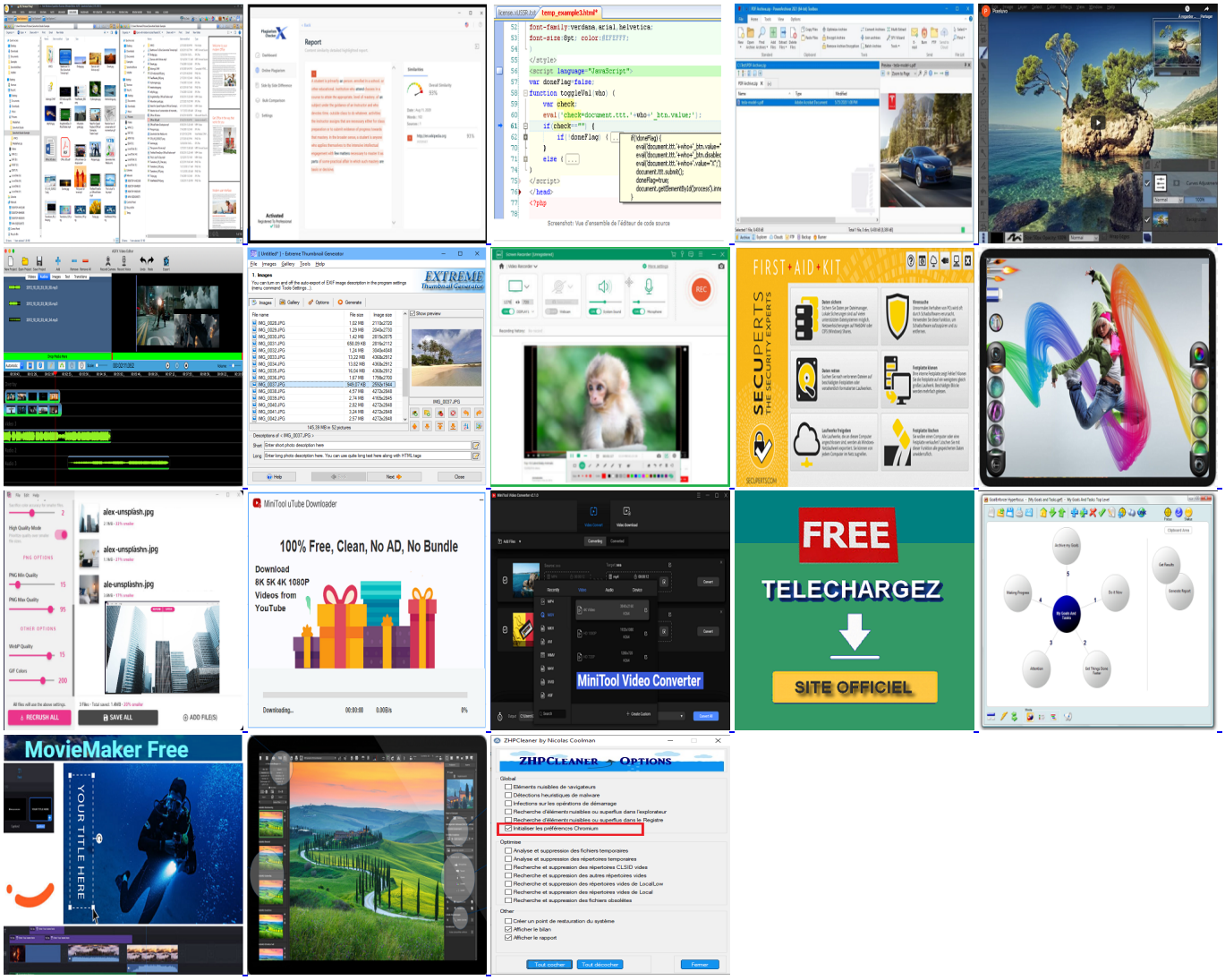
NEWS ZONE ANTIMALWARE



RAPPORT DE DIAGNOSTIC DE ZHPDIAG

```
~ ZHPDiag v2020.11.29.258 Par Nicolas Coolman (2020/11/29)
~ Démarré par Ousmane (Administrator)  (2020/12/03 12:13:08)
~ 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: C:\Users\couli\OneDrive\Bureau\ZHPDiag.txt
~ Rapport: C:\Users\couli\AppData\Roaming\ZHP\ZHPDiag.txt
~ UAC: Activate
~ Démarrage du système: Normal (Normal boot)
Windows 10 Home, 64-bit  (Build 19042)  =>.Microsoft Corporation


---\ NAVIGATEURS INTERNET (5) - 0s
~ GCIE: Google Chrome v87.0.4280.88
~ MFIE: Mozilla Firefox 83.0 (x64 fr)
~ OPIE: Opera 72.0.3815.400
~ MSIE: Internet Explorer v11.630.19041.0
~ OBIE: Microsoft Edge v87.0.664.52

---\ 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 : K2D94
Windows License : OK
~ Windows Remaining Initializations Number :  1001
Windows Automatic Updates : OK

---\ LOGICIELS DE PROTECTION (3) - 1s
Avast Antivirus Gratuit v20.9.2437 (Protection)
Windows Defender W10 (Deactivate) (Protection)
```

```
Avast SecureLine VPN v5.8.5262.1418 (Protection)

---\ SURVEILLANCE LOGICIEL (2) - 1s
~ Adobe Flash Player 32 NPAPI (Surveillance)
~ Adobe Acrobat Reader DC - Français (Surveillance)

---\ LOGICIELS D'OPTIMISATION (1) - 1s
~ CCleaner v5.74 (Optimisation)

---\ LOGICIELS DE PARTAGE P2P (1) - 1s
~ µTorrent v3.5.5.45628 (P2P)

---\ INFORMATIONS SUR LE SYSTÈME (6) - 0s
~ Operating System: Intel64 Family 6 Model 158 Stepping 9, GenuineIntel
~ Operating System:  64-bit
~ Boot mode: Normal (Normal boot)
Total RAM: 16709.492 MB (73% free) : OK  =>.RAM Value
System Restore: Activé (Enable)
System drive C: has 7 GB (2%) free of 242 GB : ATTENTION  =>Warning Disk Space

---\ MODE DE CONNEXION AU SYSTÈME (3) - 0s
~ Computer Name: DESKTOP-9A8RAVS
~ User Name: Ousmane
~ Logged in as Administrator

---\ ÉNUMÉRATION DES UNITÉS DE STOCKAGE (6) - 0s
~ Drive C: has 7 GB free of 242 GB  (System)
~ Drive D: has 93 GB free of 936 GB
~ Drive E: has 1 GB free of 17 GB
~ Drive G: has 70 GB free of 476 GB
~ Drive H: has 3 GB free of 3 GB
~ Drive I: has 1524 GB free of 1620 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
[MD5.3EAF5EA1C9299228730164390 91C21A0] - 13/11/2020 - (.Microsoft Corporation - Explorateur Windows.) -- C:\WINDOWS\Explorer.exe [4651032]  =>.Microsc
[MD5.44B041922105E01BFD0D096123F7D312] - 07/12/2019 - (.Microsoft Corporation - Processus hôte Windows (Rundll32).) -- C:\WINDOWS\System32\rundll32.ex
[MD5.DB516676B9D40004985E6D25A74943D7] - 16/10/2020 - (.Microsoft Corporation - Application de démarrage de Windows.) -- C:\WINDOWS\System32\Wininit.e
[MD5.02575AF42913ADC86345684381AAC23A] - 16/10/2020 - (.Microsoft Corporation - Extensions Internet pour Win32.) -- C:\WINDOWS\System32\wininet.dll [5
[MD5.790D2A6C194038513919DA17C6B91549] - 16/10/2020 - (.Microsoft Corporation - Application d'ouverture de session Windows.) -- C:\WINDOWS\System32\Wi
[MD5.3F910E7BB716BCD9B4C06EE6CF20304A] - 10/09/2020 - (.Microsoft Corporation - Bibliothèque de licences.) -- C:\WINDOWS\System32\sppcomapi.dll [31641
[MD5.C1D0F62643FB7B87BB44B705754B8B86] - 13/11/2020 - (.Microsoft Corporation - DNS DLL de l'API Client.) -- C:\WINDOWS\System32\dnsapi.dll [828432]
[MD5.35CC261A565BF54BA739024040559ED8] - 13/11/2020 - (.Microsoft Corporation - DNS DLL de l'API Client.) -- C:\WINDOWS\Syswow64\dnsapi.dll [586240]
[MD5.548E5FAA852134C7F380DC45C6A0A0B8] - 13/11/2020 - (.Microsoft Corporation - Agent de mise à jour automatique Windows Up.) -- C:\WINDOWS\System32\w
[MD5.3996E9A5F0CC85E93AA7ADE49A892C5E] - 07/12/2019 - (.Microsoft Corporation - DLL client de l'API uilisateur de Windows m.) -- C:\WINDOWS\System32\f
[MD5.6F082A5EB40F9BFD6873F3796F10F866] - 10/09/2020 - (.Microsoft Corporation - Pilote de fonction connexe pour WinSock.) -- C:\WINDOWS\System32\drive
[MD5.C394B2347795AB247F4F4FFAB46B8935] - 10/09/2020 - (.Microsoft Corporation - ATAPI IDE Miniport Driver.) -- C:\WINDOWS\System32\drivers\atapi.sys
[MD5.764FE2149251A246F6B047A0F09F5F0B] - 07/12/2019 - (.Microsoft Corporation - CD-ROM File System Driver.) -- C:\WINDOWS\System32\drivers\Cdfs.sys [1
[MD5.26255C953A69CCD32EF4491411737904] - 07/12/2019 - (.Microsoft Corporation - SCSI CD-ROM Driver.) -- C:\WINDOWS\System32\drivers\Cdrom.sys [174080]
[MD5.E958B2741A04DD6442F8AD0FE543D473] - 07/12/2019 - (.Microsoft Corporation - DFS Namespace Client Driver.) -- C:\WINDOWS\System32\drivers\DfsC.sys
[MD5.4BFD517F80F247590AB6C03E3FF55E1A] - 07/12/2019 - (.Microsoft Corporation - High Definition Audio Bus Driver.) -- C:\WINDOWS\System32\drivers\HDAu
[MD5.E4B36C6EAAAB703CBFECB92EE590FB31] - 07/12/2019 - (.Microsoft Corporation - Pilote de port i8042.) -- C:\WINDOWS\System32\drivers\i8042prt.sys [11
[MD5.F63572DF4295C78B3F7036AEDA878176] - 07/12/2019 - (.Microsoft Corporation - IP Network Address Translator.) -- C:\WINDOWS\System32\drivers\IpNat.s
[MD5.6EE28BABC5134E6FBEE8335496C55B39] - 10/09/2020 - (.Microsoft Corporation - Minirdr SMB Windows NT.) -- C:\WINDOWS\System32\drivers\MRxSmb.sys [57
[MD5.49F7DE6F689C47B64A2C2D46CD98E327] - 16/10/2020 - (.Microsoft Corporation - MBT Transport driver.) -- C:\WINDOWS\System32\drivers\netBT.sys [34156
[MD5.99041A92D27B61BB6606D6F31F980451] - 13/11/2020 - (.Microsoft Corporation - Pilote du système de fichiers NT.) -- C:\WINDOWS\System32\drivers\ntfs
[MD5.138FDB1EBCB61287A645BD3B06DBED5E] - 07/12/2019 - (.Microsoft Corporation - Pilote de port parallèle.) -- C:\WINDOWS\System32\drivers\Parport.sys
[MD5.40CBDB4B80284451536C8CA49561E5CD] - 10/09/2020 - (.Microsoft Corporation - RAS L2TP mini-port/call-manager driver.) -- C:\WINDOWS\System32\driver
[MD5.5C322D590CEBCAF2F333EBE70E178AB4] - 07/12/2019 - (.Microsoft Corporation - Redirecteur de périphérique de Microsoft RD.) -- C:\WINDOWS\System32\d
[MD5.9C4C6E0C590F789CECB7A6D437E5A284] - 07/12/2019 - (.Microsoft Corporation - TDI Translation Driver.) -- C:\WINDOWS\System32\drivers\tdx.sys [11756
[MD5.988A7A685BB51BAC62F4E176BE5432AC] - 10/09/2020 - (.Microsoft Corporation - Pilote de cliché instantané du volume.) -- C:\WINDOWS\System32\drivers

---\ LISTE DES SERVICES (Non désactivés) (92) - 3s
O23 - Service: Adobe Acrobat Update Service (AdobeARMservice) . (.Adobe Inc. - Adobe Acrobat Update Service.) - C:\Program Files (x86)\Common Files\Ac
O23 - Service: Intel® SGX AESM (AESMService) . (.Intel Corporation - Intel® SGX Application Enclave Services Man.) - C:\Program Files\Intel\IntelSGXPS
O23 - Service: C:\Windows\System32\inetsrv\iisres.dll (AppHostSvc) . (.Microsoft Corporation - IIS Application Host Helper Service.) - C:\Windows\Syst
O23 - Service: C:\WINDOWS\System32\AudioEndpointBuilder.dll (AudioEndpointBuilder) . (.Microsoft Corporation - Générateur de points de terminaison du
O23 - Service: C:\WINDOWS\System32\audiosrv.dll (Audiosrv) . (.Microsoft Corporation - Service Audio Windows.) - C:\WINDOWS\System32\Audiosrv.dll [Uns
O23 - Service: Avast Antivirus (avast! Antivirus) . (.AVAST Software - Avast Service.) - C:\Program Files\AVAST Software\Avast\AvastSvc.exe  =>.Avast
O23 - Service: Avast Tools (avast! Tools) . (.AVAST Software - Avast Antivirus.) - C:\Program Files\AVAST Software\Avast\aswToolsSvc.exe  =>.Avast Sof
O23 - Service: AvastWscReporter (AvastWscReporter) . (.AVAST Software - Avast remediation exe.) - C:\Program Files\AVAST Software\Avast\wsc_proxy.exe
O23 - Service: AOMEI Backupper Scheduler Service (Backupper Service) . (.AOMEI Tech Co., Ltd. - AOMEI Backupper Schedule task service.) - C:\Program F
O23 - Service: C:\WINDOWS\System32\bfe.dll (BFE) . (.Microsoft Corporation - Moteur de filtrage de base.) - C:\WINDOWS\System32\bfe.dll [Unsigned]  =>
O23 - Service: C:\WINDOWS\System32\qmgr.dll (BITS) . (.Microsoft Corporation - Service de transfert intelligent en arrière.) - C:\WINDOWS\System32\qmg
O23 - Service: Service Bonjour (Bonjour Service) . (.Apple Inc. - Bonjour Service.) - C:\Program Files\Bonjour\mDNSResponder.exe  =>.Apple Inc.®
O23 - Service: C:\WINDOWS\system32\bisrv.dll (BrokerInfrastructure) . (.Microsoft Corporation - Process State Manager (PSM) Service.) - C:\WINDOWS\Sys
O23 - Service: C:\WINDOWS\System32\cdpusersvc.dll (CDPUserSvc) . (.Microsoft Corporation - Composants utilisateur Microsoft (R) CDP.) - C:\WINDOWS\Sys
O23 - Service: CDPUserSvc_3a53e (CDPUserSvc_3a53e) . (.Microsoft Corporation - Processus hôte pour les services Windows.) - C:\Windows\System32\svchos
O23 - Service: C:\Windows\System32\coremessaging.dll (CoreMessagingRegistrar) . (.Microsoft Corporation - Microsoft CoreMessaging Dll.) - C:\Windows\S
O23 - Service: Cron Service (CronService) . (.Prey, Inc. - Execution Service.) - C:\Windows\Prey\wpxsvc.exe {01E84CE2860CF3D794990EDED64D5F0A}.  =>.Pr
O23 - Service: C:\WINDOWS\System32\cryptsvc.dll (CryptSvc) . (.Microsoft Corporation - Services de chiffrement.) - C:\WINDOWS\System32\cryptsvc.dll [U
O23 - Service: Service Mise à jour Dropbox (dbupdate) (dbupdate) . (.Dropbox, Inc. - Dropbox Update.) - C:\Program Files (x86)\Dropbox\Update\DropboxU
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
O23 - Service: C:\Windows\System32\dhcpcore.dll (Dhcp) . (.Microsoft Corporation - Service client DHCP.) - C:\Windows\System32\dhcpcore.dll [Unsigned]
O23 - Service: C:\WINDOWS\System32\diagtrack.dll (DiagTrack) . (.Microsoft Corporation - Suivi des diagnostics Microsoft Windows.) - C:\WINDOWS\System
O23 - Service: C:\WINDOWS\System32\dispbroker.desktop.dll (DispBrokerDesktopSvc) . (.Microsoft Corporation - Courtier d'affichage du bureau.) - C:\WIN
O23 - Service: C:\Windows\System32\dnsapi.dll (Dnscache) . (.Microsoft Corporation - Service de résolution du cache DNS.) - C:\WINDOWS\System32\dnsrsl
O23 - Service: C:\WINDOWS\System32\dusmsvc.dll (DusmSvc) . (.Microsoft Corporation - Service Consommation des données.) - C:\WINDOWS\System32\dusmsvc
O23 - Service: Service Mise à jour de Microsoft Edge (edgeupdate) (edgeupdate) . (.Microsoft Corporation - Microsoft Edge Update.) - C:\Program Files
O23 - Service: C:\WINDOWS\System32\wevtsvc.dll (EventLog) . (.Microsoft Corporation - Service journal des événements.) - C:\WINDOWS\System32\wevtsvc.d
O23 - Service: @comres.dll,-2450 (EventSystem) . (.Microsoft Corporation - COM+.) - C:\Windows\System32\es.dll [Unsigned]  =>.Microsoft Corporation
O23 - Service: C:\WINDOWS\System32\FntCache.dll (FontCache) . (.Microsoft Corporation - Service de cache de police Windows.) - C:\WINDOWS\System32\Fnt
O23 - Service: @gpapi.dll,-112 (gpsvc) . (.Microsoft Corporation - Client de stratégie de groupe.) - C:\WINDOWS\System32\gpsvc.dll [Unsigned]  =>.Micr
O23 - Service: Service Google Update (gupdate) (gupdate) . (.Google LLC - Programme d'installation de Google.) - C:\Program Files (x86)\Google\Update\
O23 - Service: HP Comm Recovery (HP Comm Recover) . (.HP Inc. - CommRecovery.) - C:\Program Files\HPCommRecovery\HPCommRecovery.exe  =>.HP Inc.®
```

```
O23 - Service: HP App Helper HSA Service (HPAppHelperCap) . (.HP Inc. - .) - C:\Windows\System32\DriverStore\FileRepository\hpcustomcapcomp.inf_amd64_
O23 - Service: HP Network HSA Service (HPNetworkCap) . (.HP Inc. - .) - C:\Windows\System32\DriverStore\FileRepository\hpcustomcapcomp.inf_amd64_66856
O23 - Service: HP Omen HSA Service (HPOmenCap) . (.HP Inc. - Description.) - C:\Windows\System32\DriverStore\FileRepository\hpomencustomcapcomp.inf_am
O23 - Service: HP System Info HSA Service (HPSysInfoCap) . (.HP Inc. - .) - C:\Windows\System32\DriverStore\FileRepository\hpcustomcapcomp.inf_amd64_6
O23 - Service: HP Analytics service (HpTouchpointAnalyticsService) . (.HP Inc. - HP Touchpoint Analytics Client Service.) - C:\Windows\System32\Driver
O23 - Service: HPWMISVC (HPWMISVC) . (.HP Inc. - HP WMI Service.) - C:\Program Files (x86)\HP\HP System Event\HPWMISVC.exe  =>.HP Inc.®
O23 - Service: C:\WINDOWS\System32\ikeext.dll (IKEEXT) . (.Microsoft Corporation - Extension IKE.) - C:\WINDOWS\System32\ikeext.dll [Unsigned]  =>.Mic
O23 - Service: Intel(R) TPM Provisioning Service (Intel(R) TPM Provisioning Service) . (.Intel(R) Corporation - Intel(R) TPM Provisioning Service.) -
O23 - Service: C:\WINDOWS\System32\iphlpsvc.dll (iphlpsvc) . (.Microsoft Corporation - Service offrant une connectivité IPv6 sur u.) - C:\WINDOWS\Syst
O23 - Service: Intel(R) Dynamic Application Loader Host Interface Service (jhi_service) . (.Intel Corporation - Intel(R) Dynamic Application Loader Ho
O23 - Service: JumpStart Push-Button Service (jswpbapi) . (.Atheros Communications, Inc. - JumpStart PushButton Service.) - C:\Program Files (x86)\Jum
O23 - Service: C:\WINDOWS\System32\srvsvc.dll (LanmanServer) . (.Microsoft Corporation - DLL du service Serveur.) - C:\WINDOWS\System32\srvsvc.dll [Un
O23 - Service: C:\WINDOWS\System32\wkssvc.dll (LanmanWorkstation) . (.Microsoft Corporation - DLL du service Station de travail.) - C:\WINDOWS\System3
O23 - Service: Intel(R) Management and Security Application Local Manageme (LMS) . (.Intel Corporation - Intel(R) Local Management Service.) - C:\Prog
O23 - Service: C:\WINDOWS\system32\lsm.dll (LSM) . (.Microsoft Corporation - Service du gestionnaire de session locale.) - C:\WINDOWS\System32\lsm.dll
O23 - Service: C:\WINDOWS\System32\moshost.dll (MapsBroker) . (.Microsoft Corporation - Gestionnaire des cartes téléchargées.) - C:\WINDOWS\System32\m
O23 - Service: McAfee WebAdvisor (McAfee WebAdvisor) . (.McAfee, LLC - McAfee WebAdvisor.) - C:\Program Files\McAfee\WebAdvisor\ServiceHost.exe  =>.Mc
O23 - Service: MEmuSVC (MEmuSVC) . (.Shanghai Microvirt Software Technology Co., Ltd. - .) - C:\Program Files (x86)\Microvirt\MEmu\MemuService.exe  =>
O23 - Service: C:\Windows\System32\FirewallAPI.dll (mpssvc) . (.Microsoft Corporation - Service de protection Microsoft.) - C:\WINDOWS\System32\mpssvc
O23 - Service: C:\WINDOWS\System32\nlasvc.dll (NlaSvc) . (.Microsoft Corporation - Connaissance des emplacements réseau 2.) - C:\WINDOWS\System32\nlas
O23 - Service: C:\WINDOWS\System32\nsisvc.dll (nsi) . (.Microsoft Corporation - Serveur RPC de l'interface du magasin résea.) - C:\WINDOWS\System32\ns
O23 - Service: NVIDIA LocalSystem Container (NvContainerLocalSystem) . (.NVIDIA Corporation - NVIDIA Container.) - C:\Program Files\NVIDIA Corporation
O23 - Service: NVIDIA Display Container LS (NVDisplay.ContainerLocalSystem) . (.NVIDIA Corporation - NVIDIA Container.) - C:\Program Files\NVIDIA Corp
O23 - Service: C:\WINDOWS\System32\APHostRes.dll (OneSyncSvc) . (.Microsoft Corporation - Accounts Host Service.) - C:\WINDOWS\System32\APHostService
O23 - Service: OneSyncSvc_3a53e (OneSyncSvc_3a53e) . (.Microsoft Corporation - Processus hôte pour les services Windows.) - C:\Windows\System32\svchos
O23 - Service: Origin Web Helper Service (Origin Web Helper Service) . (.Electronic Arts - OriginWebHelperService.) - C:\Program Files (x86)\Origin\Or
O23 - Service: PG Manager (pgt_svc) . (.Gold Click Ltd - PG Control Center.) - C:\Program Files (x86)\ProxyGate\MainService.exe  =>.SUP.GoldClick
O23 - Service: C:\WINDOWS\System32\umpo.dll (Power) . (.Microsoft Corporation - Service d'alimentation en mode utilisateur.) - C:\WINDOWS\System32\ump
O23 - Service: C:\WINDOWS\System32\profsvc.dll (ProfSvc) . (.Microsoft Corporation - ProfSvc.) - C:\WINDOWS\System32\profsvc.dll [Unsigned]  =>.Micros
O23 - Service: C:\WINDOWS\System32\rasmans.dll (RasMan) . (.Microsoft Corporation - Gestionnaire des connexions d'accès à dista.) - C:\WINDOWS\System3
O23 - Service: C:\WINDOWS\system32\RpcEpMap.dll (RpcEptMapper) . (.Microsoft Corporation - Mappeur de point de terminaison RPC.) - C:\WINDOWS\System32
O23 - Service: @combase.dll,-5010 (RpcSs) . (.Microsoft Corporation - Distributed COM Services.) - C:\WINDOWS\System32\rpcss.dll [Unsigned]  =>.Micros
O23 - Service: Realtek Audio Service (RtkAudioService) . (.Realtek Semiconductor - Realtek Audio Service.) - C:\Program Files\Realtek\Audio\HDA\RtkAuc
O23 - Service: Realtek Bluetooth Audio Service (RtkBtAudioServ) . (.Realtek Semiconductor Corp. - Realtek Bluetooth RtkBTAudio Service Applic.) - C:\W
O23 - Service: Realtek Bluetooth Device Manager Service (RtkBtManServ) . (.Realtek Semiconductor Corp. - Realtek Bluetooth BTDevManager Service Appl.)
O23 - Service: C:\WINDOWS\System32\schedsvc.dll (Schedule) . (.Microsoft Corporation - Service du Planificateur de tâches.) - C:\WINDOWS\System32\sche
O23 - Service: Avast SecureLine VPN (SecureLine) . (.AVAST Software - Avast VPN Service.) - C:\Program Files\AVAST Software\SecureLine VPN\VpnSvc.exe
O23 - Service: C:\WINDOWS\System32\Sens.dll (SENS) . (.Microsoft Corporation - Service de notification d'événements système.) - C:\WINDOWS\System32\ser
O23 - Service: C:\WINDOWS\System32\SgrmBroker.exe,-100 (SgrmBroker) . (.Microsoft Corporation - Service Broker du moniteur d'exécution Syst.) - C:\WIN
O23 - Service: C:\Windows\System32\shsvcs.dll (ShellHWDetection) . (.Microsoft Corporation - Dll des services Windows Shell.) - C:\Windows\System32\sh
O23 - Service: C:\WINDOWS\System32\spoolsv.exe,-1 (Spooler) . (.Microsoft Corporation - Application sous-système spouleur.) - C:\WINDOWS\System32\spoo
O23 - Service: C:\WINDOWS\System32\sppsvc.exe,-101 (sppsvc) . (.Microsoft Corporation - Service de la plateforme de protection logi.) - C:\WINDOWS\Sys
O23 - Service: SAMSUNG Mobile Connectivity Service (ss_conn_service) . (.DEVGURU Co., LTD. - MSS CS Connectivity Service.) - C:\Program Files\Samsung\
O23 - Service: C:\WINDOWS\System32\wiaservc.dll (stisvc) . (.Microsoft Corporation - Service de périphériques d'images fixes.) - C:\WINDOWS\System32\w
O23 - Service: C:\WINDOWS\System32\StorSvc.dll (StorSvc) . (.Microsoft Corporation - Services de stockage.) - C:\WINDOWS\System32\storsvc.dll [Unsigne
O23 - Service: C:\WINDOWS\System32\sysmain.dll (SysMain) . (.Microsoft Corporation - Hôte de Service SysMain.) - C:\WINDOWS\System32\sysmain.dll [Unsi
O23 - Service: C:\WINDOWS\system32\SystemEventsBrokerServer.dll (SystemEventsBroker) . (.Microsoft Corporation - Service Broker pour les événements sy
O23 - Service: TeamViewer 14 (TeamViewer) . (.TeamViewer GmbH - TeamViewer 14.) - C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe  =>.TeamVie
O23 - Service: C:\WINDOWS\System32\themeservice.dll (Themes) . (.Microsoft Corporation - DLL du service des thèmes Windows Shell.) - C:\WINDOWS\System
O23 - Service: C:\WINDOWS\System32\usermgr.dll (UserManager) . (.Microsoft Corporation - UserMgr.) - C:\WINDOWS\System32\usermgr.dll [Unsigned]  =>.Mi
O23 - Service: C:\WINDOWS\System32\usosvc.dll (UsoSvc) . (.Microsoft Corporation - Mettre à jour la session du service Orchest.) - C:\WINDOWS\System32
O23 - Service: VMware Authorization Service (VMAuthdService) . (.VMware, Inc. - VMware Authorization Service.) - C:\Program Files (x86)\VMware\VMware
O23 - Service: VMware DHCP Service (VMnetDHCP) . (.VMware, Inc. - VMware VMnet DHCP service.) - C:\Windows\SysWOW64\vmnetdhcp.exe  =>.VMware, Inc.®
O23 - Service: VMware USB Arbitration Service (VMUSBArbService) . (.VMware, Inc. - VMware USB Arbitration Service.) - C:\Program Files (x86)\Common Fi
O23 - Service: VMware NAT Service (VMware NAT Service) . (.VMware, Inc. - VMware NAT Service.) - C:\Windows\SysWOW64\vmnat.exe  =>.VMware, Inc.®
O23 - Service: VMware Workstation Server (VMwareHostd) . (.VMware, Inc. - .) - C:\Program Files (x86)\VMware\VMware Workstation\vmware-hostd.exe  =>.\
O23 - Service: C:\WINDOWS\System32\w32time.dll (W32Time) . (.Microsoft Corporation - Service de temps Windows.) - C:\WINDOWS\System32\w32time.dll [Uns
O23 - Service: C:\WINDOWS\System32\wcmsvc.dll (Wcmsvc) . (.Microsoft Corporation - DLL du service de gestion des connexions Wi.) - C:\WINDOWS\System32
O23 - Service: WeMod Version Guard (WeMod Version Guard) . (.WeMod - WeMod Version Guard.) - C:\Program Files\WeMod\Version Guard\VersionGuard.exe  =>

---\ SERVICES NON MICROSOFT (SR=Démarré,SS=Stoppé) (203) - 18s
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
SS - Demand [03/12/2020] [  335416]  Adobe Flash Player Update Service (AdobeFlashPlayerUpdateSvc) . (.Adobe.) - C:\Windows\SysWOW64\Macromed\Flash\Fl
SR - Boot   [07/12/2019] [ 1135416]  (ADP80XX) . (.PMC-Sierra.) - C:\WINDOWS\System32\drivers\ADP80XX.SYS  =>.Microsoft®
SR - Auto   [18/05/2016] [ 3759752]  Intel® SGX AESM (AESMService) . (.Intel Corporation.) - C:\Program Files\Intel\IntelSGXPSW\bin\x64\Release\aesm_s
SR - Boot   [21/12/2016] [   51120]  ambakdrv (ambakdrv) . (.CHENGDU AOMEI Tech Co., Ltd..) - C:\WINDOWS\System32\ambakdrv.sys  =>.CHENGDU AOMEI Tech
SR - Demand [07/12/2019] [   18432]  AMD GPIO Client Driver (amdgpio2) . (.Advanced Micro Devices, Inc.) - C:\WINDOWS\System32\drivers\amdgpio2.sys [U
SR - Demand [07/12/2019] [   45568]  AMD I2C Controller Service (amdi2c) . (.Advanced Micro Devices, Inc.) - C:\WINDOWS\System32\drivers\amdi2c.sys [U
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 - Auto   [21/12/2016] [  171952]  ammntdrv (ammntdrv) . (.CHENGDU AOMEI Tech Co., Ltd..) - C:\WINDOWS\system32\ammntdrv.sys  =>.CHENGDU AOMEI Tech
SR - Auto   [01/09/2017] [   38320]  amwrtdrv (amwrtdrv) . (.CHENGDU AOMEI Tech Co., Ltd..) - C:\WINDOWS\system32\amwrtdrv.sys  =>.CHENGDU AOMEI Tech
SR - Demand [10/05/2018] [   35560]  Apple Lower Filter Driver (AppleLowerFilter) . (.Apple Inc..) - C:\WINDOWS\System32\drivers\AppleLowerFilter.sys
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   [24/11/2020] [   37152]  aswArDisk (aswArDisk) . (.AVAST Software.) - C:\WINDOWS\System32\drivers\aswArDisk.sys  =>.Avast Software s.r.o.®
SR - System [24/11/2020] [  206408]  aswArPot (aswArPot) . (.AVAST Software.) - C:\WINDOWS\System32\drivers\aswArPot.sys  =>.Avast Software s.r.o.®
SR - System [24/11/2020] [  332368]  aswbidsdriver (aswbidsdriver) . (.AVAST Software.) - C:\WINDOWS\System32\drivers\aswbidsdriver.sys  =>.Avast Soft
SR - Boot   [24/11/2020] [  247888]  aswbidsh (aswbidsh) . (.AVAST Software.) - C:\WINDOWS\System32\drivers\aswbidsh.sys  =>.Avast Software s.r.o.®
SR - Boot   [24/11/2020] [   97352]  aswbuniv (aswbuniv) . (.AVAST Software.) - C:\WINDOWS\System32\drivers\aswbuniv.sys  =>.Avast Software s.r.o.®
SR - Boot   [24/11/2020] [   16816]  aswElam (aswElam) . (.AVAST Software.) - C:\WINDOWS\System32\drivers\aswElam.sys  =>.Microsoft®
SR - System [24/11/2020] [   42784]  aswKbd (aswKbd) . (.AVAST Software.) - C:\WINDOWS\System32\drivers\aswKbd.sys  =>.Avast Software s.r.o.®
SR - System [24/11/2020] [  176744]  aswMonFlt (aswMonFlt) . (.AVAST Software.) - C:\WINDOWS\System32\drivers\aswMonFlt.sys  =>.Avast Software s.r.o.®
SR - System [24/11/2020] [  521752]  aswNetHub (aswNetHub) . (.AVAST Software.) - C:\WINDOWS\System32\drivers\aswNetHub.sys  =>.Avast Software s.r.o.®
SR - System [24/11/2020] [  109280]  aswRdr (aswRdr) . (.AVAST Software.) - C:\WINDOWS\System32\drivers\aswRdr2.sys  =>.Avast Software s.r.o.®
SR - Boot   [24/11/2020] [   84856]  aswRvrt (aswRvrt) . (.AVAST Software.) - C:\WINDOWS\System32\drivers\aswRvrt.sys  =>.Avast Software s.r.o.®
SR - System [24/11/2020] [  851608]  aswSnx (aswSnx) . (.AVAST Software.) - C:\WINDOWS\System32\drivers\aswSnx.sys  =>.Avast Software s.r.o.®
SR - System [24/11/2020] [  469832]  aswSP (aswSP) . (.AVAST Software.) - C:\WINDOWS\System32\drivers\aswSP.sys  =>.Avast Software s.r.o.®
SR - Auto   [24/11/2020] [  217336]  aswStm (aswStm) . (.AVAST Software.) - C:\WINDOWS\System32\drivers\aswStm.sys  =>.Avast Software s.r.o.®
SR - Demand [16/05/2020] [   53904]  avast! SecureLine TAP Adapter (aswTap) . (.The OpenVPN Project.) - C:\WINDOWS\System32\drivers\aswTap.sys  =>.AVA
SR - Boot   [24/11/2020] [  326416]  aswVmm (aswVmm) . (.AVAST Software.) - C:\WINDOWS\System32\drivers\aswVmm.sys  =>.Avast Software s.r.o.®
SR - Demand [16/07/2020] [   59312]  Avast SecureLine VPN Driver (aswVpnRdr) . (.Avast Software.) - C:\WINDOWS\System32\drivers\aswVpnRdr.sys  =>.Avas
SR - Auto   [24/11/2020] [  365648]  Avast Antivirus (avast! Antivirus) . (.AVAST Software.) - C:\Program Files\AVAST Software\Avast\AvastSvc.exe  =>
SR - Auto   [24/11/2020] [ 3096160]  Avast Tools (avast! Tools) . (.AVAST Software.) - C:\Program Files\AVAST Software\Avast\aswToolsSvc.exe  =>.Avast
SR - Auto   [24/11/2020] [   58048]  AvastWscReporter (AvastWscReporter) . (.AVAST Software.) - C:\Program Files\AVAST Software\Avast\wsc_proxy.exe  =
SR - Boot   [07/12/2019] [  533816]  QLogic Network Adapter VBD (b06bdrv) . (.QLogic Corporation.) - C:\WINDOWS\System32\drivers\bxvbda.sys  =>.Micros
SR - Auto   [22/01/2019] [  483184]  AOMEI Backupper Scheduler Service (Backupper Service) . (.AOMEI Tech Co., Ltd..) - C:\Program Files (x86)\AOMEI B
SR - Demand [07/12/2019] [    9728]  bcmfn2 Service (bcmfn2) . (...) - C:\WINDOWS\System32\drivers\bcmfn2.sys [Unsigned]  =>.Broadcom Corporation
SS - Demand [16/10/2020] [ 8730200]  BattlEye Service (BEService) . (.BattlEye Innovations e.K..) - C:\Program Files (x86)\Common Files\BattlEye\BESer
SR - Auto   [12/08/2015] [  462096]  Service Bonjour (Bonjour Service) . (.Apple Inc..) - C:\Program Files\Bonjour\mDNSResponder.exe  =>.Apple Inc.®
SR - System [29/03/2018] [  475224]  cbfsconnect2017 (cbfsconnect2017) . (.Callback Technologies, Inc..) - C:\WINDOWS\system32\drivers\cbfsconnect2017
SR - System [30/01/2018] [  347736]  cbfsfilter2017 (cbfsfilter2017) . (.Callback Technologies, Inc..) - C:\WINDOWS\system32\drivers\cbfsfilter2017.sy
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  =>
SR - Demand [24/07/2018] [ 3819744]  USB Audio Class 1.0 and 2 (CMUSBDAC) . (.C-MEDIA.) - C:\WINDOWS\System32\DRIVERS\CMUSBDAC.sys {4038604836B4D4BC44
SR - Auto   [28/06/2019] [ 6886432]  Cron Service (CronService) . (.Prey, Inc..) - C:\Windows\Prey\wpxsvc.exe {01E84CE2860CF3D794990EDED64D5F0A}.  =>
SR - Auto   [23/08/2018] [  143144]  Service Mise à jour Dropbox (dbupdate) (dbupdate) . (.Dropbox, Inc..) - C:\Program Files (x86)\Dropbox\Update\Drc
SS - Demand [23/08/2018] [  143144]  Service Mise à jour Dropbox (dbupdatem) (dbupdatem) . (.Dropbox, Inc..) - C:\Program Files (x86)\Dropbox\Update\D
SR - Auto   [01/12/2020] [   44552]  DbxSvc (DbxSvc) . (.Dropbox, Inc..) - C:\WINDOWS\System32\DbxSvc.exe  =>.Dropbox, Inc®
SR - Demand [16/01/2017] [  131712]  SAMSUNG Mobile USB Com (dg_ssudbus) . (.Samsung Electronics Co., Ltd..) - C:\WINDOWS\System32\DRIVERS\ssudbus.sys
SS - Demand [27/03/2020] [  803440]  EasyAntiCheat (EasyAntiCheat) . (.EasyAntiCheat Ltd.) - C:\Program Files (x86)\EasyAntiCheat\EasyAntiCheat.exe  =
SR - Boot   [07/12/2019] [ 3418936]  QLogic 10 Gigabit Ethernet Ada (ebdrv) . (.QLogic Corporation.) - C:\WINDOWS\System32\drivers\evbda.sys  =>.Micro
SR - Boot   [23/01/2019] [   17616]  System Reflection Flash Boot (FlashBoot) . (.Challenger Backup Solutions, LLC.) - C:\WINDOWS\System32\drivers\Fla
SS - Demand [19/10/2020] [  287720]  NVIDIA FrameView SDK service (FvSvc) . (.NVIDIA.) - C:\Program Files\NVIDIA Corporation\FrameViewSDK\nvfvsdksvc_x
SS - Demand [02/12/2020] [ 1426928]  Google Chrome Elevation Service (GoogleChromeElevationServi (GoogleChromeElevationService) . (.Google LLC.) - C:\
SR - System [20/01/2019] [   28936]  GUBootStartup (GUBootStartup) . (.Glarysoft Ltd.) - C:\WINDOWS\System32\drivers\GUBootStartup.sys  =>.Glarysoft L
SR - Auto   [03/12/2020] [  155592]  Service Google Update (gupdate) (gupdate) . (.Google LLC.) - C:\Program Files (x86)\Google\Update\GoogleUpdate.ex
SS - Demand [03/12/2020] [  155592]  Service Google Update (gupdatem) (gupdatem) . (.Google LLC.) - C:\Program Files (x86)\Google\Update\GoogleUpdate
SR - Auto   [02/11/2018] [   84752]  VMware hcmon (hcmon) . (.VMware, Inc..) - C:\WINDOWS\System32\DRIVERS\hcmon.sys  =>.VMware, Inc.®
SR - Demand [01/01/2019] [   83920]  HfAudio (HfAudio) . (.Screenovate Technologies Ltd..) - C:\WINDOWS\System32\drivers\HfAudio.sys  =>.SCREENOVATE T
SR - Auto   [19/12/2019] [  905080]  HP Comm Recovery (HP Comm Recover) . (.HP Inc..) - C:\Program Files\HPCommRecovery\HPCommRecovery.exe  =>.HP Inc
SR - Auto   [18/10/2020] [  601368]  HP App Helper HSA Service (HPAppHelperCap) . (.HP Inc..) - C:\Windows\System32\DriverStore\FileRepository\hpcusto
SR - Demand [06/07/2018] [   23960]  HP Application Driver (HPCustomCapDriver) . (.HP Inc..) - C:\Windows\System32\DriverStore\FileRepository\hpcustom
SR - Auto   [00/00/0000] [       0]  HP JumpStart Bridge (HPJumpStartBridge) . (...) - Bridge\HPJumpStartBridge.exe (.not file.) [Unsigned]  =>.Hewlet
SR - Auto   [18/10/2020] [  599832]  HP Network HSA Service (HPNetworkCap) . (.HP Inc..) - C:\Windows\System32\DriverStore\FileRepository\hpcustomcapc
SR - Auto   [14/06/2020] [  523544]  HP Omen HSA Service (HPOmenCap) . (.HP Inc..) - C:\Windows\System32\DriverStore\FileRepository\hpomencustomcapcom
SR - Demand [21/10/2018] [   24056]  HP Omen Driver (HPOmenCustomCapDriver) . (.HP Inc..) - C:\Windows\System32\DriverStore\FileRepository\hpomencusto
SR - Auto   [03/08/2020] [   31488]  (HpPortIo) . (.HP Inc..) - C:\Windows\System32\drivers\HpPortIox64.sys  =>.HP Inc.®
SR - Boot   [07/12/2019] [   64312]  (HpSAMD) . (.Hewlett-Packard Company.) - C:\WINDOWS\System32\drivers\HpSAMD.sys  =>.Microsoft®
SR - Auto   [18/10/2020] [  600344]  HP System Info HSA Service (HPSysInfoCap) . (.HP Inc..) - C:\Windows\System32\DriverStore\FileRepository\hpcustom
SR - Auto   [02/11/2020] [  465168]  HP Analytics service (HpTouchpointAnalyticsService) . (.HP Inc..) - C:\Windows\System32\DriverStore\FileRepositor
SR - Auto   [13/07/2017] [  628768]  HPWMISVC (HPWMISVC) . (.HP Inc..) - C:\Program Files (x86)\HP\HP System Event\HPWMISVC.exe  =>.HP Inc.®
SR - System [16/02/2019] [   27552]  HWiNFO32/64 Kernel Driver (HWiNFO32) . (.REALiX(tm).) - C:\Windows\SysWOW64\drivers\HWiNFO64A.SYS  =>.Martin Mali
SR - Demand [07/12/2019] [   36352]  Intel Serial IO GPIO Controlle (iagpio) . (.Intel(R) Corporation.) - C:\WINDOWS\System32\drivers\iagpio.sys [Unsi
SR - Demand [07/12/2019] [   91136]  Intel(R) Serial IO I2C Host Cont (iai2c) . (.Intel(R) Corporation.) - C:\WINDOWS\System32\drivers\iai2c.sys [Unsi
SR - Demand [07/12/2019] [   79360]  Intel(R) S (iaLPSS2i_GPIO2) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i_GPIO2.sys [Unsigned]
SR - Demand [07/12/2019] [   93184]  In (iaLPSS2i_GPIO2_BXT_P) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i_GPIO2_BXT_P.sys [Unsigne
SR - Demand [07/12/2019] [  112128]  Intel( (iaLPSS2i_GPIO2_CNL) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i_GPIO2_CNL.sys [Unsigne
SR - Demand [07/12/2019] [   96256]  Intel( (iaLPSS2i_GPIO2_GLK) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i_GPIO2_GLK.sys [Unsigne
SR - Demand [07/12/2019] [  171520]  Intel(R) Seria (iaLPSS2i_I2C) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i_I2C.sys [Unsigned]
SR - Demand [07/12/2019] [  175104]  Intel( (iaLPSS2i_I2C_BXT_P) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i_I2C_BXT_P.sys [Unsigne
SR - Demand [07/12/2019] [  177152]  Intel(R) S (iaLPSS2i_I2C_CNL) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i_I2C_CNL.sys [Unsigne
SR - Demand [07/12/2019] [  177664]  Intel(R) S (iaLPSS2i_I2C_GLK) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i_I2C_GLK.sys [Unsigne
SR - Demand [07/12/2019] [   38128]  Intel(R) Serial IO (iaLPSSi_GPIO) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSSi_GPIO.sys  =>.Inte
SR - Demand [07/12/2019] [  113152]  Intel(R) Serial IO I (iaLPSSi_I2C) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSSi_I2C.sys [Unsigne
SR - Demand [24/05/2017] [  891392]  Intel Chipset SATA RAID Controller (iaStorA) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaStorA.sys  =
SR - Boot   [05/08/2019] [  909152]  Intel(R) Chipset SATA/PCIe (iaStorAC) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaStorAC.sys  =>.Inte
SR - Demand [24/05/2017] [   69632]  iaStorAfs (iaStorAfs) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaStorAfs.sys  =>.Intel(R) Rapid Stor
SS - Demand [24/05/2017] [ 2398840]  Intel(R) Optane(TM) Memory Service (iaStorAfsService) . (.Intel Corporation.) - C:\Windows\IAStorAfsService\iaSto
SR - Boot   [07/12/2019] [  884752]  Intel Chipset SATA RAI (iaStorAVC) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaStorAVC.sys  =>.Micros
SR - Boot   [07/12/2019] [  412176]  Intel RAID Controller Wi (iaStorV) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaStorV.sys  =>.Microsof
SR - Demand [07/12/2019] [  558904]  Mellanox InfiniBand Bus/A (ibbus) . (.Mellanox.) - C:\WINDOWS\System32\drivers\ibbus.sys  =>.Microsoft®
SR - Demand [03/08/2020] [   48224]  Intel(R) Watchdog Timer Driver  (ICCWDT) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\ICCWDT.sys  =>.Int
SR - Demand [23/01/2019] [ 6544888]  Service for Realtek HD Audio (WDM) (IntcAzAudAddService) . (.Realtek Semiconductor Corp..) - C:\WINDOWS\System32\
SS - Demand [22/04/2020] [  856848]  Intel(R) Capability Lice (Intel(R) Capability Licensing Service TCP IP Interface) . (.Intel(R) Corporation.) - C
SR - Auto   [22/04/2020] [  783112]  Intel(R) TPM Provis (Intel(R) TPM Provisioning Service) . (.Intel(R) Corporation.) - C:\Windows\System32\DriverSt
SR - Auto   [26/12/2019] [  190464]  Intel HAXM Service (IntelHaxm) . (.Intel Corporation.) - C:\WINDOWS\System32\DRIVERS\IntelHaxm.sys  =>.Microsoft®
SR - Boot   [07/12/2019] [  172344]  (ItSas35i) . (.Avago Technologies.) - C:\WINDOWS\System32\drivers\ItSas35i.sys  =>.Microsoft®
SR - Auto   [16/08/2020] [  629752]  Intel(R) Dynamic Application Loader Host Interface Service (jhi_service) . (.Intel Corporation.) - C:\Windows\Sys
SR - Auto   [26/09/2008] [  265216]  JumpStart Push-Button Service (jswpbapi) . (.Atheros Communications, Inc..) - C:\Program Files (x86)\Jumpstart\js
SS - Demand [26/09/2008] [  954368]  JumpStart Wi-Fi Protected Setup (jswpsapi) . (.Atheros Communications, Inc..) - C:\Program Files (x86)\Jumpstart\
SR - System [15/05/2008] [   26624]  JumpStart Wireless Filter Driver (JSWPSLWF) . (.Atheros Communications, Inc..) - C:\WINDOWS\System32\DRIVERS\jswp
SR - Demand [05/10/2018] [   36496]  Logitech Gaming Virtual Bus Enumerator Driver (LGBusEnum) . (.Logitech Inc..) - C:\WINDOWS\System32\drivers\LGBus
SR - Auto   [25/01/2020] [   25448]  LGHUB Core Temperature Service (LGHUBTemperatureService) . (.Logitech.) - C:\ProgramData\LGHUB\depots\35872\drive
SR - Demand [05/10/2018] [   67736]  Logitech Translation Layer Driver (LGS) (LGJoyXlCore) . (.Logitech Inc..) - C:\WINDOWS\System32\drivers\LGJoyXlCo
SR - Auto   [03/12/2017] [  419984]  Intel(R) Management and Security Application Local Manageme (LMS) . (.Intel Corporation.) - C:\Program Files (x86
SR - Demand [08/12/2019] [   56584]  Logitech G HUB KMDF H (logi_generic_hid_filter) . (.Logitech.) - C:\WINDOWS\System32\drivers\logi_generic_hid_fil
SR - Demand [08/12/2019] [   38136]  Logitech G HUB Virtual Bus E (logi_joy_bus_enum) . (.Logitech.) - C:\WINDOWS\System32\drivers\logi_joy_bus_enum.s
SR - Demand [08/12/2019] [   57608]  Logitech G HUB HID Filt (logi_joy_hid_filter) . (.Logitech.) - C:\WINDOWS\System32\drivers\logi_joy_hid_filter.sy
SR - Demand [08/12/2019] [   46880]  Logitech G HUB USB Filter D (logi_joy_hid_lo) . (.Logitech.) - C:\WINDOWS\System32\drivers\logi_joy_hid_lo.sys  =
SR - Demand [08/12/2019] [   20624]  Logitech G HUB Virtual HID De (logi_joy_vir_hid) . (.Logitech, Inc..) - C:\WINDOWS\System32\drivers\logi_joy_vir_
SR - Demand [08/12/2019] [   66808]  Logitech G HUB Translation (logi_joy_xlcore) . (.Logitech.) - C:\WINDOWS\System32\drivers\logi_joy_xlcore.sys  =>
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   [21/11/2020] [  955656]  McAfee WebAdvisor (McAfee WebAdvisor) . (.McAfee, LLC.) - C:\Program Files\McAfee\WebAdvisor\ServiceHost.exe  =>
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 [17/09/2020] [  311216]  Intel(R) Management Engine Interf (MEIx64) . (.Intel Corporation.) - C:\Windows\System32\DriverStore\FileReposito
SR - System [21/09/2019] [  319192]  MemuHyperv Service (MEmuDrv) . (.Maiwei Corporation.) - C:\WINDOWS\System32\DRIVERS\MEmuDrv.sys  =>.Shanghai Micr
SR - Auto   [12/09/2019] [   85304]  MEmuSVC (MEmuSVC) . (.Shanghai Microvirt Software Technology Co., Ltd..) - C:\Program Files (x86)\Microvirt\MEmu\
SR - Demand [07/12/2019] [ 1131320]  Mellanox ConnectX Bus E (mlx4_bus) . (.Mellanox.) - C:\WINDOWS\System32\drivers\mlx4_bus.sys  =>.Microsoft®
SS - Demand [02/12/2020] [  242896]  Mozilla Maintenance Service (MozillaMaintenance) . (.Mozilla Foundation.) - C:\Program Files (x86)\Mozilla Mainte
SR - Boot   [07/12/2019] [   63800]  (mvumis) . (.Marvell Semiconductor, Inc..) - C:\WINDOWS\System32\drivers\mvumis.sys  =>.Microsoft®
SS - Demand [28/06/2017] [  714712]  MyEpson Portal Service (MyEpson Portal Service) . (.Seiko Epson Corporation.) - C:\Program Files (x86)\EPSON\MyEp
SR - Demand [07/12/2019] [  146232]  NetworkDirect Service (ndfltr) . (.Mellanox.) - C:\WINDOWS\System32\drivers\ndfltr.sys  =>.Microsoft®
SR - Auto   [01/03/2013] [   36600]  NetGroup Packet Filter Driver (NPF) . (.Riverbed Technology, Inc..) - C:\WINDOWS\System32\drivers\npf.sys  =>.Riv
SR - Auto   [17/10/2020] [  874472]  NVIDIA LocalSystem Container (NvContainerLocalSystem) . (.NVIDIA Corporation.) - C:\Program Files\NVIDIA Corporat
SR - Auto   [07/11/2020] [  885224]  NVIDIA Display Container LS (NVDisplay.ContainerLocalSystem) . (.NVIDIA Corporation.) - C:\Program Files\NVIDIA C
SR - Demand [07/11/2020] [  222112]  Service for NVIDIA High Definit (NVHDA) . (.NVIDIA Corporation.) - C:\WINDOWS\System32\drivers\nvhda64v.sys  =>.N
SR - Demand [07/11/2020] [33065368]  (nvlddmkm) . (.NVIDIA Corporation.) - C:\Windows\System32\DriverStore\FileRepository\nvhdci.inf_amd64_cabc1251ab
SR - Demand [04/03/2020] [   50592]  NvModuleTracker (NvModuleTracker) . (.NVIDIA Corporation.) - C:\WINDOWS\System32\drivers\NvModuleTracker.sys  =>
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 - Demand [19/03/2019] [   69840]  NVIDIA Virtual Au (nvvad_WaveExtensible) . (.NVIDIA Corporation.) - C:\WINDOWS\System32\drivers\nvvad64v.sys  =>
SR - Demand [11/03/2020] [   67456]  NVVHCI Enumerator Service (nvvhci) . (.NVIDIA Corporation.) - C:\WINDOWS\System32\drivers\nvvhci.sys  =>.NVIDIA C
SS - Demand [23/11/2020] [ 2523448]  Origin Client Service (Origin Client Service) . (.Electronic Arts.) - C:\Program Files (x86)\Origin\OriginClientS
SR - Auto   [23/11/2020] [ 3478336]  Origin Web Helper Service (Origin Web Helper Service) . (.Electronic Arts.) - C:\Program Files (x86)\Origin\Origi
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   [22/02/2017] [ 2285664]  PG Manager (pgt_svc) . (.Gold Click Ltd.) - C:\Program Files (x86)\ProxyGate\MainService.exe  =>.SUP.GoldClick
SR - Boot   [03/11/2011] [   56208]  PxHlpa64 (PxHlpa64) . (.Rovi Corporation.) - C:\WINDOWS\System32\Drivers\PxHlpa64.sys  =>.Sonic Solutions®
SS - Demand [25/09/2019] [  471696]  Rockstar Game Library Service (Rockstar Service) . (.Rockstar Games.) - D:\Launcher\RockstarService.exe  =>.Rocks
SS - Demand [01/03/2013] [  118520]  Remote Packet Capture Protocol v.0 (experimental) (rpcapd) . (.Riverbed Technology, Inc..) - C:\Program Files (x8
```

```
SR - Demand [16/02/2019] [ 1122200]  Realtek RT640 NT Driver (rt640x64) . (.Realtek.) - C:\WINDOWS\System32\drivers\rt640x64.sys  =>.Realtek Semicondu
SR - System [03/08/2020] [   70560]  Realtek LightWeight Filter (NDIS6.4 (rtf64) . (.Realtek.) - C:\WINDOWS\System32\DRIVERS\rtf64x64.sys  =>.Realtek
SR - Demand [17/05/2019] [  217032]  RtkA2dp Driver (RtkA2dp) . (.Realtek Semiconductor Corporation.) - C:\WINDOWS\System32\drivers\RtkA2dp.sys  =>.Re
SR - Auto   [23/01/2019] [  267768]  Realtek Audio Service (RtkAudioService) . (.Realtek Semiconductor.) - C:\Program Files\Realtek\Audio\HDA\RtkAudio
SR - Demand [17/05/2019] [   96984]  Realtek Bluetooth A/V Remote  (RtkAvrcp) . (.Realtek Semiconductor Corporation.) - C:\WINDOWS\System32\drivers\Rt
SR - Demand [23/01/2019] [   78720]  Realtek Bluetooth A/V Re (RtkAvrcpCtrlr) . (.Realtek Semiconductor Corporation.) - C:\WINDOWS\System32\drivers\Rt
SR - Auto   [26/06/2019] [  348224]  Realtek Bluetooth Audio Service (RtkBtAudioServ) . (.Realtek Semiconductor Corp..) - C:\Windows\RtkBtAudioServ.ex
SR - Demand [30/11/2019] [  787232]  Realtek Bluetooth Filter Driver (RtkBtFilter) . (.Realtek Semiconductor Corporation.) - C:\WINDOWS\System32\drive
SR - Auto   [30/11/2019] [  738712]  Realtek Bluetooth Device  (RtkBtManServ) . (.Realtek Semiconductor Corp..) - C:\Windows\RtkBtManServ.exe  =>.Micr
SR - Demand [23/01/2019] [ 1090216]  Realtek 8167 NT Driver (RTL8167) . (.Realtek.) - C:\WINDOWS\System32\DRIVERS\Rt64win7.sys  =>.Realtek Semiconduct
SR - Demand [23/01/2019] [  450152]  Realtek USB Card Reader - UER (RTSUER) . (.Realsil Semiconductor Corporation.) - C:\WINDOWS\System32\Drivers\RtsU
SR - Demand [04/12/2019] [11722328]  Realtek Wireless L (RTWlanE) . (.Realtek Semiconductor Corporation.) - C:\WINDOWS\System32\drivers\rtwlane.sys  =
SR - Demand [19/05/2013] [   39168]  Scp Virtual Bus Driver (ScpVBus) . (.Scarlet.Crush Productions.) - C:\WINDOWS\System32\drivers\ScpVBus.sys  =>.Br
SR - Demand [29/06/2019] [   56792]  ScrHIDDriver (ScrHIDDriver) . (.Screenovate Technologies Ltd..) - C:\WINDOWS\System32\DRIVERS\ScrHIDDriver.sys {0
SR - Demand [01/01/2019] [   59960]  ScrHIDDriver2 (ScrHIDDriver2) . (.Screenovate Technologies Ltd..) - C:\WINDOWS\System32\drivers\ScrHIDDriver2.sys
SR - Boot   [23/01/2019] [   91352]  (secnvme) . (.Samsung Electronics Co., Ltd.) - C:\WINDOWS\System32\drivers\secnvme.sys  =>.Samsung Electronics C
SR - Boot   [23/01/2019] [   30624]  (secnvmeF) . (.Samsung Electronics Co., Ltd.) - C:\WINDOWS\System32\drivers\secnvmeF.sys  =>.Samsung Electronics
SR - Auto   [18/11/2020] [ 7897696]  Avast SecureLine VPN (SecureLine) . (.AVAST Software.) - C:\Program Files\AVAST Software\SecureLine VPN\VpnSvc.ex
SR - Demand [18/05/2016] [   52824]  Software Guard Extensions Device Driver (SGXEPC) . (. {07501595A92EC5C8248A64548954DBB8}..) - C:\WINDOWS\System32
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 [23/01/2019] [   54928]  (SmbDrvI) . (.Synaptics Incorporated.) - C:\WINDOWS\System32\DRIVERS\Smb_driver_Intel.sys  =>.Synaptics Incorpor
SR - Demand [16/01/2017] [  165504]  SAMSUNG  Mobile USB Modem Dr (ssudmdm) . (.Samsung Electronics Co., Ltd..) - C:\WINDOWS\System32\DRIVERS\ssudmdm
SR - Auto   [16/01/2017] [  752224]  SAMSUNG Mobile Connectivity Service (ss_conn_service) . (.DEVGURU Co., LTD..) - C:\Program Files\Samsung\USB Driv
SS - Demand [02/11/2020] [ 1883424]  Steam Client Service (Steam Client Service) . (.Valve Corporation.) - C:\Program Files (x86)\Common Files\Steam\S
SR - Boot   [07/12/2019] [   31032]  (stexstor) . (.Promise Technology, Inc..) - C:\WINDOWS\System32\drivers\stexstor.sys  =>.Microsoft®
SR - Demand [17/05/2020] [   25608]  SWDUMon (SWDUMon) . (.SlimWare Utilities, Inc..) - C:\WINDOWS\System32\DRIVERS\SWDUMon.sys  =>.AVG Technologies C
SR - Demand [21/04/2016] [   27136]  TAP-Windows Adapter V9 (tap0901) . (.The OpenVPN Project.) - C:\WINDOWS\System32\drivers\tap0901.sys [Unsigned]
SR - Demand [24/07/2018] [   44896]  TAP-NordVPN Windows Adapter V9 (tapnordvpn) . (.The OpenVPN Project.) - C:\WINDOWS\System32\drivers\tapnordvpn.sy
SR - Auto   [05/06/2019] [11814232]  TeamViewer 14 (TeamViewer) . (.TeamViewer GmbH.) - C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe  =>.T
SR - Demand [21/08/2017] [   50224]  USBPcap Capture Service (USBPcap) . (.USBPcap.) - C:\WINDOWS\System32\DRIVERS\USBPcap.sys  =>.Tomasz Moń®
SR - System [14/01/2019] [ 1021768]  VirtualBox Service (VBoxDrv) . (.Oracle Corporation.) - C:\WINDOWS\System32\DRIVERS\VBoxDrv.sys  =>.Oracle Corpor
SR - Demand [14/01/2019] [  235832]  VirtualBox NDIS 6.0 Miniport Service (VBoxNetAdp) . (.Oracle Corporation.) - C:\WINDOWS\System32\DRIVERS\VBoxNetA
SR - System [14/01/2019] [  247216]  VirtualBox NDIS6 Bridged Networking Service (VBoxNetLwf) . (.Oracle Corporation.) - C:\WINDOWS\System32\DRIVERS\V
SS - Demand [14/01/2019] [  690424]  VirtualBox system service (VBoxSDS) . (.Oracle Corporation.) - C:\Program Files\Oracle\VirtualBox\VBoxSDS.exe  =>
SR - System [14/01/2019] [  185960]  VirtualBox USB Monitor Service (VBoxUSBMon) . (.Oracle Corporation.) - C:\WINDOWS\System32\DRIVERS\VBoxUSBMon.sys
SR - Demand [01/08/2018] [   74648]  Virtual Gamepad Emulation Se (ViGEmBus) . (.Benjamin Höglinger-Stelzer.) - C:\Windows\System32\DriverStore\FileRe
SR - Auto   [21/11/2018] [  100784]  VMware Authorization Service (VMAuthdService) . (.VMware, Inc..) - C:\Program Files (x86)\VMware\VMware Workstati
SR - Boot   [22/06/2018] [  105024]  VMware VMCI Bus Dri (vmci) . (.VMware, Inc..) - C:\WINDOWS\System32\drivers\vmci.sys  =>.VMware, Inc.®
SR - System [21/11/2018] [   52288]  VMware Input Filter and Injection Driver (vmkbd) (vmkbd3) . (.VMware, Inc..) - C:\WINDOWS\System32\DRIVERS\vmkbd
SR - Demand [21/11/2018] [   46040]  VMware Virtual Ethernet Adapter Driver (VMnetAdapter) . (.VMware, Inc..) - C:\WINDOWS\System32\DRIVERS\vmnetadapt
SR - Auto   [21/11/2018] [  374192]  VMware DHCP Service (VMnetDHCP) . (.VMware, Inc..) - C:\Windows\SysWOW64\vmnetdhcp.exe  =>.VMware, Inc.®
SR - Auto   [21/11/2018] [   43992]  VMware Virtual Ethernet Userif for VMnet (VMnetuserif) . (.VMware, Inc..) - C:\WINDOWS\System32\DRIVERS\vmnetuser
SR - Auto   [02/11/2018] [  929712]  VMware USB Arbitration Service (VMUSBArbService) . (.VMware, Inc..) - C:\Program Files (x86)\Common Files\VMware\
SR - Auto   [21/11/2018] [  396208]  VMware NAT Service (VMware NAT Service) . (.VMware, Inc..) - C:\Windows\SysWOW64\vmnat.exe  =>.VMware, Inc.®
SR - Auto   [21/11/2018] [15446960]  VMware Workstation Server (VMwareHostd) . (.VMware, Inc..) - C:\Program Files (x86)\VMware\VMware Workstation\vmw
SR - Auto   [21/11/2018] [   99272]  VMware vmx86 (vmx86) . (.VMware, Inc..) - C:\WINDOWS\System32\DRIVERS\vmx86.sys  =>.VMware, Inc.®
SR - Boot   [07/12/2019] [  166712]  (vsmraid) . (.VIA Technologies Inc.,Ltd.) - C:\WINDOWS\System32\drivers\vsmraid.sys  =>.Microsoft®
SR - Boot   [22/06/2018] [   92040]  vSockets Virtual Machine Communication Interface Sockets dr (vsock) . (.VMware, Inc..) - C:\WINDOWS\System32\DRIV
SR - Auto   [28/02/2018] [   52576]  Vstor2 MntApi 2.0 Driver (shared) (vstor2-mntapi20-shared) . (.VMware, Inc..) - C:\Windows\SysWOW64\drivers\vstor
SR - Boot   [07/12/2019] [  305464]  VIA StorX Storage RAID Co (VSTXRAID) . (.VIA Corporation.) - C:\WINDOWS\System32\drivers\vstxraid.sys  =>.Microsc
SS - Demand [09/08/2019] [   29696]  wampapache64 (wampapache64) . (.Apache Software Foundation.) - G:\wamp64\bin\apache\apache2.4.41\bin\httpd.exe [U
SS - Demand [07/11/2019] [15837608]  wampmariadb64 (wampmariadb64) . (.MariaDB Corporation Ab.) - G:\wamp64\bin\mariadb\mariadb10.4.10\bin\mysqld.exe
SS - Demand [20/09/2019] [48781920]  wampmysqld64 (wampmysqld64) . (.Oracle America, Inc..) - G:\wamp64\bin\mysql\mysql8.0.18\bin\mysqld.exe  =>.Oracl
SR - Auto   [24/05/2018] [  922256]  WeMod Version Guard (WeMod Version Guard) . (.WeMod.) - C:\Program Files\WeMod\Version Guard\VersionGuard.exe  =>

---\ TÂCHES PLANIFIÉES EN AUTOMATIQUE (Registre) (70) - 9s
O38 - TASK: {03137AA4-56E1-44AD-842F-DF16EC8ABCC7} [64Bits][\Avast Software\Avast SecureLine VPN Update] - (.Avast Software - Avast Installer.) -- C:\
O38 - TASK: {0BEF08E8-D278-4760-9C25-6A734847D8B5} [64Bits][\GyazoUpdateTaskMachine] - (.Nota Inc. - Gyazo Auto Update Machine.) -- C:\Program Files (
O38 - TASK: {10EEE7E4-C1EB-4C63-89ED-038D8A602B7F} [64Bits][\NvTmRep_CrashReport1_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation - NVI
O38 - TASK: {1EE09AD9-9F36-4940-BD61-B713DA92142A} [64Bits][\NvProfileUpdaterDaily_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation - NV
O38 - TASK: {1F8A4F3B-63A6-4879-81E4-A3EEE132CEA5} [64Bits][\NvTmRep_CrashReport2_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation - NVI
O38 - TASK: {2057B086-45FC-4153-B205-BC5B4A386A2C} [64Bits][\NvDriverUpdateCheckDaily_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation -
O38 - TASK: {270C743C-75DB-4384-82B5-FB947103B951} [64Bits][\Avast Emergency Update] - (.AVAST Software - Avast Emergency Update.) -- C:\Program Files
O38 - TASK: {29A03350-42B8-41AF-9237-B7ABBD988A41} [64Bits][\RTKCPL] - (.Realtek Semiconductor - Gestionnaire audio HD Realtek.) -- C:\Program Files\R
O38 - TASK: {438EA983-B233-4F05-A995-5E3C00301A90} [64Bits][\Avast Software\Avast SecureLine VPN Bug Report] - (.AVAST Software - Avast Antivirus Bug
O38 - TASK: {4BAB0BC2-B7DB-442F-8C2E-F4D55F37BDB0} [64Bits][\Mozilla\Firefox Default Browser Agent 308046B0AF4A39CB] - (.Mozilla Foundation - Firefox
O38 - TASK: {51DCA780-9356-4F35-9A30-65CE47FB70FB} [64Bits][\Mozilla\Firefox Developer Edition Default Browser Agent CA9422711AE1A81C] - (.Mozilla Fou
O38 - TASK: {54A62B27-9A05-4C17-8696-3ACD3FEB9DBF} [64Bits][\Opera scheduled Autoupdate 1560214543] - (.Opera Software - Opera Internet Browser.) -- C
O38 - TASK: {681803EA-A78F-4B9D-9388-09EE5F735136} [64Bits][\Avast SecureLine VPN Update] - (.AVAST Software - Avast VPN Update.) -- C:\Program Files\
O38 - TASK: {68757C94-BD1D-4E22-9686-EFABA5F883B4} [64Bits][\Adobe Acrobat Update Task] - (.Adobe Inc. - Adobe Reader and Acrobat Manager.) -- C:\Prog
O38 - TASK: {6956CA3E-AE0F-43A8-B018-5AE43C7091D4} [64Bits][\GyazoUpdateTaskMachineDaily] - (.Nota Inc. - Gyazo Auto Update Machine.) -- C:\Program Fi
O38 - TASK: {71068D79-2234-45D1-A2BC-878C7E19AE68} [64Bits][\Opera scheduled assistant Autoupdate 1564930334] - (.Opera Software - Opera Internet Brow
O38 - TASK: {7907C012-AC50-4B3F-AC46-F3C76409F108} [64Bits][\NvBatteryBoostCheckOnLogon_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation
O38 - TASK: {8051BA02-DABB-418A-87AE-FD79D36C068E} [64Bits][\CCleanerSkipUAC] - (.Piriform Software Ltd - CCleaner.) -- C:\Program Files\CCleaner\CCle
O38 - TASK: {8EC274FB-8120-43E0-99DA-2AA1A7FA1C6D} [64Bits][\GoogleUpdateTaskMachineCore] - (.Google LLC - Programme d'installation de Google.) -- C:\
O38 - TASK: {92375299-E122-4727-9A2F-1AE2CB3A778D} [64Bits][\GoogleUpdateTaskMachineUA] - (.Google LLC - Programme d'installation de Google.) -- C:\Pr
O38 - TASK: {9492FF0A-5CC3-4E68-AC2A-091A3B785C99} [64Bits][\NvTmRep_CrashReport3_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation - NVI
O38 - TASK: {9D2FD9CC-261F-4CC5-8014-45ABD7AD92B4} [64Bits][\NvNodeLauncher_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation - NVIDIA no
O38 - TASK: {A3825B5C-DF99-4445-8C44-99A14A15BC2F} [64Bits][\DropboxUpdateTaskMachineCore] - (.Dropbox, Inc. - Dropbox Update.) -- C:\Program Files (x
O38 - TASK: {AD18EB43-AA3E-4293-8073-4FA809F449CF} [64Bits][\DropboxOEM] - (.DropboxOEM - DropboxOEM.) -- C:\Program Files (x86)\Dropbox\DropboxOEM\Dr
O38 - TASK: {AE046C4A-8685-4733-A2F2-44D3900C8C00} [64Bits][\NvTmRep_CrashReport4_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation - NVI
O38 - TASK: {AE12F474-4A17-4E11-A0A7-F94C446C2BA6} [64Bits][\DriverHubUACDisablingTask] - (...) -- C:/Program Files (x86)/DriverHub/DriverHub.exe  [0]
O38 - TASK: {B1317E28-7B29-4C81-BAE7-2F103A24D60B} [64Bits][\Avast Software\Overseer] - (.Avast Software - Avast Overseer.) -- C:\Program Files\Commor
O38 - TASK: {B5545E2D-88E8-4156-B9FF-4F45936E1A26} [64Bits][\GlaryOneClickOptimizer 5] - (.Glarysoft Ltd - OneClickMaintenance.) -- C:\Program Files (
O38 - TASK: {BCE14735-E1F8-45B2-865F-95A080664091} [64Bits][\NVIDIA GeForce Experience SelfUpdate_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA C
O38 - TASK: {C0F1F2E3-77C6-443B-A88F-7AA3FBF3BAC8} [64Bits][\MEGA\MEGAsync Update Task S-1-5-21-2155290971-1816436987-1419378802-1001] - (.Mega Limite
O38 - TASK: {C499A905-2B5A-49BD-A260-C6251CD5626A} [64Bits][\Adobe Flash Player Updater] - (.Adobe - Adobe® Flash® Player Update Service 32.0 r0.) --
O38 - TASK: {CA246C58-287A-4909-8814-402D084A1FF9} [64Bits][\DropboxUpdateTaskMachineUA] - (.Dropbox, Inc. - Dropbox Update.) -- C:\Program Files (x86
O38 - TASK: {E0FD1FED-A244-4E9B-B0E5-46791064C344} [64Bits][\CCleaner Update] - (.Piriform Software Ltd - CCleaner emergency updater.) -- C:\Program F
O38 - TASK: {EE5FCAF5-9588-4563-8874-2501FE40BF08} [64Bits][\Adobe Flash Player NPAPI Notifier] - (.Adobe - Adobe® Flash® Player Installer/Uninstaller
O38 - TASK: {EFAF4927-73E2-4911-A612-35314946BB03} [64Bits][\NvProfileUpdaterOnLogon_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation -
C:\WINDOWS\System32\Tasks\Avast Software\Avast SecureLine VPN Update - (.Avast Software.) -- C:\Program Files\Common Files\Avast Software\Icarus\avast
C:\WINDOWS\System32\Tasks\GyazoUpdateTaskMachine - (.Nota Inc..) -- C:\Program Files (x86)\Gyazo\GyazoUpdate.exe  []   =>.Nota Inc.
C:\WINDOWS\System32\Tasks\NvTmRep_CrashReport1_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files\NVIDIA Corporation\
C:\WINDOWS\System32\Tasks\NvProfileUpdaterDaily_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files\NVIDIA Corporation
C:\WINDOWS\System32\Tasks\NvTmRep_CrashReport2_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files\NVIDIA Corporation\
C:\WINDOWS\System32\Tasks\NvDriverUpdateCheckDaily_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files\NVIDIA Corporat
C:\WINDOWS\System32\Tasks\Avast Emergency Update - (.AVAST Software.) -- C:\Program Files\AVAST Software\Avast\AvEmUpdate.exe  []   =>.AVAST Software
C:\WINDOWS\System32\Tasks\RTKCPL - (.Realtek Semiconductor.) -- C:\Program Files\Realtek\Audio\HDA\RtkNGUI64.exe  [-s]   =>.Realtek Semiconductor
C:\WINDOWS\System32\Tasks\Avast Software\Avast SecureLine VPN Bug Report - (.AVAST Software.) -- C:\Program Files\Avast Software\SecureLine VPN\AvBugR
C:\WINDOWS\System32\Tasks\Mozilla\Firefox Default Browser Agent 308046B0AF4A39CB - (.Mozilla Foundation.) -- C:\Program Files\Mozilla Firefox\default-
C:\WINDOWS\System32\Tasks\Mozilla\Firefox Developer Edition Default Browser Agent CA9422711AE1A81C - (.Mozilla Foundation.) -- C:\Program Files\Firefo
```

```
C:\WINDOWS\System32\Tasks\Opera scheduled Autoupdate 1560214543 - (.Opera Software.) -- C:\Users\couli\AppData\Local\Programs\Opera\launcher.exe  [--s
C:\WINDOWS\System32\Tasks\Avast SecureLine VPN Update - (.AVAST Software.) -- C:\Program Files\Avast Software\SecureLine VPN\VpnUpdate.exe  []   =>.AV
C:\WINDOWS\System32\Tasks\Adobe Acrobat Update Task - (.Adobe Inc..) -- C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe  []   =>.Adobe
C:\WINDOWS\System32\Tasks\GyazoUpdateTaskMachineDaily - (.Nota Inc..) -- C:\Program Files (x86)\Gyazo\GyazoUpdate.exe  []   =>.Nota Inc.
C:\WINDOWS\System32\Tasks\Opera scheduled assistant Autoupdate 1564930334 - (.Opera Software.) -- C:\Users\couli\AppData\Local\Programs\Opera\launcher
C:\WINDOWS\System32\Tasks\NvBatteryBoostCheckOnLogon_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files\NVIDIA Corpor
C:\WINDOWS\System32\Tasks\CCleanerSkipUAC - (.Piriform Software Ltd.) -- C:\Program Files\CCleaner\CCleaner.exe  [$(Arg0)]   =>.Piriform Software Ltd
C:\WINDOWS\System32\Tasks\GoogleUpdateTaskMachineCore - (.Google LLC.) -- C:\Program Files (x86)\Google\Update\GoogleUpdate.exe  [/c]   =>.Google LLC
C:\WINDOWS\System32\Tasks\GoogleUpdateTaskMachineUA - (.Google LLC.) -- C:\Program Files (x86)\Google\Update\GoogleUpdate.exe  [/ua ./ua]   =>.Google
C:\WINDOWS\System32\Tasks\NvTmRep_CrashReport3_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files\NVIDIA Corporation\
C:\WINDOWS\System32\Tasks\NvNodeLauncher_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files (x86)\NVIDIA Corporation\
C:\WINDOWS\System32\Tasks\DropboxUpdateTaskMachineCore - (.Dropbox, Inc..) -- C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe  [/c]   =>.Dropb
C:\WINDOWS\System32\Tasks\DropboxOEM - (.DropboxOEM.) -- C:\Program Files (x86)\Dropbox\DropboxOEM\DropboxOEM.exe  [auto]   =>.DropboxOEM
C:\WINDOWS\System32\Tasks\NvTmRep_CrashReport4_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files\NVIDIA Corporation\
C:\WINDOWS\System32\Tasks\DriverHubUACDisablingTask - (...) -- C:/Program Files (x86)/DriverHub/DriverHub.exe  [$(Arg0)]
C:\WINDOWS\System32\Tasks\Avast Software\Overseer - (.Avast Software.) -- C:\Program Files\Common Files\AVAST Software\Overseer\overseer.exe  [/from_s
C:\WINDOWS\System32\Tasks\GlaryOneClickOptimizer 5 - (.Glarysoft Ltd.) -- C:\Program Files (x86)\Glary Utilities 5\OneClickMaintenance.exe  [/schedule
C:\WINDOWS\System32\Tasks\NVIDIA GeForce Experience SelfUpdate_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files\NVI
C:\WINDOWS\System32\Tasks\MEGA\MEGAsync Update Task S-1-5-21-2155290971-1816436987-1419378802-1001 - (.Mega Limited.) -- C:\ProgramData\MEGAsync\MEGAu
C:\WINDOWS\System32\Tasks\Adobe Flash Player Updater - (.Adobe.) -- C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe  []   =>.Adobe
C:\WINDOWS\System32\Tasks\DropboxUpdateTaskMachineUA - (.Dropbox, Inc..) -- C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe  [/ua ./ua]   =>.D
C:\WINDOWS\System32\Tasks\CCleaner Update - (.Piriform Software Ltd.) -- C:\Program Files\CCleaner\CCUpdate.exe  []   =>.Piriform Software Ltd
C:\WINDOWS\System32\Tasks\Adobe Flash Player NPAPI Notifier - (.Adobe.) -- C:\Windows\SysWOW64\Macromed\Flash\FlashUtil32_32_0_0_453_Plugin.exe  [-che
C:\WINDOWS\System32\Tasks\NvProfileUpdaterOnLogon_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files\NVIDIA Corporati

---\ APPLICATIONS LANCÉES AU DÉMARRAGE DU SYSTÈME (28) - 1s
O4 - HKLM\..\Run: [SecurityHealth] . (.Microsoft Corporation - Windows Security notification icon.) -- C:\WINDOWS\system32\SecurityHealthSystray.exe
O4 - HKLM\..\Run: [DellMobileConnectWelcome] . (.Screenovate Technologies Ltd. - Dell Mobile Connect Welcome.) -- C:\Program Files\Dell\DellMobileConn
O4 - HKLM\..\Run: [AdobeAAMUpdater-1.0] . (.Adobe Systems Incorporated - Adobe Updater Startup Utility.) -- C:\Program Files (x86)\Common Files\Adobe\
O4 - HKLM\..\Run: [AvastUI.exe] . (.AVAST Software - Avast AvLaunch component.) -- C:\Program Files\AVAST Software\Avast\AvLaunch.exe  =>.Avast Softwa
O4 - HKCU\..\Run: [ultracopier] . (.ultracopier.first-world.info - Supercopier under GPL3.) -- C:\Program Files (x86)\Supercopier\supercopier.exe [Uns
O4 - HKCU\..\Run: [LGHUB] . (.Logitech, Inc. - LGHUB.) -- C:\Program Files\LGHUB\lghub.exe  =>.Logitech Inc®
O4 - HKCU\..\Run: [ApowerMirror] . (.Apowersoft - ApowerMirror.) -- C:\Program Files (x86)\Apowersoft\ApowerMirror\ApowerMirror.exe  =>.Apowersoft Ltd
O4 - HKCU\..\Run: [MiPhoneManager] . (...) -- C:\Users\couli\AppData\Local\MiPhoneManager\main\MiPhoneHelper.exe  =>.Xiaomi Technology Inc®
O4 - HKCU\..\Run: [CCXProcess] . (.Adobe Systems Incorporated - CCXProcess.) -- C:\Program Files (x86)\Adobe\Adobe Creative Cloud Experience\CCXProces
O4 - HKCU\..\Run: [GUDelayStartup] . (.Glarysoft Ltd - Glary Utilities StartupManager.) -- C:\Program Files (x86)\Glary Utilities 5\StartupManager.exe
O4 - HKUS\S-1-5-19\..\Run: [OneDriveSetup] . (.Microsoft Corporation - Microsoft OneDrive (32 bit) Setup.) -- C:\Windows\SysWOW64\OneDriveSetup.exe  =
O4 - HKUS\S-1-5-20\..\Run: [OneDriveSetup] . (.Microsoft Corporation - Microsoft OneDrive (32 bit) Setup.) -- C:\Windows\SysWOW64\OneDriveSetup.exe  =
O4 - HKLM\..\Wow6432Node\Run: [vmware-tray.exe] . (.VMware, Inc. - VMware Tray Process.) -- C:\Program Files (x86)\VMware\VMware Workstation\vmware-tr
O4 - HKLM\..\Wow6432Node\Run: [jswtrayutil] . (.Atheros Communications, Inc. - Tray Utility for JumpStart for Wireless.) -- C:\Program Files (x86)\Jum
O4 - HKLM\..\Wow6432Node\Run: [SunJavaUpdateSched] . (.Oracle Corporation - Java Update Scheduler.) -- C:\Program Files (x86)\Common Files\Java\Java U
O4 - HKLM\..\Wow6432Node\Run: [Dropbox] . (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe  =>.Dropbox, Inc®
O4 - HKLM\..\Wow6432Node\Run: [Wondershare Helper Compact.exe] . (.Wondershare - Wondershare Studio.) -- C:\Program Files (x86)\Common Files\Wondersha
O4 - HKLM\..\Wow6432Node\Run: [RtlS5Wake] . (.Realtek - Realtek WOWL Utility.) -- C:\Program Files (x86)\Realtek\PCIE Wireless LAN\RtlS5Wake\RtlS5Wake
O4 - HKLM\..\Wow6432Node\Run: [HPMessageService] . (.HP Inc. - HP Message Service.) -- C:\Program Files (x86)\HP\HP System Event\HPMSGSVC.exe  =>.HP I
O4 - HKLM\..\Wow6432Node\Run: [PWRISOVM.EXE] . (.Power Software Ltd - PowerISO Virtual Drive Manager.) -- C:\Program Files\PowerISO\PWRISOVM.EXE {19EA
O4 - HKUS\S-1-5-19\..\StartupApproved\Run: [OneDriveSetup] . (. - .) -- 0x020000000000000000000000  =>.SUP.Orphan
O4 - HKUS\S-1-5-20\..\StartupApproved\Run: [OneDriveSetup] . (. - .) -- 0x020000000000000000000000  =>.SUP.Orphan
O4 - HKUS\S-1-5-21-2155290971-1816436987-1419378802-1001\..\Run: [ultracopier] . (.ultracopier.first-world.info - Supercopier under GPL3.) -- C:\Progr
O4 - HKUS\S-1-5-21-2155290971-1816436987-1419378802-1001\..\Run: [LGHUB] . (.Logitech, Inc. - LGHUB.) -- C:\Program Files\LGHUB\lghub.exe  =>.Logitech
O4 - HKUS\S-1-5-21-2155290971-1816436987-1419378802-1001\..\Run: [ApowerMirror] . (.Apowersoft - ApowerMirror.) -- C:\Program Files (x86)\Apowersoft\A
O4 - HKUS\S-1-5-21-2155290971-1816436987-1419378802-1001\..\Run: [MiPhoneManager] . (...) -- C:\Users\couli\AppData\Local\MiPhoneManager\main\MiPhoneH
O4 - HKUS\S-1-5-21-2155290971-1816436987-1419378802-1001\..\Run: [CCXProcess] . (.Adobe Systems Incorporated - CCXProcess.) -- C:\Program Files (x86)\
O4 - HKUS\S-1-5-21-2155290971-1816436987-1419378802-1001\..\Run: [GUDelayStartup] . (.Glarysoft Ltd - Glary Utilities StartupManager.) -- C:\Program F

---\ PROCESSUS LANCÉS (73) - 7s
[MD5.07F534F4C0B3351CEFBC0506251FF314] - (.HP Inc. - Description.) -- C:\Windows\System32\DriverStore\FileRepository\hpomencustomcapcomp.inf_amd64_b6e
[MD5.5156DCC4470BCFA06172FE63F21849B7] - (.HP Inc. - .) -- C:\Windows\System32\DriverStore\FileRepository\hpcustomcapcomp.inf_amd64_66856cbf5000451f\
[MD5.5414DC5A9C809817D167383AAFB56F81] - (.HP Inc. - .) -- C:\Windows\System32\DriverStore\FileRepository\hpcustomcapcomp.inf_amd64_66856cbf5000451f\
[MD5.2F00C76D2E5B8EB9385DC939F26C8D3F] - (.HP Inc. - .) -- C:\Windows\System32\DriverStore\FileRepository\hpcustomcapcomp.inf_amd64_66856cbf5000451f\
[MD5.1604D9B61B9190F90DEB7CED22DACCFA] - (.HP Inc. - HP Touchpoint Analytics Client Service.) -- C:\Windows\System32\DriverStore\FileRepository\hpanal
[MD5.3923516F4855C856D7C8D92431593DBA] - (.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporation\Display.NvContainer\NVDispla
[MD5.3923516F4855C856D7C8D92431593DBA] - (.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporation\Display.NvContainer\NVDispla
[MD5.A85905B98BE430F0061B3B9603015F7B] - (.Realtek Semiconductor - Realtek Audio Service.) -- C:\Program Files\Realtek\Audio\HDA\RtkAudioService64.exe
[MD5.691AB1A682E7134F26CD051A34245992] - (.Realtek Semiconductor - HD Audio Background Process.) -- C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe [15
[MD5.691AB1A682E7134F26CD051A34245992] - (.Realtek Semiconductor - HD Audio Background Process.) -- C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe [15
[MD5.BE806D910B83F0EC498AA14247903DA2] - (.AVAST Software - Avast Antivirus.) -- C:\Program Files\AVAST Software\Avast\aswToolsSvc.exe [3096160] [PID
[MD5.9ED98E2FF9DF69FDEB082B3160ADFE0B] - (.AOMEI Tech Co., Ltd. - AOMEI Backupper Schedule task service.) -- C:\Program Files (x86)\AOMEI Backupper\AE
[MD5.8706E6B028ADC6C2348250F508BC4975] - (.Prey, Inc. - Execution Service.) -- C:\Windows\Prey\wpxsvc.exe [6886432] [PID.7200] {01E84CE2860CF3D794990E
[MD5.76E4BE50B2917EA57B62C35344E89E39] - (.Adobe Inc. - Adobe Acrobat Update Service.) -- C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe
[MD5.AA2B1E79957B0656093C9E791FACD57C] - (.Dropbox, Inc. - Dropbox Service.) -- C:\WINDOWS\system32\DbxSvc.exe [44552] [PID.7328] [Unsigned]  =>.Dropb
[MD5.B5C2F92EE1106DFE7BB1CCE4D35B6037] - (.Apple Inc. - Bonjour Service.) -- C:\Program Files\Bonjour\mDNSResponder.exe [462096] [PID.7392]  =>.Apple
[MD5.258A11B27A9CC70D85B01BBD94389B2F] - (.Atheros Communications, Inc. - JumpStart PushButton Service.) -- C:\Program Files (x86)\Jumpstart\jswpbapi
[MD5.7926F886BD4328540D88C1E8492BDE7B] - (...) -- C:\Program Files (x86)\Microvirt\MEmu\MemuService.exe [85304] [PID.7488]  =>.Shanghai Microvirt Soft
[MD5.BA02B8B8D32B492A70BBB3DBA564390C] - (.McAfee, LLC - McAfee WebAdvisor.) -- C:\Program Files\McAfee\WebAdvisor\ServiceHost.exe [955656] [PID.7496]
[MD5.EC37EFD653F9FAEA7526C055735E1DE3] - (.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe
[MD5.E6900CD558C69BBDECB3214A789F671E] - (.Electronic Arts - OriginWebHelperService.) -- C:\Program Files (x86)\Origin\OriginWebHelperService.exe [347
[MD5.74A713B8FF013724DBC2F46DB95B4ABB] - (.Realtek Semiconductor Corp. - Realtek Bluetooth RtkBTAudio Service Applic.) -- C:\Windows\RtkBtAudioServ.ex
[MD5.5315C25300635E21E9B668ED0E0027F5] - (.AVAST Software - Avast VPN Service.) -- C:\Program Files\AVAST Software\SecureLine VPN\VpnSvc.exe [7897696]
[MD5.7B5EDAD629FC8BAB0D4D953AB0EAFE34] - (.Realtek Semiconductor Corp. - Realtek Bluetooth BTDevManager Service Appl.) -- C:\Windows\RtkBtManServ.exe
[MD5.46826B02C346D48A62FF11882AF662BB] - (.DEVGURU Co., LTD. - MSS CS Connectivity Service.) -- C:\Program Files\Samsung\USB Drivers\27_ssconn\conn\ss
[MD5.E71D8D771B0B87F732F1DC2881703593] - (.TeamViewer GmbH - TeamViewer 14.) -- C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe [11814232] [P
[MD5.ADC2A1F46DA3BF1D5B6F53976290FB7D] - (.VMware, Inc. - VMware Authorization Service.) -- C:\Program Files (x86)\VMware\VMware Workstation\vmware-au
[MD5.59C8BF1A8C9CBB6EC136DC7F7476250D] - (.VMware, Inc. - VMware USB Arbitration Service.) -- C:\Program Files (x86)\Common Files\VMware\USB\vmware-us
[MD5.CF3EDFAA9CC87E223F9316B5D0F1AA84] - (.VMware, Inc. - VMware VMnet DHCP service.) -- C:\Windows\SysWOW64\vmnetdhcp.exe [374192] [PID.8016]  =>.VMw
[MD5.92BBB76CDF269E7373F153A8296B13E2] - (.VMware, Inc. - VMware NAT Service.) -- C:\Windows\SysWOW64\vmnat.exe [396208] [PID.8028]  =>.VMware, Inc.®
[MD5.33E2ED11AA6CF38C302A391B236EAB7D] - (.WeMod - WeMod Version Guard.) -- C:\Program Files\WeMod\Version Guard\VersionGuard.exe [922256] [PID.8092]
[MD5.50A653B05523839530AFB67B64C9B5AE] - (.Intel(R) Corporation - XtuService.) -- C:\Windows\SysWOW64\XtuService.exe [81984] [PID.8420] {00B15FDDBBCD5
[MD5.C4F6ADC632029D6E2E7F84629DC6C22B] - (.Intel Corporation - Intel(R) Dynamic Application Loader Host In.) -- C:\Windows\System32\DriverStore\FileRe
[MD5.DEE2497B558B765C9C07EA23A8FA11B0] - (...) -- C:\Program Files (x86)\VMware\VMware Workstation\vmware-hostd.exe [15446960] [PID.10572]  =>.VMware,
[MD5.357306CF8AD2D18F06CBEC4FC2D33692] - (.Node.js - Node.js: Server-side JavaScript.) -- C:\Windows\Prey\current\bin\node.exe [21910168] [PID.10856]
[MD5.4CB8D900C485BBBF9B2469D11BC42C2A] - (.McAfee, LLC - McAfee WebAdvisor.) -- C:\Program Files\McAfee\WebAdvisor\uihost.exe [954568] [PID.10904]  =>
[MD5.EC37EFD653F9FAEA7526C055735E1DE3] - (.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe
[MD5.EC37EFD653F9FAEA7526C055735E1DE3] - (.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe
[MD5.6AECA53F405206CAD08032B2FE2423D7] - (...) -- C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHos
[MD5.F00EA296DDA78FE0D3E830F680737664] - (.Fork, Ltd. - Light Event Monitor.) -- C:\Windows\Prey\versions\1.9.6\node_modules\os-triggers\bin\lightevt
[MD5.7A67AEB4C77D30787B3BAC516A81F2B1] - (.Gold Click Ltd - PG Network Component.) -- C:\Program Files (x86)\ProxyGate\Cloud.exe [1503328] [PID.15568]
[MD5.96C36729FFEEEE3B7BA7ADD80C4418F6] - (.Gold Click Ltd - PG Helper Process.) -- C:\Program Files (x86)\ProxyGate\PGChk.exe [1007200] [PID.16236]  =
[MD5.18E7C4F315650666F813E055EABFCC60] - (.NVIDIA Corporation - NVIDIA ShadowPlay Helper.) -- C:\Program Files\NVIDIA Corporation\ShadowPlay\nvsphelpe
[MD5.CA9C8A1264F8FE0C2C5DF7A700BC0470] - (.NVIDIA Corporation - NVIDIA Share.) -- C:\Program Files\NVIDIA Corporation\NVIDIA GeForce Experience\NVIDIA
[MD5.CA9C8A1264F8FE0C2C5DF7A700BC0470] - (.NVIDIA Corporation - NVIDIA Share.) -- C:\Program Files\NVIDIA Corporation\NVIDIA GeForce Experience\NVIDIA
[MD5.CD1E662E6914EAFF07F7A8F954307E0F] - (.Node.js - NVIDIA Web Helper Service.) -- C:\Program Files (x86)\NVIDIA Corporation\NvNode\NVIDIA Web Helper
[MD5.58BFC1D570D95A2D8BF24BBB4FF1018B] - (.Google LLC - Google Crash Handler.) -- C:\Program Files (x86)\Google\Update\1.3.36.32\GoogleCrashHandler.ex
[MD5.F6F578B921C7EA22A87DEC983A812935] - (.Google LLC - Google Crash Handler.) -- C:\Program Files (x86)\Google\Update\1.3.36.32\GoogleCrashHandler64
```

```
[MD5.EC37EFD653F9FAEA7526C055735E1DE3] - (.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe
[MD5.EC37EFD653F9FAEA7526C055735E1DE3] - (.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe
[MD5.CA9C8A1264F8FE0C2C5DF7A700BC0470] - (.NVIDIA Corporation - NVIDIA Share.) -- C:\Program Files\NVIDIA Corporation\NVIDIA GeForce Experience\NVIDIA
[MD5.B821F15AB566147EA75B1ABB6FCD2D9B] - (.HP Inc. - HPSystemEventUtilityHost.) -- C:\Program Files\WindowsApps\AD2F1837.HPSystemEventUtility_1.1.21.6
[MD5.AD6873887790C73170728BF5766D571E] - (.AVAST Software - Avast Antivirus.) -- C:\Program Files\AVAST Software\Avast\AvastUI.exe [9986144] [PID.1838
[MD5.AC31C642D258E154BF65365BCD24F8B9] - (.AVAST Software - Avast SecureLine VPN.) -- C:\Program Files\AVAST Software\SecureLine VPN\Vpn.exe [5340264]
[MD5.39185FDF8D49D97D06035B3B2B4F1CD1] - (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe [7992832] [PID.18436]  =>.Dr
[MD5.39185FDF8D49D97D06035B3B2B4F1CD1] - (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe [7992832] [PID.18504]  =>.Dr
[MD5.39185FDF8D49D97D06035B3B2B4F1CD1] - (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe [7992832] [PID.18564]  =>.Dr
[MD5.AC31C642D258E154BF65365BCD24F8B9] - (.AVAST Software - Avast SecureLine VPN.) -- C:\Program Files\AVAST Software\SecureLine VPN\Vpn.exe [5340264]
[MD5.AC31C642D258E154BF65365BCD24F8B9] - (.AVAST Software - Avast SecureLine VPN.) -- C:\Program Files\AVAST Software\SecureLine VPN\Vpn.exe [5340264]
[MD5.C1CBE291B368CEDF7115974D14A9B63B] - (.Scarlet.Crush Productions 2012, 2013; InhexSTER, Hect - DS4Windows.) -- C:\Users\couli\OneDrive\Bureau\DS4W
[MD5.AD329C90AFCAE0CA94126F5851431DF7] - (.Realtek - Realtek WOWL Utility.) -- C:\Program Files (x86)\Realtek\PCIE Wireless LAN\Rtl5S5Wake\Rtl5S5Wake.ex
[MD5.82A4658E3D76822F04BC24BE2B247A15] - (.HP Inc. - HP Message Service.) -- C:\Program Files (x86)\HP\HP System Event\HPMSGSVC.exe [707624] [PID.1927
[MD5.3435BEF9AF5615467C7645027CC34D84] - (.The Qt Company Ltd. - Qt Qtwebengineprocess.) -- C:\Program Files (x86)\Dropbox\Client\111.4.472\QtWebEngir
[MD5.3435BEF9AF5615467C7645027CC34D84] - (.The Qt Company Ltd. - Qt Qtwebengineprocess.) -- C:\Program Files (x86)\Dropbox\Client\111.4.472\QtWebEngir
[MD5.AD6873887790C73170728BF5766D571E] - (.AVAST Software - Avast Antivirus.) -- C:\Program Files\AVAST Software\Avast\AvastUI.exe [9986144] [PID.2036
[MD5.AD6873887790C73170728BF5766D571E] - (.AVAST Software - Avast Antivirus.) -- C:\Program Files\AVAST Software\Avast\AvastUI.exe [9986144] [PID.2033
[MD5.09B2B041FC70C65C03D9806815741E99] - (.Intel Corporation - Intel® SGX Application Enclave Services Man.) -- C:\Program Files\Intel\IntelSGXPSW\bir
[MD5.A1F58FFF448E4099297D6EE0641D4D0E] - (.Dropbox, Inc. - Dropbox Update.) -- C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe [143144] [PID.9
[MD5.4E56582C73772B621B21310FCA8D57AC] - (.HP Inc. - CommRecovery.) -- C:\Program Files\HPCommRecovery\HPCommRecovery.exe [905080] [PID.21080]  =>.HP
[MD5.D6314611A197BACD59669A2784E290FD] - (.HP Inc. - HP JumpStart Bridge.) -- C:\Program Files (x86)\HP\HP JumpStart Bridge\HPJumpStartBridge.exe [471
[MD5.1ED6E48252C137E23674AE8FBBE75882] - (.Intel Corporation - Intel(R) Local Management Service.) -- C:\Program Files (x86)\Intel\Intel(R) Management
[MD5.8C433B757234147A90650869CB856C80] - (.HP Inc. - HP WMI Service.) -- C:\Program Files (x86)\HP\HP System Event\HPWMISVC.exe [628768] [PID.21224]
[MD5.804D47DAF5AA8B367D912F2BA8B7C1DD] - (.Nicolas Coolman - ZHPSuite.) -- H:\ZHPSuite.exe [3443584] [PID.1124] [Unsigned]  =>.Nicolas Coolman

---\ CHROME, Démarrage, Recherche, Extensions (6) - 0s
G2 - GCE: Preference [Ousmane][User Data\Default\Extensions] [apdfllckaahabafndbhieahigkjlhalf] http://drive.google.com/  =>.Google Inc. {Drive}
G2 - GCE: Preference [Ousmane][User Data\Default\Extensions] [blpcfgokakmgnkcojhhkbfbldkacnbeo] http://www.youtube.com  =>.Youtube {Youtube}
G2 - GCE: Preference [Ousmane][User Data\Default\Extensions] [nmmhkkegccagdldgiimedpiccmgmieda]  =>.Google Inc. {Wallet}
G2 - GCE: Preference [Ousmane][User Data\Default\Extensions] [pjkljhegncpnkpknbcohdijeoejaedia] http://mail.google.com/  =>.Google Inc. {Gmail}
G2 - GCE: Preference [Ousmane][User Data\Default\Extensions] [pkedcjkdefgpdelpbcmbmeomcjbeemfm] Chrome Media Router  =>.Google Inc.
G2 - GCE: Preference [Ousmane][User Data\Default\Sync Extension Settings] [pkedcjkdefgpdelpbcmbmeomcjbeemfm]  =>.Google Inc. {Chrome Media Router}

---\ FIREFOX, Plugins,Démarrage,Recherche,Extensions (64) - 6s
P2 - EXT FILE: (.French Dict. - Dictionnaire orthographique pour la la.) -- C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-editi
P2 - EXT FILE: (.Français Language Pack - Language pack for Firefox for fr.) -- C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-e
P2 - EXT FILE: (.Avast Software s.r.o.) -- C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-edition-default\extensions\sp@avast.co
P2 - EXT FILE: (.Avast Software s.r.o.) -- C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-edition-default\extensions\wrc@avast.c
P2 - EXT FILE: (.ImTranslator.) -- C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-edition-default\extensions\{9AA46F4F-4DC7-4c0
P2 - EXT FILE: (.Google Inc..) -- C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-edition-default\extensions\{d10d0bf8-f5b5-c8b4-
P2 - EXT FILE: (.Legitimate.) -- C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\extensions\adguardadblocker@adguard.com.xpi
P2 - EXT FILE: (...) -- C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\extensions\bdtbe@bitdefender.com.xpi [Unsigned]
P2 - EXT FILE: (.Mozilla Corporation.) -- C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\extensions\jid1-93WyvpgvxzGATw@jetp
P2 - EXT FILE: (.adblocker-for-youtube - Removes all annoying ads and banners f.) -- C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq
P2 - EXT FILE: (.Avast Software s.r.o.) -- C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\extensions\sp@avast.com.xpi [Unsig
P2 - EXT FILE: (.Avast Software s.r.o.) -- C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\extensions\wrc@avast.com.xpi [Unsi
P2 - EXT FILE: (.Matte Black (Red).) -- C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\extensions\{a7589411-c5f6-41cf-8bdc-f
P2 - EXT FILE: (.BandcampVolume - Adds volume slider to bandcamp music p.) -- C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default
P2 - EXT FILE: (.Google Inc..) -- C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\extensions\{d10d0bf8-f5b5-c8b4-a8b2-2b9879e
P2 - EXT FILE: (.Abstract Neon Robots.) -- C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\extensions\{d3b696dc-7d5a-4279-b5f
P2 - EXT FILE: (.Matte Black (Orange).) -- C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\extensions\{e7c9fb23-17c0-4bb6-a8b
P2 - EXT FILE: (.Bing Search Engine - Bing. Search by Microsoft..) -- C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\searchp
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 Corpor
P2 - EXT FILE: (.Mozilla Corporation.) -- C:\Program Files\Mozilla Firefox\browser\features\screenshots@mozilla.org.xpi [Unsigned]  =>.Mozilla Corpora
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
P2 - FPN: [HKLM] [@adobe.com/FlashPlayer] - (.Adobe.) -- C:\Windows\SysWOW64\Macromed\Flash\NPSWF32_32_0_0_453.dll  =>.Adobe
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-edition-default\bookmarkbackups  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-edition-default\crashes  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-edition-default\datareporting  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-edition-default\extensions  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-edition-default\gmp  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-edition-default\gmp-gmpopenh264  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-edition-default\gmp-widevinecdm  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-edition-default\minidumps  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-edition-default\saved-telemetry-pings  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-edition-default\security_state  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-edition-default\sessionstore-backups  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-edition-default\shader-cache  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-edition-default\storage  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\2ztgmk95.dev-edition-default\weave  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\bookmarkbackups  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\browser-extension-data  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\crashes  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\datareporting  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\extensions  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\features  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\gmp  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\gmp-gmpopenh264  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\gmp-widevinecdm  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\mediacapabilities  =>Legitimate
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\minidumps  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\saved-telemetry-pings  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\searchplugins  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\security_state  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\sessionstore-backups  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\shader-cache  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\storage  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\weave  =>Mozilla Corporation
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\browser-extension-data\firefox@ghostery.com  =>Ghostery
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\browser-extension-data\fxmonitor@mozilla.org  =>Firefox Monitor
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\browser-extension-data\hotfix-update-xpi-intermediate@mozilla.com  =>Mozilla
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\browser-extension-data\mozilla_cc3@internetdownloadmanager.com  =>Tonec Inc
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\browser-extension-data\webcompat@mozilla.org  =>webcompat.com
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\browser-extension-data\{d10d0bf8-f5b5-c8b4-a8b2-2b9879e08c5d}  =>Google Inc.
C:\Program Files\Mozilla Firefox\defaults\pref\secure_cert.js
C:\Program Files\Mozilla Firefox\defaults\pref\pref('security.enterprise_roots.enabled', true);

---\ OPERA, Démarrage,Recherche,Plugins (4) - 0s
B2 - EXT: [Avira Operations GmbH & Co. KG] C:\Users\couli\AppData\Roaming\Opera Software\Opera Stable\Extensions\dalelnnofafalcmkmnhdbigbjjkloabo  =>
B2 - EXT: [Opera Software AS] C:\Users\couli\AppData\Roaming\Opera Software\Opera Stable\Extensions\enegjkbbakeegngfapepobipndnebkdk
B2 - EXT: [Avira Operations GmbH & Co. KG] C:\Users\couli\AppData\Roaming\Opera Software\Opera Stable\Extensions\ngohaaocccbohaffogpbgfpmpgbcgccg  =>
```

```
B2 - EXT: [Unknown] C:\Users\couli\AppData\Roaming\Opera Software\Opera Stable\Extensions\pcgkmkjdikhiodinhloioejnpjgmfigd  =>.Unknown

---\ INTERNET EXPLORER,Démarrage,Recherche,URLSearchHook (15) - 0s
R0 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = http://go.microsoft.com/  =>.Microsoft Corporation
R0 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = http://go.microsoft.com/  =>.Microsoft Corporation
R0 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main,Start Page = http://go.microsoft.com/  =>.Microsoft Corporation
R1 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft.com/  =>.Microsoft Corporation
R1 - 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.) (11.00.19041.561 (WinBu

---\ INTERNET EXPLORER, Site de confiance et site sensible (3) - 0s
~ IE Restricted Site Good: localhost
IE Restricted Site Good: webcompanion.com  =>PUP.Optional.LavasoftWebCompanion
~ Microsoft Internet Explorer Restricted Site(s) Domains: 2(Good) / 0(Bad)

---\ MICROSOFT EDGE, Plugin,Favoris,Démarrage,Recherche,Extension (1) - 0s
E2 - GCE: Preference [Ousmane][User Data\Default\Local Extension Settings] [jdiccldimpdaibmpdkjnbmckianbfold]  =>.Microsoft Corporation

---\ INTERNET EXPLORER,Proxy Management (5) - 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\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyEnable = 0  =>.Default.Value
R5 - HKLM\SYSTEM\CurrentControlSet\services\NlaSvc\Parameters\Internet\ManualProxies []  =>.Microsoft
R5 - HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyEnable = 0  =>.Default.Value

---\ 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) (2)

---\ BROWSER HELPER OBJECT DE NAVIGATEUR (BHO) (5) - 0s
O2 - BHO: IEToEdge BHO [64Bits] - {1FD49718-1D00-4B19-AF5F-070AF6D5D54C} . (.Microsoft Corporation - IEToEdge BHO.) -- C:\Program Files (x86)\Microsof
O2 - BHO: Java(tm) Plug-In SSV Helper [64Bits] - {761497BB-D6F0-462C-B6EB-D4DAF1D92D43} . (.Oracle Corporation - Java(TM) Platform SE binary.) -- C:\P
O2 - BHO: McAfee WebAdvisor [64Bits] - {B164E929-A1B6-4A06-B104-2CD0E90A88FF} . (.McAfee, LLC - McAfee WebAdvisor.) -- C:\Program Files\McAfee\WebAdvi
O2 - BHO: Java(tm) Plug-In 2 SSV Helper [64Bits] - {DBC80044-A445-435b-BC74-9C25C1C588A9} . (.Oracle Corporation - Java(TM) Platform SE binary.) -- C
O2 - BHO: HP Network Check Helper [64Bits] - {E76FD755-C1BA-4DCB-9F13-99BD91223ADE} . (.HP Inc. - HP Network Check IE Plug-in.) -- C:\Program Files (x

---\ RACCOURCIS GLOBAL STARTUP (232) - 27s
O4 - GS\Desktop [Ousmane]: Airport CEO.exe - Raccourci.lnk . (...) D:\Téléchargerment New\Airport.CEO.v32.6-4\Airport.CEO.v32.6-4\Airport CEO\Airport
O4 - GS\Desktop [Ousmane]: AoC2.lnk . (...) D:\Age of Civilizations II\Age.of.Civilizations.II.v1.0145\Age of Civilizations II\AoC2.exe  [Unsigned]
O4 - GS\Desktop [Ousmane]: Assistant Mise à jour de Windows 10.lnk . (.Microsoft Corporation - Assistant Mise à jour de Windows 10.) C:\Windows10Upgra
O4 - GS\Desktop [Ousmane]: Atom.lnk . (.GitHub, Inc. - Atom.) C:\Users\couli\AppData\Local\atom\atom.exe  [Unsigned]  =>.GitHub, Inc.
O4 - GS\Desktop [Ousmane]: Brackets.lnk . (.brackets.io - Raccourci vers Brackets.) C:\Program Files (x86)\Brackets\Brackets.exe  =>.Adobe Inc.®
O4 - GS\Desktop [Ousmane]: Cain.lnk . (.oxid.it - Cain - Password Recovery Utility.) C:\Program Files (x86)\Cain\Cain.exe  [Unsigned]  =>.oxid.it
O4 - GS\Desktop [Ousmane]: Cheat Engine.lnk . (...) C:\Program Files\Cheat Engine 7.0\Cheat Engine.exe  =>.Cheat Engine®
O4 - GS\Desktop [Ousmane]: CodeBlocks.lnk . (.Code::Blocks Team - Code::Blocks IDE.) C:\Program Files (x86)\CodeBlocks\codeblocks.exe  [Unsigned]  =>
O4 - GS\Desktop [Ousmane]: Compressed - Raccourci.lnk . (...) D:\Téléchargerment New\Compressed  [Unsigned]
O4 - GS\Desktop [Ousmane]: CrystalDiskInfo.lnk . (.Crystal Dew World - CrystalDiskInfo.) C:\Program Files (x86)\CrystalDiskInfo\DiskInfo32.exe  =>.M
O4 - GS\Desktop [Ousmane]: CrystalDiskMark 5.lnk . (.Crystal Dew World - CrystalDiskMark.) C:\Program Files\CrystalDiskMark5\DiskMark64.exe  =>.Nori
O4 - GS\Desktop [Ousmane]: Discord.lnk . (.GitHub - Update.) C:\Users\couli\AppData\Local\Discord\Update.exe --processStart Discord.exe  =>.Discord I
O4 - GS\Desktop [Ousmane]: Dropbox.lnk . (.Dropbox, Inc. - Dropbox.) C:\Program Files (x86)\Dropbox\Client\Dropbox.exe /home  =>.Dropbox, Inc®
O4 - GS\Desktop [Ousmane]: Eclipse Java 2019-03.lnk . (...) C:\Users\couli\eclipse\java-2019-03\eclipse\eclipse.exe  [Unsigned]
O4 - GS\Desktop [Ousmane]: F1 2018.lnk . (.Codemasters Software Company Limited - F1 2018 Executable.) G:\Games\F1 2018\F1_2018.exe  [Unsigned]  =>.C
O4 - GS\Desktop [Ousmane]: Farming Simulator 19.lnk . (.GIANTS Software GmbH - GIANTS Engine 8.0.0.) D:\Games\Farming Simulator 19\x64\FarmingSimulato
O4 - GS\Desktop [Ousmane]: Fishing Sim World.lnk . (...) G:\FishingSimWorld\FishingGame.exe  [Unsigned]
O4 - GS\Desktop [Ousmane]: FiveM Singleplayer.lnk . (.cfx-collective - FiveM.) C:\Users\couli\AppData\Local\FiveM\FiveM.exe -sp  [Unsigned]  =>.cfx-co
O4 - GS\Desktop [Ousmane]: FiveM.lnk . (.cfx-collective - FiveM.) C:\Users\couli\AppData\Local\FiveM\FiveM.exe  [Unsigned]  =>.cfx-collective
O4 - GS\Desktop [Ousmane]: Fonts Ninja.lnk . (.Fonts Ninja - Fonts Ninja.) C:\Users\couli\AppData\Local\Programs\FontsNinja\Fonts Ninja.exe  {00ED647
O4 - GS\Desktop [Ousmane]: Free Flash eBook Maker .lnk . (.flipbuilder.com - .) C:\Program Files (x86)\Free Flash eBook Maker\flipchm.exe  [Unsigned]
O4 - GS\Desktop [Ousmane]: Frostpunk The Fall of Winterhome.lnk . (.11 bit studios S.A. - Frostpunk.) G:\Games\Frostpunk The Fall of Winterhome\Frostp
O4 - GS\Desktop [Ousmane]: Game.exe - Raccourci.lnk . (...) D:\Téléchargerment New\Project.Highrise.v1.4.2.20170208\Project.Highrise.v1.4.2.20170208\G
O4 - GS\Desktop [Ousmane]: HTTrack Website Copier.lnk . (.HTTrack - WinHTTrack Website Copier, Copy Websites to.) C:\Program Files (x86)\WinHTTrack\Wi
O4 - GS\Desktop [Ousmane]: Install Kaspersky Internet Security version 19.0.0.1088.lnk . (.Kaspersky Lab - Kaspersky Internet Security [19.0.0.1088.0
O4 - GS\Desktop [Ousmane]: Jarvee.lnk . (.Jarvee - Jarvee.) C:\Users\couli\AppData\Roaming\Jarvee\Jarvee.exe  {0B414C00BF45EDB4865CE431D4954843}.
O4 - GS\Desktop [Ousmane]: Jurassic World Evolution.lnk . (.Frontier Developments - Jurassic World Evolution.) D:\Games\Jurassic World Evolution\JWE.e
O4 - GS\Desktop [Ousmane]: LAUNCHER.exe - Raccourci.lnk . (...) D:\SteamLibrary\steamapps\common\Startup Company\LAUNCHER.exe  [Unsigned]  =>.Steam C
O4 - GS\Desktop [Ousmane]: LOA mme Coulibaly.pdf - Raccourci.lnk . (...) D:\Téléchargerment New\LOA mme Coulibaly.pdf  [Unsigned]
O4 - GS\Desktop [Ousmane]: MadGamesTycoon.exe -.lnk . (...) D:\Mad.Games.Tycoon.v1.171020A\Mad.Games.Tycoon.v1.171020A\MadGamesTycoon.exe  [Unsigned]
O4 - GS\Desktop [Ousmane]: MEmu.lnk . (.Microvirt Software Technology Co. Ltd. - MEmu App Player.) C:\Program Files (x86)\Microvirt\MEmu\MEmu.exe  =
O4 - GS\Desktop [Ousmane]: Microsoft Edge.lnk . (.Microsoft Corporation - Microsoft Edge.) C:\Program Files (x86)\Microsoft\Edge\Application\msedge.ex
O4 - GS\Desktop [Ousmane]: MiPCSuite.lnk . (.Xiaomi.Inc - MiPCSuite Module.) C:\Users\couli\AppData\Local\MiPhoneManager\main\MiPCSuite.exe -desktop
O4 - GS\Desktop [Ousmane]: Molotov.lnk . (.GitHub - Update.) C:\Users\couli\AppData\Local\Molotov\Update.exe --processStart 'Molotov.exe'  [Unsigned]
O4 - GS\Desktop [Ousmane]: Multi-Drive.lnk . (...) D:\Program Files\Nox\bin\MultiPlayerManager.exe  =>.Nox Limited®
O4 - GS\Desktop [Ousmane]: Multi-MEmu.lnk . (.Microvirt Software Technology Co. Ltd. - MEmu Multiple Instances Manager.) C:\Program Files (x86)\Microv
O4 - GS\Desktop [Ousmane]: Navigateur Opera.lnk . (.Opera Software - Opera Internet Browser.) C:\Users\couli\AppData\Local\Programs\Opera\launcher.exe
O4 - GS\Desktop [Ousmane]: NBA 2K19.lnk . (...) G:\Games\NBA 2K19\NBA2K19.exe  [Unsigned]
O4 - GS\Desktop [Ousmane]: Nox.lnk . (.Duodian Technology Co. Ltd. - NoxPlayer.) D:\Program Files\Nox\bin\Nox.exe  =>.Nox Limited®
O4 - GS\Desktop [Ousmane]: OpenIV.lnk . (.New Technology Studio - OpenIV.) C:\Users\couli\AppData\Local\New Technology Studio\Apps\OpenIV\OpenIV.exe
O4 - GS\Desktop [Ousmane]: Outil de téléchargement USB DVD Windows 7.lnk . (.Microsoft Corporation - Microsoft Store ISO Backup Tool.) C:\Users\couli\
O4 - GS\Desktop [Ousmane]: PC Building Simulator Razer Workshop.lnk . (...) D:\Games\PC Building Simulator Razer Workshop\PCBS.exe  [Unsigned]
O4 - GS\Desktop [Ousmane]: PhotoFiltre 7.lnk . (.PhotoFiltre - PhotoFiltre 7.) C:\Program Files (x86)\PhotoFiltre 7\PhotoFiltre7.exe  [Unsigned]  =>
O4 - GS\Desktop [Ousmane]: PhotoFiltre.lnk . (.Antonio Da Cruz - PhotoFiltre.) C:\Program Files (x86)\PhotoFiltre\PhotoFiltre.exe  [Unsigned]  =>.Ant
O4 - GS\Desktop [Ousmane]: Popcorn-Time.lnk . (.The NW.js Community - nwjs.) C:\Users\couli\AppData\Local\Popcorn-Time\Popcorn-Time.exe  [Unsigned]
O4 - GS\Desktop [Ousmane]: Prison Architect The Clink.lnk . (...) D:\Games\Prison Architect The Clink\Prison Architect.exe  [Unsigned]
O4 - GS\Desktop [Ousmane]: Programs - Raccourci.lnk . (...) D:\Téléchargerment New\Programs  [Unsigned]
O4 - GS\Desktop [Ousmane]: PureFarming.lnk . (...) D:\Pure.Farming.2018.v1.1.2\Pure.Farming.2018.v1.1.2\Pure.Farming.2018\PureFarming.exe  [Unsigned]
O4 - GS\Desktop [Ousmane]: Rockstar Games Launcher.lnk . (.Rockstar Games - Rockstar Games Launcher Patcher.) D:\Launcher\LauncherPatcher.exe  =>.Ro
O4 - GS\Desktop [Ousmane]: RVL Hacker.lnk . (.exosyphen studios - Hacker Evolution engine.) C:\Program Files (x86)\RVL Hacker\RVLHacker.exe  [Unsigne
O4 - GS\Desktop [Ousmane]: SimAirport.exe - Raccourci.lnk . (...) D:\Téléchargerment New\SimAirport.v02.07.2019\SimAirport.v02.07.2019\SimAirport.exe
O4 - GS\Desktop [Ousmane]: Spintires MudRunner American Wilds.lnk . (.Focus Home Interactive - MudRunner™.) G:\Games\Spintires MudRunner American Wild
O4 - GS\Desktop [Ousmane]: Start Tor Browser.lnk . (.Mozilla Corporation - Tor Browser.) C:\Users\couli\OneDrive\Bureau\Tor Browser\Browser\firefox.ex
O4 - GS\Desktop [Ousmane]: Sublime Text 3.lnk . (.Sublime HQ Pty Ltd - Sublime Text.) C:\Program Files\Sublime Text 3\sublime_text.exe  =>.Sublime H
```

```
O4 - GS\Desktop [Ousmane]: Subnautica.lnk . (...) D:\Games\Subnautica\Subnautica.exe -silent-crashes -vrmode none  [Unsigned]
O4 - GS\Desktop [Ousmane]: SurfOffline Professional - Raccourci.lnk . (...) C:\ProgramData\Bimesoft\SurfOffline Professional  [Unsigned]
O4 - GS\Desktop [Ousmane]: Sync.lnk . (...) C:\Users\couli\AppData\Local\Sync\Update.exe --processStart 'Sync.exe'  [Unsigned]
O4 - GS\Desktop [Ousmane]: TS4_x64.exe - Raccourci.lnk . (.Electronic Arts Inc. - The Sims™ 4.) I:\The Sims 4\Game\Bin\TS4_x64.exe  [Unsigned]  =>.El
O4 - GS\Desktop [Ousmane]: Twitch.lnk . (.Twitch Interactive, Inc. - Twitch.) C:\Users\couli\AppData\Roaming\Twitch\Bin\Twitch.exe  =>.Twitch Intera
O4 - GS\Desktop [Ousmane]: Two Point Hospital.lnk . (...) D:\SteamLibrary\Two Point Hospital\TPH.exe /run  [Unsigned]
O4 - GS\Desktop [Ousmane]: Uplay.lnk . (.Ubisoft - Uplay launcher.) C:\Program Files (x86)\Ubisoft\Ubisoft Game Launcher\Uplay.exe  =>.Ubisoft Enter
O4 - GS\Desktop [Ousmane]: userdata - Raccourci.lnk . (...) C:\Program Files (x86)\Steam\userdata  [Unsigned]
O4 - GS\Desktop [Ousmane]: WhatsApp.lnk . (.WhatsApp - WhatsApp.) C:\Users\couli\AppData\Local\WhatsApp\WhatsApp.exe  =>.WhatsApp, Inc®
O4 - GS\Desktop [Ousmane]: ZHPSuite.lnk . (.Nicolas Coolman - ZHPSuite.) C:\Users\couli\AppData\Roaming\ZHP\ZHPSuite.exe  =>.Nicolas Coolman
O4 - GS\Desktop [Ousmane]: µTorrent.lnk . (.BitTorrent Inc. - µTorrent.) C:\Users\couli\AppData\Roaming\uTorrent\uTorrent.exe  =>BitTorrent (P2P)
O4 - GS\Quicklaunch [Ousmane]: AirDroid.lnk . (.Sand Studio - AirDroid 3 Launcher.) C:\Program Files (x86)\AirDroid\Launcher.exe  {0DAE46486B3CF0B6DF
O4 - GS\Quicklaunch [Ousmane]: ApowerMirror.lnk . (.Apowersoft - ApowerMirror.) C:\Program Files (x86)\Apowersoft\ApowerMirror\ApowerMirror.exe  =>
O4 - GS\Quicklaunch [Ousmane]: CodeBlocks.lnk . (.Code::Blocks Team - Code::Blocks IDE.) C:\Program Files (x86)\CodeBlocks\codeblocks.exe  [Unsigned]
O4 - GS\Quicklaunch [Ousmane]: Free Flash eBook Maker .lnk . (.flipbuilder.com - .) C:\Program Files (x86)\Free Flash eBook Maker\flipchm.exe  [Unsig
O4 - GS\Quicklaunch [Ousmane]: Glary Utilities 5.lnk . (.Glarysoft Ltd - Glary Utilities 5.) C:\Program Files (x86)\Glary Utilities 5\Integrator.exe
O4 - GS\Quicklaunch [Ousmane]: Google Chrome.lnk . (.Google LLC - Accéder à Internet.) C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
O4 - GS\Quicklaunch [Ousmane]: Gyazo GIF.lnk . (.Nota Inc. - GyazoGIF.) C:\Program Files (x86)\Gyazo\GyazoGIF.exe  =>.Nota Inc.®
O4 - GS\Quicklaunch [Ousmane]: Gyazo Replay.lnk . (.Nota Inc. - GyazoReplay.) C:\Program Files (x86)\Gyazo\GyazoReplay.exe  =>.Nota Inc.®
O4 - GS\Quicklaunch [Ousmane]: Gyazo.lnk . (.Nota Inc. - Gyazo: Screen Uploader.) C:\Program Files (x86)\Gyazo\Gyazowin.exe  =>.Nota Inc.®
O4 - GS\Quicklaunch [Ousmane]: Microsoft Edge.lnk . (.Microsoft Corporation - Microsoft Edge.) C:\Program Files (x86)\Microsoft\Edge\Application\msedg
O4 - GS\Quicklaunch [Ousmane]: Navigateur Opera.lnk . (.Opera Software - Opera Internet Browser.) C:\Users\couli\AppData\Local\Programs\Opera\launcher
O4 - GS\Quicklaunch [Ousmane]: Oracle VM VirtualBox.lnk . (.Oracle Corporation - Oracle VM VirtualBox.) C:\Program Files (x86)\Oracle\VirtualBox\Virtu
O4 - GS\Quicklaunch [Ousmane]: Smart Switch.lnk . (.Samsung - Smart Switch PC.) C:\Program Files (x86)\Samsung\Smart Switch PC\SmartSwitchPC.exe  =>
O4 - GS\Quicklaunch [Ousmane]: SurfOffline Professional 2.lnk . (.Bimesoft - SurfOffline.) C:\Program Files (x86)\SurfOffline Professional 2\SO_PRO.ex
O4 - GS\Quicklaunch [Ousmane]: UniConverter.lnk . (.Wondershare - UniConverter.) C:\Program Files (x86)\Wondershare\Video Converter Ultimate\VideoConv
O4 - GS\Quicklaunch [Ousmane]: µTorrent.lnk . (.BitTorrent Inc. - µTorrent.) C:\Users\couli\AppData\Roaming\uTorrent\uTorrent.exe  =>BitTorrent (P2P
O4 - GS\sendTo [Ousmane]: Destinataire de télécopie.lnk . (.Microsoft Corporation - Microsoft Windows Fax and Scan.) C:\Windows\System32\WFS.exe /Send
O4 - GS\sendTo [Ousmane]: Fax Recipient.lnk . (.Microsoft Corporation - Microsoft Windows Fax and Scan.) C:\WINDOWS\system32\WFS.exe /SendTo  =>.Micr
O4 - GS\sendTo [Ousmane]: TeamViewer.lnk . (.TeamViewer GmbH - TeamViewer 14.) C:\Program Files (x86)\TeamViewer\TeamViewer.exe --sendto  =>.TeamView
O4 - GS\sendTo [Ousmane]: Transfert de fichiers Bluetooth.LNK . (.Microsoft Corporation - Transfère les fichiers entre l.) C:\Windows\System32\fsquirt
O4 - GS\TaskBar [Ousmane]: AirDroid.lnk . (.Sand Studio - AirDroid 3.) C:\Program Files (x86)\AirDroid\AirDroid.exe  {0DAE46486B3CF0B6DF5F76680285EB2
O4 - GS\TaskBar [Ousmane]: Discord.lnk . (.GitHub - Update.) C:\Users\couli\AppData\Local\Discord\Update.exe --processStart Discord.exe  =>.Discord I
O4 - GS\TaskBar [Ousmane]: Dropbox 25 GB.lnk . (.Dropbox, Inc. - Dropbox.) C:\Program Files (x86)\Dropbox\Client\Dropbox.exe /home  =>.Dropbox, Inc®
O4 - GS\TaskBar [Ousmane]: EpicGamesLauncher.lnk . (.Epic Games, Inc. - EpicGamesLauncher.) C:\Program Files (x86)\Epic Games\Launcher\Portal\Binaries
O4 - GS\TaskBar [Ousmane]: Firefox Developer Edition.lnk . (.Mozilla Corporation - Firefox Developer Edition.) C:\Program Files\Firefox Developer Edit
O4 - GS\TaskBar [Ousmane]: Firefox.lnk . (.Mozilla Corporation - Firefox.) C:\Program Files\Mozilla Firefox\firefox.exe  =>.Mozilla Corporation®
O4 - GS\TaskBar [Ousmane]: Microsoft Edge.lnk . (.Microsoft Corporation - Microsoft Edge.) C:\Program Files (x86)\Microsoft\Edge\Application\msedge.ex
O4 - GS\TaskBar [Ousmane]: Molotov.lnk . (.GitHub - Update.) C:\Users\couli\AppData\Local\Molotov\Update.exe --processStart 'Molotov.exe'  [Unsigned]
O4 - GS\TaskBar [Ousmane]: Navigateur Opera.lnk . (.Opera Software - Opera Internet Browser.) C:\Users\couli\AppData\Local\Programs\Opera\launcher.exe
O4 - GS\TaskBar [Ousmane]: OBS Studio (64bit).lnk . (...) C:\Program Files\obs-studio\bin\64bit\obs64.exe  =>.Hugh Bailey®
O4 - GS\TaskBar [Ousmane]: Origin.lnk . (.Electronic Arts - Origin.) C:\Program Files (x86)\Origin\Origin.exe  =>.Electronic Arts, Inc.®
O4 - GS\TaskBar [Ousmane]: Start Tor Browser.lnk . (.Mozilla Corporation - Tor Browser.) C:\Users\couli\OneDrive\Bureau\Tor Browser\Browser\firefox.ex
O4 - GS\TaskBar [Ousmane]: Steam Client Bootstrapper.lnk . (.Valve Corporation - Steam Client Bootstrapper.) C:\Program Files (x86)\Steam\Steam.exe
O4 - GS\TaskBar [Ousmane]: Streamlabs OBS.lnk . (.General Workings, Inc. - Streamlabs streaming software.) C:\Program Files (x86)\Streamlabs OBS\Strea
O4 - GS\TaskBar [Ousmane]: TeamSpeak 3 Client.lnk . (.TeamSpeak Systems GmbH - TeamSpeak 3 Client.) C:\Program Files\TeamSpeak 3 Client\ts3client_win6
O4 - GS\TaskBar [Ousmane]: Twitch.lnk . (.Twitch Interactive, Inc. - Twitch.) C:\Users\couli\AppData\Roaming\Twitch\Bin\Twitch.exe  =>.Twitch Intera
O4 - GS\TaskBar [Ousmane]: Uplay launcher.lnk . (.Ubisoft - Uplay launcher.) C:\Program Files (x86)\Ubisoft\Ubisoft Game Launcher\upc.exe  =>.Ubisof
O4 - GS\TaskBar [Ousmane]: WhatsApp.lnk . (.WhatsApp - WhatsApp.) C:\Users\couli\AppData\Local\WhatsApp\WhatsApp.exe  =>.WhatsApp, Inc®
O4 - GS\TaskBar [Ousmane]: Wondershare Filmora9.lnk . (.Wondershare - Wondershare Filmora9.) C:\Program Files\Wondershare\Wondershare Filmora (FR)\Wor
O4 - GS\Startup [Ousmane]: DS4Windows.lnk . (.Scarlet.Crush Productions 2012, 2013; InhexSTER, Hect - DS4Windows.) C:\Users\couli\OneDrive\Bureau\DS4W
O4 - GS\Startup [Ousmane]: Twitch.lnk . (.Twitch Interactive, Inc. - Twitch.) C:\Users\couli\AppData\Roaming\Twitch\Bin\Twitch.exe /startup  =>.Twitc
O4 - GS\Programs [Ousmane]: FiveM Singleplayer.lnk . (.cfx-collective - FiveM.) C:\Users\couli\AppData\Local\FiveM\FiveM.exe -sp  [Unsigned]  =>.cfx-c
O4 - GS\Programs [Ousmane]: FiveM.lnk . (.cfx-collective - FiveM.) C:\Users\couli\AppData\Local\FiveM\FiveM.exe  [Unsigned]  =>.cfx-collective
O4 - GS\Programs [Ousmane]: Fonts Ninja.lnk . (.Fonts Ninja - Fonts Ninja.) C:\Users\couli\AppData\Local\Programs\FontsNinja\Fonts Ninja.exe  {00ED64
O4 - GS\Programs [Ousmane]: Navigateur Opera.lnk . (.Opera Software - Opera Internet Browser.) C:\Users\couli\AppData\Local\Programs\Opera\launcher.ex
O4 - GS\Programs [Ousmane]: OneDrive (1).lnk . (.Microsoft Corporation - Microsoft OneDrive.) C:\Users\couli\AppData\Local\Microsoft\OneDrive\OneDrive
O4 - GS\Programs [Ousmane]: OneDrive.lnk . (.Microsoft Corporation - Microsoft OneDrive.) C:\Users\couli\AppData\Local\Microsoft\OneDrive\OneDrive.exe
O4 - GS\Programs [Ousmane]: Start Tor Browser.lnk . (.Mozilla Corporation - Tor Browser.) C:\Users\couli\OneDrive\Bureau\Tor Browser\Browser\firefox.e
O4 - GS\Programs [Ousmane]: Twitch.lnk . (.Twitch Interactive, Inc. - Twitch.) C:\Users\couli\AppData\Roaming\Twitch\Bin\Twitch.exe  =>.Twitch Inter
O4 - GS\CommonDesktop [Public]: Acrobat Reader DC.lnk . (.Adobe Systems Incorporated - Adobe Acrobat Reader DC.) C:\Program Files (x86)\Adobe\Acrobat
O4 - GS\CommonDesktop [Public]: AirDroid.lnk . (.Sand Studio - AirDroid 3.) C:\Program Files (x86)\AirDroid\AirDroid.exe  {0DAE46486B3CF0B6DF5F766802
O4 - GS\CommonDesktop [Public]: Amazing Audio Player.lnk . (...) C:\Program Files (x86)\Amazing Audio Player\amazingaudioplayer.exe  =>.Magic Hills
O4 - GS\CommonDesktop [Public]: AOMEI Backupper Standard.lnk . (.AOMEI Tech Co., Ltd. - AOMEI Backupper.) C:\Program Files (x86)\AOMEI Backupper\Backu
O4 - GS\CommonDesktop [Public]: APK Easy Tool.lnk . (...) C:\WINDOWS\Installer\{E25D8561-5A50-4363-B8D4-90627F19ABDB}\_0B86FA3996571F8BDA6081.exe  [U
O4 - GS\CommonDesktop [Public]: APK Editor Studio.lnk . (.Alexander Gorishnyak - APK Editor Studio v1.4.0.) C:\Program Files (x86)\APK Editor Studio\a
O4 - GS\CommonDesktop [Public]: ApowerCompress.lnk . (.Apowersoft - ApowerCompress.) C:\Program Files (x86)\Apowersoft\ApowerCompress\ApowerCompress.e
O4 - GS\CommonDesktop [Public]: ApowerMirror.lnk . (.Apowersoft - ApowerMirror.) C:\Program Files (x86)\Apowersoft\ApowerMirror\ApowerMirror.exe  =>
O4 - GS\CommonDesktop [Public]: ArmA3Sync.lnk . (...) C:\Program Files (x86)\ArmA3Sync\ArmA3Sync.exe  [Unsigned]
O4 - GS\CommonDesktop [Public]: Avast Antivirus Gratuit.lnk . (.AVAST Software - .) C:\Program Files (x86)\AVAST Software\Avast\AvastUI.exe  [Unsigne
O4 - GS\CommonDesktop [Public]: Avast SecureLine VPN.lnk . (.AVAST Software - .) C:\Program Files (x86)\AVAST Software\SecureLine VPN\Vpn.exe  [Unsig
O4 - GS\CommonDesktop [Public]: Battle.net.lnk . (.Blizzard Entertainment - Blizzard Battle.net App Launcher.) C:\Program Files (x86)\Battle.net\Battl
O4 - GS\CommonDesktop [Public]: Binary Viewer.lnk . (.ProXoft L.L.C. - Binary Viewer.) C:\Program Files (x86)\ProXoft\Binary Viewer\Binary Viewer.exe
O4 - GS\CommonDesktop [Public]: BlueGriffon.lnk . (.Mozilla Foundation - .) C:\Program Files\BlueGriffon\bluegriffon.exe  [Unsigned]  =>.Mozilla Four
O4 - GS\CommonDesktop [Public]: CCleaner.lnk . (.Piriform Software Ltd - CCleaner.) C:\Program Files\CCleaner\CCleaner64.exe  =>.Piriform Software L
O4 - GS\CommonDesktop [Public]: Cyotek WebCopy.lnk . (.Cyotek Ltd - Cyotek WebCopy Client.) C:\Program Files (x86)\Cyotek\WebCopy\cyowcopy.exe  {290C
O4 - GS\CommonDesktop [Public]: DriversCloud.com - Démarrer la détection.lnk . (.CybelSoft - .) C:\Program Files (x86)\DriversCloud.com\DriversCloud.e
O4 - GS\CommonDesktop [Public]: Epic Games Launcher.lnk . (.Epic Games, Inc. - UnrealEngineLauncherProxy.) C:\Program Files (x86)\Epic Games\Launcher\
O4 - GS\CommonDesktop [Public]: FIFA 20.lnk . (.Electronic Arts - FIFA 20.) D:\Origin\FIFA 20\FIFA20.exe  =>.Electronic Arts, Inc.®
O4 - GS\CommonDesktop [Public]: File Magic.lnk . (.Solvusoft Corporation - FileMagic.) C:\Program Files\File Magic\FileMagic.exe  =>SUP.Optional.Sol
O4 - GS\CommonDesktop [Public]: FileZilla Client.lnk . (.FileZilla Project - FileZilla FTP Client.) C:\Program Files\FileZilla FTP Client\filezilla.ex
O4 - GS\CommonDesktop [Public]: Firefox Developer Edition.lnk . (.Mozilla Corporation - Firefox Developer Edition.) C:\Program Files\Firefox Developer
O4 - GS\CommonDesktop [Public]: Firefox.lnk . (.Mozilla Corporation - Firefox.) C:\Program Files\Mozilla Firefox\firefox.exe  =>.Mozilla Corporation
O4 - GS\CommonDesktop [Public]: GeForce Experience.lnk . (.NVIDIA Corporation - .) C:\Program Files (x86)\NVIDIA Corporation\NVIDIA GeForce Experience
O4 - GS\CommonDesktop [Public]: Glary Utilities 5.lnk . (.Glarysoft Ltd - Glary Utilities 5.) C:\Program Files (x86)\Glary Utilities 5\Integrator.exe
O4 - GS\CommonDesktop [Public]: Google Chrome.lnk . (.Google LLC - Accéder à Internet.) C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
O4 - GS\CommonDesktop [Public]: Gyazo GIF.lnk . (.Nota Inc. - GyazoGIF.) C:\Program Files (x86)\Gyazo\GyazoGIF.exe  =>.Nota Inc.®
O4 - GS\CommonDesktop [Public]: Gyazo Replay.lnk . (.Nota Inc. - GyazoReplay.) C:\Program Files (x86)\Gyazo\GyazoReplay.exe  =>.Nota Inc.®
O4 - GS\CommonDesktop [Public]: Gyazo.lnk . (.Nota Inc. - Gyazo: Screen Uploader.) C:\Program Files (x86)\Gyazo\Gyazowin.exe  =>.Nota Inc.®
O4 - GS\CommonDesktop [Public]: IntelliJ IDEA Community Edition 2018.3.3 x64.lnk . (.JetBrains s.r.o. - IntelliJ IDEA.) C:\Program Files\JetBrains\Int
O4 - GS\CommonDesktop [Public]: ISO Workshop.lnk . (.Glorylogic - ISO Workshop.) C:\Program Files (x86)\Glorylogic\ISO Workshop\ISOWorkshop.exe  [Uns
O4 - GS\CommonDesktop [Public]: Jarvee.lnk . (.Jarvee - Jarvee.) C:\Users\couli\AppData\Roaming\Jarvee\Jarvee.exe  {0B414C00BF45EDB4865CE431D4954843}
O4 - GS\CommonDesktop [Public]: Jumpstart.lnk . (.Atheros Communications, Inc. - Jumpstart for Wireless.) C:\Program Files (x86)\Jumpstart\jswscapp.ex
O4 - GS\CommonDesktop [Public]: Lecture à distance PS4.lnk . (.Sony Interactive Entertainment Inc. - PS4 Remote Play.) C:\Program Files (x86)\Sony\PS4
O4 - GS\CommonDesktop [Public]: Logitech G HUB.lnk . (.Logitech, Inc. - .) C:\Program Files (x86)\LGHUB\lghub.exe  [Unsigned]  =>.Logitech, Inc.
O4 - GS\CommonDesktop [Public]: MEGAsync.lnk . (.Mega Limited - MEGAsync.) C:\ProgramData\MEGAsync\MEGAsync.exe  =>.Mega Limited®
O4 - GS\CommonDesktop [Public]: Microsoft Edge.lnk . (.Microsoft Corporation - Microsoft Edge.) C:\Program Files (x86)\Microsoft\Edge\Application\msed
O4 - GS\CommonDesktop [Public]: Minimal ADB and Fastboot.lnk . (...) C:\Program Files (x86)\Minimal ADB and Fastboot\cmd-here.exe  [Unsigned]
O4 - GS\CommonDesktop [Public]: MyEpson Portal.lnk . (.Seiko Epson Corporation - MyEpson Portal.) C:\Program Files (x86)\EPSON\MyEpson Portal\mep.exe
O4 - GS\CommonDesktop [Public]: Notepad++.lnk . (.Don HO don.h@free.fr - Notepad++ : a free (GNU) source code editor.) C:\Program Files (x86)\Notepad+
O4 - GS\CommonDesktop [Public]: OBS Studio.lnk . (...) C:\Program Files\obs-studio\bin\64bit\obs64.exe  =>.Hugh Bailey®
O4 - GS\CommonDesktop [Public]: Oracle VM VirtualBox.lnk . (.Oracle Corporation - Oracle VM VirtualBox.) C:\Program Files (x86)\Oracle\VirtualBox\Virt
O4 - GS\CommonDesktop [Public]: Origin.lnk . (.Electronic Arts - Origin.) C:\Program Files (x86)\Origin\Origin.exe  =>.Electronic Arts, Inc.®
O4 - GS\CommonDesktop [Public]: paint.net.lnk . (.dotPDN LLC - Créer, modifier, numériser et .) C:\Program Files (x86)\paint.net\PaintDotNet.exe  [Un
```

```
O4 - GS\CommonDesktop [Public]: PBOManager v.1.4 beta.lnk . (...) C:\windows\Installer\{127B5371-1802-4EDD-A25A-A43BF761D383}\_4722DB8B0F9A73756EFD05
O4 - GS\CommonDesktop [Public]: PowerISO.lnk . (.Power Software Ltd - PowerISO.) C:\Program Files\PowerISO\PowerISO.exe   {19EA4DAF089570861408E9F05EF
O4 - GS\CommonDesktop [Public]: Project Hospital.lnk . (...) G:\Project Hospital\ProjectHospital.exe   [Unsigned]
O4 - GS\CommonDesktop [Public]: Quran Explorer Desktop.lnk . (...) C:\WINDOWS\Installer\{34A9F183-1011-4845-9826-FBAA53DA59DF}\_A681DE592082BF1943574E
O4 - GS\CommonDesktop [Public]: Quranflash Desktop.lnk . (...) C:\Program Files (x86)\Quranflash Desktop\Quranflash Desktop.exe   [Unsigned]
O4 - GS\CommonDesktop [Public]: SideSync.lnk . (.Copyright(c) 2013 Samsung Electronics Co., Ltd. All r - SideSync 4.0.) C:\Program Files (x86)\Samsung
O4 - GS\CommonDesktop [Public]: Smart Switch.lnk . (.Samsung - Smart Switch PC.) C:\Program Files (x86)\Samsung\Smart Switch PC\SmartSwitchPC.exe    =
O4 - GS\CommonDesktop [Public]: Snaz.lnk . (.JimsApps - Snaz.) C:\Snaz\Snaz.exe   [Unsigned]  =>.JimsApps
O4 - GS\CommonDesktop [Public]: Speccy.lnk . (.Piriform Ltd - Speccy.) C:\Program Files\Speccy\Speccy64.exe    =>.Piriform Ltd®
O4 - GS\CommonDesktop [Public]: Steam.lnk . (.Valve Corporation - Steam Client Bootstrapper.) C:\Program Files (x86)\Steam\Steam.exe    =>.Valve®
O4 - GS\CommonDesktop [Public]: Streamlabs OBS.lnk . (.General Workings, Inc. - Streamlabs OBS.) C:\Program Files\Streamlabs OBS\Streamlabs OBS.exe
O4 - GS\CommonDesktop [Public]: SurfOffline Professional 2.lnk . (.Bimesoft - SurfOffline.) C:\Program Files (x86)\SurfOffline Professional 2\SO_PRO.e
O4 - GS\CommonDesktop [Public]: TeamSpeak 3 Client.lnk . (.TeamSpeak Systems GmbH - TeamSpeak 3 Client.) C:\Program Files\TeamSpeak 3 Client\ts3client
O4 - GS\CommonDesktop [Public]: TeamViewer 14.lnk . (.TeamViewer GmbH - TeamViewer 14.) C:\Program Files (x86)\TeamViewer\TeamViewer.exe    =>.TeamVie
O4 - GS\CommonDesktop [Public]: TerannForLife Launcher.lnk . (.Common-Apps - Uni-Launcher.) C:\Program Files\TerannForLife Launcher\Uni-Launcher\Uni-L
O4 - GS\CommonDesktop [Public]: The Sims 4.lnk . (.Electronic Arts Inc. - The Sims™ 4.) I:\The Sims 4\Game\Bin\TS4_x64.exe   [Unsigned]  =>.Electronic
O4 - GS\CommonDesktop [Public]: TruckersMP.lnk . (.Truckersmp.com - TruckersMP Launcher.) D:\TruckersMP Launcher\Launcher.exe   [Unsigned]  =>.Trucker
O4 - GS\CommonDesktop [Public]: VLC media player.lnk . (.VideoLAN - VLC media player.) C:\Program Files\VideoLAN\VLC\vlc.exe    =>.VideoLAN®
O4 - GS\CommonDesktop [Public]: VMware Workstation Pro.lnk . (.VMware, Inc. - VMware Workstation.) C:\Program Files (x86)\VMware\VMware Workstation\vm
O4 - GS\CommonDesktop [Public]: Wampserver64.lnk . (.Private - AeTrayMenu.) G:\wamp64\wampmanager.exe   [Unsigned]
O4 - GS\CommonDesktop [Public]: WebCopier.lnk . (.MaximumSoft Corp. - WebCopier website download tool.) C:\Program Files (x86)\WebCopier\WebCopier.exe
O4 - GS\CommonDesktop [Public]: Website Ripper Copier.lnk . (.Tensons Corporation - Website Ripper Copier.) C:\Program Files\Tensons\Website Ripper Co
O4 - GS\CommonDesktop [Public]: Win32DiskImager.lnk . (.Windows ImageWriter Team - DiskImager.) C:\Program Files (x86)\ImageWriter\Win32DiskImager.exe
O4 - GS\CommonDesktop [Public]: Wondershare Filmora9.lnk . (.Wondershare - Wondershare Filmora9.) C:\Program Files\Wondershare\Wondershare Filmora (FF
O4 - GS\CommonDesktop [Public]: Wondershare UniConverter.lnk . (.Wondershare - UniConverter.) C:\Program Files (x86)\Wondershare\Video Converter Ultim
O4 - GS\Programs [Public]: FiveM Singleplayer.lnk . (.cfx-collective - FiveM.) C:\Users\couli\AppData\Local\FiveM\FiveM.exe -sp  [Unsigned]  =>.cfx-co
O4 - GS\Programs [Public]: FiveM.lnk . (.cfx-collective - FiveM.) C:\Users\couli\AppData\Local\FiveM\FiveM.exe   [Unsigned]  =>.cfx-collective
O4 - GS\Programs [Public]: Fonts Ninja.lnk . (.Fonts Ninja - Fonts Ninja.) C:\Users\couli\AppData\Local\Programs\FontsNinja\Fonts Ninja.exe   {00ED647
O4 - GS\Programs [Public]: Navigateur Opera.lnk . (.Opera Software - Opera Internet Browser.) C:\Users\couli\AppData\Local\Programs\Opera\launcher.exe
O4 - GS\Programs [Public]: OneDrive (1).lnk . (.Microsoft Corporation - Microsoft OneDrive.) C:\Users\couli\AppData\Local\Microsoft\OneDrive\OneDrive
O4 - GS\Programs [Public]: OneDrive.lnk . (.Microsoft Corporation - Microsoft OneDrive.) C:\Users\couli\AppData\Local\Microsoft\OneDrive\OneDrive.exe
O4 - GS\Programs [Public]: Start Tor Browser.lnk . (.Mozilla Corporation - Tor Browser.) C:\Users\couli\OneDrive\Bureau\Tor Browser\Browser\firefox.ex
O4 - GS\Programs [Public]: Twitch.lnk . (.Twitch Interactive, Inc. - Twitch.) C:\Users\couli\AppData\Roaming\Twitch\Bin\Twitch.exe    =>.Twitch Intera
O4 - GS\Accessories [Public]: Internet Explorer.lnk . (.Microsoft Corporation - Internet Explorer.) C:\Program Files (x86)\Internet Explorer\iexplore
O4 - GS\Startup [Public]: Avast SecureLine VPN.lnk . (.AVAST Software - .) C:\Program Files (x86)\AVAST Software\SecureLine VPN\Vpn.exe /nogui  [Unsig
O4 - GS\Accessories [Public]: Math Input Panel.lnk . (.Microsoft Corporation - .) C:\Program Files (x86)\Common Files\Microsoft Shared\Ink\mip.exe
O4 - GS\Accessories [Public]: Notepad.lnk . (.Microsoft Corporation - Bloc-notes.) C:\WINDOWS\system32\notepad.exe    =>.Microsoft Corporation
O4 - GS\Accessories [Public]: Paint.lnk . (.Microsoft Corporation - Paint.) C:\WINDOWS\system32\mspaint.exe    =>.Microsoft Corporation
O4 - GS\Accessories [Public]: Quick Assist.lnk . (.Microsoft Corporation - Quick Assist.) C:\WINDOWS\system32\quickassist.exe    =>.Microsoft Corporat
O4 - GS\Accessories [Public]: Remote Desktop Connection.lnk . (.Microsoft Corporation - Connexion Bureau à distance.) C:\WINDOWS\system32\mstsc.exe
O4 - GS\Accessories [Public]: Snipping Tool.lnk . (.Microsoft Corporation - Outil Capture d'écran.) C:\WINDOWS\system32\SnippingTool.exe    =>.Microsc
O4 - GS\Accessories [Public]: Steps Recorder.lnk . (.Microsoft Corporation - Enregistreur d'actions.) C:\WINDOWS\system32\psr.exe    =>.Microsoft Corp
O4 - GS\Accessories [Public]: Windows Fax and Scan.lnk . (.Microsoft Corporation - Microsoft Windows Fax and Scan.) C:\WINDOWS\system32\WFS.exe    =>
O4 - GS\Accessories [Public]: Windows Media Player.lnk . (.Microsoft Corporation - Lecteur Windows Media.) C:\Program Files (x86)\Windows Media Player
O4 - GS\Accessories [Public]: Wordpad.lnk . (.Microsoft Corporation - Application Windows Wordpad.) C:\Program Files (x86)\Windows NT\Accessories\word
O4 - GS\Accessories [Public]: XPS Viewer.lnk . (.Microsoft Corporation - Visionneuse XPS.) C:\WINDOWS\system32\xpsrchvw.exe    =>.Microsoft Corporatio
O4 - GS\SystemTools [Public]: Character Map.lnk . (.Microsoft Corporation - Table des caractères.) C:\WINDOWS\system32\charmap.exe    =>.Microsoft Cor
O4 - GS\ProgramsCommon [Public]: Acrobat Reader DC.lnk . (.Adobe Systems Incorporated - Adobe Acrobat Reader DC.) C:\Program Files (x86)\Adobe\Acrobat
O4 - GS\ProgramsCommon [Public]: Adobe Illustrator 2020.lnk . (.Adobe Inc. - Adobe Illustrator 2020.) D:\Adobe illustrator\Adobe Illustrator 2020\Supp
O4 - GS\ProgramsCommon [Public]: Adobe Lightroom Classic.lnk . (.Adobe Systems - Adobe Photoshop Lightroom Classic.) D:\Adobe Lightroom\Adobe Lightroo
O4 - GS\ProgramsCommon [Public]: Adobe Photoshop 2020.lnk . (.Adobe - Adobe Photoshop 2020.) D:\Photoshop 2020\Adobe Photoshop 2020\Photoshop.exe   [U
O4 - GS\ProgramsCommon [Public]: Adobe Premiere Pro 2020.lnk . (.Adobe - Adobe Premiere Pro 2020.) D:\Adobe Premier 2020\Adobe Premiere Pro 2020\Adobe
O4 - GS\ProgramsCommon [Public]: APK Easy Tool.lnk . (...) C:\WINDOWS\Installer\{E25D8561-5A50-4363-B8D4-90627F19ABDB}\_1D1FDED58255B22C865E81.exe
O4 - GS\ProgramsCommon [Public]: Assistant Mise à jour de Windows 10.lnk . (.Microsoft Corporation - Assistant Mise à jour de Windows 10.) C:\Windows1
O4 - GS\ProgramsCommon [Public]: Avast Antivirus Gratuit.lnk . (.AVAST Software - .) C:\Program Files (x86)\AVAST Software\Avast\AvastUI.exe   [Unsign
O4 - GS\ProgramsCommon [Public]: Avast SecureLine VPN.lnk . (.AVAST Software - .) C:\Program Files (x86)\AVAST Software\SecureLine VPN\Vpn.exe   [Unsi
O4 - GS\ProgramsCommon [Public]: Brackets.lnk . (.brackets.io - Raccourci vers Brackets.) C:\Program Files (x86)\Brackets\Brackets.exe    =>.Adobe Inc
O4 - GS\ProgramsCommon [Public]: Epic Games Launcher.lnk . (.Epic Games, Inc. - UnrealEngineLauncherProxy.) C:\Program Files (x86)\Epic Games\Launcher
O4 - GS\ProgramsCommon [Public]: Firefox Developer Edition.lnk . (.Mozilla Corporation - Firefox Developer Edition.) C:\Program Files\Firefox Develope
O4 - GS\ProgramsCommon [Public]: Firefox.lnk . (.Mozilla Corporation - Firefox.) C:\Program Files\Mozilla Firefox\firefox.exe    =>.Mozilla Corporatio
O4 - GS\ProgramsCommon [Public]: Glary Utilities 5.lnk . (.Glarysoft Ltd - Glary Utilities 5.) C:\Program Files (x86)\Glary Utilities 5\Integrator.exe
O4 - GS\ProgramsCommon [Public]: Google Chrome.lnk . (.Google LLC - Accéder à Internet.) C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
O4 - GS\ProgramsCommon [Public]: HP Audio Switch.lnk . (.HP Inc. - HPAudioSwitch.) C:\Program Files (x86)\HP\HPAudioSwitch\HPAudioSwitch.exe    =>.HP
O4 - GS\ProgramsCommon [Public]: Immersive Control Panel.lnk . (.Microsoft Corporation - Windows Control Panel.) C:\WINDOWS\System32\Control.exe    =>
O4 - GS\ProgramsCommon [Public]: Lecture à distance PS4.lnk . (.Sony Interactive Entertainment Inc. - PS4 Remote Play.) C:\Program Files (x86)\Sony\PS
O4 - GS\ProgramsCommon [Public]: Microsoft Edge.lnk . (.Microsoft Corporation - Microsoft Edge.) C:\Program Files (x86)\Microsoft\Edge\Application\mse
O4 - GS\ProgramsCommon [Public]: Notepad++.lnk . (.Don HO don.h@free.fr - Notepad++ : a free (GNU) source code editor.) C:\Program Files (x86)\Notepad
O4 - GS\ProgramsCommon [Public]: OMEN Audio Control.lnk . (.Realtek Semiconductor - OMEN Audio Control.) C:\Program Files (x86)\Realtek\Audio\HDA\RtkN
O4 - GS\ProgramsCommon [Public]: paint.net.lnk . (.dotPDN LLC - Créer, modifier, numériser et .) C:\Program Files (x86)\paint.net\PaintDotNet.exe   [U
O4 - GS\ProgramsCommon [Public]: Quran Explorer Desktop.lnk . (...) C:\WINDOWS\Installer\{34A9F183-1011-4845-9826-FBAA53DA59DF}\_58CB4F353BE349A23AAC1
O4 - GS\ProgramsCommon [Public]: Streamlabs OBS.lnk . (.General Workings, Inc. - Streamlabs OBS.) C:\Program Files\Streamlabs OBS\Streamlabs OBS.exe
O4 - GS\ProgramsCommon [Public]: TeamSpeak 3 Client.lnk . (.TeamSpeak Systems GmbH - TeamSpeak 3 Client.) C:\Program Files\TeamSpeak 3 Client\ts3clier
O4 - GS\ProgramsCommon [Public]: TeamViewer 14.lnk . (.TeamViewer GmbH - TeamViewer 14.) C:\Program Files (x86)\TeamViewer\TeamViewer.exe    =>.TeamVi
O4 - GS\ProgramsCommon [Public]: TerannForLife Launcher.lnk . (.Common-Apps - Uni-Launcher.) C:\Program Files\TerannForLife Launcher\Uni-Launcher\Uni-

---\ MODIFICATION DOMAINE/ADRESSES (DNS) (8) - 1s
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\..\{03d3df5e-2974-4002-a37c-69f709e775d5}: NameServer = 82.163.143.146,82.163.142.148  =>Adware.DNSUnlocker
O17 - HKLM\System\CCS\Services\Tcpip\..\{07ed73fd-c258-4761-bdef-a6b8acc2253b}: NameServer = 82.163.143.146,82.163.142.148  =>Adware.DNSUnlocker
O17 - HKLM\System\CCS\Services\Tcpip\..\{03d3df5e-2974-4002-a37c-69f709e775d5}: DhcpNameServer = 192.168.1.254  =>.Local IP Adress
O17 - HKLM\System\CCS\Services\Tcpip\..\{0f45889c-bf22-4acc-bcce-b01d3a667f92}: DhcpNameServer = 93.158.32.10 93.158.32.20  =>.France Paris Ibrowse Sa
O17 - HKLM\System\CCS\Services\Tcpip\..\{1f52e700-d9ce-4b59-99af-a9b895733b28}: DhcpNameServer = 192.168.1.1  =>.Local IP Adress
O17 - HKLM\System\CCS\Services\Tcpip\..\{03d3df5e-2974-4002-a37c-69f709e775d5}: DhcpDomain = lan  =>.Local Domain

---\ PROTOCOLE ADDITIONNEL (22) - 0s
O18 - Handler: about [64Bits] - {3050F406-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Visionneuse HTML Microsoft (R).) -- C:\Windows\Syst
O18 - Handler: cdl [64Bits] - {3dd53d40-7b8b-11D0-b013-00aa0059ce02} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\System32\
O18 - Handler: dvd [64Bits] - {12D51199-0DB5-46FE-A120-47A3D7D937CC} . (.Microsoft Corporation - Contrôle ActiveX pour le flux vidéo.) -- C:\Windows\S
O18 - Handler: file [64Bits] - {79eac9e7-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\System32
O18 - Handler: ftp [64Bits] - {79eac9e3-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\System32\
O18 - Handler: http [64Bits] - {79eac9e2-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\System32
O18 - Handler: https [64Bits] - {79eac9e5-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\System3
O18 - Handler: its [64Bits] - {9D148291-B9C8-11D0-A4CC-0000F80149F6} . (.Microsoft Corporation - Microsoft® InfoTech Storage System Library.) -- C:\Wi
O18 - Handler: javascript [64Bits] - {3050F3B2-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Visionneuse HTML Microsoft (R).) -- C:\Windows
O18 - Handler: local [64Bits] - {79eac9e7-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\System3
O18 - Handler: mailto [64Bits] - {3050f3DA-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Visionneuse HTML Microsoft (R).) -- C:\Windows\Sys
O18 - Handler: mhtml [64Bits] - {05300401-BCBC-11d0-85E3-00C04FD85AB4} . (.Microsoft Corporation - Microsoft Internet Messaging API Resources.) -- C:\
O18 - Handler: mk [64Bits] - {79eac9e6-baf9-11ce-8c82-00aa004ba90b} . (.Microsoft Corporation - Extensions OLE32 pour Win32.) -- C:\Windows\System32\u
O18 - Handler: ms-its [64Bits] - {9D148291-B9C8-11D0-A4CC-0000F80149F6} . (.Microsoft Corporation - Microsoft® InfoTech Storage System Library.) -- C
O18 - Handler: res [64Bits] - {3050F3BC-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Visionneuse HTML Microsoft (R).) -- C:\Windows\System
O18 - Handler: tbauth [64Bits] - {14654CA6-5711-491D-B89A-58E571679951} . (.Microsoft Corporation - TBAuth protocol handler.) -- C:\Windows\System32\t
O18 - Handler: tv [64Bits] - {CBD30858-AF45-11D2-B6D6-00C04FBBDE6E} . (.Microsoft Corporation - Contrôle ActiveX pour le flux vidéo.) -- C:\Windows\Sy
O18 - Handler: vbscript [64Bits] - {3050F3B2-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Visionneuse HTML Microsoft (R).) -- C:\Windows\S
```

```
O18 - Handler: windows.tbauth [64Bits] - {14654CA6-5711-491D-B89A-58E571679951} . (.Microsoft Corporation - TBAuth protocol handler.) -- C:\Windows\Sy
O18 - Filter: application/octet-stream [64Bits] - {1E66F26B-79EE-11D2-8710-00C04F79ED0D} . (.Microsoft Corporation - Microsoft .NET Runtime Execution
O18 - Filter: application/x-complus [64Bits] - {1E66F26B-79EE-11D2-8710-00C04F79ED0D} . (.Microsoft Corporation - Microsoft .NET Runtime Execution Eng
O18 - Filter: application/x-msdownload [64Bits] - {1E66F26B-79EE-11D2-8710-00C04F79ED0D} . (.Microsoft Corporation - Microsoft .NET Runtime Execution

---\ 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 C

---\ ÉNUMÈRE LES DONNÉES DE BOOTEXECUTE (1) - 0s
O34 - HKLM BootExecute: (icarus_rvrt.exe) (. - Avast Installer.) -- icarus_rvrt.exe

---\ CLÉ DE REGISTRE EXPLORER StartupApproved (72) - 1s
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:OneDriveSetup  =>.Microsoft Corporation
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:CCXProcess  =>.Legitimate
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:EpicGamesLauncher  =>.Epic Games
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:Gyazo
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:OneDrive  =>.Microsoft Corporation
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:Steam  =>.Valve
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:withSIX
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:EPLTarget\P0000000000000000
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:uTorrent
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:Web Companion  =>PUP.Optional.LavasoftWebCompanion
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:CCleaner Smart Cleaning  =>.Piriform Ltd
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:GUDelayStartup  =>.GlarySoft
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:IDMan  =>.Tonec Inc
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:AvastBrowserAutoLaunch_018BE0419A1FB51785C82A6408AC86F3  =>PUP.Optional
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:Parsec.App.0
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:Plex Media Server  =>.Plex Inc
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder]:DS4Windows.lnk
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder]:Twitch.lnk  =>.Twitch
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder]:MEGAsync.lnk  =>.MegaSystems
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder]:x.vbs
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder]:Jarvee.lnk
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:OneDriveSetup  =>.M
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:CCXProcess  =>.Legi
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:EpicGamesLauncher
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:Gyazo
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:OneDrive  =>.Micros
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:Steam  =>.Valve
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:withSIX
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:EPLTarget\P00000000
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:uTorrent
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:Web Companion  =>PU
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:CCleaner Smart Clea
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:GUDelayStartup  =>
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:IDMan  =>.Tonec Inc
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:AvastBrowserAutoLau
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:Parsec.App.0
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:Plex Media Server
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder]:DS4Windows
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder]:Twitch.lr
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder]:MEGAsync
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder]:x.vbs
[HKEY_USERS\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder]:Jarvee.lr
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:AdobeAAMUpdater-1.0  =>.Adobe Inc.
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:AvastUI.exe  =>.Avast Software s.r.o
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:SecurityHealth  =>.Microsoft Corporation
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:RUNFBI  =>.Hewlett-Packard
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:ShadowPlay  =>.nVidia Corporation
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:GameSessionsTray  =>.GameSessions
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:Launch LCore  =>.Logitech Inc.
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:WindowsDefender  =>.Microsoft Corporation
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run32]:Dropbox  =>.Dropbox Inc.
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run32]:RtlS5Wake  =>.Realtek Semiconductor Corp.
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run32]:HPMessageService  =>.Hewlett-Packard
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run32]:FileZilla Server Interface
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run32]:SunJavaUpdateSched  =>.Oracle
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run32]:jswtrayutil
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run32]:vmware-tray.exe  =>.VMware
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run32]:AvastUI.exe  =>.Avast Software s.r.o
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run32]:Wondershare Helper Compact.exe  =>.Wondershare
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder]:AnyDesk.lnk
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder]:Avast SecureLine VPN.lnk
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder]:Avast Cleanup Premium.lnk  =>.Avast Software s.r.o
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:DellMobileConnectWelcome
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:BtServer  =>.Realtek Semiconductor Corp.
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:BdVpnApp
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:CL-24-5D183DC4-75E3-4CA9-9427-C42C1E06C8E6
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:Wondershare Helper Compact.exe  =>.Wondershare
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run32]:Avira SystrayStartTrigger  =>.Avira Software
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run32]:Avira System Speedup User Starter  =>.Avira Software
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run32]:SwitchBoard  =>.Adobe Inc.
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run32]:AdobeCS6ServiceManager  =>.Adobe Inc.
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run32]:PWRISOVM.EXE

---\ COMPOSANTS ACTIVESETUP INSTALLÉS (ASIC) (7) - 1s
O40 - ASIC: Microsoft Windows Media Player [64Bits] - >{22d6f312-b0f6-11d0-94ab-0080c74c7e95} . (.Microsoft Corporation - Utilitaire d'installation du
O40 - ASIC: Microsoft Windows Media Player 12.0 [64Bits] - {22d6f312-b0f6-11d0-94ab-0080c74c7e95} . (.Microsoft Corporation - Windows Media Player Ext
O40 - ASIC: Microsoft Windows Media Player [64Bits] - {6BF52A52-394A-11d3-B153-00C04F79FAA6} . (.Microsoft Corporation - Utilitaire d'installation du
O40 - ASIC: Web Platform Customizations [64Bits] - {89820200-ECBD-11cf-8B85-00AA005B4383} . (.Microsoft Corporation - Utilitaire d'initialisation d'Ir
O40 - ASIC: (no name) [64Bits] - {89B4C1CD-B018-4511-B0A1-5476DBF70820} . (.Microsoft Corporation - Microsoft .NET IE SECURITY REGISTRATION.) -- C:\Wi
O40 - ASIC: Google Chrome [64Bits] - {8A69D345-D564-463c-AFF1-A69D9E530F96} . (.Google LLC - Google Chrome Installer.) -- C:\Program Files\Google\Chro
O40 - ASIC: Microsoft Edge [64Bits] - {9459C573-B17A-45AE-9F64-1857B5D58CEE} . (.Microsoft Corporation - Microsoft Edge Installer.) -- C:\Program File

---\ LOGICIELS INSTALLÉS (288) - 56s
O42 - Logiciel: µTorrent - (.BitTorrent Inc..) [HKCU][64Bits] -- uTorrent  =>BitTorrent (P2P)
O42 - Logiciel: 7-Zip 19.00 - (.Igor Pavlov.) [HKLM][64Bits] -- {23170F69-40C1-2701-1900-000001000000} [Unsigned]  =>.Igor Pavlov
O42 - Logiciel: 7-Zip 19.00 - (.Igor Pavlov.) [HKLM][64Bits] -- 7-Zip [Unsigned]  =>.Igor Pavlov
O42 - Logiciel: Adobe Acrobat Reader DC - Français - (.Adobe Systems Incorporated.) [HKLM][64Bits] -- {AC76BA86-7AD7-1036-7B44-AC0F074E4100} [Unsigned
O42 - Logiciel: Adobe Flash Player 32 NPAPI - (.Adobe.) [HKLM][64Bits] -- Adobe Flash Player NPAPI  =>.Adobe Inc.®
O42 - Logiciel: Adobe Illustrator 2020 - (.Adobe Systems Incorporated.) [HKLM][64Bits] -- ILST_24_0  =>.Adobe Inc.®
O42 - Logiciel: Adobe Lightroom Classic - (.Adobe Systems Incorporated.) [HKLM][64Bits] -- LTRM_9_0  =>.Adobe Inc.®
O42 - Logiciel: Adobe Photoshop 2020 - (.Adobe Systems Incorporated.) [HKLM][64Bits] -- PHSP_21_0_1  =>.Adobe Inc.®
O42 - Logiciel: Adobe Premiere Pro 2020 - (.Adobe Systems Incorporated.) [HKLM][64Bits] -- PPRO_14_0  =>.Adobe Inc.®
```

```
O42 - Logiciel: Adobe Refresh Manager - (.Adobe Systems Incorporated.) [HKLM][64Bits] -- {AC76BA86-0804-1033-1959-001824399311} [Unsigned]  =>.Adobe S
O42 - Logiciel: AirDroid 3.6.7.0 - (.Sand Studio.) [HKLM][64Bits] -- AirDroid [Unsigned]  =>.Sand Studio
O42 - Logiciel: Amazing Audio Player version 4.1 - (.Magic Hills Pty Ltd.) [HKLM][64Bits] -- {15D0E2B0-A58F-4BDE-B17D-C761E0174BE0}_is1 [Unsigned]  =>
O42 - Logiciel: Android Studio - (.Google LLC.) [HKLM][64Bits] -- Android Studio  =>.Google LLC®
O42 - Logiciel: Anno 2205 - (.Blue Byte.) [HKLM][64Bits] -- Steam App 375910  =>.Valve®
O42 - Logiciel: AOMEI Backupper Standard - (.AOMEI Technology Co., Ltd..) [HKLM][64Bits] -- {A83692F5-3E9B-4E95-9E7E-B5DF5536CE9D}_is1 [Unsigned]  =>
O42 - Logiciel: APK Easy Tool - (.evildog1.) [HKLM][64Bits] -- {E25D8561-5A50-4363-B8D4-90627F19ABDB} [Unsigned]
O42 - Logiciel: APK Editor Studio - (.Alexander Gorishnyak.) [HKLM][64Bits] -- {D866E8D4-0F6D-448D-BA11-D12A1813BB1C} [Unsigned]
O42 - Logiciel: ApowerCompress V1.1.3 - (.Apowersoft LIMITED.) [HKLM][64Bits] -- {10998dc6-e8e2-48ef-9378-0db3d4c7f32a}_is1 [Unsigned]  =>.APOWERSOFT
O42 - Logiciel: ApowerMirror V1.4.7.5 - (.APOWERSOFT LIMITED.) [HKLM][64Bits] -- {a9482532-9c34-478c-80c3-85bdccbb981f}_is1  =>.Apowersoft Ltd®
O42 - Logiciel: Arma 3 - (.Bohemia Interactive.) [HKLM][64Bits] -- Steam App 107410  =>.Valve®
O42 - Logiciel: Arma 3 Tools - (.Bohemia Interactive.) [HKLM][64Bits] -- Steam App 233800  =>.Valve®
O42 - Logiciel: ArmA3Sync 1.7 Update 4 - (.The [S.o.E] team.) [HKLM][64Bits] -- {F097E7D7-D093-4394-9EED-43AFCCD12B7A}_is1 [Unsigned]  =>.The [S.o.E]
O42 - Logiciel: Assistant Mise à jour de Windows 10 - (.Microsoft Corporation.) [HKLM][64Bits] -- {D5C69738-B486-402E-85AC-2456D98A64E4}  =>.Microsoft
O42 - Logiciel: Atom - (.GitHub Inc..) [HKCU][64Bits] -- atom [Unsigned]  =>.GitHub Inc.
O42 - Logiciel: Avast Antivirus Gratuit - (.Avast Software.) [HKLM][64Bits] -- Avast Antivirus  =>.Avast Software s.r.o.®
O42 - Logiciel: Avast SecureLine VPN - (.Avast Software.) [HKLM][64Bits] -- Avast SecureLine  =>.Avast Software s.r.o.®
O42 - Logiciel: Battle.net - (.Blizzard Entertainment.) [HKLM][64Bits] -- Battle.net  =>.Blizzard Entertainment, Inc.®
O42 - Logiciel: Binary Viewer 6.17.04.26 - (.ProXoft L.L.C..) [HKLM][64Bits] -- {A15E821D-0A75-4B45-BA20-481051C7F4E5}_is1 [Unsigned]
O42 - Logiciel: bl - (.Your Company Name.) [HKLM][64Bits] -- {2A075BB4-E976-4278-BF3F-E5C6945D84C0} [Unsigned]  =>.Your Company Name (Hidden)
O42 - Logiciel: BlueGriffon version 3.0.1 - (.Disruptive Innovations SAS.) [HKLM][64Bits] -- {A9015334-10BE-4D64-A776-203336EFE806}_is1 [Unsigned]  =>
O42 - Logiciel: BlueGriffon version 3.1 - (.Disruptive Innovations SAS.) [HKLM][64Bits] -- {A9015334-10BE-4D64-A776-203336EFE806}_is1 [Unsigned]  =>.D
O42 - Logiciel: Bonjour - (.Apple Inc..) [HKLM][64Bits] -- {56DDDFB8-7F79-4480-89D5-25E1F52AB28F} [Unsigned]  =>.Apple Inc.
O42 - Logiciel: Brackets - (.brackets.io.) [HKLM][64Bits] -- {74925DBB-B507-4A3B-A260-E19B82FFE7FB} [Unsigned]  =>.brackets.io
O42 - Logiciel: Cain & Abel 4.9.56 - (..) [HKLM][64Bits] -- Cain & Abel 4.9.56 [Unsigned]
O42 - Logiciel: Car Mechanic Simulator 2018 - (.Red Dot Games.) [HKLM][64Bits] -- Steam App 645630  =>.Valve®
O42 - Logiciel: CCleaner - (.Piriform.) [HKLM][64Bits] -- CCleaner  =>.Piriform Software Ltd®
O42 - Logiciel: Cheat Engine 6.8.3 - (.Cheat Engine.) [HKLM][64Bits] -- Cheat Engine 6.8.3_is1  =>.Cheat Engine®
O42 - Logiciel: Cheat Engine 7.0 - (.Cheat Engine.) [HKLM][64Bits] -- Cheat Engine 7.0_is1  =>.Cheat Engine®
O42 - Logiciel: Cities: Skylines - (.Colossal Order Ltd..) [HKLM][64Bits] -- Steam App 255710  =>.Valve®
O42 - Logiciel: CodeBlocks - (.The Code::Blocks Team.) [HKCU][64Bits] -- CodeBlocks [Unsigned]  =>.The Code::Blocks Team
O42 - Logiciel: CrystalDiskInfo 8.0.0 - (.Crystal Dew World.) [HKLM][64Bits] -- CrystalDiskInfo_is1 [Unsigned]  =>.Crystal Dew World
O42 - Logiciel: CrystalDiskMark 5.5.0 - (.Crystal Dew World.) [HKLM][64Bits] -- CrystalDiskMark5_is1 [Unsigned]  =>.Crystal Dew World
O42 - Logiciel: Cyotek WebCopy version 1.7.0.586 - (.Cyotek Ltd.) [HKLM][64Bits] -- {D5FAF1F8-C903-41b2-AC66-2682A02A78CB}_is1 [Unsigned]  =>.Cyotek L
O42 - Logiciel: Dell Mobile Connect Drivers - (.Screenovate Technologies Ltd..) [HKLM][64Bits] -- {1E754E2C-CF3B-42CB-B36D-D560CEA96149} [Unsigned]  =
O42 - Logiciel: Discord - (.Discord Inc..) [HKCU][64Bits] -- Discord  =>.Discord Inc.®
O42 - Logiciel: DriversCloud.com (64 bits) - (.Cybelsoft.) [HKLM][64Bits] -- {29DC4128-CF89-49D9-A524-B4430F036F14} [Unsigned]  =>.CybelSoft
O42 - Logiciel: Dropbox - (.Dropbox, Inc..) [HKLM][64Bits] -- Dropbox  =>.Dropbox, Inc®
O42 - Logiciel: Dropbox 25 GB - (.Dropbox, Inc..) [HKLM][64Bits] -- {84D8451D-2ED6-3A59-ABA5-2A447F7C6310} [Unsigned]  =>.Dropbox, Inc.
O42 - Logiciel: Dropbox Update Helper - (.Dropbox, Inc..) [HKLM][64Bits] -- {099218A5-A723-43DC-8DB5-6173656A1E94} [Unsigned]  =>.Dropbox, Inc. (Hidde
O42 - Logiciel: Dying Light - (.Techland.) [HKLM][64Bits] -- Steam App 239140  =>.Valve®
O42 - Logiciel: eFootball PES 2020 - (.Konami Digital Entertainment.) [HKLM][64Bits] -- Steam App 996470  =>.Valve®
O42 - Logiciel: Energy Star - (.HP Inc..) [HKLM][64Bits] -- {5CB22648-35F8-41BC-9C35-1E41FE6E12A5} [Unsigned]  =>.HP Inc.
O42 - Logiciel: Epic Games Launcher - (.Epic Games, Inc..) [HKLM][64Bits] -- {6653362F-9365-4A3C-9BF8-71494529DE06} [Unsigned]  =>.Epic Games, Inc.
O42 - Logiciel: EPSON WF-2510 Series Printer Uninstall - (.SEIKO EPSON Corporation.) [HKLM][64Bits] -- EPSON WF-2510 Series  =>.SEIKO EPSON Corporatio
O42 - Logiciel: Euro Truck Simulator 2 - (.SCS Software.) [HKLM][64Bits] -- Steam App 227300  =>.Valve®
O42 - Logiciel: Farm Manager 2018 - (.Cleversan Software.) [HKLM][64Bits] -- Steam App 495560  =>.Valve®
O42 - Logiciel: FastDataX 1.20 - (..) [HKLM][64Bits] -- FastDataX_is1 [Unsigned]  =>Adware.FastDataX
O42 - Logiciel: FIFA 20 - (.Electronic Arts.) [HKLM][64Bits] -- {9EC414D8-8C49-4310-BCC7-C72AB0776F4C}  =>.Electronic Arts, Inc.®
O42 - Logiciel: File Magic - (.Solvusoft Corporation.) [HKLM][64Bits] -- File Magic_is1  =>SUP.Optional.Solvusoft
O42 - Logiciel: FileZilla Client 3.46.3 - (.Tim Kosse.) [HKLM][64Bits] -- FileZilla Client [Unsigned]  =>.Tim Kosse
O42 - Logiciel: Firefox Developer Edition 84.0 (x64 en-US) - (.Mozilla.) [HKLM][64Bits] -- Firefox Developer Edition 84.0 (x64 en-US)  =>.Mozilla Corp
O42 - Logiciel: Fishing Sim World - (.HOODLUM.) [HKCU][64Bits] -- Fishing Sim World [Unsigned]  =>.Hoodlum
O42 - Logiciel: Fonts Ninja 0.1.33 - (.Fonts Ninja.) [HKCU][64Bits] -- {681da0eb-374d-5be1-94a8-a3b514928885} {00ED6477F116E0A1C95681D6E2609DA432}.
O42 - Logiciel: Free Flash eBook Maker - (.flippagemaker Solution.) [HKLM][64Bits] -- Free Flash eBook Maker_is1 [Unsigned]
O42 - Logiciel: Glary Utilities PRO 5.151 - (.Glarysoft Ltd.) [HKLM][64Bits] -- Glary Utilities 5  =>.Glarysoft LTD®
O42 - Logiciel: GNU Privacy Guard - (.Free Software Foundation.) [HKLM][64Bits] -- GnuPG [Unsigned]  =>.Free Software Foundation
O42 - Logiciel: Google Update Helper - (.Google LLC.) [HKLM][64Bits] -- {60EC980A-BDA2-4CB6-A427-B07A5498B4CA} [Unsigned]  =>.Google LLC (Hidden)
O42 - Logiciel: Google Chrome - (.Google LLC.) [HKLM][64Bits] -- Google Chrome  =>.Google LLC®
O42 - Logiciel: Gyazo 4.0.1.0 - (.Nota Inc..) [HKLM][64Bits] -- {6DB8C365-E719-4BA5-9594-10DFC244D3FD}_is1  =>.Nota Inc.®
O42 - Logiciel: Hacker Evolution IMMERSION Demo - (.exosyphen studios.) [HKLM][64Bits] -- Steam App 530090  =>.Valve®
O42 - Logiciel: Homeville version 1.5 - (..) [HKLM][64Bits] -- {E1527582-8509-4011-B922-29E3FB548882}_is1 [Unsigned]  =>Adware.DNSUnlocker
O42 - Logiciel: HP Audio Switch - (.HP Inc..) [HKLM][64Bits] -- {3A5141D4-47DB-4302-9B1C-272BE585BC8A} [Unsigned]  =>.HP Inc.
O42 - Logiciel: HP Connection Optimizer - (.HP Inc..) [HKLM][64Bits] -- {6468C4A5-E47E-405F-B675-A70A70983EA6}  =>.HP Inc.®
O42 - Logiciel: HP Customer Experience Enhancements - (.HP Inc..) [HKLM][64Bits] -- {9720A595-3D2D-440E-9523-0B6F970745DD} [Unsigned]  =>.HP Inc. (Hic
O42 - Logiciel: HP Documentation - (.HP Inc..) [HKLM][64Bits] -- HP_Documentation [Unsigned]  =>.HP Inc.
O42 - Logiciel: HP ePrint SW - (.HP Inc..) [HKLM][64Bits] -- {20185BDA-D396-4C93-95C7-ECD0FB397FF7} [Unsigned]  =>.HP Inc. (Hidden)
O42 - Logiciel: HP ePrint SW - (.HP Inc..) [HKLM][64Bits] -- {2889C948-F002-4992-815F-DBE0AFB5DC6E} [Unsigned]  =>.HP Inc. (Hidden)
O42 - Logiciel: HP ePrint SW - (.HP Inc..) [HKLM][64Bits] -- {54da9769-2364-4bd3-8139-6400500778b3}  =>.HP Inc.®
O42 - Logiciel: HP ePrint SW - (.HP Inc..) [HKLM][64Bits] -- {5BBB44D5-3CC0-4434-AA0C-5883B975E45E} [Unsigned]  =>.HP Inc. (Hidden)
O42 - Logiciel: HP ePrint SW - (.HP Inc..) [HKLM][64Bits] -- {6884D818-9E0E-4984-A6CA-B17757DCB8FA} [Unsigned]  =>.HP Inc. (Hidden)
O42 - Logiciel: HP ePrint SW - (.HP Inc..) [HKLM][64Bits] -- {98AA8BB0-0C0A-411A-BB43-1265CA769155} [Unsigned]  =>.HP Inc. (Hidden)
O42 - Logiciel: HP ePrint SW - (.HP Inc..) [HKLM][64Bits] -- {F7E8A494-97B6-4786-9E2C-A42A082483EB} [Unsigned]  =>.HP Inc. (Hidden)
O42 - Logiciel: HP JumpStart Apps - (.HP Inc..) [HKLM][64Bits] -- HP JumpStart Apps [Unsigned]  =>.HP Inc.
O42 - Logiciel: HP JumpStart Bridge - (.HP Inc..) [HKLM][64Bits] -- {1E7D6A6F-E28B-4057-BD4F-9989C1F5353D} [Unsigned]  =>.HP Inc.
O42 - Logiciel: HP JumpStart Launch - (.HP Inc..) [HKLM][64Bits] -- {4380D813-39E5-46FD-AC23-FC9A1A8B98AA} [Unsigned]  =>.HP Inc.
O42 - Logiciel: HP PC Hardware Diagnostics UEFI - (.HP.) [HKLM][64Bits] -- {924D3ABC-FC75-4042-9DDB-FB846A45848D} [Unsigned]  =>.HP (Hidden)
O42 - Logiciel: HP Recovery Manager - (.HP.) [HKLM][64Bits] -- {64BAA990-F1FC-4145-A7B1-E41FBBC9DA47} [Unsigned]  =>.HP (Hidden)
O42 - Logiciel: HP System Event Utility - (.HP Inc..) [HKLM][64Bits] -- {57058272-92B0-4EFA-8FDD-ED3E5D689D37} [Unsigned]  =>.HP Inc.
O42 - Logiciel: IIS 10.0 Express - (.Microsoft Corporation.) [HKLM][64Bits] -- {ACE1F06E-DB73-449B-ADEF-C94F4C8685A9} [Unsigned]  =>.Microsoft Corpora
O42 - Logiciel: Insurgency: Sandstorm - (.New World Interactive.) [HKLM][64Bits] -- Steam App 581320  =>.Valve®
O42 - Logiciel: Intel XTU SDK - (.HP Inc..) [HKLM][64Bits] -- {43A58350-CB99-4F4E-9BB6-F058D7B27985} [Unsigned]  =>.HP Inc. (Hidden)
O42 - Logiciel: Intel(R) Chipset Device Software - (.Intel Corporation.) [HKLM][64Bits] -- {6FAC699B-7992-4C62-9839-4783564CAEDD} [Unsigned]  =>.Intel
O42 - Logiciel: Intel(R) Management Engine Components - (.Intel Corporation.) [HKLM][64Bits] -- {1CEAC85D-2590-4760-800F-8DE5E91F3700}  =>.Intel(R) Em
O42 - Logiciel: Intel(R) Management Engine Components - (.Intel Corporation.) [HKLM][64Bits] -- {90291EBF-187A-4C7E-A9AD-DCCB6C946536} [Unsigned]  =>
O42 - Logiciel: Intel(R) Management Engine Components - (.Intel Corporation.) [HKLM][64Bits] -- {FBDA24D3-1A19-4D75-B3F1-F2A1FB6B61BF} [Unsigned]  =>
O42 - Logiciel: Intel(R) Management Engine Driver - (.Intel Corporation.) [HKLM][64Bits] -- {8DEA4234-C97D-41BE-B2BC-313A196BCD09} [Unsigned]  =>.Inte
O42 - Logiciel: Intel(R) ME UninstallLegacy - (.Intel Corporation.) [HKLM][64Bits] -- {E9B9A1A5-6398-4C99-8FDE-10794F6505C5} [Unsigned]  =>.Intel Corp
O42 - Logiciel: Intel(R) Rapid Storage Technology - (.Intel Corporation.) [HKLM][64Bits] -- {409CB30E-E457-4008-9B1A-ED1B9EA21140}  =>.Intel Corporati
O42 - Logiciel: Intel(R) Rapid Storage Technology - (.Intel Corporation.) [HKLM][64Bits] -- {A8E0E91F-CFE8-4C29-B4A9-723CAB834675} [Unsigned]  =>.Inte
O42 - Logiciel: Intel(R) Trusted Connect Service Client x64 - (.Intel Corporation.) [HKLM][64Bits] -- {C9552825-7BF2-4344-BA91-D3CD46F4C442} [Unsigned
O42 - Logiciel: Intel(R) Trusted Connect Service Client x86 - (.Intel Corporation.) [HKLM][64Bits] -- {C9552825-7BF2-4344-BA91-D3CD46F4C441} [Unsigned
O42 - Logiciel: Intel(R) Trusted Connect Services Client - (.Intel Corporation.) [HKLM][64Bits] -- {df682aff-4294-4ad1-aaa7-276931d5781f}  =>.Intel(R)
O42 - Logiciel: Intel® Hardware Accelerated Execution Manager - (.Intel Corporation.) [HKLM][64Bits] -- {7563302D-BD6B-4153-BA7D-3E3432E7C22D} [Unsign
O42 - Logiciel: Intel® Software Guard Extensions Platform Software - (.Intel Corporation.) [HKLM][64Bits] -- {2DF17C75-9627-4213-8612-17955E92F782} [U
O42 - Logiciel: IntelliJ IDEA Community Edition 2018.3.3 - (.JetBrains s.r.o..) [HKLM][64Bits] -- IntelliJ IDEA Community Edition 2018.3.3 [Unsigned]
O42 - Logiciel: ISO Workshop 8.3 - (.Glorylogic.) [HKLM][64Bits] -- ISO Workshop_is1 [Unsigned]  =>.Glorylogic
O42 - Logiciel: Jarvee - (.Jarvee.) [HKLM][64Bits] -- {9D1EA30B-26FB-4FD9-BE37-0927E7E6F315} [Unsigned] (Hidden)
O42 - Logiciel: Jarvee - (.Jarvee.) [HKLM][64Bits] -- Jarvee 14.1.7 [Unsigned]
O42 - Logiciel: Java 8 Update 181 - (.Oracle Corporation.) [HKLM][64Bits] -- {26A24AE4-039D-4CA4-87B4-2F32180181F0} [Unsigned]  =>.Oracle Corporation
O42 - Logiciel: Java 8 Update 201 - (.Oracle Corporation.) [HKLM][64Bits] -- {26A24AE4-039D-4CA4-87B4-2F32180201F0} [Unsigned]  =>.Oracle Corporation
O42 - Logiciel: Java 8 Update 211 - (.Oracle Corporation.) [HKLM][64Bits] -- {26A24AE4-039D-4CA4-87B4-2F32180211F0} [Unsigned]  =>.Oracle Corporation
O42 - Logiciel: Java 8 Update 211 (64-bit) - (.Oracle Corporation.) [HKLM][64Bits] -- {26A24AE4-039D-4CA4-87B4-2F64180211F0} [Unsigned]  =>.Oracle Cor
O42 - Logiciel: Java Auto Updater - (.Oracle Corporation.) [HKLM][64Bits] -- {4A03706F-666A-4037-7777-5F2748764D10} [Unsigned]  =>.Oracle Corporation
```

```
O42 - Logiciel: Java(TM) SE Development Kit 12.0.1 (64-bit) - (.Oracle Corporation.) [HKLM][64Bits] -- {0D60E96D-0B74-55A5-ACA5-0F6786FDF256} [Unsigne
O42 - Logiciel: Jumpstart Installation Program - (.Atheros.) [HKLM][64Bits] -- {B0BCDCBD-863D-4CAB-BF68-8D1F6B1BDC13} [Unsigned]  =>.Atheros
O42 - Logiciel: kdenlive - (.KDE.) [HKLM][64Bits] -- kdenlive [Unsigned]  =>.KDE
O42 - Logiciel: Launcher Prerequisites (x64) - (.Epic Games, Inc..) [HKLM][64Bits] -- {c6c5a357-c7ca-4a5f-9789-3bb1af579253}  =>.Epic Games Inc.® (Hic
O42 - Logiciel: Lecture à distance PS4 - (.Sony Interactive Entertainment Inc..) [HKLM][64Bits] -- {2D85EE38-9BD4-4833-AB01-2467916BB7AE} [Unsigned]
O42 - Logiciel: Litecoin Core (64-bit) - (.Litecoin Core project.) [HKCU][64Bits] -- Litecoin Core (64-bit) [Unsigned]
O42 - Logiciel: Logiciel pour périphérique à chipset Intel® - (.Intel(R) Corporation.) [HKLM][64Bits] -- {314d4c01-f54b-4125-a71f-1e2722c29050}  =>.Ir
O42 - Logiciel: Logitech G HUB - (.Logitech.) [HKLM][64Bits] -- {521c89be-637f-4274-a840-baaf7460c2b2}  =>.Logitech Inc®
O42 - Logiciel: MEGAsync - (.Mega Limited.) [HKLM][64Bits] -- MEGAsync  =>.Mega Limited®
O42 - Logiciel: MegaTrainer Ultimate version 2.4.3.2 - (.MegaDev GmbH.) [HKLM][64Bits] -- {68A5CFDB-E05C-46BC-B2EB-988D1E2C2444}_is1 [Unsigned]
O42 - Logiciel: MegaTrainer Ultimate version 2.5.0.0 - (.MegaDev GmbH.) [HKLM][64Bits] -- {68A5CFDB-E05C-46BC-B2EB-988D1E2C2444}_is1 [Unsigned]
O42 - Logiciel: MEmu - (.Microvirt Software Technology Co. Ltd..) [HKLM][64Bits] -- MEmu  =>.Shanghai Microvirt Software Technology Co., Ltd.®
O42 - Logiciel: Mi PC Suite - (.Xiaomi Inc..) [HKCU][64Bits] -- MiPhoneManager  =>.Xiaomi Technology Inc®
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 OneDrive - (.Microsoft Corporation.) [HKCU][64Bits] -- OneDriveSetup.exe  =>.Microsoft®
O42 - Logiciel: Microsoft SQL Server Compact 3.5 SP2 ENU - (.Microsoft Corporation.) [HKLM][64Bits] -- {3A9FC03D-C685-4831-94CF-4EDFD3749497} [Unsigne
O42 - Logiciel: Microsoft SQL Server Compact 3.5 SP2 x64 ENU - (.Microsoft Corporation.) [HKLM][64Bits] -- {D4AD39AD-091E-4D33-BB2B-59F6FCB8ADC3} [Uns
O42 - Logiciel: Microsoft VC++ redistributables repacked. - (.Intel Corporation.) [HKLM][64Bits] -- {200969CA-4114-4553-832D-4286C5ACBB98} [Unsigned]
O42 - Logiciel: Microsoft VC++ redistributables repacked. - (.Intel Corporation.) [HKLM][64Bits] -- {BD2E4F7B-30B0-46A7-8E5C-D99D21C52336} [Unsigned]
O42 - Logiciel: Microsoft Visual C++ 2005 Redistributable - (.Microsoft Corporation.) [HKLM][64Bits] -- {710f4c1c-cc18-4c49-8cbf-51240c89a1a2} [Unsigr
O42 - Logiciel: Microsoft Visual C++ 2005 Redistributable (x64) - (.Microsoft Corporation.) [HKLM][64Bits] -- {ad8a2fa1-06e7-4b0d-927d-6e54b3d31028}
O42 - Logiciel: Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.17 - (.Microsoft Corporation.) [HKLM][64Bits] -- {8220EEFE-38CD-377E-8595-13
O42 - Logiciel: Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148 - (.Microsoft Corporation.) [HKLM][64Bits] -- {4B6C7001-C7D6-3710-913E-
O42 - Logiciel: Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161 - (.Microsoft Corporation.) [HKLM][64Bits] -- {5FCE6D76-F5DC-37AB-B2B8-
O42 - Logiciel: Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17 - (.Microsoft Corporation.) [HKLM][64Bits] -- {9A25302D-30C0-39D9-BD6F-21
O42 - Logiciel: Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 - (.Microsoft Corporation.) [HKLM][64Bits] -- {1F1C2DFC-2D24-3E06-BCB8-
O42 - Logiciel: Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 - (.Microsoft Corporation.) [HKLM][64Bits] -- {9BE518E6-ECC6-35A9-88E4-
O42 - Logiciel: Microsoft Visual C++ 2010  x64 Redistributable - 10.0.40219 - (.Microsoft Corporation.) [HKLM][64Bits] -- {1D8E6291-B0D5-35EC-8441-661
O42 - Logiciel: Microsoft Visual C++ 2010  x86 Redistributable - 10.0.40219 - (.Microsoft Corporation.) [HKLM][64Bits] -- {F0C3E5D1-1ADE-321E-8167-68E
O42 - Logiciel: Microsoft Visual C++ 2012 Redistributable (x64) - 11.0.60610 - (.Microsoft Corporation.) [HKLM][64Bits] -- {a1909659-0a08-4554-8af1-21
O42 - Logiciel: Microsoft Visual C++ 2012 Redistributable (x64) - 11.0.61030 - (.Microsoft Corporation.) [HKLM][64Bits] -- {ca67548a-5ebe-413a-b50c-4b
O42 - Logiciel: Microsoft Visual C++ 2012 Redistributable (x86) - 11.0.60610 - (.Microsoft Corporation.) [HKLM][64Bits] -- {95716cce-fc71-413f-8ad5-56
O42 - Logiciel: Microsoft Visual C++ 2012 Redistributable (x86) - 11.0.61030 - (.Microsoft Corporation.) [HKLM][64Bits] -- {33d1fd90-4274-48a1-9bc1-97
O42 - Logiciel: Microsoft Visual C++ 2012 x64 Additional Runtime - 11.0.61030 - (.Microsoft Corporation.) [HKLM][64Bits] -- {37B8F9C7-03FB-3253-8781-2
O42 - Logiciel: Microsoft Visual C++ 2012 x64 Minimum Runtime - 11.0.61030 - (.Microsoft Corporation.) [HKLM][64Bits] -- {CF2BEA3C-26EA-32F8-AA9B-331F
O42 - Logiciel: Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.61030 - (.Microsoft Corporation.) [HKLM][64Bits] -- {B175520C-86A2-35A7-8619-8
O42 - Logiciel: Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.61030 - (.Microsoft Corporation.) [HKLM][64Bits] -- {BD95A8CD-1D9F-35AD-981A-3E7
O42 - Logiciel: Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 - (.Microsoft Corporation.) [HKLM][64Bits] -- {050d4fc8-5d48-4b8f-8972-47
O42 - Logiciel: Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.40660 - (.Microsoft Corporation.) [HKLM][64Bits] -- {ef6b00ec-13e1-4c25-9064-b2
O42 - Logiciel: Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 - (.Microsoft Corporation.) [HKLM][64Bits] -- {f65db027-aff3-4070-886a-0d
O42 - Logiciel: Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.40660 - (.Microsoft Corporation.) [HKLM][64Bits] -- {61087a79-ac85-455c-934d-1f
O42 - Logiciel: Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.40660 - (.Microsoft Corporation.) [HKLM][64Bits] -- {5740BD44-B58D-321A-AFC0-6
O42 - Logiciel: Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.40660 - (.Microsoft Corporation.) [HKLM][64Bits] -- {CB0836EC-B072-368D-82B2-D347
O42 - Logiciel: Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.40660 - (.Microsoft Corporation.) [HKLM][64Bits] -- {7DAD0258-515C-3DD4-8964-B
O42 - Logiciel: Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.40660 - (.Microsoft Corporation.) [HKLM][64Bits] -- {E30D8B21-D82D-3211-82CC-0F0A
O42 - Logiciel: Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.24.28127 - (.Microsoft Corporation.) [HKLM][64Bits] -- {282975d8-55fe-4991-b
O42 - Logiciel: Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.24.28127 - (.Microsoft Corporation.) [HKLM][64Bits] -- {e31cb1a4-76b5-46a5-a
O42 - Logiciel: Microsoft Visual C++ 2019 X64 Additional Runtime - 14.24.28127 - (.Microsoft Corporation.) [HKLM][64Bits] -- {8678BA04-D161-45BE-ACA4-
O42 - Logiciel: Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.24.28127 - (.Microsoft Corporation.) [HKLM][64Bits] -- {7DC387B8-E6A2-480C-8EF9-A6B
O42 - Logiciel: Microsoft Visual C++ 2019 X86 Additional Runtime - 14.24.28127 - (.Microsoft Corporation.) [HKLM][64Bits] -- {EAC73207-74BD-4B13-AACF-
O42 - Logiciel: Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.24.28127 - (.Microsoft Corporation.) [HKLM][64Bits] -- {2E72FA1F-BADB-4337-B8AE-F7C
O42 - Logiciel: Microsoft Web Deploy 4.0 - (.Microsoft Corporation.) [HKLM][64Bits] -- {B9DCF505-5A79-4CB4-8440-28B89798ABAB} [Unsigned]  =>.Microsoft
O42 - Logiciel: Microsoft_VC80_CRT_x86 - (.Adobe.) [HKLM][64Bits] -- {92D58719-BBC1-4CC3-A08B-56C9E884CC2C} [Unsigned]  =>.Adobe (Hidden)
O42 - Logiciel: Microsoft_VC90_CRT_x86 - (.Adobe.) [HKLM][64Bits] -- {08D2E121-7F6A-43EB-97FD-629B44903403} [Unsigned]  =>.Adobe (Hidden)
O42 - Logiciel: Minimal ADB and Fastboot version 1.4.3 - (.Samuel Rodberg.) [HKLM][64Bits] -- {B561660D-8B3C-491D-9E3E-293F14FCAADA}_is1 [Unsigned]  =
O42 - Logiciel: Mises à jour NVIDIA 38.0.5.0 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_Display.Update [Unsigne
O42 - Logiciel: Molotov - (.Molotov.) [HKCU][64Bits] -- Molotov [Unsigned]  =>.Molotov
O42 - Logiciel: Mozilla Firefox 83.0 (x64 fr) - (.Mozilla.) [HKLM][64Bits] -- Mozilla Firefox 83.0 (x64 fr)  =>.Mozilla Corporation®
O42 - Logiciel: Mozilla Maintenance Service - (.Mozilla.) [HKLM][64Bits] -- MozillaMaintenanceService [Unsigned]  =>.Mozilla
O42 - Logiciel: MyEpson Portal - (.SEIKO EPSON CORPORATION.) [HKLM][64Bits] -- {3361D415-BA35-4143-B301-661991BA6219} [Unsigned]  =>.Seiko Epson Corpo
O42 - Logiciel: MyEpson Portal - (.SEIKO EPSON Corporation.) [HKLM][64Bits] -- MyEpson Portal [Unsigned]  =>.Seiko Epson Corporation
O42 - Logiciel: No-IP DUC - (.Vitalwerks Internet Solutions LLC.) [HKLM][64Bits] -- NoIPDUC [Unsigned]  =>.Vitalwerks Internet Solutions LLC
O42 - Logiciel: Notepad++ (32-bit x86) - (.Notepad++ Team.) [HKLM][64Bits] -- Notepad++ [Unsigned]  =>.Notepad++ Team
O42 - Logiciel: Nox APP Player - (.Duodian Technology Co. Ltd..) [HKLM][64Bits] -- Nox  =>.Nox Limited®
O42 - Logiciel: NVAPI Monitor plugin for NvContainer - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvContainer.Nva
O42 - Logiciel: NVIDIA ABHub - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvAbHub [Unsigned]  =>.NVIDIA Corporati
O42 - Logiciel: NVIDIA Ansel - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_Ansel [Unsigned]  =>.NVIDIA Corporation
O42 - Logiciel: NVIDIA Backend - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvBackend [Unsigned]  =>.NVIDIA Corpo
O42 - Logiciel: NVIDIA Container - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvContainer [Unsigned]  =>.NVIDIA C
O42 - Logiciel: NVIDIA Display Container - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NVDisplayContainer [Unsigne
O42 - Logiciel: NVIDIA Display Container LS - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NVDisplayContainerLS [Un
O42 - Logiciel: NVIDIA Display MessageBus - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvDisplay.MessageBus [Unsi
O42 - Logiciel: NVIDIA Display Session Container - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NVDisplaySessionCon
O42 - Logiciel: NVIDIA Display Watchdog Plugin - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NVDisplayPluginWatch
O42 - Logiciel: NVIDIA FrameView SDK 1.1.4923.29214634 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_FrameViewSdk
O42 - Logiciel: NVIDIA GeForce Experience 3.20.5.70 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_Display.GFExperi
O42 - Logiciel: NVIDIA Install Application - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_installer [Unsigned]  =>
O42 - Logiciel: NVIDIA LocalSystem Container - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvContainer.LocalSystem
O42 - Logiciel: NVIDIA Logiciel système PhysX 9.19.0218 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_Display.Phys
O42 - Logiciel: NVIDIA Message Bus for NvContainer - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvContainer.Messa
O42 - Logiciel: NVIDIA NetworkService Container - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvContainer.ServiceL
O42 - Logiciel: NVIDIA NodeJS - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvNodejs [Unsigned]  =>.NVIDIA Corpora
O42 - Logiciel: NVIDIA Optimus Update 38.0.5.0 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_Display.Optimus [Unsi
O42 - Logiciel: NVIDIA Pilote audio HD : 1.3.38.35 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_HDAudio.Driver [U
O42 - Logiciel: NVIDIA Pilote graphique 457.30 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_Display.Driver [Unsig
O42 - Logiciel: NVIDIA Session Container - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvContainer.Session [Unsigr
O42 - Logiciel: NVIDIA ShadowPlay 3.20.5.70 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_ShadowPlay [Unsigned]  =
O42 - Logiciel: Nvidia Share - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_OSC [Unsigned]  =>.NVIDIA Corporation (
O42 - Logiciel: NVIDIA SHIELD Streaming - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_GFExperience.NvStreamSrv [Un
O42 - Logiciel: NVIDIA SHIELD Wireless Controller Driver - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_ShieldWirel
O42 - Logiciel: NVIDIA Telemetry Client - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvTelemetry [Unsigned]  =>.N
O42 - Logiciel: NVIDIA TelemetryApi helper for NvContainer - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvContair
O42 - Logiciel: NVIDIA Update Core - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_Update.Core [Unsigned]  =>.NVIDIA
O42 - Logiciel: NVIDIA User Container - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvContainer.User [Unsigned]  =
O42 - Logiciel: NVIDIA Virtual Audio 4.13.0.0 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_VirtualAudio.Driver [U
O42 - Logiciel: NVIDIA Virtual Host Controller - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvvHci [Unsigned]  =>
O42 - Logiciel: NVIDIA Watchdog Plugin for NvContainer - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvPlugin.Watc
O42 - Logiciel: NvModuleTracker - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvModuleTracker.Driver [Unsigned]  =
O42 - Logiciel: OBS Studio - (.OBS Project.) [HKLM][64Bits] -- OBS Studio [Unsigned]  =>.OBS Project
O42 - Logiciel: Online Application - (.Microleaves.) [HKLM][64Bits] -- {5266F634-7B7D-4537-BDDC-98DD6CFCBAA1} [Unsigned]  =>SUP.Optional.Microleaves (
O42 - Logiciel: OpenIV - (..black/OpenIV Team.) [HKCU][64Bits] -- OpenIV [Unsigned]  =>..black/OpenIV Team
O42 - Logiciel: Opera Stable 72.0.3815.400 - (.Opera Software.) [HKCU][64Bits] -- Opera 72.0.3815.400  =>.Opera Software AS®
O42 - Logiciel: Oracle VM VirtualBox 6.0.2 - (.Oracle Corporation.) [HKLM][64Bits] -- {4D3D3639-3132-4F5E-840D-C182E3E5C901} [Unsigned]  =>.Oracle Cor
```

```
O42 - Logiciel: Origin - (.Electronic Arts, Inc..) [HKLM][64Bits] -- Origin  =>.Electronic Arts, Inc.®
O42 - Logiciel: Outil de téléchargement USB/DVD Windows 7 - (.Microsoft Corporation.) [HKLM][64Bits] -- {5F8683B5-5056-411C-B808-B289E29E9BBB} [Unsigr
O42 - Logiciel: Package de pilotes Windows - Google, Inc. (WinUSB) AndroidUsbDeviceClass  ( - (.Google, Inc..) [HKLM][64Bits] -- 092555911492C6959D25S
O42 - Logiciel: paint.net - (.dotPDN LLC.) [HKLM][64Bits] -- {B998B716-4001-4919-BA90-BA14B51DFEB5} [Unsigned]  =>.dotPDN LLC
O42 - Logiciel: Panneau de configuration NVIDIA 457.30 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_Display.Contr
O42 - Logiciel: Paradox Launcher v2 - (.Paradox Interactive.) [HKLM][64Bits] -- {F0072197-FCF6-41BF-9D38-832B145922DC} [Unsigned]  =>.Paradox Interact
O42 - Logiciel: PBO Manager v.1.4 beta - (..) [HKLM][64Bits] -- {127B5371-1802-4EDD-A25A-A43BF761D383} [Unsigned]
O42 - Logiciel: PC Building Simulator Razer Workshop - (..) [HKLM][64Bits] -- PC Building Simulator Razer Workshop_is1 [Unsigned]
O42 - Logiciel: ph - (.Your Company Name.) [HKLM][64Bits] -- {185F9795-9663-4F13-9EF9-307A282ADB5A} [Unsigned]  =>.Your Company Name (Hidden)
O42 - Logiciel: PhotoFiltre - (.Antonio Da Cruz.) [HKCU][64Bits] -- PhotoFiltre [Unsigned]  =>.Antonio Da Cruz
O42 - Logiciel: PhotoFiltre 7 - (.Antonio Da Cruz.) [HKCU][64Bits] -- PhotoFiltre 7 [Unsigned]  =>.Antonio Da Cruz
O42 - Logiciel: Popcorn-Time - (.Popcorn Time.) [HKCU][64Bits] -- Popcorn-Time [Unsigned]  =>.SUP.PopcornTime
O42 - Logiciel: PowerISO - (.Power Software Ltd.) [HKLM][64Bits] -- PowerISO [Unsigned]  =>.Power Software Ltd
O42 - Logiciel: Prey Anti-Theft - (.Prey, Inc..) [HKLM][64Bits] -- {3086FB3E-CBA5-4DFE-BAB6-E34192ECF456} [Unsigned]  =>.Prey, Inc. (Hidden)
O42 - Logiciel: Prison Architect - (.Double Eleven.) [HKLM][64Bits] -- Steam App 233450  =>.Valve®
O42 - Logiciel: Project Hospital - (.GOG.com.) [HKLM][64Bits] -- 1660194629_is1  =>.GOG Sp. z o.o.®
O42 - Logiciel: Quran Explorer Desktop - (.Quran Explorer.) [HKLM][64Bits] -- {34A9F183-1011-4845-9826-FBAA53DA59DF} [Unsigned]
O42 - Logiciel: Quranflash Desktop version 1.3 - (.Vijua, Inc..) [HKLM][64Bits] -- {628E798A-4A77-46F8-9E3D-5A5D6377323E}}_is1 {00F0A5CD9EA2DD1322C07D
O42 - Logiciel: REALTEK Bluetooth Driver - (.REALTEK Semiconductor Corp..) [HKLM][64Bits] -- {9D3D8C60-A5EF-4123-B2B9-172095903AB}  =>.Realtek Semicor
O42 - Logiciel: Realtek Card Reader - (.Realtek Semiconductor Corp..) [HKLM][64Bits] -- {5BC2B5AB-80DE-4E83-B8CF-426902051D0A}  =>.Realtek Semiconduct
O42 - Logiciel: Realtek Ethernet Controller Driver - (.Realtek.) [HKLM][64Bits] -- {8833FFB6-5B0C-4764-81AA-06DFEED9A476}  =>.Realtek Semiconductor Co
O42 - Logiciel: Realtek High Definition Audio Driver - (.Realtek Semiconductor Corp..) [HKLM][64Bits] -- {F132AF7F-7BCA-4EDE-8A7C-958108FE7DBC}  =>.Re
O42 - Logiciel: REALTEK RTL8187B Wireless LAN Driver - (.REALTEK Semiconductor Corp..) [HKLM][64Bits] -- {7095FD27-37F0-4750-9DE8-D37DC0043706} [Unsig
O42 - Logiciel: REALTEK Wireless LAN Driver - (.REALTEK Semiconductor Corp..) [HKLM][64Bits] -- {A5107464-AA9B-4177-8129-5FF2F42DD322}  =>.Realtek Sem
O42 - Logiciel: Rockstar Games Launcher - (.Rockstar Games.) [HKLM][64Bits] -- Rockstar Games Launcher [Unsigned]  =>.Rockstar Games
O42 - Logiciel: Rockstar Games Social Club - (.Rockstar Games.) [HKLM][64Bits] -- Rockstar Games Social Club  =>.Rockstar Games, Inc.®
O42 - Logiciel: RVL Hacker (1.00.095) (remove only) - (..) [HKLM][64Bits] -- RVLHacker [Unsigned]
O42 - Logiciel: Samsung SideSync - (.Samsung Electronics Co., Ltd..) [HKLM][64Bits] -- Samsung SideSync [Unsigned]  =>.Samsung Electronics Co., Ltd.
O42 - Logiciel: Samsung USB Driver for Mobile Phones - (.Samsung Electronics Co., Ltd..) [HKLM][64Bits] -- {D0795B21-0CDA-4a92-AB9E-6E92D8111E44}  =>
O42 - Logiciel: Smart City Plan - (.Ambiera.) [HKLM][64Bits] -- Steam App 1074180  =>.Valve®
O42 - Logiciel: Smart Switch - (.Samsung Electronics Co., Ltd..) [HKLM][64Bits] -- {74FA5314-85C8-4E2A-907D-D9ECCCB770A7} [Unsigned]  =>.Samsung Elect
O42 - Logiciel: Smart Switch - (.Samsung Electronics Co., Ltd..) [HKLM][64Bits] -- InstallShield_{74FA5314-85C8-4E2A-907D-D9ECCCB770A7} [Unsigned]  =>
O42 - Logiciel: Smartphone Tycoon - (.Roastery Games.) [HKLM][64Bits] -- Steam App 996380  =>.Valve®
O42 - Logiciel: Snaz version 1.12.7.0 - (.JimsApps.) [HKLM][64Bits] -- {70A76031-FDC6-4F9B-BB5C-33776703F45A}_is1 [Unsigned]  =>.JimsApps
O42 - Logiciel: Speccy - (.Piriform.) [HKLM][64Bits] -- Speccy  =>.Piriform Ltd®
O42 - Logiciel: Spintires MudRunner American Wilds - (..) [HKLM][64Bits] -- Spintires MudRunner American Wilds_is1 [Unsigned]
O42 - Logiciel: Startup Company - (.Hovgaard Games.) [HKLM][64Bits] -- Steam App 606800  =>.Valve®
O42 - Logiciel: Steam - (.Valve Corporation.) [HKLM][64Bits] -- Steam  =>.Valve®
O42 - Logiciel: Streamlabs OBS 0.11.6 - (.General Workings, Inc..) [HKLM][64Bits] -- 029c4619-0385-5543-9426-46f9987161d9  =>.General Workings Inc (St
O42 - Logiciel: Sublime Text Build 3143 - (.Sublime HQ Pty Ltd.) [HKLM][64Bits] -- Sublime Text 3_is1  =>.Sublime HQ Pty Ltd®
O42 - Logiciel: Supercopier 2.0.3.11 - (.Supercopier.) [HKLM][64Bits] -- Supercopier [Unsigned]  =>.Supercopier
O42 - Logiciel: SurfOffline Professional 2 - (.Bimesoft.) [HKLM][64Bits] -- SurfOffline Professional 2 [Unsigned]  =>.Bimesoft
O42 - Logiciel: Sync withSIX - (.SIX Networks GmbH.) [HKCU][64Bits] -- Sync [Unsigned]  =>.SIX Networks GmbH
O42 - Logiciel: TDM-GCC - (.TDM.) [HKLM][64Bits] -- TDM-GCC [Unsigned]  =>.TDM
O42 - Logiciel: TeamSpeak 3 Client - (.TeamSpeak Systems GmbH.) [HKLM][64Bits] -- TeamSpeak 3 Client [Unsigned]  =>.TeamSpeak Systems GmbH
O42 - Logiciel: TeamViewer 14 - (.TeamViewer.) [HKLM][64Bits] -- TeamViewer  =>.TeamViewer GmbH®
O42 - Logiciel: TerannForLife Launcher version 5.2.0 - (.TerannForLife.) [HKLM][64Bits] -- {914fe91e-2546-4b7d-9f06-7a470c56bc70}_is1 [Unsigned]
O42 - Logiciel: Tourist Bus Simulator - (.TML-Studios.) [HKLM][64Bits] -- Steam App 953580  =>.Valve®
O42 - Logiciel: TruckersMP Launcher 1.0.0.4 - (.TruckersMP Team.) [HKLM][64Bits] -- {A227B892-C548-4490-9C5D-DB341F8194A6}_is1 [Unsigned]  =>.Truckers
O42 - Logiciel: Twitch - (.Twitch Interactive, Inc..) [HKCU][64Bits] -- {DEE70742-F4E9-44CA-B2B9-EE95DCF37295}  =>.Twitch Interactive, Inc.®
O42 - Logiciel: Two Point Hospital - (.SKIDROW.) [HKLM][64Bits] -- SKIDROW - Two Point Hospital [Unsigned]  =>.SKIDROW
O42 - Logiciel: UE4 Prerequisites (x64) - (.Epic Games, Inc..) [HKLM][64Bits] -- {4e242cc8-5e3c-4b08-9d55-dbc62ddd1208}  =>.Epic Games Inc.® (Hidden)
O42 - Logiciel: UE4 Prerequisites (x64) - (.Epic Games, Inc..) [HKLM][64Bits] -- {F9EC45F9-074A-48BF-92E9-A8CADD56F693} [Unsigned]  =>.Epic Games, Inc
O42 - Logiciel: Update for Windows 10 for x64-based Systems (KB4023057) - (.Microsoft Corporation.) [HKLM][64Bits] -- {32DC821E-4A7D-4878-BEE8-337FA15
O42 - Logiciel: UpdateAssistant - (.Microsoft Corporation.) [HKLM][64Bits] -- {52C1DD03-104E-4AC6-9DC6-21D585721ED1} [Unsigned]  =>.Microsoft Corporat
O42 - Logiciel: Uplay - (.Ubisoft.) [HKLM][64Bits] -- Uplay  =>.Ubisoft Entertainment Sweden AB®
O42 - Logiciel: USBPcap 1.2.0.4 - (.Tomasz Mon.) [HKLM][64Bits] -- USBPcap  =>.Tomasz Moń®
O42 - Logiciel: VLC media player - (.VideoLAN.) [HKLM][64Bits] -- VLC media player [Unsigned]  =>.VideoLAN
O42 - Logiciel: Wampserver64 3.2.0 - (.Dominique Ottello aka Otomatic.) [HKLM][64Bits] -- {wampserver64}_is1 [Unsigned]  =>.Dominique Ottello aka Otom
O42 - Logiciel: WebAdvisor par McAfee - (.McAfee, LLC.) [HKLM][64Bits] -- {35ED3F83-4BDC-4c44-8EC6-6A8301C7413A}  =>.McAfee, LLC®
O42 - Logiciel: WebCopier 5.3 - (.MaximumSoft Corp..) [HKLM][64Bits] -- {0C72BD21-2BBB-43E6-8EEB-C8BE42FE90E5}_is1 [Unsigned]  =>.MaximumSoft Corp.
O42 - Logiciel: Website Ripper Copier - (..) [HKLM][64Bits] -- Website Ripper Copier [Unsigned]
O42 - Logiciel: WeMod Version Guard - (.WeMod.) [HKLM][64Bits] -- {7761C1A0-D828-4CB8-8F3C-9D9B5937CECB} [Unsigned]  =>.WeMod
O42 - Logiciel: WhatsApp - (.WhatsApp.) [HKCU][64Bits] -- WhatsApp  =>.WhatsApp, Inc®
O42 - Logiciel: Win32DiskImager version 1.0.0 - (.ImageWriter Developers.) [HKLM][64Bits] -- {3DFFA293-DF2C-4B23-92E5-3433BDC310E1}}_is1 [Unsigned]  =
O42 - Logiciel: WinHTTrack Website Copier 3.49-2 - (.HTTrack.) [HKLM][64Bits] -- WinHTTrack Website Copier_is1  =>.Open Source Developer, Xavier Roche
O42 - Logiciel: WinPcap 4.1.3 - (.Riverbed Technology, Inc..) [HKLM][64Bits] -- WinPcapInst [Unsigned]  =>.Riverbed Technology, Inc.
O42 - Logiciel: WinRAR 5.91 (32-bit) - (.win.rar GmbH.) [HKLM][64Bits] -- WinRAR archiver  =>.win.rar GmbH®
O42 - Logiciel: Wondershare Filmora9(Build 9.4.5) - (.Wondershare Software.) [HKLM][64Bits] -- Wondershare Filmora9_is1 [Unsigned]  =>.Wondershare Sof
O42 - Logiciel: Wondershare Helper Compact 2.6.0 - (.Wondershare.) [HKLM][64Bits] -- {5363CE84-5F09-48A1-8B6C-6BB590FFEDF2}_is1 [Unsigned]  =>.Wonders
O42 - Logiciel: Wondershare UniConverter(Build 11.7.0.3) - (.Wondershare Software.) [HKLM][64Bits] -- UniConverter_is1  =>.Wondershare Technology Co.,

---\ CLÉ DE REGISTRE SOFTWARE HKCU & HKLM (472) - 57s
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\csastats  =>Adware.InstallCore
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\drp.su  =>.SUP.DriverPa
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\webcompanion.com  =>PUP
HKCU\Software\Lavasoft\Web Companion  =>PUP.Optional.LavasoftWebCompanion
HKCU\Software\csastats  =>Adware.InstallCore
HKCU\Software\undefined  =>.SUP.Downloader
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\drp.su  =>.SUP.DriverPack
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\webcompanion.com  =>PUP.Optional.LavasoftWebCompanion
HKLM\SOFTWARE\Wow6432Node\IObit\RealTimeProtector  =>SUP.Optional.AdvancedSystemCare
HKLM\SOFTWARE\Wow6432Node\IObit\Advanced SystemCare  =>SUP.Optional.AdvancedSystemCare
HKLM\SOFTWARE\Wow6432Node\IObit\ASC  =>SUP.Optional.AdvancedSystemCare
HKLM\SOFTWARE\Wow6432Node\Lavasoft\Web Companion  =>PUP.Optional.LavasoftWebCompanion
HKLM\SOFTWARE\Lavasoft\Web Companion  =>PUP.Optional.LavasoftWebCompanion
HKLM\SOFTWARE\Google\Chrome\NativeMessagingHosts\com.ascplugin.protect  =>SUP.Optional.AdvancedSystemCare
HKLM\SOFTWARE\IObit\RealTimeProtector  =>SUP.Optional.AdvancedSystemCare
HKLM\SOFTWARE\IObit\Advanced SystemCare  =>SUP.Optional.AdvancedSystemCare
HKLM\SOFTWARE\Iobit\ASC  =>SUP.Optional.AdvancedSystemCare
HKLM\SOFTWARE\029c4619-0385-5543-9426-46f9987161d9  =>Adware.CrossRider
HKLM\SOFTWARE\Adobe  =>.Adobe
HKLM\SOFTWARE\AGEIA Technologies  =>.AGEIA Technologies
HKLM\SOFTWARE\Android Studio  =>.Android Studio
HKLM\SOFTWARE\Apple Inc.  =>.Apple Inc.
HKLM\SOFTWARE\ASIO  =>.Steinberg Media Technologies
HKLM\SOFTWARE\Atheros  =>.Qualcomm Atheros
HKLM\SOFTWARE\AVAST Software  =>.AVAST Software
HKLM\SOFTWARE\Bitcoin Core (64-bit)
HKLM\SOFTWARE\BlueStacksInstaller
HKLM\SOFTWARE\Canon  =>.Canon
HKLM\SOFTWARE\CVSM  =>.Legitimate
HKLM\SOFTWARE\cybelsoft  =>.CybelSoft
HKLM\SOFTWARE\CyberGhost  =>.CyberGhost S.R.L
```

HKLM\SOFTWARE\DefaultUserEnvironment =>.Microsoft Corporation
HKLM\SOFTWARE\EA Sports =>.Electronic Arts, Inc.
HKLM\SOFTWARE\EPSON =>.EPSON
HKLM\SOFTWARE\fdx
HKLM\SOFTWARE\FileZilla 3 =>.FileZilla
HKLM\SOFTWARE\Fortemedia =>.Lugert Europe
HKLM\SOFTWARE\Google =>.Google
HKLM\SOFTWARE\HAXM
HKLM\SOFTWARE\Hewlett-Packard =>.Hewlett-Packard
HKLM\SOFTWARE\HP =>.HP
HKLM\SOFTWARE\Intel =>.Intel
HKLM\SOFTWARE\JavaSoft =>.JavaSoft
HKLM\SOFTWARE\JreMetrics =>.JreMetrics
HKLM\SOFTWARE\Khronos =>.Khronos
HKLM\SOFTWARE\Litecoin Core (64-bit)
HKLM\SOFTWARE\Macromedia =>.Macromedia
HKLM\SOFTWARE\Maxis =>.Maxis
HKLM\SOFTWARE\McAfee =>.McAfee Inc.
HKLM\SOFTWARE\MegaTrainerUltimate =>.MegaDev
HKLM\SOFTWARE\Minnetonka Audio Software =>.Minnetonka Audio Software
HKLM\SOFTWARE\Mozilla =>.Mozilla
HKLM\SOFTWARE\mozilla.org =>.mozilla.org
HKLM\SOFTWARE\MozillaPlugins =>.MozillaPlugins
HKLM\SOFTWARE\Nuance =>.Nuance
HKLM\SOFTWARE\NVIDIA Corporation =>.nVidia Corporation
HKLM\SOFTWARE\ODBC =>.DB Connectivity Solutions
HKLM\SOFTWARE\OEM =>.OEM
HKLM\SOFTWARE\Oracle =>.Oracle
HKLM\SOFTWARE\paint.net =>.Rick Brewster
HKLM\SOFTWARE\PBOManager
HKLM\SOFTWARE\Piriform =>.Piriform
HKLM\SOFTWARE\Realtek =>.Realtek Semiconductor Corp.
HKLM\SOFTWARE\RegisteredApplications =>.Microsoft Corporation
HKLM\SOFTWARE\Rockstar Games =>.Rockstar Games
HKLM\SOFTWARE\RTLSetup =>.Realtek Semiconductor Corp.
HKLM\SOFTWARE\SAMSUNG =>.Samsung Electronics
HKLM\SOFTWARE\SonicFocus =>.Sonic Focus
HKLM\SOFTWARE\SoundResearch =>.Sound Research
HKLM\SOFTWARE\SRS Labs =>.SRS Labs
HKLM\SOFTWARE\Synaptics =>.Synaptics
HKLM\SOFTWARE\Tangentix =>.Tangentix
HKLM\SOFTWARE\TeamSpeak 3 Client =>.TeamSpeak
HKLM\SOFTWARE\TruckersMP =>.TruckersMP
HKLM\SOFTWARE\VideoLAN =>.VideoLan Team
HKLM\SOFTWARE\VMware, Inc. =>.VMware, Inc.
HKLM\SOFTWARE\Volatile =>.Microsoft Corporation
HKLM\SOFTWARE\Wondershare =>.Wondershare
HKLM\SOFTWARE\WOW6432Node =>.Microsoft Corporation
HKLM\SOFTWARE\WOW6432Node\3DMLAUNCHER
HKLM\SOFTWARE\WOW6432Node\7-Zip =>.Igor Pavlov
HKLM\SOFTWARE\WOW6432Node\Adobe =>.Adobe
HKLM\SOFTWARE\WOW6432Node\AGEIA Technologies =>.AGEIA Technologies
HKLM\SOFTWARE\WOW6432Node\APK Editor Studio
HKLM\SOFTWARE\WOW6432Node\Apple Inc. =>.Apple Inc.
HKLM\SOFTWARE\WOW6432Node\ASIO =>.Steinberg Media Technologies
HKLM\SOFTWARE\WOW6432Node\Atheros =>.Qualcomm Atheros
HKLM\SOFTWARE\WOW6432Node\Avanquest =>.Avanquest
HKLM\SOFTWARE\WOW6432Node\Avast Software =>.AVAST Software
HKLM\SOFTWARE\WOW6432Node\Avira =>.Avira
HKLM\SOFTWARE\WOW6432Node\Bimesoft =>.Bimesoft
HKLM\SOFTWARE\WOW6432Node\bistudio
HKLM\SOFTWARE\WOW6432Node\Bitdefender Agent =>.Bitdefender
HKLM\SOFTWARE\WOW6432Node\Blizzard Entertainment =>.Blizzard Entertainment
HKLM\SOFTWARE\WOW6432Node\Bluestacks =>.BlueStack Systems, Inc.
HKLM\SOFTWARE\WOW6432Node\bohemia interactive =>.Bohemia Interactive
HKLM\SOFTWARE\WOW6432Node\Brackets =>.Brackets
HKLM\SOFTWARE\WOW6432Node\Chromium =>.Chromium
HKLM\SOFTWARE\WOW6432Node\CyberGhost =>.CyberGhost S.R.L
HKLM\SOFTWARE\WOW6432Node\Dropbox =>.Dropbox
HKLM\SOFTWARE\WOW6432Node\DropboxUpdate =>.Dropbox Inc.
HKLM\SOFTWARE\WOW6432Node\DuoDianOnline =>.DuoDian Online
HKLM\SOFTWARE\WOW6432Node\EA Sports =>.Electronic Arts, Inc.
HKLM\SOFTWARE\WOW6432Node\EasyAntiCheat =>.EasyAntiCheat
HKLM\SOFTWARE\WOW6432Node\Electronic Arts =>.Electronic Arts
HKLM\SOFTWARE\WOW6432Node\Epic Games =>.Epic Games
HKLM\SOFTWARE\WOW6432Node\EpicGames =>.Epic Games
HKLM\SOFTWARE\WOW6432Node\EPSON =>.EPSON
HKLM\SOFTWARE\WOW6432Node\FileZilla 3 =>.FileZilla
HKLM\SOFTWARE\WOW6432Node\FileZilla Client =>.Tim Kosse
HKLM\SOFTWARE\WOW6432Node\FreeGrabApp =>.FreeGrabApp
HKLM\SOFTWARE\WOW6432Node\GlarySoft =>.GlarySoft
HKLM\SOFTWARE\WOW6432Node\GNU =>.GNU
HKLM\SOFTWARE\WOW6432Node\GOG.com =>.GOG.com
HKLM\SOFTWARE\WOW6432Node\Google =>.Google
HKLM\SOFTWARE\WOW6432Node\Hewlett-Packard =>.Hewlett-Packard
HKLM\SOFTWARE\WOW6432Node\HP =>.HP
HKLM\SOFTWARE\WOW6432Node\HP Inc. =>.HP Inc.
HKLM\SOFTWARE\WOW6432Node\Intel =>.Intel
HKLM\SOFTWARE\WOW6432Node\IObit =>.IObit
HKLM\SOFTWARE\WOW6432Node\Jarvee
HKLM\SOFTWARE\WOW6432Node\JavaSoft =>.JavaSoft
HKLM\SOFTWARE\WOW6432Node\JetBrains =>.JetBrains
HKLM\SOFTWARE\WOW6432Node\JreMetrics =>.JreMetrics
HKLM\SOFTWARE\WOW6432Node\KasperskyLab =>.Kaspersky Labs
HKLM\SOFTWARE\WOW6432Node\KDE =>.KDE
HKLM\SOFTWARE\WOW6432Node\Khronos =>.Khronos
HKLM\SOFTWARE\WOW6432Node\Lavasoft =>.Lavasoft
HKLM\SOFTWARE\WOW6432Node\LogMeInRescueCallingCard =>.LogMeIn Entreprise
HKLM\SOFTWARE\WOW6432Node\LogMeInRescueCallingCards =>.LogMeIn Entreprise
HKLM\SOFTWARE\WOW6432Node\Macromedia =>.Macromedia
HKLM\SOFTWARE\WOW6432Node\Maxis =>.Maxis
HKLM\SOFTWARE\WOW6432Node\McAfee NGI =>.McAfee Inc.
HKLM\SOFTWARE\WOW6432Node\MegaTrainerUltimate =>.MegaDev
HKLM\SOFTWARE\WOW6432Node\Microleaves =>SUP.Optional.Microleaves

HKLM\SOFTWARE\WOW6432Node\Mozilla =>.Mozilla
HKLM\SOFTWARE\WOW6432Node\MozillaPlugins =>.MozillaPlugins
HKLM\SOFTWARE\WOW6432Node\Nemu
HKLM\SOFTWARE\WOW6432Node\Notepad++ =>.Don Ho
HKLM\SOFTWARE\WOW6432Node\Nuance =>.Nuance
HKLM\SOFTWARE\WOW6432Node\NVIDIA Corporation =>.nVidia Corporation
HKLM\SOFTWARE\WOW6432Node\OBS Studio =>.OBS Studio
HKLM\SOFTWARE\WOW6432Node\ODBC =>.DB Connectivity Solutions
HKLM\SOFTWARE\WOW6432Node\Oracle =>.Oracle
HKLM\SOFTWARE\WOW6432Node\Origin =>.Electronic Arts, Inc.
HKLM\SOFTWARE\WOW6432Node\Origin Games =>.Electronic Arts, Inc.
HKLM\SOFTWARE\WOW6432Node\PowerISO =>.PowerISO Computing
HKLM\SOFTWARE\WOW6432Node\Prey
HKLM\SOFTWARE\WOW6432Node\Realtek =>.Realtek Semiconductor Corp.
HKLM\SOFTWARE\WOW6432Node\Realtek Semiconductor Corp. =>.Realtek Semiconductor Corp.
HKLM\SOFTWARE\WOW6432Node\Rockstar Games =>.Rockstar Games
HKLM\SOFTWARE\WOW6432Node\RtWLan =>.Realtek Semiconductor Corp.
HKLM\SOFTWARE\WOW6432Node\RVLHacker
HKLM\SOFTWARE\WOW6432Node\Samsung =>.Samsung Electronics
HKLM\SOFTWARE\WOW6432Node\Sonic =>.Sonic
HKLM\SOFTWARE\WOW6432Node\Sony Corporation =>.Sony Corporation
HKLM\SOFTWARE\WOW6432Node\Tangentix =>.Tangentix
HKLM\SOFTWARE\WOW6432Node\TeamViewer =>.TeamViewer GmbH
HKLM\SOFTWARE\WOW6432Node\ThinPrint =>.ThinPrint
HKLM\SOFTWARE\WOW6432Node\TVInstallTemp =>.TeamViewer GmbH
HKLM\SOFTWARE\WOW6432Node\Ubisoft =>.Ubisoft
HKLM\SOFTWARE\WOW6432Node\Valve =>.Valve
HKLM\SOFTWARE\WOW6432Node\VMware, Inc. =>.VMware, Inc.
HKLM\SOFTWARE\WOW6432Node\Volatile =>.Microsoft Corporation
HKLM\SOFTWARE\WOW6432Node\WafCX =>.WafCX
HKLM\SOFTWARE\WOW6432Node\WinHTTrack Website Copier =>.Xavier Roche
HKLM\SOFTWARE\WOW6432Node\WinPcap =>.Riverbed Technology
HKLM\SOFTWARE\WOW6432Node\WinRAR =>.WinRAR
HKLM\SOFTWARE\WOW6432Node\Wondershare =>.Wondershare
HKLM\SOFTWARE\WOW6432Node\WOW6432Node =>.Microsoft Corporation
HKLM\SOFTWARE\WOW6432Node\XiaoMi =>.XiaoMi Tech
HKLM\SOFTWARE\WOW6432Node\RegisteredApplications =>.Microsoft Corporation
HKCU\SOFTWARE\681da0eb-374d-5be1-94a8-a3b514928885 =>Adware.CrossRider
HKCU\SOFTWARE\7-Zip =>.Igor Pavlov
HKCU\SOFTWARE\A-PDF =>.A-PDF Software
HKCU\SOFTWARE\Adobe =>.Adobe
HKCU\SOFTWARE\Akeo Consulting =>.Akeo Consulting
HKCU\SOFTWARE\Android Open Source Project =>.Open Source
HKCU\SOFTWARE\APK Editor Studio
HKCU\SOFTWARE\Apoapsis Studios
HKCU\SOFTWARE\Apowersoft =>.Apowersoft
HKCU\SOFTWARE\Apple Inc. =>.Apple Inc.
HKCU\SOFTWARE\Astragon =>.Astragon
HKCU\SOFTWARE\Atheros =>.Qualcomm Atheros
HKCU\SOFTWARE\Avast Software =>.AVAST Software
HKCU\SOFTWARE\AvastAdSDK =>.Avast Software s.r.o
HKCU\SOFTWARE\Avira =>.Avira
HKCU\SOFTWARE\Bimesoft =>.Bimesoft
HKCU\SOFTWARE\Bitcoin
HKCU\SOFTWARE\Bitdefender VPN =>.Bitdefender
HKCU\SOFTWARE\BitTorrent =>.BitTorrent (P2P)
HKCU\SOFTWARE\Blizzard Entertainment =>.Blizzard Entertainment
HKCU\SOFTWARE\BlueStacksInstaller
HKCU\SOFTWARE\Bohemia Interactive =>.Bohemia Interactive
HKCU\SOFTWARE\Brackets =>.Brackets
HKCU\SOFTWARE\Browser Cleanup =>.Avast Software s.r.o
HKCU\SOFTWARE\BugSplat =>.Bugsplat Game
HKCU\SOFTWARE\Cain
HKCU\SOFTWARE\Canon =>.Canon
HKCU\SOFTWARE\Cheat Engine =>.Dark Byte
HKCU\SOFTWARE\Chromium =>.Chromium
HKCU\SOFTWARE\CodeBlocks =>.CodeBlocks Team
HKCU\SOFTWARE\Colossal Order =>.Colossal Order
HKCU\SOFTWARE\Coredumping
HKCU\SOFTWARE\CyberLink =>.CyberLink Corporation
HKCU\SOFTWARE\Cygwin =>.Cygwin
HKCU\SOFTWARE\Cyotek =>.Cyotek
HKCU\SOFTWARE\Dapper Penguin Studios
HKCU\SOFTWARE\Dashlane_profiles =>.Dashlane, Inc
HKCU\SOFTWARE\DC3_FEXEC =>Trojan.Fynloski
HKCU\SOFTWARE\DefaultCompany =>.Unity
HKCU\SOFTWARE\Dell =>.Dell
HKCU\SOFTWARE\DriverHub
HKCU\SOFTWARE\Dropbox =>.Dropbox
HKCU\SOFTWARE\DropboxUpdate =>.Dropbox Inc.
HKCU\SOFTWARE\DuoDianApp =>.DuoDianApp
HKCU\SOFTWARE\Eggcode
HKCU\SOFTWARE\Electronic Arts =>.Electronic Arts
HKCU\SOFTWARE\emagmaker
HKCU\SOFTWARE\Empyrean
HKCU\SOFTWARE\Epic Games =>.Epic Games
HKCU\SOFTWARE\EPSON =>.EPSON
HKCU\SOFTWARE\FastDataX =>Adware.FastDataX
HKCU\SOFTWARE\FlipBuilder =>.FlipBuilder
HKCU\SOFTWARE\FreeGrabApp =>.FreeGrabApp
HKCU\SOFTWARE\Glarysoft =>.GlarySoft
HKCU\SOFTWARE\GNU =>.GNU
HKCU\SOFTWARE\GOG.com =>.GOG.com
HKCU\SOFTWARE\Google =>.Google
HKCU\SOFTWARE\Gyazo =>.Nota Inc.
HKCU\SOFTWARE\Haemimont Games =>.Haemimont Games
HKCU\SOFTWARE\Hewlett-Packard =>.Hewlett-Packard
HKCU\SOFTWARE\HP =>.HP
HKCU\SOFTWARE\Intel Corporation =>.Intel Corporation
HKCU\SOFTWARE\JavaSoft =>.JavaSoft
HKCU\SOFTWARE\JMG
HKCU\SOFTWARE\KasperskyLabSetup =>.Kaspersky Labs
HKCU\SOFTWARE\Khronos =>.Khronos
HKCU\SOFTWARE\LaRuina

HKCU\SOFTWARE\Lavasoft =>.Lavasoft
HKCU\SOFTWARE\Litecoin
HKCU\SOFTWARE\Litecoin Core (64-bit)
HKCU\SOFTWARE\Logitech =>.Logitech
HKCU\SOFTWARE\LVGameDev LLC
HKCU\SOFTWARE\Macromedia =>.Macromedia
HKCU\SOFTWARE\MaximumSoft
HKCU\SOFTWARE\McAfee =>.McAfee Inc.
HKCU\SOFTWARE\Meltytech =>.Meltytech LLC
HKCU\SOFTWARE\Mercury32
HKCU\SOFTWARE\ModManager
HKCU\SOFTWARE\Mozilla =>.Mozilla
HKCU\SOFTWARE\Mythical
HKCU\SOFTWARE\Netscape =>.Netscape
HKCU\SOFTWARE\NTSCorp =>.NTSCorp Ltd
HKCU\SOFTWARE\NVIDIA Corporation =>.nVidia Corporation
HKCU\SOFTWARE\nwjs =>.NW.js
HKCU\SOFTWARE\ODBC =>.DB Connectivity Solutions
HKCU\SOFTWARE\oneClickRoot =>.OneClickRoot
HKCU\SOFTWARE\OpenAutomate =>.nVidia Corporation
HKCU\SOFTWARE\Opera Software =>.Opera Software
HKCU\SOFTWARE\Oracle =>.Oracle
HKCU\SOFTWARE\Oxymoron Games
HKCU\SOFTWARE\paint.net =>.Rick Brewster
HKCU\SOFTWARE\Paradox Interactive =>.Paradox Interactive
HKCU\SOFTWARE\PhotoFiltre =>.Antonio Da Cruz
HKCU\SOFTWARE\PhotoFiltre 7 =>.Antonio Da Cruz
HKCU\SOFTWARE\Piriform =>.Piriform
HKCU\SOFTWARE\Playsport Games =>.Playsport Games
HKCU\SOFTWARE\PlayWay
HKCU\SOFTWARE\Plex, Inc. =>.Plex, Inc.
HKCU\SOFTWARE\PowerISO =>.PowerISO Computing
HKCU\SOFTWARE\QtProject =>.QtProject
HKCU\SOFTWARE\Realtek =>.Realtek Semiconductor Corp.
HKCU\SOFTWARE\Red Dot Games =>.Red Dot Games
HKCU\SOFTWARE\Reflect Studios
HKCU\SOFTWARE\RegisteredApplications =>.Microsoft Corporation
HKCU\SOFTWARE\Samsung =>.Samsung Electronics
HKCU\SOFTWARE\SaurikIT =>.SaurikIT, LLC
HKCU\SOFTWARE\ScriptHookV
HKCU\SOFTWARE\SeriesMakers
HKCU\SOFTWARE\Soccer Manager Ltd
HKCU\SOFTWARE\SomaSim
HKCU\SOFTWARE\Squeaky Wheel =>PUP.Optional.Squeaky
HKCU\SOFTWARE\SyncEngines =>.Microsoft Corporation
HKCU\SOFTWARE\Tangentix =>.Tangentix
HKCU\SOFTWARE\TeamViewer =>.TeamViewer GmbH
HKCU\SOFTWARE\Techland =>.Techland
HKCU\SOFTWARE\Tencent =>.Tencent
HKCU\SOFTWARE\TGInstallStatus
HKCU\SOFTWARE\The Irregular Corp
HKCU\SOFTWARE\Toplitz Productions
HKCU\SOFTWARE\Trolltech =>.Trolltech
HKCU\SOFTWARE\Twitch Desktop =>.Twitch
HKCU\SOFTWARE\Two Point Studios
HKCU\SOFTWARE\U-Play online =>.Legitimate
HKCU\SOFTWARE\Ubisoft =>.Ubisoft
HKCU\SOFTWARE\Ultracopier =>.Herman Brule
HKCU\SOFTWARE\Unity =>.Unity
HKCU\SOFTWARE\Unknown Worlds =>.Unknown Worlds
HKCU\SOFTWARE\Vaibhav Pandey
HKCU\SOFTWARE\Valve =>.Valve
HKCU\SOFTWARE\VB and VBA Program Settings =>.Microsoft Corporation
HKCU\SOFTWARE\Vitalwerks =>.Vitalwerks
HKCU\SOFTWARE\Website Ripper Copier
HKCU\SOFTWARE\weltenbauer. Software Entwicklung GmbH
HKCU\SOFTWARE\WinHTTrack Website Copier =>.Xavier Roche
HKCU\SOFTWARE\WinRAR =>.WinRAR
HKCU\SOFTWARE\WinRAR SFX =>.RarLab
HKCU\SOFTWARE\Wireshark =>.Wireshark
HKCU\SOFTWARE\Wonderbox Games
HKCU\SOFTWARE\Wondershare =>.Wondershare
HKCU\SOFTWARE\Wow6432Node =>.Microsoft Corporation
HKCU\SOFTWARE\ZHP =>.Nicolas Coolman
HKU\.DEFAULT\SOFTWARE\7-Zip =>.Igor Pavlov
HKU\.DEFAULT\SOFTWARE\AVAST Software =>.AVAST Software
HKU\.DEFAULT\SOFTWARE\Avira =>.Avira
HKU\.DEFAULT\SOFTWARE\Canon =>.Canon
HKU\.DEFAULT\SOFTWARE\Dropbox =>.Dropbox
HKU\.DEFAULT\SOFTWARE\ESET =>.ESET
HKU\.DEFAULT\SOFTWARE\HP =>.HP
HKU\.DEFAULT\SOFTWARE\Intel =>.Intel
HKU\.DEFAULT\SOFTWARE\IObit =>.IObit
HKU\.DEFAULT\SOFTWARE\McAfee =>.McAfee Inc.
HKU\.DEFAULT\SOFTWARE\Mozilla =>.Mozilla
HKU\.DEFAULT\SOFTWARE\Netscape =>.Netscape
HKU\.DEFAULT\SOFTWARE\Nico Mak Computing =>.Nico Mak Computing
HKU\.DEFAULT\SOFTWARE\NVIDIA Corporation =>.nVidia Corporation
HKU\.DEFAULT\SOFTWARE\Piriform =>.Piriform
HKU\.DEFAULT\SOFTWARE\Plex, Inc. =>.Plex, Inc.
HKU\.DEFAULT\SOFTWARE\SetID =>.Bitdefender
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\681da0eb-374d-5be1-94a8-a3b514928885 =>Adware.CrossRider
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\7-Zip =>.Igor Pavlov
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\A-PDF =>.A-PDF Software
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Adobe =>.Adobe
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Akeo Consulting =>.Akeo Consulting
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Android Open Source Project =>.Open Source
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\APK Editor Studio
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Apoapsis Studios
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Apowersoft =>.Apowersoft
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Apple Inc. =>.Apple Inc.
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Astragon =>.Astragon
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Atheros =>.Qualcomm Atheros
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Avast Software =>.AVAST Software

HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\AvastAdSDK =>.Avast Software s.r.o
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Avira =>.Avira
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Bimesoft =>.Bimesoft
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Bitcoin
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Bitdefender VPN =>.Bitdefender
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\BitTorrent =>.BitTorrent (P2P)
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Blizzard Entertainment =>.Blizzard Entertainment
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\BlueStacksInstaller
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Bohemia Interactive =>.Bohemia Interactive
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Brackets =>.Brackets
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Browser Cleanup =>.Avast Software s.r.o
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\BugSplat =>.Bugsplat Game
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Cain
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Canon =>.Canon
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Cheat Engine =>.Dark Byte
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Chromium =>.Chromium
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\CodeBlocks =>.CodeBlocks Team
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Colossal Order =>.Colossal Order
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Coredumping
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\CyberLink =>.CyberLink Corporation
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Cygwin =>.Cygwin
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Cyotek =>.Cyotek
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Dapper Penguin Studios
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Dashlane_profiles =>.Dashlane, Inc
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\DC3_FEXEC =>Trojan.Fynloski
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\DefaultCompany =>.Unity
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Dell =>.Dell
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\DriverHub
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Dropbox =>.Dropbox
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\DropboxUpdate =>.Dropbox Inc.
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\DuoDianApp =>.DuoDianApp
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Eggcode
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Electronic Arts =>.Electronic Arts
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\emagmaker
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Empyrean
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Epic Games =>.Epic Games
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\EPSON =>.EPSON
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\FastDataX =>Adware.FastDataX
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\FlipBuilder =>.FlipBuilder
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\FreeGrabApp =>.FreeGrabApp
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Glarysoft =>.GlarySoft
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\GNU =>.GNU
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\GOG.com =>.GOG.com
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Google =>.Google
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Gyazo =>.Nota Inc.
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Haemimont Games =>.Haemimont Games
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Hewlett-Packard =>.Hewlett-Packard
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\HP =>.HP
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Intel Corporation =>.Intel Corporation
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\JavaSoft =>.JavaSoft
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\JMG
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\KasperskyLabSetup =>.Kaspersky Labs
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Khronos =>.Khronos
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\LaRuina
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Lavasoft =>.Lavasoft
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Litecoin
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Litecoin Core (64-bit)
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Logitech =>.Logitech
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\LVGameDev LLC
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Macromedia =>.Macromedia
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\MaximumSoft
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\McAfee =>.McAfee Inc.
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Meltytech =>.Meltytech LLC
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Mercury32
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\ModManager
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Mozilla =>.Mozilla
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Mythical
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Netscape =>.Netscape
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\NTSCorp =>.NTSCorp Ltd
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\NVIDIA Corporation =>.nVidia Corporation
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\nwjs =>.NW.js
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\ODBC =>.DB Connectivity Solutions
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\oneClickRoot =>.OneClickRoot
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\OpenAutomate =>.nVidia Corporation
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Opera Software =>.Opera Software
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Oracle =>.Oracle
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Oxymoron Games
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\paint.net =>.Rick Brewster
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Paradox Interactive =>.Paradox Interactive
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\PhotoFiltre =>.Antonio Da Cruz
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\PhotoFiltre 7 =>.Antonio Da Cruz
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Piriform =>.Piriform
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Playsport Games =>.Playsport Games
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\PlayWay
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Plex, Inc. =>.Plex, Inc.
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\PowerISO =>.PowerISO Computing
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\QtProject =>.QtProject
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Realtek =>.Realtek Semiconductor Corp.
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Red Dot Games =>.Red Dot Games
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Reflect Studios
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\RegisteredApplications =>.Microsoft Corporation
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Samsung =>.Samsung Electronics
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\SaurikIT =>.SaurikIT, LLC
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\ScriptHookV
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\SeriesMakers
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Soccer Manager Ltd
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\SomaSim
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Squeaky Wheel =>PUP.Optional.Squeaky
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\SyncEngines =>.Microsoft Corporation
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Tangentix =>.Tangentix
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\TeamViewer =>.TeamViewer GmbH
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Techland =>.Techland
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Tencent =>.Tencent
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\TGInstallStatus

HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\The Irregular Corp
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Toplitz Productions
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Trolltech =>.Trolltech
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Twitch Desktop =>.Twitch
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Two Point Studios
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\U-Play online =>.Legitimate
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Ubisoft =>.Ubisoft
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Ultracopier =>.Herman Brule
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\undefined =>.SUP.Downloader
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Unity =>.Unity
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Unknown Worlds =>.Unknown Worlds
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Vaibhav Pandey
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Valve =>.Valve
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\VB and VBA Program Settings =>.Microsoft Corporation
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Vitalwerks =>.Vitalwerks
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Website Ripper Copier
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\weltenbauer. Software Entwicklung GmbH
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\WinHTTrack Website Copier =>.Xavier Roche
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\WinRAR =>.WinRAR
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\WinRAR SFX =>.RarLab
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Wireshark =>.Wireshark
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Wonderbox Games
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Wondershare =>.Wondershare
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\Wow6432Node =>.Microsoft Corporation
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\SOFTWARE\ZHP =>.Nicolas Coolman

---\ PACKAGES (22) - 0s
C:\Program Files (x86)\WindowsApps\2691AnsgarBeckerSoftwareD.19284136982C_11.1.0.0_x86__peg9cky9b9hfj - (..) [][HeidiSQL]
C:\Program Files (x86)\WindowsApps\2FE3CB00.PICSART-PHOTOSTUDIO_9.1.5.0_x64__crhqpqs3x1ygc - (.PicsArt Inc..) [][PicsArt - Photo Studio]
C:\Program Files (x86)\WindowsApps\34791E63.CanonInkjetPrintUtility_2.9.0.1_neutral__6e5tt8cgb93ep - (.Canon Inc..) [][Canon Inkjet Print Utility] =>
C:\Program Files (x86)\WindowsApps\4DF9E0F8.Netflix_6.97.752.0_x64__mcm4njqhnhss8 - (.Netflix.) [][Netflix] =>Netflix
C:\Program Files (x86)\WindowsApps\89006A2E.AutodeskSketchBook_5.1.0.0_x64__tf1gferkr813w - (.Autodesk Inc..) [][Autodesk SketchBook] =>Autodesk Inc
C:\Program Files (x86)\WindowsApps\AD2F1837.HPJumpStart_1.2.378.0_x64__v10z8vjag6ke6 - (.HP Inc..) [][HP JumpStart] =>HP Inc.
C:\Program Files (x86)\WindowsApps\AD2F1837.HPPCHardwareDiagnosticsWindows_1.6.7.0_x64__v10z8vjag6ke6 - (.Hewlett-Packard.) [][HP PC Hardware Diagnost
C:\Program Files (x86)\WindowsApps\AD2F1837.HPPrinterControl_121.1.193.0_x64__v10z8vjag6ke6 - (.Hewlett-Packard.) [][HP Smart] =>Hewlett-Packard
C:\Program Files (x86)\WindowsApps\AD2F1837.HPPrivacySettings_1.0.39.0_x64__v10z8vjag6ke6 - (.HP Inc..) [][HP Privacy Settings] =>HP Inc.
C:\Program Files (x86)\WindowsApps\AD2F1837.HPSupportAssistant_9.6.839.0_x64__v10z8vjag6ke6 - (.Hewlett-Packard.) [][HP Support Assistant] =>Hewlett-
C:\Program Files (x86)\WindowsApps\AD2F1837.HPSystemEventUtility_1.1.21.0_x64__v10z8vjag6ke6 - (.Hewlett-Packard.) [][HP System Event Utility] =>Hewl
C:\Program Files (x86)\WindowsApps\AD2F1837.OMENCommandCenter_11.0.11.0_x64__v10z8vjag6ke6 - (..) [][OMEN Gaming Hub]
C:\Program Files (x86)\WindowsApps\Appgeneration.myTunerRadio_1.4.0.0_x64__ctqvr9qvqkbd6 - (.APPGENERATION SOFTWARE TECHNOLOGIES LDA.) [][myTuner Radi
C:\Program Files (x86)\WindowsApps\CAF9E577.Plex_3.2.20.0_x64__aam28m9va5cke - (.Plex.) [][Plex] =>Plex
C:\Program Files (x86)\WindowsApps\Deezer.62021768415AF_4.28.0.0_x86__q7m17pa7q8kj0 - (.Deezer.) [][Deezer Music] =>Deezer
C:\Program Files (x86)\WindowsApps\DolbyLaboratories.DolbyAccess_3.6.181.0_x64__rz1tebttyb220 - (.Dolby Laboratories.) [][Dolby Access] =>Dolby Labor
C:\Program Files (x86)\WindowsApps\MicrosoftWindows.Client.CBS_120.2212.31.0_x64__cw5n1h2txyewy - (.Microsoft Corporation.) [][Windows Feature Experie
C:\Program Files (x86)\WindowsApps\MicrosoftWindows.UndockedDevKit_10.0.19041.423_neutral_neutral_cw5n1h2txyewy - (.Microsoft Corporation.) [][UDK Pac
C:\Program Files (x86)\WindowsApps\NcsiUwpApp_1000.19041.423.0_neutral_neutral_8wekyb3d8bbwe - (.Microsoft.) [][NcsiUwpApp] =>Microsoft
C:\Program Files (x86)\WindowsApps\NRJ.ChrieFM_1.1.0.8_neutral__js6xree90qvwe - (.NRJ-AUDIO.) [][Chérie FM] =>NRJ-AUDIO
C:\Program Files (x86)\WindowsApps\Ookla.SpeedtestbyOokla_1.12.132.0_x64__43tkc6nmykmb6 - (.Ookla.) [][Speedtest by Ookla] =>Ookla
C:\Program Files (x86)\WindowsApps\SpotifyAB.SpotifyMusic_1.147.684.0_x86__zpdnekdrzrea0 - (.Spotify.) [][Spotify Music] =>Spotify

---\ CONTENU DES DOSSIERS PROGRAMMES (812) - 50s
O43 - CFD: 15/05/2020 - [] D -- C:\Program Files\Adobe =>.Adobe
O43 - CFD: 20/06/2019 - [] D -- C:\Program Files\APK Easy Tool [Unsigned]
O43 - CFD: 16/05/2020 - [] D -- C:\Program Files\AVAST Software =>.Avast Software s.r.o.®
O43 - CFD: 16/05/2020 - [0] D -- C:\Program Files\Bitdefender =>.Bitdefender
O43 - CFD: 17/02/2020 - [] D -- C:\Program Files\BlueGriffon [Unsigned]
O43 - CFD: 28/06/2019 - [] D -- C:\Program Files\Bonjour =>.Apple Inc.
O43 - CFD: 03/12/2020 - [] D -- C:\Program Files\CCleaner =>.Piriform Ltd
O43 - CFD: 04/10/2020 - [] D -- C:\Program Files\Cheat Engine 7.0 =>.Dark Byte
O43 - CFD: 02/06/2020 - [] D -- C:\Program Files\Common Files =>.Microsoft Corporation
O43 - CFD: 30/01/2019 - [] D -- C:\Program Files\CrystalDiskMark5 =>.Crystal Dew World
O43 - CFD: 29/06/2019 - [] D -- C:\Program Files\Dell =>.Dell
O43 - CFD: 26/12/2019 - [] D -- C:\Program Files\DIFX =>.Microsoft Corporation
O43 - CFD: 27/06/2019 - [] D -- C:\Program Files\dotnet =>.Microsoft Corporation®
O43 - CFD: 23/01/2019 - [] D -- C:\Program Files\DriversCloud.com =>.Cybelsoft
O43 - CFD: 23/08/2018 - [] D -- C:\Program Files\DTS =>.DTS
O43 - CFD: 23/08/2018 - [0] SHD -- C:\Program Files\Fichiers communs =>.Microsoft Corporation
O43 - CFD: 28/03/2020 - [] D -- C:\Program Files\File Magic =>SUP.Optional.Solvusoft
O43 - CFD: 17/02/2020 - [] D -- C:\Program Files\FileZilla FTP Client =>.Tim Kosse
O43 - CFD: 02/12/2020 - [] D -- C:\Program Files\Firefox Developer Edition =>.Mozilla Corporation®
O43 - CFD: 03/12/2020 - [] D -- C:\Program Files\Google =>.Google LLC®
O43 - CFD: 10/09/2019 - [] D -- C:\Program Files\Homeville [Unsigned] =>Adware.DNSUnlocker
O43 - CFD: 14/09/2018 - [] D -- C:\Program Files\HP =>.Hewlett-Packard
O43 - CFD: 09/03/2020 - [] D -- C:\Program Files\HPCommRecovery =>.HP Inc.®
O43 - CFD: 02/06/2020 - [] D -- C:\Program Files\IIS =>.Microsoft Corporation
O43 - CFD: 27/06/2019 - [] D -- C:\Program Files\IIS Express =>.Microsoft Corporation®
O43 - CFD: 02/06/2020 - [] D -- C:\Program Files\Intel =>.Intel Corporation
O43 - CFD: 07/12/2019 - [] D -- C:\Program Files\Internet Explorer =>.Microsoft Corporation
O43 - CFD: 04/11/2019 - [] D -- C:\Program Files\Java =>.Oracle
O43 - CFD: 25/01/2019 - [] D -- C:\Program Files\JetBrains =>.JetBrains Inc
O43 - CFD: 01/07/2019 - [] D -- C:\Program Files\kdenlive [Unsigned]
O43 - CFD: 13/02/2019 - [] D -- C:\Program Files\KMSpico [Unsigned] =>HackTool.KMSpico
O43 - CFD: 13/11/2018 - [] AD -- C:\Program Files\Launcher HeroLife
O43 - CFD: 26/01/2020 - [] D -- C:\Program Files\LGHUB =>.Logitech Inc®
O43 - CFD: 17/09/2019 - [] D -- C:\Program Files\Litecoin [Unsigned]
O43 - CFD: 03/09/2020 - [] D -- C:\Program Files\McAfee =>.McAfee
O43 - CFD: 10/04/2020 - [] D -- C:\Program Files\MegaDev {00A7A7F8DAE29DDB343E15624827840946}.
O43 - CFD: 16/05/2020 - [] D -- C:\Program Files\Microsoft Office =>.Microsoft Corporation
O43 - CFD: 11/01/2019 - [] D -- C:\Program Files\Microsoft SQL Server Compact Edition =>.Microsoft Corporation
O43 - CFD: 11/01/2019 - [] D -- C:\Program Files\Microsoft Synchronization Services =>.Microsoft Corporation
O43 - CFD: 07/12/2019 - [0] D -- C:\Program Files\ModifiableWindowsApps =>.Microsoft Corporation
O43 - CFD: 02/12/2020 - [] D -- C:\Program Files\Mozilla Firefox =>.Mozilla
O43 - CFD: 02/06/2020 - [] D -- C:\Program Files\MSBuild =>.Microsoft Corporation
O43 - CFD: 12/11/2020 - [] D -- C:\Program Files\NVIDIA Corporation =>.nVidia Corporation
O43 - CFD: 21/01/2019 - [] D -- C:\Program Files\NzIxNzgxMWJm
O43 - CFD: 23/08/2018 - [] D -- C:\Program Files\obs-studio =>.OBS-Studio
O43 - CFD: 14/09/2018 - [] RD -- C:\Program Files\Online Services =>.Hewlett-Packard
O43 - CFD: 15/01/2019 - [] D -- C:\Program Files\Oracle =>.Oracle
O43 - CFD: 20/06/2019 - [] D -- C:\Program Files\paint.net =>.Rick Brewster
O43 - CFD: 30/08/2018 - [] AD -- C:\Program Files\PBO Manager v.1.4 beta [Unsigned]
O43 - CFD: 03/09/2020 - [] D -- C:\Program Files\PowerISO =>.PowerISO Computing
O43 - CFD: 02/06/2020 - [] D -- C:\Program Files\Realtek =>.Realtek
O43 - CFD: 02/06/2020 - [] D -- C:\Program Files\Reference Assemblies =>.Microsoft Corporation
O43 - CFD: 23/09/2019 - [] AD -- C:\Program Files\rempl =>.Microsoft Corporation

```
O43 - CFD: 06/10/2019 - [] D -- C:\Program Files\Rockstar Games  =>.Rockstar Games, Inc.®
O43 - CFD: 25/06/2019 - [] D -- C:\Program Files\Samsung  =>.Samsung Electronics
O43 - CFD: 06/02/2019 - [] D -- C:\Program Files\Speccy  =>.Piriform
O43 - CFD: 08/11/2020 - [] D -- C:\Program Files\Streamlabs OBS  =>.Streamlabs (General Workings, Inc.)®
O43 - CFD: 12/05/2019 - [] DC -- C:\Program Files\Sublime Text 3  =>.Sublime HQ Pty Ltd®
O43 - CFD: 26/11/2020 - [] AD -- C:\Program Files\TeamSpeak 3 Client  =>.TeamSpeak
O43 - CFD: 02/02/2019 - [] D -- C:\Program Files\Tensons [Unsigned]
O43 - CFD: 17/10/2020 - [] D -- C:\Program Files\TerannForLife Launcher [Unsigned]
O43 - CFD: 18/03/2017 - [0] HD -- C:\Program Files\Uninstall Information  =>.Microsoft Corporation
O43 - CFD: 02/06/2020 - [] D -- C:\Program Files\UNP  =>.Microsoft Corporation
O43 - CFD: 17/01/2019 - [] D -- C:\Program Files\USBPcap  =>.Desowin
O43 - CFD: 23/08/2018 - [] D -- C:\Program Files\VideoLAN  =>.VideoLan Team
O43 - CFD: 09/06/2019 - [] D -- C:\Program Files\WeMod  =>.Daring Development Inc.®
O43 - CFD: 02/06/2020 - [] D -- C:\Program Files\Windows Defender  =>.Microsoft Corporation
O43 - CFD: 15/07/2020 - [] D -- C:\Program Files\Windows Mail  =>.Microsoft Corporation
O43 - CFD: 13/06/2020 - [] 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: 02/06/2020 - [] D -- C:\Program Files\Windows NT  =>.Microsoft Corporation
O43 - CFD: 13/06/2020 - [] 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: 03/12/2020 - [] HD -- C:\Program Files\WindowsApps  =>.Microsoft Corporation
O43 - CFD: 07/12/2019 - [] D -- C:\Program Files\WindowsPowerShell  =>.Microsoft Corporation
O43 - CFD: 04/11/2019 - [] D -- C:\Program Files\Wireshark  =>.Wireshark
O43 - CFD: 31/05/2020 - [] D -- C:\Program Files\Wondershare  =>.Wondershare
O43 - CFD: 27/10/2018 - [] D -- C:\Program Files (x86)\3dm_game_files
O43 - CFD: 13/03/2019 - [] AD -- C:\Program Files (x86)\7-Zip  =>.Igor Pavlov
O43 - CFD: 15/05/2020 - [] D -- C:\Program Files (x86)\Adobe  =>.Adobe Inc.®
O43 - CFD: 05/07/2020 - [] D -- C:\Program Files (x86)\AirDroid  =>.AirDroid
O43 - CFD: 26/03/2020 - [] D -- C:\Program Files (x86)\Amazing Audio Player  =>.Magic Hills Pty Ltd®
O43 - CFD: 19/01/2020 - [] D -- C:\Program Files (x86)\AnyDesk  =>.philandro Software GmbH
O43 - CFD: 03/12/2020 - [] D -- C:\Program Files (x86)\AOMEI Backupper  =>.AOMEI Tech Co
O43 - CFD: 10/05/2020 - [] D -- C:\Program Files (x86)\APK Editor Studio [Unsigned]
O43 - CFD: 04/06/2020 - [] D -- C:\Program Files (x86)\Apowersoft  =>.Apowersoft
O43 - CFD: 06/11/2020 - [] D -- C:\Program Files (x86)\ArmA3Sync [Unsigned]
O43 - CFD: 06/02/2019 - [] AD -- C:\Program Files (x86)\Aurelius Launcher
O43 - CFD: 22/02/2020 - [] D -- C:\Program Files (x86)\Avira  =>.Avira Software
O43 - CFD: 29/01/2020 - [] D -- C:\Program Files (x86)\Battle.net  =>.Games Software
O43 - CFD: 10/09/2019 - [] D -- C:\Program Files (x86)\bernasconi
O43 - CFD: 22/06/2020 - [] D -- C:\Program Files (x86)\Bignox  =>.BigNox
O43 - CFD: 07/02/2019 - [] D -- C:\Program Files (x86)\BlueGriffon [Unsigned]
O43 - CFD: 28/06/2019 - [] D -- C:\Program Files (x86)\Bonjour  =>.Apple Inc.
O43 - CFD: 05/05/2020 - [] D -- C:\Program Files (x86)\Brackets  =>.Adobe Inc.®
O43 - CFD: 02/07/2020 - [] D -- C:\Program Files (x86)\Cain [Unsigned]
O43 - CFD: 04/10/2020 - [] D -- C:\Program Files (x86)\Cheat Engine 6.8.3  =>.Dark Byte
O43 - CFD: 29/06/2019 - [] D -- C:\Program Files (x86)\ClockworkMod  =>.ClockworkMod
O43 - CFD: 18/01/2019 - [] D -- C:\Program Files (x86)\CodeBlocks  =>.CodeBlocks Team
O43 - CFD: 09/09/2020 - [] D -- C:\Program Files (x86)\Common Files  =>.Microsoft Corporation
O43 - CFD: 30/01/2019 - [] D -- C:\Program Files (x86)\CrystalDiskInfo  =>.Crystal Dew World
O43 - CFD: 02/02/2019 - [] D -- C:\Program Files (x86)\Cyotek {0082E3575D491A060D54453B7B0AB1AB01}.  =>.Cyotek
O43 - CFD: 03/12/2020 - [] D -- C:\Program Files (x86)\Dropbox  =>.Dropbox, Inc®
O43 - CFD: 27/03/2020 - [] D -- C:\Program Files (x86)\EasyAntiCheat  =>.EasyAntiCheat
O43 - CFD: 30/01/2020 - [] AD -- C:\Program Files (x86)\Epic Games  =>.Epic Games
O43 - CFD: 18/09/2018 - [] D -- C:\Program Files (x86)\EPSON  =>.SEIKO EPSON CORPORATION®
O43 - CFD: 25/12/2018 - [0] D -- C:\Program Files (x86)\Farm Manager 2018
O43 - CFD: 11/09/2019 - [] D -- C:\Program Files (x86)\FastDataX [Unsigned]  =>Adware.FastDataX
O43 - CFD: 19/09/2019 - [] D -- C:\Program Files (x86)\FlipBook Creator
O43 - CFD: 10/02/2019 - [] D -- C:\Program Files (x86)\Free Flash eBook Maker [Unsigned]
O43 - CFD: 03/12/2020 - [] D -- C:\Program Files (x86)\Glary Utilities 5  =>.GlarySoft
O43 - CFD: 19/01/2019 - [] D -- C:\Program Files (x86)\Glorylogic [Unsigned]  =>.Glorylogic
O43 - CFD: 01/01/2019 - [] D -- C:\Program Files (x86)\GNU [Unsigned]  =>.GNU
O43 - CFD: 03/12/2020 - [] D -- C:\Program Files (x86)\Google  =>.Google LLC®
O43 - CFD: 05/08/2019 - [] AD -- C:\Program Files (x86)\Gyazo  =>.Toshiyuki Masui
O43 - CFD: 12/02/2019 - [] D -- C:\Program Files (x86)\Hewlett-Packard  =>.Hewlett-Packard
O43 - CFD: 08/07/2019 - [] AD -- C:\Program Files (x86)\HP  =>.Hewlett-Packard
O43 - CFD: 27/06/2019 - [] D -- C:\Program Files (x86)\IIS  =>.Microsoft Corporation
O43 - CFD: 27/06/2019 - [] D -- C:\Program Files (x86)\IIS Express  =>.Microsoft Corporation®
O43 - CFD: 19/01/2019 - [] D -- C:\Program Files (x86)\ImageWriter  =>.Legitimate
O43 - CFD: 10/09/2019 - [0] D -- C:\Program Files (x86)\Indians
O43 - CFD: 19/01/2020 - [0] D -- C:\Program Files (x86)\inPixio  =>.InPixio
O43 - CFD: 04/11/2019 - [] HD -- C:\Program Files (x86)\InstallShield Installation Information  =>.InstallShield
O43 - CFD: 03/08/2020 - [] D -- C:\Program Files (x86)\Intel  =>.Intel Corporation
O43 - CFD: 07/12/2019 - [] D -- C:\Program Files (x86)\Internet Explorer  =>.Microsoft Corporation
O43 - CFD: 20/02/2019 - [] D -- C:\Program Files (x86)\IObit  =>.IObit
O43 - CFD: 16/06/2019 - [] D -- C:\Program Files (x86)\Java  =>.Oracle
O43 - CFD: 17/02/2019 - [] D -- C:\Program Files (x86)\Jumpstart  =>.Jumpstart Inc
O43 - CFD: 01/04/2020 - [0] D -- C:\Program Files (x86)\Martens
O43 - CFD: 23/08/2018 - [] D -- C:\Program Files (x86)\MegaDev {00A7A7F8DAE29DDB343E15624827840946}.
O43 - CFD: 14/01/2019 - [] D -- C:\Program Files (x86)\Microleaves  =>SUP.Optional.Microleaves
O43 - CFD: 15/03/2020 - [] D -- C:\Program Files (x86)\Microsoft  =>.Microsoft Corporation
O43 - CFD: 16/05/2020 - [0] AD -- C:\Program Files (x86)\Microsoft Office  =>.Microsoft Corporation
O43 - CFD: 11/01/2019 - [] D -- C:\Program Files (x86)\Microsoft SQL Server Compact Edition  =>.Microsoft Corporation
O43 - CFD: 11/01/2019 - [] D -- C:\Program Files (x86)\Microsoft Synchronization Services  =>.Microsoft Corporation
O43 - CFD: 27/06/2019 - [0] D -- C:\Program Files (x86)\Microsoft Visual Studio  =>.Microsoft Corporation
O43 - CFD: 07/12/2019 - [] D -- C:\Program Files (x86)\Microsoft.NET  =>.Microsoft Corporation
O43 - CFD: 22/06/2020 - [] D -- C:\Program Files (x86)\Microvirt  =>.Shanghai Microvirt Software Technology Co., Ltd.®
O43 - CFD: 25/06/2019 - [] D -- C:\Program Files (x86)\Minimal ADB and Fastboot [Unsigned]
O43 - CFD: 10/09/2019 - [] HD -- C:\Program Files (x86)\motrin
O43 - CFD: 02/12/2020 - [] D -- C:\Program Files (x86)\Mozilla Maintenance Service  =>.Mozilla
O43 - CFD: 02/06/2020 - [] D -- C:\Program Files (x86)\MSBuild  =>.Microsoft Corporation
O43 - CFD: 20/06/2019 - [] D -- C:\Program Files (x86)\My Company Name  =>.My Company Name
O43 - CFD: 12/03/2019 - [] D -- C:\Program Files (x86)\No-IP  =>.No-IP
O43 - CFD: 18/02/2020 - [] D -- C:\Program Files (x86)\Notepad++  =>.Don Ho
O43 - CFD: 23/08/2018 - [] D -- C:\Program Files (x86)\NSIS Uninstall Information  =>.MSIS
O43 - CFD: 12/11/2020 - [] D -- C:\Program Files (x86)\NVIDIA Corporation  =>.nVidia Corporation
O43 - CFD: 14/09/2018 - [] RD -- C:\Program Files (x86)\Online Services  =>.Hewlett-Packard
O43 - CFD: 30/11/2020 - [] AD -- C:\Program Files (x86)\Origin  =>.Electronic Arts, Inc.
O43 - CFD: 13/09/2018 - [0] D -- C:\Program Files (x86)\Origin Games  =>.Electronic Arts, Inc.
O43 - CFD: 01/04/2020 - [0] HD -- C:\Program Files (x86)\Oscars
O43 - CFD: 05/02/2019 - [] D -- C:\Program Files (x86)\PhotoFiltre  =>.Antonio Da Cruz
O43 - CFD: 05/02/2019 - [] D -- C:\Program Files (x86)\PhotoFiltre 7  =>.Antonio Da Cruz
O43 - CFD: 31/10/2019 - [] D -- C:\Program Files (x86)\ProXoft {3DFEDC4BE9CA7167974E822F50867BB1}.
O43 - CFD: 05/11/2020 - [] D -- C:\Program Files (x86)\ProxyGate  =>.SUP.GoldClick
```

```
O43 - CFD: 11/01/2019 - [] D -- C:\Program Files (x86)\Quran Explorer {00AD4CE8B9CBA67D329BCB15612EA5F082}.
O43 - CFD: 04/02/2019 - [] D -- C:\Program Files (x86)\Quranflash Desktop [Unsigned]
O43 - CFD: 02/11/2019 - [] AD -- C:\Program Files (x86)\Realtek  =>.Realtek
O43 - CFD: 23/01/2019 - [] D -- C:\Program Files (x86)\REALTEK RTL8187B Wireless LAN Driver  =>.Realtek Semiconductor Corp.
O43 - CFD: 02/06/2020 - [] D -- C:\Program Files (x86)\Reference Assemblies  =>.Microsoft Corporation
O43 - CFD: 06/10/2019 - [] D -- C:\Program Files (x86)\Rockstar Games  =>.Rockstar Games, Inc.®
O43 - CFD: 02/01/2019 - [] D -- C:\Program Files (x86)\RVL Hacker [Unsigned]
O43 - CFD: 28/06/2019 - [] D -- C:\Program Files (x86)\Samsung  =>.Samsung Electronics
O43 - CFD: 01/04/2020 - [] D -- C:\Program Files (x86)\seconds
O43 - CFD: 23/08/2018 - [] D -- C:\Program Files (x86)\Sony  =>.Sony Interactive Entertainment Inc.®
O43 - CFD: 02/12/2020 - [] D -- C:\Program Files (x86)\Steam  =>.Steam Games
O43 - CFD: 28/11/2019 - [] D -- C:\Program Files (x86)\Supercopier  =>.SFX Team
O43 - CFD: 02/02/2019 - [] D -- C:\Program Files (x86)\SurfOffline Professional 2 [Unsigned]
O43 - CFD: 03/12/2020 - [] AD -- C:\Program Files (x86)\TeamViewer  =>.TeamViewer GmbH
O43 - CFD: 23/08/2018 - [0] HD -- C:\Program Files (x86)\Temp  =>.Microsoft Corporation
O43 - CFD: 23/08/2018 - [] D -- C:\Program Files (x86)\Ubisoft  =>.Ubisoft
O43 - CFD: 19/01/2019 - [] D -- C:\Program Files (x86)\VMware  =>.VMware, Inc.®
O43 - CFD: 10/09/2018 - [] D -- C:\Program Files (x86)\VulkanRT  =>.LunarG, Inc
O43 - CFD: 21/02/2019 - [] D -- C:\Program Files (x86)\WebCopier [Unsigned]
O43 - CFD: 02/06/2020 - [] D -- C:\Program Files (x86)\Windows Defender  =>.Microsoft Corporation
O43 - CFD: 15/07/2020 - [] D -- C:\Program Files (x86)\Windows Mail  =>.Microsoft Corporation
O43 - CFD: 13/06/2020 - [] 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: 13/06/2020 - [] 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: 31/01/2019 - [] D -- C:\Program Files (x86)\WinHTTrack  =>.HTTrack
O43 - CFD: 02/07/2020 - [] D -- C:\Program Files (x86)\WinPcap  =>.Riverbed Technology
O43 - CFD: 03/12/2020 - [] AD -- C:\Program Files (x86)\WinRAR  =>.win.rar GmbH®
O43 - CFD: 03/01/2020 - [] D -- C:\Program Files (x86)\Wondershare  =>.Wondershare
O43 - CFD: 18/05/2019 - [0] D -- C:\Program Files (x86)\WondershareUpdate  =>.Wondershare
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\7-Zip  =>.Igor Pavlov
O43 - CFD: 15/08/2020 - [] 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: 17/10/2020 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools  =>.Administrative Tools
O43 - CFD: 05/07/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\AirDroid  =>.AirDroid
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Amazing Audio Player
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Android Studio  =>.Google Inc.
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\AOMEI Backupper  =>.AOMEI Tech Co
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\APK Editor Studio
O43 - CFD: 04/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Apowersoft  =>.Apowersoft
O43 - CFD: 06/11/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\ArmA3Sync
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Atheros  =>.Qualcomm Atheros
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\AVAST Software  =>.AVAST Software
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Avira  =>.Avira Software
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Battle.net  =>.Games Software
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Binary Viewer
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\BlueGriffon
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\CCleaner  =>.Piriform Ltd
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Cheat Engine 6.8.3  =>.Dark Byte
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Cheat Engine 7.0  =>.Dark Byte
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\CodeBlocks  =>.CodeBlocks Team
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\CrystalDiskInfo  =>.Crystal Dew World
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\CrystalDiskMark5  =>.Crystal Dew World
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Cyotek WebCopy
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\DriversCloud.com  =>.Cybelsoft
O43 - CFD: 03/12/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Dropbox  =>.Dropbox
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\EPSON  =>.EPSON
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\F1 2018  =>.Codemasters
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Farm Manager 2018
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Farming Simulator 19  =>.GIANTS Software
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\FIFA 20  =>.Electronic Arts, Inc.
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\File Magic
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\FileZilla FTP Client  =>.Tim Kosse
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Free Flash eBook Maker
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Frostpunk The Fall of Winterhome
O43 - CFD: 20/09/2018 - [0] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Games  =>.Microsoft Corporation
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Glary Utilities 5  =>.GlarySoft
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Glorylogic  =>.Glorylogic
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Gyazo  =>.Toshiyuki Masui
O43 - CFD: 02/06/2020 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\HP Help and Support  =>.Hewlett-Packard
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Image Writer  =>.Michael Casadevall
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Jarvee
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Java  =>.Oracle
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\JetBrains  =>.JetBrains Inc
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Jurassic World Evolution
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\kdenlive
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\KMSpico  =>HackTool.KMSpico
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Logi
O43 - CFD: 07/12/2019 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Maintenance  =>.Microsoft Corporation
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\MEGAsync  =>.MegaSystems
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\MegaTrainerUltimate  =>.MegaDev
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Minimal ADB and Fastboot
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\NBA 2K19
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\NVIDIA Corporation  =>.nVidia Corporation
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OBS Studio  =>.OBS Studio
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Oracle VM VirtualBox  =>.Oracle
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Origin  =>.Electronic Arts, Inc.
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\PBO Manager
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\PC Building Simulator Razer Workshop
O43 - CFD: 03/09/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\PowerISO  =>.PowerISO Computing
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Prison Architect The Clink
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Project Hospital [GOG.com]
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Quranflash Desktop
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Samsung  =>.Samsung Electronics
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Snaz
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Speccy  =>.Piriform
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Spintires MudRunner American Wilds
O43 - CFD: 18/11/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp  =>.Microsoft Corporation
O43 - CFD: 18/02/2020 - [0] HD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup-Disabled  =>.Microsoft Corporation
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Steam  =>.Steam Games
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Subnautica
```

```
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\SurfOffline Professional 2
O43 - CFD: 17/10/2020 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\System Tools  =>.Microsoft Corporation
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\TDM-GCC-64
O43 - CFD: 25/06/2019 - [0] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\theHunter Call of the Wild  =>.Expansive Worlds
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Tropico 5 [GOG.com]  =>.Kalypso Media
O43 - CFD: 02/09/2019 - [0] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Tropico 6  =>.Kalypso Media
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\TruckersMP Launcher  =>.TruckersMP
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\VideoLAN  =>.VideoLan Team
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Visual Studio 2019  =>.Pinnacle Systems, Inc.
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\VMware  =>.VMware
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Wampserver64  =>.Aestan Software
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\WebCopier
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Website Ripper Copier
O43 - CFD: 07/12/2019 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Windows PowerShell  =>.Microsoft Corporation
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\WinHTTrack  =>.HTTrack
O43 - CFD: 02/07/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\WinPcap  =>.Riverbed Technology
O43 - CFD: 03/12/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\WinRAR  =>.WinRAR
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Wondershare  =>.Wondershare
O43 - CFD: 05/11/2018 - [] D -- C:\ProgramData\.mono  =>.Legitimate
O43 - CFD: 10/02/2019 - [] D -- C:\ProgramData\A-PDF  =>.A-PDF Software
O43 - CFD: 16/05/2020 - [] D -- C:\ProgramData\Adobe  =>.Adobe
O43 - CFD: 05/07/2020 - [] D -- C:\ProgramData\AirDroid  =>.AirDroid
O43 - CFD: 28/06/2019 - [] D -- C:\ProgramData\AnyDesk  =>.philandro Software GmbH
O43 - CFD: 16/02/2019 - [] D -- C:\ProgramData\Aomei  =>.AOMEI Tech Co
O43 - CFD: 26/05/2019 - [] D -- C:\ProgramData\AomeiBR  =>.AOMEI Technology
O43 - CFD: 02/01/2019 - [] D -- C:\ProgramData\Apple  =>.Apple Inc.
O43 - CFD: 02/01/2019 - [] D -- C:\ProgramData\Apple Computer  =>.Apple Inc.
O43 - CFD: 02/06/2020 - [0] SHD -- C:\ProgramData\Application Data  =>.Microsoft Corporation
O43 - CFD: 01/04/2020 - [] D -- C:\ProgramData\Atc
O43 - CFD: 20/01/2019 - [] D -- C:\ProgramData\Atheros  =>.Qualcomm Atheros
O43 - CFD: 03/12/2020 - [] D -- C:\ProgramData\AVAST Software  =>.AVAST Software
O43 - CFD: 22/02/2020 - [] D -- C:\ProgramData\Avira  =>.Avira Software
O43 - CFD: 10/10/2018 - [] D -- C:\ProgramData\Battle.net  =>.Games Software
O43 - CFD: 01/04/2020 - [] D -- C:\ProgramData\BDLogging  =>.Bitdefender
O43 - CFD: 02/02/2019 - [] D -- C:\ProgramData\Bimesoft  =>.Bimesoft
O43 - CFD: 01/04/2020 - [] D -- C:\ProgramData\Bitdefender Agent  =>.Bitdefender
O43 - CFD: 01/04/2020 - [] D -- C:\ProgramData\Bitdefender Device Management  =>.Bitdefender
O43 - CFD: 01/04/2020 - [] D -- C:\ProgramData\Bitdefender VPN  =>.Bitdefender
O43 - CFD: 10/10/2018 - [] D -- C:\ProgramData\Blizzard Entertainment  =>.Blizzard Entertainment
O43 - CFD: 24/08/2018 - [] D -- C:\ProgramData\Bohemia Interactive  =>.Bohemia Interactive
O43 - CFD: 14/01/2019 - [] D -- C:\ProgramData\boost_interprocess  =>.boost.org
O43 - CFD: 23/08/2018 - [0] SHD -- C:\ProgramData\Bureau  =>.Microsoft Corporation
O43 - CFD: 28/09/2018 - [] HD -- C:\ProgramData\CanonBJ  =>.Canon Inc.
O43 - CFD: 07/06/2019 - [] D -- C:\ProgramData\CheatHappens Temp
O43 - CFD: 27/10/2018 - [] D -- C:\ProgramData\Codemasters  =>.Codemasters
O43 - CFD: 04/11/2019 - [] D -- C:\ProgramData\CyberLink  =>.CyberLink Corporation
O43 - CFD: 29/06/2019 - [] D -- C:\ProgramData\Dell  =>.Dell
O43 - CFD: 27/06/2019 - [] D -- C:\ProgramData\dftmp
O43 - CFD: 02/06/2020 - [0] SHD -- C:\ProgramData\Documents  =>.Microsoft Corporation
O43 - CFD: 23/01/2019 - [] D -- C:\ProgramData\DriversCloud.com  =>.Cybelsoft
O43 - CFD: 02/08/2017 - [] D -- C:\ProgramData\Dropbox  =>.Dropbox
O43 - CFD: 13/09/2018 - [] D -- C:\ProgramData\Electronic Arts  =>.Electronic Arts
O43 - CFD: 10/02/2019 - [] D -- C:\ProgramData\emagmaker
O43 - CFD: 30/01/2020 - [] D -- C:\ProgramData\Epic  =>.Epic
O43 - CFD: 18/09/2018 - [] D -- C:\ProgramData\EPSON  =>.EPSON
O43 - CFD: 28/03/2020 - [0] D -- C:\ProgramData\File Magic
O43 - CFD: 20/02/2019 - [] D -- C:\ProgramData\flipBook
O43 - CFD: 10/02/2019 - [] D -- C:\ProgramData\FlipBook Creator
O43 - CFD: 27/10/2018 - [] D -- C:\ProgramData\Frontier Developments  =>.Frontier Developments
O43 - CFD: 01/04/2020 - [] D -- C:\ProgramData\Gemma
O43 - CFD: 04/02/2019 - [] D -- C:\ProgramData\GlarySoft  =>.GlarySoft
O43 - CFD: 01/11/2018 - [] D -- C:\ProgramData\GOG.com  =>.GOG.com
O43 - CFD: 18/05/2019 - [] D -- C:\ProgramData\GraphicsType
O43 - CFD: 10/10/2018 - [] D -- C:\ProgramData\Gyazo  =>.Toshiyuki Masui
O43 - CFD: 12/02/2019 - [] D -- C:\ProgramData\Hewlett-Packard  =>.Hewlett-Packard
O43 - CFD: 10/09/2020 - [] AD -- C:\ProgramData\HP  =>.Hewlett-Packard
O43 - CFD: 04/11/2019 - [0] D -- C:\ProgramData\install_backup
O43 - CFD: 23/08/2018 - [] D -- C:\ProgramData\install_clap  =>.Microsoft Corporation
O43 - CFD: 14/09/2018 - [] D -- C:\ProgramData\Intel  =>.Intel Corporation
O43 - CFD: 20/02/2019 - [] D -- C:\ProgramData\IObit  =>.IObit
O43 - CFD: 18/12/2018 - [] D -- C:\ProgramData\IsolatedStorage  =>.id Software
O43 - CFD: 20/06/2019 - [] D -- C:\ProgramData\Kaspersky Lab  =>.Kaspersky Lab
O43 - CFD: 20/06/2019 - [] D -- C:\ProgramData\Kaspersky Lab Setup Files  =>.Kaspersky Lab
O43 - CFD: 13/09/2019 - [] D -- C:\ProgramData\KONAMI  =>.Konami
O43 - CFD: 08/12/2019 - [] D -- C:\ProgramData\LGHUB
O43 - CFD: 28/11/2018 - [] D -- C:\ProgramData\LogiShrd  =>.Logitech Inc.
O43 - CFD: 03/09/2020 - [] D -- C:\ProgramData\McAfee  =>.McAfee
O43 - CFD: 23/09/2018 - [] D -- C:\ProgramData\MEGAsync  =>.MegaSystems
O43 - CFD: 07/03/2019 - [] D -- C:\ProgramData\MegaTrainerUltimate  =>.MegaDev
O43 - CFD: 23/08/2018 - [0] SHD -- C:\ProgramData\Menu Démarrer  =>.Microsoft Corporation
O43 - CFD: 12/11/2020 - [] SD -- C:\ProgramData\Microsoft  =>.Microsoft Corporation
O43 - CFD: 16/05/2020 - [] D -- C:\ProgramData\Microsoft Help  =>.Microsoft Corporation
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\Microsoft OneDrive  =>.Microsoft Corporation
O43 - CFD: 27/06/2019 - [] D -- C:\ProgramData\Microsoft Visual Studio  =>.Microsoft Corporation
O43 - CFD: 23/08/2018 - [0] SHD -- C:\ProgramData\Modèles  =>.Microsoft Corporation
O43 - CFD: 03/12/2020 - [] D -- C:\ProgramData\Mozilla  =>.Mozilla Corporation
O43 - CFD: 01/01/2019 - [] D -- C:\ProgramData\NordVpn  =>.NordVPN
O43 - CFD: 19/01/2019 - [] D -- C:\ProgramData\Norton  =>.Symantec Corporation
O43 - CFD: 14/01/2019 - [] D -- C:\ProgramData\NortonInstaller  =>.Symantec
O43 - CFD: 03/12/2020 - [] D -- C:\ProgramData\NVIDIA  =>.nVidia Corporation
O43 - CFD: 12/11/2020 - [] D -- C:\ProgramData\NVIDIA Corporation  =>.nVidia Corporation
O43 - CFD: 23/06/2020 - [] D -- C:\ProgramData\obs-studio-hook
O43 - CFD: 19/06/2019 - [] D -- C:\ProgramData\Oracle  =>.Oracle
O43 - CFD: 09/09/2020 - [] D -- C:\ProgramData\Origin  =>.Electronic Arts, Inc.
O43 - CFD: 20/06/2019 - [] D -- C:\ProgramData\PACE Anti-Piracy  =>.PACE Anti-Piracy
O43 - CFD: 15/05/2020 - [] D -- C:\ProgramData\Package Cache  =>.Microsoft Corporation
O43 - CFD: 02/12/2020 - [] D -- C:\ProgramData\Packages  =>.Microsoft Corporation
O43 - CFD: 20/02/2019 - [] D -- C:\ProgramData\ProductData  =>.Microsoft Corporation
O43 - CFD: 02/11/2019 - [] D -- C:\ProgramData\Realtek  =>.Realtek
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\regid.1986-12.com.adobe  =>.Adobe Inc.
O43 - CFD: 03/12/2020 - [] D -- C:\ProgramData\regid.1991-06.com.microsoft  =>.Microsoft Corporation
O43 - CFD: 06/10/2019 - [] D -- C:\ProgramData\Rockstar Games  =>.Rockstar Games
O43 - CFD: 29/06/2019 - [] D -- C:\ProgramData\Samsung  =>.Samsung Electronics
O43 - CFD: 07/12/2019 - [0] D -- C:\ProgramData\SoftwareDistribution  =>.Microsoft Corporation
```

```
O43 - CFD: 23/08/2018 - [] D -- C:\ProgramData\SRS Labs  =>.SRS Labs
O43 - CFD: 11/05/2020 - [0] D -- C:\ProgramData\ssh  =>.Microsoft Corporation
O43 - CFD: 04/11/2019 - [] D -- C:\ProgramData\SUPPORTDIR  =>.Microsoft Corporation
O43 - CFD: 17/01/2019 - [] D -- C:\ProgramData\TDM-GCC
O43 - CFD: 04/11/2019 - [] D -- C:\ProgramData\Temp  =>.Microsoft Corporation
O43 - CFD: 27/12/2019 - [] D -- C:\ProgramData\TruckersMP  =>.TruckersMP
O43 - CFD: 23/08/2018 - [] D -- C:\ProgramData\Twitch  =>.Twitch
O43 - CFD: 13/12/2019 - [] D -- C:\ProgramData\Ubisoft  =>.Ubisoft
O43 - CFD: 20/12/2018 - [] D -- C:\ProgramData\UniqueId  =>.Microsoft Corporation
O43 - CFD: 13/01/2019 - [] D -- C:\ProgramData\Unknown Worlds
O43 - CFD: 02/06/2020 - [] D -- C:\ProgramData\USOPrivate  =>.Microsoft Corporation
O43 - CFD: 07/12/2019 - [] D -- C:\ProgramData\USOShared  =>.Microsoft Corporation
O43 - CFD: 07/08/2019 - [] D -- C:\ProgramData\VirtualBox  =>.Oracle
O43 - CFD: 03/12/2020 - [] D -- C:\ProgramData\VMware  =>.VMware
O43 - CFD: 09/06/2019 - [] D -- C:\ProgramData\WeMod  =>.WeMod
O43 - CFD: 07/12/2019 - [] D -- C:\ProgramData\WindowsHolographicDevices  =>.Microsoft Corporation
O43 - CFD: 03/01/2020 - [] D -- C:\ProgramData\Wondershare  =>.Wondershare
O43 - CFD: 01/09/2020 - [] D -- C:\ProgramData\Wondershare Filmora  =>.Wondershare
O43 - CFD: 18/05/2019 - [] D -- C:\ProgramData\Wondershare MediaServer  =>.Wondershare
O43 - CFD: 01/07/2019 - [] D -- C:\ProgramData\wsr
O43 - CFD: 25/08/2018 - [] D -- C:\ProgramData\X360CE  =>.Microsoft Corporation
O43 - CFD: 14/01/2019 - [] D -- C:\ProgramData\XSoftbet
O43 - CFD: 16/02/2019 - [0] D -- C:\ProgramData\{13CFD044-61E4-4EAC-AD61-02536D961216}
O43 - CFD: 01/10/2019 - [0] D -- C:\ProgramData\{60ABF7CD-EE17-963F-6FF3-BC1A6F14E54B}
O43 - CFD: 18/02/2019 - [0] D -- C:\ProgramData\{BE2ACE5C-32B7-4777-9BDF-ECF87CDAB705}
O43 - CFD: 01/10/2019 - [0] D -- C:\ProgramData\{EFB0B76F-AEB5-1924-CDB3-A795CD54FEC4}
O43 - CFD: 16/05/2020 - [] AD -- C:\Program Files (x86)\Common Files\Adobe  =>.Adobe
O43 - CFD: 20/12/2018 - [] D -- C:\Program Files (x86)\Common Files\Avanquest Software  =>.Avanquest Software
O43 - CFD: 01/12/2020 - [] D -- C:\Program Files (x86)\Common Files\BattlEye  =>.BattlEye
O43 - CFD: 20/02/2019 - [] D -- C:\Program Files (x86)\Common Files\IObit  =>.IObit
O43 - CFD: 16/06/2019 - [] D -- C:\Program Files (x86)\Common Files\Java  =>.Oracle
O43 - CFD: 02/06/2020 - [] D -- C:\Program Files (x86)\Common Files\Microsoft Shared  =>.Microsoft Corporation
O43 - CFD: 16/06/2019 - [] D -- C:\Program Files (x86)\Common Files\Oracle  =>.Oracle
O43 - CFD: 14/09/2018 - [] D -- C:\Program Files (x86)\Common Files\PostureAgent  =>.Microsoft Corporation
O43 - CFD: 20/06/2019 - [] D -- C:\Program Files (x86)\Common Files\PX Storage Engine  =>.Sonic Solutions
O43 - CFD: 07/12/2019 - [] D -- C:\Program Files (x86)\Common Files\Services  =>.Microsoft Corporation
O43 - CFD: 20/06/2019 - [] D -- C:\Program Files (x86)\Common Files\Sonic Shared  =>.Sonic
O43 - CFD: 03/11/2020 - [] D -- C:\Program Files (x86)\Common Files\Steam  =>.Steam Games
O43 - CFD: 15/07/2020 - [] D -- C:\Program Files (x86)\Common Files\System  =>.Microsoft Corporation
O43 - CFD: 19/01/2019 - [] D -- C:\Program Files (x86)\Common Files\ThinPrint  =>.ThinPrint
O43 - CFD: 19/01/2019 - [] D -- C:\Program Files (x86)\Common Files\VMware  =>.VMware
O43 - CFD: 18/05/2019 - [] D -- C:\Program Files (x86)\Common Files\Wondershare  =>.Wondershare
O43 - CFD: 05/11/2018 - [] DC -- C:\Users\couli\AppData\Roaming\.mono  =>.Legitimate
O43 - CFD: 27/10/2018 - [] DC -- C:\Users\couli\AppData\Roaming\2K Sports  =>.2K Sports
O43 - CFD: 05/02/2019 - [] DC -- C:\Users\couli\AppData\Roaming\ActiveState  =>.ActiveState
O43 - CFD: 26/12/2019 - [] D -- C:\Users\couli\AppData\Roaming\ADBDriverInstaller  =>.Samsung Electronics
O43 - CFD: 16/05/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Adobe  =>.Adobe
O43 - CFD: 16/07/2020 - [] D -- C:\Users\couli\AppData\Roaming\AirDroid  =>.AirDroid
O43 - CFD: 25/10/2020 - [] DC -- C:\Users\couli\AppData\Roaming\AnyDesk  =>.philandro Software GmbH
O43 - CFD: 11/07/2020 - [] DC -- C:\Users\couli\AppData\Roaming\apk-editor-studio
O43 - CFD: 13/07/2019 - [] DC -- C:\Users\couli\AppData\Roaming\Apoapsis Studios
O43 - CFD: 04/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Apowersoft  =>.Apowersoft
O43 - CFD: 10/06/2020 - [] D -- C:\Users\couli\AppData\Roaming\Atom
O43 - CFD: 16/05/2020 - [] D -- C:\Users\couli\AppData\Roaming\AVAST Software  =>.AVAST Software
O43 - CFD: 10/10/2018 - [] DC -- C:\Users\couli\AppData\Roaming\Battle.net  =>.Games Software
O43 - CFD: 02/01/2019 - [] DC -- C:\Users\couli\AppData\Roaming\Bitcoin  =>.Bitcoin Core project
O43 - CFD: 17/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Brackets  =>.Brackets
O43 - CFD: 18/01/2019 - [] DC -- C:\Users\couli\AppData\Roaming\CodeBlocks  =>.CodeBlocks Team
O43 - CFD: 18/10/2019 - [] D -- C:\Users\couli\AppData\Roaming\CyberLink  =>.CyberLink Corporation
O43 - CFD: 02/02/2019 - [] DC -- C:\Users\couli\AppData\Roaming\Cyotek  =>.Cyotek
O43 - CFD: 12/03/2019 - [] DC -- C:\Users\couli\AppData\Roaming\dclogs  =>Trojan.StolenData
O43 - CFD: 04/02/2019 - [] DC -- C:\Users\couli\AppData\Roaming\desktop.quranflash
O43 - CFD: 12/10/2020 - [] DC -- C:\Users\couli\AppData\Roaming\discord  =>.GitHub
O43 - CFD: 14/01/2019 - [0] DC -- C:\Users\couli\AppData\Roaming\DiskDefrag  =>SUP.Optional.AuslogicsDiskDefrag
O43 - CFD: 07/02/2019 - [] DC -- C:\Users\couli\AppData\Roaming\Disruptive Innovations SARL  =>.Disruptive Innovations SARL
O43 - CFD: 23/01/2019 - [] DC -- C:\Users\couli\AppData\Roaming\DriverHub
O43 - CFD: 19/12/2019 - [] D -- C:\Users\couli\AppData\Roaming\Dropbox  =>.Dropbox
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Roaming\DropboxOEM  =>.Dropbox Inc.
O43 - CFD: 03/12/2020 - [] DC -- C:\Users\couli\AppData\Roaming\DS4Windows  =>.DSDCS
O43 - CFD: 27/03/2020 - [] D -- C:\Users\couli\AppData\Roaming\EasyAntiCheat  =>.EasyAntiCheat
O43 - CFD: 10/02/2019 - [0] DC -- C:\Users\couli\AppData\Roaming\EurekaLog  =>.EurekaLog
O43 - CFD: 18/02/2020 - [] DC -- C:\Users\couli\AppData\Roaming\FileZilla  =>.FileZilla
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Roaming\FileZilla Server  =>.FileZilla
O43 - CFD: 24/05/2020 - [] D -- C:\Users\couli\AppData\Roaming\FontsNinja
O43 - CFD: 27/11/2019 - [] D -- C:\Users\couli\AppData\Roaming\Frontier Developments  =>.Frontier Developments
O43 - CFD: 17/06/2019 - [] DC -- C:\Users\couli\AppData\Roaming\GlarySoft  =>.GlarySoft
O43 - CFD: 19/01/2019 - [] DC -- C:\Users\couli\AppData\Roaming\Glorylogic  =>.Glorylogic
O43 - CFD: 28/10/2018 - [] DC -- C:\Users\couli\AppData\Roaming\Godot
O43 - CFD: 27/02/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Google  =>.Google
O43 - CFD: 27/08/2018 - [] DC -- C:\Users\couli\AppData\Roaming\Gyazo  =>.Toshiyuki Masui
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Roaming\Hewlett-Packard  =>.Hewlett-Packard
O43 - CFD: 08/07/2019 - [] DC -- C:\Users\couli\AppData\Roaming\HP  =>.Hewlett-Packard
O43 - CFD: 12/02/2019 - [] DC -- C:\Users\couli\AppData\Roaming\hpqLog  =>.Hewlett-Packard
O43 - CFD: 07/03/2020 - [] D -- C:\Users\couli\AppData\Roaming\HP_Easy_Start  =>.Hewlett-Packard
O43 - CFD: 20/01/2019 - [] DC -- C:\Users\couli\AppData\Roaming\InstallShield  =>.InstallShield
O43 - CFD: 20/02/2019 - [] DC -- C:\Users\couli\AppData\Roaming\IObit  =>.IObit
O43 - CFD: 28/03/2020 - [] DC -- C:\Users\couli\AppData\Roaming\IsolatedStorage  =>.id Software
O43 - CFD: 08/03/2020 - [] D -- C:\Users\couli\AppData\Roaming\Jarvee
O43 - CFD: 26/01/2019 - [] DC -- C:\Users\couli\AppData\Roaming\JetBrains  =>.JetBrains Inc
O43 - CFD: 19/09/2019 - [] DC -- C:\Users\couli\AppData\Roaming\Kalypso Media  =>.Kalypso Media
O43 - CFD: 01/07/2019 - [] DC -- C:\Users\couli\AppData\Roaming\kdenlive
O43 - CFD: 15/05/2019 - [] DC -- C:\Users\couli\AppData\Roaming\KingRoot  =>.Kingosoft Technology Ltd
O43 - CFD: 29/06/2019 - [] DC -- C:\Users\couli\AppData\Roaming\Kinvey Studio
O43 - CFD: 29/06/2019 - [] DC -- C:\Users\couli\AppData\Roaming\KinveyStudio
O43 - CFD: 17/10/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Launcher  =>.Unknown
O43 - CFD: 08/03/2020 - [] D -- C:\Users\couli\AppData\Roaming\launcher-main
O43 - CFD: 09/09/2020 - [] D -- C:\Users\couli\AppData\Roaming\LGHUB
O43 - CFD: 28/11/2018 - [] DC -- C:\Users\couli\AppData\Roaming\Logishrd  =>.Logitech Inc.
O43 - CFD: 28/11/2018 - [] DC -- C:\Users\couli\AppData\Roaming\Logitech  =>.Logitech
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Roaming\Macromedia  =>.Macromedia
O43 - CFD: 14/01/2019 - [] DC -- C:\Users\couli\AppData\Roaming\Microleaves  =>SUP.Optional.Microleaves
O43 - CFD: 02/06/2020 - [] SD -- C:\Users\couli\AppData\Roaming\Microsoft  =>.Microsoft Corporation
O43 - CFD: 28/06/2019 - [] DC -- C:\Users\couli\AppData\Roaming\MobileBackupForeverIni
O43 - CFD: 03/12/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Molotov  =>.Molotov
```

```
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Roaming\Mozilla  =>.Mozilla Corporation
O43 - CFD: 03/12/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Notepad++  =>.Don Ho
O43 - CFD: 22/06/2020 - [] D -- C:\Users\couli\AppData\Roaming\NoxSrv
O43 - CFD: 29/06/2019 - [] DC -- C:\Users\couli\AppData\Roaming\npm-cache
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Roaming\NVIDIA  =>.nVidia Corporation
O43 - CFD: 06/12/2018 - [] DC -- C:\Users\couli\AppData\Roaming\obs-studio  =>.OBS-Studio
O43 - CFD: 11/09/2019 - [] DC -- C:\Users\couli\AppData\Roaming\obs-studio-node-server
O43 - CFD: 28/01/2019 - [] DC -- C:\Users\couli\AppData\Roaming\One Click Root  =>.One Click Root
O43 - CFD: 11/06/2019 - [] DC -- C:\Users\couli\AppData\Roaming\Opera Software  =>.Opera Software
O43 - CFD: 10/09/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Origin  =>.Electronic Arts, Inc.
O43 - CFD: 20/06/2019 - [] DC -- C:\Users\couli\AppData\Roaming\PACE Anti-Piracy  =>.PACE Anti-Piracy
O43 - CFD: 11/01/2020 - [] D -- C:\Users\couli\AppData\Roaming\Paradox Interactive  =>.Paradox Interactive
O43 - CFD: 11/01/2020 - [] D -- C:\Users\couli\AppData\Roaming\Paradox Launcher
O43 - CFD: 03/01/2019 - [] DC -- C:\Users\couli\AppData\Roaming\PerfectPlayer  =>.Niklabs
O43 - CFD: 05/02/2019 - [] DC -- C:\Users\couli\AppData\Roaming\PhotoFiltre  =>.Antonio Da Cruz
O43 - CFD: 05/02/2019 - [] DC -- C:\Users\couli\AppData\Roaming\PhotoFiltre 7  =>.Antonio Da Cruz
O43 - CFD: 03/09/2020 - [] D -- C:\Users\couli\AppData\Roaming\PowerISO  =>.PowerISO Computing
O43 - CFD: 31/10/2019 - [] D -- C:\Users\couli\AppData\Roaming\ProXoft
O43 - CFD: 11/01/2019 - [] DC -- C:\Users\couli\AppData\Roaming\Quran Explorer
O43 - CFD: 04/02/2019 - [] DC -- C:\Users\couli\AppData\Roaming\QuranflashProxy
O43 - CFD: 01/06/2019 - [0] DC -- C:\Users\couli\AppData\Roaming\RiseOfIndustry
O43 - CFD: 28/06/2019 - [] DC -- C:\Users\couli\AppData\Roaming\Samsung  =>.Samsung Electronics
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Roaming\SIX Networks
O43 - CFD: 15/11/2020 - [] DC -- C:\Users\couli\AppData\Roaming\slobs-client
O43 - CFD: 10/11/2018 - [] DC -- C:\Users\couli\AppData\Roaming\slobs-plugins
O43 - CFD: 31/12/2019 - [] DC -- C:\Users\couli\AppData\Roaming\SmartSteamEmu  =>.SmartSteam
O43 - CFD: 30/06/2019 - [] DC -- C:\Users\couli\AppData\Roaming\Softbank Robotics
O43 - CFD: 13/08/2020 - [] D -- C:\Users\couli\AppData\Roaming\Startup Company
O43 - CFD: 25/12/2019 - [] D -- C:\Users\couli\AppData\Roaming\StartupCompany
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Roaming\Streamlabs OBS
O43 - CFD: 12/07/2019 - [] DC -- C:\Users\couli\AppData\Roaming\StudioKing
O43 - CFD: 05/10/2018 - [] DC -- C:\Users\couli\AppData\Roaming\Sublime Text 3
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Roaming\Sun  =>.Oracle
O43 - CFD: 24/08/2018 - [] DC -- C:\Users\couli\AppData\Roaming\Sync withSIX
O43 - CFD: 02/12/2020 - [0] DC -- C:\Users\couli\AppData\Roaming\TeamViewer  =>.TeamViewer GmbH
O43 - CFD: 01/07/2019 - [] DC -- C:\Users\couli\AppData\Roaming\TempiTunes
O43 - CFD: 15/05/2019 - [] DC -- C:\Users\couli\AppData\Roaming\Tencent  =>.Tencent
O43 - CFD: 18/05/2019 - [] DC -- C:\Users\couli\AppData\Roaming\TransferSupport
O43 - CFD: 08/09/2019 - [] DC -- C:\Users\couli\AppData\Roaming\Tropico 5  =>.Kalypso Media
O43 - CFD: 01/12/2020 - [] DC -- C:\Users\couli\AppData\Roaming\TS3Client  =>.TeamSpeak
O43 - CFD: 03/12/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Twitch  =>.Twitch
O43 - CFD: 02/12/2020 - [] D -- C:\Users\couli\AppData\Roaming\twitch-electron  =>.Twitch
O43 - CFD: 03/03/2020 - [] D -- C:\Users\couli\AppData\Roaming\ucs
O43 - CFD: 02/12/2020 - [] DC -- C:\Users\couli\AppData\Roaming\uTorrent
O43 - CFD: 05/09/2018 - [] DC -- C:\Users\couli\AppData\Roaming\v5.VitalityRP
O43 - CFD: 18/01/2019 - [] DC -- C:\Users\couli\AppData\Roaming\VirusMaker  =>PUP.Optional.VirusMaker
O43 - CFD: 27/06/2019 - [] DC -- C:\Users\couli\AppData\Roaming\Visual Studio Setup  =>.Pinnacle Systems, Inc.
O43 - CFD: 03/12/2020 - [] D -- C:\Users\couli\AppData\Roaming\vlc  =>.VideoLan Team
O43 - CFD: 18/02/2019 - [] DC -- C:\Users\couli\AppData\Roaming\VMware  =>.VMware
O43 - CFD: 27/06/2019 - [] DC -- C:\Users\couli\AppData\Roaming\vstelemetry  =>.Legitimate
O43 - CFD: 27/06/2019 - [] DC -- C:\Users\couli\AppData\Roaming\vs_installershell
O43 - CFD: 19/09/2019 - [0] DC -- C:\Users\couli\AppData\Roaming\WeMod  =>.WeMod
O43 - CFD: 27/11/2020 - [] DC -- C:\Users\couli\AppData\Roaming\WhatsApp  =>.WhatsApp
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Roaming\WinRAR  =>.WinRAR
O43 - CFD: 17/01/2019 - [] DC -- C:\Users\couli\AppData\Roaming\Wireshark  =>.Wireshark
O43 - CFD: 03/01/2020 - [] D -- C:\Users\couli\AppData\Roaming\Wondershare  =>.Wondershare
O43 - CFD: 15/02/2020 - [] D -- C:\Users\couli\AppData\Roaming\Xiaomi  =>.XiaoMi
O43 - CFD: 03/12/2020 - [] D -- C:\Users\couli\AppData\Roaming\ZHP  =>.Nicolas Coolman
O43 - CFD: 05/02/2019 - [] DC -- C:\Users\couli\AppData\Local\ActiveState  =>.ActiveState
O43 - CFD: 16/05/2020 - [] DC -- C:\Users\couli\AppData\Local\Adobe  =>.Adobe
O43 - CFD: 08/06/2019 - [] DC -- C:\Users\couli\AppData\Local\ADT
O43 - CFD: 25/01/2019 - [] DC -- C:\Users\couli\AppData\Local\Android  =>.Android
O43 - CFD: 06/04/2020 - [] D -- C:\Users\couli\AppData\Local\Android Open Source Project
O43 - CFD: 16/06/2019 - [] DC -- C:\Users\couli\AppData\Local\apk-editor-studio
O43 - CFD: 28/06/2019 - [] DC -- C:\Users\couli\AppData\Local\Apowersoft  =>.Apowersoft
O43 - CFD: 02/06/2020 - [0] SHD -- C:\Users\couli\AppData\Local\Application Data  =>.Microsoft Corporation
O43 - CFD: 22/01/2019 - [] DC -- C:\Users\couli\AppData\Local\Apps  =>.Microsoft Corporation
O43 - CFD: 01/12/2020 - [] DC -- C:\Users\couli\AppData\Local\Arma 3  =>.Bohemia Interactive Studio
O43 - CFD: 01/12/2020 - [] DC -- C:\Users\couli\AppData\Local\Arma 3 Launcher  =>.Bohemia Interactive Studio
O43 - CFD: 21/05/2020 - [] D -- C:\Users\couli\AppData\Local\atom
O43 - CFD: 09/06/2020 - [] DC -- C:\Users\couli\AppData\Local\AVAST Software  =>.AVAST Software
O43 - CFD: 11/06/2019 - [] DC -- C:\Users\couli\AppData\Local\Avira  =>.Avira Software
O43 - CFD: 28/01/2019 - [] DC -- C:\Users\couli\AppData\Local\AWSToolkit  =>.Amazon Corporation
O43 - CFD: 29/01/2020 - [] DC -- C:\Users\couli\AppData\Local\Battle.net  =>.Games Software
O43 - CFD: 24/08/2018 - [] DC -- C:\Users\couli\AppData\Local\BattlEye  =>.BattlEye
O43 - CFD: 10/09/2020 - [] DC -- C:\Users\couli\AppData\Local\BitTorrentHelper
O43 - CFD: 29/01/2020 - [0] DC -- C:\Users\couli\AppData\Local\Blizzard  =>.Blizzard
O43 - CFD: 29/01/2020 - [] DC -- C:\Users\couli\AppData\Local\Blizzard Entertainment  =>.Blizzard Entertainment
O43 - CFD: 24/06/2020 - [] DC -- C:\Users\couli\AppData\Local\Bluestacks  =>.BlueStack Systems, Inc.
O43 - CFD: 13/06/2019 - [] DC -- C:\Users\couli\AppData\Local\Bohemia_Interactive  =>.Bohemia Interactive Studio
O43 - CFD: 23/01/2020 - [] DC -- C:\Users\couli\AppData\Local\cache  =>.Legitimate
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Local\CEF  =>.CEF
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Local\Chromium  =>.Chromium
O43 - CFD: 05/11/2018 - [] DC -- C:\Users\couli\AppData\Local\Colossal Order  =>.Colossal Order Ltd
O43 - CFD: 05/02/2019 - [] DC -- C:\Users\couli\AppData\Local\Comms  =>.Microsoft Corporation
O43 - CFD: 10/06/2020 - [] DC -- C:\Users\couli\AppData\Local\ConnectedDevicesPlatform  =>.Microsoft Corporation
O43 - CFD: 08/03/2019 - [] DC -- C:\Users\couli\AppData\Local\Cosmos  =>.Cosmos
O43 - CFD: 02/12/2020 - [] DC -- C:\Users\couli\AppData\Local\CrashDumps  =>.Microsoft Corporation
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Local\Crashpad  =>.Unknown
O43 - CFD: 29/10/2018 - [] DC -- C:\Users\couli\AppData\Local\CrashRpt
O43 - CFD: 18/10/2019 - [] D -- C:\Users\couli\AppData\Local\CyberLink  =>.CyberLink Corporation
O43 - CFD: 03/02/2019 - [] DC -- C:\Users\couli\AppData\Local\Cyotek  =>.Cyotek
O43 - CFD: 25/10/2020 - [] DC -- C:\Users\couli\AppData\Local\D3DSCache  =>.Legitimate
O43 - CFD: 24/08/2018 - [0] DC -- C:\Users\couli\AppData\Local\DBG  =>.DBG
O43 - CFD: 30/06/2019 - [] DC -- C:\Users\couli\AppData\Local\Dell  =>.Dell
O43 - CFD: 03/12/2020 - [] DC -- C:\Users\couli\AppData\Local\Diagnostics  =>.Microsoft Corporation
O43 - CFD: 29/09/2020 - [] DC -- C:\Users\couli\AppData\Local\Discord  =>.GitHub
O43 - CFD: 07/02/2019 - [] DC -- C:\Users\couli\AppData\Local\Disruptive Innovations SARL  =>.Disruptive Innovations SARL
O43 - CFD: 15/01/2019 - [] DC -- C:\Users\couli\AppData\Local\Dovetail Games  =>.Dovetail Games
O43 - CFD: 29/06/2019 - [] DC -- C:\Users\couli\AppData\Local\Downloaded Installations  =>.Microsoft Corporation
O43 - CFD: 24/03/2020 - [] D -- C:\Users\couli\AppData\Local\Dropbox  =>.Dropbox
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Local\DropboxOEM  =>.Dropbox Inc.
O43 - CFD: 27/06/2019 - [] DC -- C:\Users\couli\AppData\Local\Eclipse  =>.Eclipse
O43 - CFD: 26/01/2020 - [] D -- C:\Users\couli\AppData\Local\Electronic Arts  =>.Electronic Arts
```

```
O43 - CFD: 02/12/2020 - [] DC -- C:\Users\couli\AppData\Local\ElevatedDiagnostics  =>.Microsoft Corporation
O43 - CFD: 24/08/2018 - [] DC -- C:\Users\couli\AppData\Local\EpicGamesLauncher  =>.Epic Games
O43 - CFD: 14/01/2019 - [] DC -- C:\Users\couli\AppData\Local\ESET  =>.ESET
O43 - CFD: 23/07/2019 - [] DC -- C:\Users\couli\AppData\Local\EStartup
O43 - CFD: 06/02/2019 - [] DC -- C:\Users\couli\AppData\Local\FileZilla  =>.FileZilla
O43 - CFD: 28/10/2018 - [] DC -- C:\Users\couli\AppData\Local\FishingGame
O43 - CFD: 24/08/2018 - [] DC -- C:\Users\couli\AppData\Local\FiveM  =>.cfx-collective
O43 - CFD: 24/05/2020 - [] D -- C:\Users\couli\AppData\Local\fontsninja-updater
O43 - CFD: 27/11/2019 - [] DC -- C:\Users\couli\AppData\Local\Frontier Developments  =>.Frontier Developments
O43 - CFD: 06/12/2018 - [0] DC -- C:\Users\couli\AppData\Local\GameAnalytics
O43 - CFD: 03/12/2020 - [] D -- C:\Users\couli\AppData\Local\Google  =>.Google
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Local\Hewlett-Packard  =>.Hewlett-Packard
O43 - CFD: 02/06/2020 - [0] SHD -- C:\Users\couli\AppData\Local\Historique  =>.Microsoft Corporation
O43 - CFD: 07/03/2020 - [] D -- C:\Users\couli\AppData\Local\HP  =>.Hewlett-Packard
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Local\HP JumpStart Apps
O43 - CFD: 12/11/2020 - [] DC -- C:\Users\couli\AppData\Local\HP_Inc  =>.Hewlett-Packard
O43 - CFD: 21/05/2019 - [] DC -- C:\Users\couli\AppData\Local\INetHistory
O43 - CFD: 27/03/2020 - [] D -- C:\Users\couli\AppData\Local\Insurgency  =>.Insurgency
O43 - CFD: 13/07/2019 - [] DC -- C:\Users\couli\AppData\Local\Introversion  =>.Introversion
O43 - CFD: 03/03/2020 - [] D -- C:\Users\couli\AppData\Local\IsolatedStorage  =>.id Software
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Local\JimsApps  =>.JimsApps
O43 - CFD: 19/09/2019 - [] DC -- C:\Users\couli\AppData\Local\Kalypso Media  =>.Kalypso Media
O43 - CFD: 01/07/2019 - [] DC -- C:\Users\couli\AppData\Local\kdenlive
O43 - CFD: 29/06/2019 - [] DC -- C:\Users\couli\AppData\Local\kinvey-studio-updater
O43 - CFD: 26/01/2019 - [] DC -- C:\Users\couli\AppData\Local\kotlin
O43 - CFD: 21/02/2019 - [] DC -- C:\Users\couli\AppData\Local\Kotobee Author
O43 - CFD: 20/06/2019 - [] HDC -- C:\Users\couli\AppData\Local\LaNFGrgekANZw
O43 - CFD: 08/09/2020 - [] D -- C:\Users\couli\AppData\Local\LGHUB
O43 - CFD: 28/11/2018 - [] DC -- C:\Users\couli\AppData\Local\Logitech  =>.Logitech
O43 - CFD: 26/03/2020 - [] D -- C:\Users\couli\AppData\Local\Magic Hills  =>.Magic Hills Pty Ltd
O43 - CFD: 10/09/2018 - [] DC -- C:\Users\couli\AppData\Local\Mega Limited  =>.MEGA Limited
O43 - CFD: 20/06/2019 - [] DC -- C:\Users\couli\AppData\Local\Meltytech
O43 - CFD: 02/10/2020 - [] D -- C:\Users\couli\AppData\Local\Microsoft  =>.Microsoft Corporation
O43 - CFD: 17/01/2019 - [] DC -- C:\Users\couli\AppData\Local\Microsoft Help  =>.Microsoft Corporation
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Local\MicrosoftEdge  =>.Microsoft Corporation
O43 - CFD: 22/06/2020 - [] D -- C:\Users\couli\AppData\Local\Microvirt  =>.Microvirt
O43 - CFD: 01/07/2019 - [] DC -- C:\Users\couli\AppData\Local\mime  =>.Mime
O43 - CFD: 15/02/2020 - [] D -- C:\Users\couli\AppData\Local\MiPhoneManager
O43 - CFD: 02/12/2020 - [] DC -- C:\Users\couli\AppData\Local\Molotov  =>.Molotov
O43 - CFD: 18/10/2019 - [] D -- C:\Users\couli\AppData\Local\Movavi  =>.Movavi
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Local\Mozilla  =>.Mozilla Corporation
O43 - CFD: 22/06/2020 - [] D -- C:\Users\couli\AppData\Local\MultiPlayerManager
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Local\New Technology Studio  =>.New Technology Studio
O43 - CFD: 02/01/2019 - [] DC -- C:\Users\couli\AppData\Local\NordVPN  =>.NordVPN
O43 - CFD: 23/08/2018 - [0] DC -- C:\Users\couli\AppData\Local\Notepad++  =>.Don Ho
O43 - CFD: 22/06/2020 - [] D -- C:\Users\couli\AppData\Local\Nox  =>.FFmpeg Project
O43 - CFD: 09/04/2020 - [] D -- C:\Users\couli\AppData\Local\NoxSrv
O43 - CFD: 12/11/2020 - [] DC -- C:\Users\couli\AppData\Local\NVIDIA  =>.nVidia Corporation
O43 - CFD: 27/08/2019 - [] DC -- C:\Users\couli\AppData\Local\NVIDIA Corporation  =>.nVidia Corporation
O43 - CFD: 17/01/2019 - [] DC -- C:\Users\couli\AppData\Local\OfficeBSCache-OD-coulibaly_64@hotmail.com
O43 - CFD: 28/01/2019 - [] DC -- C:\Users\couli\AppData\Local\oneClickRoot  =>.Legitimate
O43 - CFD: 11/06/2019 - [] DC -- C:\Users\couli\AppData\Local\Opera Software  =>.Opera Software
O43 - CFD: 09/09/2020 - [] DC -- C:\Users\couli\AppData\Local\Origin  =>.Electronic Arts, Inc.
O43 - CFD: 20/06/2019 - [0] DC -- C:\Users\couli\AppData\Local\PACE Anti-Piracy  =>.PACE Anti-Piracy
O43 - CFD: 02/12/2020 - [] DC -- C:\Users\couli\AppData\Local\Packages  =>.Microsoft Corporation
O43 - CFD: 02/06/2020 - [] DC -- C:\Users\couli\AppData\Local\PackageStaging  =>.Apcera
O43 - CFD: 20/06/2019 - [] DC -- C:\Users\couli\AppData\Local\paint.net  =>.Rick Brewster
O43 - CFD: 26/10/2019 - [] D -- C:\Users\couli\AppData\Local\PajdaPanel
O43 - CFD: 11/01/2020 - [] D -- C:\Users\couli\AppData\Local\Paradox Interactive  =>.Paradox Interactive
O43 - CFD: 20/01/2019 - [] DC -- C:\Users\couli\AppData\Local\Patcher
O43 - CFD: 30/08/2018 - [] DC -- C:\Users\couli\AppData\Local\PboM
O43 - CFD: 02/12/2020 - [] DC -- C:\Users\couli\AppData\Local\PlaceholderTileLogoFolder  =>.Microsoft Corporation
O43 - CFD: 13/06/2019 - [] DC -- C:\Users\couli\AppData\Local\Plex Media Server  =>.Plex Inc.
O43 - CFD: 18/03/2020 - [] D -- C:\Users\couli\AppData\Local\Popcorn-Time  =>.SUP.PopcornTime
O43 - CFD: 24/05/2020 - [] DC -- C:\Users\couli\AppData\Local\Programs  =>.Microsoft Corporation
O43 - CFD: 21/10/2020 - [] DC -- C:\Users\couli\AppData\Local\Publishers  =>.Microsoft Corporation
O43 - CFD: 06/08/2019 - [] DC -- C:\Users\couli\AppData\Local\RDAExplorerGUI
O43 - CFD: 01/07/2019 - [] DC -- C:\Users\couli\AppData\Local\RecentDocuments
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Local\Recovery  =>.Recovery Labs
O43 - CFD: 06/10/2019 - [] DC -- C:\Users\couli\AppData\Local\Rockstar Games  =>.Rockstar Games
O43 - CFD: 27/06/2019 - [] DC -- C:\Users\couli\AppData\Local\ServiceHub
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Local\SIX Networks
O43 - CFD: 17/05/2020 - [] D -- C:\Users\couli\AppData\Local\SlimWare Utilities Inc  =>.SUP.SlimWareUtilities
O43 - CFD: 17/03/2020 - [] D -- C:\Users\couli\AppData\Local\Smart City Plan
O43 - CFD: 28/03/2020 - [] D -- C:\Users\couli\AppData\Local\SmartphoneTycoon  =>.Roblox Corporation
O43 - CFD: 18/12/2018 - [] DC -- C:\Users\couli\AppData\Local\Solvusoft_Corporation  =>SUP.Optional.Solvusoft
O43 - CFD: 13/12/2019 - [] D -- C:\Users\couli\AppData\Local\speech  =>.Microsoft Corporation
O43 - CFD: 06/11/2018 - [] DC -- C:\Users\couli\AppData\Local\Sports Interactive  =>.Sports Interactive
O43 - CFD: 23/11/2020 - [] DC -- C:\Users\couli\AppData\Local\SquirrelTemp  =>.Squirrels
O43 - CFD: 01/07/2019 - [] DC -- C:\Users\couli\AppData\Local\stalefiles
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Local\Steam  =>.Steam Games
O43 - CFD: 12/05/2019 - [] DC -- C:\Users\couli\AppData\Local\Sublime Text 3
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Local\Sync
O43 - CFD: 20/06/2019 - [] HDC -- C:\Users\couli\AppData\Local\TD3SX5jbbHQ1
O43 - CFD: 28/06/2019 - [] DC -- C:\Users\couli\AppData\Local\TeamViewer  =>.TeamViewer GmbH
O43 - CFD: 03/12/2020 - [] D -- C:\Users\couli\AppData\Local\Temp  =>.Microsoft Corporation
O43 - CFD: 02/06/2020 - [0] SHD -- C:\Users\couli\AppData\Local\Temporary Internet Files  =>.Microsoft Corporation
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\Local\TileDataLayer  =>.Microsoft Corporation
O43 - CFD: 27/11/2019 - [] DC -- C:\Users\couli\AppData\Local\TouristBusSimulator
O43 - CFD: 25/10/2018 - [] DC -- C:\Users\couli\AppData\Local\Tropico6 - Beta  =>.Kalypso Media
O43 - CFD: 22/02/2020 - [] DC -- C:\Users\couli\AppData\Local\Ubisoft Game Launcher  =>.Ubisoft
O43 - CFD: 22/02/2020 - [] DC -- C:\Users\couli\AppData\Local\UnrealEngine  =>.Unreal Software
O43 - CFD: 24/08/2018 - [] DC -- C:\Users\couli\AppData\Local\UnrealEngineLauncher  =>.Unreal Software
O43 - CFD: 15/05/2020 - [] D -- C:\Users\couli\AppData\Local\UXP  =>.UXP
O43 - CFD: 18/10/2019 - [] D -- C:\Users\couli\AppData\Local\VideoEditor  =>.Oposoft.com
O43 - CFD: 20/06/2019 - [] DC -- C:\Users\couli\AppData\Local\VirtualStore  =>.Microsoft Corporation
O43 - CFD: 12/03/2019 - [] DC -- C:\Users\couli\AppData\Local\Vitalwerks  =>.Vitalwerks
O43 - CFD: 18/02/2019 - [] DC -- C:\Users\couli\AppData\Local\VMware  =>.VMware
O43 - CFD: 19/09/2019 - [] DC -- C:\Users\couli\AppData\Local\WeMod  =>.WeMod
O43 - CFD: 23/11/2020 - [] DC -- C:\Users\couli\AppData\Local\WhatsApp  =>.WhatsApp
O43 - CFD: 01/07/2019 - [] DC -- C:\Users\couli\AppData\Local\WonderShare  =>.Wondershare
O43 - CFD: 03/12/2020 - [] D -- C:\Users\couli\AppData\Local\ZHP  =>.Nicolas Coolman
O43 - CFD: 21/10/2018 - [] DC -- C:\Users\couli\AppData\Local\Zombie Army Trilogy  =>.Games Software
O43 - CFD: 12/05/2020 - [] D -- C:\Users\couli\AppData\Local\_
```

```
O43 - CFD: 21/02/2019 - [] HDC -- C:\Users\couli\AppData\Local\_wc
O43 - CFD: 23/08/2018 - [0] DC -- C:\Users\couli\AppData\Local\Programs\Common  =>.Microsoft Corporation
O43 - CFD: 24/05/2020 - [] DC -- C:\Users\couli\AppData\Local\Programs\FontsNinja
O43 - CFD: 02/12/2020 - [] DC -- C:\Users\couli\AppData\Local\Programs\Opera  =>.Opera Software
O43 - CFD: 27/11/2020 - [] DC -- C:\Users\couli\AppData\Local\Programs\Paradox Interactive  =>.Paradox Interactive
O43 - CFD: 15/10/2018 - [] DC -- C:\Users\couli\AppData\LocalLow\Adobe  =>.Adobe
O43 - CFD: 13/07/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\Apoapsis Studios
O43 - CFD: 13/11/2018 - [] DC -- C:\Users\couli\AppData\LocalLow\Astragon  =>.Astragon
O43 - CFD: 04/04/2020 - [] DC -- C:\Users\couli\AppData\LocalLow\Colossal Order  =>.Colossal Order Ltd
O43 - CFD: 01/06/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\Dapper Penguin Studios
O43 - CFD: 20/08/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\DefaultCompany
O43 - CFD: 06/06/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\Eggcode
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\LocalLow\Empyrean
O43 - CFD: 17/02/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\IObit  =>.IObit
O43 - CFD: 14/08/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\JMG
O43 - CFD: 28/10/2018 - [] DC -- C:\Users\couli\AppData\LocalLow\LaRuina
O43 - CFD: 08/07/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\LVGameDev LLC
O43 - CFD: 23/08/2018 - [] SDC -- C:\Users\couli\AppData\LocalLow\Microsoft  =>.Microsoft Corporation
O43 - CFD: 03/12/2020 - [] DC -- C:\Users\couli\AppData\LocalLow\Mozilla  =>.Mozilla Corporation
O43 - CFD: 16/06/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\Oracle  =>.Oracle
O43 - CFD: 01/11/2018 - [] DC -- C:\Users\couli\AppData\LocalLow\Oxymoron Games
O43 - CFD: 24/08/2018 - [] DC -- C:\Users\couli\AppData\LocalLow\Playsport Games
O43 - CFD: 25/12/2018 - [] DC -- C:\Users\couli\AppData\LocalLow\PlayWay
O43 - CFD: 10/10/2018 - [] DC -- C:\Users\couli\AppData\LocalLow\Red Dot Games
O43 - CFD: 07/01/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\Reflect Studios
O43 - CFD: 07/06/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\SeriesMakers
O43 - CFD: 17/05/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\Soccer Manager Ltd
O43 - CFD: 03/06/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\SomaSim
O43 - CFD: 20/07/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\Squeaky Wheel  =>PUP.Optional.Squeaky
O43 - CFD: 23/08/2018 - [] DC -- C:\Users\couli\AppData\LocalLow\Sun  =>.Oracle
O43 - CFD: 24/12/2018 - [] DC -- C:\Users\couli\AppData\LocalLow\Techland  =>.Techland
O43 - CFD: 26/07/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\Temp  =>.Microsoft Corporation
O43 - CFD: 30/10/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\The Irregular Corp
O43 - CFD: 12/07/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\Toplitz Productions
O43 - CFD: 10/09/2018 - [] DC -- C:\Users\couli\AppData\LocalLow\Two Point Studios
O43 - CFD: 11/12/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\U-Play online
O43 - CFD: 31/10/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\Unity  =>.Unity
O43 - CFD: 13/01/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\Unknown Worlds
O43 - CFD: 09/09/2020 - [] DC -- C:\Users\couli\AppData\LocalLow\uTorrent
O43 - CFD: 27/10/2018 - [] DC -- C:\Users\couli\AppData\LocalLow\weltenbauer. Software Entwicklung GmbH
O43 - CFD: 22/06/2019 - [] DC -- C:\Users\couli\AppData\LocalLow\Wonderbox Games
O43 - CFD: 04/11/2019 - [] D -- C:\Users\couli\OneDrive\Bureau\Adenis
O43 - CFD: 05/10/2018 - [] D -- C:\Users\couli\OneDrive\Bureau\Car_Workshop_Building
O43 - CFD: 06/08/2019 - [] D -- C:\Users\couli\OneDrive\Bureau\CoSMOS_Advanced_513
O43 - CFD: 06/08/2019 - [] D -- C:\Users\couli\OneDrive\Bureau\CoSMOS_Beg_Release_5020
O43 - CFD: 20/09/2018 - [] D -- C:\Users\couli\OneDrive\Bureau\Crack
O43 - CFD: 06/03/2019 - [0] D -- C:\Users\couli\OneDrive\Bureau\Diffusion
O43 - CFD: 05/02/2019 - [] D -- C:\Users\couli\OneDrive\Bureau\Ecouter et télécharger le saint coran, récitation et lecture du quran mp3_fichiers
O43 - CFD: 08/02/2019 - [] D -- C:\Users\couli\OneDrive\Bureau\Hack wifi
O43 - CFD: 07/01/2020 - [] D -- C:\Users\couli\OneDrive\Bureau\Hacking Darknet
O43 - CFD: 02/10/2018 - [] AD -- C:\Users\couli\OneDrive\Bureau\html5up-dimension
O43 - CFD: 22/02/2019 - [] D -- C:\Users\couli\OneDrive\Bureau\Iss814-13-Bala-Mbedocratie
O43 - CFD: 21/02/2019 - [] D -- C:\Users\couli\OneDrive\Bureau\logo site
O43 - CFD: 21/02/2019 - [] D -- C:\Users\couli\OneDrive\Bureau\logo site 2
O43 - CFD: 09/02/2019 - [] D -- C:\Users\couli\OneDrive\Bureau\mbrfix
O43 - CFD: 28/11/2020 - [] D -- C:\Users\couli\OneDrive\Bureau\Mix
O43 - CFD: 20/02/2020 - [] D -- C:\Users\couli\OneDrive\Bureau\Muslim Coran
O43 - CFD: 30/08/2018 - [] D -- C:\Users\couli\OneDrive\Bureau\Nouveau dossier
O43 - CFD: 10/01/2020 - [] D -- C:\Users\couli\OneDrive\Bureau\Nouveau dossier (10)
O43 - CFD: 22/06/2020 - [] D -- C:\Users\couli\OneDrive\Bureau\Nouveau dossier (11)
O43 - CFD: 12/09/2018 - [] D -- C:\Users\couli\OneDrive\Bureau\Nouveau dossier (2)
O43 - CFD: 15/11/2018 - [] D -- C:\Users\couli\OneDrive\Bureau\Nouveau dossier (3)
O43 - CFD: 15/05/2019 - [] D -- C:\Users\couli\OneDrive\Bureau\Nouveau dossier (4)
O43 - CFD: 25/03/2020 - [] D -- C:\Users\couli\OneDrive\Bureau\Nouveau dossier (5)
O43 - CFD: 27/06/2019 - [] D -- C:\Users\couli\OneDrive\Bureau\Nouveau dossier (6)
O43 - CFD: 06/08/2019 - [] D -- C:\Users\couli\OneDrive\Bureau\Nouveau dossier (7)
O43 - CFD: 19/12/2019 - [] D -- C:\Users\couli\OneDrive\Bureau\Nouveau dossier (8)
O43 - CFD: 19/12/2019 - [] D -- C:\Users\couli\OneDrive\Bureau\Nouveau dossier (9)
O43 - CFD: 28/11/2020 - [] D -- C:\Users\couli\OneDrive\Bureau\Nouveau Musique
O43 - CFD: 10/02/2019 - [] D -- C:\Users\couli\OneDrive\Bureau\quran
O43 - CFD: 20/02/2020 - [] D -- C:\Users\couli\OneDrive\Bureau\Quran flash
O43 - CFD: 11/06/2019 - [0] D -- C:\Users\couli\OneDrive\Bureau\RATS
O43 - CFD: 09/02/2019 - [] D -- C:\Users\couli\OneDrive\Bureau\rufus_files
O43 - CFD: 06/02/2020 - [] D -- C:\Users\couli\OneDrive\Bureau\Selection Moussa
O43 - CFD: 20/09/2018 - [] D -- C:\Users\couli\OneDrive\Bureau\Setup
O43 - CFD: 17/06/2019 - [] D -- C:\Users\couli\OneDrive\Bureau\Test Apk
O43 - CFD: 26/12/2018 - [] D -- C:\Users\couli\OneDrive\Bureau\Tor Browser  =>.Roger Dingledine
O43 - CFD: 20/10/2018 - [] D -- C:\Users\couli\OneDrive\Bureau\Tropico Save Game  =>.Kalypso Media
O43 - CFD: 23/10/2019 - [] D -- C:\Users\couli\OneDrive\Bureau\TS.SE.Tool.0.2.2
O43 - CFD: 04/09/2018 - [] D -- C:\Users\couli\OneDrive\Bureau\VBus
O43 - CFD: 04/09/2018 - [] D -- C:\Users\couli\OneDrive\Bureau\Virtual Bus Driver
O43 - CFD: 16/05/2020 - [] D -- C:\Users\couli\OneDrive\Bureau\Wallpaper Engine
O43 - CFD: 14/01/2019 - [0] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\1xWin
O43 - CFD: 11/05/2020 - [] RD -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility  =>.Microsoft Corporation
O43 - CFD: 02/06/2020 - [] RD -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories  =>.Microsoft Corporation
O43 - CFD: 02/06/2020 - [] RDC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools  =>.Administrative Tools
O43 - CFD: 02/07/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Cain
O43 - CFD: 02/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\CodeBlocks  =>.CodeBlocks Team
O43 - CFD: 29/09/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Discord Inc  =>.Discord Inc
O43 - CFD: 03/09/2019 - [0] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\DriverHub
O43 - CFD: 02/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Eclipse  =>.Eclipse
O43 - CFD: 02/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\GitHub, Inc  =>.GitHub
O43 - CFD: 02/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\GNU Privacy Guard
O43 - CFD: 02/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Litecoin Core
O43 - CFD: 07/12/2019 - [] D -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance  =>.Microsoft Corporation
O43 - CFD: 22/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\MEmu  =>.Microvirt Software Technology Ltd.
O43 - CFD: 02/12/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Molotov  =>.Molotov
O43 - CFD: 02/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\No-IP DUC  =>.Vitalwerks Internet Solutions
O43 - CFD: 02/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Outil de téléchargement USB DVD Windows 7
O43 - CFD: 02/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\PhotoFiltre  =>.Antonio Da Cruz
O43 - CFD: 02/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\PhotoFiltre 7  =>.Antonio Da Cruz
O43 - CFD: 02/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Popcorn-Time  =>.SUP.PopcornTime
O43 - CFD: 02/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Rockstar Games  =>.Rockstar Games
O43 - CFD: 02/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\RVL Hacker
```

```
O43 - CFD: 02/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\SIX Networks GmbH  =>.SIX Networks GmbH
O43 - CFD: 02/12/2020 - [] RDC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup  =>.Microsoft Corporation
O43 - CFD: 02/12/2020 - [] HDC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup-Disabled  =>.Microsoft Corporation
O43 - CFD: 24/11/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Steam  =>.Steam Games
O43 - CFD: 02/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Supercopier  =>.SFX Team
O43 - CFD: 02/06/2020 - [] RD -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools  =>.Microsoft Corporation
O43 - CFD: 02/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Ubisoft  =>.Ubisoft
O43 - CFD: 18/10/2019 - [0] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Website Ripper Copier
O43 - CFD: 19/09/2019 - [0] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\WeMod  =>.WeMod
O43 - CFD: 02/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\WhatsApp  =>.WhatsApp
O43 - CFD: 02/06/2020 - [] D -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Windows PowerShell  =>.Microsoft Corporation
O43 - CFD: 03/12/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\WinRAR  =>.WinRAR
O43 - CFD: 02/06/2020 - [] DC -- C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Xiaomi  =>.XiaoMi
O43 - CFD: 02/06/2020 - [0] SHD -- C:\Users\Default\AppData\Local\Application Data  =>.Microsoft Corporation
O43 - CFD: 23/08/2018 - [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: 02/06/2020 - [0] SHD -- C:\Users\Default\AppData\Local\Temporary Internet Files  =>.Microsoft Corporation
O43 - CFD: 02/06/2020 - [0] SHD -- C:\Users\Default User\AppData\Local\Application Data  =>.Microsoft Corporation
O43 - CFD: 23/08/2018 - [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: 02/06/2020 - [0] SHD -- C:\Users\Default User\AppData\Local\Temporary Internet Files  =>.Microsoft Corporation
O43 - CFD: 03/06/2020 - []  -- C:\WINDOWS\System32\Config\systemprofile\AppData\Local\Adobe  =>.Adobe
O43 - CFD: 10/11/2020 - [] D -- C:\WINDOWS\System32\Config\systemprofile\AppData\Local\CrashDumps  =>.Microsoft Corporation
O43 - CFD: 24/07/2020 - []  -- C:\WINDOWS\System32\Config\systemprofile\AppData\Local\Dropbox  =>.Dropbox
O43 - CFD: 02/06/2020 - [] D -- C:\WINDOWS\System32\Config\systemprofile\AppData\Local\Microsoft  =>.Microsoft Corporation
O43 - CFD: 10/06/2020 - []  -- C:\WINDOWS\System32\Config\systemprofile\AppData\Roaming\Dropbox  =>.Dropbox
O43 - CFD: 08/06/2020 - [] D -- C:\WINDOWS\System32\Config\systemprofile\AppData\Roaming\Microsoft  =>.Microsoft Corporation
O43 - CFD: 09/06/2020 - []  -- C:\WINDOWS\System32\Config\systemprofile\AppData\Roaming\Origin  =>.Electronic Arts, Inc.
O43 - CFD: 03/12/2020 - [0]  -- C:\WINDOWS\System32\Config\systemprofile\AppData\Roaming\VMware  =>.VMware

---\ ShellIconOverlayIdentifiers (SIOI) (18) - 1s
O106 - SIOI: ▯ MEGA (Pending) [▯ MEGA (Pending)] - {056D528D-CE28-4194-9BA3-BA2E9197FF8C}. (...) -- C:\ProgramData\MEGAsync\ShellExtX64.dll [Unsigned]
O106 - SIOI: ▯ MEGA (Synced) [▯ MEGA (Synced)] - {05B38830-F4E9-4329-978B-1DD28605D202}. (...) -- C:\ProgramData\MEGAsync\ShellExtX64.dll [Unsigned]
O106 - SIOI: ▯ MEGA (Syncing) [▯ MEGA (Syncing)] - {0596C850-7BDD-4C9D-AFDF-873BE6890637}. (...) -- C:\ProgramData\MEGAsync\ShellExtX64.dll [Unsigned]
O106 - SIOI:  [   AccExtIco1] - {AB9CF9F8-8A96-4F9D-BF21-CE85714C3A47}. (.2013-2018, Adobe Systems Incorporated. All rights res - Core Sync.) -- C:\Pr
O106 - SIOI:  [   AccExtIco2] - {853B7E05-C47D-4985-909A-D0DC5C6D7303}. (.2013-2018, Adobe Systems Incorporated. All rights res - Core Sync.) -- C:\Pr
O106 - SIOI:  [   AccExtIco3] - {42D38F2E-98E9-4382-B546-E24E4D6D04BB}. (.2013-2018, Adobe Systems Incorporated. All rights res - Core Sync.) -- C:\Pr
O106 - SIOI: DropboxExt1 Class [   DropboxExt01] - {FB314ED9-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program F
O106 - SIOI: DropboxExt7 Class [   DropboxExt02] - {FB314EDF-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program F
O106 - SIOI: DropboxExt9 Class [   DropboxExt03] - {FB314EE1-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program F
O106 - SIOI: DropboxExt3 Class [   DropboxExt04] - {FB314EDB-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program F
O106 - SIOI: DropboxExt2 Class [   DropboxExt05] - {FB314EDA-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program F
O106 - SIOI: DropboxExt4 Class [   DropboxExt06] - {FB314EDC-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program F
O106 - SIOI: DropboxExt5 Class [   DropboxExt07] - {FB314EDD-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program F
O106 - SIOI: DropboxExt8 Class [   DropboxExt08] - {FB314EE0-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program F
O106 - SIOI: DropboxExt10 Class [   DropboxExt09] - {FB314EE2-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program
O106 - SIOI: DropboxExt6 Class [   DropboxExt10] - {FB314EDE-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program F
O106 - SIOI: avast [00asw] - {472083B0-C522-11CF-8763-00608CC02F24}. (.AVAST Software - Avast Shell Extension.) -- C:\Program Files\AVAST Software\Ava
O106 - SIOI:  [EnhancedStorageShell] - {D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}. (.Microsoft Corporation - DLL d'extension d'environnement de stockage.)

---\ RACCOURCIS DES MENUS CONTEXTUELS (SCMH) (65) - 2s
O108 - CMH1:  FileSyncEx [64Bits] - {CB3D0F55-BC2C-4C1A-85ED-23ED75B5106B} . (.Orphan.) [Unsigned]
O108 - CMH1: 7-Zip [64Bits] - {23170F69-40C1-278A-1000-000100020000} . (.Orphan.) [Unsigned]
O108 - CMH1: AccExt [64Bits] - {2A118EB5-5797-4F5E-8B3D-F4ECBA3C98E4} . (.2013-2018, Adobe Systems Incorporated. All rights res - Core Sync.) -- C:\Pr
O108 - CMH1: ANotepad++64 [64Bits] - {B298D29A-A6ED-11DE-BA8C-A68E55D89593} . (. - ShellHandler for Notepad++ (64 bit).) -- C:\Program Files (x86)\Not
O108 - CMH1: avast [64Bits] - {472083B0-C522-11CF-8763-00608CC02F24} . (.AVAST Software - Avast Shell Extension.) -- C:\Program Files\AVAST Software\A
O108 - CMH1: BriefcaseMenu [64Bits] - {85BBD920-42A0-1069-A2E4-08002B30309D} . (.Orphan.) [Unsigned]
O108 - CMH1: DropboxExt [64Bits] - {ECD97DE5-3C8F-4ACB-AEEE-CCAB78F7711C} . (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Drop
O108 - CMH1: EPP [64Bits] - {09A47860-11B0-4DA5-AFA5-26D86198A780} . (.Microsoft Corporation - Extension Microsoft Security Client Shell.) -- C:\Progr
O108 - CMH1: Glary Utilities [64Bits] - {B3C418F8-922B-4faf-915E-59BC14448CF7} . (.Glarysoft Ltd - Context Menu Handler.) -- C:\Program Files (x86)\Gl
O108 - CMH1: IObit Malware Fighter [64Bits] -  . (.Orphan.) [Unsigned]
O108 - CMH1: IObitUnstaler [64Bits] - {836AB26C-2DE4-41D3-AC24-4C6C2699B960} . (.Orphan.) [Unsigned]
O108 - CMH1: MEGA (Context menu) [64Bits] - {0229E5E7-09E9-45CF-9228-0228EC7D5F17} . (...) -- C:\ProgramData\MEGAsync\ShellExtX64.dll [Unsigned]  =>.M
O108 - CMH1: ModernSharing [64Bits] - {e2bf9676-5f8f-435c-97eb-11607a5bedf7} . (.Microsoft Corporation - Extensions de l'interpréteur de commandes p.)
O108 - CMH1: Open With [64Bits] - {09799AFB-AD67-11d1-ABCD-00C04FC30936} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\Windows\Syst
O108 - CMH1: Open With EncryptionMenu [64Bits] - {A470F8CF-A1E8-4f65-8335-227475AA5C46} . (.Microsoft Corporation - DLL commune du shell Windows.) --
O108 - CMH1: PowerISO [64Bits] - {967B2D40-8B7D-4127-9049-61EA0C2C6DCE} . (.Power Software Ltd - PowerISOShell DLL.) -- C:\Program Files\PowerISO\PWRI
O108 - CMH1: Sharing [64Bits] - {f81e9010-6ea4-11ce-a7ff-00aa003ca9f6} . (.Microsoft Corporation - Extensions de l'interpréteur de commandes p.) -- C
O108 - CMH1: WinRAR [64Bits] - {B41DB860-64E4-11D2-9906-E49FADC173CA} . (.Alexander Roshal - WinRAR shell extension.) -- C:\Program Files (x86)\WinRAR
O108 - CMH1: WinRAR32 [64Bits] - {B41DB860-8EE4-11D2-9906-E49FADC173CA} . (.Orphan.) [Unsigned]
O108 - CMH1: WorkFolders [64Bits] - {E61BF828-5E63-4287-BEF1-60B1A4FDE0E3} . (.Microsoft Corporation - Extension d'environnement de Dossiers de tr.) -
O108 - CMH2: DropboxExt [64Bits] - {ECD97DE5-3C8F-4ACB-AEEE-CCAB78F7711C} . (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Drop
O108 - CMH2: IObitUnstaler [64Bits] - {836AB26C-2DE4-41D3-AC24-4C6C2699B960} . (.Orphan.) [Unsigned]
O108 - CMH2: NvAppShExt [64Bits] - {A929C4CE-FD36-4270-B4F5-34ECAC5BD63C} . (.NVIDIA Corporation - NVIDIA Shell Extensions.) -- C:\WINDOWS\system32\nv
O108 - CMH2: OpenContainingFolderMenu [64Bits] - {37ea3a21-7493-4208-a011-7f9ea79ce9f5} . (.Microsoft Corporation - DLL commune du shell Windows.) --
O108 - CMH2: OpenGLShExt [64Bits] - {E97DEC16-A50D-49bb-AE24-CF682282E08D} . (.NVIDIA Corporation - NVIDIA Shell Extensions.) -- C:\WINDOWS\system32\r
O108 - CMH2: WinRAR [64Bits] - {B41DB860-64E4-11D2-9906-E49FADC173CA} . (.Alexander Roshal - WinRAR shell extension.) -- C:\Program Files (x86)\WinRAR
O108 - CMH2: WinRAR32 [64Bits] - {B41DB860-8EE4-11D2-9906-E49FADC173CA} . (.Orphan.) [Unsigned]
O108 - CMH3: 00asw [64Bits] - {472083B0-C522-11CF-8763-00608CC02F24} . (.AVAST Software - Avast Shell Extension.) -- C:\Program Files\AVAST Software\A
O108 - CMH3: CopyAsPathMenu [64Bits] - {f3d06e7c-1e45-4a26-847e-f9fcdee59be0} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\Windows
O108 - CMH3: MEGA (Context menu) [64Bits] - {0229E5E7-09E9-45CF-9228-0228EC7D5F17} . (...) -- C:\ProgramData\MEGAsync\ShellExtX64.dll [Unsigned]  =>.M
O108 - CMH3: SendTo [64Bits] - {7BA4C740-9E81-11CF-99D3-00AA004AE837} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\Windows\System3
O108 - CMH4:  FileSyncEx [64Bits] - {CB3D0F55-BC2C-4C1A-85ED-23ED75B5106B} . (.Orphan.) [Unsigned]
O108 - CMH4: 7-Zip [64Bits] - {23170F69-40C1-278A-1000-000100020000} . (.Orphan.) [Unsigned]
O108 - CMH4: DropboxExt [64Bits] - {ECD97DE5-3C8F-4ACB-AEEE-CCAB78F7711C} . (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Drop
O108 - CMH4: EncryptionMenu [64Bits] - {A470F8CF-A1E8-4f65-8335-227475AA5C46} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\Windows
O108 - CMH4: EPP [64Bits] - {09A47860-11B0-4DA5-AFA5-26D86198A780} . (.Microsoft Corporation - Extension Microsoft Security Client Shell.) -- C:\Progr
O108 - CMH4: IObit Malware Fighter [64Bits] -  . (.Orphan.) [Unsigned]
O108 - CMH4: IObitUnstaler [64Bits] - {836AB26C-2DE4-41D3-AC24-4C6C2699B960} . (.Orphan.) [Unsigned]
O108 - CMH4: MEGA (Context menu) [64Bits] - {0229E5E7-09E9-45CF-9228-0228EC7D5F17} . (...) -- C:\ProgramData\MEGAsync\ShellExtX64.dll [Unsigned]  =>.M
O108 - CMH4: PowerISO [64Bits] - {967B2D40-8B7D-4127-9049-61EA0C2C6DCE} . (.Power Software Ltd - PowerISOShell DLL.) -- C:\Program Files\PowerISO\PWRI
O108 - CMH4: Sharing [64Bits] - {f81e9010-6ea4-11ce-a7ff-00aa003ca9f6} . (.Microsoft Corporation - Extensions de l'interpréteur de commandes p.) -- C
O108 - CMH4: WorkFolders [64Bits] - {E61BF828-5E63-4287-BEF1-60B1A4FDE0E3} . (.Microsoft Corporation - Extension d'environnement de Dossiers de tr.) -
O108 - CMH5: DropboxExt [64Bits] - {ECD97DE5-3C8F-4ACB-AEEE-CCAB78F7711C} . (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Drop
O108 - CMH5: New [64Bits] - {D969A300-E7FF-11d0-A93B-00A0C90F2719} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\Windows\System32\s
O108 - CMH5: NvCplDesktopContext [64Bits] - {3D1975AF-48C6-4f8e-A182-BE0E08FA86A9} . (.NVIDIA Corporation - NVIDIA Display Shell Extension.) -- C:\WIN
O108 - CMH5: Sharing [64Bits] - {f81e9010-6ea4-11ce-a7ff-00aa003ca9f6} . (.Microsoft Corporation - Extensions de l'interpréteur de commandes p.) -- C
O108 - CMH5: WorkFolders [64Bits] - {E61BF828-5E63-4287-BEF1-60B1A4FDE0E3} . (.Microsoft Corporation - Extension d'environnement de Dossiers de tr.) -
O108 - CMH6: 7-Zip [64Bits] - {23170F69-40C1-278A-1000-000100020000} . (.Orphan.) [Unsigned]
O108 - CMH6: AccExt [64Bits] - {2A118EB5-5797-4F5E-8B3D-F4ECBA3C98E4} . (.2013-2018, Adobe Systems Incorporated. All rights res - Core Sync.) -- C:\Pr
O108 - CMH6: avast [64Bits] - {472083B0-C522-11CF-8763-00608CC02F24} . (.AVAST Software - Avast Shell Extension.) -- C:\Program Files\AVAST Software\A
O108 - CMH6: BriefcaseMenu [64Bits] - {85BBD920-42A0-1069-A2E4-08002B30309D} . (.Orphan.) [Unsigned]
```

```
O108 - CMH6: Glary Utilities [64Bits] - {B3C418F8-922B-4faf-915E-59BC14448CF7} . (.Glarysoft Ltd - Context Menu Handler.) -- C:\Program Files (x86)\Gl
O108 - CMH6: IObitUnstaler [64Bits] - {836AB26C-2DE4-41D3-AC24-4C6C2699B960} . (.Orphan.) [Unsigned]
O108 - CMH6: Library Location [64Bits] - {3dad6c5d-2167-4cae-9914-f99e41c12cfa} . (.Microsoft Corporation - DLL commune du shell Windows.) -- C:\Windo
O108 - CMH6: PintoStartScreen [64Bits] - {470C0EBD-5D73-4d58-9CED-E91E22E23282} . (.Microsoft Corporation - Programme de résolution d'applications.) -
O108 - CMH6: PowerISO [64Bits] - {967B2D40-8B7D-4127-9049-61EA0C2C6DCE} . (.Power Software Ltd - PowerISOShell DLL.) -- C:\Program Files\PowerISO\PWRI
O108 - CMH6: WinRAR [64Bits] - {B41DB860-64E4-11D2-9906-E49FADC173CA} . (.Alexander Roshal - WinRAR shell extension.) -- C:\Program Files (x86)\WinRAR
O108 - CMH6: WinRAR32 [64Bits] - {B41DB860-8EE4-11D2-9906-E49FADC173CA} . (.Orphan.) [Unsigned]
O108 - CMH7: EnhancedStorageShell [64Bits] - {2854F705-3548-414C-A113-93E27C808C85} . (.Microsoft Corporation - DLL d'extension d'environnement de sto
O108 - CMH7: EPP [64Bits] - {09A47860-11B0-4DA5-AFA5-26D86198A780} . (.Microsoft Corporation - Extension Microsoft Security Client Shell.) -- C:\Progr
O108 - CMH7: Glary Utilities [64Bits] - {B3C418F8-922B-4faf-915E-59BC14448CF7} . (.Glarysoft Ltd - Context Menu Handler.) -- C:\Program Files (x86)\Gl
O108 - CMH7: MEGA (Context menu) [64Bits] - {0229E5E7-09E9-45CF-9228-0228EC7D5F17} . (...) -- C:\ProgramData\MEGAsync\ShellExtX64.dll [Unsigned]  =>.M
O108 - CMH7: Sharing [64Bits] - {f81e9010-6ea4-11ce-a7ff-00aa003ca9f6} . (.Microsoft Corporation - Extensions de l'interpréteur de commandes p.) -- C
O108 - CMH7: VMDiskMenuHandler [64Bits] - {271DC252-6FE1-4D59-9053-E4CF50AB99DE} . (.Orphan.) [Unsigned]
O108 - CMH7: VMDiskMenuHandler64 [64Bits] - {E4D28EDC-8C0B-43EE-9E7D-C8A8682334DC} . (.VMware, Inc. - VMware Workstation.) -- C:\Program Files (x86)\V

---\ IMAGE FILE EXECUTION OPTIONS (IFEO) (17) - 1s
O50 - IFEO:C:\Windows\System32\cscript.exe - (.Microsoft Corporation - Microsoft ® Console Based Script Host.) [DisableExceptionChainValidation\\3] [U
O50 - IFEO:C:\Windows\System32\dllhost.exe - (.Microsoft Corporation - COM Surrogate.) [DisableExceptionChainValidation\\3]  =>.Microsoft®
O50 - IFEO:C:\WINDOWS\System32\drvinst.exe - (.Microsoft Corporation - Driver Installation Module.) [DisableExceptionChainValidation\\3] [Unsigned]  =
O50 - IFEO:C:\WINDOWS\System32\ie4uinit.exe - (.Microsoft Corporation - Utilitaire d'initialisation d'Internet Expl.) [MitigationOptions\\256] [Unsign
O50 - IFEO:C:\Windows\System32\ieUnatt.exe - (.Microsoft Corporation - Outil d'installation sans assistance d'IE 7.) [MitigationOptions\\256] [Unsigne
O50 - IFEO:C:\Windows\System32\mmc.exe - (.Microsoft Corporation - Microsoft Management Console.) [DisableExceptionChainValidation\\3] [Unsigned]  =>
O50 - IFEO:C:\WINDOWS\System32\MRT.exe - (.Microsoft Corporation - Outil de suppression de logiciels malveilla.) [CFGOptions\\1] [Unsigned]  =>.Micros
O50 - IFEO:C:\Windows\System32\msfeedssync.exe - (.Microsoft Corporation - Microsoft Feeds Synchronization.) [MitigationOptions\\256] [Unsigned]  =>.M
O50 - IFEO:C:\Windows\System32\mshta.exe - (.Microsoft Corporation - Hôte des applications HTML de Microsoft(R).) [MitigationOptions\\256] [Unsigned]
O50 - IFEO:C:\Windows\System32\PresentationHost.exe - (.Microsoft Corporation - Windows Presentation Foundation Host.) [MitigationOptions\\1118481] [U
O50 - IFEO:C:\WINDOWS\System32\PrintIsolationHost.exe - (.Microsoft Corporation - PrintIsolationHost.) [MitigationOptions\\2097152] [Unsigned]  =>.Mic
O50 - IFEO:C:\Windows\System32\rundll32.exe - (.Microsoft Corporation - Processus hôte Windows (Rundll32).) [DisableExceptionChainValidation\\3] [Unsi
O50 - IFEO:C:\WINDOWS\System32\runtimebroker.exe - (.Microsoft Corporation - Runtime Broker.) [MitigationOptions\\4294967296] [Unsigned]  =>.Microsoft
O50 - IFEO:C:\Windows\System32\searchprotocolhost.exe - (.Microsoft Corporation - Microsoft Windows Search Protocol Host.) [DisableExceptionChainValic
O50 - IFEO:C:\WINDOWS\System32\spoolsv.exe - (.Microsoft Corporation - Application sous-système spouleur.) [MitigationOptions\\2097152] [Unsigned]  =>
O50 - IFEO:C:\Windows\System32\svchost.exe - (.Microsoft Corporation - Processus hôte pour les services Windows.) [MinimumStackCommitInBytes\\32768]
O50 - IFEO:C:\Windows\System32\wscript.exe - (.Microsoft Corporation - Microsoft ® Windows Based Script Host.) [DisableExceptionChainValidation\\3] [U

---\ LISTE DES PILOTES DU SYSTÈME (513) - 18s
O58 - SDL:2019/12/07 10:07:53 A . (.Microsoft Corporation - 1394 OpenHCI Driver.) -- C:\WINDOWS\System32\drivers\1394ohci.sys   [266240] [Unsigned]  =
O58 - SDL:2019/12/07 10:07:53 A . (.LSI - LSI 3ware SCSI Storport Driver.) -- C:\WINDOWS\System32\drivers\3ware.sys   [107320]  =>.Microsoft®
O58 - SDL:2020/09/10 22:42:10 A . (.Microsoft Corporation - Pilote ACPI pour NT.) -- C:\WINDOWS\System32\drivers\acpi.sys   [809280]  =>.Microsoft®
O58 - SDL:2019/12/07 10:07:53 A . (.Microsoft Corporation - ACPI Devices Driver.) -- C:\WINDOWS\System32\drivers\AcpiDev.sys   [23040] [Unsigned]  =>
O58 - SDL:2019/12/07 10:08:09 A . (.Microsoft Corporation - ACPIEx Driver.) -- C:\WINDOWS\System32\drivers\acpiex.sys   [139792]  =>.Microsoft®
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - ACPI Processor Aggregator Device Driver.) -- C:\WINDOWS\System32\drivers\acpipagr.sys   [1
O58 - SDL:2019/12/07 10:07:50 A . (.Microsoft Corporation - ACPI Power Metering Driver.) -- C:\WINDOWS\System32\drivers\acpipmi.sys   [18432] [Unsigne
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - ACPI Wake Alarm.) -- C:\WINDOWS\System32\drivers\acpitime.sys   [16384] [Unsigned]  =>.Mic
O58 - SDL:2019/12/07 10:08:09 A . (.Microsoft Corporation - Audio KMDF Class Extension.) -- C:\WINDOWS\System32\drivers\Acx01000.sys   [415232] [Unsig
O58 - SDL:2019/12/07 10:07:53 A . (.PMC-Sierra - PMC-Sierra Storport Driver For SPC8x6G SAS.) -- C:\WINDOWS\System32\drivers\adp80xx.sys   [1135416]
O58 - SDL:2020/09/10 22:42:40 A . (.Microsoft Corporation - Pilote de fonction connexe pour WinSock.) -- C:\WINDOWS\System32\drivers\afd.sys   [647480
O58 - SDL:2020/09/10 22:42:45 A . (.Microsoft Corporation - AF_UNIX socket provider.) -- C:\WINDOWS\System32\drivers\afunix.sys   [41984] [Unsigned]
O58 - SDL:2020/11/13 18:55:08 A . (.Microsoft Corporation - Gestionnaire d'appels RAS Agile Vpn Minipor.) -- C:\WINDOWS\System32\drivers\agilevpn.sys
O58 - SDL:2019/12/07 10:08:58 A . (.Microsoft Corporation - Application Compatibility Cache.) -- C:\WINDOWS\System32\drivers\ahcache.sys   [292864] [U
O58 - SDL:2019/12/07 10:07:47 A . (.Advanced Micro Devices, Inc - AMD GPIO Controller Driver.) -- C:\WINDOWS\System32\drivers\amdgpio2.sys   [18432]
O58 - SDL:2019/12/07 10:07:47 A . (.Advanced Micro Devices, Inc - AMD I2C Controller Driver.) -- C:\WINDOWS\System32\drivers\amdi2c.sys   [45568] [Uns
O58 - SDL:2020/10/16 13:24:14 A . (.Microsoft Corporation - Processor Device Driver.) -- C:\WINDOWS\System32\drivers\amdk8.sys   [207160]  =>.Microsof
O58 - SDL:2020/10/16 13:24:14 A . (.Microsoft Corporation - Processor Device Driver.) -- C:\WINDOWS\System32\drivers\amdppm.sys   [211256]  =>.Microsc
O58 - SDL:2019/12/07 10:07:53 A . (.Advanced Micro Devices - AHCI 1.3 Device Driver.) -- C:\WINDOWS\System32\drivers\amdsata.sys   [83256]  =>.Microsc
O58 - SDL:2019/12/07 10:07:53 A . (.AMD Technologies Inc. - AMD Technology AHCI Compatible Controller D.) -- C:\WINDOWS\System32\drivers\amdsbs.sys
O58 - SDL:2019/12/07 10:07:53 A . (.Advanced Micro Devices - Storage Filter Driver.) -- C:\WINDOWS\System32\drivers\amdxata.sys   [26936]  =>.Microsof
O58 - SDL:2020/10/16 13:24:44 A . (.Microsoft Corporation - AppID Driver.) -- C:\WINDOWS\System32\drivers\appid.sys   [208696]  =>.Microsoft®
O58 - SDL:2018/05/10 14:05:04 A . (.Apple Inc. - Apple Mobile Device USB Device.) -- C:\WINDOWS\System32\drivers\AppleLowerFilter.sys   [35560]  =>.WD
O58 - SDL:2020/10/16 13:24:44 A . (.Microsoft Corporation - Applocker Filter.) -- C:\WINDOWS\System32\drivers\applockerfltr.sys   [18432] [Unsigned]
O58 - SDL:2019/12/07 10:07:53 A . (.PMC-Sierra, Inc. - Adaptec SAS RAID WS03 Driver.) -- C:\WINDOWS\System32\drivers\arcsas.sys   [131896]  =>.Microsc
O58 - SDL:2020/11/24 13:53:20 A . (.AVAST Software - Avast Anti Rootkit Disk Filter.) -- C:\WINDOWS\System32\drivers\aswArDisk.sys   [37152]  =>.Avast
O58 - SDL:2020/11/24 13:53:20 A . (.AVAST Software - Avast Anti Rootkit.) -- C:\WINDOWS\System32\drivers\aswArPot.sys   [206408]  =>.Avast Software s
O58 - SDL:2020/11/24 13:53:20 A . (.AVAST Software - Avast IDS Application Activity Monitor Driv.) -- C:\WINDOWS\System32\drivers\aswbidsdriver.sys
O58 - SDL:2020/11/24 13:53:23 A . (.AVAST Software - Avast Application Activity Monitor Helper D.) -- C:\WINDOWS\System32\drivers\aswbidsh.sys   [2478
O58 - SDL:2020/11/24 13:53:23 A . (.AVAST Software - Avast Universal Driver.) -- C:\WINDOWS\System32\drivers\aswbuniv.sys   [97352]  =>.Avast Software
O58 - SDL:2020/11/24 13:53:22 A . (.AVAST Software - Avast ELAM Driver.) -- C:\WINDOWS\System32\drivers\aswElam.sys   [16816]  =>.Microsoft®
O58 - SDL:2020/11/24 13:53:22 A . (.AVAST Software - Avast Keyboard Filter Driver.) -- C:\WINDOWS\System32\drivers\aswKbd.sys   [42784]  =>.Avast Soft
O58 - SDL:2020/11/24 13:53:22 A . (.AVAST Software - Avast File System Filter.) -- C:\WINDOWS\System32\drivers\aswMonFlt.sys   [176744]  =>.Avast Soft
O58 - SDL:2020/11/24 13:53:22 A . (.AVAST Software - Avast Network Security Driver.) -- C:\WINDOWS\System32\drivers\aswNetHub.sys   [521752]  =>.Avast
O58 - SDL:2020/11/24 13:53:22 A . (.AVAST Software - Avast Antivirus.) -- C:\WINDOWS\System32\drivers\aswRdr2.sys   [109280]  =>.Avast Software s.r.o
O58 - SDL:2020/11/24 13:53:22 A . (.AVAST Software - Avast Revert.) -- C:\WINDOWS\System32\drivers\aswRvrt.sys   [84856]  =>.Avast Software s.r.o.® (A
O58 - SDL:2020/11/24 13:53:20 A . (.AVAST Software - Avast Antivirus.) -- C:\WINDOWS\System32\drivers\aswSnx.sys   [851608]  =>.Avast Software s.r.o.®
O58 - SDL:2020/11/24 13:53:22 A . (.AVAST Software - Avast Self Protection.) -- C:\WINDOWS\System32\drivers\aswSP.sys   [469832]  =>.Avast Software s
O58 - SDL:2020/11/24 13:53:23 A . (.AVAST Software - Avast Stream Filter.) -- C:\WINDOWS\System32\drivers\aswStm.sys   [217336]  =>.Avast Software s.r
O58 - SDL:2020/05/16 23:13:19 A . (.The OpenVPN Project - TAP-Windows Virtual Network Driver.) -- C:\WINDOWS\System32\drivers\aswTap.sys   [53904]  =>
O58 - SDL:2020/11/24 13:53:23 A . (.AVAST Software - Avast VM Monitor.) -- C:\WINDOWS\System32\drivers\aswVmm.sys   [326416]  =>.Avast Software s.r.o
O58 - SDL:2020/07/16 11:22:34 A . (.Avast Software - Avast SecureLine.) -- C:\WINDOWS\System32\drivers\aswVpnRdr.sys   [59312]  =>.Avast Software s.r
O58 - SDL:2019/12/07 10:09:07 A . (.Microsoft Corporation - MS Remote Access serial network driver.) -- C:\WINDOWS\System32\drivers\asyncmac.sys   [31
O58 - SDL:2020/09/10 22:42:10 A . (.Microsoft Corporation - ATAPI IDE Miniport Driver.) -- C:\WINDOWS\System32\drivers\atapi.sys   [30024]  =>.Microsc
O58 - SDL:2020/09/10 22:42:10 A . (.Microsoft Corporation - ATAPI Driver Extension.) -- C:\WINDOWS\System32\drivers\ataport.sys   [223040]  =>.Microsc
O58 - SDL:2019/12/07 10:08:41 A . (.Microsoft Corporation - BAM Kernel Driver.) -- C:\WINDOWS\System32\drivers\bam.sys   [78136]  =>.Microsoft®
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - Battery Class Driver.) -- C:\WINDOWS\System32\drivers\battc.sys   [41272]  =>.Microsoft®
O58 - SDL:2019/12/07 10:07:47 A . (. - BCM Function 2 Device Driver.) -- C:\WINDOWS\System32\drivers\bcmfn2.sys   [9728] [Unsigned]  =>.Broadcom Corpo
O58 - SDL:2019/12/07 10:09:00 A . (.Microsoft Corporation - BEEP Driver.) -- C:\WINDOWS\System32\drivers\beep.sys   [10240] [Unsigned]  =>.Microsoft C
O58 - SDL:2020/06/12 23:05:13 A . (.Microsoft Corporation - Windows Bind Filter Driver.) -- C:\WINDOWS\System32\drivers\bindflt.sys   [143160]  =>.Mic
O58 - SDL:2019/12/07 10:08:12 A . (.Microsoft Corporation - NT Lan Manager Datagram Receiver Driver.) -- C:\WINDOWS\System32\drivers\bowser.sys   [117
O58 - SDL:2019/12/07 10:09:39 A . (.Microsoft Corporation - MAC Bridge Driver.) -- C:\WINDOWS\System32\drivers\bridge.sys   [127488] [Unsigned]  =>.Mi
O58 - SDL:2019/12/07 10:07:47 A . (.Microsoft Corporation - Microsoft Bluetooth Audio Multiprofile Mana.) -- C:\WINDOWS\System32\drivers\BtaMPM.sys
O58 - SDL:2020/09/10 22:42:09 A . (.Microsoft Corporation - Bluetooth A2DP Driver.) -- C:\WINDOWS\System32\drivers\BthA2dp.sys   [279040] [Unsigned]
O58 - SDL:2020/09/10 22:42:10 A . (.Microsoft Corporation - Extension de bus Bluetooth.) -- C:\WINDOWS\System32\drivers\bthenum.sys   [113664] [Unsigr
O58 - SDL:2019/12/07 10:07:47 A . (.Microsoft Corporation - Bluetooth Hands-free Audio Device Driver.) -- C:\WINDOWS\System32\drivers\BthHfAud.sys
O58 - SDL:2019/12/07 10:07:47 A . (.Microsoft Corporation - Bluetooth Hands-Free Audio and Call Control.) -- C:\WINDOWS\System32\drivers\BthHfEnum.sys
O58 - SDL:2020/09/10 22:42:10 A . (.Microsoft Corporation - Bluetooth Transport Extensibility Miniport.) -- C:\WINDOWS\System32\drivers\BthMini.SYS
O58 - SDL:2019/12/07 10:07:50 A . (.Microsoft Corporation - Bluetooth Communications Driver.) -- C:\WINDOWS\System32\drivers\bthmodem.sys   [76800] [U
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Bluetooth Personal Area Networking.) -- C:\WINDOWS\System32\drivers\bthpan.sys   [133632]
O58 - SDL:2020/09/10 22:42:10 A . (.Microsoft Corporation - Pilote de bus Bluetooth.) -- C:\WINDOWS\System32\drivers\bthport.sys   [1548288] [Unsigned
O58 - SDL:2020/09/10 22:42:10 A . (.Microsoft Corporation - Pilote de Miniport Bluetooth.) -- C:\WINDOWS\System32\drivers\BTHUSB.SYS   [110592] [Unsig
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - VHD BTT Filter Driver.) -- C:\WINDOWS\System32\drivers\bttflt.sys   [43832]  =>.Microsoft®
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Button Converter Driver.) -- C:\WINDOWS\System32\drivers\buttonconverter.sys   [44032] [Un
O58 - SDL:2019/12/07 10:07:50 A . (.QLogic Corporation - QLogic Gigabit Ethernet VBD.) -- C:\WINDOWS\System32\drivers\bxvbda.sys   [533816]  =>.Micros
O58 - SDL:2019/12/07 10:07:47 A . (.Microsoft Corporation - Charge Arbiration Driver.) -- C:\WINDOWS\System32\drivers\CAD.sys   [66576]  =>.Microsoft®
O58 - SDL:2018/03/29 07:57:16 A . (.Callback Technologies, Inc. - CBFS Connect Driver.) -- C:\WINDOWS\System32\drivers\cbfsconnect2017.sys   [475224]
O58 - SDL:2018/01/30 12:28:08 A . (.Callback Technologies, Inc. - CBFS Filter (filesystem filter driver).) -- C:\WINDOWS\System32\drivers\cbfsfilter26
O58 - SDL:2019/12/07 10:09:37 A . (.Microsoft Corporation - CD-ROM File System Driver.) -- C:\WINDOWS\System32\drivers\cdfs.sys   [100864] [Unsigned]
```

```
O58 - SDL:2011/10/17 02:00:00 A . (.Sonic Solutions - CDR4 64-bit CD and DVD Place Holder Driver.) -- C:\WINDOWS\System32\drivers\cdr4_xp.sys   [10224
O58 - SDL:2011/10/17 02:00:00 A . (.Sonic Solutions - CDRAL 64-bit Place Holder Driver (see PxHel.) -- C:\WINDOWS\System32\drivers\cdralw2k.sys   [102
O58 - SDL:2019/12/07 10:07:53 A . (.Microsoft Corporation - SCSI CD-ROM Driver.) -- C:\WINDOWS\System32\drivers\cdrom.sys   [174080] [Unsigned]  =>.Mi
O58 - SDL:2019/12/07 10:08:33 A . (.Microsoft Corporation - Event Aggregation Kernel Mode Library.) -- C:\WINDOWS\System32\drivers\CEA.sys   [81720]
O58 - SDL:2019/12/07 10:07:54 A . (.Chelsio Communications - Chelsio iSCSI Crash Dump Driver.) -- C:\WINDOWS\System32\drivers\cht4dx64.sys   [144184]
O58 - SDL:2019/12/07 10:07:54 A . (.Chelsio Communications - Chelsio iSCSI VMiniport Driver.) -- C:\WINDOWS\System32\drivers\cht4sx64.sys   [319800]
O58 - SDL:2019/12/07 10:07:54 A . (.Chelsio Communications - VF library for Chelsio ® T5/T6 Chipset.) -- C:\WINDOWS\System32\drivers\cht4vfx.sys   [28
O58 - SDL:2019/12/07 10:07:54 A . (.Chelsio Communications - Virtual Bus Driver for Chelsio ® T5/T6 Chip.) -- C:\WINDOWS\System32\drivers\cht4vx64.sys
O58 - SDL:2019/12/07 10:08:34 A . (...) -- C:\WINDOWS\System32\drivers\cimfs.sys   [91136] [Unsigned]  =>.Microsoft Corporation
O58 - SDL:2019/12/07 10:07:50 A . (.Microsoft Corporation - Consumer IR Class Driver for eHome.) -- C:\WINDOWS\System32\drivers\circlass.sys   [52224]
O58 - SDL:2019/12/07 10:08:49 A . (.Microsoft Corporation - SCSI Class System Dll.) -- C:\WINDOWS\System32\drivers\Classpnp.sys   [417080]  =>.Microsc
O58 - SDL:2020/09/10 22:42:37 A . (.Microsoft Corporation - Cloud Files Mini Filter Driver.) -- C:\WINDOWS\System32\drivers\cldflt.sys   [491520] [Uns
O58 - SDL:2020/11/13 18:55:06 A . (.Microsoft Corporation - Common Log File System Driver.) -- C:\WINDOWS\System32\drivers\clfs.sys   [409408]  =>.Mic
O58 - SDL:2020/10/16 13:24:24 A . (.Microsoft Corporation - CLIP Service.) -- C:\WINDOWS\System32\drivers\ClipSp.sys   [1089856]  =>.Microsoft®
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - Control Method Battery Driver.) -- C:\WINDOWS\System32\drivers\CmBatt.sys   [36864] [Unsig
O58 - SDL:2019/12/07 10:08:09 A . (.Microsoft Corporation - Noyau Gestionnaire de configuration Configu.) -- C:\WINDOWS\System32\drivers\cmimcext.sys
O58 - SDL:2018/07/24 22:50:40 A . (.C-MEDIA - C-MEDIA CMUSBDAC Audio Driver.) -- C:\WINDOWS\System32\drivers\CMUSBDAC.sys   [3819744] {4038604836B4D4E
O58 - SDL:2020/11/13 18:55:05 A . (.Microsoft Corporation - Kernel Cryptography, Next Generation.) -- C:\WINDOWS\System32\drivers\cng.sys   [732448]
O58 - SDL:2019/12/07 10:08:37 A . (.Microsoft Corporation - CNG Hardware Assist algorithm provider.) -- C:\WINDOWS\System32\drivers\cnghwassist.sys
O58 - SDL:2019/12/07 10:08:34 A . (.Microsoft Corporation - Console Driver.) -- C:\WINDOWS\System32\drivers\condrv.sys   [58168]  =>.Microsoft®
O58 - SDL:2019/12/07 10:08:49 A . (.Microsoft Corporation - Crash Dump Driver.) -- C:\WINDOWS\System32\drivers\crashdmp.sys   [99368]  =>.Microsoft®
O58 - SDL:2019/12/07 10:08:41 A . (.Microsoft Corporation - DAM Kernel Driver.) -- C:\WINDOWS\System32\drivers\dam.sys   [97080]  =>.Microsoft®
O58 - SDL:2020/12/01 23:10:50 A . (.Dropbox, Inc. - Dropbox Filter Driver.) -- C:\WINDOWS\System32\drivers\dbx-canary.sys   [47600]  =>.Microsoft®
O58 - SDL:2020/12/01 23:10:50 A . (.Dropbox, Inc. - Dropbox Filter Driver.) -- C:\WINDOWS\System32\drivers\dbx-dev.sys   [47600]  =>.Microsoft®
O58 - SDL:2020/12/01 23:10:50 A . (.Dropbox, Inc. - Dropbox Filter Driver.) -- C:\WINDOWS\System32\drivers\dbx-stable.sys   [47600]  =>.Microsoft®
O58 - SDL:2020/11/13 18:54:45 A . (.Microsoft Corporation - Xbox Device Authentication Driver.) -- C:\WINDOWS\System32\drivers\devauthe.sys   [47104]
O58 - SDL:2019/12/07 10:08:51 A . (.Microsoft Corporation - DFS Namespace Client Driver.) -- C:\WINDOWS\System32\drivers\dfsc.sys   [152064] [Unsigned
O58 - SDL:2019/12/07 10:07:53 A . (.Microsoft Corporation - PnP Disk Driver.) -- C:\WINDOWS\System32\drivers\disk.sys   [98856]  =>.Microsoft®
O58 - SDL:2019/12/07 10:08:52 A . (.Microsoft Corporation - Crash Dump Disk Driver.) -- C:\WINDOWS\System32\drivers\Diskdump.sys   [38200]  =>.Microsc
O58 - SDL:2019/12/07 10:08:52 A . (.Microsoft Corporation - Boot Over USB Dump Driver.) -- C:\WINDOWS\System32\drivers\Dmpusbstor.sys   [15360] [Unsig
O58 - SDL:2019/12/07 10:07:57 A . (.Microsoft Corporation - Mémoire dynamique.) -- C:\WINDOWS\System32\drivers\dmvsc.sys   [59192]  =>.Microsoft®
O58 - SDL:2020/11/13 18:54:45 A . (.Microsoft Corporation - Microsoft Trusted Audio Drivers.) -- C:\WINDOWS\System32\drivers\drmk.sys   [97792] [Unsig
O58 - SDL:2020/11/13 18:54:45 A . (.Microsoft Corporation - Microsoft Trusted Audio Drivers.) -- C:\WINDOWS\System32\drivers\drmkaud.sys   [16136]  =>
O58 - SDL:2019/12/07 10:08:46 A . (.Microsoft Corporation - ATAPI Dump Driver.) -- C:\WINDOWS\System32\drivers\Dumpata.sys   [37392]  =>.Microsoft®
O58 - SDL:2020/10/16 13:25:45 A . (.Microsoft Corporation - Bitlocker Drive Encryption Crashdump Filter.) -- C:\WINDOWS\System32\drivers\dumpfve.sys
O58 - SDL:2020/11/13 18:54:46 A . (.Microsoft Corporation - SD Crashdump Port Driver.) -- C:\WINDOWS\System32\drivers\dumpsd.sys   [195400]  =>.Micros
O58 - SDL:2019/12/07 10:08:37 A . (.Microsoft Corporation - SD Host Controller Crashdump Port Driver.) -- C:\WINDOWS\System32\drivers\dumpsdport.sys
O58 - SDL:2019/12/07 10:08:52 A . (.Microsoft Corporation - Storport Dump Driver.) -- C:\WINDOWS\System32\drivers\Dumpstorport.sys   [35128]  =>.Micro
O58 - SDL:2020/11/13 18:54:56 A . (.Microsoft Corporation - DirectX Graphics Kernel.) -- C:\WINDOWS\System32\drivers\dxgkrnl.sys   [3779392]  =>.Micro
O58 - SDL:2020/11/13 18:54:56 A . (.Microsoft Corporation - DirectX Graphics MMS.) -- C:\WINDOWS\System32\drivers\dxgmms1.sys   [454968]  =>.Microsoft
O58 - SDL:2020/11/13 18:54:56 A . (.Microsoft Corporation - DirectX Graphics MMS.) -- C:\WINDOWS\System32\drivers\dxgmms2.sys   [904008]  =>.Microsoft
O58 - SDL:2019/12/07 10:09:37 A . (.Microsoft Corporation - Enhanced Storage Class driver for IEEE 1667.) -- C:\WINDOWS\System32\drivers\EhStorClass.s
O58 - SDL:2019/12/07 10:07:50 A . (.Microsoft Corporation - Microsoft driver for storage devices suppor.) -- C:\WINDOWS\System32\drivers\EhStorTcgDrv
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - Error Device Driver.) -- C:\WINDOWS\System32\drivers\errdev.sys   [15872] [Unsigned]  =>.M
O58 - SDL:2019/12/07 10:07:50 A . (.QLogic Corporation - QLogic 10 GigE VBD.) -- C:\WINDOWS\System32\drivers\evbda.sys   [3418936]  =>.Microsoft®
O58 - SDL:2019/12/07 10:08:05 A . (.Microsoft Corporation - Microsoft Extended FAT File System.) -- C:\WINDOWS\System32\drivers\exfat.sys   [415032]
O58 - SDL:2020/10/16 13:24:15 A . (.Microsoft Corporation - Fast FAT File System Driver.) -- C:\WINDOWS\System32\drivers\fastfat.sys   [425272]  =>.Mi
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - Floppy Disk Controller Driver.) -- C:\WINDOWS\System32\drivers\fdc.sys   [34816] [Unsigned
O58 - SDL:2019/12/07 10:08:09 A . (.Microsoft Corporation - Windows sandboxing and encryption filter.) -- C:\WINDOWS\System32\drivers\filecrypt.sys
O58 - SDL:2019/12/07 10:08:46 A . (.Microsoft Corporation - FileInfo Filter Driver.) -- C:\WINDOWS\System32\drivers\fileinfo.sys   [94736]  =>.Microsc
O58 - SDL:2019/12/07 10:08:46 A . (.Microsoft Corporation - File Trace Filter Driver.) -- C:\WINDOWS\System32\drivers\filetrace.sys   [40448] [Unsigne
O58 - SDL:2019/01/23 01:17:47 A . (.Challenger Backup Solutions, LLC - System Reflection Filter Driver.) -- C:\WINDOWS\System32\drivers\FlashBoot.sys
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - Floppy Driver.) -- C:\WINDOWS\System32\drivers\flpydisk.sys   [28672] [Unsigned]  =>.Micro
O58 - SDL:2020/05/11 06:40:33 A . (.Microsoft Corporation - Gestionnaire de filtres de système de fichi.) -- C:\WINDOWS\System32\drivers\fltMgr.sys
O58 - SDL:2019/12/07 10:08:09 A . (.Microsoft Corporation - File System Dependency Manager Mini Filter.) -- C:\WINDOWS\System32\drivers\fsdepends.sys
O58 - SDL:2019/12/07 10:08:49 A . (.Microsoft Corporation - File System Recognizer Driver.) -- C:\WINDOWS\System32\drivers\fs_rec.sys   [33592]  =>.Mi
O58 - SDL:2020/10/16 13:25:45 A . (.Microsoft Corporation - BitLocker Drive Encryption Driver.) -- C:\WINDOWS\System32\drivers\fvevol.sys   [800072]
O58 - SDL:2020/11/13 18:55:06 A . (.Microsoft Corporation - FWP/IPsec Kernel-Mode API.) -- C:\WINDOWS\System32\drivers\FWPKCLNT.SYS   [502584]  =>.Mic
O58 - SDL:2019/12/07 10:08:05 A . (.Microsoft Corporation - GPU Energy Kernel Driver.) -- C:\WINDOWS\System32\drivers\gpuenergydrv.sys   [8704] [Unsig
O58 - SDL:2019/01/20 16:27:05 A . (.Glarysoft Ltd - The driver for the Startup Manager tool.) -- C:\WINDOWS\System32\drivers\GUBootStartup.sys   [2893
O58 - SDL:2018/11/02 05:21:58 A . (.VMware, Inc. - VMware USB monitor.) -- C:\WINDOWS\System32\drivers\hcmon.sys   [84752]  =>.VMware, Inc.®
O58 - SDL:2019/12/07 10:07:50 A . (.Microsoft Corporation - High Definition Audio Bus Driver.) -- C:\WINDOWS\System32\drivers\hdaudbus.sys   [132608]
O58 - SDL:2020/05/11 06:40:14 A . (.Microsoft Corporation - High Definition Audio Function Driver.) -- C:\WINDOWS\System32\drivers\HdAudio.sys   [4300
O58 - SDL:2019/01/01 15:44:38 A . (.Screenovate Technologies Ltd. - Phone Call Audio Device.) -- C:\WINDOWS\System32\drivers\HfAudio.sys   [83920]  =>
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - Hid Battery Driver.) -- C:\WINDOWS\System32\drivers\hidbatt.sys   [39440]  =>.Microsoft®
O58 - SDL:2020/08/14 21:05:56 A . (.Microsoft Corporation - Pilote de miniport Bluetooth pour les périp.) -- C:\WINDOWS\System32\drivers\hidbth.sys
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Bibliothèque Hid Class.) -- C:\WINDOWS\System32\drivers\hidclass.sys   [225792] [Unsigned]
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - I2C HID Miniport Driver.) -- C:\WINDOWS\System32\drivers\hidi2c.sys   [57344] [Unsigned]
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - HID Button over Interrupt Driver.) -- C:\WINDOWS\System32\drivers\hidinterrupt.sys   [5582
O58 - SDL:2019/12/07 10:07:50 A . (.Microsoft Corporation - Infrared Miniport Driver for Input Devices.) -- C:\WINDOWS\System32\drivers\hidir.sys   [4
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Hid Parsing Library.) -- C:\WINDOWS\System32\drivers\hidparse.sys   [46080] [Unsigned]  =>
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - SPI HID Miniport Driver.) -- C:\WINDOWS\System32\drivers\hidspi.sys   [66560] [Unsigned]
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - USB Miniport Driver for Input Devices.) -- C:\WINDOWS\System32\drivers\hidusb.sys   [44032
O58 - SDL:2020/08/03 23:18:47 A . (...) -- C:\WINDOWS\System32\drivers\HpPortIox64.sys   [31488]  =>.HP Inc.®
O58 - SDL:2019/12/07 10:07:53 A . (.Hewlett-Packard Company - Smart Array SAS/SATA Controller Media Drive.) -- C:\WINDOWS\System32\drivers\HpSAMD.sys
O58 - SDL:2019/12/07 10:08:49 A . (.Microsoft Corporation - HTTP Pile du protocole.) -- C:\WINDOWS\System32\drivers\http.sys   [1567032]  =>.Microsoft
O58 - SDL:2019/12/07 10:07:57 A . (.Microsoft Corporation - Hyper-V Crashdump.) -- C:\WINDOWS\System32\drivers\hvcrash.sys   [35128]  =>.Microsoft®
O58 - SDL:2020/11/13 18:55:15 A . (.Microsoft Corporation - Hypervisor Boot Driver.) -- C:\WINDOWS\System32\drivers\hvservice.sys   [95048]  =>.Micros
O58 - SDL:2019/12/07 10:09:51 A . (.Microsoft Corporation - Microsoft Hyper-V Socket Provider.) -- C:\WINDOWS\System32\drivers\hvsocket.sys   [147984]
O58 - SDL:2020/08/14 21:06:24 A . (.Microsoft Corporation - Hardware Policy Driver.) -- C:\WINDOWS\System32\drivers\hwpolicy.sys   [33096]  =>.Microsc
O58 - SDL:2019/12/07 10:07:57 A . (.Microsoft Corporation - Microsoft VMBus Synthetic Keyboard Driver.) -- C:\WINDOWS\System32\drivers\hyperkbd.sys
O58 - SDL:2019/12/07 10:07:57 A . (.Microsoft Corporation - Microsoft VMBus Video Device Miniport Drive.) -- C:\WINDOWS\System32\drivers\HyperVideo.sy
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Pilote de port i8042.) -- C:\WINDOWS\System32\drivers\i8042prt.sys   [118272] [Unsigned]
O58 - SDL:2019/12/07 10:07:47 A . (.Intel(R) Corporation - Intel(R) Serial IO GPIO Controller Driver.) -- C:\WINDOWS\System32\drivers\iagpio.sys   [36
O58 - SDL:2019/12/07 10:07:47 A . (.Intel(R) Corporation - Intel(R) Serial IO I2C Driver.) -- C:\WINDOWS\System32\drivers\iai2c.sys   [91136] [Unsigne
O58 - SDL:2019/12/07 10:07:47 A . (.Intel Corporation - Intel(R) Serial IO GPIO Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i_GPIO2.sys   [79360
O58 - SDL:2019/12/07 10:07:47 A . (.Intel Corporation - Intel(R) Serial IO GPIO Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i_GPIO2_BXT_P.sys
O58 - SDL:2019/12/07 10:07:47 A . (.Intel Corporation - Intel(R) Serial IO GPIO Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i_GPIO2_CNL.sys   [1
O58 - SDL:2019/12/07 10:07:47 A . (.Intel Corporation - Intel(R) Serial IO GPIO Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i_GPIO2_GLK.sys   [9
O58 - SDL:2019/12/07 10:07:47 A . (.Intel Corporation - Intel(R) Serial IO I2C Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i_I2C.sys   [171520]
O58 - SDL:2019/12/07 10:07:47 A . (.Intel Corporation - Intel(R) Serial IO I2C Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i_I2C_BXT_P.sys   [17
O58 - SDL:2019/12/07 10:07:47 A . (.Intel Corporation - Intel(R) Serial IO I2C Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i_I2C_CNL.sys   [1771
O58 - SDL:2019/12/07 10:07:47 A . (.Intel Corporation - Intel(R) Serial IO I2C Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i_I2C_GLK.sys   [1776
O58 - SDL:2019/12/07 10:07:50 A . (.Intel Corporation - Intel(R) Serial IO GPIO Controller Driver.) -- C:\WINDOWS\System32\drivers\iaLPSSi_GPIO.sys
O58 - SDL:2019/12/07 10:07:50 A . (.Intel Corporation - Intel(R) Serial IO I2C Controller Driver.) -- C:\WINDOWS\System32\drivers\iaLPSSi_I2C.sys   [1
O58 - SDL:2017/05/24 08:07:19 A . (.Intel Corporation - Intel(R) Rapid Storage Technology driver -.) -- C:\WINDOWS\System32\drivers\iaStorA.sys   [891
O58 - SDL:2019/08/05 07:05:46 A . (.Intel Corporation - Intel(R) Rapid Storage Technology driver -.) -- C:\WINDOWS\System32\drivers\iaStorAC.sys   [96
O58 - SDL:2017/05/24 08:07:19 A . (.Intel Corporation - Intel(R) Optane(TM) Memory Minifilter Drive.) -- C:\WINDOWS\System32\drivers\iaStorAfs.sys
O58 - SDL:2019/12/07 10:07:54 A . (.Intel Corporation - Intel(R) Rapid Storage Technology driver (i.) -- C:\WINDOWS\System32\drivers\iaStorAVC.sys
O58 - SDL:2019/12/07 10:07:54 A . (.Intel Corporation - Intel Matrix Storage Manager driver - x64.) -- C:\WINDOWS\System32\drivers\iaStorV.sys   [4121
O58 - SDL:2019/12/07 10:07:54 A . (.Mellanox - InfiniBand Fabric Bus Driver.) -- C:\WINDOWS\System32\drivers\ibbus.sys   [558904]  =>.Microsoft®
O58 - SDL:2020/08/03 23:18:47 A . (.Intel Corporation - Intel(R) Watchdog Timer Driver (Intel(R) WD.) -- C:\WINDOWS\System32\drivers\ICCWDT.sys   [482
O58 - SDL:2020/10/16 13:24:39 A . (.Microsoft Corporation - Indirect displays kernel-mode filter driver.) -- C:\WINDOWS\System32\drivers\IndirectKmd.s
O58 - SDL:2019/12/26 14:40:38 A . (.Intel Corporation - HAXM_Driver.) -- C:\WINDOWS\System32\drivers\IntelHaxm.sys   [190464]  =>.Microsoft®
```

```
O58 - SDL:2020/09/10 22:42:10 A . (.Microsoft Corporation - Intel PCI IDE Driver.) -- C:\WINDOWS\System32\drivers\intelide.sys   [19776]  =>.Microsoft
O58 - SDL:2020/10/16 13:24:14 A . (.Microsoft Corporation - Intel Power Engine Plugin.) -- C:\WINDOWS\System32\drivers\intelpep.sys   [418800]  =>.Mic
O58 - SDL:2019/12/07 10:07:47 A . (.Microsoft Corporation - Intel Power Limit Driver.) -- C:\WINDOWS\System32\drivers\intelpmax.sys   [30720] [Unsigne
O58 - SDL:2020/10/16 13:24:14 A . (.Microsoft Corporation - Processor Device Driver.) -- C:\WINDOWS\System32\drivers\intelppm.sys   [230728]  =>.Micro
O58 - SDL:2020/10/16 13:24:14 A . (.Microsoft Corporation - Intel Telemetry Driver.) -- C:\WINDOWS\System32\drivers\IntelTA.sys   [26608]  =>.Microsof
O58 - SDL:2020/04/21 09:49:50 A . (.Intel Corporation - Intel(R) Overclocking Device Driver.) -- C:\WINDOWS\System32\drivers\iocbios2.sys   [47072] {0
O58 - SDL:2019/12/07 10:08:05 A . (.Microsoft Corporation - Filtre de contrôle de taux d'E/S.) -- C:\WINDOWS\System32\drivers\iorate.sys   [57360]  =>
O58 - SDL:2019/12/07 10:09:07 A . (.Microsoft Corporation - IP FILTER DRIVER.) -- C:\WINDOWS\System32\drivers\ipfltdrv.sys   [90112] [Unsigned]  =>.Mi
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - PILOT IPMI WMI.) -- C:\WINDOWS\System32\drivers\IPMIDrv.sys   [117560]  =>.Microsoft®
O58 - SDL:2019/12/07 10:08:34 A . (.Microsoft Corporation - IP Network Address Translator.) -- C:\WINDOWS\System32\drivers\ipnat.sys   [225280] [Unsig
O58 - SDL:2019/12/07 10:08:09 A . (.Microsoft Corporation - IPT Driver.) -- C:\WINDOWS\System32\drivers\ipt.sys   [59704]  =>.Microsoft®
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - Pilote de bus PNP ISA.) -- C:\WINDOWS\System32\drivers\isapnp.sys   [22840]  =>.Microsoft®
O58 - SDL:2019/12/07 10:07:53 A . (.Avago Technologies - Avago SAS Gen3.5 Driver (StorPort).) -- C:\WINDOWS\System32\drivers\ItSas35i.sys   [172344]
O58 - SDL:2008/05/15 03:28:52 A . (.Atheros Communications, Inc. - Atheros Security NDIS 6.0 Filter Driver.) -- C:\WINDOWS\System32\drivers\jswpslwfx
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Pilote de la classe Clavier.) -- C:\WINDOWS\System32\drivers\kbdclass.sys   [71480]  =>.Mi
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Pilote de filtre clavier HID.) -- C:\WINDOWS\System32\drivers\kbdhid.sys   [46592] [Unsign
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Microsoft Kernel Debugger Network Miniport.) -- C:\WINDOWS\System32\drivers\kdnic.sys   [3
O58 - SDL:2020/11/13 18:54:50 A . (.Microsoft Corporation - Network Power Dependency Broker.) -- C:\WINDOWS\System32\drivers\KNetPwrDepBroker.sys   [3
O58 - SDL:2020/11/13 18:55:07 A . (.Microsoft Corporation - Kernel CSA Library.) -- C:\WINDOWS\System32\drivers\ks.sys   [449024] [Unsigned]  =>.Micro
O58 - SDL:2020/10/16 13:24:50 A . (.Microsoft Corporation - Kernel Security Support Provider Interface.) -- C:\WINDOWS\System32\drivers\ksecdd.sys
O58 - SDL:2020/11/13 18:55:05 A . (.Microsoft Corporation - Kernel Security Support Provider Interface.) -- C:\WINDOWS\System32\drivers\ksecpkg.sys
O58 - SDL:2019/12/07 10:08:58 A . (.Microsoft Corporation - Kernel Streaming WOW Thunk Service.) -- C:\WINDOWS\System32\drivers\ksthunk.sys   [29696]
O58 - SDL:2018/10/05 09:44:14 A . (.Logitech Inc. - Logitech WingMan Virtual Bus Enumerator Dri.) -- C:\WINDOWS\System32\drivers\LGBusEnum.sys   [3649
O58 - SDL:2018/10/05 09:44:14 A . (.Logitech Inc. - Logitech Gaming Software Joystick Hid Filte.) -- C:\WINDOWS\System32\drivers\LGJoyHidFilter.sys
O58 - SDL:2018/10/05 09:44:14 A . (.Logitech Inc. - Logitech WingMan Hid Lower Filter Driver.) -- C:\WINDOWS\System32\drivers\LGJoyHidLo.sys   [47256]
O58 - SDL:2018/10/05 09:44:14 A . (.Logitech Inc. - Logitech Gaming Software Joystick Translati.) -- C:\WINDOWS\System32\drivers\LGJoyXlCore.sys   [67
O58 - SDL:2018/10/05 09:44:14 A . (.Logitech Inc. - Logitech GamePanel Virtual Hid Device Drive.) -- C:\WINDOWS\System32\drivers\LGVirHid.sys   [26008
O58 - SDL:2019/12/07 10:08:55 A . (.Microsoft Corporation - Link-Layer Topology Mapper I/O Driver.) -- C:\WINDOWS\System32\drivers\lltdio.sys   [72704
O58 - SDL:2019/12/08 01:51:14 A . (.Logitech - Logitech G Driver.) -- C:\WINDOWS\System32\drivers\logi_generic_hid_filter.sys   [56584]  =>.Logitech I
O58 - SDL:2019/12/08 01:49:49 A . (.Logitech - Logitech G Driver.) -- C:\WINDOWS\System32\drivers\logi_joy_bus_enum.sys   [38136]  =>.Logitech Inc®
O58 - SDL:2019/12/08 01:51:14 A . (.Logitech - Logitech G Driver.) -- C:\WINDOWS\System32\drivers\logi_joy_hid_filter.sys   [57608]  =>.Logitech Inc®
O58 - SDL:2019/12/08 01:51:14 A . (.Logitech - Logitech G Driver.) -- C:\WINDOWS\System32\drivers\logi_joy_hid_lo.sys   [46880]  =>.Logitech Inc®
O58 - SDL:2019/12/08 01:49:49 A . (.Logitech, Inc. - G HUB Virtual Device Driver.) -- C:\WINDOWS\System32\drivers\logi_joy_vir_hid.sys   [20624]  =>.W
O58 - SDL:2019/12/08 01:49:49 A . (.Logitech - Logitech G Driver.) -- C:\WINDOWS\System32\drivers\logi_joy_xlcore.sys   [66808]  =>.Logitech Inc®
O58 - SDL:2019/12/07 10:07:53 A . (.LSI Corporation - LSI Fusion-MPT SAS Driver (StorPort).) -- C:\WINDOWS\System32\drivers\lsi_sas.sys   [108856]  =>
O58 - SDL:2019/12/07 10:07:53 A . (.LSI Corporation - LSI SAS Gen2 Driver (StorPort).) -- C:\WINDOWS\System32\drivers\lsi_sas2i.sys   [124216]  =>.Mic
O58 - SDL:2019/12/07 10:07:53 A . (.Avago Technologies - Avago SAS Gen3 Driver (StorPort).) -- C:\WINDOWS\System32\drivers\lsi_sas3i.sys   [135992]  =
O58 - SDL:2019/12/07 10:07:53 A . (.LSI Corporation - LSI SSS PCIe/Flash Driver (StorPort).) -- C:\WINDOWS\System32\drivers\lsi_sss.sys   [82744]  =>
O58 - SDL:2019/12/07 10:08:58 A . (.Microsoft Corporation - Pilote de filtre de virtualisation de fichi.) -- C:\WINDOWS\System32\drivers\luafv.sys
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - MA-USB Host Controller Driver.) -- C:\WINDOWS\System32\drivers\mausbhost.sys   [537608]  =
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - MA-USB IP Driver.) -- C:\WINDOWS\System32\drivers\mausbip.sys   [64016]  =>.Microsoft®
O58 - SDL:2020/08/14 21:05:57 A . (.Microsoft Corporation - Windows Mobile Broadband Class Extension.) -- C:\WINDOWS\System32\drivers\MbbCx.sys   [386
O58 - SDL:2019/12/07 10:09:00 A . (.Microsoft Corporation - Medium changer class driver.) -- C:\WINDOWS\System32\drivers\mcd.sys   [25088] [Unsigned]
O58 - SDL:2019/12/07 10:07:53 A . (.Avago Technologies - MEGASAS RAID Controller Driver for Windows.) -- C:\WINDOWS\System32\drivers\megasas.sys   [59
O58 - SDL:2019/12/07 10:07:53 A . (.Avago Technologies - MEGASAS RAID Controller Driver for Windows.) -- C:\WINDOWS\System32\drivers\MegaSas2i.sys
O58 - SDL:2019/12/07 10:07:53 A . (.Avago Technologies - MEGASAS RAID Controller Driver for Windows.) -- C:\WINDOWS\System32\drivers\megasas35i.sys
O58 - SDL:2019/12/07 10:07:53 A . (.LSI Corporation, Inc. - LSI MegaRAID Software RAID Driver.) -- C:\WINDOWS\System32\drivers\megasr.sys   [575800]
O58 - SDL:2019/09/21 09:10:24 A . (.Maiwei Corporation - MemuHyperv Support Driver.) -- C:\WINDOWS\System32\drivers\MEmuDrv.sys   [319192]  =>.Shangha
O58 - SDL:2019/12/07 10:07:47 A . (.Microsoft Corporation - Pilote de transport Microsoft Bluetooth Avr.) -- C:\WINDOWS\System32\drivers\Microsoft.Blu
O58 - SDL:2020/09/10 22:42:10 A . (.Microsoft Corporation - Legacy Bluetooth LE Bus Enumerator.) -- C:\WINDOWS\System32\drivers\Microsoft.Bluetooth.Le
O58 - SDL:2019/12/07 10:07:54 A . (.Mellanox - MLX4 Bus Driver.) -- C:\WINDOWS\System32\drivers\mlx4_bus.sys   [1131320]  =>.Microsoft®
O58 - SDL:2020/10/16 13:24:16 A . (.Microsoft Corporation - MMCSS Driver.) -- C:\WINDOWS\System32\drivers\mmcss.sys   [53248] [Unsigned]  =>.Microsoft
O58 - SDL:2019/12/07 10:09:51 A . (.Microsoft Corporation - Pilote de périphérique modem.) -- C:\WINDOWS\System32\drivers\modem.sys   [47104] [Unsigne
O58 - SDL:2020/09/10 22:42:10 A . (.Microsoft Corporation - Monitor Driver.) -- C:\WINDOWS\System32\drivers\monitor.sys   [80896] [Unsigned]  =>.Micro
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Pilote de la classe Souris.) -- C:\WINDOWS\System32\drivers\mouclass.sys   [67600]  =>.Mic
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Pilote de filtre souris HID.) -- C:\WINDOWS\System32\drivers\mouhid.sys   [35328] [Unsigne
O58 - SDL:2019/12/07 10:08:49 A . (.Microsoft Corporation - Gestionnaire des points de montage.) -- C:\WINDOWS\System32\drivers\mountmgr.sys   [110392
O58 - SDL:2019/12/07 10:08:33 A . (.Microsoft Corporation - Microsoft Protection Service Driver.) -- C:\WINDOWS\System32\drivers\mpsdrv.sys   [80896]
O58 - SDL:2019/12/07 10:09:54 A . (.Microsoft Corporation - Windows NT WebDav Minirdr.) -- C:\WINDOWS\System32\drivers\mrxdav.sys   [157696] [Unsigned
O58 - SDL:2020/09/10 22:42:41 A . (.Microsoft Corporation - Minirdr SMB Windows NT.) -- C:\WINDOWS\System32\drivers\mrxsmb.sys   [573752]  =>.Microsof
O58 - SDL:2020/09/10 22:43:12 A . (.Microsoft Corporation - Longhorn SMB Downlevel SubRdr.) -- C:\WINDOWS\System32\drivers\mrxsmb10.sys   [307712] [Un
O58 - SDL:2020/09/10 22:42:41 A . (.Microsoft Corporation - Longhorn SMB 2.0 Redirector.) -- C:\WINDOWS\System32\drivers\mrxsmb20.sys   [259888]  =>.M
O58 - SDL:2019/12/07 10:08:49 A . (.Microsoft Corporation - Mailslot driver.) -- C:\WINDOWS\System32\drivers\msfs.sys   [44048]  =>.Microsoft®
O58 - SDL:2020/09/10 22:42:21 A . (.Microsoft Corporation - GPIO Class Extension Driver.) -- C:\WINDOWS\System32\drivers\msgpioclx.sys   [183112]  =>
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - GPIO Button Driver.) -- C:\WINDOWS\System32\drivers\msgpiowin32.sys   [56120]  =>.Microsof
O58 - SDL:2019/12/07 10:08:36 A . (.Microsoft Corporation - Pass-through HID to KMDF Filter Driver.) -- C:\WINDOWS\System32\drivers\mshidkmdf.sys   [8
O58 - SDL:2019/12/07 10:08:16 A . (.Microsoft Corporation - Pilote direct pour interface HID-UMDF.) -- C:\WINDOWS\System32\drivers\mshidumdf.sys   [12
O58 - SDL:2019/12/07 10:08:36 A . (.Microsoft Corporation - Hardware Notification Class Extension Drive.) -- C:\WINDOWS\System32\drivers\mshwnclx.sys
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - ISA Driver.) -- C:\WINDOWS\System32\drivers\msisadrv.sys   [20280]  =>.Microsoft®
O58 - SDL:2020/11/13 18:54:46 A . (.Microsoft Corporation - Microsoft iSCSI Initiator Driver.) -- C:\WINDOWS\System32\drivers\msiscsi.sys   [298808]
O58 - SDL:2020/11/13 18:55:07 A . (.Microsoft Corporation - MS KS Server.) -- C:\WINDOWS\System32\drivers\mskssrv.sys   [34816] [Unsigned]  =>.Microso
O58 - SDL:2019/12/07 10:09:05 A . (.Microsoft Corporation - Pilote de protocole LLDP (Link Layer Discov.) -- C:\WINDOWS\System32\drivers\mslldp.sys
O58 - SDL:2019/12/07 10:08:58 A . (.Microsoft Corporation - MS Proxy Clock.) -- C:\WINDOWS\System32\drivers\mspclock.sys   [11264] [Unsigned]  =>.Micr
O58 - SDL:2019/12/07 10:08:58 A . (.Microsoft Corporation - MS Proxy Quality Manager.) -- C:\WINDOWS\System32\drivers\mspqm.sys   [11264] [Unsigned]
O58 - SDL:2020/09/10 22:42:38 A . (.Microsoft Corporation - Windows QUIC Driver.) -- C:\WINDOWS\System32\drivers\msquic.sys   [322376]  =>.Microsoft®
O58 - SDL:2020/11/13 18:55:06 A . (.Microsoft Corporation - Kernel Remote Procedure Call Provider.) -- C:\WINDOWS\System32\drivers\msrpc.sys   [380728
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - System Management BIOS Driver.) -- C:\WINDOWS\System32\drivers\mssmbios.sys   [47928]  =>
O58 - SDL:2019/12/07 10:08:58 A . (.Microsoft Corporation - WDM Tee/Communication Transform Filter.) -- C:\WINDOWS\System32\drivers\mstee.sys   [12288
O58 - SDL:2019/12/07 10:07:53 A . (.Microsoft Corporation - Pilote HID multipoint Microsoft.) -- C:\WINDOWS\System32\drivers\MTConfig.sys   [17920] [U
O58 - SDL:2019/12/07 10:08:51 A . (.Microsoft Corporation - Pilote de fournisseur UNC multiples.) -- C:\WINDOWS\System32\drivers\mup.sys   [133136]  =
O58 - SDL:2019/12/07 10:07:53 A . (.Marvell Semiconductor, Inc. - Marvell Flash Controller Driver.) -- C:\WINDOWS\System32\drivers\mvumis.sys   [63800
O58 - SDL:2019/12/07 10:07:54 A . (.Mellanox - NetworkDirect Support Filter Driver.) -- C:\WINDOWS\System32\drivers\ndfltr.sys   [146232]  =>.Microsof
O58 - SDL:2020/11/13 18:55:06 A . (.Microsoft Corporation - NDIS (Network Driver Interface Specificatio.) -- C:\WINDOWS\System32\drivers\ndis.sys   [1
O58 - SDL:2019/12/07 10:09:48 A . (.Microsoft Corporation - Microsoft NDIS Packet Capture Filter Driver.) -- C:\WINDOWS\System32\drivers\ndiscap.sys
O58 - SDL:2020/10/16 13:24:55 A . (.Microsoft Corporation - Microsoft Network Adapter Multiplexor.) -- C:\WINDOWS\System32\drivers\NdisImPlatform.sys
O58 - SDL:2020/10/16 13:24:56 A . (.Microsoft Corporation - NDIS 3.0 connection wrapper driver.) -- C:\WINDOWS\System32\drivers\ndistapi.sys   [28672]
O58 - SDL:2019/12/07 10:08:49 A . (.Microsoft Corporation - Pilote d'E/S du mode utilisateur NDIS.) -- C:\WINDOWS\System32\drivers\ndisuio.sys   [7065
O58 - SDL:2019/12/07 10:09:05 A . (.Microsoft Corporation - Énumérateur de cartes réseau virtuelles Mic.) -- C:\WINDOWS\System32\drivers\NdisVirtualBu
O58 - SDL:2020/09/10 22:42:46 A . (.Microsoft Corporation - MS PPP Framing Driver (Strong Encryption).) -- C:\WINDOWS\System32\drivers\ndiswan.sys
O58 - SDL:2019/12/07 10:09:48 A . (.Microsoft Corporation - RDMA Sample Driver.) -- C:\WINDOWS\System32\drivers\NDKPing.sys   [72720]  =>.Microsoft®
O58 - SDL:2020/10/16 13:24:56 A . (.Microsoft Corporation - NDIS Proxy.) -- C:\WINDOWS\System32\drivers\ndproxy.sys   [93696] [Unsigned]  =>.Microsoft
O58 - SDL:2019/12/07 10:09:33 A . (.Microsoft Corporation - Windows Network Data Usage Monitoring Drive.) -- C:\WINDOWS\System32\drivers\Ndu.sys   [13
O58 - SDL:2020/10/16 13:24:50 A . (.Microsoft Corporation - Network Adapter Class Extension for WDF.) -- C:\WINDOWS\System32\drivers\NetAdapterCx.sys
O58 - SDL:2019/12/07 10:09:04 A . (.Microsoft Corporation - NetBIOS interface driver.) -- C:\WINDOWS\System32\drivers\netbios.sys   [64312]  =>.Micros
O58 - SDL:2020/10/16 13:24:55 A . (.Microsoft Corporation - MBT Transport driver.) -- C:\WINDOWS\System32\drivers\netbt.sys   [341504] [Unsigned]  =>
O58 - SDL:2020/11/13 18:55:06 A . (.Microsoft Corporation - Network I/O Subsystem.) -- C:\WINDOWS\System32\drivers\netio.sys   [603448]  =>.Microsoft®
O58 - SDL:2020/11/13 18:54:46 A . (.Microsoft Corporation - Miniport NDIS virtuel.) -- C:\WINDOWS\System32\drivers\netvsc.sys   [250176]  =>.Microsoft
O58 - SDL:2013/03/01 02:49:12 A . (.Riverbed Technology, Inc. - npf.sys (NT5/6 AMD64) Kernel Driver.) -- C:\WINDOWS\System32\drivers\npf.sys   [36600]
O58 - SDL:2019/12/07 10:08:49 A . (.Microsoft Corporation - NPFS Driver.) -- C:\WINDOWS\System32\drivers\npfs.sys   [87568]  =>.Microsoft®
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Named pipe service triggers.) -- C:\WINDOWS\System32\drivers\npsvctrig.sys   [27648] [Unsi
O58 - SDL:2020/10/16 13:24:50 A . (.Microsoft Corporation - NSI Proxy.) -- C:\WINDOWS\System32\drivers\nsiproxy.sys   [48640] [Unsigned]  =>.Microsoft
O58 - SDL:2020/11/13 18:55:05 A . (.Microsoft Corporation - Pilote du système de fichiers NT.) -- C:\WINDOWS\System32\drivers\ntfs.sys   [2850616]  =>
O58 - SDL:2019/12/07 10:08:58 A . (.Microsoft Corporation - NTOS extension host driver.) -- C:\WINDOWS\System32\drivers\ntosext.sys   [20792]  =>.Micr
O58 - SDL:2019/12/07 10:08:49 A . (.Microsoft Corporation - NULL Driver.) -- C:\WINDOWS\System32\drivers\null.sys   [7680] [Unsigned]  =>.Microsoft Co
```

```
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - Pilote de périphérique NVDIMM.) -- C:\WINDOWS\System32\drivers\nvdimm.sys   [168464]  =>.M
O58 - SDL:2020/11/07 05:01:33 A . (.NVIDIA Corporation - NVIDIA HDMI Audio Driver.) -- C:\WINDOWS\System32\drivers\nvhda64v.sys   [222112]  =>.NVIDIA
O58 - SDL:2020/11/07 23:25:58 A . (.NVIDIA Corporation - NVIDIA Windows Kernel Mode Driver, Version.) -- C:\WINDOWS\System32\drivers\nvlddmkm.sys   [3
O58 - SDL:2020/03/04 13:54:38 A . (.NVIDIA Corporation - Process and module monitoring driver.) -- C:\WINDOWS\System32\drivers\NvModuleTracker.sys
O58 - SDL:2019/12/07 10:07:53 A . (.NVIDIA Corporation - NVIDIA® nForce(TM) RAID Driver.) -- C:\WINDOWS\System32\drivers\nvraid.sys   [150328]  =>.Mic
O58 - SDL:2019/12/07 10:07:53 A . (.NVIDIA Corporation - NVIDIA® nForce(TM) Sata Performance Driver.) -- C:\WINDOWS\System32\drivers\nvstor.sys   [166
O58 - SDL:2019/03/19 06:42:20 A . (.NVIDIA Corporation - NVIDIA Virtual Audio Driver.) -- C:\WINDOWS\System32\drivers\nvvad64v.sys   [69840]  =>.NVIDI
O58 - SDL:2020/03/11 20:26:38 A . (.NVIDIA Corporation - Virtual USB Host Controller driver.) -- C:\WINDOWS\System32\drivers\nvvhci.sys   [67456]  =>
O58 - SDL:2020/09/10 22:42:17 A . (.Microsoft Corporation - Pilote de miniport WiFi natif.) -- C:\WINDOWS\System32\drivers\nwifi.sys   [733696] [Unsig
O58 - SDL:2020/10/16 13:24:38 A . (.Microsoft Corporation - Planificateur de paquets QoS.) -- C:\WINDOWS\System32\drivers\pacer.sys   [161608]  =>.Mic
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - Pilote de port parallèle.) -- C:\WINDOWS\System32\drivers\parport.sys   [109056] [Unsigned
O58 - SDL:2019/12/07 10:08:49 A . (.Microsoft Corporation - Partition driver.) -- C:\WINDOWS\System32\drivers\partmgr.sys   [182584]  =>.Microsoft®
O58 - SDL:2020/09/10 22:42:10 A . (.Microsoft Corporation - Énumérateur Plug-and-Play PCI pour NT.) -- C:\WINDOWS\System32\drivers\pci.sys   [472376]
O58 - SDL:2020/09/10 22:42:10 A . (.Microsoft Corporation - Generic PCI IDE Bus Driver.) -- C:\WINDOWS\System32\drivers\pciide.sys   [16704]  =>.Micro
O58 - SDL:2020/09/10 22:42:10 A . (.Microsoft Corporation - PCI IDE Bus Driver Extension.) -- C:\WINDOWS\System32\drivers\pciidex.sys   [56648]  =>.Mi
O58 - SDL:2019/12/07 10:07:50 A . (.Microsoft Corporation - Pilote de bus PCMCIA.) -- C:\WINDOWS\System32\drivers\pcmcia.sys   [127800]  =>.Microsoft®
O58 - SDL:2019/12/07 10:08:46 A . (.Microsoft Corporation - Performance Counters for Windows Driver.) -- C:\WINDOWS\System32\drivers\pcw.sys   [57656]
O58 - SDL:2020/09/10 22:42:14 A . (.Microsoft Corporation - Power Dependency Coordinator Driver.) -- C:\WINDOWS\System32\drivers\pdc.sys   [159048]  =
O58 - SDL:2020/09/10 22:42:14 A . (.Microsoft Corporation - Protected Environment Authentication and Au.) -- C:\WINDOWS\System32\drivers\PEAuth.sys
O58 - SDL:2019/12/07 10:07:53 A . (.Avago Technologies - MEGASAS RAID Controller Driver for Windows.) -- C:\WINDOWS\System32\drivers\percsas2i.sys
O58 - SDL:2019/12/07 10:07:53 A . (.Avago Technologies - MEGASAS RAID Controller Driver for Windows.) -- C:\WINDOWS\System32\drivers\percsas3i.sys
O58 - SDL:2020/11/13 18:55:23 A . (.Microsoft Corporation - Pilote du moniteur de paquets.) -- C:\WINDOWS\System32\drivers\PktMon.sys   [104760]  =>.M
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - Pilote de mémoire persistante.) -- C:\WINDOWS\System32\drivers\pmem.sys   [138040]  =>.Mic
O58 - SDL:2019/12/07 10:07:50 A . (.Microsoft Corporation - Pilote mémoire Plug and Play.) -- C:\WINDOWS\System32\drivers\pnpmem.sys   [17408] [Unsigr
O58 - SDL:2019/12/07 10:08:36 A . (.Microsoft Corporation - Port Device Class Configuration Filter Driv.) -- C:\WINDOWS\System32\drivers\portcfg.sys
O58 - SDL:2020/11/13 18:54:45 A . (.Microsoft Corporation - Port Class (Class Driver for Port/Miniport.) -- C:\WINDOWS\System32\drivers\portcls.sys
O58 - SDL:2020/10/16 13:24:14 A . (.Microsoft Corporation - Processor Device Driver.) -- C:\WINDOWS\System32\drivers\processr.sys   [216376]  =>.Micro
O58 - SDL:2019/12/07 10:08:33 A . (.Microsoft Corporation - Time Travel Debugging Process Launch Monito.) -- C:\WINDOWS\System32\drivers\ProcLaunchMor
O58 - SDL:2011/11/03 02:01:00 A . (.Rovi Corporation - Px Engine Device Driver for 64-bit Windows.) -- C:\WINDOWS\System32\drivers\PxHlpa64.sys   [562
O58 - SDL:2019/12/07 10:09:05 A . (.Microsoft Corporation - Pilote du support de Microsoft Quality Wind.) -- C:\WINDOWS\System32\drivers\qwavedrv.sys
O58 - SDL:2019/12/07 10:08:09 A . (.Microsoft Corporation - RAM Disk Driver.) -- C:\WINDOWS\System32\drivers\ramdisk.sys   [42296]  =>.Microsoft®
O58 - SDL:2020/10/16 13:24:55 A . (.Microsoft Corporation - RAS Automatic Connection Driver.) -- C:\WINDOWS\System32\drivers\rasacd.sys   [20480] [Uns
O58 - SDL:2020/09/10 22:42:46 A . (.Microsoft Corporation - RAS L2TP mini-port/call-manager driver.) -- C:\WINDOWS\System32\drivers\ras2tp.sys   [110
O58 - SDL:2019/12/07 10:09:07 A . (.Microsoft Corporation - RAS PPPoE mini-port/call-manager driver.) -- C:\WINDOWS\System32\drivers\raspppoe.sys   [8
O58 - SDL:2020/09/10 22:42:46 A . (.Microsoft Corporation - Peer-to-Peer Tunneling Protocol.) -- C:\WINDOWS\System32\drivers\raspptp.sys   [101888] [U
O58 - SDL:2020/09/10 22:42:46 A . (.Microsoft Corporation - RAS SSTP Miniport Call Manager.) -- C:\WINDOWS\System32\drivers\rassstp.sys   [86016] [Uns
O58 - SDL:2020/09/10 22:42:41 A . (.Microsoft Corporation - Pilote du sous-système de mise en mémoire t.) -- C:\WINDOWS\System32\drivers\rdbss.sys
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Microsoft RDP Bus Device driver.) -- C:\WINDOWS\System32\drivers\rdpbus.sys   [28672] [Uns
O58 - SDL:2019/12/07 10:09:47 A . (.Microsoft Corporation - Redirecteur de périphérique de Microsoft RD.) -- C:\WINDOWS\System32\drivers\rdpdr.sys
O58 - SDL:2020/05/11 06:40:49 A . (.Microsoft Corporation - Microsoft RDP Video Miniport driver.) -- C:\WINDOWS\System32\drivers\rdpvideominiport.sys
O58 - SDL:2019/12/07 10:09:54 A . (.Microsoft Corporation - ReadyBoost Driver.) -- C:\WINDOWS\System32\drivers\rdyboost.sys   [297784]  =>.Microsoft®
O58 - SDL:2019/12/07 10:08:46 A . (.Microsoft Corporation - Pilote du système de fichiers ReFS NT.) -- C:\WINDOWS\System32\drivers\refs.sys   [1999160
O58 - SDL:2019/12/07 10:08:46 A . (.Microsoft Corporation - Pilote du système de fichiers ReFS NT.) -- C:\WINDOWS\System32\drivers\refsv1.sys   [99000
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Bluetooth RFCOMM Driver.) -- C:\WINDOWS\System32\drivers\rfcomm.sys   [213504] [Unsigned]
O58 - SDL:2019/12/07 10:07:57 A . (.Microsoft Corporation - Transport d'ordinateur virtuel Microsoft Re.) -- C:\WINDOWS\System32\drivers\RfxVmt.sys
O58 - SDL:2019/12/07 10:07:50 A . (.Microsoft Corporation - ResourceHub Proxy Driver.) -- C:\WINDOWS\System32\drivers\rhproxy.sys   [115712] [Unsigned]
O58 - SDL:2016/01/08 06:57:00 A . (.BlackBerry Limited - BlackBerry Device Driver.) -- C:\WINDOWS\System32\drivers\RimUsb_AMD64.sys   [89096]  =>.Micr
O58 - SDL:2019/12/07 10:09:41 A . (.Microsoft Corporation - Reliable Multicast Transport.) -- C:\WINDOWS\System32\drivers\rmcast.sys   [158208] [Unsig
O58 - SDL:2019/12/07 10:09:07 A . (.Microsoft Corporation - Remote NDIS Miniport.) -- C:\WINDOWS\System32\drivers\RNDISMP.sys   [37376] [Unsigned]  =>
O58 - SDL:2019/12/07 10:09:51 A . (.Microsoft Corporation - Legacy Non-Pnp Modem Device Driver.) -- C:\WINDOWS\System32\drivers\rootmdm.sys   [13824]
O58 - SDL:2019/12/07 10:08:55 A . (.Microsoft Corporation - Link-Layer Topology Responder Driver for ND.) -- C:\WINDOWS\System32\drivers\rspndr.sys
O58 - SDL:2019/02/16 23:12:02 A . (.Realtek - Realtek 8125/8136/8168/8169 NDIS 6.40 64-bi.) -- C:\WINDOWS\System32\drivers\rt640x64.sys   [1122200]  =
O58 - SDL:2019/01/23 01:18:26 A . (.Realtek - Realtek 8125/8136/8168/8169 NDIS 6.20 64-bi.) -- C:\WINDOWS\System32\drivers\Rt64win7.sys   [1090216]  =
O58 - SDL:2019/12/07 10:08:09 RA . (.Realtek - Realtek PCIe GBE Family Controller Flight.) -- C:\WINDOWS\System32\drivers\rteth.sys   [48640] [Unsigne
O58 - SDL:2020/08/03 23:18:47 A . (.Realtek - Realtek packet filter driver.) -- C:\WINDOWS\System32\drivers\rtf64x64.sys   [70560]  =>.Realtek Semicor
O58 - SDL:2019/05/17 05:05:16 A . (.Realtek Semiconductor Corporation - Realtek bluetooth A2DP Driver.) -- C:\WINDOWS\System32\drivers\RtkA2dp.sys
O58 - SDL:2019/05/17 02:05:20 A . (.Realtek Semiconductor Corporation - Realtek Bluetooth AVRCP Driver.) -- C:\WINDOWS\System32\drivers\RtkAvrcp.sys
O58 - SDL:2019/01/23 01:18:16 A . (.Realtek Semiconductor Corporation - Realtek Bluetooth Avrcp Controller Driver.) -- C:\WINDOWS\System32\drivers\Rtk
O58 - SDL:2019/11/30 18:57:46 A . (.Realtek Semiconductor Corporation - Realtek Bluetooth Filter Driver.) -- C:\WINDOWS\System32\drivers\RtkBtfilter.s
O58 - SDL:2019/01/23 01:18:52 A . (.Realtek Semiconductor Corp. - Realtek(r) High Definition Audio Function D.) -- C:\WINDOWS\System32\drivers\RTKVHDE
O58 - SDL:2019/01/23 01:18:49 A . (.Realsil Semiconductor Corporation - RTS USB READER Driver.) -- C:\WINDOWS\System32\drivers\RtsUer.sys   [450152]
O58 - SDL:2019/12/04 04:23:30 A . (.Realtek Semiconductor Corporation - Realtek PCIE NDIS Driver 85905 38554.) -- C:\WINDOWS\System32\drivers\rtwlane
O58 - SDL:2019/12/07 10:07:53 A . (.Microsoft Corporation - SBP-2 Protocol Driver.) -- C:\WINDOWS\System32\drivers\sbp2port.sys   [116752]  =>.Microsc
O58 - SDL:2017/06/07 01:36:28 A . (.Power Software Ltd - PowerISO Virtual Drive.) -- C:\WINDOWS\System32\drivers\scdemu.sys   [138296]  =>.Power Softw
O58 - SDL:2020/11/13 18:55:08 A . (.Microsoft Corporation - Pilote de filtre de lecteur de carte à puce.) -- C:\WINDOWS\System32\drivers\scfilter.sys
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - Pilote de bus de mémoire de classe stockage.) -- C:\WINDOWS\System32\drivers\scmbus.sys
O58 - SDL:2013/05/19 01:02:52 A . (.Scarlet.Crush Productions - Scp Virtual Bus Driver.) -- C:\WINDOWS\System32\drivers\ScpVBus.sys   [39168]  =>.Bruc
O58 - SDL:2019/06/29 10:37:53 A . (.Screenovate Technologies Ltd. - Phone Input Device.) -- C:\WINDOWS\System32\drivers\ScrHIDDriver.sys   [56792] {03
O58 - SDL:2019/01/01 15:44:38 A . (.Screenovate Technologies Ltd. - Phone Input Device.) -- C:\WINDOWS\System32\drivers\ScrHIDDriver2.sys   [59960]  =
O58 - SDL:2019/12/07 10:09:00 A . (.Microsoft Corporation - SCSI Port Driver.) -- C:\WINDOWS\System32\drivers\scsiport.sys   [187704]  =>.Microsoft®
O58 - SDL:2020/11/13 18:54:46 A . (.Microsoft Corporation - Pilote du bus numérique sécurisé (SD).) -- C:\WINDOWS\System32\drivers\sdbus.sys   [305472
O58 - SDL:2019/12/07 10:07:50 A . (.Microsoft Corporation - SDF Reflector.) -- C:\WINDOWS\System32\drivers\SDFRd.sys   [35128]  =>.Microsoft®
O58 - SDL:2019/12/07 10:08:09 A . (.Microsoft Corporation - SD Host Controller Port Driver.) -- C:\WINDOWS\System32\drivers\sdport.sys   [105488]  =>
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Pilote de classe de stockage SD.) -- C:\WINDOWS\System32\drivers\sdstor.sys   [103736]  =>
O58 - SDL:2019/01/23 01:18:22 A . (.Samsung Electronics Co., Ltd - Samsung NVM Express Storport Miniport Drive.) -- C:\WINDOWS\System32\drivers\secnvm
O58 - SDL:2019/01/23 01:18:22 A . (.Samsung Electronics Co., Ltd - Samsung NVMe Filter driver.) -- C:\WINDOWS\System32\drivers\secnvmeF.sys   [30624]
O58 - SDL:2019/12/07 10:08:36 A . (.Microsoft Corporation - Serial Class Extension.) -- C:\WINDOWS\System32\drivers\SerCx.sys   [86328]  =>.Microsoft®
O58 - SDL:2019/12/07 10:08:36 A . (.Microsoft Corporation - Serial Class Extension V2.) -- C:\WINDOWS\System32\drivers\SerCx2.sys   [173072]  =>.Micro
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - Serial Port Enumerator.) -- C:\WINDOWS\System32\drivers\serenum.sys   [27648] [Unsigned]
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - Pilote de périphérique série.) -- C:\WINDOWS\System32\drivers\serial.sys   [90624] [Unsigr
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Pilote de filtre souris série.) -- C:\WINDOWS\System32\drivers\sermouse.sys   [29184] [Uns
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - SCSI Floppy Driver.) -- C:\WINDOWS\System32\drivers\sfloppy.sys   [19456] [Unsigned]  =>.M
O58 - SDL:2019/12/07 10:09:33 A . (.Microsoft Corporation - System Guard Runtime Monitor Agent Driver.) -- C:\WINDOWS\System32\drivers\SgrmAgent.sys
O58 - SDL:2016/05/18 11:20:14 A . (. - Intel® Software Guard Extensions Device.) -- C:\WINDOWS\System32\drivers\sgx_driver.sys   [52824] {07501595A92E
O58 - SDL:2019/12/07 10:07:53 A . (.Silicon Integrated Systems Corp. - SiS RAID Stor Miniport Driver.) -- C:\WINDOWS\System32\drivers\sisraid2.sys
O58 - SDL:2019/12/07 10:07:53 A . (.Silicon Integrated Systems - SiS AHCI Stor-Miniport Driver.) -- C:\WINDOWS\System32\drivers\sisraid4.sys   [81720]
O58 - SDL:2019/12/07 10:08:49 A . (.Microsoft Corporation - Sleep Study Helper.) -- C:\WINDOWS\System32\drivers\SleepStudyHelper.sys   [38200]  =>.Mic
O58 - SDL:2019/12/07 10:07:53 A . (.Microsemi Corportation - Storport Miniport Driver for SmartRAID/Smar.) -- C:\WINDOWS\System32\drivers\SmartSAMD.sy
O58 - SDL:2019/01/23 01:18:47 A . (.Synaptics Incorporated - Synaptics SMBus Driver.) -- C:\WINDOWS\System32\drivers\Smb_driver_Intel.sys   [54928]  =
O58 - SDL:2019/12/07 10:09:09 A . (.Microsoft Corporation - Smart Card Driver Library.) -- C:\WINDOWS\System32\drivers\smclib.sys   [21504] [Unsigned]
O58 - SDL:2020/08/14 21:05:56 A . (.Microsoft Corporation - Storage Spaces Dump Driver.) -- C:\WINDOWS\System32\drivers\spacedump.sys   [215880]  =>.M
O58 - SDL:2019/12/07 10:09:34 A . (.Microsoft Corporation - Storage Spaces Parser.) -- C:\WINDOWS\System32\drivers\spaceparser.sys   [26624] [Unsigned
O58 - SDL:2020/08/14 21:05:56 A . (.Microsoft Corporation - Storage Spaces Driver.) -- C:\WINDOWS\System32\drivers\spaceport.sys   [678200]  =>.Micros
O58 - SDL:2019/12/07 15:52:56 A . (.Microsoft Corporation - Holographic Spatial Graph Filter.) -- C:\WINDOWS\System32\drivers\SpatialGraphFilter.sys
O58 - SDL:2019/12/07 10:08:37 A . (.Microsoft Corporation - SPB Class Extension.) -- C:\WINDOWS\System32\drivers\SpbCx.sys   [87352]  =>.Microsoft®
O58 - SDL:2020/09/08 19:12:30 A . (.Microsoft Corporation - Server driver.) -- C:\WINDOWS\System32\drivers\srv.sys   [443904] [Unsigned]  =>.Microsoft
O58 - SDL:2020/11/13 18:55:06 A . (.Microsoft Corporation - Pilote de serveur SMB 2.0.) -- C:\WINDOWS\System32\drivers\srv2.sys   [783360] [Unsigned]
O58 - SDL:2020/11/13 18:55:06 A . (.Microsoft Corporation - Server Network driver.) -- C:\WINDOWS\System32\drivers\srvnet.sys   [315392] [Unsigned]  =
O58 - SDL:2017/01/16 07:26:40 A . (.Samsung Electronics Co., Ltd. - SAMSUNG USB Composite Device Driver.) -- C:\WINDOWS\System32\drivers\ssudbus.sys
O58 - SDL:2017/01/16 07:26:40 A . (.Samsung Electronics Co., Ltd. - SAMSUNG Android Modem Device Driver.) -- C:\WINDOWS\System32\drivers\ssudmdm.sys
O58 - SDL:2019/12/07 10:07:53 A . (.Promise Technology, Inc. - Promise SuperTrak EX Series Driver for Wind.) -- C:\WINDOWS\System32\drivers\stexstor.s
O58 - SDL:2020/09/10 22:42:10 A . (.Microsoft Corporation - MS AHCI Storport Miniport Driver.) -- C:\WINDOWS\System32\drivers\storahci.sys   [185672]
O58 - SDL:2020/10/16 13:24:14 A . (.Microsoft Corporation - Microsoft NVM Express Storport Miniport Dri.) -- C:\WINDOWS\System32\drivers\stornvme.sys
O58 - SDL:2020/09/10 22:42:14 A . (.Microsoft Corporation - Microsoft Storage Port Driver.) -- C:\WINDOWS\System32\drivers\storport.sys   [702776]  =>
```

```
O58 - SDL:2019/12/07 10:08:37 A . (.Microsoft Corporation - Filtre de qualité de service de stockage.) -- C:\WINDOWS\System32\drivers\storqosflt.sys
O58 - SDL:2020/09/10 22:42:10 A . (.Microsoft Corporation - MS UFS Storport Miniport Driver.) -- C:\WINDOWS\System32\drivers\storufs.sys   [60744]  =>
O58 - SDL:2019/12/07 10:07:57 A . (.Microsoft Corporation - Storage VSC Driver.) -- C:\WINDOWS\System32\drivers\storvsc.sys   [44048]  =>.Microsoft®
O58 - SDL:2019/12/07 10:09:00 A . (.Microsoft Corporation - WDM CODEC Class Device Driver 2.0.) -- C:\WINDOWS\System32\drivers\stream.sys   [82432] [U
O58 - SDL:2020/05/17 03:54:45 A . (.SlimWare Utilities, Inc. - Driver Update Installer Monitor.) -- C:\WINDOWS\System32\drivers\SWDUMon.sys   [25608]
O58 - SDL:2019/12/07 10:07:57 A . (.Microsoft Corporation - VSC vidéo Synth3D RemoteFX Microsoft.) -- C:\WINDOWS\System32\drivers\Synth3dVsc.sys   [67
O58 - SDL:2016/04/21 10:10:04 A . (.The OpenVPN Project - TAP-Windows Virtual Network Driver (NDIS 6..) -- C:\WINDOWS\System32\drivers\tap0901.sys
O58 - SDL:2019/12/07 10:09:00 A . (.Microsoft Corporation - SCSI Tape Class Driver.) -- C:\WINDOWS\System32\drivers\tape.sys   [33280] [Unsigned]  =>
O58 - SDL:2018/07/24 14:50:08 A . (.The OpenVPN Project - TAP-Windows Virtual Network Driver (NDIS 6..) -- C:\WINDOWS\System32\drivers\tapnordvpn.sys
O58 - SDL:2020/10/16 13:24:17 A . (.Microsoft Corporation - Export driver for kernel mode TPM API.) -- C:\WINDOWS\System32\drivers\tbs.sys   [31552]
O58 - SDL:2020/11/13 18:55:06 A . (.Microsoft Corporation - Pilote TCP/IP.) -- C:\WINDOWS\System32\drivers\tcpip.sys   [2983736]  =>.Microsoft®
O58 - SDL:2019/12/07 10:09:04 A . (.Microsoft Corporation - TCP/IP Registry Compatibility Driver.) -- C:\WINDOWS\System32\drivers\tcpipreg.sys   [5478
O58 - SDL:2019/12/07 10:08:49 A . (.Microsoft Corporation - TDI Wrapper.) -- C:\WINDOWS\System32\drivers\tdi.sys   [39736]  =>.Microsoft®
O58 - SDL:2019/12/07 10:09:33 A . (.Microsoft Corporation - TDI Translation Driver.) -- C:\WINDOWS\System32\drivers\tdx.sys   [117560]  =>.Microsoft®
O58 - SDL:2018/05/06 07:52:26 A . (.Intel Corporation - Intel(R) Management Engine Interface.) -- C:\WINDOWS\System32\drivers\TeeDriverW8x64.sys   [22
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Terminal Server Input Driver.) -- C:\WINDOWS\System32\drivers\terminpt.sys   [41272]  =>.M
O58 - SDL:2019/12/07 10:08:51 A . (.Microsoft Corporation - Kernel Transaction Manager Driver.) -- C:\WINDOWS\System32\drivers\tm.sys   [141328]  =>.M
O58 - SDL:2020/09/10 22:42:10 A . (.Microsoft Corporation - Pilote de périphérique TPM.) -- C:\WINDOWS\System32\drivers\tpm.sys   [255296]  =>.Microso
O58 - SDL:2019/12/07 10:08:09 A . (.Microsoft Corporation - Pilote de filtre pour concentrateur USB du.) -- C:\WINDOWS\System32\drivers\TsUsbFlt.sys
O58 - SDL:2019/12/07 10:07:53 A . (.Microsoft Corporation - Remote Desktop Generic USB Driver.) -- C:\WINDOWS\System32\drivers\TsUsbGD.sys   [37888]
O58 - SDL:2019/12/07 10:09:04 A . (.Microsoft Corporation - Pilote d’interface de tunnel Microsoft.) -- C:\WINDOWS\System32\drivers\tunnel.sys   [1296
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - Microsoft Uasp Driver.) -- C:\WINDOWS\System32\drivers\uaspstor.sys   [79376]  =>.Microsoft®
O58 - SDL:2019/12/07 10:08:37 A . (.Microsoft Corporation - USB Connector Manager KMDF Class Extension.) -- C:\WINDOWS\System32\drivers\UcmCx.sys   [1
O58 - SDL:2019/12/07 10:08:37 A . (.Microsoft Corporation - UCM-TCPCI KMDF Class Extension.) -- C:\WINDOWS\System32\drivers\UcmTcpciCx.sys   [188416]
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - UCM-UCSI ACPI Client Driver.) -- C:\WINDOWS\System32\drivers\UcmUcsiAcpiClient.sys   [3686
O58 - SDL:2020/09/10 22:42:32 A . (.Microsoft Corporation - UCM-UCSI KMDF Class Extension.) -- C:\WINDOWS\System32\drivers\UcmUcsiCx.sys   [113152] [U
O58 - SDL:2019/12/07 10:08:09 A . (.Microsoft Corporation - USB Controller Extension.) -- C:\WINDOWS\System32\drivers\Ucx01000.sys   [259896]  =>.Micr
O58 - SDL:2019/12/07 10:08:09 A . (.Microsoft Corporation - 'udecx.DRIVER'.) -- C:\WINDOWS\System32\drivers\Udecx.sys   [52736] [Unsigned]  =>.Microso
O58 - SDL:2019/12/07 10:09:51 A . (.Microsoft Corporation - UDF File System Driver.) -- C:\WINDOWS\System32\drivers\udfs.sys   [344064] [Unsigned]  =>
O58 - SDL:2019/12/07 10:08:37 A . (.Microsoft Corporation - USB Function Driver Class Extension.) -- C:\WINDOWS\System32\drivers\ufx01000.sys   [32104
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - UFX Synopsys Client Driver.) -- C:\WINDOWS\System32\drivers\ufxsynopsys.sys   [168248]  =>
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Generic pass-through driver.) -- C:\WINDOWS\System32\drivers\umpass.sys   [15360] [Unsigne
O58 - SDL:2019/12/07 10:08:37 A . (.Microsoft Corporation - USB Role-Switch Class Extension.) -- C:\WINDOWS\System32\drivers\urscx01000.sys   [76304]
O58 - SDL:2019/12/07 10:09:07 A . (.Microsoft Corporation - Remote NDIS USB Driver.) -- C:\WINDOWS\System32\drivers\usb8023.sys   [24064] [Unsigned]
O58 - SDL:2020/07/15 10:49:29 A . (.Microsoft Corporation - USB Audio Class Driver.) -- C:\WINDOWS\System32\drivers\USBAUDIO.sys   [202752] [Unsigned]
O58 - SDL:2019/12/07 10:07:50 A . (.Microsoft Corporation - Microsoft USB Audio Class 2.0 Driver.) -- C:\WINDOWS\System32\drivers\usbaudio2.sys   [266
O58 - SDL:2019/12/07 10:08:41 A . (.Microsoft Corporation - Universal Serial Bus Camera Driver.) -- C:\WINDOWS\System32\drivers\USBCAMD2.sys   [40448]
O58 - SDL:2020/09/10 22:42:10 A . (.Microsoft Corporation - USB Common Class Generic Parent Driver.) -- C:\WINDOWS\System32\drivers\usbccgp.sys   [185
O58 - SDL:2019/12/07 10:07:50 A . (.Microsoft Corporation - USB Consumer IR Driver for eHome.) -- C:\WINDOWS\System32\drivers\usbcir.sys   [107520] [U
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Universal Serial Bus Driver.) -- C:\WINDOWS\System32\drivers\usbd.sys   [33080]  =>.Micros
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - EHCI eUSB Miniport Driver.) -- C:\WINDOWS\System32\drivers\usbehci.sys   [86544]  =>.Micro
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Pilote de concentrateur USB par défaut.) -- C:\WINDOWS\System32\drivers\usbhub.sys   [5281
O58 - SDL:2020/05/11 06:40:14 A . (.Microsoft Corporation - Pilote de concentrateur USB3.) -- C:\WINDOWS\System32\drivers\USBHUB3.SYS   [647992]  =>.M
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - OHCI USB Miniport Driver.) -- C:\WINDOWS\System32\drivers\usbohci.sys   [30208] [Unsigned]
O58 - SDL:2017/08/21 02:50:50 A . (.USBPcap - USBPcap Driver.) -- C:\WINDOWS\System32\drivers\USBPcap.sys   [50224]  =>.Tomasz Moń®
O58 - SDL:2019/12/07 10:08:37 A . (...) -- C:\WINDOWS\System32\drivers\UsbPmApi.sys   [53248] [Unsigned]  =>.Microsoft Corporation
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Pilote de port USB 1.1 & 2.0.) -- C:\WINDOWS\System32\drivers\usbport.sys   [473400]  =>.M
O58 - SDL:2019/12/07 10:07:50 A . (.Microsoft Corporation - USB Printer driver.) -- C:\WINDOWS\System32\drivers\usbprint.sys   [35328] [Unsigned]  =>
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - USB Serial Driver.) -- C:\WINDOWS\System32\drivers\usbser.sys   [81408] [Unsigned]  =>.Mic
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Pilote de classe de stockage de masse USB.) -- C:\WINDOWS\System32\drivers\USBSTOR.SYS
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - UHCI USB Miniport Driver.) -- C:\WINDOWS\System32\drivers\usbuhci.sys   [39424] [Unsigned]
O58 - SDL:2020/09/10 22:42:10 A . (.Microsoft Corporation - Pilote XHCI USB.) -- C:\WINDOWS\System32\drivers\USBXHCI.SYS   [602440]  =>.Microsoft®
O58 - SDL:2019/01/14 13:55:28 A . (.Oracle Corporation - VirtualBox Support Driver.) -- C:\WINDOWS\System32\drivers\VBoxDrv.sys   [1021768]  =>.Oracle
O58 - SDL:2019/01/14 13:55:32 A . (.Oracle Corporation - VirtualBox NDIS 6.0 Host-Only Network Adapt.) -- C:\WINDOWS\System32\drivers\VBoxNetAdp6.sys
O58 - SDL:2019/01/14 13:55:34 A . (.Oracle Corporation - VirtualBox NDIS 6.0 Lightweight Filter Driv.) -- C:\WINDOWS\System32\drivers\VBoxNetLwf.sys
O58 - SDL:2019/01/14 13:55:36 A . (.Oracle Corporation - VirtualBox USB Monitor Driver.) -- C:\WINDOWS\System32\drivers\VBoxUSBMon.sys   [185960]  =>
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - Virtual Drive Root Enumerator.) -- C:\WINDOWS\System32\drivers\vdrvroot.sys   [67384]  =>
O58 - SDL:2019/12/07 10:08:49 A . (.Microsoft Corporation - Extension du vérificateur de pilotes.) -- C:\WINDOWS\System32\drivers\VerifierExt.sys   [3
O58 - SDL:2020/11/13 18:54:46 A . (.Microsoft Corporation - VHD Miniport Driver.) -- C:\WINDOWS\System32\drivers\vhdmp.sys   [820552]  =>.Microsoft®
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - Virtual HID Framework (VHF) Driver.) -- C:\WINDOWS\System32\drivers\vhf.sys   [47616] [Uns
O58 - SDL:2020/08/14 21:05:56 A . (.Microsoft Corporation - Microsoft Hyper-V Virtualization Infrastruc.) -- C:\WINDOWS\System32\drivers\Vid.sys   [63
O58 - SDL:2019/12/07 10:08:49 A . (.Microsoft Corporation - Video Port Driver.) -- C:\WINDOWS\System32\drivers\videoprt.sys   [47104] [Unsigned]  =>.M
O58 - SDL:2019/12/07 10:09:51 A . (.Microsoft Corporation - Hyper-V VMBus KMCL.) -- C:\WINDOWS\System32\drivers\vmbkmcl.sys   [114488]  =>.Microsoft®
O58 - SDL:2020/10/16 13:24:14 A . (.Microsoft Corporation - Pilote enfant de bus VMBus sous Microsoft H.) -- C:\WINDOWS\System32\drivers\vmbus.sys
O58 - SDL:2019/12/07 10:07:57 A . (.Microsoft Corporation - Microsoft VMBus HID Miniport.) -- C:\WINDOWS\System32\drivers\VMBusHID.sys   [36664]  =>.M
O58 - SDL:2018/06/22 01:31:02 A . (.VMware, Inc. - VMware PCI VMCI Bus Device.) -- C:\WINDOWS\System32\drivers\vmci.sys   [105024]  =>.VMware, Inc.®
O58 - SDL:2019/12/07 10:07:57 A . (.Microsoft Corporation - Virtual Machine Generation Counter.) -- C:\WINDOWS\System32\drivers\vmgencounter.sys   [23
O58 - SDL:2019/12/07 10:07:57 A . (.Microsoft Corporation - Virtual Machine Guest Infrastructure Driver.) -- C:\WINDOWS\System32\drivers\vmgid.sys
O58 - SDL:2018/11/21 01:21:54 A . (.VMware, Inc. - VMware VMware Input Filter and Injection Dr.) -- C:\WINDOWS\System32\drivers\vmkbd.sys   [52288]  =
O58 - SDL:2018/11/21 01:27:46 A . (.VMware, Inc. - VMware virtual network driver (64-bit).) -- C:\WINDOWS\System32\drivers\vmnet.sys   [46040]  =>.VMw
O58 - SDL:2018/11/21 01:27:52 A . (.VMware, Inc. - VMware virtual network adapter driver (64-b.) -- C:\WINDOWS\System32\drivers\vmnetadapter.sys   [46
O58 - SDL:2018/11/21 01:27:52 A . (.VMware, Inc. - VMware network application interface driver.) -- C:\WINDOWS\System32\drivers\vmnetuserif.sys   [439
O58 - SDL:2019/12/07 10:07:57 A . (.Microsoft Corporation - Microsoft S3 Emulated Device Cap Driver.) -- C:\WINDOWS\System32\drivers\vms3cap.sys   [18
O58 - SDL:2019/12/07 10:07:57 A . (.Microsoft Corporation - Pilote de filtre de stockage virtuel.) -- C:\WINDOWS\System32\drivers\vmstorfl.sys   [5428
O58 - SDL:2018/11/21 01:21:42 A . (.VMware, Inc. - VMware kernel driver.) -- C:\WINDOWS\System32\drivers\vmx86.sys   [99272]  =>.VMware, Inc.®
O58 - SDL:2020/10/16 13:24:14 A . (.Microsoft Corporation - Pilote du gestionnaire de volumes.) -- C:\WINDOWS\System32\drivers\volmgr.sys   [90432]  =
O58 - SDL:2019/12/07 10:09:37 A . (.Microsoft Corporation - Pilote d’extension du gestionnaire de volum.) -- C:\WINDOWS\System32\drivers\volmgrx.sys
O58 - SDL:2020/09/10 22:42:18 A . (.Microsoft Corporation - Pilote de cliché instantané du volume.) -- C:\WINDOWS\System32\drivers\volsnap.sys   [4298
O58 - SDL:2019/12/07 10:07:53 A . (.Microsoft Corporation - Volume driver.) -- C:\WINDOWS\System32\drivers\volume.sys   [16696]  =>.Microsoft®
O58 - SDL:2019/12/07 10:07:57 A . (.Microsoft Corporation - Virtual PCI Bus.) -- C:\WINDOWS\System32\drivers\vpci.sys   [89400]  =>.Microsoft®
O58 - SDL:2019/12/07 10:07:54 A . (.VIA Technologies Inc.,Ltd - VIA RAID DRIVER FOR AMD-X86-64.) -- C:\WINDOWS\System32\drivers\vsmraid.sys   [166712]
O58 - SDL:2018/06/22 01:31:02 A . (.VMware, Inc. - VMware vSockets Service.) -- C:\WINDOWS\System32\drivers\vsock.sys   [92040]  =>.VMware, Inc.®
O58 - SDL:2019/12/07 10:07:54 A . (.VIA Corporation - VIA StorX RAID Controller Driver.) -- C:\WINDOWS\System32\drivers\VSTXRAID.SYS   [305464]  =>.Mi
O58 - SDL:2019/12/07 10:08:13 A . (.Microsoft Corporation - Virtual Wireless Bus Driver.) -- C:\WINDOWS\System32\drivers\vwifibus.sys   [29184] [Unsig
O58 - SDL:2019/12/07 10:08:13 A . (.Microsoft Corporation - Virtual WiFi Filter Driver.) -- C:\WINDOWS\System32\drivers\vwififlt.sys   [77824] [Unsigr
O58 - SDL:2019/12/07 10:08:13 A . (.Microsoft Corporation - Virtual WiFi Miniport Driver.) -- C:\WINDOWS\System32\drivers\vwifimp.sys   [50688] [Unsig
O58 - SDL:2019/12/07 10:07:53 A . (.Microsoft Corporation - Pilote de tablette Wacom à stylet série.) -- C:\WINDOWS\System32\drivers\wacompen.sys   [3
O58 - SDL:2020/10/16 13:24:56 A . (.Microsoft Corporation - MS Remote Access and Routing ARP Driver.) -- C:\WINDOWS\System32\drivers\wanarp.sys   [931
O58 - SDL:2019/12/07 10:08:24 A . (.Microsoft Corporation - Watchdog Driver.) -- C:\WINDOWS\System32\drivers\watchdog.sys   [74752] [Unsigned]  =>.Mic
O58 - SDL:2019/12/07 10:08:34 A . (.Microsoft Corporation - Windows Container Isolation FS Filter Drive.) -- C:\WINDOWS\System32\drivers\wcifs.sys
O58 - SDL:2019/12/07 10:08:34 A . (.Microsoft Corporation - Windows Container Name Virtualization FS Fi.) -- C:\WINDOWS\System32\drivers\wcnfs.sys
O58 - SDL:2019/12/07 10:08:15 A . (.Microsoft Corporation - Microsoft antimalware boot driver.) -- C:\WINDOWS\System32\drivers\WdBoot.sys   [46688]  =
O58 - SDL:2020/08/14 21:06:25 A . (.Microsoft Corporation - Runtime de l’infrastructure de pilotes en m.) -- C:\WINDOWS\System32\drivers\Wdf01000.sys
O58 - SDL:2019/12/07 10:08:15 A . (.Microsoft Corporation - Microsoft antimalware file system filter dr.) -- C:\WINDOWS\System32\drivers\WdFilter.sys
O58 - SDL:2020/08/14 21:06:25 A . (.Microsoft Corporation - Kernel Mode Driver Framework Loader.) -- C:\WINDOWS\System32\drivers\WdfLdr.sys   [59192]
O58 - SDL:2020/09/10 22:42:17 A . (.Microsoft Corporation - WDI Driver Framework Driver.) -- C:\WINDOWS\System32\drivers\WdiWiFi.sys   [951808] [Unsig
O58 - SDL:2019/12/07 10:08:39 A . (.Microsoft Corporation - WDM Companion Filter.) -- C:\WINDOWS\System32\drivers\WdmCompanionFilter.sys   [23560]  =>
O58 - SDL:2019/12/07 10:08:16 A . (.Microsoft Corporation - Windows Defender Network Stream Filter.) -- C:\WINDOWS\System32\drivers\WdNisDrv.sys   [54
O58 - SDL:2019/12/07 10:08:49 A . (.Microsoft Corporation - Windows Error Reporting Kernel Driver.) -- C:\WINDOWS\System32\drivers\werkernel.sys   [52
O58 - SDL:2020/10/16 13:24:38 A . (.Microsoft Corporation - WFP NDIS 6.30 Lightweight Filter Driver.) -- C:\WINDOWS\System32\drivers\wfplwfs.sys   [18
O58 - SDL:2020/08/14 21:06:23 A . (.Microsoft Corporation - Wim file system Driver.) -- C:\WINDOWS\System32\drivers\wimmount.sys   [39736]  =>.Microso
O58 - SDL:2019/12/07 10:08:37 A . (.Microsoft Corporation - Windows Trusted Runtime Interface Driver.) -- C:\WINDOWS\System32\drivers\WindowsTrustedRT
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Windows Trusted Runtime Service Proxy Drive.) -- C:\WINDOWS\System32\drivers\WindowsTruste
O58 - SDL:2019/12/07 10:09:51 A . (.Microsoft Corporation - Windows Hypervisor Interface Driver.) -- C:\WINDOWS\System32\drivers\winhv.sys   [32784]
```

```
O58 - SDL:2019/12/07 10:09:33 A . (.Microsoft Corporation - Windows Hypervisor Root Interface Driver.) -- C:\WINDOWS\System32\drivers\winhvr.sys   [96
O58 - SDL:2019/12/07 10:07:54 A . (.Mellanox - Kernel WinMad.) -- C:\WINDOWS\System32\drivers\winmad.sys   [36152]  =>.Microsoft®
O58 - SDL:2020/09/10 22:42:14 A . (.Microsoft Corporation - Pilote NAT Windows.) -- C:\WINDOWS\System32\drivers\winnat.sys   [259584] [Unsigned]  =>.M
O58 - SDL:2019/12/07 10:07:56 A . (.Microsoft Corporation - Windows WinUSB Class Driver.) -- C:\WINDOWS\System32\drivers\winusb.sys   [107008] [Unsigr
O58 - SDL:2019/12/07 10:07:54 A . (.Mellanox - Kernel WinVerbs.) -- C:\WINDOWS\System32\drivers\winverbs.sys   [73016]  =>.Microsoft®
O58 - SDL:2019/12/07 10:07:54 A . (.Microsoft Corporation - Windows Management Interface for ACPI.) -- C:\WINDOWS\System32\drivers\wmiacpi.sys   [1945
O58 - SDL:2019/12/07 10:08:49 A . (.Microsoft Corporation - WMILIB WMI support library Dll.) -- C:\WINDOWS\System32\drivers\wmilib.sys   [19472]  =>.M
O58 - SDL:2019/12/07 10:08:46 A . (.Microsoft Corporation - Filtre de superposition Windows.) -- C:\WINDOWS\System32\drivers\wof.sys   [234504]  =>.Mi
O58 - SDL:2019/12/07 15:52:58 A . (.Microsoft Corporation - Windows Portable Device Upper Class Filter.) -- C:\WINDOWS\System32\drivers\WpdUpFltr.sys
O58 - SDL:2019/12/07 10:08:49 A . (.Microsoft Corporation - WPP Trace Recorder.) -- C:\WINDOWS\System32\drivers\WppRecorder.sys   [43832]  =>.Microsof
O58 - SDL:2019/12/07 10:08:41 A . (.Microsoft Corporation - Couche IFS Winsock2.) -- C:\WINDOWS\System32\drivers\ws2ifsl.sys   [25088] [Unsigned]  =>
O58 - SDL:2019/12/07 10:07:50 A . (.Microsoft Corporation - Web Services Print Device Driver.) -- C:\WINDOWS\System32\drivers\WSDPrint.sys   [23552]
O58 - SDL:2020/05/11 06:40:14 A . (.Microsoft Corporation - Web Service Based Scan Device Driver.) -- C:\WINDOWS\System32\drivers\WSDScan.sys   [26112
O58 - SDL:2019/12/07 10:08:58 A . (.Microsoft Corporation - Windows Driver Foundation - User-mode Drive.) -- C:\WINDOWS\System32\drivers\WUDFPf.sys
O58 - SDL:2019/12/07 10:08:58 A . (.Microsoft Corporation - Windows Driver Foundation - User-mode Drive.) -- C:\WINDOWS\System32\drivers\WUDFRd.sys
O58 - SDL:2020/11/13 18:54:45 A . (.Microsoft Corporation - Game Input Protocol Driver.) -- C:\WINDOWS\System32\drivers\xboxgip.sys   [324608] [Unsigr
O58 - SDL:2020/11/13 18:54:45 A . (.Microsoft Corporation - XINPUT filter driver for HID.) -- C:\WINDOWS\System32\drivers\xinputhid.sys   [48640] [Uns
O58 - SDL:2016/08/17 23:53:26 A . (.Intel Corporation - Intel(R) Acpi Control Driver.) -- C:\WINDOWS\System32\drivers\XtuAcpiDriver.sys   [54352]  =>
O58 - SDL:2019/12/07 10:07:47 A . (.Microsoft Corporation - Xbox 360 Common Controller for Windows Driv.) -- C:\WINDOWS\System32\drivers\xusb22.sys
O58 - SDL:2016/12/21 22:54:56 A . (...) -- C:\WINDOWS\System32\ambakdrv.sys   [51120]  =>.CHENGDU AOMEI Tech Co., Ltd.®
O58 - SDL:2016/12/21 22:52:42 A . (...) -- C:\WINDOWS\System32\ammntdrv.sys   [171952]  =>.CHENGDU AOMEI Tech Co., Ltd.®
O58 - SDL:2017/09/01 18:12:38 A . (...) -- C:\WINDOWS\System32\amwrtdrv.sys   [38320]  =>.CHENGDU AOMEI Tech Co., Ltd.®
O58 - SDL:2020/11/13 18:54:58 A . (.Microsoft Corporation - Multi-User Win32 Driver.) -- C:\WINDOWS\System32\win32k.sys   [596992] [Unsigned]  =>.Micr
O58 - SDL:2020/11/13 18:54:56 A . (.Microsoft Corporation - Pilote du noyau Base Win32k.) -- C:\WINDOWS\System32\win32kbase.sys   [2942976] [Unsigned]
O58 - SDL:2020/11/13 18:54:58 A . (.Microsoft Corporation - Full/Desktop Win32k Kernel Driver.) -- C:\WINDOWS\System32\win32kfull.sys   [3815936] [Uns
O58 - SDL:2019/12/07 10:08:34 A . (.Microsoft Corporation - Win32k non session driver.) -- C:\WINDOWS\System32\win32kns.sys   [30208] [Unsigned]  =>.M
O58 - SDL:2020/11/13 18:55:14 A . (.Microsoft Corporation - Multi-User Win32 Driver.) -- C:\WINDOWS\SysWOW64\win32k.sys   [329728] [Unsigned]  =>.Micr
O58 - SDL:2020/11/13 18:55:14 A . (.Microsoft Corporation - Full/Desktop Win32k Kernel Driver.) -- C:\WINDOWS\SysWOW64\win32kfull.sys   [2749952] [Uns

---\ ASSOCIATION Shell Spawning (10) - 1s
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]
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\eve
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
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
O67 - Shell Spawning: <.scr> [HKLM\..\open\Command] (...) -- '%1' /S  =>.Default.Value

---\ MENU DE DÉMARRAGE INTERNET (20) - 0s
O68 - StartMenuInternet:   [64Bits][HKLM\..\Shell\open\Command] (.Mozilla Corporation - Firefox.) -- C:\Program Files\Mozilla Firefox\firefox.exe   =>
O68 - StartMenuInternet:   [64Bits][HKLM\..\Shell\open\Command] (.Mozilla Corporation - Firefox Developer Edition.) -- C:\Program Files\Firefox Develo
O68 - StartMenuInternet:   [64Bits][HKLM\..\Shell\open\Command] (.Google LLC - Google Chrome.) -- C:\Program Files\Google\Chrome\Application\chrome.ex
O68 - StartMenuInternet:   [64Bits][HKLM\..\Shell\open\Command] (.Microsoft Corporation - Internet Explorer.) -- C:\Program Files\Internet Explorer\ie
O68 - StartMenuInternet:   [64Bits][HKLM\..\Shell\open\Command] (.Microsoft Corporation - Microsoft Edge.) -- C:\Program Files (x86)\Microsoft\Edge\Ap
O68 - StartMenuInternet:   [64Bits][HKLM\..\InstallInfo\ShowIconsCommand] (.Mozilla Corporation - Firefox Helper.) -- C:\Program Files\Mozilla Firefox
O68 - StartMenuInternet:   [64Bits][HKLM\..\InstallInfo\ShowIconsCommand] (.mozilla.org - Firefox Developer Edition Helper.) -- C:\Program Files\Firef
O68 - StartMenuInternet:   [64Bits][HKLM\..\InstallInfo\ShowIconsCommand] (.Google LLC - Google Chrome.) -- C:\Program Files\Google\Chrome\Applicatior
O68 - StartMenuInternet:   [64Bits][HKLM\..\InstallInfo\ShowIconsCommand] (.Microsoft Corporation - IE Per-User Show IE Icon Utility.) -- C:\WINDOWS\S
O68 - StartMenuInternet:   [64Bits][HKLM\..\InstallInfo\ShowIconsCommand] (.Microsoft Corporation - Microsoft Edge.) -- C:\Program Files (x86)\Microsc
O68 - StartMenuInternet:   [64Bits][HKLM\..\InstallInfo\ReinstallCommand] (.Mozilla Corporation - Firefox Helper.) -- C:\Program Files\Mozilla Firefox
O68 - StartMenuInternet:   [64Bits][HKLM\..\InstallInfo\ReinstallCommand] (.mozilla.org - Firefox Developer Edition Helper.) -- C:\Program Files\Firef
O68 - StartMenuInternet:   [64Bits][HKLM\..\InstallInfo\ReinstallCommand] (.Google LLC - Google Chrome.) -- C:\Program Files\Google\Chrome\Applicatior
O68 - StartMenuInternet:   [64Bits][HKLM\..\InstallInfo\ReinstallCommand] (.Microsoft Corporation - Utilitaire d'initialisation d'Internet Expl.) -- C
O68 - StartMenuInternet:   [64Bits][HKLM\..\InstallInfo\ReinstallCommand] (.Microsoft Corporation - Microsoft Edge.) -- C:\Program Files (x86)\Microsc
O68 - StartMenuInternet:   [64Bits][HKLM\..\InstallInfo\HideIconsCommand] (.Mozilla Corporation - Firefox Helper.) -- C:\Program Files\Mozilla Firefox
O68 - StartMenuInternet:   [64Bits][HKLM\..\InstallInfo\HideIconsCommand] (.mozilla.org - Firefox Developer Edition Helper.) -- C:\Program Files\Firef
O68 - StartMenuInternet:   [64Bits][HKLM\..\InstallInfo\HideIconsCommand] (.Google LLC - Google Chrome.) -- C:\Program Files\Google\Chrome\Applicatior
O68 - StartMenuInternet:   [64Bits][HKLM\..\InstallInfo\HideIconsCommand] (.Microsoft Corporation - IE Per-User Show IE Icon Utility.) -- C:\WINDOWS\S
O68 - StartMenuInternet:   [64Bits][HKLM\..\InstallInfo\HideIconsCommand] (.Microsoft Corporation - Microsoft Edge.) -- C:\Program Files (x86)\Microsc

---\ RECHERCHE D'INFECTION SUR NAVIGATEURS (2) - 15s
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} [DefaultScope] - (Bing) - http://www.bing.com/  =>.Bing.com

---\ ÉNUMÈRE LES FICHIERS Crack et Keygen (1) - 84s
O82 - LFC: 2019/11/15 09:02:01 A . (...) -- C:\Users\couli\Downloads\PowerISO_7-5_Multilingual\PowerISO 7.5 Multilingual\PowerISO_Keygen.exe   [258566

---\ ÉNUMÈRE LES SERVICES DÉMARRÉS PAR Svchost (50) - 2s
O83 - Search Svchost Services: CertPropSvc (CertPropSvc) . (.Microsoft Corporation - Service de propagation de certificats de ca.) -- C:\WINDOWS\Syste
O83 - Search Svchost Services: SCPolicySvc (SCPolicySvc) . (.Microsoft Corporation - Service de propagation de certificats de ca.) -- C:\Windows\Syste
O83 - Search Svchost Services: lanmanserver (lanmanserver) . (.Microsoft Corporation - DLL du service Serveur.) -- C:\Windows\System32\srvsvc.dll   [3
O83 - Search Svchost Services: gpsvc (gpsvc) . (.Microsoft Corporation - Client de stratégie de groupe.) -- C:\Windows\System32\gpsvc.dll   [1306624]
O83 - Search Svchost Services: IKEEXT (IKEEXT) . (.Microsoft Corporation - Extension IKE.) -- C:\Windows\System32\IKEEXT.DLL   [1051136] [Unsigned]  =
O83 - Search Svchost Services: iphlpsvc (iphlpsvc) . (.Microsoft Corporation - Service offrant une connectivité IPv6 sur u.) -- C:\Windows\System32\ip
O83 - Search Svchost Services: seclogon (seclogon) . (.Microsoft Corporation - DLL de service d'ouverture de session secon.) -- C:\Windows\System32\se
O83 - Search Svchost Services: msiscsi (msiscsi) . (.Microsoft Corporation - Service de découverte iSCSI.) -- C:\Windows\System32\iscsiexe.dll   [1602
O83 - Search Svchost Services: EapHost (EapHost) . (.Microsoft Corporation - Service EAPHost Microsoft.) -- C:\Windows\System32\eapsvc.dll   [112640]
O83 - Search Svchost Services: schedule (schedule) . (.Microsoft Corporation - Service du Planificateur de tâches.) -- C:\Windows\System32\schedsvc.dl
O83 - Search Svchost Services: winmgmt (winmgmt) . (.Microsoft Corporation - WMI.) -- C:\Windows\System32\wbem\WMIsvc.dll   [243712] [Unsigned]  =>.Mi
O83 - Search Svchost Services: ProfSvc (ProfSvc) . (.Microsoft Corporation - ProfSvc.) -- C:\Windows\System32\profsvc.dll   [486912] [Unsigned]  =>.Mi
O83 - Search Svchost Services: SessionEnv (SessionEnv) . (.Microsoft Corporation - Service Configuration des services Bureau à.) -- C:\Windows\System3
O83 - Search Svchost Services: wercplsupport (wercplsupport) . (.Microsoft Corporation - Rapports de problèmes.) -- C:\Windows\System32\wercplsupport
O83 - Search Svchost Services: InstallService (InstallService) . (.Microsoft Corporation - InstallService.) -- C:\Windows\System32\InstallService.dll
O83 - Search Svchost Services: PushToInstall (PushToInstall) . (.Microsoft Corporation - PushToInstall.) -- C:\Windows\System32\PushToInstall.dll   [2
O83 - Search Svchost Services: TroubleshootingSvc (TroubleshootingSvc) . (.Microsoft Corporation - MitigationClient.) -- C:\Windows\System32\Mitigatic
O83 - Search Svchost Services: LxpSvc (LxpSvc) . (.Microsoft Corporation - Fournit une prise en charge de l'infrastruc.) -- C:\Windows\System32\Langua
O83 - Search Svchost Services: shpamsvc (shpamsvc) . (.Microsoft Corporation - SharedPC.AccountManager.) -- C:\Windows\System32\Windows.SharedPC.Accou
O83 - Search Svchost Services: XblGameSave (XblGameSave) . (.Microsoft Corporation - Xbox Live Game Save Service.) -- C:\Windows\System32\XblGameSave
O83 - Search Svchost Services: DmEnrollmentSvc (DmEnrollmentSvc) . (.Microsoft Corporation - DLL Windows Management Service.) -- C:\Windows\System32\W
O83 - Search Svchost Services: WManSvc (WManSvc) . (.Microsoft Corporation - DLL du Service de gestion de Windows.) -- C:\Windows\System32\Windows.Mar
O83 - Search Svchost Services: Themes (Themes) . (.Microsoft Corporation - DLL du service des thèmes Windows Shell.) -- C:\Windows\System32\themeservi
O83 - Search Svchost Services: UserManager (UserManager) . (.Microsoft Corporation - UserMgr.) -- C:\Windows\System32\usermgr.dll   [1488896] [Unsigne
O83 - Search Svchost Services: NetSetupSvc (NetSetupSvc) . (.Microsoft Corporation - Service Configuration du réseau.) -- C:\Windows\System32\NetSetup
O83 - Search Svchost Services: wlidsvc (wlidsvc) . (.Microsoft Corporation - Service de compte Microsoft®.) -- C:\Windows\System32\wlidsvc.dll   [2242
O83 - Search Svchost Services: TokenBroker (TokenBroker) . (.Microsoft Corporation - Broker à jetons.) -- C:\Windows\System32\TokenBroker.dll   [15319
O83 - Search Svchost Services: lfsvc (lfsvc) . (.Microsoft Corporation - Service de géolocalisation.) -- C:\Windows\System32\lfsvc.dll   [48640] [Unsi
O83 - Search Svchost Services: NaturalAuthentication (NaturalAuthentication) . (.Microsoft Corporation - Service d'authentification naturelle.) -- C:\
O83 - Search Svchost Services: Rasauto (Rasauto) . (.Microsoft Corporation - Gestionnaire de numérotation automatique d'.) -- C:\Windows\System32\rasa
O83 - Search Svchost Services: Rasman (Rasman) . (.Microsoft Corporation - Gestionnaire des connexions d'accès à dista.) -- C:\Windows\System32\rasmar
O83 - Search Svchost Services: Remoteaccess (Remoteaccess) . (.Microsoft Corporation - Gestionnaire d'interface dynamique.) -- C:\Windows\System32\mpr
O83 - Search Svchost Services: SENS (SENS) . (.Microsoft Corporation - Service de notification d'événements systèm.) -- C:\Windows\System32\Sens.dll
```

```
O83 - Search Svchost Services: Sharedaccess (Sharedaccess) . (.Microsoft Corporation - Composants de l'application d'assistance à.) -- C:\Windows\Syst
O83 - Search Svchost Services: Tapisrv (Tapisrv) . (.Microsoft Corporation - Serveur de téléphonie Microsoft® Windows(TM.) -- C:\Windows\System32\tapi
O83 - Search Svchost Services: wuauserv (wuauserv) . (.Microsoft Corporation - Agent de mise à jour automatique Windows Up.) -- C:\Windows\System32\wu
O83 - Search Svchost Services: BITS (BITS) . (.Microsoft Corporation - Service de transfert intelligent en arrière.) -- C:\Windows\System32\qmgr.dll
O83 - Search Svchost Services: ShellHWDetection (ShellHWDetection) . (.Microsoft Corporation - Dll des services Windows Shell.) -- C:\Windows\System32
O83 - Search Svchost Services: dmwappushservice (dmwappushservice) . (.Microsoft Corporation - dmwappushsvc.) -- C:\Windows\System32\dmwappushsvc.dll
O83 - Search Svchost Services: wisvc (wisvc) . (.Microsoft Corporation - Paramètres de vol.) -- C:\Windows\System32\flightsettings.dll   [939448]  =>
O83 - Search Svchost Services: WpnService (WpnService) . (.Microsoft Corporation - Service du système de notifications Push Wi.) -- C:\Windows\System3
O83 - Search Svchost Services: AppInfo (AppInfo) . (.Microsoft Corporation - Service Informations d'application.) -- C:\Windows\System32\appinfo.dll
O83 - Search Svchost Services: XboxNetApiSvc (XboxNetApiSvc) . (.Microsoft Corporation - Xbox Live Networking Service.) -- C:\Windows\System32\XboxNet
O83 - Search Svchost Services: UsoSvc (UsoSvc) . (.Microsoft Corporation - Mettre à jour la session du service Orchest.) -- C:\Windows\System32\usosvc
O83 - Search Svchost Services: XboxGipSvc (XboxGipSvc) . (.Microsoft Corporation - Xbox Gip Management Service.) -- C:\Windows\System32\XboxGipSvc.dll
O83 - Search Svchost Services: NcaSvc (NcaSvc) . (.Microsoft Corporation - Service Assistant Connectivité réseau Micro.) -- C:\Windows\System32\NcaSvc
O83 - Search Svchost Services: XblAuthManager (XblAuthManager) . (.Microsoft Corporation - Xbox Live Auth Manager.) -- C:\Windows\System32\XblAuthMana
O83 - Search Svchost Services: DsmSvc (DsmSvc) . (.Microsoft Corporation - Gestionnaire d'installation de périphérique.) -- C:\Windows\System32\Device
O83 - Search Svchost Services: BDESVC (BDESVC) . (.Microsoft Corporation - Service BDE.) -- C:\Windows\System32\bdesvc.dll   [562688] [Unsigned]  =>.M
O83 - Search Svchost Services: browser (browser) . (.Microsoft Corporation - DLL du service Explorateur d'ordinateurs.) -- C:\Windows\System32\browser

---\ LISTE DES EXCEPTIONS PAREFEU WINDOWS (193) - 16s
O87 - FAEL: 'UDP Query User{15E8F11C-D3E3-44A2-84BF-8EA6B9143136}C:\users\couli\appdata\local\programs\opera\68.0.3618.104\opera.exe' [In-None-P17-TRU
O87 - FAEL: 'TCP Query User{A9A9FFF9-05D1-4647-B7EA-AC8554199FE3}C:\users\couli\appdata\local\programs\opera\68.0.3618.104\opera.exe' [In-None-P6-TRUE
O87 - FAEL: 'UDP Query User{F0A8516D-71E0-464D-9F94-43346BF89167}D:\android studio\jre\bin\java.exe' [In-None-P17-TRUE] .(.N/A - OpenJDK Platform bina
O87 - FAEL: 'TCP Query User{B4D40525-4D43-41A6-910F-78DA36BC42DE}D:\android studio\jre\bin\java.exe' [In-None-P6-TRUE] .(.N/A - OpenJDK Platform binar
O87 - FAEL: 'UDP Query User{5E2B05C7-5306-4189-9FAD-E54418AD2F5F}D:\origin\fifa 20\fifa20.exe' [In-None-P17-TRUE] .(.Electronic Arts - FIFA 20.) -- D
O87 - FAEL: 'TCP Query User{F3D19871-3B86-4474-9870-3D54C7B00BF7}D:\origin\fifa 20\fifa20.exe' [In-None-P6-TRUE] .(.Electronic Arts - FIFA 20.) -- D:\
O87 - FAEL: '{3857175C-9827-49E3-8387-FC12B74F58CE}' [In-None-P17-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\Hacker Evolution IMMERSION Demo\HEI
O87 - FAEL: '{D52EE035-ED86-41ED-B4A5-0904B22EC459}' [In-None-P6-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\Hacker Evolution IMMERSION Demo\HEI
O87 - FAEL: '{90586DCA-0623-4F74-8282-72B6DDAFDDC2}' [In-None-P17-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\Hacker Evolution IMMERSION Demo\Hac
O87 - FAEL: '{8F5DB80E-AEC2-445F-A8A2-F81649BA92FF}' [In-None-P6-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\Hacker Evolution IMMERSION Demo\Hack
O87 - FAEL: '{1EAE9E2D-B510-4525-8983-6C78FD2CAC6B}' [In-None-P17-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\Cities_Skylines\dowser.exe  =>.Para
O87 - FAEL: '{5641996B-A310-46A7-AA08-958778652A9C}' [In-None-P6-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\Cities_Skylines\dowser.exe  =>.Parad
O87 - FAEL: '{EFB43127-A123-4F2C-ADEC-0542A2DDEB71}' [In-None-P17-TRUE] .(.The NW.js Community - nwjs.) -- D:\SteamLibrary\steamapps\common\Smartphone
O87 - FAEL: '{02D7F381-CEBD-43C7-9447-A244978D5214}' [In-None-P6-TRUE] .(.The NW.js Community - nwjs.) -- D:\SteamLibrary\steamapps\common\Smartphone
O87 - FAEL: 'UDP Query User{7069223C-EF75-45E3-966C-00D6FB4DA7F9}D:\steamlibrary\steamapps\common\sandstorm\insurgency\binaries\win64\insurgencyclient
O87 - FAEL: 'TCP Query User{80FE6555-23E1-4B88-85DD-37A76B87B907}D:\steamlibrary\steamapps\common\sandstorm\insurgency\binaries\win64\insurgencyclient
O87 - FAEL: '{E26CC0C3-2968-4B4D-ABAA-9BEF3B7E2B6C}' [In-None-P17-TRUE] .(.Epic Games, Inc. - BootstrapPackagedGame.) -- D:\SteamLibrary\steamapps\com
O87 - FAEL: '{533F3834-43AD-477D-A649-4F5B3B6B7899}' [In-None-P6-TRUE] .(.Epic Games, Inc. - BootstrapPackagedGame.) -- D:\SteamLibrary\steamapps\comm
O87 - FAEL: '{79A8350B-F79C-4D09-AF34-862A7659221D}' [In-None-P17-TRUE] .(.EasyAntiCheat Ltd - EasyAntiCheat Launcher.) -- D:\SteamLibrary\steamapps\c
O87 - FAEL: '{05D6DD8C-BC30-404E-A8B8-1206A6A6A508}' [In-None-P6-TRUE] .(.EasyAntiCheat Ltd - EasyAntiCheat Launcher.) -- D:\SteamLibrary\steamapps\co
O87 - FAEL: '{6ACF66F5-0C57-43BB-8595-0833AD0E7DC8}' [In-None-P6-TRUE] .(...) -- C:\Program Files\WindowsApps\AD2F1837.OMENCommandCenter_9.9.3.0_x64__
O87 - FAEL: '{69EC754C-3023-43FE-99FD-FEF816F6B97C}' [In-None-P6-TRUE] .(...) -- C:\Program Files\WindowsApps\AD2F1837.OMENCommandCenter_9.9.3.0_x64__
O87 - FAEL: '{8D08AEE4-A3F2-4B20-829F-A40D7E17EF4A}' [In-None-P6-TRUE] .(...) -- C:\Program Files\WindowsApps\AD2F1837.OMENCommandCenter_9.9.3.0_x64__
O87 - FAEL: '{B20FDE13-8322-4F3D-8A45-5DB0673BBC72}' [In-None-P6-TRUE] .(...) -- C:\Program Files\WindowsApps\AD2F1837.OMENCommandCenter_9.9.3.0_x64__
O87 - FAEL: 'UDP Query User{5A6A6AA2-46DB-45C1-8E31-2124A8D313FB}C:\users\couli\appdata\local\popcorn-time\popcorn-time.exe' [In-None-P17-TRUE] .(.The
O87 - FAEL: 'TCP Query User{9E2B1826-2E16-47D7-8F64-FD7383A11DAB}C:\users\couli\appdata\local\popcorn-time\popcorn-time.exe' [In-None-P6-TRUE] .(.The
O87 - FAEL: 'UDP Query User{A5AC917A-3D9F-496A-AB58-95CEE08A7880}C:\users\couli\appdata\local\programs\opera\67.0.3575.53\opera.exe' [In-None-P17-TRUE
O87 - FAEL: 'TCP Query User{2C71F9C3-E692-4A4C-B5FE-F1185A724322}C:\users\couli\appdata\local\programs\opera\67.0.3575.53\opera.exe' [In-None-P6-TRUE]
O87 - FAEL: '{FC5E5853-EA51-41C8-973A-B387D74666ED}' [In-None-P17-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\Smart City Plan\game.exe {6E27D4BA1
O87 - FAEL: '{A4E9FBD3-F494-4282-861C-F5D9DDD1C4DF}' [In-None-P6-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\Smart City Plan\game.exe {6E27D4BA14
O87 - FAEL: '{765C09F3-ECC4-4CF1-8DDD-89369560959D}' [In-None-P6-TRUE] .(...) -- C:\Users\couli\AppData\Local\Temp\7zS5257\HP.EasyStart.exe [Unsigned]
O87 - FAEL: 'UDP Query User{24E7DBDD-A1F7-4BEF-B831-5BEE81BFF345}C:\users\couli\appdata\local\programs\opera\66.0.3515.115\opera.exe' [In-None-P17-TRU
O87 - FAEL: 'TCP Query User{1E403A3E-C7D0-4784-9DDF-F05421B53106}C:\users\couli\appdata\local\programs\opera\66.0.3515.115\opera.exe' [In-None-P6-TRUE
O87 - FAEL: 'UDP Query User{7A4F3A2D-3CD4-4301-9D4E-02F1675E4474}C:\users\couli\appdata\local\programs\opera\66.0.3515.103\opera.exe' [In-None-P17-TRU
O87 - FAEL: 'TCP Query User{E7ED12B3-B4F6-4C9A-BCB3-20A5184FF518}C:\users\couli\appdata\local\programs\opera\66.0.3515.103\opera.exe' [In-None-P6-TRUE
O87 - FAEL: 'UDP Query User{0AB23904-795E-4ED5-AD3C-9B590234592D}C:\users\couli\appdata\local\programs\opera\66.0.3515.72\opera.exe' [In-None-P17-TRUE
O87 - FAEL: 'TCP Query User{7C1C0F8A-37FE-4A62-9B1E-90E717FE6E15}C:\users\couli\appdata\local\programs\opera\66.0.3515.72\opera.exe' [In-None-P6-TRUE]
O87 - FAEL: '{0C6B127D-B90A-4AD1-B330-54F937D6BAF6}' [In-None-P17-TRUE] .(.Techland - DyingLight.) -- D:\SteamLibrary\steamapps\common\Dying Light\Dev
O87 - FAEL: '{F2C2AFBF-38BF-4A82-9638-7B23B4A2E69D}' [In-None-P6-TRUE] .(.Techland - DyingLight.) -- D:\SteamLibrary\steamapps\common\Dying Light\DevT
O87 - FAEL: '{5D23A6D6-64C3-4503-A65C-A07179273B28}' [In-None-P17-TRUE] .(.Techland - DyingLight.) -- D:\SteamLibrary\steamapps\common\Dying Light\Dyi
O87 - FAEL: '{26082E74-38EE-4D90-AA7F-FA48A699B329}' [In-None-P6-TRUE] .(.Techland - DyingLight.) -- D:\SteamLibrary\steamapps\common\Dying Light\Dyin
O87 - FAEL: '{5158EE62-F1CA-4A91-BCEE-119CE86F3F37}' [In-None-P17-TRUE] .(.Mozilla Corporation - Firefox Developer Edition.) -- C:\Program Files\Firef
O87 - FAEL: '{8EF483D7-B2CD-4AD6-B899-2F5CA28C85B3}' [In-None-P6-TRUE] .(.Mozilla Corporation - Firefox Developer Edition.) -- C:\Program Files\Firefo
O87 - FAEL: '{AF84980D-7F01-4993-913F-F265C1F0FB36}' [In-None-P6-TRUE] .(.Xiaomi.Inc - MiPCSuite Module.) -- C:\Users\couli\AppData\Local\MiPhoneManag
O87 - FAEL: 'UDP Query User{18740AF6-0294-4CCF-B8DA-309924244A4C}C:\users\couli\appdata\local\programs\opera\66.0.3515.44\opera.exe' [In-None-P17-TRUE
O87 - FAEL: 'TCP Query User{15CA0D88-DE08-4A85-B614-9A500FA2DEB8}C:\users\couli\appdata\local\programs\opera\66.0.3515.44\opera.exe' [In-None-P6-TRUE]
O87 - FAEL: '{5F9D16C3-7E0B-460D-967F-A9CF947F73A3}' [In-None-P6-TRUE] .(...) -- C:\Program Files (x86)\Avira\SoftwareUpdater\avirasoftwareupdatertoas
O87 - FAEL: '{2DAF5637-BA17-4CE8-A349-FC054DB63D57}' [In-None-P6-TRUE] .(...) -- C:\Program Files (x86)\Avira\SoftwareUpdater\avirasoftwareupdatertoas
O87 - FAEL: '{2B3FBAC7-8D1E-4416-B5F2-8C83CFF1D1D5}' [In-None-P6-TRUE] .(...) -- C:\Program Files (x86)\Avira\SoftwareUpdater\avirasoftwareupdatertoas
O87 - FAEL: '{6A239D03-9368-4509-AF82-5EDEE7AB7162}' [In-None-P17-TRUE] .(...) -- C:\Program Files (x86)\AnyDesk\AnyDesk.exe [Unsigned] (.not file.)
O87 - FAEL: '{E6347150-1DED-4C68-B2F2-E6EECFD46E4B}' [In-None-P6-TRUE] .(...) -- C:\Program Files (x86)\AnyDesk\AnyDesk.exe [Unsigned] (.not file.)  =
O87 - FAEL: '{14ACA864-FC1F-4C95-B835-433973C4A9E6}' [In-None-P17-TRUE] .(...) -- C:\Program Files (x86)\AnyDesk\AnyDesk.exe [Unsigned] (.not file.)
O87 - FAEL: '{335DDD2D-240A-4C0C-A5DA-BC8D6EA73798}' [In-None-P6-TRUE] .(...) -- C:\Program Files (x86)\AnyDesk\AnyDesk.exe [Unsigned] (.not file.)  =
O87 - FAEL: '{92BEB795-D579-430F-AF43-D08BCB8FF98F}' [In-None-P17-TRUE] .(...) -- C:\Program Files (x86)\AnyDesk\AnyDesk.exe [Unsigned] (.not file.)
O87 - FAEL: '{2D29953D-AD19-46CE-B17D-8180DAA76FD4}' [In-None-P6-TRUE] .(...) -- C:\Program Files (x86)\AnyDesk\AnyDesk.exe [Unsigned] (.not file.)  =
O87 - FAEL: '{51210AB7-CE71-4D0E-86BB-28C8677CAA36}' [In-None-P17-TRUE] .(...) -- G:\SteamLibrary\steamapps\common\Car Mechanic Simulator 2018\cms2018
O87 - FAEL: '{FB65C12B-DEAE-482A-A9F7-C8E3F288E64B}' [In-None-P6-TRUE] .(...) -- G:\SteamLibrary\steamapps\common\Car Mechanic Simulator 2018\cms2018
O87 - FAEL: '{0D978030-061F-4AFD-BBBB-2F222639E75A}' [In-None-P17-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\Prison Architect\Prison Architect.e
O87 - FAEL: '{B83E011B-09AD-49D0-A3F6-257A7203C458}' [In-None-P6-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\Prison Architect\Prison Architect.ex
O87 - FAEL: '{962FA75E-EE39-4F7B-9A85-87B8D97D6827}' [In-None-P17-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\Prison Architect\Launcher\dowser.ex
O87 - FAEL: '{5B771EB9-8B76-4988-BEA5-F5CC55DB8866}' [In-None-P6-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\Prison Architect\Launcher\dowser.exe
O87 - FAEL: '{A5531FA0-87BF-45B4-82C6-94621AD69D01}' [In-None-P17-TRUE] .(.GitHub, Inc. - StartupCompany.) -- D:\SteamLibrary\steamapps\common\Startup
O87 - FAEL: '{067E34F0-0B1C-4F02-80B4-19068CFC8DE5}' [In-None-P6-TRUE] .(.GitHub, Inc. - StartupCompany.) -- D:\SteamLibrary\steamapps\common\Startup
O87 - FAEL: '{7C639360-E22E-4A91-BC25-143F86D74449}' [Out-None-P6-TRUE] .(.Apowersoft - ApowerMirror.) -- C:\Program Files (x86)\Apowersoft\ApowerMirr
O87 - FAEL: '{1E695030-BEB7-475E-99AB-8AB520FC8E28}' [In-None-P6-TRUE] .(.Apowersoft - ApowerMirror.) -- C:\Program Files (x86)\Apowersoft\ApowerMirro
O87 - FAEL: '{652C950F-8E3E-4CC5-9F47-AB84ACFF15FB}' [In-None-P17-TRUE] .(.SCS Software - Euro Truck Simulator 2 - Steam.) -- C:\Program Files (x86)\S
O87 - FAEL: '{C4B2E910-B30F-43FB-9892-3CA6C26493AD}' [In-None-P6-TRUE] .(.SCS Software - Euro Truck Simulator 2 - Steam.) -- C:\Program Files (x86)\St
O87 - FAEL: '{68F95965-D6F9-4E64-8FA2-08CC1B7C697F}' [In-None-P17-TRUE] .(.SCS Software - Euro Truck Simulator 2 - Steam.) -- C:\Program Files (x86)\S
O87 - FAEL: '{D0958E8E-21FA-49B8-B32B-B4A65418BD81}' [In-None-P6-TRUE] .(.SCS Software - Euro Truck Simulator 2 - Steam.) -- C:\Program Files (x86)\St
O87 - FAEL: 'UDP Query User{78C09F6B-D761-42BA-8C64-61C1A73593FE}C:\program files\lghub\lghub_agent.exe' [In-None-P17-TRUE] .(.Logitech, Inc. - LGHUB
O87 - FAEL: 'TCP Query User{BE32A701-E455-4B59-8556-52765901F5C8}C:\program files\lghub\lghub_agent.exe' [In-None-P6-TRUE] .(.Logitech, Inc. - LGHUB A
O87 - FAEL: 'UDP Query User{EE9ACAC0-7E92-4C69-813D-4C568F51E113}C:\program files\lghub\lghub_agent.exe' [In-None-P17-TRUE] .(.Logitech, Inc. - LGHUB
O87 - FAEL: 'TCP Query User{8F0C757D-779C-4541-AF35-EC109CFB9B16}C:\program files\lghub\lghub_agent.exe' [In-None-P6-TRUE] .(.Logitech, Inc. - LGHUB A
O87 - FAEL: '{6D23EB64-F478-4F74-B8F5-EF563B4C3EEC}' [In-None-P17-TRUE] .(.Blender Foundation - Blender.) -- D:\SteamLibrary\steamapps\common\Blender\
O87 - FAEL: '{D0987774-7477-462C-A8B5-81231E9B123B}' [In-None-P6-TRUE] .(.Blender Foundation - Blender.) -- D:\SteamLibrary\steamapps\common\Blender\b
O87 - FAEL: '{E96CFBFF-A250-4B33-B407-C4523D6A5785}' [In-None-P17-TRUE] .(.Frontier Developments - Planet Coaster.) -- D:\SteamLibrary\steamapps\commo
O87 - FAEL: '{7D94CA0B-1D14-48A2-853F-4DBCA41FDF79}' [In-None-P6-TRUE] .(.Frontier Developments - Planet Coaster.) -- D:\SteamLibrary\steamapps\commor
O87 - FAEL: 'UDP Query User{101D4E98-9B5F-44DC-B6B1-2CA5929814B5}G:\farming.simulator.19.v1.3.0.1.incl.dlcs\farming.simulator.19.v1.3.0.1.incl.dlcs\fa
O87 - FAEL: 'TCP Query User{1027CB7B-5DAE-44B3-8B0A-AB20E76914DF}G:\farming.simulator.19.v1.3.0.1.incl.dlcs\farming.simulator.19.v1.3.0.1.incl.dlcs\fa
O87 - FAEL: 'UDP Query User{B790D152-9839-4AD4-AED8-CEC373D24CB6}D:\games\farming simulator 19\dedicatedserver.exe' [In-None-P17-TRUE] .(.GIANTS Softw
O87 - FAEL: 'TCP Query User{0D58D7D2-19BD-4A12-A981-70EE5AC30908}D:\games\farming simulator 19\dedicatedserver.exe' [In-None-P6-TRUE] .(.GIANTS Softwa
O87 - FAEL: '{1DAB0AD3-F6C4-4032-86E5-EB056C5FC74B}' [In-None-P17-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\YoutubersLife\YoutubersLife.exe [Un
O87 - FAEL: '{605F4E6E-49E2-482D-ADF2-7E3536BE25ED}' [In-None-P6-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\YoutubersLife\YoutubersLife.exe [Uns
O87 - FAEL: '{3EF334C9-B1DB-4EB3-8BA1-91E5E75F5EE4}' [In-None-P17-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\PC Building Simulator\PCBS.exe [Uns
O87 - FAEL: '{8752F5EF-89C5-4099-B57D-F5ED2B3B1463}' [In-None-P6-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\PC Building Simulator\PCBS.exe [Unsi
```

```
O87 - FAEL: '{A0FC7B6F-23B3-48E3-9A66-DC61E585563E}' [In-None-P17-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\Production Line\ProductionLine.exe
O87 - FAEL: '{A7F231BE-ED67-4B2D-8B97-CB0481593001}' [In-None-P6-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\Production Line\ProductionLine.exe
O87 - FAEL: '{8F1D713A-E9F5-421A-AB5A-6EE94E0475F9}' [In-None-P17-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\Tourist Bus Simulator\TouristBusSim
O87 - FAEL: '{12686F5A-BE73-47EA-94B5-E1FAE6D8DC3D}' [In-None-P6-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\Tourist Bus Simulator\TouristBusSimu
O87 - FAEL: 'UDP Query User{D2A98534-FA00-48BE-9BB0-E91725EAE4E6}C:\program files\logitech gaming software\lcore.exe' [In-None-P17-TRUE] .(...) -- C:\
O87 - FAEL: 'TCP Query User{D28D077A-757F-4AD0-B514-BDCD77960818}C:\program files\logitech gaming software\lcore.exe' [In-None-P6-TRUE] .(...) -- C:\p
O87 - FAEL: '{D3CCC3F1-2503-4636-9C2D-E243636DF2AD}' [In-None-P6-TRUE] .(.AOMEI Tech Co., Ltd. - AOMEI Backupper Schedule task service.) -- C:\Program
O87 - FAEL: '{6306050A-F8A2-4A05-9A87-5F1F1D0B16C2}' [In-None-P17-TRUE] .(.AOMEI Tech Co., Ltd. - AOMEI Backupper Schedule task service.) -- C:\Progra
O87 - FAEL: 'TCP Query User{5C065518-68EA-4E23-BB83-6A88049921AA}C:\program files\windowsapps\spotifyab.spotifymusic_1.114.475.0_x86__zpdnekdrzrea0\sp
O87 - FAEL: 'UDP Query User{8640E25D-72DC-48E8-BF52-AF2F56380194}C:\program files\windowsapps\spotifyab.spotifymusic_1.114.475.0_x86__zpdnekdrzrea0\sp
O87 - FAEL: 'TCP Query User{B5B8D90F-BF6B-4483-A78D-074E64546B96}C:\program files (x86)\plex\plex media server\plex media server.exe' [In-None-P17-TRU
O87 - FAEL: 'TCP Query User{CBE89006-E1CA-408B-8D99-BE15F24EE7B6}C:\program files (x86)\plex\plex media server\plex dlna server.exe' [In-None-P6-TRUE]
O87 - FAEL: 'UDP Query User{1FEA72DE-31CC-4B0F-B53E-2B1EA9855C67}C:\program files (x86)\plex\plex media server\plex dlna server.exe' [In-None-P17-TRUE
O87 - FAEL: '{AD0C9D6F-D512-472D-A89B-91008C702918}' [In-None-P6-TRUE] .(.AOMEI Tech Co., Ltd. - AOMEI Backupper Schedule task service.) -- C:\Program
O87 - FAEL: '{67498C34-DB30-4F60-9246-39D2DB4D5AA3}' [In-None-P17-TRUE] .(.AOMEI Tech Co., Ltd. - AOMEI Backupper Schedule task service.) -- C:\Progra
O87 - FAEL: '{2930349B-A560-4A09-A062-0292A2038777}' [In-None-P6-TRUE] .(.Mozilla Corporation - Firefox.) -- C:\Program Files\Mozilla Firefox\firefox
O87 - FAEL: '{1740C05E-D259-4752-9886-89D9622DAE42}' [In-None-P17-TRUE] .(.Mozilla Corporation - Firefox.) -- C:\Program Files\Mozilla Firefox\firefox
O87 - FAEL: 'TCP Query User{020DE46E-27B6-41FE-B968-EF4B2BD78CC5}C:\users\couli\appdata\roaming\utorrent\utorrent.exe' [In-None-P6-TRUE] .(.BitTorrent
O87 - FAEL: 'UDP Query User{30978466-E117-4EF6-B45A-38196A9EA5AB}C:\users\couli\appdata\roaming\utorrent\utorrent.exe' [In-None-P17-TRUE] .(.BitTorrer
O87 - FAEL: '{6FDF5ED9-608E-4DD2-BDC1-40B60D84A589}' [In-None-P6-TRUE] .(.Valve Corporation - Steam Client Bootstrapper.) -- C:\Program Files (x86)\St
O87 - FAEL: '{FAA14265-2263-434F-A754-7928CE70AE47}' [In-None-P17-TRUE] .(.Valve Corporation - Steam Client Bootstrapper.) -- C:\Program Files (x86)\S
O87 - FAEL: '{E6F76C00-1C84-47DD-A88F-0383E1A3B673}' [In-None-P6-TRUE] .(.Valve Corporation - Steam Client WebHelper.) -- C:\Program Files (x86)\Steam
O87 - FAEL: '{59C59573-0CE6-4FE7-BDE8-C45B252D5300}' [In-None-P17-TRUE] .(.Valve Corporation - Steam Client WebHelper.) -- C:\Program Files (x86)\Stea
O87 - FAEL: '{C7A4B029-A590-4194-BCC7-00B2E85DE123}' [In-None-P6-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\Sniper Fury\mcfw.exe [Unsigned]  =>
O87 - FAEL: '{3C21EF69-55DE-4CD3-A0C6-8CD879C9DC6C}' [In-None-P17-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\Sniper Fury\mcfw.exe [Unsigned]  =>
O87 - FAEL: 'TCP Query User{0F9BD42B-6F4A-40DA-820D-C7684B7539C1}C:\program files (x86)\plex\plex media server\plex media server.exe' [In-None-P6-TRUE
O87 - FAEL: 'UDP Query User{AE633865-85D9-4225-825E-5E4BA0CADA0E}C:\program files (x86)\plex\plex media server\plex media server.exe' [In-None-P17-TRU
O87 - FAEL: '{0EA7CF86-35B0-46EF-8F38-9A596C394400}' [In-None-P6-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\House Flipper\HouseFlipper.exe [Unsi
O87 - FAEL: '{D3DCF70D-AD5E-4576-A8E9-C4F0C0525D2F}' [In-None-P17-TRUE] .(...) -- D:\SteamLibrary\steamapps\common\House Flipper\HouseFlipper.exe [Uns
O87 - FAEL: 'TCP Query User{18FCC423-0588-40F7-90A9-C3525C7F9012}C:\program files (x86)\brackets\node.exe' [In-None-P6-TRUE] .(.Node.js - Node.js: Ser
O87 - FAEL: 'UDP Query User{E49BA383-0F96-466A-AFE9-7033DD5753FF}C:\program files (x86)\brackets\node.exe' [In-None-P17-TRUE] .(.Node.js - Node.js: Se
O87 - FAEL: '{A4A16B50-F69C-478C-A1A0-AEF17984A780}' [In-None-P6-TRUE] .(.Konami Digital Entertainment Co., Ltd. - eFootball PES 2020.) -- D:\SteamLib
O87 - FAEL: '{F953B42F-227E-4995-9F71-E82F3E721A60}' [In-None-P17-TRUE] .(.Konami Digital Entertainment Co., Ltd. - eFootball PES 2020.) -- D:\SteamLi
O87 - FAEL: '{54CF6D8D-097D-448F-A3AE-AA25A7A46686}' [In-None-P6-TRUE] .(.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporati
O87 - FAEL: '{798FD3BB-F2EF-441D-9EEF-3CED991195E8}' [In-None-P17-TRUE] .(.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporat
O87 - FAEL: 'TCP Query User{537324C1-F497-47AD-91FE-AA54E41E5AEA}C:\program files\litecoin\litecoin-qt.exe' [In-None-P6-TRUE] .(...) -- C:\program fil
O87 - FAEL: 'UDP Query User{660ACD51-BD17-426D-98F0-B3FB53CF8794}C:\program files\litecoin\litecoin-qt.exe' [In-None-P17-TRUE] .(...) -- C:\program fi
O87 - FAEL: '{CF5F34CD-A1D4-40B2-9CDA-691A8D041166}' [In-None-P17-TRUE] .(.Apowersoft - ApowerCompress.) -- C:\Program Files (x86)\Apowersoft\ApowerCo
O87 - FAEL: '{043A9F29-74BD-4139-A00D-0A78C62E75E6}' [Out-None-P17-TRUE] .(.Apowersoft - ApowerCompress.) -- C:\Program Files (x86)\Apowersoft\ApowerC
O87 - FAEL: '{B5B7312A-E444-4FC4-A57B-F4BFE8161EE7}' [In-None-P17-TRUE] .(...) -- C:\Program Files\BlueStacks\HD-Player.exe [Unsigned] (.not file.)  =
O87 - FAEL: '{E261B0E0-934D-42AB-BE20-4F466ABB8A46}' [In-None-P17-TRUE] .(.Duodian Technology Co. Ltd. - NoxPlayer.) -- D:\Program Files\Nox\bin\Nox.e
O87 - FAEL: '{1F35318C-484F-427C-AC31-B21FA671979F}' [In-None-P17-TRUE] .(.BigNox Corporation - NoxVMHandle Frontend.) -- C:\Program Files (x86)\Bignc
O87 - FAEL: 'TCP Query User{DF26ADF5-B22E-4C47-B9D2-D77C64575541}C:\users\couli\appdata\local\programs\opera\68.0.3618.173\opera.exe' [In-None-P6-TRUE
O87 - FAEL: 'UDP Query User{6368AE51-3552-44BF-8902-EB88CE90F319}C:\users\couli\appdata\local\programs\opera\68.0.3618.173\opera.exe' [In-None-P17-TRU
O87 - FAEL: 'TCP Query User{FC8520BF-DA51-4EDB-9746-F01A36C3CBA1}C:\users\couli\appdata\local\programs\opera\69.0.3686.95\opera.exe' [In-None-P6-TRUE]
O87 - FAEL: 'UDP Query User{AD5E48D1-3870-4412-B2B8-11ABB173257C}C:\users\couli\appdata\local\programs\opera\69.0.3686.95\opera.exe' [In-None-P17-TRUE
O87 - FAEL: '{0B263922-BE32-4540-92A5-264F528AB3B9}' [In-None-P6-TRUE] .(.Electronic Arts - FIFA Launcher.) -- D:\Origin\FIFA 20\FIFASetup\fifaconfig
O87 - FAEL: '{21AE459E-4E71-4D06-9EDF-7C3AA3582F7F}' [In-None-P17-TRUE] .(.Electronic Arts - FIFA Launcher.) -- D:\Origin\FIFA 20\FIFASetup\fifaconfig
O87 - FAEL: 'TCP Query User{12874611-F23D-4E94-8FCD-BCFA15F366E3}I:\the sims 4\game\bin\ts4_x64.exe' [In-None-P6-TRUE] .(.Electronic Arts Inc. - The S
O87 - FAEL: 'UDP Query User{7148501D-4417-4B84-8CFC-AB1099F21973}I:\the sims 4\game\bin\ts4_x64.exe' [In-None-P17-TRUE] .(.Electronic Arts Inc. - The
O87 - FAEL: '{4197FC59-1327-4987-83B4-5A220A5B8489}' [In-None-P6-TRUE] .(.Bohemia Interactive - Arma 3 Launcher.) -- D:\SteamLibrary\steamapps\common\
O87 - FAEL: '{5D89A77B-B6C4-4976-AFB9-CFB561E4FB9D}' [In-None-P17-TRUE] .(.Bohemia Interactive - Arma 3 Launcher.) -- D:\SteamLibrary\steamapps\commor
O87 - FAEL: 'TCP Query User{9F3D76F8-0AB5-4AE0-9C30-F56F00FF8CD1}D:\steamlibrary\steamapps\common\arma 3\arma3_x64.exe' [In-None-P6-TRUE] .(.Bohemia I
O87 - FAEL: 'UDP Query User{D29FB3A5-FA9E-4CF6-B2B2-8DF7810C1DF5}D:\steamlibrary\steamapps\common\arma 3\arma3_x64.exe' [In-None-P17-TRUE] .(.Bohemia
O87 - FAEL: '{1B43AF52-3182-445A-892F-9ECAFACA2463}' [In-None-P17-TRUE] .(.Node.js - Node.js: Server-side JavaScript.) -- C:\Windows\Prey\versions\1.9
O87 - FAEL: 'TCP Query User{F170B5AA-2424-45A1-BA1A-985CC918064A}C:\users\couli\appdata\local\programs\opera\71.0.3770.198\opera.exe' [In-None-P6-TRUE
O87 - FAEL: 'UDP Query User{A0EC7CBC-261D-44E2-B152-18A5E786C9DD}C:\users\couli\appdata\local\programs\opera\71.0.3770.198\opera.exe' [In-None-P17-TRU
O87 - FAEL: 'TCP Query User{2941A9CE-0F9B-47B8-812B-D15D64AD9F37}C:\users\couli\downloads\anydesk.exe' [In-None-P6-TRUE] .(.philandro Software GmbH -
O87 - FAEL: 'UDP Query User{9B35C7FF-0EE0-4F78-A193-7D515178AA39}C:\users\couli\downloads\anydesk.exe' [In-None-P17-TRUE] .(.philandro Software GmbH -
O87 - FAEL: 'TCP Query User{CEB5E843-3B6F-4238-9BB5-A37616233055}C:\users\couli\appdata\local\programs\opera\71.0.3770.284\opera.exe' [In-None-P6-TRUE
O87 - FAEL: 'UDP Query User{1E377A99-E76B-4BC6-B740-D6D6D8A3C5A8}C:\users\couli\appdata\local\programs\opera\71.0.3770.284\opera.exe' [In-None-P17-TRU
O87 - FAEL: '{029EF670-FC7C-417C-A060-7C43597DB373}' [In-None-P17-TRUE] .(.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporat
O87 - FAEL: '{BD598ECA-B6EF-4015-B405-ABCFA6D790D5}' [In-None-P17-TRUE] .(.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporat
O87 - FAEL: '{2A058A07-F0AD-49AF-BDDE-3EF01DA602E4}' [In-None-P6-TRUE] .(.NVIDIA Corporation - NVIDIA Streamer Server Component.) -- C:\Program Files\
O87 - FAEL: '{9EBA18BA-C9D0-40BD-A719-3713A0DF570E}' [In-None-P17-TRUE] .(.NVIDIA Corporation - NVIDIA Streamer Server Component.) -- C:\Program Files
O87 - FAEL: '{6CC19022-D2C0-4549-9AE7-280F7C5FFED3}' [In-None-P6-TRUE] .(.Skype Technologies S.A. - Skype.) -- C:\Program Files\WindowsApps\Microsoft
O87 - FAEL: '{F2B3EE8A-D375-4F5B-ADBD-A631A91171FA}' [Out-None-P6-TRUE] .(.Skype Technologies S.A. - Skype.) -- C:\Program Files\WindowsApps\Microsoft
O87 - FAEL: '{25444584-ED18-4ADD-9AFF-6652A3DB0ACF}' [In-None-P17-TRUE] .(.Skype Technologies S.A. - Skype.) -- C:\Program Files\WindowsApps\Microsoft
O87 - FAEL: '{989FF1A3-DF31-4552-A01C-A88FB45F79EF}' [Out-None-P17-TRUE] .(.Skype Technologies S.A. - Skype.) -- C:\Program Files\WindowsApps\Microsof
O87 - FAEL: '{693C8D85-63A3-4CF0-B83E-4775F2519B6A}' [In-None-P6-TRUE] .(.SCS Software - Euro Truck Simulator 2 - Steam.) -- C:\Program Files (x86)\St
O87 - FAEL: '{AA765C7B-8506-4440-96CE-9E295EF809EA}' [In-None-P17-TRUE] .(.SCS Software - Euro Truck Simulator 2 - Steam.) -- C:\Program Files (x86)\S
O87 - FAEL: '{05E75E0C-050A-4699-99B7-DB45BEE70DC3}' [In-None-P6-TRUE] .(.SCS Software - Euro Truck Simulator 2 - Steam.) -- C:\Program Files (x86)\St
O87 - FAEL: '{35996494-C824-4BA4-B695-0E9D95232B8A}' [In-None-P17-TRUE] .(.SCS Software - Euro Truck Simulator 2 - Steam.) -- C:\Program Files (x86)\S
O87 - FAEL: '{3867E98C-907A-4415-A133-0F040C3CDACD}' [In-None-P6-TRUE] .(.Bohemia Interactive a.s. - Arma 3 Tools.) -- D:\SteamLibrary\steamapps\commo
O87 - FAEL: '{B9F69AF1-F96A-4388-AA86-8343B4DEF1F7}' [In-None-P17-TRUE] .(.Bohemia Interactive a.s. - Arma 3 Tools.) -- D:\SteamLibrary\steamapps\comm
O87 - FAEL: '{58F254DC-C179-4D45-A455-04B2B85711B9}' [In-None-P6-TRUE] .(.Bohemia Interactive a.s. - starter.) -- D:\SteamLibrary\steamapps\common\Arm
O87 - FAEL: '{DDEA5768-2616-4B15-84CD-BD25033EA01C}' [In-None-P17-TRUE] .(.Bohemia Interactive a.s. - starter.) -- D:\SteamLibrary\steamapps\common\Ar
O87 - FAEL: '{0CBE18FD-5AE4-4939-A68F-2D5EF8099073}' [In-None-P6-TRUE] .(.Bohemia Interactive - Addon Builder.) -- D:\SteamLibrary\steamapps\common\Ar
O87 - FAEL: '{074E1E16-32C8-4C54-82BA-6447C908D51E}' [In-None-P17-TRUE] .(.Bohemia Interactive - Addon Builder.) -- D:\SteamLibrary\steamapps\common\A
O87 - FAEL: '{6178CD61-06F3-4922-A808-482D226BE878}' [In-None-P6-TRUE] .(.Bohemia Interactive - Arma 3 Publisher.) -- D:\SteamLibrary\steamapps\commor
O87 - FAEL: '{3AFBD95A-E63D-4271-A893-68CCAE841BAE}' [In-None-P17-TRUE] .(.Bohemia Interactive - Arma 3 Publisher.) -- D:\SteamLibrary\steamapps\commo
O87 - FAEL: '{2BE56417-69DC-456C-A237-3644EF338CFF}' [In-None-P17-TRUE] .(.HP Inc - RemotePlay feature of the Omen Command Cent.) -- C:\Program Files\
O87 - FAEL: '{B38B3C64-B0FA-45D2-AA1D-75927B05476F}' [Out-None-P17-TRUE] .(.HP Inc - RemotePlay feature of the Omen Command Cent.) -- C:\Program Files
O87 - FAEL: '{C87457A0-8D25-42B4-B276-0FD5D46784A6}' [In-None-P6-TRUE] .(.HP Inc - RemotePlay feature of the Omen Command Cent.) -- C:\Program Files\W
O87 - FAEL: '{9AA324CF-8A35-4694-9EE7-36731E8F0621}' [Out-None-P6-TRUE] .(.HP Inc - RemotePlay feature of the Omen Command Cent.) -- C:\Program Files\
O87 - FAEL: '{60485BC1-25DB-437A-A0B3-0D8D968E10C2}' [In-None-P6-TRUE] .(.HP Inc. - HP.Omen.OmenCommandCenter.) -- C:\Program Files\WindowsApps\AD2F18
O87 - FAEL: '{FE1C7809-2FB6-47AF-B179-4B03E9617565}' [Out-None-P6-TRUE] .(.HP Inc. - HP.Omen.OmenCommandCenter.) -- C:\Program Files\WindowsApps\AD2F1
O87 - FAEL: '{7BF05CFB-FB37-4585-AD0C-1B932CFFEEA8}' [In-None-P6-TRUE] .(.HP Inc. - HP.Omen.OmenCommandCenter.) -- C:\Program Files\WindowsApps\AD2F18
O87 - FAEL: '{272B9C38-22CB-4737-B0DD-6CF5F3ED0FB4}' [In-None-P6-TRUE] .(.HP Inc. - HP.Omen.OmenCommandCenter.) -- C:\Program Files\WindowsApps\AD2F18
O87 - FAEL: '{E5402B38-572E-4FBC-9CED-0AC6ACA2B392}' [In-None-P6-TRUE] .(.HP Inc. - HP.Omen.OmenCommandCenter.) -- C:\Program Files\WindowsApps\AD2F18
O87 - FAEL: '{84992369-388B-41C5-91EC-849D51F3A343}' [In-None-P6-TRUE] .(.HP Inc. - HP.Omen.OmenCommandCenter.) -- C:\Program Files\WindowsApps\AD2F18
O87 - FAEL: '{131D53DF-43E8-487B-BA98-8F26B71BC7B6}' [In-None-P6-TRUE] .(.HP Inc. - HP.Omen.OmenCommandCenter.) -- C:\Program Files\WindowsApps\AD2F18
O87 - FAEL: '{3410127A-20EA-4825-813A-51AB9A28A494}' [In-None-P17-TRUE] .(.HP Inc. - HP.Omen.OmenCommandCenter.) -- C:\Program Files\WindowsApps\AD2F1
O87 - FAEL: '{97616C5E-A63B-4FCE-BB45-886820606 77E}' [Out-None-P17-TRUE] .(.HP Inc. - HP.Omen.OmenCommandCenter.) -- C:\Program Files\WindowsApps\AD2F
O87 - FAEL: '{2A9F3CB5-FDCD-47C7-9D80-14FCDB03102B}' [In-None-P17-TRUE] .(.HP Inc. - OMEN Command Center Background.) -- C:\Program Files\WindowsApps\
O87 - FAEL: '{63537750-12D2-41F2-B39D-0D55E08348E2}' [Out-None-P17-TRUE] .(.HP Inc. - OMEN Command Center Background.) -- C:\Program Files\WindowsApps
O87 - FAEL: '{5329DD34-2580-4928-8919-A6578061 5903}' [In-None-P6-TRUE] .(.Spotify Ltd - Spotify.) -- C:\Program Files\WindowsApps\SpotifyAB.SpotifyMus
O87 - FAEL: '{EA7AD1CD-8715-48F1-A5C4-CD49A2055A03}' [In-None-P6-TRUE] .(.Spotify Ltd - Spotify.) -- C:\Program Files\WindowsApps\SpotifyAB.SpotifyMus
O87 - FAEL: '{176BF005-2DA9-48B8-886A-AF8A2C81B671}' [In-None-P6-TRUE] .(.Spotify Ltd - Spotify.) -- C:\Program Files\WindowsApps\SpotifyAB.SpotifyMus
O87 - FAEL: '{89C8AF5C-1F88-40C9-B268-5B89B3731526}' [In-None-P17-TRUE] .(.Spotify Ltd - Spotify.) -- C:\Program Files\WindowsApps\SpotifyAB.SpotifyMu
O87 - FAEL: '{D8FB463F-90EC-4D6E-BFC9-07AA6733E5DD}' [In-None-P17-TRUE] .(.Spotify Ltd - Spotify.) -- C:\Program Files\WindowsApps\SpotifyAB.SpotifyMu
O87 - FAEL: '{E95B318B-ED9A-45EA-BE7C-7FAC1A1D839C}' [In-None-P6-TRUE] .(.Spotify Ltd - Spotify.) -- C:\Program Files\WindowsApps\SpotifyAB.SpotifyMus
O87 - FAEL: '{FDFCF629-C42A-4E78-B43D-E988FEBB6BA6}' [Out-None-P6-TRUE] .(.Spotify Ltd - Spotify.) -- C:\Program Files\WindowsApps\SpotifyAB.SpotifyMu
O87 - FAEL: '{44B8F9D3-60DC-41C8-B85A-80459E0640FD}' [Out-None-P17-TRUE] .(.Spotify Ltd - Spotify.) -- C:\Program Files\WindowsApps\SpotifyAB.SpotifyM
```

```
O87 - FAEL: 'TCP Query User{51D76C08-E6E2-4891-A61B-1EC90863BF71}C:\users\couli\appdata\local\programs\opera\72.0.3815.400\opera.exe' [In-None-P6-TRUE
O87 - FAEL: 'UDP Query User{9D175C55-01D9-4EEF-A69A-5296CFE4852C}C:\users\couli\appdata\local\programs\opera\72.0.3815.400\opera.exe' [In-None-P17-TRU
O87 - FAEL: '{D45CF639-294D-49E7-9166-A35E79795138}' [In-None-P17-TRUE] .(.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox
O87 - FAEL: '{82D1A4BF-E214-47E2-A2AA-3E28A237516D}' [In-None-P17-TRUE] .(.Google LLC - Google Chrome.) -- C:\Program Files\Google\Chrome\Application\

---\ CODES PRODUITS LOGICIELS (95) - 2s
O90 - PUC: '05385A3499BCE4F4B96B0F857D2B9758' [HKLM] . (.Intel XTU SDK.)
O90 - PUC: '099AAB46CF1F54147A1B4EF1BB9CAD74' [HKLM] . (.HP Recovery Manager.) -- c:\windows\Installer\{64BAA990-F1FC-4145-A7B1-E41FBBC9DA47}\_853F67D
O90 - PUC: '0A1C1677828D8BC4F8C3D9B99573ECBC' [HKLM] . (.WeMod Version Guard.)
O90 - PUC: '0BB8AA89A0C0A114BB342156AC671955' [HKLM] . (.HP ePrint SW.)  =>.Hewlett-Packard
O90 - PUC: '1007C6B46D7C017319E3B52CF3EC196E' [HKLM] . (.Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148.)  =>.bl.org
O90 - PUC: '121E2D80A6F7BE3479DF26B944094330' [HKLM] . (.Microsoft_VC90_CRT_x86.) -- C:\WINDOWS\Installer\{08D2E121-7F6A-43EB-97FD-629B44903403}\ARPPF
O90 - PUC: '12B8D03ED28D112328CCF0A0D541598E' [HKLM] . (.Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.40660.)  =>.Microsoft Corporation
O90 - PUC: '1658D52E05A536348B4D0926F791BABD' [HKLM] . (.APK Easy Tool.) -- C:\WINDOWS\Installer\{E25D8561-5A50-4363-B8D4-90627F19ABDB}\_853F67D554F05
O90 - PUC: '1735B7212081DDE42AA54AB37F163D38' [HKLM] . (.PBO Manager v.1.4 beta.)  =>.WINSE
O90 - PUC: '1926E8D15D0BCE53481466615F760A7F' [HKLM] . (.Microsoft Visual C++ 2010  x64 Redistributable - 10.0.40219.)  =>.bl.org
O90 - PUC: '1af2a8da7e60d0b429d7e6453b3d0182' [HKLM] . (.Microsoft Visual C++ 2005 Redistributable (x64).)  =>.bl.org
O90 - PUC: '1D5E3C0FEDA1E123187686FED06E995A' [HKLM] . (.Microsoft Visual C++ 2010  x86 Redistributable - 10.0.40219.)  =>.bl.org
O90 - PUC: '272850750B29AFE4F8DDDEE3D586D973' [HKLM] . (.HP System Event Utility.) -- C:\WINDOWS\Installer\{57058272-92B0-4EFA-8FDD-ED3E5D689D37}\_853
O90 - PUC: '30DD1C25E4016CA4D96C125D5827E11D' [HKLM] . (.UpdateAssistant.)  =>.Corel Corporation
O90 - PUC: '318D08345E93DF64CA32CFA9A1B889AA' [HKLM] . (.HP JumpStart Launch.) -- C:\windows\Installer\{4380D813-39E5-46FD-AC23-FC9A1A8B98AA}\HPlogo_b
O90 - PUC: '381F9A43110154848962BFAA35AD95FD' [HKLM] . (.Quran Explorer Desktop.)
O90 - PUC: '3D42ADBF91A157D43B1F2F1ABFB616FB' [HKLM] . (.Intel(R) Management Engine Components.)  =>.Intel Corporation
O90 - PUC: '40AB8768161DEB54CA4ACCD53170F353' [HKLM] . (.Microsoft Visual C++ 2019 X64 Additional Runtime - 14.24.28127.)  =>.Microsoft Corporation
O90 - PUC: '4135AF478C58A2E409D79DCECC7B077A' [HKLM] . (.Smart Switch.) -- C:\WINDOWS\Installer\{74FA5314-85C8-4E2A-907D-D9ECCCB770A7}\ARPPRODUCTICON
O90 - PUC: '4324AED8D79CEB142BCB13A391B6DC90' [HKLM] . (.Intel(R) Management Engine Driver.)  =>.Intel Corporation
O90 - PUC: '436F6625D7B77354DBCD89DDC6CFAB1A' [HKLM] . (.Online Application.) -- C:\WINDOWS\Installer\{5266F634-7B7D-4537-BDDC-98DD6CFCBAA1}\online.ex
O90 - PUC: '44DB0475D85BA123FA0CD6D35465DDC6' [HKLM] . (.Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.40660.)  =>.Microsoft Corporation
O90 - PUC: '494A8E7F6B796874E9C24AA2804238BE' [HKLM] . (.HP ePrint SW.)  =>.Hewlett-Packard
O90 - PUC: '4BB570A2679E8724FBF35E6C49D5480C' [HKLM] . (.bl.) -- C:\WINDOWS\Installer\{2A075BB4-E976-4278-BF3F-E5C6945D84C0}\ARPPRODUCTICON.exe  =>.bl
O90 - PUC: '4D1415A3BD742034B9C172B25E58CBA8' [HKLM] . (.HP Audio Switch.) -- C:\WINDOWS\Installer\{3A5141D4-47DB-4302-9B1C-272BE585BC8A}\HPlogo_blue
O90 - PUC: '4D8E668DD6F0D844AB111DA28131BBC1' [HKLM] . (.APK Editor Studio.) -- C:\WINDOWS\Installer\{D866E8D4-0F6D-448D-BA11-D12A1813BB1C}\Icon
O90 - PUC: '4EA42A62D9304AC4784BF2238110180F' [HKLM] . (.Java 8 Update 181.) -- C:\Program Files (x86)\Java\jre1.8.0_181\\bin\javaws.exe  =>.Sun Micro
O90 - PUC: '4EA42A62D9304AC4784BF2238120100F' [HKLM] . (.Java 8 Update 201.) -- C:\Program Files (x86)\Java\jre1.8.0_201\\bin\javaws.exe  =>.Sun Micro
O90 - PUC: '4EA42A62D9304AC4784BF2238120110F' [HKLM] . (.Java 8 Update 211.) -- C:\Program Files (x86)\Java\jre1.8.0_211\\bin\javaws.exe  =>.Sun Micro
O90 - PUC: '4EA42A62D9304AC4784BF2468120110F' [HKLM] . (.Java 8 Update 211 (64-bit).) -- C:\Program Files\Java\jre1.8.0_211\\bin\javaws.exe  =>.Sun Mi
O90 - PUC: '505FCD9B97A54BC44804828B7989BABA' [HKLM] . (.Microsoft Web Deploy 4.0.) -- C:\WINDOWS\Installer\{B9DCF505-5A79-4CB4-8440-28B89798ABAB}\MSD
O90 - PUC: '514D163353AB34143B10669119AB2691' [HKLM] . (.MyEpson Portal.)  =>.Epson/Seico
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: '57C71FD27269312468217159E5297F28' [HKLM] . (.Intel® Software Guard Extensions Platform Software.) -- C:\windows\Installer\{2DF17C75-9627-4
O90 - PUC: '595A0279D2D3E0445932B0F6797054DD' [HKLM] . (.HP Customer Experience Enhancements.) -- C:\windows\Installer\{9720A595-3D2D-440E-9523-0B6F97
O90 - PUC: '5979F581366931F4E99F03A782A2BDA5' [HKLM] . (.ph.) -- C:\WINDOWS\Installer\{185F9795-9663-4F13-9EF9-307A282ADB5A}\ARPPRODUCTICON.exe
O90 - PUC: '5A1A9B9E893699C4F8ED0197F456505C' [HKLM] . (.Intel(R) ME UninstallLegacy.)  =>.Intel Corporation
O90 - PUC: '5A812990327ACD34D85B163756A6E149' [HKLM] . (.Dropbox Update Helper.)  =>.WINSE
O90 - PUC: '5D44BBB50CC34344AAC085389B574EE5' [HKLM] . (.HP ePrint SW.)  =>.Hewlett-Packard
O90 - PUC: '617B899B10049194AB09AB415BD1EF5B' [HKLM] . (.paint.net.) -- C:\WINDOWS\Installer\{B998B716-4001-4919-BA90-BA14B51DFEB5}\_853F67D554F054494
O90 - PUC: '67D6ECF5CD5FBA732B8B22BAC8DE1B4D' [HKLM] . (.Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161.)  =>.bl.org
O90 - PUC: '68AB67CA4080330191959008142933911' [HKLM] . (.Adobe Refresh Manager.) -- C:\WINDOWS\Installer\{AC76BA86-0804-1033-1959-001824399311}\ARPPRO
O90 - PUC: '68AB67CA7DA76301B744CAF070E41400' [HKLM] . (.Adobe Acrobat Reader DC - Français.) -- C:\WINDOWS\Installer\{AC76BA86-7AD7-1036-7B44-AC0F074
O90 - PUC: '6E815EB96CCE9A53884E7857C57002F0' [HKLM] . (.Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161.)  =>.bl.org
O90 - PUC: '70237CAEDB4731B4AAFCC8E057F14A8E' [HKLM] . (.Microsoft Visual C++ 2019 X86 Additional Runtime - 14.24.28127.)  =>.Microsoft Corporation
O90 - PUC: '7C9F8B73BF3035237818527 19CD9C700' [HKLM] . (.Microsoft Visual C++ 2012 x64 Additional Runtime - 11.0.61030.)  =>.Microsoft Corporation
O90 - PUC: '818D4886E0E948946AAC1B7775CD8BAF' [HKLM] . (.HP ePrint SW.)  =>.Hewlett-Packard
O90 - PUC: '8214CD9298FC9D945A424B34F030F641' [HKLM] . (.DriversCloud.com (64 bits).) -- C:\WINDOWS\Installer\{29DC4128-CF89-49D9-A524-B4430F036F14}\m
O90 - PUC: '83EE58D24DB93384BA10427619B67BEA' [HKLM] . (.Lecture à distance PS4.) -- C:\windows\Installer\{2D85EE38-9BD4-4833-AB01-2467916BB7AE}\Remot
O90 - PUC: '84622BC58F53CB14C953E114EFE6215A' [HKLM] . (.Energy Star.) -- c:\windows\Installer\{5CB22648-35F8-41BC-9C35-1E41FE6E12A5}\_853F67D554F0544
O90 - PUC: '849C9882200F299418F5BD0EFA5BCDE6' [HKLM] . (.HP ePrint SW.)  =>.Hewlett-Packard
O90 - PUC: '8520DAD7C5154DD39846DB1714990E7F' [HKLM] . (.Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.40660.)  =>.Microsoft Corporation
O90 - PUC: '8B783CD72A6EC084E89F6A5EA18EC191' [HKLM] . (.Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.24.28127.)  =>.Microsoft Corporation
O90 - PUC: '8BFDDD6597F70844985D521E5FA22BF8' [HKLM] . (.Bonjour.) -- C:\WINDOWS\Installer\{56DDDFB8-7F79-4480-89D5-25E1F52AB28F}\Bonjour.ico  =>.Micr
O90 - PUC: '91785D291CBB3CC40AB8659C8E48CCC2' [HKLM] . (.Microsoft_VC80_CRT_x86.) -- C:\WINDOWS\Installer\{92D58719-BBC1-4CC3-A08B-56C9E884CC2C}\ARPPF
O90 - PUC: '9363D3D42313E5F448D01C283E5E9C10' [HKLM] . (.Oracle VM VirtualBox 6.0.2.) -- C:\WINDOWS\Installer\{4D3D3639-3132-4F5E-840D-C182E3E5C901}\I
O90 - PUC: '96F071321C0410729100000010000000' [HKLM] . (.7-Zip 19.00.)  =>.Igor Pavlov
O90 - PUC: '9F54CE9FA470FB84299E8AACDD656F39' [HKLM] . (.UE4 Prerequisites (x64).) -- C:\WINDOWS\Installer\{F9EC45F9-074A-48BF-92E9-A8CADD56F693}\Setu
O90 - PUC: 'A089CE062ADB6BC44A720BA745894BAC' [HKLM] . (.Google Update Helper.)  =>.Google Inc.
O90 - PUC: 'AC9690024114355438D224685CCABB89' [HKLM] . (.Microsoft VC++ redistributables repacked..)  =>.bl.org
O90 - PUC: 'ADB58102693D39C4597CCE0DBF93F77F' [HKLM] . (.HP ePrint SW.)  =>.Hewlett-Packard
O90 - PUC: 'B03AE1D9BF629DF4EB7390727E6E3F51' [HKLM] . (.Jarvee.)
O90 - PUC: 'B7F4E2DB0B037A64E8C59DD9125C3263' [HKLM] . (.Microsoft VC++ redistributables repacked..)  =>.bl.org
O90 - PUC: 'B996CAF6299726C48993743865C4EADD' [HKLM] . (.Intel(R) Chipset Device Software.)  =>.Intel Corporation
O90 - PUC: 'BBD52947705BB3A42A061EB928FF7EBF' [HKLM] . (.Brackets.) -- C:\WINDOWS\Installer\{74925DBB-B507-4A3B-A260-E19B82FFE7FB}\appicon.ico  =>.Ama
O90 - PUC: 'C025571B2A687A53689168CD7369889B' [HKLM] . (.Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.61030.)  =>.Microsoft Corporation
O90 - PUC: 'c1c4f01781cc94c4c8fb1542c0981a2a' [HKLM] . (.Microsoft Visual C++ 2005 Redistributable.)  =>.bl.org
O90 - PUC: 'C2E457E1B3FCBC243BD65D06EC9A1694' [HKLM] . (.Dell Mobile Connect Drivers.) -- C:\WINDOWS\Installer\{1E754E2C-CF3B-42CB-B36D-D560CEA96149}\
O90 - PUC: 'C3AEB2FCAE628F23AAB933F1E743AB79' [HKLM] . (.Microsoft Visual C++ 2012 x64 Minimum Runtime - 11.0.61030.)  =>.Microsoft Corporation
O90 - PUC: 'CBA3D42957CF2404D9BDBF48A65448D8' [HKLM] . (.HP PC Hardware Diagnostics UEFI.) -- C:\windows\Installer\{924D3ABC-FC75-4042-9DDB-FB846A4584
O90 - PUC: 'CE6380BC270BD863282B3D74B09F7570' [HKLM] . (.Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.40660.)  =>.Microsoft Corporation
O90 - PUC: 'CFD2C1F142D260E3CB8B271543DA9F98' [HKLM] . (.Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148.)  =>.bl.org
O90 - PUC: 'D1548D486DE295A3BA5AA244F7C73601' [HKLM] . (.Dropbox 25 GB.) -- C:\windows\Installer\{84D8451D-2ED6-3A59-ABA5-2A447F7C6310}\DropboxOEM.exe
O90 - PUC: 'D2033657B6DB3514ABD7E343237E2CD2' [HKLM] . (.Intel® Hardware Accelerated Execution Manager.) -- C:\WINDOWS\Installer\{7563302D-BD6B-4153-B
O90 - PUC: 'D20352A90C039D93DBF6126ECE614057' [HKLM] . (.Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17.)  =>.bl.org
O90 - PUC: 'D30CF9A3586C138449FCE4FD3D474979' [HKLM] . (.Microsoft SQL Server Compact 3.5 SP2 ENU.) -- C:\WINDOWS\Installer\{3A9FC03D-C685-4831-94CF-4
O90 - PUC: 'D69E06D047B05A55CA5AF07668DF2F65' [HKLM] . (.Java(TM) SE Development Kit 12.0.1 (64-bit).) -- C:\Program Files\Java\jdk-12.0.1\\bin\java.e
O90 - PUC: 'DA93DA4DE19033D4BBB2956FCF8BDA3C' [HKLM] . (.Microsoft SQL Server Compact 3.5 SP2 x64 ENU.) -- C:\WINDOWS\Installer\{D4AD39AD-091E-4D33-BE
O90 - PUC: 'DC8A59DBF9D1DA5389A1E3975220E6BB' [HKLM] . (.Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.61030.)  =>.Microsoft Corporation
O90 - PUC: 'DDEEE13417D69624F8F738C6AF6FA971' [HKLM] . (.VMware Workstation.)  =>.VMware
O90 - PUC: 'E128CD23D7A48784EB8E33F71A357D2F' [HKLM] . (.Update for Windows 10 for x64-based Systems (KB4023057).)  =>.Microsoft Corporation
O90 - PUC: 'E3BF68035ABCEFD4AB6B3E1429CE4F65' [HKLM] . (.Prey Anti-Theft.)
O90 - PUC: 'E60F1ECA37BDB944DAFE9CF4C468589A' [HKLM] . (.IIS 10.0 Express.) -- C:\WINDOWS\Installer\{ACE1F06E-DB73-449B-ADEF-C94F4C8685A9}\Icon_IisExp
O90 - PUC: 'EFEE0228DC83E77358593193D847A0EC' [HKLM] . (.Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.17.)  =>.bl.org
O90 - PUC: 'F19E0E8A8EFC92C44B9A27C3BA386457' [HKLM] . (.Intel(R) Rapid Storage Technology.)  =>.Intel Corporation
O90 - PUC: 'F1AF27E2BDAB73348BEA7F1CE75CD7D1' [HKLM] . (.Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.24.28127.)  =>.Microsoft Corporation
O90 - PUC: 'F26335665639C3A4B98F17945492ED60' [HKLM] . (.Epic Games Launcher.) -- C:\WINDOWS\Installer\{6653362F-9365-4A3C-9BF8-71494529DE06}\Installe
O90 - PUC: 'F60730A4A66673047777F5728467D401' [HKLM] . (.Java Auto Updater.)  =>.Sun Microsystems
O90 - PUC: 'F6A6D7E1B82E7504DBF499981C5F53D3' [HKLM] . (.HP JumpStart Bridge.) -- C:\windows\Installer\{1E7D6A6F-E28B-4057-BD4F-9989C1F5353D}\HPlogo_b
O90 - PUC: 'FBE19209A781E7C49ADACDBCC6495663' [HKLM] . (.Intel(R) Management Engine Components.)  =>.Intel Corporation
O90 - PUC: '5B3868F56505C1148B802B982EE9B9BB' [HKCU] . (.Outil de téléchargement USB/DVD Windows 7.)
O90 - PUC: '7912700F6FCFFB14D98338B2419522CD' [HKCU] . (.Paradox Launcher v2.) -- %APPDATA%\Microsoft\Installer\{F0072197-FCF6-41BF-9D38-832B145922DC}
O90 - PUC: '5B3868F56505C1148B802B982EE9B9BB' [HKU] . (.Outil de téléchargement USB/DVD Windows 7.)
O90 - PUC: '7912700F6FCFFB14D98338B2419522CD' [HKU] . (.Paradox Launcher v2.) -- %APPDATA%\Microsoft\Installer\{F0072197-FCF6-41BF-9D38-832B145922DC}\

---\ PACKAGES WINDOWS INSTALLER (74) - 12s
[MD5.70235242FE09F640D7ED0A813A36CC42] [WIS][2012/07/26 17:57:32] (.SEIKO EPSON CORPORATION - MyEpson Portal Setup.) -- C:\WINDOWS\Installer\1414c7ec
```

```
[MD5.51BA383AACF996B14E313B4B9C08C0B0] [WIS][2019/12/26 15:42:00] (.Intel Corporation - Intel® Hardware Accelerated Execution Manag.) -- C:\WINDOWS\Ir
[MD5.E4AF16B0574B2598AADD353A35A3722B] [WIS][2012/04/15 03:34:36] (.Adobe.) -- C:\WINDOWS\Installer\16497ee.msi   [2211328]  =>.Adobe
[MD5.78B41A323699DAF1C25265890733BE26] [WIS][2012/04/15 03:34:36] (.Adobe.) -- C:\WINDOWS\Installer\16497f6.msi   [1997312]  =>.Adobe
[MD5.196C1593D5125203D8A7E874DBFA3176] [WIS][2012/04/15 03:34:36] (.InstallShield.) -- C:\WINDOWS\Installer\1649824.msi   [593408]  =>.InstallShield
[MD5.108C5BD11E8A89108594525A03ADB716] [WIS][2012/04/15 03:34:38] (.InstallShield.) -- C:\WINDOWS\Installer\164982c.msi   [1436672]  =>.InstallShield
[MD5.D3E5D958F1971A2E89DA564D1752AF89] [WIS][2019/07/08 21:22:49] (.HP Inc. - HP Audio Switch.) -- C:\WINDOWS\Installer\182580b.msi  [2396160]  =>.HP
[MD5.64865E9386EE3B24A8231837C6A8F36E] [WIS][2019/03/25 21:36:54] (.Prey, Inc. - Prey Anti-Theft.) -- C:\WINDOWS\Installer\192bff8.msi  [25112576]  =>
[MD5.4BE455D72E738C0F7DD8840FB3484522] [WIS][2020/05/05 00:52:54] (.brackets.io - Brackets.) -- C:\WINDOWS\Installer\1a61a309.msi  [80896000]  =>.brac
[MD5.BED4F5058624589D002AFC8D306D1D9B] [WIS][2019/03/13 17:14:49] (.Igor Pavlov - 7-Zip Package.) -- C:\WINDOWS\Installer\1ac6b7.msi  [1369600]  =>.Ig
[MD5.74082EB88C49A2A04F11488A02D90679] [WIS][2019/03/13 17:15:03] (.Oracle Corporation - Java SE Runtime Environment 8 Update 201.) -- C:\WINDOWS\Inst
[MD5.B6FD320476DB923C342A88A1C3B2192E] [WIS][2017/01/03 21:10:14] (.Intel Corporation - Intel(R) Chipset Device Software.) -- C:\WINDOWS\Installer\1bc
[MD5.0BB59749B49DB6A921C709C3C935A22E] [WIS][2017/03/06 11:44:10] (.Intel Corporation - Intel(R) ME UninstallLegacy.) -- C:\WINDOWS\Installer\1bc91.ms
[MD5.BBB96DAD28092A1A807D7FC30E42CBC1] [WIS][2016/12/22 05:55:48] (.Intel Corporation - Intel® Software Guard Extensions Platform S.) -- C:\WINDOWS\Ir
[MD5.AA07034DCF0CA3C4D7DA4882465F62F5] [WIS][2020/12/03 01:29:38] (.Google LLC - Google Update Helper.) -- C:\WINDOWS\Installer\1e7479.msi  [40960]  =
[MD5.A6B96516D619D33C470E3CA09F0EF1C5] [WIS][2019/01/19 05:00:39] (.VMware, Inc. - VMware Workstation.) -- C:\WINDOWS\Installer\217e776.msi  [50522112
[MD5.54A89CB50BA56622791537978F433BF1] [WIS][2019/06/09 00:17:05] (.WeMod - WeMod Version Guard.) -- C:\WINDOWS\Installer\219e2d1.msi  [4919296]  =>.W
[MD5.8455DE183203CAC17B2AB05C91D99D2B] [WIS][2012/06/28 19:21:38] (.Nikita 'WINSE' Kobzev.) -- C:\WINDOWS\Installer\21af93fe.msi   [3546624]
[MD5.B52F41878CF146EE3864FED671675513] [WIS][2019/06/19 02:02:55] (.Oracle Corporation - Java(TM) SE Development Kit 12.0.1 (64-bit).) -- C:\WINDOWS\I
[MD5.BAB85911E99F454B8231466E33969F7C] [WIS][2017/11/02 12:18:13] (.Microleaves - Online Application.) -- C:\WINDOWS\Installer\2c5b1ca.msi  [2806272]
[MD5.DF1F244B129A8F1CE5108C87FDF6E1F1] [WIS][2019/03/18 22:10:52] (.dotPDN LLC.) -- C:\WINDOWS\Installer\34a776.msi   [36268544]  =>.dotPDN LLC
[MD5.C608FCA2D224F12968F793AFB35D0E4F] [WIS][2020/11/03 02:52:50] (.Dropbox, Inc. - Dropbox Update Helper.) -- C:\WINDOWS\Installer\34f98c6.msi  [2457
[MD5.D85D050D3D4E00D3413FCD52C19BB58A] [WIS][2020/03/03 15:38:14] (.Jarvee - Jarvee.) -- C:\WINDOWS\Installer\36c11b28.msi  [144118784]
[MD5.437B37DF0CF73F5146349FB1201D6F6C] [WIS][2020/05/10 21:42:34] (.Alexander Gorishnyak - APK Editor Studio.) -- C:\WINDOWS\Installer\389955a4.msi
[MD5.4894A62FE5FD50E1BD20C8B32D6180A1] [WIS][2019/05/11 16:55:39] (.evildog1.) -- C:\WINDOWS\Installer\3e4635.msi   [22525440]
[MD5.5361F48C9C2192F744A738CC365DB67A] [WIS][2019/06/28 16:20:49] (.Samsung Electronics Co., Ltd..) -- C:\WINDOWS\Installer\439509.msi   [38800896]  =
[MD5.E3DCC677F55212145A01AB5FC2D5E69E] [WIS][2020/01/30 21:13:19] (.Epic Games, Inc. - Epic Games Launcher.) -- C:\WINDOWS\Installer\46cb697.msi  [437
[MD5.E22AE5C548B39D554B643EBA58FDC3AD] [WIS][2018/03/15 15:06:08] (.Intel Corporation - Intel(R) Management Engine Driver.) -- C:\WINDOWS\Installer\4a
[MD5.CF91CA8448E27B27E612034555CB1DBE] [WIS][2018/03/15 15:04:48] (.Intel Corporation - Intel(R) Management Engine Components.) -- C:\WINDOWS\Installe
[MD5.FE90C64EA7AE9634E7E70DF2C77DEF19] [WIS][2018/03/15 15:05:14] (.Intel Corporation - Microsoft VC++ redistributables repacked..) -- C:\WINDOWS\Inst
[MD5.A44B304D91D159CAB0F5C64631CA75C2] [WIS][2018/03/15 15:05:22] (.Intel Corporation - Microsoft VC++ redistributables repacked..) -- C:\WINDOWS\Inst
[MD5.8E25F5E1D396FAD09F9567698FD1D71F] [WIS][2018/03/15 15:05:52] (.Intel Corporation - Intel(R) Management Engine Components.) -- C:\WINDOWS\Installe
[MD5.DAF1C0F27B49EADDA9508679169668C8] [WIS][2018/03/02 11:37:34] (.Intel Corporation - Intel(R) Trusted Connect Service Client x64.) -- C:\WINDOWS\Ir
[MD5.DCA638460F442142B0C11870328E5440] [WIS][2018/03/02 11:30:50] (.Intel Corporation - Intel(R) Trusted Connect Service Client x86.) -- C:\WINDOWS\Ir
[MD5.33849E896416335E9F90BAB6979FCC08] [WIS][2017/12/14 11:55:00] (.Cybelsoft - Hardware Detection DriversCloud.com.) -- C:\WINDOWS\Installer\4c5d0.ms
[MD5.1504667BA3C10D841C0B76B6412FAFB5] [WIS][2015/03/17 09:41:29] (.Adobe Systems Incorporated.) -- C:\WINDOWS\Installer\5ce873.msi   [2805760]  =>.Ad
[MD5.5DAF9ED90DF8CD3249F5B088AF8540DA] [WIS][2017/02/02 23:18:10] (.HP Inc..) -- C:\WINDOWS\Installer\6576.msi   [1717248]  =>.HP Inc.
[MD5.55EB54A2CDA4A5268F220EC6DB1B526B] [WIS][2017/04/02 01:03:28] (.HP.) -- C:\WINDOWS\Installer\6583.msi   [4495872]  =>.HP
[MD5.FE8D4E3A786A9934EDCCB9B36C06F24A] [WIS][2018/02/27 03:50:11] (.Sony Interactive Entertainment Inc. - PS4 Remote Play.) -- C:\WINDOWS\Installer\6c
[MD5.8A6CF86064D498F1B698A7BCE527ABDD] [WIS][2011/07/15 11:11:04] (.Faisal Jameel.) -- C:\WINDOWS\Installer\72a11c.msi   [24851456]
[MD5.6AA07BDB0520FBB3D69D0EC8F3EF2171] [WIS][2019/06/29 10:48:15] (.Screenovate Technologies Ltd. - Virtoo Drivers.) -- C:\WINDOWS\Installer\7436de.ms
[MD5.613165B952AB31F900C66009E080F168] [WIS][2017/08/02 01:51:46] (.HP Inc..) -- C:\WINDOWS\Installer\7b56.msi   [736256]  =>.HP Inc.
[MD5.94D1A734DD7EA7AE700CF4EFC50C8D7C] [WIS][2017/03/15 02:32:08] (.HP Inc. - HP ePrint SW.) -- C:\WINDOWS\Installer\7b5b.msi  [1007616]  =>.HP Inc.
[MD5.925540D56DF3D97116A6D2350A3310A4] [WIS][2017/03/15 02:33:20] (.HP Inc. - HP ePrint SW.) -- C:\WINDOWS\Installer\7b60.msi  [348160]  =>.HP Inc.
[MD5.C8EFE4AF6D3D7B808D5F859E25AE5E3F] [WIS][2017/03/15 02:26:32] (.HP Inc. - HP ePrint SW.) -- C:\WINDOWS\Installer\7b6a.msi  [19410944]  =>.HP Inc.
[MD5.7FB856E6D2BAB8701EF64BA8673778DF] [WIS][2017/03/15 02:28:58] (.HP Inc. - HP ePrint SW.) -- C:\WINDOWS\Installer\7b6f.msi  [655360]  =>.HP Inc.
[MD5.D0811A62D14AB3AE4B7DFEBDEDDFE150] [WIS][2017/03/15 02:30:10] (.HP Inc. - HP ePrint SW.) -- C:\WINDOWS\Installer\7b74.msi  [1089536]  =>.HP Inc.
[MD5.50021AD28C17B5EBC8EBB19C6D2C0C1D] [WIS][2017/03/15 02:27:48] (.HP Inc. - HP ePrint SW.) -- C:\WINDOWS\Installer\7b79.msi  [1626112]  =>.HP Inc.
[MD5.F64E5503C91DC7970F4EE088CDF80D5F] [WIS][2016/12/05 20:34:40] (.Dropbox, Inc. - Dropbox 25 GB.) -- C:\WINDOWS\Installer\7b8f.msi  [6011392]  =>.Dr
[MD5.4EA4151EB8CA26CE15251672EE7B9670] [WIS][2019/01/11 16:48:02] (.© Copyright 2015 HP Development Company, L.P..) -- C:\WINDOWS\Installer\7bdda.msi
[MD5.E160C2252D5A6059D3A3C2C82CCCFDCA] [WIS][2018/09/11 10:36:20] (.Intel Corporation - Intel(R) Rapid Storage Technology.) -- C:\WINDOWS\Installer\7b
[MD5.9ECDDD325FFD9C28CA25470F50634CCF] [WIS][2019/06/16 14:47:25] (.Oracle Corporation - Java SE Runtime Environment 8 Update 211.) -- C:\WINDOWS\Inst
[MD5.D89CC1E11DCD5EFDD4D3C0EAF98C8280] [WIS][2019/06/16 14:47:22] (.Oracle Corporation - Java Auto Updater.) -- C:\WINDOWS\Installer\7cf28b.msi  [782
[MD5.02AA0265E4B4B042709643BCEE86C83E] [WIS][2019/06/16 14:50:12] (.Oracle Corporation - Java SE Runtime Environment 8 Update 211.) -- C:\WINDOWS\Inst
[MD5.36DD2D17A31E93F2A609E6AE81E1AD53] [WIS][2020/08/03 23:18:23] (.HP - HP PC Hardware Diagnostics UEFI.) -- C:\WINDOWS\Installer\aeb2b8.msi  [434698
[MD5.6E099E2FC95A7AA8157A9D40C69BF7AE] [WIS][2020/08/03 23:18:47] (.HP Inc..) -- C:\WINDOWS\Installer\aeb2ea.msi   [12011008]  =>.HP Inc.
[MD5.0E4585720A4205E884AB245D4ACDCAAE] [WIS][2018/08/24 01:13:14] (.Oracle Corporation - Java SE Runtime Environment 8 Update 181.) -- C:\WINDOWS\Inst
[MD5.D701D2883A1040AAF0B72548EC21B93C] [WIS][2018/04/02 15:15:40] (.Epic Games, Inc. - UE4 Prerequisites (x64).) -- C:\WINDOWS\Installer\c5c3596.msi
[MD5.86E2B390629665FBC20E06DFBF01A48F] [WIS][2019/04/04 10:11:10] (.Apple Inc. - [ProductName] Installer.) -- C:\WINDOWS\Installer\d3bc8a.msi  [273203
[MD5.76CA109CC56BD019F4EB2B967590092D] [WIS][2020/09/27 21:00:33] (.Adobe Systems Incorporated - Adobe ARM Installer.) -- C:\WINDOWS\Installer\dd21.ms
[MD5.5C35499F0F051A28E9264DADB553E526] [WIS][2019/01/15 15:14:54] (.Oracle Corporation - Oracle VM VirtualBox 6.0.2 installation pac.) -- C:\WINDOWS\I
[MD5.5630DF5178914355FFAEE705ECA7012D] [WIS][2018/08/31 19:51:36] (.HP Inc. - HP JumpStart Launch.) -- C:\WINDOWS\Installer\fa1bcf.msi  [708608]  =>.H
[MD5.C1A197F8BC93BD85A24CED0DD88483B3] [WIS][2018/08/31 19:51:36] (.HP Inc. - HP JumpStart Bridge.) -- C:\WINDOWS\Installer\fa1bef.msi  [4816896]  =>
[MD5.F1D7C4CA034C2F9C10C474CFD3205C93] [WIS][2020/01/11 15:47:41] (.Paradox Interactive - Paradox Launcher v2.) -- C:\WINDOWS\Installer\fea77fd.msi
[MD5.BD4173F416AC180D7AD46CB583BAB949] [WIS][2020/05/21 17:16:51] (.Adobe Inc..) -- C:\WINDOWS\Installer\1006a282.msp   [1392640]  =>.Adobe Inc.
[MD5.2AD3AE06875E8C704DA9F109422277CF] [WIS][2020/07/06 13:20:53] (.Adobe Inc..) -- C:\WINDOWS\Installer\13f306ad.msp   [5853184]  =>.Adobe Inc.
[MD5.DB596E2ADC480687F78F34B7D452D2CB] [WIS][2020/03/16 07:28:35] (.Adobe Inc..) -- C:\WINDOWS\Installer\14ba540d.msp   [8130560]  =>.Adobe Inc.
[MD5.16CD2BA3438D2627805A64D0F4DC063E] [WIS][2020/08/19 12:46:52] (.Adobe Inc..) -- C:\WINDOWS\Installer\1f527240.msp   [2781184]  =>.Adobe Inc.
[MD5.AC729EF5FD5047779136DD8670413E03] [WIS][2020/07/31 04:39:02] (.Adobe Inc..) -- C:\WINDOWS\Installer\2930cbaa.msp   [70844416]  =>.Adobe Inc.
[MD5.ADF98A69CAA202C2435AC97C124413AC] [WIS][2020/02/05 01:29:55] (.Adobe Inc..) -- C:\WINDOWS\Installer\5ce874.msp   [244162560]  =>.Adobe Inc.
[MD5.7F1419CD81DEB4E238B7F0426B0782B7] [WIS][2020/05/11 07:43:48] (.Adobe Inc..) -- C:\WINDOWS\Installer\6ce4b10.msp   [50810880]  =>.Adobe Inc.
[MD5.59776CD5E3E33907213B1E8249F64A02] [WIS][2020/11/02 07:52:52] (.Adobe Inc..) -- C:\WINDOWS\Installer\7d32716.msp   [20647936]  =>.Adobe Inc.
[MD5.923228256AD8BBCA145AE48027AA92BF] [WIS][2020/06/02 13:40:08] (.Adobe Inc..) -- C:\WINDOWS\Installer\942a528.msp   [3026944]  =>.Adobe Inc.
[MD5.6C872B8971E67A78A683FD192919AB70] [WIS][2020/09/23 06:58:22] (.Adobe Inc..) -- C:\WINDOWS\Installer\dd8e.msp   [33984512]  =>.Adobe Inc.

---\ RECHERCHE DE CLÉS DE REGISTRE Tracing (1) - 1s
HKLM\SOFTWARE\Microsoft\Tracing\svchost_RASCHAP  =>SUP.Optional.AdvancedSystemCare

---\ FEATURE CONTROL. (134) - 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_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]:RemotePlay.exe  =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BROWSER_EMULATION]:AndroidServer.exe  =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BROWSER_EMULATION]:ApowerMirror.exe  =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BROWSER_EMULATION]:Approximately.exe  =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BROWSER_EMULATION]:Wetzel.exe  =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BROWSER_EMULATION]:HP.EasyStart.exe  =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BROWSER_EMULATION]:ApowerCompress.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 =>.L
[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 =>.Legitimat
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_SCRIPT_PASTE_URLACTION_IF_PROMPT]:helppane.exe =>.Legitimat
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_SCRIPT_PASTE_URLACTION_IF_PROMPT]:PresentationHost.exe =>.L
[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_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_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_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_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_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_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_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_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_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_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_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_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_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_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

---\ OBSERVATEURS des évènements (70) - 8s
Application.Error: SideBySide (10)
~Numéro: 24655
~Date: 12/03/2020 11:54:09 AM
~ID: 78
~Description: La création du contexte d'activation a échoué pour « %11 ». Erreur dans le fichier de manifeste ou de stratégie « %12 » à la ligne %13.
~Suggestion: Aucune
Application.Warning: AutoEnrollment (1)
~Numéro: 24651
~Date: 12/03/2020 11:53:51 AM
~ID: 64
~Description: Système local93 8a e8 ef 22 04 7f 51 09 69 38 c8 ea ec 9f 12 d9 b3 68 f4
~Suggestion: Installer le Kit de développement logiciel (SDK).
Application.Error: SecurityCenter (1)
~Numéro: 24646
~Date: 12/03/2020 11:53:36 AM
~ID: 18
~Description: Le service Centre de sécurité Windows n'a pas pu charger les instances de FirewallProduct à partir du magasin de services.
Application.Warning: ESENT (2)
~Numéro: 24621
~Date: 12/03/2020 11:53:32 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 donr
Application.Error: VSS (4)
~Numéro: 24617
~Date: 12/03/2020 03:01:21 AM
~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: .NET Runtime (1)
~Numéro: 24615
~ID: 1026
~Description: Application : HPCommRecovery.exeVersion du Framework : v4.0.30319Description : le processus a été arrêté en raison d'une exception non g
~Suggestion: Essayer d'installer la dernière version de l'application ou du dernier correctif
System.Warning: hcmon (19)
~Numéro: 32396
~Date: 12/03/2020 12:04:04 PM
~ID: 0
~Description: Detected unrecognized USB driver (%2).
System.Warning: DCOM (18)
~Numéro: 32395
~Date: 12/03/2020 12:04:03 PM
~ID: 10016
~Description: par défaut de l'ordinateurLocalActivation{C2F03A33-21F5-47FA-B4BB-156362A2F239}{316CDED5-E4AE-4B15-9113-7055D84DCC97}DESKTOP-9A8RAVSOusm
~Suggestion: Vérifier les autorisations pour l'accès DCOM
System.Warning: BROWSER (1)
~Numéro: 32393
~Date: 12/03/2020 12:01:37 PM
~ID: 8021
~Description: Le service Explorateur n'a pas pu retrouver la liste des serveurs du maître explorateur %1 sur le réseau %2. Maître explorateur : \\l
System.Warning: Microsoft-Windows-Time-Service (2)
~Numéro: 32380
~Date: 12/03/2020 11:53:37 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'. NtpC
~Suggestion: Resynchroniser le client avec l'homologue de source de temps
System.Warning: Server (1)
~Numéro: 32373
~Date: 12/03/2020 11:53:35 AM
~ID: 2511
~Description: Le service Serveur n'a pas pu recréer le partage %1 car le répertoire %2 n'existe plus. Veuillez exécuter 'netshare %1/supprimer' pour s
System.Warning: BTHUSB (1)
~Numéro: 32349
~Date: 12/03/2020 11:53:28 AM
~ID: 34
~Description: La carte locale ne prend pas en charge un état de contrôleur Low Energy important pour la prise en charge du mode périphérique. Le masqu
System.Error: Service Control Manager (1)
~Numéro: 32299
~Date: 12/03/2020 03:01:18 AM
~ID: 7031
~Description: Le service %1 s'est terminé de manière inattendue. Ceci s'est produit %2 fois. L'action corrective suivante va être effectuée dans %3 mi

---\ SCAN ADDITIONNEL (133) - 10s
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\searchplugins\bing-lavasoft-ff59.xml =>PUP.Optional.LavasoftWebCompanion
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{E1527582-8509-4011-B922-29E3FB548882}_is1 =>Adware.DNSUnlocker
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FastDataX_is1 =>Adware.FastDataX
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5266F634-7B7D-4537-BDDC-98DD6CFCBAA1} =>SUP.Optional.Microleaves
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\FastDataX_is1 =>Adware.FastDataX
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{5266F634-7B7D-4537-BDDC-98DD6CFCBAA1} =>SUP.Optional.Microleaves
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Popcorn-Time =>.SUP.PopcornTime
C:\Program Files\Homeville =>Adware.DNSUnlocker
C:\Program Files\KMSpico =>HackTool.KMSpico
C:\Program Files (x86)\FastDataX =>Adware.FastDataX
C:\Program Files (x86)\Microleaves =>SUP.Optional.Microleaves
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\KMSpico =>HackTool.KMSpico
C:\Users\couli\AppData\Roaming\dclogs =>Trojan.StolenData
C:\Users\couli\AppData\Roaming\DiskDefrag =>SUP.Optional.AuslogicsDiskDefrag
C:\Users\couli\AppData\Roaming\Microleaves =>SUP.Optional.Microleaves
C:\Users\couli\AppData\Roaming\VirusMaker =>PUP.Optional.VirusMaker
C:\Users\couli\AppData\Local\Popcorn-Time =>.SUP.PopcornTime
C:\Users\couli\AppData\Local\SlimWare Utilities Inc =>.SUP.SlimWareUtilities
C:\Users\couli\AppData\Local\Solvusoft_Corporation =>SUP.Optional.Solvusoft
C:\Users\couli\AppData\LocalLow\Squeaky Wheel =>PUP.Optional.Squeaky
C:\Users\couli\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Popcorn-Time =>.SUP.PopcornTime
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers\ FileSyncEx =>.SUP.Orphan
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers\7-Zip =>.SUP.Orphan
HKLM\Software\Classes\CLSID\{23170F69-40C1-278A-1000-000100020000} =>.SUP.Orphan
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers\BriefcaseMenu =>.SUP.Orphan
HKLM\Software\Classes\CLSID\{85BBD920-42A0-1069-A2E4-08002B30309D} =>.SUP.Orphan

HKLM\Software\Wow6432Node\Classes\CLSID\{85BBD920-42A0-1069-A2E4-08002B30309D} =>.SUP.Orphan
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers\IObit Malware Fighter =>.SUP.Orphan
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers\IObitUnstaler =>.SUP.Orphan
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers\WinRAR32 =>.SUP.Orphan
HKLM\Software\Classes\CLSID\{B41DB860-8EE4-11D2-9906-E49FADC173CA} =>.SUP.Orphan
HKLM\Software\Classes\lnkfile\shellex\ContextMenuHandlers\IObitUnstaler =>.SUP.Orphan
HKLM\Software\Classes\lnkfile\shellex\ContextMenuHandlers\WinRAR32 =>.SUP.Orphan
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers\ FileSyncEx =>.SUP.Orphan
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers\7-Zip =>.SUP.Orphan
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers\IObit Malware Fighter =>.SUP.Orphan
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers\IObitUnstaler =>.SUP.Orphan
HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers\7-Zip =>.SUP.Orphan
HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers\BriefcaseMenu =>.SUP.Orphan
HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers\IObitUnstaler =>.SUP.Orphan
HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers\WinRAR32 =>.SUP.Orphan
HKLM\Software\Classes\Drive\shellex\ContextMenuHandlers\VMDiskMenuHandler =>.SUP.Orphan
HKLM\Software\Classes\CLSID\{271DC252-6FE1-4D59-9053-E4CF50AB99DE} =>.SUP.Orphan
C:\WINDOWS\Installer\{5266F634-7B7D-4537-BDDC-98DD6CFCBAA1}\online.exe =>SUP.Optional.Microleaves
HKLM\SOFTWARE\Wow6432Node\Classes\Installer\Products\436F6625D7B77354DBCD89DDC6CFAB1A =>SUP.Optional.Microleaves
HKLM\SOFTWARE\Wow6432Node\Classes\Installer\Features\436F6625D7B77354DBCD89DDC6CFAB1A =>SUP.Optional.Microleaves
C:\WINDOWS\Installer\2c5b1ca.msi =>SUP.Optional.Microleaves
HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\svchost_RASCHAP =>SUP.Optional.AdvancedSystemCare
C:\Users\couli\AppData\Local\Temp\mat-debug-10172.log =>.SUP.Temporary.Microsoft
C:\Users\couli\AppData\Local\Temp\mat-debug-20532.log =>.SUP.Temporary.Microsoft
C:\Users\couli\AppData\Local\Temp\mat-debug-24100.log =>.SUP.Temporary.Microsoft
C:\Users\couli\AppData\Local\Temp\mat-debug-24316.log =>.SUP.Temporary.Microsoft
C:\Users\couli\AppData\Local\Temp\mat-debug-5724.log =>.SUP.Temporary.Microsoft
ADS Présent [:com.dropbox.attrs] C:\Users\couli\Downloads\20200310_221354.jpg:com.dropbox.attrs =>.SUP.FileADS
ADS Présent [:com.dropbox.attrs] C:\Users\couli\Downloads\20200310_221444.jpg:com.dropbox.attrs =>.SUP.FileADS
ADS Présent [:com.dropbox.attrs] C:\Users\couli\Downloads\20200310_221556.jpg:com.dropbox.attrs =>.SUP.FileADS
ADS Présent [:com.dropbox.attrs] C:\Users\couli\Downloads\PL.7z:com.dropbox.attrs =>.SUP.FileADS
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\csastats =>Adware.InstallCore
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\drp.su =>.SUP.DriverPa
HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\webcompanion.com =>PUP
HKCU\Software\Lavasoft\Web Companion =>PUP.Optional.LavasoftWebCompanion
HKCU\Software\csastats =>Adware.InstallCore
HKCU\Software\undefined =>.SUP.Downloader
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\drp.su =>.SUP.DriverPack
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\webcompanion.com =>PUP.Optional.LavasoftWebCompanion
HKLM\SOFTWARE\Wow6432Node\IObit\RealTimeProtector =>SUP.Optional.AdvancedSystemCare
HKLM\SOFTWARE\Wow6432Node\IObit\Advanced SystemCare =>SUP.Optional.AdvancedSystemCare
HKLM\SOFTWARE\Wow6432Node\IObit\ASC =>SUP.Optional.AdvancedSystemCare
HKLM\SOFTWARE\Wow6432Node\Lavasoft\Web Companion =>PUP.Optional.LavasoftWebCompanion
HKLM\SOFTWARE\Lavasoft\Web Companion =>PUP.Optional.LavasoftWebCompanion
HKLM\SOFTWARE\Google\Chrome\NativeMessagingHosts\com.ascplugin.protect =>SUP.Optional.AdvancedSystemCare
HKLM\SOFTWARE\IObit\RealTimeProtector =>SUP.Optional.AdvancedSystemCare
HKLM\SOFTWARE\IObit\Advanced SystemCare =>SUP.Optional.AdvancedSystemCare
HKLM\SOFTWARE\Iobit\ASC =>SUP.Optional.AdvancedSystemCare
C:\Users\couli\AppData\Roaming\Mozilla\Firefox\Profiles\kpwwegsq.default\invalidprefs.js =>PUP.Optional.Legacy
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files (x86)\Google\Chrome\Application\chrome.exe.Friendly
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files (x86)\Google\Chrome\Application\chrome.exe.Applicati
C:\Program Files\File Magic\FileMagic.exe =>SUP.Optional.Solvusoft
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files\File Magic\FileMagic.exe.FriendlyAppName =>SUP.Optic
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files\File Magic\FileMagic.exe.ApplicationCompany =>SUP.Op
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:D:\Téléchargement New\Airport.CEO.v32.6-4\Airport.CEO.v32.6-4\Airpor
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:D:\Program Files\Nox\bin\MultiPlayerManager.exe.FriendlyAppName =>.Ur
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:D:\BlueStacks\BlueStacks\Client\Bluestacks.exe.FriendlyAppName =>.SL
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:D:\BlueStacks\BlueStacks\Client\Bluestacks.exe.ApplicationCompany =>
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Users\couli\AppData\Local\WhatsApp\app-2.2025.7\WhatsApp.exe.Frier
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Users\couli\AppData\Local\WhatsApp\app-2.2025.7\WhatsApp.exe.Appli
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Users\couli\Downloads\AirDroid_Desktop_Client_3.6.7.0.exe.Friendly
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\users\couli\appdata\local\programs\opera\68.0.3618.173\opera.exe.F
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\users\couli\appdata\local\programs\opera\68.0.3618.173\opera.exe.A
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\users\couli\appdata\local\programs\opera\69.0.3686.95\opera.exe.Fr
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\users\couli\appdata\local\programs\opera\69.0.3686.95\opera.exe.Ap
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files (x86)\Quranflash Desktop\Quranflash Desktop.exe.Frie
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:D:\Games\Prison Architect The Clink\Prison Architect.exe.FriendlyAppN
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files (x86)\Battle.net\Battle.net Launcher.exe.FriendlyApp
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files (x86)\Battle.net\Battle.net Launcher.exe.Applicatior
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:D:\SteamLibrary\Two Point Hospital\TPH.exe.FriendlyAppName =>.Unsigne
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Users\couli\Downloads\DpFileList Generator 2020 v1.0\DpFileList Ge
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\users\couli\appdata\local\programs\opera\71.0.3770.198\opera.exe.F
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\users\couli\appdata\local\programs\opera\71.0.3770.198\opera.exe.A
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\users\couli\appdata\local\programs\opera\71.0.3770.284\opera.exe.F
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\users\couli\appdata\local\programs\opera\71.0.3770.284\opera.exe.A
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files (x86)\
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files (x86)\
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files\File M
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files\File M
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:D:\Téléchargement New\
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:D:\Program Files\Nox\bi
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:D:\BlueStacks\BlueStack
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:D:\BlueStacks\BlueStack
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Users\couli\AppData\
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Users\couli\AppData\
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Users\couli\Downloac
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\users\couli\appdata\
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\users\couli\appdata\
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\users\couli\appdata\
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\users\couli\appdata\
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files (x86)\
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:D:\Games\Prison Archite
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files (x86)\
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files (x86)\
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:D:\SteamLibrary\Two Poi
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Users\couli\Downloac
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\users\couli\appdata\
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\users\couli\appdata\
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\users\couli\appdata\
[HKU\S-1-5-21-2155290971-1816436987-1419378802-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\users\couli\appdata\
C:\Windows\SysWOW64\SSL =>Trojan.Agent
C:\Users\couli\AppData\LocalLow\IObit\Advanced SystemCare =>SUP.Optional.AdvancedSystemCare
C:\Users\couli\AppData\Roaming\IObit\Advanced SystemCare =>SUP.Optional.AdvancedSystemCare
C:\Program Files (x86)\Common Files\IObit\Advanced SystemCare =>SUP.Optional.AdvancedSystemCare

C:\ProgramData\IObit\Advanced SystemCare =>SUP.Optional.AdvancedSystemCare
C:\ProgramData\Application Data\IObit\ASCDownloader =>SUP.Optional.AdvancedSystemCare
C:\ProgramData\IObit\ASCDownloader =>SUP.Optional.AdvancedSystemCare

---\ RÉCAPITULATIF DES ÉLÉMENTS TROUVÉS (28) - 0s
https://nicolascoolman.eu/2017/09/12/origine-lignes-orphelines/ =>.SUP.Orphan
https://nicolascoolman.eu/2017/03/12/superfluous-lavasoftwebcompanion/ =>PUP.Optional.LavasoftWebCompanion
https://nicolascoolman.eu/forum/Topic/repaquetage-et-infection/ =>BitTorrent (P2P)
https://nicolascoolman.eu/forum/Topic/solvusoft-logiciel-potentiellement-superflu-lps/ =>SUP.Optional.Solvusoft
https://nicolascoolman.eu/2017/11/01/adware-mybrowser/ =>PUP.Optional.MyBrowser
https://nicolascoolman.eu/2017/09/27/adware-dnsunlocker/ =>Adware.DNSUnlocker
https://nicolascoolman.eu/2017/06/21/adware-fastdatax/ =>Adware.FastDataX
https://nicolascoolman.eu/2017/12/24/sup-microleaves/ =>SUP.Optional.Microleaves
https://nicolascoolman.eu/2017/02/26/superfluous-popcorntime/ =>.SUP.PopcornTime
https://nicolascoolman.eu/2017/03/11/pup-optional-crossrider/ =>Adware.CrossRider
https://nicolascoolman.eu/2017/09/19/adware-installcore-3/ =>Adware.InstallCore
trojan-fynloski/ =>Trojan.Fynloski
https://nicolascoolman.eu/forum/Topic/repaquetage-et-infection/ =>PUP.Optional.Squeaky
https://nicolascoolman.eu/2017/12/22/sup-downloader/ =>.SUP.Downloader
https://nicolascoolman.eu/2017/02/16/hacktool-kmspico/ =>HackTool.KMSpico
https://nicolascoolman.eu/forum/Topic/repaquetage-et-infection/ =>Trojan.StolenData
https://nicolascoolman.eu/forum/Topic/repaquetage-et-infection/ =>SUP.Optional.AuslogicsDiskDefrag
https://nicolascoolman.eu/forum/Topic/repaquetage-et-infection/ =>PUP.Optional.VirusMaker
https://nicolascoolman.eu/2017/03/03/superfluous-slimwareutilities/ =>.SUP.SlimWareUtilities
https://nicolascoolman.eu/wp-content/uploads/2017/12/26/sup-advancedsystemcare/ =>SUP.Optional.AdvancedSystemCare
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.Microsoft
https://nicolascoolman.eu/2018/01/04/ads-alternate-data-stream/ =>.SUP.FileADS
https://nicolascoolman.eu/2018/07/04/sup-driverpack/ =>.SUP.DriverPack
https://nicolascoolman.eu/forum/Topic/legacy-logiciel-potentiellement-indesirable-pup-lpi/ =>PUP.Optional.Legacy
https://nicolascoolman.eu/forum/Topic/orphan-muicache-logiciel-potentiellement-superflu-lps/ =>.SUP.Orphan.MUICache
https://nicolascoolman.eu/forum/Topic/repaquetage-et-infection/ =>Trojan.Agent

~ Unselected Options:
~ End of the scan, 21518 items in 07mn02s (4498)(1)

NUMEROS DE SÉRIE

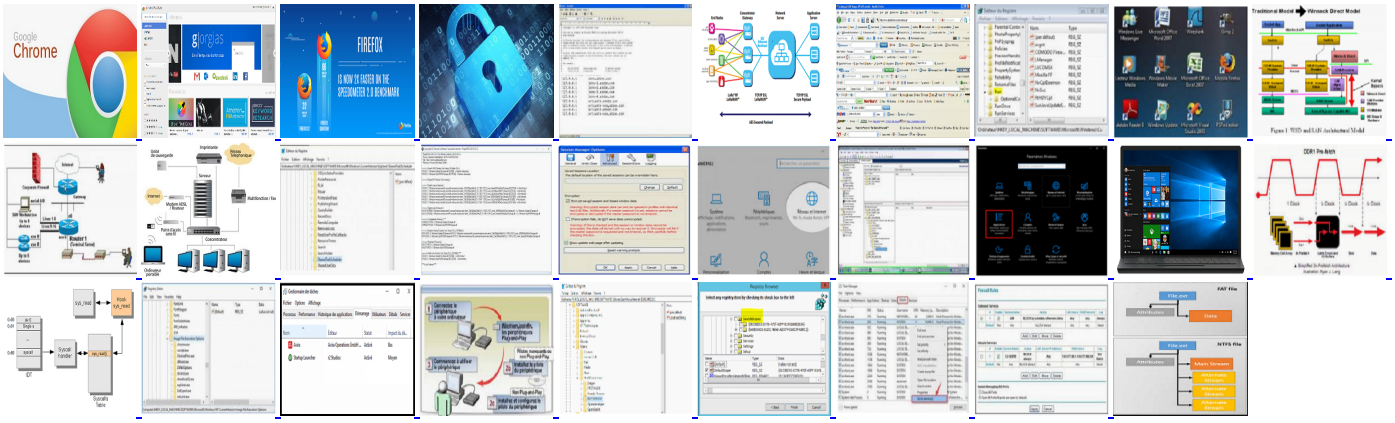
[0082E3575D491A060D54453B7B0AB1AB01] [30/12/2018] (.Cyotek Ltd.) - C:\Program Files (x86)\Cyotek\WebCopy\ctkaupld.exe =>.Not verified
[00881CCC851C6F73A2] [10/04/2020] (.Paradox Interactive Ab (Publ).) - D:\SteamLibrary\steamapps\common\Cities_Skylines\dowser.exe
[00A7A7F8DAE29DDB343E15624827840946] [02/04/2020] (.MegaDev GmbH.) - C:\Program Files\MegaDev\MegaTrainerUltimate\MTU.exe =>.Not verified
[00A7A7F8DAE29DDB343E15624827840946] [30/09/2019] (.MegaDev GmbH.) - C:\Program Files (x86)\MegaDev\MegaTrainerUltimate\MTU.exe =>.Not verified
[00AD4CE8B9CBA67D329BCB15612EA5F082] [11/01/2019] (.Noble Education Institue, Inc..) - C:\Program Files (x86)\Quran Explorer\Quran Explorer Desktop\QE
[00B911CC7038EA832D7CFB12525AFCC7A4] [26/07/2017] (.Tensons Corporation.) - C:\Program Files\Tensons\Website Ripper Copier\Website Ripper Copier.exe
[00D4954D484B4CBF248215948647FDB462] [26/06/2017] (.MaximumSoft Corp..) - C:\Program Files (x86)\WebCopier\WebCopier.exe =>.Not verified
[00E49E47111FEC98CD0000000055662B3E] [09/09/2019] (.Rockstar Games, Inc..) - C:\Program Files (x86)\Rockstar Games\Social Club\SocialClubHelper.exe
[00E49E47111FEC98CD0000000055662B3E] [09/09/2019] (.Rockstar Games, Inc..) - C:\Program Files\Rockstar Games\Social Club\SocialClubHelper.exe
[00E49E47111FEC98CD0000000055662B3E] [09/09/2019] (.Rockstar Games, Inc..) - C:\Program Files\Rockstar Games\Social Club\uninstallRGSCRedistributable
[00E49E47111FEC98CD0000000055662B3E] [25/09/2019] (.Rockstar Games, Inc..) - D:\Launcher\LauncherPatcher.exe
[00E49E47111FEC98CD0000000055662B3E] [25/09/2019] (.Rockstar Games, Inc..) - D:\Launcher\RockstarService.exe
[00ED6477F116E0A1C95681D6E2609DA432] [08/05/2020] (.Fonts Ninja.) - C:\Users\couli\AppData\Local\Programs\FontsNinja\Fonts Ninja.exe =>.Not verified
[00ED6477F116E0A1C95681D6E2609DA432] [08/05/2020] (.Fonts Ninja.) - C:\Users\couli\AppData\Local\Programs\FontsNinja\Uninstall Fonts Ninja.exe =>.Not
[00F0A5CD9EA2DD1322C07D410D0E1A945B] [04/02/2019] (.Vijua.) - C:\Program Files (x86)\Quranflash Desktop\unins000.exe =>.Not verified
[01342592A0010CB1109C11C0519CFD24] [21/04/2020] (.Notepad++.) - C:\Program Files (x86)\Notepad++\notepad++.exe
[016E69B09933857FE2F910CEDD57125D] [02/12/2020] (.Twitch Interactive, Inc..) - C:\Users\couli\AppData\Roaming\Twitch\Bin\Twitch.exe
[016E69B09933857FE2F910CEDD57125D] [02/12/2020] (.Twitch Interactive, Inc..) - C:\Users\couli\AppData\Roaming\Twitch\Bin\UninstallTwitch.exe
[017CA19B5859E83F44D874C1CE506E6D] [23/08/2018] (.Dropbox, Inc.) - C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe
[0195C200D3BEB4976805ACD3973BB6DF] [22/10/2019] (.Adobe Inc..) - C:\Program Files (x86)\Adobe\Adobe Creative Cloud Experience\CCXProcess.exe
[01C41F7849CDD7ACF166AD3177685D24] [01/12/2020] (.Spotify AB.) - C:\Program Files\WindowsApps\SpotifyAB.SpotifyMusic_1.147.684.0_x86__zpdnekdrzrea0\Sp
[01E84CE2860CF3D794990EDED64D5F0A] [28/06/2019] (.Prey, Inc..) - C:\Windows\Prey\wpxsvc.exe =>.Not verified
[01F5E7B9243B50531605AF6141A6F8D8] [13/07/2017] (.HP Inc..) - C:\Program Files (x86)\HP\HP System Event\HPWMISVC.exe
[025A1BF3E3892383825371900349E56A] [16/07/2020] (.Avast Software s.r.o..) - C:\WINDOWS\System32\drivers\aswVpnRdr.sys
[025A1BF3E3892383825371900349E56A] [16/11/2020] (.Avast Software s.r.o..) - C:\Program Files\Common Files\Avast Software\Icarus\avast-vpn\icarus.exe
[025A1BF3E3892383825371900349E56A] [18/11/2020] (.Avast Software s.r.o..) - C:\Program Files\AVAST Software\SecureLine VPN\AvBugReport.exe
[025A1BF3E3892383825371900349E56A] [18/11/2020] (.Avast Software s.r.o..) - C:\Program Files\AVAST Software\SecureLine VPN\Vpn.exe
[025A1BF3E3892383825371900349E56A] [18/11/2020] (.Avast Software s.r.o..) - C:\Program Files\AVAST Software\SecureLine VPN\VpnSvc.exe
[025A1BF3E3892383825371900349E56A] [24/11/2020] (.Avast Software s.r.o..) - C:\Program Files\AVAST Software\Avast\ashShell.dll
[025A1BF3E3892383825371900349E56A] [24/11/2020] (.Avast Software s.r.o..) - C:\Program Files\AVAST Software\Avast\aswToolsSvc.exe
[025A1BF3E3892383825371900349E56A] [24/11/2020] (.Avast Software s.r.o..) - C:\Program Files\AVAST Software\Avast\AvastUI.exe
[025A1BF3E3892383825371900349E56A] [24/11/2020] (.Avast Software s.r.o..) - C:\Program Files\AVAST Software\Avast\AvLaunch.exe
[025A1BF3E3892383825371900349E56A] [24/11/2020] (.Avast Software s.r.o..) - C:\Program Files\AVAST Software\Avast\setup\instup.exe
[0271E10D9F2E8264FCE4B2669A6299CE] [23/11/2020] (.WhatsApp, Inc.) - C:\Users\couli\AppData\Local\WhatsApp\Update.exe
[0271E10D9F2E8264FCE4B2669A6299CE] [23/11/2020] (.WhatsApp, Inc.) - C:\Users\couli\AppData\Local\WhatsApp\WhatsApp.exe
[02F3643033F852C4A904A4BE7F8DC715] [14/05/2020] (.Shanghai Microvirt Software Technology Co., Ltd..) - C:\Program Files (x86)\Microvirt\MEmu\MEmu.exe
[02F3643033F852C4A904A4BE7F8DC715] [14/05/2020] (.Shanghai Microvirt Software Technology Co., Ltd..) - C:\Program Files (x86)\Microvirt\MEmu\MEmuConsc
[02F3643033F852C4A904A4BE7F8DC715] [14/05/2020] (.Shanghai Microvirt Software Technology Co., Ltd..) - C:\Program Files (x86)\Microvirt\MEmu\uninstall
[02F7B07C5525B8C907016C37798A6355] [03/01/2020] (.Wondershare Technology Co.,Ltd.) - C:\Program Files (x86)\Wondershare\Video Converter Ultimate\Videc
[02F7B07C5525B8C907016C37798A6355] [10/01/2020] (.Wondershare Technology Co.,Ltd.) - C:\Program Files (x86)\Wondershare\Video Converter Ultimate\unins
[02FA994D660DE659EE9037ECB437D766] [10/11/2020] (.Piriform Software Ltd.) - C:\Program Files\CCleaner\CCleaner64.exe
[02FA994D660DE659EE9037ECB437D766] [10/11/2020] (.Piriform Software Ltd.) - C:\Program Files\CCleaner\uninst.exe
[0304E53E0F9B762F0EEB0F5F7E3B549D] [20/05/2017] (.Open Source Developer, Xavier Roche.) - C:\Program Files (x86)\WinHTTrack\WinHTTrack.exe
[0304E53E0F9B762F0EEB0F5F7E3B549D] [31/01/2019] (.Open Source Developer, Xavier Roche.) - C:\Program Files (x86)\WinHTTrack\unins000.exe
[0320BE3EB866526927F999B97B04346E] [03/08/2020] (.Realtek Semiconductor Corp..) - C:\WINDOWS\System32\DRIVERS\rtf64x64.sys
[0320BE3EB866526927F999B97B04346E] [16/02/2019] (.Realtek Semiconductor Corp..) - C:\WINDOWS\System32\drivers\rt640x64.sys
[0320BE3EB866526927F999B97B04346E] [17/05/2019] (.Realtek Semiconductor Corp..) - C:\WINDOWS\System32\drivers\RtkA2dp.sys
[0320BE3EB866526927F999B97B04346E] [17/05/2019] (.Realtek Semiconductor Corp..) - C:\WINDOWS\System32\drivers\RtkAvrcp.sys
[0320BE3EB866526927F999B97B04346E] [23/01/2019] (.Realtek Semiconductor Corp..) - C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe
[0320BE3EB866526927F999B97B04346E] [23/01/2019] (.Realtek Semiconductor Corp..) - C:\Program Files\Realtek\Audio\HDA\RtlUpd64.exe
[0320BE3EB866526927F999B97B04346E] [23/01/2019] (.Realtek Semiconductor Corp..) - C:\WINDOWS\System32\DRIVERS\Rt64win7.sys
[0320BE3EB866526927F999B97B04346E] [23/01/2019] (.Realtek Semiconductor Corp..) - C:\WINDOWS\System32\drivers\RtkAvrcpCtrlr.sys
[0320BE3EB866526927F999B97B04346E] [23/01/2019] (.Realtek Semiconductor Corp..) - C:\WINDOWS\System32\Drivers\RtsUer.sys
[032A2CC22EF44007ADE9E0C4F28024D0] [08/08/2018] (.HP Inc..) - C:\Program Files (x86)\HP\HP System Event\HPMSGSVC.exe
[03471E2C8171B1679D898AC19BDA37BB] [05/06/2019] (.TeamViewer GmbH.) - C:\Program Files (x86)\TeamViewer\TeamViewer.exe
[03471E2C8171B1679D898AC19BDA37BB] [05/06/2019] (.TeamViewer GmbH.) - C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe
[03471E2C8171B1679D898AC19BDA37BB] [05/06/2019] (.TeamViewer GmbH.) - C:\Program Files (x86)\TeamViewer\uninstall.exe
[03498E828081693140DAE8DCBD1D723D] [07/11/2019] (.MariaDB Corporation Ab.) - G:\wamp64\bin\mariadb\mariadb10.4.10\bin\mysqld.exe
[034B2981B20F76E6BC69D2ED44EBF2E8] [08/12/2019] (.Logitech Inc.) - C:\WINDOWS\System32\drivers\logi_generic_hid_filter.sys
[034B2981B20F76E6BC69D2ED44EBF2E8] [08/12/2019] (.Logitech Inc.) - C:\WINDOWS\System32\drivers\logi_joy_bus_enum.sys

```
[034B2981B20F76E6BC69D2ED44EBF2E8] [08/12/2019] (.Logitech Inc.) - C:\WINDOWS\System32\drivers\logi_joy_hid_filter.sys
[034B2981B20F76E6BC69D2ED44EBF2E8] [08/12/2019] (.Logitech Inc.) - C:\WINDOWS\System32\drivers\logi_joy_hid_lo.sys
[034B2981B20F76E6BC69D2ED44EBF2E8] [08/12/2019] (.Logitech Inc.) - C:\WINDOWS\System32\drivers\logi_joy_xlcore.sys
[03772A500B925E363DD8172F157C7668] [29/06/2019] (.SCREENOVATE TECHNOLOGIES LTD..) - C:\WINDOWS\System32\DRIVERS\ScrHIDDriver.sys  =>.Not verified
[03ACACAA3FCBB6B2930EADC5A4633841] [01/08/2018] (.HP Inc..) - C:\Windows\System32\DriverStore\FileRepository\vigembus.inf_amd64_e84845c70c38fbe7\x64\V
[03ACACAA3FCBB6B2930EADC5A4633841] [06/07/2018] (.HP Inc..) - C:\Windows\System32\DriverStore\FileRepository\hpcustomcapdriver.inf_amd64_1f5602eb8a12a
[03ACACAA3FCBB6B2930EADC5A4633841] [21/10/2018] (.HP Inc..) - C:\Windows\System32\DriverStore\FileRepository\hpomencustomcapdriver.inf_amd64_326f2e1d1
[03DA4C26C76E1255DC8279AA9A751ACC] [07/07/2016] (.Realtek Semiconductor Corp..) - C:\Program Files (x86)\InstallShield Installation Information\{8833F
[03DA4C26C76E1255DC8279AA9A751ACC] [26/06/2017] (.Realtek Semiconductor Corp..) - C:\Program Files (x86)\Realtek\PCIE Wireless LAN\RtlS5Wake\RtlS5Wake
[03E9EB4DFF67D4F9A554A422D5ED86F3] [25/10/2020] (.philandro Software GmbH.) - C:\users\couli\downloads\anydesk.exe
[03F02ACA051D1C9330EEABD3706E836F] [24/11/2020] (.Avast Software s.r.o..) - C:\Program Files\AVAST Software\Avast\AvastSvc.exe
[03F02ACA051D1C9330EEABD3706E836F] [24/11/2020] (.Avast Software s.r.o..) - C:\Program Files\AVAST Software\Avast\wsc_proxy.exe
[03F02ACA051D1C9330EEABD3706E836F] [24/11/2020] (.Avast Software s.r.o..) - C:\WINDOWS\System32\drivers\aswArDisk.sys
[03F02ACA051D1C9330EEABD3706E836F] [24/11/2020] (.Avast Software s.r.o..) - C:\WINDOWS\System32\drivers\aswArPot.sys
[03F02ACA051D1C9330EEABD3706E836F] [24/11/2020] (.Avast Software s.r.o..) - C:\WINDOWS\System32\drivers\aswbidsdriver.sys
[03F02ACA051D1C9330EEABD3706E836F] [24/11/2020] (.Avast Software s.r.o..) - C:\WINDOWS\System32\drivers\aswbidsh.sys
[03F02ACA051D1C9330EEABD3706E836F] [24/11/2020] (.Avast Software s.r.o..) - C:\WINDOWS\System32\drivers\aswbuniv.sys
[03F02ACA051D1C9330EEABD3706E836F] [24/11/2020] (.Avast Software s.r.o..) - C:\WINDOWS\System32\drivers\aswKbd.sys
[03F02ACA051D1C9330EEABD3706E836F] [24/11/2020] (.Avast Software s.r.o..) - C:\WINDOWS\System32\drivers\aswMonFlt.sys
[03F02ACA051D1C9330EEABD3706E836F] [24/11/2020] (.Avast Software s.r.o..) - C:\WINDOWS\System32\drivers\aswNetHub.sys
[03F02ACA051D1C9330EEABD3706E836F] [24/11/2020] (.Avast Software s.r.o..) - C:\WINDOWS\System32\drivers\aswRdr2.sys
[03F02ACA051D1C9330EEABD3706E836F] [24/11/2020] (.Avast Software s.r.o..) - C:\WINDOWS\System32\drivers\aswRvrt.sys
[03F02ACA051D1C9330EEABD3706E836F] [24/11/2020] (.Avast Software s.r.o..) - C:\WINDOWS\System32\drivers\aswSnx.sys
[03F02ACA051D1C9330EEABD3706E836F] [24/11/2020] (.Avast Software s.r.o..) - C:\WINDOWS\System32\drivers\aswSP.sys
[03F02ACA051D1C9330EEABD3706E836F] [24/11/2020] (.Avast Software s.r.o..) - C:\WINDOWS\System32\drivers\aswStm.sys
[03F02ACA051D1C9330EEABD3706E836F] [24/11/2020] (.Avast Software s.r.o..) - C:\WINDOWS\System32\drivers\aswVmm.sys
[0443B567BFFBAA3BC083FE45A46DD041] [29/01/2020] (.Blizzard Entertainment, Inc..) - C:\Program Files (x86)\Battle.net\Battle.net Launcher.exe
[0443B567BFFBAA3BC083FE45A46DD041] [29/01/2020] (.Blizzard Entertainment, Inc..) - C:\ProgramData\Battle.net\Agent\Blizzard Uninstaller.exe
[0449EDEF08B987F05203C4E0F2356499] [06/09/2020] (.HP Inc..) - C:\Program Files\WindowsApps\AD2F1837.HPSystemEventUtility_1.1.21.0_x64__v10z8vjag6ke6\S
[045F7B840FB74D1CD3FD9920335A93A0] [05/10/2018] (.Logitech Inc.) - C:\WINDOWS\System32\drivers\LGBusEnum.sys
[045F7B840FB74D1CD3FD9920335A93A0] [05/10/2018] (.Logitech Inc.) - C:\WINDOWS\System32\drivers\LGJoyHidFilter.sys
[045F7B840FB74D1CD3FD9920335A93A0] [05/10/2018] (.Logitech Inc.) - C:\WINDOWS\System32\drivers\LGJoyHidLo.sys
[045F7B840FB74D1CD3FD9920335A93A0] [05/10/2018] (.Logitech Inc.) - C:\WINDOWS\System32\drivers\LGJoyXlCore.sys
[045F7B840FB74D1CD3FD9920335A93A0] [05/10/2018] (.Logitech Inc.) - C:\WINDOWS\System32\drivers\LGVirHid.sys
[04F131322CC31D92C849FCA351D2F141] [10/09/2020] (.Discord Inc..) - C:\Users\couli\AppData\Local\Discord\Update.exe
[04F942C68E5028A4346758EC406E21E1] [02/11/2020] (.HP Inc..) - C:\Windows\System32\DriverStore\FileRepository\hpanalyticscomp.inf_amd64_3b1a7f8fd6029da
[054F466CECCBE9D6BEE81F5435E64D47] [02/11/2020] (.Valve.) - C:\Program Files (x86)\Common Files\Steam\SteamService.exe
[054F466CECCBE9D6BEE81F5435E64D47] [29/10/2020] (.Valve.) - C:\Program Files (x86)\Steam\bin\cef\cef.win7x64\steamwebhelper.exe
[054F466CECCBE9D6BEE81F5435E64D47] [29/10/2020] (.Valve.) - C:\Program Files (x86)\Steam\Steam.exe
[055F937A9DF73DFD90BA9889E4C50A11] [23/07/2018] (.Notepad++.) - C:\Program Files (x86)\Notepad++\NppShell_06.dll
[05F4210DB2B283A32FF2AED29FCB68A4] [02/12/2020] (.Opera Software AS.) - C:\users\couli\appdata\local\programs\opera\72.0.3815.400\opera.exe
[05F4210DB2B283A32FF2AED29FCB68A4] [25/11/2020] (.Opera Software AS.) - C:\Users\couli\AppData\Local\Programs\Opera\launcher.exe
[0600B9631A0C75311B31FE7E3FF288EA] [25/01/2020] (.Logitech Inc..) - C:\ProgramData\LGHUB\depots\35872\driver_cpu_temperature\logi_core_temp.sys
[063D0C011B143C57893FE839779AFCD0] [04/12/2019] (.Realtek Semiconductor Corp..) - C:\WINDOWS\System32\drivers\rtwlane.sys
[063D0C011B143C57893FE839779AFCD0] [23/01/2019] (.Realtek Semiconductor Corp..) - C:\Program Files\Realtek\Audio\HDA\RtkAudioService64.exe
[063D0C011B143C57893FE839779AFCD0] [23/01/2019] (.Realtek Semiconductor Corp..) - C:\WINDOWS\System32\drivers\RTKVHD64.sys
[0658F9A568F8C58CD6862779059C0792] [24/10/2019] (.Adobe Inc..) - D:\Adobe Premier 2020\Adobe Premiere Pro 2020\Adobe Premiere Pro.exe
[06AEA76BAC46A9E8CFE6D29E45AAF033] [03/12/2020] (.Google LLC.) - C:\Program Files (x86)\Google\Update\1.3.36.32\GoogleCrashHandler.exe
[06AEA76BAC46A9E8CFE6D29E45AAF033] [03/12/2020] (.Google LLC.) - C:\Program Files (x86)\Google\Update\1.3.36.32\GoogleCrashHandler64.exe
[06AEA76BAC46A9E8CFE6D29E45AAF033] [03/12/2020] (.Google LLC.) - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
[06AEA76BAC46A9E8CFE6D29E45AAF033] [11/07/2020] (.Google LLC.) - D:\android studio\jre\bin\java.exe
[06AEA76BAC46A9E8CFE6D29E45AAF033] [11/07/2020] (.Google LLC.) - D:\android studio\uninstall.exe
[06B922A8397E632FE5348DA267275B4F] [10/04/2018] (.Adobe Systems Incorporated.) - C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\UWA\UpdaterStart
[06F08C060B0BFDDB7160D114A7D2E700] [21/06/2019] (.HP Inc..) - C:\Program Files (x86)\HP\HPAudioSwitch\HPAudioSwitch.exe
[06F24D9F4DB07BD7ECAD067F5EE26C29] [27/09/2019] (.Adobe Inc..) - C:\Program Files (x86)\Adobe\Adobe Sync\CoreSyncPlugins\LiveType\customhook\uninstall
[06F24D9F4DB07BD7ECAD067F5EE26C29] [27/09/2019] (.Adobe Inc..) - C:\Program Files (x86)\Common Files\Adobe\Adobe Desktop Common\HDBox\Uninstaller.exe
[06F56DD38538018E9A31248796E640AB] [01/11/2018] (.GOG Sp. z o.o..) - G:\Project Hospital\unins000.exe
[07C70F7CAB145BC1ED385FBE69FA3130] [16/05/2020] (.AVAST Software s.r.o..) - C:\WINDOWS\System32\drivers\aswTap.sys
[07CDE1A1A0F336D740B9572374138D6B] [11/03/2020] (.Electronic Arts, Inc..) - C:\Program Files\Common Files\EAInstaller\FIFA 20\Cleanup.exe
[07FED0B8E61270E83F5AEC8B91E3B679] [01/01/2019] (.SCREENOVATE TECHNOLOGIES LTD..) - C:\WINDOWS\System32\drivers\HfAudio.sys
[07FED0B8E61270E83F5AEC8B91E3B679] [01/01/2019] (.SCREENOVATE TECHNOLOGIES LTD..) - C:\WINDOWS\System32\drivers\ScrHIDDriver2.sys
[07FED0B8E61270E83F5AEC8B91E3B679] [13/02/2019] (.SCREENOVATE TECHNOLOGIES LTD..) - C:\Program Files\Dell\DellMobileConnectDrivers\DellMobileConnectWe
[084CAF4DF499141D404B7199AA2C2131] [22/05/2018] (.Valve.) - C:\Program Files (x86)\Steam\uninstall.exe
[084CE11D0AEB94BF0EAEEC32A755A013] [11/01/2019] (.Samsung Electronics CO., LTD..) - C:\Program Files (x86)\Samsung\SideSync4\SideSync.exe
[084CE11D0AEB94BF0EAEEC32A755A013] [28/12/2018] (.Samsung Electronics CO., LTD..) - C:\Program Files (x86)\Samsung\Smart Switch PC\SmartSwitchPC.exe
[08557A49A29FFD9253CA5AC8780F2C95] [01/12/2020] (.Dropbox, Inc.) - C:\Program Files (x86)\Dropbox\Client\111.4.472\QtWebEngineProcess.exe
[08557A49A29FFD9253CA5AC8780F2C95] [01/12/2020] (.Dropbox, Inc.) - C:\Program Files (x86)\Dropbox\Client\Dropbox.exe
[08557A49A29FFD9253CA5AC8780F2C95] [01/12/2020] (.Dropbox, Inc.) - C:\Program Files (x86)\Dropbox\Client\DropboxUninstaller.exe
[08557A49A29FFD9253CA5AC8780F2C95] [01/12/2020] (.Dropbox, Inc.) - C:\WINDOWS\System32\DbxSvc.exe
[08557A49A29FFD9253CA5AC8780F2C95] [06/10/2020] (.Dropbox, Inc.) - C:\Program Files (x86)\Dropbox\Client\DropboxExt64.46.0.dll
[094DC9C3B9D09B4F1D07FA327100E5D5] [16/10/2020] (.BattlEye Innovations e.K..) - C:\Program Files (x86)\Common Files\BattlEye\BEService.exe
[09AD5E1AF13A4E4A690B66B9A8EE2175] [31/03/2020] (.Adobe Inc..) - C:\Program Files (x86)\Brackets\Brackets.exe
[09AD5E1AF13A4E4A690B66B9A8EE2175] [31/03/2020] (.Adobe Inc..) - C:\program files (x86)\brackets\node.exe
[09E002ED55EBC92B8A799574F80069FD] [03/08/2020] (.HP Inc..) - C:\Windows\System32\drivers\HpPortIox64.sys
[0A5C0955B9E3AC705430FCAC2EDEEDD0] [09/10/2020] (.Node.js Foundation.) - C:\Windows\Prey\current\bin\node.exe
[0A5C0955B9E3AC705430FCAC2EDEEDD0] [09/10/2020] (.Node.js Foundation.) - C:\Windows\Prey\versions\1.9.6\bin\node.exe
[0A9997ACCB4B384C80E313DD2854407B] [20/04/2017] (.Realtek Semiconductor Corp..) - C:\Windows\RtCRU64.exe
[0A9F96AABFB5DAC0F29F565D33FF1AF6] [17/04/2020] (.Wondershare Technology Co.,Ltd.) - C:\Program Files\Wondershare\Wondershare Filmora (FR)\Wondershare
[0AD6B2BE1D9DF100355F73D9F824DD3B] [19/12/2019] (.HP Inc..) - C:\Program Files\HPCommRecovery\HPCommRecovery.exe
[0AD6B2BE1D9DF100355F73D9F824DD3B] [20/12/2019] (.HP Inc..) - C:\Program Files (x86)\InstallShield Installation Information\{6468C4A5-E47E-405F-B675-A
[0B012EB98C703AA9B06D264355E9FE39] [26/11/2020] (.TeamSpeak Systems GmbH.) - C:\Program Files\TeamSpeak 3 Client\ts3client_win64.exe  =>.Not verified
[0B414C00BF45EDB4865CE431D4954843] [06/03/2020] (.SMAG Services.) - C:\Users\couli\AppData\Roaming\Jarvee\Jarvee.exe  =>.Not verified
[0BBE43DA41204BB6D7E5622C07C3290D] [02/03/2018] (.Daring Development Inc..) - C:\Program Files\WeMod\Version Guard\7za.exe
[0BBE43DA41204BB6D7E5622C07C3290D] [24/05/2018] (.Daring Development Inc..) - C:\Program Files\WeMod\Version Guard\VersionGuard.exe
[0BD1353EF0AC8CB40B25FA361AF292AC] [08/11/2020] (.Streamlabs (General Workings, Inc.).) - C:\Program Files\Streamlabs OBS\Streamlabs OBS.exe
[0BE5F20C15519E2ABD71DB9B8D41AB08] [28/07/2017] (.HP Inc..) - C:\Program Files (x86)\HP\HP JumpStart Bridge\HPJumpStartBridge.exe
[0C15BE4A15BB0903C901B1D6C265302F] [02/12/2020] (.Google LLC.) - C:\Program Files\Google\Chrome\Application\87.0.4280.88\elevation_service.exe
[0C15BE4A15BB0903C901B1D6C265302F] [02/12/2020] (.Google LLC.) - C:\Program Files\Google\Chrome\Application\chrome.exe
[0C15BE4A15BB0903C901B1D6C265302F] [03/12/2020] (.Google LLC.) - C:\Program Files\Google\Chrome\Application\87.0.4280.88\Installer\chrmstp.exe
[0C15BE4A15BB0903C901B1D6C265302F] [03/12/2020] (.Google LLC.) - C:\Program Files\Google\Chrome\Application\87.0.4280.88\Installer\setup.exe
[0C4F13796AF8A01FC4EC4C83A621C557] [25/01/2020] (.Logitech Inc.) - C:\Program Files\LGHUB/lghub_updater.exe
[0C4F13796AF8A01FC4EC4C83A621C557] [25/01/2020] (.Logitech Inc.) - C:\Program Files\LGHUB\lghub.exe
[0C4F13796AF8A01FC4EC4C83A621C557] [25/01/2020] (.Logitech Inc.) - C:\program files\lghub\lghub_agent.exe
[0C834A23A8F6DA243E24A688741CCB0F] [17/12/2019] (.HP Inc..) - C:\Program Files (x86)\HP\HP Support Framework\Resources\HPNetworkCheck\HPNetworkCheckPl
[0C94D893919168382DEABA62201C7A05] [28/03/2020] (.New World Interactive LLC.) - D:\SteamLibrary\steamapps\common\sandstorm\Insurgency.exe  =>.Not veri
[0C94D893919168382DEABA62201C7A05] [28/03/2020] (.New World Interactive LLC.) - D:\steamlibrary\steamapps\common\sandstorm\insurgency\binaries\win64\i
[0CEFAB1F7C07370C77DFB61C3CA4F5F0] [05/03/2018] (.Adobe Systems Incorporated.) - C:\Program Files (x86)\Common Files\Adobe\CoreSyncExtension\CoreSync_
[0D2CACCD3E9EEC06738410BA31BF6595] [00/00/0000] (.Adobe Inc..) - C:\Windows\System32\FlashPlayerApp.exe
[0D2CACCD3E9EEC06738410BA31BF6595] [03/12/2020] (.Adobe Inc..) - C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe
[0D2CACCD3E9EEC06738410BA31BF6595] [03/12/2020] (.Adobe Inc..) - C:\Windows\SysWOW64\Macromed\Flash\FlashUtil32_32_0_0_453_Plugin.exe
[0D7026D55EB74EF39F9E3FF81EE1DFE7] [20/12/2019] (.Apowersoft Ltd.) - C:\Program Files (x86)\Apowersoft\ApowerMirror\ApowerMirror.exe
[0D7026D55EB74EF39F9E3FF81EE1DFE7] [26/12/2019] (.Apowersoft Ltd.) - C:\Program Files (x86)\Apowersoft\ApowerMirror\unins000.exe
[0D7026D55EB74EF39F9E3FF81EE1DFE7] [27/05/2020] (.Apowersoft Ltd.) - C:\Program Files (x86)\Apowersoft\ApowerCompress\ApowerCompress.exe
[0DAE46486B3CF0B6DF5F76680285EB28] [16/03/2020] (.SAND STUDIO CORPORATION LIMITED.) - C:\Program Files (x86)\AirDroid\AirDroid.exe  =>.Not verified
```

```
[0DAE46486B3CF0B6DF5F76680285EB28] [16/03/2020] (.SAND STUDIO CORPORATION LIMITED.) - C:\Program Files (x86)\AirDroid\Launcher.exe  =>.Not verified
[0DC038E478186B672A3A7B21BA85DC62] [20/08/2018] (.Hugh Bailey.) - C:\Program Files\obs-studio\bin\64bit\obs64.exe
[0DDEB53F957337FBEAF98C4A615B149D] [02/12/2020] (.Mozilla Corporation.) - C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe
[0DDEB53F957337FBEAF98C4A615B149D] [02/12/2020] (.Mozilla Corporation.) - C:\Program Files\Firefox Developer Edition\crashreporter.exe
[0DDEB53F957337FBEAF98C4A615B149D] [02/12/2020] (.Mozilla Corporation.) - C:\Program Files\Firefox Developer Edition\firefox.exe
[0DDEB53F957337FBEAF98C4A615B149D] [02/12/2020] (.Mozilla Corporation.) - C:\Program Files\Firefox Developer Edition\uninstall\helper.exe
[0DDEB53F957337FBEAF98C4A615B149D] [02/12/2020] (.Mozilla Corporation.) - C:\Program Files\Mozilla Firefox\firefox.exe
[0DDEB53F957337FBEAF98C4A615B149D] [02/12/2020] (.Mozilla Corporation.) - C:\Program Files\Mozilla Firefox\uninstall\helper.exe
[0EBBFEB6F50A63A4585A1FE72483D97F] [14/06/2020] (.HP Inc..) - C:\Windows\System32\DriverStore\FileRepository\hpomencustomcapcomp.inf_amd64_b6eaa96b215
[0EBBFEB6F50A63A4585A1FE72483D97F] [18/10/2020] (.HP Inc..) - C:\Windows\System32\DriverStore\FileRepository\hpcustomcapcomp.inf_amd64_66856cbf5000451
[0EBBFEB6F50A63A4585A1FE72483D97F] [18/10/2020] (.HP Inc..) - C:\Windows\System32\DriverStore\FileRepository\hpcustomcapcomp.inf_amd64_66856cbf5000451
[0EBBFEB6F50A63A4585A1FE72483D97F] [18/10/2020] (.HP Inc..) - C:\Windows\System32\DriverStore\FileRepository\hpcustomcapcomp.inf_amd64_66856cbf5000451
[0EBBFEB6F50A63A4585A1FE72483D97F] [21/10/2020] (.HP Inc..) - C:\Program Files\WindowsApps\AD2F1837.OMENCommandCenter_11.0.11.0_x64__v10z8vjag6ke6\wir
[0EE3F1C8F451CBF21203341A53F23E71] [06/09/2020] (.Adobe Inc..) - C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe
[0EE3F1C8F451CBF21203341A53F23E71] [22/10/2020] (.Adobe Inc..) - C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
[0F05AE21CDC17B9F3CF09D7BFC659BA3] [18/09/2020] (.Glarysoft LTD.) - C:\Program Files (x86)\Glary Utilities 5\Integrator.exe
[0F05AE21CDC17B9F3CF09D7BFC659BA3] [18/09/2020] (.Glarysoft LTD.) - C:\Program Files (x86)\Glary Utilities 5\StartupManager.exe
[0F05AE21CDC17B9F3CF09D7BFC659BA3] [18/09/2020] (.Glarysoft LTD.) - C:\Program Files (x86)\Glary Utilities 5\uninst.exe
[0F05AE21CDC17B9F3CF09D7BFC659BA3] [18/09/2020] (.Glarysoft LTD.) - C:\Program Files (x86)\Glary Utilities 5\x64\ContextHandler.dll
[0F9D91C6ABA86F4E54CBB9EF57E68346] [20/06/2019] (.Kaspersky Lab.) - D:\Kaspersky Internet & Total Security 2019 v19.0.0.1088 + Crack {B4tman}\Kaspersk
[0FA41A17EFFB667DA065C0DA] [27/02/2018] (.Sony Interactive Entertainment Inc..) - C:\Program Files (x86)\Sony\PS4 Remote Play\RemotePlay.exe
[0FA5B80428F4624CF9672211E1956FBE] [04/06/2020] (.VideoLAN.) - C:\Program Files\VideoLAN\VLC\vlc.exe
[0FFE515D4E13FCE2E02867B89A57A7AA] [22/06/2020] (.Nox Limited.) - C:\Program Files (x86)\Bignox\BigNoxVM\RT\NoxVMHandle.exe
[0FFE515D4E13FCE2E02867B89A57A7AA] [22/06/2020] (.Nox Limited.) - D:\Program Files\Nox\bin\MultiPlayerManager.exe
[0FFE515D4E13FCE2E02867B89A57A7AA] [22/06/2020] (.Nox Limited.) - D:\Program Files\Nox\bin\Nox.exe
[0FFE515D4E13FCE2E02867B89A57A7AA] [22/06/2020] (.Nox Limited.) - D:\Program Files\Nox\bin\Nox_unload.exe
[11214584BFDF9CB01A1BC50672A7EE9B881C] [20/11/2018] (.GIANTS Software GmbH.) - D:\games\farming simulator 19\dedicatedserver.exe
[11217744F4734203086E7A2B2312FE1225D5] [16/02/2019] (.Martin Malik - REALiX.) - C:\Windows\SysWOW64\drivers\HWiNFO64A.SYS
[11218B069CCBEDB332B1EC4560BEE4BF2C14] [19/11/2018] (.Noriyuki Miyazaki.) - C:\Program Files (x86)\CrystalDiskInfo\DiskInfo32.exe
[11218B069CCBEDB332B1EC4560BEE4BF2C14] [25/10/2017] (.Noriyuki Miyazaki.) - C:\Program Files\CrystalDiskMark5\DiskMark64.exe
[1121ACEBD596BFF219C4231915D84B0B0549] [23/01/2019] (.Samsung Electronics Co., Ltd..) - C:\WINDOWS\System32\drivers\secnvme.sys
[1121ACEBD596BFF219C4231915D84B0B0549] [23/01/2019] (.Samsung Electronics Co., Ltd..) - C:\WINDOWS\System32\drivers\secnvmeF.sys
[1121E1CE57747D3AA0E2D8A055EE1FA5696D] [22/02/2017] (.GOLD CLICK LIMITED.) - C:\Program Files (x86)\ProxyGate\MainService.exe  =>.SUP.GoldClick
[1121E1CE57747D3AA0E2D8A055EE1FA5696D] [22/02/2017] (.GOLD CLICK LIMITED.) - C:\Program Files (x86)\ProxyGate\PGChk.exe  =>.SUP.GoldClick
[1121E1CE57747D3AA0E2D8A055EE1FA5696D] [22/08/2016] (.GOLD CLICK LIMITED.) - C:\Program Files (x86)\ProxyGate\Cloud.exe  =>.SUP.GoldClick
[1121F611BAE8352E9201C65095879D7BDAB1] [19/05/2013] (.Bruce James.) - C:\WINDOWS\System32\drivers\ScpVBus.sys
[1402AEEF0D31BE743E73F6A7A960C4F4] [01/03/2013] (.Riverbed Technology, Inc..) - C:\Program Files (x86)\WinPcap\rpcapd.exe
[1402AEEF0D31BE743E73F6A7A960C4F4] [01/03/2013] (.Riverbed Technology, Inc..) - C:\WINDOWS\System32\drivers\npf.sys
[18A7A453386A0FEFF304B137BDB60FC7] [23/01/2019] (.Challenger Backup Solutions, LLC.) - C:\WINDOWS\System32\drivers\FlashBoot.sys
[19EA4DAF089570861408E9F05EFD9B89] [22/06/2020] (.Power Software Limited.) - C:\Program Files\PowerISO\PowerISO.exe  =>.Not verified
[19EA4DAF089570861408E9F05EFD9B89] [22/06/2020] (.Power Software Limited.) - C:\Program Files\PowerISO\PWRISOSH.DLL  =>.Not verified
[19EA4DAF089570861408E9F05EFD9B89] [22/06/2020] (.Power Software Limited.) - C:\Program Files\PowerISO\PWRISOVM.EXE  =>.Not verified
[19FE2B7721886C7BCAC1364C90CD7FA9] [23/01/2019] (.Synaptics Incorporated.) - C:\WINDOWS\System32\DRIVERS\Smb_driver_Intel.sys
[1A9706FDE692D88CA99B822D] [07/03/2019] (.Cheat Engine.) - C:\Program Files (x86)\Cheat Engine 6.8.3\unins000.exe
[1A9706FDE692D88CA99B822D] [25/03/2019] (.Cheat Engine.) - C:\Program Files\Cheat Engine 7.0\Cheat Engine.exe
[1C71DEFE3284E66D55131E70] [24/07/2018] (.TEFINCOM S.A..) - C:\WINDOWS\System32\drivers\tapnordvpn.sys
[227EFDF22825BA270530FB09D52B32F8] [07/06/2017] (.Power Software Limited.) - C:\WINDOWS\System32\drivers\scdemu.sys
[228A24C9151537B7BA32F5A98EA053FD] [23/02/2019] (.Magic Hills Pty Ltd.) - C:\Program Files (x86)\Amazing Audio Player\amazingaudioplayer.exe
[234175E3D1A23EF8ACB50245] [27/03/2020] (.EasyAntiCheat Oy.) - C:\Program Files (x86)\EasyAntiCheat\EasyAntiCheat.exe
[234175E3D1A23EF8ACB50245] [27/03/2020] (.EasyAntiCheat Oy.) - D:\SteamLibrary\steamapps\common\sandstorm\InsurgencyEAC.exe
[26181CEDF2C113E16AC74820DF7A38A3] [16/01/2017] (.Samsung Electronics CO., LTD..) - C:\Program Files\Samsung\USB Drivers\27_ssconn\conn\ss_conn_servic
[26181CEDF2C113E16AC74820DF7A38A3] [16/01/2017] (.Samsung Electronics CO., LTD..) - C:\Program Files\Samsung\USB Drivers\Uninstall.exe
[26181CEDF2C113E16AC74820DF7A38A3] [16/01/2017] (.Samsung Electronics CO., LTD..) - C:\WINDOWS\System32\DRIVERS\ssudbus.sys
[26181CEDF2C113E16AC74820DF7A38A3] [16/01/2017] (.Samsung Electronics CO., LTD..) - C:\WINDOWS\System32\DRIVERS\ssudmdm.sys
[28736D0D296789512BAC66CCE86C4A00] [01/09/2017] (.CHENGDU AOMEI Tech Co., Ltd..) - C:\WINDOWS\system32\amwrtdrv.sys
[28736D0D296789512BAC66CCE86C4A00] [21/12/2016] (.CHENGDU AOMEI Tech Co., Ltd..) - C:\WINDOWS\System32\ambakdrv.sys
[28736D0D296789512BAC66CCE86C4A00] [21/12/2016] (.CHENGDU AOMEI Tech Co., Ltd..) - C:\WINDOWS\system32\ammntdrv.sys
[28736D0D296789512BAC66CCE86C4A00] [22/01/2019] (.CHENGDU AOMEI Tech Co., Ltd..) - C:\Program Files (x86)\AOMEI Backupper\ABService.exe
[28736D0D296789512BAC66CCE86C4A00] [22/01/2019] (.CHENGDU AOMEI Tech Co., Ltd..) - C:\Program Files (x86)\AOMEI Backupper\Backupper.exe
[290C2B6FBB3B4B72EA719F765D1E0782] [26/01/2019] (.Cyotek Ltd.) - C:\Program Files (x86)\Cyotek\WebCopy\cyowcopy.exe  =>.Not verified
[2B20EB3380792AB011F662C064FDB473] [12/08/2015] (.Apple Inc..) - C:\Program Files\Bonjour\mDNSResponder.exe
[2C80892E0115B0B77AA3594B9A733953] [10/11/2010] (.Realtek Semiconductor Corp.) - C:\Program Files (x86)\InstallShield Installation Information\{A51074
[2C80892E0115B0B77AA3594B9A733953] [20/09/2016] (.Realtek Semiconductor Corp.) - C:\Program Files (x86)\InstallShield Installation Information\{9D3D8C
[30AA59DD718CFBDE163AB821] [21/11/2020] (.McAfee, LLC.) - C:\Program Files\McAfee\WebAdvisor\ServiceHost.exe
[30AA59DD718CFBDE163AB821] [21/11/2020] (.McAfee, LLC.) - C:\Program Files\McAfee\WebAdvisor\uihost.exe
[30AA59DD718CFBDE163AB821] [21/11/2020] (.McAfee, LLC.) - C:\Program Files\McAfee\WebAdvisor\Uninstaller.exe
[30AA59DD718CFBDE163AB821] [21/11/2020] (.McAfee, LLC.) - C:\Program Files\McAfee\WebAdvisor\x64\IEPlugin.dll
[330000017BB47778D9105DF03500000000017B] [18/11/2020] (.Skype Software Sarl.) - C:\Program Files\WindowsApps\Microsoft.SkypeApp_15.66.77.0_x86__kzf8q
[330000B90B047705E529835D1400020000B90B] [18/05/2016] (.Intel(R) Corporation.) - C:\Program Files\Intel\IntelSGXPSW\bin\x64\Release\aesm_service.exe
[330000B97FAEF583F53CC47FCD00020000B97F] [24/05/2017] (.Intel(R) Rapid Storage Technology.) - C:\WINDOWS\System32\drivers\iaStorA.sys
[330000B97FAEF583F53CC47FCD00020000B97F] [24/05/2017] (.Intel(R) Rapid Storage Technology.) - C:\WINDOWS\System32\drivers\iaStorAfs.sys
[3991D810FB336E5A7D8C2822] [01/08/2019] (.Nota Inc..) - C:\Program Files (x86)\Gyazo\GyazoGIF.exe
[3991D810FB336E5A7D8C2822] [01/08/2019] (.Nota Inc..) - C:\Program Files (x86)\Gyazo\GyazoReplay.exe
[3991D810FB336E5A7D8C2822] [01/08/2019] (.Nota Inc..) - C:\Program Files (x86)\Gyazo\Gyazowin.exe
[3991D810FB336E5A7D8C2822] [05/08/2019] (.Nota Inc..) - C:\Program Files (x86)\Gyazo\unins000.exe
[3A23E70970D46A6F5E1A5807C4C5E653] [09/09/2020] (.Electronic Arts, Inc..) - D:\Origin\FIFA 20\FIFASetup\fifaconfig.exe
[3A23E70970D46A6F5E1A5807C4C5E653] [27/07/2020] (.Electronic Arts, Inc..) - D:\Origin\FIFA 20\FIFA20.exe
[3C19EA87B1E9179F] [25/06/2020] (.Paradox Interactive AB (publ).) - D:\SteamLibrary\steamapps\common\Prison Architect\Launcher\dowser.exe
[3CBC877B99BA185889A4368A9C6938D9] [14/10/2020] (.BOHEMIA INTERACTIVE a.s..) - D:\steamlibrary\steamapps\common\arma 3\arma3_x64.exe
[3CBC877B99BA185889A4368A9C6938D9] [14/10/2020] (.BOHEMIA INTERACTIVE a.s..) - D:\SteamLibrary\steamapps\common\Arma 3\arma3launcher.exe
[3CBC877B99BA185889A4368A9C6938D9] [24/11/2020] (.BOHEMIA INTERACTIVE a.s..) - D:\SteamLibrary\steamapps\common\Arma 3 Tools\AddonBuilder\AddonBuilder
[3CBC877B99BA185889A4368A9C6938D9] [24/11/2020] (.BOHEMIA INTERACTIVE a.s..) - D:\SteamLibrary\steamapps\common\Arma 3 Tools\Arma3Tools.exe
[3CBC877B99BA185889A4368A9C6938D9] [24/11/2020] (.BOHEMIA INTERACTIVE a.s..) - D:\SteamLibrary\steamapps\common\Arma 3 Tools\Publisher\Publisher.exe
[3CBC877B99BA185889A4368A9C6938D9] [24/11/2020] (.BOHEMIA INTERACTIVE a.s..) - D:\SteamLibrary\steamapps\common\Arma 3 Tools\starter.exe
[3D3C455A5C7B7B2666915EB21857D7EA] [02/05/2018] (.Piriform Ltd.) - C:\Program Files\Speccy\Speccy64.exe
[3D3C455A5C7B7B2666915EB21857D7EA] [02/05/2018] (.Piriform Ltd.) - C:\Program Files\Speccy\uninst.exe
[3D542418AC4FE319D034B2185B5E5738] [09/01/2019] (.JetBrains s.r.o..) - C:\Program Files\JetBrains\IntelliJ IDEA Community Edition 2018.3.3\bin\idea64
[3DFEDC4BE9CA7167974E822F50867BB1] [24/04/2017] (.ProXoft L.L.C..) - C:\Program Files (x86)\ProXoft\Binary Viewer\Binary Viewer.exe  =>.Not verified
[4034F5C0880036DE88FD5DEF726BF594] [23/11/2020] (.Electronic Arts, Inc..) - C:\Program Files (x86)\Origin\Origin.exe
[4034F5C0880036DE88FD5DEF726BF594] [23/11/2020] (.Electronic Arts, Inc..) - C:\Program Files (x86)\Origin\OriginClientService.exe
[4034F5C0880036DE88FD5DEF726BF594] [23/11/2020] (.Electronic Arts, Inc..) - C:\Program Files (x86)\Origin\OriginUninstall.exe
[4034F5C0880036DE88FD5DEF726BF594] [23/11/2020] (.Electronic Arts, Inc..) - C:\Program Files (x86)\Origin\OriginWebHelperService.exe
[4038604836B4D4BC4450656C0E6D3D0F] [24/07/2018] (.WDKTestCert cm359,131641702659254692.) - C:\WINDOWS\System32\DRIVERS\CMUSBDAC.sys  =>.Not verified
[411239DA46A29C98B8A15077] [23/03/2020] (.Cheat Engine.) - C:\Program Files\Cheat Engine 7.0\unins000.exe
[4161A3C9C03DBAA06CC04C1FF8EF3172] [03/12/2018] (.General Workings Inc (Streamlabs).) - C:\Program Files\Streamlabs OBS\Uninstall Streamlabs OBS.exe
[42E8AE1425ABF510A0EFCDE3844200CF] [11/03/2016] (.Xiaomi Technology Inc.) - C:\Users\couli\AppData\Local\MiPhoneManager\main\MiPCSuite.exe
[42E8AE1425ABF510A0EFCDE3844200CF] [11/03/2016] (.Xiaomi Technology Inc.) - C:\Users\couli\AppData\Local\MiPhoneManager\main\MiPhoneHelper.exe
[42E8AE1425ABF510A0EFCDE3844200CF] [11/03/2016] (.Xiaomi Technology Inc.) - C:\Users\couli\AppData\Local\MiPhoneManager\main\uninstall.exe
[437FF9CB5A2648EB522CA10E087B4AB4] [25/11/2020] (.Stichting Blender Foundation.) - D:\SteamLibrary\steamapps\common\Blender\blender.exe  =>.Not verifi
[4451AD3717CFA22371FFBC07DF13E65D] [21/11/2018] (.VMware, Inc..) - C:\WINDOWS\System32\DRIVERS\vmkbd.sys
[4451AD3717CFA22371FFBC07DF13E65D] [22/06/2018] (.VMware, Inc..) - C:\WINDOWS\System32\drivers\vmci.sys
[459F81C4546FDEFCFF2F1A1105A6EFBD] [03/11/2011] (.Sonic Solutions.) - C:\WINDOWS\System32\Drivers\PxHlpa64.sys
[459F81C4546FDEFCFF2F1A1105A6EFBD] [17/10/2011] (.Sonic Solutions.) - C:\WINDOWS\System32\drivers\cdr4_xp.sys
[459F81C4546FDEFCFF2F1A1105A6EFBD] [17/10/2011] (.Sonic Solutions.) - C:\WINDOWS\System32\drivers\cdralw2k.sys
```

```
[46D86FF4A6092EECB3918FA9] [15/01/2018] (.Mega Limited.) - C:\ProgramData\MEGAsync\uninst.exe
[46D86FF4A6092EECB3918FA9] [23/09/2018] (.Mega Limited.) - C:\ProgramData\MEGAsync\MEGAsync.exe
[47A513BFC1DCE987473C139CDE53F6BA] [08/12/2019] (.WDKTestCert sqa,131523902232810150.) - C:\WINDOWS\System32\drivers\logi_joy_vir_hid.sys
[4EA7A05936A3D21C8E85AFF6E99C0EFC] [12/09/2019] (.Shanghai Microvirt Software Technology Co., Ltd..) - C:\Program Files (x86)\Microvirt\MEmu\MemuServi
[4EA7A05936A3D21C8E85AFF6E99C0EFC] [14/02/2019] (.Shanghai Microvirt Software Technology Co., Ltd..) - C:\Program Files (x86)\Microvirt\MEmuHyperv\MEm
[4EA7A05936A3D21C8E85AFF6E99C0EFC] [21/09/2019] (.Shanghai Microvirt Software Technology Co., Ltd..) - C:\WINDOWS\System32\DRIVERS\MEmuDrv.sys
[4FBE0A02426EBD20C26244B5ECA652A3] [19/03/2019] (.NVIDIA Corporation.) - C:\WINDOWS\System32\drivers\nvvad64v.sys
[51029B3B9CB48FA076FA2DA87A91DB42] [06/12/2018] (.Epic Games Inc..) - C:\ProgramData\Package Cache\{4e242cc8-5e3c-4b08-9d55-dbc62ddd1208}\UE4PrereqSet
[51029B3B9CB48FA076FA2DA87A91DB42] [22/02/2020] (.Epic Games Inc..) - C:\Program Files (x86)\Epic Games\Launcher\Portal\Binaries\Win32\EpicGamesLaunch
[51029B3B9CB48FA076FA2DA87A91DB42] [22/02/2020] (.Epic Games Inc..) - C:\Program Files (x86)\Epic Games\Launcher\Portal\Binaries\Win64\EpicGamesLaunch
[54CCA67C86AD2DDFBB5CE4D41DC7A3E2] [24/08/2018] (.Epic Games Inc..) - C:\ProgramData\Package Cache\{c6c5a357-c7ca-4a5f-9789-3bb1af579253}\LauncherPrer
[5600000071934283BFC7A54FBD000000000071] [23/08/2018] (.Intel(R) Software and Firmware Products.) - C:\ProgramData\Package Cache\{314d4c01-f54b-4125-a
[56000001475EA46CCAEF0B7481000000000147] [14/09/2018] (.Intel(R) Trust Services.) - C:\ProgramData\Package Cache\{df682aff-4294-4ad1-aaa7-276931d5781f
[5600000171757376CD78AD000C9A000000000175] [03/08/2020] (.Intel(R) Embedded Subsystems and IP Blocks Group.) - C:\WINDOWS\System32\drivers\ICCWDT.sys
[5600000171757376CD78AD000C9A000000000175] [03/12/2017] (.Intel(R) Embedded Subsystems and IP Blocks Group.) - C:\Program Files (x86)\Intel\Intel(R) Mar
[5600000171757376CD78AD000C9A000000000175] [06/05/2018] (.Intel(R) Embedded Subsystems and IP Blocks Group.) - C:\WINDOWS\System32\drivers\TeeDriverW8x6
[5600000171757376CD78AD000C9A000000000175] [15/03/2018] (.Intel(R) Embedded Subsystems and IP Blocks Group.) - C:\ProgramData\Intel\Package Cache\{1CEAC
[560000082B1E36C56B00276A8A00000000082B] [16/08/2020] (.Intel(R) Embedded Subsystems and IP Blocks Group.) - C:\Windows\System32\DriverStore\FileRepos
[560000082B1E36C56B00276A8A00000000082B] [17/09/2020] (.Intel(R) Embedded Subsystems and IP Blocks Group.) - C:\Windows\System32\DriverStore\FileRepos
[560000088689EFB89169C165B1000000000886] [22/04/2020] (.Intel(R) Trust Services.) - C:\Windows\System32\DriverStore\FileRepository\iclsclient.inf_amd6
[560000088689EFB89169C165B1000000000886] [22/04/2020] (.Intel(R) Trust Services.) - C:\Windows\System32\DriverStore\FileRepository\iclsclient.inf_amd6
[56F0265C641B51A2544F9ED1DA73265F] [23/11/2020] (.SCS Software s.r.o..) - C:\Program Files (x86)\Steam\steamapps\common\Euro Truck Simulator 2\bin\wir
[56F0265C641B51A2544F9ED1DA73265F] [23/11/2020] (.SCS Software s.r.o..) - C:\Program Files (x86)\Steam\steamapps\common\Euro Truck Simulator 2\bin\wir
[586949448B11998044814E89345A337F] [10/05/2018] (.WDKTestCert build,131474841775766162.) - C:\WINDOWS\System32\drivers\AppleLowerFilter.sys
[59040957F20843302BA52AA1F6ABCEEF] [02/11/2018] (.VMware, Inc..) - C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe
[59040957F20843302BA52AA1F6ABCEEF] [02/11/2018] (.VMware, Inc..) - C:\WINDOWS\System32\DRIVERS\hcmon.sys
[59040957F20843302BA52AA1F6ABCEEF] [21/11/2018] (.VMware, Inc..) - C:\Program Files (x86)\VMware\VMware Workstation\7za.exe
[59040957F20843302BA52AA1F6ABCEEF] [21/11/2018] (.VMware, Inc..) - C:\Program Files (x86)\VMware\VMware Workstation\vmware.exe
[59040957F20843302BA52AA1F6ABCEEF] [21/11/2018] (.VMware, Inc..) - C:\Program Files (x86)\VMware\VMware Workstation\vmware-authd.exe
[59040957F20843302BA52AA1F6ABCEEF] [21/11/2018] (.VMware, Inc..) - C:\Program Files (x86)\VMware\VMware Workstation\vmware-hostd.exe
[59040957F20843302BA52AA1F6ABCEEF] [21/11/2018] (.VMware, Inc..) - C:\Program Files (x86)\VMware\VMware Workstation\vmware-tray.exe
[59040957F20843302BA52AA1F6ABCEEF] [21/11/2018] (.VMware, Inc..) - C:\Program Files (x86)\VMware\VMware Workstation\x64\vmdkShellExt64.dll
[59040957F20843302BA52AA1F6ABCEEF] [21/11/2018] (.VMware, Inc..) - C:\WINDOWS\System32\drivers\vmnet.sys
[59040957F20843302BA52AA1F6ABCEEF] [21/11/2018] (.VMware, Inc..) - C:\WINDOWS\System32\DRIVERS\vmnetadapter.sys
[59040957F20843302BA52AA1F6ABCEEF] [21/11/2018] (.VMware, Inc..) - C:\WINDOWS\System32\DRIVERS\vmnetuserif.sys
[59040957F20843302BA52AA1F6ABCEEF] [21/11/2018] (.VMware, Inc..) - C:\WINDOWS\System32\DRIVERS\vmx86.sys
[59040957F20843302BA52AA1F6ABCEEF] [21/11/2018] (.VMware, Inc..) - C:\Windows\SysWOW64\vmnat.exe
[59040957F20843302BA52AA1F6ABCEEF] [21/11/2018] (.VMware, Inc..) - C:\Windows\SysWOW64\vmnetdhcp.exe
[59040957F20843302BA52AA1F6ABCEEF] [22/06/2018] (.VMware, Inc..) - C:\WINDOWS\System32\DRIVERS\vsock.sys
[59040957F20843302BA52AA1F6ABCEEF] [28/02/2018] (.VMware, Inc..) - C:\Windows\SysWOW64\drivers\vstor2-x64.sys
[597E4E45CBC115BBA6402602E89CBF45] [01/04/2019] (.Oracle America, Inc..) - C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe
[597E4E45CBC115BBA6402602E89CBF45] [16/06/2019] (.Oracle America, Inc..) - C:\Program Files\Java\jre1.8.0_211\bin\jp2ssv.dll
[597E4E45CBC115BBA6402602E89CBF45] [16/06/2019] (.Oracle America, Inc..) - C:\Program Files\Java\jre1.8.0_211\bin\ssv.dll
[597E4E45CBC115BBA6402602E89CBF45] [20/09/2019] (.Oracle America, Inc..) - G:\wamp64\bin\mysql\mysql8.0.18\bin\mysqld.exe
[59C83F99C96761FA39E5C07FDA2AC755] [04/06/2019] (.SOLVUSOFT CORPORATION.) - C:\Program Files\File Magic\FileMagic.exe  =>SUP.Optional.Solvusoft
[59C83F99C96761FA39E5C07FDA2AC755] [28/03/2020] (.SOLVUSOFT CORPORATION.) - C:\Program Files\File Magic\unins000.exe  =>SUP.Optional.Solvusoft
[5CCAA82369A26AEE30D017616B1CEB69] [12/09/2017] (.Wondershare Technology Co.,Ltd.) - C:\Program Files (x86)\Common Files\Wondershare\Wondershare Helpe
[5D38D8BD64455068C2D1C74088C5E28A] [06/01/2020] (.Tim Kosse.) - C:\Program Files\FileZilla FTP Client\filezilla.exe
[5F11DE21CBDC4A392F6EDDCD1F11530A] [23/10/2018] (.Focus Home Interactive.) - G:\Games\Spintires MudRunner American Wilds\MudRunner.exe
[61909F3F8B9706C042B08547A3D76E81] [28/06/2017] (.SEIKO EPSON CORPORATION.) - C:\Program Files (x86)\EPSON\MyEpson Portal\mepService.exe
[6207AD04EFA2FD166CC7D986887E4B18] [02/08/2017] (.HP Inc..) - C:\ProgramData\Package Cache\{54da9769-2364-4bd3-8139-6400500778b3}\HPEPrintAppSetup.exe
[62E745E92165213C971F5C490AEA12A5] [07/11/2020] (.NVIDIA Corporation.) - C:\Program Files\NVIDIA Corporation\Display.NvContainer\NVDisplay.Container.e
[62E745E92165213C971F5C490AEA12A5] [07/11/2020] (.NVIDIA Corporation.) - C:\WINDOWS\System32\drivers\nvhda64v.sys
[62E745E92165213C971F5C490AEA12A5] [07/11/2020] (.NVIDIA Corporation.) - C:\WINDOWS\System32\drivers\nvlddmkm.sys
[62E745E92165213C971F5C490AEA12A5] [07/11/2020] (.NVIDIA Corporation.) - C:\Windows\System32\DriverStore\FileRepository\nvhdci.inf_amd64_cabc1251ab233
[62E745E92165213C971F5C490AEA12A5] [17/10/2020] (.NVIDIA Corporation.) - C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe
[62E745E92165213C971F5C490AEA12A5] [19/10/2020] (.NVIDIA Corporation.) - C:\Program Files (x86)\NVIDIA Corporation\NvNode\NVIDIA Web Helper.exe
[62E745E92165213C971F5C490AEA12A5] [19/10/2020] (.NVIDIA Corporation.) - C:\Program Files\NVIDIA Corporation\FrameViewSDK\nvfvsdksvc_x64.exe
[62E745E92165213C971F5C490AEA12A5] [20/10/2020] (.NVIDIA Corporation.) - C:\Program Files\NVIDIA Corporation\NVIDIA GeForce Experience\NVIDIA Share.ex
[62E745E92165213C971F5C490AEA12A5] [20/10/2020] (.NVIDIA Corporation.) - C:\Program Files\NVIDIA Corporation\ShadowPlay\nvsphelper64.exe
[62E745E92165213C971F5C490AEA12A5] [21/08/2020] (.NVIDIA Corporation.) - C:\Program Files\NVIDIA Corporation\NvStreamSrv\nvstreamer.exe
[63C924EF6594B5566CDC0B18350FA6D1] [17/05/2020] (.AVG Technologies CZ, s.r.o..) - C:\WINDOWS\System32\DRIVERS\SWDUMon.sys
[65D365A24EE7E137105BBAC2335816D8] [14/01/2019] (.Oracle Corporation.) - C:\Program Files\Oracle\VirtualBox\VBoxSDS.exe
[65D365A24EE7E137105BBAC2335816D8] [14/01/2019] (.Oracle Corporation.) - C:\WINDOWS\System32\DRIVERS\VBoxDrv.sys
[65D365A24EE7E137105BBAC2335816D8] [14/01/2019] (.Oracle Corporation.) - C:\WINDOWS\System32\DRIVERS\VBoxNetAdp6.sys
[65D365A24EE7E137105BBAC2335816D8] [14/01/2019] (.Oracle Corporation.) - C:\WINDOWS\System32\DRIVERS\VBoxNetLwf.sys
[65D365A24EE7E137105BBAC2335816D8] [14/01/2019] (.Oracle Corporation.) - C:\WINDOWS\System32\DRIVERS\VBoxUSBMon.sys
[6D4606FAF6D69E1D063390B38AFF8F82] [21/08/2017] (.Tomasz Moń.) - C:\WINDOWS\System32\DRIVERS\USBPcap.sys
[6D9B7FD9A35FF6D4A9BAEDA62F24BBFE] [20/01/2019] (.Glarysoft LTD.) - C:\WINDOWS\System32\drivers\GUBootStartup.sys
[6E27D4BA14DCD51B36D8E33F664D9271] [09/03/2020] (.Ambiera e.U..) - D:\SteamLibrary\steamapps\common\Smart City Plan\game.exe  =>.Not verified
[6F13BCD50963D2F309439E37FD459C7C] [15/05/2020] (.BitTorrent Inc.) - C:\Users\couli\AppData\Roaming\uTorrent\uTorrent.exe  =>BitTorrent (P2P)
[715F924E283F98915DBF1A5C4F38C658] [14/08/2018] (.Tomasz Moń.) - C:\Program Files\USBPcap\Uninstall.exe
[71E68684F7A885A24ABF921CBBF4E0C3] [04/03/2020] (.NVIDIA Corporation.) - C:\WINDOWS\System32\drivers\NvModuleTracker.sys
[71E68684F7A885A24ABF921CBBF4E0C3] [11/03/2020] (.NVIDIA Corporation.) - C:\WINDOWS\System32\drivers\nvvhci.sys
[722A666775DC480EA2B841413D7B8765] [22/02/2020] (.Ubisoft Entertainment Sweden AB.) - C:\Program Files (x86)\Ubisoft\Ubisoft Game Launcher\Uninstall.e
[722A666775DC480EA2B841413D7B8765] [22/02/2020] (.Ubisoft Entertainment Sweden AB.) - C:\Program Files (x86)\Ubisoft\Ubisoft Game Launcher\upc.exe
[722A666775DC480EA2B841413D7B8765] [22/02/2020] (.Ubisoft Entertainment Sweden AB.) - C:\Program Files (x86)\Ubisoft\Ubisoft Game Launcher\Uplay.exe
[7429B2CD7A4D91C3C6AF13C4E14C7078] [01/11/2018] (.SEIKO EPSON CORPORATION.) - C:\Program Files (x86)\EPSON\MyEpson Portal\mep.exe
[7524DBFE413001B3B345768A4F60DF46] [06/01/2015] (.SEIKO EPSON Corporation.) - C:\WINDOWS\system32\spool\DRIVERS\x64\3\E_YINSIXE.EXE
[754020F5FC0992BA4DAD6BF986E5C1D7] [30/11/2019] (.WDKTestCert VSAuto,131800073559665678.) - C:\WINDOWS\System32\drivers\RtkBtfilter.sys
[76101A6757EFD8186742057C6A6ACAA4] [20/08/2018] (.SEIKO EPSON CORPORATION.) - C:\Program Files (x86)\EPSON\MyEpson Portal\64DriverLoad.exe
[7625A59EA40A7E7B913F910723328E26] [25/06/2020] (.win.rar GmbH.) - C:\Program Files (x86)\WinRAR\Rar.exe
[7625A59EA40A7E7B913F910723328E26] [25/06/2020] (.win.rar GmbH.) - C:\Program Files (x86)\WinRAR\RarExt64.dll
[7625A59EA40A7E7B913F910723328E26] [25/06/2020] (.win.rar GmbH.) - C:\Program Files (x86)\WinRAR\uninstall.exe
[7AB1AD93C837B6DF8A0C44BF615D0110] [21/02/2020] (.Techland Sp. z o.o..) - D:\SteamLibrary\steamapps\common\Dying Light\DevTools\DyingLightPlayer.exe
[7AB1AD93C837B6DF8A0C44BF615D0110] [21/02/2020] (.Techland Sp. z o.o..) - D:\SteamLibrary\steamapps\common\Dying Light\DyingLightGame.exe
[7F74C210CC0D477C7F54A8D4822D6A] [12/05/2019] (.Sublime HQ Pty Ltd.) - C:\Program Files\Sublime Text 3\crash_reporter.exe
[7F74C210CC0D477C7F54A8D4822D6A] [12/05/2019] (.Sublime HQ Pty Ltd.) - C:\Program Files\Sublime Text 3\sublime_text.exe
[7F74C210CC0D477C7F54A8D4822D6A] [24/08/2018] (.Sublime HQ Pty Ltd.) - C:\Program Files\Sublime Text 3\unins000.exe
```

INFORMATIONS SUR LES MODULES ZHPDIAG



FIN DE RAPPORT ZHPDIAG