x86 Minimum Runtime - 14.13.26020 - (.Microsoft Corporation.) [HKLM][64Bits] -- {8F271F6C-6E7B-3D0A-951B-6E7B694D78BD} [Unsigned] =>.Microsoft Corporation (Hidden)

O42 - Logiciel: MindFusion XML Viewer - (.MindFusion.) [HKLM][64Bits] -- {30C45D8E-530B-4C3A-9010-38319FE3CD97} [Unsigned]

O42 - Logiciel: Mozilla Firefox 78.0.2 (x64 fr) - (.Mozilla.) [HKLM][64Bits] -- Mozilla Firefox 78.0.2 (x64 fr) =>.Mozilla Corporation®

O42 - Logiciel: Mozilla Maintenance Service - (.Mozilla.) [HKLM][64Bits] -- MozillaMaintenanceService [Unsigned] =>.Mozilla

O42 - Logiciel: NVIDIA Ansel - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_Ansel [Unsigned] =>.NVIDIA Corporation (Hidden)

O42 - Logiciel: NVIDIA Display Container - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_NVDisplayContainer [Unsigned] =>.NVIDIA Corporation (Hidden)

O42 - Logiciel: NVIDIA Display Container LS - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_NVDisplayContainerLS [Unsigned] =>.NVIDIA Corporation (Hidden)

O42 - Logiciel: NVIDIA Display Session Container - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_NVDisplaySessionContainer [Unsigned] =>.NVIDIA Corporation (Hidden)

O42 - Logiciel: NVIDIA Display Watchdog Plugin - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_NVDisplayPluginWatchdog [Unsigned] =>.NVIDIA Corporation (Hidden)

O42 - Logiciel: NVIDIA Install Application - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_installer [Unsigned] =>.NVIDIA Corporation (Hidden)

O42 - Logiciel: NVIDIA Optimus Update 37.0.0.0 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_Display.Optimus [Unsigned] =>.NVIDIA Corporation (Hidden)

O42 - Logiciel: NVIDIA PhysX System Software 9.18.0628 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_Display.PhysX [Unsigned] =>.NVIDIA Corporation

O42 - Logiciel: NVIDIA Telemetry Client - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_NvTelemetry [Unsigned] =>.NVIDIA Corporation (Hidden)

O42 - Logiciel: NVIDIA Telemetry Container - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_NvTelemetryContainer [Unsigned] =>.NVIDIA Corporation (Hidden)

O42 - Logiciel: NVIDIA Update Core - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_Update.Core [Unsigned] =>.NVIDIA Corporation (Hidden)

O42 - Logiciel: Office 16 Click-to-Run Extensibility Component - (.Microsoft Corporation.) [HKLM][64Bits] -- {90160000-008C-0000-1000-0000000FF1CE} [Unsigned] =>.Microsoft Corporation (Hidden)

O42 - Logiciel: Office 16 Click-to-Run Licensing Component - (.Microsoft Corporation.) [HKLM][64Bits] -- {90160000-007E-0000-1000-0000000FF1CE} [Unsigned] =>.Microsoft Corporation (Hidden)

O42 - Logiciel: Office 16 Click-to-Run Localization Component - (.Microsoft Corporation.) [HKLM][64Bits] -- {90160000-008C-0409-1000-0000000FF1CE} [Unsigned] =>.Microsoft Corporation (Hidden)

O42 - Logiciel: Office 16 Click-to-Run Localization Component - (.Microsoft Corporation.) [HKLM][64Bits] -- {90160000-008C-040C-1000-0000000FF1CE} [Unsigned] =>.Microsoft Corporation (Hidden)

O42 - Logiciel: Panneau de configuration NVIDIA 399.10 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_Display.ControlPanel [Unsigned] =>.NVIDIA Corporation (Hidden)

O42 - Logiciel: PC Manager - (.Huawei Technologies Co., Ltd..) [HKLM][64Bits] -- PC Manager {6E715E33F17AD55BCBF98C1F14D21F2F}. =>.Huawei Technologies Co., Ltd.

O42 - Logiciel: PDFsam Basic - (.Sober Lemur S.a.s. di Vacondio Andrea.) [HKLM][64Bits] -- {1304BB7D-3790-4FA3-AF8B-76499669F543} [Unsigned]

O42 - Logiciel: Preme for Windows - (.Preme for Windows.) [HKCU][64Bits] -- Preme for Windows [Unsigned]

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

O42 - Logiciel: RocketDock 1.3.5 - (.Punk Software.) [HKLM][64Bits] -- RocketDock\_is1 [Unsigned] =>.Punk Software

O42 - Logiciel: Skype Meetings App - (.Microsoft Corporation.) [HKLM][64Bits] -- {BC1D9E47-8927-4AA1-A891-7763BC2475B7} [Unsigned] =>.Microsoft Corporation

O42 - Logiciel: SyncToy 2.1 (x64) - (.Microsoft.) [HKLM][64Bits] -- {88DAAF05-5A72-46D2-A7C5-C3759697E943} [Unsigned] =>.Microsoft

O42 - Logiciel: Thunderbolt™ Software - (.Intel Corporation.) [HKLM][64Bits] -- {6ECDE40C-4023-419A-8A4E-50FB71275876} [Unsigned] =>.Intel Corporation

O42 - Logiciel: TiCS - DXC TimeCard System - (.DXC.technology.) [HKLM][64Bits] -- TiCS [Unsigned]

O42 - Logiciel: Update for Windows 10 for x64-based Systems (KB4023057) - (.Microsoft Corporation.) [HKLM][64Bits] -- {32DC821E-4A7D-4878-BEE8-337FA153D7F2} [Unsigned] =>.Microsoft Corporation (Hidden)

O42 - Logiciel: Update for Windows 10 for x64-based Systems (KB4480730) - (.Microsoft Corporation.) [HKLM][64Bits] -- {344F3227-F502-4219-9DC4-1967E586FAFA} [Unsigned] =>.Microsoft Corporation

O42 - Logiciel: VdhCoApp 1.5.0 - (.DownloadHelper.) [HKLM][64Bits] -- weh-iss-net.downloadhelper.coapp\_is1 [Unsigned] =>.DownloadHelper

O42 - Logiciel: VLC media player - (.VideoLAN.) [HKLM][64Bits] -- VLC media player [Unsigned] =>.VideoLAN

O42 - Logiciel: WDT Device Driver version 1.0.2.9 - (.Huawei Technologies Co., Ltd..) [HKLM][64Bits] -- {5B06CB06-0929-48BC-BE1F-7E41461440C7}\_is1 {6E715E33F17AD55BCBF98C1F14D21F2F}. =>.Huawei Technologies Co., Ltd.

O42 - Logiciel: Zoom - (.Zoom Video Communications, Inc..) [HKCU][64Bits] -- ZoomUMX =>.Zoom Video Communications, Inc.®

**---\ CLÉ DE REGISTRE SOFTWARE HKCU & HKLM (143) - 18s**

HKLM\SOFTWARE\AGEIA Technologies =>.AGEIA Technologies

HKLM\SOFTWARE\AVAST Software =>.AVAST Software

HKLM\SOFTWARE\Chromium =>.Chromium

HKLM\SOFTWARE\Clover =>.Ejie

HKLM\SOFTWARE\CVSM =>.Legitimate

HKLM\SOFTWARE\DefaultUserEnvironment =>.Microsoft Corporation

HKLM\SOFTWARE\Dolby =>.Dolby

HKLM\SOFTWARE\DownloadHelper =>.DownloadHelper

HKLM\SOFTWARE\Goodix

HKLM\SOFTWARE\Google =>.Google

HKLM\SOFTWARE\Hewlett-Packard =>.Hewlett-Packard

HKLM\SOFTWARE\Huawei =>.Huawei

HKLM\SOFTWARE\IM Providers =>.IM Providers

HKLM\SOFTWARE\Intel =>.Intel

HKLM\SOFTWARE\Khronos =>.Khronos

HKLM\SOFTWARE\Macromedia =>.Macromedia

HKLM\SOFTWARE\Malwarebytes =>.Malwarebytes

HKLM\SOFTWARE\McAfee.com =>.McAfee Inc.

HKLM\SOFTWARE\Mozilla =>.Mozilla

HKLM\SOFTWARE\mozilla.org =>.mozilla.org

HKLM\SOFTWARE\MozillaPlugins =>.MozillaPlugins

HKLM\SOFTWARE\NVIDIA Corporation =>.nVidia Corporation

HKLM\SOFTWARE\ODBC =>.DB Connectivity Solutions

HKLM\SOFTWARE\OEM =>.OEM

HKLM\SOFTWARE\OpenSSH =>.OpenBSD

HKLM\SOFTWARE\Partner =>.Google Inc.

HKLM\SOFTWARE\PCManager

HKLM\SOFTWARE\PDFsam Basic =>.PDFsam Basic

HKLM\SOFTWARE\Piriform =>.Piriform

HKLM\SOFTWARE\Quizo =>.Quizo

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

HKLM\SOFTWARE\RegisteredApplications =>.Microsoft Corporation

HKLM\SOFTWARE\TXlTb2Z0

HKLM\SOFTWARE\VideoLAN =>.VideoLan Team

HKLM\SOFTWARE\Windows =>.Microsoft Corporation

HKLM\SOFTWARE\WOW6432Node =>.Microsoft Corporation

HKLM\SOFTWARE\WOW6432Node\Adobe =>.Adobe

HKLM\SOFTWARE\WOW6432Node\AGEIA Technologies =>.AGEIA Technologies

HKLM\SOFTWARE\WOW6432Node\Borland =>.Borland

HKLM\SOFTWARE\WOW6432Node\Clover =>.Ejie

HKLM\SOFTWARE\WOW6432Node\CSC

HKLM\SOFTWARE\WOW6432Node\Dropbox =>.Dropbox

HKLM\SOFTWARE\WOW6432Node\DropboxUpdate =>.Dropbox Inc.

HKLM\SOFTWARE\WOW6432Node\Google =>.Google

HKLM\SOFTWARE\WOW6432Node\Hewlett-Packard =>.Hewlett-Packard

HKLM\SOFTWARE\WOW6432Node\Intel =>.Intel

HKLM\SOFTWARE\WOW6432Node\InterBase Corp

HKLM\SOFTWARE\WOW6432Node\Khronos =>.Khronos

HKLM\SOFTWARE\WOW6432Node\Macromedia =>.Macromedia

HKLM\SOFTWARE\WOW6432Node\McAfee.com =>.McAfee Inc.

HKLM\SOFTWARE\WOW6432Node\Mozilla =>.Mozilla

HKLM\SOFTWARE\WOW6432Node\MozillaPlugins =>.MozillaPlugins

HKLM\SOFTWARE\WOW6432Node\NVIDIA Corporation =>.nVidia Corporation

HKLM\SOFTWARE\WOW6432Node\ObviousIdea =>.ObviousIdea

HKLM\SOFTWARE\WOW6432Node\ODBC =>.DB Connectivity Solutions

HKLM\SOFTWARE\WOW6432Node\Piriform =>.Piriform

HKLM\SOFTWARE\WOW6432Node\Realtek =>.Realtek Semiconductor Corp.

HKLM\SOFTWARE\WOW6432Node\Realtek Semiconductor Corp. =>.Realtek Semiconductor Corp.

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

HKCU\SOFTWARE\Adobe =>.Adobe

HKCU\SOFTWARE\AppDataLow =>.Microsoft Corporation

HKCU\SOFTWARE\AvastAdSDK =>.Avast Software s.r.o

HKCU\SOFTWARE\AWIND =>.Legitimate

HKCU\SOFTWARE\Browser Cleanup =>.Avast Software s.r.o

HKCU\SOFTWARE\Chromium =>.Chromium

HKCU\SOFTWARE\Clover =>.Ejie

HKCU\SOFTWARE\Dropbox =>.Dropbox

HKCU\SOFTWARE\DropboxUpdate =>.Dropbox Inc.

HKCU\SOFTWARE\Explorer++ =>.Explorer++

HKCU\SOFTWARE\Google =>.Google

HKCU\SOFTWARE\Hewlett-Packard =>.Hewlett-Packard

HKCU\SOFTWARE\Huawei =>.Huawei

HKCU\SOFTWARE\IM Providers =>.IM Providers

HKCU\SOFTWARE\Intel =>.Intel

HKCU\SOFTWARE\JavaSoft =>.JavaSoft

HKCU\SOFTWARE\Malwarebytes =>.Malwarebytes

HKCU\SOFTWARE\Mozilla =>.Mozilla

HKCU\SOFTWARE\MozillaPlugins =>.MozillaPlugins

HKCU\SOFTWARE\Netscape =>.Netscape

HKCU\SOFTWARE\NVIDIA Corporation =>.nVidia Corporation

HKCU\SOFTWARE\ObviousIdea =>.ObviousIdea

HKCU\SOFTWARE\ODBC =>.DB Connectivity Solutions

HKCU\SOFTWARE\PCManager

HKCU\SOFTWARE\PDFsam Basic =>.PDFsam Basic

HKCU\SOFTWARE\Piriform =>.Piriform

HKCU\SOFTWARE\QtProject =>.QtProject

HKCU\SOFTWARE\Quizo =>.Quizo

HKCU\SOFTWARE\Realtek =>.Realtek Semiconductor Corp.

HKCU\SOFTWARE\RegisteredApplications =>.Microsoft Corporation

HKCU\SOFTWARE\RocketDock =>.Punk Software

HKCU\SOFTWARE\SyncEngines =>.Microsoft Corporation

HKCU\SOFTWARE\Wow6432Node =>.Microsoft Corporation

HKCU\SOFTWARE\ZHP =>.Nicolas Coolman

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

HKU\.DEFAULT\SOFTWARE\Dropbox =>.Dropbox

HKU\.DEFAULT\SOFTWARE\Google =>.Google

HKU\.DEFAULT\SOFTWARE\Hewlett-Packard =>.Hewlett-Packard

HKU\.DEFAULT\SOFTWARE\Huawei =>.Huawei

HKU\.DEFAULT\SOFTWARE\Inj

HKU\.DEFAULT\SOFTWARE\Intel =>.Intel

HKU\.DEFAULT\SOFTWARE\Malwarebytes =>.Malwarebytes

HKU\.DEFAULT\SOFTWARE\MiNi

HKU\.DEFAULT\SOFTWARE\Mozilla =>.Mozilla

HKU\.DEFAULT\SOFTWARE\Netscape =>.Netscape

HKU\.DEFAULT\SOFTWARE\NVIDIA Corporation =>.nVidia Corporation

HKU\.DEFAULT\SOFTWARE\PCManager

HKU\.DEFAULT\SOFTWARE\Piriform =>.Piriform

HKU\.DEFAULT\SOFTWARE\Tips

HKU\.DEFAULT\SOFTWARE\WixSharp =>.Legitimate

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Adobe =>.Adobe

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\AppDataLow =>.Microsoft Corporation

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\AvastAdSDK =>.Avast Software s.r.o

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\AWIND =>.Legitimate

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Browser Cleanup =>.Avast Software s.r.o

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Chromium =>.Chromium

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Clover =>.Ejie

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Dropbox =>.Dropbox

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\DropboxUpdate =>.Dropbox Inc.

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Explorer++ =>.Explorer++

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Google =>.Google

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Hewlett-Packard =>.Hewlett-Packard

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Huawei =>.Huawei

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\IM Providers =>.IM Providers

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Intel =>.Intel

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\JavaSoft =>.JavaSoft

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Malwarebytes =>.Malwarebytes

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Mozilla =>.Mozilla

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\MozillaPlugins =>.MozillaPlugins

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Netscape =>.Netscape

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\NVIDIA Corporation =>.nVidia Corporation

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\ObviousIdea =>.ObviousIdea

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\ODBC =>.DB Connectivity Solutions

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\PCManager

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\PDFsam Basic =>.PDFsam Basic

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Piriform =>.Piriform

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\QtProject =>.QtProject

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Quizo =>.Quizo

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Realtek =>.Realtek Semiconductor Corp.

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\RegisteredApplications =>.Microsoft Corporation

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\RocketDock =>.Punk Software

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\SyncEngines =>.Microsoft Corporation

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\Wow6432Node =>.Microsoft Corporation

HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\SOFTWARE\ZHP =>.Nicolas Coolman

**---\ PACKAGES (6) - 0s**

C:\Program Files (x86)\WindowsApps\AD2F1837.HPPrinterControl\_115.1.152.0\_x64\_\_v10z8vjag6ke6 - (.Hewlett-Packard.) [][HP Smart] =>Hewlett-Packard

C:\Program Files (x86)\WindowsApps\DolbyLaboratories.DolbyAtmosSoundSystem\_3.20201.255.0\_x64\_\_rz1tebttyb220 - (.Dolby Laboratories.) [][Dolby Atmos Sound System] =>Dolby Laboratories

C:\Program Files (x86)\WindowsApps\MicrosoftWindows.Client.CBS\_120.2212.31.0\_x64\_\_cw5n1h2txyewy - (..) [][Windows Feature Experience Pack]

C:\Program Files (x86)\WindowsApps\MicrosoftWindows.UndockedDevKit\_10.0.19041.423\_neutral\_neutral\_cw5n1h2txyewy - (.Microsoft Corporation.) [][UDK Package] =>Microsoft Corporation

C:\Program Files (x86)\WindowsApps\NcsiUwpApp\_1000.19041.423.0\_neutral\_neutral\_8wekyb3d8bbwe - (.Microsoft.) [][NcsiUwpApp] =>Microsoft

C:\Program Files (x86)\WindowsApps\RealtekSemiconductorCorp.RealtekAudioControl\_1.2.174.0\_x64\_\_dt26b99r8h8gj - (.Realtek Semiconductor Corp.) [][Realtek Audio Control] =>Realtek Semiconductor Corp

**---\ CONTENU DES DOSSIERS PROGRAMMES (228) - 10s**

O43 - CFD: 18/10/2019 - [] D -- C:\Program Files\CCleaner =>.Piriform Ltd

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files\Common Files =>.Microsoft Corporation

O43 - CFD: 24/04/2019 - [] D -- C:\Program Files\CUAssistant =>.Microsoft Windows®

O43 - CFD: 02/09/2019 - [0] SHD -- C:\Program Files\Fichiers communs =>.Microsoft Corporation

O43 - CFD: 30/09/2019 - [] D -- C:\Program Files\GIMP 2 =>.Jernej Simončič®

O43 - CFD: 07/11/2018 - [0] D -- C:\Program Files\Goodix Fingerprint SPI Device

O43 - CFD: 07/11/2019 - [] D -- C:\Program Files\Google =>.Google LLC®

O43 - CFD: 14/02/2020 - [] D -- C:\Program Files\Hewlett-Packard =>.Hewlett-Packard

O43 - CFD: 01/09/2019 - [] D -- C:\Program Files\Huawei {6E715E33F17AD55BCBF98C1F14D21F2F}. =>.Huawei

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files\Intel =>.Intel Corporation

O43 - CFD: 07/12/2019 - [] D -- C:\Program Files\Internet Explorer =>.Microsoft Corporation

O43 - CFD: 25/04/2019 - [] D -- C:\Program Files\Malwarebytes =>.Malwarebytes

O43 - CFD: 22/09/2020 - [] D -- C:\Program Files\Microsoft Office =>.Microsoft Corporation

O43 - CFD: 26/04/2019 - [] D -- C:\Program Files\Microsoft Office 15 =>.Microsoft Corporation

O43 - CFD: 13/10/2019 - [] D -- C:\Program Files\Microsoft Sync Framework =>.Microsoft Corporation

O43 - CFD: 07/12/2019 - [0] D -- C:\Program Files\ModifiableWindowsApps =>.Microsoft Corporation

O43 - CFD: 13/07/2020 - [] D -- C:\Program Files\Mozilla Firefox =>.Mozilla

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files\MSBuild =>.Microsoft Corporation

O43 - CFD: 03/05/2020 - [] D -- C:\Program Files\net.downloadhelper.coapp [Unsigned]

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files\NVIDIA Corporation =>.nVidia Corporation

O43 - CFD: 26/04/2019 - [] D -- C:\Program Files\PDFsam Basic =>.Andrea Vacondio

O43 - CFD: 13/06/2019 - [] D -- C:\Program Files\Preme for Windows [Unsigned]

O43 - CFD: 17/02/2020 - [] D -- C:\Program Files\QTTabBar =>.Quizo

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files\Reference Assemblies =>.Microsoft Corporation

O43 - CFD: 02/09/2019 - [] D -- C:\Program Files\rempl =>.Microsoft Corporation

O43 - CFD: 13/10/2019 - [] D -- C:\Program Files\SyncToy 2.1 =>.Microsoft Corporation®

O43 - CFD: 07/11/2018 - [0] HD -- C:\Program Files\Uninstall Information =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files\UNP =>.Microsoft Corporation

O43 - CFD: 27/04/2019 - [] D -- C:\Program Files\VideoLAN =>.VideoLan Team

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files\Windows Defender =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files\Windows Mail =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files\Windows Media Player =>.Microsoft Corporation

O43 - CFD: 07/12/2019 - [] D -- C:\Program Files\Windows Multimedia Platform =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files\Windows NT =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files\Windows Photo Viewer =>.Microsoft Corporation

O43 - CFD: 07/12/2019 - [] D -- C:\Program Files\Windows Portable Devices =>.Microsoft Corporation

O43 - CFD: 07/12/2019 - [] D -- C:\Program Files\Windows Security =>.Microsoft Corporation

O43 - CFD: 07/12/2019 - [] SHD -- C:\Program Files\Windows Sidebar =>.Microsoft Corporation

O43 - CFD: 30/09/2020 - [] HD -- C:\Program Files\WindowsApps =>.Microsoft Corporation

O43 - CFD: 07/12/2019 - [] D -- C:\Program Files\WindowsPowerShell =>.Microsoft Corporation

O43 - CFD: 03/05/2019 - [] D -- C:\Program Files (x86)\Adobe =>.Adobe Inc.®

O43 - CFD: 21/09/2020 - [] D -- C:\Program Files (x86)\CCleaner Browser =>.Piriform Software Ltd®

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files (x86)\Common Files =>.Microsoft Corporation

O43 - CFD: 24/09/2020 - [] D -- C:\Program Files (x86)\Dropbox =>.Dropbox, Inc®

O43 - CFD: 07/11/2019 - [] D -- C:\Program Files (x86)\Google =>.Google Inc®

O43 - CFD: 22/01/2019 - [] HD -- C:\Program Files (x86)\InstallShield Installation Information =>.InstallShield

O43 - CFD: 26/04/2019 - [] D -- C:\Program Files (x86)\Intel =>.Intel Corporation

O43 - CFD: 07/12/2019 - [] D -- C:\Program Files (x86)\Internet Explorer =>.Microsoft Corporation

O43 - CFD: 15/07/2020 - [] D -- C:\Program Files (x86)\Microsoft =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files (x86)\Microsoft.NET =>.Microsoft Corporation

O43 - CFD: 26/08/2019 - [] D -- C:\Program Files (x86)\MindFusion [Unsigned]

O43 - CFD: 17/07/2020 - [] D -- C:\Program Files (x86)\Mozilla Maintenance Service =>.Mozilla

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files (x86)\MSBuild =>.Microsoft Corporation

O43 - CFD: 15/08/2019 - [] D -- C:\Program Files (x86)\NVIDIA Corporation =>.nVidia Corporation

O43 - CFD: 03/12/2019 - [] D -- C:\Program Files (x86)\ObviousIdea =>.ObviousIdea

O43 - CFD: 22/01/2019 - [] D -- C:\Program Files (x86)\Realtek =>.Realtek

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files (x86)\Reference Assemblies =>.Microsoft Corporation

O43 - CFD: 24/04/2019 - [] D -- C:\Program Files (x86)\RocketDock =>.Punk Software

O43 - CFD: 13/06/2019 - [0] HD -- C:\Program Files (x86)\Temp =>.Microsoft Corporation

O43 - CFD: 27/03/2020 - [] D -- C:\Program Files (x86)\TiCS [Unsigned]

O43 - CFD: 02/09/2019 - [0] HD -- C:\Program Files (x86)\Uninstall Information =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files (x86)\VulkanRT =>.LunarG, Inc

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files (x86)\Windows Defender =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files (x86)\Windows Mail =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files (x86)\Windows Media Player =>.Microsoft Corporation

O43 - CFD: 07/12/2019 - [] D -- C:\Program Files (x86)\Windows Multimedia Platform =>.Microsoft Corporation

O43 - CFD: 07/12/2019 - [] D -- C:\Program Files (x86)\Windows NT =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files (x86)\Windows Photo Viewer =>.Microsoft Corporation

O43 - CFD: 07/12/2019 - [] D -- C:\Program Files (x86)\Windows Portable Devices =>.Microsoft Corporation

O43 - CFD: 07/12/2019 - [] SHD -- C:\Program Files (x86)\Windows Sidebar =>.Microsoft Corporation

O43 - CFD: 07/12/2019 - [] D -- C:\Program Files (x86)\WindowsPowerShell =>.Microsoft Corporation

O43 - CFD: 17/08/2020 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessibility =>.Microsoft Corporation

O43 - CFD: 11/09/2020 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories =>.Microsoft Corporation

O43 - CFD: 17/08/2020 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools =>.Administrative Tools

O43 - CFD: 28/09/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Backup and Sync from Google

O43 - CFD: 22/07/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\CCleaner =>.Piriform Ltd

O43 - CFD: 24/09/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Dropbox =>.Dropbox

O43 - CFD: 22/07/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\HUAWEI =>.Huawei

O43 - CFD: 07/12/2019 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Maintenance =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Office Tools =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\ObviousIdea =>.ObviousIdea

O43 - CFD: 22/07/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\PDFsam Basic =>.Andrea Vacondio

O43 - CFD: 22/07/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\RocketDock =>.Punk Software

O43 - CFD: 07/12/2019 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\System Tools =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Thunderbolt™ Software

O43 - CFD: 22/07/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\TimeCard System

O43 - CFD: 22/07/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\VideoLAN =>.VideoLan Team

O43 - CFD: 07/12/2019 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Windows PowerShell =>.Microsoft Corporation

O43 - CFD: 03/05/2019 - [] D -- C:\ProgramData\Adobe =>.Adobe

O43 - CFD: 22/07/2020 - [0] SHD -- C:\ProgramData\Application Data =>.Microsoft Corporation

O43 - CFD: 30/07/2019 - [] D -- C:\ProgramData\AVAST Software =>.AVAST Software

O43 - CFD: 02/09/2019 - [0] SHD -- C:\ProgramData\Bureau =>.Microsoft Corporation

O43 - CFD: 01/10/2019 - [] D -- C:\ProgramData\CCleaner Browser

O43 - CFD: 01/09/2019 - [] D -- C:\ProgramData\Comms =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [0] SHD -- C:\ProgramData\Documents =>.Microsoft Corporation

O43 - CFD: 26/04/2019 - [] D -- C:\ProgramData\Dropbox =>.Dropbox

O43 - CFD: 27/09/2020 - [] D -- C:\ProgramData\Goodix

O43 - CFD: 24/05/2019 - [] D -- C:\ProgramData\Google =>.Google

O43 - CFD: 14/02/2020 - [] D -- C:\ProgramData\Hewlett-Packard =>.Hewlett-Packard

O43 - CFD: 07/11/2018 - [] D -- C:\ProgramData\Huawei =>.Huawei

O43 - CFD: 24/09/2020 - [] D -- C:\ProgramData\HwSynergy

O43 - CFD: 26/04/2019 - [] D -- C:\ProgramData\Intel =>.Intel Corporation

O43 - CFD: 25/04/2019 - [] D -- C:\ProgramData\Malwarebytes =>.Malwarebytes

O43 - CFD: 03/05/2019 - [] D -- C:\ProgramData\McAfee =>.McAfee

O43 - CFD: 02/09/2019 - [0] SHD -- C:\ProgramData\Menu Démarrer =>.Microsoft Corporation

O43 - CFD: 11/08/2020 - [] SD -- C:\ProgramData\Microsoft =>.Microsoft Corporation

O43 - CFD: 23/07/2020 - [] D -- C:\ProgramData\Microsoft OneDrive =>.Microsoft Corporation

O43 - CFD: 02/09/2019 - [0] SHD -- C:\ProgramData\Modèles =>.Microsoft Corporation

O43 - CFD: 21/05/2019 - [] D -- C:\ProgramData\Mozilla =>.Mozilla Corporation

O43 - CFD: 24/09/2020 - [] D -- C:\ProgramData\NVIDIA =>.nVidia Corporation

O43 - CFD: 15/08/2019 - [] D -- C:\ProgramData\NVIDIA Corporation =>.nVidia Corporation

O43 - CFD: 02/04/2020 - [] D -- C:\ProgramData\Package Cache =>.Microsoft Corporation

O43 - CFD: 23/07/2020 - [] D -- C:\ProgramData\Packages =>.Microsoft Corporation

O43 - CFD: 30/09/2020 - [] D -- C:\ProgramData\regid.1991-06.com.microsoft =>.Microsoft Corporation

O43 - CFD: 07/11/2018 - [] D -- C:\ProgramData\Roaming =>.Microsoft Corporation

O43 - CFD: 07/12/2019 - [0] D -- C:\ProgramData\SoftwareDistribution =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [0] D -- C:\ProgramData\ssh

O43 - CFD: 22/07/2020 - [] D -- C:\ProgramData\USOPrivate =>.Microsoft Corporation

O43 - CFD: 07/12/2019 - [] D -- C:\ProgramData\USOShared =>.Microsoft Corporation

O43 - CFD: 02/04/2020 - [] D -- C:\ProgramData\Western Digital =>.Western Digital

O43 - CFD: 07/12/2019 - [] D -- C:\ProgramData\WindowsHolographicDevices =>.Microsoft Corporation

O43 - CFD: 19/03/2020 - [] D -- C:\Program Files (x86)\Common Files\Adobe =>.Adobe

O43 - CFD: 24/04/2019 - [] D -- C:\Program Files (x86)\Common Files\Clover =>.Ejie

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files (x86)\Common Files\Intel =>.Intel Corporation

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files (x86)\Common Files\Microsoft Shared =>.Microsoft Corporation

O43 - CFD: 07/11/2018 - [] D -- C:\Program Files (x86)\Common Files\PostureAgent =>.Microsoft Corporation

O43 - CFD: 07/12/2019 - [] D -- C:\Program Files (x86)\Common Files\Services =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] D -- C:\Program Files (x86)\Common Files\System =>.Microsoft Corporation

O43 - CFD: 02/04/2020 - [] D -- C:\Program Files (x86)\Common Files\Western Digital =>.Western Digital

O43 - CFD: 03/05/2019 - [] DC -- C:\Users\ericl\AppData\Roaming\Adobe =>.Adobe

O43 - CFD: 26/04/2019 - [] DC -- C:\Users\ericl\AppData\Roaming\Dropbox =>.Dropbox

O43 - CFD: 05/05/2019 - [] DC -- C:\Users\ericl\AppData\Roaming\dvdcss =>.VideoLan Team

O43 - CFD: 28/09/2019 - [] D -- C:\Users\ericl\AppData\Roaming\GIMP =>.The GIMP Team

O43 - CFD: 20/08/2020 - [] DC -- C:\Users\ericl\AppData\Roaming\HwSynergy

O43 - CFD: 07/11/2018 - [] DC -- C:\Users\ericl\AppData\Roaming\Intel =>.Intel Corporation

O43 - CFD: 29/07/2020 - [] SD -- C:\Users\ericl\AppData\Roaming\Microsoft =>.Microsoft Corporation

O43 - CFD: 26/04/2019 - [] DC -- C:\Users\ericl\AppData\Roaming\Microsoft Teams =>.Microsoft Corporation

O43 - CFD: 11/03/2020 - [] DC -- C:\Users\ericl\AppData\Roaming\Mozilla =>.Mozilla Corporation

O43 - CFD: 20/03/2020 - [] D -- C:\Users\ericl\AppData\Roaming\ObviousIdea =>.ObviousIdea

O43 - CFD: 14/09/2020 - [] DC -- C:\Users\ericl\AppData\Roaming\Preme for Windows

O43 - CFD: 15/07/2020 - [] DC -- C:\Users\ericl\AppData\Roaming\Skype =>.Skype

O43 - CFD: 14/02/2020 - [] D -- C:\Users\ericl\AppData\Roaming\UPD

O43 - CFD: 12/09/2020 - [] DC -- C:\Users\ericl\AppData\Roaming\vlc =>.VideoLan Team

O43 - CFD: 22/05/2019 - [0] DC -- C:\Users\ericl\AppData\Roaming\XnView =>.Pierre-Emmanuel Gougelet

O43 - CFD: 30/09/2020 - [] D -- C:\Users\ericl\AppData\Roaming\ZHP =>.Nicolas Coolman

O43 - CFD: 12/05/2020 - [] DC -- C:\Users\ericl\AppData\Roaming\Zoom =>.ZOOM

O43 - CFD: 17/10/2019 - [] DC -- C:\Users\ericl\AppData\Local\Adobe =>.Adobe

O43 - CFD: 22/07/2020 - [0] SHD -- C:\Users\ericl\AppData\Local\Application Data =>.Microsoft Corporation

O43 - CFD: 07/10/2019 - [] D -- C:\Users\ericl\AppData\Local\Apps =>.Microsoft Corporation

O43 - CFD: 30/09/2019 - [] D -- C:\Users\ericl\AppData\Local\babl-0.1 =>.The GIMP Team

O43 - CFD: 16/03/2020 - [] D -- C:\Users\ericl\AppData\Local\cache =>.Legitimate

O43 - CFD: 01/10/2019 - [] D -- C:\Users\ericl\AppData\Local\CCleaner Browser

O43 - CFD: 24/04/2019 - [] DC -- C:\Users\ericl\AppData\Local\CEF =>.CEF

O43 - CFD: 10/11/2019 - [] DC -- C:\Users\ericl\AppData\Local\Comms =>.Microsoft Corporation

O43 - CFD: 17/07/2020 - [] DC -- C:\Users\ericl\AppData\Local\ConnectedDevicesPlatform =>.Microsoft Corporation

O43 - CFD: 27/09/2020 - [] DC -- C:\Users\ericl\AppData\Local\CrashDumps =>.Microsoft Corporation

O43 - CFD: 23/08/2020 - [] DC -- C:\Users\ericl\AppData\Local\D3DSCache =>.Legitimate

O43 - CFD: 25/04/2019 - [0] DC -- C:\Users\ericl\AppData\Local\DBG =>.DBG

O43 - CFD: 28/08/2020 - [0] DC -- C:\Users\ericl\AppData\Local\Diagnostics =>.Microsoft Corporation

O43 - CFD: 17/10/2019 - [] DC -- C:\Users\ericl\AppData\Local\Dropbox =>.Dropbox

O43 - CFD: 27/09/2020 - [0] D -- C:\Users\ericl\AppData\Local\ElevatedDiagnostics =>.Microsoft Corporation

O43 - CFD: 30/09/2019 - [] D -- C:\Users\ericl\AppData\Local\fontconfig =>.Portable Apps

O43 - CFD: 30/09/2019 - [] D -- C:\Users\ericl\AppData\Local\gegl-0.2 =>.Portable Apps

O43 - CFD: 28/09/2019 - [] D -- C:\Users\ericl\AppData\Local\gegl-0.4 =>.Portable Apps

O43 - CFD: 28/09/2019 - [] D -- C:\Users\ericl\AppData\Local\GIMP =>.The GIMP Team

O43 - CFD: 29/09/2020 - [] DC -- C:\Users\ericl\AppData\Local\Google =>.Google

O43 - CFD: 30/09/2019 - [] D -- C:\Users\ericl\AppData\Local\gtk-2.0 =>.GTK Project

O43 - CFD: 22/07/2020 - [0] SHD -- C:\Users\ericl\AppData\Local\Historique =>.Microsoft Corporation

O43 - CFD: 22/01/2019 - [] DC -- C:\Users\ericl\AppData\Local\Intel =>.Intel Corporation

O43 - CFD: 27/04/2020 - [] D -- C:\Users\ericl\AppData\Local\IsolatedStorage =>.id Software

O43 - CFD: 25/04/2019 - [] DC -- C:\Users\ericl\AppData\Local\mbam =>.Malwarebytes

O43 - CFD: 25/04/2019 - [] DC -- C:\Users\ericl\AppData\Local\mbamtray =>.Malwarebytes

O43 - CFD: 24/07/2020 - [] D -- C:\Users\ericl\AppData\Local\Microsoft =>.Microsoft Corporation

O43 - CFD: 22/01/2019 - [] DC -- C:\Users\ericl\AppData\Local\MicrosoftEdge =>.Microsoft Corporation

O43 - CFD: 21/05/2019 - [] DC -- C:\Users\ericl\AppData\Local\Mozilla =>.Mozilla Corporation

O43 - CFD: 15/08/2019 - [0] DC -- C:\Users\ericl\AppData\Local\NVIDIA =>.nVidia Corporation

O43 - CFD: 15/08/2019 - [] DC -- C:\Users\ericl\AppData\Local\NVIDIA Corporation =>.nVidia Corporation

O43 - CFD: 24/04/2019 - [] DC -- C:\Users\ericl\AppData\Local\OneDrive =>.Microsoft Corporation

O43 - CFD: 30/09/2020 - [] DC -- C:\Users\ericl\AppData\Local\Packages =>.Microsoft Corporation

O43 - CFD: 23/07/2020 - [] DC -- C:\Users\ericl\AppData\Local\PackageStaging =>.Apcera

O43 - CFD: 29/09/2020 - [] DC -- C:\Users\ericl\AppData\Local\PlaceholderTileLogoFolder =>.Microsoft Corporation

O43 - CFD: 25/04/2019 - [] DC -- C:\Users\ericl\AppData\Local\Programs =>.Microsoft Corporation

O43 - CFD: 24/04/2019 - [] DC -- C:\Users\ericl\AppData\Local\Publishers =>.Microsoft Corporation

O43 - CFD: 09/08/2019 - [] DC -- C:\Users\ericl\AppData\Local\speech =>.Microsoft Corporation

O43 - CFD: 17/02/2020 - [] DC -- C:\Users\ericl\AppData\Local\SquirrelTemp =>.Squirrels

O43 - CFD: 30/09/2020 - [] D -- C:\Users\ericl\AppData\Local\Temp =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [0] SHD -- C:\Users\ericl\AppData\Local\Temporary Internet Files =>.Microsoft Corporation

O43 - CFD: 14/02/2020 - [] DC -- C:\Users\ericl\AppData\Local\VirtualStore =>.Microsoft Corporation

O43 - CFD: 30/09/2020 - [] D -- C:\Users\ericl\AppData\Local\ZHP =>.Nicolas Coolman

O43 - CFD: 25/04/2019 - [0] DC -- C:\Users\ericl\AppData\Local\Programs\Common =>.Microsoft Corporation

O43 - CFD: 03/05/2019 - [] DC -- C:\Users\ericl\AppData\LocalLow\Adobe =>.Adobe

O43 - CFD: 24/04/2019 - [] DC -- C:\Users\ericl\AppData\LocalLow\BubblesPop

O43 - CFD: 24/04/2019 - [0] DC -- C:\Users\ericl\AppData\LocalLow\Inj

O43 - CFD: 24/04/2019 - [] SDC -- C:\Users\ericl\AppData\LocalLow\Microsoft =>.Microsoft Corporation

O43 - CFD: 24/04/2019 - [] DC -- C:\Users\ericl\AppData\LocalLow\MiNiNews

O43 - CFD: 28/07/2020 - [0] DC -- C:\Users\ericl\AppData\LocalLow\Mozilla =>.Mozilla Corporation

O43 - CFD: 24/04/2019 - [] DC -- C:\Users\ericl\AppData\LocalLow\SHSoft

O43 - CFD: 22/07/2019 - [] DC -- C:\Users\ericl\AppData\LocalLow\Temp =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] RD -- C:\Users\ericl\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility =>.Microsoft Corporation

O43 - CFD: 23/07/2020 - [] RD -- C:\Users\ericl\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories =>.Microsoft Corporation

O43 - CFD: 23/07/2020 - [] RDC -- C:\Users\ericl\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools =>.Administrative Tools

O43 - CFD: 22/07/2020 - [] DC -- C:\Users\ericl\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Applications Chrome =>.Google Inc.

O43 - CFD: 22/07/2020 - [] DC -- C:\Users\ericl\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\HP Office Print

O43 - CFD: 07/12/2019 - [] D -- C:\Users\ericl\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance =>.Microsoft Corporation

O43 - CFD: 05/05/2019 - [0] DC -- C:\Users\ericl\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Microsoft Corporation =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] DC -- C:\Users\ericl\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\MindFusion XML Viewer

O43 - CFD: 23/07/2020 - [] RDC -- C:\Users\ericl\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] RD -- C:\Users\ericl\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] D -- C:\Users\ericl\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Windows PowerShell =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [] DC -- C:\Users\ericl\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Zoom =>.ZOOM

O43 - CFD: 22/07/2020 - [0] SHD -- C:\Users\Default\AppData\Local\Application Data =>.Microsoft Corporation

O43 - CFD: 12/01/2020 - [] D -- C:\Users\Default\AppData\Local\Google =>.Google

O43 - CFD: 02/09/2019 - [0] SHD -- C:\Users\Default\AppData\Local\Historique =>.Microsoft Corporation

O43 - CFD: 07/12/2019 - [] D -- C:\Users\Default\AppData\Local\Microsoft =>.Microsoft Corporation

O43 - CFD: 07/12/2019 - [0] D -- C:\Users\Default\AppData\Local\Temp =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [0] SHD -- C:\Users\Default\AppData\Local\Temporary Internet Files =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [0] SHD -- C:\Users\Default User\AppData\Local\Application Data =>.Microsoft Corporation

O43 - CFD: 12/01/2020 - [] D -- C:\Users\Default User\AppData\Local\Google =>.Google

O43 - CFD: 02/09/2019 - [0] SHD -- C:\Users\Default User\AppData\Local\Historique =>.Microsoft Corporation

O43 - CFD: 07/12/2019 - [] D -- C:\Users\Default User\AppData\Local\Microsoft =>.Microsoft Corporation

O43 - CFD: 07/12/2019 - [0] D -- C:\Users\Default User\AppData\Local\Temp =>.Microsoft Corporation

O43 - CFD: 22/07/2020 - [0] SHD -- C:\Users\Default User\AppData\Local\Temporary Internet Files =>.Microsoft Corporation

O43 - CFD: 12/08/2020 - [] -- C:\WINDOWS\System32\Config\systemprofile\AppData\Local\Adobe =>.Adobe

O43 - CFD: 24/07/2020 - [] -- C:\WINDOWS\System32\Config\systemprofile\AppData\Local\Dropbox =>.Dropbox

O43 - CFD: 22/07/2020 - [] D -- C:\WINDOWS\System32\Config\systemprofile\AppData\Local\Microsoft =>.Microsoft Corporation

O43 - CFD: 23/07/2020 - [] -- C:\WINDOWS\System32\Config\systemprofile\AppData\Roaming\Dropbox =>.Dropbox

O43 - CFD: 23/07/2020 - [] D -- C:\WINDOWS\System32\Config\systemprofile\AppData\Roaming\Microsoft =>.Microsoft Corporation

**---\ ShellIconOverlayIdentifiers (SIOI) (14) - 0s**

O106 - SIOI: DropboxExt1 Class [ DropboxExt01] - {FB314ED9-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.45.0.dll =>.Dropbox, Inc®

O106 - SIOI: DropboxExt7 Class [ DropboxExt02] - {FB314EDF-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.45.0.dll =>.Dropbox, Inc®

O106 - SIOI: DropboxExt9 Class [ DropboxExt03] - {FB314EE1-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.45.0.dll =>.Dropbox, Inc®

O106 - SIOI: DropboxExt3 Class [ DropboxExt04] - {FB314EDB-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.45.0.dll =>.Dropbox, Inc®

O106 - SIOI: DropboxExt2 Class [ DropboxExt05] - {FB314EDA-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.45.0.dll =>.Dropbox, Inc®

O106 - SIOI: DropboxExt4 Class [ DropboxExt06] - {FB314EDC-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.45.0.dll =>.Dropbox, Inc®

O106 - SIOI: DropboxExt5 Class [ DropboxExt07] - {FB314EDD-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.45.0.dll =>.Dropbox, Inc®

O106 - SIOI: DropboxExt8 Class [ DropboxExt08] - {FB314EE0-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.45.0.dll =>.Dropbox, Inc®

O106 - SIOI: DropboxExt10 Class [ DropboxExt09] - {FB314EE2-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.45.0.dll =>.Dropbox, Inc®

O106 - SIOI: DropboxExt6 Class [ DropboxExt10] - {FB314EDE-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.45.0.dll =>.Dropbox, Inc®

O106 - SIOI: [ GoogleDriveBlacklisted] - {81539FE6-33C7-4CE7-90C7-1C7B8F2F2D42}. (.Google - Google Drive shell extension.) -- C:\Program Files\Google\Drive\googledrivesync64.dll =>.Google LLC®

O106 - SIOI: [ GoogleDriveSynced] - {81539FE6-33C7-4CE7-90C7-1C7B8F2F2D40}. (.Google - Google Drive shell extension.) -- C:\Program Files\Google\Drive\googledrivesync64.dll =>.Google LLC®

O106 - SIOI: [ GoogleDriveSyncing] - {81539FE6-33C7-4CE7-90C7-1C7B8F2F2D41}. (.Google - Google Drive shell extension.) -- C:\Program Files\Google\Drive\googledrivesync64.dll =>.Google LLC®

O106 - SIOI: [EnhancedStorageShell] - {D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}. (.Microsoft Corporation - DLL d’extension d’environnement de stockage.) -- C:\Windows\System32\EhStorShell.dll [Unsigned] =>.Microsoft Corporation

**---\ RACCOURCIS DES MENUS CONTEXTUELS (SCMH) (34) - 2s**

O108 - CMH1: DropboxExt [64Bits] - {ECD97DE5-3C8F-4ACB-AEEE-CCAB78F7711C} . (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.45.0.dll =>.Dropbox, Inc®

O108 - CMH1: EPP [64Bits] - {09A47860-11B0-4DA5-AFA5-26D86198A780} . (.Microsoft Corporation - Extension Microsoft Security Client Shell.) -- C:\Program Files\Windows Defender\shellext.dll =>.Microsoft®

O108 - CMH1: GDContextMenu [64Bits] - {BB02B294-8425-42E5-983F-41A1FA970CD6} . (.Google - Google Drive shell extension.) -- C:\Program Files\Google\Drive\contextmenu64.dll =>.Google LLC®

O108 - CMH1: ModernSharing [64Bits] - {e2bf9676-5f8f-435c-97eb-11607a5bedf7} . (.Microsoft Corporation - Extensions de l’interpréteur de commandes p.) -- C:\Windows\System32\ntshrui.dll [Unsigned] =>.Microsoft Corporation

O108 - CMH1: Open With [64Bits] - {09799AFB-AD67-11d1-ABCD-00C04FC30936} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\Windows\System32\shell32.dll =>.Microsoft®

O108 - CMH1: Open With EncryptionMenu [64Bits] - {A470F8CF-A1E8-4f65-8335-227475AA5C46} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\Windows\System32\shell32.dll =>.Microsoft®

O108 - CMH1: Sharing [64Bits] - {f81e9010-6ea4-11ce-a7ff-00aa003ca9f6} . (.Microsoft Corporation - Extensions de l’interpréteur de commandes p.) -- C:\Windows\System32\ntshrui.dll [Unsigned] =>.Microsoft Corporation

O108 - CMH1: WorkFolders [64Bits] - {E61BF828-5E63-4287-BEF1-60B1A4FDE0E3} . (.Microsoft Corporation - Extension d’environnement de Dossiers de tr.) -- C:\Windows\System32\WorkfoldersShell.dll [Unsigned] =>.Microsoft Corporation

O108 - CMH2: DropboxExt [64Bits] - {ECD97DE5-3C8F-4ACB-AEEE-CCAB78F7711C} . (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.45.0.dll =>.Dropbox, Inc®

O108 - CMH2: GDContextMenu [64Bits] - {BB02B294-8425-42E5-983F-41A1FA970CD6} . (.Google - Google Drive shell extension.) -- C:\Program Files\Google\Drive\contextmenu64.dll =>.Google LLC®

O108 - CMH2: NvAppShExt [64Bits] - {A929C4CE-FD36-4270-B4F5-34ECAC5BD63C} . (.NVIDIA Corporation - NVIDIA Shell Extensions.) -- C:\WINDOWS\system32\nv3dappshext.dll [Unsigned] =>.NVIDIA Corporation

O108 - CMH2: OpenContainingFolderMenu [64Bits] - {37ea3a21-7493-4208-a011-7f9ea79ce9f5} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\Windows\System32\shell32.dll =>.Microsoft®

O108 - CMH2: OpenGLShExt [64Bits] - {E97DEC16-A50D-49bb-AE24-CF682282E08D} . (.NVIDIA Corporation - NVIDIA Shell Extensions.) -- C:\WINDOWS\system32\nv3dappshext.dll [Unsigned] =>.NVIDIA Corporation

O108 - CMH3: CopyAsPathMenu [64Bits] - {f3d06e7c-1e45-4a26-847e-f9fcdee59be0} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\Windows\System32\shell32.dll =>.Microsoft®

O108 - CMH3: MBAMShlExt [64Bits] - {57CE581A-0CB6-4266-9CA0-19364C90A0B3} . (.Malwarebytes - Malwarebytes.) -- C:\Program Files\Malwarebytes\Anti-Malware\mbshlext.dll =>.Malwarebytes Corporation®

O108 - CMH3: SendTo [64Bits] - {7BA4C740-9E81-11CF-99D3-00AA004AE837} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\Windows\System32\shell32.dll =>.Microsoft®

O108 - CMH4: DropboxExt [64Bits] - {ECD97DE5-3C8F-4ACB-AEEE-CCAB78F7711C} . (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.45.0.dll =>.Dropbox, Inc®

O108 - CMH4: EncryptionMenu [64Bits] - {A470F8CF-A1E8-4f65-8335-227475AA5C46} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\Windows\System32\shell32.dll =>.Microsoft®

O108 - CMH4: EPP [64Bits] - {09A47860-11B0-4DA5-AFA5-26D86198A780} . (.Microsoft Corporation - Extension Microsoft Security Client Shell.) -- C:\Program Files\Windows Defender\shellext.dll =>.Microsoft®

O108 - CMH4: GDContextMenu [64Bits] - {BB02B294-8425-42E5-983F-41A1FA970CD6} . (.Google - Google Drive shell extension.) -- C:\Program Files\Google\Drive\contextmenu64.dll =>.Google LLC®

O108 - CMH4: Sharing [64Bits] - {f81e9010-6ea4-11ce-a7ff-00aa003ca9f6} . (.Microsoft Corporation - Extensions de l’interpréteur de commandes p.) -- C:\Windows\System32\ntshrui.dll [Unsigned] =>.Microsoft Corporation

O108 - CMH4: WorkFolders [64Bits] - {E61BF828-5E63-4287-BEF1-60B1A4FDE0E3} . (.Microsoft Corporation - Extension d’environnement de Dossiers de tr.) -- C:\Windows\System32\WorkfoldersShell.dll [Unsigned] =>.Microsoft Corporation

O108 - CMH5: DropboxExt [64Bits] - {ECD97DE5-3C8F-4ACB-AEEE-CCAB78F7711C} . (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.45.0.dll =>.Dropbox, Inc®

O108 - CMH5: igfxDTCM [64Bits] - {9B5F5829-A529-4B12-814A-E81BCB8D93FC} . (.Intel Corporation - igfxDTCM Module.) -- C:\Windows\System32\DriverStore\FileRepository\igdlh64.inf\_amd64\_c8634ed19e331cda\igfxDTCM.dll =>.Microsoft Windows Hardware Compatibility Publisher®

O108 - CMH5: New [64Bits] - {D969A300-E7FF-11d0-A93B-00A0C90F2719} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\Windows\System32\shell32.dll =>.Microsoft®

O108 - CMH5: NvCplDesktopContext [64Bits] - {3D1975AF-48C6-4f8e-A182-BE0E08FA86A9} . (.NVIDIA Corporation - NVIDIA Display Shell Extension.) -- C:\WINDOWS\System32\nvshext.dll [Unsigned] =>.NVIDIA Corporation

O108 - CMH5: Sharing [64Bits] - {f81e9010-6ea4-11ce-a7ff-00aa003ca9f6} . (.Microsoft Corporation - Extensions de l’interpréteur de commandes p.) -- C:\Windows\System32\ntshrui.dll [Unsigned] =>.Microsoft Corporation

O108 - CMH5: WorkFolders [64Bits] - {E61BF828-5E63-4287-BEF1-60B1A4FDE0E3} . (.Microsoft Corporation - Extension d’environnement de Dossiers de tr.) -- C:\Windows\System32\WorkfoldersShell.dll [Unsigned] =>.Microsoft Corporation

O108 - CMH6: Library Location [64Bits] - {3dad6c5d-2167-4cae-9914-f99e41c12cfa} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\Windows\System32\shell32.dll =>.Microsoft®

O108 - CMH6: MBAMShlExt [64Bits] - {57CE581A-0CB6-4266-9CA0-19364C90A0B3} . (.Malwarebytes - Malwarebytes.) -- C:\Program Files\Malwarebytes\Anti-Malware\mbshlext.dll =>.Malwarebytes Corporation®

O108 - CMH6: PintoStartScreen [64Bits] - {470C0EBD-5D73-4d58-9CED-E91E22E23282} . (.Microsoft Corporation - Programme de résolution d’applications.) -- C:\Windows\System32\appresolver.dll =>.Microsoft®

O108 - CMH7: EnhancedStorageShell [64Bits] - {2854F705-3548-414C-A113-93E27C808C85} . (.Microsoft Corporation - DLL d’extension d’environnement de stockage.) -- C:\Windows\System32\EhStorShell.dll [Unsigned] =>.Microsoft Corporation

O108 - CMH7: EPP [64Bits] - {09A47860-11B0-4DA5-AFA5-26D86198A780} . (.Microsoft Corporation - Extension Microsoft Security Client Shell.) -- C:\Program Files\Windows Defender\shellext.dll =>.Microsoft®

O108 - CMH7: Sharing [64Bits] - {f81e9010-6ea4-11ce-a7ff-00aa003ca9f6} . (.Microsoft Corporation - Extensions de l’interpréteur de commandes p.) -- C:\Windows\System32\ntshrui.dll [Unsigned] =>.Microsoft Corporation

**---\ IMAGE FILE EXECUTION OPTIONS (IFEO) (10) - 1s**

O50 - IFEO:C:\WINDOWS\System32\ie4uinit.exe - (.Microsoft Corporation - Utilitaire d'initialisation d'Internet Expl.) [MitigationOptions\\256] [Unsigned] =>.Microsoft Corporation

O50 - IFEO:C:\Windows\System32\ieUnatt.exe - (.Microsoft Corporation - Outil d’installation sans assistance d’IE 7.) [MitigationOptions\\256] [Unsigned] =>.Microsoft Corporation

O50 - IFEO:C:\WINDOWS\System32\MRT.exe - (.Microsoft Corporation - Outil de suppression de logiciels malveilla.) [CFGOptions\\1] [Unsigned] =>.Microsoft Corporation

O50 - IFEO:C:\Windows\System32\msfeedssync.exe - (.Microsoft Corporation - Microsoft Feeds Synchronization.) [MitigationOptions\\256] [Unsigned] =>.Microsoft Corporation

O50 - IFEO:C:\Windows\System32\mshta.exe - (.Microsoft Corporation - Hôte des applications HTML de Microsoft(R).) [MitigationOptions\\256] [Unsigned] =>.Microsoft Corporation

O50 - IFEO:C:\Windows\System32\PresentationHost.exe - (.Microsoft Corporation - Windows Presentation Foundation Host.) [MitigationOptions\\1118481] [Unsigned] =>.Microsoft Corporation

O50 - IFEO:C:\WINDOWS\System32\PrintIsolationHost.exe - (.Microsoft Corporation - PrintIsolationHost.) [MitigationOptions\\2097152] [Unsigned] =>.Microsoft Corporation

O50 - IFEO:C:\WINDOWS\System32\runtimebroker.exe - (.Microsoft Corporation - Runtime Broker.) [MitigationOptions\\4294967296] [Unsigned] =>.Microsoft Corporation

O50 - IFEO:C:\WINDOWS\System32\spoolsv.exe - (.Microsoft Corporation - Application sous-système spouleur.) [MitigationOptions\\2097152] [Unsigned] =>.Microsoft Corporation

O50 - IFEO:C:\Windows\System32\svchost.exe - (.Microsoft Corporation - Processus hôte pour les services Windows.) [MinimumStackCommitInBytes\\32768] =>.Microsoft®

**---\ LISTE DES PILOTES DU SYSTÈME (434) - 19s**

O58 - SDL:2019/12/07 11:07:53 A . (.Microsoft Corporation - 1394 OpenHCI Driver.) -- C:\WINDOWS\System32\drivers\1394ohci.sys [266240] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:53 A . (.LSI - LSI 3ware SCSI Storport Driver.) -- C:\WINDOWS\System32\drivers\3ware.sys [107320] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:24 A . (.Microsoft Corporation - Pilote ACPI pour NT.) -- C:\WINDOWS\System32\drivers\acpi.sys [809280] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - ACPI ALS Sensor Lower Filter Driver.) -- C:\WINDOWS\System32\drivers\acpials.sys [13312] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:53 A . (.Microsoft Corporation - ACPI Devices Driver.) -- C:\WINDOWS\System32\drivers\AcpiDev.sys [23040] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:09 A . (.Microsoft Corporation - ACPIEx Driver.) -- C:\WINDOWS\System32\drivers\acpiex.sys [139792] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - ACPI Processor Aggregator Device Driver.) -- C:\WINDOWS\System32\drivers\acpipagr.sys [14336] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:50 A . (.Microsoft Corporation - ACPI Power Metering Driver.) -- C:\WINDOWS\System32\drivers\acpipmi.sys [18432] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - ACPI Wake Alarm.) -- C:\WINDOWS\System32\drivers\acpitime.sys [16384] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:09 A . (.Microsoft Corporation - Audio KMDF Class Extension.) -- C:\WINDOWS\System32\drivers\Acx01000.sys [415232] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:53 A . (.PMC-Sierra - PMC-Sierra Storport Driver For SPC8x6G SAS.) -- C:\WINDOWS\System32\drivers\adp80xx.sys [1135416] =>.Microsoft®

O58 - SDL:2020/09/10 19:31:02 A . (.Microsoft Corporation - Pilote de fonction connexe pour WinSock.) -- C:\WINDOWS\System32\drivers\afd.sys [647480] =>.Microsoft®

O58 - SDL:2020/09/10 19:31:06 A . (.Microsoft Corporation - AF\_UNIX socket provider.) -- C:\WINDOWS\System32\drivers\afunix.sys [41984] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:31:07 A . (.Microsoft Corporation - Gestionnaire d'appels RAS Agile Vpn Minipor.) -- C:\WINDOWS\System32\drivers\agilevpn.sys [113152] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:58 A . (.Microsoft Corporation - Application Compatibility Cache.) -- C:\WINDOWS\System32\drivers\ahcache.sys [292864] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:47 A . (.Advanced Micro Devices, Inc - AMD GPIO Controller Driver.) -- C:\WINDOWS\System32\drivers\amdgpio2.sys [18432] [Unsigned] =>.Advanced Micro Devices, Inc

O58 - SDL:2019/12/07 11:07:47 A . (.Advanced Micro Devices, Inc - AMD I2C Controller Driver.) -- C:\WINDOWS\System32\drivers\amdi2c.sys [45568] [Unsigned] =>.Advanced Micro Devices, Inc

O58 - SDL:2019/12/07 11:07:53 A . (.Microsoft Corporation - Processor Device Driver.) -- C:\WINDOWS\System32\drivers\amdk8.sys [207160] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.Microsoft Corporation - Processor Device Driver.) -- C:\WINDOWS\System32\drivers\amdppm.sys [211472] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.Advanced Micro Devices - AHCI 1.3 Device Driver.) -- C:\WINDOWS\System32\drivers\amdsata.sys [83256] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.AMD Technologies Inc. - AMD Technology AHCI Compatible Controller D.) -- C:\WINDOWS\System32\drivers\amdsbs.sys [259384] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.Advanced Micro Devices - Storage Filter Driver.) -- C:\WINDOWS\System32\drivers\amdxata.sys [26936] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:58 A . (.Microsoft Corporation - AppID Driver.) -- C:\WINDOWS\System32\drivers\appid.sys [208696] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:58 A . (.Microsoft Corporation - Applocker Filter.) -- C:\WINDOWS\System32\drivers\applockerfltr.sys [18432] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:53 A . (.PMC-Sierra, Inc. - Adaptec SAS RAID WS03 Driver.) -- C:\WINDOWS\System32\drivers\arcsas.sys [131896] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:07 A . (.Microsoft Corporation - MS Remote Access serial network driver.) -- C:\WINDOWS\System32\drivers\asyncmac.sys [31232] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:30:24 A . (.Microsoft Corporation - ATAPI IDE Miniport Driver.) -- C:\WINDOWS\System32\drivers\atapi.sys [30024] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:24 A . (.Microsoft Corporation - ATAPI Driver Extension.) -- C:\WINDOWS\System32\drivers\ataport.sys [223040] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:41 A . (.Microsoft Corporation - BAM Kernel Driver.) -- C:\WINDOWS\System32\drivers\bam.sys [78136] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - Battery Class Driver.) -- C:\WINDOWS\System32\drivers\battc.sys [41272] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:47 A . (. - BCM Function 2 Device Driver.) -- C:\WINDOWS\System32\drivers\bcmfn2.sys [9728] [Unsigned] =>.Broadcom Corporation

O58 - SDL:2019/12/07 11:09:00 A . (.Microsoft Corporation - BEEP Driver.) -- C:\WINDOWS\System32\drivers\beep.sys [10240] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/07/22 22:17:23 A . (.Microsoft Corporation - Windows Bind Filter Driver.) -- C:\WINDOWS\System32\drivers\bindflt.sys [143160] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:12 A . (.Microsoft Corporation - NT Lan Manager Datagram Receiver Driver.) -- C:\WINDOWS\System32\drivers\bowser.sys [117760] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:39 A . (.Microsoft Corporation - MAC Bridge Driver.) -- C:\WINDOWS\System32\drivers\bridge.sys [127488] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:47 A . (.Microsoft Corporation - Microsoft Bluetooth Audio Multiprofile Mana.) -- C:\WINDOWS\System32\drivers\BtaMPM.sys [36352] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:30:23 A . (.Microsoft Corporation - Bluetooth A2DP Driver.) -- C:\WINDOWS\System32\drivers\BthA2dp.sys [279040] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:30:24 A . (.Microsoft Corporation - Extension de bus Bluetooth.) -- C:\WINDOWS\System32\drivers\bthenum.sys [113664] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:47 A . (.Microsoft Corporation - Bluetooth Hands-free Audio Device Driver.) -- C:\WINDOWS\System32\drivers\BthHfAud.sys [65536] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:47 A . (.Microsoft Corporation - Bluetooth Hands-Free Audio and Call Control.) -- C:\WINDOWS\System32\drivers\BthHfEnum.sys [144896] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:30:24 A . (.Microsoft Corporation - Bluetooth Transport Extensibility Miniport.) -- C:\WINDOWS\System32\drivers\BthMini.SYS [45568] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:50 A . (.Microsoft Corporation - Bluetooth Communications Driver.) -- C:\WINDOWS\System32\drivers\bthmodem.sys [76800] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Bluetooth Personal Area Networking.) -- C:\WINDOWS\System32\drivers\bthpan.sys [133632] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:30:24 A . (.Microsoft Corporation - Pilote de bus Bluetooth.) -- C:\WINDOWS\System32\drivers\bthport.sys [1548288] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:30:24 A . (.Microsoft Corporation - Pilote de Miniport Bluetooth.) -- C:\WINDOWS\System32\drivers\BTHUSB.SYS [110592] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - VHD BTT Filter Driver.) -- C:\WINDOWS\System32\drivers\bttflt.sys [43832] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Button Converter Driver.) -- C:\WINDOWS\System32\drivers\buttonconverter.sys [44032] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:50 A . (.QLogic Corporation - QLogic Gigabit Ethernet VBD.) -- C:\WINDOWS\System32\drivers\bxvbda.sys [533816] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:47 A . (.Microsoft Corporation - Charge Arbiration Driver.) -- C:\WINDOWS\System32\drivers\CAD.sys [66576] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:37 A . (.Microsoft Corporation - CD-ROM File System Driver.) -- C:\WINDOWS\System32\drivers\cdfs.sys [100864] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:53 A . (.Microsoft Corporation - SCSI CD-ROM Driver.) -- C:\WINDOWS\System32\drivers\cdrom.sys [174080] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:33 A . (.Microsoft Corporation - Event Aggregation Kernel Mode Library.) -- C:\WINDOWS\System32\drivers\CEA.sys [81720] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Chelsio Communications - Chelsio iSCSI Crash Dump Driver.) -- C:\WINDOWS\System32\drivers\cht4dx64.sys [144184] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Chelsio Communications - Chelsio iSCSI VMiniport Driver.) -- C:\WINDOWS\System32\drivers\cht4sx64.sys [319800] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Chelsio Communications - VF library for Chelsio ® T5/T6 Chipset.) -- C:\WINDOWS\System32\drivers\cht4vfx.sys [28672] [Unsigned] =>.Chelsio Communications

O58 - SDL:2019/12/07 11:07:54 A . (.Chelsio Communications - Virtual Bus Driver for Chelsio ® T5/T6 Chip.) -- C:\WINDOWS\System32\drivers\cht4vx64.sys [1853752] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:34 A . (...) -- C:\WINDOWS\System32\drivers\cimfs.sys [91136] [Unsigned]

O58 - SDL:2019/12/07 11:07:50 A . (.Microsoft Corporation - Consumer IR Class Driver for eHome.) -- C:\WINDOWS\System32\drivers\circlass.sys [52224] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:49 A . (.Microsoft Corporation - SCSI Class System Dll.) -- C:\WINDOWS\System32\drivers\Classpnp.sys [417080] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:58 A . (.Microsoft Corporation - Cloud Files Mini Filter Driver.) -- C:\WINDOWS\System32\drivers\cldflt.sys [491520] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:31:03 A . (.Microsoft Corporation - Common Log File System Driver.) -- C:\WINDOWS\System32\drivers\clfs.sys [403768] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:37 A . (.Microsoft Corporation - CLIP Service.) -- C:\WINDOWS\System32\drivers\ClipSp.sys [1089344] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - Control Method Battery Driver.) -- C:\WINDOWS\System32\drivers\CmBatt.sys [36864] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:09 A . (.Microsoft Corporation - Noyau Gestionnaire de configuration Configu.) -- C:\WINDOWS\System32\drivers\cmimcext.sys [28984] =>.Microsoft®

O58 - SDL:2020/07/22 22:17:31 A . (.Microsoft Corporation - Kernel Cryptography, Next Generation.) -- C:\WINDOWS\System32\drivers\cng.sys [732432] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:37 A . (.Microsoft Corporation - CNG Hardware Assist algorithm provider.) -- C:\WINDOWS\System32\drivers\cnghwassist.sys [40968] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:34 A . (.Microsoft Corporation - Console Driver.) -- C:\WINDOWS\System32\drivers\condrv.sys [58168] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:49 A . (.Microsoft Corporation - Crash Dump Driver.) -- C:\WINDOWS\System32\drivers\crashdmp.sys [99368] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:41 A . (.Microsoft Corporation - DAM Kernel Driver.) -- C:\WINDOWS\System32\drivers\dam.sys [97080] =>.Microsoft®

O58 - SDL:2020/09/22 20:59:38 A . (.Dropbox, Inc. - Dropbox Filter Driver.) -- C:\WINDOWS\System32\drivers\dbx-canary.sys [47600] =>.Microsoft®

O58 - SDL:2020/09/22 20:59:38 A . (.Dropbox, Inc. - Dropbox Filter Driver.) -- C:\WINDOWS\System32\drivers\dbx-dev.sys [47600] =>.Microsoft®

O58 - SDL:2020/09/22 20:59:38 A . (.Dropbox, Inc. - Dropbox Filter Driver.) -- C:\WINDOWS\System32\drivers\dbx-stable.sys [47600] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:47 A . (.Microsoft Corporation - Xbox Device Authentication Driver.) -- C:\WINDOWS\System32\drivers\devauthe.sys [47104] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:51 A . (.Microsoft Corporation - DFS Namespace Client Driver.) -- C:\WINDOWS\System32\drivers\dfsc.sys [152064] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:53 A . (.Microsoft Corporation - PnP Disk Driver.) -- C:\WINDOWS\System32\drivers\disk.sys [98856] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:52 A . (.Microsoft Corporation - Crash Dump Disk Driver.) -- C:\WINDOWS\System32\drivers\Diskdump.sys [38200] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:52 A . (.Microsoft Corporation - Boot Over USB Dump Driver.) -- C:\WINDOWS\System32\drivers\Dmpusbstor.sys [15360] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:57 A . (.Microsoft Corporation - Mémoire dynamique.) -- C:\WINDOWS\System32\drivers\dmvsc.sys [59192] =>.Microsoft®

O58 - SDL:2017/11/08 21:40:26 A . (.Intel Corporation - DPTF ACPI Device (64-Bit).) -- C:\WINDOWS\System32\drivers\dptf\_acpi.sys [74144] =>.Intel Corporation®

O58 - SDL:2017/11/08 21:40:30 A . (.Intel Corporation - DPTF CPU Device (64-Bit).) -- C:\WINDOWS\System32\drivers\dptf\_cpu.sys [69536] =>.Intel Corporation®

O58 - SDL:2019/12/07 11:07:50 A . (.Microsoft Corporation - Microsoft Trusted Audio Drivers.) -- C:\WINDOWS\System32\drivers\drmk.sys [97792] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:50 A . (.Microsoft Corporation - Microsoft Trusted Audio Drivers.) -- C:\WINDOWS\System32\drivers\drmkaud.sys [16136] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:46 A . (.Microsoft Corporation - ATAPI Dump Driver.) -- C:\WINDOWS\System32\drivers\Dumpata.sys [37392] =>.Microsoft®

O58 - SDL:2019/12/07 16:53:00 A . (.Microsoft Corporation - Bitlocker Drive Encryption Crashdump Filter.) -- C:\WINDOWS\System32\drivers\dumpfve.sys [93312] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:25 A . (.Microsoft Corporation - SD Crashdump Port Driver.) -- C:\WINDOWS\System32\drivers\dumpsd.sys [195896] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:37 A . (.Microsoft Corporation - SD Host Controller Crashdump Port Driver.) -- C:\WINDOWS\System32\drivers\dumpsdport.sys [32768] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:52 A . (.Microsoft Corporation - Storport Dump Driver.) -- C:\WINDOWS\System32\drivers\Dumpstorport.sys [35128] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:37 A . (.Microsoft Corporation - DirectX Graphics Kernel.) -- C:\WINDOWS\System32\drivers\dxgkrnl.sys [3779384] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:37 A . (.Microsoft Corporation - DirectX Graphics MMS.) -- C:\WINDOWS\System32\drivers\dxgmms1.sys [454960] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:37 A . (.Microsoft Corporation - DirectX Graphics MMS.) -- C:\WINDOWS\System32\drivers\dxgmms2.sys [903992] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:37 A . (.Microsoft Corporation - Enhanced Storage Class driver for IEEE 1667.) -- C:\WINDOWS\System32\drivers\EhStorClass.sys [95032] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:50 A . (.Microsoft Corporation - Microsoft driver for storage devices suppor.) -- C:\WINDOWS\System32\drivers\EhStorTcgDrv.sys [124728] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - Error Device Driver.) -- C:\WINDOWS\System32\drivers\errdev.sys [15872] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2017/11/08 21:40:36 A . (.Intel Corporation - DPTF Zone (64-Bit).) -- C:\WINDOWS\System32\drivers\esif\_lf.sys [382880] =>.Intel Corporation®

O58 - SDL:2019/12/07 11:07:50 A . (.QLogic Corporation - QLogic 10 GigE VBD.) -- C:\WINDOWS\System32\drivers\evbda.sys [3418936] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:05 A . (.Microsoft Corporation - Microsoft Extended FAT File System.) -- C:\WINDOWS\System32\drivers\exfat.sys [415032] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:05 A . (.Microsoft Corporation - Fast FAT File System Driver.) -- C:\WINDOWS\System32\drivers\fastfat.sys [425272] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - Floppy Disk Controller Driver.) -- C:\WINDOWS\System32\drivers\fdc.sys [34816] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:09 A . (.Microsoft Corporation - Windows sandboxing and encryption filter.) -- C:\WINDOWS\System32\drivers\filecrypt.sys [59392] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:46 A . (.Microsoft Corporation - FileInfo Filter Driver.) -- C:\WINDOWS\System32\drivers\fileinfo.sys [94736] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:46 A . (.Microsoft Corporation - File Trace Filter Driver.) -- C:\WINDOWS\System32\drivers\filetrace.sys [40448] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - Floppy Driver.) -- C:\WINDOWS\System32\drivers\flpydisk.sys [28672] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/07/22 22:17:31 A . (.Microsoft Corporation - Gestionnaire de filtres de système de fichi.) -- C:\WINDOWS\System32\drivers\fltMgr.sys [430392] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:09 A . (.Microsoft Corporation - File System Dependency Manager Mini Filter.) -- C:\WINDOWS\System32\drivers\fsdepends.sys [68408] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:49 A . (.Microsoft Corporation - File System Recognizer Driver.) -- C:\WINDOWS\System32\drivers\fs\_rec.sys [33592] =>.Microsoft®

O58 - SDL:2019/12/07 16:53:00 A . (.Microsoft Corporation - BitLocker Drive Encryption Driver.) -- C:\WINDOWS\System32\drivers\fvevol.sys [800784] =>.Microsoft®

O58 - SDL:2020/09/10 19:31:02 A . (.Microsoft Corporation - FWP/IPsec Kernel-Mode API.) -- C:\WINDOWS\System32\drivers\FWPKCLNT.SYS [502592] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:05 A . (.Microsoft Corporation - GPU Energy Kernel Driver.) -- C:\WINDOWS\System32\drivers\gpuenergydrv.sys [8704] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:50 A . (.Microsoft Corporation - High Definition Audio Bus Driver.) -- C:\WINDOWS\System32\drivers\hdaudbus.sys [132608] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/07/22 22:17:04 A . (.Microsoft Corporation - High Definition Audio Function Driver.) -- C:\WINDOWS\System32\drivers\HdAudio.sys [430080] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - Hid Battery Driver.) -- C:\WINDOWS\System32\drivers\hidbatt.sys [39440] =>.Microsoft®

O58 - SDL:2020/08/14 10:24:28 A . (.Microsoft Corporation - Pilote de miniport Bluetooth pour les périp.) -- C:\WINDOWS\System32\drivers\hidbth.sys [120320] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Bibliothèque Hid Class.) -- C:\WINDOWS\System32\drivers\hidclass.sys [225792] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - I2C HID Miniport Driver.) -- C:\WINDOWS\System32\drivers\hidi2c.sys [57344] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - HID Button over Interrupt Driver.) -- C:\WINDOWS\System32\drivers\hidinterrupt.sys [55824] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:50 A . (.Microsoft Corporation - Infrared Miniport Driver for Input Devices.) -- C:\WINDOWS\System32\drivers\hidir.sys [48640] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Hid Parsing Library.) -- C:\WINDOWS\System32\drivers\hidparse.sys [46080] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - SPI HID Miniport Driver.) -- C:\WINDOWS\System32\drivers\hidspi.sys [66560] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - USB Miniport Driver for Input Devices.) -- C:\WINDOWS\System32\drivers\hidusb.sys [44032] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:53 A . (.Hewlett-Packard Company - Smart Array SAS/SATA Controller Media Drive.) -- C:\WINDOWS\System32\drivers\HpSAMD.sys [64312] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:49 A . (.Microsoft Corporation - HTTP Pile du protocole.) -- C:\WINDOWS\System32\drivers\http.sys [1567032] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:57 A . (.Microsoft Corporation - Hyper-V Crashdump.) -- C:\WINDOWS\System32\drivers\hvcrash.sys [35128] =>.Microsoft®

O58 - SDL:2020/09/10 19:31:23 A . (.Microsoft Corporation - Hypervisor Boot Driver.) -- C:\WINDOWS\System32\drivers\hvservice.sys [95032] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:51 A . (.Microsoft Corporation - Microsoft Hyper-V Socket Provider.) -- C:\WINDOWS\System32\drivers\hvsocket.sys [147984] =>.Microsoft®

O58 - SDL:2020/08/14 10:25:20 A . (.Microsoft Corporation - Hardware Policy Driver.) -- C:\WINDOWS\System32\drivers\hwpolicy.sys [33096] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:57 A . (.Microsoft Corporation - Microsoft VMBus Synthetic Keyboard Driver.) -- C:\WINDOWS\System32\drivers\hyperkbd.sys [27448] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:57 A . (.Microsoft Corporation - Microsoft VMBus Video Device Miniport Drive.) -- C:\WINDOWS\System32\drivers\HyperVideo.sys [41784] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Pilote de port i8042.) -- C:\WINDOWS\System32\drivers\i8042prt.sys [118272] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:47 A . (.Intel(R) Corporation - Intel(R) Serial IO GPIO Controller Driver.) -- C:\WINDOWS\System32\drivers\iagpio.sys [36352] [Unsigned] =>.Intel(R) Corporation

O58 - SDL:2019/12/07 11:07:47 A . (.Intel(R) Corporation - Intel(R) Serial IO I2C Driver.) -- C:\WINDOWS\System32\drivers\iai2c.sys [91136] [Unsigned] =>.Intel(R) Corporation

O58 - SDL:2019/12/07 11:07:47 A . (.Intel Corporation - Intel(R) Serial IO GPIO Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i\_GPIO2.sys [79360] [Unsigned] =>.Intel Corporation

O58 - SDL:2019/12/07 11:07:47 A . (.Intel Corporation - Intel(R) Serial IO GPIO Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i\_GPIO2\_BXT\_P.sys [93184] [Unsigned] =>.Intel Corporation

O58 - SDL:2019/12/07 11:07:47 A . (.Intel Corporation - Intel(R) Serial IO GPIO Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i\_GPIO2\_CNL.sys [112128] [Unsigned] =>.Intel Corporation

O58 - SDL:2019/12/07 11:07:47 A . (.Intel Corporation - Intel(R) Serial IO GPIO Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i\_GPIO2\_GLK.sys [96256] [Unsigned] =>.Intel Corporation

O58 - SDL:2019/12/07 11:07:47 A . (.Intel Corporation - Intel(R) Serial IO I2C Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i\_I2C.sys [171520] [Unsigned] =>.Intel Corporation

O58 - SDL:2019/12/07 11:07:47 A . (.Intel Corporation - Intel(R) Serial IO I2C Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i\_I2C\_BXT\_P.sys [175104] [Unsigned] =>.Intel Corporation

O58 - SDL:2019/12/07 11:07:47 A . (.Intel Corporation - Intel(R) Serial IO I2C Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i\_I2C\_CNL.sys [177152] [Unsigned] =>.Intel Corporation

O58 - SDL:2019/12/07 11:07:47 A . (.Intel Corporation - Intel(R) Serial IO I2C Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i\_I2C\_GLK.sys [177664] [Unsigned] =>.Intel Corporation

O58 - SDL:2017/11/14 14:46:32 A . (.Intel Corporation - Intel(R) Serial IO SPI Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2\_SPI.sys [158880] =>.Intel(R) Embedded Subsystems and IP Blocks Group®

O58 - SDL:2017/11/14 14:46:38 A . (.Intel Corporation - Intel(R) Serial IO UART Driver.) -- C:\WINDOWS\System32\drivers\iaLPSS2\_UART2.sys [310936] =>.Intel(R) Embedded Subsystems and IP Blocks Group®

O58 - SDL:2019/12/07 11:07:50 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:2019/12/07 11:07:50 A . (.Intel Corporation - Intel(R) Serial IO I2C Controller Driver.) -- C:\WINDOWS\System32\drivers\iaLPSSi\_I2C.sys [113152] [Unsigned] =>.Intel Corporation

O58 - SDL:2019/12/07 11:07:54 A . (.Intel Corporation - Intel(R) Rapid Storage Technology driver (i.) -- C:\WINDOWS\System32\drivers\iaStorAVC.sys [884752] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Intel Corporation - Intel Matrix Storage Manager driver - x64.) -- C:\WINDOWS\System32\drivers\iaStorV.sys [412176] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Mellanox - InfiniBand Fabric Bus Driver.) -- C:\WINDOWS\System32\drivers\ibbus.sys [558904] =>.Microsoft®

O58 - SDL:2018/03/09 11:10:42 A . (.Intel Corporation - Intel(R) Wireless Bluetooth(R) Filter Drive.) -- C:\WINDOWS\System32\drivers\ibtusb.sys [197696] =>.Intel(R) Wireless Connectivity Solutions®

O58 - SDL:2019/12/07 11:08:36 A . (.Microsoft Corporation - Indirect displays kernel-mode filter driver.) -- C:\WINDOWS\System32\drivers\IndirectKmd.sys [47104] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:30:24 A . (.Microsoft Corporation - Intel PCI IDE Driver.) -- C:\WINDOWS\System32\drivers\intelide.sys [19776] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:24 A . (.Microsoft Corporation - Intel Power Engine Plugin.) -- C:\WINDOWS\System32\drivers\intelpep.sys [418800] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:47 A . (.Microsoft Corporation - Intel Power Limit Driver.) -- C:\WINDOWS\System32\drivers\intelpmax.sys [30720] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:53 A . (.Microsoft Corporation - Processor Device Driver.) -- C:\WINDOWS\System32\drivers\intelppm.sys [230712] =>.Microsoft®

O58 - SDL:2020/08/14 10:24:27 A . (.Microsoft Corporation - Intel Telemetry Driver.) -- C:\WINDOWS\System32\drivers\IntelTA.sys [26600] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:05 A . (.Microsoft Corporation - Filtre de contrôle de taux d’E/S.) -- C:\WINDOWS\System32\drivers\iorate.sys [57360] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:07 A . (.Microsoft Corporation - IP FILTER DRIVER.) -- C:\WINDOWS\System32\drivers\ipfltdrv.sys [90112] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - PILOT IPMI WMI.) -- C:\WINDOWS\System32\drivers\IPMIDrv.sys [117560] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:34 A . (.Microsoft Corporation - IP Network Address Translator.) -- C:\WINDOWS\System32\drivers\ipnat.sys [225280] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:09 A . (.Microsoft Corporation - IPT Driver.) -- C:\WINDOWS\System32\drivers\ipt.sys [59704] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - Pilote de bus PNP ISA.) -- C:\WINDOWS\System32\drivers\isapnp.sys [22840] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.Avago Technologies - Avago SAS Gen3.5 Driver (StorPort).) -- C:\WINDOWS\System32\drivers\ItSas35i.sys [172344] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Pilote de la classe Clavier.) -- C:\WINDOWS\System32\drivers\kbdclass.sys [71480] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Pilote de filtre clavier HID.) -- C:\WINDOWS\System32\drivers\kbdhid.sys [46592] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Microsoft Kernel Debugger Network Miniport.) -- C:\WINDOWS\System32\drivers\kdnic.sys [33296] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:27 A . (.Microsoft Corporation - Network Power Dependency Broker.) -- C:\WINDOWS\System32\drivers\KNetPwrDepBroker.sys [32256] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:58 A . (.Microsoft Corporation - Kernel CSA Library.) -- C:\WINDOWS\System32\drivers\ks.sys [449024] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:31:02 A . (.Microsoft Corporation - Kernel Security Support Provider Interface.) -- C:\WINDOWS\System32\drivers\ksecdd.sys [147256] =>.Microsoft®

O58 - SDL:2020/09/10 19:31:00 A . (.Microsoft Corporation - Kernel Security Support Provider Interface.) -- C:\WINDOWS\System32\drivers\ksecpkg.sys [180024] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:58 A . (.Microsoft Corporation - Kernel Streaming WOW Thunk Service.) -- C:\WINDOWS\System32\drivers\ksthunk.sys [29696] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:55 A . (.Microsoft Corporation - Link-Layer Topology Mapper I/O Driver.) -- C:\WINDOWS\System32\drivers\lltdio.sys [72704] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:53 A . (.LSI Corporation - LSI Fusion-MPT SAS Driver (StorPort).) -- C:\WINDOWS\System32\drivers\lsi\_sas.sys [108856] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.LSI Corporation - LSI SAS Gen2 Driver (StorPort).) -- C:\WINDOWS\System32\drivers\lsi\_sas2i.sys [124216] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.Avago Technologies - Avago SAS Gen3 Driver (StorPort).) -- C:\WINDOWS\System32\drivers\lsi\_sas3i.sys [135992] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.LSI Corporation - LSI SSS PCIe/Flash Driver (StorPort).) -- C:\WINDOWS\System32\drivers\lsi\_sss.sys [82744] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:58 A . (.Microsoft Corporation - Pilote de filtre de virtualisation de fichi.) -- C:\WINDOWS\System32\drivers\luafv.sys [140288] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - MA-USB Host Controller Driver.) -- C:\WINDOWS\System32\drivers\mausbhost.sys [537608] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - MA-USB IP Driver.) -- C:\WINDOWS\System32\drivers\mausbip.sys [64016] =>.Microsoft®

O58 - SDL:2020/09/22 09:55:22 A . (.Malwarebytes - Malwarebytes Anti-Exploit.) -- C:\WINDOWS\System32\drivers\mbae64.sys [153312] =>.Malwarebytes Corporation®

O58 - SDL:2020/09/18 15:59:44 A . (.Malwarebytes - Malwarebytes Chameleon.) -- C:\WINDOWS\System32\drivers\MbamChameleon.sys [217592] =>.Malwarebytes Inc®

O58 - SDL:2020/09/22 09:55:22 A . (.Malwarebytes - Malwarebytes Early Launch Anti-Malware Driv.) -- C:\WINDOWS\System32\drivers\MbamElam.sys [19912] =>.Microsoft®

O58 - SDL:2020/09/22 09:55:58 A . (.Malwarebytes - Malwarebytes SwissArmy.) -- C:\WINDOWS\System32\drivers\mbamswissarmy.sys [248968] =>.Malwarebytes Inc®

O58 - SDL:2020/08/14 10:24:29 A . (.Microsoft Corporation - Windows Mobile Broadband Class Extension.) -- C:\WINDOWS\System32\drivers\MbbCx.sys [386048] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:00 A . (.Microsoft Corporation - Medium changer class driver.) -- C:\WINDOWS\System32\drivers\mcd.sys [25088] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:53 A . (.Avago Technologies - MEGASAS RAID Controller Driver for Windows.) -- C:\WINDOWS\System32\drivers\megasas.sys [59704] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.Avago Technologies - MEGASAS RAID Controller Driver for Windows.) -- C:\WINDOWS\System32\drivers\MegaSas2i.sys [81720] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.Avago Technologies - MEGASAS RAID Controller Driver for Windows.) -- C:\WINDOWS\System32\drivers\megasas35i.sys [105480] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.LSI Corporation, Inc. - LSI MegaRAID Software RAID Driver.) -- C:\WINDOWS\System32\drivers\megasr.sys [575800] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:47 A . (.Microsoft Corporation - Pilote de transport Microsoft Bluetooth Avr.) -- C:\WINDOWS\System32\drivers\Microsoft.Bluetooth.AvrcpTransport.sys [65024] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:30:25 A . (.Microsoft Corporation - Legacy Bluetooth LE Bus Enumerator.) -- C:\WINDOWS\System32\drivers\Microsoft.Bluetooth.Legacy.LEEnumerator.sys [106496] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:54 A . (.Mellanox - MLX4 Bus Driver.) -- C:\WINDOWS\System32\drivers\mlx4\_bus.sys [1131320] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:07 A . (.Microsoft Corporation - MMCSS Driver.) -- C:\WINDOWS\System32\drivers\mmcss.sys [53248] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:51 A . (.Microsoft Corporation - Pilote de périphérique modem.) -- C:\WINDOWS\System32\drivers\modem.sys [47104] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:30:24 A . (.Microsoft Corporation - Monitor Driver.) -- C:\WINDOWS\System32\drivers\monitor.sys [80896] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Pilote de la classe Souris.) -- C:\WINDOWS\System32\drivers\mouclass.sys [67600] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Pilote de filtre souris HID.) -- C:\WINDOWS\System32\drivers\mouhid.sys [35328] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:49 A . (.Microsoft Corporation - Gestionnaire des points de montage.) -- C:\WINDOWS\System32\drivers\mountmgr.sys [110392] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:33 A . (.Microsoft Corporation - Microsoft Protection Service Driver.) -- C:\WINDOWS\System32\drivers\mpsdrv.sys [80896] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:54 A . (.Microsoft Corporation - Windows NT WebDav Minirdr.) -- C:\WINDOWS\System32\drivers\mrxdav.sys [157696] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:31:03 A . (.Microsoft Corporation - Minirdr SMB Windows NT.) -- C:\WINDOWS\System32\drivers\mrxsmb.sys [573752] =>.Microsoft®

O58 - SDL:2020/09/10 19:31:03 A . (.Microsoft Corporation - Longhorn SMB 2.0 Redirector.) -- C:\WINDOWS\System32\drivers\mrxsmb20.sys [259888] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:49 A . (.Microsoft Corporation - Mailslot driver.) -- C:\WINDOWS\System32\drivers\msfs.sys [44048] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:38 A . (.Microsoft Corporation - GPIO Class Extension Driver.) -- C:\WINDOWS\System32\drivers\msgpioclx.sys [183112] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - GPIO Button Driver.) -- C:\WINDOWS\System32\drivers\msgpiowin32.sys [56120] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:36 A . (.Microsoft Corporation - Pass-through HID to KMDF Filter Driver.) -- C:\WINDOWS\System32\drivers\mshidkmdf.sys [8192] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:16 A . (.Microsoft Corporation - Pilote direct pour interface HID-UMDF.) -- C:\WINDOWS\System32\drivers\mshidumdf.sys [12288] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:36 A . (.Microsoft Corporation - Hardware Notification Class Extension Drive.) -- C:\WINDOWS\System32\drivers\mshwnclx.sys [30208] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - ISA Driver.) -- C:\WINDOWS\System32\drivers\msisadrv.sys [20280] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - Microsoft iSCSI Initiator Driver.) -- C:\WINDOWS\System32\drivers\msiscsi.sys [292664] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:58 A . (.Microsoft Corporation - MS KS Server.) -- C:\WINDOWS\System32\drivers\mskssrv.sys [34816] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:05 A . (.Microsoft Corporation - Pilote de protocole LLDP (Link Layer Discov.) -- C:\WINDOWS\System32\drivers\mslldp.sys [78848] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:58 A . (.Microsoft Corporation - MS Proxy Clock.) -- C:\WINDOWS\System32\drivers\mspclock.sys [11264] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:58 A . (.Microsoft Corporation - MS Proxy Quality Manager.) -- C:\WINDOWS\System32\drivers\mspqm.sys [11264] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:31:00 A . (.Microsoft Corporation - Windows QUIC Driver.) -- C:\WINDOWS\System32\drivers\msquic.sys [322376] =>.Microsoft®

O58 - SDL:2020/09/10 19:31:02 A . (.Microsoft Corporation - Kernel Remote Procedure Call Provider.) -- C:\WINDOWS\System32\drivers\msrpc.sys [380728] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - System Management BIOS Driver.) -- C:\WINDOWS\System32\drivers\mssmbios.sys [47928] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:58 A . (.Microsoft Corporation - WDM Tee/Communication Transform Filter.) -- C:\WINDOWS\System32\drivers\mstee.sys [12288] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:53 A . (.Microsoft Corporation - Pilote HID multipoint Microsoft.) -- C:\WINDOWS\System32\drivers\MTConfig.sys [17920] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:51 A . (.Microsoft Corporation - Pilote de fournisseur UNC multiples.) -- C:\WINDOWS\System32\drivers\mup.sys [133136] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.Marvell Semiconductor, Inc. - Marvell Flash Controller Driver.) -- C:\WINDOWS\System32\drivers\mvumis.sys [63800] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Mellanox - NetworkDirect Support Filter Driver.) -- C:\WINDOWS\System32\drivers\ndfltr.sys [146232] =>.Microsoft®

O58 - SDL:2020/09/10 19:31:02 A . (.Microsoft Corporation - NDIS (Network Driver Interface Specificatio.) -- C:\WINDOWS\System32\drivers\ndis.sys [1472824] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:48 A . (.Microsoft Corporation - Microsoft NDIS Packet Capture Filter Driver.) -- C:\WINDOWS\System32\drivers\ndiscap.sys [54272] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:05 A . (.Microsoft Corporation - Microsoft Network Adapter Multiplexor.) -- C:\WINDOWS\System32\drivers\NdisImPlatform.sys [135168] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:07 A . (.Microsoft Corporation - NDIS 3.0 connection wrapper driver.) -- C:\WINDOWS\System32\drivers\ndistapi.sys [28672] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:49 A . (.Microsoft Corporation - Pilote d’E/S du mode utilisateur NDIS.) -- C:\WINDOWS\System32\drivers\ndisuio.sys [70656] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:05 A . (.Microsoft Corporation - Énumérateur de cartes réseau virtuelles Mic.) -- C:\WINDOWS\System32\drivers\NdisVirtualBus.sys [23040] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:31:07 A . (.Microsoft Corporation - MS PPP Framing Driver (Strong Encryption).) -- C:\WINDOWS\System32\drivers\ndiswan.sys [206848] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:48 A . (.Microsoft Corporation - RDMA Sample Driver.) -- C:\WINDOWS\System32\drivers\NDKPing.sys [72720] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:07 A . (.Microsoft Corporation - NDIS Proxy.) -- C:\WINDOWS\System32\drivers\ndproxy.sys [93696] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:33 A . (.Microsoft Corporation - Windows Network Data Usage Monitoring Drive.) -- C:\WINDOWS\System32\drivers\Ndu.sys [131584] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:49 A . (.Microsoft Corporation - Network Adapter Class Extension for WDF.) -- C:\WINDOWS\System32\drivers\NetAdapterCx.sys [206336] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:04 A . (.Microsoft Corporation - NetBIOS interface driver.) -- C:\WINDOWS\System32\drivers\netbios.sys [64312] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:05 A . (.Microsoft Corporation - MBT Transport driver.) -- C:\WINDOWS\System32\drivers\netbt.sys [342016] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:31:02 A . (.Microsoft Corporation - Network I/O Subsystem.) -- C:\WINDOWS\System32\drivers\netio.sys [603464] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:57 A . (.Microsoft Corporation - Miniport NDIS virtuel.) -- C:\WINDOWS\System32\drivers\netvsc.sys [249144] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:47 A . (.Intel Corporation - Intel® Wireless WiFi Link Driver.) -- C:\WINDOWS\System32\drivers\Netwtw06.sys [8803328] [Unsigned] =>.Intel Corporation

O58 - SDL:2019/12/07 11:08:49 A . (.Microsoft Corporation - NPFS Driver.) -- C:\WINDOWS\System32\drivers\npfs.sys [87568] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Named pipe service triggers.) -- C:\WINDOWS\System32\drivers\npsvctrig.sys [27648] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:49 A . (.Microsoft Corporation - NSI Proxy.) -- C:\WINDOWS\System32\drivers\nsiproxy.sys [48640] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:31:01 A . (.Microsoft Corporation - Pilote du système de fichiers NT.) -- C:\WINDOWS\System32\drivers\ntfs.sys [2851128] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:58 A . (.Microsoft Corporation - NTOS extension host driver.) -- C:\WINDOWS\System32\drivers\ntosext.sys [20792] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:49 A . (.Microsoft Corporation - NULL Driver.) -- C:\WINDOWS\System32\drivers\null.sys [7680] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - Pilote de périphérique NVDIMM.) -- C:\WINDOWS\System32\drivers\nvdimm.sys [168464] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.NVIDIA Corporation - NVIDIA® nForce(TM) RAID Driver.) -- C:\WINDOWS\System32\drivers\nvraid.sys [150328] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.NVIDIA Corporation - NVIDIA® nForce(TM) Sata Performance Driver.) -- C:\WINDOWS\System32\drivers\nvstor.sys [166200] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:32 A . (.Microsoft Corporation - Pilote de miniport WiFi natif.) -- C:\WINDOWS\System32\drivers\nwifi.sys [733696] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:34 A . (.Microsoft Corporation - Planificateur de paquets QoS.) -- C:\WINDOWS\System32\drivers\pacer.sys [161592] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - Pilote de port parallèle.) -- C:\WINDOWS\System32\drivers\parport.sys [109056] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:49 A . (.Microsoft Corporation - Partition driver.) -- C:\WINDOWS\System32\drivers\partmgr.sys [182584] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:24 A . (.Microsoft Corporation - Énumérateur Plug-and-Play PCI pour NT.) -- C:\WINDOWS\System32\drivers\pci.sys [472376] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:24 A . (.Microsoft Corporation - Generic PCI IDE Bus Driver.) -- C:\WINDOWS\System32\drivers\pciide.sys [16704] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:24 A . (.Microsoft Corporation - PCI IDE Bus Driver Extension.) -- C:\WINDOWS\System32\drivers\pciidex.sys [56648] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:50 A . (.Microsoft Corporation - Pilote de bus PCMCIA.) -- C:\WINDOWS\System32\drivers\pcmcia.sys [127800] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:46 A . (.Microsoft Corporation - Performance Counters for Windows Driver.) -- C:\WINDOWS\System32\drivers\pcw.sys [57656] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:28 A . (.Microsoft Corporation - Power Dependency Coordinator Driver.) -- C:\WINDOWS\System32\drivers\pdc.sys [159048] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:29 A . (.Microsoft Corporation - Protected Environment Authentication and Au.) -- C:\WINDOWS\System32\drivers\PEAuth.sys [822784] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:53 A . (.Avago Technologies - MEGASAS RAID Controller Driver for Windows.) -- C:\WINDOWS\System32\drivers\percsas2i.sys [58680] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.Avago Technologies - MEGASAS RAID Controller Driver for Windows.) -- C:\WINDOWS\System32\drivers\percsas3i.sys [68408] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:48 A . (.Microsoft Corporation - Pilote du moniteur de paquets.) -- C:\WINDOWS\System32\drivers\PktMon.sys [104456] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - Pilote de mémoire persistante.) -- C:\WINDOWS\System32\drivers\pmem.sys [138040] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:50 A . (.Microsoft Corporation - Pilote mémoire Plug and Play.) -- C:\WINDOWS\System32\drivers\pnpmem.sys [17408] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:36 A . (.Microsoft Corporation - Port Device Class Configuration Filter Driv.) -- C:\WINDOWS\System32\drivers\portcfg.sys [27136] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:50 A . (.Microsoft Corporation - Port Class (Class Driver for Port/Miniport.) -- C:\WINDOWS\System32\drivers\portcls.sys [389120] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:53 A . (.Microsoft Corporation - Processor Device Driver.) -- C:\WINDOWS\System32\drivers\processr.sys [216376] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:33 A . (.Microsoft Corporation - Time Travel Debugging Process Launch Monito.) -- C:\WINDOWS\System32\drivers\ProcLaunchMon.sys [43448] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:05 A . (.Microsoft Corporation - Pilote du support de Microsoft Quality Wind.) -- C:\WINDOWS\System32\drivers\qwavedrv.sys [53248] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:09 A . (.Microsoft Corporation - RAM Disk Driver.) -- C:\WINDOWS\System32\drivers\ramdisk.sys [42296] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:07 A . (.Microsoft Corporation - RAS Automatic Connection Driver.) -- C:\WINDOWS\System32\drivers\rasacd.sys [20480] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:31:07 A . (.Microsoft Corporation - RAS L2TP mini-port/call-manager driver.) -- C:\WINDOWS\System32\drivers\rasl2tp.sys [110080] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:07 A . (.Microsoft Corporation - RAS PPPoE mini-port/call-manager driver.) -- C:\WINDOWS\System32\drivers\raspppoe.sys [87552] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:31:07 A . (.Microsoft Corporation - Peer-to-Peer Tunneling Protocol.) -- C:\WINDOWS\System32\drivers\raspptp.sys [101888] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:31:07 A . (.Microsoft Corporation - RAS SSTP Miniport Call Manager.) -- C:\WINDOWS\System32\drivers\rassstp.sys [86016] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:31:03 A . (.Microsoft Corporation - Pilote du sous-système de mise en mémoire t.) -- C:\WINDOWS\System32\drivers\rdbss.sys [455480] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Microsoft RDP Bus Device driver.) -- C:\WINDOWS\System32\drivers\rdpbus.sys [28672] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:47 A . (.Microsoft Corporation - Redirecteur de périphérique de Microsoft RD.) -- C:\WINDOWS\System32\drivers\rdpdr.sys [168448] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/07/22 22:18:08 A . (.Microsoft Corporation - Microsoft RDP Video Miniport driver.) -- C:\WINDOWS\System32\drivers\rdpvideominiport.sys [31760] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:54 A . (.Microsoft Corporation - ReadyBoost Driver.) -- C:\WINDOWS\System32\drivers\rdyboost.sys [297784] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:46 A . (.Microsoft Corporation - Pilote du système de fichiers ReFS NT.) -- C:\WINDOWS\System32\drivers\refs.sys [1999160] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:46 A . (.Microsoft Corporation - Pilote du système de fichiers ReFS NT.) -- C:\WINDOWS\System32\drivers\refsv1.sys [990008] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Bluetooth RFCOMM Driver.) -- C:\WINDOWS\System32\drivers\rfcomm.sys [213504] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:57 A . (.Microsoft Corporation - Transport d’ordinateur virtuel Microsoft Re.) -- C:\WINDOWS\System32\drivers\RfxVmt.sys [41472] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:50 A . (.Microsoft Corporation - ResourceHub Proxy Driver.) -- C:\WINDOWS\System32\drivers\rhproxy.sys [115712] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:41 A . (.Microsoft Corporation - Reliable Multicast Transport.) -- C:\WINDOWS\System32\drivers\rmcast.sys [158208] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:07 A . (.Microsoft Corporation - Remote NDIS Miniport.) -- C:\WINDOWS\System32\drivers\RNDISMP.sys [37376] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:51 A . (.Microsoft Corporation - Legacy Non-Pnp Modem Device Driver.) -- C:\WINDOWS\System32\drivers\rootmdm.sys [13824] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:55 A . (.Microsoft Corporation - Link-Layer Topology Responder Driver for ND.) -- C:\WINDOWS\System32\drivers\rspndr.sys [89088] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:09 RA . (.Realtek - Realtek PCIe GBE Family Controller Flight.) -- C:\WINDOWS\System32\drivers\rteth.sys [48640] [Unsigned] =>.Realtek

O58 - SDL:2019/03/29 12:22:58 A . (.Realtek Semiconductor Corp. - Realtek(r) High Definition Audio Function D.) -- C:\WINDOWS\System32\drivers\RTKVHD64.sys [6787872] =>.Realtek Semiconductor Corp.®

O58 - SDL:2020/02/12 23:28:28 A . (.Realtek Corporation - Realtek USB FE/1GbE/2.5GbE NIC NDIS6.40 64-.) -- C:\WINDOWS\System32\drivers\rtux64w10.sys [710232] =>.Realtek Semiconductor Corp.®

O58 - SDL:2019/12/07 11:07:53 A . (.Microsoft Corporation - SBP-2 Protocol Driver.) -- C:\WINDOWS\System32\drivers\sbp2port.sys [116752] =>.Microsoft®

O58 - SDL:2020/08/14 10:25:33 A . (.Microsoft Corporation - Pilote de filtre de lecteur de carte à puce.) -- C:\WINDOWS\System32\drivers\scfilter.sys [44032] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - Pilote de bus de mémoire de classe stockage.) -- C:\WINDOWS\System32\drivers\scmbus.sys [158736] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:00 A . (.Microsoft Corporation - SCSI Port Driver.) -- C:\WINDOWS\System32\drivers\scsiport.sys [187704] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:25 A . (.Microsoft Corporation - Pilote du bus numérique sécurisé (SD).) -- C:\WINDOWS\System32\drivers\sdbus.sys [305472] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:50 A . (.Microsoft Corporation - SDF Reflector.) -- C:\WINDOWS\System32\drivers\SDFRd.sys [35128] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:09 A . (.Microsoft Corporation - SD Host Controller Port Driver.) -- C:\WINDOWS\System32\drivers\sdport.sys [105488] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Pilote de classe de stockage SD.) -- C:\WINDOWS\System32\drivers\sdstor.sys [103736] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:36 A . (.Microsoft Corporation - Serial Class Extension.) -- C:\WINDOWS\System32\drivers\SerCx.sys [86328] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:36 A . (.Microsoft Corporation - Serial Class Extension V2.) -- C:\WINDOWS\System32\drivers\SerCx2.sys [173072] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - Serial Port Enumerator.) -- C:\WINDOWS\System32\drivers\serenum.sys [27648] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - Pilote de périphérique série.) -- C:\WINDOWS\System32\drivers\serial.sys [90624] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Pilote de filtre souris série.) -- C:\WINDOWS\System32\drivers\sermouse.sys [29184] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - SCSI Floppy Driver.) -- C:\WINDOWS\System32\drivers\sfloppy.sys [19456] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:33 A . (.Microsoft Corporation - System Guard Runtime Monitor Agent Driver.) -- C:\WINDOWS\System32\drivers\SgrmAgent.sys [88080] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.Silicon Integrated Systems Corp. - SiS RAID Stor Miniport Driver.) -- C:\WINDOWS\System32\drivers\sisraid2.sys [44856] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.Silicon Integrated Systems - SiS AHCI Stor-Miniport Driver.) -- C:\WINDOWS\System32\drivers\sisraid4.sys [81720] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:49 A . (.Microsoft Corporation - Sleep Study Helper.) -- C:\WINDOWS\System32\drivers\SleepStudyHelper.sys [38200] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.Microsemi Corportation - Storport Miniport Driver for SmartRAID/Smar.) -- C:\WINDOWS\System32\drivers\SmartSAMD.sys [209720] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:09 A . (.Microsoft Corporation - Smart Card Driver Library.) -- C:\WINDOWS\System32\drivers\smclib.sys [21504] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/08/14 10:24:27 A . (.Microsoft Corporation - Storage Spaces Dump Driver.) -- C:\WINDOWS\System32\drivers\spacedump.sys [215880] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:34 A . (.Microsoft Corporation - Storage Spaces Parser.) -- C:\WINDOWS\System32\drivers\spaceparser.sys [26624] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/08/14 10:24:27 A . (.Microsoft Corporation - Storage Spaces Driver.) -- C:\WINDOWS\System32\drivers\spaceport.sys [678200] =>.Microsoft®

O58 - SDL:2019/12/07 16:52:56 A . (.Microsoft Corporation - Holographic Spatial Graph Filter.) -- C:\WINDOWS\System32\drivers\SpatialGraphFilter.sys [90936] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:37 A . (.Microsoft Corporation - SPB Class Extension.) -- C:\WINDOWS\System32\drivers\SpbCx.sys [87352] =>.Microsoft®

O58 - SDL:2020/07/22 22:17:33 A . (.Microsoft Corporation - Pilote de serveur SMB 2.0.) -- C:\WINDOWS\System32\drivers\srv2.sys [783360] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/07/22 22:17:33 A . (.Microsoft Corporation - Server Network driver.) -- C:\WINDOWS\System32\drivers\srvnet.sys [314880] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2017/05/18 22:17:28 A . (.Samsung Electronics Co., Ltd. - SAMSUNG USB Composite Device Driver.) -- C:\WINDOWS\System32\drivers\ssudbus.sys [131984] =>.Samsung Electronics Co., Ltd.®

O58 - SDL:2017/05/18 22:17:30 A . (.Samsung Electronics Co., Ltd. - SAMSUNG Android Modem Device Driver.) -- C:\WINDOWS\System32\drivers\ssudmdm.sys [166288] =>.Samsung Electronics Co., Ltd.®

O58 - SDL:2019/12/07 11:07:53 A . (.Promise Technology, Inc. - Promise SuperTrak EX Series Driver for Wind.) -- C:\WINDOWS\System32\drivers\stexstor.sys [31032] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:24 A . (.Microsoft Corporation - MS AHCI Storport Miniport Driver.) -- C:\WINDOWS\System32\drivers\storahci.sys [185672] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:24 A . (.Microsoft Corporation - Microsoft NVM Express Storport Miniport Dri.) -- C:\WINDOWS\System32\drivers\stornvme.sys [155952] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:28 A . (.Microsoft Corporation - Microsoft Storage Port Driver.) -- C:\WINDOWS\System32\drivers\storport.sys [702776] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:37 A . (.Microsoft Corporation - Filtre de qualité de service de stockage.) -- C:\WINDOWS\System32\drivers\storqosflt.sys [92984] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:24 A . (.Microsoft Corporation - MS UFS Storport Miniport Driver.) -- C:\WINDOWS\System32\drivers\storufs.sys [60744] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:57 A . (.Microsoft Corporation - Storage VSC Driver.) -- C:\WINDOWS\System32\drivers\storvsc.sys [44048] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:00 A . (.Microsoft Corporation - WDM CODEC Class Device Driver 2.0.) -- C:\WINDOWS\System32\drivers\stream.sys [82432] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:57 A . (.Microsoft Corporation - VSC vidéo Synth3D RemoteFX Microsoft.) -- C:\WINDOWS\System32\drivers\Synth3dVsc.sys [67072] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:00 A . (.Microsoft Corporation - SCSI Tape Class Driver.) -- C:\WINDOWS\System32\drivers\tape.sys [33280] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:13 A . (.Microsoft Corporation - Export driver for kernel mode TPM API.) -- C:\WINDOWS\System32\drivers\tbs.sys [31760] =>.Microsoft®

O58 - SDL:2020/09/10 19:31:02 A . (.Microsoft Corporation - Pilote TCP/IP.) -- C:\WINDOWS\System32\drivers\tcpip.sys [2991416] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:04 A . (.Microsoft Corporation - TCP/IP Registry Compatibility Driver.) -- C:\WINDOWS\System32\drivers\tcpipreg.sys [54784] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:49 A . (.Microsoft Corporation - TDI Wrapper.) -- C:\WINDOWS\System32\drivers\tdi.sys [39736] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:33 A . (.Microsoft Corporation - TDI Translation Driver.) -- C:\WINDOWS\System32\drivers\tdx.sys [117560] =>.Microsoft®

O58 - SDL:2017/11/28 06:27:38 A . (.Intel Corporation - Intel(R) Management Engine Interface.) -- C:\WINDOWS\System32\drivers\TeeDriverW8x64.sys [206488] =>.Intel(R) Embedded Subsystems and IP Blocks Group®

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Terminal Server Input Driver.) -- C:\WINDOWS\System32\drivers\terminpt.sys [41272] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:51 A . (.Microsoft Corporation - Kernel Transaction Manager Driver.) -- C:\WINDOWS\System32\drivers\tm.sys [141328] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:25 A . (.Microsoft Corporation - Pilote de périphérique TPM.) -- C:\WINDOWS\System32\drivers\tpm.sys [255296] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:09 A . (.Microsoft Corporation - Pilote de filtre pour concentrateur USB du.) -- C:\WINDOWS\System32\drivers\TsUsbFlt.sys [66560] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:53 A . (.Microsoft Corporation - Remote Desktop Generic USB Driver.) -- C:\WINDOWS\System32\drivers\TsUsbGD.sys [37888] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:04 A . (.Microsoft Corporation - Pilote d’interface de tunnel Microsoft.) -- C:\WINDOWS\System32\drivers\tunnel.sys [129024] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - Microsoft Uasp Driver.) -- C:\WINDOWS\System32\drivers\uaspstor.sys [79376] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:37 A . (.Microsoft Corporation - USB Connector Manager KMDF Class Extension.) -- C:\WINDOWS\System32\drivers\UcmCx.sys [160256] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:37 A . (.Microsoft Corporation - UCM-TCPCI KMDF Class Extension.) -- C:\WINDOWS\System32\drivers\UcmTcpciCx.sys [188416] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - UCM-UCSI ACPI Client Driver.) -- C:\WINDOWS\System32\drivers\UcmUcsiAcpiClient.sys [36864] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:30:53 A . (.Microsoft Corporation - UCM-UCSI KMDF Class Extension.) -- C:\WINDOWS\System32\drivers\UcmUcsiCx.sys [113152] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:09 A . (.Microsoft Corporation - USB Controller Extension.) -- C:\WINDOWS\System32\drivers\Ucx01000.sys [259896] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:09 A . (.Microsoft Corporation - 'udecx.DRIVER'.) -- C:\WINDOWS\System32\drivers\Udecx.sys [52736] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:51 A . (.Microsoft Corporation - UDF File System Driver.) -- C:\WINDOWS\System32\drivers\udfs.sys [344064] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:37 A . (.Microsoft Corporation - USB Function Driver Class Extension.) -- C:\WINDOWS\System32\drivers\ufx01000.sys [321040] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - UFX Synopsys Client Driver.) -- C:\WINDOWS\System32\drivers\ufxsynopsys.sys [168248] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Generic pass-through driver.) -- C:\WINDOWS\System32\drivers\umpass.sys [15360] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:37 A . (.Microsoft Corporation - USB Role-Switch Class Extension.) -- C:\WINDOWS\System32\drivers\urscx01000.sys [76304] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:07 A . (.Microsoft Corporation - Remote NDIS USB Driver.) -- C:\WINDOWS\System32\drivers\usb8023.sys [24064] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/07/22 22:17:04 A . (.Microsoft Corporation - USB Audio Class Driver.) -- C:\WINDOWS\System32\drivers\USBAUDIO.sys [202752] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:50 A . (.Microsoft Corporation - Microsoft USB Audio Class 2.0 Driver.) -- C:\WINDOWS\System32\drivers\usbaudio2.sys [260608] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:41 A . (.Microsoft Corporation - Universal Serial Bus Camera Driver.) -- C:\WINDOWS\System32\drivers\USBCAMD2.sys [40448] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:30:25 A . (.Microsoft Corporation - USB Common Class Generic Parent Driver.) -- C:\WINDOWS\System32\drivers\usbccgp.sys [185664] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:50 A . (.Microsoft Corporation - USB Consumer IR Driver for eHome.) -- C:\WINDOWS\System32\drivers\usbcir.sys [107520] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Universal Serial Bus Driver.) -- C:\WINDOWS\System32\drivers\usbd.sys [33080] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - EHCI eUSB Miniport Driver.) -- C:\WINDOWS\System32\drivers\usbehci.sys [86544] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Pilote de concentrateur USB par défaut.) -- C:\WINDOWS\System32\drivers\usbhub.sys [528184] =>.Microsoft®

O58 - SDL:2020/07/22 22:17:05 A . (.Microsoft Corporation - Pilote de concentrateur USB3.) -- C:\WINDOWS\System32\drivers\USBHUB3.SYS [647992] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - OHCI USB Miniport Driver.) -- C:\WINDOWS\System32\drivers\usbohci.sys [30208] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:37 A . (...) -- C:\WINDOWS\System32\drivers\UsbPmApi.sys [53248] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Pilote de port USB 1.1 & 2.0.) -- C:\WINDOWS\System32\drivers\usbport.sys [473400] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:50 A . (.Microsoft Corporation - USB Printer driver.) -- C:\WINDOWS\System32\drivers\usbprint.sys [35328] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - USB Serial Driver.) -- C:\WINDOWS\System32\drivers\usbser.sys [81408] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Pilote de classe de stockage de masse USB.) -- C:\WINDOWS\System32\drivers\USBSTOR.SYS [135480] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - UHCI USB Miniport Driver.) -- C:\WINDOWS\System32\drivers\usbuhci.sys [39424] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:30:24 A . (.Microsoft Corporation - USB Video Class Driver.) -- C:\WINDOWS\System32\drivers\usbvideo.sys [314688] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:25 A . (.Microsoft Corporation - Pilote XHCI USB.) -- C:\WINDOWS\System32\drivers\USBXHCI.SYS [602440] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - Virtual Drive Root Enumerator.) -- C:\WINDOWS\System32\drivers\vdrvroot.sys [67384] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:49 A . (.Microsoft Corporation - Extension du vérificateur de pilotes.) -- C:\WINDOWS\System32\drivers\VerifierExt.sys [347448] =>.Microsoft®

O58 - SDL:2020/07/22 22:17:05 A . (.Microsoft Corporation - VHD Miniport Driver.) -- C:\WINDOWS\System32\drivers\vhdmp.sys [821048] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - Virtual HID Framework (VHF) Driver.) -- C:\WINDOWS\System32\drivers\vhf.sys [47616] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/08/14 10:24:28 A . (.Microsoft Corporation - Microsoft Hyper-V Virtualization Infrastruc.) -- C:\WINDOWS\System32\drivers\Vid.sys [639288] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:49 A . (.Microsoft Corporation - Video Port Driver.) -- C:\WINDOWS\System32\drivers\videoprt.sys [47104] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:51 A . (.Microsoft Corporation - Hyper-V VMBus KMCL.) -- C:\WINDOWS\System32\drivers\vmbkmcl.sys [114488] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:26 A . (.Microsoft Corporation - Pilote enfant de bus VMBus sous Microsoft H.) -- C:\WINDOWS\System32\drivers\vmbus.sys [160064] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:57 A . (.Microsoft Corporation - Microsoft VMBus HID Miniport.) -- C:\WINDOWS\System32\drivers\VMBusHID.sys [36664] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:57 A . (.Microsoft Corporation - Virtual Machine Generation Counter.) -- C:\WINDOWS\System32\drivers\vmgencounter.sys [23864] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:57 A . (.Microsoft Corporation - Virtual Machine Guest Infrastructure Driver.) -- C:\WINDOWS\System32\drivers\vmgid.sys [19768] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:57 A . (.Microsoft Corporation - Microsoft S3 Emulated Device Cap Driver.) -- C:\WINDOWS\System32\drivers\vms3cap.sys [18960] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:57 A . (.Microsoft Corporation - Pilote de filtre de stockage virtuel.) -- C:\WINDOWS\System32\drivers\vmstorfl.sys [54280] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.Microsoft Corporation - Pilote du gestionnaire de volumes.) -- C:\WINDOWS\System32\drivers\volmgr.sys [90424] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:37 A . (.Microsoft Corporation - Pilote d’extension du gestionnaire de volum.) -- C:\WINDOWS\System32\drivers\volmgrx.sys [389432] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:34 A . (.Microsoft Corporation - Pilote de cliché instantané du volume.) -- C:\WINDOWS\System32\drivers\volsnap.sys [429880] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:53 A . (.Microsoft Corporation - Volume driver.) -- C:\WINDOWS\System32\drivers\volume.sys [16696] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:57 A . (.Microsoft Corporation - Virtual PCI Bus.) -- C:\WINDOWS\System32\drivers\vpci.sys [89400] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.VIA Technologies Inc.,Ltd - VIA RAID DRIVER FOR AMD-X86-64.) -- C:\WINDOWS\System32\drivers\vsmraid.sys [166712] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.VIA Corporation - VIA StorX RAID Controller Driver.) -- C:\WINDOWS\System32\drivers\VSTXRAID.SYS [305464] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:13 A . (.Microsoft Corporation - Virtual Wireless Bus Driver.) -- C:\WINDOWS\System32\drivers\vwifibus.sys [29184] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:13 A . (.Microsoft Corporation - Virtual WiFi Filter Driver.) -- C:\WINDOWS\System32\drivers\vwififlt.sys [77824] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:13 A . (.Microsoft Corporation - Virtual WiFi Miniport Driver.) -- C:\WINDOWS\System32\drivers\vwifimp.sys [50688] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:53 A . (.Microsoft Corporation - Pilote de tablette Wacom à stylet série.) -- C:\WINDOWS\System32\drivers\wacompen.sys [31232] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:09:07 A . (.Microsoft Corporation - MS Remote Access and Routing ARP Driver.) -- C:\WINDOWS\System32\drivers\wanarp.sys [93184] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:24 A . (.Microsoft Corporation - Watchdog Driver.) -- C:\WINDOWS\System32\drivers\watchdog.sys [74752] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:34 A . (.Microsoft Corporation - Windows Container Isolation FS Filter Drive.) -- C:\WINDOWS\System32\drivers\wcifs.sys [202552] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:34 A . (.Microsoft Corporation - Windows Container Name Virtualization FS Fi.) -- C:\WINDOWS\System32\drivers\wcnfs.sys [93184] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:15 A . (.Microsoft Corporation - Microsoft antimalware boot driver.) -- C:\WINDOWS\System32\drivers\WdBoot.sys [46688] =>.Microsoft®

O58 - SDL:2020/08/14 10:25:21 A . (.Microsoft Corporation - Runtime de l’infrastructure de pilotes en m.) -- C:\WINDOWS\System32\drivers\Wdf01000.sys [827704] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:15 A . (.Microsoft Corporation - Microsoft antimalware file system filter dr.) -- C:\WINDOWS\System32\drivers\WdFilter.sys [350136] =>.Microsoft®

O58 - SDL:2020/08/14 10:25:21 A . (.Microsoft Corporation - Kernel Mode Driver Framework Loader.) -- C:\WINDOWS\System32\drivers\WdfLdr.sys [59192] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:33 A . (.Microsoft Corporation - WDI Driver Framework Driver.) -- C:\WINDOWS\System32\drivers\WdiWiFi.sys [951808] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:39 A . (.Microsoft Corporation - WDM Companion Filter.) -- C:\WINDOWS\System32\drivers\WdmCompanionFilter.sys [23560] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:16 A . (.Microsoft Corporation - Windows Defender Network Stream Filter.) -- C:\WINDOWS\System32\drivers\WdNisDrv.sys [54200] =>.Microsoft®

O58 - SDL:2018/08/30 02:27:40 A . (.Huawei Device - WDTDevice Driver.) -- C:\WINDOWS\System32\drivers\WDTDrv.sys [37152] {6E715E33F17AD55BCBF98C1F14D21F2F}.

O58 - SDL:2019/12/07 11:08:49 A . (.Microsoft Corporation - Windows Error Reporting Kernel Driver.) -- C:\WINDOWS\System32\drivers\werkernel.sys [52024] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:53 A . (.Microsoft Corporation - WFP NDIS 6.30 Lightweight Filter Driver.) -- C:\WINDOWS\System32\drivers\wfplwfs.sys [180040] =>.Microsoft®

O58 - SDL:2020/08/14 10:25:17 A . (.Microsoft Corporation - Wim file system Driver.) -- C:\WINDOWS\System32\drivers\wimmount.sys [39736] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:37 A . (.Microsoft Corporation - Windows Trusted Runtime Interface Driver.) -- C:\WINDOWS\System32\drivers\WindowsTrustedRT.sys [76984] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Windows Trusted Runtime Service Proxy Drive.) -- C:\WINDOWS\System32\drivers\WindowsTrustedRTProxy.sys [18920] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:51 A . (.Microsoft Corporation - Windows Hypervisor Interface Driver.) -- C:\WINDOWS\System32\drivers\winhv.sys [32784] =>.Microsoft®

O58 - SDL:2019/12/07 11:09:33 A . (.Microsoft Corporation - Windows Hypervisor Root Interface Driver.) -- C:\WINDOWS\System32\drivers\winhvr.sys [96056] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Mellanox - Kernel WinMad.) -- C:\WINDOWS\System32\drivers\winmad.sys [36152] =>.Microsoft®

O58 - SDL:2020/09/10 19:30:27 A . (.Microsoft Corporation - Pilote NAT Windows.) -- C:\WINDOWS\System32\drivers\winnat.sys [259584] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:56 A . (.Microsoft Corporation - Windows WinUSB Class Driver.) -- C:\WINDOWS\System32\drivers\winusb.sys [107008] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:54 A . (.Mellanox - Kernel WinVerbs.) -- C:\WINDOWS\System32\drivers\winverbs.sys [73016] =>.Microsoft®

O58 - SDL:2019/12/07 11:07:54 A . (.Microsoft Corporation - Windows Management Interface for ACPI.) -- C:\WINDOWS\System32\drivers\wmiacpi.sys [19456] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:49 A . (.Microsoft Corporation - WMILIB WMI support library Dll.) -- C:\WINDOWS\System32\drivers\wmilib.sys [19472] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:46 A . (.Microsoft Corporation - Filtre de superposition Windows.) -- C:\WINDOWS\System32\drivers\wof.sys [234504] =>.Microsoft®

O58 - SDL:2019/12/07 16:52:58 A . (.Microsoft Corporation - Windows Portable Device Upper Class Filter.) -- C:\WINDOWS\System32\drivers\WpdUpFltr.sys [32568] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:49 A . (.Microsoft Corporation - WPP Trace Recorder.) -- C:\WINDOWS\System32\drivers\WppRecorder.sys [43832] =>.Microsoft®

O58 - SDL:2019/12/07 11:08:41 A . (.Microsoft Corporation - Couche IFS Winsock2.) -- C:\WINDOWS\System32\drivers\ws2ifsl.sys [25088] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:50 A . (.Microsoft Corporation - Web Services Print Device Driver.) -- C:\WINDOWS\System32\drivers\WSDPrint.sys [23552] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/07/22 22:17:04 A . (.Microsoft Corporation - Web Service Based Scan Device Driver.) -- C:\WINDOWS\System32\drivers\WSDScan.sys [26112] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:58 A . (.Microsoft Corporation - Windows Driver Foundation - User-mode Drive.) -- C:\WINDOWS\System32\drivers\WUDFPf.sys [136192] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:58 A . (.Microsoft Corporation - Windows Driver Foundation - User-mode Drive.) -- C:\WINDOWS\System32\drivers\WUDFRd.sys [315392] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:47 A . (.Microsoft Corporation - Game Input Protocol Driver.) -- C:\WINDOWS\System32\drivers\xboxgip.sys [324608] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:07:47 A . (.Microsoft Corporation - XINPUT filter driver for HID.) -- C:\WINDOWS\System32\drivers\xinputhid.sys [48640] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:30:53 A . (.Microsoft Corporation - Multi-User Win32 Driver.) -- C:\WINDOWS\System32\win32k.sys [596992] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:30:49 A . (.Microsoft Corporation - Pilote du noyau Base Win32k.) -- C:\WINDOWS\System32\win32kbase.sys [2951680] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:30:53 A . (.Microsoft Corporation - Full/Desktop Win32k Kernel Driver.) -- C:\WINDOWS\System32\win32kfull.sys [3815424] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2019/12/07 11:08:34 A . (.Microsoft Corporation - Win32k non session driver.) -- C:\WINDOWS\System32\win32kns.sys [30208] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:31:17 A . (.Microsoft Corporation - Multi-User Win32 Driver.) -- C:\WINDOWS\SysWOW64\win32k.sys [329728] [Unsigned] =>.Microsoft Corporation

O58 - SDL:2020/09/10 19:31:17 A . (.Microsoft Corporation - Full/Desktop Win32k Kernel Driver.) -- C:\WINDOWS\SysWOW64\win32kfull.sys [2749440] [Unsigned] =>.Microsoft Corporation

**---\ ASSOCIATION Shell Spawning (10) - 0s**

O67 - Shell Spawning: <.bat> [HKLM\..\open\Command] (...) -- '%1' %\* =>.Default.Value

O67 - Shell Spawning: <.cpl> [HKLM\..\cplopen\Command] (.Microsoft Corporation - Windows Control Panel.) -- C:\Windows\System32\control.exe [Unsigned] =>.Microsoft Corporation

O67 - Shell Spawning: <.cmd> [HKLM\..\open\Command] (...) -- '%1' %\* =>.Default.Value

O67 - Shell Spawning: <.com> [HKLM\..\open\Command] (...) -- '%1' %\* =>.Default.Value

O67 - Shell Spawning: <.evt> [HKLM\..\open\Command] (.Microsoft Corporation - Lanceur du composant logiciel enfichable Ob.) -- C:\Windows\System32\eventvwr.exe [Unsigned] =>.Microsoft Corporation

O67 - Shell Spawning: <.exe> [HKLM\..\open\Command] (...) -- '%1' %\* =>.Default.Value

O67 - Shell Spawning: <.html> [HKLM\..\open\Command] (.Microsoft Corporation - Internet Explorer.) -- C:\Program Files\Internet Explorer\iexplore.exe =>.Microsoft®

O67 - Shell Spawning: <.js> [HKLM\..\open\Command] (...) -- C:\Windows\System32\WScript.exe '%1' %\* =>.Default.Value

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

O67 - Shell Spawning: <.scr> [HKLM\..\open\Command] (...) -- '%1' /S =>.Default.Value

**---\ MENU DE DÉMARRAGE INTERNET (16) - 1s**

O68 - StartMenuInternet: [64Bits][HKLM\..\Shell\open\Command] (.Piriform Software - CCleaner Browser.) -- C:\Program Files (x86)\CCleaner Browser\Application\CCleanerBrowser.exe =>.Piriform Software Ltd®

O68 - StartMenuInternet: [64Bits][HKLM\..\Shell\open\Command] (.Mozilla Corporation - Firefox.) -- C:\Program Files\Mozilla Firefox\firefox.exe =>.Mozilla Corporation®

O68 - StartMenuInternet: [64Bits][HKLM\..\Shell\open\Command] (.Microsoft Corporation - Internet Explorer.) -- C:\Program Files\Internet Explorer\iexplore.exe =>.Microsoft®

O68 - StartMenuInternet: [64Bits][HKLM\..\Shell\open\Command] (.Microsoft Corporation - Microsoft Edge.) -- C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe =>.Microsoft®

O68 - StartMenuInternet: [64Bits][HKLM\..\InstallInfo\ShowIconsCommand] (.Piriform Software - CCleaner Browser.) -- C:\Program Files (x86)\CCleaner Browser\Application\CCleanerBrowser.exe =>.Piriform Software

O68 - StartMenuInternet: [64Bits][HKLM\..\InstallInfo\ShowIconsCommand] (.Mozilla Corporation - Firefox Helper.) -- C:\Program Files\Mozilla Firefox\uninstall\helper.exe =>.Mozilla Corporation

O68 - StartMenuInternet: [64Bits][HKLM\..\InstallInfo\ShowIconsCommand] (.Microsoft Corporation - IE Per-User Show IE Icon Utility.) -- C:\WINDOWS\System32\ie4ushowIE.exe =>.Microsoft Corporation

O68 - StartMenuInternet: [64Bits][HKLM\..\InstallInfo\ShowIconsCommand] (.Microsoft Corporation - Microsoft Edge.) -- C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe =>.Microsoft Corporation

O68 - StartMenuInternet: [64Bits][HKLM\..\InstallInfo\ReinstallCommand] (.Piriform Software - CCleaner Browser.) -- C:\Program Files (x86)\CCleaner Browser\Application\CCleanerBrowser.exe =>.Piriform Software

O68 - StartMenuInternet: [64Bits][HKLM\..\InstallInfo\ReinstallCommand] (.Mozilla Corporation - Firefox Helper.) -- C:\Program Files\Mozilla Firefox\uninstall\helper.exe =>.Mozilla Corporation

O68 - StartMenuInternet: [64Bits][HKLM\..\InstallInfo\ReinstallCommand] (.Microsoft Corporation - Utilitaire d'initialisation d'Internet Expl.) -- C:\Windows\System32\ie4uinit.exe =>.Microsoft Corporation

O68 - StartMenuInternet: [64Bits][HKLM\..\InstallInfo\ReinstallCommand] (.Microsoft Corporation - Microsoft Edge.) -- C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe =>.Microsoft Corporation

O68 - StartMenuInternet: [64Bits][HKLM\..\InstallInfo\HideIconsCommand] (.Piriform Software - CCleaner Browser.) -- C:\Program Files (x86)\CCleaner Browser\Application\CCleanerBrowser.exe =>.Piriform Software

O68 - StartMenuInternet: [64Bits][HKLM\..\InstallInfo\HideIconsCommand] (.Mozilla Corporation - Firefox Helper.) -- C:\Program Files\Mozilla Firefox\uninstall\helper.exe =>.Mozilla Corporation

O68 - StartMenuInternet: [64Bits][HKLM\..\InstallInfo\HideIconsCommand] (.Microsoft Corporation - IE Per-User Show IE Icon Utility.) -- C:\WINDOWS\System32\ie4ushowIE.exe =>.Microsoft Corporation

O68 - StartMenuInternet: [64Bits][HKLM\..\InstallInfo\HideIconsCommand] (.Microsoft Corporation - Microsoft Edge.) -- C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe =>.Microsoft Corporation

**---\ RECHERCHE D'INFECTION SUR NAVIGATEURS (3) - 8s**

O69 - SBI: SearchScopes [HKCU] [64Bits]{0633EE93-D776-472f-A0FF-E1416B8B2E3A} [DefaultScope] - (Bing) - http://www.bing.com/ =>.Bing.com

O69 - SBI: SearchScopes [HKLM] [64Bits]{0633EE93-D776-472f-A0FF-E1416B8B2E3A} - (@ieframe.dll,-12512) - http://www.bing.com/ =>.Bing.com

O69 - SBI: SearchScopes [HKLM] [64Bits]{AEC7B97C-FFE2-4E9E-B31E-CBC0F9DAF1D9} [DefaultScope] - () - http://www.bing.com/ =>.Bing.com

**---\ ÉNUMÈRE LES SERVICES DÉMARRÉS PAR Svchost (49) - 2s**

O83 - Search Svchost Services: CertPropSvc (CertPropSvc) . (.Microsoft Corporation - Service de propagation de certificats de ca.) -- C:\WINDOWS\System32\certprop.dll [196096] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: SCPolicySvc (SCPolicySvc) . (.Microsoft Corporation - Service de propagation de certificats de ca.) -- C:\Windows\System32\certprop.dll [196096] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: lanmanserver (lanmanserver) . (.Microsoft Corporation - DLL du service Serveur.) -- C:\Windows\System32\srvsvc.dll [301568] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: gpsvc (gpsvc) . (.Microsoft Corporation - Client de stratégie de groupe.) -- C:\Windows\System32\gpsvc.dll [1296384] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: IKEEXT (IKEEXT) . (.Microsoft Corporation - Extension IKE.) -- C:\Windows\System32\IKEEXT.DLL [1046016] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: iphlpsvc (iphlpsvc) . (.Microsoft Corporation - Service offrant une connectivité IPv6 sur u.) -- C:\Windows\System32\iphlpsvc.dll [836096] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: seclogon (seclogon) . (.Microsoft Corporation - DLL de service d’ouverture de session secon.) -- C:\Windows\System32\seclogon.dll [32768] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: msiscsi (msiscsi) . (.Microsoft Corporation - Service de découverte iSCSI.) -- C:\Windows\System32\iscsiexe.dll [160256] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: EapHost (EapHost) . (.Microsoft Corporation - Service EAPHost Microsoft.) -- C:\Windows\System32\eapsvc.dll [112640] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: schedule (schedule) . (.Microsoft Corporation - Service du Planificateur de tâches.) -- C:\Windows\System32\schedsvc.dll [813568] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: winmgmt (winmgmt) . (.Microsoft Corporation - WMI.) -- C:\Windows\System32\wbem\WMIsvc.dll [243200] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: ProfSvc (ProfSvc) . (.Microsoft Corporation - ProfSvc.) -- C:\Windows\System32\profsvc.dll [485888] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: SessionEnv (SessionEnv) . (.Microsoft Corporation - Service Configuration des services Bureau à.) -- C:\Windows\System32\SessEnv.dll [515072] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: wercplsupport (wercplsupport) . (.Microsoft Corporation - Rapports de problèmes.) -- C:\Windows\System32\wercplsupport.dll [126464] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: InstallService (InstallService) . (.Microsoft Corporation - InstallService.) -- C:\Windows\System32\InstallService.dll [2422784] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: PushToInstall (PushToInstall) . (.Microsoft Corporation - PushToInstall.) -- C:\Windows\System32\PushToInstall.dll [263168] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: TroubleshootingSvc (TroubleshootingSvc) . (.Microsoft Corporation - MitigationClient.) -- C:\Windows\System32\MitigationClient.dll [417792] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: LxpSvc (LxpSvc) . (.Microsoft Corporation - Fournit une prise en charge de l'infrastruc.) -- C:\Windows\System32\LanguageOverlayServer.dll [302592] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: shpamsvc (shpamsvc) . (.Microsoft Corporation - SharedPC.AccountManager.) -- C:\Windows\System32\Windows.SharedPC.AccountManager.dll [224768] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: XblGameSave (XblGameSave) . (.Microsoft Corporation - Xbox Live Game Save Service.) -- C:\Windows\System32\XblGameSave.dll [1267712] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: DmEnrollmentSvc (DmEnrollmentSvc) . (.Microsoft Corporation - DLL Windows Management Service.) -- C:\Windows\System32\Windows.Internal.Management.dll [1008640] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: WManSvc (WManSvc) . (.Microsoft Corporation - DLL du Service de gestion de Windows.) -- C:\Windows\System32\Windows.Management.Service.dll [934912] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: Themes (Themes) . (.Microsoft Corporation - DLL du service des thèmes Windows Shell.) -- C:\Windows\System32\themeservice.dll [70656] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: UserManager (UserManager) . (.Microsoft Corporation - UserMgr.) -- C:\Windows\System32\usermgr.dll [1488384] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: NetSetupSvc (NetSetupSvc) . (.Microsoft Corporation - Service Configuration du réseau.) -- C:\Windows\System32\NetSetupSvc.dll [309248] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: wlidsvc (wlidsvc) . (.Microsoft Corporation - Service de compte Microsoft®.) -- C:\Windows\System32\wlidsvc.dll [2242048] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: TokenBroker (TokenBroker) . (.Microsoft Corporation - Broker à jetons.) -- C:\Windows\System32\TokenBroker.dll [1530880] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: lfsvc (lfsvc) . (.Microsoft Corporation - Service de géolocalisation.) -- C:\Windows\System32\lfsvc.dll [48640] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: NaturalAuthentication (NaturalAuthentication) . (.Microsoft Corporation - Service d’authentification naturelle.) -- C:\Windows\System32\NaturalAuth.dll [454144] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: Rasauto (Rasauto) . (.Microsoft Corporation - Gestionnaire de numérotation automatique d’.) -- C:\Windows\System32\rasauto.dll [111616] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: Rasman (Rasman) . (.Microsoft Corporation - Gestionnaire des connexions d’accès à dista.) -- C:\Windows\System32\rasmans.dll [969216] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: Remoteaccess (Remoteaccess) . (.Microsoft Corporation - Gestionnaire d’interface dynamique.) -- C:\Windows\System32\mprdim.dll [520192] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: SENS (SENS) . (.Microsoft Corporation - Service de notification d’événements systèm.) -- C:\Windows\System32\Sens.dll [77824] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: Sharedaccess (Sharedaccess) . (.Microsoft Corporation - Composants de l’application d’assistance à.) -- C:\Windows\System32\ipnathlp.dll [617984] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: Tapisrv (Tapisrv) . (.Microsoft Corporation - Serveur de téléphonie Microsoft® Windows(TM.) -- C:\Windows\System32\tapisrv.dll [316928] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: wuauserv (wuauserv) . (.Microsoft Corporation - Agent de mise à jour automatique Windows Up.) -- C:\Windows\System32\wuaueng.dll [3384832] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: BITS (BITS) . (.Microsoft Corporation - Service de transfert intelligent en arrière.) -- C:\Windows\System32\qmgr.dll [1473024] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: ShellHWDetection (ShellHWDetection) . (.Microsoft Corporation - Dll des services Windows Shell.) -- C:\Windows\System32\shsvcs.dll [259584] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: dmwappushservice (dmwappushservice) . (.Microsoft Corporation - dmwappushsvc.) -- C:\Windows\System32\dmwappushsvc.dll [58880] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: wisvc (wisvc) . (.Microsoft Corporation - Paramètres de vol.) -- C:\Windows\System32\flightsettings.dll [939448] =>.Microsoft®

O83 - Search Svchost Services: WpnService (WpnService) . (.Microsoft Corporation - Service du système de notifications Push Wi.) -- C:\Windows\System32\WpnService.dll [244736] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: AppInfo (AppInfo) . (.Microsoft Corporation - Service Informations d’application.) -- C:\Windows\System32\appinfo.dll [219648] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: XboxNetApiSvc (XboxNetApiSvc) . (.Microsoft Corporation - Xbox Live Networking Service.) -- C:\Windows\System32\XboxNetApiSvc.dll [1293824] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: UsoSvc (UsoSvc) . (.Microsoft Corporation - Mettre à jour la session du service Orchest.) -- C:\Windows\System32\usosvc.dll [566272] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: XboxGipSvc (XboxGipSvc) . (.Microsoft Corporation - Xbox Gip Management Service.) -- C:\Windows\System32\XboxGipSvc.dll [72704] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: NcaSvc (NcaSvc) . (.Microsoft Corporation - Service Assistant Connectivité réseau Micro.) -- C:\Windows\System32\NcaSvc.dll [171520] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: XblAuthManager (XblAuthManager) . (.Microsoft Corporation - Xbox Live Auth Manager.) -- C:\Windows\System32\XblAuthManager.dll [1046528] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: DsmSvc (DsmSvc) . (.Microsoft Corporation - Gestionnaire d’installation de périphérique.) -- C:\Windows\System32\DeviceSetupManager.dll [288256] [Unsigned] =>.Microsoft Corporation

O83 - Search Svchost Services: BDESVC (BDESVC) . (.Microsoft Corporation - Service BDE.) -- C:\Windows\System32\bdesvc.dll [553984] [Unsigned] =>.Microsoft Corporation

**---\ LISTE DES EXCEPTIONS PAREFEU WINDOWS (18) - 5s**

O87 - FAEL: '{0518D3C4-4ABB-4094-9A54-99A825262B9D}' [Out-None-P17-TRUE] .(.Skype Technologies S.A. - Skype.) -- C:\Program Files\WindowsApps\Microsoft.SkypeApp\_15.61.100.0\_x86\_\_kzf8qxf38zg5c\Skype\Skype.exe =>.Skype Software Sarl®

O87 - FAEL: '{7EBA8704-979D-4491-B117-9D983F331256}' [In-None-P17-TRUE] .(.Skype Technologies S.A. - Skype.) -- C:\Program Files\WindowsApps\Microsoft.SkypeApp\_15.61.100.0\_x86\_\_kzf8qxf38zg5c\Skype\Skype.exe =>.Skype Software Sarl®

O87 - FAEL: '{451193AE-B2E0-410B-AC73-B6CD6B0A9980}' [Out-None-P6-TRUE] .(.Skype Technologies S.A. - Skype.) -- C:\Program Files\WindowsApps\Microsoft.SkypeApp\_15.61.100.0\_x86\_\_kzf8qxf38zg5c\Skype\Skype.exe =>.Skype Software Sarl®

O87 - FAEL: '{9347139E-819A-482C-8B27-3EB7506AC2FE}' [In-None-P6-TRUE] .(.Skype Technologies S.A. - Skype.) -- C:\Program Files\WindowsApps\Microsoft.SkypeApp\_15.61.100.0\_x86\_\_kzf8qxf38zg5c\Skype\Skype.exe =>.Skype Software Sarl®

O87 - FAEL: 'UDP Query User{3C607751-7F5B-4F14-8B02-1D96A0FD90EC}C:\program files\videolan\vlc\vlc.exe' [In-None-P17-TRUE] .(.VideoLAN - VLC media player.) -- C:\program files\videolan\vlc\vlc.exe =>.VideoLAN®

O87 - FAEL: 'TCP Query User{C79F3F3C-D6D2-4E61-ADE1-9258DEBB9373}C:\program files\videolan\vlc\vlc.exe' [In-None-P6-TRUE] .(.VideoLAN - VLC media player.) -- C:\program files\videolan\vlc\vlc.exe =>.VideoLAN®

O87 - FAEL: '{9384529F-6CF8-43B3-8F55-616EF37DEB95}' [In-None-P6-TRUE] .(.Zoom Video Communications, Inc. - Zoom Meetings.) -- C:\Users\ericl\AppData\Roaming\Zoom\bin\Zoom.exe =>.Zoom Video Communications, Inc.®

O87 - FAEL: '{7E3A5E69-6B43-4CF9-861D-472A4A506783}' [In-None-P6-TRUE] .(.by Achal Dhir - Wireless PAN DHCP and DNS Server.) -- C:\Program Files\Intel\WiFi\bin\PanDhcpDns.exe =>.Intel Corporation®

O87 - FAEL: 'TCP Query User{3EE52DDD-CDEC-4230-B3F5-A357A14C9DDE}C:\users\ericl\appdata\local\google\chrome\application\chrome.exe' [In-None-P6-TRUE] .(.Google LLC - Google Chrome.) -- C:\users\ericl\appdata\local\google\chrome\application\chrome.exe =>.Google LLC®

O87 - FAEL: 'UDP Query User{FC785C5E-C554-46D3-98FC-7823F1EE4C13}C:\users\ericl\appdata\local\google\chrome\application\chrome.exe' [In-None-P17-TRUE] .(.Google LLC - Google Chrome.) -- C:\users\ericl\appdata\local\google\chrome\application\chrome.exe =>.Google LLC®

O87 - FAEL: 'TCP Query User{ABF98677-6EBA-4274-B715-8BCE69372B5B}C:\users\ericl\appdata\local\google\chrome\application\chrome.exe' [In-None-P6-TRUE] .(.Google LLC - Google Chrome.) -- C:\users\ericl\appdata\local\google\chrome\application\chrome.exe =>.Google LLC®

O87 - FAEL: 'UDP Query User{E5821981-F3FB-4A70-846A-3218C8518515}C:\users\ericl\appdata\local\google\chrome\application\chrome.exe' [In-None-P17-TRUE] .(.Google LLC - Google Chrome.) -- C:\users\ericl\appdata\local\google\chrome\application\chrome.exe =>.Google LLC®

O87 - FAEL: '{B5C60CB9-712D-444C-A28E-F9833F654021}' [In-None-P6-TRUE] .(.Mozilla Corporation - Firefox.) -- C:\Program Files\Mozilla Firefox\firefox.exe =>.Mozilla Corporation®

O87 - FAEL: '{81FFA65F-AE5F-43EC-95E0-B0FF5E6464FD}' [In-None-P17-TRUE] .(.Mozilla Corporation - Firefox.) -- C:\Program Files\Mozilla Firefox\firefox.exe =>.Mozilla Corporation®

O87 - FAEL: '{9DC80834-52DF-4C60-8188-C3EB489B6E66}' [In-None-P17-TRUE] .(.Piriform Software - CCleaner Browser.) -- C:\Program Files (x86)\CCleaner Browser\Application\CCleanerBrowser.exe =>.Piriform Software Ltd®

O87 - FAEL: '{13E519A6-86C0-463A-ABCA-9F850690F05C}' [In-None-P17-TRUE] .(.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe =>.Dropbox, Inc®

O87 - FAEL: '{57E7668D-4C64-40A2-8049-274F4D418F22}' [In-None-P17-TRUE] .(...) -- C:\Program Files\Huawei\PCManager\MBAMessageCenter.exe {6E715E33F17AD55BCBF98C1F14D21F2F}.

O87 - FAEL: '{EA248777-5ED7-411B-B03C-5DE8E46E498F}' [In-None-P6-TRUE] .(...) -- C:\Program Files\Huawei\PCManager\HWVCR.exe {6E715E33F17AD55BCBF98C1F14D21F2F}.

**---\ CODES PRODUITS LOGICIELS (43) - 1s**

O90 - PUC: '00006109C80000000100000000F01FEC' [HKLM] . (.Office 16 Click-to-Run Extensibility Component.) =>.Microsoft Corporation

O90 - PUC: '00006109C80090400100000000F01FEC' [HKLM] . (.Office 16 Click-to-Run Localization Component.) =>.Microsoft Corporation

O90 - PUC: '00006109C800C0400100000000F01FEC' [HKLM] . (.Office 16 Click-to-Run Localization Component.) =>.Microsoft Corporation

O90 - PUC: '00006109E70000000100000000F01FEC' [HKLM] . (.Office 16 Click-to-Run Licensing Component.) =>.Microsoft Corporation

O90 - PUC: '19BA12E58FE2A8E4AB3315E566C7CDB4' [HKLM] . (.Intel(R) Management Engine Components.) =>.Intel Corporation

O90 - PUC: '21EE4A31AE32173319EEFE3BD6FDFFE3' [HKLM] . (.Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005.) =>.Microsoft Corporation

O90 - PUC: '22BEFC8F7E2A1793E9ADB411DEFE1C58' [HKLM] . (.Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005.) =>.Microsoft Corporation

O90 - PUC: '22CEBCC8BD2D9CD45AA81E1A3F3AC8A8' [HKLM] . (.Microsoft Sync Framework 2.0 Core Components (x64) ENU .) -- C:\WINDOWS\Installer\{8CCBEC22-D2DB-4DC9-A58A-E1A1F3A38C8A}\ARPIco =>.Microsoft Corporation

O90 - PUC: '2E9444B40CBA15A489C9BC21713D4A33' [HKLM] . (.Intel(R) Serial IO.) =>.Intel Corporation

O90 - PUC: '4BD6D1222E64C3330BB9F59453D19008' [HKLM] . (.Microsoft Visual C++ 2017 x64 Minimum Runtime - 14.13.26020.) =>.Microsoft Corporation

O90 - PUC: '50FAAD8827A52D647A5C3C5769799E34' [HKLM] . (.SyncToy 2.1 (x64).) -- C:\WINDOWS\Installer\{88DAAF05-5A72-46D2-A7C5-C3759697E943}\\_6FEFF9B68218417F98F549.exe

O90 - PUC: '5282559C2FB74434AB193DDC644F4C14' [HKLM] . (.Intel(R) Trusted Connect Service Client x86.) =>.Intel Corporation

O90 - PUC: '5282559C2FB74434AB193DDC644F4C24' [HKLM] . (.Intel(R) Trusted Connect Service Client x64.) =>.Intel Corporation

O90 - PUC: '5A1A9B9E893699C4F8ED0197F456505C' [HKLM] . (.Intel(R) ME UninstallLegacy.) =>.Intel Corporation

O90 - PUC: '5A812990327ACD34D85B163756A6E149' [HKLM] . (.Dropbox Update Helper.) =>.WINSE

O90 - PUC: '62DBF9290209B993A9A757D1160F9B24' [HKLM] . (.Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005.) =>.Microsoft Corporation

O90 - PUC: '68AB67CA408033019195008142933911' [HKLM] . (.Adobe Refresh Manager.) -- C:\WINDOWS\Installer\{AC76BA86-0804-1033-1959-001824399311}\ARPPRODUCTICON.exe =>.Western Digital Technologies

O90 - PUC: '68AB67CA7DA76301B744CAF070E41400' [HKLM] . (.Adobe Acrobat Reader DC - Français.) -- C:\Windows\Installer\{AC76BA86-7AD7-1036-7B44-AC0F074E4100}\SC\_Reader.ico =>.Adobe Inc.

O90 - PUC: '6E8D947A316B3EB3F8F540C548BE2AB9' [HKLM] . (.Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005.) =>.Microsoft Corporation

O90 - PUC: '7223F443205F9124D94C91765E68AFAF' [HKLM] . (.Update for Windows 10 for x64-based Systems (KB4480730).) =>.Microsoft Corporation

O90 - PUC: '806DE995FDABD3C41927AEE56083E66F' [HKLM] . (.Microsoft VC++ redistributables repacked..) =>.bl.org

O90 - PUC: '80D53BF7C57C81A45B39D1C7E39807DA' [HKLM] . (.Intel(R) Chipset Device Software.) =>.Intel Corporation

O90 - PUC: '86DB901BA907B584796E56F1BE32A49C' [HKLM] . (.Backup and Sync from Google.) -- C:\WINDOWS\Installer\{B109BD68-709A-485B-97E6-651FEB234AC9}\DriveIcon =>.Google Inc.

O90 - PUC: '8915D598BD5CE57368BA31F3D4AAF92E' [HKLM] . (.Microsoft Visual C++ 2017 x86 Additional Runtime - 14.13.26020.) =>.Microsoft Corporation

O90 - PUC: '93BAD29AC2E44034A96BCB446EB8552E' [HKLM] . (.CCleaner Update Helper.)

O90 - PUC: 'A089CE062ADB6BC44A720BA745894BAC' [HKLM] . (.Google Update Helper.) =>.Google Inc.

O90 - PUC: 'A9BDCE5C0B9D7013AB58219699A8B5E3' [HKLM] . (.Microsoft Visual C++ 2017 x64 Additional Runtime - 14.13.26020.) =>.Microsoft Corporation

O90 - PUC: 'BDE526241FC9C1245804E0661F04D2CE' [HKLM] . (.Intel(R) Management Engine Driver.) =>.Intel Corporation

O90 - PUC: 'BFFA17FE5B58C7043A1093AE529F3831' [HKLM] . (.Intel® PROSet/Wireless WiFi Software.) -- C:\Windows\Installer\{EF71AFFB-85B5-407C-A301-39EA25F98313}\ARPPRODUCTICON.exe =>.Intel Corporation

O90 - PUC: 'C04EDCE63204A914A8E405BF17728567' [HKLM] . (.Thunderbolt™ Software.) -- C:\windows\Installer\{6ECDE40C-4023-419A-8A4E-50FB71275876}\app\_icon.ico =>.Thunderbolt

O90 - PUC: 'C6F172F8B7E6A0D359B1E6B796D487DB' [HKLM] . (.Microsoft Visual C++ 2017 x86 Minimum Runtime - 14.13.26020.) =>.Microsoft Corporation

O90 - PUC: 'C7C9AD31BFBE0D04491A554B8238FD12' [HKLM] . (.64 Bit HP CIO Components Installer.) =>.Hewlett-Packard

O90 - PUC: 'D7BB403109733AF4FAB8679469965F34' [HKLM] . (.PDFsam Basic.) -- C:\Windows\Installer\{1304BB7D-3790-4FA3-AF8B-76499669F543}\pdfsam.ico =>.Legitimate

O90 - PUC: 'E128CD23D7A48784EB8E33F71A357D2F' [HKLM] . (.Update for Windows 10 for x64-based Systems (KB4023057).) =>.Microsoft Corporation

O90 - PUC: 'E2D7D4DED46AA3C48A9B2BC71E352A6A' [HKLM] . (.Microsoft VC++ redistributables repacked..) =>.bl.org

O90 - PUC: 'E3DE76BEAC5E53F4D8D20FFE0108D2FB' [HKLM] . (.Intel(R) Management Engine Components.) =>.Intel Corporation

O90 - PUC: 'F542CA3046C4C52498FC77381C3DBAC2' [HKLM] . (.Microsoft Sync Framework 2.0 Provider Services (x64) ENU .) -- C:\WINDOWS\Installer\{03AC245F-4C64-425C-89CF-7783C1D3AB2C}\ARPIco =>.Microsoft Corporation

O90 - PUC: '4645D6EBF1B0CC6498379F56F16E4AA5' [HKCU] . (.Microsoft Lync Web App Plug-in.) -- %APPDATA%\Microsoft\Installer\{BE6D5464-0B1F-46CC-8973-F9651FE6A45A}\Icon\_Setup =>.Microsoft Corporation

O90 - PUC: '74E9D1CB72981AA48A197736CB42577B' [HKCU] . (.Skype Meetings App.) -- %APPDATA%\Microsoft\Installer\{BC1D9E47-8927-4AA1-A891-7763BC2475B7}\Icon\_Setup =>.Skype Technologies

O90 - PUC: 'E8D54C03B035A3C409018313F93EDC79' [HKCU] . (.MindFusion XML Viewer.) -- %APPDATA%\Microsoft\Installer\{30C45D8E-530B-4C3A-9010-38319FE3CD97}\\_853F67D554F05449430E7E.exe

O90 - PUC: '4645D6EBF1B0CC6498379F56F16E4AA5' [HKU] . (.Microsoft Lync Web App Plug-in.) -- %APPDATA%\Microsoft\Installer\{BE6D5464-0B1F-46CC-8973-F9651FE6A45A}\Icon\_Setup =>.Microsoft Corporation

O90 - PUC: '74E9D1CB72981AA48A197736CB42577B' [HKU] . (.Skype Meetings App.) -- %APPDATA%\Microsoft\Installer\{BC1D9E47-8927-4AA1-A891-7763BC2475B7}\Icon\_Setup =>.Skype Technologies

O90 - PUC: 'E8D54C03B035A3C409018313F93EDC79' [HKU] . (.MindFusion XML Viewer.) -- %APPDATA%\Microsoft\Installer\{30C45D8E-530B-4C3A-9010-38319FE3CD97}\\_853F67D554F05449430E7E.exe

**---\ PACKAGES WINDOWS INSTALLER (41) - 12s**

[MD5.1766B021B0BAB4F82259974154C5A920] [WIS][2020/03/21 10:10:14] (.Google LLC - Google Update Helper.) -- C:\WINDOWS\Installer\19489cab.msi [40960] =>.Google LLC

[MD5.76CA109CC56BD019F4EB2B967590092D] [WIS][2020/09/27 09:22:13] (.Adobe Systems Incorporated - Adobe ARM Installer.) -- C:\WINDOWS\Installer\19a1c620.msi [983040] =>.Adobe Systems Incorporated

[MD5.B986FCB841798312FE542D86ED1DBDB8] [WIS][2020/09/28 11:03:20] (.Google, Inc. - Backup and Sync from Google.) -- C:\WINDOWS\Installer\1f24ccda.msi [59670528] =>.Google, Inc.

[MD5.835F26FBE9F2DB8CD869D6E04FBCDB17] [WIS][2018/09/26 15:44:54] (.Intel Corporation - Intel® WiFi.) -- C:\WINDOWS\Installer\25f10f5.msi [65212416] =>.Intel Corporation

[MD5.1504667BA3C10D841C0B76B6412FAFB5] [WIS][2015/03/17 10:41:29] (.Adobe Systems Incorporated.) -- C:\WINDOWS\Installer\28d09d.msi [2805760] =>.Adobe Systems Incorporated

[MD5.EC3FE9BF98E5F91DE6AAF48C9E7FFCD7] [WIS][2018/01/26 11:06:34] (.Intel Corporation - Thunderbolt™ Software.) -- C:\WINDOWS\Installer\3539062.msi [8798208] =>.Intel Corporation

[MD5.F25913348DEEB950255F2AD51041F47E] [WIS][2019/08/26 09:20:51] (.MindFusion.) -- C:\WINDOWS\Installer\3c59c9d2.msi [1012736]

[MD5.0A96A49FDCF5129979DC7C33FB42B7C8] [WIS][2019/04/26 11:46:43] (.Sober Lemur S.a.s. di Vacondio Andrea - A free open source tool to manipulate PDF d.) -- C:\WINDOWS\Installer\4ccff2.msi [52801536]

[MD5.5FABCEE0867C1FF9E504E8B5DE26D592] [WIS][2018/03/04 16:51:52] (.HP Inc. - 64 Bit HP CIO Components Installer Package.) -- C:\WINDOWS\Installer\521231d1.msi [524288] =>.HP Inc.

[MD5.CDF265683C23467A1665DD8285DBD92A] [WIS][2017/11/09 23:09:06] (.Intel Corporation - Intel(R) Chipset Device Software.) -- C:\WINDOWS\Installer\7cc6.msi [1220608] =>.Intel Corporation

[MD5.0BB59749B49DB6A921C709C3C935A22E] [WIS][2017/11/08 12:24:56] (.Intel Corporation - Intel(R) ME UninstallLegacy.) -- C:\WINDOWS\Installer\7ccc.msi [471040] =>.Intel Corporation

[MD5.B7854FD5E7E1459B6998A628EB1A6F95] [WIS][2017/12/03 21:04:24] (.Intel Corporation - Intel(R) Management Engine Driver.) -- C:\WINDOWS\Installer\7cd2.msi [1675264] =>.Intel Corporation

[MD5.BE91AE3397278CD4933D3B9A8674C31A] [WIS][2017/12/03 21:03:10] (.Intel Corporation - Intel(R) Management Engine Components.) -- C:\WINDOWS\Installer\7cd8.msi [303104] =>.Intel Corporation

[MD5.72A53D555B641CE62E08FED70B4A9EAF] [WIS][2017/12/03 21:03:32] (.Intel Corporation - Microsoft VC++ redistributables repacked..) -- C:\WINDOWS\Installer\7cde.msi [12840960] =>.Intel Corporation

[MD5.D5FAAEA9D5F647E06D13FCD178BC912D] [WIS][2017/12/03 21:03:40] (.Intel Corporation - Microsoft VC++ redistributables repacked..) -- C:\WINDOWS\Installer\7ce4.msi [14307328] =>.Intel Corporation

[MD5.B02F1198FEE85D40B927AC56C5AA9C40] [WIS][2017/12/03 21:04:12] (.Intel Corporation - Intel(R) Management Engine Components.) -- C:\WINDOWS\Installer\7cea.msi [7324084] =>.Intel Corporation

[MD5.2D818C2D5E817EC87A1CD952B0E35A0A] [WIS][2017/11/16 20:24:52] (.Intel Corporation - Intel(R) Trusted Connect Service Client x64.) -- C:\WINDOWS\Installer\7cf0.msi [3686400] =>.Intel Corporation

[MD5.86C7E46126FABBB2ACAC9ED553423908] [WIS][2017/11/16 20:21:12] (.Intel Corporation - Intel(R) Trusted Connect Service Client x86.) -- C:\WINDOWS\Installer\7cf6.msi [8237056] =>.Intel Corporation

[MD5.3727EB96604C3100D153DF6A8A4BB0CF] [WIS][2017/11/15 10:38:10] (.Intel Corporation - Intel(R) Serial IO.) -- C:\WINDOWS\Installer\7cfc.msi [1351680] =>.Intel Corporation

[MD5.8D2A3DD90A921CC34164C04ACA1DED00] [WIS][2020/07/24 12:07:04] (.Dropbox, Inc. - Dropbox Update Helper.) -- C:\WINDOWS\Installer\83c9b3f.msi [24576] =>.Dropbox, Inc.

[MD5.881F98AF62764B6A8C21C2946F955167] [WIS][2020/09/03 17:52:40] (.Piriform Software - CCleaner Update Helper.) -- C:\WINDOWS\Installer\b80bd99.msi [32768] =>.Piriform Software

[MD5.16CD2BA3438D2627805A64D0F4DC063E] [WIS][2020/08/19 13:46:52] (.Adobe Inc..) -- C:\WINDOWS\Installer\100a8d19.msp [2781184] =>.Adobe Inc.

[MD5.DB596E2ADC480687F78F34B7D452D2CB] [WIS][2020/03/16 08:28:35] (.Adobe Inc..) -- C:\WINDOWS\Installer\10d5ea9d.msp [8130560] =>.Adobe Inc.

[MD5.2AD3AE06875E8C704DA9F109422277CF] [WIS][2020/07/06 14:20:53] (.Adobe Inc..) -- C:\WINDOWS\Installer\137a7499.msp [5853184] =>.Adobe Inc.

[MD5.7F1419CD81DEB4E238B7F0426B0782B7] [WIS][2020/05/11 08:43:48] (.Adobe Inc..) -- C:\WINDOWS\Installer\15123e2a.msp [50810880] =>.Adobe Inc.

[MD5.6C872B8971E67A78A683FD192919AB70] [WIS][2020/09/23 07:58:22] (.Adobe Inc..) -- C:\WINDOWS\Installer\1b2a673d.msp [33984512] =>.Adobe Inc.

[MD5.2CD061E09E48D7EFD5571169C5BB1386] [WIS][2019/10/24 14:03:06] (.Adobe Inc..) -- C:\WINDOWS\Installer\1ebd712c.msp [4616192] =>.Adobe Inc.

[MD5.2EA8602FA7F1CC88E5BB14CC6FCEE714] [WIS][2019/10/14 12:12:32] (.Adobe Inc..) -- C:\WINDOWS\Installer\264981f9.msp [20799488] =>.Adobe Inc.

[MD5.5705BA59CE2D386789436E2C34FC5635] [WIS][2019/12/19 10:53:18] (.Adobe Inc..) -- C:\WINDOWS\Installer\269257ec.msp [1863680] =>.Adobe Inc.

[MD5.923228256AD8BBCA145AE48027AA92BF] [WIS][2020/06/02 14:40:08] (.Adobe Inc..) -- C:\WINDOWS\Installer\26cb38c.msp [3026944] =>.Adobe Inc.

[MD5.C5D6FE428F4C19D4B0C11D189F6853F2] [WIS][2019/03/26 01:38:10] (.Adobe Inc..) -- C:\WINDOWS\Installer\28d09e.msp [228941824] =>.Adobe Inc.

[MD5.31A1DBE1A433F065C401CD0A73642712] [WIS][2019/11/13 13:16:36] (.Adobe Inc..) -- C:\WINDOWS\Installer\2f1fbc.msp [1527808] =>.Adobe Inc.

[MD5.BD4173F416AC180D7AD46CB583BAB949] [WIS][2020/05/21 18:16:51] (.Adobe Inc..) -- C:\WINDOWS\Installer\346440e1.msp [1392640] =>.Adobe Inc.

[MD5.04B8B2DEC9DFE83D56183D74F3ED40FB] [WIS][2019/08/22 13:14:18] (.Adobe Inc..) -- C:\WINDOWS\Installer\3953b376.msp [2002944] =>.Adobe Inc.

[MD5.AC729EF5FD5047779136DD8670413E03] [WIS][2020/07/31 05:39:02] (.Adobe Inc..) -- C:\WINDOWS\Installer\4290520d.msp [70844416] =>.Adobe Inc.

[MD5.B2D96888BC6646EBDEEFB59B363FD015] [WIS][2019/12/09 10:07:55] (.Adobe Inc..) -- C:\WINDOWS\Installer\430d6ce0.msp [30273536] =>.Adobe Inc.

[MD5.59E0FCA0A7F48848A6EF34ED7AC987C0] [WIS][2019/06/13 14:38:00] (.Adobe Inc..) -- C:\WINDOWS\Installer\48ae298.msp [2260992] =>.Adobe Inc.

[MD5.497275FFB9E10B5A29223D2A99322F49] [WIS][2020/02/10 09:01:58] (.Adobe Inc..) -- C:\WINDOWS\Installer\4a6af008.msp [25227264] =>.Adobe Inc.

[MD5.4777B622A4EA5AE5F2B67516AB0254AD] [WIS][2019/08/12 08:29:03] (.Adobe Inc..) -- C:\WINDOWS\Installer\4fb89e4.msp [50438144] =>.Adobe Inc.

[MD5.EF167BD45D286A7E38E769B6787DD73F] [WIS][2019/10/17 11:30:59] (.Adobe Inc..) -- C:\WINDOWS\Installer\9a57936.msp [2490368] =>.Adobe Inc.

[MD5.16551A09D3B9A3BC9049D098FBB4D529] [WIS][2019/05/13 08:57:34] (.Adobe Inc..) -- C:\WINDOWS\Installer\ba669.msp [59400192] =>.Adobe Inc.

**---\ FEATURE CONTROL. (145) - 0s**

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ACTIVEX\_REPURPOSEDETECTION]:PresentationHost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ADDON\_MANAGEMENT]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ADDON\_MANAGEMENT]:prevhost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ADDON\_MANAGEMENT]:wmplayer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ADDON\_MANAGEMENT]:VSTOInstaller.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_BEHAVIORS]:explorer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_BEHAVIORS]:iexplore.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_BEHAVIORS]:infopath.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_BEHAVIORS]:wmplayer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_BLOCK\_INPUT\_PROMPTS]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_BLOCK\_INPUT\_PROMPTS]:prevhost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_BLOCK\_LMZ\_IMG]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_BLOCK\_LMZ\_IMG]:PresentationHost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_BLOCK\_LMZ\_OBJECT]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_BLOCK\_LMZ\_OBJECT]:PresentationHost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_BLOCK\_LMZ\_SCRIPT]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_BLOCK\_LMZ\_SCRIPT]:PresentationHost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_BROWSER\_EMULATION]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_BROWSER\_EMULATION]:prevhost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_BROWSER\_EMULATION]:mbamtray.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_BROWSER\_EMULATION]:mbam.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_DISABLE\_LEGACY\_COMPRESSION]:PresentationHost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_DISABLE\_MK\_PROTOCOL]:explorer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_DISABLE\_MK\_PROTOCOL]:iexplore.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_DISABLE\_MK\_PROTOCOL]:SAPfewgsrv.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_DISABLE\_MK\_PROTOCOL]:SAPGUI.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_DISABLE\_MK\_PROTOCOL]:SAPGuiIT.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_DISABLE\_MK\_PROTOCOL]:SAPLgPad.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_DISABLE\_MK\_PROTOCOL]:SAPLOGON.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_DISABLE\_MK\_PROTOCOL]:Scale\_for\_R3.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_DISABLE\_MK\_PROTOCOL]:wmplayer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_DISABLE\_SQM\_UPLOAD\_FOR\_APP]:ieuser.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_DISABLE\_SQM\_UPLOAD\_FOR\_APP]:iexplore.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_DISABLE\_TELNET\_PROTOCOL]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_DISABLE\_TELNET\_PROTOCOL]:PresentationHost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_DISABLE\_UNICODE\_HANDLE\_CLOSING\_CALLBACK]:YahooMusicEngine.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_DOCUMENT\_COMPATIBLE\_MODE]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ENABLE\_SCRIPT\_PASTE\_URLACTION\_IF\_PROMPT]:devenv.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ENABLE\_SCRIPT\_PASTE\_URLACTION\_IF\_PROMPT]:dexplore.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ENABLE\_SCRIPT\_PASTE\_URLACTION\_IF\_PROMPT]:helppane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ENABLE\_SCRIPT\_PASTE\_URLACTION\_IF\_PROMPT]:PresentationHost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_FEEDS]:msfeedssync.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_FORCE\_ADDR\_AND\_STATUS]:PresentationHost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_FORCE\_ADDR\_AND\_STATUS]:prevhost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_HTTP\_USERNAME\_PASSWORD\_DISABLE]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_HTTP\_USERNAME\_PASSWORD\_DISABLE]:wmplayer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_HTTP\_USERNAME\_PASSWORD\_DISABLE]:VSTOInstaller.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_IGNORE\_XML\_PROLOG]:msiexec.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_IMAGING\_USE\_ART]:cs.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_IMAGING\_USE\_ART]:waol.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_IMAGING\_USE\_ART]:wm.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_INTERNET\_SHELL\_FOLDERS]:iexplore.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_LEGACY\_DISPPARAMS]:helppane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_LEGACY\_DLCONTROL\_BEHAVIORS]:wlmail.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN]:explorer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN]:iexplore.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN]:PresentationHost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN]:prevhost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN]:wmplayer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_LOCALMACHINE\_LOCKDOWN]:VSTOInstaller.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_MAXCONNECTIONSPER1\_0SERVER]:explorer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_MAXCONNECTIONSPERSERVER]:explorer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_MIME\_HANDLING]:explorer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_MIME\_HANDLING]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_MIME\_HANDLING]:iexplore.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_MIME\_HANDLING]:prevhost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_MIME\_HANDLING]:wmplayer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_MIME\_HANDLING]:VSTOInstaller.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_MIME\_SNIFFING]:explorer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_MIME\_SNIFFING]:iexplore.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_MIME\_SNIFFING]:wmplayer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_MIME\_SNIFFING]:VSTOInstaller.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_MSHTML\_AUTOLOAD\_IEFRAME]:mshta.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_MSHTML\_AUTOLOAD\_IEFRAME]:outlook.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_MSHTML\_AUTOLOAD\_IEFRAME]:sidebar.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_OBJECT\_CACHING]:explorer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_OBJECT\_CACHING]:iexplore.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_OBJECT\_CACHING]:wmplayer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_OBJECT\_CACHING]:VSTOInstaller.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_PROTOCOL\_LOCKDOWN]:explorer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_PROTOCOL\_LOCKDOWN]:iexplore.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_PROTOCOL\_LOCKDOWN]:wmplayer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_PROTOCOL\_LOCKDOWN]:VSTOInstaller.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_RELEASE\_CALLBACK\_ON\_STOP\_BINDING]:communicator.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_RESTRICT\_ABOUT\_PROTOCOL\_IE7]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_RESTRICT\_ABOUT\_PROTOCOL\_IE7]:PresentationHost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_RESTRICT\_ABOUT\_PROTOCOL\_IE7]:prevhost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_RESTRICT\_ACTIVEXINSTALL]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_RESTRICT\_ACTIVEXINSTALL]:prevhost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_RESTRICT\_ACTIVEXINSTALL]:wmplayer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_RESTRICT\_ACTIVEXINSTALL]:VSTOInstaller.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_RESTRICT\_FILEDOWNLOAD]:msimn.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_RESTRICT\_FILEDOWNLOAD]:prevhost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_RESTRICT\_FILEDOWNLOAD]:winmail.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_RESTRICT\_FILEDOWNLOAD]:wmplayer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_RESTRICT\_FILEDOWNLOAD]:VSTOInstaller.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_RESTRICT\_OBJECT\_DATA\_ATTRIBUTE]:PresentationHost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_RESTRICT\_RES\_TO\_LMZ]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_RESTRICT\_RES\_TO\_LMZ]:PresentationHost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_RESTRICT\_RES\_TO\_LMZ]:prevhost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_SAFE\_BINDTOOBJECT]:explorer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_SAFE\_BINDTOOBJECT]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_SAFE\_BINDTOOBJECT]:iexplore.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_SAFE\_BINDTOOBJECT]:wmplayer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_SAFE\_BINDTOOBJECT]:VSTOInstaller.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_SECURITYBAND]:prevhost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_SECURITYBAND]:wmplayer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_SECURITYBAND]:VSTOInstaller.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_SHIM\_MSHELP\_COMBINE]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_SHIM\_MSHELP\_COMBINE]:prevhost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_SHOW\_APP\_PROTOCOL\_WARN\_DIALOG]:PresentationHost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_SSLUX]:PresentationHost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_SUBDOWNLOAD\_LOCKDOWN]:msimn.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_SUBDOWNLOAD\_LOCKDOWN]:outlook.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_SUBDOWNLOAD\_LOCKDOWN]:winmail.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_UNC\_SAVEDFILECHECK]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_UNC\_SAVEDFILECHECK]:wmplayer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_UNC\_SAVEDFILECHECK]:VSTOInstaller.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_USE\_WINDOWEDSELECTCONTROL]:infopath.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_USE\_WINDOWEDSELECTCONTROL]:excel.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_USE\_WINDOWEDSELECTCONTROL]:powerpnt.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_USE\_WINDOWEDSELECTCONTROL]:winword.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_VALIDATE\_NAVIGATE\_URL]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_VALIDATE\_NAVIGATE\_URL]:prevhost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_VALIDATE\_NAVIGATE\_URL]:wmplayer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_VALIDATE\_NAVIGATE\_URL]:VSTOInstaller.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_VIEWLINKEDWEBOC\_IS\_UNSAFE]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_WEBOC\_MOVESIZECHILD]:msn.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_WEBOC\_POPUPMANAGEMENT]:explorer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_WEBOC\_POPUPMANAGEMENT]:iexplore.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_WEBOC\_POPUPMANAGEMENT]:wmplayer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_WEBOC\_POPUPMANAGEMENT]:VSTOInstaller.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_WINDOW\_RESTRICTIONS]:explorer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_WINDOW\_RESTRICTIONS]:iexplore.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_WINDOW\_RESTRICTIONS]:wmplayer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_WINDOW\_RESTRICTIONS]:VSTOInstaller.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_XSSFILTER]:iexplore.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_XSSFILTER]:prevhost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ZONE\_ELEVATION]:explorer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ZONE\_ELEVATION]:iexplore.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ZONE\_ELEVATION]:PresentationHost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ZONE\_ELEVATION]:prevhost.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ZONE\_ELEVATION]:wmplayer.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE\_ZONE\_ELEVATION]:VSTOInstaller.exe =>.Legitimate

**---\ OBSERVATEURS des évènements (116) - 47s**

Application.Error: Outlook (108)

~Numéro: 16314

~Date: 09/30/2020 04:23:19 PM

~ID: 62

~Description: Une session du moteur de classification Microsoft a échoué pour l’utilisateur : eric.loutre@dxc.com - code d’erreur 0x80040206.

~Suggestion: Aucune

Application.Warning: ESENT (132)

~Numéro: 16248

~Date: 09/30/2020 09:06:51 AM

~ID: 642

~Description: %1 (%2) %3La version %5 de la fonctionnalité de format de base de données n’a pas pu être utilisée, car le format actuel de base de données %6 est contrôlé par le paramètre %4.

Application.Error: Application Error (4)

~Numéro: 15627

~Date: 09/27/2020 07:18:39 PM

~ID: 1000

~Description: Nom de l’application défaillante %1, version : %2, horodatage : 0x5f4ec140 Nom du module défaillant : %4, version : %5, horodatage : 0x5b4a3325 Code d’exception : 0xc000027b Décalage d’erreur : 0x000000000010b3cc ID du processus défaillant : 0x2f44 H

~Suggestion: Réparer ou réinstaller l'application.

Application.Error: DPTF (4)

~Numéro: 14167

~Date: 09/22/2020 09:55:14 AM

~ID: 256

~Description: %1 : %2

Application.Warning: Microsoft-Windows-RestartManager (148)

~Numéro: 14128

~Date: 09/22/2020 09:16:30 AM

~ID: 10010

~Description: Impossible de redémarrer l’application « %3 » (pid %2) - %9.

~Suggestion: Redémarrer manuellement l'application ou le service

Application.Warning: Goodix (4)

~Numéro: 13242

~Date: 09/16/2020 07:38:06 PM

~ID: 1519

~Description:

Application.Error: VSS (2)

~Numéro: 13092

~Date: 09/16/2020 05:08:36 PM

~ID: 8193

~Description: Erreur du service de cliché instantané des volumes : erreur lors de l’appel de la routine %1. hr = %2.

~Suggestion: Utiliser la procédure de reconstruction du VSS

Application.Error: Application Hang (2)

~Numéro: 11847

~Date: 09/13/2020 06:10:12 PM

~ID: 1002

~Description: Le programme %1 version %2 a cessé d'interagir avec Windows et a été fermé. Pour voir si plus d'informations sur le problème sont disponibles, vérifiez l'historique des problèmes dans le Panneau de configuration Sécurité et maintenance. ID de proces

~Suggestion: Essayer les commandes suivantes ipconfig /release et ipconfig / renew.

Application.Warning: Microsoft-Windows-WMI (6)

~Numéro: 11331

~Date: 09/11/2020 10:18:32 AM

~ID: 63

~Description: Un fournisseur, %1, a été inscrit dans l’espace de noms Windows Management Instrumentation %2, afin d’utiliser le compte LocalSystem. Ce compte bénéficie de privilèges et le fournisseur peut provoquer une violation de sécurité s’il ne représente pas

~Suggestion: Généralement LocalSystem n'est pas nécessaire et le contexte de sécurité NetworkServiceHost est plus approprié.

System.Warning: DCOM (355)

~Numéro: 11277

~Date: 09/30/2020 04:34:15 PM

~ID: 10016

~Description: propres à l’applicationLocalExécution{21B896BF-008D-4D01-A27B-26061B960DD7}{03E09F3B-DCE4-44FE-A9CF-82D050827E1C}ELOUTRE\_PCericlS-1-5-21-4226646855-4164925663-2316759709-1001LocalHost (avec LRPC)Non disponibleNon disponible

~Suggestion: Vérifier les autorisations pour l'accès DCOM

System.Warning: HidBth (43)

~Numéro: 11150

~Date: 09/30/2020 10:11:05 AM

~ID: 2

~Description: Le périphérique HID Bluetooth %2 est hors de portée ou ne répond plus.

System.Warning: Netwtw06 (58)

~Numéro: 11111

~Date: 09/30/2020 02:43:09 AM

~ID: 6105

~Description: 6105 - deauth after EAPOL key exchange sequence

System.Warning: Microsoft-Windows-DNS-Client (57)

~Numéro: 10987

~Date: 09/29/2020 07:20:23 AM

~ID: 1014

~Description: La résolution du nom %1 a expiré lorsqu’aucun des serveurs DNS configurés n’a répondu.

~Suggestion: https://social.technet.microsoft.com/wiki/contents/articles/3336.event-id-1014-microsoft-windows-dns-client.aspx

System.Warning: Microsoft-Windows-Kernel-Processor-Power (12)

~Numéro: 10947

~Date: 09/28/2020 06:04:17 PM

~ID: 37

~Description: La vitesse du processeur logique Hyper-V %2 est limitée par le microprogramme du système. Le processeur a connu cet état de performances réduites pendant %3 secondes depuis le dernier rapport.

System.Warning: Microsoft-Windows-WLAN-AutoConfig (21)

~Numéro: 10813

~Date: 09/28/2020 11:32:50 AM

~ID: 10002

~Description: Le module d’extensibilité WLAN s’est arrêté. Chemin d’accès du module : C:\WINDOWS\system32\IntelWifiIhv06.dll

~Suggestion: 1)Désactivez/Réactiver la connexion réseau sans fil. ou 2) Redémarrer le service WLAN AutoConfig

System.Warning: Microsoft-Windows-Resource-Exhaustion-Detector (7)

~Numéro: 10723

~Date: 09/27/2020 07:18:16 PM

~ID: 2004

~Description: Windows a diagnostiqué avec succès une insuffisance en mémoire virtuelle. La plus grande consommation de mémoire virtuelle s’est répartie entre les programmes suivants : %21 (%22) avec %24 octets, %28 (%29) avec %31 octets et %35 (%36) avec %38 octet

System.Warning: Microsoft-Windows-TPM-WMI (3)

~Numéro: 9450

~Date: 09/22/2020 09:55:20 AM

~ID: 1538

~Description: Impossible de connecter l’approvisionnement du certificat d’intégrité d’appareil à %1. -2147012889

System.Warning: Microsoft-Windows-Kernel-PnP (26)

~Numéro: 9424

~Date: 09/22/2020 09:55:09 AM

~ID: 219

~Description: Le chargement du pilote %5 a échoué pour le périphérique %2.

~Suggestion: Vérifier que le pilote a bien été chargé dans les informations système

System.Warning: BTHUSB (1)

~Numéro: 9090

~Date: 09/18/2020 10:22:45 AM

~ID: 3

~Description: Une commande envoyée à la carte a expiré ; la carte n'a pas répondu.

System.Error: Schannel (8)

~Numéro: 8327

~Date: 09/15/2020 09:17:17 AM

~ID: 4103

~Description: Une erreur irrécupérable s'est produite lors de la création des informations d'identification %1 pour TLS. État d'erreur interne : %2.

System.Warning: Microsoft-Windows-Time-Service (6)

~Numéro: 7488

~Date: 09/11/2020 08:58:24 AM

~ID: 134

~Description: NtpClient n'a pas pu définir d'homologue manuel utilisable comme source de temps en raison d'une erreur de résolution DNS sur '%3'. NtpClient réessaiera dans %2 minutes, puis doublera l'intervalle d'attente pour les tentatives suivantes. L'erreur éta

~Suggestion: Resynchroniser le client avec l'homologue de source de temps

**---\ SCAN ADDITIONNEL (8) - 6s**

C:\Users\ericl\AppData\Local\Google\Chrome\User Data\Default\File System\000 =>.SUP.Temporary.Chrome

C:\Users\ericl\AppData\Local\Google\Chrome\User Data\Default\File System\001 =>.SUP.Temporary.Chrome

C:\Users\ericl\AppData\Local\Google\Chrome\User Data\Default\File System\002 =>.SUP.Temporary.Chrome

C:\Users\ericl\AppData\Local\Google\Chrome\User Data\Default\File System\003 =>.SUP.Temporary.Chrome

[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files\Huawei\PCManager\HwPhotoViewer.exe.FriendlyAppName =>.Unsigned

[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files\Huawei\PCManager\HwPhotoViewer.exe.ApplicationCompany =>.Unsigned

[HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files\Huawei\PCManager\HwPhotoViewer.exe.FriendlyAppName =>.Unsigned

[HKU\S-1-5-21-4226646855-4164925663-2316759709-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files\Huawei\PCManager\HwPhotoViewer.exe.ApplicationCompany =>.Unsigned

**---\ RÉCAPITULATIF DES ÉLÉMENTS TROUVÉS (4) - 0s**

https://nicolascoolman.eu/2017/09/12/origine-lignes-orphelines/ =>.SUP.Orphan

https://nicolascoolman.eu/forum/Topic/warning-eventlogapp-evenement-dapplication/ =>Warning.EventLogApp

https://nicolascoolman.eu/forum/Topic/warning-eventlogsys-evenement-systeme/ =>Warning.EventLogSys

https://nicolascoolman.eu/forum/Topic/logiciels-potentiellement-superflus-lps/ =>.SUP.Temporary.Chrome

~ Unselected Options: WR, O82,

~ End of the scan, 9129 items in 03mn53s (2252)(0)

**NUMEROS DE SÉRIE**

[017CA19B5859E83F44D874C1CE506E6D] [26/04/2019] (.Dropbox, Inc.) - C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe

[019BB53DD06F10B3DBA82E8D3FAF6588] [19/01/2019] (.Dolby Laboratories, Inc..) - C:\WINDOWS\System32\dolbyaposvc\DAX3API.exe

[02FA994D660DE659EE9037ECB437D766] [03/09/2020] (.Piriform Software Ltd.) - C:\Program Files (x86)\CCleaner Browser\Update\1.8.1067.0\CCleanerBrowserCrashHandler.exe

[02FA994D660DE659EE9037ECB437D766] [03/09/2020] (.Piriform Software Ltd.) - C:\Program Files (x86)\CCleaner Browser\Update\1.8.1067.0\CCleanerBrowserCrashHandler64.exe

[02FA994D660DE659EE9037ECB437D766] [03/09/2020] (.Piriform Software Ltd.) - C:\Program Files (x86)\CCleaner Browser\Update\CCleanerBrowserUpdate.exe

[02FA994D660DE659EE9037ECB437D766] [05/08/2020] (.Piriform Software Ltd.) - C:\Program Files\CCleaner\CCleaner64.exe

[02FA994D660DE659EE9037ECB437D766] [05/08/2020] (.Piriform Software Ltd.) - C:\Program Files\CCleaner\uninst.exe

[02FA994D660DE659EE9037ECB437D766] [10/09/2020] (.Piriform Software Ltd.) - C:\Program Files (x86)\CCleaner Browser\Application\85.0.5824.105\elevation\_service.exe

[02FA994D660DE659EE9037ECB437D766] [10/09/2020] (.Piriform Software Ltd.) - C:\Program Files (x86)\CCleaner Browser\Application\CCleanerBrowser.exe

[02FA994D660DE659EE9037ECB437D766] [19/08/2020] (.Piriform Software Ltd.) - C:\Program Files (x86)\CCleaner Browser\CCleanerBrowserUninstall.exe

[031CE845CCA97AAE1EAD8B6464F9C7B6] [10/05/2017] (.Jernej Simončič.) - C:\Program Files\GIMP 2\bin\gimp-2.8.exe

[031CE845CCA97AAE1EAD8B6464F9C7B6] [30/09/2019] (.Jernej Simončič.) - C:\Program Files\GIMP 2\uninst\unins000.exe

[044E3BF58976880FFD074448A8F7A058] [22/09/2020] (.Malwarebytes Corporation.) - C:\WINDOWS\System32\drivers\mbae64.sys

[044E3BF58976880FFD074448A8F7A058] [26/06/2019] (.Malwarebytes Corporation.) - C:\Program Files\Malwarebytes\Anti-Malware\mbshlext.dll

[045D9B6716C516EF45A1216DFD9F3060] [29/03/2019] (.Realtek Semiconductor Corp..) - C:\WINDOWS\System32\drivers\RTKVHD64.sys

[04DF4D56733AE38D598EA004DD2D9C51] [12/02/2020] (.Realtek Semiconductor Corp..) - C:\WINDOWS\System32\drivers\rtux64w10.sys

[0510C6B2FF7AB71C786EF572239B1243] [12/05/2020] (.Zoom Video Communications, Inc..) - C:\Users\ericl\AppData\Roaming\Zoom\bin\Zoom.exe

[0510C6B2FF7AB71C786EF572239B1243] [12/05/2020] (.Zoom Video Communications, Inc..) - C:\Users\ericl\AppData\Roaming\Zoom\uninstall\Installer.exe

[063D0C011B143C57893FE839779AFCD0] [23/01/2019] (.Realtek Semiconductor Corp..) - C:\Program Files (x86)\InstallShield Installation Information\{F132AF7F-7BCA-4EDE-8A7C-958108FE7DBC}\setup.exe

[063D0C011B143C57893FE839779AFCD0] [29/03/2019] (.Realtek Semiconductor Corp..) - C:\WINDOWS\System32\RtkAudUService64.exe

[06AEA76BAC46A9E8CFE6D29E45AAF033] [21/03/2020] (.Google LLC.) - C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleCrashHandler.exe

[06AEA76BAC46A9E8CFE6D29E45AAF033] [21/03/2020] (.Google LLC.) - C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleCrashHandler64.exe

[08557A49A29FFD9253CA5AC8780F2C95] [09/09/2020] (.Dropbox, Inc.) - C:\Program Files (x86)\Dropbox\Client\DropboxExt64.45.0.dll

[08557A49A29FFD9253CA5AC8780F2C95] [22/09/2020] (.Dropbox, Inc.) - C:\Program Files (x86)\Dropbox\Client\106.4.368\QtWebEngineProcess.exe

[08557A49A29FFD9253CA5AC8780F2C95] [22/09/2020] (.Dropbox, Inc.) - C:\Program Files (x86)\Dropbox\Client\Dropbox.exe

[08557A49A29FFD9253CA5AC8780F2C95] [22/09/2020] (.Dropbox, Inc.) - C:\Program Files (x86)\Dropbox\Client\DropboxUninstaller.exe

[08557A49A29FFD9253CA5AC8780F2C95] [22/09/2020] (.Dropbox, Inc.) - C:\WINDOWS\System32\DbxSvc.exe

[08A2EC4E78A09E174B192E5535984B59] [05/09/2020] (.Malwarebytes Inc.) - C:\ProgramData\Malwarebytes\MBAMService\IrisPlugins\mbam\_modal\_bg\_precon\_r01.1.0.3.x64.dll

[08A2EC4E78A09E174B192E5535984B59] [16/09/2020] (.Malwarebytes Inc.) - C:\ProgramData\Malwarebytes\MBAMService\IrisPlugins\UIPlugin.EXPT-71.x64.dll

[08A2EC4E78A09E174B192E5535984B59] [16/09/2020] (.Malwarebytes Inc.) - C:\ProgramData\Malwarebytes\MBAMService\IrisPlugins\UIPlugin.EXPT-97-CU16.x64.dll

[08A2EC4E78A09E174B192E5535984B59] [18/09/2020] (.Malwarebytes Inc.) - C:\WINDOWS\System32\Drivers\MbamChameleon.sys

[08A2EC4E78A09E174B192E5535984B59] [21/09/2020] (.Malwarebytes Inc.) - C:\Program Files\Malwarebytes\Anti-Malware\mbuns.exe

[08A2EC4E78A09E174B192E5535984B59] [21/09/2020] (.Malwarebytes Inc.) - C:\ProgramData\Malwarebytes\MBAMService\instlrupdate\MBSetup.exe

[08A2EC4E78A09E174B192E5535984B59] [22/09/2020] (.Malwarebytes Inc.) - C:\Program Files\Malwarebytes\Anti-Malware\MBAMService.exe

[08A2EC4E78A09E174B192E5535984B59] [22/09/2020] (.Malwarebytes Inc.) - C:\Program Files\Malwarebytes\Anti-Malware\mbamtray.exe

[08A2EC4E78A09E174B192E5535984B59] [22/09/2020] (.Malwarebytes Inc.) - C:\WINDOWS\System32\Drivers\mbamswissarmy.sys

[0C15BE4A15BB0903C901B1D6C265302F] [04/09/2020] (.Google LLC.) - C:\Users\ericl\AppData\Local\Google\Chrome\Temp\scoped\_dir2400\_443439412\old\_chrome.exe

[0C15BE4A15BB0903C901B1D6C265302F] [09/09/2020] (.Google LLC.) - C:\Program Files\Google\Drive\contextmenu64.dll

[0C15BE4A15BB0903C901B1D6C265302F] [09/09/2020] (.Google LLC.) - C:\Program Files\Google\Drive\googledrivesync.exe

[0C15BE4A15BB0903C901B1D6C265302F] [09/09/2020] (.Google LLC.) - C:\Program Files\Google\Drive\googledrivesync64.dll

[0C15BE4A15BB0903C901B1D6C265302F] [19/09/2020] (.Google LLC.) - C:\Users\ericl\AppData\Local\Google\Chrome\Application\85.0.4183.121\chrome.dll

[0C15BE4A15BB0903C901B1D6C265302F] [19/09/2020] (.Google LLC.) - C:\Users\ericl\AppData\Local\Google\Chrome\Application\85.0.4183.121\chrome\_elf.dll

[0C15BE4A15BB0903C901B1D6C265302F] [19/09/2020] (.Google LLC.) - C:\Users\ericl\AppData\Local\Google\Chrome\Application\85.0.4183.121\chrome\_pwa\_launcher.exe

[0C15BE4A15BB0903C901B1D6C265302F] [19/09/2020] (.Google LLC.) - C:\Users\ericl\AppData\Local\Google\Chrome\Application\85.0.4183.121\elevation\_service.exe

[0C15BE4A15BB0903C901B1D6C265302F] [19/09/2020] (.Google LLC.) - C:\Users\ericl\AppData\Local\Google\Chrome\Application\85.0.4183.121\eventlog\_provider.dll

[0C15BE4A15BB0903C901B1D6C265302F] [19/09/2020] (.Google LLC.) - C:\Users\ericl\AppData\Local\Google\Chrome\Application\85.0.4183.121\libEGL.dll

[0C15BE4A15BB0903C901B1D6C265302F] [19/09/2020] (.Google LLC.) - C:\Users\ericl\AppData\Local\Google\Chrome\Application\85.0.4183.121\libGLESv2.dll

[0C15BE4A15BB0903C901B1D6C265302F] [19/09/2020] (.Google LLC.) - C:\Users\ericl\AppData\Local\Google\Chrome\Application\85.0.4183.121\mojo\_core.dll

[0C15BE4A15BB0903C901B1D6C265302F] [19/09/2020] (.Google LLC.) - C:\Users\ericl\AppData\Local\Google\Chrome\Application\85.0.4183.121\notification\_helper.exe

[0C15BE4A15BB0903C901B1D6C265302F] [19/09/2020] (.Google LLC.) - C:\Users\ericl\AppData\Local\Google\Chrome\Application\85.0.4183.121\swiftshader\libEGL.dll

[0C15BE4A15BB0903C901B1D6C265302F] [19/09/2020] (.Google LLC.) - C:\Users\ericl\AppData\Local\Google\Chrome\Application\85.0.4183.121\swiftshader\libGLESv2.dll

[0C15BE4A15BB0903C901B1D6C265302F] [19/09/2020] (.Google LLC.) - C:\Users\ericl\AppData\Local\Google\Chrome\Application\85.0.4183.121\WidevineCdm\\_platform\_specific\win\_x64\widevinecdm.dll

[0C15BE4A15BB0903C901B1D6C265302F] [19/09/2020] (.Google LLC.) - C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome.exe

[0C15BE4A15BB0903C901B1D6C265302F] [19/09/2020] (.Google LLC.) - C:\Users\ericl\AppData\Local\Google\Chrome\Application\chrome\_proxy.exe

[0C15BE4A15BB0903C901B1D6C265302F] [22/09/2020] (.Google LLC.) - C:\Users\ericl\AppData\Local\Google\Chrome\User Data\SwReporter\85.244.200\software\_reporter\_tool.exe

[0C15BE4A15BB0903C901B1D6C265302F] [23/09/2020] (.Google LLC.) - C:\Users\ericl\AppData\Local\Google\Chrome\Application\85.0.4183.121\Installer\setup.exe

[0D2CACCD3E9EEC06738410BA31BF6595] [08/09/2020] (.Adobe Inc..) - C:\Users\ericl\AppData\Local\Google\Chrome\User Data\PepperFlash\32.0.0.433\pepflashplayer.dll

[0DDEB53F957337FBEAF98C4A615B149D] [13/07/2020] (.Mozilla Corporation.) - C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe

[0DDEB53F957337FBEAF98C4A615B149D] [13/07/2020] (.Mozilla Corporation.) - C:\Program Files\Mozilla Firefox\firefox.exe

[0DDEB53F957337FBEAF98C4A615B149D] [13/07/2020] (.Mozilla Corporation.) - C:\Program Files\Mozilla Firefox\uninstall\helper.exe

[0E4C1A84EE436C73F30978E7D4C34C0B] [18/05/2017] (.Samsung Electronics Co., Ltd..) - C:\WINDOWS\System32\DRIVERS\ssudbus.sys

[0E4C1A84EE436C73F30978E7D4C34C0B] [18/05/2017] (.Samsung Electronics Co., Ltd..) - C:\WINDOWS\System32\DRIVERS\ssudmdm.sys

[0EE3F1C8F451CBF21203341A53F23E71] [06/09/2020] (.Adobe Inc..) - C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe

[0EE3F1C8F451CBF21203341A53F23E71] [11/09/2020] (.Adobe Inc..) - C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe

[0EE3F1C8F451CBF21203341A53F23E71] [31/07/2020] (.Adobe Inc..) - C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe

[0FA5B80428F4624CF9672211E1956FBE] [23/04/2020] (.VideoLAN.) - C:\program files\videolan\vlc\vlc.exe

[1044F31AE1F93A0BB95F19AB9FAAC6BB] [24/09/2020] (.ESET, spol. s r.o..) - C:\Users\ericl\AppData\Local\Google\Chrome\User Data\SwReporter\85.244.200\edls\_64.dll

[1044F31AE1F93A0BB95F19AB9FAAC6BB] [24/09/2020] (.ESET, spol. s r.o..) - C:\Users\ericl\AppData\Local\Google\Chrome\User Data\SwReporter\85.244.200\em000\_64.dll

[1044F31AE1F93A0BB95F19AB9FAAC6BB] [24/09/2020] (.ESET, spol. s r.o..) - C:\Users\ericl\AppData\Local\Google\Chrome\User Data\SwReporter\85.244.200\em001\_64.dll

[1044F31AE1F93A0BB95F19AB9FAAC6BB] [24/09/2020] (.ESET, spol. s r.o..) - C:\Users\ericl\AppData\Local\Google\Chrome\User Data\SwReporter\85.244.200\em002\_64.dll

[1044F31AE1F93A0BB95F19AB9FAAC6BB] [24/09/2020] (.ESET, spol. s r.o..) - C:\Users\ericl\AppData\Local\Google\Chrome\User Data\SwReporter\85.244.200\em003\_64.dll

[1044F31AE1F93A0BB95F19AB9FAAC6BB] [24/09/2020] (.ESET, spol. s r.o..) - C:\Users\ericl\AppData\Local\Google\Chrome\User Data\SwReporter\85.244.200\em004\_64.dll

[1044F31AE1F93A0BB95F19AB9FAAC6BB] [24/09/2020] (.ESET, spol. s r.o..) - C:\Users\ericl\AppData\Local\Google\Chrome\User Data\SwReporter\85.244.200\em005\_64.dll

[14F8FDD167F92402B1570B5DC495C815] [07/11/2019] (.Google Inc.) - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe

[330000017BB47778D9105DF03500000000017B] [11/07/2020] (.Skype Software Sarl.) - C:\Program Files\WindowsApps\Microsoft.SkypeApp\_15.61.100.0\_x86\_\_kzf8qxf38zg5c\Skype\Skype.exe

[330000B960C6D07C955AC0FCF000020000B960] [03/11/2017] (.Intel(R) Software.) - C:\Program Files\Intel\Intel(R) Dynamic Platform and Thermal Framework\Uninstall\Setup.exe

[330000C1099D64BE0C43EAE20500020000C109] [03/02/2018] (.Intel(R) pGFX.) - C:\Windows\System32\DriverStore\FileRepository\sgx\_psw.inf\_amd64\_1781f8bae8fdf5c0\aesm\_service.exe

[4FBE0A02426EBD20C26244B5ECA652A3] [11/09/2018] (.NVIDIA Corporation.) - C:\Windows\System32\DriverStore\FileRepository\nvhw.inf\_amd64\_98eca3702c3cd36e\nvlddmkm.sys

[4FBE0A02426EBD20C26244B5ECA652A3] [18/06/2019] (.NVIDIA Corporation.) - C:\Program Files\NVIDIA Corporation\NvTelemetry\NvTelemetryContainer.exe

[4FBE0A02426EBD20C26244B5ECA652A3] [27/08/2018] (.NVIDIA Corporation.) - C:\Program Files\NVIDIA Corporation\Display.NvContainer\NVDisplay.Container.exe

[56000001475EA46CCAEF0B7481000000000147] [07/11/2018] (.Intel(R) Trust Services.) - C:\ProgramData\Package Cache\{66129f84-d3f0-4884-ac54-369ae6fc2cf6}\iclsClientInstaller.exe

[56000001475EA46CCAEF0B7481000000000147] [16/11/2017] (.Intel(R) Trust Services.) - C:\Program Files\Intel\Intel(R) Management Engine Components\iCLS\SocketHeciServer.exe

[56000001475EA46CCAEF0B7481000000000147] [16/11/2017] (.Intel(R) Trust Services.) - C:\Program Files\Intel\Intel(R) Management Engine Components\iCLS\TPMProvisioningService.exe

[5600000159652951D46F2579A1000000000159] [26/01/2018] (.Intel(R) Client Connectivity Division SW.) - C:\Program Files (x86)\Intel\Thunderbolt Software\tbtsvc.exe

[56000001757376CD78AD000C9A000000000175] [03/12/2017] (.Intel(R) Embedded Subsystems and IP Blocks Group.) - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\DAL\jhi\_service.exe

[56000001757376CD78AD000C9A000000000175] [03/12/2017] (.Intel(R) Embedded Subsystems and IP Blocks Group.) - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe

[56000001757376CD78AD000C9A000000000175] [03/12/2017] (.Intel(R) Embedded Subsystems and IP Blocks Group.) - C:\ProgramData\Intel\Package Cache\{1CEAC85D-2590-4760-800F-8DE5E91F3700}\Setup.exe

[56000001757376CD78AD000C9A000000000175] [14/11/2017] (.Intel(R) Embedded Subsystems and IP Blocks Group.) - C:\WINDOWS\System32\drivers\iaLPSS2\_SPI.sys

[56000001757376CD78AD000C9A000000000175] [14/11/2017] (.Intel(R) Embedded Subsystems and IP Blocks Group.) - C:\WINDOWS\System32\drivers\iaLPSS2\_UART2.sys

[56000001757376CD78AD000C9A000000000175] [28/11/2017] (.Intel(R) Embedded Subsystems and IP Blocks Group.) - C:\WINDOWS\System32\drivers\TeeDriverW8x64.sys

[56000001F46907127A1D6406CD0000000001F4] [09/03/2018] (.Intel(R) Wireless Connectivity Solutions.) - C:\WINDOWS\System32\drivers\ibtusb.sys

[56000001F46907127A1D6406CD0000000001F4] [26/04/2019] (.Intel(R) Wireless Connectivity Solutions.) - C:\ProgramData\Package Cache\{3d609846-847c-46e5-9a23-682bec1569ea}\ISetup.exe

[56000002143D5BA1B4E496B7C1000000000214] [07/11/2018] (.Intel(R) Software and Firmware Products.) - C:\ProgramData\Package Cache\{44ded3eb-1686-46a6-9770-fd79096c29f7}\SetupChipset.exe

[56000002630B69CF9D33644CF0000000000263] [15/11/2017] (.Intel(R) Serial IO.) - C:\ProgramData\Intel\Package Cache\{9FD91C5C-44AE-4D9D-85BE-AE52816B0294}\Setup.exe

[56000005DAB0988313DA8AB3E10000000005DA] [10/10/2018] (.Intel(R) pGFX.) - C:\Windows\System32\DriverStore\FileRepository\igdlh64.inf\_amd64\_c8634ed19e331cda\igdkmd64.sys

[56000005DAB0988313DA8AB3E10000000005DA] [10/10/2018] (.Intel(R) pGFX.) - C:\Windows\System32\DriverStore\FileRepository\igdlh64.inf\_amd64\_c8634ed19e331cda\igfxCUIService.exe

[56000005DAB0988313DA8AB3E10000000005DA] [10/10/2018] (.Intel(R) pGFX.) - C:\Windows\System32\DriverStore\FileRepository\igdlh64.inf\_amd64\_c8634ed19e331cda\igfxEM.exe

[56000005DAB0988313DA8AB3E10000000005DA] [10/10/2018] (.Intel(R) pGFX.) - C:\Windows\System32\DriverStore\FileRepository\igdlh64.inf\_amd64\_c8634ed19e331cda\IntelCpHDCPSvc.exe

[56000005DAB0988313DA8AB3E10000000005DA] [10/10/2018] (.Intel(R) pGFX.) - C:\Windows\System32\DriverStore\FileRepository\igdlh64.inf\_amd64\_c8634ed19e331cda\IntelCpHeciSvc.exe

[56000005DAB0988313DA8AB3E10000000005DA] [10/10/2018] (.Intel(R) pGFX.) - C:\Windows\System32\DriverStore\FileRepository\intcdaud.inf\_amd64\_3b876fb0bfb3390a\IntcDAud.sys

[6E715E33F17AD55BCBF98C1F14D21F2F] [07/11/2018] (.Huawei Technologies Co., Ltd..) - C:\ProgramData\Huawei\Driver\WDT Device Driver\unins000.exe =>.Not verified

[6E715E33F17AD55BCBF98C1F14D21F2F] [18/01/2019] (.Huawei Technologies Co., Ltd..) - C:\Program Files\Huawei\HwOsd\OSDListener.exe =>.Not verified

[6E715E33F17AD55BCBF98C1F14D21F2F] [18/01/2019] (.Huawei Technologies Co., Ltd..) - C:\Program Files\Huawei\HwOsd\OSDMainService.exe =>.Not verified

[6E715E33F17AD55BCBF98C1F14D21F2F] [18/01/2019] (.Huawei Technologies Co., Ltd..) - C:\Program Files\Huawei\HwOsd\uninst.exe =>.Not verified

[6E715E33F17AD55BCBF98C1F14D21F2F] [25/06/2019] (.Huawei Technologies Co., Ltd..) - C:\Program Files\Huawei\HwLcdEnhancement\LCD\_Service.exe =>.Not verified

[6E715E33F17AD55BCBF98C1F14D21F2F] [25/06/2019] (.Huawei Technologies Co., Ltd..) - C:\Program Files\Huawei\PCManager\DumpReport.exe =>.Not verified

[6E715E33F17AD55BCBF98C1F14D21F2F] [25/06/2019] (.Huawei Technologies Co., Ltd..) - C:\Program Files\Huawei\PCManager\HwOs2EC10x64.sys =>.Not verified

[6E715E33F17AD55BCBF98C1F14D21F2F] [25/06/2019] (.Huawei Technologies Co., Ltd..) - C:\Program Files\Huawei\PCManager\HWVCR.exe =>.Not verified

[6E715E33F17AD55BCBF98C1F14D21F2F] [25/06/2019] (.Huawei Technologies Co., Ltd..) - C:\Program Files\Huawei\PCManager\MateBookService.exe =>.Not verified

[6E715E33F17AD55BCBF98C1F14D21F2F] [25/06/2019] (.Huawei Technologies Co., Ltd..) - C:\Program Files\Huawei\PCManager\MBAMessageCenter.exe =>.Not verified

[6E715E33F17AD55BCBF98C1F14D21F2F] [25/06/2019] (.Huawei Technologies Co., Ltd..) - C:\Program Files\Huawei\PCManager\UninstallGuide.exe =>.Not verified

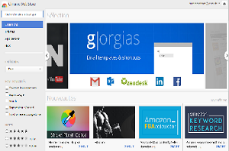
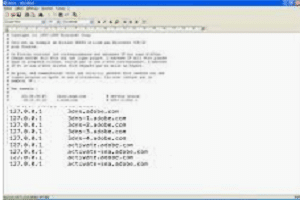
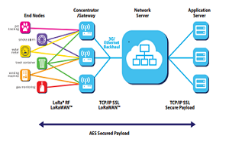
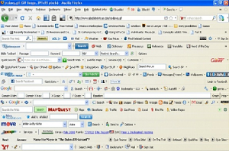
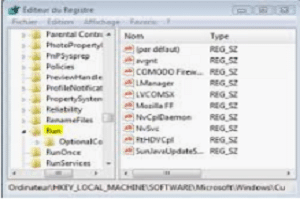
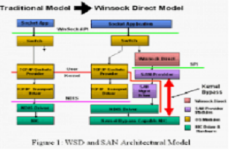
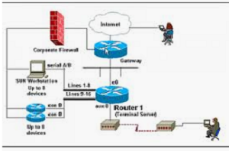
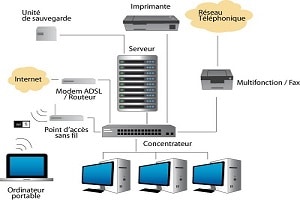
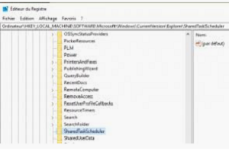
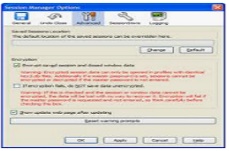
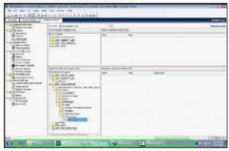
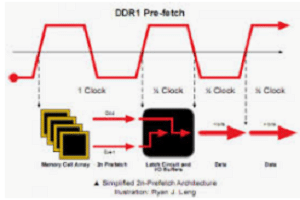
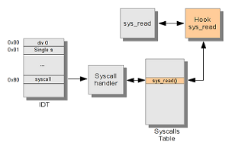
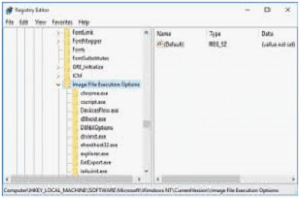
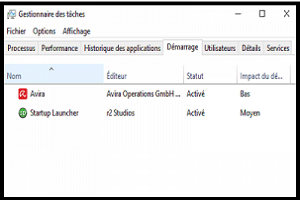
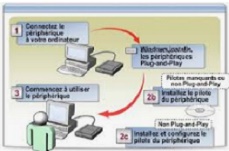
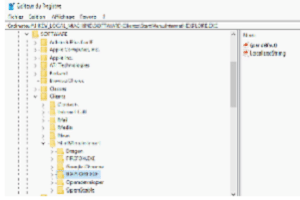
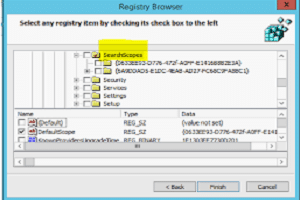
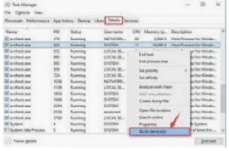
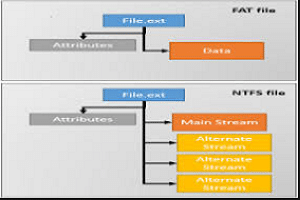
[6E715E33F17AD55BCBF98C1F14D21F2F] [25/06/2019] (.Huawei Technologies Co., Ltd..) - C:\Program Files\Huawei\PCManager\WFPDriver.sys =>.Not verified

[6E715E33F17AD55BCBF98C1F14D21F2F] [30/08/2018] (.Huawei Technologies Co., Ltd..) - C:\WINDOWS\System32\Drivers\WDTDrv.sys =>.Not verified

[73AB6F42D137AA7A291DF22FD16A3430] [03/12/2019] (.ObviousIdea SARLU.) - C:\Program Files (x86)\ObviousIdea\Light Image Resizer 5\unins000.exe

[73AB6F42D137AA7A291DF22FD16A3430] [20/02/2019] (.ObviousIdea SARLU.) - C:\Program Files (x86)\ObviousIdea\Light Image Resizer 5\Resize.exe

**INFORMATIONS SUR LES MODULES ZHPDIAG**

[[](https://nicolascoolman.eu/wp-content/uploads/2017/10/20/zhpdiag-module-g0-gcsp/)](https://nicolascoolman.eu/wp-content/uploads/2017/10/20/zhpdiag-module-g0-gcsp/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/11/02/zhpdiag-module-g2-gce/)](https://nicolascoolman.eu/wp-content/uploads/2017/11/02/zhpdiag-module-g2-gce/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/11/10/zhpdiag-module-m2-mfep/)](https://nicolascoolman.eu/wp-content/uploads/2017/11/10/zhpdiag-module-m2-mfep/)[[](https://nicolascoolman.eu/wp-content/uploads/2019/06/29/r5-internet-explorer-proxy-management-iepm/)](https://nicolascoolman.eu/wp-content/uploads/2019/06/29/r5-internet-explorer-proxy-management-iepm/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/10/23/zhpdiag-module-o1-ush/)](https://nicolascoolman.eu/wp-content/uploads/2017/10/23/zhpdiag-module-o1-ush/)[[](https://nicolascoolman.eu/wp-content/uploads/2019/06/29/o2-browser-helper-objects-de-navigateur-bho/)](https://nicolascoolman.eu/wp-content/uploads/2019/06/29/o2-browser-helper-objects-de-navigateur-bho/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/11/26/zhpdiag-module-o3-barre-doutils-de-navigateurs/)](https://nicolascoolman.eu/wp-content/uploads/2017/11/26/zhpdiag-module-o3-barre-doutils-de-navigateurs/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/11/02/zhpdiag-module-o4-adar/)](https://nicolascoolman.eu/wp-content/uploads/2017/11/02/zhpdiag-module-o4-adar/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/11/27/zhpdiag-module-o4-global-startup/)](https://nicolascoolman.eu/wp-content/uploads/2017/11/27/zhpdiag-module-o4-global-startup/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/10/19/zhpdiag-module-o10-lsp/)](https://nicolascoolman.eu/wp-content/uploads/2017/10/19/zhpdiag-module-o10-lsp/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/10/19/zhpdiag-module-o17-mdad/)](https://nicolascoolman.eu/wp-content/uploads/2017/10/19/zhpdiag-module-o17-mdad/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/11/05/zhpdiag-module-o18-papp/)](https://nicolascoolman.eu/wp-content/uploads/2017/11/05/zhpdiag-module-o18-papp/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/10/30/zhpdiag-module-o22-sharedtaskscheduler-sts/)](https://nicolascoolman.eu/wp-content/uploads/2017/10/30/zhpdiag-module-o22-sharedtaskscheduler-sts/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/10/20/zhpdiag-module-o23-smnd/)](https://nicolascoolman.eu/wp-content/uploads/2017/10/20/zhpdiag-module-o23-smnd/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/10/27/zhpdiag-module-o34-bootexecute-bex/)](https://nicolascoolman.eu/wp-content/uploads/2017/10/27/zhpdiag-module-o34-bootexecute-bex/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/10/18/zhpdiag-module-o38-apt/)](https://nicolascoolman.eu/wp-content/uploads/2017/10/18/zhpdiag-module-o38-apt/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/10/18/zhpdiag-module-o40-asic/)](https://nicolascoolman.eu/wp-content/uploads/2017/10/18/zhpdiag-module-o40-asic/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/11/01/zhpdiag-module-o42-loin/)](https://nicolascoolman.eu/wp-content/uploads/2017/11/01/zhpdiag-module-o42-loin/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/11/12/zhpdiag-module-o43-cfd/)](https://nicolascoolman.eu/wp-content/uploads/2017/11/12/zhpdiag-module-o43-cfd/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/10/22/zhpdiag-module-o45-lfp/)](https://nicolascoolman.eu/wp-content/uploads/2017/10/22/zhpdiag-module-o45-lfp/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/10/22/zhpdiag-module-o46-seh/)](https://nicolascoolman.eu/wp-content/uploads/2017/10/22/zhpdiag-module-o46-seh/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/03/24/module-zhpdiag-o50/)](https://nicolascoolman.eu/wp-content/uploads/2017/03/24/module-zhpdiag-o50/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/10/31/zhpdiag-module-o53-smsr/)](https://nicolascoolman.eu/wp-content/uploads/2017/10/31/zhpdiag-module-o53-smsr/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/10/21/zhpdiag-module-o58-sdl/)](https://nicolascoolman.eu/wp-content/uploads/2017/10/21/zhpdiag-module-o58-sdl/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/10/21/zhpdiag-module-o68-smi/)](https://nicolascoolman.eu/wp-content/uploads/2017/10/21/zhpdiag-module-o68-smi/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/11/04/zhpdiag-module-o69-sbi/)](https://nicolascoolman.eu/wp-content/uploads/2017/11/04/zhpdiag-module-o69-sbi/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/10/24/zhpdiag-module-o83-sss/)](https://nicolascoolman.eu/wp-content/uploads/2017/10/24/zhpdiag-module-o83-sss/)[[](https://nicolascoolman.eu/wp-content/uploads/2017/10/24/zhpdiag-module-o87-fael/)](https://nicolascoolman.eu/wp-content/uploads/2017/10/24/zhpdiag-module-o87-fael/)[](https://nicolascoolman.eu/wp-content/uploads/ads-alternate-data-stream/)

**FIN DE RAPPORT ZHPDIAG**