

ZHPDiag v2022.10.27.82 By Nicolas Coolman (2022/10/27)
~ Run by User (Administrator) (2022/10/31 08:10:26)
~ Web: <https://www.nicolascoolman.com>
~ Blog: <https://nicolascoolman.eu/>
~ Facebook: <https://www.facebook.com/nicolascoolman1>
~ Certificate ZHPDiag: Legal
~ State version: Version OK
~ Mode: Scan
~ Report: C:\Users\User\Desktop\ZHPDiag.txt
~ Report: C:\Users\User\AppData\Roaming\ZHP\ZHPDiag.txt
~ UAC: Activate
~ System startup: Normal (Normal boot)
Windows 11 =>.Microsoft Corporation

---\ Internet Browsers (3) - 0s

~ GCIE: Google Chrome v107.0.5304.87
~ MSIE: Internet Explorer v11.1.22621.0
~ OBIE: Microsoft Edge v107.0.1418.26

---\ Windows Product Information (3) - 3s

~ Windows Server License Manager Script : OK
~ Licence Script File Génération : OK
Windows Automatic Updates : OK

---\ System protection software (1) - 1s

Windows Defender W10 (Activate) (Protection)

---\ Surveillance software (1) - 1s

~ Adobe Reader 6.0 - Français (Surveillance)

---\ Sharing software PeerToPeer (1) - 1s

~ Vuze v5.7.7.0 (P2P)

---\ Informations on the system (6) - 0s

~ Operating System: Intel64 Family 6 Model 158 Stepping 10, GenuineIntel
~ Operating System: 64-bit
~ Boot mode: Normal (Normal boot)
Total RAM: 8227.444 MB (42% free) : OK =>.RAM Value
System Restore: Activé (Enable)
System drive C: has 81 GB (33%) free of 243 GB : OK =>.Disk Space

---\ Connection to the system mode (3) - 0s

~ Computer Name: LAPTOP-3SI7NK72
~ User Name: User
~ Logged in as Administrator

---\ Enumeration of the disk units (4) - 0s

~ Drive C: has 81 GB free of 243 GB (System)
~ Drive D: has 244 GB free of 299 GB
~ Drive E: has 249 GB free of 299 GB
~ Drive F: has 277 GB free of 353 GB

---\ SYSTEM DISK MAIN FEATURES (20) - 15s

~ Model: ST1000LM049-2GH172 vACM1 (243 Gb)
~ Media Type: SSD Fixed Disk (Bus: RAID)

---\ SYSTEM DISK GENERAL ATTRIBUTES

OK - N0 - Indicateur d'usure du périphérique de stockage (Storage Device Wear Indicator) (%): 0
OK - N1 - Temps de latence maximal de vidage (Maximum Flash latency) (ms): 0.698
OK - N2 - Temps de latence maximal d'écriture (Maximum write latency) (ms): 1.801

OK - N3 - Temps de latence maximal de lecture (Maximum read latency) (ms): 1.71
OK - N4 - Vitesse de rotation (Spindle Speed) (RPM): Unknown

---\ **S.M.A.R.T. PARAMETERS** - [Flag][Value][Worst] [Threshold][Raw Value]
OK - BE - Temperature débit d'air (Temperature Airflow) - [0][63][63] [16][37]
RE - E8 - Espace de réserve disponible (Available reserved Space) - [0][100]
[100] [100][0]
OK - 05 - Nombre de secteurs réalloués (Reallocated Sector Count) - [0][67][0]
[0][0]
OK - F2 - Nombre total de lecture Hôte (Total LBA Read, Lifetime Host Reads) -
[0][100][0] [0][13663]
OK - F1 - Nombre total d'écriture Hôte (Total LBA Written, Lifetime Host Writes)
- [0][100][0] [0][12086]
OK - 0C - Nombre de cycles en fonctionnement (Power Cycles Count) - [0][100][0]
[0][2897]
OK - 09 - Heures de fonctionnement (Power-On Hours Count (POH) - [0][100][0]
[0][796]
OK - AE - Nombre inattendu de perte de puissance (Unexpected Power Off Count) -
[0][100][0] [0][86]
OK - BB - Nombre d'erreurs incorrigibles (Reported Uncorrectable Errors) - [0]
[100][0] [0][0]

---\ **State of the Windows Security Center (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

---\ **Search Generic System Files (26) - 1s**

[MD5.FD116263EE7E7E8F731748EFBDFC60EA] - 16/10/2022 - (.Microsoft Corporation -
Windows Explorer.) -- C:\WINDOWS\Explorer.exe [4997000] =>.Microsoft®
[MD5.57A6B4BDF247C1A6CA08AC09A8F9B742] - 07/05/2022 - (.Microsoft Corporation -
Windows host process (Rundll32).) -- C:\WINDOWS\System32\rundll32.exe [73728]
[Unsigned] =>.Microsoft Corporation
[MD5.0BBFBDE2146292B46BAA037C8C32BF4D] - 16/10/2022 - (.Microsoft Corporation -
Windows Start-Up Application.) -- C:\WINDOWS\System32\Wininit.exe [579912]
[Unsigned] =>.Microsoft Corporation
[MD5.9AC036A82C513E99F9201B76E1CFFD08] - 16/10/2022 - (.Microsoft Corporation -
Internet Extensions for Win32.) -- C:\WINDOWS\System32\wininet.dll [5232512]
=>.Microsoft®
[MD5.94CAF17B3418175EF5EB50C94BACD308] - 22/10/2022 - (.Microsoft Corporation -
Windows Logon Application.) -- C:\WINDOWS\System32\Winlogon.exe [901120]
[Unsigned] =>.Microsoft Corporation
[MD5.A25984968D7841E684031105CCF0E418] - 16/10/2022 - (.Microsoft Corporation -
Software Licensing Library.) -- C:\WINDOWS\System32\sppcomapi.dll [356352]
[Unsigned] =>.Microsoft Corporation
[MD5.31FB3E81A27A3518B9898AE396391032] - 07/05/2022 - (.Microsoft Corporation -
DNS Client API DLL.) -- C:\WINDOWS\System32\dnsapi.dll [1005464] =>.Microsoft®
[MD5.05AA79C0776E5F1E67EEEEAA4872655F] - 07/05/2022 - (.Microsoft Corporation -
DNS Client API DLL.) -- C:\WINDOWS\Syswow64\dnsapi.dll [753056] =>.Microsoft®
[MD5.EB004A063907EFD068C0EE4B419CF428] - 16/10/2022 - (.Microsoft Corporation -
Windows Update Agent.) -- C:\WINDOWS\System32\wuaueng.dll [3464008] [Unsigned]
=>.Microsoft Corporation

[MD5.54DB796A38084C3DDC564713528E8FBD] - 16/10/2022 - (.Microsoft Corporation - DLL client de l'API utilisateur de Windows m.) -- C:\WINDOWS\System32\fr-FR\user32.dll.mui [19968] [Unsigned] =>.Microsoft Corporation
[MD5.D9AFA784F62D5A2C282074C90F220E35] - 16/10/2022 - (.Microsoft Corporation - Ancillary Function Driver for WinSock.) -- C:\WINDOWS\System32\drivers\AFD.sys [697696] [Unsigned] =>.Microsoft Corporation
[MD5.5EB4309B030968F9B884CBEF5049C473] - 16/10/2022 - (.Microsoft Corporation - ATAPI IDE Miniport Driver.) -- C:\WINDOWS\System32\drivers\atapi.sys [62808] [Unsigned] =>.Microsoft Corporation
[MD5.8D74B96430DDC074D1A21A2E93514696] - 16/10/2022 - (.Microsoft Corporation - CD-ROM File System Driver.) -- C:\WINDOWS\System32\drivers\Cdfs.sys [131072] [Unsigned] =>.Microsoft Corporation
[MD5.BD94BB6159F87B6D4D3E10CDC20C069A] - 07/05/2022 - (.Microsoft Corporation - SCSI CD-ROM Driver.) -- C:\WINDOWS\System32\drivers\Cdrom.sys [204800] [Unsigned] =>.Microsoft Corporation
[MD5.0B247F7C404B32481ABE9C7DAB0E0F3B] - 16/10/2022 - (.Microsoft Corporation - DFS Namespace Client Driver.) -- C:\WINDOWS\System32\drivers\DfsC.sys [184320] [Unsigned] =>.Microsoft Corporation
[MD5.5BD21405A85342B3B8E92E06611870B4] - 16/10/2022 - (.Microsoft Corporation - High Definition Audio Bus Driver.) -- C:\WINDOWS\System32\drivers\HDAudBus.sys [192512] [Unsigned] =>.Microsoft Corporation
[MD5.566132924EBEEAE1A41FB521B56E0AAA] - 07/05/2022 - (.Microsoft Corporation - i8042 Port Driver.) -- C:\WINDOWS\System32\drivers\i8042prt.sys [159744] [Unsigned] =>.Microsoft Corporation
[MD5.78085A907F90C8BE1018FF571796A0C5] - 16/10/2022 - (.Microsoft Corporation - IP Network Address Translator.) -- C:\WINDOWS\System32\drivers\IpNat.sys [258048] [Unsigned] =>.Microsoft Corporation
[MD5.242CD1730A6446A8D6BE463B76760C38] - 16/10/2022 - (.Microsoft Corporation - Windows NT SMB Minirdr.) -- C:\WINDOWS\System32\drivers\MRxSmb.sys [660816] [Unsigned] =>.Microsoft Corporation
[MD5.E04590A290CD698C8E56426E00427A7F] - 16/10/2022 - (.Microsoft Corporation - MBT Transport driver.) -- C:\WINDOWS\System32\drivers\netBT.sys [327680] [Unsigned] =>.Microsoft Corporation
[MD5.7FB574FEFF7088B9926B323763E8FF00] - 16/10/2022 - (.Microsoft Corporation - NT File System Driver.) -- C:\WINDOWS\System32\drivers\ntfs.sys [3343712] [Unsigned] =>.Microsoft Corporation
[MD5.3A4E501001979A77B7F2C353944699A9] - 07/05/2022 - (.Microsoft Corporation - Parallel Port Driver.) -- C:\WINDOWS\System32\drivers\Parport.sys [135168] [Unsigned] =>.Microsoft Corporation
[MD5.CF06B9BD81B68A1D57FEEBF665EBDA5A] - 16/10/2022 - (.Microsoft Corporation - RAS L2TP mini-port/call-manager driver.) -- C:\WINDOWS\System32\drivers\Rasl2tp.sys [139264] [Unsigned] =>.Microsoft Corporation
[MD5.9327D2D9AEA1C64BC6993E48849232E9] - 07/05/2022 - (.Microsoft Corporation - Microsoft RDP Device redirector.) -- C:\WINDOWS\System32\drivers\rdpdr.sys [196608] [Unsigned] =>.Microsoft Corporation
[MD5.0764FE1EDF3CFE3133B0BD42A51447EC] - 16/10/2022 - (.Microsoft Corporation - TDI Translation Driver.) -- C:\WINDOWS\System32\drivers\tdx.sys [157000] [Unsigned] =>.Microsoft Corporation
[MD5.346AFD3A66E77F234E05BE439730013C] - 07/05/2022 - (.Microsoft Corporation - Volume Shadow Copy driver.) -- C:\WINDOWS\System32\drivers\volsnap.sys [468312] [Unsigned] =>.Microsoft Corporation

---\ No disabled Windows Services (82) - 3s

023 - Service: ACC Service (ACCSvc) . (.Acer Incorporated - ACCSvc.) - C:\Program Files (x86)\Acer\Care Center\ACCSvc.exe =>.Acer Incorporated®
023 - Service: C:\WINDOWS\System32\AudioEndpointBuilder.dll (AudioEndpointBuilder) . (.Microsoft Corporation - Windows Audio Endpoint Builder.) - C:\WINDOWS\System32\AudioEndpointBuilder.dll [Unsigned] =>.Microsoft Corporation
023 - Service: C:\WINDOWS\System32\audiosrv.dll (Audiosrv) . (.Microsoft Corporation - Windows Audio Service.) - C:\WINDOWS\System32\Audiosrv.dll [Unsigned] =>.Microsoft Corporation

023 - Service: C:\WINDOWS\System32\bfe.dll (BFE) . (.Microsoft Corporation - Base Filtering Engine.) - C:\WINDOWS\System32\bfe.dll [Unsigned] =>.Microsoft Corporation

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

023 - Service: C:\WINDOWS\System32\cbdhsvc.dll (cbdhsvc) . (.Microsoft Corporation - Microsoft (R) Clipboard History.) - C:\WINDOWS\System32\cbdhsvc.dll [Unsigned] =>.Microsoft Corporation

023 - Service: cbdhsvc_5bed4 (cbdhsvc_5bed4) . (.Microsoft Corporation - Host Process for Windows Services.) - C:\Windows\System32\svchost.exe =>.Microsoft®

023 - Service: C:\WINDOWS\System32\cdpusersvc.dll (CDPUserSvc) . (.Microsoft Corporation - Microsoft (R) CDP User Components.) - C:\WINDOWS\System32\CDPUserSvc.dll [Unsigned] =>.Microsoft Corporation

023 - Service: CDPUserSvc_5bed4 (CDPUserSvc_5bed4) . (.Microsoft Corporation - Host Process for Windows Services.) - C:\Windows\System32\svchost.exe =>.Microsoft®

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

023 - Service: Intel(R) Content Protection HDCP Service (cplspcon) . (.Intel Corporation - Intel HD Graphics Drivers for Windows(R).) - C:\Windows\System32\DriverStore\FileRepository\iigd_dch.inf_amd64_7d6ad0397c5dc3fd\IntelCpHDCPSvc.exe =>.Intel(R) pGFX®

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

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

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

023 - Service: C:\WINDOWS\System32\das.dll (DeviceAssociationService) . (.Microsoft Corporation - Device Association Service.) - C:\WINDOWS\System32\das.dll [Unsigned] =>.Microsoft Corporation

023 - Service: C:\Windows\System32\dhcpcore.dll (Dhcp) . (.Microsoft Corporation - DHCP Client Service.) - C:\Windows\System32\dhcpcore.dll =>.Microsoft®

023 - Service: C:\WINDOWS\System32\diagtrack.dll (DiagTrack) . (.Microsoft Corporation - Microsoft Windows Diagnostics Tracking.) - C:\WINDOWS\System32\diagtrack.dll [Unsigned] =>.Microsoft Corporation

023 - Service: C:\WINDOWS\System32\dispbroker.desktop.dll (DispBrokerDesktopSvc) . (.Microsoft Corporation - Desktop Display Broker.) - C:\WINDOWS\System32\DispBroker.Desktop.dll [Unsigned] =>.Microsoft Corporation

023 - Service: C:\Windows\System32\dnsapi.dll (Dnscache) . (.Microsoft Corporation - DNS Caching Resolver Service.) - C:\WINDOWS\System32\dnsrslvr.dll [Unsigned] =>.Microsoft Corporation

023 - Service: C:\WINDOWS\System32\dosvc.dll (DoSvc) . (.Microsoft Corporation - Host Process for Windows Services.) - C:\Windows\System32\svchost.exe =>.Microsoft®

023 - Service: C:\WINDOWS\System32\dusmsvc.dll (DusmSvc) . (.Microsoft Corporation - Data Usage Service.) - C:\WINDOWS\System32\dusmsvc.dll [Unsigned] =>.Microsoft Corporation

023 - Service: Microsoft Edge Update Service (edgeupdate) (edgeupdate) . (.Microsoft Corporation - Microsoft Edge Update.) - C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe =>.Microsoft®

023 - Service: EMP_UDSA (EMP_UDSA) . (.SEIKO EPSON CORPORATION - EPSON USB Display Ver.1.50.) - C:\Program Files (x86)\EPSON Projector\Epson USB Display V1.5\EMP_UDSA.exe [Unsigned] =>.Seiko Epson Corporation

023 - Service: C:\WINDOWS\System32\wevtvc.dll (EventLog) . (.Microsoft Corporation - Event Logging Service.) - C:\WINDOWS\System32\wevtvc.dll [Unsigned] =>.Microsoft Corporation

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

023 - Service: C:\WINDOWS\System32\FntCache.dll (FontCache) . (.Microsoft Corporation - Windows Font Cache Service.) - C:\WINDOWS\System32\FntCache.dll [Unsigned] =>.Microsoft Corporation

023 - Service: Foxit PDF Reader Update Service (FoxitReaderUpdateService) . (.Foxit Software Inc. - Foxit PDF Reader Update Service.) - C:\PROGRAM FILES (X86)\FOXIT SOFTWARE\FOXIT READER\FoxitPDFReaderUpdateService.exe {0B022E5567D2577010644DE52C9A3656}. =>.Foxit Software Inc.

023 - Service: Garena platform service (GarenaPlatform) . (.Garena Online - Garena platform service.) - C:\Program Files (x86)\Garena\Garena\2.0.1909.2618\gxxsvc.exe {46A0800C34C5FEE85DB1758D556C2D0E}. =>.Garena Online

023 - Service: @gpapi.dll,-112 (gpsvc) . (.Microsoft Corporation - Group Policy Client.) - C:\WINDOWS\System32\gpsvc.dll [Unsigned] =>.Microsoft Corporation

023 - Service: Google Update Service (gupdate) (gupdate) . (.Google Inc. - Google Installer.) - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe =>.Google Inc®

023 - Service: HP Print Scan Doctor Service (HPPrintScanDoctorService) . (.HP Inc. - .) - C:\Program Files\HP\PrintScanDoctor\HPPrintScanDoctorService.exe =>.HP Inc.®

023 - Service: Hotspot Shield Service 11.3.0 (hshld_11.3.0) . (.Pango Inc. - Hss.Service.Application.) - C:\Program Files (x86)\Hotspot Shield\11.3.0\bin\cmw_srv.exe {054E8D30374B037A81D8EC3D5DCCB1D4}. =>.Pango Inc.

023 - Service: Intel(R) HD Graphics Control Panel Service (igfxCUIService2.0.0.0) . (.Intel Corporation - igfxCUIService Module.) - C:\Windows\System32\DriverStore\FileRepository\cui_dch.inf_amd64_92cf9d9d84f1d3db\igfxCUIService.exe =>.Intel(R) pGFX®

023 - Service: Intel(R) TPM Provisioning Service (Intel(R) TPM Provisioning Service) . (.Intel(R) Corporation - Intel(R) TPM Provisioning Service.) - C:\Windows\System32\DriverStore\FileRepository\iclsclient.inf_amd64_dec9bbf83f76d9e5\lib\TPMProvisioningService.exe {0082885CBA74ECF5581D8ACC6367A4695E}. =>.Intel(R) Corporation

023 - Service: C:\WINDOWS\System32\iphlpvc.dll (iphlpvc) . (.Microsoft Corporation - Service that offers IPv6 connectivity over.) - C:\WINDOWS\System32\iphlpvc.dll [Unsigned] =>.Microsoft Corporation

023 - Service: C:\WINDOWS\System32\srsvsc.dll (LanmanServer) . (.Microsoft Corporation - Server Service DLL.) - C:\WINDOWS\System32\srsvsc.dll [Unsigned] =>.Microsoft Corporation

023 - Service: C:\WINDOWS\System32\wkssvc.dll (LanmanWorkstation) . (.Microsoft Corporation - Workstation Service DLL.) - C:\WINDOWS\System32\wkssvc.dll [Unsigned] =>.Microsoft Corporation

023 - Service: C:\WINDOWS\system32\lsm.dll (LSM) . (.Microsoft Corporation - Local Session Manager Service.) - C:\WINDOWS\System32\lsm.dll [Unsigned] =>.Microsoft Corporation

023 - Service: Mise à jour automatique - Index Education (MajIndexEducationService) . (.Index Education - .) - C:\program files (x86)\index education\mise a jour automatique\ServiceMiseAJourIndex.exe {59BFA29DD2D6F208659847D2}. =>.Index Education

023 - Service: C:\WINDOWS\System32\moshost.dll (MapsBroker) . (.Microsoft Corporation - Downloaded Maps Manager.) - C:\WINDOWS\System32\moshost.dll [Unsigned] =>.Microsoft Corporation

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

023 - Service: C:\WINDOWS\System32\nsisvc.dll (nsi) . (.Microsoft Corporation - Network Store Interface RPC server.) - C:\WINDOWS\System32\nsisvc.dll [Unsigned] =>.Microsoft Corporation

023 - Service: NVIDIA LocalSystem Container (NvContainerLocalSystem) . (.NVIDIA Corporation - NVIDIA Container.) - C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe =>.Nvidia Corporation®

023 - Service: NVIDIA Display Container LS (NvDisplay.ContainerLocalSystem) . (.NVIDIA Corporation - NVIDIA Container.) - C:\Windows\System32\DriverStore\FileRepository\nvaci.inf_amd64_91df09c5579a85f3\Display.NvContainer\NvDisplay.Container.exe =>.Nvidia Corporation®

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

023 - Service: OneSyncSvc_5bed4 (OneSyncSvc_5bed4) . (.Microsoft Corporation - Host Process for Windows Services.) - C:\Windows\System32\svchost.exe =>.Microsoft@

023 - Service: C:\WINDOWS\System32\pcasvc.dll (PcaSvc) . (.Microsoft Corporation - Program Compatibility Assistant Service.) - C:\WINDOWS\System32\pcasvc.dll [Unsigned] =>.Microsoft Corporation

023 - Service: C:\WINDOWS\System32\umpo.dll (Power) . (.Microsoft Corporation - User-mode Power Service.) - C:\WINDOWS\System32\umpo.dll [Unsigned] =>.Microsoft Corporation

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

023 - Service: C:\WINDOWS\System32\rasmans.dll (RasMan) . (.Microsoft Corporation - Remote Access Connection Manager.) - C:\WINDOWS\System32\rasmans.dll [Unsigned] =>.Microsoft Corporation

023 - Service: C:\WINDOWS\system32\RpcEpMap.dll (RpcEptMapper) . (.Microsoft Corporation - RPC Endpoint Mapper.) - C:\WINDOWS\System32\RpcEpMap.dll [Unsigned] =>.Microsoft Corporation

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

023 - Service: Intel(R) Storage Middleware Service (RstMwService) . (.Intel Corporation - Intel(R) Rapid Storage Technology Managemen.) - C:\Windows\System32\DriverStore\FileRepository\iastorac.inf_amd64_ba273d0fffb93e225\RstMwService.exe {34770BB53021480D308F5E5593B49D84}. =>.Intel Corporation

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

023 - Service: C:\WINDOWS\System32\schedsvc.dll (Schedule) . (.Microsoft Corporation - Task Scheduler Service.) - C:\WINDOWS\System32\schedsvc.dll [Unsigned] =>.Microsoft Corporation

023 - Service: C:\WINDOWS\System32\Sens.dll (SENS) . (.Microsoft Corporation - System Event Notification Service (SENS).) - C:\WINDOWS\System32\sens.dll [Unsigned] =>.Microsoft Corporation

023 - Service: C:\WINDOWS\System32\Sgrm\SgrmBroker.exe,-100 (SgrmBroker) . (.Microsoft Corporation - System Guard Runtime Monitor Broker Service.) - C:\WINDOWS\System32\Sgrm\SgrmBroker.exe [Unsigned] =>.Microsoft Corporation

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

023 - Service: C:\WINDOWS\System32\spoolsv.exe,-1 (Spooler) . (.Microsoft Corporation - Spooler SubSystem App.) - C:\WINDOWS\System32\spoolsv.exe [Unsigned] =>.Microsoft Corporation

023 - Service: C:\WINDOWS\System32\spssvc.exe,-101 (spssvc) . (.Microsoft Corporation - Microsoft Software Protection Platform Serv.) - C:\WINDOWS\System32\spssvc.exe [Unsigned] =>.Microsoft Corporation

023 - Service: C:\Windows\System32\windows.staterepository.dll (StateRepository) . (.Microsoft Corporation - Windows StateRepository API Server.) - C:\Windows\System32\windows.staterepository.dll =>.Microsoft@

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

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

023 - Service: C:\WINDOWS\System32\SystemEventsBrokerServer.dll (SystemEventsBroker) . (.Microsoft Corporation - System Events Broker.) - C:\WINDOWS\System32\SystemEventsBrokerServer.dll [Unsigned] =>.Microsoft Corporation

023 - Service: C:\WINDOWS\System32\TabSvc.dll (TextInputManagementService) . (.Microsoft Corporation - Microsoft Text Input Management Service.) - C:\WINDOWS\System32\TabSvc.dll [Unsigned] =>.Microsoft Corporation

023 - Service: C:\WINDOWS\System32\themeservice.dll (Themes) . (.Microsoft Corporation - Windows Shell Theme Service Dll.) - C:\WINDOWS\System32\themeservice.dll [Unsigned] =>.Microsoft Corporation

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

023 - Service: C:\WINDOWS\System32\usosvc.dll (Usosvc) . (.Microsoft Corporation - Update Session Orchestrator Service.) - C:\WINDOWS\System32\usosvc.dll [Unsigned] =>.Microsoft Corporation

023 - Service: Waves Audio Services (WavesSysSvc) . (.Waves Audio Ltd. - WavesSysSvc Service Application.) - C:\Windows\System32\DriverStore\FileRepository\wavesapo77ac.inf_amd64_d5839c9d7c0bda64\WavesSysSvc64.exe =>.Waves Inc@

023 - Service: C:\WINDOWS\System32\wcmssvc.dll (Wcmssvc) . (.Microsoft Corporation - Windows Connection Manager Service DLL.) - C:\WINDOWS\System32\wcmssvc.dll [Unsigned] =>.Microsoft Corporation

023 - Service: C:\WINDOWS\System32\webthreatdefusersvc.dll (webthreatdefusersvc) . (.Microsoft Corporation - Web Threat Defense User Service.) - C:\WINDOWS\System32\webthreatdefusersvc.dll [Unsigned] =>.Microsoft Corporation

023 - Service: webthreatdefusersvc_5bed4 (webthreatdefusersvc_5bed4) . (.Microsoft Corporation - Host Process for Windows Services.) - C:\Windows\System32\svchost.exe =>.Microsoft@

023 - Service: @%ProgramFiles%\Windows Defender\MpAsDesc.dll,-310 (WinDefend) . (.Microsoft Corporation - Antimalware Service Executable.) - C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2210.4-0\MsMpEng.exe =>.Microsoft@

023 - Service: WindscribeService (WindscribeService) . (.Windscribe Limited - Manages the firewall and controls the VPN t.) - C:\Program Files (x86)\Windscribe\WindscribeService.exe =>.Windscribe Limited@

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

023 - Service: C:\WINDOWS\System32\wlansvc.dll (WlanSvc) . (.Microsoft Corporation - Windows WLAN AutoConfig Service DLL.) - C:\WINDOWS\System32\wlansvc.dll [Unsigned] =>.Microsoft Corporation

023 - Service: Intel(R) Management Engine WMI Provider Registration (WMIRegistrationService) . (.Intel Corporation - Intel(R) Management Engine WMI Provider Reg.) - C:\Windows\System32\DriverStore\FileRepository\mewmiprov.inf_amd64_21e0cf0737fd48af\WMIRegistrationService.exe {0ADE8114D7679B066F2DB2DFD2F67AC2}. =>.Intel Corporation

023 - Service: C:\WINDOWS\System32\wpnservice.dll (WpnService) . (.Microsoft Corporation - Windows Push Notification System Service.) - C:\WINDOWS\System32\WpnService.dll [Unsigned] =>.Microsoft Corporation

023 - Service: C:\WINDOWS\System32\WpnUserService.dll (WpnUserService) . (.Microsoft Corporation - Windows Push Notification User Service.) - C:\WINDOWS\System32\WpnUserService.dll [Unsigned] =>.Microsoft Corporation

023 - Service: WpnUserService_5bed4 (WpnUserService_5bed4) . (.Microsoft Corporation - Host Process for Windows Services.) - C:\Windows\System32\svchost.exe =>.Microsoft@

023 - Service: C:\WINDOWS\System32\wscsvc.dll (wscsvc) . (.Microsoft Corporation - Windows Security Center Service.) - C:\WINDOWS\System32\wscsvc.dll [Unsigned] =>.Microsoft Corporation

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

---\ Services not Microsoft (SR=Run, SS=Stop) (128) - 10s

SR - Boot [07/05/2022] [108376] (3ware) . (.LSI.) - C:\WINDOWS\System32\drivers\3ware.sys =>.Microsoft@

SR - Auto [22/04/2019] [300336] ACC Service (ACCSvc) . (.Acer Incorporated.) - C:\Program Files (x86)\Acer\Care Center\ACCSvc.exe =>.Acer Incorporated@

SR - Demand [09/08/2021] [31896] Acer Airplane Mode Controller (AcerAirplaneModeController) . (.Acer Incorporated.) - C:\WINDOWS\System32\drivers\AcerAirplaneModeController.sys =>.Acer Incorporated®

SR - Boot [07/05/2022] [1136472] (ADP80XX) . (.PMC-Sierra.) - C:\WINDOWS\System32\drivers\ADP80XX.SYS =>.Microsoft®

SR - Demand [07/05/2022] [18432] AMD GPIO Client Driver (amdgpio2) . (.Advanced Micro Devices, Inc.) - C:\WINDOWS\System32\drivers\amdgpio2.sys [Unsigned] =>.Advanced Micro Devices, Inc

SR - Demand [07/05/2022] [45568] AMD I2C Controller Service (amdi2c) . (.Advanced Micro Devices, Inc.) - C:\WINDOWS\System32\drivers\amdi2c.sys [Unsigned] =>.Advanced Micro Devices, Inc

SR - Boot [07/05/2022] [84312] (amdsata) . (.Advanced Micro Devices.) - C:\WINDOWS\System32\drivers\amdsata.sys =>.Microsoft®

SR - Boot [07/05/2022] [260440] (amdsbs) . (.AMD Technologies Inc..) - C:\WINDOWS\System32\drivers\amdsbs.sys =>.Microsoft®

SR - Boot [07/05/2022] [28008] (amdxtata) . (.Advanced Micro Devices.) - C:\WINDOWS\System32\drivers\amdxtata.sys =>.Microsoft®

SR - Boot [07/05/2022] [113496] Apple Solid State Drive Device (AppleSSD) . (.Apple Inc..) - C:\WINDOWS\System32\drivers\AppleSSD.sys =>.Microsoft®

SR - Boot [07/05/2022] [132968] Adaptec SAS/SATA-II RAID S (arcsas) . (.PMC-Sierra, Inc..) - C:\WINDOWS\System32\drivers\arcsas.sys =>.Microsoft®

SS - Demand [30/08/2021] [576216] Armoury Live Update (ArmouryLiveUpdate) . (.ASUSTeK Computer Inc..) - C:\Windows\System32\DriverStore\FileRepository\rogms.inf_amd64_94d9766656ff6011\ArmouryLiveUpdate.exe =>.ASUSTeK Computer Inc.®

SR - Boot [07/05/2022] [534872] QLogic Network Adapter VBD (b06bdrv) . (.QLogic Corporation.) - C:\WINDOWS\System32\drivers\bxbvda.sys =>.Microsoft®

SR - Demand [07/05/2022] [9728] bcmfn2 Service (bcmfn2) . (...) - C:\WINDOWS\System32\drivers\bcmfn2.sys [Unsigned] =>.Broadcom Corporation

SR - Boot [07/05/2022] [320880] (cht4iscsi) . (.Chelsio Communications.) - C:\WINDOWS\System32\drivers\cht4sx64.sys =>.Microsoft®

SR - Demand [07/05/2022] [1854832] Chelsio Virtual Bus Driver (cht4vbd) . (.Chelsio Communications.) - C:\WINDOWS\System32\drivers\cht4vx64.sys =>.Microsoft®

SS - Demand [03/07/2019] [508984] Intel(R) Content Protection HECI Service (cphs) . (.Intel Corporation.) - C:\Windows\System32\DriverStore\FileRepository\iigd_dch.inf_amd64_7d6ad0397c5dc3fd\IntelCpHeciSvc.exe =>.Intel(R) pGFX®

SR - Auto [03/07/2019] [516696] Intel(R) Content Protection HDCP Service (cplspcon) . (.Intel Corporation.) - C:\Windows\System32\DriverStore\FileRepository\iigd_dch.inf_amd64_7d6ad0397c5dc3fd\IntelCpHDCPSvc.exe =>.Intel(R) pGFX®

SR - Auto [12/11/2021] [130320] Dropbox Update Service (dbupdate) (dbupdate) . (.Dropbox, Inc..) - C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe =>.Dropbox, Inc®

SS - Demand [12/11/2021] [130320] Dropbox Update Service (dbupdatem) (dbupdatem) . (.Dropbox, Inc..) - C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe =>.Dropbox, Inc®

SR - Auto [10/10/2022] [46824] DbxSvc (DbxSvc) . (.Dropbox, Inc..) - C:\WINDOWS\System32\DbxSvc.exe =>.Dropbox, Inc®

SR - Demand [08/10/2021] [160376] SAMSUNG Mobile USB Composite Device Driver (DEVGURU Ver.) (dg_ssudbus) . (.Samsung Electronics Co., Ltd..) - C:\WINDOWS\System32\DRIVERS\ssudbus2.sys =>.Samsung Electronics Co., Ltd.®

SR - Boot [07/05/2022] [3441512] QLogic 10 Gigabit Ethernet Ada (ebdrv) . (.Marvell Semiconductor Inc..) - C:\WINDOWS\System32\drivers\evbda.sys =>.Microsoft®

SR - Boot [07/05/2022] [3424104] QLogic Legacy Ethernet Adapte (ebdrv0) . (.QLogic Corporation.) - C:\WINDOWS\System32\drivers\evbd0a.sys =>.Microsoft®

SR - Auto [06/01/2011] [98304] EMP_UDSA (EMP_UDSA) . (.SEIKO EPSON CORPORATION.) - C:\Program Files (x86)\EPSON Projector\Epson USB Display V1.5\EMP_UDSA.exe [Unsigned] =>.Seiko Epson Corporation

SS - Demand [27/10/2021] [16029472] Epic Online Services (EpicOnlineServices) . (.Epic Games, Inc..) - C:\Program Files (x86)\Epic Games\Epic Online Services\service\EpicOnlineServicesHost.exe =>.Epic Games Inc.®

SR - Demand [06/01/2011] [23040] EPSON Projector UD Audio (eppvad_simple) .
(.SEIKO EPSON CORPORATION.) - C:\WINDOWS\System32\drivers\EMP_UDAU.sys
[Unsigned] =>.Seiko Epson Corporation

SR - Demand [20/06/2019] [218048] ELAN I2C Filter Driver (ETDI2C) . (.ELAN
Microelectronic Corp..) - C:\WINDOWS\System32\drivers\ETDI2C.sys =>.ELAN
MICROELECTRONICS CORPORATION®

SR - Auto [20/05/2022] [2358800] Foxit PDF Reader Update Service
(FoxitReaderUpdateService) . (.Foxit Software Inc..) - C:\PROGRAM FILES (X86)\
FOXIT SOFTWARE\FOXIT READER\FoxitPDFReaderUpdateService.exe
{0B022E5567D2577010644DE52C9A3656}. =>.Foxit Software Inc.

SS - Demand [07/09/2022] [401960] NVIDIA FrameView SDK service (FvSvc) .
(.NVIDIA.) - C:\Program Files\NVIDIA Corporation\FrameViewSDK\nvfvsdksvc_x64.exe
=>.Nvidia Corporation®

SR - Auto [26/09/2019] [320512] Garena platform service (GarenaPlatform) .
(.Garena Online.) - C:\Program Files (x86)\Garena\Garena\2.0.1909.2618\
gxsvc.exe {46A0800C34C5FEE85DB1758D556C2D0E}. =>.Garena Online

SR - Demand [15/07/2020] [51016] Boom Audio Driver (GDPL_BOOM) . (.
{254E21C741DC779A4EC68054D3FFA4BF}..) - C:\WINDOWS\System32\drivers\boomvad.sys
{254E21C741DC779A4EC68054D3FFA4BF}.

SS - Demand [27/10/2022] [1730328] Google Chrome Elevation Service
(GoogleChromeElevationServi (GoogleChromeElevationService) . (.Google LLC.) -
C:\Program Files (x86)\Google\Chrome\Application\107.0.5304.87\
elevation_service.exe =>.Google LLC®

SR - Auto [12/08/2020] [144200] Google Update Service (gupdate) (gupdate) .
(.Google Inc..) - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
=>.Google Inc®

SS - Demand [12/08/2020] [144200] Google Update Service (gupdatem) (gupdatem)
. (.Google Inc..) - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
=>.Google Inc®

SR - Disabl [12/10/2021] [1917632] Intel(R) RST HFC (HfcDisableService) .
(.Intel Corporation.) - C:\Windows\System32\DriverStore\FileRepository\
iastorac.inf_amd64_ba273d0ffb93e225\HfcDisableService.exe
{34770BB53021480D308F5E5593B49D84}. =>.Intel Corporation

SR - Auto [15/07/2022] [225368] HP Print Scan Doctor Service
(HPPrintScanDoctorService) . (.HP Inc..) - C:\Program Files\HPPrintScanDoctor\
HPPrintScanDoctorService.exe =>.HP Inc.®

SR - Boot [07/05/2022] [65360] (HpSAMD) . (.Hewlett-Packard Company.) -
C:\WINDOWS\System32\drivers\HpSAMD.sys =>.Microsoft®

SR - Auto [04/08/2022] [247608] Hotspot Shield Service 11.3.0
(hshld_11.3.0) . (.Pango Inc..) - C:\Program Files (x86)\Hotspot Shield\11.3.0\
bin\cmw_srv.exe {054E8D30374B037A81D8EC3D5DCCB1D4}. =>.Pango Inc.

SR - Demand [29/09/2020] [39424] HotspotShield TAP-Windows Ad (hsstap) .
(.Pango.) - C:\WINDOWS\System32\drivers\hsstap.sys =>.Microsoft®

SR - Demand [07/05/2022] [36352] Intel Serial IO GPIO Controlle (iagpio) .
(.Intel(R) Corporation.) - C:\WINDOWS\System32\drivers\iagpio.sys [Unsigned]
=>.Intel(R) Corporation

SR - Demand [07/05/2022] [91136] Intel(R) Serial IO I2C Host Cont (iai2c) .
(.Intel(R) Corporation.) - C:\WINDOWS\System32\drivers\iai2c.sys [Unsigned]
=>.Intel(R) Corporation

SR - Demand [07/05/2022] [79360] Intel(R) S (iaLPSS2i_GPI02) . (.Intel
Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i_GPI02.sys [Unsigned]
=>.Intel Corporation

SR - Demand [07/05/2022] [93184] In (iaLPSS2i_GPI02_BXT_P) . (.Intel
Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i_GPI02_BXT_P.sys [Unsigned]
=>.Intel Corporation

SR - Demand [07/05/2022] [112128] Intel((iaLPSS2i_GPI02_CNL) . (.Intel
Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i_GPI02_CNL.sys [Unsigned]
=>.Intel Corporation

SR - Demand [07/05/2022] [96256] Intel((iaLPSS2i_GPI02_GLK) . (.Intel
Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i_GPI02_GLK.sys [Unsigned]
=>.Intel Corporation

SR - Demand [07/05/2022] [171520] Intel(R) Seria (iaLPSS2i_I2C) . (.Intel
Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i_I2C.sys [Unsigned]
=>.Intel Corporation

SR - Demand [07/05/2022] [175104] Intel((iaLPSS2i_I2C_BXT_P) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i_I2C_BXT_P.sys [Unsigned] =>.Intel Corporation

SR - Demand [07/05/2022] [177152] Intel(R) S (iaLPSS2i_I2C_CNL) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i_I2C_CNL.sys [Unsigned] =>.Intel Corporation

SR - Demand [07/05/2022] [177664] Intel(R) S (iaLPSS2i_I2C_GLK) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2i_I2C_GLK.sys [Unsigned] =>.Intel Corporation

SR - Demand [29/11/2018] [131744] Intel(R) Serial IO GPIO Driver v2 (iaLPSS2_GPIO2) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2_GPIO2.sys =>.Intel(R) Embedded Subsystems and IP Blocks Group®

SR - Demand [14/05/2020] [128776] Intel(R) Serial IO (iaLPSS2_GPIO2_CNL) . (.Intel Corporation.) - C:\Windows\System32\DriverStore\FileRepository\ialpss2_gpio2_cnl.inf_amd64_d920c2a844f26eba\iaLPSS2_GPIO2_CNL.sys {00B15FDDBBBCD5912920FFAB85C4F6064D5}. =>.Intel Corporation

SR - Demand [29/11/2018] [200352] Intel(R) Serial IO I2C Driver v2 (iaLPSS2_I2C) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2_I2C.sys =>.Intel(R) Embedded Subsystems and IP Blocks Group®

SR - Demand [14/05/2020] [196360] Intel(R) Serial IO I2C (iaLPSS2_I2C_CNL) . (.Intel Corporation.) - C:\Windows\System32\DriverStore\FileRepository\ialpss2_i2c_cnl.inf_amd64_666eef21665eb26\iaLPSS2_I2C_CNL.sys {00B15FDDBBBCD5912920FFAB85C4F6064D5}. =>.Intel Corporation

SR - Demand [29/11/2018] [161440] Intel(R) Serial IO SPI Driver v2 (iaLPSS2_SPI) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2_SPI.sys =>.Intel(R) Embedded Subsystems and IP Blocks Group®

SR - Demand [29/11/2018] [320160] Intel(R) Serial IO UART Driver v2 (iaLPSS2_UART2) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSS2_UART2.sys =>.Intel(R) Embedded Subsystems and IP Blocks Group®

SR - Demand [14/05/2020] [305928] Intel(R) Serial IO (iaLPSS2_UART2_CNL) . (.Intel Corporation.) - C:\Windows\System32\DriverStore\FileRepository\ialpss2_uart2_cnl.inf_amd64_df1115697e57a59a\iaLPSS2_UART2_CNL.sys {00B15FDDBBBCD5912920FFAB85C4F6064D5}. =>.Intel Corporation

SR - Demand [07/05/2022] [38128] Intel(R) Serial IO (iaLPSSi_GPIO) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSSi_GPIO.sys =>.Intel Corporation - Client Components Group®

SR - Demand [07/05/2022] [113152] Intel(R) Serial IO I (iaLPSSi_I2C) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaLPSSi_I2C.sys [Unsigned] =>.Intel Corporation

SR - Boot [12/10/2021] [1347776] Intel(R) Chipset SATA/PCI (iaStorAC) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaStorAC.sys {34770BB53021480D308F5E5593B49D84}. =>.Intel Corporation

SR - Demand [12/10/2021] [73920] iaStorAfs (iaStorAfs) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaStorAfs.sys {34770BB53021480D308F5E5593B49D84}. =>.Intel Corporation

SS - Demand [12/10/2021] [3031232] Intel(R) Optane(T (iaStorAfsService) . (.Intel Corporation.) - C:\WINDOWS\System32\iaStorAfsService.exe {34770BB53021480D308F5E5593B49D84}. =>.Intel Corporation

SR - Boot [07/05/2022] [885584] Intel Chipset SATA RAI (iaStorAVC) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaStorAVC.sys =>.Microsoft®

SR - Boot [07/05/2022] [413008] Intel RAID Controller Wi (iaStorV) . (.Intel Corporation.) - C:\WINDOWS\System32\drivers\iaStorV.sys =>.Microsoft®

SR - Demand [07/05/2022] [559976] Mellanox InfiniBand Bus/A (ibbus) . (.Mellanox.) - C:\WINDOWS\System32\drivers\ibbus.sys =>.Microsoft®

SR - Demand [25/08/2022] [8093784] Intel(R) Wireless Bluetooth (ibtusb) . (.Intel Corporation.) - C:\Windows\System32\DriverStore\FileRepository\ibtusb.inf_amd64_7a73cc2cc004485f\ibtusb.sys {28D8BD3C11854B538A3996B7E4F8EE23}. =>.Intel Corporation

SR - Demand [03/07/2019] [19800424] (igfx) . (.Intel Corporation.) - C:\Windows\System32\DriverStore\FileRepository\iigd_dch.inf_amd64_7d6ad0397c5dc3fd\igdkmd64.sys =>.Intel(R) pGFX®

SR - Auto [03/07/2019] [414056] Intel(R) HD Graphics Control Panel Service (igfxCUIService2.0.0.0) . (.Intel Corporation.) - C:\Windows\System32\

DriverStore\FileRepository\cui_dch.inf_amd64_92cf9d9d84f1d3db\igfxCUIService.exe
=>.Intel(R) pGFX®
SR - Demand [08/04/2020] [7322920] Service for Realtek HD Audio (WDM)
(IntcAzAudAddService) . (.Realtek Semiconductor Corp..) - C:\WINDOWS\System32\
drivers\RTKVHD64.sys =>.Realtek Semiconductor Corp.®
SS - Demand [14/06/2022] [805336] Intel(R) Capability Lice (Intel(R)
Capability Licensing Service TCP IP Interface) . (.Intel(R) Corporation.) - C:\
Windows\System32\DriverStore\FileRepository\
iclsclient.inf_amd64_dec9bbf83f76d9e5\lib\SocketHeciServer.exe
{0082885CBA74ECF5581D8ACC6367A4695E}. =>.Intel(R) Corporation
SR - Auto [14/06/2022] [767432] Intel(R) TPM Provis (Intel(R) TPM
Provisioning Service) . (.Intel(R) Corporation.) - C:\Windows\System32\
DriverStore\FileRepository\iclsclient.inf_amd64_dec9bbf83f76d9e5\lib\
TPMProvisioningService.exe {0082885CBA74ECF5581D8ACC6367A4695E}. =>.Intel(R)
Corporation
SR - Boot [07/05/2022] [187224] (ItSas35i) . (.Avago Technologies.) - C:\
WINDOWS\System32\drivers\ItSas35i.sys =>.Microsoft®
SR - Boot [07/05/2022] [109920] (LSI_SAS) . (.LSI Corporation.) - C:\
WINDOWS\System32\drivers\lsi_sas.sys =>.Microsoft®
SR - Boot [07/05/2022] [125280] (LSI_SAS2i) . (.LSI Corporation.) - C:\
WINDOWS\System32\drivers\lsi_sas2i.sys =>.Microsoft®
SR - Boot [07/05/2022] [138600] (LSI_SAS3i) . (.Avago Technologies.) - C:\
WINDOWS\System32\drivers\lsi_sas3i.sys =>.Microsoft®
SR - Auto [10/05/2022] [3652216] Mise à jour automatique - Index Education
(MajIndexEducationService) . (.Index Education.) - C:\program files (x86)\index
education\mise a jour automatique\ServiceMiseAJourIndex.exe
{59BFA29DD2D6F208659847D2}. =>.Index Education
SR - Boot [07/05/2022] [81752] (megasas2i) . (.Avago Technologies.) - C:\
WINDOWS\System32\drivers\MegaSas2i.sys =>.Microsoft®
SR - Boot [07/05/2022] [101224] (megasas35i) . (.Broadcom Inc.) - C:\
WINDOWS\System32\drivers\megasas35i.sys =>.Microsoft®
SR - Boot [07/05/2022] [576856] (megasr) . (.LSI Corporation, Inc..) - C:\
WINDOWS\System32\drivers\megasr.sys =>.Microsoft®
SR - Demand [14/06/2022] [318112] Intel(R) Management Engine Interfa (MEIx64)
. (.Intel Corporation.) - C:\Windows\System32\DriverStore\FileRepository\
heci.inf_amd64_aa2b01253f0c03cb\x64\TeeDriverW10x64.sys
{0ADE8114D7679B066F2DB2DFD2F67AC2}. =>.Intel Corporation
SR - Demand [07/05/2022] [1132392] Mellanox ConnectX Bus E (mlx4_bus) .
(.Mellanox.) - C:\WINDOWS\System32\drivers\mlx4_bus.sys =>.Microsoft®
SR - Boot [07/05/2022] [90472] (mpi3drvi) . (.Broadcom Limited.) - C:\
WINDOWS\System32\drivers\mpi3drvi.sys =>.Microsoft®
SR - Boot [07/05/2022] [64872] (mvumis) . (.Marvell Semiconductor, Inc..) -
C:\WINDOWS\System32\drivers\mvumis.sys =>.Microsoft®
SR - Demand [07/05/2022] [147304] NetworkDirect Service (ndfltr) .
(.Mellanox.) - C:\WINDOWS\System32\drivers\ndfltr.sys =>.Microsoft®
SR - Demand [07/05/2022] [83288] NDKPerf Driver (NDKPerf) . (.Microsoft.) -
C:\WINDOWS\System32\drivers\NDKPerf.sys =>.Microsoft®
SR - Demand [07/01/2022] [8815680] ___ Intel(R) Wireless Adapter Driver for
Windows 10 - 64 Bit (Netwtw08) . (.Intel Corporation.) - C:\WINDOWS\System32\
drivers\Netwtw08.sys {58B1C1C43E999C1CF7C694A1D776D0FE}. =>.Intel Corporation
SR - Auto [30/08/2022] [1003128] NVIDIA LocalSystem Container
(NvContainerLocalSystem) . (.NVIDIA Corporation.) - C:\Program Files\NVIDIA
Corporation\NvContainer\nvcontainer.exe =>.Nvidia Corporation®
SR - Auto [11/10/2022] [1014784] NVIDIA Display Container LS
(NVDisplay.ContainerLocalSystem) . (.NVIDIA Corporation.) - C:\Windows\System32\
DriverStore\FileRepository\nvaci.inf_amd64_91df09c5579a85f3\Display.NvContainer\
NVDisplay.Container.exe =>.Nvidia Corporation®
SR - Demand [22/07/2022] [130216] Service for NVIDIA High Definition Audio
Driver (NVHDA) . (.NVIDIA Corporation.) - C:\WINDOWS\System32\drivers\
nvhda64v.sys =>.Nvidia Corporation®
SR - Demand [11/10/2022] [56966160] (nvlddmkm) . (.NVIDIA Corporation.) - C:\
Windows\System32\DriverStore\FileRepository\nvaci.inf_amd64_91df09c5579a85f3\
nvlddmkm.sys =>.Nvidia Corporation®

SR - Demand [14/07/2022] [45656] NvModuleTracker (NvModuleTracker) .
(.NVIDIA Corporation.) - C:\Windows\System32\DriverStore\FileRepository\
nvmoduletracker.inf_amd64_0c1cc60a4b422185\NvModuleTracker.sys =>.Nvidia
Corporation®

SR - Boot [07/05/2022] [151392] (nvraid) . (.NVIDIA Corporation.) - C:\
WINDOWS\System32\drivers\nvraid.sys =>.Microsoft®

SR - Boot [07/05/2022] [167256] (nvstor) . (.NVIDIA Corporation.) - C:\
WINDOWS\System32\drivers\nvstor.sys =>.Microsoft®

SR - Demand [15/07/2022] [59368] NVIDIA Virtual Au (nvvad_waveExtensible) .
(.NVIDIA Corporation.) - C:\WINDOWS\System32\drivers\nvvad64v.sys =>.Nvidia
Corporation®

SR - Demand [14/07/2022] [60112] NVVHCI Enumerator Service (nvvhci) .
(.NVIDIA Corporation.) - C:\WINDOWS\System32\drivers\nvvhci.sys =>.Nvidia
Corporation®

SR - System [04/08/2022] [89088] pango_netfilter2 (pango_netfilter2) .
(.Pango Inc.) - C:\WINDOWS\System32\drivers\pango_netfilter2.sys =>.Microsoft®

SR - Boot [07/05/2022] [59752] (percsas2i) . (.Avago Technologies.) - C:\
WINDOWS\System32\drivers\percsas2i.sys =>.Microsoft®

SR - Boot [07/05/2022] [69464] (percsas3i) . (.Avago Technologies.) - C:\
WINDOWS\System32\drivers\percsas3i.sys =>.Microsoft®

SS - Demand [24/04/2019] [820016] Predator Service (PSSvc) . (.Acer
Incorporated.) - C:\Program Files\Acer\NitroSense Service\PSSvc.exe =>.Acer
Incorporated®

SR - Boot [07/05/2022] [45408] pvscsi Storage Controller Dr (pvscsi) .
(.VMware, Inc..) - C:\WINDOWS\System32\drivers\pvscsii.sys =>.Microsoft®

SS - Demand [03/01/2022] [466080] Quick Access Local Service (QALSvc) .
(.Acer Incorporated.) - C:\Program Files\Acer\Quick Access Service\QALSvc.exe
{1CA1247CCA4C07CD3F3751E8}. =>.Acer Incorporated

SS - Demand [03/01/2022] [504480] Quick Access Service (QASvc) . (.Acer
Incorporated.) - C:\Program Files\Acer\Quick Access Service\QASvc.exe
{1CA1247CCA4C07CD3F3751E8}. =>.Acer Incorporated

SR - Demand [30/08/2021] [33680] ROG Keyboard (ROGKB) . (.ASUSTeK Computer
Inc..) - C:\Windows\System32\DriverStore\FileRepository\
rogkb.inf_amd64_9c19ffffb5d62d536\ROGKB.sys =>.ASUSTeK Computer Inc.®

SR - Demand [30/08/2021] [33184] ROG Mouse (ROGMS) . (.ASUSTeK Computer
Inc..) - C:\Windows\System32\DriverStore\FileRepository\
rogms.inf_amd64_94d9766656ff6011\ROGMS.sys =>.ASUSTeK Computer Inc.®

SR - Demand [07/05/2022] [98304] Microsoft Route Poli (RoutePolicy) . (...)
- C:\WINDOWS\System32\drivers\RoutePolicy.sys [Unsigned]

SR - Auto [12/10/2021] [2244800] Intel(R) Storage Midd (RstMwService) .
(.Intel Corporation.) - C:\Windows\System32\DriverStore\FileRepository\
iastorac.inf_amd64_ba273d0ffb93e225\RstMwService.exe
{34770BB53021480D308F5E5593B49D84}. =>.Intel Corporation

SR - Demand [18/08/2022] [1188672] Realtek RT640 NT Driver (rt640x64) .
(.Realtek.) - C:\WINDOWS\System32\drivers\rt640x64.sys =>.Realtek Semiconductor
Corp.®

SR - System [03/09/2018] [70560] Realtek LightWeight Filter (NDIS6.4 (rtf64)
(.Realtek.) - C:\WINDOWS\System32\DRIVERS\rtf64x64.sys =>.Realtek
Semiconductor Corp.®

SR - Auto [08/04/2020] [1093872] Realtek Audio Universal Service
(RtkAudioUniversalService) . (.Realtek Semiconductor.) - C:\WINDOWS\System32\
RtkAudUService64.exe =>.Realtek Semiconductor Corp.®

SR - Boot [07/05/2022] [45920] (SiSRaid2) . (.Silicon Integrated Systems
Corp..) - C:\WINDOWS\System32\drivers\SiSRaid2.sys =>.Microsoft®

SR - Boot [07/05/2022] [82784] (SiSRaid4) . (.Silicon Integrated
Systems.) - C:\WINDOWS\System32\drivers\sisraid4.sys =>.Microsoft®

SR - Boot [07/05/2022] [210784] (SmartSAMD) . (.Microsemi Corportation.) -
C:\WINDOWS\System32\drivers\SmartSAMD.sys =>.Microsoft®

SR - Demand [08/10/2021] [167544] SAMSUNG Mobile USB Modem Drivers (DEVGURU
Ver.) (ssudmdm) . (.Samsung Electronics Co., Ltd..) - C:\WINDOWS\System32\
DRIVERS\ssudmdm.sys =>.Samsung Electronics Co., Ltd.®

SR - Boot [07/05/2022] [32080] (stexstor) . (.Promise Technology, Inc..)
- C:\WINDOWS\System32\drivers\stexstor.sys =>.Microsoft®

SR - Demand [25/09/2020] [38656] TunnelBear Adapter V9 (tap-tb-0901) . (.The OpenVPN Project.) - C:\WINDOWS\System32\drivers\tap-tb-0901.sys =>.TunnelBear, Inc.®

SR - Demand [23/10/2019] [39920] TAP-Windows Adapter V9 (tap0901) . (.The OpenVPN Project.) - C:\WINDOWS\System32\drivers\tap0901.sys =>.Microsoft®

SR - Demand [06/07/2018] [54896] Windscribe VPN (tapwindscribe0901) . (.The OpenVPN Project.) - C:\WINDOWS\System32\drivers\tapwindscribe0901.sys =>.Windscribe Limited®

SR - Demand [14/10/2022] [37888] USBDeviceShare USB Device Stub (udsstub) . (.SysNucleus.) - C:\WINDOWS\System32\drivers\udsstub.sys [Unsigned] =>.SysNucleus

SS - Demand [17/12/2018] [305984] User Experience Improvement Program (UEIPSvc) . (.Acer Incorporated.) - C:\Program Files\Acer\User Experience Improvement Program Service\Framework\UBTService.exe =>.Acer Incorporated®

SR - Demand [14/07/2019] [67448] vJoy Device (vjoy) . (.Shaul Eizikovich.) - C:\WINDOWS\System32\drivers\vjoy.sys {08DF1FFB8B0EEF71ED9573AAE3ECFCDC}. =>.Shaul Eizikovich

SR - Boot [07/05/2022] [167784] (vsmraid) . (.VIA Technologies Inc.,Ltd.) - C:\WINDOWS\System32\drivers\vsmraid.sys =>.Microsoft®

SR - Boot [07/05/2022] [306512] VIA StorX Storage RAID Co (VSTXRAID) . (.VIA Corporation.) - C:\WINDOWS\System32\drivers\vstxraid.sys =>.Microsoft®

SR - Auto [31/01/2019] [1127320] Waves Audio Services (WavesSysSvc) . (.Waves Audio Ltd..) - C:\Windows\System32\DriverStore\FileRepository\wavesapo77ac.inf_amd64_d5839c9d7c0bda64\WavesSysSvc64.exe =>.Waves Inc®

SR - Auto [19/01/2019] [493232] WindscribeService (WindscribeService) . (.Windscribe Limited.) - C:\Program Files (x86)\Windscribe\WindscribeService.exe =>.Windscribe Limited®

SR - Demand [07/05/2022] [37224] WinMad Service (WinMad) . (.Mellanox.) - C:\WINDOWS\System32\drivers\winmad.sys =>.Microsoft®

SR - System [00/00/0000] [0] WinSetupMon (WinSetupMon) . (...) - C:\WINDOWS\System32\DRIVERS\WinSetupMon.sys (.not file.) [Unsigned]

SR - Demand [07/05/2022] [74096] WinVerbs Service (WinVerbs) . (.Mellanox.) - C:\WINDOWS\System32\drivers\winverbs.sys =>.Microsoft®

SR - Auto [14/06/2022] [171672] Intel(R) Management Engine WMI Provider Registration (WMIRegistrationService) . (.Intel Corporation.) - C:\Windows\System32\DriverStore\FileRepository\mewmiprov.inf_amd64_21e0cf0737fd48af\WMIRegistrationService.exe {0ADE8114D7679B066F2DB2DFD2F67AC2}. =>.Intel Corporation

---\ Task Planned Automatically (Register) (50) - 8s

038 - TASK: {03EDBFAC-7518-4E18-ABC2-CBCA87C077D2} [64Bits][\Software Update Application] - (.Acer Incorporated - ListCheck.) -- C:\ProgramData\OEM\UpgradeTool\ListCheck.exe [461472] =>.Acer Incorporated

038 - TASK: {08BD09F4-BBD5-4759-9418-2A6680D41823} [64Bits][\Microsoft\Windows\PI\SecureBootEncodeUEFI] - (...) -- C:\WINDOWS\system32\SecureBootEncodeUEFI.exe [49152]

038 - TASK: {1486BE54-BC65-4176-97C9-DB859F05FE4D} [64Bits][\ACCAgent] - (.Acer Inc. - LiveUpdate Agent.) -- C:\Program Files (x86)\Acer\Care Center\LiveUpdateAgent.exe [41776] Acer Inc. =>Acer Inc.

038 - TASK: {30CABB4C-0880-401F-8E66-4101F832EA70} [64Bits][\DropboxUpdateTaskMachineUA] - (.Dropbox, Inc. - Dropbox Update.) -- C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe [130320] =>.Dropbox, Inc.

038 - TASK: {3A8A744E-2DFE-4C40-B263-4ECE4B3FD854} [64Bits][\UbtFrameworkService] - (.Acer Incorporated - TriggerFramework.) -- C:\Program Files\Acer\User Experience Improvement Program Service\Framework\TriggerFramework.exe [268096] =>.Acer Incorporated

038 - TASK: {42A6005D-FBA6-4F78-96A1-05D75AA0E820} [64Bits][\Quick Access] - (.Acer Incorporated - QALauncher.) -- C:\Program Files\Acer\Quick Access Service\QALauncher.exe [446624] =>.Acer Incorporated

038 - TASK: {4965BFCD-57C3-4B3C-80BF-27F45926DAD1} [64Bits][\NvTmRep_CrashReport2_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation - NVIDIA crash and telemetry reporter.) -- C:\Program Files\NVIDIA Corporation\NvBackend\NvTmRep.exe [1655864] =>.NVIDIA Corporation

038 - TASK: {54A6C967-C475-4784-9F34-167FAFAD1D14} [64Bits][\GoogleUpdateTaskMachineCore] - (.Google Inc. - Google Installer.) -- C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [144200] =>.Google Inc.

038 - TASK: {5D4D1A33-C0C6-43B7-8E3E-4B1C98A5541F} [64Bits][\NvDriverUpdateCheckDaily_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe [1003128] =>.NVIDIA Corporation

038 - TASK: {70433FB2-D7FD-41CF-B6D8-A47B4A75D1E8} [64Bits][\gxx speed launcher] - (.Garena Online - Garena Platform.) -- C:\Program Files (x86)\Garena\Garena\Garena.exe [457600] =>.Garena Online

038 - TASK: {8ACFC7F5-44C7-4473-9FE2-7F744E4C6218} [64Bits][\NvNodeLauncher_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation - NVIDIA nodejs launcher.) -- C:\Program Files (x86)\NVIDIA Corporation\NvNode\nvnodejslauncher.exe [649784] =>.NVIDIA Corporation

038 - TASK: {8F3E970D-573B-4366-B4AC-FE1CB3910584} [64Bits][\ACCBbackgroundApplication] - (.Acer Inc. - ACCStd.) -- C:\Program Files (x86)\Acer\Care Center\ACCStd.exe [4794672] Acer Inc. =>Acer Inc.

038 - TASK: {99832C5D-640F-4460-8644-DB928C34B06A} [64Bits][\ACC] - (.ASUSTeK - LiveUpdate Checker.) -- C:\Program Files (x86)\Acer\Care Center\LiveUpdateChecker.exe [2935088] =>.ASUSTeK

038 - TASK: {9F5C5860-10A1-42BA-A772-B72AE3D6F8DA} [64Bits][\UEIPInvitation] - (.Acer Incorporated - UEIPOBECHECK.) -- C:\Program Files\Acer\User Experience Improvement Program Service\Framework\UEIPOBECHECK.exe [2211136] =>.Acer Incorporated

038 - TASK: {A2EA9B18-A54C-49EE-8DDE-5E9A04BEEB11} [64Bits][\Power Button] - (.Acer Incorporated - ePowerButton_NB.) -- C:\Program Files\Acer\Quick Access Service\ePowerButton_NB.exe [2771616] =>.Acer Incorporated

038 - TASK: {A33EEA71-4AFB-46AB-875E-7B71061F4789} [64Bits][\NvProfileUpdaterDaily_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation - NVIDIA driver profile updater.) -- C:\Program Files\NVIDIA Corporation\Update Core\NvProfileUpdater64.exe [908856] =>.NVIDIA Corporation

038 - TASK: {B9B8EC6F-8C5C-4211-A2C5-A418DFFF6771} [64Bits][\NvTmRep_CrashReport4_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation - NVIDIA crash and telemetry reporter.) -- C:\Program Files\NVIDIA Corporation\NvBackend\NvTmRep.exe [1655864] =>.NVIDIA Corporation

038 - TASK: {BE10932C-EA86-490E-B156-A7F5F22ADAB5} [64Bits][\NvProfileUpdaterOnLogon_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation - NVIDIA driver profile updater.) -- C:\Program Files\NVIDIA Corporation\Update Core\NvProfileUpdater64.exe [908856] =>.NVIDIA Corporation

038 - TASK: {C0D2DA12-E040-4ED3-B960-8735A68B7AA5} [64Bits][\NvTmRep_CrashReport1_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation - NVIDIA crash and telemetry reporter.) -- C:\Program Files\NVIDIA Corporation\NvBackend\NvTmRep.exe [1655864] =>.NVIDIA Corporation

038 - TASK: {C144562A-1482-4317-8CB4-23966FEFDF73} [64Bits][\NvTmRep_CrashReport3_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation - NVIDIA crash and telemetry reporter.) -- C:\Program Files\NVIDIA Corporation\NvBackend\NvTmRep.exe [1655864] =>.NVIDIA Corporation

038 - TASK: {C64617B6-1E5F-498D-BE04-A23F7B440A58} [64Bits][\NitroSense] - (.Acer Incorporated - PSLauncher.) -- C:\Program Files\Acer\NitroSense Service\PSLauncher.exe [601904] =>.Acer Incorporated

038 - TASK: {CAC718F6-D039-4791-A46B-1B57603237D7} [64Bits][\NVIDIA GeForce Experience SelfUpdate_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}] - (.NVIDIA Corporation - NVIDIA GeForce Experience.) -- C:\Program Files\NVIDIA Corporation\NVIDIA GeForce Experience\NVIDIA GeForce Experience.exe [3342376] =>.NVIDIA Corporation

038 - TASK: {DFB6874E-2D5C-424B-9335-9C859AE1DBB1} [64Bits][\AcerNetworkOptimizerStart] - (.2019 Realtek Semiconductor Corp. All rights reserved. - Acer Network Optimizer.) -- C:\Program Files (x86)\Acer\Acer Network Optimizer\AcerNetworkOptimizer.exe [1987584]

038 - TASK: {E4E274F5-B479-4B3A-BED0-B94A17F35444} [64Bits][\DropboxUpdateTaskMachineCore] - (.Dropbox, Inc. - Dropbox Update.) -- C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe [130320] =>.Dropbox, Inc.

038 - TASK: {EB9B0807-8E75-48A8-A400-BDAB1F556FB7} [64Bits][\GoogleUpdateTaskMachineUA] - (.Google Inc. - Google Installer.) -- C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [144200] =>.Google Inc.
C:\WINDOWS\System32\Tasks\Software Update Application - (.Acer Incorporated.) -- C:\ProgramData\OEM\UpgradeTool\ListCheck.exe [] =>.Acer Incorporated
C:\WINDOWS\System32\Tasks\Microsoft\Windows\PI\SecureBootEncodeUEFI - (...) -- C:\WINDOWS\system32\SecureBootEncodeUEFI.exe []
C:\WINDOWS\System32\Tasks\ACCAgent - (.Acer Inc..) -- C:\Program Files (x86)\Acer\Care Center\LiveUpdateAgent.exe [] Acer Inc. =>Acer Inc.
C:\WINDOWS\System32\Tasks\DropboxUpdateTaskMachineUA - (.Dropbox, Inc..) -- C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe [/ua ./ua] =>.Dropbox, Inc.
C:\WINDOWS\System32\Tasks\UbtFrameworkService - (.Acer Incorporated.) -- C:\Program Files\Acer\User Experience Improvement Program Service\Framework\TriggerFramework.exe [] =>.Acer Incorporated
C:\WINDOWS\System32\Tasks\Quick Access - (.Acer Incorporated.) -- C:\Program Files\Acer\Quick Access Service\QALauncher.exe [] =>.Acer Incorporated
C:\WINDOWS\System32\Tasks\NvTmRep_CrashReport2_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files\NVIDIA Corporation\NvBackend\NvTmRep.exe [] =>.NVIDIA Corporation
C:\WINDOWS\System32\Tasks\GoogleUpdateTaskMachineCore - (.Google Inc..) -- C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [/c] =>.Google Inc.
C:\WINDOWS\System32\Tasks\NvDriverUpdateCheckDaily_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe [-d 'C:\Program Files\NVIDIA Corporation\NvDriverUpdateCheck' -l 3 -f C:\ProgramData\NVIDIA\NvContain] =>.NVIDIA Corporation
C:\WINDOWS\System32\Tasks\gxx speed launcher - (.Garena Online.) -- C:\Program Files (x86)\Garena\Garena\Garena.exe [-silentlaunch -gxxsvclaunch.-silentlaunch] =>.Garena Online
C:\WINDOWS\System32\Tasks\NvNodeLauncher_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files (x86)\NVIDIA Corporation\NvNode\nvnodejslauncher.exe [--launcher=TaskScheduler] =>.NVIDIA Corporation
C:\WINDOWS\System32\Tasks\ACCBackgroundApplication - (.Acer Inc..) -- C:\Program Files (x86)\Acer\Care Center\ACCStd.exe [] Acer Inc. =>Acer Inc.
C:\WINDOWS\System32\Tasks\ACC - (.ASUSTeK.) -- C:\Program Files (x86)\Acer\Care Center\LiveUpdateChecker.exe [-auto] =>.ASUSTeK
C:\WINDOWS\System32\Tasks\UEIPIInvitation - (.Acer Incorporated.) -- C:\Program Files\Acer\User Experience Improvement Program Service\Framework\UEIPOBEChech.exe [] =>.Acer Incorporated
C:\WINDOWS\System32\Tasks\Power Button - (.Acer Incorporated.) -- C:\Program Files\Acer\Quick Access Service\ePowerButton_NB.exe [-s] =>.Acer Incorporated
C:\WINDOWS\System32\Tasks\NvProfileUpdaterDaily_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files\NVIDIA Corporation\Update Core\NvProfileUpdater64.exe [] =>.NVIDIA Corporation
C:\WINDOWS\System32\Tasks\NvTmRep_CrashReport4_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files\NVIDIA Corporation\NvBackend\NvTmRep.exe [] =>.NVIDIA Corporation
C:\WINDOWS\System32\Tasks\NvProfileUpdaterOnLogon_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files\NVIDIA Corporation\Update Core\NvProfileUpdater64.exe [] =>.NVIDIA Corporation
C:\WINDOWS\System32\Tasks\NvTmRep_CrashReport1_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files\NVIDIA Corporation\NvBackend\NvTmRep.exe [] =>.NVIDIA Corporation
C:\WINDOWS\System32\Tasks\NvTmRep_CrashReport3_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files\NVIDIA Corporation\NvBackend\NvTmRep.exe [] =>.NVIDIA Corporation
C:\WINDOWS\System32\Tasks\NitroSense - (.Acer Incorporated.) -- C:\Program Files\Acer\NitroSense Service\PSLauncher.exe [] =>.Acer Incorporated
C:\WINDOWS\System32\Tasks\NVIDIA GeForce Experience SelfUpdate_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} - (.NVIDIA Corporation.) -- C:\Program Files\NVIDIA Corporation\NVIDIA GeForce Experience\NVIDIA GeForce Experience.exe [] =>.NVIDIA Corporation

C:\WINDOWS\System32\Tasks\AcerNetworkOptimizerStart - (.2019 Realtek Semiconductor Corp. All rights reserved..) -- C:\Program Files (x86)\Acer\Acer Network Optimizer\AcerNetworkOptimizer.exe [/hw]
C:\WINDOWS\System32\Tasks\DropboxUpdateTaskMachineCore - (.Dropbox, Inc..) -- C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe [/c] =>.Dropbox, Inc.
C:\WINDOWS\System32\Tasks\GoogleUpdateTaskMachineUA - (.Google Inc..) -- C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [/ua ./ua] =>.Google Inc.

---\ Auto loading programs from Registry and folders (18) - 1s

04 - HKLM\..\Run: [SecurityHealth] . (.Microsoft Corporation - Windows Security notification icon.) -- C:\WINDOWS\system32\SecurityHealthSystray.exe [Unsigned] =>.Microsoft Corporation
04 - HKLM\..\Run: [RtkAudUService] . (.Realtek Semiconductor - Realtek HD Audio Universal Service.) -- C:\WINDOWS\System32\RtkAudUService64.exe [Unsigned] =>.Realtek Semiconductor
04 - HKLM\..\Run: [WavesSvc] . (.Waves Audio Ltd. - Waves MaxxAudio Service Application.) -- C:\Windows\System32\DriverStore\FileRepository\wavesapo77ac.inf_amd64_d5839c9d7c0bda64\WavesSvc64.exe =>.Waves Inc®
04 - HKLM\..\Run: [LogiOptions] . (.Logitech, Inc. - LogiOptions.exe (UNICODE).) -- C:\Program Files\Logitech\LogiOptions\LogiOptions.exe =>.Logitech Inc®
04 - HKCU\..\Run: [OneDrive] . (.Microsoft Corporation - Microsoft OneDrive.) -- C:\Users\User\AppData\Local\Microsoft\OneDrive\OneDrive.exe =>.Microsoft®
04 - HKCU\..\Run: [Azureus] . (.Azureus Software, Inc - Vuze Launcher.) -- C:\Program Files\Vuze\Azureus.exe =>.Azureus Software, Inc.®
04 - HKCU\..\Run: [EpicGamesLauncher] . (.Epic Games, Inc. - EpicGamesLauncher.) -- C:\Program Files (x86)\Epic Games\Launcher\Portal\Binaries\Win64\EpicGamesLauncher.exe =>.Epic Games Inc.®
04 - HKCU\..\Run: [MicrosoftEdgeAutoLaunch_C46CFC0629905CC775E70B50EA8A519C] . (...) -- . [Unsigned]
04 - HKUS\S-1-5-19\..\Run: [OneDriveSetup] . (.Microsoft Corporation - Microsoft OneDrive (64 bit) Setup.) -- C:\Windows\System32\OneDriveSetup.exe [Unsigned] =>.Microsoft Corporation
04 - HKUS\S-1-5-20\..\Run: [OneDriveSetup] . (.Microsoft Corporation - Microsoft OneDrive (64 bit) Setup.) -- C:\Windows\System32\OneDriveSetup.exe [Unsigned] =>.Microsoft Corporation
04 - HKUS\S-1-5-19\..\RunOnce: [WAB Migrate] . (.Microsoft Corporation - Windows Contacts.) -- C:\Program Files\Windows Mail\wab.exe [Unsigned] =>.Microsoft Corporation
04 - HKUS\S-1-5-20\..\RunOnce: [WAB Migrate] . (.Microsoft Corporation - Windows Contacts.) -- C:\Program Files\Windows Mail\wab.exe [Unsigned] =>.Microsoft Corporation
04 - HKLM\..\Wow6432Node\Run: [Dropbox] . (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe =>.Dropbox, Inc®
04 - HKLM\..\Wow6432Node\Run: [EPSON_UD_START] . (.SEIKO EPSON CORPORATION - Epson USB Display Ver.1.51.) -- C:\Program Files (x86)\EPSON Projector\Epson USB Display V1.5\EMP_UD.exe =>.SEIKO EPSON Corporation®
04 - HKUS\S-1-5-21-3140157745-1616442026-3104895479-1001\..\Run: [OneDrive] . (.Microsoft Corporation - Microsoft OneDrive.) -- C:\Users\User\AppData\Local\Microsoft\OneDrive\OneDrive.exe =>.Microsoft®
04 - HKUS\S-1-5-21-3140157745-1616442026-3104895479-1001\..\Run: [Azureus] . (.Azureus Software, Inc - Vuze Launcher.) -- C:\Program Files\Vuze\Azureus.exe =>.Azureus Software, Inc.®
04 - HKUS\S-1-5-21-3140157745-1616442026-3104895479-1001\..\Run: [EpicGamesLauncher] . (.Epic Games, Inc. - EpicGamesLauncher.) -- C:\Program Files (x86)\Epic Games\Launcher\Portal\Binaries\Win64\EpicGamesLauncher.exe =>.Epic Games Inc.®
04 - HKUS\S-1-5-21-3140157745-1616442026-3104895479-1001\..\Run: [MicrosoftEdgeAutoLaunch_C46CFC0629905CC775E70B50EA8A519C] . (...) -- . [Unsigned]

---\ Process running (57) - 10s

[MD5.BE426CBCBD1C91B7AD526DAE1C94B54B] - (.Intel Corporation - igfxCUIService Module.) -- C:\Windows\System32\DriverStore\FileRepository\

cui_dch.inf_amd64_92cf9d9d84f1d3db\igfxcUIService.exe [414056] [PID.2152]
=>.Intel(R) pGFX®
[MD5.A84A1262B5BBBC70D63016355A6DAAD] - (.NVIDIA Corporation - NVIDIA Container.) -- C:\Windows\System32\DriverStore\FileRepository\nvaci.inf_amd64_91df09c5579a85f3\Display.NvContainer\NvDisplay.Container.exe [1014784] [PID.2348] =>.Nvidia Corporation®
[MD5.2314FA0A951DBE97F9A1B69224BBFA70] - (.Garena Online - Garena platform service.) -- C:\Program Files (x86)\Garena\Garena\2.0.1909.2618\gxxsvc.exe [320512] [PID.2500] {46A0800C34C5FEE85DB1758D556C2D0E}. =>.Garena Online
[MD5.A84A1262B5BBBC70D63016355A6DAAD] - (.NVIDIA Corporation - NVIDIA Container.) -- C:\Windows\System32\DriverStore\FileRepository\nvaci.inf_amd64_91df09c5579a85f3\Display.NvContainer\NvDisplay.Container.exe [1014784] [PID.2936] =>.Nvidia Corporation®
[MD5.53D3C02D32D633D99609B94A86F44601] - (.Index Education - .) -- C:\program files (x86)\index education\mise a jour automatique\ServiceMiseAJourIndex.exe [3652216] [PID.4336] {59BFA29DD2D6F208659847D2}. =>.Index Education
[MD5.EA159236136380086D3DF5D5B14EC337] - (.Dropbox, Inc. - Dropbox Service.) -- C:\Windows\System32\DbxSvc.exe [46824] [PID.4800] [Unsigned] =>.Dropbox, Inc.
[MD5.0CD3BD824DA8047219959DACB45943B8] - (.Acer Incorporated - ACCSvc.) -- C:\Program Files (x86)\Acer\Care Center\ACCSvc.exe [300336] [PID.4820] =>.Acer Incorporated®
[MD5.D6EBDCC8AFA123E3265F1BD36F8B7CAA] - (.Intel Corporation - Intel HD Graphics Drivers for Windows(R).) -- C:\Windows\System32\DriverStore\FileRepository\iigd_dch.inf_amd64_7d6ad0397c5dc3fd\IntelCpHDCPSvc.exe [516696] [PID.4828] =>.Intel(R) pGFX®
[MD5.FAA735CB77474DEB4E4E327340117D3A] - (.SEIKO EPSON CORPORATION - EPSON USB Display Ver.1.50.) -- C:\Program Files (x86)\EPSON Projector\Epson USB Display V1.5\EMP_UDSA.exe [98304] [PID.4860] [Unsigned] =>.Seiko Epson Corporation
[MD5.42435D7D5AD53998CB330F8CD020A574] - (.Pango Inc. - Hss.Service.Application.) -- C:\Program Files (x86)\Hotspot Shield\11.3.0\bin\cmw_srv.exe [247608] [PID.4872] {054E8D30374B037A81D8EC3D5DCCB1D4}. =>.Pango Inc.
[MD5.239E001896C3304EAEC9D2B16DBE3BD] - (.HP Inc. - .) -- C:\Program Files\HP\PrintScanDoctor\HPPrintScanDoctorService.exe [225368] [PID.4880] =>.HP Inc.®
[MD5.E3AD95DA9EE3F655DC97A19CC0746AB9] - (.Foxit Software Inc. - Foxit PDF Reader Update Service.) -- C:\PROGRAM FILES (X86)\FOXIT SOFTWARE\FOXIT READER\FoxitPDFReaderUpdateService.exe [2358800] [PID.4924] {0B022E5567D2577010644DE52C9A3656}. =>.Foxit Software Inc.
[MD5.878EC4C4C1EFA66AAAB836A1A4709627] - (.Realtek Semiconductor - Realtek HD Audio Universal Service.) -- C:\Windows\System32\RtkAudUSvc64.exe [1093872] [PID.5096] [Unsigned] =>.Realtek Semiconductor
[MD5.CBAAFB385D466B9D65A5DFE9A0FABC2D] - (.Intel Corporation - Intel(R) Rapid Storage Technology Managemen.) -- C:\Windows\System32\DriverStore\FileRepository\iastorac.inf_amd64_ba273d0fffb93e225\RstMwService.exe [2244800] [PID.5104] {34770BB53021480D308F5E5593B49D84}. =>.Intel Corporation
[MD5.45E63493AA5450B19C91ECCCF46859A6] - (.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe [1003128] [PID.952] =>.Nvidia Corporation®
[MD5.C46D4D83245CD1AFA3C67BA9A8AC1A1A] - (.Waves Audio Ltd. - WavesSysSvc Service Application.) -- C:\Windows\System32\DriverStore\FileRepository\wavesapo77ac.inf_amd64_d5839c9d7c0bda64\WavesSysSvc64.exe [1127320] [PID.4536] =>.Waves Inc®
[MD5.6E5A6C253AA58A75BD678A09B547339E] - (.Windscribe Limited - Manages the firewall and controls the VPN t.) -- C:\Program Files (x86)\Windscribe\WindscribeService.exe [493232] [PID.4704] =>.Windscribe Limited®
[MD5.ACDE72D3796DAD197F58E387FE3AC392] - (.Intel Corporation - Intel(R) Management Engine WMI Provider Reg.) -- C:\Windows\System32\DriverStore\FileRepository\mewmiprov.inf_amd64_21e0cf0737fd48af\WMIRegistrationService.exe [171672] [PID.5144] {0ADE8114D7679B066F2DB2DFD2F67AC2}. =>.Intel Corporation
[MD5.7BF0600301798142D3298BA2144C05D6] - (.Intel Corporation - IntelCpHeciSvc Executable.) -- C:\Windows\System32\DriverStore\FileRepository\iigd_dch.inf_amd64_7d6ad0397c5dc3fd\IntelCpHeciSvc.exe [508984] [PID.5564] =>.Intel(R) pGFX®

[MD5.8AD76E0B347BB690697535CE95B1C656] - (.Dropbox, Inc. - Dropbox Update.) -- C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe [130320] [PID.7084] =>.Dropbox, Inc®

[MD5.20CB81E8CDEC6790EC9421D2A6D8476F] - (.Intel Corporation - igfxEM Module.) -- C:\Windows\System32\DriverStore\FileRepository\cui_dch.inf_amd64_92cf9d9d84f1d3db\igfxEM.exe [1082424] [PID.7848] =>.Intel(R) pGFX®

[MD5.45E63493AA5450B19C91ECCCF46859A6] - (.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe [1003128] [PID.6580] =>.Nvidia Corporation®

[MD5.822DC710EE8A2C179FE3BE8E29ED3411] - (.Acer Incorporated - PSSvc.) -- C:\Program Files\Acer\NitroSense Service\PSSvc.exe [820016] [PID.8772] =>.Acer Incorporated®

[MD5.381C22092074255A291F4C9946A5C28F] - (.Google LLC - Google Crash Handler.) -- C:\Program Files (x86)\Google\Update\1.3.36.152\GoogleCrashHandler.exe [309720] [PID.9708] =>.Google LLC®

[MD5.F1DE10A8B9909A4AF635112C8866D534] - (.Google LLC - Google Crash Handler.) -- C:\Program Files (x86)\Google\Update\1.3.36.152\GoogleCrashHandler64.exe [408536] [PID.9748] =>.Google LLC®

[MD5.B562E89CA15E65E8040582A1481C1682] - (.Node.js - NVIDIA Web Helper Service.) -- C:\Program Files (x86)\NVIDIA Corporation\NvNode\NVIDIA Web Helper.exe [29447224] [PID.10076] =>.Nvidia Corporation®

[MD5.29311DA0C05E614E722607B9A865CBC9] - (.Acer Incorporated - PSAgent.) -- C:\Program Files\Acer\NitroSense Service\PSAgent.exe [717616] [PID.10340] =>.Acer Incorporated®

[MD5.DB3B521CA60BA9093D0B736BEC64D686] - (.Acer Incorporated - PSAdminAgent.) -- C:\Program Files\Acer\NitroSense Service\PSAdminAgent.exe [849712] [PID.10744] =>.Acer Incorporated®

[MD5.878EC4C4C1EFA66AAAB836A1A4709627] - (.Realtek Semiconductor - Realtek HD Audio Universal Service.) -- C:\Windows\System32\RtkAudUService64.exe [1093872] [PID.13240] [Unsigned] =>.Realtek Semiconductor

[MD5.BAFF94A9811AC9A3F758849E53FF840F] - (.Logitech, Inc. - LogiOptions.exe (UNICODE).) -- C:\Program Files\Logitech\LogiOptions\LogiOptions.exe [1667208] [PID.11068] =>.Logitech Inc®

[MD5.5940EE0CE26DC92908D357700628AA84] - (.Logitech, Inc. - LogiOptionsMgr.exe (UNICODE).) -- C:\ProgramData\Logishrd\LogiOptions\Software\Current\LogiOptionsMgr.exe [14056072] [PID.13052] =>.Logitech Inc®

[MD5.1C5AF95B8D420E744DF8557B71BE8A77] - (.Logitech - Logi Overlay.) -- C:\ProgramData\Logishrd\LogiOptions\Software\Current\LogiOverlay.exe [660104] [PID.8456] =>.Logitech Inc®

[MD5.6B81EE660D76F63EE3E7A277568F01F6] - (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe [11209952] [PID.14248] =>.Dropbox, Inc®

[MD5.6B81EE660D76F63EE3E7A277568F01F6] - (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe [11209952] [PID.13716] =>.Dropbox, Inc®

[MD5.6B81EE660D76F63EE3E7A277568F01F6] - (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe [11209952] [PID.13412] =>.Dropbox, Inc®

[MD5.6B81EE660D76F63EE3E7A277568F01F6] - (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe [11209952] [PID.16964] =>.Dropbox, Inc®

[MD5.6B81EE660D76F63EE3E7A277568F01F6] - (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe [11209952] [PID.17176] =>.Dropbox, Inc®

[MD5.6B81EE660D76F63EE3E7A277568F01F6] - (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe [11209952] [PID.1748] =>.Dropbox, Inc®

[MD5.83CD93BD7DE68220EE9D5B885BCDD1FD] - (.Acer Incorporated - QASvc.) -- C:\Program Files\Acer\Quick Access Service\QASvc.exe [504480] [PID.4852] {1CA1247CCA4C07CD3F3751E8}. =>.Acer Incorporated

[MD5.6B81EE660D76F63EE3E7A277568F01F6] - (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe [11209952] [PID.4900] =>.Dropbox, Inc®

```
[MD5.FE2CC78CE289208BA077F36675227650] - (.Acer Incorporated - QAAgent.) -- C:\
Program Files\Acer\Quick Access Service\QAAgent.exe [479904] [PID.17080]
{1CA1247CCA4C07CD3F3751E8}. =>.Acer Incorporated
[MD5.7218B0C7CDB9959C0EAE8915312D9845] - (.Acer Incorporated - QAAdminAgent.) --
C:\Program Files\Acer\Quick Access Service\QAAdminAgent.exe [660640] [PID.13192]
{1CA1247CCA4C07CD3F3751E8}. =>.Acer Incorporated
[MD5.279E094CB1A2D14167B00FBE51DE9F0A] - (.Intel Corporation - igfxext Module.)
-- C:\Windows\System32\DriverStore\FileRepository\
cui_dch.inf_amd64_92cf9d9d84f1d3db\igfxext.exe [369720] [PID.14684] =>.Intel(R)
pGFX®
[MD5.D6FCDD70625B68BE991226061552B168] - (. - ACCStd.) -- C:\Program Files
(x86)\Acer\Care Center\ACCStd.exe [4794672] [PID.2240] =>.Acer Incorporated®
[MD5.80DBFF1E3542B868A009B902605101F4] - (.Acer Incorporated - ePowerButton_NB.)
-- C:\Program Files\Acer\Quick Access Service\ePowerButton_NB.exe [2771616]
[PID.1836] {1CA1247CCA4C07CD3F3751E8}. =>.Acer Incorporated
[MD5.C345F3E69DC75740B472B6C552855476] - (.Google LLC - Google Chrome.) -- C:\
Program Files (x86)\Google\Chrome\Application\chrome.exe [3217176] [PID.11916]
=>.Google LLC®
[MD5.C345F3E69DC75740B472B6C552855476] - (.Google LLC - Google Chrome.) -- C:\
Program Files (x86)\Google\Chrome\Application\chrome.exe [3217176] [PID.2412]
=>.Google LLC®
[MD5.C345F3E69DC75740B472B6C552855476] - (.Google LLC - Google Chrome.) -- C:\
Program Files (x86)\Google\Chrome\Application\chrome.exe [3217176] [PID.11040]
=>.Google LLC®
[MD5.C345F3E69DC75740B472B6C552855476] - (.Google LLC - Google Chrome.) -- C:\
Program Files (x86)\Google\Chrome\Application\chrome.exe [3217176] [PID.1788]
=>.Google LLC®
[MD5.C345F3E69DC75740B472B6C552855476] - (.Google LLC - Google Chrome.) -- C:\
Program Files (x86)\Google\Chrome\Application\chrome.exe [3217176] [PID.13832]
=>.Google LLC®
[MD5.C345F3E69DC75740B472B6C552855476] - (.Google LLC - Google Chrome.) -- C:\
Program Files (x86)\Google\Chrome\Application\chrome.exe [3217176] [PID.6804]
=>.Google LLC®
[MD5.C345F3E69DC75740B472B6C552855476] - (.Google LLC - Google Chrome.) -- C:\
Program Files (x86)\Google\Chrome\Application\chrome.exe [3217176] [PID.3744]
=>.Google LLC®
[MD5.C345F3E69DC75740B472B6C552855476] - (.Google LLC - Google Chrome.) -- C:\
Program Files (x86)\Google\Chrome\Application\chrome.exe [3217176] [PID.18284]
=>.Google LLC®
[MD5.F1AFCD8EDD78473C040E96F7DDA6E30B] - (. - StoreExperienceHost.) -- C:\
Program Files\WindowsApps\
Microsoft.StorePurchaseApp_12207.44.5.0_x64__8wekyb3d8bbwe\
StoreExperienceHost.exe [19456] [PID.18080] [Unsigned]
[MD5.2B206F67E9BCF6F16ED77428A4FC611C] - (.Nicolas Coolman - ZHPDiag.) -- C:\
Users\User\Downloads\ZHPDiag3.exe [3311304] [PID.756] [Unsigned] =>.Nicolas
Coolman
[MD5.C345F3E69DC75740B472B6C552855476] - (.Google LLC - Google Chrome.) -- C:\
Program Files (x86)\Google\Chrome\Application\chrome.exe [3217176] [PID.2516]
=>.Google LLC®
[MD5.C345F3E69DC75740B472B6C552855476] - (.Google LLC - Google Chrome.) -- C:\
Program Files (x86)\Google\Chrome\Application\chrome.exe [3217176] [PID.3712]
=>.Google LLC®
```

---\ **Google Chrome, Start, Search, Extensions (11) - 1s**

```
G2 - GCE: Preference [User][User Data\Default\Extensions]
[cfhdojbkjhnlbpbkdaibdcddilifddb] eyeo GmbH =>.Eyeo GmbH
G2 - GCE: Preference [User][User Data\Default\Extensions]
[coobgpohoikkiipiblmjeljniedjppf] http://www.google.com/ =>.Google Inc.
{Hidden Chrome extensions}
G2 - GCE: Preference [User][User Data\Default\Extensions]
[ghbmnnjooekpmoecnninlnbdlohkhi] =>.Google Inc. {Docs hors connexion}
G2 - GCE: Preference [User][User Data\Default\Extensions]
[hdokiejnpimakedhajhdlcegeplioahd] LastPass =>.LastPass
```


G2 - GCE: Preference [User][User Data\Default\Extensions]
[mfhcmdonhekjhfbjmeacdjbhlfpgjabb] Web Safety =>.Legitimate
G2 - GCE: Preference [User][User Data\Default\Extensions]
[nmmhkkegccagdldgiimedpiccmgmieda] =>.Google Inc. {Wallet}
G2 - GCE: Preference [User][User Data\Default\Local Extension Settings]
[cfhdojbkjhnklbpkdaibdcddilifddb] =>.eyeo GmbH {AdBlock Plus}
G2 - GCE: Preference [User][User Data\Default\Local Extension Settings]
[ghbmnnjooekpmoecnnlnnbdlolhkh] =>.Google Inc. {Docs hors connexion}
G2 - GCE: Preference [User][User Data\Default\Local Extension Settings]
[mfhcmdonhekjhfbjmeacdjbhlfpgjabb]
G2 - GCE: Preference [User][User Data\Default\Managed Extension Settings]
[cfhdojbkjhnklbpkdaibdcddilifddb] =>.eyeo GmbH {AdBlock Plus}
G2 - GCE: Preference [User][User Data\Default\Sync Extension Settings]
[mfhcmdonhekjhfbjmeacdjbhlfpgjabb]

---\ Mozilla Firefox, Plugins, Start, Search, Extensions (15) - 1s

P2 - EXT FILE: (.English (US) Language Pack - Language pack for Firefox for en-US'.) -- C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\9fzozgr2.default\extensions\langpack-en-US@firefox.mozilla.org.xpi [Unsigned]
P2 - FPN: [HKLM] [@update.ccleanerbrowser.com/CCleaner Browser;version=3] - (.Piriform Software.) -- C:\Program Files (x86)\CCleaner Browser\Update\1.8.1067.0\npCCleanerBrowserUpdate3.dll =>.Piriform Software
P2 - FPN: [HKLM] [@update.ccleanerbrowser.com/CCleaner Browser;version=9] - (.Piriform Software.) -- C:\Program Files (x86)\CCleaner Browser\Update\1.8.1067.0\npCCleanerBrowserUpdate3.dll =>.Piriform Software
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\9fzozgr2.default\crashes =>Mozilla Corporation
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\9fzozgr2.default\datareporting =>Mozilla Corporation
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\9fzozgr2.default\extensions =>Mozilla Corporation
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\9fzozgr2.default\gmp =>Mozilla Corporation
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\9fzozgr2.default\gmp-gmpopenh264 =>Mozilla Corporation
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\9fzozgr2.default\gmp-widevinecdm =>Mozilla Corporation
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\9fzozgr2.default\healthreport =>Mozilla Corporation
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\9fzozgr2.default\minidumps =>Mozilla Corporation
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\9fzozgr2.default\saved-telemetry-pings =>Mozilla Corporation
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\9fzozgr2.default\sessionstore-backups =>Mozilla Corporation
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\9fzozgr2.default\storage =>Mozilla Corporation
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\9fzozgr2.default\webapps =>Mozilla Corporation

---\ Internet Explorer Extensions, Start, Search (16) - 0s

R0 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = http://acer17win10.msn.com/ =>.Microsoft Corporation
R0 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = http://go.microsoft.com/ =>.Microsoft Corporation
R0 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main,Start Page = http://go.microsoft.com/ =>.Microsoft Corporation
R1 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft.com/ =>.Microsoft Corporation
R1 - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Default_Page_URL = http://acer17win10.msn.com/ =>.Microsoft Corporation
R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft.com/ =>.Microsoft Corporation

R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Default_Page_URL = http://go.microsoft.com/ =>.Microsoft Corporation
R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Extensions Off Page = about:noadd-ons =>.Microsoft Corporation
R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Security Risk Page = about:securityrisk =>.Microsoft Corporation
R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Default_Search_URL = http://go.microsoft.com/ =>.Microsoft Corporation
R1 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft.com/ =>.Microsoft Corporation
R1 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main,Default_Page_URL = http://go.microsoft.com/ =>.Microsoft Corporation
R1 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main,Default_Search_URL = http://go.microsoft.com/ =>.Microsoft Corporation
R1 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main,Extensions Off Page = about:noadd-ons =>.Microsoft Corporation
R1 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main,Security Risk Page = about:securityrisk =>.Microsoft Corporation
R3 - URLSearchHook: (no name)[HKCU] - {CFBFAE00-17A6-11D0-99CB-00C04FD64497} . (.Microsoft Corporation - Internet Browser.) (11.00.22621.608 (WinBuild.160101.0800)) -- C:\Windows\System32\ieframe.dll =>.Microsoft Corporation

---\ INTERNET EXPLORER, trusted site and sensitive site (2) - 0s
~ IE Restricted Site Good: localhost
~ Microsoft Internet Explorer Restricted Site(s) Domains: 1(Good) / 0(Bad)

---\ Microsoft Edge,Plugins,Start,Search,Extensions (1) - 0s
E2 - GCE: Preference [User][User Data\Default\Local Extension Settings][jdicldimpdaibmpdkjnbmckianbfold] =>.Microsoft Corporation

---\ Internet Explorer, Proxy Management (3) - 0s
R5 - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyEnable = 0 =>.Default.Value
R5 - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings,MigrateProxy = 1 =>.Default.Value
R5 - HKLM\SYSTEM\CurrentControlSet\services\NlaSvc\Parameters\Internet\ManualProxies [] =>.Microsoft

---\ Line Analysis, IniFiles, Auto loading 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=

---\ Hosts file redirection (1) - 0s
~ Le fichier hôte est sain (The hosts file is clean) (42)

---\ Browser Helper Object (BHO) (1) - 0s
O2 - BHO: IEToEdge BHO [64Bits] - {1FD49718-1D00-4B19-AF5F-070AF6D5D54C} . (.Microsoft Corporation - IEToEdge BHO.) -- C:\Program Files (x86)\Microsoft\Edge\Application\107.0.1418.26\BHO\ie_to_edge_bho_64.dll =>.Microsoft®

---\ Global shortcuts Startup (75) - 5s
04 - GS\Desktop [Administrator]: lubumbashi - Shortcut.lnk . (...) E:\dropbox\Dropbox\lubumbashi [Unsigned]
04 - GS\Desktop [Administrator]: pereir cours - Shortcut.lnk . (...) E:\dropbox\Dropbox\pereir cours [Unsigned]
04 - GS\Desktop [Administrator]: ZHPDiag.lnk . (.Nicolas Coolman - ZHPDiag.) C:\Users\User\AppData\Roaming\ZHP\ZHPDiag3.exe [Unsigned] =>.Nicolas Coolman
04 - GS\Quicklaunch [Administrator]: Adobe Digital Editions 4.5.lnk . (.Adobe Systems Incorporated - Adobe Digital Editions 4.5.11.) C:\Program Files (x86)\Adobe\Adobe Digital Editions 4.5\DigitalEditions.exe =>.Adobe Inc.®

04 - GS\Quicklaunch [Administrator]: Foxit PDF Reader.lnk . (.Foxit Software Inc. - Foxit PDF Reader 12.0.) C:\Program Files (x86)\Foxit Software\Foxit Reader\FoxitPDFReader.exe {0B022E5567D2577010644DE52C9A3656}. =>.Foxit Software Inc.

04 - GS\Quicklaunch [Administrator]: Google Chrome.lnk . (.Google LLC - Google Chrome.) C:\Program Files (x86)\Google\Chrome\Application\chrome.exe =>.Google LLC@

04 - GS\Quicklaunch [Administrator]: Microsoft Edge.lnk . (.Microsoft Corporation - Microsoft Edge.) C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe =>.Microsoft@

04 - GS\Quicklaunch [Administrator]: Vuze.lnk . (.Azureus Software, Inc - .) C:\Program Files (x86)\Vuze\Azureus.exe [Unsigned] =>.Azureus Software, Inc

04 - GS\Quicklaunch [Administrator]: WebZIP.lnk . (.Spidersoft - WebZIP.) E:\siteinterent\WebZIP.exe [Unsigned] =>.Spidersoft

04 - GS\sendTo [Administrator]: Bluetooth File Transfer.LNK . (.Microsoft Corporation - Transfers files between device.) C:\Windows\System32\fsquirt.exe [Unsigned] =>.Microsoft Corporation

04 - GS\sendTo [Administrator]: Fax Recipient.lnk . (.Microsoft Corporation - Microsoft Windows Fax and Scan.) C:\Windows\System32\WFS.exe /SendTo [Unsigned] =>.Microsoft Corporation

04 - GS\TaskBar [Administrator]: calibre 64bit - E-book management.lnk . (...) C:\Program Files\Calibre2\calibre.exe {097F6A856F52B668E857667755982884}.

04 - GS\TaskBar [Administrator]: Google Chrome.lnk . (.Google LLC - Google Chrome.) C:\Program Files (x86)\Google\Chrome\Application\chrome.exe =>.Google LLC@

04 - GS\TaskBar [Administrator]: LibreOffice 7.0.lnk . (.The Document Foundation - LibreOffice, the office produc.) C:\Program Files (x86)\LibreOffice\program\soffice.exe [Unsigned] =>.The Document Foundation

04 - GS\TaskBar [Administrator]: Vuze.lnk . (.Azureus Software, Inc - .) C:\Program Files (x86)\Vuze\Azureus.exe [Unsigned] =>.Azureus Software, Inc

04 - GS\TaskBar [Administrator]: WhatsApp.lnk . (.WhatsApp - WhatsApp.) C:\Users\User\AppData\Local\WhatsApp\WhatsApp.exe {0C16D074311A3365FAE8200C7E160C54}. =>.WhatsApp

04 - GS\Programs [Administrator]: Administrative Tools.lnk . (.Microsoft Corporation - Windows Control Panel.) C:\WINDOWS\system32\control.exe /name Microsoft.AdministrativeTools [Unsigned] =>.Microsoft Corporation

04 - GS\Programs [Administrator]: OneDrive.lnk . (.Microsoft Corporation - Microsoft OneDrive.) C:\Users\User\AppData\Local\Microsoft\OneDrive\OneDrive.exe =>.Microsoft@

04 - GS\Programs [Administrator]: Wii U USB Helper.lnk . (...) E:\usbhelper\USBHelperLauncher.exe [Unsigned]

04 - GS\Desktop [Guest]: lubumbashi - Shortcut.lnk . (...) E:\dropbox\Dropbox\lubumbashi [Unsigned]

04 - GS\Desktop [Guest]: pereir cours - Shortcut.lnk . (...) E:\dropbox\Dropbox\pereir cours [Unsigned]

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

04 - GS\Quicklaunch [Guest]: Adobe Digital Editions 4.5.lnk . (.Adobe Systems Incorporated - Adobe Digital Editions 4.5.11.) C:\Program Files (x86)\Adobe\Adobe Digital Editions 4.5\DigitalEditions.exe =>.Adobe Inc.®

04 - GS\Quicklaunch [Guest]: Foxit PDF Reader.lnk . (.Foxit Software Inc. - Foxit PDF Reader 12.0.) C:\Program Files (x86)\Foxit Software\Foxit Reader\FoxitPDFReader.exe {0B022E5567D2577010644DE52C9A3656}. =>.Foxit Software Inc.

04 - GS\Quicklaunch [Guest]: Google Chrome.lnk . (.Google LLC - Google Chrome.) C:\Program Files (x86)\Google\Chrome\Application\chrome.exe =>.Google LLC@

04 - GS\Quicklaunch [Guest]: Microsoft Edge.lnk . (.Microsoft Corporation - Microsoft Edge.) C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe =>.Microsoft@

04 - GS\Quicklaunch [Guest]: Vuze.lnk . (.Azureus Software, Inc - .) C:\Program Files (x86)\Vuze\Azureus.exe [Unsigned] =>.Azureus Software, Inc

04 - GS\Quicklaunch [Guest]: WebZIP.lnk . (.Spidersoft - WebZIP.) E:\siteinterent\WebZIP.exe [Unsigned] =>.Spidersoft

04 - GS\sendTo [Guest]: Bluetooth File Transfer.LNK . (.Microsoft Corporation - Transfers files between device.) C:\Windows\System32\fsquirt.exe [Unsigned]
=>.Microsoft Corporation

04 - GS\sendTo [Guest]: Fax Recipient.lnk . (.Microsoft Corporation - Microsoft Windows Fax and Scan.) C:\Windows\System32\WFS.exe /SendTo [Unsigned]
=>.Microsoft Corporation

04 - GS\TaskBar [Guest]: calibre 64bit - E-book management.lnk . (...) C:\Program Files\Calibre2\calibre.exe {097F6A856F52B668E857667755982884}.

04 - GS\TaskBar [Guest]: Google Chrome.lnk . (.Google LLC - Google Chrome.) C:\Program Files (x86)\Google\Chrome\Application\chrome.exe =>.Google LLC®

04 - GS\TaskBar [Guest]: LibreOffice 7.0.lnk . (.The Document Foundation - LibreOffice, the office produc.) C:\Program Files (x86)\LibreOffice\program\soffice.exe [Unsigned] =>.The Document Foundation

04 - GS\TaskBar [Guest]: Vuze.lnk . (.Azureus Software, Inc - .) C:\Program Files (x86)\Vuze\Azureus.exe [Unsigned] =>.Azureus Software, Inc

04 - GS\TaskBar [Guest]: WhatsApp.lnk . (.WhatsApp - WhatsApp.) C:\Users\User\AppData\Local\WhatsApp\WhatsApp.exe {0C16D074311A3365FAE8200C7E160C54}.

=>.WhatsApp

04 - GS\Programs [Guest]: Administrative Tools.lnk . (.Microsoft Corporation - Windows Control Panel.) C:\WINDOWS\system32\control.exe /name Microsoft.AdministrativeTools [Unsigned] =>.Microsoft Corporation

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

04 - GS\Programs [Guest]: Wii U USB Helper.lnk . (...) E:\usbhelper\USBHelperLauncher.exe [Unsigned]

04 - GS\Desktop [User]: lubumbashi - Shortcut.lnk . (...) E:\dropbox\Dropbox\lubumbashi [Unsigned]

04 - GS\Desktop [User]: pereir cours - Shortcut.lnk . (...) E:\dropbox\Dropbox\pereir cours [Unsigned]

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

04 - GS\Quicklaunch [User]: Adobe Digital Editions 4.5.lnk . (.Adobe Systems Incorporated - Adobe Digital Editions 4.5.11.) C:\Program Files (x86)\Adobe\Adobe Digital Editions 4.5\DigitalEditions.exe =>.Adobe Inc.®

04 - GS\Quicklaunch [User]: Foxit PDF Reader.lnk . (.Foxit Software Inc. - Foxit PDF Reader 12.0.) C:\Program Files (x86)\Foxit Software\Foxit Reader\FoxitPDFReader.exe {0B022E5567D2577010644DE52C9A3656}. =>.Foxit Software Inc.

04 - GS\Quicklaunch [User]: Google Chrome.lnk . (.Google LLC - Google Chrome.) C:\Program Files (x86)\Google\Chrome\Application\chrome.exe =>.Google LLC®

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

04 - GS\Quicklaunch [User]: Vuze.lnk . (.Azureus Software, Inc - .) C:\Program Files (x86)\Vuze\Azureus.exe [Unsigned] =>.Azureus Software, Inc

04 - GS\Quicklaunch [User]: WebZIP.lnk . (.Spidersoft - WebZIP.) E:\siteinterent\WebZIP.exe [Unsigned] =>.Spidersoft

04 - GS\sendTo [User]: Bluetooth File Transfer.LNK . (.Microsoft Corporation - Transfers files between device.) C:\Windows\System32\fsquirt.exe [Unsigned]
=>.Microsoft Corporation

04 - GS\sendTo [User]: Fax Recipient.lnk . (.Microsoft Corporation - Microsoft Windows Fax and Scan.) C:\Windows\System32\WFS.exe /SendTo [Unsigned]
=>.Microsoft Corporation

04 - GS\TaskBar [User]: calibre 64bit - E-book management.lnk . (...) C:\Program Files\Calibre2\calibre.exe {097F6A856F52B668E857667755982884}.

04 - GS\TaskBar [User]: Google Chrome.lnk . (.Google LLC - Google Chrome.) C:\Program Files (x86)\Google\Chrome\Application\chrome.exe =>.Google LLC®

04 - GS\TaskBar [User]: LibreOffice 7.0.lnk . (.The Document Foundation - LibreOffice, the office produc.) C:\Program Files (x86)\LibreOffice\program\soffice.exe [Unsigned] =>.The Document Foundation

04 - GS\TaskBar [User]: Vuze.lnk . (.Azureus Software, Inc - .) C:\Program Files (x86)\Vuze\Azureus.exe [Unsigned] =>.Azureus Software, Inc

04 - GS\TaskBar [User]: WhatsApp.lnk . (.WhatsApp - WhatsApp.) C:\Users\User\AppData\Local\WhatsApp\WhatsApp.exe {0C16D074311A3365FAE8200C7E160C54}. =>.WhatsApp

04 - GS\Programs [User]: Administrative Tools.lnk . (.Microsoft Corporation - Windows Control Panel.) C:\WINDOWS\system32\control.exe /name Microsoft.AdministrativeTools [Unsigned] =>.Microsoft Corporation

04 - GS\Programs [User]: OneDrive.lnk . (.Microsoft Corporation - Microsoft OneDrive.) C:\Users\User\AppData\Local\Microsoft\OneDrive\OneDrive.exe =>.Microsoft@

04 - GS\Programs [User]: Wii U USB Helper.lnk . (...) E:\usbhelper\USBHelperLauncher.exe [Unsigned]

04 - GS\Programs [Public]: Administrative Tools.lnk . (.Microsoft Corporation - Windows Control Panel.) C:\WINDOWS\system32\control.exe /name Microsoft.AdministrativeTools [Unsigned] =>.Microsoft Corporation

04 - GS\Programs [Public]: OneDrive.lnk . (.Microsoft Corporation - Microsoft OneDrive.) C:\Users\User\AppData\Local\Microsoft\OneDrive\OneDrive.exe =>.Microsoft@

04 - GS\Programs [Public]: Wii U USB Helper.lnk . (...) E:\usbhelper\USBHelperLauncher.exe [Unsigned]

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

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

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

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

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

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

04 - GS\ProgramsCommon [Public]: Adobe Digital Editions 4.5.lnk . (.Adobe Systems Incorporated - Adobe Digital Editions 4.5.11.) C:\Program Files (x86)\Adobe\Adobe Digital Editions 4.5\DigitalEditions.exe =>.Adobe Inc.®

04 - GS\ProgramsCommon [Public]: Adobe Reader 6.0.lnk . (...) C:\WINDOWS\Installer\{AC76BA86-7AD7-1036-7B44-000000000001}\SC_Reader_PM.ico [Unsigned]

04 - GS\ProgramsCommon [Public]: Epic Games Launcher.lnk . (.Epic Games, Inc. - UnrealEngineLauncherProxy.) C:\Program Files (x86)\Epic Games\Launcher\Portal\Binaries\Win32\EpicGamesLauncher.exe =>.Epic Games Inc.®

04 - GS\ProgramsCommon [Public]: Google Chrome.lnk . (.Google LLC - Google Chrome.) C:\Program Files (x86)\Google\Chrome\Application\chrome.exe =>.Google LLC®

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

04 - GS\ProgramsCommon [Public]: Movie Maker.lnk . (.Microsoft Corporation - Movie Maker.) C:\Program Files (x86)\Windows Live\Photo Gallery\MovieMaker.exe =>.Microsoft@

04 - GS\ProgramsCommon [Public]: PC Health Check.lnk . (...) C:\Program Files (x86)\PCHealthCheck\PCHealthCheck.exe [Unsigned] =>.Microsoft Corporation

04 - GS\ProgramsCommon [Public]: Photo Gallery.lnk . (.Microsoft Corporation - Photo Gallery.) C:\Program Files (x86)\Windows Live\Photo Gallery\WLXPhotoGallery.exe =>.Microsoft@

04 - GS\ProgramsCommon [Public]: Vuze.lnk . (.Azureus Software, Inc - .) C:\Program Files (x86)\Vuze\Azureus.exe [Unsigned] =>.Azureus Software, Inc

017 - HKLM\System\CCS\Services\Tcpip\Parameters: DhcpNameServer = 192.168.81.80
=>.Local IP Adress
017 - HKLM\System\CCS\Services\Tcpip\..\{ff16d0f5-b25b-4c1d-83c3-7c9c886514fa}:
NameServer = 8.8.8.8 =>.France Google Cloud
017 - HKLM\System\CCS\Services\Tcpip\..\{0afef0a3-e30b-4d5c-ace2-38519d75360f}:
DhcpNameServer = 8.8.8.8 =>.France Google Cloud
017 - HKLM\System\CCS\Services\Tcpip\..\{7a5e30dc-1bf3-4668-949d-24a7d209482f}:
DhcpNameServer = 192.168.170.161 =>.Local IP Adress
017 - HKLM\System\CCS\Services\Tcpip\..\{801b5ff5-55dc-4f8f-9281-87d5e9fd6507}:
DhcpNameServer = 192.168.81.80 =>.Local IP Adress

---\ **Extra protocols (22) - 1s**

018 - Handler: about [64Bits] - {3050F406-98B5-11CF-BB82-00AA00BDCE0B} .
(.Microsoft Corporation - Microsoft (R) HTML Viewer.) -- C:\Windows\System32\
mshtml.dll [Unsigned] =>.Microsoft Corporation
018 - Handler: cdl [64Bits] - {3dd53d40-7b8b-11D0-b013-00aa0059ce02} .
(.Microsoft Corporation - OLE32 Extensions for Win32.) -- C:\Windows\System32\
urlmon.dll [Unsigned] =>.Microsoft Corporation
018 - Handler: dvd [64Bits] - {12D51199-0DB5-46FE-A120-47A3D7D937CC} .
(.Microsoft Corporation - ActiveX control for streaming video.) -- C:\Windows\
System32\MSVidCtl.dll [Unsigned] =>.Microsoft Corporation
018 - Handler: file [64Bits] - {79eac9e7-baf9-11ce-8c82-00aa004ba90b} .
(.Microsoft Corporation - OLE32 Extensions for Win32.) -- C:\Windows\System32\
urlmon.dll [Unsigned] =>.Microsoft Corporation
018 - Handler: ftp [64Bits] - {79eac9e3-baf9-11ce-8c82-00aa004ba90b} .
(.Microsoft Corporation - OLE32 Extensions for Win32.) -- C:\Windows\System32\
urlmon.dll [Unsigned] =>.Microsoft Corporation
018 - Handler: http [64Bits] - {79eac9e2-baf9-11ce-8c82-00aa004ba90b} .
(.Microsoft Corporation - OLE32 Extensions for Win32.) -- C:\Windows\System32\
urlmon.dll [Unsigned] =>.Microsoft Corporation
018 - Handler: https [64Bits] - {79eac9e5-baf9-11ce-8c82-00aa004ba90b} .
(.Microsoft Corporation - OLE32 Extensions for Win32.) -- C:\Windows\System32\
urlmon.dll [Unsigned] =>.Microsoft Corporation
018 - Handler: its [64Bits] - {9D148291-B9C8-11D0-A4CC-0000F80149F6} .
(.Microsoft Corporation - Microsoft@ InfoTech Storage System Library.) -- C:\
Windows\System32\itss.dll [Unsigned] =>.Microsoft Corporation
018 - Handler: javascript [64Bits] - {3050F3B2-98B5-11CF-BB82-00AA00BDCE0B} .
(.Microsoft Corporation - Microsoft (R) HTML Viewer.) -- C:\Windows\System32\
mshtml.dll [Unsigned] =>.Microsoft Corporation
018 - Handler: local [64Bits] - {79eac9e7-baf9-11ce-8c82-00aa004ba90b} .
(.Microsoft Corporation - OLE32 Extensions for Win32.) -- C:\Windows\System32\
urlmon.dll [Unsigned] =>.Microsoft Corporation
018 - Handler: mailto [64Bits] - {3050f3DA-98B5-11CF-BB82-00AA00BDCE0B} .
(.Microsoft Corporation - Microsoft (R) HTML Viewer.) -- C:\Windows\System32\
mshtml.dll [Unsigned] =>.Microsoft Corporation
018 - Handler: mhtml [64Bits] - {05300401-BCBC-11d0-85E3-00C04FD85AB4} .
(.Microsoft Corporation - Microsoft Internet Messaging API Resources.) -- C:\
Windows\System32\inetcomm.dll [Unsigned] =>.Microsoft Corporation
018 - Handler: mk [64Bits] - {79eac9e6-baf9-11ce-8c82-00aa004ba90b} .
(.Microsoft Corporation - OLE32 Extensions for Win32.) -- C:\Windows\System32\
urlmon.dll [Unsigned] =>.Microsoft Corporation
018 - Handler: ms-its [64Bits] - {9D148291-B9C8-11D0-A4CC-0000F80149F6} .
(.Microsoft Corporation - Microsoft@ InfoTech Storage System Library.) -- C:\
Windows\System32\itss.dll [Unsigned] =>.Microsoft Corporation
018 - Handler: res [64Bits] - {3050F3BC-98B5-11CF-BB82-00AA00BDCE0B} .
(.Microsoft Corporation - Microsoft (R) HTML Viewer.) -- C:\Windows\System32\
mshtml.dll [Unsigned] =>.Microsoft Corporation
018 - Handler: tbauth [64Bits] - {14654CA6-5711-491D-B89A-58E571679951} .
(.Microsoft Corporation - TBAuth protocol handler.) -- C:\Windows\System32\
tbauth.dll [Unsigned] =>.Microsoft Corporation
018 - Handler: tv [64Bits] - {CBD30858-AF45-11D2-B6D6-00C04FBBDE6E} .
(.Microsoft Corporation - ActiveX control for streaming video.) -- C:\Windows\
System32\MSVidCtl.dll [Unsigned] =>.Microsoft Corporation

018 - Handler: vbscript [64Bits] - {3050F3B2-98B5-11CF-BB82-00AA00BDCE0B} . (.Microsoft Corporation - Microsoft (R) HTML Viewer.) -- C:\Windows\System32\mshtml.dll [Unsigned] =>.Microsoft Corporation
018 - Handler: windows.tbauth [64Bits] - {14654CA6-5711-491D-B89A-58E571679951} . (.Microsoft Corporation - TBAuth protocol handler.) -- C:\Windows\System32\tbauth.dll [Unsigned] =>.Microsoft Corporation
018 - Filter: application/octet-stream [64Bits] - {1E66F26B-79EE-11D2-8710-00C04F79ED0D} . (.Microsoft Corporation - Microsoft .NET Runtime Execution Engine.) -- C:\Windows\System32\mscoree.dll [Unsigned] =>.Microsoft Corporation
018 - Filter: application/x-complus [64Bits] - {1E66F26B-79EE-11D2-8710-00C04F79ED0D} . (.Microsoft Corporation - Microsoft .NET Runtime Execution Engine.) -- C:\Windows\System32\mscoree.dll [Unsigned] =>.Microsoft Corporation
018 - Filter: application/x-msdownload [64Bits] - {1E66F26B-79EE-11D2-8710-00C04F79ED0D} . (.Microsoft Corporation - Microsoft .NET Runtime Execution Engine.) -- C:\Windows\System32\mscoree.dll [Unsigned] =>.Microsoft Corporation

---\ AppInit_DLLs Registry value Autorun (1) - 0s

020 - Winlogon : UserInit . (.Microsoft Corporation - Userinit Logon Application.) - C:\Windows\system32\userinit.exe =>.Microsoft Corporation

---\ List of key exploring StartupApproved (19) - 1s

[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:OneDrive =>.Microsoft Corporation
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:CCleaner Smart Cleaning =>.Piriform Ltd
[\[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run\]:Azureus](#)
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:Windscribe =>.Windscribe
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:Opera Browser Assistant =>.Opera Software
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:EpicGamesLauncher =>.Epic Games
[HKEY_USERS\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:OneDrive =>.Microsoft Corporation
[HKEY_USERS\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:CCleaner Smart Cleaning =>.Piriform Ltd
[\[HKEY_USERS\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run\]:Azureus](#)
[HKEY_USERS\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:Windscribe =>.Windscribe
[HKEY_USERS\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:Opera Browser Assistant =>.Opera Software
[HKEY_USERS\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:EpicGamesLauncher =>.Epic Games
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:SecurityHealth =>.Microsoft Corporation
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:RtkAudUService =>.Realtek Semiconductor Corp.
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:WavesSvc =>.Waves Audio
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:AvastUI.exe =>.Avast Software s.r.o
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run]:LogiOptions =>.Logitech Inc.
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run32]:Dropbox =>.Dropbox Inc.
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run32]:SunJavaUpdateSched =>.Oracle

---\ ASIC (ActiveSetup Installed Components) (7) - 0s

040 - ASIC: Microsoft Windows Media Player [64Bits] - >{22d6f312-b0f6-11d0-94ab-0080c74c7e95} . (.Microsoft Corporation - Microsoft Windows Media Player Legacy Setup.) -- C:\Windows\System32\unregmp2.exe [Unsigned] =>.Microsoft Corporation
040 - ASIC: Microsoft Windows Media Player 12.0 [64Bits] - {22d6f312-b0f6-11d0-94ab-0080c74c7e95} . (.Microsoft Corporation - Windows Media Player Extension.) -- C:\Windows\System32\wmpdxdm.dll [Unsigned] =>.Microsoft Corporation
040 - ASIC: Microsoft Windows Media Player [64Bits] - {6BF52A52-394A-11d3-B153-00C04F79FAA6} . (.Microsoft Corporation - Microsoft Windows Media Player Legacy Setup.) -- C:\Windows\System32\unregmp2.exe [Unsigned] =>.Microsoft Corporation
040 - ASIC: Web Platform Customizations [64Bits] - {89820200-ECBD-11cf-8B85-00AA005B4383} . (.Microsoft Corporation - IE Per-User Initialization Utility.) -- C:\Windows\System32\ie4uinit.exe [Unsigned] =>.Microsoft Corporation
040 - ASIC: (no name) [64Bits] - {89B4C1CD-B018-4511-B0A1-5476DBF70820} . (.Microsoft Corporation - Microsoft .NET IE SECURITY REGISTRATION.) -- C:\Windows\System32\mscories.dll =>.Microsoft®
040 - ASIC: Google Chrome [64Bits] - {8A69D345-D564-463c-AFF1-A69D9E530F96} . (.Google LLC - Google Chrome Installer.) -- C:\Program Files (x86)\Google\Chrome\Application\107.0.5304.87\Installer\chromstp.exe =>.Google LLC®
040 - ASIC: Microsoft Edge [64Bits] - {9459C573-B17A-45AE-9F64-1857B5D58CEE} . (.Microsoft Corporation - Microsoft Edge Installer.) -- C:\Program Files (x86)\Microsoft\Edge\Application\107.0.1418.26\Installer\setup.exe =>.Microsoft®

---\ Software installed (166) - 37s

042 - Logiciel: Acer Network Optimizer - (.Acer.) [HKLM][64Bits] -- {3C8FA4F4-8471-4C60-9002-9B9F78B7B483} [Unsigned] =>.Acer
042 - Logiciel: Adobe Digital Editions 4.5 - (.Adobe Systems Incorporated.) [HKLM][64Bits] -- Adobe Digital Editions 4.5 [Unsigned] =>.Adobe Systems Incorporated
042 - Logiciel: Adobe Reader 6.0 - Français - (.Adobe Systems Incorporated.) [HKLM][64Bits] -- {AC76BA86-7AD7-1036-7B44-000000000001} [Unsigned] =>.Adobe Systems Incorporated
042 - Logiciel: Anagène 2 - (.CNDP.) [HKLM][64Bits] -- {6E83FF05-B414-4AA8-A782-927CB7D516EC} [Unsigned]
042 - Logiciel: Battle.net - (.Blizzard Entertainment.) [HKLM][64Bits] -- Battle.net =>.Blizzard Entertainment, Inc.®
042 - Logiciel: calibre 64bit - (.Kovid Goyal.) [HKLM][64Bits] -- {F337A397-2601-4BF3-8028-C0940FB26549} [Unsigned] =>.Kovid Goyal
042 - Logiciel: Care Center Service - (.Acer Incorporated.) [HKLM][64Bits] -- {AFB52E98-7597-4484-9202-58F0FD3512ED} [Unsigned] =>.Acer Incorporated
042 - Logiciel: Celeste Farewell - (..) [HKLM][64Bits] -- Celeste Farewell_is1 [Unsigned]
042 - Logiciel: D3DX10 - (.Microsoft.) [HKLM][64Bits] -- {E09C4DB7-630C-4F06-A631-8EA7239923AF} [Unsigned] =>.Microsoft (Hidden)
042 - Logiciel: Dome Keeper - (..) [HKLM][64Bits] -- Dome Keeper_is1 [Unsigned]
042 - Logiciel: Dome Keeper MULTi22 - ElAmigos version 41.3.7 - (.Raw Fury.) [HKLM][64Bits] -- {F312C474-274D-4716-83C9-0558B408A8BF}_is1 [Unsigned]
042 - Logiciel: Dome Romantik Demo - (.bippinbits.) [HKLM][64Bits] -- Steam App 1650980 [Unsigned] =>.SteamApp.Game
042 - Logiciel: DriversCloud.com - (.Cybelsoft.) [HKLM][64Bits] -- {0337BFA9-63C1-41A6-BB12-85690990C119} [Unsigned] =>.CybelSoft
042 - Logiciel: DriverSetupUtility - (.Acer Incorporated.) [HKLM][64Bits] -- {2B51C83A-465D-4EA9-9CDC-1ED95ED09AC6} [Unsigned] =>.Acer Incorporated
042 - Logiciel: Dropbox - (.Dropbox, Inc..) [HKLM][64Bits] -- Dropbox =>.Dropbox, Inc®
042 - Logiciel: Dropbox Update Helper - (.Dropbox, Inc..) [HKLM][64Bits] -- {099218A5-A723-43DC-8DB5-6173656A1E94} [Unsigned] =>.Dropbox, Inc. (Hidden)
042 - Logiciel: Dynamic Application Loader Host Interface Service - (.Intel Corporation.) [HKLM][64Bits] -- {B8AD0F0B-6ED6-4121-9ABF-592203F4C43C} [Unsigned] =>.Intel Corporation (Hidden)
042 - Logiciel: Epic Games Launcher - (.Epic Games, Inc..) [HKLM][64Bits] -- {209F4B4B-3DF2-4825-9906-D4D6A80EC09E} [Unsigned] =>.Epic Games, Inc.

042 - Logiciel: Epic Games Launcher Prerequisites (x64) - (.Epic Games, Inc.) [HKLM][64Bits] -- {F9C5C994-F6B9-4D75-B3E7-AD01B84073E9} [Unsigned] =>.Epic Games, Inc. (Hidden)

042 - Logiciel: Epic Online Services - (.Epic Games, Inc.) [HKLM][64Bits] -- {32C68D93-D32F-4B01-8250-61642BFC22F8} [Unsigned] =>.Epic Games, Inc.

042 - Logiciel: Epson USB Display - (.SEIKO EPSON CORPORATION.) [HKLM][64Bits] -- {7650F538-6274-44EA-8F50-843479073333} =>.SEIKO EPSON Corporation®

042 - Logiciel: FastStone Photo Resizer 4.3 - (.FastStone Soft..) [HKLM][64Bits] -- FastStone Photo Resizer [Unsigned] =>.FastStone Soft.

042 - Logiciel: Foxit PDF Reader - (.Foxit Software Inc..) [HKLM][64Bits] -- Foxit Reader_is1 {0109EDFF81A3392E578D219812C053E1}. =>.Foxit Software Inc.

042 - Logiciel: Garena (remove only) - (.Garena.) [HKLM][64Bits] -- gxx {46A0800C34C5FEE85DB1758D556C2D0E}. =>.Garena

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

042 - Logiciel: Hearthstone - (.Blizzard Entertainment.) [HKLM][64Bits] -- Hearthstone =>.Blizzard Entertainment, Inc.®

042 - Logiciel: Hotspot Shield 11.3.0 - (.Pango Inc..) [HKLM][64Bits] -- {66896e6b-e420-4356-8a7d-afee469a59b7} {054E8D30374B037A81D8EC3D5DCCB1D4}. =>.Pango Inc.

042 - Logiciel: Hotspot Shield 11.3.0 - (.Pango Inc..) [HKLM][64Bits] -- {AF599C42-A2E5-4251-B7EE-49250157B251} [Unsigned] =>.Pango Inc. (Hidden)

042 - Logiciel: Hotspot Shield 11.3.0 - (.Pango Inc..) [HKLM][64Bits] -- HotspotShield [Unsigned] =>.Pango Inc. (Hidden)

042 - Logiciel: HotspotShield TAP-Windows 9.24.4 - (.Pango Inc..) [HKLM][64Bits] -- HotspotShield TAP-Windows [Unsigned] =>.Pango Inc. (Hidden)

042 - Logiciel: Intel(R) Chipset Device Software - (.Intel Corporation.) [HKLM][64Bits] -- {148D6ED8-24B8-443D-9C5B-5D6BF506671B} [Unsigned] =>.Intel Corporation (Hidden)

042 - Logiciel: Intel(R) Chipset Device Software - (.Intel(R) Corporation.) [HKLM][64Bits] -- {70281077-96c3-4f75-938c-dc4746110c00} [Unsigned] =>.Intel(R) Corporation

042 - Logiciel: Intel(R) Icls - (.Intel Corporation.) [HKLM][64Bits] -- {64B0A16A-994C-4291-AE4D-1C918BB66F86} [Unsigned] =>.Intel Corporation (Hidden)

042 - Logiciel: Intel(R) Management Engine Components - (.Intel Corporation.) [HKLM][64Bits] -- {1CEAC85D-2590-4760-800F-8DE5E91F3700} {0ADE8114D7679B066F2DB2DFD2F67AC2}. =>.Intel Corporation

042 - Logiciel: Intel(R) Management Engine Components - (.Intel Corporation.) [HKLM][64Bits] -- {6EE6F343-0BD5-4F43-BFB4-A04D8B1FE8CB} [Unsigned] =>.Intel Corporation (Hidden)

042 - Logiciel: Intel(R) Management Engine Driver - (.Intel Corporation.) [HKLM][64Bits] -- {3224ECD1-BFF4-4DEF-ABE9-B244881A871A} [Unsigned] =>.Intel Corporation (Hidden)

042 - Logiciel: Intel(R) ME WMI Provider - (.Intel Corporation.) [HKLM][64Bits] -- {231F417E-7EEB-446F-AEC4-81F6EADE738B} [Unsigned] =>.Intel Corporation (Hidden)

042 - Logiciel: Intel(R) Serial IO - (.Intel Corporation.) [HKLM][64Bits] -- {0940A8E6-DBBC-4554-B07D-EBFB10627716} [Unsigned] =>.Intel Corporation (Hidden)

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

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

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

042 - Logiciel: Intel(R) Trusted Connect Services Client - (.Intel Corporation.) [HKLM][64Bits] -- {2391a86e-5ab5-40d2-a274-1867cd576686} =>.Intel(R) Trust Services® (Hidden)

042 - Logiciel: Intel(R) Wireless Bluetooth(R) - (.Intel Corporation.) [HKLM][64Bits] -- {00000170-0220-1033-84C8-B8D95FA3C8C3} [Unsigned] =>.Intel Corporation

042 - Logiciel: Intel® Optane™ Pinning Explorer Extensions - (.Intel Corporation.) [HKLM][64Bits] -- {F4F771E2-6E23-4F27-93E1-27C22C71B7E2} [Unsigned] =>.Intel Corporation

042 - Logiciel: Latis version 5.0.5.30 - (.EUROSMART S.A.S.) [HKLM][64Bits] -- {0697EBAD-DC65-4345-A543-08D37440D59A}_is1 [Unsigned] =>.EUROSMART S.A.S

042 - Logiciel: Launcher Prerequisites (x64) - (.Epic Games, Inc.) [HKLM][64Bits] -- {43a03b9c-4770-409c-a999-587b60700b63} =>.Epic Games Inc.® (Hidden)

042 - Logiciel: LibreOffice 7.0.0.3 - (.The Document Foundation.) [HKLM][64Bits] -- {7C7F19DA-6107-4284-9263-EC5C4792C8C7} [Unsigned] =>.The Document Foundation

042 - Logiciel: Light Image Resizer 6.1.0.0 - (.ObviousIdea.) [HKLM][64Bits] -- {4AC2BB90-D86E-4E4A-84E7-62ED7D564488}_is1 =>.ObviousIdea®

042 - Logiciel: Logitech Options - (.Logitech.) [HKLM][64Bits] -- LogiOptions =>.Logitech Inc®

042 - Logiciel: Microsoft Application Error Reporting - (.Microsoft Corporation.) [HKLM][64Bits] -- {95120000-00B9-0409-1000-00000000FF1CE} [Unsigned] =>.Microsoft Corporation (Hidden)

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

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

042 - Logiciel: Microsoft Edge WebView2 Runtime - (.Microsoft Corporation.) [HKLM][64Bits] -- Microsoft EdgeWebView =>.Microsoft®

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

042 - Logiciel: Microsoft SQL Server 2005 Compact Edition [ENU] - (.Microsoft Corporation.) [HKLM][64Bits] -- {F0B430D1-B6AA-473D-9B06-AA3DD01FD0B8} [Unsigned] =>.Microsoft Corporation

042 - Logiciel: Microsoft Update Health Tools - (.Microsoft Corporation.) [HKLM][64Bits] -- {6A2A8076-135F-4F55-BB02-DED67C8C6934} [Unsigned] =>.Microsoft Corporation

042 - Logiciel: Microsoft VC++ redistributables repacked. - (.Intel Corporation.) [HKLM][64Bits] -- {C022DCCA-DEA7-458A-97D1-F5BD4AAEE4A0} [Unsigned] =>.Intel Corporation (Hidden)

042 - Logiciel: Microsoft VC++ redistributables repacked. - (.Intel Corporation.) [HKLM][64Bits] -- {E1F8AD73-09C5-434A-A2C4-15EC6B98CF21} [Unsigned] =>.Intel Corporation (Hidden)

042 - Logiciel: Microsoft Visual C++ 2005 Redistributable - (.Microsoft Corporation.) [HKLM][64Bits] -- {710f4c1c-cc18-4c49-8cbf-51240c89a1a2} [Unsigned] =>.Microsoft Corporation

042 - Logiciel: Microsoft Visual C++ 2005 Redistributable - (.Microsoft Corporation.) [HKLM][64Bits] -- {7299052b-02a4-4627-81f2-1818da5d550d} [Unsigned] =>.Microsoft Corporation

042 - Logiciel: Microsoft Visual C++ 2005 Redistributable (x64) - (.Microsoft Corporation.) [HKLM][64Bits] -- {ad8a2fa1-06e7-4b0d-927d-6e54b3d31028} [Unsigned] =>.Microsoft Corporation

042 - Logiciel: Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.17 - (.Microsoft Corporation.) [HKLM][64Bits] -- {8220EEFE-38CD-377E-8595-13398D740ACE} [Unsigned] =>.Microsoft Corporation

042 - Logiciel: Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161 - (.Microsoft Corporation.) [HKLM][64Bits] -- {5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4} [Unsigned] =>.Microsoft Corporation

042 - Logiciel: Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17 - (.Microsoft Corporation.) [HKLM][64Bits] -- {9A25302D-30C0-39D9-BD6F-21E6EC160475} [Unsigned] =>.Microsoft Corporation

042 - Logiciel: Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 - (.Microsoft Corporation.) [HKLM][64Bits] -- {9BE518E6-ECC6-35A9-88E4-87755C07200F} [Unsigned] =>.Microsoft Corporation

042 - Logiciel: Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219 - (.Microsoft Corporation.) [HKLM][64Bits] -- {1D8E6291-B0D5-35EC-8441-6616F567A0F7} [Unsigned] =>.Microsoft Corporation

042 - Logiciel: Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 - (.Microsoft Corporation.) [HKLM][64Bits] -- {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5} [Unsigned] =>.Microsoft Corporation

042 - Logiciel: Microsoft Visual C++ 2012 Redistributable (x64) - 11.0.61030 - (.Microsoft Corporation.) [HKLM][64Bits] -- {ca67548a-5ebe-413a-b50c-4b9ceb6d66c6} =>.Microsoft®

042 - Logiciel: Microsoft Visual C++ 2012 Redistributable (x86) - 11.0.61030 - (.Microsoft Corporation.) [HKLM][64Bits] -- {33d1fd90-4274-48a1-9bc1-97e33d9c2d6f} =>.Microsoft®

042 - Logiciel: Microsoft Visual C++ 2012 x64 Additional Runtime - 11.0.61030 - (.Microsoft Corporation.) [HKLM][64Bits] -- {37B8F9C7-03FB-3253-8781-2517C99D7C00} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Microsoft Visual C++ 2012 x64 Minimum Runtime - 11.0.61030 - (.Microsoft Corporation.) [HKLM][64Bits] -- {CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.61030 - (.Microsoft Corporation.) [HKLM][64Bits] -- {B175520C-86A2-35A7-8619-86DC379688B9} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.61030 - (.Microsoft Corporation.) [HKLM][64Bits] -- {BD95A8CD-1D9F-35AD-981A-3E7925026EBB} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 - (.Microsoft Corporation.) [HKLM][64Bits] -- {050d4fc8-5d48-4b8f-8972-47c82c46020f} =>.Microsoft®

042 - Logiciel: Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.40664 - (.Microsoft Corporation.) [HKLM][64Bits] -- {042d26ef-3dbe-4c25-95d3-4c1b11b235a7} =>.Microsoft®

042 - Logiciel: Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 - (.Microsoft Corporation.) [HKLM][64Bits] -- {f65db027-aff3-4070-886a-0d87064aabb1} =>.Microsoft®

042 - Logiciel: Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.40664 - (.Microsoft Corporation.) [HKLM][64Bits] -- {9dff3540-fc85-4ed5-ac84-9e3c7fd8bece} =>.Microsoft®

042 - Logiciel: Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.40664 - (.Microsoft Corporation.) [HKLM][64Bits] -- {010792BA-551A-3AC0-A7EF-0FAB4156C382} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.40664 - (.Microsoft Corporation.) [HKLM][64Bits] -- {53CF6934-A98D-3D84-9146-FC4EDF3D5641} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.40664 - (.Microsoft Corporation.) [HKLM][64Bits] -- {D401961D-3A20-3AC7-943B-6139D5BD490A} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.40664 - (.Microsoft Corporation.) [HKLM][64Bits] -- {8122DAB1-ED4D-3676-BB0A-CA368196543E} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.28.29334 - (.Microsoft Corporation.) [HKLM][64Bits] -- {a9cfe9c7-e54f-46cd-9c5c-542ff8e3e8c4} =>.Microsoft®

042 - Logiciel: Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.29.30037 - (.Microsoft Corporation.) [HKLM][64Bits] -- {dfea0fad-88b2-4a1f-8536-3f8f9391f4ef} =>.Microsoft®

042 - Logiciel: Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29334 - (.Microsoft Corporation.) [HKLM][64Bits] -- {2E11EF4E-901F-4B2D-B68E-3DB2A566C857} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29334 - (.Microsoft Corporation.) [HKLM][64Bits] -- {8A3F7D5B-422D-49D9-84F7-8DC1B7782967} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Microsoft Visual C++ 2019 X86 Additional Runtime - 14.29.30037 - (.Microsoft Corporation.) [HKLM][64Bits] -- {01FAEC41-B3BC-44F4-B185-5E8475AEB855} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.29.30037 - (.Microsoft Corporation.) [HKLM][64Bits] -- {7D75664A-6C04-424C-82A1-EE88913E5F16} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Microsoft WSE 3.0 Runtime - (.Microsoft Corp..) [HKLM][64Bits] -- {E3E71D07-CD27-46CB-8448-16D4FB29AA13} [Unsigned] =>.Microsoft Corp.

042 - Logiciel: Microsoft XNA Framework Redistributable 4.0 - (.Microsoft Corporation.) [HKLM][64Bits] -- {2BFC7AA0-544C-4E3A-8796-67F3BE655BE9} [Unsigned] =>.Microsoft Corporation

042 - Logiciel: Mise à jour automatique - (.Index Education.) [HKLM][64Bits] -- {775E087D-A428-428C-A5FD-000010008000} [Unsigned] =>.Index Education

042 - Logiciel: Movie Maker - (.Microsoft Corporation.) [HKLM][64Bits] -- {DD67BE4B-7E62-4215-AFA3-F123A800A389} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: MSVCRT - (.Microsoft.) [HKLM][64Bits] -- {8DD46C6A-0056-4FEC-B70A-28BB16A1F11F} [Unsigned] =>.Microsoft (Hidden)

042 - Logiciel: MSVCRT110 - (.Microsoft.) [HKLM][64Bits] -- {8E14DDC8-EA60-4E18-B3E3-1937104D5BDA} [Unsigned] =>.Microsoft (Hidden)

042 - Logiciel: MSVCRT110_amd64 - (.Microsoft.) [HKLM][64Bits] -- {E9FA781F-3E80-4399-825A-AD3E11C28C77} [Unsigned] =>.Microsoft (Hidden)

042 - Logiciel: NitroSense Service - (.Acer Incorporated.) [HKLM][64Bits] -- {6FC78E80-6385-43D6-8A43-FA80094F1A2E} [Unsigned] =>.Acer Incorporated

042 - Logiciel: NVIDIA Backend - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvBackend [Unsigned] =>.NVIDIA Corporation (Hidden)

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

042 - Logiciel: NVIDIA FrameView SDK 1.3.8107.31782123 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_FrameViewSdk [Unsigned] =>.NVIDIA Corporation

042 - Logiciel: NVIDIA GeForce Experience 3.26.0.154 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_Display.GFExperience [Unsigned] =>.NVIDIA Corporation

042 - Logiciel: NVIDIA GPX Common OSS binaries (POCO, OpenSSL, libprotobuf) - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_GpxCommon.Oss [Unsigned] =>.NVIDIA Corporation (Hidden)

042 - Logiciel: NVIDIA Graphics Driver 522.25 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_Display.Driver [Unsigned] =>.NVIDIA Corporation

042 - Logiciel: NVIDIA HD Audio Driver 1.3.39.16 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_HDAudio.Driver [Unsigned] =>.NVIDIA Corporation

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

042 - Logiciel: NVIDIA LocalSystem Container - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvContainer.LocalSystem [Unsigned] =>.NVIDIA Corporation (Hidden)

042 - Logiciel: NVIDIA Message Bus for NvContainer - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvContainer.MessageBus [Unsigned] =>.NVIDIA Corporation (Hidden)

042 - Logiciel: NVIDIA NetworkService Container - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvContainer.ServiceUser [Unsigned] =>.NVIDIA Corporation (Hidden)

042 - Logiciel: NVIDIA NodeJS - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvNodejs [Unsigned] =>.NVIDIA Corporation (Hidden)

042 - Logiciel: NVIDIA NVAPI Monitor plugin for NvContainer - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvContainer.NvapiMonitor [Unsigned] =>.NVIDIA Corporation (Hidden)

042 - Logiciel: NVIDIA NvModuleTracker - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvModuleTracker.Driver [Unsigned] =>.NVIDIA Corporation (Hidden)

042 - Logiciel: NVIDIA Optimus Update 39.4.0.0 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_Display.Optimus [Unsigned] =>.NVIDIA Corporation (Hidden)

042 - Logiciel: NVIDIA PhysX System Software 9.21.0713 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_Display.PhysX [Unsigned] =>.NVIDIA Corporation

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

042 - Logiciel: NVIDIA ShadowPlay 3.26.0.154 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_ShadowPlay [Unsigned] =>.NVIDIA Corporation (Hidden)

042 - Logiciel: Nvidia Share - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_OSC [Unsigned] =>.NVIDIA Corporation (Hidden)

042 - Logiciel: NVIDIA SHIELD Streaming - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_GFXperience.NvStreamSrv [Unsigned] =>.NVIDIA Corporation (Hidden)

042 - Logiciel: NVIDIA SHIELD Wireless Controller Driver - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_ShieldWirelessController [Unsigned] =>.NVIDIA Corporation (Hidden)

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

042 - Logiciel: NVIDIA TelemetryApi helper for NvContainer - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvContainer.ContainerTelemetryApiHelper [Unsigned] =>.NVIDIA Corporation (Hidden)

042 - Logiciel: NVIDIA Update 39.4.0.0 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_Display.Update [Unsigned] =>.NVIDIA Corporation (Hidden)

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

042 - Logiciel: NVIDIA User Container - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvContainer.User [Unsigned] =>.NVIDIA Corporation (Hidden)

042 - Logiciel: NVIDIA Virtual Audio 4.45.0.0 - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_VirtualAudio.Driver [Unsigned] =>.NVIDIA Corporation (Hidden)

042 - Logiciel: NVIDIA Virtual Host Controller - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvVHCI [Unsigned] =>.NVIDIA Corporation (Hidden)

042 - Logiciel: NVIDIA Watchdog Plugin for NvContainer - (.NVIDIA Corporation.) [HKLM][64Bits] -- {B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_NvPlugin.Watchdog [Unsigned] =>.NVIDIA Corporation (Hidden)

042 - Logiciel: OpenAL - (.Open Audio Library.) [HKLM][64Bits] -- OpenAL =>.Creative Labs Inc®

042 - Logiciel: OptaneDowngradeGuard - (.Intel Corporation.) [HKLM][64Bits] -- {86B0E6C1-32E0-42CC-BC4F-BF3C0730CECB} [Unsigned] =>.Intel Corporation (Hidden)

042 - Logiciel: Ori and the Will of the Wisps - (.HOODLUM.) [HKCU][64Bits] -- Ori and the Will of the Wisps [Unsigned] =>.Hoodlum

042 - Logiciel: Othercide - (.HOODLUM.) [HKCU][64Bits] -- Othercide [Unsigned] =>.Hoodlum

042 - Logiciel: Outer Wilds Echoes of the Eye - (..) [HKLM][64Bits] -- Outer Wilds Echoes of the Eye_is1 [Unsigned]

042 - Logiciel: Paradox Launcher v2 - (.Paradox Interactive.) [HKLM][64Bits] -- {A92DB5D9-A24D-4678-9F91-B4FA6D895718} [Unsigned] =>.Paradox Interactive

042 - Logiciel: Photo Gallery - (.Microsoft Corporation.) [HKLM][64Bits] -- {07AAB66E-4718-422D-9218-4AFB3C922A71} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Quick Access Service - (.Acer Incorporated.) [HKLM][64Bits] -- {AB25551C-74EF-4BAB-9989-891517FCF9FF} [Unsigned] =>.Acer Incorporated

042 - Logiciel: Realtek Ethernet Controller Driver - (.Realtek.) [HKLM][64Bits] -- {8833FFB6-5B0C-4764-81AA-06DFEED9A476} =>.Realtek Semiconductor Corp.®

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

042 - Logiciel: RstDowngradeGuard - (.Intel Corporation.) [HKLM][64Bits] -- {13C2A26E-7AD4-4D82-BB4F-DEA6E871B958} [Unsigned] =>.Intel Corporation (Hidden)

042 - Logiciel: Stellarium 0.22.2 - (.Stellarium team.) [HKLM][64Bits] -- Stellarium_is1 [Unsigned] =>.Stellarium team

042 - Logiciel: TAP-Windows 9.24.2 - (.OpenVPN Technologies, Inc..) [HKLM][64Bits] -- TAP-Windows [Unsigned] =>.OpenVPN Technologies, Inc.

042 - Logiciel: Telegram Desktop - (.Telegram FZ-LLC.) [HKCU][64Bits] -- {53F49750-6209-4FBF-9CA8-7A333C87D1ED}_is1 [Unsigned] =>.Telegram FZ-LLC

042 - Logiciel: This War of Mine - (.11 bit studios.) [HKLM][64Bits] -- Steam App 282070 [Unsigned] =>.SteamApp.Game

042 - Logiciel: USBHelperLauncher - (.FailedShack.) [HKCU][64Bits] -- USBHelperLauncher [Unsigned] =>.FailedShack

042 - Logiciel: User Experience Improvement Program Service - (.Acer Incorporated.) [HKLM][64Bits] -- {E9495FD3-F73D-4D33-A104-047F9E8BE6C7} [Unsigned] =>.Acer Incorporated

042 - Logiciel: Vampire Survivors - (.poncle.) [HKLM][64Bits] -- Steam App 1794680 [Unsigned] =>.SteamApp.Game

042 - Logiciel: vJoy Device Driver 2.1.9.1 - (.Shaul Eizikovich.) [HKLM][64Bits] -- {8E31F76F-74C3-47F1-9550-E041EEDC5FBB}_is1 [Unsigned] =>.Shaul Eizikovich

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

042 - Logiciel: Vuze - (.Azureus Software, Inc..) [HKLM][64Bits] -- 8461-7759-5462-8226 =>.Azureus Software, Inc.®

042 - Logiciel: WebZIP - (.Spidersoft.) [HKLM][64Bits] -- WebZIP [Unsigned] =>.Spidersoft

042 - Logiciel: WhatsApp - (.WhatsApp.) [HKCU][64Bits] -- WhatsApp {0C16D074311A3365FAE8200C7E160C54}. =>.WhatsApp

042 - Logiciel: WiFi Password Decryptor - (.SecurityXploded.) [HKLM][64Bits] -- {91760CF3-BF46-462A-8A73-511F3B675DDE} [Unsigned] =>.SecurityXploded (Hidden)

042 - Logiciel: WiFi Password Decryptor 14.0 - (.SecurityXploded.) [HKLM][64Bits] -- WiFi Password Decryptor 14.0 [Unsigned] =>.SecurityXploded

042 - Logiciel: Windows Driver Package - Tucsen (TUUSB3) Image (05/22/2020 1.2.3.10) - (.Tucsen.) [HKLM][64Bits] -- D41001EB8EC500D71E79BBE6ED680C52041269FF =>.Microsoft Windows®

042 - Logiciel: Windows Driver Package - Tucsen Camera (02/23/2013 1.2.6.0) - (.Tucsen.) [HKLM][64Bits] -- D53CC780FA01D1B3F58392A4B8607B2404BB11C5 =>.Microsoft Windows®

042 - Logiciel: Windows Live - (.Microsoft Corporation.) [HKLM][64Bits] -- {B99F248C-B4B3-4D61-9FFC-AE59A1F13723} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Windows Live - (.Microsoft Corporation.) [HKLM][64Bits] -- WinLiveSuite =>.Microsoft®

042 - Logiciel: Windows Live Communications Platform - (.Microsoft Corporation.) [HKLM][64Bits] -- {41C61308-6CFD-4D54-AB6A-7136ED08A18E} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Windows Live Installer - (.Microsoft Corporation.) [HKLM][64Bits] -- {659CB81C-B54E-4DF1-B618-F35777393A54} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Windows Live Photo Common - (.Microsoft Corporation.) [HKLM][64Bits] -- {1D6432B4-E24D-405E-A4AB-D7E6D088CBC9} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Windows Live PIMT Platform - (.Microsoft Corporation.) [HKLM][64Bits] -- {B2611F8A-EFE7-4E88-875D-19F0EFAE87E4} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Windows Live SOXE - (.Microsoft Corporation.) [HKLM][64Bits] -- {CDC1AB00-01FF-4FC7-816A-16C67F0923C0} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Windows Live SOXE Definitions - (.Microsoft Corporation.) [HKLM][64Bits] -- {D1893000-EA77-493C-8DDD-E262436E959B} [Unsigned] =>.Microsoft Corporation (Hidden)

042 - Logiciel: Windows Live UX Platform - (.Microsoft Corporation.) [HKLM] [64Bits] -- {00F9DB8C-65D7-4D47-AB5F-F698EE38580D} [Unsigned] =>.Microsoft Corporation (Hidden)
042 - Logiciel: Windows Live UX Platform Language Pack - (.Microsoft Corporation.) [HKLM][64Bits] -- {33B992ED-B59B-4E25-9F3F-CF2D79BBA914} [Unsigned] =>.Microsoft Corporation (Hidden)
042 - Logiciel: Windows PC Health Check - (.Microsoft Corporation.) [HKLM] [64Bits] -- {B1E7D0FD-7CFE-4E0C-A5DA-0F676499DB91} [Unsigned] =>.Microsoft Corporation
042 - Logiciel: Windscribe - (.Windscribe Limited.) [HKLM][64Bits] -- {fa690e90-ddb0-4f0c-b3f1-136c084e5fc7}_is1 =>.Windscribe Limited®
042 - Logiciel: WinHTTrack Website Copier 3.49-2 (x64) - (.HTTrack.) [HKLM] [64Bits] -- WinHTTrack Website Copier_is1 =>.Open Source Developer, Xavier Roche®
042 - Logiciel: WinRAR 6.02 (64-bit) - (.win.rar GmbH.) [HKLM][64Bits] -- WinRAR archiver =>.win.rar GmbH®
042 - Logiciel: Zoom - (.Zoom Video Communications, Inc..) [HKCU][64Bits] -- ZoomUMX =>.Zoom Video Communications, Inc.®

---\ HKCU & HKLM Software Keys (301) - 37s

HKLM\SOFTWARE\POLICIES\Mozilla\Firefox =>.SUP.FirefoxRestriction
HKLM\SOFTWARE\AGEIA Technologies =>.AGEIA Technologies
HKLM\SOFTWARE\Apple Inc. =>.Apple Inc.
HKLM\SOFTWARE\ASUS =>.ASUS
HKLM\SOFTWARE\Avast Software =>.AVAST Software
HKLM\SOFTWARE\AVG =>.AVG Software
HKLM\SOFTWARE\Azureus =>.Azureus Software (P2P)
HKLM\SOFTWARE\BlueStacksInstaller =>.BlueStack Systems, Inc.
HKLM\SOFTWARE\calibre 64bit
HKLM\SOFTWARE\Caphyon =>.Caphyon
HKLM\SOFTWARE\COMPAL =>.Compal
HKLM\SOFTWARE\CVSM =>.Legitimate
HKLM\SOFTWARE\Cybelsoft =>.CybelSoft
HKLM\SOFTWARE\DefaultUserEnvironment =>.Microsoft Corporation
HKLM\SOFTWARE\Dell =>.Dell
HKLM\SOFTWARE\ej-technologies =>.ej-technologies
HKLM\SOFTWARE\Global Delight
HKLM\SOFTWARE\Google =>.Google
HKLM\SOFTWARE\Hewlett-Packard =>.Hewlett-Packard
HKLM\SOFTWARE\HotspotShield =>.AnchorFree Inc.
HKLM\SOFTWARE\HP =>.HP
HKLM\SOFTWARE\Index Education =>.Index Education
HKLM\SOFTWARE\Intel =>.Intel
HKLM\SOFTWARE\JavaSoft =>.JavaSoft
HKLM\SOFTWARE\JreMetrics =>.JreMetrics
HKLM\SOFTWARE\Khronos =>.Khronos
HKLM\SOFTWARE\LibreOffice =>.LibreOffice
HKLM\SOFTWARE\Logitech =>.Logitech
HKLM\SOFTWARE\Magnet =>.Magnet
HKLM\SOFTWARE\ManageableUpdatePackage =>.Dell Inc.
HKLM\SOFTWARE\Maxis =>.Maxis
HKLM\SOFTWARE\Mozilla =>.Mozilla
HKLM\SOFTWARE\mozilla.org =>.mozilla.org
HKLM\SOFTWARE\MozillaPlugins =>.MozillaPlugins
HKLM\SOFTWARE\NVIDIA Corporation =>.nVidia Corporation
HKLM\SOFTWARE\ODBC =>.DB Connectivity Solutions
HKLM\SOFTWARE\OEM =>.OEM
HKLM\SOFTWARE\OpenSSH =>.OpenBSD
HKLM\SOFTWARE\Oracle =>.Oracle
HKLM\SOFTWARE\Partner =>.Google Inc.
HKLM\SOFTWARE\Piriform =>.Piriform
HKLM\SOFTWARE\Realtek =>.Realtek Semiconductor Corp.
HKLM\SOFTWARE\RegisteredApplications =>.Microsoft Corporation
HKLM\SOFTWARE\RTLSetup =>.Realtek Semiconductor Corp.

HKLM\SOFTWARE\Setup =>.Unknown
HKLM\SOFTWARE\Symantec =>.Symantec
HKLM\SOFTWARE\TAP-Windows =>.OpenVPN Technologie
HKLM\SOFTWARE\The Document Foundation =>.The Document Foundation
HKLM\SOFTWARE\VideoLAN =>.VideoLan Team
HKLM\SOFTWARE\Waves Audio =>.Waves Audio
HKLM\SOFTWARE\Windows =>.Microsoft Corporation
HKLM\SOFTWARE\WinHTTrack Website Copier =>.Xavier Roche
HKLM\SOFTWARE\WinRAR =>.WinRAR
HKLM\SOFTWARE\WOW6432Node =>.Microsoft Corporation
HKLM\SOFTWARE\WOW6432Node\Acer =>.Acer
HKLM\SOFTWARE\WOW6432Node\Adobe =>.Adobe
HKLM\SOFTWARE\WOW6432Node\AGEIA Technologies =>.AGEIA Technologies
HKLM\SOFTWARE\WOW6432Node\Apple Inc. =>.Apple Inc.
HKLM\SOFTWARE\WOW6432Node\ASUS =>.ASUS
HKLM\SOFTWARE\WOW6432Node\Aureal =>.Aureal Semiconductor
HKLM\SOFTWARE\WOW6432Node\Blizzard Entertainment =>.Blizzard Entertainment
HKLM\SOFTWARE\WOW6432Node\BSD =>.Berkeley
HKLM\SOFTWARE\WOW6432Node\Caphyon =>.Caphyon
HKLM\SOFTWARE\WOW6432Node\DownloadCenter =>.DownloadCenter
HKLM\SOFTWARE\WOW6432Node\Dropbox =>.Dropbox
HKLM\SOFTWARE\WOW6432Node\DropboxUpdate =>.Dropbox Inc.
HKLM\SOFTWARE\WOW6432Node\ej-technologies =>.ej-technologies
HKLM\SOFTWARE\WOW6432Node\Epic Games =>.Epic Games
HKLM\SOFTWARE\WOW6432Node\EpicGames =>.Epic Games
HKLM\SOFTWARE\WOW6432Node\Foxit Software =>.Foxit Software
HKLM\SOFTWARE\WOW6432Node\Garena =>.Garena
HKLM\SOFTWARE\WOW6432Node\GOG.com =>.GOG.com
HKLM\SOFTWARE\WOW6432Node\Google =>.Google
HKLM\SOFTWARE\WOW6432Node\HotspotShield =>.AnchorFree Inc.
HKLM\SOFTWARE\WOW6432Node\InstallShield =>.InstallShield
HKLM\SOFTWARE\WOW6432Node\Intel =>.Intel
HKLM\SOFTWARE\WOW6432Node\JavaSoft =>.JavaSoft
HKLM\SOFTWARE\WOW6432Node\JreMetrics =>.JreMetrics
HKLM\SOFTWARE\WOW6432Node\Khronos =>.Khronos
HKLM\SOFTWARE\WOW6432Node\Malwarebytes =>.Malwarebytes
HKLM\SOFTWARE\WOW6432Node\Maxis =>.Maxis
HKLM\SOFTWARE\WOW6432Node\Mozilla =>.Mozilla
HKLM\SOFTWARE\WOW6432Node\mozilla.org =>.mozilla.org
HKLM\SOFTWARE\WOW6432Node\MozillaPlugins =>.MozillaPlugins
HKLM\SOFTWARE\WOW6432Node\NVIDIA Corporation =>.nVidia Corporation
HKLM\SOFTWARE\WOW6432Node\ObviousIdea =>.ObviousIdea
HKLM\SOFTWARE\WOW6432Node\ODBC =>.DB Connectivity Solutions
HKLM\SOFTWARE\WOW6432Node\OEM =>.OEM
HKLM\SOFTWARE\WOW6432Node\Origin =>.Electronic Arts, Inc.
HKLM\SOFTWARE\WOW6432Node\Piriform =>.Piriform
HKLM\SOFTWARE\WOW6432Node\Realtek =>.Realtek Semiconductor Corp.
HKLM\SOFTWARE\WOW6432Node\Realtek Semiconductor Corp. =>.Realtek Semiconductor Corp.
HKLM\SOFTWARE\WOW6432Node\SEIKO EPSON CORPORATION =>.Epson/Seico
HKLM\SOFTWARE\WOW6432Node\Symantec =>.Symantec
HKLM\SOFTWARE\WOW6432Node\TVInstallTemp =>.TeamViewer GmbH
HKLM\SOFTWARE\WOW6432Node\Valve =>.Valve
HKLM\SOFTWARE\WOW6432Node\RegisteredApplications =>.Microsoft Corporation
HKCU\SOFTWARE\Acer =>.Acer
HKCU\SOFTWARE\Adobe =>.Adobe
HKCU\SOFTWARE\Amanita Design =>.Amanita Design
HKCU\SOFTWARE\appdata\low =>.Microsoft Corporation
HKCU\SOFTWARE\Appwork =>.Appwork GmbH
HKCU\SOFTWARE\AvastAdSDK =>.Avast Software s.r.o
HKCU\SOFTWARE\AVG =>.AVG Software
HKCU\SOFTWARE\Azureus =>.Azureus Software (P2P)
HKCU\SOFTWARE\Blizzard Entertainment =>.Blizzard Entertainment
HKCU\SOFTWARE\BlueStacksInstaller =>.BlueStack Systems, Inc.

HKCU\SOFTWARE\BugSplat =>.Bugsplat Game
HKCU\SOFTWARE\Bulwark Studios
HKCU\SOFTWARE\calibre =>.Kovid Goyal
HKCU\SOFTWARE\Cellar Door Games
HKCU\SOFTWARE\ChangeTracker =>.Legitimate
HKCU\SOFTWARE\Chromium =>.Chromium
HKCU\SOFTWARE\Daniel Mullins Games
HKCU\SOFTWARE\Dead Mage
HKCU\SOFTWARE\Draknek and Friends
HKCU\SOFTWARE\DrawMeAPixel
HKCU\SOFTWARE\Dropbox =>.Dropbox
HKCU\SOFTWARE\DropboxUpdate =>.Dropbox Inc.
HKCU\SOFTWARE\ej-technologies =>.ej-technologies
HKCU\SOFTWARE\ElAmigos =>.ElAmigos
HKCU\SOFTWARE\Electronic Arts =>.Electronic Arts
HKCU\SOFTWARE\Epic Games =>.Epic Games
HKCU\SOFTWARE\EqualizerAPO
HKCU\SOFTWARE\EurekaLab =>.EurekaLab
HKCU\SOFTWARE\EUROSMART =>.EUROSMART
HKCU\SOFTWARE\Foxit Software =>.Foxit Software
HKCU\SOFTWARE\GNU =>.GNU
HKCU\SOFTWARE\GOG.com =>.GOG.com
HKCU\SOFTWARE\Google =>.Google
HKCU\SOFTWARE\Haemimont Games =>.Haemimont Games
HKCU\SOFTWARE\HotspotShield =>.AnchorFree Inc.
HKCU\SOFTWARE\Index Education =>.Index Education
HKCU\SOFTWARE\Intel =>.Intel
HKCU\SOFTWARE\JavaSoft =>.JavaSoft
HKCU\SOFTWARE\Khronos =>.Khronos
HKCU\SOFTWARE\Klei
HKCU\SOFTWARE\Konfa Games
HKCU\SOFTWARE\Lantern Studio
HKCU\SOFTWARE\Larian Studios =>.Larian Studios
HKCU\SOFTWARE\LightbulbCrew
HKCU\SOFTWARE\Local AppWizard-Generated Applications =>.ZWCAD
HKCU\SOFTWARE\Logitech =>.Logitech
HKCU\SOFTWARE\Magnet =>.Magnet
HKCU\SOFTWARE\MatchWare =>.MatchWare
HKCU\SOFTWARE\Michael Herf =>.Michael Herf
HKCU\SOFTWARE\Mobius Digital
HKCU\SOFTWARE\Mojang =>.Mojang
HKCU\SOFTWARE\Moon Studios
HKCU\SOFTWARE\Mozilla =>.Mozilla
HKCU\SOFTWARE\MozillaPlugins =>.MozillaPlugins
HKCU\SOFTWARE\My Application
HKCU\SOFTWARE\Nerial
HKCU\SOFTWARE\Netscape =>.Netscape
HKCU\SOFTWARE\NVIDIA Corporation =>.nVidia Corporation
HKCU\SOFTWARE\ObviousIdea =>.ObviousIdea
HKCU\SOFTWARE\OEM =>.OEM
HKCU\SOFTWARE\Opera Software =>.Opera Software
HKCU\SOFTWARE\Opera Stable Offer =>.Opera Software
HKCU\SOFTWARE\Optillusion
HKCU\SOFTWARE\Owlcat Games
HKCU\SOFTWARE\Paradox Interactive =>.Paradox Interactive
HKCU\SOFTWARE\Parisprog
HKCU\SOFTWARE\Piriform =>.Piriform
HKCU\SOFTWARE\QtProject =>.QtProject
HKCU\SOFTWARE\RasTop
HKCU\SOFTWARE\Realtek =>.Realtek Semiconductor Corp.
HKCU\SOFTWARE\RedHook
HKCU\SOFTWARE\RegisteredApplications =>.Microsoft Corporation
HKCU\SOFTWARE\Simogo
HKCU\SOFTWARE\Softdeluxe =>.Softdeluxe

HKCU\SOFTWARE\Spidersoft =>.Spidersoft
HKCU\SOFTWARE\Studio Seufz =>.Pinnacle Systems, Inc.
HKCU\SOFTWARE\SunheadGames
HKCU\SOFTWARE\Team17 Digital Limited =>.Team17
HKCU\SOFTWARE\Team17 Digital Ltd.
HKCU\SOFTWARE\TelegramDesktop =>.TelegramDesktop
HKCU\SOFTWARE\The Document Foundation =>.The Document Foundation
HKCU\SOFTWARE\Thunder Lotus Games =>.Thunder Lotus Games
HKCU\SOFTWARE\UnPas2Asp.exe
HKCU\SOFTWARE\Valve =>.Valve
HKCU\SOFTWARE\Wargaming.net =>.Wargaming.net
HKCU\SOFTWARE\Winamp =>.Nullsoft Inc.
HKCU\SOFTWARE\Windscribe =>.Windscribe
HKCU\SOFTWARE\WinHTTrack Website Copier =>.Xavier Roche
HKCU\SOFTWARE\WinRAR =>.WinRAR
HKCU\SOFTWARE\WinRAR SFX =>.RarLab
HKCU\SOFTWARE\Wintertree =>.Wintertree Software
HKCU\SOFTWARE\WixSharp =>.Legitimate
HKCU\SOFTWARE\Wow6432Node =>.Microsoft Corporation
HKCU\SOFTWARE\ZAUM Studio
HKCU\SOFTWARE\ZHP =>.Nicolas Coolman
HKCU\SOFTWARE\ZoomUMX
HKCU\SOFTWARE\AppDataLow\software =>.Microsoft Corporation
HKCU\SOFTWARE\AppDataLow\Software\Norton =>.Symantec Corporation
HKU\DEFAULT\SOFTWARE\AppDataLow =>.Microsoft Corporation
HKU\DEFAULT\SOFTWARE\Dropbox =>.Dropbox
HKU\DEFAULT\SOFTWARE\Epic Games =>.Epic Games
HKU\DEFAULT\SOFTWARE\Google =>.Google
HKU\DEFAULT\SOFTWARE\HotspotShield =>.AnchorFree Inc.
HKU\DEFAULT\SOFTWARE\Local AppWizard-Generated Applications =>.ZWCAD
HKU\DEFAULT\SOFTWARE\Norton =>.Symantec Corporation
HKU\DEFAULT\SOFTWARE\NVIDIA Corporation =>.nVidia Corporation
HKU\DEFAULT\SOFTWARE\Piriform =>.Piriform
HKU\DEFAULT\SOFTWARE\WixSharp =>.Legitimate
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Acer =>.Acer
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Adobe =>.Adobe
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Amanita Design
=>.Amanita Design
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\appdatalow
=>.Microsoft Corporation
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\AppWork =>.Appwork
GmbH
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\AvastAdSDK =>.Avast
Software s.r.o
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\AVG =>.AVG Software
[HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Azureus =>.Azureus
Software \(P2P\)](#)
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Blizzard
Entertainment =>.Blizzard Entertainment
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\BlueStacksInstaller
=>.BlueStack Systems, Inc.
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\BugSplat
=>.Bugsplat Game
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Bulwark Studios
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\calibre =>.Kovid
Goyal
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Cellar Door Games
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\ChangeTracker
=>.Legitimate
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Chromium
=>.Chromium
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Daniel Mullins Games
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Dead Mage
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Draknek and Friends

HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\DrawMeAPixel
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Dropbox =>.Dropbox
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\DropboxUpdate
=>.Dropbox Inc.
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\ej-technologies
=>.ej-technologies
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\ElAmigos
=>.ElAmigos
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Electronic Arts
=>.Electronic Arts
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Epic Games =>.Epic
Games
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\EqualizerAPO
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\EurekaLab
=>.EurekaLab
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\EUROSMART
=>.EUROSMART
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Foxit Software
=>.Foxit Software
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\GNU =>.GNU
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\GOG.com =>.GOG.com
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Google =>.Google
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Haemimont Games
=>.Haemimont Games
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\HotspotShield
=>.AnchorFree Inc.
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Index Education
=>.Index Education
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Intel =>.Intel
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\JavaSoft
=>.JavaSoft
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Khronos =>.Khronos
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Klei
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Konfa Games
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Lantern Studio
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Larian Studios
=>.Larian Studios
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\LightbulbCrew
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Local AppWizard-
Generated Applications =>.ZWCAD
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Logitech
=>.Logitech
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Magnet =>.Magnet
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\MatchWare
=>.MatchWare
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Michael Herf
=>.Michael Herf
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Mobius Digital
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Mojang =>.Mojang
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Moon Studios
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Mozilla =>.Mozilla
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\MozillaPlugins
=>.MozillaPlugins
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\My Application
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Nerial
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Netscape
=>.Netscape
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\NVIDIA Corporation
=>.nVidia Corporation
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\ObviousIdea
=>.ObviousIdea
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\OEM =>.OEM
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Opera Software
=>.Opera Software

HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Opera Stable Offer
=>.Opera Software
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Optillusion
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Owlcat Games
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Paradox Interactive
=>.Paradox Interactive
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Parisprog
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Piriform
=>.Piriform
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\QtProject
=>.QtProject
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\RasTop
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Realtek =>.Realtek
Semiconductor Corp.
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\RedHook
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\
RegisteredApplications =>.Microsoft Corporation
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Simogo
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Softdeluxe
=>.Softdeluxe
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Spidersoft
=>.Spidersoft
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Studio Seufz
=>.Pinnacle Systems, Inc.
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\SunheadGames
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Team17 Digital
Limited =>.Team17
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Team17 Digital Ltd.
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\TelegramDesktop
=>.TelegramDesktop
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\The Document
Foundation =>.The Document Foundation
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Thunder Lotus Games
=>.Thunder Lotus Games
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\UnPas2Asp.exe
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Valve =>.Valve
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Wargaming.net
=>.Wargaming.net
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Winamp =>.Nullsoft
Inc.
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Windscribe
=>.Windscribe
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\WinHTTrack Website
Copier =>.Xavier Roche
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\WinRAR =>.WinRAR
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\WinRAR SFX
=>.RarLab
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Wintertree
=>.Wintertree Software
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\WixSharp
=>.Legitimate
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\Wow6432Node
=>.Microsoft Corporation
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\ZAUM Studio
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\ZHP =>.Nicolas
Coolman
HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\SOFTWARE\ZoomUMX

---\ Packages (23) - 0s

C:\Program Files (x86)\WindowsApps\1527c705-839a-4832-9118-54d4Bd6a0c89_10.0.19640.1000_neutral_neutral_cw5n1h2txyewy - (..) [][ms-resource:AppxManifest_DisplayName]

C:\Program Files (x86)\WindowsApps\
AcerIncorporated.AcerCareCenterS_4.0.3042.0_x64__48frkmn4z8aw4 - (.Acer Inc..) []
[Care Center S] =>Acer Inc.
C:\Program Files (x86)\WindowsApps\
AcerIncorporated.NitroSenseV31_3.1.3008.0_x64__48frkmn4z8aw4 - (.Acer Inc..) []
[NitroSense_V31] =>Acer Inc.
C:\Program Files (x86)\WindowsApps\
AcerIncorporated.QuickAccess_3.0.3038.0_x64__48frkmn4z8aw4 - (.Acer Inc..) []
[QuickAccess] =>Acer Inc.
C:\Program Files (x86)\WindowsApps\
AD2F1837.HPPrinterControl_139.2.289.0_x64__v10z8vjag6ke6 - (.Hewlett-Packard.)
[HP Smart] =>Hewlett-Packard
C:\Program Files (x86)\WindowsApps\
AppUp.IntelGraphicsControlPanel_3.3.0.0_x64__8j3eq9eme6ctt - (.Intel
Corporation.) [] [Intel® Graphics Control Panel] =>Intel Corporation
C:\Program Files (x86)\WindowsApps\
AppUp.IntelGraphicsExperience_1.100.3408.0_x64__8j3eq9eme6ctt - (.INTEL CORP.)
[ms-resource:System_Item_Title_IntelGraphicsControlPanel] =>INTEL CORP
C:\Program Files (x86)\WindowsApps\c5e2524a-ea46-4f67-841f-
6a9465d9d515_10.0.22621.1_neutral_neutral_cw5n1h2txyewy - (.Microsoft
Corporation.) [] [ms-resource:AppxManifest_DisplayName] =>Microsoft Corporation
C:\Program Files (x86)\WindowsApps\
Clipchamp.Clipchamp_2.5.1.0_neutral_yxz26nhyzhsrt - (..) [] [Clipchamp]
C:\Program Files (x86)\WindowsApps\
CyberLinkCorp.ac.PhotoDirectorforacerDesktop_8.0.5229.0_x64__ypz87dpkv292 -
(.CyberLink Corporation.) [] [PhotoDirector for acer] =>CyberLink Corporation
C:\Program Files (x86)\WindowsApps\
CyberLinkCorp.ac.PowerDirectorforacerDesktop_14.0.4304.0_x64__ypz87dpkv292 -
(.CyberLink Corporation.) [] [PowerDirector for acer] =>CyberLink Corporation
C:\Program Files (x86)\WindowsApps\
DropboxInc.Dropbox_159.4.5870.0_x64__wkt425jdc3sga - (.Dropbox Inc..) []
[Dropbox] =>Dropbox Inc.
C:\Program Files (x86)\WindowsApps\E2A4F912-2574-4A75-9BB0-
0D023378592B_10.0.19640.1000_neutral_neutral_cw5n1h2txyewy - (..) [] [ms-
resource:AppxManifest_DisplayName]
C:\Program Files (x86)\WindowsApps\F46D4000-FD22-4DB4-AC8E-
4E1DDDE828FE_10.0.22621.1_neutral_neutral_cw5n1h2txyewy - (.Microsoft
Corporation.) [] [ms-resource:AppxManifest_DisplayName] =>Microsoft Corporation
C:\Program Files (x86)\WindowsApps\G0TrustTechnologyInc.G0-
TrustAuthenticator_3.1.21.0_x64__0r04f53sqacg6 - (.GoTrustID Inc..) [] [GoTrust
ID]
C:\Program Files (x86)\WindowsApps\
MicrosoftCorporationII.MicrosoftFamily_0.1.28.0_x64__8wekyb3d8bbwe - (..) []
[Microsoft Family]
C:\Program Files (x86)\WindowsApps\
MicrosoftCorporationII.QuickAssist_2.0.9.0_x64__8wekyb3d8bbwe - (..) [] [ms-
resource:APP_WINDOW_NAME]
C:\Program Files (x86)\WindowsApps\
MicrosoftWindows.Client.CBS_1000.22634.1000.0_x64__cw5n1h2txyewy - (.Microsoft
Corporation.) [] [ms-resource:ProductPkgDisplayName] =>Microsoft Corporation
C:\Program Files (x86)\WindowsApps\
MicrosoftWindows.Client.WebExperience_421.20070.715.0_x64__cw5n1h2txyewy -
(.Microsoft Corporation.) [] [Windows Web Experience Pack] =>Microsoft
Corporation
C:\Program Files (x86)\WindowsApps\
MicrosoftWindows.UndockedDevKit_10.0.22621.1_neutral_neutral_cw5n1h2txyewy -
(..) [] [UDK Package]
C:\Program Files (x86)\WindowsApps\
NcsiUwpApp_1000.22621.1.0_neutral_neutral_8wekyb3d8bbwe - (.Microsoft.) []
[NcsiUwpApp] =>Microsoft
C:\Program Files (x86)\WindowsApps\
NVIDIACorp.NVIDIAControlPanel_8.1.963.0_x64__56jybvy8sckqj - (.nVidia
Corporation.) [] [NVIDIA Control Panel] =>nVidia Corporation

C:\Program Files (x86)\WindowsApps\
RealtekSemiconductorCorp.RealtekAudioControl_1.10.216.0_x64_dt26b99r8h8gj -
(.Realtek Semiconductor Corp.) [][Realtek Audio Control] =>Realtek
Semiconductor Corp

---\ Contents of the Common Files folders (399) - 16s

043 - CFD: 27/06/2019 - [] D -- C:\Program Files\Acer =>.Acer Incorporated®
043 - CFD: 24/10/2022 - [] D -- C:\Program Files\Adobe =>.Adobe
043 - CFD: 17/09/2022 - [] D -- C:\Program Files\Calibre2 =>.Kovid Goyal
043 - CFD: 24/10/2022 - [] D -- C:\Program Files\Common Files =>.Microsoft
Corporation
043 - CFD: 24/10/2021 - [] D -- C:\Program Files\Cybelsoft =>.Cybelsoft
043 - CFD: 14/10/2022 - [] D -- C:\Program Files\DIFX =>.Microsoft Corporation
043 - CFD: 27/06/2019 - [] D -- C:\Program Files\DriverSetupUtility =>.Acer
Incorporated®
043 - CFD: 24/08/2020 - [] D -- C:\Program Files\EqualizerAPO
043 - CFD: 23/04/2021 - [] D -- C:\Program Files\HotspotShield TAP-Windows
=>.OpenVPN Technologie
043 - CFD: 15/07/2022 - [] D -- C:\Program Files\HPPrintScanDoctor =>.HP Inc.®
043 - CFD: 16/10/2022 - [] D -- C:\Program Files\Intel =>.Intel Corporation
043 - CFD: 16/10/2022 - [] D -- C:\Program Files\Internet Explorer =>.Microsoft
Corporation
043 - CFD: 04/09/2020 - [] D -- C:\Program Files\JBL
{056D88813EC335DA59DD5AF48295961F}.
043 - CFD: 19/08/2020 - [] D -- C:\Program Files\LibreOffice =>.LibreOffice
043 - CFD: 24/10/2022 - [] D -- C:\Program Files\Logitech =>.Logitech Inc®
043 - CFD: 05/04/2022 - [] D -- C:\Program Files\Microsoft Update Health Tools
=>.Microsoft Corporation
043 - CFD: 07/05/2022 - [0] D -- C:\Program Files\ModifiableWindowsApps
=>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] D -- C:\Program Files\MSBuild =>.Microsoft
Corporation
043 - CFD: 22/10/2022 - [] D -- C:\Program Files\NVIDIA Corporation =>.nVidia
Corporation
043 - CFD: 24/10/2021 - [] D -- C:\Program Files\PCHealthCheck =>.Microsoft®
043 - CFD: 16/10/2022 - [] D -- C:\Program Files\Reference Assemblies
=>.Microsoft Corporation
043 - CFD: 27/09/2022 - [] D -- C:\Program Files\Stellarium =>.The Qt Company
Oy®
043 - CFD: 19/08/2020 - [] D -- C:\Program Files\TAP-Windows =>.OpenVPN
Technologie
043 - CFD: 14/10/2022 - [] D -- C:\Program Files\TUCam Camera Driver
043 - CFD: 27/06/2019 - [0] HD -- C:\Program Files\Uninstall Information
=>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] D -- C:\Program Files\UNP =>.Microsoft Corporation
043 - CFD: 19/08/2020 - [] D -- C:\Program Files\VideoLAN =>.VideoLan Team
043 - CFD: 30/04/2021 - [] D -- C:\Program Files\vJoy [Unsigned]
043 - CFD: 19/08/2020 - [] D -- C:\Program Files\Vuze =>.Azureus Software,
Inc.®
043 - CFD: 16/10/2022 - [] D -- C:\Program Files\Windows Defender =>.Microsoft
Corporation
043 - CFD: 16/10/2022 - [] D -- C:\Program Files\Windows Mail =>.Microsoft
Corporation
043 - CFD: 16/10/2022 - [] D -- C:\Program Files\Windows Media Player
=>.Microsoft Corporation
043 - CFD: 07/05/2022 - [] D -- C:\Program Files\Windows NT =>.Microsoft
Corporation
043 - CFD: 16/10/2022 - [] D -- C:\Program Files\Windows Photo Viewer
=>.Microsoft Corporation
043 - CFD: 07/05/2022 - [] SHD -- C:\Program Files\Windows Sidebar =>.Microsoft
Corporation
043 - CFD: 31/10/2022 - [] HD -- C:\Program Files\WindowsApps =>.Microsoft
Corporation

043 - CFD: 07/05/2022 - [] D -- C:\Program Files\WindowsPowerShell =>.Microsoft Corporation
043 - CFD: 15/07/2022 - [] D -- C:\Program Files\WinHTTrack =>.HTTrack
043 - CFD: 24/10/2021 - [] D -- C:\Program Files\WinRAR =>.win.rar GmbH®
043 - CFD: 24/08/2020 - [] D -- C:\Program Files (x86)\Acer =>.Acer Incorporated®
043 - CFD: 22/05/2022 - [] D -- C:\Program Files (x86)\Adobe =>.Adobe Inc.®
043 - CFD: 04/10/2021 - [] D -- C:\Program Files (x86)\Anagene2 [Unsigned]
043 - CFD: 14/10/2021 - [] D -- C:\Program Files (x86)\ASUS =>.ASUSTeK Computer Inc.®
043 - CFD: 03/08/2022 - [] D -- C:\Program Files (x86)\Battle.net =>.Games Software
043 - CFD: 19/08/2020 - [] D -- C:\Program Files (x86)\CCleaner Browser
043 - CFD: 16/10/2022 - [] D -- C:\Program Files (x86)\Common Files =>.Microsoft Corporation
043 - CFD: 13/10/2022 - [] D -- C:\Program Files (x86)\Dropbox =>.Dropbox, Inc®
043 - CFD: 22/04/2022 - [] D -- C:\Program Files (x86)\Electronic Arts =>.Electronic Arts®
043 - CFD: 27/10/2021 - [] D -- C:\Program Files (x86)\Epic Games =>.Epic Games
043 - CFD: 05/09/2022 - [] D -- C:\Program Files (x86)\EPSON Projector =>.Epson/Seico
043 - CFD: 13/10/2022 - [] D -- C:\Program Files (x86)\Eurosmart [Unsigned] =>.EUROSMART
043 - CFD: 18/12/2021 - [] D -- C:\Program Files (x86)\FastStone Photo Resizer =>.FastStone Soft
043 - CFD: 24/10/2021 - [0] D -- C:\Program Files (x86)\Firaxis Games =>.Firaxis Games
043 - CFD: 19/08/2020 - [] D -- C:\Program Files (x86)\Foxit Software =>.Foxit Software
043 - CFD: 11/09/2020 - [] D -- C:\Program Files (x86)\Garena {46A0800C34C5FEE85DB1758D556C2D0E}. =>.Garena
043 - CFD: 31/10/2022 - [] D -- C:\Program Files (x86)\Google =>.Google Inc®
043 - CFD: 03/08/2022 - [] D -- C:\Program Files (x86)\Hearthstone =>.Blizzard Entertainment
043 - CFD: 19/08/2022 - [] D -- C:\Program Files (x86)\Hotspot Shield =>.Pango Inc.®
043 - CFD: 24/05/2022 - [] D -- C:\Program Files (x86)\index education {59BFA29DD2D6F208659847D2}. =>.Index Education
043 - CFD: 06/09/2022 - [] HD -- C:\Program Files (x86)\InstallShield Installation Information =>.InstallShield
043 - CFD: 22/10/2022 - [] D -- C:\Program Files (x86)\Intel =>.Intel Corporation
043 - CFD: 16/10/2022 - [] D -- C:\Program Files (x86)\Internet Explorer =>.Microsoft Corporation
043 - CFD: 25/08/2020 - [] D -- C:\Program Files (x86)\Letasoft Sound Booster
043 - CFD: 16/10/2022 - [] D -- C:\Program Files (x86)\Microsoft =>.Microsoft Corporation
043 - CFD: 09/07/2022 - [] D -- C:\Program Files (x86)\Microsoft SQL Server Compact Edition =>.Microsoft Corporation
043 - CFD: 22/04/2022 - [] D -- C:\Program Files (x86)\Microsoft WSE =>.Microsoft Corporation
043 - CFD: 26/12/2020 - [] D -- C:\Program Files (x86)\Microsoft XNA =>.Microsoft Corporation
043 - CFD: 07/05/2022 - [] D -- C:\Program Files (x86)\Microsoft.NET =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] D -- C:\Program Files (x86)\MSBuild =>.Microsoft Corporation
043 - CFD: 22/10/2022 - [] D -- C:\Program Files (x86)\NVIDIA Corporation =>.nVidia Corporation
043 - CFD: 18/12/2021 - [] D -- C:\Program Files (x86)\ObviousIdea =>.ObviousIdea
043 - CFD: 21/12/2020 - [] D -- C:\Program Files (x86)\OpenAL =>.Open Audio Library
043 - CFD: 24/10/2022 - [] D -- C:\Program Files (x86)\Realtek =>.Realtek

043 - CFD: 16/10/2022 - [] D -- C:\Program Files (x86)\Reference Assemblies
=>.Microsoft Corporation
043 - CFD: 25/08/2020 - [0] HD -- C:\Program Files (x86)\Temp =>.Microsoft
Corporation
043 - CFD: 26/10/2021 - [0] HD -- C:\Program Files (x86)\Uninstall Information
=>.Microsoft Corporation
043 - CFD: 12/05/2021 - [] D -- C:\Program Files (x86)\Web Dumper
043 - CFD: 16/10/2022 - [] D -- C:\Program Files (x86)\Windows Defender
=>.Microsoft Corporation
043 - CFD: 09/07/2022 - [] D -- C:\Program Files (x86)\Windows Live
=>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] D -- C:\Program Files (x86)\Windows Mail
=>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] D -- C:\Program Files (x86)\Windows Media Player
=>.Microsoft Corporation
043 - CFD: 07/05/2022 - [] D -- C:\Program Files (x86)\Windows NT =>.Microsoft
Corporation
043 - CFD: 16/10/2022 - [] D -- C:\Program Files (x86)\Windows Photo Viewer
=>.Microsoft Corporation
043 - CFD: 07/05/2022 - [] SHD -- C:\Program Files (x86)\Windows Sidebar
=>.Microsoft Corporation
043 - CFD: 07/05/2022 - [] D -- C:\Program Files (x86)\WindowsPowerShell
=>.Microsoft Corporation
043 - CFD: 06/01/2021 - [] D -- C:\Program Files (x86)\Windscribe =>.Windscribe
043 - CFD: 07/05/2022 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\Accessibility =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\Accessories =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\Acer =>.Acer
043 - CFD: 07/05/2022 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\Administrative Tools =>.Administrative Tools
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\Adobe =>.Adobe
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\Anagène 2
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\Battle.net =>.Games Software
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\calibre 64bit - E-book Management =>.Kovid Goyal
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\Celeste Farewell
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\Dome Keeper
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\DriversCloud.com =>.Cybelsoft
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\Dropbox =>.Dropbox
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\EPSON Projector =>.Epson/Seico
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\Eurosmart =>.EUROSMART
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\FastStone Photo Resizer =>.FastStone Soft
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\Foxit PDF Reader
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\Garena =>.Garena
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\Hearthstone =>.Blizzard Entertainment
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\Hotspot Shield =>.Hotspot Shield
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\
Programs\LibreOffice 7.0 =>.LibreOffice

043 - CFD: 24/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Logitech =>.Logitech
043 - CFD: 07/05/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Maintenance =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\NVIDIA Corporation =>.nVidia Corporation
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\ObviousIdea =>.ObviousIdea
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Outer Wilds Echoes of the Eye
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\PrintMe Internet Printing
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Riot Games =>.Riot Games
043 - CFD: 07/05/2022 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Stellarium
043 - CFD: 07/05/2022 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\System Tools =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\VideoLAN =>.VideoLan Team
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\vJoy
043 - CFD: 26/10/2021 - [0] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\WiFi Password Decryptor
043 - CFD: 07/05/2022 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Windows PowerShell =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Windscribe =>.Windscribe
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\WinHTTrack =>.HTTrack
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\WinRAR =>.WinRAR
043 - CFD: 19/08/2020 - [] D -- C:\ProgramData\Acer =>.Acer
043 - CFD: 04/10/2021 - [] D -- C:\ProgramData\Adobe =>.Adobe
043 - CFD: 16/10/2022 - [0] SHD -- C:\ProgramData\Application Data =>.Microsoft Corporation
043 - CFD: 22/10/2020 - [] D -- C:\ProgramData\ASUS =>.ASUS
043 - CFD: 11/11/2020 - [] D -- C:\ProgramData\Avast Software =>.AVAST Software
043 - CFD: 24/01/2022 - [] D -- C:\ProgramData\AVG =>.AVG Software
043 - CFD: 11/09/2020 - [] D -- C:\ProgramData\Battle.net =>.Games Software
043 - CFD: 11/09/2020 - [] D -- C:\ProgramData\Blizzard Entertainment
=>.Blizzard Entertainment
043 - CFD: 31/10/2022 - [] D -- C:\ProgramData\boost_interprocess =>.boost.org
043 - CFD: 12/04/2022 - [] D -- C:\ProgramData\BSD =>.Berkeley
043 - CFD: 26/12/2020 - [] HD -- C:\ProgramData\CyberLink =>.CyberLink Corporation
043 - CFD: 16/10/2022 - [0] SHD -- C:\ProgramData\Desktop =>.Microsoft Corporation
043 - CFD: 24/08/2020 - [] SHD -- C:\ProgramData\DIBsection
043 - CFD: 16/10/2022 - [0] SHD -- C:\ProgramData\Documents =>.Microsoft Corporation
043 - CFD: 24/10/2021 - [] D -- C:\ProgramData\DriversCloud.com =>.Cybelsoft
043 - CFD: 27/06/2019 - [] D -- C:\ProgramData\DriverSetupUtility
043 - CFD: 28/08/2020 - [] D -- C:\ProgramData\Dropbox =>.Dropbox
043 - CFD: 27/10/2021 - [] D -- C:\ProgramData\Epic =>.Epic
043 - CFD: 19/08/2020 - [] D -- C:\ProgramData\Foxit ContentPlatform =>.Foxit Corporation
043 - CFD: 09/06/2021 - [] D -- C:\ProgramData\Foxit Software =>.Foxit Software
043 - CFD: 28/08/2020 - [] D -- C:\ProgramData\Garena =>.Garena
043 - CFD: 19/08/2020 - [] D -- C:\ProgramData\GOG.com =>.GOG.com
043 - CFD: 19/08/2022 - [] D -- C:\ProgramData\Hotspot Shield =>.Hotspot Shield
043 - CFD: 08/07/2022 - [] D -- C:\ProgramData\HP =>.Hewlett-Packard

043 - CFD: 06/09/2022 - [] D -- C:\ProgramData\IndexEducation =>.ION
043 - CFD: 24/10/2022 - [] D -- C:\ProgramData\Intel =>.Intel Corporation
043 - CFD: 24/10/2022 - [] D -- C:\ProgramData\Intel Package Cache {1CEAC85D-2590-4760-800F-8DE5E91F3700}
043 - CFD: 24/10/2022 - [] D -- C:\ProgramData\Intel Package Cache {58E22E6B-0E58-4E93-AF9A-036556EB66F5}
043 - CFD: 24/10/2022 - [] D -- C:\ProgramData\Intel Package Cache {9f9c9e51-d42f-4462-a27a-7d419da18045}
043 - CFD: 24/10/2022 - [] D -- C:\ProgramData\Intel Package Cache {d8170687-85fa-4716-bafd-087205d0db72}
043 - CFD: 22/10/2022 - [] D -- C:\ProgramData\Logishrd =>.Logitech Inc.
043 - CFD: 16/10/2022 - [] SD -- C:\ProgramData\Microsoft =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Microsoft OneDrive =>.Microsoft Corporation
043 - CFD: 19/08/2020 - [] D -- C:\ProgramData\Mozilla =>.Mozilla Corporation
043 - CFD: 16/09/2020 - [] D -- C:\ProgramData\Norton =>.Symantec Corporation
043 - CFD: 27/06/2019 - [] D -- C:\ProgramData\NortonInstaller =>.Symantec
043 - CFD: 31/10/2022 - [] D -- C:\ProgramData\NVIDIA =>.nVidia Corporation
043 - CFD: 22/10/2022 - [] D -- C:\ProgramData\NVIDIA Corporation =>.nVidia Corporation
043 - CFD: 12/08/2020 - [] D -- C:\ProgramData\OEM =>.OEM
043 - CFD: 19/08/2020 - [] D -- C:\ProgramData\Oracle =>.Oracle
043 - CFD: 14/10/2022 - [] D -- C:\ProgramData\Package Cache =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\Packages =>.Microsoft Corporation
043 - CFD: 31/10/2022 - [] D -- C:\ProgramData\regid.1991-06.com.microsoft =>.Microsoft Corporation
043 - CFD: 23/12/2021 - [] D -- C:\ProgramData\Riot Games =>.Riot Games
043 - CFD: 07/05/2022 - [0] D -- C:\ProgramData\SoftwareDistribution =>.Microsoft Corporation
043 - CFD: 01/08/2022 - [] D -- C:\ProgramData\SplitMediaLabs =>.SplitMediaLabs
043 - CFD: 07/05/2022 - [0] D -- C:\ProgramData\ssh =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [0] SHD -- C:\ProgramData\Start Menu =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [0] SHD -- C:\ProgramData\Templates =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] D -- C:\ProgramData\USOPrivate =>.Microsoft Corporation
043 - CFD: 07/05/2022 - [] D -- C:\ProgramData\USOShared =>.Microsoft Corporation
043 - CFD: 18/12/2020 - [] D -- C:\ProgramData\Wargaming.net =>.Wargaming.net
043 - CFD: 07/05/2022 - [] D -- C:\ProgramData\WindowsHolographicDevices =>.Microsoft Corporation
043 - CFD: 21/02/2021 - [] D -- C:\Program Files (x86)\Common Files\InstallShield =>.InstallShield
043 - CFD: 04/11/2020 - [] D -- C:\Program Files (x86)\Common Files\Java =>.Oracle
043 - CFD: 16/10/2022 - [] D -- C:\Program Files (x86)\Common Files\Microsoft Shared =>.Microsoft Corporation
043 - CFD: 16/07/2022 - [] D -- C:\Program Files (x86)\Common Files\Steam =>.Steam Games
043 - CFD: 16/09/2020 - [0] D -- C:\Program Files (x86)\Common Files\Symantec Shared =>.Symantec Corporation
043 - CFD: 16/10/2022 - [] D -- C:\Program Files (x86)\Common Files\System =>.Microsoft Corporation
043 - CFD: 09/07/2022 - [] D -- C:\Program Files (x86)\Common Files\Windows Live =>.Microsoft Corporation
043 - CFD: 05/09/2021 - [] D -- C:\Users\User\AppData\Roaming\.minecraft =>.Microsoft Corporation
043 - CFD: 19/08/2020 - [] D -- C:\Users\User\AppData\Roaming\.mono =>.Legitimate

043 - CFD: 09/03/2022 - [] D -- C:\Users\User\AppData\Roaming\11bitstudios
=>.11 Bit Studios
043 - CFD: 12/08/2020 - [] D -- C:\Users\User\AppData\Roaming\Adobe =>.Adobe
043 - CFD: 27/09/2020 - [] D -- C:\Users\User\AppData\Roaming\AoD
043 - CFD: 23/10/2022 - [] D -- C:\Users\User\AppData\Roaming\Azureus
043 - CFD: 15/04/2022 - [] D -- C:\Users\User\AppData\Roaming\Baba_Is_You
043 - CFD: 11/09/2020 - [] D -- C:\Users\User\AppData\Roaming\Battle.net
=>.Games Software
043 - CFD: 23/10/2022 - [] D -- C:\Users\User\AppData\Roaming\calibre =>.Kovid
Goyal
043 - CFD: 24/10/2021 - [] D -- C:\Users\User\AppData\Roaming\Cybelsoft
=>.Cybelsoft
043 - CFD: 22/04/2022 - [] D -- C:\Users\User\AppData\Roaming\Doublefine
043 - CFD: 28/08/2020 - [] D -- C:\Users\User\AppData\Roaming\Dropbox
=>.Dropbox
043 - CFD: 31/10/2022 - [] D -- C:\Users\User\AppData\Roaming\DropboxElectron
043 - CFD: 12/02/2022 - [] D -- C:\Users\User\AppData\Roaming\EMPRESS
043 - CFD: 31/01/2022 - [] D -- C:\Users\User\AppData\Roaming\FasterThanLight
043 - CFD: 18/12/2021 - [] D -- C:\Users\User\AppData\Roaming\FastStone
=>.FastStone Soft
043 - CFD: 19/08/2020 - [] D -- C:\Users\User\AppData\Roaming\FiraxisLive
=>.Firaxis
043 - CFD: 19/08/2020 - [] D -- C:\Users\User\AppData\Roaming\Foxit
AgentInformation =>.Foxit Corporation
043 - CFD: 09/06/2021 - [] D -- C:\Users\User\AppData\Roaming\Foxit Software
=>.Foxit Software
043 - CFD: 16/03/2022 - [] D -- C:\Users\User\AppData\Roaming\Godot
043 - CFD: 16/11/2020 - [] D -- C:\Users\User\AppData\Roaming\Goldberg
SocialClub Emu Saves
043 - CFD: 13/08/2021 - [] D -- C:\Users\User\AppData\Roaming\
HearthstoneDeckTracker =>.GitHub
043 - CFD: 19/08/2020 - [] D -- C:\Users\User\AppData\Roaming\HOODLUM
=>.Hoodlum
043 - CFD: 19/08/2020 - [] D -- C:\Users\User\AppData\Roaming\Identities
=>.Microsoft Corporation
043 - CFD: 12/08/2020 - [] D -- C:\Users\User\AppData\Roaming\Intel Corporation
=>.Intel Corporation
043 - CFD: 19/08/2020 - [] D -- C:\Users\User\AppData\Roaming\LibreOffice
=>.LibreOffice
043 - CFD: 22/10/2022 - [] D -- C:\Users\User\AppData\Roaming\Logishrd
=>.Logitech Inc.
043 - CFD: 27/09/2020 - [] D -- C:\Users\User\AppData\Roaming\Macromedia
=>.Macromedia
043 - CFD: 16/10/2022 - [] SD -- C:\Users\User\AppData\Roaming\Microsoft
=>.Microsoft Corporation
043 - CFD: 19/08/2020 - [] D -- C:\Users\User\AppData\Roaming\Mozilla
=>.Mozilla Corporation
043 - CFD: 18/12/2021 - [] D -- C:\Users\User\AppData\Roaming\Neos Eureka S.r.l
043 - CFD: 19/08/2020 - [] D -- C:\Users\User\AppData\Roaming\NVIDIA =>.nVidia
Corporation
043 - CFD: 18/12/2021 - [] D -- C:\Users\User\AppData\Roaming\ObviousIdea
=>.ObviousIdea
043 - CFD: 14/10/2022 - [0] D -- C:\Users\User\AppData\Roaming\Opera Software
=>.Opera Software
043 - CFD: 26/03/2021 - [] D -- C:\Users\User\AppData\Roaming\Paradox
Interactive =>.Paradox Interactive
043 - CFD: 04/09/2020 - [] D -- C:\Users\User\AppData\Roaming\RSI Launcher
043 - CFD: 22/02/2021 - [] D -- C:\Users\User\AppData\Roaming\rsilauncher
043 - CFD: 29/08/2020 - [] D -- C:\Users\User\AppData\Roaming\Skype =>.Skype
043 - CFD: 18/04/2021 - [] D -- C:\Users\User\AppData\Roaming\Steam =>.Steam
Games
043 - CFD: 28/09/2022 - [] D -- C:\Users\User\AppData\Roaming\Stellarium
043 - CFD: 07/04/2021 - [] D -- C:\Users\User\AppData\Roaming\Surviving Mars

043 - CFD: 24/10/2021 - [] D -- C:\Users\User\AppData\Roaming\TeamViewer
=>.TeamViewer GmbH
043 - CFD: 15/10/2022 - [] D -- C:\Users\User\AppData\Roaming\Telegram Desktop
=>.Telegram Messenger LLP
043 - CFD: 15/04/2022 - [] D -- C:\Users\User\AppData\Roaming\The Witness
043 - CFD: 20/11/2020 - [] D -- C:\Users\User\AppData\Roaming\TunnelBear
=>.TunnelBear
043 - CFD: 14/10/2022 - [] D -- C:\Users\User\AppData\Roaming\Unknown
Organization
043 - CFD: 12/02/2022 - [] D -- C:\Users\User\AppData\Roaming\uplay_emu
043 - CFD: 30/04/2021 - [] D -- C:\Users\User\AppData\Roaming\USB_HELPER
043 - CFD: 06/04/2022 - [] D -- C:\Users\User\AppData\Roaming\Vampire_Survivors
043 - CFD: 20/10/2022 - [] D -- C:\Users\User\AppData\Roaming\vlc =>.VideoLan
Team
043 - CFD: 24/10/2021 - [] D -- C:\Users\User\AppData\Roaming\Wargaming.net
=>.Wargaming.net
043 - CFD: 25/10/2022 - [] D -- C:\Users\User\AppData\Roaming\WhatsApp
=>.WhatsApp
043 - CFD: 23/08/2020 - [] D -- C:\Users\User\AppData\Roaming\WinRAR =>.WinRAR
043 - CFD: 31/10/2022 - [] D -- C:\Users\User\AppData\Roaming\ZHP =>.Nicolas
Coolman
043 - CFD: 09/12/2021 - [] D -- C:\Users\User\AppData\Roaming\Zoom =>.ZOOM
043 - CFD: 31/07/2021 - [] D -- C:\Users\User\AppData\Local\3DClouds
043 - CFD: 30/08/2021 - [] D -- C:\Users\User\AppData\Local\AcLoader
043 - CFD: 06/06/2021 - [] D -- C:\Users\User\AppData\Local\Adaware =>.adaware
043 - CFD: 22/05/2022 - [] D -- C:\Users\User\AppData\Local\
Adobe_Systems_Incorporate =>.Adobe Inc.
043 - CFD: 16/10/2022 - [0] SHD -- C:\Users\User\AppData\Local\Application Data
=>.Microsoft Corporation
043 - CFD: 24/10/2022 - [] D -- C:\Users\User\AppData\Local\Apps =>.Microsoft
Corporation
043 - CFD: 14/10/2021 - [] D -- C:\Users\User\AppData\Local\ArmouryLiveUpdate
043 - CFD: 03/08/2022 - [] D -- C:\Users\User\AppData\Local\Battle.net =>.Games
Software
043 - CFD: 11/09/2020 - [] D -- C:\Users\User\AppData\Local\Blizzard
=>.Blizzard
043 - CFD: 11/09/2020 - [] D -- C:\Users\User\AppData\Local\Blizzard
Entertainment =>.Blizzard Entertainment
043 - CFD: 08/07/2022 - [] D -- C:\Users\User\AppData\Local\BlueStacks
=>.BlueStack Systems, Inc.
043 - CFD: 24/08/2020 - [] D -- C:\Users\User\AppData\Local\Boom 3D
043 - CFD: 27/09/2022 - [] D -- C:\Users\User\AppData\Local\cache =>.Legitimate
043 - CFD: 11/10/2022 - [] D -- C:\Users\User\AppData\Local\calibre-cache
=>.Kovid Goyal
043 - CFD: 27/11/2020 - [] D -- C:\Users\User\AppData\Local\calibre-ebook.com
043 - CFD: 22/09/2020 - [] D -- C:\Users\User\AppData\Local\calibre-parallel
043 - CFD: 12/08/2020 - [] D -- C:\Users\User\AppData\Local\CareCenter =>.Acer
Inc.
043 - CFD: 19/08/2020 - [] D -- C:\Users\User\AppData\Local\CEF =>.CEF
043 - CFD: 30/04/2021 - [] D -- C:\Users\User\AppData\Local\Cemu
043 - CFD: 12/08/2020 - [] D -- C:\Users\User\AppData\Local\Comms =>.Microsoft
Corporation
043 - CFD: 12/08/2020 - [] D -- C:\Users\User\AppData\Local\
ConnectedDevicesPlatform =>.Microsoft Corporation
043 - CFD: 22/10/2022 - [] D -- C:\Users\User\AppData\Local\CrashDumps
=>.Microsoft Corporation
043 - CFD: 28/10/2021 - [] D -- C:\Users\User\AppData\Local\CrashReportClient
043 - CFD: 19/08/2022 - [] D -- C:\Users\User\AppData\Local\D3DSCache
=>.Legitimate
043 - CFD: 19/08/2020 - [0] D -- C:\Users\User\AppData\Local\DBG =>.DBG
043 - CFD: 24/10/2022 - [0] D -- C:\Users\User\AppData\Local\Deployment
=>.Microsoft Corporation
043 - CFD: 24/10/2022 - [] D -- C:\Users\User\AppData\Local\Diagnostics
=>.Microsoft Corporation

043 - CFD: 31/10/2022 - [] D -- C:\Users\User\AppData\Local\Dropbox =>.Dropbox
043 - CFD: 24/10/2022 - [] D -- C:\Users\User\AppData\Local\ElevatedDiagnostics
=>.Microsoft Corporation
043 - CFD: 27/10/2021 - [] D -- C:\Users\User\AppData\Local\EOSUserHelper
043 - CFD: 14/10/2022 - [] D -- C:\Users\User\AppData\Local\Epic Games =>.Epic
Games
043 - CFD: 14/10/2022 - [] D -- C:\Users\User\AppData\Local\EpicGamesLauncher
=>.Epic Games
043 - CFD: 18/12/2021 - [] D -- C:\Users\User\AppData\Local\FastStone
=>.FastStone Soft
043 - CFD: 27/09/2022 - [0] D -- C:\Users\User\AppData\Local\FluxSoftware
=>.Stereopsis
043 - CFD: 07/09/2020 - [] D -- C:\Users\User\AppData\Local\Foxit Reader
=>.Foxit Corporation
043 - CFD: 23/12/2020 - [] D -- C:\Users\User\AppData\Local\GameAnalytics
043 - CFD: 24/08/2020 - [] D -- C:\Users\User\AppData\Local\Global-Delight
043 - CFD: 14/11/2020 - [] D -- C:\Users\User\AppData\Local\GOG.com =>.GOG.com
043 - CFD: 19/08/2020 - [] D -- C:\Users\User\AppData\Local\Google =>.Google
043 - CFD: 24/10/2021 - [] D -- C:\Users\User\AppData\Local\
HearthstoneDeckTracker =>.GitHub
043 - CFD: 28/02/2021 - [] D -- C:\Users\User\AppData\Local\Helios =>.Helios
043 - CFD: 09/04/2022 - [] D -- C:\Users\User\AppData\Local\Hero_s_Hour
043 - CFD: 29/04/2021 - [] D -- C:\Users\User\AppData\Local\Hikari06
043 - CFD: 16/10/2022 - [0] SHD -- C:\Users\User\AppData\Local\History
=>.Microsoft Corporation
043 - CFD: 24/08/2020 - [0] SHD -- C:\Users\User\AppData\Local\icsxml
043 - CFD: 19/08/2020 - [] D -- C:\Users\User\AppData\Local\Indiana
043 - CFD: 12/08/2020 - [] D -- C:\Users\User\AppData\Local\Intel =>.Intel
Corporation
043 - CFD: 24/08/2020 - [] D -- C:\Users\User\AppData\Local\IsolatedStorage
=>.id Software
043 - CFD: 24/10/2021 - [] D -- C:\Users\User\AppData\Local\JDownloader 2.0
=>.JDownloader
043 - CFD: 17/04/2021 - [] D -- C:\Users\User\AppData\Local\LarianLauncher
043 - CFD: 16/03/2021 - [] D -- C:\Users\User\AppData\Local\Loop_Hero
043 - CFD: 24/01/2022 - [] D -- C:\Users\User\AppData\Local\mbam
=>.Malwarebytes
043 - CFD: 16/10/2022 - [] D -- C:\Users\User\AppData\Local\Microsoft
=>.Microsoft Corporation
043 - CFD: 19/08/2020 - [] D -- C:\Users\User\AppData\Local\MicrosoftEdge
=>.Microsoft Corporation
043 - CFD: 19/08/2020 - [] D -- C:\Users\User\AppData\Local\Mozilla =>.Mozilla
Corporation
043 - CFD: 24/08/2020 - [0] SHD -- C:\Users\User\AppData\Local\ms-drivers
043 - CFD: 20/08/2022 - [] D -- C:\Users\User\AppData\Local\Notepad
043 - CFD: 14/04/2021 - [] D -- C:\Users\User\AppData\Local\nuclearthrone
043 - CFD: 22/10/2022 - [] D -- C:\Users\User\AppData\Local\NVIDIA =>.nVidia
Corporation
043 - CFD: 02/12/2021 - [] D -- C:\Users\User\AppData\Local\NVIDIA Corporation
=>.nVidia Corporation
043 - CFD: 20/08/2020 - [] D -- C:\Users\User\AppData\Local\OneDrive
=>.Microsoft Corporation
043 - CFD: 14/10/2022 - [0] D -- C:\Users\User\AppData\Local\Opera Software
=>.Opera Software
043 - CFD: 21/08/2020 - [] D -- C:\Users\User\AppData\Local\Ori and the Will of
The Wisps
043 - CFD: 22/04/2022 - [] D -- C:\Users\User\AppData\Local\Origin
=>.Electronic Arts, Inc.
043 - CFD: 22/10/2022 - [] D -- C:\Users\User\AppData\Local\Packages
=>.Microsoft Corporation
043 - CFD: 26/03/2021 - [] D -- C:\Users\User\AppData\Local\Paradox Interactive
=>.Paradox Interactive
043 - CFD: 03/09/2022 - [] D -- C:\Users\User\AppData\Local\
PlaceholderTileLogoFolder =>.Microsoft Corporation

043 - CFD: 06/06/2021 - [] D -- C:\Users\User\AppData\Local\Programs
=>.Microsoft Corporation
043 - CFD: 28/08/2020 - [] D -- C:\Users\User\AppData\Local\Publishers
=>.Microsoft Corporation
043 - CFD: 22/10/2020 - [] D -- C:\Users\User\AppData\Local\Riot Games =>.Riot
Games
043 - CFD: 16/11/2020 - [] D -- C:\Users\User\AppData\Local\Rockstar Games
=>.Rockstar Games
043 - CFD: 25/08/2020 - [] D -- C:\Users\User\AppData\Local\Softdeluxe
=>.Softdeluxe
043 - CFD: 29/03/2022 - [] D -- C:\Users\User\AppData\Local\SquirrelTemp
=>.Squirrels
043 - CFD: 23/04/2021 - [] D -- C:\Users\User\AppData\Local\Steam =>.Steam
Games
043 - CFD: 27/09/2022 - [] D -- C:\Users\User\AppData\Local\stellarium
043 - CFD: 24/10/2021 - [] D -- C:\Users\User\AppData\Local\TeamViewer
=>.TeamViewer GmbH
043 - CFD: 31/10/2022 - [] D -- C:\Users\User\AppData\Local\Temp =>.Microsoft
Corporation
043 - CFD: 16/10/2022 - [0] SHD -- C:\Users\User\AppData\Local\Temporary
Internet Files =>.Microsoft Corporation
043 - CFD: 01/08/2021 - [] D -- C:\Users\User\AppData\Local\TheAscent
043 - CFD: 20/11/2020 - [] D -- C:\Users\User\AppData\Local\TunnelBear
=>.TunnelBear
043 - CFD: 01/08/2021 - [] D -- C:\Users\User\AppData\Local\UnrealEngine
=>.Unreal Software
043 - CFD: 27/10/2021 - [] D -- C:\Users\User\AppData\Local\UnrealEngineLauncher
=>.Unreal Software
043 - CFD: 13/10/2022 - [] D -- C:\Users\User\AppData\Local\VirtualStore
=>.Microsoft Corporation
043 - CFD: 22/10/2022 - [] D -- C:\Users\User\AppData\Local\WhatsApp
=>.WhatsApp
043 - CFD: 11/10/2022 - [] D -- C:\Users\User\AppData\Local\Windows Live
=>.Microsoft Corporation
043 - CFD: 28/12/2020 - [] D -- C:\Users\User\AppData\Local\Windscribe
=>.Windscribe
043 - CFD: 31/10/2022 - [] D -- C:\Users\User\AppData\Local\ZHP =>.Nicolas
Coolman
043 - CFD: 19/08/2020 - [0] D -- C:\Users\User\AppData\Local\Programs\Common
=>.Microsoft Corporation
043 - CFD: 14/10/2022 - [] D -- C:\Users\User\AppData\Local\Programs\Opera
=>.Opera Software
043 - CFD: 26/03/2021 - [] D -- C:\Users\User\AppData\Local\Programs\Paradox
Interactive =>.Paradox Interactive
043 - CFD: 19/03/2022 - [] D -- C:\Users\User\AppData\LocalLow\Amanita Design
=>.Amanita Design
043 - CFD: 11/09/2020 - [] D -- C:\Users\User\AppData\LocalLow\Blizzard
Entertainment =>.Blizzard Entertainment
043 - CFD: 27/02/2022 - [] D -- C:\Users\User\AppData\LocalLow\Bulwark Studios
043 - CFD: 01/02/2022 - [] D -- C:\Users\User\AppData\LocalLow\Cellar Door Games
043 - CFD: 19/03/2022 - [] D -- C:\Users\User\AppData\LocalLow\Daniel Mullins
Games
043 - CFD: 14/11/2020 - [] D -- C:\Users\User\AppData\LocalLow\Dead Mage
043 - CFD: 16/09/2020 - [] D -- C:\Users\User\AppData\LocalLow\Draknek and
Friends
043 - CFD: 23/08/2020 - [] D -- C:\Users\User\AppData\LocalLow\DrawMeAPixel
043 - CFD: 28/08/2020 - [] D -- C:\Users\User\AppData\LocalLow\Foxit
043 - CFD: 28/08/2020 - [] D -- C:\Users\User\AppData\LocalLow\Intel =>.Intel
Corporation
043 - CFD: 19/08/2020 - [] D -- C:\Users\User\AppData\LocalLow\Klei
043 - CFD: 13/02/2021 - [] D -- C:\Users\User\AppData\LocalLow\Konfa Games
043 - CFD: 19/01/2021 - [] D -- C:\Users\User\AppData\LocalLow\Lantern Studio
043 - CFD: 19/08/2020 - [] D -- C:\Users\User\AppData\LocalLow\LightbulbCrew

043 - CFD: 09/07/2022 - [] SD -- C:\Users\User\AppData\LocalLow\Microsoft
=>.Microsoft Corporation
043 - CFD: 19/08/2020 - [] D -- C:\Users\User\AppData\LocalLow\Mobius Digital
043 - CFD: 19/08/2020 - [] D -- C:\Users\User\AppData\LocalLow\Moon Studios
043 - CFD: 19/08/2020 - [0] D -- C:\Users\User\AppData\LocalLow\Mozilla
=>.Mozilla Corporation
043 - CFD: 19/08/2020 - [] D -- C:\Users\User\AppData\LocalLow\Nerial
043 - CFD: 20/03/2022 - [] D -- C:\Users\User\AppData\LocalLow\Optillusion
043 - CFD: 09/10/2020 - [] D -- C:\Users\User\AppData\LocalLow\Oracle =>.Oracle
043 - CFD: 03/11/2020 - [] D -- C:\Users\User\AppData\LocalLow\Owlcat Games
043 - CFD: 27/10/2021 - [] D -- C:\Users\User\AppData\LocalLow\RedHook
043 - CFD: 18/12/2020 - [] D -- C:\Users\User\AppData\LocalLow\Simogo
043 - CFD: 30/12/2020 - [] D -- C:\Users\User\AppData\LocalLow\Studio Seufz
=>.Pinnacle Systems, Inc.
043 - CFD: 09/10/2020 - [] D -- C:\Users\User\AppData\LocalLow\Sun =>.Oracle
043 - CFD: 19/01/2021 - [] D -- C:\Users\User\AppData\LocalLow\SunheadGames
043 - CFD: 30/12/2020 - [] D -- C:\Users\User\AppData\LocalLow\Team17 Digital
Ltd_
043 - CFD: 05/02/2021 - [] D -- C:\Users\User\AppData\LocalLow\Temp
=>.Microsoft Corporation
043 - CFD: 19/01/2021 - [] D -- C:\Users\User\AppData\LocalLow\Thunder Lotus
Games =>.Thunder Lotus Games
043 - CFD: 08/09/2020 - [] D -- C:\Users\User\AppData\LocalLow\ZAUM Studio
043 - CFD: 05/09/2022 - [] D -- C:\Users\User\Desktop\cle usb
043 - CFD: 10/07/2022 - [] D -- C:\Users\User\Desktop\cours
043 - CFD: 20/01/2022 - [] AD -- C:\Users\User\Desktop\cv2020
043 - CFD: 16/10/2022 - [] AD -- C:\Users\User\Desktop\jeux =>.Games Software
043 - CFD: 01/10/2022 - [] D -- C:\Users\User\Desktop\labo
043 - CFD: 21/10/2022 - [] D -- C:\Users\User\Desktop\livre
043 - CFD: 22/10/2022 - [] D -- C:\Users\User\Desktop\lubumbashi
043 - CFD: 28/10/2022 - [] D -- C:\Users\User\Desktop\medete
043 - CFD: 13/10/2022 - [] D -- C:\Users\User\Desktop\orientation seconde
043 - CFD: 22/10/2022 - [] AD -- C:\Users\User\Desktop\photo
043 - CFD: 31/08/2021 - [] D -- C:\Users\User\Desktop\Phylogène-Lycée-2021
043 - CFD: 28/10/2022 - [] D -- C:\Users\User\Desktop\sci
043 - CFD: 22/10/2022 - [] D -- C:\Users\User\Desktop\spc term
043 - CFD: 27/10/2022 - [] D -- C:\Users\User\Desktop\tp7
043 - CFD: 07/05/2022 - [] RD -- C:\Users\User\AppData\Roaming\Microsoft\
Windows\Start Menu\Programs\Accessibility =>.Microsoft Corporation
043 - CFD: 07/05/2022 - [] D -- C:\Users\User\AppData\Roaming\Microsoft\Windows\
Start Menu\Programs\Accessories =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] RD -- C:\Users\User\AppData\Roaming\Microsoft\
Windows\Start Menu\Programs\Administrative Tools =>.Administrative Tools
043 - CFD: 24/10/2021 - [0] D -- C:\Users\User\AppData\Roaming\Microsoft\
Windows\Start Menu\Programs\HearthSim =>.HearthSim
043 - CFD: 07/05/2022 - [] D -- C:\Users\User\AppData\Roaming\Microsoft\Windows\
Start Menu\Programs\Maintenance =>.Microsoft Corporation
043 - CFD: 22/10/2020 - [0] D -- C:\Users\User\AppData\Roaming\Microsoft\
Windows\Start Menu\Programs\Riot Games =>.Riot Games
043 - CFD: 16/10/2022 - [] RD -- C:\Users\User\AppData\Roaming\Microsoft\
Windows\Start Menu\Programs\Startup =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] D -- C:\Users\User\AppData\Roaming\Microsoft\Windows\
Start Menu\Programs\Steam =>.Steam Games
043 - CFD: 07/05/2022 - [] RD -- C:\Users\User\AppData\Roaming\Microsoft\
Windows\Start Menu\Programs\System Tools =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] D -- C:\Users\User\AppData\Roaming\Microsoft\Windows\
Start Menu\Programs\Telegram Desktop =>.Telegram Messenger LLP
043 - CFD: 16/10/2022 - [] D -- C:\Users\User\AppData\Roaming\Microsoft\Windows\
Start Menu\Programs\WebZIP
043 - CFD: 16/10/2022 - [] D -- C:\Users\User\AppData\Roaming\Microsoft\Windows\
Start Menu\Programs\WhatsApp =>.WhatsApp
043 - CFD: 16/10/2022 - [] D -- C:\Users\User\AppData\Roaming\Microsoft\Windows\
Start Menu\Programs\Windows PowerShell =>.Microsoft Corporation

043 - CFD: 16/10/2022 - [] D -- C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\WinRAR =>.WinRAR
043 - CFD: 16/10/2022 - [] D -- C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Zoom =>.ZOOM
043 - CFD: 16/10/2022 - [0] SHD -- C:\Users\Default\AppData\Local\Application Data =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [0] SHD -- C:\Users\Default\AppData\Local\History =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] D -- C:\Users\Default\AppData\Local\Microsoft =>.Microsoft Corporation
043 - CFD: 07/05/2022 - [0] D -- C:\Users\Default\AppData\Local\Temp =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [0] SHD -- C:\Users\Default\AppData\Local\Temporary Internet Files =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [0] SHD -- C:\Users\Default User\AppData\Local\Application Data =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [0] SHD -- C:\Users\Default User\AppData\Local\History =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] D -- C:\Users\Default User\AppData\Local\Microsoft =>.Microsoft Corporation
043 - CFD: 07/05/2022 - [0] D -- C:\Users\Default User\AppData\Local\Temp =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [0] SHD -- C:\Users\Default User\AppData\Local\Temporary Internet Files =>.Microsoft Corporation
043 - CFD: 16/10/2022 - [] D -- C:\WINDOWS\System32\Config\systemprofile\AppData\Local\Microsoft =>.Microsoft Corporation

---\ ShellIconOverlayIdentifiers (SIOI) (11) - 0s

0106 - SIOI: DropboxExt1 Class [DropboxExt01] - {FB314ED9-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.55.0.dll =>.Dropbox, Inc®
0106 - SIOI: DropboxExt7 Class [DropboxExt02] - {FB314EDF-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.55.0.dll =>.Dropbox, Inc®
0106 - SIOI: DropboxExt9 Class [DropboxExt03] - {FB314EE1-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.55.0.dll =>.Dropbox, Inc®
0106 - SIOI: DropboxExt3 Class [DropboxExt04] - {FB314EDB-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.55.0.dll =>.Dropbox, Inc®
0106 - SIOI: DropboxExt2 Class [DropboxExt05] - {FB314EDA-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.55.0.dll =>.Dropbox, Inc®
0106 - SIOI: DropboxExt4 Class [DropboxExt06] - {FB314EDC-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.55.0.dll =>.Dropbox, Inc®
0106 - SIOI: DropboxExt5 Class [DropboxExt07] - {FB314EDD-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.55.0.dll =>.Dropbox, Inc®
0106 - SIOI: DropboxExt8 Class [DropboxExt08] - {FB314EE0-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.55.0.dll =>.Dropbox, Inc®
0106 - SIOI: DropboxExt10 Class [DropboxExt09] - {FB314EE2-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.55.0.dll =>.Dropbox, Inc®
0106 - SIOI: DropboxExt6 Class [DropboxExt10] - {FB314EDE-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.55.0.dll =>.Dropbox, Inc®
0106 - SIOI: [EnhancedStorageShell] - {D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}. (.Microsoft Corporation - Windows Enhanced Storage Shell Extension DL.) -- C:\Windows\System32\EhStorShell.dll [Unsigned] =>.Microsoft Corporation

---\ Search Context Menu Handlers (SCMH) (34) - 2s

0108 - CMH1: DropboxExt [64Bits] - {ECD97DE5-3C8F-4ACB-AEEE-CCAB78F7711C} .
(.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\
Client\DropboxExt64.55.0.dll =>.Dropbox, Inc®

0108 - CMH1: EPP [64Bits] - {09A47860-11B0-4DA5-AFA5-26D86198A780} . (.Microsoft
Corporation - Microsoft Security Client Shell Extension.) -- C:\Program Files\
Windows Defender\shellext.dll =>.Microsoft®

0108 - CMH1: Open With [64Bits] - {09799AFB-AD67-11d1-ABCD-00C04FC30936} .
(.Microsoft Corporation - Windows Shell Common Dll.) -- C:\Windows\System32\
shell32.dll =>.Microsoft®

0108 - CMH1: Open With EncryptionMenu [64Bits] - {A470F8CF-A1E8-4f65-8335-
227475AA5C46} . (.Microsoft Corporation - Windows Shell Common Dll.) -- C:\
Windows\System32\shell32.dll =>.Microsoft®

0108 - CMH1: Sharing [64Bits] - {f81e9010-6ea4-11ce-a7ff-00aa003ca9f6} .
(.Microsoft Corporation - Shell extensions for sharing.) -- C:\Windows\System32\
ntshrui.dll [Unsigned] =>.Microsoft Corporation

0108 - CMH1: WinRAR [64Bits] - {B41DB860-64E4-11D2-9906-E49FADC173CA} .
(.Alexander Roshal - WinRAR shell extension.) -- C:\Program Files\WinRAR\
RarExt.dll =>.win.rar GmbH®

0108 - CMH1: WinRAR32 [64Bits] - {B41DB860-8EE4-11D2-9906-E49FADC173CA} .
(.Orphan.) [Unsigned]

0108 - CMH1: WorkFolders [64Bits] - {E61BF828-5E63-4287-BEF1-60B1A4FDE0E3} .
(.Microsoft Corporation - Microsoft (C) Work Folders Shell Extension.) -- C:\
Windows\System32\WorkfoldersShell.dll [Unsigned] =>.Microsoft Corporation

0108 - CMH2: DropboxExt [64Bits] - {ECD97DE5-3C8F-4ACB-AEEE-CCAB78F7711C} .
(.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\
Client\DropboxExt64.55.0.dll =>.Dropbox, Inc®

0108 - CMH2: NvAppShExt [64Bits] - {A929C4CE-FD36-4270-B4F5-34ECAC5BD63C} .
(.NVIDIA Corporation - NVIDIA Shell Extensions.) -- C:\Windows\System32\
DriverStore\FileRepository\nvaci.inf_amd64_91df09c5579a85f3\nv3dappsnext.dll
=>.Nvidia Corporation®

0108 - CMH2: OpenContainingFolderMenu [64Bits] - {37ea3a21-7493-4208-a011-
7f9ea79ce9f5} . (.Microsoft Corporation - Windows Shell Common Dll.) -- C:\
Windows\System32\shell32.dll =>.Microsoft®

0108 - CMH2: OpenGLShExt [64Bits] - {E97DEC16-A50D-49bb-AE24-CF682282E08D} .
(.NVIDIA Corporation - NVIDIA Shell Extensions.) -- C:\Windows\System32\
DriverStore\FileRepository\nvaci.inf_amd64_91df09c5579a85f3\nv3dappsnext.dll
=>.Nvidia Corporation®

0108 - CMH2: WinRAR [64Bits] - {B41DB860-64E4-11D2-9906-E49FADC173CA} .
(.Alexander Roshal - WinRAR shell extension.) -- C:\Program Files\WinRAR\
RarExt.dll =>.win.rar GmbH®

0108 - CMH2: WinRAR32 [64Bits] - {B41DB860-8EE4-11D2-9906-E49FADC173CA} .
(.Orphan.) [Unsigned]

0108 - CMH3: CopyAsPathMenu [64Bits] - {f3d06e7c-1e45-4a26-847e-f9fcdee59be0} .
(.Microsoft Corporation - Windows Shell Common Dll.) -- C:\Windows\System32\
shell32.dll =>.Microsoft®

0108 - CMH3: ModernSharing [64Bits] - {e2bf9676-5f8f-435c-97eb-11607a5bedf7} .
(.Microsoft Corporation - Shell extensions for sharing.) -- C:\Windows\System32\
ntshrui.dll [Unsigned] =>.Microsoft Corporation

0108 - CMH3: SendTo [64Bits] - {7BA4C740-9E81-11CF-99D3-00AA004AE837} .
(.Microsoft Corporation - Windows Shell Common Dll.) -- C:\Windows\System32\
shell32.dll =>.Microsoft®

0108 - CMH4: DropboxExt [64Bits] - {ECD97DE5-3C8F-4ACB-AEEE-CCAB78F7711C} .
(.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\
Client\DropboxExt64.55.0.dll =>.Dropbox, Inc®

0108 - CMH4: EncryptionMenu [64Bits] - {A470F8CF-A1E8-4f65-8335-227475AA5C46} .
(.Microsoft Corporation - Windows Shell Common Dll.) -- C:\Windows\System32\
shell32.dll =>.Microsoft®

0108 - CMH4: EPP [64Bits] - {09A47860-11B0-4DA5-AFA5-26D86198A780} . (.Microsoft
Corporation - Microsoft Security Client Shell Extension.) -- C:\Program Files\
Windows Defender\shellext.dll =>.Microsoft®

0108 - CMH4: Sharing [64Bits] - {f81e9010-6ea4-11ce-a7ff-00aa003ca9f6} .
(.Microsoft Corporation - Shell extensions for sharing.) -- C:\Windows\System32\
ntshrui.dll [Unsigned] =>.Microsoft Corporation

0108 - CMH4: WorkFolders [64Bits] - {E61BF828-5E63-4287-BEF1-60B1A4FDE0E3} . (.Microsoft Corporation - Microsoft (C) Work Folders Shell Extension.) -- C:\Windows\System32\WorkfoldersShell.dll [Unsigned] =>.Microsoft Corporation

0108 - CMH5: DropboxExt [64Bits] - {ECD97DE5-3C8F-4ACB-AEEE-CCAB78F7711C} . (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.55.0.dll =>.Dropbox, Inc®

0108 - CMH5: New [64Bits] - {D969A300-E7FF-11d0-A93B-00A0C90F2719} . (.Microsoft Corporation - Windows Shell Common Dll.) -- C:\Windows\System32\shell32.dll =>.Microsoft®

0108 - CMH5: NvCplDesktopContext [64Bits] - {3D1975AF-48C6-4f8e-A182-BE0E08FA86A9} . (.NVIDIA Corporation - NVIDIA Display Shell Extension.) -- C:\Windows\System32\DriverStore\FileRepository\nvaci.inf_amd64_91df09c5579a85f3\nvshext.dll =>.Nvidia Corporation®

0108 - CMH5: Sharing [64Bits] - {f81e9010-6ea4-11ce-a7ff-00aa003ca9f6} . (.Microsoft Corporation - Shell extensions for sharing.) -- C:\Windows\System32\ntshrui.dll [Unsigned] =>.Microsoft Corporation

0108 - CMH5: WorkFolders [64Bits] - {E61BF828-5E63-4287-BEF1-60B1A4FDE0E3} . (.Microsoft Corporation - Microsoft (C) Work Folders Shell Extension.) -- C:\Windows\System32\WorkfoldersShell.dll [Unsigned] =>.Microsoft Corporation

0108 - CMH6: Library Location [64Bits] - {3dad6c5d-2167-4cae-9914-f99e41c12cfa} . (.Microsoft Corporation - Windows Shell Common Dll.) -- C:\Windows\System32\shell32.dll =>.Microsoft®

0108 - CMH6: PintoStartScreen [64Bits] - {470C0EBD-5D73-4d58-9CED-E91E22E23282} . (.Microsoft Corporation - App Resolver.) -- C:\Windows\System32\appresolver.dll =>.Microsoft®

0108 - CMH6: WinRAR [64Bits] - {B41DB860-64E4-11D2-9906-E49FADC173CA} . (.Alexander Roshal - WinRAR shell extension.) -- C:\Program Files\WinRAR\RarExt.dll =>.win.rar GmbH®

0108 - CMH6: WinRAR32 [64Bits] - {B41DB860-8EE4-11D2-9906-E49FADC173CA} . (.Orphan.) [Unsigned]

0108 - CMH7: EnhancedStorageShell [64Bits] - {2854F705-3548-414C-A113-93E27C808C85} . (.Microsoft Corporation - Windows Enhanced Storage Shell Extension DL.) -- C:\Windows\System32\EhStorShell.dll [Unsigned] =>.Microsoft Corporation

0108 - CMH7: EPP [64Bits] - {09A47860-11B0-4DA5-AFA5-26D86198A780} . (.Microsoft Corporation - Microsoft Security Client Shell Extension.) -- C:\Program Files\Windows Defender\shellext.dll =>.Microsoft®

0108 - CMH7: Sharing [64Bits] - {f81e9010-6ea4-11ce-a7ff-00aa003ca9f6} . (.Microsoft Corporation - Shell extensions for sharing.) -- C:\Windows\System32\ntshrui.dll [Unsigned] =>.Microsoft Corporation

---\ Image File Execution Options (12) - 0s

050 - IFE0:C:\WINDOWS\System32\ie4uinit.exe - (.Microsoft Corporation - IE Per-User Initialization Utility.) [MitigationOptions\256] [Unsigned] =>.Microsoft Corporation

050 - IFE0:C:\Windows\System32\ieUnatt.exe - (.Microsoft Corporation - IE 7.0 Unattended Install Utility.) [MitigationOptions\256] [Unsigned] =>.Microsoft Corporation

050 - IFE0:C:\WINDOWS\System32\LSASS.exe - (.Microsoft Corporation - Local Security Authority Process.) [AuditLevel\8] [Unsigned] =>.Microsoft Corporation

050 - IFE0:C:\WINDOWS\System32\MRT.exe - (.Microsoft Corporation - Microsoft Windows Malicious Software Remova.) [CFGOptions\1] [Unsigned] =>.Microsoft Corporation

050 - IFE0:C:\Windows\System32\msfeedssync.exe - (.Microsoft Corporation - Microsoft Feeds Synchronization.) [MitigationOptions\256] [Unsigned] =>.Microsoft Corporation

050 - IFE0:C:\Windows\System32\mshta.exe - (.Microsoft Corporation - Microsoft (R) HTML Application host.) [MitigationOptions\256] [Unsigned] =>.Microsoft Corporation

050 - IFE0:C:\Windows\System32\notepad.exe - (.Microsoft Corporation - Notepad.) [UseFilter\1] [Unsigned] =>.Microsoft Corporation

050 - IFE0:C:\Windows\System32\PresentationHost.exe - (.Microsoft Corporation - Windows Presentation Foundation Host.) [MitigationOptions\1118481] [Unsigned] =>.Microsoft Corporation
050 - IFE0:C:\WINDOWS\System32\PrintIsolationHost.exe - (.Microsoft Corporation - PrintIsolationHost.) [MitigationOptions\2097152] [Unsigned] =>.Microsoft Corporation
050 - IFE0:C:\WINDOWS\System32\runtimebroker.exe - (.Microsoft Corporation - Runtime Broker.) [MitigationOptions\4294967296] [Unsigned] =>.Microsoft Corporation
050 - IFE0:C:\WINDOWS\System32\spoolsv.exe - (.Microsoft Corporation - Spooler SubSystem App.) [MitigationOptions\2097152] [Unsigned] =>.Microsoft Corporation
050 - IFE0:C:\Windows\System32\svchost.exe - (.Microsoft Corporation - Host Process for Windows Services.) [MinimumStackCommitInBytes\32768] =>.Microsoft®

---\ System Drivers List (452) - 15s

058 - SDL:2022/10/16 11:26:00 A . (.Microsoft Corporation - 1394 OpenHCI Driver.) -- C:\WINDOWS\System32\drivers\1394ohci.sys [299008] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:03 A . (.LSI - LSI 3ware SCSI Storport Driver.) -- C:\WINDOWS\System32\drivers\3ware.sys [108376] =>.Microsoft®
058 - SDL:2021/08/09 04:28:16 A . (.Acer Incorporated - AcerAirplaneModeController.) -- C:\WINDOWS\System32\drivers\AcerAirplaneModeController.sys [31896] =>.Acer Incorporated®
058 - SDL:2022/10/16 11:26:00 A . (.Microsoft Corporation - ACPI Driver for NT.) -- C:\WINDOWS\System32\drivers\acpi.sys [755040] =>.Microsoft®
058 - SDL:2022/10/16 11:26:00 A . (.Microsoft Corporation - ACPI Devices Driver.) -- C:\WINDOWS\System32\drivers\AcpiDev.sys [57344] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - ACPIEx Driver.) -- C:\WINDOWS\System32\drivers\acpiex.sys [169304] =>.Microsoft®
058 - SDL:2022/05/07 07:19:04 A . (.Microsoft Corporation - ACPI Processor Aggregator Device Driver.) -- C:\WINDOWS\System32\drivers\acpipagr.sys [49152] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:02 A . (.Microsoft Corporation - ACPI Power Metering Driver.) -- C:\WINDOWS\System32\drivers\acpipmi.sys [53248] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:04 A . (.Microsoft Corporation - ACPI Wake Alarm.) -- C:\WINDOWS\System32\drivers\acpitime.sys [57344] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:25:59 A . (.Microsoft Corporation - Audio KMDf Class Extension.) -- C:\WINDOWS\System32\drivers\Acx01000.sys [733184] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:03 A . (.PMC-Sierra - PMC-Sierra Storport Driver For SPC8x6G SAS.) -- C:\WINDOWS\System32\drivers\adp80xx.sys [1136472] =>.Microsoft®
058 - SDL:2022/10/16 11:26:30 A . (.Microsoft Corporation - Ancillary Function Driver for WinSock.) -- C:\WINDOWS\System32\drivers\afd.sys [697696] =>.Microsoft®
058 - SDL:2022/05/07 07:19:42 A . (.Microsoft Corporation - AF_UNIX socket provider.) -- C:\WINDOWS\System32\drivers\afunix.sys [81920] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:43 A . (.Microsoft Corporation - RAS Agile Vpn Miniport Call Manager.) -- C:\WINDOWS\System32\drivers\agilevpn.sys [143360] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:39 A . (.Microsoft Corporation - Application Compatibility Cache.) -- C:\WINDOWS\System32\drivers\ahcache.sys [372736] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:00 A . (.Advanced Micro Devices, Inc - AMD GPIO Controller Driver.) -- C:\WINDOWS\System32\drivers\amdgpio2.sys [18432] [Unsigned] =>.Advanced Micro Devices, Inc
058 - SDL:2022/05/07 07:19:00 A . (.Advanced Micro Devices, Inc - AMD I2C Controller Driver.) -- C:\WINDOWS\System32\drivers\amdi2c.sys [45568] [Unsigned] =>.Advanced Micro Devices, Inc

058 - SDL:2022/10/16 11:26:00 A . (.Microsoft Corporation - Processor Device Driver.) -- C:\WINDOWS\System32\drivers\amd8.sys [251232] =>.Microsoft®
058 - SDL:2022/10/16 11:26:00 A . (.Microsoft Corporation - Processor Device Driver.) -- C:\WINDOWS\System32\drivers\amdppm.sys [259408] =>.Microsoft®
058 - SDL:2022/05/07 07:19:03 A . (.Advanced Micro Devices - AHCI 1.3 Device Driver.) -- C:\WINDOWS\System32\drivers\amdsata.sys [84312] =>.Microsoft®
058 - SDL:2022/05/07 07:19:03 A . (.AMD Technologies Inc. - AMD Technology AHCI Compatible Controller D.) -- C:\WINDOWS\System32\drivers\amdsbs.sys [260440] =>.Microsoft®
058 - SDL:2022/05/07 07:19:03 A . (.Advanced Micro Devices - Storage Filter Driver.) -- C:\WINDOWS\System32\drivers\amdxta.sys [28008] =>.Microsoft®
058 - SDL:2022/10/16 11:26:33 A . (.Microsoft Corporation - AppID Driver.) -- C:\WINDOWS\System32\drivers\appid.sys [247144] =>.Microsoft®
058 - SDL:2022/05/07 07:19:00 A . (.Apple Inc. - Apple Solid State Drive Device.) -- C:\WINDOWS\System32\drivers\AppleSSD.sys [113496] =>.Microsoft®
058 - SDL:2022/10/16 11:26:33 A . (.Microsoft Corporation - Applocker Filter.) -- C:\WINDOWS\System32\drivers\applockerfltr.sys [49152] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:03 A . (.PMC-Sierra, Inc. - Adaptec SAS RAID WS03 Driver.) -- C:\WINDOWS\System32\drivers\arcsas.sys [132968] =>.Microsoft®
058 - SDL:2022/05/07 07:19:43 A . (.Microsoft Corporation - MS Remote Access serial network driver.) -- C:\WINDOWS\System32\drivers\asynctac.sys [61440] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - ATAPI IDE Miniport Driver.) -- C:\WINDOWS\System32\drivers\atapi.sys [62808] =>.Microsoft®
058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - ATAPI Driver Extension.) -- C:\WINDOWS\System32\drivers\ataport.sys [259424] =>.Microsoft®
058 - SDL:2022/05/07 07:19:29 A . (.Microsoft Corporation - BAM Kernel Driver.) -- C:\WINDOWS\System32\drivers\bam.sys [116056] =>.Microsoft®
058 - SDL:2022/05/07 07:19:04 A . (.Microsoft Corporation - Battery Class Driver.) -- C:\WINDOWS\System32\drivers\battc.sys [107880] =>.Microsoft®
058 - SDL:2022/05/07 07:19:00 A . (. - BCM Function 2 Device Driver.) -- C:\WINDOWS\System32\drivers\bcmfn2.sys [9728] [Unsigned] =>.Broadcom Corporation
058 - SDL:2022/05/07 07:19:45 A . (.Microsoft Corporation - BEEP Driver.) -- C:\WINDOWS\System32\drivers\beep.sys [40960] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - Bfs Filter Driver.) -- C:\WINDOWS\System32\drivers\bfs.sys [91480] =>.Microsoft®
058 - SDL:2022/10/16 11:26:20 A . (.Microsoft Corporation - Windows Bind Filter Driver.) -- C:\WINDOWS\System32\drivers\bindflt.sys [173408] =>.Microsoft®
058 - SDL:2020/07/15 19:21:58 A . (. - Boom 3D Virtual Audio Driver.) -- C:\WINDOWS\System32\drivers\boomvad.sys [51016] {254E21C741DC779A4EC68054D3FFA4BF}.
058 - SDL:2022/05/07 07:19:10 A . (.Microsoft Corporation - NT Lan Manager Datagram Receiver Driver.) -- C:\WINDOWS\System32\drivers\bowser.sys [155648] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:27:07 A . (.Microsoft Corporation - MAC Bridge Driver.) -- C:\WINDOWS\System32\drivers\bridge.sys [159744] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:00 A . (.Microsoft Corporation - Microsoft Bluetooth Audio Multiprofile Mana.) -- C:\WINDOWS\System32\drivers\BtaMPM.sys [73728] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:25:57 A . (.Microsoft Corporation - Bluetooth A2DP Driver.) -- C:\WINDOWS\System32\drivers\BthA2dp.sys [532480] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - Bluetooth Bus Extender.) -- C:\WINDOWS\System32\drivers\bthenum.sys [143360] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:25:57 A . (.Microsoft Corporation - Bluetooth Hands-free Audio Device Driver.) -- C:\WINDOWS\System32\drivers\BthHfAud.sys [110592] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:25:57 A . (.Microsoft Corporation - Bluetooth Hands-Free Audio and Call Control.) -- C:\WINDOWS\System32\drivers\BthHfEnum.sys [184320] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - Bluetooth Transport Extensibility Miniport.) -- C:\WINDOWS\System32\drivers\BthMini.SYS [86016] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:01 A . (.Microsoft Corporation - Bluetooth Communications Driver.) -- C:\WINDOWS\System32\drivers\bthmodem.sys [106496] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:25 A . (.Microsoft Corporation - Bluetooth Personal Area Networking.) -- C:\WINDOWS\System32\drivers\bthpan.sys [159744] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - Bluetooth Bus Driver.) -- C:\WINDOWS\System32\drivers\bthport.sys [2031616] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - Bluetooth Miniport Driver.) -- C:\WINDOWS\System32\drivers\BTHUSB.SYS [139264] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:05 A . (.Microsoft Corporation - VHD BTT Filter Driver.) -- C:\WINDOWS\System32\drivers\bttflt.sys [79184] =>.Microsoft®

058 - SDL:2022/05/07 07:19:25 A . (.Microsoft Corporation - Button Converter Driver.) -- C:\WINDOWS\System32\drivers\buttonconverter.sys [90112] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:02 A . (.QLogic Corporation - QLogic Gigabit Ethernet VBD.) -- C:\WINDOWS\System32\drivers\bxxvnda.sys [534872] =>.Microsoft®

058 - SDL:2022/05/07 07:19:01 A . (.Microsoft Corporation - Charge Arbitration Driver.) -- C:\WINDOWS\System32\drivers\CAD.sys [99672] =>.Microsoft®

058 - SDL:2022/10/16 11:27:06 A . (.Microsoft Corporation - CD-ROM File System Driver.) -- C:\WINDOWS\System32\drivers\cdfs.sys [131072] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:03 A . (.Microsoft Corporation - SCSI CD-ROM Driver.) -- C:\WINDOWS\System32\drivers\cdrom.sys [204800] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:20 A . (.Microsoft Corporation - Event Aggregation Kernel Mode Library.) -- C:\WINDOWS\System32\drivers\CEA.sys [107880] =>.Microsoft®

058 - SDL:2022/05/07 07:19:04 A . (.Chelsio Communications - Chelsio iSCSI Crash Dump Driver.) -- C:\WINDOWS\System32\drivers\cht4dx64.sys [145256] =>.Microsoft®

058 - SDL:2022/05/07 07:19:04 A . (.Chelsio Communications - Chelsio iSCSI VMiniport Driver.) -- C:\WINDOWS\System32\drivers\cht4sx64.sys [320880] =>.Microsoft®

058 - SDL:2022/05/07 07:19:04 A . (.Chelsio Communications - VF library for Chelsio ® T5/T6 Chipset.) -- C:\WINDOWS\System32\drivers\cht4vfx.sys [28672] [Unsigned] =>.Chelsio Communications

058 - SDL:2022/05/07 07:19:04 A . (.Chelsio Communications - Virtual Bus Driver for Chelsio ® T5/T6 Chip.) -- C:\WINDOWS\System32\drivers\cht4vx64.sys [1854832] =>.Microsoft®

058 - SDL:2022/05/07 07:19:23 A . (.Microsoft Corporation - CimFS driver.) -- C:\WINDOWS\System32\drivers\cimfs.sys [173424] =>.Microsoft®

058 - SDL:2022/05/07 07:19:01 A . (.Microsoft Corporation - Consumer IR Class Driver for eHome.) -- C:\WINDOWS\System32\drivers\circlass.sys [90112] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:30 A . (.Microsoft Corporation - SCSI Class System Dll.) -- C:\WINDOWS\System32\drivers\Classnp.sys [488792] =>.Microsoft®

058 - SDL:2022/10/16 11:26:35 A . (.Microsoft Corporation - Cloud Files Mini Filter Driver.) -- C:\WINDOWS\System32\drivers\cldfilt.sys [569344] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:37 A . (.Microsoft Corporation - Common Log File System Driver.) -- C:\WINDOWS\System32\drivers\clfs.sys [451936] =>.Microsoft®

058 - SDL:2022/05/07 07:19:16 A . (.Microsoft Corporation - CLIP Service.) -- C:\WINDOWS\System32\drivers\ClipSp.sys [1135952] =>.Microsoft®

058 - SDL:2022/05/07 07:19:04 A . (.Microsoft Corporation - Control Method Battery Driver.) -- C:\WINDOWS\System32\drivers\CmBatt.sys [73728] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:05 A . (.Microsoft Corporation - Kernel Configuration Manager Initial Config.) -- C:\WINDOWS\System32\drivers\cmimcext.sys [71008] =>.Microsoft®

058 - SDL:2022/10/16 11:26:28 A . (.Microsoft Corporation - Kernel Cryptography, Next Generation.) -- C:\WINDOWS\System32\drivers\cng.sys [782352] =>.Microsoft®

058 - SDL:2022/05/07 07:19:23 A . (.Microsoft Corporation - CNG Hardware Assist algorithm provider.) -- C:\WINDOWS\System32\drivers\cnghwassist.sys [75088] =>.Microsoft®

058 - SDL:2022/05/07 07:19:23 A . (.Microsoft Corporation - Console Driver.) -- C:\WINDOWS\System32\drivers\condrv.sys [87376] =>.Microsoft®

058 - SDL:2022/10/16 11:26:36 A . (.Microsoft Corporation - Crash Dump Driver.) -- C:\WINDOWS\System32\drivers\crashdump.sys [161112] =>.Microsoft®

058 - SDL:2022/10/16 11:26:27 A . (.Microsoft Corporation - DAM Kernel Driver.) -- C:\WINDOWS\System32\drivers\dam.sys [140656] =>.Microsoft®

058 - SDL:2022/10/10 21:45:58 A . (.Dropbox, Inc. - Dropbox Filter Driver.) -- C:\WINDOWS\System32\drivers\dbx-canary.sys [47600] =>.Microsoft®

058 - SDL:2022/10/10 21:45:58 A . (.Dropbox, Inc. - Dropbox Filter Driver.) -- C:\WINDOWS\System32\drivers\dbx-dev.sys [47600] =>.Microsoft®

058 - SDL:2022/10/10 21:45:58 A . (.Dropbox, Inc. - Dropbox Filter Driver.) -- C:\WINDOWS\System32\drivers\dbx-stable.sys [47600] =>.Microsoft®

058 - SDL:2022/10/16 11:25:57 A . (.Microsoft Corporation - Xbox Device Authentication Driver.) -- C:\WINDOWS\System32\drivers\devauthe.sys [86016] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:37 A . (.Microsoft Corporation - DFS Namespace Client Driver.) -- C:\WINDOWS\System32\drivers\dfsc.sys [184320] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:00 A . (.Microsoft Corporation - PnP Disk Driver.) -- C:\WINDOWS\System32\drivers\disk.sys [140616] =>.Microsoft®

058 - SDL:2022/05/07 07:19:35 A . (.Microsoft Corporation - Crash Dump Disk Driver.) -- C:\WINDOWS\System32\drivers\Diskdump.sys [79200] =>.Microsoft®

058 - SDL:2022/05/07 07:19:35 A . (.Microsoft Corporation - Boot Over USB Dump Driver.) -- C:\WINDOWS\System32\drivers\Dmpusbstor.sys [57344] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:20:16 A . (.Microsoft Corporation - Dynamic Memory.) -- C:\WINDOWS\System32\drivers\dmvsc.sys [99664] =>.Microsoft®

058 - SDL:2022/05/07 07:19:01 A . (.Microsoft Corporation - Microsoft Trusted Audio Drivers.) -- C:\WINDOWS\System32\drivers\drmk.sys [143360] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:01 A . (.Microsoft Corporation - Microsoft Trusted Audio Drivers.) -- C:\WINDOWS\System32\drivers\drmkaud.sys [50984] =>.Microsoft®

058 - SDL:2022/05/07 07:19:33 A . (.Microsoft Corporation - ATAPI Dump Driver.) -- C:\WINDOWS\System32\drivers\Dumpata.sys [79216] =>.Microsoft®

058 - SDL:2022/10/16 11:27:24 A . (.Microsoft Corporation - Bitlocker Drive Encryption Crashdump Filter.) -- C:\WINDOWS\System32\drivers\dumpfve.sys [133624] =>.Microsoft®

058 - SDL:2022/05/07 07:19:25 A . (.Microsoft Corporation - SD Crashdump Port Driver.) -- C:\WINDOWS\System32\drivers\dumpsd.sys [230744] =>.Microsoft®

058 - SDL:2022/05/07 07:19:23 A . (.Microsoft Corporation - SD Host Controller Crashdump Port Driver.) -- C:\WINDOWS\System32\drivers\dumpsdport.sys [73728] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:35 A . (.Microsoft Corporation - Storport Dump Driver.) -- C:\WINDOWS\System32\drivers\Dumpstorport.sys [79184] =>.Microsoft®

058 - SDL:2022/10/22 07:47:55 A . (.Microsoft Corporation - DirectX Graphics Kernel.) -- C:\WINDOWS\System32\drivers\dxgkrnl.sys [4687200] =>.Microsoft®

058 - SDL:2022/10/16 11:26:11 A . (.Microsoft Corporation - DirectX Graphics MMS.) -- C:\WINDOWS\System32\drivers\dxgmms1.sys [566632] =>.Microsoft®

058 - SDL:2022/10/16 11:26:11 A . (.Microsoft Corporation - DirectX Graphics MMS.) -- C:\WINDOWS\System32\drivers\dxgmms2.sys [1148256] =>.Microsoft®

058 - SDL:2022/05/07 07:20:05 A . (.Microsoft Corporation - Enhanced Storage Class driver for IEEE 1667.) -- C:\WINDOWS\System32\drivers\EhStorClass.sys [152944] =>.Microsoft®

058 - SDL:2022/10/16 11:25:58 A . (.Microsoft Corporation - Microsoft driver for storage devices suppor.) -- C:\WINDOWS\System32\drivers\EhStorTcgDrv.sys [165216] =>.Microsoft®

058 - SDL:2011/01/06 11:37:26 A . (.SEIKO EPSON CORPORATION - EPSON Projector Virtual Audio Device.) -- C:\WINDOWS\System32\drivers\EMP_UDAU.sys [23040] [Unsigned] =>.Seiko Epson Corporation

058 - SDL:2022/05/07 07:19:04 A . (.Microsoft Corporation - Error Device Driver.) -- C:\WINDOWS\System32\drivers\errdev.sys [53248] [Unsigned] =>.Microsoft Corporation

058 - SDL:2019/06/20 19:59:06 A . (.ELAN Microelectronic Corp. - ELAN I2C Driver.) -- C:\WINDOWS\System32\drivers\ETDI2C.sys [218048] =>.ELAN MICROELECTRONICS CORPORATION®

058 - SDL:2022/05/07 07:19:02 A . (.QLogic Corporation - QLogic 10 GigE VBD.) -- C:\WINDOWS\System32\drivers\evbd0a.sys [3424104] =>.Microsoft®

058 - SDL:2022/05/07 07:19:02 A . (.Marvell Semiconductor Inc. - QLogic 10 GigE VBD.) -- C:\WINDOWS\System32\drivers\evbda.sys [3441512] =>.Microsoft®

058 - SDL:2022/10/16 11:26:32 A . (.Microsoft Corporation - CPU Scheduler for High Performance I/O.) -- C:\WINDOWS\System32\drivers\ExecutionContext.sys [75088] =>.Microsoft®

058 - SDL:2022/10/16 11:25:56 A . (.Microsoft Corporation - Microsoft Extended FAT File System.) -- C:\WINDOWS\System32\drivers\exfat.sys [451920] =>.Microsoft®

058 - SDL:2022/10/16 11:25:56 A . (.Microsoft Corporation - Fast FAT File System Driver.) -- C:\WINDOWS\System32\drivers\fastfat.sys [456008] =>.Microsoft®

058 - SDL:2022/05/07 07:19:04 A . (.Microsoft Corporation - Floppy Disk Controller Driver.) -- C:\WINDOWS\System32\drivers\fdc.sys [69632] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:02 A . (.Microsoft Corporation - Windows sandboxing and encryption filter.) -- C:\WINDOWS\System32\drivers\filecrypt.sys [90112] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:33 A . (.Microsoft Corporation - FileInfo Filter Driver.) -- C:\WINDOWS\System32\drivers\fileinfo.sys [124240] =>.Microsoft®

058 - SDL:2022/05/07 07:19:33 A . (.Microsoft Corporation - File Trace Filter Driver.) -- C:\WINDOWS\System32\drivers\filetrace.sys [73728] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:04 A . (.Microsoft Corporation - Floppy Driver.) -- C:\WINDOWS\System32\drivers\flpydisk.sys [65536] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:28 A . (.Microsoft Corporation - Microsoft Filesystem Filter Manager.) -- C:\WINDOWS\System32\drivers\fltMgr.sys [488800] =>.Microsoft®

058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - File System Dependency Manager Mini Filter.) -- C:\WINDOWS\System32\drivers\fsdepends.sys [103760] =>.Microsoft®

058 - SDL:2022/05/07 07:19:30 A . (.Microsoft Corporation - File System Recognizer Driver.) -- C:\WINDOWS\System32\drivers\fs_rec.sys [71008] =>.Microsoft®

058 - SDL:2022/10/16 11:27:24 A . (.Microsoft Corporation - BitLocker Drive Encryption Driver.) -- C:\WINDOWS\System32\drivers\fvevol.sys [877920] =>.Microsoft®

058 - SDL:2022/10/16 11:26:32 A . (.Microsoft Corporation - FWP/IPsec Kernel-Mode API.) -- C:\WINDOWS\System32\drivers\FWPKCLNT.SYS [546136] =>.Microsoft®

058 - SDL:2022/10/16 11:25:58 A . (.Microsoft Corporation - High Definition Audio Bus Driver.) -- C:\WINDOWS\System32\drivers\hdaudbus.sys [192512] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:25:58 A . (.Microsoft Corporation - High Definition Audio Function Driver.) -- C:\WINDOWS\System32\drivers\HdAudio.sys [528384] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:04 A . (.Microsoft Corporation - Hid Battery Driver.) -- C:\WINDOWS\System32\drivers\hidbatt.sys [71016] =>.Microsoft®

058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - Bluetooth Miniport Driver for HID Devices.) -- C:\WINDOWS\System32\drivers\hidbth.sys [151552] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:25 A . (.Microsoft Corporation - Hid Class Library.)
-- C:\WINDOWS\System32\drivers\hidclass.sys [278528] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - I2C HID Miniport Driver.) -- C:\WINDOWS\System32\drivers\hidi2c.sys [102400] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:25 A . (.Microsoft Corporation - HID Button over Interrupt Driver.) -- C:\WINDOWS\System32\drivers\hidinterrupt.sys [91472] =>.Microsoft@

058 - SDL:2022/05/07 07:19:01 A . (.Microsoft Corporation - Infrared Miniport Driver for Input Devices.) -- C:\WINDOWS\System32\drivers\hidir.sys [81920] [Unsigned] =>.Microsoft Corporation

058 - SDL:2019/07/14 07:06:50 A . (. - Filter Driver for HID-KMDF Interface.) -- C:\WINDOWS\System32\drivers\hidkmdf.sys [26808] {08DF1FFB8B0EEF71ED9573AAE3ECFCDC}.

058 - SDL:2022/05/07 07:19:25 A . (.Microsoft Corporation - Hid Parsing Library.) -- C:\WINDOWS\System32\drivers\hidparse.sys [90112] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - SPI HID Miniport Driver.) -- C:\WINDOWS\System32\drivers\hidspi.sys [139264] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:20 A . (.Microsoft Corporation - HidSpi KMDF Class Extension.) -- C:\WINDOWS\System32\drivers\HidSpiCx.sys [126976] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:25 A . (.Microsoft Corporation - USB Miniport Driver for Input Devices.) -- C:\WINDOWS\System32\drivers\hidusb.sys [77824] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:03 A . (.Hewlett-Packard Company - Smart Array SAS/SATA Controller Media Drive.) -- C:\WINDOWS\System32\drivers\HpSAMD.sys [65360] =>.Microsoft@

058 - SDL:2022/05/07 07:19:08 A . (.Microsoft Corporation - HSP Device Driver.) -- C:\WINDOWS\System32\drivers\Hsp.sys [124264] =>.Microsoft@

058 - SDL:2020/09/29 18:20:12 A . (.Pango - HotspotShield TAP-Windows Virtual Network D.) -- C:\WINDOWS\System32\drivers\hsstap.sys [39424] =>.Microsoft@

058 - SDL:2022/10/16 11:26:27 A . (.Microsoft Corporation - HTTP Protocol Stack.) -- C:\WINDOWS\System32\drivers\http.sys [1774944] =>.Microsoft@

058 - SDL:2022/05/07 07:20:16 A . (.Microsoft Corporation - Hyper-V Crashdump.) -- C:\WINDOWS\System32\drivers\hvcrash.sys [75112] =>.Microsoft@

058 - SDL:2022/10/16 11:27:04 A . (.Microsoft Corporation - Hypervisor Boot Driver.) -- C:\WINDOWS\System32\drivers\hvservice.sys [91472] =>.Microsoft@

058 - SDL:2022/10/16 11:27:16 A . (.Microsoft Corporation - Microsoft Hyper-V Socket Provider.) -- C:\WINDOWS\System32\drivers\hvsocket.sys [181584] =>.Microsoft@

058 - SDL:2022/05/07 07:19:30 A . (.Microsoft Corporation - Hardware Policy Driver.) -- C:\WINDOWS\System32\drivers\hwpolicy.sys [79200] =>.Microsoft@

058 - SDL:2022/05/07 07:20:16 A . (.Microsoft Corporation - Microsoft VMBus Synthetic Keyboard Driver.) -- C:\WINDOWS\System32\drivers\hyperkbd.sys [62800] =>.Microsoft@

058 - SDL:2022/05/07 07:20:16 A . (.Microsoft Corporation - Microsoft VMBus Video Device Miniport Drive.) -- C:\WINDOWS\System32\drivers\HyperVideo.sys [79200] =>.Microsoft@

058 - SDL:2022/05/07 07:19:25 A . (.Microsoft Corporation - i8042 Port Driver.) -- C:\WINDOWS\System32\drivers\i8042prt.sys [159744] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:00 A . (.Intel(R) Corporation - Intel(R) Serial IO GPIO Controller Driver.) -- C:\WINDOWS\System32\drivers\iagpio.sys [36352] [Unsigned] =>.Intel(R) Corporation

058 - SDL:2022/05/07 07:19:00 A . (.Intel(R) Corporation - Intel(R) Serial IO I2C Driver.) -- C:\WINDOWS\System32\drivers\iai2c.sys [91136] [Unsigned] =>.Intel(R) Corporation

058 - SDL:2022/05/07 07:19:00 A . (.Intel Corporation - Intel(R) Serial IO GPIO Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i_GPIO2.sys [79360] [Unsigned] =>.Intel Corporation

058 - SDL:2022/05/07 07:19:00 A . (.Intel Corporation - Intel(R) Serial IO GPIO Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i_GPIO2_BXT_P.sys [93184] [Unsigned] =>.Intel Corporation
058 - SDL:2022/05/07 07:19:00 A . (.Intel Corporation - Intel(R) Serial IO GPIO Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i_GPIO2_CNL.sys [112128] [Unsigned] =>.Intel Corporation
058 - SDL:2022/05/07 07:19:00 A . (.Intel Corporation - Intel(R) Serial IO GPIO Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i_GPIO2_GLK.sys [96256] [Unsigned] =>.Intel Corporation
058 - SDL:2022/05/07 07:19:00 A . (.Intel Corporation - Intel(R) Serial IO I2C Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i_I2C.sys [171520] [Unsigned] =>.Intel Corporation
058 - SDL:2022/05/07 07:19:00 A . (.Intel Corporation - Intel(R) Serial IO I2C Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i_I2C_BXT_P.sys [175104] [Unsigned] =>.Intel Corporation
058 - SDL:2022/05/07 07:19:00 A . (.Intel Corporation - Intel(R) Serial IO I2C Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i_I2C_CNL.sys [177152] [Unsigned] =>.Intel Corporation
058 - SDL:2022/05/07 07:19:00 A . (.Intel Corporation - Intel(R) Serial IO I2C Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2i_I2C_GLK.sys [177664] [Unsigned] =>.Intel Corporation
058 - SDL:2018/11/29 18:39:48 A . (.Intel Corporation - Intel(R) Serial IO GPIO Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2_GPIO2.sys [131744] =>.Intel(R) Embedded Subsystems and IP Blocks Group®
058 - SDL:2018/11/29 18:39:48 A . (.Intel Corporation - Intel(R) Serial IO I2C Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2_I2C.sys [200352] =>.Intel(R) Embedded Subsystems and IP Blocks Group®
058 - SDL:2018/11/29 18:39:48 A . (.Intel Corporation - Intel(R) Serial IO SPI Driver v2.) -- C:\WINDOWS\System32\drivers\iaLPSS2_SPI.sys [161440] =>.Intel(R) Embedded Subsystems and IP Blocks Group®
058 - SDL:2018/11/29 18:39:48 A . (.Intel Corporation - Intel(R) Serial IO UART Driver.) -- C:\WINDOWS\System32\drivers\iaLPSS2_UART2.sys [320160] =>.Intel(R) Embedded Subsystems and IP Blocks Group®
058 - SDL:2022/05/07 07:19:02 A . (.Intel Corporation - Intel(R) Serial IO GPIO Controller Driver.) -- C:\WINDOWS\System32\drivers\iaLPSSi_GPIO.sys [38128] =>.Intel Corporation - Client Components Group®
058 - SDL:2022/05/07 07:19:01 A . (.Intel Corporation - Intel(R) Serial IO I2C Controller Driver.) -- C:\WINDOWS\System32\drivers\iaLPSSi_I2C.sys [113152] [Unsigned] =>.Intel Corporation
058 - SDL:2021/10/12 15:12:44 N . (.Intel Corporation - Intel(R) Rapid Storage Technology driver -.) -- C:\WINDOWS\System32\drivers\iaStorAC.sys [1347776] {34770BB53021480D308F5E5593B49D84}. =>.Intel Corporation
058 - SDL:2021/10/12 15:12:44 A . (.Intel Corporation - Intel(R) Optane(TM) Memory Minifilter Drive.) -- C:\WINDOWS\System32\drivers\iaStorAfs.sys [73920] {34770BB53021480D308F5E5593B49D84}. =>.Intel Corporation
058 - SDL:2022/05/07 07:19:04 A . (.Intel Corporation - Intel(R) Rapid Storage Technology driver (i.)) -- C:\WINDOWS\System32\drivers\iaStorAVC.sys [885584] =>.Microsoft®
058 - SDL:2022/05/07 07:19:04 A . (.Intel Corporation - Intel Matrix Storage Manager driver - x64.) -- C:\WINDOWS\System32\drivers\iaStorV.sys [413008] =>.Microsoft®
058 - SDL:2022/05/07 07:19:04 A . (.Mellanox - InfiniBand Fabric Bus Driver.) -- C:\WINDOWS\System32\drivers\ibbus.sys [559976] =>.Microsoft®
058 - SDL:2021/09/06 22:59:08 A . (.Intel Corporation - Intel(R) Wireless Bluetooth(R) Filter Drive.) -- C:\WINDOWS\System32\drivers\ibtusb.sys [7426616] {28D8BD3C11854B538A3996B7E4F8EE23}. =>.Intel Corporation
058 - SDL:2022/10/16 11:26:20 A . (.Microsoft Corporation - Indirect displays kernel-mode filter driver.) -- C:\WINDOWS\System32\drivers\IndirectKmd.sys [77824] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - Intel PCI IDE Driver.) -- C:\WINDOWS\System32\drivers\intelide.sys [58704] =>.Microsoft®
058 - SDL:2022/05/07 07:19:03 A . (.Microsoft Corporation - Intel Power Engine Plugin.) -- C:\WINDOWS\System32\drivers\intelpep.sys [488960] =>.Microsoft®

058 - SDL:2022/05/07 07:19:00 A . (.Microsoft Corporation - Intel Power Limit Driver.) -- C:\WINDOWS\System32\drivers\intelppm.sys [65536] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:03 A . (.Microsoft Corporation - Intel Platform Monitoring Driver.) -- C:\WINDOWS\System32\drivers\IntelPMT.sys [87552] =>.Microsoft®
058 - SDL:2022/10/16 11:26:00 A . (.Microsoft Corporation - Processor Device Driver.) -- C:\WINDOWS\System32\drivers\intelppm.sys [288080] =>.Microsoft®
058 - SDL:2022/05/07 07:18:58 A . (.Microsoft Corporation - I/O rate control Filter.) -- C:\WINDOWS\System32\drivers\iorate.sys [87392] =>.Microsoft®
058 - SDL:2022/05/07 07:19:43 A . (.Microsoft Corporation - IP FILTER DRIVER.) -- C:\WINDOWS\System32\drivers\ipfltdrv.sys [118784] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - WMI IPMI DRIVER.) -- C:\WINDOWS\System32\drivers\IPMIDrv.sys [148816] =>.Microsoft®
058 - SDL:2022/10/16 11:26:20 A . (.Microsoft Corporation - IP Network Address Translator.) -- C:\WINDOWS\System32\drivers\ipnat.sys [258048] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:00 A . (.Microsoft Corporation - IPT Driver.) -- C:\WINDOWS\System32\drivers\ipt.sys [99688] =>.Microsoft®
058 - SDL:2022/05/07 07:19:04 A . (.Microsoft Corporation - PNP ISA Bus Driver.) -- C:\WINDOWS\System32\drivers\isapnp.sys [54624] =>.Microsoft®
058 - SDL:2022/05/07 07:19:03 A . (.Avago Technologies - Avago SAS Gen3.5 Driver (StorPort).) -- C:\WINDOWS\System32\drivers\ItSas35i.sys [187224] =>.Microsoft®
058 - SDL:2022/05/07 07:19:25 A . (.Microsoft Corporation - Keyboard Class Driver.) -- C:\WINDOWS\System32\drivers\kbdclass.sys [95576] =>.Microsoft®
058 - SDL:2022/05/07 07:19:25 A . (.Microsoft Corporation - HID Keyboard Filter Driver.) -- C:\WINDOWS\System32\drivers\kbdhid.sys [73728] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:31 A . (.Microsoft Corporation - Microsoft Kernel Debugger Network Miniport.) -- C:\WINDOWS\System32\drivers\kdnic.sys [70992] =>.Microsoft®
058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - Kernel Mode Power Dependency Coordinator.) -- C:\WINDOWS\System32\drivers\kmpdc.sys [71008] =>.Microsoft®
058 - SDL:2022/10/16 11:25:55 A . (.Microsoft Corporation - Network Power Dependency Broker.) -- C:\WINDOWS\System32\drivers\KNetPwrDepBroker.sys [73728] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:38 A . (.Microsoft Corporation - Kernel CSA Library.) -- C:\WINDOWS\System32\drivers\ks.sys [544768] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:29 A . (.Microsoft Corporation - Kernel Security Support Provider Interface.) -- C:\WINDOWS\System32\drivers\ksecdd.sys [189776] =>.Microsoft®
058 - SDL:2022/10/16 11:26:31 A . (.Microsoft Corporation - Kernel Security Support Provider Interface.) -- C:\WINDOWS\System32\drivers\ksecpkg.sys [218464] =>.Microsoft®
058 - SDL:2022/05/07 07:19:38 A . (.Microsoft Corporation - Kernel Streaming WOW Thunk Service.) -- C:\WINDOWS\System32\drivers\ksthunk.sys [65536] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:38 A . (.Microsoft Corporation - Link-Layer Topology Mapper I/O Driver.) -- C:\WINDOWS\System32\drivers\lltdio.sys [102400] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:03 A . (.LSI Corporation - LSI Fusion-MPT SAS Driver (StorPort).) -- C:\WINDOWS\System32\drivers\lsi_sas.sys [109920] =>.Microsoft®
058 - SDL:2022/05/07 07:19:03 A . (.LSI Corporation - LSI SAS Gen2 Driver (StorPort).) -- C:\WINDOWS\System32\drivers\lsi_sas2i.sys [125280] =>.Microsoft®
058 - SDL:2022/05/07 07:19:03 A . (.Avago Technologies - Avago SAS Gen3 Driver (StorPort).) -- C:\WINDOWS\System32\drivers\lsi_sas3i.sys [138600] =>.Microsoft®

058 - SDL:2022/10/16 11:26:39 A . (.Microsoft Corporation - LUA File Virtualization Filter Driver.) -- C:\WINDOWS\System32\drivers\luafv.sys [167936] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:04 A . (.Microsoft Corporation - MA-USB Host Controller Driver.) -- C:\WINDOWS\System32\drivers\mausbhost.sys [566632] =>.Microsoft®
058 - SDL:2022/05/07 07:19:04 A . (.Microsoft Corporation - MA-USB IP Driver.) -- C:\WINDOWS\System32\drivers\mausbip.sys [99664] =>.Microsoft®
058 - SDL:2022/10/16 11:25:55 A . (.Microsoft Corporation - Windows Mobile Broadband Class Extension.) -- C:\WINDOWS\System32\drivers\MbbCx.sys [454656] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:45 A . (.Microsoft Corporation - Medium changer class driver.) -- C:\WINDOWS\System32\drivers\mcd.sys [61440] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:03 A . (.Avago Technologies - MEGASAS2i RAID Controller Driver for Window.) -- C:\WINDOWS\System32\drivers\MegaSas2i.sys [81752] =>.Microsoft®
058 - SDL:2022/05/07 07:19:03 A . (.Broadcom Inc - MEGASAS RAID Controller Driver for Windows.) -- C:\WINDOWS\System32\drivers\megasas35i.sys [101224] =>.Microsoft®
058 - SDL:2022/05/07 07:19:03 A . (.LSI Corporation, Inc. - LSI MegaRAID Software RAID Driver.) -- C:\WINDOWS\System32\drivers\megasr.sys [576856] =>.Microsoft®
058 - SDL:2022/05/07 07:19:00 A . (.Microsoft Corporation - Microsoft Bluetooth Avrcp Transport Driver.) -- C:\WINDOWS\System32\drivers\Microsoft.Bluetooth.AvrCpTransport.sys [98304] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - Legacy Bluetooth LE Bus Enumerator.) -- C:\WINDOWS\System32\drivers\Microsoft.Bluetooth.Legacy.LEEnumerator.sys [143360] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:04 A . (.Mellanox - MLX4 Bus Driver.) -- C:\WINDOWS\System32\drivers\mlx4_bus.sys [1132392] =>.Microsoft®
058 - SDL:2022/10/16 11:25:57 A . (.Microsoft Corporation - MMCSS Driver.) -- C:\WINDOWS\System32\drivers\mmcsc.sys [90112] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:27:15 A . (.Microsoft Corporation - Modem Device Driver.) -- C:\WINDOWS\System32\drivers\modem.sys [81920] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:25:59 A . (.Microsoft Corporation - Monitor Driver.) -- C:\WINDOWS\System32\drivers\monitor.sys [118784] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:25 A . (.Microsoft Corporation - Mouse Class Driver.) -- C:\WINDOWS\System32\drivers\mouseclass.sys [95592] =>.Microsoft®
058 - SDL:2022/05/07 07:19:25 A . (.Microsoft Corporation - HID Mouse Filter Driver.) -- C:\WINDOWS\System32\drivers\mousehid.sys [69632] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:28 A . (.Microsoft Corporation - Mount Point Manager.) -- C:\WINDOWS\System32\drivers\mountmgr.sys [136544] =>.Microsoft®
058 - SDL:2022/05/07 07:19:03 A . (.Broadcom Limited - Broadcom MPI 3.0 Driver (StorPort).) -- C:\WINDOWS\System32\drivers\mpi3drvi.sys [90472] =>.Microsoft®
058 - SDL:2022/10/16 11:26:10 A . (.Microsoft Corporation - Microsoft Protection Service Driver.) -- C:\WINDOWS\System32\drivers\mpsdrv.sys [110592] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:20:16 A . (.Microsoft Corporation - Windows NT WebDav Minirdr.) -- C:\WINDOWS\System32\drivers\mrxdav.sys [196608] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:37 A . (.Microsoft Corporation - Windows NT SMB Minirdr.) -- C:\WINDOWS\System32\drivers\mrxsmb.sys [660816] =>.Microsoft®
058 - SDL:2022/10/16 11:26:37 A . (.Microsoft Corporation - Longhorn SMB 2.0 Redirector.) -- C:\WINDOWS\System32\drivers\mrxsmb20.sys [333160] =>.Microsoft®

058 - SDL:2022/10/16 11:26:29 A . (.Microsoft Corporation - Mailslot driver.) -- C:\WINDOWS\System32\drivers\msfs.sys [79192] =>.Microsoft®
058 - SDL:2022/10/16 11:26:11 A . (.Microsoft Corporation - GPIO Class Extension Driver.) -- C:\WINDOWS\System32\drivers\msgpioclx.sys [218464] =>.Microsoft®
058 - SDL:2022/10/16 11:26:39 A . (.Microsoft Corporation - GPIO Button Driver.) -- C:\WINDOWS\System32\drivers\msgpiowin32.sys [95568] =>.Microsoft®
058 - SDL:2022/05/07 07:19:23 A . (.Microsoft Corporation - Pass-through HID to KMD Filter Driver.) -- C:\WINDOWS\System32\drivers\mshidkmdf.sys [49152] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:13 A . (.Microsoft Corporation - Pass-through Driver for HID-UMDF Interface.) -- C:\WINDOWS\System32\drivers\mshidumdf.sys [49152] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:23 A . (.Microsoft Corporation - Hardware Notification Class Extension Drive.) -- C:\WINDOWS\System32\drivers\mshwncld.sys [61440] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:04 A . (.Microsoft Corporation - ISA Driver.) -- C:\WINDOWS\System32\drivers\msisadv.sys [54608] =>.Microsoft®
058 - SDL:2022/05/07 07:19:04 A . (.Microsoft Corporation - Microsoft iSCSI Initiator Driver.) -- C:\WINDOWS\System32\drivers\msiscsi.sys [333168] =>.Microsoft®
058 - SDL:2022/05/07 07:19:38 A . (.Microsoft Corporation - MS KS Server.) -- C:\WINDOWS\System32\drivers\mskssrv.sys [73728] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:41 A . (.Microsoft Corporation - Microsoft Link-Layer Discovery Protocol Dri.) -- C:\WINDOWS\System32\drivers\mslldp.sys [102400] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:38 A . (.Microsoft Corporation - MS Proxy Clock.) -- C:\WINDOWS\System32\drivers\mspclock.sys [49152] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:38 A . (.Microsoft Corporation - MS Proxy Quality Manager.) -- C:\WINDOWS\System32\drivers\mspqm.sys [49152] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:31 A . (.Microsoft Corporation - Microsoft® QUIC Library.) -- C:\WINDOWS\System32\drivers\msquic.sys [404336] =>.Microsoft®
058 - SDL:2022/05/07 07:19:30 A . (.Microsoft Corporation - Kernel Remote Procedure Call Provider.) -- C:\WINDOWS\System32\drivers\msrpc.sys [406872] =>.Microsoft®
058 - SDL:2022/05/07 07:19:04 A . (.Microsoft Corporation - System Management BIOS Driver.) -- C:\WINDOWS\System32\drivers\mssmbios.sys [79216] =>.Microsoft®
058 - SDL:2022/05/07 07:19:38 A . (.Microsoft Corporation - WDM Tee/Communication Transform Filter.) -- C:\WINDOWS\System32\drivers\mstee.sys [53248] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:03 A . (.Microsoft Corporation - Microsoft Multi-Touch HID Driver.) -- C:\WINDOWS\System32\drivers\MTConfig.sys [53248] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:37 A . (.Microsoft Corporation - Multiple UNC Provider Driver.) -- C:\WINDOWS\System32\drivers\mup.sys [169288] =>.Microsoft®
058 - SDL:2022/05/07 07:19:03 A . (.Marvell Semiconductor, Inc. - Marvell Flash Controller Driver.) -- C:\WINDOWS\System32\drivers\mvumis.sys [64872] =>.Microsoft®
058 - SDL:2022/05/07 07:19:04 A . (.Mellanox - NetworkDirect Support Filter Driver.) -- C:\WINDOWS\System32\drivers\ndfltr.sys [147304] =>.Microsoft®
058 - SDL:2022/10/16 11:26:30 A . (.Microsoft Corporation - Network Driver Interface Specification (NDI.) -- C:\WINDOWS\System32\drivers\ndis.sys [1631584] =>.Microsoft®
058 - SDL:2022/05/07 07:20:14 A . (.Microsoft Corporation - Microsoft NDIS Packet Capture Filter Driver.) -- C:\WINDOWS\System32\drivers\ndiscap.sys [86016] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:41 A . (.Microsoft Corporation - Microsoft Network Adapter Multiplexor.) -- C:\WINDOWS\System32\drivers\NdisImPlatform.sys [163840] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:43 A . (.Microsoft Corporation - NDIS 3.0 connection wrapper driver.) -- C:\WINDOWS\System32\drivers\ndistapi.sys [65536] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:31 A . (.Microsoft Corporation - NDIS User mode I/O driver.) -- C:\WINDOWS\System32\drivers\ndisuiio.sys [102400] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:42 A . (.Microsoft Corporation - Microsoft Virtual Network Adapter Enumerato.) -- C:\WINDOWS\System32\drivers\NdisVirtualBus.sys [57344] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:43 A . (.Microsoft Corporation - MS PPP Framing Driver (Strong Encryption).) -- C:\WINDOWS\System32\drivers\ndiswan.sys [237568] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:20:14 A . (...) -- C:\WINDOWS\System32\drivers\NDKPerf.sys [83288] =>.Microsoft®
058 - SDL:2022/05/07 07:20:14 A . (.Microsoft Corporation - RDMA Sample Driver.) -- C:\WINDOWS\System32\drivers\NDKPing.sys [107872] =>.Microsoft®
058 - SDL:2022/10/16 11:26:43 A . (.Microsoft Corporation - NDIS Proxy.) -- C:\WINDOWS\System32\drivers\ndproxy.sys [122880] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:27:04 A . (.Microsoft Corporation - Windows Network Data Usage Monitoring Drive.) -- C:\WINDOWS\System32\drivers\Ndu.sys [188416] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:32 A . (.Microsoft Corporation - Network Adapter Class Extension for WDF.) -- C:\WINDOWS\System32\drivers\NetAdapterCx.sys [394592] =>.Microsoft®
058 - SDL:2022/10/16 11:26:41 A . (.Microsoft Corporation - NetBIOS interface driver.) -- C:\WINDOWS\System32\drivers\netbios.sys [95584] =>.Microsoft®
058 - SDL:2022/10/16 11:26:41 A . (.Microsoft Corporation - MBT Transport driver.) -- C:\WINDOWS\System32\drivers\netbt.sys [327680] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:30 A . (.Microsoft Corporation - Network I/O Subsystem.) -- C:\WINDOWS\System32\drivers\netio.sys [652640] =>.Microsoft®
058 - SDL:2022/10/16 11:27:16 A . (.Microsoft Corporation - Virtual NDIS Miniport.) -- C:\WINDOWS\System32\drivers\netvsc.sys [329040] =>.Microsoft®
058 - SDL:2018/09/15 09:28:15 A . (.Intel Corporation - Intel® Wireless WiFi Link Driver.) -- C:\WINDOWS\System32\drivers\Netwtw06.sys [8723968] [Unsigned] =>.Intel Corporation
058 - SDL:2022/01/07 20:36:26 N . (.Intel Corporation - Intel® Wireless WiFi Link Driver.) -- C:\WINDOWS\System32\drivers\Netwtw08.sys [8815680] {58B1C1C43E999C1CF7C694A1D776D0FE}. =>.Intel Corporation
058 - SDL:2022/10/16 11:26:29 A . (.Microsoft Corporation - NPFS Driver.) -- C:\WINDOWS\System32\drivers\npfs.sys [120128] =>.Microsoft®
058 - SDL:2022/05/07 07:19:32 A . (.Microsoft Corporation - Named pipe service triggers.) -- C:\WINDOWS\System32\drivers\npsvc trig.sys [65536] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:31 A . (.Microsoft Corporation - NSI Proxy.) -- C:\WINDOWS\System32\drivers\nsiproxy.sys [77824] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:28 A . (.Microsoft Corporation - NT File System Driver.) -- C:\WINDOWS\System32\drivers\ntfs.sys [3343712] =>.Microsoft®
058 - SDL:2022/05/07 07:19:39 A . (.Microsoft Corporation - NTOS extension host driver.) -- C:\WINDOWS\System32\drivers\ntosext.sys [58704] =>.Microsoft®
058 - SDL:2022/05/07 07:19:30 A . (.Microsoft Corporation - NULL Driver.) -- C:\WINDOWS\System32\drivers\null.sys [45056] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:05 A . (.Microsoft Corporation - NVDIMM device driver.) -- C:\WINDOWS\System32\drivers\nvdimms.sys [206160] =>.Microsoft®
058 - SDL:2022/07/22 06:25:37 A . (.NVIDIA Corporation - NVIDIA HDMI Audio Driver.) -- C:\WINDOWS\System32\drivers\nvhda64v.sys [130216] =>.Nvidia Corporation®
058 - SDL:2022/05/07 07:19:03 A . (.Microsoft Corporation - Nvme Disk Driver.) -- C:\WINDOWS\System32\drivers\nvmedisk.sys [91496] =>.Microsoft®
058 - SDL:2022/05/07 07:19:04 A . (.NVIDIA Corporation - NVIDIA® nForce(TM) RAID Driver.) -- C:\WINDOWS\System32\drivers\nvraid.sys [151392] =>.Microsoft®

058 - SDL:2022/05/07 07:19:04 A . (.NVIDIA Corporation - NVIDIA® nForce(TM) Sata Performance Driver.) -- C:\WINDOWS\System32\drivers\nvstor.sys [167256] =>.Microsoft®

058 - SDL:2022/07/15 18:59:26 A . (.NVIDIA Corporation - NVIDIA Virtual Audio Driver.) -- C:\WINDOWS\System32\drivers\nvad64v.sys [59368] =>.Nvidia Corporation®

058 - SDL:2022/07/14 01:32:50 A . (.NVIDIA Corporation - Virtual USB Host Controller driver.) -- C:\WINDOWS\System32\drivers\nvvhci.sys [60112] =>.Nvidia Corporation®

058 - SDL:2022/10/16 11:26:05 A . (.Microsoft Corporation - NativeWiFi Miniport Driver.) -- C:\WINDOWS\System32\drivers\nwifi.sys [753664] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:20:18 A . (.Microsoft Corporation - Plan 9 redirector.) -- C:\WINDOWS\System32\drivers\p9rdr.sys [148816] =>.Microsoft®

058 - SDL:2022/10/16 11:26:16 A . (.Microsoft Corporation - QoS Packet Scheduler.) -- C:\WINDOWS\System32\drivers\pacer.sys [185680] =>.Microsoft®

058 - SDL:2022/08/04 11:03:54 A . (.Pango Inc - Pango NetFilter WFP Driver.) -- C:\WINDOWS\System32\drivers\pango_netfilter2.sys [89088] =>.Microsoft®

058 - SDL:2022/05/07 07:19:04 A . (.Microsoft Corporation - Parallel Port Driver.) -- C:\WINDOWS\System32\drivers\parport.sys [135168] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:29 A . (.Microsoft Corporation - Partition driver.) -- C:\WINDOWS\System32\drivers\partmgr.sys [218448] =>.Microsoft®

058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - NT Plug and Play PCI Enumerator.) -- C:\WINDOWS\System32\drivers\pci.sys [566624] =>.Microsoft®

058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - Generic PCI IDE Bus Driver.) -- C:\WINDOWS\System32\drivers\pciide.sys [54608] =>.Microsoft®

058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - PCI IDE Bus Driver Extension.) -- C:\WINDOWS\System32\drivers\pciindex.sys [91488] =>.Microsoft®

058 - SDL:2022/05/07 07:19:01 A . (.Microsoft Corporation - PCMCIA Bus Driver.) -- C:\WINDOWS\System32\drivers\pcmcia.sys [157016] =>.Microsoft®

058 - SDL:2022/10/16 11:26:28 A . (.Microsoft Corporation - Performance Counters for Windows Driver.) -- C:\WINDOWS\System32\drivers\pcw.sys [99672] =>.Microsoft®

058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - Power Dependency Coordinator Driver.) -- C:\WINDOWS\System32\drivers\pdc.sys [202080] =>.Microsoft®

058 - SDL:2022/05/07 07:19:08 A . (.Microsoft Corporation - Protected Environment Authentication and Au.) -- C:\WINDOWS\System32\drivers\PEAuth.sys [856064] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:04 A . (.Avago Technologies - MEGASAS RAID Controller Driver for Windows.) -- C:\WINDOWS\System32\drivers\percsas2i.sys [59752] =>.Microsoft®

058 - SDL:2022/05/07 07:19:04 A . (.Avago Technologies - MEGASAS RAID Controller Driver for Windows.) -- C:\WINDOWS\System32\drivers\percsas3i.sys [69464] =>.Microsoft®

058 - SDL:2022/10/16 11:27:14 A . (.Microsoft Corporation - Packet Monitor Driver.) -- C:\WINDOWS\System32\drivers\PktMon.sys [177504] =>.Microsoft®

058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - Persistent memory driver.) -- C:\WINDOWS\System32\drivers\pmem.sys [181600] =>.Microsoft®

058 - SDL:2022/05/07 07:19:02 A . (.Microsoft Corporation - Plug and Play Memory Driver.) -- C:\WINDOWS\System32\drivers\pnpmem.sys [53248] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:23 A . (.Microsoft Corporation - Port Device Class Configuration Filter Driv.) -- C:\WINDOWS\System32\drivers\portcfg.sys [61440] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:01 A . (.Microsoft Corporation - Port Class (Class Driver for Port/Miniport.) -- C:\WINDOWS\System32\drivers\portcls.sys [471040] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:00 A . (.Microsoft Corporation - Processor Device Driver.) -- C:\WINDOWS\System32\drivers\processr.sys [259400] =>.Microsoft®

058 - SDL:2022/05/07 07:19:23 A . (.Microsoft Corporation - Time Travel Debugging Process Launch Monito.) -- C:\WINDOWS\System32\drivers\ProcLaunchMon.sys [79896] =>.Microsoft®

058 - SDL:2022/05/07 07:19:04 A . (.VMware, Inc. - VMware PVSCSI StorPort driver (64-bit).) -- C:\WINDOWS\System32\drivers\pvscsii.sys [45408] =>.Microsoft®

058 - SDL:2022/10/16 11:26:41 A . (.Microsoft Corporation - Microsoft Quality Windows Audio Video Exper.) -- C:\WINDOWS\System32\drivers\qwavedrv.sys [86016] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:02 A . (.Microsoft Corporation - RAM Disk Driver.) -- C:\WINDOWS\System32\drivers\ramdisk.sys [75104] =>.Microsoft®

058 - SDL:2022/05/07 07:19:43 A . (.Microsoft Corporation - RAS Automatic Connection Driver.) -- C:\WINDOWS\System32\drivers\rasacd.sys [57344] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:43 A . (.Microsoft Corporation - RAS L2TP mini-port/call-manager driver.) -- C:\WINDOWS\System32\drivers\rasl2tp.sys [139264] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:43 A . (.Microsoft Corporation - RAS PPPoE mini-port/call-manager driver.) -- C:\WINDOWS\System32\drivers\rasppoe.sys [118784] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:43 A . (.Microsoft Corporation - Peer-to-Peer Tunneling Protocol.) -- C:\WINDOWS\System32\drivers\raspttp.sys [139264] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:43 A . (.Microsoft Corporation - RAS SSTP Miniport Call Manager.) -- C:\WINDOWS\System32\drivers\rassstp.sys [122880] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:37 A . (.Microsoft Corporation - Redirected Drive Buffering SubSystem Driver.) -- C:\WINDOWS\System32\drivers\rdbss.sys [496992] =>.Microsoft®

058 - SDL:2022/10/16 11:27:14 A . (.Microsoft Corporation - Microsoft RDP Bus Device driver.) -- C:\WINDOWS\System32\drivers\rdpbus.sys [65536] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:20:14 A . (.Microsoft Corporation - Microsoft RDP Device redirector.) -- C:\WINDOWS\System32\drivers\rdpdr.sys [196608] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:27:13 A . (.Microsoft Corporation - Microsoft RDP Video Miniport driver.) -- C:\WINDOWS\System32\drivers\rdpvideominiport.sys [66888] =>.Microsoft®

058 - SDL:2022/10/16 11:27:16 A . (.Microsoft Corporation - ReadyBoost Driver.) -- C:\WINDOWS\System32\drivers\rdyboost.sys [329056] =>.Microsoft®

058 - SDL:2022/10/16 11:26:34 A . (.Microsoft Corporation - NT ReFS FS Driver.) -- C:\WINDOWS\System32\drivers\refs.sys [2868608] =>.Microsoft®

058 - SDL:2022/10/16 11:26:34 A . (.Microsoft Corporation - NT ReFS FS Driver.) -- C:\WINDOWS\System32\drivers\refsv1.sys [1000800] =>.Microsoft®

058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - Bluetooth RFCOMM Driver.) -- C:\WINDOWS\System32\drivers\rfcomm.sys [253952] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:25:59 A . (.Microsoft Corporation - ResourceHub Proxy Driver.) -- C:\WINDOWS\System32\drivers\rhproxy.sys [147456] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:20:09 A . (.Microsoft Corporation - Reliable Multicast Transport.) -- C:\WINDOWS\System32\drivers\rmcst.sys [184320] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:43 A . (.Microsoft Corporation - Remote NDIS Miniport.) -- C:\WINDOWS\System32\drivers\RNDISMP.sys [69632] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:20:15 A . (.Microsoft Corporation - Legacy Non-Pnp Modem Device Driver.) -- C:\WINDOWS\System32\drivers\rootmdm.sys [49152] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:20:02 A . (...) -- C:\WINDOWS\System32\drivers\RoutePolicy.sys [98304] [Unsigned]

058 - SDL:2022/10/16 11:26:38 A . (.Microsoft Corporation - Link-Layer Topology Responder Driver for ND.) -- C:\WINDOWS\System32\drivers\rspndr.sys [118784] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/08/18 16:47:10 A . (.Realtek - Realtek 8125/8136/8168/8169 NDIS 6.40 64-bi.) -- C:\WINDOWS\System32\drivers\rt640x64.sys [1188672] =>.Realtek Semiconductor Corp.®

058 - SDL:2022/05/07 07:19:00 RA . (.Realtek - Realtek PCIe GBE Family Controller Flight.) -- C:\WINDOWS\System32\drivers\rteth.sys [86016] [Unsigned] =>.Realtek

058 - SDL:2018/09/03 14:33:42 A . (.Realtek - Realtek packet filter driver.) -- C:\WINDOWS\System32\drivers\rtf64x64.sys [70560] =>.Realtek Semiconductor Corp.®

058 - SDL:2020/04/08 21:25:14 A . (.Realtek Semiconductor Corp. - Realtek(r) High Definition Audio Function D.) -- C:\WINDOWS\System32\drivers\RTKVHD64.sys [7322920] =>.Realtek Semiconductor Corp.®

058 - SDL:2022/10/16 11:26:00 A . (.Microsoft Corporation - SBP-2 Protocol Driver.) -- C:\WINDOWS\System32\drivers\sbp2port.sys [148816] =>.Microsoft®

058 - SDL:2022/05/07 07:19:44 A . (.Microsoft Corporation - Microsoft Smart Card Reader Filter Driver.) -- C:\WINDOWS\System32\drivers\scfilter.sys [77824] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - Storage Class Memory Bus Driver.) -- C:\WINDOWS\System32\drivers\scmbus.sys [222536] =>.Microsoft®

058 - SDL:2022/05/07 07:19:45 A . (.Microsoft Corporation - SCSI Port Driver.) -- C:\WINDOWS\System32\drivers\scsiport.sys [226656] =>.Microsoft®

058 - SDL:2022/05/07 07:19:25 A . (.Microsoft Corporation - SecureDigital Bus Driver.) -- C:\WINDOWS\System32\drivers\sdbus.sys [341336] =>.Microsoft®

058 - SDL:2022/05/07 07:19:02 A . (.Microsoft Corporation - SDF Reflector.) -- C:\WINDOWS\System32\drivers\SDFRd.sys [71016] =>.Microsoft®

058 - SDL:2022/10/16 11:25:59 A . (.Microsoft Corporation - SD Host Controller Port Driver.) -- C:\WINDOWS\System32\drivers\sdport.sys [140656] =>.Microsoft®

058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - SD Storage Class Driver.) -- C:\WINDOWS\System32\drivers\sdstor.sys [132456] =>.Microsoft®

058 - SDL:2022/05/07 07:19:23 A . (.Microsoft Corporation - Serial Class Extension.) -- C:\WINDOWS\System32\drivers\SerCx.sys [120144] =>.Microsoft®

058 - SDL:2022/10/16 11:26:20 A . (.Microsoft Corporation - Serial Class Extension V2.) -- C:\WINDOWS\System32\drivers\SerCx2.sys [206184] =>.Microsoft®

058 - SDL:2022/05/07 07:19:04 A . (.Microsoft Corporation - Serial Port Enumerator.) -- C:\WINDOWS\System32\drivers\serenum.sys [65536] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:04 A . (.Microsoft Corporation - Serial Device Driver.) -- C:\WINDOWS\System32\drivers\serial.sys [122880] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:25 A . (.Microsoft Corporation - Serial Mouse Filter Driver.) -- C:\WINDOWS\System32\drivers\sermouse.sys [65536] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:04 A . (.Microsoft Corporation - SCSI Floppy Driver.) -- C:\WINDOWS\System32\drivers\sfloppy.sys [57344] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:20:01 A . (.Microsoft Corporation - System Guard Runtime Monitor Agent Driver.) -- C:\WINDOWS\System32\drivers\SgrmAgent.sys [124264] =>.Microsoft®

058 - SDL:2022/05/07 07:19:04 A . (.Silicon Integrated Systems Corp. - SiS RAID Stor Miniport Driver.) -- C:\WINDOWS\System32\drivers\sisraid2.sys [45920] =>.Microsoft®

058 - SDL:2022/05/07 07:19:04 A . (.Silicon Integrated Systems - SiS AHCI Stor-Miniport Driver.) -- C:\WINDOWS\System32\drivers\sisraid4.sys [82784] =>.Microsoft®

058 - SDL:2022/05/07 07:19:04 A . (.Microsemi Corportation - Storport Miniport Driver for SmartRAID/Smr.) -- C:\WINDOWS\System32\drivers\SmartSAMD.sys [210784] =>.Microsoft®

058 - SDL:2022/05/07 07:19:44 A . (.Microsoft Corporation - Smart Card Driver Library.) -- C:\WINDOWS\System32\drivers\smclib.sys [65536] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:00 A . (.Microsoft Corporation - Storage Spaces Dump Driver.) -- C:\WINDOWS\System32\drivers\spacedump.sys [284000] =>.Microsoft®

058 - SDL:2022/05/07 07:20:02 A . (.Microsoft Corporation - Storage Spaces Parser driver.) -- C:\WINDOWS\System32\drivers\spaceparser.sys [81920] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:00 A . (.Microsoft Corporation - Storage Spaces Driver.) -- C:\WINDOWS\System32\drivers\spaceport.sys [931144] =>.Microsoft®

058 - SDL:2022/05/07 08:10:24 A . (.Microsoft Corporation - Holographic Spatial Graph Filter.) -- C:\WINDOWS\System32\drivers\SpatialGraphFilter.sys [132448] =>.Microsoft®

058 - SDL:2022/10/16 11:26:20 A . (.Microsoft Corporation - SPB Class Extension.) -- C:\WINDOWS\System32\drivers\SpbCx.sys [124256] =>.Microsoft®

058 - SDL:2022/10/16 11:26:37 A . (.Microsoft Corporation - Smb 2.0 Server driver.) -- C:\WINDOWS\System32\drivers\srv2.sys [868352] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:37 A . (.Microsoft Corporation - Server Network driver.) -- C:\WINDOWS\System32\drivers\srvnet.sys [368640] [Unsigned] =>.Microsoft Corporation

058 - SDL:2021/10/08 18:00:36 A . (.Samsung Electronics Co., Ltd. - SAMSUNG USB Composite Device Driver.) -- C:\WINDOWS\System32\drivers\ssudbus2.sys [160376] =>.Samsung Electronics Co., Ltd.®

058 - SDL:2021/10/08 18:00:42 A . (.Samsung Electronics Co., Ltd. - SAMSUNG Android Modem Device Driver.) -- C:\WINDOWS\System32\drivers\ssudmdm.sys [167544] =>.Samsung Electronics Co., Ltd.®

058 - SDL:2022/05/07 07:19:04 A . (.Promise Technology, Inc. - Promise SuperTrak EX Series Driver for Wind.) -- C:\WINDOWS\System32\drivers\stexstor.sys [32080] =>.Microsoft®

058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - MS AHCI Storport Miniport Driver.) -- C:\WINDOWS\System32\drivers\storahci.sys [214352] =>.Microsoft®

058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - Microsoft NVM Express Storport Miniport Dri.) -- C:\WINDOWS\System32\drivers\stornvme.sys [238928] =>.Microsoft®

058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - Microsoft Storage Port Driver.) -- C:\WINDOWS\System32\drivers\storport.sys [1164640] =>.Microsoft®

058 - SDL:2022/05/07 07:19:23 A . (.Microsoft Corporation - Storage QoS Filter.) -- C:\WINDOWS\System32\drivers\storqosflt.sys [120144] =>.Microsoft®

058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - MS UFS Storport Miniport Driver.) -- C:\WINDOWS\System32\drivers\storufs.sys [107848] =>.Microsoft®

058 - SDL:2022/10/16 11:27:16 A . (.Microsoft Corporation - Storage VSC Driver.) -- C:\WINDOWS\System32\drivers\stovsc.sys [87392] =>.Microsoft®

058 - SDL:2022/05/07 07:19:45 A . (.Microsoft Corporation - WDM CODEC Class Device Driver 2.0.) -- C:\WINDOWS\System32\drivers\stream.sys [118784] [Unsigned] =>.Microsoft Corporation

058 - SDL:2020/09/25 10:05:26 A . (.The OpenVPN Project - TAP-Windows Virtual Network Driver.) -- C:\WINDOWS\System32\drivers\tap-tb-0901.sys [38656] =>.TunnelBear, Inc.®

058 - SDL:2019/10/23 10:58:40 A . (.The OpenVPN Project - TAP-Windows Virtual Network Driver (NDIS 6..)) -- C:\WINDOWS\System32\drivers\tap0901.sys [39920] =>.Microsoft®

058 - SDL:2022/05/07 07:19:45 A . (.Microsoft Corporation - SCSI Tape Class Driver.) -- C:\WINDOWS\System32\drivers\tape.sys [69632] [Unsigned] =>.Microsoft Corporation

058 - SDL:2018/07/06 13:22:44 A . (.The OpenVPN Project - TAP-Windows Virtual Network Driver (NDIS 6..)) -- C:\WINDOWS\System32\drivers\tapwindscribe0901.sys [54896] =>.Windscribe Limited®

058 - SDL:2022/10/16 11:26:04 A . (.Microsoft Corporation - Export driver for kernel mode TPM API.) -- C:\WINDOWS\System32\drivers\tbs.sys [75112] =>.Microsoft®

058 - SDL:2022/10/16 11:26:32 A . (.Microsoft Corporation - TCP/IP Driver.) -- C:\WINDOWS\System32\drivers\tcpip.sys [3306840] =>.Microsoft®

058 - SDL:2022/10/16 11:26:32 A . (.Microsoft Corporation - TCP/IP Registry Compatibility Driver.) -- C:\WINDOWS\System32\drivers\tcpipreg.sys [86016] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:31 A . (.Microsoft Corporation - TDI Wrapper.) -- C:\WINDOWS\System32\drivers\tdi.sys [79184] =>.Microsoft®

058 - SDL:2022/10/16 11:27:04 A . (.Microsoft Corporation - TDI Translation Driver.) -- C:\WINDOWS\System32\drivers\tdx.sys [157000] =>.Microsoft®

058 - SDL:2022/05/07 07:20:12 A . (.Microsoft Corporation - Terminal Server Input Driver.) -- C:\WINDOWS\System32\drivers\termintpt.sys [75104] =>.Microsoft®

058 - SDL:2022/10/16 11:26:37 A . (.Microsoft Corporation - Kernel Transaction Manager Driver.) -- C:\WINDOWS\System32\drivers\tm.sys [177504] =>.Microsoft®

058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - TPM Device Driver.) -- C:\WINDOWS\System32\drivers\tpm.sys [365920] =>.Microsoft®

058 - SDL:2022/05/07 07:19:02 A . (.Microsoft Corporation - Remote Desktop USB Hub Filter Driver.) -- C:\WINDOWS\System32\drivers\TsUsbFlt.sys [98304] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:03 A . (.Microsoft Corporation - Remote Desktop Generic USB Driver.) -- C:\WINDOWS\System32\drivers\TsUsbGD.sys [69632] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:41 A . (.Microsoft Corporation - Microsoft Tunnel Interface Driver.) -- C:\WINDOWS\System32\drivers\tunnel.sys [167936] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - Microsoft Uasp Driver.) -- C:\WINDOWS\System32\drivers\uasptor.sys [116064] =>.Microsoft®

058 - SDL:2022/10/16 11:26:20 A . (.Microsoft Corporation - USB Connector Manager KMDF Class Extension.) -- C:\WINDOWS\System32\drivers\UcmCx.sys [204800] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:20 A . (.Microsoft Corporation - UCM-TCPCI KMDF Class Extension.) -- C:\WINDOWS\System32\drivers\UcmTcpciCx.sys [217088] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:25 A . (.Microsoft Corporation - UCM-UCSI ACPI Client Driver.) -- C:\WINDOWS\System32\drivers\UcmUcsiAcpiClient.sys [69632] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:20 A . (.Microsoft Corporation - UCM-UCSI KMDF Class Extension.) -- C:\WINDOWS\System32\drivers\UcmUcsiCx.sys [155648] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:05 A . (.Microsoft Corporation - USB Controller Extension.) -- C:\WINDOWS\System32\drivers\Ucx01000.sys [292184] =>.Microsoft®

058 - SDL:2022/05/07 07:19:05 A . (.Microsoft Corporation - 'udecx.DRIVER'.) -- C:\WINDOWS\System32\drivers\Udecx.sys [90112] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:20:15 A . (.Microsoft Corporation - UDF File System Driver.) -- C:\WINDOWS\System32\drivers\udfs.sys [389120] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/14 10:30:16 A . (.SysNucleus - USBDeviceShare Device Stub.) -- C:\WINDOWS\System32\drivers\udsstub.sys [37888] [Unsigned] =>.SysNucleus

058 - SDL:2022/10/16 11:26:20 A . (.Microsoft Corporation - USB Function Driver Class Extension.) -- C:\WINDOWS\System32\drivers\ufx01000.sys [361816] =>.Microsoft®

058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - UFX Synopsys Client Driver.) -- C:\WINDOWS\System32\drivers\ufxsynopsys.sys [197968] =>.Microsoft®

058 - SDL:2022/05/07 07:19:25 A . (.Microsoft Corporation - Generic pass-through driver.) -- C:\WINDOWS\System32\drivers\umpass.sys [53248] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:20 A . (.Microsoft Corporation - USB Role-Switch Class Extension.) -- C:\WINDOWS\System32\drivers\urscx01000.sys [111952] =>.Microsoft®

058 - SDL:2022/05/07 07:19:43 A . (.Microsoft Corporation - Remote NDIS USB Driver.) -- C:\WINDOWS\System32\drivers\usb8023.sys [57344] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:25:58 A . (.Microsoft Corporation - USB Audio Class Driver.) -- C:\WINDOWS\System32\drivers\USBAUDIO.sys [282624] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:01 A . (.Microsoft Corporation - Microsoft USB Audio Class 2.0 Driver.) -- C:\WINDOWS\System32\drivers\usbaudio2.sys [397312] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:29 A . (.Microsoft Corporation - Universal Serial Bus Camera Driver.) -- C:\WINDOWS\System32\drivers\USBCAMD2.sys [81920] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - USB Common Class Generic Parent Driver.) -- C:\WINDOWS\System32\drivers\usbccgp.sys [230736] =>.Microsoft®
058 - SDL:2022/05/07 07:19:01 A . (.Microsoft Corporation - USB Consumer IR Driver for eHome.) -- C:\WINDOWS\System32\drivers\usbcir.sys [143360] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - Universal Serial Bus Driver.) -- C:\WINDOWS\System32\drivers\usbd.sys [70992] =>.Microsoft®
058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - EHCI eUSB Miniport Driver.) -- C:\WINDOWS\System32\drivers\usbehci.sys [120160] =>.Microsoft®
058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - Default Hub Driver for USB.) -- C:\WINDOWS\System32\drivers\usbhub.sys [558416] =>.Microsoft®
058 - SDL:2022/05/07 07:19:25 A . (.Microsoft Corporation - USB3 HUB Driver.) -- C:\WINDOWS\System32\drivers\USBHUB3.SYS [72256] =>.Microsoft®
058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - OHCI USB Miniport Driver.) -- C:\WINDOWS\System32\drivers\usbohci.sys [65536] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:23 A . (.Microsoft Corporation - USB Policy Manager Kernel-Mode Library.) -- C:\WINDOWS\System32\drivers\UsbPmApi.sys [94208] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - USB 1.1 & 2.0 Port Driver.) -- C:\WINDOWS\System32\drivers\usbport.sys [505184] =>.Microsoft®
058 - SDL:2022/10/16 11:25:59 A . (.Microsoft Corporation - USB Printer driver.) -- C:\WINDOWS\System32\drivers\usbprint.sys [110592] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:25:59 A . (.Microsoft Corporation - USB Scanner Driver.) -- C:\WINDOWS\System32\drivers\usbscan.sys [81920] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - USB Serial Driver.) -- C:\WINDOWS\System32\drivers\usbser.sys [126976] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:25 A . (.Microsoft Corporation - USB Mass Storage Class Driver.) -- C:\WINDOWS\System32\drivers\USBSTOR.SYS [173392] =>.Microsoft®
058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - UHCI USB Miniport Driver.) -- C:\WINDOWS\System32\drivers\usbuhci.sys [73728] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - USB XHCI Driver.) -- C:\WINDOWS\System32\drivers\USBXHCI.SYS [677200] =>.Microsoft®
058 - SDL:2022/05/07 07:19:05 A . (.Microsoft Corporation - Virtual Drive Root Enumerator.) -- C:\WINDOWS\System32\drivers\vdrvroot.sys [124248] =>.Microsoft®
058 - SDL:2022/10/16 11:26:29 A . (.Microsoft Corporation - Driver Verifier Extension.) -- C:\WINDOWS\System32\drivers\VerifierExt.sys [247136] =>.Microsoft®
058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - VHD Miniport Driver.) -- C:\WINDOWS\System32\drivers\vhdmp.sys [1013120] =>.Microsoft®
058 - SDL:2022/10/16 11:26:01 A . (.Microsoft Corporation - Virtual HID Framework (VHF) Driver.) -- C:\WINDOWS\System32\drivers\vhf.sys [90112] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:27:03 A . (.Microsoft Corporation - Microsoft Hyper-V Virtualization Infrastruc.) -- C:\WINDOWS\System32\drivers\Vid.sys [828744] =>.Microsoft®
058 - SDL:2022/05/07 07:19:35 A . (.Microsoft Corporation - Video Port Driver.) -- C:\WINDOWS\System32\drivers\videoprt.sys [90112] [Unsigned] =>.Microsoft Corporation
058 - SDL:2021/07/14 07:06:50 A . (.Shaul Eizikovich - KMDF Virtual Joystick Driver.) -- C:\WINDOWS\System32\drivers\vjoy.sys [67448] {08DF1FFB8B0EEF71ED9573AAE3ECFCDC}. =>.Shaul Eizikovich
058 - SDL:2022/10/16 11:27:16 A . (.Microsoft Corporation - Hyper-V VMBus KMCL.) -- C:\WINDOWS\System32\drivers\mbkmcl.sys [169296] =>.Microsoft®

058 - SDL:2022/10/16 11:27:16 A . (.Microsoft Corporation - Microsoft Hyper-V Virtual Machine Bus Child.) -- C:\WINDOWS\System32\drivers\vmusb.sys [206152] =>.Microsoft®

058 - SDL:2022/05/07 07:20:16 A . (.Microsoft Corporation - Microsoft VMBus HID Miniport.) -- C:\WINDOWS\System32\drivers\VBUSHID.sys [71000] =>.Microsoft®

058 - SDL:2022/05/07 07:20:16 A . (.Microsoft Corporation - Virtual Machine Generation Counter.) -- C:\WINDOWS\System32\drivers\vmgencounter.sys [58720] =>.Microsoft®

058 - SDL:2022/05/07 07:20:16 A . (.Microsoft Corporation - Virtual Machine Guest Infrastructure Driver.) -- C:\WINDOWS\System32\drivers\vmgid.sys [58720] =>.Microsoft®

058 - SDL:2022/05/07 07:20:16 A . (.Microsoft Corporation - Microsoft S3 Emulated Device Cap Driver.) -- C:\WINDOWS\System32\drivers\vms3cap.sys [54616] =>.Microsoft®

058 - SDL:2022/05/07 07:20:16 A . (.Microsoft Corporation - Virtual Storage Filter Driver.) -- C:\WINDOWS\System32\drivers\vmstorfl.sys [87376] =>.Microsoft®

058 - SDL:2022/10/16 11:26:00 A . (.Microsoft Corporation - Volume Manager Driver.) -- C:\WINDOWS\System32\drivers\volmgr.sys [124256] =>.Microsoft®

058 - SDL:2022/05/07 07:20:03 A . (.Microsoft Corporation - Volume Manager Extension Driver.) -- C:\WINDOWS\System32\drivers\volmgrx.sys [419168] =>.Microsoft®

058 - SDL:2022/05/07 07:19:13 A . (.Microsoft Corporation - Volume Shadow Copy driver.) -- C:\WINDOWS\System32\drivers\volsnap.sys [468312] =>.Microsoft®

058 - SDL:2022/05/07 07:19:03 A . (.Microsoft Corporation - Volume driver.) -- C:\WINDOWS\System32\drivers\volume.sys [54640] =>.Microsoft®

058 - SDL:2022/05/07 07:20:16 A . (.Microsoft Corporation - Virtual PCI Bus.) -- C:\WINDOWS\System32\drivers\vpci.sys [120160] =>.Microsoft®

058 - SDL:2022/05/07 07:19:04 A . (.VIA Technologies Inc.,Ltd - VIA RAID DRIVER FOR AMD-X86-64.) -- C:\WINDOWS\System32\drivers\vsraid.sys [167784] =>.Microsoft®

058 - SDL:2022/05/07 07:19:04 A . (.VIA Corporation - VIA StorX RAID Controller Driver.) -- C:\WINDOWS\System32\drivers\VSTXRAID.SYS [306512] =>.Microsoft®

058 - SDL:2022/05/07 07:19:11 A . (.Microsoft Corporation - Virtual Wireless Bus Driver.) -- C:\WINDOWS\System32\drivers\vwifibus.sys [65536] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:11 A . (.Microsoft Corporation - Virtual WiFi Filter Driver.) -- C:\WINDOWS\System32\drivers\vwififlt.sys [110592] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:11 A . (.Microsoft Corporation - Virtual WiFi Miniport Driver.) -- C:\WINDOWS\System32\drivers\vwifimp.sys [86016] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:03 A . (.Microsoft Corporation - Wacom Serial Pen Tablet HID Driver.) -- C:\WINDOWS\System32\drivers\wacompen.sys [65536] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:43 A . (.Microsoft Corporation - MS Remote Access and Routing ARP Driver.) -- C:\WINDOWS\System32\drivers\wanarp.sys [126976] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:11 A . (.Microsoft Corporation - Watchdog Driver.) -- C:\WINDOWS\System32\drivers\watchdog.sys [139264] [Unsigned] =>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:20 A . (.Microsoft Corporation - Windows Container Isolation FS Filter Drive.) -- C:\WINDOWS\System32\drivers\wcifs.sys [251224] =>.Microsoft®

058 - SDL:2022/05/07 07:19:08 A . (.Microsoft Corporation - Microsoft antimalware boot driver.) -- C:\WINDOWS\System32\drivers\WdBoot.sys [48536] =>.Microsoft®

058 - SDL:2022/05/07 07:19:08 A . (.Microsoft Corporation - Microsoft antimalware device filter driver.) -- C:\WINDOWS\System32\drivers\WdDevFlt.sys [169232] =>.Microsoft®

058 - SDL:2022/10/16 11:26:29 A . (.Microsoft Corporation - Kernel Mode Driver Framework Runtime.) -- C:\WINDOWS\System32\drivers\wdf01000.sys [820576] =>.Microsoft®

058 - SDL:2022/05/07 07:19:08 A . (.Microsoft Corporation - Microsoft
antimalware file system filter dr.) -- C:\WINDOWS\System32\drivers\WdFilter.sys
[438544] =>.Microsoft@

058 - SDL:2022/10/16 11:26:29 A . (.Microsoft Corporation - Kernel Mode Driver
Framework Loader.) -- C:\WINDOWS\System32\drivers\WdfLdr.sys [103752]
=>.Microsoft@

058 - SDL:2022/10/16 11:26:05 A . (.Microsoft Corporation - WDI Driver Framework
Driver.) -- C:\WINDOWS\System32\drivers\WdiWiFi.sys [1073152] [Unsigned]
=>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:26 A . (.Microsoft Corporation - WDM Companion
Filter.) -- C:\WINDOWS\System32\drivers\WdmCompanionFilter.sys [62800]
=>.Microsoft@

058 - SDL:2022/05/07 07:19:08 A . (.Microsoft Corporation - Windows Defender
Network Stream Filter.) -- C:\WINDOWS\System32\drivers\WdNisDrv.sys [90384]
=>.Microsoft@

058 - SDL:2022/10/16 11:26:32 A . (.Microsoft Corporation - Windows Error
Reporting Kernel Driver.) -- C:\WINDOWS\System32\drivers\werkernel.sys [99672]
=>.Microsoft@

058 - SDL:2022/10/16 11:26:16 A . (.Microsoft Corporation - WFP NDIS 6.30
Lightweight Filter Driver.) -- C:\WINDOWS\System32\drivers\wfplwfs.sys
[210272] =>.Microsoft@

058 - SDL:2022/10/16 11:26:05 A . (.Microsoft Corporation - Windows Wifi Class
Extension.) -- C:\WINDOWS\System32\drivers\WifiCx.sys [835584] [Unsigned]
=>.Microsoft Corporation

058 - SDL:2022/10/16 11:26:35 A . (.Microsoft Corporation - Wim file system
Driver.) -- C:\WINDOWS\System32\drivers\wimmount.sys [71000] =>.Microsoft@

058 - SDL:2022/10/16 11:26:20 A . (.Microsoft Corporation - Windows Trusted
Runtime Interface Driver.) -- C:\WINDOWS\System32\drivers\WindowsTrustedRT.sys
[108032] =>.Microsoft@

058 - SDL:2022/05/07 07:19:25 A . (.Microsoft Corporation - Windows Trusted
Runtime Service Proxy Drive.) -- C:\WINDOWS\System32\drivers\
WindowsTrustedRTProxy.sys [54784] =>.Microsoft@

058 - SDL:2022/05/07 07:20:16 A . (.Microsoft Corporation - Windows Hypervisor
Interface Driver.) -- C:\WINDOWS\System32\drivers\winhiv.sys [75096]
=>.Microsoft@

058 - SDL:2022/10/16 11:27:04 A . (.Microsoft Corporation - Windows Hypervisor
Root Interface Driver.) -- C:\WINDOWS\System32\drivers\winhvr.sys [152928]
=>.Microsoft@

058 - SDL:2022/05/07 07:19:04 A . (.Mellanox - Kernel WinMad.) -- C:\WINDOWS\
System32\drivers\winmad.sys [37224] =>.Microsoft@

058 - SDL:2022/10/16 11:25:57 A . (.Microsoft Corporation - Windows NAT Driver.)
-- C:\WINDOWS\System32\drivers\winnat.sys [307168] =>.Microsoft@

058 - SDL:2022/10/16 11:42:09 A . (.Microsoft Corporation - SetupPlatform NEO
Mini-Filter.) -- C:\WINDOWS\System32\drivers\WinSetupBoot.sys [111960]
=>.Microsoft@

058 - SDL:2022/10/16 11:26:21 A . (.Microsoft Corporation - Windows WinUSB Class
Driver.) -- C:\WINDOWS\System32\drivers\winusb.sys [139264] [Unsigned]
=>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:04 A . (.Mellanox - Kernel WinVerbs.) -- C:\WINDOWS\
System32\drivers\winverbs.sys [74096] =>.Microsoft@

058 - SDL:2022/05/07 07:19:05 A . (.Microsoft Corporation - Windows Management
Interface for ACPI.) -- C:\WINDOWS\System32\drivers\wmiacpi.sys [53248]
[Unsigned] =>.Microsoft Corporation

058 - SDL:2022/05/07 07:19:30 A . (.Microsoft Corporation - WMILIB WMI support
library Dll.) -- C:\WINDOWS\System32\drivers\wmilib.sys [58704] =>.Microsoft@

058 - SDL:2022/05/07 07:19:34 A . (.Microsoft Corporation - Windows Overlay
Filter.) -- C:\WINDOWS\System32\drivers\wof.sys [283992] =>.Microsoft@

058 - SDL:2022/05/07 08:10:26 A . (.Microsoft Corporation - Windows Portable
Device Upper Class Filter.) -- C:\WINDOWS\System32\drivers\WpdUpFltr.sys
[71000] =>.Microsoft@

058 - SDL:2022/05/07 07:19:30 A . (.Microsoft Corporation - WPP Trace Recorder.)
-- C:\WINDOWS\System32\drivers\WppRecorder.sys [87384] =>.Microsoft@

058 - SDL:2022/05/07 07:19:29 A . (.Microsoft Corporation - Winsock2 IFS Layer.)
-- C:\WINDOWS\System32\drivers\ws2ifsl.sys [57344] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:27:04 A . (.Microsoft Corporation - WTD Driver.) -- C:\WINDOWS\System32\drivers\wtd.sys [118784] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:29 A . (.Microsoft Corporation - Windows Driver Foundation - User-mode Drive.) -- C:\WINDOWS\System32\drivers\WUDFPf.sys [167936] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:29 A . (.Microsoft Corporation - Windows Driver Foundation - User-mode Drive.) -- C:\WINDOWS\System32\drivers\WUDFRd.sys [352256] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:25:57 A . (.Microsoft Corporation - Game Input Protocol Driver.) -- C:\WINDOWS\System32\drivers\xboxgip.sys [393216] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:00 A . (.Microsoft Corporation - XINPUT filter driver for HID.) -- C:\WINDOWS\System32\drivers\xinputhid.sys [81920] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:19 A . (.Microsoft Corporation - Multi-User Win32 Driver.) -- C:\WINDOWS\System32\win32k.sys [688128] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:17 A . (.Microsoft Corporation - Base Win32k Kernel Driver.) -- C:\WINDOWS\System32\win32kbase.sys [3575808] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/10/16 11:26:19 A . (.Microsoft Corporation - Full/Desktop Win32k Kernel Driver.) -- C:\WINDOWS\System32\win32kfull.sys [3821568] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:23 A . (.Microsoft Corporation - Win32k non session driver.) -- C:\WINDOWS\System32\win32kns.sys [69632] [Unsigned] =>.Microsoft Corporation
058 - SDL:2022/05/07 07:19:23 A . (.Microsoft Corporation - Win32k temporary session global driver.) -- C:\WINDOWS\System32\win32ksgd.sys [49152] [Unsigned] =>.Microsoft Corporation

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

067 - Shell Spawning: <.bat> [HKLM\...\open\Command] (...) -- '%1' %* =>.Default.Value
067 - Shell Spawning: <.cpl> [HKLM\...\cplopen\Command] (.Microsoft Corporation - Windows Control Panel.) -- C:\Windows\System32\control.exe [Unsigned] =>.Microsoft Corporation
067 - Shell Spawning: <.cmd> [HKLM\...\open\Command] (...) -- '%1' %* =>.Default.Value
067 - Shell Spawning: <.com> [HKLM\...\open\Command] (...) -- '%1' %* =>.Default.Value
067 - Shell Spawning: <.evt> [HKLM\...\open\Command] (.Microsoft Corporation - Event Viewer Snapin Launcher.) -- C:\Windows\System32\eventvwr.exe [Unsigned] =>.Microsoft Corporation
067 - Shell Spawning: <.exe> [HKLM\...\open\Command] (...) -- '%1' %* =>.Default.Value
067 - Shell Spawning: <.html> [HKLM\...\open\Command] (.Microsoft Corporation - Internet Explorer.) -- C:\Program Files\Internet Explorer\iexplore.exe =>.Microsoft@
067 - Shell Spawning: <.js> [HKLM\...\open\Command] (...) -- C:\Windows\System32\WScript.exe '%1' %* =>.Default.Value
067 - Shell Spawning: <.reg> [HKLM\...\open\Command] (.Microsoft Corporation - Registry Editor.) -- C:\Windows\regedit.exe [Unsigned] =>.Microsoft Corporation
067 - Shell Spawning: <.scr> [HKLM\...\open\Command] (...) -- '%1' /S =>.Default.Value

---\ Start Menu Internet (12) - 0s

068 - StartMenuInternet: [64Bits][HKLM\...\Shell\open\Command] (.Google LLC - Google Chrome.) -- C:\Program Files (x86)\Google\Chrome\Application\chrome.exe =>.Google LLC@

068 - StartMenuInternet: [64Bits][HKLM\...\Shell\open\Command] (.Microsoft Corporation - Internet Explorer.) -- C:\Program Files\Internet Explorer\iexplore.exe =>.Microsoft®
068 - StartMenuInternet: [64Bits][HKLM\...\Shell\open\Command] (.Microsoft Corporation - Microsoft Edge.) -- C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe =>.Microsoft®
068 - StartMenuInternet: [64Bits][HKLM\...\InstallInfo\ShowIconsCommand] (.Google LLC - Google Chrome.) -- C:\Program Files (x86)\Google\Chrome\Application\chrome.exe =>.Google LLC
068 - StartMenuInternet: [64Bits][HKLM\...\InstallInfo\ShowIconsCommand] (.Microsoft Corporation - IE Per-User Show IE Icon Utility.) -- C:\WINDOWS\System32\ie4ushowIE.exe =>.Microsoft Corporation
068 - StartMenuInternet: [64Bits][HKLM\...\InstallInfo\ShowIconsCommand] (.Microsoft Corporation - Microsoft Edge.) -- C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe =>.Microsoft Corporation
068 - StartMenuInternet: [64Bits][HKLM\...\InstallInfo\ReinstallCommand] (.Google LLC - Google Chrome.) -- C:\Program Files (x86)\Google\Chrome\Application\chrome.exe =>.Google LLC
068 - StartMenuInternet: [64Bits][HKLM\...\InstallInfo\ReinstallCommand] (.Microsoft Corporation - IE Per-User Initialization Utility.) -- C:\Windows\System32\ie4uinit.exe =>.Microsoft Corporation
068 - StartMenuInternet: [64Bits][HKLM\...\InstallInfo\ReinstallCommand] (.Microsoft Corporation - Microsoft Edge.) -- C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe =>.Microsoft Corporation
068 - StartMenuInternet: [64Bits][HKLM\...\InstallInfo\HideIconsCommand] (.Google LLC - Google Chrome.) -- C:\Program Files (x86)\Google\Chrome\Application\chrome.exe =>.Google LLC
068 - StartMenuInternet: [64Bits][HKLM\...\InstallInfo\HideIconsCommand] (.Microsoft Corporation - IE Per-User Show IE Icon Utility.) -- C:\WINDOWS\System32\ie4ushowIE.exe =>.Microsoft Corporation
068 - StartMenuInternet: [64Bits][HKLM\...\InstallInfo\HideIconsCommand] (.Microsoft Corporation - Microsoft Edge.) -- C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe =>.Microsoft Corporation

---\ Search Browser Infection (4) - 4s

069 - SBI: SearchScopes [HKCU] [64Bits]{0633EE93-D776-472f-A0FF-E1416B8B2E3A} - (Bing) - http://www.bing.com/ =>.Bing.com
069 - SBI: SearchScopes [HKCU] [64Bits]{C235EA63-A6EE-4908-8B9E-AFB559864A25} [DefaultScope] - () - http://www.bing.com/ =>.Bing.com
069 - SBI: SearchScopes [HKLM] [64Bits]{0633EE93-D776-472f-A0FF-E1416B8B2E3A} - (@iframe.dll, -12512) - http://www.bing.com/ =>.Bing.com
069 - SBI: SearchScopes [HKLM] [64Bits]{C235EA63-A6EE-4908-8B9E-AFB559864A25} [DefaultScope] - (Bing) - http://www.bing.com/ =>.Bing.com

---\ Search Svchost Services (49) - 2s

083 - Search Svchost Services: lanmanserver (lanmanserver) . (.Microsoft Corporation - Server Service DLL.) -- C:\WINDOWS\System32\svrsvc.dll [344064] [Unsigned] =>.Microsoft Corporation
083 - Search Svchost Services: gpsvc (gpsvc) . (.Microsoft Corporation - Group Policy Client.) -- C:\Windows\System32\gpsvc.dll [1359872] [Unsigned] =>.Microsoft Corporation
083 - Search Svchost Services: IKEEXT (IKEEXT) . (.Microsoft Corporation - IKE extension.) -- C:\Windows\System32\IKEEXT.DLL [1531904] [Unsigned] =>.Microsoft Corporation
083 - Search Svchost Services: iphlpsvc (iphlpvc) . (.Microsoft Corporation - Service that offers IPV6 connectivity over.) -- C:\Windows\System32\iphlpvc.dll [843776] [Unsigned] =>.Microsoft Corporation
083 - Search Svchost Services: seclogon (seclogon) . (.Microsoft Corporation - Secondary Logon Service DLL.) -- C:\Windows\System32\seclogon.dll [57344] [Unsigned] =>.Microsoft Corporation
083 - Search Svchost Services: msiscsi (msiscsi) . (.Microsoft Corporation - iSCSI Discovery service.) -- C:\Windows\System32\iscsiexe.dll [176128] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: EapHost (EapHost) . (.Microsoft Corporation - Microsoft EAPHost service.) -- C:\Windows\System32\eapsvc.dll [122880] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: schedule (schedule) . (.Microsoft Corporation - Task Scheduler Service.) -- C:\Windows\System32\schedsvc.dll [815104] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: winmgmt (winmgmt) . (.Microsoft Corporation - WMI.) -- C:\Windows\System32\wbem\WMIsvc.dll [245760] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: SessionEnv (SessionEnv) . (.Microsoft Corporation - Remote Desktop Configuration service.) -- C:\Windows\System32\SessEnv.dll [598016] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: wercplsupport (wercplsupport) . (.Microsoft Corporation - Problem Reports.) -- C:\Windows\System32\wercplsupport.dll [102400] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: wlidsvc (wlidsvc) . (.Microsoft Corporation - Microsoft® Account Service.) -- C:\Windows\System32\wlidsvc.dll [2052096] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: UserManager (UserManager) . (.Microsoft Corporation - UserMgr.) -- C:\Windows\System32\usermgr.dll [1425408] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: NaturalAuthentication (NaturalAuthentication) . (.Microsoft Corporation - Natural Authentication Service.) -- C:\Windows\System32\NaturalAuth.dll [434176] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: Themes (Themes) . (.Microsoft Corporation - Windows Shell Theme Service DLL.) -- C:\Windows\System32\themeservice.dll [114688] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: XblAuthManager (XblAuthManager) . (.Microsoft Corporation - Xbox Live Auth Manager.) -- C:\Windows\System32\XblAuthManager.dll [1044480] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: DmEnrollmentSvc (DmEnrollmentSvc) . (.Microsoft Corporation - Windows Managent Service DLL.) -- C:\Windows\System32\Windows.Internal.Management.dll [1187840] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: XblGameSave (XblGameSave) . (.Microsoft Corporation - Xbox Live Game Save Service.) -- C:\Windows\System32\XblGameSave.dll [1040384] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: TokenBroker (TokenBroker) . (.Microsoft Corporation - Token Broker.) -- C:\Windows\System32\TokenBroker.dll [1810432] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: lfsvc (lfsvc) . (.Microsoft Corporation - Geolocation Service.) -- C:\Windows\System32\lfsvc.dll [69632] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: shpamsvc (shpamsvc) . (.Microsoft Corporation - SharedPC.AccountManager.) -- C:\Windows\System32\Windows.SharedPC.AccountManager.dll [241664] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: Rasauto (Rasauto) . (.Microsoft Corporation - Remote Access AutoDial Manager.) -- C:\Windows\System32\rasauto.dll [135168] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: Rasman (Rasman) . (.Microsoft Corporation - Remote Access Connection Manager.) -- C:\Windows\System32\rasmans.dll [1101824] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: Remoteaccess (Remoteaccess) . (.Microsoft Corporation - Dynamic Interface Manager.) -- C:\Windows\System32\mprdim.dll [512000] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: SENS (SENS) . (.Microsoft Corporation - System Event Notification Service (SENS).) -- C:\Windows\System32\Sens.dll [98304] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: Sharedaccess (Sharedaccess) . (.Microsoft Corporation - Microsoft NAT Helper Components.) -- C:\Windows\System32\ipnathlp.dll [683168] =>.Microsoft®

083 - Search Svchost Services: Tapisrv (Tapisrv) . (.Microsoft Corporation - Microsoft® Windows(TM) Telephony Server.) -- C:\Windows\System32\tapisrv.dll [335872] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: wuauerv (wuauerv) . (.Microsoft Corporation - Windows Update Shell DLL - Docked.) -- C:\Windows\System32\wuauerv.dll [137544] =>.Microsoft@

083 - Search Svchost Services: BITS (BITS) . (.Microsoft Corporation - Background Intelligent Transfer Service.) -- C:\Windows\System32\qmgr.dll [1388544] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: ShellHWDetection (ShellHWDetection) . (.Microsoft Corporation - Windows Shell Services DLL.) -- C:\Windows\System32\shsvcs.dll [270336] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: dmwappushservice (dmwappushservice) . (.Microsoft Corporation - dmwappushsvc.) -- C:\Windows\System32\dmwappushsvc.dll [143360] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: wisvc (wisvc) . (.Microsoft Corporation - Flight Settings.) -- C:\Windows\System32\flightsettings.dll [1013728] =>.Microsoft@

083 - Search Svchost Services: WManSvc (WManSvc) . (.Microsoft Corporation - Windows Management Service DLL.) -- C:\Windows\System32\Windows.Management.Service.dll [1245184] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: WpnService (WpnService) . (.Microsoft Corporation - Windows Push Notification System Service.) -- C:\Windows\System32\WpnService.dll [266240] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: XboxNetApiSvc (XboxNetApiSvc) . (.Microsoft Corporation - Xbox Live Networking Service.) -- C:\Windows\System32\XboxNetApiSvc.dll [1392640] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: UsoSvc (UsoSvc) . (.Microsoft Corporation - Update Session Orchestrator Service.) -- C:\Windows\System32\usosvc.dll [102400] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: NetSetupSvc (NetSetupSvc) . (.Microsoft Corporation - Network Setup Service.) -- C:\Windows\System32\NetSetupSvc.dll [315392] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: InstallService (InstallService) . (.Microsoft Corporation - InstallService.) -- C:\Windows\System32\InstallService.dll [2781184] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: LxpSvc (LxpSvc) . (.Microsoft Corporation - Provides infrastructure support for deployi.) -- C:\Windows\System32\LanguageOverlayServer.dll [552960] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: TroubleshootingSvc (TroubleshootingSvc) . (.Microsoft Corporation - MitigationClient.) -- C:\Windows\System32\MitigationClient.dll [507904] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: DsmSvc (DsmSvc) . (.Microsoft Corporation - Device Setup Manager.) -- C:\Windows\System32\DeviceSetupManager.dll [299008] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: DcSvc (DcSvc) . (.Microsoft Corporation - dcsvc.) -- C:\Windows\System32\dcsvc.dll [802816] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: NcaSvc (NcaSvc) . (.Microsoft Corporation - Microsoft Network Connectivity Assistant Se.) -- C:\Windows\System32\NcaSvc.dll [188416] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: AppInfo (AppInfo) . (.Microsoft Corporation - Application Information Service.) -- C:\Windows\System32\appinfo.dll [294912] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: XboxGipSvc (XboxGipSvc) . (.Microsoft Corporation - Xbox Gip Management Service.) -- C:\Windows\System32\XboxGipSvc.dll [131072] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: PushToInstall (PushToInstall) . (.Microsoft Corporation - PushToInstall.) -- C:\Windows\System32\PushToInstall.dll [425984] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: CertPropSvc (CertPropSvc) . (.Microsoft Corporation - Microsoft Smartcard Certificate Propagation.) -- C:\Windows\System32\certprop.dll [221184] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: SCPolicySvc (SCPolicySvc) . (.Microsoft Corporation - Microsoft Smartcard Certificate Propagation.) -- C:\Windows\System32\certprop.dll [221184] [Unsigned] =>.Microsoft Corporation

083 - Search Svchost Services: BDESVC (BDESVC) . (.Microsoft Corporation - BDE Service.) -- C:\Windows\System32\bdesvc.dll [647168] [Unsigned] =>.Microsoft Corporation

---\ Firewall Active Exception List (71) - 8s

087 - FAEL: 'UDP Query User{98233D13-0699-47C4-96EC-676A7218E22C}C:\program files (x86)\epic games\launcher\engine\binaries\win64\epicwebhelper.exe' [In-None-P17-TRUE] (.Epic Games, Inc. - EpicWebHelper.) -- C:\program files (x86)\epic games\launcher\engine\binaries\win64\epicwebhelper.exe =>.Epic Games Inc.®

087 - FAEL: 'TCP Query User{E1F4DE95-FF9A-4B17-B07A-4F79785A46D0}C:\program files (x86)\epic games\launcher\engine\binaries\win64\epicwebhelper.exe' [In-None-P6-TRUE] (.Epic Games, Inc. - EpicWebHelper.) -- C:\program files (x86)\epic games\launcher\engine\binaries\win64\epicwebhelper.exe =>.Epic Games Inc.®

087 - FAEL: '{3C99A206-29D6-4E94-8D99-A00A7CBFEBD4}' [In-None-P17-TRUE] (...) -- C:\Users\User\AppData\Local\Programs\Opera\91.0.4516.77\opera.exe [Unsigned] (.not file.) =>.SUP.Orphan

087 - FAEL: '{AA327031-1DB6-4493-ABEC-2636F86A803C}' [Out-None-P17-TRUE] (.Skype Technologies S.A. - Skype.) -- C:\Program Files\WindowsApps\Microsoft.SkypeApp_15.89.3403.0_x86__kzf8qxf38zg5c\Skype\Skype.exe =>.Skype Software Sarl®

087 - FAEL: '{111428B2-43F5-40F0-9D2E-4E1C2C9D1687}' [In-None-P17-TRUE] (.Skype Technologies S.A. - Skype.) -- C:\Program Files\WindowsApps\Microsoft.SkypeApp_15.89.3403.0_x86__kzf8qxf38zg5c\Skype\Skype.exe =>.Skype Software Sarl®

087 - FAEL: '{93387A9F-75C6-4665-A095-5A22F8555FDD}' [Out-None-P6-TRUE] (.Skype Technologies S.A. - Skype.) -- C:\Program Files\WindowsApps\Microsoft.SkypeApp_15.89.3403.0_x86__kzf8qxf38zg5c\Skype\Skype.exe =>.Skype Software Sarl®

087 - FAEL: '{F44359E6-D1BD-482E-8DD8-55AEEED511D0}' [In-None-P6-TRUE] (.Skype Technologies S.A. - Skype.) -- C:\Program Files\WindowsApps\Microsoft.SkypeApp_15.89.3403.0_x86__kzf8qxf38zg5c\Skype\Skype.exe =>.Skype Software Sarl®

087 - FAEL: '{E1A343FA-88F3-4014-A0F5-1915A5A72090}' [In-None-P6-TRUE] (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe =>.Dropbox, Inc®

087 - FAEL: '{6ACFAAE1-016A-438D-8CD1-C0812A8E4AD2}' [In-None-P17-TRUE] (...) -- C:\Users\User\AppData\Local\Programs\Opera\87.0.4390.45\opera.exe [Unsigned] (.not file.) =>.SUP.Orphan

087 - FAEL: '{72DBEA5C-2E15-4CA6-904E-EF3CDF6043DF}' [In-None-P17-TRUE] (...) -- C:\Users\User\AppData\Local\Programs\Opera\87.0.4390.36\opera.exe [Unsigned] (.not file.) =>.SUP.Orphan

087 - FAEL: 'UDP Query User{5A04C3B2-071F-4881-9D4A-110753BB659C}C:\users\user\desktop\jeux\rogue legacy 2\rogue legacy 2.exe' [In-None-P17-TRUE] (...) -- C:\users\user\desktop\jeux\rogue legacy 2\rogue legacy 2.exe [Unsigned]

087 - FAEL: 'TCP Query User{A9F20A98-F546-40DA-BD11-9CF41BE1679D}C:\users\user\desktop\jeux\rogue legacy 2\rogue legacy 2.exe' [In-None-P6-TRUE] (...) -- C:\users\user\desktop\jeux\rogue legacy 2\rogue legacy 2.exe [Unsigned]

087 - FAEL: '{F1055660-3EC4-40A8-B30A-1C9FFC0E1B}' [In-None-P6-TRUE] (...) -- C:\Program Files\BlueStacks_nxt\HD-Player.exe [Unsigned] (.not file.) =>.SUP.Orphan

087 - FAEL: '{242B0829-B575-47CF-A5F0-EF7D8AFB3F08}' [In-None-P6-TRUE] (...) -- C:\Program Files (x86)\BlueStacks X\Cloud Game.exe [Unsigned] (.not file.) =>.SUP.Orphan

087 - FAEL: '{52ECBB19-C1C6-4E71-AC37-343FC38B4D2E}' [In-None-P6-TRUE] (...) -- C:\Program Files (x86)\BlueStacks X\BlueStacksWeb.exe [Unsigned] (.not file.) =>.SUP.Orphan

087 - FAEL: 'UDP Query User{E9C05E2A-AE37-41C2-80DE-65A7274D8826}C:\users\user\desktop\rogue legacy 2\rogue legacy 2.exe' [In-None-P17-TRUE] (...) -- C:\users\user\desktop\rogue legacy 2\rogue legacy 2.exe [Unsigned] (.not file.) =>.SUP.Orphan

087 - FAEL: 'TCP Query User{A8060F24-039B-4EC7-A655-4B20C475D21F}C:\users\user\desktop\rogue legacy 2\rogue legacy 2.exe' [In-None-P6-TRUE] (...) -- C:\users\user\desktop\rogue legacy 2\rogue legacy 2.exe [Unsigned] (.not file.) =>.SUP.Orphan

087 - FAEL: 'UDP Query User{D6A49CD9-28A3-48ED-A025-D2A490967092}C:\users\user\desktop\rogue.legacy.2\rogue legacy 2\rogue legacy 2.exe' [In-None-P17-TRUE] .

```
(...) -- C:\users\user\desktop\rogue.legacy.2\rogue legacy 2\rogue legacy 2.exe
[Unsigned] (.not file.) =>.SUP.Orphan
087 - FAEL: 'TCP Query User{33AD10A0-0697-4E37-BCA6-516C9343FCBB}C:\users\user\
desktop\rogue.legacy.2\rogue legacy 2\rogue legacy 2.exe' [In-None-P6-TRUE] .
(...) -- C:\users\user\desktop\rogue.legacy.2\rogue legacy 2\rogue legacy 2.exe
[Unsigned] (.not file.) =>.SUP.Orphan
087 - FAEL: 'UDP Query User{23ECEF9D-0F58-402D-8BD2-2C4DE9FCDB5}C:\games\the
sims 4\game\bin\ts4_x64.exe' [In-None-P17-TRUE] (...) -- C:\games\the sims 4\
game\bin\ts4_x64.exe [Unsigned] (.not file.) =>.SUP.Orphan
087 - FAEL: 'TCP Query User{4A6AA747-629B-481D-B1F1-18FED1DD1B24}C:\games\the
sims 4\game\bin\ts4_x64.exe' [In-None-P6-TRUE] (...) -- C:\games\the sims 4\
game\bin\ts4_x64.exe [Unsigned] (.not file.) =>.SUP.Orphan
087 - FAEL: '{8B4F51B4-5EC4-4A7B-A46E-E4FB0CECAE0A}' [In-None-P17-TRUE] (...)
-- C:\Program Files (x86)\Steam\steamapps\common\Dome Romantik Demo\
domeromantik.exe [Unsigned] (.not file.) =>.Steam Games
087 - FAEL: '{A1A0D898-1538-4953-A270-9A530660228B}' [In-None-P6-TRUE] (...) --
C:\Program Files (x86)\Steam\steamapps\common\Dome Romantik Demo\
domeromantik.exe [Unsigned] (.not file.) =>.Steam Games
087 - FAEL: '{328FE6FA-EDD4-4FAC-B95C-37AF8D94710B}' [In-None-P17-TRUE] (...)
-- C:\Program Files (x86)\Steam\steamapps\common\This War of Mine\
Storyteller.exe [Unsigned] (.not file.) =>.Steam Games
087 - FAEL: '{D16B04F2-C833-4CF4-81D8-5E2B7D2661B4}' [In-None-P6-TRUE] (...) --
C:\Program Files (x86)\Steam\steamapps\common\This War of Mine\Storyteller.exe
[Unsigned] (.not file.) =>.Steam Games
087 - FAEL: '{BC6B7099-405F-4436-90BA-4836CE56509D}' [In-None-P17-TRUE] (...)
-- C:\Program Files (x86)\Steam\steamapps\common\This War of Mine\This War of
Mine.exe [Unsigned] (.not file.) =>.Steam Games
087 - FAEL: '{2E173AE8-5C33-486C-AE86-35F5B6A0B273}' [In-None-P6-TRUE] (...) --
C:\Program Files (x86)\Steam\steamapps\common\This War of Mine\This War of
Mine.exe [Unsigned] (.not file.) =>.Steam Games
087 - FAEL: 'UDP Query User{C3DE7739-52A7-4C96-99B3-A7C3BE7013CD}F:\vuze\
anno.1800.complete.edition.uplay.rip-insaneramzes\anno 1800\bin\win64\
anno1800.exe' [In-None-P17-TRUE] (...) -- F:\vuze\
anno.1800.complete.edition.uplay.rip-insaneramzes\anno 1800\bin\win64\
anno1800.exe [Unsigned] (.not file.) =>.SUP.Orphan
087 - FAEL: 'TCP Query User{914D7B97-552D-468D-A1DC-73F73C70F6C6}F:\vuze\
anno.1800.complete.edition.uplay.rip-insaneramzes\anno 1800\bin\win64\
anno1800.exe' [In-None-P6-TRUE] (...) -- F:\vuze\
anno.1800.complete.edition.uplay.rip-insaneramzes\anno 1800\bin\win64\
anno1800.exe [Unsigned] (.not file.) =>.SUP.Orphan
087 - FAEL: '{8BEE0A2A-C101-456D-B833-7203008870DA}' [In-None-P17-TRUE] (...)
-- C:\Program Files (x86)\Steam\steamapps\common\Vampire Survivors\
VampireSurvivors.exe [Unsigned] (.not file.) =>.Steam Games
087 - FAEL: '{9B3AD033-B053-426C-B325-C5D780CA2EF3}' [In-None-P6-TRUE] (...) --
C:\Program Files (x86)\Steam\steamapps\common\Vampire Survivors\
VampireSurvivors.exe [Unsigned] (.not file.) =>.Steam Games
087 - FAEL: '{6065A769-F831-4F66-8217-B99EC5CD5D0C}' [In-None-P17-TRUE] (...)
-- C:\Program Files (x86)\Steam\bin\cef\cef.win7x64\steamwebhelper.exe
[Unsigned] (.not file.) =>.SUP.Orphan
087 - FAEL: '{36BF55B9-0848-4990-BA72-279627CD2EB2}' [In-None-P6-TRUE] (...) --
C:\Program Files (x86)\Steam\bin\cef\cef.win7x64\steamwebhelper.exe [Unsigned]
(.not file.) =>.SUP.Orphan
087 - FAEL: '{1E4AC171-54B5-43B7-94E9-9C40829B6CCF}' [In-None-P17-TRUE] (...)
-- C:\Program Files (x86)\Steam\Steam.exe [Unsigned] (.not file.) =>.SUP.Orphan
087 - FAEL: '{98815E43-A15E-45FA-A4C6-AAE96F2E2A4D}' [In-None-P6-TRUE] (...) --
C:\Program Files (x86)\Steam\Steam.exe [Unsigned] (.not file.) =>.SUP.Orphan
087 - FAEL: '{DD311BDA-5E52-4BC8-A72F-3ADC57D12A15}' [In-None-P17-TRUE] (.Zoom
Video Communications, Inc. - AirHost.) -- C:\Users\User\AppData\Roaming\Zoom\
bin_00\airhost.exe =>.Zoom Video Communications, Inc.®
087 - FAEL: '{578B778B-D473-436E-B538-14D690FD72EC}' [In-None-P6-TRUE] (.Zoom
Video Communications, Inc. - AirHost.) -- C:\Users\User\AppData\Roaming\Zoom\
bin_00\airhost.exe =>.Zoom Video Communications, Inc.®
```


087 - FAEL: '{69FA6E83-0242-42DC-ADCF-53ED8F50BC73}' [In-None-P17-TRUE] (.Zoom Video Communications, Inc. - Zoom Meetings.) -- C:\Users\User\AppData\Roaming\Zoom\bin_00\Zoom.exe =>.Zoom Video Communications, Inc.®

087 - FAEL: 'UDP Query User{538B1141-58E3-4EC6-8429-8628B3214B0B}C:\users\user\appdata\local\programs\opera\opera.exe' [In-None-P17-TRUE] (...) -- C:\users\user\appdata\local\programs\opera\opera.exe [Unsigned] (.not file.) =>.SUP.Orphan

087 - FAEL: 'TCP Query User{B547BC4B-6A65-4C24-89CD-20E29EE19F25}C:\users\user\appdata\local\programs\opera\opera.exe' [In-None-P6-TRUE] (...) -- C:\users\user\appdata\local\programs\opera\opera.exe [Unsigned] (.not file.) =>.SUP.Orphan

087 - FAEL: 'UDP Query User{984300C6-B849-4031-8EED-A47B4F39C841}C:\users\user\appdata\local\programs\opera\opera.exe' [In-None-P17-TRUE] (...) -- C:\users\user\appdata\local\programs\opera\opera.exe [Unsigned] (.not file.) =>.SUP.Orphan

087 - FAEL: 'TCP Query User{3FD3711C-C19D-40F6-903E-1404B42473DE}C:\users\user\appdata\local\programs\opera\opera.exe' [In-None-P6-TRUE] (...) -- C:\users\user\appdata\local\programs\opera\opera.exe [Unsigned] (.not file.) =>.SUP.Orphan

087 - FAEL: 'UDP Query User{E46F18C7-79E6-4282-9933-722251F5CB74}C:\program files (x86)\windscribe\wsappcontrol.exe' [In-None-P17-TRUE] (.Windscribe Limited - Windscribe auto-login utility.) -- C:\program files (x86)\windscribe\wsappcontrol.exe =>.Windscribe Limited®

087 - FAEL: 'TCP Query User{E48A34E6-2709-4EC4-A7FD-B5EF16B3EEE3}C:\program files (x86)\windscribe\wsappcontrol.exe' [In-None-P6-TRUE] (.Windscribe Limited - Windscribe auto-login utility.) -- C:\program files (x86)\windscribe\wsappcontrol.exe =>.Windscribe Limited®

087 - FAEL: 'UDP Query User{1E8A17E5-DBFF-4A4E-B466-6454F2BD2181}C:\program files\vuze\azureus.exe' [In-None-P17-TRUE] (.Azureus Software, Inc - Vuze Launcher.) -- C:\program files\vuze\azureus.exe =>.Azureus Software, Inc.®

087 - FAEL: 'TCP Query User{C313FEC8-B546-4FB7-A0EA-06157D7AEC0E}C:\program files\vuze\azureus.exe' [In-None-P6-TRUE] (.Azureus Software, Inc - Vuze Launcher.) -- C:\program files\vuze\azureus.exe =>.Azureus Software, Inc.®

087 - FAEL: 'UDP Query User{81968090-998D-466D-BD12-D9FC0A84071C}C:\program files (x86)\hearthstone\hearthstone.exe' [In-None-P17-TRUE] (...) -- C:\program files (x86)\hearthstone\hearthstone.exe =>.Blizzard Entertainment, Inc.®

087 - FAEL: 'TCP Query User{B6402BE7-8C97-4821-8AA0-213BD1484953}C:\program files (x86)\hearthstone\hearthstone.exe' [In-None-P6-TRUE] (...) -- C:\program files (x86)\hearthstone\hearthstone.exe =>.Blizzard Entertainment, Inc.®

087 - FAEL: 'UDP Query User{B87E5E90-EDBA-46E5-A2DA-8838C3797F46}C:\program files (x86)\hearthstone\hearthstone.exe' [In-None-P17-TRUE] (...) -- C:\program files (x86)\hearthstone\hearthstone.exe =>.Blizzard Entertainment, Inc.®

087 - FAEL: 'TCP Query User{B994B126-8C9C-478A-A050-070C24593B06}C:\program files (x86)\hearthstone\hearthstone.exe' [In-None-P6-TRUE] (...) -- C:\program files (x86)\hearthstone\hearthstone.exe =>.Blizzard Entertainment, Inc.®

087 - FAEL: '{4629731F-B6E4-4C60-99C7-A62AA1A1D88F}' [In-None-P6-TRUE] (.Garena Online - Garena platform service.) -- C:\Program Files (x86)\Garena\Garena\2.0.1909.2618\gxxsvc.exe {46A0800C34C5FEE85DB1758D556C2D0E}. =>.Garena Online

087 - FAEL: '{40A29EFE-D079-4EBD-B53A-79B41408408E}' [In-None-P6-TRUE] (.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe =>.Nvidia Corporation®

087 - FAEL: '{15314422-02D7-4DDF-A2EF-E5C5D996A71B}' [In-None-P17-TRUE] (.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe =>.Nvidia Corporation®

087 - FAEL: '{5A268CD9-9D4B-4E52-8D1B-BCCD87896017}' [In-None-P6-TRUE] (.Azureus Software, Inc - Vuze Launcher.) -- C:\Program Files\Vuze\Azureus.exe =>.Azureus Software, Inc.®

087 - FAEL: '{51E0787F-5C3B-49F2-89F0-AB5651C91038}' [In-None-P17-TRUE] (.Azureus Software, Inc - Vuze Launcher.) -- C:\Program Files\Vuze\Azureus.exe =>.Azureus Software, Inc.®

087 - FAEL: 'TCP Query User{814EFF39-D1B3-44FD-965D-8E8EFD1A412F}C:\users\user\desktop\jeux\loop hero\loop hero.exe' [In-None-P6-TRUE] (.FourQuarters team - Loop Hero.) -- C:\users\user\desktop\jeux\loop hero\loop hero.exe [Unsigned]

087 - FAEL: 'UDP Query User{D3B42729-B253-4D58-ADC4-D78C9D2AFAFB}C:\users\user\desktop\jeux\loop hero\loop hero.exe' [In-None-P17-TRUE] (.FourQuarters team - Loop Hero.) -- C:\users\user\desktop\jeux\loop hero\loop hero.exe [Unsigned]
087 - FAEL: 'TCP Query User{4FC7A377-FD17-44E0-9CD1-38D20E6FD94E}E:\usbhelper\usbhelperlauncher.exe' [In-None-P6-TRUE] (...) -- E:\usbhelper\usbhelperlauncher.exe [Unsigned]
087 - FAEL: 'UDP Query User{DC3FD3FC-6CFD-4E9D-853B-4EC23872F1AE}E:\usbhelper\usbhelperlauncher.exe' [In-None-P17-TRUE] (...) -- E:\usbhelper\usbhelperlauncher.exe [Unsigned]
087 - FAEL: 'TCP Query User{4B66CFE5-2391-453D-83F0-D4EF8F3B8D6D}E:\usbhelper\wiiu_usb_helper_.exe' [In-None-P6-TRUE] (.Hikari06 - Wii U USB Helper.) -- E:\usbhelper\wiiu_usb_helper_.exe [Unsigned]
087 - FAEL: 'UDP Query User{AB0991BD-A873-49AA-9CB0-F929A2F932C6}E:\usbhelper\wiiu_usb_helper_.exe' [In-None-P17-TRUE] (.Hikari06 - Wii U USB Helper.) -- E:\usbhelper\wiiu_usb_helper_.exe [Unsigned]
087 - FAEL: 'TCP Query User{41A203E7-3402-4902-B524-ACEAEBC065DB}C:\users\user\desktop\jeux\there is no game wrong dimension v16.08.2020\ting.exe' [In-None-P6-TRUE] (...) -- C:\users\user\desktop\jeux\there is no game wrong dimension v16.08.2020\ting.exe [Unsigned]
087 - FAEL: 'UDP Query User{4304EE52-7D6E-441D-B707-AB3495EB2010}C:\users\user\desktop\jeux\there is no game wrong dimension v16.08.2020\ting.exe' [In-None-P17-TRUE] (...) -- C:\users\user\desktop\jeux\there is no game wrong dimension v16.08.2020\ting.exe [Unsigned]
087 - FAEL: '{06F1890A-A784-4DE8-BF54-A40C308D3FA9}' [In-None-P6-TRUE] . (.CybelSoft - DriversCloud.com start detection.) -- C:\Program Files\Cybelsoft\DriversCloud.com\DriversCloud.exe =>.CYBELSOFT®
087 - FAEL: '{5BBC1D98-8F55-49EA-B06C-202DCDEC51C1}' [In-None-P17-TRUE] . (.CybelSoft - DriversCloud.com start detection.) -- C:\Program Files\Cybelsoft\DriversCloud.com\DriversCloud.exe =>.CYBELSOFT®
087 - FAEL: '{45A37C38-137C-4DF7-8FD1-863CF1B9D3B8}' [In-None-P17-TRUE] . (.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe =>.Nvidia Corporation®
087 - FAEL: '{E9E1D3A4-CCB3-4951-AF9A-6EFAF12A6D12}' [In-None-P17-TRUE] . (.NVIDIA Corporation - NVIDIA Container.) -- C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe =>.Nvidia Corporation®
087 - FAEL: '{60E24349-3E7C-4B3C-8BE2-1F88A3465AF2}' [In-None-P6-TRUE] (.NVIDIA Corporation - NVIDIA Streamer Server Component.) -- C:\Program Files\NVIDIA Corporation\NvStreamSrv\nvstreamer.exe =>.Nvidia Corporation®
087 - FAEL: '{0199042F-FFB8-4AD4-BC67-033719BB9A4A}' [In-None-P17-TRUE] . (.NVIDIA Corporation - NVIDIA Streamer Server Component.) -- C:\Program Files\NVIDIA Corporation\NvStreamSrv\nvstreamer.exe =>.Nvidia Corporation®
087 - FAEL: '{0FB084CC-5745-4A74-80C5-A02357FAF681}' [In-None-P17-TRUE] . (.Logitech, Inc. - LogiOptionsMgr.exe (UNICODE).) -- C:\ProgramData\Logishrd\LogiOptions\Software\Current\LogiOptionsMgr.EXE =>.Logitech Inc®
087 - FAEL: '{093EE80B-35F4-4EDE-A822-F65C9FC31BFD}' [In-None-P17-TRUE] . (.Google LLC - Google Chrome.) -- C:\Program Files (x86)\Google\Chrome\Application\chrome.exe =>.Google LLC®

---\ Product Upgrade Codes (76) - 2s

090 - PUC: '000021599B0090400100000000F01FEC' [HKLM] . (.Microsoft Application Error Reporting.) =>.Microsoft Corporation
090 - PUC: '0003981D77AEC394D8DD2E2634E659B9' [HKLM] . (.Windows Live SOXE Definitions.) =>.Microsoft Corporation
090 - PUC: '00BA1CDCFF107CF418A6616CF790320C' [HKLM] . (.Windows Live SOXE.) =>.Microsoft Corporation
090 - PUC: '0710000002203301488C8B9DF53A8C3C' [HKLM] . (.Intel(R) Wireless Bluetooth(R).) -- C:\WINDOWS\Installer\{00000170-0220-1033-84C8-B8D95FA3C8C3}\IntelBluetooth.ico =>.bl.org
090 - PUC: '08E87CF658366D34A834AF0890F4A1E2' [HKLM] . (.NitroSense Service.)
090 - PUC: '0AA7CFB2C445A3E47869763FEB56B59E' [HKLM] . (.Microsoft XNA Framework Redistributable 4.0.) -- C:\WINDOWS\Installer\{2BFC7AA0-544C-4E3A-8796-67F3BE655BE9}\ProductIcon =>.bl.org
090 - PUC: '14CEAF10CB3B4F441B58E54857EA8B55' [HKLM] . (.Microsoft Visual C++ 2019 X86 Additional Runtime - 14.29.30037.) =>.Microsoft Corporation

090 - PUC: '1926E8D15D0BCE53481466615F760A7F' [HKLM] . (.Microsoft Visual C++
2010 x64 Redistributable - 10.0.40219.) =>.bl.org
090 - PUC: '1af2a8da7e60d0b429d7e6453b3d0182' [HKLM] . (.Microsoft Visual C++
2005 Redistributable (x64).) =>.bl.org
090 - PUC: '1BAD2218D4DE6763BBA0AC63186945E3' [HKLM] . (.Microsoft Visual C++
2013 x86 Minimum Runtime - 12.0.40664.) =>.Microsoft Corporation
090 - PUC: '1C6E0B680E23CC24CBF4FBC37003ECBC' [HKLM] . (.OptaneDowngradeGuard.)
090 - PUC: '1D034B0FAA6BD374B960AAD30DF10D8B' [HKLM] . (.Microsoft SQL Server
2005 Compact Edition [ENU].) -- C:\WINDOWS\Installer\{F0B430D1-B6AA-473D-9B06-
AA3DD01FD0B8}\ProductIcon =>.Microsoft Corporation
090 - PUC: '1D5E3C0FEDA1E123187686FED06E995A' [HKLM] . (.Microsoft Visual C++
2010 x86 Redistributable - 10.0.40219.) =>.bl.org
090 - PUC: '1DCE42234FFBFED4BA9E2B4488A178A1' [HKLM] . (.Intel(R) Management
Engine Driver.) =>.Intel Corporation
090 - PUC: '24C995FA5E2A15247BEE945210752B15' [HKLM] . (.Hotspot Shield 11.3.0.)
=>.AnchorFree Inc.
090 - PUC: '2E177F4F32E672F4391E722CC2177B2E' [HKLM] . (.Intel® Optane™ Pinning
Explorer Extensions.) -- C:\WINDOWS\Installer\{F4F771E2-6E23-4F27-93E1-
27C22C71B7E2}\PinIcon.ico =>.Intel Corporation
090 - PUC: '343F6EE65DB034F4FB4B0AD4B8F18EBC' [HKLM] . (.Intel(R) Management
Engine Components.) =>.Intel Corporation
090 - PUC: '37DA8F1E5C90A4342A4C51CEB689FC12' [HKLM] . (.Microsoft VC++
redistributables repacked.) =>.bl.org
090 - PUC: '39D86C23F23D10B428051646B2CF228F' [HKLM] . (.Epic Online Services.)
-- C:\WINDOWS\Installer\{32C68D93-D32F-4B01-8250-61642BFC22F8}\Installer.ico
090 - PUC: '3DF5949ED37F33D41A4040F7E9B86E7C' [HKLM] . (.User Experience
Improvement Program Service.) -- C:\Windows\Installer\{E9495FD3-F73D-4D33-A104-
047F9E8BE6C7}\ProductIconIco
090 - PUC: '3FC0671964FBA264A83715F1B376D5ED' [HKLM] . (.WiFi Password
Decryptor.) -- C:\WINDOWS\Installer\{91760CF3-BF46-462A-8A73-511F3B675DDE}\
GooglePasswordDecryptor.exe
090 - PUC: '4396FC35D89A48D31964CFE4FDD36514' [HKLM] . (.Microsoft Visual C++
2013 x64 Minimum Runtime - 12.0.40664.) =>.Microsoft Corporation
090 - PUC: '499C5C9F9B6F57D43B7EDA108B04379E' [HKLM] . (.Epic Games Launcher
Prerequisites (x64).) -- C:\WINDOWS\Installer\{F9C5C994-F6B9-4D75-B3E7-
AD01B84073E9}\UnrealEngineLauncher.ico =>.Legitimate
090 - PUC: '4B2346D1D42EE5044ABA7D6E0D88BC9C' [HKLM] . (.Windows Live Photo
Common.) =>.CyberLink Corporation
090 - PUC: '50FF38E6414B8AA47A2829C77B5D61CE' [HKLM] . (.Anagène 2.) -- C:\
WINDOWS\Installer\{6E83FF05-B414-4AA8-A782-927CB7D516EC}\ARPPRODUCTICON.exe
090 - PUC: '5282559C2FB74434AB193DDC644F4C14' [HKLM] . (.Intel(R) Trusted
Connect Service Client x86.) =>.Intel Corporation
090 - PUC: '5282559C2FB74434AB193DDC644F4C24' [HKLM] . (.Intel(R) Trusted
Connect Service Client x64.) =>.Intel Corporation
090 - PUC: '5A812990327ACD34D85B163756A6E149' [HKLM] . (.Dropbox Update Helper.)
=>.WINSE
090 - PUC: '6708A2A6F53155F4BB20ED6DC7C89643' [HKLM] . (.Microsoft Update Health
Tools.) =>.Microsoft Corporation
090 - PUC: '67D6ECF5CD5FBA732B8B22BAC8DE1B4D' [HKLM] . (.Microsoft Visual C++
2008 Redistributable - x64 9.0.30729.6161.) =>.bl.org
090 - PUC: '68AB67CA7DA76301B744000000000010' [HKLM] . (.Adobe Reader 6.0 -
Français.) -- C:\WINDOWS\Installer\{AC76BA86-7AD7-1036-7B44-000000000001}\
ARPPRODUCTICON.exe =>.Adobe Inc.
090 - PUC: '6E815EB96CCE9A53884E7857C57002F0' [HKLM] . (.Microsoft Visual C++
2008 Redistributable - x86 9.0.30729.6161.) =>.bl.org
090 - PUC: '6E8A0490CBBBD45540BD7BEBF01267761' [HKLM] . (.Intel(R) Serial IO.)
=>.Intel Corporation
090 - PUC: '793A733F10623FB408820C49F02B5694' [HKLM] . (.calibre 64bit.) -- C:\
WINDOWS\Installer\{F337A397-2601-4BF3-8028-C0940FB26549}\main_icon =>.Kovid
Goyal
090 - PUC: '7BD4C90EC03660F46A13E87A329932FA' [HKLM] . (.D3DX10.) =>.Microsoft
Corporation
090 - PUC: '7C9F8B73BF303523781852719CD9C700' [HKLM] . (.Microsoft Visual C++
2012 x64 Additional Runtime - 11.0.61030.) =>.Microsoft Corporation

090 - PUC: '80316C14DFC645D4BAA61763DE801AE8' [HKLM] . (.Windows Live Communications Platform.) =>.Legitimate
090 - PUC: '89E25BFA795748442920850FDF5321DE' [HKLM] . (.Care Center Service.)
-- C:\Windows\Installer\{AFB52E98-7597-4484-9202-58F0FD3512ED}\icon.ico =>.Acer Inc.
090 - PUC: '8CDD41E806AE81E43B3E917301D4B5AD' [HKLM] . (.MSVCRT110.)
=>.Advanced Micro Devices Inc
090 - PUC: '8DE6D8418B42D344C9B5D5B65F6076B1' [HKLM] . (.Intel(R) Chipset Device Software.) =>.Intel Corporation
090 - PUC: '9AFB73301C366A14BB21589690091C91' [HKLM] . (.DriversCloud.com.) --
C:\WINDOWS\Installer\{0337BFA9-63C1-41A6-BB12-85690990C119}\DriversCloud.exe
=>.Apple Inc.
090 - PUC: 'A46657D740C6C424281AEE8819E3F561' [HKLM] . (.Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.29.30037.) =>.Microsoft Corporation
090 - PUC: 'A61A0B46C4991924EAD4C119B86BF668' [HKLM] . (.Intel(R) Icls.)
=>.Intel Corporation
090 - PUC: 'A6C64DD86500CEF47BA082BB611A1FF1' [HKLM] . (.MSVCRT.) =>.Advanced Micro Devices Inc
090 - PUC: 'A8F1162B7EFE88E478D5910FFEEA784E' [HKLM] . (.Windows Live PIMT Platform.) =>.Legitimate
090 - PUC: 'AB297010A1550CA37AFEF0BA14653C28' [HKLM] . (.Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.40664.) =>.Microsoft Corporation
090 - PUC: 'ACCD220C7AEDA854791D5FDBA4EA4E0A' [HKLM] . (.Microsoft VC++ redistributables repacked..) =>.bl.org
090 - PUC: 'AD91F7C7701648242936CEC574298C7C' [HKLM] . (.LibreOffice 7.0.0.3.)
-- C:\Windows\Installer\{7C7F19DA-6107-4284-9263-EC5C4792C8C7}\soffice.ico
=>.Open Source
090 - PUC: 'B0F0DA8B6DE61214A9FB9522304F4CC3' [HKLM] . (.Dynamic Application Loader Host Interface Service.)
090 - PUC: 'b25099274a207264182f8181add555d0' [HKLM] . (.Microsoft Visual C++ 2005 Redistributable.) =>.bl.org
090 - PUC: 'B4B4F9022FD3528499604D6D8AE00CE9' [HKLM] . (.Epic Games Launcher.)
-- C:\WINDOWS\Installer\{209F4B4B-3DF2-4825-9906-D4D6A80EC09E}\Installer.ico
=>.Epic Games
090 - PUC: 'B4EB76DD26E75124FA3A1F328A003A98' [HKLM] . (.Movie Maker.)
=>.CyberLink Corporation
090 - PUC: 'B5D7F3A8D2249D94487FD81C7B879276' [HKLM] . (.Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29334.) =>.Microsoft Corporation
090 - PUC: 'C025571B2A687A53689168CD7369889B' [HKLM] . (.Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.61030.) =>.Microsoft Corporation
090 - PUC: 'C15552BAFE47BAB49998985171CF9FFF' [HKLM] . (.Quick Access Service.)
090 - PUC: 'C18BC956E45B1FD46B813F757793A345' [HKLM] . (.Windows Live Installer.) =>.Microsoft Corporation
090 - PUC: 'c1c4f01781cc94c4c8fb1542c0981a2a' [HKLM] . (.Microsoft Visual C++ 2005 Redistributable.) =>.bl.org
090 - PUC: 'C3AEB2FCAE628F23AAB933F1E743AB79' [HKLM] . (.Microsoft Visual C++ 2012 x64 Minimum Runtime - 11.0.61030.) =>.Microsoft Corporation
090 - PUC: 'C842F99B3B4B16D4F9CFAE951A1F7332' [HKLM] . (.Windows Live.)
=>.Microsoft Corporation
090 - PUC: 'C8BD9F007D5674D4BAF56F89EE8385D0' [HKLM] . (.Windows Live UX Platform.) =>.Legitimate
090 - PUC: 'D169104D02A37CA349B316935DDB94A0' [HKLM] . (.Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.40664.) =>.Microsoft Corporation
090 - PUC: 'D20352A90C039D93DBF6126ECE614057' [HKLM] . (.Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17.) =>.bl.org
090 - PUC: 'D780E577824AC8245ADF000001000800' [HKLM] . (.INDEX EDUCATION - Mise à jour automatique.) -- C:\WINDOWS\Installer\{775E087D-A428-428C-A5FD-000010008000}\ARPPRODUCTICON.exe
090 - PUC: 'DC8A59DBF9D1DA5389A1E3975220E6BB' [HKLM] . (.Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.61030.) =>.Microsoft Corporation
090 - PUC: 'DE299B33B95B52E4F9F3FCD297BB9A41' [HKLM] . (.Windows Live UX Platform Language Pack.) =>.Legitimate

090 - PUC: 'DF0D7E1BEFC7C0E45AADF0764699BD19' [HKLM] . (.Windows PC Health Check.) -- C:\WINDOWS\Installer\{B1E7D0FD-7CFE-4E0C-A5DA-0F676499DB91}\ArpIcon.ico
090 - PUC: 'E4FE11E2F109D2B46BE8D32B5A668C75' [HKLM] . (.Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29334.) =>.Microsoft Corporation
090 - PUC: 'E62A2C314DA728D4BBF4ED6A8E179B85' [HKLM] . (.RstDowngradeGuard.)
090 - PUC: 'E66BAA708174D2242981A4BFC329A217' [HKLM] . (.Photo Gallery.) =>.CyberLink Corporation
090 - PUC: 'E714F132BEE7F644EA4C186FAEED37B8' [HKLM] . (.Intel(R) ME WMI Provider.) =>.Intel Corporation
090 - PUC: 'EFEE0228DC83E77358593193D847A0EC' [HKLM] . (.Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.17.) =>.bl.org
090 - PUC: 'F187AF9E08E3993428A5DAE3112CC877' [HKLM] . (.MSVCRT110_amd64.) =>.Advanced Micro Devices Inc
090 - PUC: '70D17E3E72DCBC644884614DBF92AA31' [HKCU] . (.Microsoft WSE 3.0 Runtime.) -- %APPDATA%\Microsoft\Installer\{E3E71D07-CD27-46CB-8448-16D4FB29AA13}\ARPPRODUCTICON.exe =>.Microsoft Corporation
090 - PUC: '9D5BD29AD42A8764F9194BAFD6987581' [HKCU] . (.Paradox Launcher v2.) -- %APPDATA%\Microsoft\Installer\{A92DB5D9-A24D-4678-9F91-B4FA6D895718}\ParadoxIcon
090 - PUC: '70D17E3E72DCBC644884614DBF92AA31' [HKU] . (.Microsoft WSE 3.0 Runtime.) -- %APPDATA%\Microsoft\Installer\{E3E71D07-CD27-46CB-8448-16D4FB29AA13}\ARPPRODUCTICON.exe =>.Microsoft Corporation
090 - PUC: '9D5BD29AD42A8764F9194BAFD6987581' [HKU] . (.Paradox Launcher v2.) -- %APPDATA%\Microsoft\Installer\{A92DB5D9-A24D-4678-9F91-B4FA6D895718}\ParadoxIcon

---\ Windows Installer Scan (33) - 18s

[MD5.65A78973BA24FF57A1AB41ED72AD6D3D] [WIS][2017/12/04 12:08:02] (.Acer Incorporated - DriverSetupUtility.) -- C:\WINDOWS\Installer\11eb2.msi [2576384] =>.Acer Incorporated
[MD5.B38E7F5B58A66857A6EE54FDDD8C6910] [WIS][2021/09/15 15:07:21] (.Cybelsoft - DriversCloud.com.) -- C:\WINDOWS\Installer\1dde6f9f.msi [3589632] =>.Cybelsoft
[MD5.B1B04109BD643E8E01FF7051CB9F0E68] [WIS][2020/09/10 15:04:54] (.Paradox Interactive - Paradox Launcher v2.) -- C:\WINDOWS\Installer\236f3c.msi [78553088] =>.Paradox Interactive
[MD5.94345AAD3689444A9342C55FFD6FE875] [WIS][2020/08/19 14:57:54] (.The Document Foundation - LibreOffice 7.0.) -- C:\WINDOWS\Installer\24d1b4e1.msi [315977728] =>.The Document Foundation
[MD5.14EBCD40BD13278C8BCD3DE08846B533] [WIS][2003/05/20 02:53:54] (.Adobe Systems Incorporated - Acrobat Reader 6.0 (Français).) -- C:\WINDOWS\Installer\2b03d04e.msi [2274816] =>.Adobe Systems Incorporated
[MD5.91EBE456C4DE09923F564608BB50BBD0] [WIS][2006/09/05 16:58:54] (.CNDP.) -- C:\WINDOWS\Installer\2b03d051.msi [518144]
[MD5.45E780924359F06368D23232904F8803] [WIS][2022/08/04 11:17:44] (.Pango Inc. - Hotspot Shield 11.3.0.) -- C:\WINDOWS\Installer\2cf2093.msi [21024768] =>.Pango Inc.
[MD5.DE0F1372A75653C0441088D82850B577] [WIS][2022/02/10 00:08:21] (.Acer Incorporated - Quick Access.) -- C:\WINDOWS\Installer\2de81b8.msi [7831552] =>.Acer Incorporated
[MD5.2BAF0AD4F8926EE333824EEEE87DCCA70] [WIS][2021/05/20 18:31:49] (.SecurityXploded - WiFi Password Decryptor.) -- C:\WINDOWS\Installer\314e7c9.msi [1444352] =>.SecurityXploded
[MD5.2D51D75B189994FB4C2EB68CC48019F7] [WIS][2022/06/14 21:43:28] (.Intel Corporation - Intel(R) Management Engine Driver.) -- C:\WINDOWS\Installer\39685d7.msi [1466368] =>.Intel Corporation
[MD5.22CC72F0D2A1A7CEFCBDF8434ED45BE3] [WIS][2022/06/14 21:42:00] (.Intel Corporation - Intel(R) Management Engine Components.) -- C:\WINDOWS\Installer\39685de.msi [311296] =>.Intel Corporation
[MD5.5AA82DEF070AA674F669109AB7D92B4C] [WIS][2022/06/14 21:43:06] (.Intel Corporation - Dynamic Application Loader Host Interface S.) -- C:\WINDOWS\Installer\39685e5.msi [2134016] =>.Intel Corporation
[MD5.6A1D7F56CEB0DFF09ACBB3DCF987C4D3] [WIS][2022/06/14 21:43:16] (.Intel Corporation - Intel(R) Icls.) -- C:\WINDOWS\Installer\39685ec.msi [20484096] =>.Intel Corporation

[MD5.9CBFA17AC51F49E59131600255B60D0E] [WIS][2022/06/14 21:43:14] (.Intel Corporation - Intel(R) ME WMI Provider.) -- C:\WINDOWS\Installer\3968785.msi [2711552] =>.Intel Corporation
[MD5.8841CA8210262F06E7D156E80D7C1310] [WIS][2022/09/17 08:55:01] (.Kovid Goyal - calibre Installer.) -- C:\WINDOWS\Installer\3b1e1f1.msi [154935296] =>.Kovid Goyal
[MD5.52651D6AB521D1EAD2102CEE2A118B2C] [WIS][2022/05/09 22:00:33] (.InstallShield.) -- C:\WINDOWS\Installer\3bca2239.msi [2493440] =>.InstallShield
[MD5.13C42749C80A96D107788D412EC82C9E] [WIS][2021/10/24 17:37:03] (.Intel Corporation - RstDowngradeGuard.) -- C:\WINDOWS\Installer\3cdad.msi [176128] =>.Intel Corporation
[MD5.8181FF384110BB6361AAD6A415DB05D7] [WIS][2021/10/24 17:37:03] (.Intel Corporation - OptaneDowngradeGuard.) -- C:\WINDOWS\Installer\3cdb4.msi [176128] =>.Intel Corporation
[MD5.F2A88A0016E1903115AA29A374D001AA] [WIS][2019/03/28 20:15:48] (.Intel Corporation - Intel® Optane™ Pinning Explorer Extensions.) -- C:\WINDOWS\Installer\3d837.msi [589824] =>.Intel Corporation
[MD5.EBDE67191BC1A483FD821DAF8E01CE46] [WIS][2021/10/27 19:34:00] (.Epic Games, Inc. - Epic Games Launcher.) -- C:\WINDOWS\Installer\429d96e.msi [157548544] =>.Epic Games, Inc.
[MD5.6C269C464C0846DB805CECEA8DD7D111] [WIS][2021/10/02 03:57:28] (.Epic Games, Inc. - Epic Online Services.) -- C:\WINDOWS\Installer\429d975.msi [112828416] =>.Epic Games, Inc.
[MD5.4D5C9A709F332236559D3BCB27BB81B1] [WIS][2020/06/18 18:28:42] (.Epic Games, Inc. - Epic Games Launcher Prerequisites (x64).) -- C:\WINDOWS\Installer\43059ef.msi [11530240] =>.Epic Games, Inc.
[MD5.D78D0FE3A00F46774880F12E14F7394C] [WIS][2022/08/18 20:18:12] (.Dropbox, Inc. - Dropbox Update Helper.) -- C:\WINDOWS\Installer\5845acf9.msi [27136] =>.Dropbox, Inc.
[MD5.186366F132F73198F9D74EE13E144FF5] [WIS][2022/10/22 06:17:58] (.Intel Corporation - Intel(R) Wireless Bluetooth(R) Patch/Audio .) -- C:\WINDOWS\Installer\709b6b.msi [16175104] =>.Intel Corporation
[MD5.FB49E7D4F22CF014E756BC3696B76C19] [WIS][2022/01/11 12:18:59] (.Acer Incorporated - Care Center Service.) -- C:\WINDOWS\Installer\78c75fa5.msi [15556608] =>.Acer Incorporated
[MD5.F834B8802B9CC9C4DC323F25E26EBC52] [WIS][2019/01/07 03:06:28] (.Intel Corporation - Intel(R) Chipset Device Software.) -- C:\WINDOWS\Installer\99d3.msi [487424] =>.Intel Corporation
[MD5.84C3547A41C3C8A489B8B27A6915C270] [WIS][2019/12/12 07:31:46] (.Intel Corporation - Microsoft VC++ redistributables repacked..) -- C:\WINDOWS\Installer\99fb6.msi [12840960] =>.Intel Corporation
[MD5.8332FD259F0D3E46FE2146350B31CF4D] [WIS][2019/12/12 07:31:56] (.Intel Corporation - Microsoft VC++ redistributables repacked..) -- C:\WINDOWS\Installer\99fbd.msi [14307328] =>.Intel Corporation
[MD5.676B548602AA7F2BC74D7B6A32A883A8] [WIS][2019/09/25 08:15:28] (.Intel Corporation - Intel(R) Trusted Connect Service Client x64.) -- C:\WINDOWS\Installer\99fcb.msi [4120576] =>.Intel Corporation
[MD5.A03E01D414E2606D00E1E2BA14796AA4] [WIS][2019/09/25 08:03:50] (.Intel Corporation - Intel(R) Trusted Connect Service Client x86.) -- C:\WINDOWS\Installer\99fd2.msi [12132352] =>.Intel Corporation
[MD5.F50246CA87623051E1D0CC12CAA33E70] [WIS][2020/05/17 12:34:14] (.Intel Corporation - Intel(R) Serial IO.) -- C:\WINDOWS\Installer\9a015.msi [1355776] =>.Intel Corporation
[MD5.B15973E1F28493C8A7207F9759278D58] [WIS][2019/04/24 12:07:50] (.Acer Incorporated - NitroSenseV31.) -- C:\WINDOWS\Installer\cbab.msi [7028736] =>.Acer Incorporated
[MD5.A266F27AC8D682F7743FD65D577CA470] [WIS][2018/12/19 10:54:42] (.Acer Incorporated - User Experience Improvement Program.) -- C:\WINDOWS\Installer\cbb6.msi [9654272] =>.Acer Incorporated

---\ FEATURE CONTROL. (129) - 1s

[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]:wmpayer.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]:wmpayer.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]:KMPlayer.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BROWSER_EMULATION]:FoxitPDFReader.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]:wmpayer.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_SQM_UPLOAD_FOR_APP]:ieuser.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_SQM_UPLOAD_FOR_APP]:iexplore.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_TELNET_PROTOCOL]:HelpPane.exe =>.Legitimate

[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_TELNET_PROTOCOL]:PresentationHost.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_UNICODE_HANDLE_CLOSING_CALLBACK]:YahooMusicEngine.exe
=>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DOCUMENT_COMPATIBLE_MODE]:HelpPane.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_SCRIPT_PASTE_URLACTION_IF_PROMPT]:devenv.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_SCRIPT_PASTE_URLACTION_IF_PROMPT]:dexplore.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_SCRIPT_PASTE_URLACTION_IF_PROMPT]:helppane.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_SCRIPT_PASTE_URLACTION_IF_PROMPT]:PresentationHost.exe
=>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_FEEDS]:msfeedssync.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_FORCE_ADDR_AND_STATUS]:PresentationHost.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_FORCE_ADDR_AND_STATUS]:prevhost.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE]:HelpPane.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE]:wmpplayer.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]:wmpplayer.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]:wmpplayer.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]:wmpplayer.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MSHTML_AUTOLOAD_IFRAME]:mshta.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MSHTML_AUTOLOAD_IFRAME]:outlook.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MSHTML_AUTOLOAD_IFRAME]: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]:wmpplayer.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]:wmpplayer.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]:wmpplayer.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]:wmpplayer.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]:wmpplayer.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]:wmpplayer.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]:wmpplayer.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]:wmpplayer.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_VIEWLINKEDWEOC_IS_UNSAFE]:HelpPane.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEOC_MOVESIZECHILD]:msn.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEOC_POPUPMANAGEMENT]:explorer.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEOC_POPUPMANAGEMENT]:iexplore.exe =>.Legitimate
[HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEOC_POPUPMANAGEMENT]:wmpplayer.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]:wmpplayer.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]:wmpayer.exe =>.Legitimate

---\ Observer Of Events (109) - 19s

Application.Error: Application Hang (4)

~Numéro: 2769

~Date: 10/31/2022 08:07:56 AM

~ID: 1002

~Description: The program %1 version %2 stopped interacting with Windows and was closed. To see if more information about the problem is available, check the problem history in the Security and Maintenance control panel.

~Suggestion: Essayer les commandes suivantes ipconfig /release et ipconfig /renew.

Application.Warning: Microsoft-Windows-WMI (107)

~Numéro: 2735

~Date: 10/31/2022 06:56:07 AM

~ID: 63

~Description: A provider, %1, has been registered in the Windows Management Instrumentation namespace %2 to use the LocalSystem account. This account is privileged and the provider may cause a security violation if it does not correctly impersonate user requests.

~Suggestion: Généralement LocalSystem n'est pas nécessaire et le contexte de sécurité NetworkServiceHost est plus approprié.

Application.Error: VSS (20)

~Numéro: 2628

~Date: 10/30/2022 11:44:00 AM

~ID: 8193

~Description: Volume Shadow Copy Service error: Unexpected error calling routine %1. hr = %2.

~Suggestion: Utiliser la procédure de reconstruction du VSS

Application.Warning: Microsoft-Windows-Perflib (14)

~Numéro: 2430

~Date: 10/28/2022 12:27:25 PM

~ID: 1008

~Description: The Open procedure for service '%1' in DLL '%2' failed with error code %3. Performance data for this service will not be available.

~Suggestion: Rechercher le concerné et décocher «Compteurs de performances activés».

Application.Warning: Microsoft-Windows-RestartManager (4)

~Numéro: 2086

~Date: 10/26/2022 08:44:34 PM

~ID: 10010

~Description: Application '%3' (pid %2) cannot be restarted - %9.

~Suggestion: Redémarrer manuellement l'application ou le service

Application.Error: Application Error (2)

~Numéro: 1975

~Date: 10/26/2022 06:48:17 AM

~ID: 1000

~Description: Faulting application name: %1, version: %2, time stamp: 0xe64c65ed
Faulting module name: %4, version: %5, time stamp: 0x4769d08d Exception code: 0xe0434352 Fault offset: 0x0000000000008fb0c Faulting process id: 0x0x1264
Faulting application start time

~Suggestion: Réparer ou réinstaller l'application.

Application.Warning: LMS (1)

~Numéro: 1452

~Date: 10/24/2022 07:54:35 AM

~ID: 2001

~Description: LMS lost connection to Intel(R) MEI driver

~Suggestion: Aucune

Application.Warning: Windows Search Service (1)

~Numéro: 103

~Date: 10/16/2022 11:47:24 AM

~Description: The Windows Search Service is starting up and attempting to remove the old search index {Reason: %2}.

System.Warning: DCOM (274)

~Numéro: 6549

~Date: 10/31/2022 08:08:12 AM

~ID: 10016

~Description: application-specificLocalActivation{2593F8B9-4EAF-457C-B68A-50F6B8EA6B54}{15C20B67-12E7-4BB6-92BB-7AFF07997402}LAPTOP-3SI7NK72UserS-1-5-21-3140157745-1616442026-3104895479-1001LocalHost (Using LRPC)UnavailableUnavailable

~Suggestion: Vérifier les autorisations pour l'accès DCOM

System.Warning: LsaSrv (270)

~Numéro: 6473

~Date: 10/31/2022 06:56:04 AM

~ID: 6155

~Description: LSA package is not signed as expected. This can cause unexpected behavior with Credential Guard. PackageName: msv1_0

System.Warning: Microsoft-Windows-Wininit (27)

~Numéro: 6461

~ID: 15

~Description: Credential Guard and/or VBS Key Isolation are configured but the secure kernel is not running; continuing without them.

System.Warning: Microsoft-Windows-WLAN-AutoConfig (28)

~Numéro: 6411

~Date: 10/30/2022 09:38:24 PM

~ID: 10002

~Description: WLAN Extensibility Module has stopped. Module Path: C:\WINDOWS\system32\IntelIHVRouter08.dll

~Suggestion: 1) Désactivez/Réactiver la connexion réseau sans fil. ou 2) Redémarrer le service WLAN AutoConfig

System.Warning: Microsoft-Windows-DNS-Client (18)

~Numéro: 6230

~Date: 10/30/2022 11:43:54 AM

~ID: 1014

~Description: Name resolution for the name %1 timed out after none of the configured DNS servers responded. Client PID %4.

~Suggestion:

<https://social.technet.microsoft.com/wiki/contents/articles/3336.event-id-1014-microsoft-windows-dns-client.aspx>

System.Error: EventLog (5)

~Numéro: 5289

~Date: 10/27/2022 10:02:08 PM

~ID: 6008

~Description: The previous system shutdown at %1 on %2 was unexpected.

System.Error: Microsoft-Windows-WindowsUpdateClient (6)

~Numéro: 5254

~Date: 10/27/2022 04:49:36 PM

~ID: 20

~Description: 0x80073d029NMPJ99VJBWV-Microsoft.YourPhone{0f591135-1c5e-45a4-9947-6d84efff79e9}1{855e8a7c-ecb4-4ca3-b045-1dfa50104289}

~Suggestion: http://kb.eventtracker.com/evtpass/evtpages/EventId_20_Microsoft-Windows-WindowsUpdateClient_63351.asp

System.Warning: MEIx64 (1)

~Numéro: 3516

~ID: 4

~Description: The Intel(R) Management Engine Interface is being disabled.

System.Warning: Microsoft-Windows-Time-Service (6)

~Numéro: 3483

~Date: 10/24/2022 04:56:14 AM

~ID: 134

~Description: NtpClient was unable to set a manual peer to use as a time source because of DNS resolution error on '%3'. NtpClient will try again in %2 minutes and double the reattempt interval thereafter. The error was: No such host is known. (0x80072AF9)

~Suggestion: Resynchroniser le client avec l'homologue de source de temps

System.Error: Service Control Manager (2)

~Numéro: 2883
~Date: 10/22/2022 07:42:45 AM
~ID: 7031
~Description: The %1 service terminated unexpectedly. It has done this %2 time(s). The following corrective action will be taken in %3 milliseconds: %5.
System.Error: Microsoft-Windows-WER-SystemErrorReporting (1)
~Numéro: 2002
~Date: 10/21/2022 09:48:23 AM
~ID: 1001
~Description: 0x0000007f (0x00000000000000008, 0xffffffff8055fddde50, 0xffffffff8055fdd7fd0, 0xffffffff80560e36b90)C:\WINDOWS\MEMORY.DMP2fa16e9e-54b5-43e0-8113-65acf6a57ff1
System.Error: volmgr (1)
~Numéro: 1917
~Date: 10/21/2022 09:48:12 AM
~ID: 162
~Description: Dump file generation succeeded.

---\ **Additional Scan (088) (122) - 9s**

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\WinRAR32
=>.SUP.Orphan
HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers\WinRAR32 =>.SUP.Orphan
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\000
=>.SUP.Temporary.Chrome
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\001
=>.SUP.Temporary.Chrome
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\002
=>.SUP.Temporary.Chrome
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\003
=>.SUP.Temporary.Chrome
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\004
=>.SUP.Temporary.Chrome
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\005
=>.SUP.Temporary.Chrome
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\006
=>.SUP.Temporary.Chrome
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\007
=>.SUP.Temporary.Chrome
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\008
=>.SUP.Temporary.Chrome
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\009
=>.SUP.Temporary.Chrome
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\010
=>.SUP.Temporary.Chrome
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\011
=>.SUP.Temporary.Chrome
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\012
=>.SUP.Temporary.Chrome
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\013
=>.SUP.Temporary.Chrome
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\014
=>.SUP.Temporary.Chrome
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\015
=>.SUP.Temporary.Chrome
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\016
=>.SUP.Temporary.Chrome
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\017
=>.SUP.Temporary.Chrome
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\018
=>.SUP.Temporary.Chrome

C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\083
=>.SUP.Temporary.Chrome
C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\File System\084
=>.SUP.Temporary.Chrome
Not deleted [:com.dropbox.attrs] - C:\users\user\desktop\jeux\there is no game
wrong dimension v16.08.2020\ting.exe:com.dropbox.attrs =>.SUP.FileADS
Not deleted [:com.dropbox.attrs] C:\Users\User\Desktop\lubumbashi -
Shortcut.lnk:com.dropbox.attrs =>.SUP.FileADS
Not deleted [:com.dropbox.attrs] C:\Users\User\Desktop\pereir cours -
Shortcut.lnk:com.dropbox.attrs =>.SUP.FileADS
HKLM\SOFTWARE\POLICIES\Mozilla\Firefox =>.SUP.FirefoxRestriction
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\
MuiCache]:C:\Program Files\Calibre2\ebook-viewer.exe.FriendlyAppName =>.Unsigned
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\
MuiCache]:C:\Program Files\Calibre2\ebook-viewer.exe.ApplicationCompany
=>.Unsigned
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\
MuiCache]:C:\Program Files\Calibre2\calibre.exe.FriendlyAppName =>.Unsigned
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\
MuiCache]:C:\Program Files\Calibre2\calibre.exe.ApplicationCompany =>.Unsigned
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\
MuiCache]:C:\Windows\Temp\63a86a6966e67497943f6b4a8418769867b212\
WirelessSetup.exe.FriendlyAppName =>.SUP.Orphan.MUICache
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\
MuiCache]:C:\Windows\Temp\63a86a6966e67497943f6b4a8418769867b212\
WirelessSetup.exe.ApplicationCompany =>.SUP.Orphan.MUICache
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\
MuiCache]:C:\Windows\Temp\b3e7d703e1c44846e587f754a47bfc1a04c22d\
WirelessSetup.exe.FriendlyAppName =>.SUP.Orphan.MUICache
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\
MuiCache]:C:\Windows\Temp\b3e7d703e1c44846e587f754a47bfc1a04c22d\
WirelessSetup.exe.ApplicationCompany =>.SUP.Orphan.MUICache
C:\Users\User\Downloads\Driver_Updater.exe =>SUP.Optional.PCHelpSoft
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\
MuiCache]:C:\Users\User\Downloads\Driver_Updater.exe.FriendlyAppName
=>SUP.Optional.PCHelpSoft
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\
MuiCache]:C:\Users\User\Downloads\Driver_Updater.exe.ApplicationCompany
=>SUP.Optional.PCHelpSoft
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\
MuiCache]:C:\Users\User\AppData\Local\Temp\
Temp1_Install_Win10_10060_08222022.zip\
Install_Win10_10060_08222022.exe.FriendlyAppName =>.Unsigned
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\
MuiCache]:C:\Users\User\Desktop\ME_Corporate-Win10_Win11-16.1.25.1865\
SetupME.exe.FriendlyAppName =>.SUP.Orphan.MUICache
[HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\
MuiCache]:C:\Users\User\Desktop\ME_Corporate-Win10_Win11-16.1.25.1865\
SetupME.exe.ApplicationCompany =>.SUP.Orphan.MUICache
[HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files\Calibre2\
ebook-viewer.exe.FriendlyAppName =>.Unsigned
[HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files\Calibre2\
ebook-viewer.exe.ApplicationCompany =>.Unsigned
[HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files\Calibre2\
calibre.exe.FriendlyAppName =>.Unsigned
[HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Program Files\Calibre2\
calibre.exe.ApplicationCompany =>.Unsigned
[HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Windows\Temp\
Temp1_Install_Win10_10060_08222022.zip

63a86a6966e67497943f6b4a8418769867b212\WirelessSetup.exe.FriendlyAppName
=>.SUP.Orphan.MUICache
[HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Windows\Temp\
63a86a6966e67497943f6b4a8418769867b212\WirelessSetup.exe.ApplicationCompany
=>.SUP.Orphan.MUICache
[HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Windows\Temp\
b3e7d703e1c44846e587f754a47bfc1a04c22d\WirelessSetup.exe.FriendlyAppName
=>.SUP.Orphan.MUICache
[HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Windows\Temp\
b3e7d703e1c44846e587f754a47bfc1a04c22d\WirelessSetup.exe.ApplicationCompany
=>.SUP.Orphan.MUICache
[HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Users\User\Downloads\
Driver_Updater.exe.FriendlyAppName =>SUP.Optional.PCHelpSoft
[HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Users\User\Downloads\
Driver_Updater.exe.ApplicationCompany =>SUP.Optional.PCHelpSoft
[HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Users\User\AppData\Local\
Temp\Temp1_Install_Win10_10060_08222022.zip\
Install_Win10_10060_08222022.exe.FriendlyAppName =>.Unsigned
[HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Users\User\Desktop\
ME_Corporate-Win10_Win11-16.1.25.1865\SetupME.exe.FriendlyAppName
=>.SUP.Orphan.MUICache
[HKU\S-1-5-21-3140157745-1616442026-3104895479-1001\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\MuiCache]:C:\Users\User\Desktop\
ME_Corporate-Win10_Win11-16.1.25.1865\SetupME.exe.ApplicationCompany
=>.SUP.Orphan.MUICache
C:\ProgramData\BSD\DriverHive =>.SUP.DriverUpdatePlus
C:\ProgramData\Application Data\BSD\DriverHive =>.SUP.DriverUpdatePlus

---\ Summary of the elements found (10) - 0s

<https://nicolascoolman.eu/2022/09/05/zhpdiag-lanalyse-s-m-a-r-t-du-disque-systeme/> => SMART Information
<https://nicolascoolman.eu/2017/09/12/origine-lignes-orphelines/> =>.SUP.Orphan
<https://nicolascoolman.eu/forum/Topic/warning-eventlogapp-evenement-application/> =>Warning.EventLogApp
<https://nicolascoolman.eu/forum/Topic/warning-eventlogsys-evenement-systeme/>
=>Warning.EventLogSys
<https://nicolascoolman.eu/forum/Topic/logiciels-potentiellement-superflus-lps/>
=>.SUP.Temporary.Chrome
<https://nicolascoolman.eu/2018/01/04/ads-alternate-data-stream/> =>.SUP.FileADS
<https://nicolascoolman.eu/forum/Topic/logiciels-potentiellement-superflus-lps/>
=>.SUP.FirefoxRestriction
<https://nicolascoolman.eu/forum/Topic/orphan-muicache-logiciel-potentiellement-superflu-lps/> =>.SUP.Orphan.MUICache
<https://nicolascoolman.eu/forum/Topic/repaketage-et-infection/>
=>SUP.Optional.PCHelpSoft
<https://nicolascoolman.eu/forum/Topic/logiciels-potentiellement-superflus-lps/>
=>.SUP.DriverUpdatePlus

~ Unselected Options: WR, 082,
~ End of the scan, 10694 items in 04mn02s (2889)(0)

Serial Number

[00B64744B953FEB17C675F056485FCFD01] [15/09/2021] (.CYBELSOFT.) - C:\Program Files\Cybelsoft\DriversCloud.com\DriversCloud.exe
[0100000000012FD3D4E90C] [19/12/2011] (.EUROSMART.) - C:\Program Files (x86)\Eurosmart\LatisJunior\LatisJunior.exe =>.Not verified
[0100000000012FD3D4E90C] [19/12/2011] (.EUROSMART.) - C:\Program Files (x86)\Eurosmart\LatisPLP\LatisPLP.exe =>.Not verified
[0100000000012FD3D4E90C] [19/12/2011] (.EUROSMART.) - C:\Program Files (x86)\Eurosmart\LatisPro\LatisPro.exe =>.Not verified
[0109EDFF81A3392E578D219812C053E1] [11/07/2022] (.FOXIT SOFTWARE INC..) - C:\PROGRAM FILES (X86)\FOXIT SOFTWARE\FOXIT READER\unins000.exe =>.Not verified
[025B15B140C4AD4C6208FD805193D189] [13/10/2022] (.Opera Norway AS.) - C:\Users\User\AppData\Local\Programs\Opera\91.0.4516.77\installer.exe
[025B15B140C4AD4C6208FD805193D189] [13/10/2022] (.Opera Norway AS.) - C:\Users\User\AppData\Local\Programs\Opera\91.0.4516.77\mojo_core.dll
[0304E53E0F9B762F0EEB0F5F7E3B549D] [15/07/2022] (.Open Source Developer, Xavier Roche.) - C:\Program Files\WinHTTrack\unins000.exe
[0320BE3EB866526927F999B97B04346E] [03/09/2018] (.Realtek Semiconductor Corp..) - C:\WINDOWS\System32\DRIVERS\rtf64x64.sys
[03B4BC5EE79D842C03930B8619EDEAE4] [09/12/2021] (.Zoom Video Communications, Inc..) - C:\Users\User\AppData\Roaming\Zoom\bin_00\airhost.exe
[03B4BC5EE79D842C03930B8619EDEAE4] [09/12/2021] (.Zoom Video Communications, Inc..) - C:\Users\User\AppData\Roaming\Zoom\bin_00\Zoom.exe
[03B4BC5EE79D842C03930B8619EDEAE4] [09/12/2021] (.Zoom Video Communications, Inc..) - C:\Users\User\AppData\Roaming\Zoom\uninstall\Installer.exe
[04DF4D56733AE38D598EA004DD2D9C51] [08/04/2020] (.Realtek Semiconductor Corp..) - C:\WINDOWS\System32\drivers\RTKVHD64.sys
[05101D15D8F858EE5327DC9BF4B5E60B] [09/09/2021] (.Realtek Semiconductor Corp..) - C:\Program Files (x86)\InstallShield Installation Information\{8833FFB6-5B0C-4764-81AA-06DFEED9A476}\setup.exe
[051F7A0F0A951C6F905F61CCF5966447] [15/07/2022] (.HP Inc..) - C:\Program Files\HP\PrintScanDoctor\HPPrinterHealthMonitor.exe
[051F7A0F0A951C6F905F61CCF5966447] [15/07/2022] (.HP Inc..) - C:\Program Files\HP\PrintScanDoctor\HPPrintScanDoctorService.exe
[054E8D30374B037A81D8EC3D5DCCB1D4] [04/08/2022] (.Pango LLC.) - C:\Program Files (x86)\Hotspot Shield\11.3.0\bin\cmw_srv.exe =>.Not verified
[054E8D30374B037A81D8EC3D5DCCB1D4] [19/08/2022] (.Pango LLC.) - C:\ProgramData\Package Cache\{66896e6b-e420-4356-8a7d-afee469a59b7}\HSS-11.3.0-update.exe =>.Not verified
[05506AFC3934A6F8A093E6D3BBD18CDB] [06/07/2018] (.Windscribe Limited.) - C:\WINDOWS\System32\drivers\tapwindscribe0901.sys
[055100FDBC3E2F470A627F03FCFE5B8] [14/07/2022] (.Nvidia Corporation.) - C:\WINDOWS\System32\drivers\nvvhci.sys
[055100FDBC3E2F470A627F03FCFE5B8] [14/07/2022] (.Nvidia Corporation.) - C:\Windows\System32\DriverStore\FileRepository\nvmoduletracker.inf_amd64_0c1cc60a4b422185\NvModuleTracker.sys
[056D88813EC335DA59DD5AF48295961F] [15/07/2020] (.Harman International Industries, Inc.) - C:\Program Files\JBL\QuantumAI\QuantumAIApp.exe =>.Not verified
[05F97D054A9BFCBF9D5E12F8D0ABBE07] [25/10/2022] (.ESET, spol. s r.o..) - C:\Users\User\AppData\Local\Google\Chrome\User Data\SwReporter\104.289.200\edls_64.dll
[05F97D054A9BFCBF9D5E12F8D0ABBE07] [25/10/2022] (.ESET, spol. s r.o..) - C:\Users\User\AppData\Local\Google\Chrome\User Data\SwReporter\104.289.200\em002_64.dll
[05F97D054A9BFCBF9D5E12F8D0ABBE07] [25/10/2022] (.ESET, spol. s r.o..) - C:\Users\User\AppData\Local\Google\Chrome\User Data\SwReporter\104.289.200\em003_64.dll
[063D0C011B143C57893FE839779AFCD0] [14/05/2019] (.Realtek Semiconductor Corp..) - C:\Program Files (x86)\InstallShield Installation Information\{F132AF7F-7BCA-4EDE-8A7C-958108FE7DBC}\setup.exe

[06AEA76BAC46A9E8CFE6D29E45AAF033] [29/08/2022] (.Google LLC.) - C:\Program Files (x86)\Google\Update\1.3.36.152\GoogleCrashHandler.exe
[06AEA76BAC46A9E8CFE6D29E45AAF033] [29/08/2022] (.Google LLC.) - C:\Program Files (x86)\Google\Update\1.3.36.152\GoogleCrashHandler64.exe
[06E9579AAB763E72079989C689D2B42D] [10/11/2019] (.The Qt Company Oy.) - C:\Program Files\Stellarium\QtWebEngineProcess.exe
[07E3509C94BE98] [25/09/2020] (.TunnelBear, Inc..) - C:\WINDOWS\System32\drivers\tap-tb-0901.sys
[0800EE4ED1A959CC9887E905AD662BFE] [04/08/2022] (.Nvidia Corporation.) - C:\Program Files\NVIDIA Corporation\NvStreamSrv\nvstreamer.exe
[0800EE4ED1A959CC9887E905AD662BFE] [07/09/2022] (.Nvidia Corporation.) - C:\Program Files\NVIDIA Corporation\FrameViewSDK\nvfvsdksvc_x64.exe
[0800EE4ED1A959CC9887E905AD662BFE] [11/10/2022] (.Nvidia Corporation.) - C:\Windows\System32\DriverStore\FileRepository\nvaci.inf_amd64_91df09c5579a85f3\Display.NvContainer\NvDisplay.Container.exe
[0800EE4ED1A959CC9887E905AD662BFE] [11/10/2022] (.Nvidia Corporation.) - C:\Windows\System32\DriverStore\FileRepository\nvaci.inf_amd64_91df09c5579a85f3\nv3dappshex.dll
[0800EE4ED1A959CC9887E905AD662BFE] [11/10/2022] (.Nvidia Corporation.) - C:\Windows\System32\DriverStore\FileRepository\nvaci.inf_amd64_91df09c5579a85f3\nvlddmkm.sys
[0800EE4ED1A959CC9887E905AD662BFE] [11/10/2022] (.Nvidia Corporation.) - C:\Windows\System32\DriverStore\FileRepository\nvaci.inf_amd64_91df09c5579a85f3\nvshext.dll
[0800EE4ED1A959CC9887E905AD662BFE] [13/10/2022] (.Nvidia Corporation.) - C:\Program Files (x86)\NVIDIA Corporation\NvNode\NVIDIA Web Helper.exe
[0800EE4ED1A959CC9887E905AD662BFE] [15/07/2022] (.Nvidia Corporation.) - C:\WINDOWS\System32\drivers\nvvd64v.sys
[0800EE4ED1A959CC9887E905AD662BFE] [22/07/2022] (.Nvidia Corporation.) - C:\WINDOWS\System32\drivers\nvhda64v.sys
[0800EE4ED1A959CC9887E905AD662BFE] [29/10/2022] (.Nvidia Corporation.) - C:\Users\User\AppData\Local\NVIDIA\NvBackend\ApplicationOntology\NvOAWrapperCache.exe
[0800EE4ED1A959CC9887E905AD662BFE] [29/10/2022] (.Nvidia Corporation.) - C:\Users\User\AppData\Local\NVIDIA\NvBackend\ApplicationOntology\OAWrapper.exe
[0800EE4ED1A959CC9887E905AD662BFE] [29/10/2022] (.Nvidia Corporation.) - C:\Users\User\AppData\Local\NVIDIA\NvBackend\ApplicationOntology\Ontology64.dll
[0800EE4ED1A959CC9887E905AD662BFE] [30/08/2022] (.Nvidia Corporation.) - C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe
[08DF1FFB8B0EEF71ED9573AAE3ECFCDC] [14/07/2019] (.On-site Dental Systems (Justin Shafer).) - C:\WINDOWS\System32\drivers\hidkmdf.sys =>.Not verified
[08DF1FFB8B0EEF71ED9573AAE3ECFCDC] [14/07/2019] (.On-site Dental Systems (Justin Shafer).) - C:\WINDOWS\System32\drivers\vjoy.sys =>.Not verified
[08FC2A6C411D88E7253C3D99170EAE62] [24/11/2020] (.Logitech Inc.) - C:\Program Files\Logitech\LogiOptions\CreateShortcut.exe
[08FC2A6C411D88E7253C3D99170EAE62] [24/11/2020] (.Logitech Inc.) - C:\Program Files\Logitech\LogiOptions\LogiOptions.exe
[08FC2A6C411D88E7253C3D99170EAE62] [24/11/2020] (.Logitech Inc.) - C:\Program Files\Logitech\LogiOptions\uninstaller.exe
[08FC2A6C411D88E7253C3D99170EAE62] [24/11/2020] (.Logitech Inc.) - C:\ProgramData\Logishrd\LogiOptions\Software\Current\LogiOptionsMgr.exe
[08FC2A6C411D88E7253C3D99170EAE62] [24/11/2020] (.Logitech Inc.) - C:\ProgramData\Logishrd\LogiOptions\Software\Current\LogiOverlay.exe
[097F6A856F52B668E857667755982884] [15/09/2022] (.Kovid Goyal.) - C:\Program Files\Calibre2\calibre.exe =>.Not verified
[09B3A7E559FCB024C4B66B794E9540CB] [19/01/2019] (.Windscribe Limited.) - C:\Program Files (x86)\Windscribe\WindscribeService.exe
[09B3A7E559FCB024C4B66B794E9540CB] [19/01/2019] (.Windscribe Limited.) - C:\program files (x86)\windscribe\wsappcontrol.exe
[09B3A7E559FCB024C4B66B794E9540CB] [28/12/2020] (.Windscribe Limited.) - C:\Program Files (x86)\Windscribe\unins000.exe
[0ACC4B9B07538D46DD1D92A8F3BE9C8D] [04/08/2022] (.Pango Inc..) - C:\Program Files (x86)\Hotspot Shield\11.3.0\driver\hsstap-windows-9.24.4-I601-Win10.exe

[0B022E5567D2577010644DE52C9A3656] [15/07/2022] (.FOXIT SOFTWARE INC..) - C:\Program Files (x86)\Foxit Software\Foxit Reader\FoxitPDFReader.exe =>.Not verified

[0B022E5567D2577010644DE52C9A3656] [20/05/2022] (.FOXIT SOFTWARE INC..) - C:\PROGRAM FILES (X86)\FOXIT SOFTWARE\FOXIT READER\FoxitPDFReaderUpdateService.exe =>.Not verified

[0B8F52FAF64C421EABB2275AE148C519] [18/08/2022] (.Realtek Semiconductor Corp..) - C:\WINDOWS\System32\drivers\rt640x64.sys

[0C16D074311A3365FAE8200C7E160C54] [22/10/2022] (.WhatsApp LLC.) - C:\Users\User\AppData\Local\WhatsApp\Update.exe =>.Not verified

[0C16D074311A3365FAE8200C7E160C54] [22/10/2022] (.WhatsApp LLC.) - C:\Users\User\AppData\Local\WhatsApp\WhatsApp.exe =>.Not verified

[0C4420483C0F11248AABBB6EA8A86E82] [03/08/2022] (.Blizzard Entertainment, Inc..) - C:\program files (x86)\hearthstone\hearthstone.exe

[0C4420483C0F11248AABBB6EA8A86E82] [03/08/2022] (.Blizzard Entertainment, Inc..) - C:\ProgramData\Battle.net\Agent\Blizzard Uninstaller.exe

[0C64962E4467EDCC1579646B7337EC8C] [14/10/2021] (.ASUSTeK Computer Inc..) - C:\Program Files (x86)\ASUS\AsusROGLSLService\Armoury Crate Installer.exe

[0C64962E4467EDCC1579646B7337EC8C] [30/08/2021] (.ASUSTeK Computer Inc..) - C:\Windows\System32\DriverStore\FileRepository\rogkb.inf_amd64_9c19ffffb5d62d536\ROGKB.sys

[0C64962E4467EDCC1579646B7337EC8C] [30/08/2021] (.ASUSTeK Computer Inc..) - C:\Windows\System32\DriverStore\FileRepository\rogms.inf_amd64_94d9766656ff6011\ArmouryLiveUpdate.exe

[0C64962E4467EDCC1579646B7337EC8C] [30/08/2021] (.ASUSTeK Computer Inc..) - C:\Windows\System32\DriverStore\FileRepository\rogms.inf_amd64_94d9766656ff6011\ROGMS.sys

[0C83ED30B3A6224906F9137ECF3D6A06] [02/04/2020] (.Adobe Inc..) - C:\Program Files (x86)\Adobe\Adobe Digital Editions 4.5\ADEAutoUpdater_450.exe

[0C83ED30B3A6224906F9137ECF3D6A06] [02/04/2020] (.Adobe Inc..) - C:\Program Files (x86)\Adobe\Adobe Digital Editions 4.5\DigitalEditions.exe

[0D9473E00150BC5EB47F29A10DCCDDBD] [08/04/2020] (.Realtek Semiconductor Corp..) - C:\WINDOWS\System32\RtkAudUService64.exe

[0DFE7BA482F076DB90BCC22B2C487CBD] [14/10/2022] (.Epic Games Inc..) - C:\program files (x86)\epic games\launcher\engine\binaries\win64\epicwebhelper.exe

[0DFE7BA482F076DB90BCC22B2C487CBD] [14/10/2022] (.Epic Games Inc..) - C:\Program Files (x86)\Epic Games\Launcher\Portal\Binaries\Win32\EpicGamesLauncher.exe

[0DFE7BA482F076DB90BCC22B2C487CBD] [14/10/2022] (.Epic Games Inc..) - C:\Program Files (x86)\Epic Games\Launcher\Portal\Binaries\Win64\EpicGamesLauncher.exe

[0DFE7BA482F076DB90BCC22B2C487CBD] [27/10/2021] (.Epic Games Inc..) - C:\Program Files (x86)\Epic Games\Epic Online Services\service\EpicOnlineServicesHost.exe

[0E4418E2DEDE36DD2974C3443AFB5CE5] [27/10/2022] (.Google LLC.) - C:\Program Files (x86)\Google\Chrome\Application\107.0.5304.87\elevation_service.exe

[0E4418E2DEDE36DD2974C3443AFB5CE5] [27/10/2022] (.Google LLC.) - C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

[0E4418E2DEDE36DD2974C3443AFB5CE5] [28/10/2022] (.Google LLC.) - C:\Program Files (x86)\Google\Chrome\Application\107.0.5304.87\Installer\chrnstp.exe

[0E4418E2DEDE36DD2974C3443AFB5CE5] [28/10/2022] (.Google LLC.) - C:\Program Files (x86)\Google\Chrome\Application\107.0.5304.87\Installer\setup.exe

[0F7A165550163D5ED7D1CAA3FC13DA06] [10/10/2022] (.Dropbox, Inc.) - C:\Program Files (x86)\Dropbox\Client\Dropbox.exe

[0F7A165550163D5ED7D1CAA3FC13DA06] [10/10/2022] (.Dropbox, Inc.) - C:\Program Files (x86)\Dropbox\Client\DropboxUninstaller.exe

[0F7A165550163D5ED7D1CAA3FC13DA06] [10/10/2022] (.Dropbox, Inc.) - C:\WINDOWS\System32\DbxSvc.exe

[0F7A165550163D5ED7D1CAA3FC13DA06] [12/11/2021] (.Dropbox, Inc.) - C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe

[0F7A165550163D5ED7D1CAA3FC13DA06] [27/09/2022] (.Dropbox, Inc.) - C:\Program Files (x86)\Dropbox\Client\DropboxExt64.55.0.dll

[1044F31AE1F93A0BB95F19AB9FAAC6BB] [25/10/2022] (.ESET, spol. s r.o..) - C:\Users\User\AppData\Local\Google\Chrome\User Data\SwReporter\104.289.200\em000_64.dll

[1704BEDA781B5AB07267C23F9163D059] [01/03/2017] (.Azureus Software, Inc..) - C:\Program Files\Vuze\Azureus.exe

[1704BEDA781B5AB07267C23F9163D059] [19/01/2020] (.Azureus Software, Inc..) - C:\Program Files\Vuze\uninstall.exe
[19A7124A8EA70E2AF207584C] [09/08/2021] (.Acer Incorporated.) - C:\WINDOWS\System32\drivers\AcerAirplaneModeController.sys
[1CA1247CCA4C07CD3F3751E8] [03/01/2022] (.Acer Incorporated.) - C:\Program Files\Acer\Quick Access Service\PowerButton_NB.exe =>.Not verified
[1CA1247CCA4C07CD3F3751E8] [03/01/2022] (.Acer Incorporated.) - C:\Program Files\Acer\Quick Access Service\QAdminAgent.exe =>.Not verified
[1CA1247CCA4C07CD3F3751E8] [03/01/2022] (.Acer Incorporated.) - C:\Program Files\Acer\Quick Access Service\QAgent.exe =>.Not verified
[1CA1247CCA4C07CD3F3751E8] [03/01/2022] (.Acer Incorporated.) - C:\Program Files\Acer\Quick Access Service\QALSvc.exe =>.Not verified
[1CA1247CCA4C07CD3F3751E8] [03/01/2022] (.Acer Incorporated.) - C:\Program Files\Acer\Quick Access Service\QASvc.exe =>.Not verified
[254E21C741DC779A4EC68054D3FFA4BF] [15/07/2020] (.WDKTestCert Adarsh,131897759775447238.) - C:\WINDOWS\System32\drivers\boomvad.sys =>.Not verified
[2912C70C9A2B8A3EF6F6074662D68B8D] [12/08/2020] (.Google Inc.) - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
[2F7A25FAD4E4CD1F5D5F97D3A9F85AC8] [06/01/2011] (.SEIKO EPSON Corporation.) - C:\Program Files (x86)\EPSON Projector\Epson USB Display V1.5\EMP_UD.exe
[2F7A25FAD4E4CD1F5D5F97D3A9F85AC8] [06/01/2011] (.SEIKO EPSON Corporation.) - C:\Program Files (x86)\EPSON Projector\Epson USB Display V1.5\EMP_UDUi.exe
[330000029B1302828FF3904ED200000000029B] [13/10/2022] (.Skype Software Sarl.) - C:\Program Files\WindowsApps\Microsoft.SkypeApp_15.89.3403.0_x86__kzf8qxf38zg5c\Skype\Skype.exe
[36336D836A19E244FF0E52882EB5B1DE] [03/06/2009] (.Creative Labs Inc.) - C:\Program Files (x86)\OpenAL\oalinst.exe
[46A0800C34C5FEE85DB1758D556C2D0E] [01/02/2019] (.Garena Online Pte Ltd.) - C:\Program Files (x86)\Garena\Garena\2.0.1909.2618\uninst.exe =>.Not verified
[46A0800C34C5FEE85DB1758D556C2D0E] [26/09/2019] (.Garena Online Pte Ltd.) - C:\Program Files (x86)\Garena\Garena\2.0.1909.2618\gxxsvc.exe =>.Not verified
[46A0800C34C5FEE85DB1758D556C2D0E] [26/09/2019] (.Garena Online Pte Ltd.) - C:\Program Files (x86)\Garena\Garena\Garena.exe =>.Not verified
[4E5F9EB5CF6150A7586FDDA0] [17/12/2018] (.Acer Incorporated.) - C:\Program Files\Acer\User Experience Improvement Program Service\Framework\UBTService.exe
[4E5F9EB5CF6150A7586FDDA0] [17/12/2018] (.Acer Incorporated.) - C:\Program Files\Acer\User Experience Improvement Program Service\Plugin\AppMonitor\AppMonitorPlugIn.exe
[4E5F9EB5CF6150A7586FDDA0] [22/04/2019] (.Acer Incorporated.) - C:\Program Files (x86)\Acer\Care Center\ACCAAppLauncher.exe
[4E5F9EB5CF6150A7586FDDA0] [22/04/2019] (.Acer Incorporated.) - C:\Program Files (x86)\Acer\Care Center\ACCStd.exe
[4E5F9EB5CF6150A7586FDDA0] [22/04/2019] (.Acer Incorporated.) - C:\Program Files (x86)\Acer\Care Center\ACCSvc.exe
[4E5F9EB5CF6150A7586FDDA0] [24/04/2019] (.Acer Incorporated.) - C:\Program Files\Acer\NitroSense Service\PSAdminAgent.exe
[4E5F9EB5CF6150A7586FDDA0] [24/04/2019] (.Acer Incorporated.) - C:\Program Files\Acer\NitroSense Service\PSAgent.exe
[4E5F9EB5CF6150A7586FDDA0] [24/04/2019] (.Acer Incorporated.) - C:\Program Files\Acer\NitroSense Service\PSSvc.exe
[51029B3B9CB48FA076FA2DA87A91DB42] [27/10/2021] (.Epic Games Inc..) - C:\ProgramData\Package Cache\{43a03b9c-4770-409c-a999-587b60700b63}\LauncherPrereqSetup_x64.exe
[56000001757376CD78AD000C9A000000000175] [29/11/2018] (.Intel(R) Embedded Subsystems and IP Blocks Group.) - C:\WINDOWS\System32\drivers\iaLPSS2_GPI02.sys
[56000001757376CD78AD000C9A000000000175] [29/11/2018] (.Intel(R) Embedded Subsystems and IP Blocks Group.) - C:\WINDOWS\System32\drivers\iaLPSS2_I2C.sys
[56000001757376CD78AD000C9A000000000175] [29/11/2018] (.Intel(R) Embedded Subsystems and IP Blocks Group.) - C:\WINDOWS\System32\drivers\iaLPSS2_SPI.sys
[56000001757376CD78AD000C9A000000000175] [29/11/2018] (.Intel(R) Embedded Subsystems and IP Blocks Group.) - C:\WINDOWS\System32\drivers\iaLPSS2_UART2.sys

[56000005DAB0988313DA8AB3E10000000005DA] [03/07/2019] (.Intel(R) pGFX.) - C:\Windows\System32\DriverStore\FileRepository\cui_dch.inf_amd64_92cf9d9d84f1d3db\igfxCUIService.exe

[56000005DAB0988313DA8AB3E10000000005DA] [03/07/2019] (.Intel(R) pGFX.) - C:\Windows\System32\DriverStore\FileRepository\cui_dch.inf_amd64_92cf9d9d84f1d3db\igfxEM.exe

[56000005DAB0988313DA8AB3E10000000005DA] [03/07/2019] (.Intel(R) pGFX.) - C:\Windows\System32\DriverStore\FileRepository\cui_dch.inf_amd64_92cf9d9d84f1d3db\igfxext.exe

[56000005DAB0988313DA8AB3E10000000005DA] [03/07/2019] (.Intel(R) pGFX.) - C:\Windows\System32\DriverStore\FileRepository\iigd_dch.inf_amd64_7d6ad0397c5dc3fd\igdkmd64.sys

[56000005DAB0988313DA8AB3E10000000005DA] [03/07/2019] (.Intel(R) pGFX.) - C:\Windows\System32\DriverStore\FileRepository\iigd_dch.inf_amd64_7d6ad0397c5dc3fd\IntelCpHDCPSvc.exe

[56000005DAB0988313DA8AB3E10000000005DA] [03/07/2019] (.Intel(R) pGFX.) - C:\Windows\System32\DriverStore\FileRepository\iigd_dch.inf_amd64_7d6ad0397c5dc3fd\IntelCpHeciSvc.exe

[560000088689EFB89169C165B1000000000886] [28/08/2020] (.Intel(R) Trust Services.) - C:\ProgramData\Package Cache\{2391a86e-5ab5-40d2-a274-1867cd576686}\iclsClientInstaller.exe

[581AB4F281B116D3FBA75C516AF0B2A6] [18/12/2021] (.ObviousIdea.) - C:\Program Files (x86)\ObviousIdea\Light Image Resizer 6\unins000.exe

[59BFA29DD2D6F208659847D2] [10/05/2022] (.INDEX EDUCATION SAS.) - C:\program files (x86)\index education\mise a jour automatique\ServiceMiseAJourIndex.exe =>.Not verified

[63F07348D0F35040ADB2EC28] [27/11/2017] (.Acer Incorporated.) - C:\Program Files\DriverSetupUtility\FUB\FUB.exe

[65628C146ACE93037FC58659F14BD35F] [25/10/2022] (.ESET, spol. s r.o..) - C:\Users\User\AppData\Local\Google\Chrome\User Data\SwReporter\104.289.200\em001_64.dll

[65628C146ACE93037FC58659F14BD35F] [25/10/2022] (.ESET, spol. s r.o..) - C:\Users\User\AppData\Local\Google\Chrome\User Data\SwReporter\104.289.200\em004_64.dll

[65628C146ACE93037FC58659F14BD35F] [25/10/2022] (.ESET, spol. s r.o..) - C:\Users\User\AppData\Local\Google\Chrome\User Data\SwReporter\104.289.200\em005_64.dll

[6E9B46A4FDC17828C3E7EA71C2BE85FB] [30/04/2009] (.Electronic Arts.) - C:\Program Files (x86)\Electronic Arts\The Sims 3\Game\Bin\Sims3Launcher.exe

[731D40AE3F3A1FB2BC3D8395] [11/06/2021] (.win.rar GmbH.) - C:\Program Files\WinRAR\Rar.exe

[731D40AE3F3A1FB2BC3D8395] [11/06/2021] (.win.rar GmbH.) - C:\Program Files\WinRAR\RarExt.dll

[731D40AE3F3A1FB2BC3D8395] [14/06/2021] (.win.rar GmbH.) - C:\Program Files\WinRAR\uninstall.exe

[737BE9572E71E147EB7F035C287710BD] [20/06/2019] (.ELAN MICROELECTRONICS CORPORATION.) - C:\WINDOWS\System32\drivers\ETDI2C.sys

[75B5499C96D676A5FAE2656B351E1FD6] [08/10/2021] (.Samsung Electronics Co., Ltd..) - C:\WINDOWS\System32\DRIVERS\ssudbus2.sys

[75B5499C96D676A5FAE2656B351E1FD6] [08/10/2021] (.Samsung Electronics Co., Ltd..) - C:\WINDOWS\System32\DRIVERS\ssudmdm.sys

[79CD8A54D02798DE82C8D60BB20D117E] [31/01/2019] (.Waves Inc.) - C:\Windows\System32\DriverStore\FileRepository\wavesapo77ac.inf_amd64_d5839c9d7c0bda64\WavesSvc64.exe

[79CD8A54D02798DE82C8D60BB20D117E] [31/01/2019] (.Waves Inc.) - C:\Windows\System32\DriverStore\FileRepository\wavesapo77ac.inf_amd64_d5839c9d7c0bda64\WavesSysSvc64.exe