**ZHPDiag Diagnostic Report**

Mail de Fred, fevrier 2018

Coucou Mymi,

Le lien pour telecharger l outil de diagnostique [ZHPDIAG](https://www.nicolascoolman.com/download/zhpdiag/)

Le forum ou poster le rapport genere par ZHPDIAG dans la section **virus/securite** ou **windows** [FORUM ENTRAIDE](https://helper-formation.fr/entraide/)

Ca ne t engage a rien, tu peux avoir confiance en ces gens, ce sont des pointures et ils te diront exactement de quoi il en retourne.

Bisous

Zhpdiag nicolas coolman

17 mars 2018

~ ZHPDiag v2018.3.17.52 By Nicolas Coolman (2018/03/17)

~ Run by Myriam (Administrator) (2018/03/18 18:43:59)

~ 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\Myriam\Desktop\ZHPDiag.txt

~ Report: C:\Users\Myriam\AppData\Roaming\ZHP\ZHPDiag.txt

~ UAC: Activate

~ System startup: Normal (Normal boot)

Windows 8, 64-bit (Build 9200) =>.Microsoft Corporation

**---\ Internet Browsers (2) - 0s**

~ MFIE: Mozilla Firefox 58.0.2 (x64 en-US)

~ MSIE: Internet Explorer v10.0.9200.17607

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

~ Windows Server License Manager Script : OK

~ Licence Script File Génération : OK

Windows Automatic Updates : OK

**---\ System protection software (2) - 11s**

Malwarebytes Anti-Malware version 2.2.1.1043 (Protection)

Windows Defender W8 (Deactivate)

**---\ Surveillance software (2) - 11s**

~ Adobe Flash Player 29 NPAPI (Surveillance)

~ Adobe Reader X (Surveillance)

**---\ System optimization software (1) - 11s**

~ Driver Booster 2.1 v2.1 (Optimisation)

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

~ Operating System: Intel64 Family 6 Model 58 Stepping 9, GenuineIntel

~ Operating System: 64-bit

~ Boot mode: Normal (Normal boot)

Total RAM: 6178.76 MB (20% free) : OK =>.RAM Value

System Restore: Activé (Enable)

System drive C: has 434 GB (61%) free of 703 GB : OK =>.Disk Space

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

~ Computer Name: MYMI

~ User Name: Myriam

~ Logged in as Administrator

**---\ Enumeration of the disk units (3) - 0s**

~ Drive C: has 434 GB free of 703 GB (System)

~ Drive F: has 950 GB free of 1907 GB

~ Drive G: has 243 GB free of 2861 GB

**---\ State of the Windows Security Center (14) - 0s**

[HKLM\Software\WOW6432Node\Microsoft\Security Center] AntiVirusDisableNotify: OK

[HKLM\Software\WOW6432Node\Microsoft\Security Center] FirewallDisableNotify: OK

[HKLM\Software\WOW6432Node\Microsoft\Security Center] UpdatesDisableNotify: OK

[HKLM\Software\WOW6432Node\Microsoft\Security Center\Svc] AntiSpywareOverride: OK

[HKLM\Software\WOW6432Node\Microsoft\Security Center\Svc] AntiVirusOverride: OK

[HKLM\Software\WOW6432Node\Microsoft\Security Center\Svc] FirewallOverride: OK

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

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

[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings] WarnOnHTTPSToHTTPRedirect: OK

[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

[HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\Results\Install] LastSuccessTime : OK

**---\ Search Generic System Files (24) - 2s**

[MD5.0E8E6463F81C80AFBED533E0F1F8895D] - 01/06/2013 - (.Microsoft Corporation - Windows Explorer.) -- C:\windows\Explorer.exe [2391280] =>.Microsoft Windows®

[MD5.3A6209AC494296C24C2065CB4392B5F4] - 25/07/2012 - (.Microsoft Corporation - Windows host process (Rundll32).) -- C:\windows\System32\rundll32.exe [51712] =>.Microsoft Corporation

[MD5.FE9AB232B56A12224E8A3F3F9878C9A3] - 25/07/2012 - (.Microsoft Corporation - Windows Start-Up Application.) -- C:\windows\System32\Wininit.exe [132608] =>.Microsoft Corporation

[MD5.513A0BEDC45862E8D89B52B272F0B4A3] - 14/12/2015 - (.Microsoft Corporation - Internet Extensions for Win32.) -- C:\windows\System32\wininet.dll [2240000] =>.Microsoft Corporation

[MD5.88B4DA29CF8C3628F3647447FD5CDAE5] - 16/11/2015 - (.Microsoft Corporation - Windows Logon Application.) -- C:\windows\System32\Winlogon.exe [578048] =>.Microsoft Corporation

[MD5.9448F5740A037EC0C18F0E9177232DD0] - 25/07/2012 - (.Microsoft Corporation - Software Licensing Library.) -- C:\windows\System32\sppcomapi.dll [273408] =>.Microsoft Corporation

[MD5.7904C03BF9C0C0337563FFAA97D0ACE8] - 08/10/2014 - (.Microsoft Corporation - DNS Client API DLL.) -- C:\windows\System32\dnsapi.dll [623616] =>.Microsoft Corporation

[MD5.0BE9606A1175C7400ED862991453A847] - 08/10/2014 - (.Microsoft Corporation - DNS Client API DLL.) -- C:\windows\Syswow64\dnsapi.dll [458240] =>.Microsoft Corporation

[MD5.8252EE6D7F87846EA409D0DA602FB1D9] - 13/10/2015 - (.Microsoft Corporation - Ancillary Function Driver for WinSock.) -- C:\windows\System32\drivers\AFD.sys [576512] =>.Microsoft Corporation

[MD5.A721FF570C2387E383BDDEA9632863C9] - 26/07/2012 - (.Microsoft Corporation - ATAPI IDE Miniport Driver.) -- C:\windows\System32\drivers\atapi.sys [25840] =>.Microsoft Windows®

[MD5.990B1BABE6E81FB18E65A87EBEFB1772] - 25/07/2012 - (.Microsoft Corporation - CD-ROM File System Driver.) -- C:\windows\System32\drivers\Cdfs.sys [108544] =>.Microsoft Corporation

[MD5.339BFF85D788268752DA8C9644B188EE] - 25/07/2012 - (.Microsoft Corporation - SCSI CD-ROM Driver.) -- C:\windows\System32\drivers\Cdrom.sys [174080] =>.Microsoft Corporation

[MD5.431141C6859990824D17F71C30A78728] - 15/01/2014 - (.Microsoft Corporation - DFS Namespace Client Driver.) -- C:\windows\System32\drivers\DfsC.sys [118784] =>.Microsoft Corporation

[MD5.58CC013EFA9893057160EDA018D8ADCE] - 15/07/2014 - (.Microsoft Corporation - High Definition Audio Bus Driver.) -- C:\windows\System32\drivers\HDAudBus.sys [71168] =>.Microsoft Corporation

[MD5.C9E9CBF73AFFBFE3E801EFB516787BA3] - 25/07/2012 - (.Microsoft Corporation - i8042 Port Driver.) -- C:\windows\System32\drivers\i8042prt.sys [112640] =>.Microsoft Corporation

[MD5.3969B9C218DD3FAA9F4ED2FFC3651C02] - 25/07/2012 - (.Microsoft Corporation - IP Network Address Translator.) -- C:\windows\System32\drivers\IpNat.sys [145920] =>.Microsoft Corporation

[MD5.6BA2A5D1C74E7CB3AFAF301A7E5D9E44] - 06/01/2015 - (.Microsoft Corporation - Windows NT SMB Minirdr.) -- C:\windows\System32\drivers\MRxSmb.sys [403456] =>.Microsoft Corporation

[MD5.7CEC25C682D319D484630B3952C31A11] - 25/07/2012 - (.Microsoft Corporation - MBT Transport driver.) -- C:\windows\System32\drivers\netBT.sys [331776] =>.Microsoft Corporation

[MD5.7BE3EDFFA3216F989A6BDCB14795DD08] - 26/01/2014 - (.Microsoft Corporation - NT File System Driver.) -- C:\windows\System32\drivers\ntfs.sys [1939288] =>.Microsoft Windows®

[MD5.4563DAF8C6A740AD7F501E219BD10766] - 25/07/2012 - (.Microsoft Corporation - Parallel Port Driver.) -- C:\windows\System32\drivers\Parport.sys [105984] =>.Microsoft Corporation

[MD5.A14D625C5AEE5FFE0F47D1A1D419FAAE] - 25/07/2012 - (.Microsoft Corporation - RAS L2TP mini-port/call-manager driver.) -- C:\windows\System32\drivers\Rasl2tp.sys [124928] =>.Microsoft Corporation

[MD5.B2A3AD74FF2E2FFA73AF2567108231B3] - 25/07/2012 - (.Microsoft Corporation - Microsoft RDP Device redirector.) -- C:\windows\System32\drivers\rdpdr.sys [179712] =>.Microsoft Corporation

[MD5.217AEE5DAE1BEF81A1E9A184C4C0BF6A] - 13/10/2015 - (.Microsoft Corporation - TDI Translation Driver.) -- C:\windows\System32\drivers\tdx.sys [129024] =>.Microsoft Corporation

[MD5.AA37946941ED3805AB3A924965907147] - 04/07/2014 - (.Microsoft Corporation - Volume Shadow Copy Driver.) -- C:\windows\System32\drivers\volsnap.sys [328000] =>.Microsoft Windows®

**---\ Non Microsoft non disabled Windows Services (26) - 4s**

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

O23 - Service: Apple Mobile Device Service (Apple Mobile Device Service) . (.Apple Inc. - MobileDeviceService.) - C:\Program Files\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe =>.Apple Inc.®

O23 - Service: Bonjour Service (Bonjour Service) . (.Apple Inc. - Bonjour Service.) - C:\Program Files\Bonjour\mDNSResponder.exe =>.Apple Inc.®

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

O23 - Service: DbxSvc (DbxSvc) . (.Dropbox, Inc. - Dropbox Service.) - C:\windows\System32\DbxSvc.exe =>.Dropbox, Inc.

O23 - Service: EpsonBidirectionalService (EpsonBidirectionalService) . (.SEIKO EPSON CORPORATION - eEBAPI Core Process module.) - C:\Program Files (x86)\Common Files\EPSON\EBAPI\eEBSvc.exe =>.Seiko Epson Corporation

O23 - Service: EpsonCustomerParticipation (EpsonCustomerParticipation) . (.SEIKO EPSON CORPORATION - Epson Customer Participation.) - C:\Program Files\EPSON\EpsonCustomerParticipation\EPCP.exe {76101A6757EFD8186742057C6A6ACAA4} =>.Seiko Epson Corporation

O23 - Service: Epson Scanner Service (EpsonScanSvc) . (.Seiko Epson Corporation - Epson Scanner Service (64bit).) - C:\windows\system32\EscSvc64.exe =>.Seiko Epson Corporation

O23 - Service: IconMan\_R (IconMan\_R) . (.Realsil Microelectronics Inc. - Realtek Card Reader Patch Tool..) - C:\Program Files (x86)\Realtek\Realtek PCIE Card Reader\RIconMan.exe =>.Realsil Microelectronics Inc.

O23 - Service: Intel(R) Capability Licensing Service Interface (Intel(R) Capability Licensing Service Interface) . (.Intel(R) Corporation - Intel(R) Capability Licensing Service Inter.) - C:\Program Files\Intel\iCLS Client\HeciServer.exe =>.Intel® Upgrade Service®

O23 - Service: Intel(R) ME Service (Intel(R) ME Service) . (.Intel Corporation - Intel(R) ME Service.) - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\FWService\IntelMeFWService.exe =>.Intel Corporation®

O23 - Service: Intel(R) Dynamic Application Loader Host Interface Service (jhi\_service) . (.Intel Corporation - Intel(R) Dynamic Application Loader Host In.) - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\DAL\jhi\_service.exe =>.Intel Corporation®

O23 - Service: Juniper Unified Network Service (JuniperAccessService) . (.Juniper Networks, Inc. - Juniper Access Service.) - C:\Program Files (x86)\Common Files\Juniper Networks\JUNS\dsAccessService.exe =>.Juniper Networks, Inc.®

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

O23 - Service: OfficeScan NT RealTime Scan (ntrtscan) . (.Trend Micro Inc. - Trend Micro Common Client Real-time Scan Se.) - C:\Program Files (x86)\Trend Micro\OfficeScan Client\Ntrtscan.exe =>.Trend Micro, Inc.®

O23 - Service: Realtek Audio Service (RtkAudioService) . (.Realtek Semiconductor - Realtek Audio Service.) - C:\Program Files\Realtek\Audio\HDA\RtkAudioService64.exe =>.Realtek Semiconductor Corp®

O23 - Service: Skype Updater (SkypeUpdate) . (.Skype Technologies - Skype Updater Service.) - C:\Program Files (x86)\Skype\Updater\Updater.exe =>.Skype Software Sarl®

O23 - Service: SMService (SMService) . (.IObit - StartMenu8 Services.) - C:\program files (x86)\IObit\Classic Start\SMService.exe =>.IObit Information Technology®

O23 - Service: TOSHIBA HDD Accelerator Service (THAccelSvc) . (.TOSHIBA CORPORATION - TOSHIBA HDD Accelerator Service.) - C:\Program Files\Toshiba\HDD Accelerator\THAccelSvc.exe =>.TOSHIBA CORPORATION®

O23 - Service: TOSHIBA HDD Protection (Thpsrv) . (.TOSHIBA Corporation - TOSHIBA HDD Protection Service.) - C:\windows\system32\ThpSrv.exe =>.Toshiba Corporation

O23 - Service: OfficeScan NT Listener (tmlisten) . (.Trend Micro Inc. - Trend Micro Common Client Communication Ser.) - C:\Program Files (x86)\Trend Micro\OfficeScan Client\TmListen.exe =>.Trend Micro, Inc.®

O23 - Service: TOSHIBA Optical Disc Drive Service (TODDSrv) . (.TOSHIBA Corporation - TDCSrv Application.) - C:\Windows\system32\TODDSrv.exe =>.Toshiba Corporation

O23 - Service: TOSHIBA eco Utility Service (TOSHIBA eco Utility Service) . (.TOSHIBA Corporation - TOSHIBA eco Utility Service.) - C:\Program Files\Toshiba\Teco\TecoService.exe =>.TOSHIBA CORPORATION®

O23 - Service: Umbrella Roaming Client (Umbrella\_RC) . (.Cisco Systems, Inc. - Umbrella RC Service.) - C:\Program Files (x86)\OpenDNS\Umbrella Roaming Client\ERCService.exe =>.OpenDNS®

O23 - Service: Intel(R) Management and Security Application User Notificat (UNS) . (.Intel Corporation - User Notification Service.) - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\UNS\UNS.exe =>.Intel Corporation®

O23 - Service: WD Drive Manager (WDDriveService) . (.Western Digital Technologies, Inc. - WD Drive Service.) - C:\Program Files (x86)\Western Digital\WD Drive Manager\WDDriveService.exe =>.Western Digital Technologies, Inc.®

**---\ Services not Microsoft (SR=Run, SS=Stop) (35) - 5s**

SR - Auto [21/12/2013] [ 65432] Adobe Acrobat Update Service (AdobeARMservice) . (.Adobe Systems Incorporated.) - C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe =>.Adobe Systems, Incorporated®

SS - Demand [18/03/2018] [ 272384] Adobe Flash Player Update Service (AdobeFlashPlayerUpdateSvc) . (.Adobe Systems Incorporated.) - C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe =>.Adobe Systems Incorporated®

SR - Auto [03/04/2017] [ 83768] Apple Mobile Device Service (Apple Mobile Device Service) . (.Apple Inc..) - C:\Program Files\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe =>.Apple Inc.®

SR - Auto [12/08/2015] [ 462096] Bonjour Service (Bonjour Service) . (.Apple Inc..) - C:\Program Files\Bonjour\mDNSResponder.exe =>.Apple Inc.®

SS - Demand [24/10/2012] [ 277024] Intel(R) Content Protection HECI Service (cphs) . (.Intel Corporation.) - C:\Windows\SysWOW64\IntelCpHeciSvc.exe =>.Intel Corporation - pGFX®

SS - Auto [19/06/2016] [ 143144] Dropbox Update Service (dbupdate) (dbupdate) . (.Dropbox, Inc..) - C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe =>.Dropbox, Inc®

SS - Demand [19/06/2016] [ 143144] Dropbox Update Service (dbupdatem) (dbupdatem) . (.Dropbox, Inc..) - C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe =>.Dropbox, Inc®

SR - Auto [15/03/2018] [ 51024] DbxSvc (DbxSvc) . (.Dropbox, Inc..) - C:\windows\System32\DbxSvc.exe =>.Dropbox, Inc®

SR - Auto [19/12/2006] [ 94208] EpsonBidirectionalService (EpsonBidirectionalService) . (.SEIKO EPSON CORPORATION.) - C:\Program Files (x86)\Common Files\EPSON\EBAPI\eEBSvc.exe =>.Seiko Epson Corporation

SR - Auto [10/03/2018] [ 674768] EpsonCustomerParticipation (EpsonCustomerParticipation) . (.SEIKO EPSON CORPORATION.) - C:\Program Files\EPSON\EpsonCustomerParticipation\EPCP.exe {76101A6757EFD8186742057C6A6ACAA4} =>.Seiko Epson Corporation

SR - Auto [17/05/2012] [ 144560] Epson Scanner Service (EpsonScanSvc) . (.Seiko Epson Corporation.) - C:\windows\system32\EscSvc64.exe =>.SEIKO EPSON Corporation®

SR - Auto [07/08/2012] [ 2451456] IconMan\_R (IconMan\_R) . (.Realsil Microelectronics Inc..) - C:\Program Files (x86)\Realtek\Realtek PCIE Card Reader\RIconMan.exe =>.Realsil Microelectronics Inc.

SR - Auto [20/04/2012] [ 635104] Intel(R) Capability Licensing Service Interface (Intel(R) Capability Licensing Service Interface) . (.Intel(R) Corporation.) - C:\Program Files\Intel\iCLS Client\HeciServer.exe =>.Intel® Upgrade Service®

SR - Auto [18/07/2012] [ 128896] Intel(R) ME Service (Intel(R) ME Service) . (.Intel Corporation.) - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\FWService\IntelMeFWService.exe =>.Intel Corporation®

SR - Demand [09/05/2017] [ 689464] iPod Service (iPod Service) . (.Apple Inc..) - C:\Program Files\iPod\bin\iPodService.exe =>.Apple Inc.®

SR - Auto [18/07/2012] [ 165760] Intel(R) Dynamic Application Loader Host Interface Service (jhi\_service) . (.Intel Corporation.) - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\DAL\jhi\_service.exe =>.Intel Corporation®

SR - Auto [15/04/2013] [ 162136] Juniper Unified Network Service (JuniperAccessService) . (.Juniper Networks, Inc..) - C:\Program Files (x86)\Common Files\Juniper Networks\JUNS\dsAccessService.exe =>.Juniper Networks, Inc.®

SR - Auto [18/07/2012] [ 276864] Intel(R) Management and Security Application Local Manageme (LMS) . (.Intel Corporation.) - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe =>.Intel Corporation®

SS - Demand [25/02/2018] [ 194512] Mozilla Maintenance Service (MozillaMaintenance) . (.Mozilla Foundation.) - C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe =>.Mozilla Corporation®

SR - Auto [07/07/2014] [ 4638784] OfficeScan NT RealTime Scan (ntrtscan) . (.Trend Micro Inc..) - C:\Program Files (x86)\Trend Micro\OfficeScan Client\Ntrtscan.exe =>.Trend Micro, Inc.®

SR - Auto [05/12/2012] [ 201872] Realtek Audio Service (RtkAudioService) . (.Realtek Semiconductor.) - C:\Program Files\Realtek\Audio\HDA\RtkAudioService64.exe =>.Realtek Semiconductor Corp®

SS - Auto [16/01/2017] [ 317400] Skype Updater (SkypeUpdate) . (.Skype Technologies.) - C:\Program Files (x86)\Skype\Updater\Updater.exe =>.Skype Software Sarl®

SR - Auto [16/01/2017] [ 1077536] SMService (SMService) . (.IObit.) - C:\program files (x86)\IObit\Classic Start\SMService.exe =>.IObit Information Technology®

SR - Auto [10/08/2012] [ 214488] TOSHIBA HDD Accelerator Service (THAccelSvc) . (.TOSHIBA CORPORATION.) - C:\Program Files\Toshiba\HDD Accelerator\THAccelSvc.exe =>.TOSHIBA CORPORATION®

SR - Auto [03/08/2012] [ 566696] TOSHIBA HDD Protection (Thpsrv) . (.TOSHIBA Corporation.) - C:\windows\system32\ThpSrv.exe =>.TOSHIBA CORPORATION®

SR - Demand [08/12/2015] [ 53040] TMachInfo (TMachInfo) . (.TOSHIBA Corporation.) - C:\Program Files\Toshiba\TOSHIBA Service Station\TMachInfo.exe =>.TOSHIBA CORPORATION®

SR - Demand [19/03/2014] [ 575024] Trend Micro Unauthorized Change Prevention Service (TMBMServer) . (.Trend Micro Inc..) - C:\Program Files (x86)\Trend Micro\BM\TMBMSRV.exe =>.Trend Micro, Inc.®

SR - Demand [07/04/2014] [ 701064] OfficeScan Common Client Solution Framework (tmccsf) . (.Trend Micro Inc..) - C:\Program Files (x86)\Trend Micro\OfficeScan Client\CCSF\TmCCSF.exe =>.Trend Micro, Inc.®

SR - Auto [07/07/2014] [ 4628200] OfficeScan NT Listener (tmlisten) . (.Trend Micro Inc..) - C:\Program Files (x86)\Trend Micro\OfficeScan Client\TmListen.exe =>.Trend Micro, Inc.®

SR - Auto [28/07/2009] [ 140632] TOSHIBA Optical Disc Drive Service (TODDSrv) . (.TOSHIBA Corporation.) - C:\Windows\system32\TODDSrv.exe =>.TOSHIBA CORPORATION®

SR - Auto [24/08/2012] [ 291240] TOSHIBA eco Utility Service (TOSHIBA eco Utility Service) . (.TOSHIBA Corporation.) - C:\Program Files\Toshiba\Teco\TecoService.exe =>.TOSHIBA CORPORATION®

SS - Demand [28/07/2012] [ 458152] TPCH Service (TPCHSrv) . (.TOSHIBA Corporation.) - C:\Program Files\Toshiba\TPHM\TPCHSrv.exe =>.TOSHIBA CORPORATION®

SR - Auto [12/06/2017] [ 36632] Umbrella Roaming Client (Umbrella\_RC) . (.Cisco Systems, Inc..) - C:\Program Files (x86)\OpenDNS\Umbrella Roaming Client\ERCService.exe =>.OpenDNS®

SR - Auto [18/07/2012] [ 364416] Intel(R) Management and Security Application User Notificat (UNS) . (.Intel Corporation.) - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\UNS\UNS.exe =>.Intel Corporation®

SR - Auto [07/12/2015] [ 308088] WD Drive Manager (WDDriveService) . (.Western Digital Technologies, Inc..) - C:\Program Files (x86)\Western Digital\WD Drive Manager\WDDriveService.exe =>.Western Digital Technologies, Inc.®

**---\ Task Planned Automatically (Register) (132) - 7s**

O38 - TASK: {10D85952-E3F6-47A1-96CF-5E1C2D874EA6} [64Bits][\Microsoft\Windows\SystemRestore\SR] - (.Microsoft Corporation - Microsoft® Windows System Protection backgr.) -- C:\windows\system32\srtasks.exe [56832] =>.Microsoft Corporation

O38 - TASK: {115A30F5-9629-4E2E-993E-F2EF77734558} [64Bits][\Microsoft\Windows\Windows Filtering Platform\BfeOnServiceStartTypeChange] - (.Microsoft Corporation - Base Filtering Engine.) -- C:\Windows\System32\bfe.dll [723968] =>.Microsoft Corporation

O38 - TASK: {16E0B46F-CBF0-4826-8301-6C6D8C1C94AD} [64Bits][\Microsoft\Windows\Setup\EOSNotify] - (.Microsoft Corporation - EOS Notification.) -- C:\windows\system32\EOSNotify.exe [282624] =>.Microsoft Corporation

O38 - TASK: {1AAFF332-5C62-4558-9991-DAA649C4C9C5} [64Bits][\Microsoft\Windows\Sysmain\WsSwapAssessmentTask] - (.Microsoft Corporation - Superfetch Service Host.) -- C:\Windows\System32\sysmain.dll [1333248] =>.Microsoft Corporation

O38 - TASK: {1D076FF4-AB47-4BA3-A27D-87AE1F46D4B3} [64Bits][\Microsoft\Windows\WindowsBackup\AutomaticBackup] - (.Microsoft Corporation - Microsoft® Windows Backup Engine.) -- C:\Windows\System32\sdengin2.dll [1079296] =>.Microsoft Corporation

O38 - TASK: {1E6440D0-D6AD-4C3C-9489-3CA13BDB619B} [64Bits][\Microsoft\Windows\RemoteAssistance\RemoteAssistanceTask] - (.Microsoft Corporation - Windows Remote Assistance COM Server.) -- C:\Windows\System32\raserver.exe [115200] =>.Microsoft Corporation

O38 - TASK: {23A5D8BE-9196-40EB-BD89-794398B2B073} [64Bits][\Microsoft\Windows\WS\WSRefreshBannedAppsListTask] - (.Microsoft Corporation - Windows Store Licensing Client.) -- C:\Windows\System32\WSClient.dll [204800] =>.Microsoft Corporation

O38 - TASK: {23C5C1A4-5B68-4DAB-93CF-DA727538396A} [64Bits][\Microsoft\Office\OfficeBackgroundTaskHandlerRegistration] - (.Microsoft Corporation - Background task for Office flighting system.) -- C:\Program Files (x86)\Microsoft Office\root\Office16\officebackgroundtaskhandler.exe [1438384] =>.Microsoft Corporation

O38 - TASK: {299D4179-2722-40D9-BE9E-51E04DFF5A16} [64Bits][\Microsoft\Windows\AppID\VerifiedPublisherCertStoreCheck] - (.Microsoft Corporation - AppID Certificate Store Verification Task.) -- C:\windows\system32\appidcertstorecheck.exe [18432] =>.Microsoft Corporation

O38 - TASK: {2A959D70-7801-4CC8-ADC6-2AF8646E7CF2} [64Bits][\Microsoft\Windows\Windows Error Reporting\QueueReporting] - (.Microsoft Corporation - Windows Problem Reporting.) -- C:\Windows\System32\wermgr.exe [136768] =>.Microsoft Corporation

O38 - TASK: {2DF79502-20F8-4877-9B95-712CBED8C785} [64Bits][\Microsoft\Windows\Customer Experience Improvement Program\Uploader] - (.Microsoft Corporation - Windows SQM Consolidator.) -- C:\windows\system32\WSqmCons.exe [360960] =>.Microsoft Corporation

O38 - TASK: {307D8C75-FDA3-49D3-AA9F-DB79F405FB59} [64Bits][\Microsoft\Windows\Autochk\Proxy] - (.Microsoft Corporation - Autochk Proxy DLL.) -- C:\Windows\System32\acproxy.dll [12288] =>.Microsoft Corporation

O38 - TASK: {368FCF03-7D08-4E0D-8CF0-8E62F92032D6} [64Bits][\TOSHIBA\Service Station] - (.TOSHIBA Corporation - TOSHIBA Service Station.) -- C:\Program Files\Toshiba\Toshiba Service Station\ToshibaServiceStation.exe [700040] =>.Toshiba Corporation

O38 - TASK: {3F2ADA94-AD3A-4888-8AD6-BD748EDF9B58} [64Bits][\Apple Diagnostics] - (.Apple Inc. - EReporter.exe.) -- C:\Program Files (x86)\Common Files\Apple\Internet Services\EReporter.exe [67896] =>.Apple Inc.

O38 - TASK: {40525C58-79C2-47A1-9AA2-F1D7FC4F0691} [64Bits][\Microsoft\Windows\WindowsBackup\ConfigNotification] - (.Microsoft Corporation - Microsoft® Windows Backup.) -- C:\windows\System32\sdclt.exe [1210368] =>.Microsoft Corporation

O38 - TASK: {483A8F5C-5D26-44B5-B49E-AF6741D1BBEB} [64Bits][\Microsoft\Windows\Mobile Broadband Accounts\MNO Metadata Parser] - (.Microsoft Corporation - Mobile Broadband Account Experience Parser.) -- C:\windows\System32\MbaeParserTask.exe [80896] =>.Microsoft Corporation

O38 - TASK: {50C93601-28B7-4CFC-9DD9-7CBC89A28C57} [64Bits][\Microsoft\Office\Office Subscription Maintenance] - (.Microsoft Corporation - Office Subscription Licensing Heartbeat.) -- C:\Program Files (x86)\Microsoft Office\root\vfs\ProgramFilesCommonx86\Microsoft Shared\OFFICE16\OLicenseHeartbeat.exe [679088] =>.Microsoft Corporation

O38 - TASK: {5CB06E59-0EC1-444A-A3B0-EAEE9BCC9F81} [64Bits][\Microsoft\Windows\Setup\8.1 auto install ping] - (.Microsoft Corporation - AutoUpdate Implementation.) -- C:\windows\system32\AutoUpdate.exe [596480] =>.Microsoft Corporation

O38 - TASK: {5F6E7439-D246-402A-AB89-BF5A32EEA3CE} [64Bits][\Microsoft\Office\OfficeTelemetryAgentFallBack2016] - (.Microsoft Corporation - Office Telemetry Agent.) -- C:\Program Files (x86)\Microsoft Office\root\Office16\msoia.exe [2278576] =>.Microsoft Corporation

O38 - TASK: {5F91E9AC-65DE-48D6-9C8E-CAF711915E8E} [64Bits][\Norton Anti-Theft\Norton Error Analyzer] - (.Symantec - Norton Error Analyzer.) -- C:\Program Files (x86)\Norton Anti-Theft\Engine\1.8.0.32\SymErr.exe (.not file.) [0] (.Orphan.) =>.SUP.Orphan

O38 - TASK: {60ED562A-9AAB-46A5-BFE2-9A134BCBC1FC} [64Bits][\Norton Anti-Theft\Norton Error Processor] - (.Symantec - Norton Error Processor.) -- C:\Program Files (x86)\Norton Anti-Theft\Engine\1.8.0.32\SymErr.exe (.not file.) [0] (.Orphan.) =>.SUP.Orphan

O38 - TASK: {627441F3-8526-4B62-BF9A-1A3EA414E71A} [64Bits][\Microsoft\Windows\SpacePort\SpaceAgentTask] - (.Microsoft Corporation - Storage Spaces Settings.) -- C:\windows\system32\SpaceAgent.exe [102400] =>.Microsoft Corporation

O38 - TASK: {6E9DE125-5583-4031-B572-FEE48F25CFFF} [64Bits][\Microsoft\Windows\Shell\FamilySafetyMonitor] - (.Microsoft Corporation - Family Safety Monitor.) -- C:\windows\System32\wpcmon.exe [2397184] =>.Microsoft Corporation

O38 - TASK: {7096CB5A-E8C5-4DB1-9262-E0DBE560424A} [64Bits][\Driver Booster Scan] - (.IObit - Driver Booster Scheduler.) -- C:\Program Files (x86)\IObit\Driver Booster\Scheduler.exe [67392] =>.IObit

O38 - TASK: {710D1009-6505-40D8-8D83-962A1985732C} [64Bits][\Microsoft\Windows\Location\Notifications] - (.Microsoft Corporation - Location Activity.) -- C:\Windows\System32\LocationNotifications.exe [86528] =>.Microsoft Corporation

O38 - TASK: {7417D36D-2BF0-4E51-871A-37E4B73EC900} [64Bits][\Microsoft\Windows\AppID\PolicyConverter] - (.Microsoft Corporation - AppID Policy Converter Task.) -- C:\windows\system32\appidpolicyconverter.exe [139776] =>.Microsoft Corporation

O38 - TASK: {75501669-22A7-4B7A-B445-5FEBA4CE9865} [64Bits][\EPSON XP-420 Series Update {CBC51009-C0F1-4B68-93C8-C3317DDE4B46}] - (.SEIKO EPSON CORPORATION - E\_DTSKSD.EXE.) -- C:\windows\system32\spool\DRIVERS\x64\3\E\_YTSNAE.EXE [690536] =>.Seiko Epson Corporation

O38 - TASK: {77770830-8886-4FA2-B3D1-54EAAF9323E7} [64Bits][\Driver Booster Update] - (.IObit - Driver Booster Updater.) -- C:\Program Files (x86)\IObit\Driver Booster\AutoUpdate.exe [1392960] =>.IObit

O38 - TASK: {82B820F9-DE95-401A-BC63-421918B11F56} [64Bits][\Microsoft\Windows\MUI\LPRemove] - (.Microsoft Corporation - MUI Language pack cleanup.) -- C:\windows\system32\lpremove.exe [92160] =>.Microsoft Corporation

O38 - TASK: {8E549D48-5F2A-4713-BD02-E927F60D78C6} [64Bits][\Microsoft\Windows\Defrag\ScheduledDefrag] - (.Microsoft Corp. - Disk Defragmenter Module.) -- C:\windows\system32\defrag.exe [181248] =>.Microsoft Corp.

O38 - TASK: {8E7CB33A-A093-4773-BB05-57CF44CFEE48} [64Bits][\DropboxUpdateTaskMachineUA] - (.Dropbox, Inc. - Dropbox Update.) -- C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe [143144] =>.Dropbox, Inc.

O38 - TASK: {93BA554C-5F5A-438D-AA27-111B286A2235} [64Bits][\Microsoft\Windows\Application Experience\ProgramDataUpdater] - (.Microsoft Corporation - Program Compatibility Data Updater.) -- C:\windows\system32\invagent.dll [294912] =>.Microsoft Corporation

O38 - TASK: {981E3FDD-7FB5-4C29-99B0-9C462B6DEF34} [64Bits][\Microsoft\Office\OfficeBackgroundTaskHandlerLogon] - (.Microsoft Corporation - Background task for Office flighting system.) -- C:\Program Files (x86)\Microsoft Office\root\Office16\officebackgroundtaskhandler.exe [1438384] =>.Microsoft Corporation

O38 - TASK: {9B87DD21-09F6-4AC2-80DE-8AD9FBB5F199} [64Bits][\EPSON XP-420 Series Update {7506ED29-D2B3-408F-9C39-C6870A815C91}] - (.SEIKO EPSON CORPORATION - E\_DTSKSD.EXE.) -- C:\windows\system32\spool\DRIVERS\x64\3\E\_YTSNAE.EXE [690536] =>.Seiko Epson Corporation

O38 - TASK: {9E1F6F82-181A-491D-A86B-BEB2242D46BC} [64Bits][\Microsoft\Office\OfficeTelemetryAgentFallBack] - (.Microsoft Corporation - Office Telemetry Agent.) -- C:\Program Files\Microsoft Office\Office15\msoia.exe [376496] =>.Microsoft Corporation

O38 - TASK: {9F1578F2-3470-4928-BC4F-310518E1E9D8} [64Bits][\Microsoft\Windows\UPnP\UPnPHostConfig] - (.Microsoft Corporation - Service Control Manager Configuration Tool.) -- C:\Windows\System32\sc.exe [66560] =>.Microsoft Corporation

O38 - TASK: {A3F09DBE-84D3-4A83-BD57-6A4DB110A738} [64Bits][\Microsoft\Office\Office Automatic Updates 2.0] - (.Microsoft Corporation - Microsoft Office Click-to-Run Client.) -- C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe [18136240] =>.Microsoft Corporation

O38 - TASK: {A6BDEA16-0910-4A1F-82FA-FED3C468394F} [64Bits][\Microsoft\Windows\Windows Media Sharing\UpdateLibrary] - (.Microsoft Corporation - Windows Media Player Network Sharing Servic.) -- C:\Program Files\Windows Media Player\wmpnscfg.exe [68096] =>.Microsoft Corporation

O38 - TASK: {A72208BF-7A49-4FB8-B684-252375F3443A} [64Bits][\Microsoft\Windows\WS\License Validation] - (.Microsoft Corporation - Windows Store Licensing Client.) -- C:\Windows\System32\WSClient.dll [204800] =>.Microsoft Corporation

O38 - TASK: {A8850237-EBE8-4FC9-B44A-E08BF153C3D9} [64Bits][\AVG-Secure-Search-Update\_0214b\_rel] - (.Copyright (C) 2011 . All rights reserved. - .) -- C:\Program Files (x86)\AVG SafeGuard toolbar\AVG-Secure-Search-Update\_0214b.exe [2606616]

O38 - TASK: {AA0CF02E-543A-42CE-BD31-A987AA663C97} [64Bits][\{D6F156B6-B064-4539-92BF-5148DDA2DE3C}] - (.BUFFALO INC. - BUFFALO tool.) -- C:\Windows\UN091222.EXE [485272] =>.BUFFALO INC.

O38 - TASK: {AF711E7E-2FB4-4361-AC09-DB15D43A66DF} [64Bits][\Adobe Flash Player Updater] - (.Adobe Systems Incorporated - Adobe® Flash® Player Update Service 29.0 r0.) -- C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe [272384] =>.Adobe Systems Incorporated

O38 - TASK: {B0B0C657-C55E-4832-8E0F-120F4860A36F} [64Bits][\OneDrive Standalone Update Task-S-1-5-21-2870124582-2670056687-1688047813-1001] - (.Microsoft Corporation - Standalone Updater.) -- C:\Users\Myriam\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe [2291360] =>.Microsoft Corporation

O38 - TASK: {B9CF3765-5761-4772-A0AF-55865ACB2A81} [64Bits][\Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticResolver] - (.Microsoft Corporation - Windows Disk Diagnostic User Resolver.) -- C:\windows\system32\DFDWiz.exe [77824] =>.Microsoft Corporation

O38 - TASK: {BEFC95F3-BF2B-4EA9-8A63-85A8326C1C1F} [64Bits][\Microsoft\Office\OfficeTelemetryAgentLogOn] - (.Microsoft Corporation - Office Telemetry Agent.) -- C:\Program Files\Microsoft Office\Office15\msoia.exe [376496] =>.Microsoft Corporation

O38 - TASK: {BF1E62E2-FFE9-4644-B716-878B3F48BD8F} [64Bits][\Driver Booster SkipUAC (Myriam)] - (.IObit - Driver Booster 2.) -- C:\Program Files (x86)\IObit\Driver Booster\DriverBooster.exe [4139840] =>.IObit

O38 - TASK: {C6A88F2D-53D2-4805-9D69-443738A1847C} [64Bits][\Microsoft\Windows\ApplicationData\CleanupTemporaryState] - (.Microsoft Corporation - Windows Application Data API Server.) -- C:\Windows\System32\Windows.Storage.ApplicationData.dll [175616] =>.Microsoft Corporation

O38 - TASK: {C772D868-20AA-486B-9279-F62850BD871D} [64Bits][\{7A4FCD95-FFBF-464C-B5B8-1BB5836C4EB6}] - (...) -- F:\msert.exe (.not file.) [0] (.Orphan.) =>.SUP.Orphan

O38 - TASK: {C8A68697-E7BB-4FE9-97AD-362141F3F755} [64Bits][\StartMenu8\_Start] - (.MYMI\Myriam - .) -- C:\program files (x86)\IObit\Classic Start\Start\_Active.exe [22816]

O38 - TASK: {D0D879C7-4CBE-4133-821A-47B1AC32EB4B} [64Bits][\Microsoft\Office\OfficeTelemetryAgentLogOn2016] - (.Microsoft Corporation - Office Telemetry Agent.) -- C:\Program Files (x86)\Microsoft Office\root\Office16\msoia.exe [2278576] =>.Microsoft Corporation

O38 - TASK: {D96EBD61-F23A-4F04-B185-A962DB97F5DD} [64Bits][\AVG-Secure-Search-Update\_0214b\_rmv] - (.Copyright (C) 2011 . All rights reserved. - .) -- C:\Program Files (x86)\AVG SafeGuard toolbar\AVG-Secure-Search-Update\_0214b.exe [2606616]

O38 - TASK: {DC2DF303-DC14-470B-B6C0-48FE0F20364D} [64Bits][\Microsoft\Windows\WindowsBackup\Windows Backup Monitor] - (.Microsoft Corporation - Microsoft® Windows Backup.) -- C:\windows\System32\sdclt.exe [1210368] =>.Microsoft Corporation

O38 - TASK: {DC37E15A-4C4B-4A71-80F0-6535827D09D4} [64Bits][\WPD\SqmUpload\_S-1-5-21-2870124582-2670056687-1688047813-1001] - (.Microsoft Corporation - Windows Portable Device API Components.) -- C:\Windows\System32\portabledeviceapi.dll [619520] =>.Microsoft Corporation

O38 - TASK: {DCBC3E2C-F360-4BBE-BB47-52004834554C} [64Bits][\EPSON XP-420 Series Update {EE36AA76-8C02-452D-AA01-97A485E70511}] - (.SEIKO EPSON CORPORATION - E\_DTSKSD.EXE.) -- C:\windows\system32\spool\DRIVERS\x64\3\E\_YTSNAE.EXE [690536] =>.Seiko Epson Corporation

O38 - TASK: {DEA0CD22-6315-4156-BBBF-379E19D52D4A} [64Bits][\Apple\AppleSoftwareUpdate] - (.Apple Inc. - Apple Software Update.) -- C:\Program Files (x86)\Apple Software Update\SoftwareUpdate.exe [570240] =>.Apple Inc.

O38 - TASK: {DF34FF18-02C7-4293-87DD-945DF34EE050} [64Bits][\DropboxUpdateTaskMachineCore] - (.Dropbox, Inc. - Dropbox Update.) -- C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe [143144] =>.Dropbox, Inc.

O38 - TASK: {E464450F-D903-4BE1-82D8-72F637A48BEC} [64Bits][\Microsoft\Windows\WindowsUpdate\Scheduled Start] - (.Microsoft Corporation - Service Control Manager Configuration Tool.) -- C:\Windows\System32\sc.exe [66560] =>.Microsoft Corporation

O38 - TASK: {E8DAA09B-DF2A-4951-9134-6FA9587793F9} [64Bits][\Microsoft\Windows\Plug and Play\Sysprep Generalize Drivers] - (.Microsoft Corporation - Driver Installation Module.) -- C:\Windows\System32\drvinst.exe [92672] =>.Microsoft Corporation

O38 - TASK: {EAD237E7-D276-4257-9F16-51DF41548733} [64Bits][\Microsoft\Windows\Time Synchronization\SynchronizeTime] - (.Microsoft Corporation - Service Control Manager Configuration Tool.) -- C:\Windows\System32\sc.exe [66560] =>.Microsoft Corporation

O38 - TASK: {EBB3C98D-55E1-456D-BF70-D05995AE71C9} [64Bits][\Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser] - (.Microsoft Corporation - Microsoft Compatibility Telemetry.) -- C:\windows\system32\CompatTelRunner.exe [50368] =>.Microsoft Corporation

O38 - TASK: {EBF06DEC-4228-4813-AC0C-62821AE4E330} [64Bits][\Microsoft\Windows\Application Experience\StartupAppTask] - (.Microsoft Corporation - Startup scan task DLL.) -- C:\Windows\System32\Startupscan.dll [17408] =>.Microsoft Corporation

O38 - TASK: {F1B0B509-9478-4AB2-A8CD-A6E9BE3E7C90} [64Bits][\Microsoft\Windows\Bluetooth\UninstallDeviceTask] - (.Microsoft Corporation - Bluetooth Uninstall Device Task.) -- C:\Windows\System32\BthUdTask.exe [37376] =>.Microsoft Corporation

O38 - TASK: {F64ED41B-18B4-4F36-959D-0F00EC7E1136} [64Bits][\Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticDataCollector] - (.Microsoft Corporation - Windows Disk Failure Diagnostic Module.) -- C:\Windows\System32\dfdts.dll [44544] =>.Microsoft Corporation

O38 - TASK: {F6EEB348-4FCE-484C-B5EE-7FDB5F66360C} [64Bits][\Microsoft\Windows\Customer Experience Improvement Program\Consolidator] - (.Microsoft Corporation - Windows SQM Consolidator.) -- C:\windows\System32\wsqmcons.exe [360960] =>.Microsoft Corporation

O38 - TASK: {FABA927C-6F55-4E10-A056-61F9D91A9AFE} [64Bits][\Microsoft\Office\Office 15 Subscription Heartbeat] - (.Microsoft Office - Task used to ensure that the Microsoft Offi.) -- C:\Program Files\Common Files\Microsoft Shared\Office15\OLicenseHeartbeat.exe (.not file.) [0] (.Orphan.) =>.SUP.Orphan

O38 - TASK: {FCDB6C27-CE10-4CAC-9BD1-D02C1E1FE8F1} [64Bits][\AV\_PWB] - (.WORKGROUP\MYMI$ - .) -- C:\Program Files (x86)\AVG SafeGuard toolbar\BundleInstall.exe (.not file.) [0] (.Orphan.)[/HP='http://mysearch.avg.com/?cid={0B7C672A-AF6C-4872-AC3D-C34268D367FB}&mid=b916433b2baa47d39dc269c1a5fb8021-18bcd87b26a5ed9451abc4cb8aeb66ef9ebec201&lang=en&ds=dl011&pr=sa&d=2013-07-25 21:02:47&v=17.1.3.3&pid=safeguard&sg=78&sap=hp' /IE=1 /FF=1 /CH=1 /UPDATE=1 /INSTID=1 /FROMSCHEDULER=1] =>Adware.TasksRedirect

C:\windows\System32\Tasks\Microsoft\Windows\SystemRestore\SR - (.Microsoft Corporation.) -- C:\windows\system32\srtasks.exe [ExecuteScheduledSPPCreation] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\Windows Filtering Platform\BfeOnServiceStartTypeChange - (.Microsoft Corporation.) -- C:\Windows\System32\bfe.dll [bfe.dll] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\Setup\EOSNotify - (.Microsoft Corporation.) -- C:\windows\system32\EOSNotify.exe [] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\Sysmain\WsSwapAssessmentTask - (.Microsoft Corporation.) -- C:\Windows\System32\sysmain.dll [sysmain.dll] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\WindowsBackup\AutomaticBackup - (.Microsoft Corporation.) -- C:\Windows\System32\sdengin2.dll [sdengin2.dll] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\RemoteAssistance\RemoteAssistanceTask - (.Microsoft Corporation.) -- C:\Windows\System32\raserver.exe [/offerraupdate] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\WS\WSRefreshBannedAppsListTask - (.Microsoft Corporation.) -- C:\Windows\System32\WSClient.dll [WSClient.dll] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Office\OfficeBackgroundTaskHandlerRegistration - (.Microsoft Corporation.) -- C:\Program Files (x86)\Microsoft Office\root\Office16\officebackgroundtaskhandler.exe [] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\AppID\VerifiedPublisherCertStoreCheck - (.Microsoft Corporation.) -- C:\windows\system32\appidcertstorecheck.exe [] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\Windows Error Reporting\QueueReporting - (.Microsoft Corporation.) -- C:\Windows\System32\wermgr.exe [-queuereporting] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\Customer Experience Improvement Program\Uploader - (.Microsoft Corporation.) -- C:\windows\system32\WSqmCons.exe [-u] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\Autochk\Proxy - (.Microsoft Corporation.) -- C:\Windows\System32\acproxy.dll [acproxy.dll] =>.Microsoft Corporation

C:\windows\System32\Tasks\TOSHIBA\Service Station - (.TOSHIBA Corporation.) -- C:\Program Files\Toshiba\Toshiba Service Station\ToshibaServiceStation.exe [/hide] =>.Toshiba Corporation

C:\windows\System32\Tasks\Apple Diagnostics - (.Apple Inc..) -- C:\Program Files (x86)\Common Files\Apple\Internet Services\EReporter.exe [] =>.Apple Inc.

C:\windows\System32\Tasks\Microsoft\Windows\WindowsBackup\ConfigNotification - (.Microsoft Corporation.) -- C:\windows\System32\sdclt.exe [/CONFIGNOTIFICATION] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\Mobile Broadband Accounts\MNO Metadata Parser - (.Microsoft Corporation.) -- C:\windows\System32\MbaeParserTask.exe [] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Office\Office Subscription Maintenance - (.Microsoft Corporation.) -- C:\Program Files (x86)\Microsoft Office\root\vfs\ProgramFilesCommonx86\Microsoft Shared\OFFICE16\OLicenseHeartbeat.exe [] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\Setup\8.1 auto install ping - (.Microsoft Corporation.) -- C:\windows\system32\AutoUpdate.exe [/Ping] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Office\OfficeTelemetryAgentFallBack2016 - (.Microsoft Corporation.) -- C:\Program Files (x86)\Microsoft Office\root\Office16\msoia.exe [scan upload mininterval:2880] =>.Microsoft Corporation

C:\windows\System32\Tasks\Norton Anti-Theft\Norton Error Analyzer - (.Symantec.) -- C:\Program Files (x86)\Norton Anti-Theft\Engine\1.8.0.32\SymErr.exe (.not file.) [/analyze] (.Orphan.) =>.SUP.Orphan

C:\windows\System32\Tasks\Norton Anti-Theft\Norton Error Processor - (.Symantec.) -- C:\Program Files (x86)\Norton Anti-Theft\Engine\1.8.0.32\SymErr.exe (.not file.) [/submit] (.Orphan.) =>.SUP.Orphan

C:\windows\System32\Tasks\Microsoft\Windows\SpacePort\SpaceAgentTask - (.Microsoft Corporation.) -- C:\windows\system32\SpaceAgent.exe [] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\Shell\FamilySafetyMonitor - (.Microsoft Corporation.) -- C:\windows\System32\wpcmon.exe [] =>.Microsoft Corporation

C:\windows\System32\Tasks\Driver Booster Scan - (.IObit.) -- C:\Program Files (x86)\IObit\Driver Booster\Scheduler.exe [/scan] =>.IObit

C:\windows\System32\Tasks\Microsoft\Windows\Location\Notifications - (.Microsoft Corporation.) -- C:\Windows\System32\LocationNotifications.exe [] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\AppID\PolicyConverter - (.Microsoft Corporation.) -- C:\windows\system32\appidpolicyconverter.exe [] =>.Microsoft Corporation

C:\windows\System32\Tasks\EPSON XP-420 Series Update {CBC51009-C0F1-4B68-93C8-C3317DDE4B46} - (.SEIKO EPSON CORPORATION.) -- C:\windows\system32\spool\DRIVERS\x64\3\E\_YTSNAE.EXE [/EXE:'{CBC51009-C0F1-4B68-93C8-C3317DDE4B46}] =>.Seiko Epson Corporation

C:\windows\System32\Tasks\Driver Booster Update - (.IObit.) -- C:\Program Files (x86)\IObit\Driver Booster\AutoUpdate.exe [/auto] =>.IObit

C:\windows\System32\Tasks\Microsoft\Windows\MUI\LPRemove - (.Microsoft Corporation.) -- C:\windows\system32\lpremove.exe [] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\Defrag\ScheduledDefrag - (.Microsoft Corp..) -- C:\windows\system32\defrag.exe [-c -h -o -$] =>.Microsoft Corp.

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

C:\windows\System32\Tasks\Microsoft\Windows\Application Experience\ProgramDataUpdater - (.Microsoft Corporation.) -- C:\windows\system32\invagent.dll [C:\windows\system32\invagent.dll] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Office\OfficeBackgroundTaskHandlerLogon - (.Microsoft Corporation.) -- C:\Program Files (x86)\Microsoft Office\root\Office16\officebackgroundtaskhandler.exe [] =>.Microsoft Corporation

C:\windows\System32\Tasks\EPSON XP-420 Series Update {7506ED29-D2B3-408F-9C39-C6870A815C91} - (.SEIKO EPSON CORPORATION.) -- C:\windows\system32\spool\DRIVERS\x64\3\E\_YTSNAE.EXE [/EXE:'{7506ED29-D2B3-408F-9C39-C6870A815C91}] =>.Seiko Epson Corporation

C:\windows\System32\Tasks\Microsoft\Office\OfficeTelemetryAgentFallBack - (.Microsoft Corporation.) -- C:\Program Files\Microsoft Office\Office15\msoia.exe [scan upload mininterval:2880] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\UPnP\UPnPHostConfig - (.Microsoft Corporation.) -- C:\Windows\System32\sc.exe [config upnphost start= auto] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Office\Office Automatic Updates 2.0 - (.Microsoft Corporation.) -- C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe [/frequentupdate SCHEDULEDTASK displaylevel=False] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\Windows Media Sharing\UpdateLibrary - (.Microsoft Corporation.) -- C:\Program Files\Windows Media Player\wmpnscfg.exe [] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\WS\License Validation - (.Microsoft Corporation.) -- C:\Windows\System32\WSClient.dll [WSClient.dll] =>.Microsoft Corporation

C:\windows\System32\Tasks\AVG-Secure-Search-Update\_0214b\_rel - (.Copyright (C) 2011 . All rights reserved..) -- C:\Program Files (x86)\AVG SafeGuard toolbar\AVG-Secure-Search-Update\_0214b.exe [--RELAUNCH=1 --CMPID=0214b]

C:\windows\System32\Tasks\{D6F156B6-B064-4539-92BF-5148DDA2DE3C} - (.BUFFALO INC..) -- C:\Windows\UN091222.EXE [C:\Windows\UN091222.EXE] =>.BUFFALO INC.

C:\windows\System32\Tasks\Adobe Flash Player Updater - (.Adobe Systems Incorporated.) -- C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe [] =>.Adobe Systems Incorporated

C:\windows\System32\Tasks\OneDrive Standalone Update Task-S-1-5-21-2870124582-2670056687-1688047813-1001 - (.Microsoft Corporation.) -- C:\Users\Myriam\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe [] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticResolver - (.Microsoft Corporation.) -- C:\windows\system32\DFDWiz.exe [] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Office\OfficeTelemetryAgentLogOn - (.Microsoft Corporation.) -- C:\Program Files\Microsoft Office\Office15\msoia.exe [scan upload] =>.Microsoft Corporation

C:\windows\System32\Tasks\Driver Booster SkipUAC (Myriam) - (.IObit.) -- C:\Program Files (x86)\IObit\Driver Booster\DriverBooster.exe [/skipuac] =>.IObit

C:\windows\System32\Tasks\Microsoft\Windows\ApplicationData\CleanupTemporaryState - (.Microsoft Corporation.) -- C:\Windows\System32\Windows.Storage.ApplicationData.dll [Windows.Storage.ApplicationData.dll] =>.Microsoft Corporation

C:\windows\System32\Tasks\{7A4FCD95-FFBF-464C-B5B8-1BB5836C4EB6} - (...) -- F:\msert.exe (.not file.) [F:\msert.exe] (.Orphan.) =>.SUP.Orphan

C:\windows\System32\Tasks\StartMenu8\_Start - (.MYMI\Myriam.) -- C:\program files (x86)\IObit\Classic Start\Start\_Active.exe []

C:\windows\System32\Tasks\Microsoft\Office\OfficeTelemetryAgentLogOn2016 - (.Microsoft Corporation.) -- C:\Program Files (x86)\Microsoft Office\root\Office16\msoia.exe [scan upload] =>.Microsoft Corporation

C:\windows\System32\Tasks\AVG-Secure-Search-Update\_0214b\_rmv - (.Copyright (C) 2011 . All rights reserved..) -- C:\Program Files (x86)\AVG SafeGuard toolbar\AVG-Secure-Search-Update\_0214b.exe [--CMPID=0214b --uninstall=1]

C:\windows\System32\Tasks\Microsoft\Windows\WindowsBackup\Windows Backup Monitor - (.Microsoft Corporation.) -- C:\windows\System32\sdclt.exe [/CHECKSKIPPED] =>.Microsoft Corporation

C:\windows\System32\Tasks\WPD\SqmUpload\_S-1-5-21-2870124582-2670056687-1688047813-1001 - (.Microsoft Corporation.) -- C:\Windows\System32\portabledeviceapi.dll [portabledeviceapi.dll] =>.Microsoft Corporation

C:\windows\System32\Tasks\EPSON XP-420 Series Update {EE36AA76-8C02-452D-AA01-97A485E70511} - (.SEIKO EPSON CORPORATION.) -- C:\windows\system32\spool\DRIVERS\x64\3\E\_YTSNAE.EXE [/EXE:'{EE36AA76-8C02-452D-AA01-97A485E70511}] =>.Seiko Epson Corporation

C:\windows\System32\Tasks\Apple\AppleSoftwareUpdate - (.Apple Inc..) -- C:\Program Files (x86)\Apple Software Update\SoftwareUpdate.exe [-task] =>.Apple Inc.

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

C:\windows\System32\Tasks\Microsoft\Windows\WindowsUpdate\Scheduled Start - (.Microsoft Corporation.) -- C:\Windows\System32\sc.exe [wuauserv] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\Plug and Play\Sysprep Generalize Drivers - (.Microsoft Corporation.) -- C:\Windows\System32\drvinst.exe [6] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\Time Synchronization\SynchronizeTime - (.Microsoft Corporation.) -- C:\Windows\System32\sc.exe [w32time task\_ed] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser - (.Microsoft Corporation.) -- C:\windows\system32\CompatTelRunner.exe [/UploadEtlFilesOnly] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\Application Experience\StartupAppTask - (.Microsoft Corporation.) -- C:\Windows\System32\Startupscan.dll [Startupscan.dll] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\Bluetooth\UninstallDeviceTask - (.Microsoft Corporation.) -- C:\Windows\System32\BthUdTask.exe [$(Arg0)] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticDataCollector - (.Microsoft Corporation.) -- C:\Windows\System32\dfdts.dll [dfdts.dll] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Windows\Customer Experience Improvement Program\Consolidator - (.Microsoft Corporation.) -- C:\windows\System32\wsqmcons.exe [] =>.Microsoft Corporation

C:\windows\System32\Tasks\Microsoft\Office\Office 15 Subscription Heartbeat - (.Microsoft Office.) -- C:\Program Files\Common Files\Microsoft Shared\Office15\OLicenseHeartbeat.exe (.not file.) [] (.Orphan.) =>.SUP.Orphan

C:\windows\System32\Tasks\AV\_PWB - (.WORKGROUP\MYMI$.) -- C:\Program Files (x86)\AVG SafeGuard toolbar\BundleInstall.exe (.not file.) [/HP='http://mysearch.avg.com/?cid={0B7C672A-AF6C-4872-AC3D-C34268D367FB}&mid=b916433b2baa47d39dc269c1a5fb8021-18bcd87b26a5ed9451abc4cb8aeb66ef9ebec201&lang=en&ds=dl011&pr=sa&d=2013-07-25 21:02:47&v=17.1.3.3&pid=safeguard&sg=78&sap=hp' /IE=1 /FF=1 /CH=1 /UPDATE=1 /INSTID=1 /FROMSCHEDULER=1] (.Orphan.)

**---\ Auto loading programs from Registry and folders (30) - 2s**

O4 - HKLM\..\Run: [HotKeysCmds] . (.Intel Corporation - hkcmd Module.) -- C:\windows\system32\hkcmd.exe =>.Intel Corporation

O4 - HKLM\..\Run: [Persistence] . (.Intel Corporation - persistence Module.) -- C:\windows\system32\igfxpers.exe =>.Intel Corporation

O4 - HKLM\..\Run: [RtHDVCpl] . (.Realtek Semiconductor - Realtek HD Audio Manager.) -- C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe =>.Realtek Semiconductor Corp®

O4 - HKLM\..\Run: [SRS Premium Sound 3D] . (.SRS Labs, Inc. - SRS Control Panel.) -- C:\Program Files\SRS Labs\SRS Control Panel\SRSPanel\_64.exe =>.SRS Labs, Inc.®

O4 - HKLM\..\Run: [TosPU] . (.Copyright (C) TOSHIBA Corp. 2012 - TOSPU Application.) -- C:\Program Files\Toshiba\PasswordUtility\TosPU.exe =>.Compal Electronics, Inc.®

O4 - HKLM\..\Run: [TCrdMain] . (. - TCrdMain Application.) -- C:\Program Files\Toshiba\Hotkey\TCrdMain\_Win8.exe =>.TOSHIBA CORPORATION®

O4 - HKLM\..\Run: [TosWaitSrv] . (.TOSHIBA Corporation - .) -- C:\Program Files\Toshiba\TPHM\TosWaitSrv.exe =>.TOSHIBA CORPORATION®

O4 - HKLM\..\Run: [TSleepSrv] . (.TOSHIBA Corporation - Sleep and Charge Service.) -- C:\Program Files (x86)\TOSHIBA\System Setting\TSleepSrv.exe =>.TOSHIBA CORPORATION®

O4 - HKLM\..\Run: [TODDMain] . (.Copyright (C) 2012 TOSHIBA Corporation. All rights re - TOSHIBA System Settings Service.) -- C:\Program Files (x86)\TOSHIBA\System Setting\TODDMain.exe =>.TOSHIBA CORPORATION®

O4 - HKLM\..\Run: [ThpSrv] . (.TOSHIBA Corporation - TOSHIBA HDD Protection Service.) -- C:\windows\system32\thpsrv.exe =>.Toshiba Corporation

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

O4 - HKLM\..\Run: [Logitech Download Assistant] . (.Logitech, Inc. - Logitech Download Assistant.) -- C:\Windows\System32\LogiLDA.dll =>.Logitech, Inc.

O4 - HKLM\..\Run: [iTunesHelper] . (.Apple Inc. - iTunesHelper.) -- C:\Program Files\iTunes\iTunesHelper.exe =>.Apple Inc.®

O4 - HKCU\..\Run: [Spotify Web Helper] . (.Spotify Ltd - SpotifyWebHelper.) -- C:\Users\Myriam\AppData\Roaming\Spotify\SpotifyWebHelper.exe =>.Spotify AB®

O4 - HKCU\..\Run: [iCloudServices] . (.Apple Inc. - iCloud Services.) -- C:\Program Files (x86)\Common Files\Apple\Internet Services\iCloudServices.exe =>.Apple Inc.®

O4 - HKCU\..\Run: [ApplePhotoStreams] . (.Apple Inc. - iCloud Photo Stream.) -- C:\Program Files (x86)\Common Files\Apple\Internet Services\ApplePhotoStreams.exe =>.Apple Inc.®

O4 - HKCU\..\Run: [EPLTarget\P0000000000000001] . (. - .) -- C:\windows\system32\spool\DRIVERS\x64\3\E\_IATIIBE.EXE (.Not File.) =>.SUP.Orphan

O4 - HKCU\..\Run: [EPLTarget\P0000000000000000] . (.SEIKO EPSON CORPORATION - EPSON Status Monitor 3.) -- C:\windows\system32\spool\DRIVERS\x64\3\E\_YATINAE.EXE =>.SEIKO EPSON CORPORATION®

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

O4 - HKLM\..\Wow6432Node\Run: [KeNotify] . (.TOSHIBA CORPORATION - KeNotify MFC Application.) -- C:\Program Files (x86)\TOSHIBA\Utilities\KeNotify.exe =>.Compal Electronics, Inc.®

O4 - HKLM\..\Wow6432Node\Run: [ToshibaAppPlace] . (.Toshiba - Toshiba App Place.) -- C:\Program Files (x86)\TOSHIBA\Toshiba App Place\ToshibaAppPlace.exe =>.Toshiba

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

O4 - HKLM\..\Wow6432Node\Run: [Acrobat Assistant 8.0] . (.Adobe Systems Inc. - AcroTray.) -- C:\Program Files (x86)\Adobe\Acrobat 11.0\Acrobat\acrotray.exe =>.Adobe Systems, Incorporated®

O4 - HKLM\..\Wow6432Node\Run: [WD Button Manager] . (. - .) -- WDBtnMgr.exe =>.SUP.Orphan

O4 - HKUS\S-1-5-21-2870124582-2670056687-1688047813-1001\..\Run: [Spotify Web Helper] . (.Spotify Ltd - SpotifyWebHelper.) -- C:\Users\Myriam\AppData\Roaming\Spotify\SpotifyWebHelper.exe =>.Spotify AB®

O4 - HKUS\S-1-5-21-2870124582-2670056687-1688047813-1001\..\Run: [iCloudServices] . (.Apple Inc. - iCloud Services.) -- C:\Program Files (x86)\Common Files\Apple\Internet Services\iCloudServices.exe =>.Apple Inc.®

O4 - HKUS\S-1-5-21-2870124582-2670056687-1688047813-1001\..\Run: [ApplePhotoStreams] . (.Apple Inc. - iCloud Photo Stream.) -- C:\Program Files (x86)\Common Files\Apple\Internet Services\ApplePhotoStreams.exe =>.Apple Inc.®

O4 - HKUS\S-1-5-21-2870124582-2670056687-1688047813-1001\..\Run: [EPLTarget\P0000000000000001] . (. - .) -- C:\windows\system32\spool\DRIVERS\x64\3\E\_IATIIBE.EXE (.Not File.) =>.SUP.Orphan

O4 - HKUS\S-1-5-21-2870124582-2670056687-1688047813-1001\..\Run: [EPLTarget\P0000000000000000] . (.SEIKO EPSON CORPORATION - EPSON Status Monitor 3.) -- C:\windows\system32\spool\DRIVERS\x64\3\E\_YATINAE.EXE =>.SEIKO EPSON CORPORATION®

O4 - HKUS\S-1-5-21-2870124582-2670056687-1688047813-1001\..\Run: [OneDrive] . (.Microsoft Corporation - Microsoft OneDrive.) -- C:\Users\Myriam\AppData\Local\Microsoft\OneDrive\OneDrive.exe =>.Microsoft Corporation®

**---\ Process running (79) - 6s**

[MD5.6831D30B0DB45E25E6C3207247C6EC36] - (.Realtek Semiconductor - Realtek Audio Service.) -- C:\Program Files\Realtek\Audio\HDA\RtkAudioService64.exe [201872] [PID.1316] =>.Realtek Semiconductor Corp®

[MD5.6436372949731033979444E0B887F14C] - (.Realtek Semiconductor - HD Audio Background Process.) -- C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe [1256080] [PID.1336] =>.Realtek Semiconductor Corp®

[MD5.459E60319770C8F01D1D75F817F57633] - (.Juniper Networks, Inc. - Juniper Access Service.) -- C:\Program Files (x86)\Common Files\Juniper Networks\JUNS\dsAccessService.exe [162136] [PID.1388] =>.Juniper Networks, Inc.®

[MD5.459E60319770C8F01D1D75F817F57633] - (.Juniper Networks, Inc. - Juniper Access Service.) -- C:\Program Files (x86)\Common Files\Juniper Networks\JUNS\dsAccessService.exe [162136] [PID.1672] =>.Juniper Networks, Inc.®

[MD5.CF3978A5F06F9090AF0B48D0240A00FE] - (.Juniper Networks - WX Connection Method Service.) -- C:\Program Files (x86)\Common Files\Juniper Networks\WX Client\WXConnectionMethod.exe [6812536] [PID.1708] =>.Juniper Networks, Inc.®

[MD5.ABDD5AD016AFFD34AD40E944CE94BF59] - (.SEIKO EPSON CORPORATION - eEBAPI Core Process module.) -- C:\Program Files (x86)\Common Files\EPSON\EBAPI\eEBSvc.exe [94208] [PID.1992] =>.Seiko Epson Corporation

[MD5.B362181ED3771DC03B4141927C80F801] - (.Adobe Systems Incorporated - Adobe Acrobat Update Service.) -- C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe [65432] [PID.1812] =>.Adobe Systems, Incorporated®

[MD5.7DEFAE8665BCEDDC2C9983138D69D7A5] - (.Apple Inc. - MobileDeviceService.) -- C:\Program Files\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe [83768] [PID.1856] =>.Apple Inc.®

[MD5.B5C2F92EE1106DFE7BB1CCE4D35B6037] - (.Apple Inc. - Bonjour Service.) -- C:\Program Files\Bonjour\mDNSResponder.exe [462096] [PID.1092] =>.Apple Inc.®

[MD5.1A866004B1E1A43A4F8DB69B62389170] - (.SEIKO EPSON CORPORATION - Epson Customer Participation.) -- C:\Program Files\EPSON\EpsonCustomerParticipation\EPCP.exe [674768] [PID.2316] {76101A6757EFD8186742057C6A6ACAA4} =>.Seiko Epson Corporation

[MD5.00000000000000000000000000000000] - (.Seiko Epson Corporation - Epson Scanner Service (64bit).) -- C:\windows\system32\EscSvc64.exe [0] [PID.2348] =>.Seiko Epson Corporation

[MD5.C99F8E90DE4B8F0C7FE15BB1CBCD29DC] - (.Intel(R) Corporation - Intel(R) Capability Licensing Service Inter.) -- C:\Program Files\Intel\iCLS Client\HeciServer.exe [635104] [PID.2384] =>.Intel® Upgrade Service®

[MD5.3C4002D339491AF73D663FFC7F6E5ECB] - (.Intel Corporation - Intel(R) Dynamic Application Loader Host In.) -- C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\DAL\jhi\_service.exe [165760] [PID.2408] =>.Intel Corporation®

[MD5.CEF9746E040CC59AEFEC0469D8BE1600] - (.Trend Micro Inc. - Trend Micro Common Client Real-time Scan Se.) -- C:\Program Files (x86)\Trend Micro\OfficeScan Client\Ntrtscan.exe [4638784] [PID.2456] =>.Trend Micro, Inc.®

[MD5.8EF3A5CD65EB67A3DC38A154FF5FBE6A] - (.IObit - StartMenu8 Services.) -- C:\program files (x86)\IObit\Classic Start\SMService.exe [1077536] [PID.2568] =>.IObit Information Technology®

[MD5.00000000000000000000000000000000] - (.TOSHIBA Corporation - TOSHIBA HDD Protection Service.) -- C:\windows\system32\ThpSrv.exe [0] [PID.2688] =>.Toshiba Corporation

[MD5.00000000000000000000000000000000] - (.TOSHIBA Corporation - TDCSrv Application.) -- C:\Windows\system32\TODDSrv.exe [0] [PID.2720] =>.Toshiba Corporation

[MD5.CE6C6ADEFD5D84AA2C920F772FD055E3] - (.Cisco Systems, Inc. - Umbrella RC Service.) -- C:\Program Files (x86)\OpenDNS\Umbrella Roaming Client\ERCService.exe [36632] [PID.2780] =>.OpenDNS®

[MD5.5E0F08C47A716FF0E3092F30809BB7C4] - (.Western Digital Technologies, Inc. - WD Drive Service.) -- C:\Program Files (x86)\Western Digital\WD Drive Manager\WDDriveService.exe [308088] [PID.2880] =>.Western Digital Technologies, Inc.®

[MD5.937FE70F6AA968E10BD757ECE2276B4F] - (.Trend Micro Inc. - Trend Micro Common Client Communication Ser.) -- C:\Program Files (x86)\Trend Micro\OfficeScan Client\TmListen.exe [4628200] [PID.3028] =>.Trend Micro, Inc.®

[MD5.4D7977197C3EC8C65F533E8A84DE229C] - (.TOSHIBA Corporation - TOSHIBA eco Utility Service.) -- C:\Program Files\Toshiba\Teco\TecoService.exe [291240] [PID.1260] =>.TOSHIBA CORPORATION®

[MD5.AF408BA0DB2701176CB550460CBCA4D2] - (.Trend Micro Inc. - Trend Micro Common Client Solution Framewor.) -- C:\Program Files (x86)\Trend Micro\OfficeScan Client\CCSF\TmCCSF.exe [701064] [PID.4088] =>.Trend Micro, Inc.®

[MD5.E3A259EECA916C161C792E2895AF3685] - (.Trend Micro Inc. - Trend Micro OfficeScan Client Plug-in Servi.) -- C:\Program Files (x86)\Trend Micro\OfficeScan Client\CNTAoSMgr.exe [472320] [PID.4312] =>.Trend Micro, Inc.®

[MD5.50D5DAF12920A7EAA6A264C87E9AF0F2] - (.Trend Micro Inc. - Manages the Trend Micro unauthorized change.) -- C:\Program Files (x86)\Trend Micro\BM\TMBMSRV.exe [575024] [PID.4504] =>.Trend Micro, Inc.®

[MD5.ABEFA4BD23329FD9BD47496BF2E58774] - (.Realsil Microelectronics Inc. - Realtek Card Reader Patch Tool..) -- C:\Program Files (x86)\Realtek\Realtek PCIE Card Reader\RIconMan.exe [2451456] [PID.3172] =>.Realsil Microelectronics Inc.

[MD5.30E9FAC23E2537D82F2836CB81AEE186] - (.Intel Corporation - Intel(R) ME Service.) -- C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\FWService\IntelMeFWService.exe [128896] [PID.3780] =>.Intel Corporation®

[MD5.4269D44BB47A6DA5D80B11F4C8536458] - (.Intel Corporation - Local Manageability Service.) -- C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe [276864] [PID.1848] =>.Intel Corporation®

[MD5.F5FD83FA082E88FE6049B1B9F78AA739] - (.TOSHIBA CORPORATION - TOSHIBA HDD Accelerator Service.) -- C:\Program Files\Toshiba\HDD Accelerator\THAccelSvc.exe [214488] [PID.1808] =>.TOSHIBA CORPORATION®

[MD5.DBE2E6388379D5CC78099650541E9566] - (.Intel Corporation - User Notification Service.) -- C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\UNS\UNS.exe [364416] [PID.4856] =>.Intel Corporation®

[MD5.00000000000000000000000000000000] - (.Dropbox, Inc. - Dropbox Service.) -- C:\windows\system32\DbxSvc.exe [0] [PID.1104] =>.Dropbox, Inc.

[MD5.4C76BE04981EB8BE76DC4AC900F16AFB] - (.Copyright (C) 2011 . All rights reserved. - .) -- C:\Program Files (x86)\AVG SafeGuard toolbar\AVG-Secure-Search-Update\_0214b.exe [2606616] [PID.6416] =>.AVG Technologies®

[MD5.880A5DF36A4DDC1D415ECC8CCABF7689] - (.IObit - .) -- C:\program files (x86)\IObit\Classic Start\ClassicStart.exe [2246432] [PID.4516] =>.IObit Information Technology®

[MD5.D82A20D1A15F2FE16A14EDAEF14F1C59] - (.IObit - .) -- C:\program files (x86)\IObit\Classic Start\StartMenu\_Hook.exe [69408] [PID.7008] =>.IObit Information Technology®

[MD5.00000000000000000000000000000000] - (.Intel Corporation - igfxTray Module.) -- C:\Windows\System32\igfxtray.exe [0] [PID.7112] =>.Intel Corporation

[MD5.00000000000000000000000000000000] - (.Intel Corporation - hkcmd Module.) -- C:\Windows\System32\hkcmd.exe [0] [PID.7116] =>.Intel Corporation

[MD5.00000000000000000000000000000000] - (.Intel Corporation - persistence Module.) -- C:\Windows\System32\igfxpers.exe [0] [PID.5344] =>.Intel Corporation

[MD5.F072EF002CE7B945DC7DBBA6F9664FCF] - (.Realtek Semiconductor - Realtek HD Audio Manager.) -- C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe [13261456] [PID.5420] =>.Realtek Semiconductor Corp®

[MD5.06726BE818CE6B4AD11B0EB54F28B941] - (.IObit - StartMenu8 InstallServices.) -- C:\program files (x86)\IObit\Classic Start\InstallServices.exe [2234656] [PID.908] =>.IObit Information Technology®

[MD5.4DF11CDE53A5AF536178AEC3D4A053B1] - (.SRS Labs, Inc. - SRS Control Panel.) -- C:\Program Files\SRS Labs\SRS Control Panel\SRSPanel\_64.exe [2170784] [PID.6516] =>.SRS Labs, Inc.®

[MD5.22C5DF38DB27F594D85163D5706EF5A1] - (. - TCrdMain Application.) -- C:\Program Files\Toshiba\Hotkey\TCrdMain\_Win8.exe [2609064] [PID.6760] =>.TOSHIBA CORPORATION®

[MD5.57C4B4289DAB34CBAEEB92865C6BC022] - (.TOSHIBA Corporation - Resident module of eco Utility.) -- C:\Program Files\Toshiba\Teco\TecoResident.exe [169896] [PID.6776] =>.TOSHIBA CORPORATION®

[MD5.CF74C5BE20CD4DE1299F6C92A738A2DF] - (.TOSHIBA Corporation - Sleep and Charge Service.) -- C:\Program Files (x86)\TOSHIBA\System Setting\TSleepSrv.exe [1548952] [PID.6936] =>.TOSHIBA CORPORATION®

[MD5.E365B567A4DC4A50B10A84B2B2D09EA7] - (.Copyright (C) 2009-2011 TOSHIBA Corporation. All righ - TCrdKBB Application.) -- C:\Program Files\Toshiba\Hotkey\Hotkey\TCrdKBB.exe [437632] [PID.4424] =>.TOSHIBA CORPORATION®

[MD5.6EF487A46FB615DF717F85D7458BD2CD] - (.Copyright (C) 2012 TOSHIBA Corporation. All rights re - TOSHIBA System Settings Service.) -- C:\Program Files (x86)\TOSHIBA\System Setting\TODDMain.exe [213136] [PID.6704] =>.TOSHIBA CORPORATION®

[MD5.00000000000000000000000000000000] - (.TOSHIBA Corporation - TOSHIBA HDD Protection Service.) -- C:\Windows\System32\ThpSrv.exe [0] [PID.1396] =>.Toshiba Corporation

[MD5.B3E7F1FBF29EF94A797238B9ACB8D993] - (.Apple Inc. - iTunesHelper.) -- C:\Program Files\iTunes\iTunesHelper.exe [303928] [PID.6148] =>.Apple Inc.®

[MD5.0C2D8CBA28E12D170FC5343F03E6D20C] - (.Spotify Ltd - SpotifyWebHelper.) -- C:\Users\Myriam\AppData\Roaming\Spotify\SpotifyWebHelper.exe [1444976] [PID.6108] =>.Spotify AB®

[MD5.D0FC75DD646C08A338A6F7D7B49BF3C3] - (.Apple Inc. - iCloud Services.) -- C:\Program Files (x86)\Common Files\Apple\Internet Services\iCloudServices.exe [67384] [PID.6268] =>.Apple Inc.®

[MD5.5451E20D9EFBDC89991C1B86A6306894] - (.SEIKO EPSON CORPORATION - EPSON Status Monitor 3.) -- C:\Windows\System32\spool\drivers\x64\3\E\_YATINAE.EXE [298560] [PID.3788] =>.SEIKO EPSON CORPORATION®

[MD5.0F62D11F94FA339B9C38EFCDE6237F7C] - (.Cisco Systems, Inc. - Umbrella RC UI.) -- C:\Program Files (x86)\OpenDNS\Umbrella Roaming Client\ERCInterface.exe [50968] [PID.3080] =>.OpenDNS®

[MD5.22819EB3C648583352AE83003E4C9A56] - (.Mozilla Corporation - Firefox.) -- C:\Program Files (x86)\Mozilla Firefox\firefox.exe [439248] [PID.6380] =>.Mozilla Corporation®

[MD5.1FAA54E9FFEA6FD3E0CEAD951CDDFEF6] - (.TOSHIBA CORPORATION - KeNotify MFC Application.) -- C:\Program Files (x86)\TOSHIBA\Utilities\KeNotify.exe [34160] [PID.6552] =>.Compal Electronics, Inc.®

[MD5.CDBE0A3516D723C9F4CC77F61C9B36E7] - (.TOSHIBA Corporation - TOSHIBA Service Station.) -- C:\Program Files\Toshiba\Toshiba Service Station\ToshibaServiceStation.exe [700040] [PID.6128] =>.TOSHIBA CORPORATION®

[MD5.048EA4B978851788E9F5E8E4F081DF7A] - (.Adobe Systems Incorporated - Adobe Reader and Acrobat Manager.) -- C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe [959904] [PID.1128] =>.Adobe Systems, Incorporated®

[MD5.54AF0144A8368F03B20A11D300795333] - (.Adobe Systems Inc. - AcroTray.) -- C:\Program Files (x86)\Adobe\Acrobat 11.0\Acrobat\acrotray.exe [3499896] [PID.7020] =>.Adobe Systems, Incorporated®

[MD5.926CF712448FEA216DEB1D30E708275C] - (.Western Digital Technologies, Inc. - WD Button Manager.) -- C:\Windows\SysWOW64\WDBtnMgr.exe [335872] [PID.1500] =>.Western Digital Technologies, Inc.

[MD5.5B6E8E09BE6401A7E022F52FDFCB2FF8] - (.Oracle Corporation - Java(TM) Update Scheduler.) -- C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe [254336] [PID.1096] =>.Oracle America, Inc.®

[MD5.3C35D4F07D5BE0E33536D505152D180E] - (.Juniper Networks, Inc. - Junos Pulse User Interface.) -- C:\Program Files (x86)\Common Files\Juniper Networks\JamUI\Pulse.exe [2104152] [PID.5284] =>.Juniper Networks, Inc.®

[MD5.BD0A0131D76DFD35B0C8A769C6AE1E74] - (.SEIKO EPSON CORPORATION - EEventManager Application.) -- C:\Program Files (x86)\Epson Software\Event Manager\EEventManager.exe [1065968] [PID.5964] =>.SEIKO EPSON CORPORATION®

[MD5.45FE3D7898C52585CB0C78AEC50740ED] - (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe [3567936] [PID.6560] =>.Dropbox, Inc®

[MD5.459E60319770C8F01D1D75F817F57633] - (.Juniper Networks, Inc. - Juniper Access Service.) -- C:\Program Files (x86)\Common Files\Juniper Networks\JUNS\dsAccessService.exe [162136] [PID.3772] =>.Juniper Networks, Inc.®

[MD5.DE9A76F5ECAA1EDC2D4D2836E8148475] - (.Western Digital Technologies, Inc. - WD Drive Auto Unlock.) -- C:\Program Files (x86)\Western Digital\WD Security\WDDriveAutoUnlock.exe [1761120] [PID.5716] =>.Western Digital Technologies, Inc.®

[MD5.8A2A79444C72D6342976724F6908495B] - (.Apple Inc. - iPodService Module (64-bit).) -- C:\Program Files\iPod\bin\iPodService.exe [689464] [PID.2536] =>.Apple Inc.®

[MD5.45FE3D7898C52585CB0C78AEC50740ED] - (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe [3567936] [PID.7152] =>.Dropbox, Inc®

[MD5.45FE3D7898C52585CB0C78AEC50740ED] - (.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe [3567936] [PID.6184] =>.Dropbox, Inc®

[MD5.E93FDA336764BBE2CB05C924AEF834B4] - (.Western Digital Technologies, Inc. - WD Drive Utilities Helper.) -- C:\Program Files (x86)\Western Digital\WD Utilities\WDDriveUtilitiesHelper.exe [1890664] [PID.7148] =>.Western Digital Technologies, Inc.®

[MD5.EFD755EF539C95995A7142753F9E171D] - (.Apple Inc. - Apple Push.) -- C:\Program Files (x86)\Common Files\Apple\Apple Application Support\APSDaemon.exe [67896] [PID.5852] =>.Apple Inc.®

[MD5.44F7F1C8873201DE4F68389DD478A425] - (.Western Digital Technologies, Inc. - WD Quick View.) -- C:\Program Files (x86)\Western Digital\WD Quick View\WDDMStatus.exe [5564784] [PID.3444] =>.Western Digital Technologies, Inc.®

[MD5.1CC5AD5FD17382905E521818876B2842] - (.Western Digital Technologies, Inc. - WD App Manager.) -- C:\Program Files (x86)\Western Digital\WD App Manager\WDAppManager.exe [1525616] [PID.6656] =>.WESTERN DIGITAL TECHNOLOGIES®

[MD5.22819EB3C648583352AE83003E4C9A56] - (.Mozilla Corporation - Firefox.) -- C:\Program Files (x86)\Mozilla Firefox\firefox.exe [439248] [PID.7280] =>.Mozilla Corporation®

[MD5.22819EB3C648583352AE83003E4C9A56] - (.Mozilla Corporation - Firefox.) -- C:\Program Files (x86)\Mozilla Firefox\firefox.exe [439248] [PID.7692] =>.Mozilla Corporation®

[MD5.22819EB3C648583352AE83003E4C9A56] - (.Mozilla Corporation - Firefox.) -- C:\Program Files (x86)\Mozilla Firefox\firefox.exe [439248] [PID.8140] =>.Mozilla Corporation®

[MD5.22819EB3C648583352AE83003E4C9A56] - (.Mozilla Corporation - Firefox.) -- C:\Program Files (x86)\Mozilla Firefox\firefox.exe [439248] [PID.6780] =>.Mozilla Corporation®

[MD5.CD015E9FF0A6A7B9DABFD9F82B4E6CDC] - (.Western Digital Technologies, Inc. - WDBackupService.) -- C:\PROGRAM FILES (X86)\WESTERN DIGITAL\WD APP MANAGER\Plugins\WD BACKUP\App\WDBackupService.exe [929152] [PID.5204] =>.WESTERN DIGITAL TECHNOLOGIES®

[MD5.22819EB3C648583352AE83003E4C9A56] - (.Mozilla Corporation - Firefox.) -- C:\Program Files (x86)\Mozilla Firefox\firefox.exe [439248] [PID.5112] =>.Mozilla Corporation®

[MD5.7421BB9A1B8C093B809FE1B0547F4A5D] - (.TOSHIBA Corporation - TSS TMachInfo Service.) -- C:\Program Files\Toshiba\TOSHIBA Service Station\TMachInfo.exe [53040] [PID.2192] =>.TOSHIBA CORPORATION®

[MD5.173B371D0069C71C379175049CE50E0C] - (.Cisco Systems, Inc. - Cisco DNS Proxy.) -- C:\Program Files (x86)\OpenDNS\Umbrella Roaming Client\dnscrypt-proxy.exe [461112] [PID.7952] =>.OpenDNS®

[MD5.22819EB3C648583352AE83003E4C9A56] - (.Mozilla Corporation - Firefox.) -- C:\Program Files (x86)\Mozilla Firefox\firefox.exe [439248] [PID.2476] =>.Mozilla Corporation®

[MD5.215DC00F6C58816AD8D3192400605D6F] - (.Nicolas Coolman - ZHPDiag.) -- C:\Users\Myriam\Downloads\ZHPDiag3.exe [3037056] [PID.8832] =>.Nicolas Coolman

**---\ Mozilla Firefox,Plugins,Start,Search,Extensions (17) - 4s**

M0 - MFSP: prefs.js [Myriam - auux7g6s.default-1378140617709] http://www.yahoo.com/ =>.Yahoo! Inc.

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

P2 - EXT FILE: (.Adobe Systems Inc. - Adobe PDF Plug-In For Firefox and Netscape.) -- C:\Program Files (x86)\Mozilla Firefox\Plugins\nppdf32.dll =>.Adobe Systems, Incorporated®

P2 - EXT FILE: (.OneTab - \_\_MSG\_manifestDescription\_\_.) -- C:\Users\Myriam\AppData\Roaming\Mozilla\Firefox\Profiles\auux7g6s.default-1378140617709\extensions\extension@one-tab.com.xpi =>.OneTab

P2 - EXT FILE: (...) -- C:\Users\Myriam\AppData\Roaming\Mozilla\Firefox\Profiles\auux7g6s.default-1378140617709\extensions\iobitapps@mybrowserbar.com =>PUP.Optional.WidgiToolbar

P2 - EXT FILE: (.AVG Secure Search - AVG Secure Search.) -- C:\Users\Myriam\AppData\Roaming\Mozilla\Firefox\Profiles\auux7g6s.default-1378140617709\searchplugins\safeguard-secure-search.xml =>.AVG Secure Search

P2 - EXT FILE: (.Mozilla Corporation.) -- C:\Program Files (x86)\Mozilla Firefox\browser\features\activity-stream@mozilla.org.xpi =>.Mozilla Corporation

P2 - EXT FILE: (.Mozilla Corporation.) -- C:\Program Files (x86)\Mozilla Firefox\browser\features\aushelper@mozilla.org.xpi =>.Mozilla Corporation

P2 - EXT FILE: (.Mozilla Corporation.) -- C:\Program Files (x86)\Mozilla Firefox\browser\features\firefox@getpocket.com.xpi =>.Mozilla Corporation

P2 - EXT FILE: (.Mozilla Corporation.) -- C:\Program Files (x86)\Mozilla Firefox\browser\features\followonsearch@mozilla.com.xpi =>.Mozilla Corporation

P2 - EXT FILE: (.Mozilla Corporation.) -- C:\Program Files (x86)\Mozilla Firefox\browser\features\formautofill@mozilla.org.xpi =>.Mozilla Corporation

P2 - EXT FILE: (.Mozilla Corporation.) -- C:\Program Files (x86)\Mozilla Firefox\browser\features\onboarding@mozilla.org.xpi =>.Mozilla Corporation

P2 - EXT FILE: (.Mozilla Corporation.) -- C:\Program Files (x86)\Mozilla Firefox\browser\features\screenshots@mozilla.org.xpi =>.Mozilla Corporation

P2 - EXT FILE: (.Mozilla Corporation.) -- C:\Program Files (x86)\Mozilla Firefox\browser\features\shield-recipe-client@mozilla.org.xpi =>.Mozilla Corporation

P2 - EXT FILE: (.Mozilla Corporation.) -- C:\Program Files (x86)\Mozilla Firefox\browser\features\webcompat@mozilla.org.xpi =>.Mozilla Corporation

P2 - FPN: [HKCU] [box.com/BoxEdit] - (...) -- C:\Users\Myriam\AppData\Local\Box\Box Edit\npBoxEdit.dll

P2 - FPN: [HKLM] [@adobe.com/FlashPlayer] - (.Adobe Systems Incorporated.) -- C:\Windows\SysWOW64\Macromed\Flash\NPSWF32\_29\_0\_0\_113.dll =>.Adobe Systems Incorporated

**---\ Internet Explorer Extensions, Start, Search (20) - 0s**

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

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

R0 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Main,Start Page = http://www.google.com =>.Google Inc.

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

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

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

R1 - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Default\_Page\_URL = http://toshiba13.msn.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\Microsoft\Internet Explorer\AboutURLs,Tabs = www.google.com =>.Google Inc.

R1 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\AboutURLs,Tabs = www.google.com =>.Google Inc.

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://toshiba13.msn.com =>.Microsoft Corporation

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

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

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

R1 - HKEY\_USERS\S-1-5-21-2870124582-2670056687-1688047813-1001\SOFTWARE\Microsoft\Internet Explorer\Main,Search Bar = preserve =>.Microsoft Corporation

R3 - URLSearchHook: (no name)[HKCU] - {CFBFAE00-17A6-11D0-99CB-00C04FD64497} . (.Microsoft Corporation - Internet Browser.) (10.00.9200.16384 (win8\_rtm.120725-1247)) -- C:\Windows\System32\ieframe.dll =>.Microsoft Corporation

R4 - HKLM\Software\WOW6432Node\Wow6432Node\Microsoft\Internet Explorer\PhishingFilter,EnabledV9 = 1 =>Default.Value

**---\ Internet Explorer, Proxy Management (7) - 0s**

R5 - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyOverride = \*.local =>.Default.Value

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 - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings,EnableHttp1\_1 = 1 =>.Default.Value

R5 - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyHttp1.1 = 1 =>.Default.Value

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

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

**---\ Line Analysis, IniFiles, Auto loading programs (3) - 0s**

F2 - REG:system.ini: UserInit=C:\windows\system32\userinit.exe (.Microsoft Corporation.) =>.Microsoft Corporation

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

F2 - REG:system.ini: VMApplet=C:\windows\SysWOW64\SystemPropertiesPerformance.exe (.Microsoft Corporation.) =>.Microsoft Corporation

**---\ Hosts file redirection (1) - 0s**

~ Le fichier hôte est sain (The hosts file is clean) (1)

**---\ Browser Helper Object (BHO) (4) - 1s**

O2 - BHO: Lync Click to Call BHO [64Bits] - {31D09BA0-12F5-4CCE-BE8A-2923E76605DA} . (.Microsoft Corporation - Skype for Business.) -- C:\Program Files (x86)\Microsoft Office\root\vfs\ProgramFilesX64\Microsoft Office\Office16\OCHelper.dll =>.Microsoft Corporation®

O2 - BHO: Adobe Acrobat Create PDF Helper [64Bits] - {AE7CD045-E861-484f-8273-0445EE161910} . (.Adobe Systems Incorporated - Adobe PDF Toolbar for Internet Explorer.) -- C:\Program Files (x86)\Common Files\Adobe\Acrobat\WCIEActiveX\x64\AcroIEFavClient.dll =>.Adobe Systems, Incorporated®

O2 - BHO: Microsoft OneDrive for Business Browser Helper [64Bits] - {D0498E0A-45B7-42AE-A9AA-ABA463DBD3BF} . (.Microsoft Corporation - Microsoft OneDrive for Business Extensions.) -- C:\Program Files (x86)\Microsoft Office\root\vfs\ProgramFilesX64\Microsoft Office\Office16\GROOVEEX.DLL =>.Microsoft Corporation®

O2 - BHO: SmartSelect [64Bits] - {F4971EE7-DAA0-4053-9964-665D8EE6A077} . (.Adobe Systems Incorporated - Adobe PDF Toolbar for Internet Explorer.) -- C:\Program Files (x86)\Common Files\Adobe\Acrobat\WCIEActiveX\x64\AcroIEFavClient.dll =>.Adobe Systems, Incorporated®

**---\ Internet Explorer Toolbars (1) - 0s**

O3 - Toolbar: IObit Apps Toolbar - [HKLM]{03EB0E9C-7A91-4381-A220-9B52B641CDB1} . (.Spigot, Inc. - Widgi Toolbar for Internet Explorer.) -- C:\Program Files (x86)\IObit Apps Toolbar\IE\7.6\iobitappsToolbarIE.dll =>PUP.Optional.Dealio

**---\ Global shortcuts Startup (115) - 24s**

O4 - GS\Desktop [Administrator]: DriveNavi\_HDGDU3\_WR\_101.lnk . (...) C:\BUFFALO\DriveNavi\_HDGDU3\_WR\_101

O4 - GS\Desktop [Administrator]: Dropbox.lnk . (.Dropbox, Inc. - Dropbox.) C:\Program Files (x86)\Dropbox\Client\Dropbox.exe /home =>.Dropbox, Inc®

O4 - GS\Desktop [Administrator]: e5 Secure Download Manager.lnk . (.Kivuto Solutions Inc. - SDM.) C:\Users\Myriam\AppData\Local\Programs\Kivuto\e5 Secure Download Manager\SecureDownloadManager.exe {51EBA420D184E64831CAFDEB4EACCCF0} =>.Kivuto Solutions Inc.

O4 - GS\Desktop [Administrator]: Shortcut to SecureDownloadManager.exe.lnk . (...) C:\Users\Myriam\AppData\Roaming\Microsoft\Installer\{E040B65B-8683-4228-8C33-D44A141E40EA}\\_80D807FC3A72E5B428F1ED.exe

O4 - GS\Desktop [Administrator]: Spotify.lnk . (.Spotify Ltd - Spotify.) C:\Users\Myriam\AppData\Roaming\Spotify\spotify.exe =>.Spotify AB®

O4 - GS\Desktop [Administrator]: WhatsApp.lnk . (...) C:\Users\Myriam\AppData\Local\WhatsApp\Update.exe --processStart WhatsApp.exe =>.WhatsApp, Inc.®

O4 - GS\Desktop [Administrator]: Windows 10 Upgrade Assistant.lnk . (.Microsoft Corporation - Windows 10 Upgrade Assistant.) C:\Windows10Upgrade\Windows10UpgraderApp.exe =>.Microsoft Corporation®

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

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

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

O4 - GS\sendTo [Administrator]: Dropbox.lnk . (...) C:\Users\Myriam\Dropbox

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

O4 - GS\sendTo [Administrator]: Skype.lnk . (.Skype Technologies S.A. - Skype.) C:\Program Files (x86)\Skype\Phone\Skype.exe /sendto: =>.Skype Software Sarl®

O4 - GS\TaskBar [Administrator]: File Explorer.lnk . (...) C:\Users\Myriam\AppData\Roaming\Microsoft\Windows\Libraries

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

O4 - GS\TaskBar [Administrator]: Mozilla Firefox.lnk . (.Mozilla Corporation - Firefox.) C:\Program Files (x86)\Mozilla Firefox\firefox.exe =>.Mozilla Corporation®

O4 - GS\TaskBar [Administrator]: Outlook 2016.lnk . (.Microsoft Corporation - Microsoft Outlook.) C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.EXE =>.Microsoft Corporation®

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

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

O4 - GS\Programs [Administrator]: Spotify.lnk . (.Spotify Ltd - Spotify.) C:\Users\Myriam\AppData\Roaming\Spotify\spotify.exe =>.Spotify AB®

O4 - GS\Desktop [Guest]: DriveNavi\_HDGDU3\_WR\_101.lnk . (...) C:\BUFFALO\DriveNavi\_HDGDU3\_WR\_101

O4 - GS\Desktop [Guest]: Dropbox.lnk . (.Dropbox, Inc. - Dropbox.) C:\Program Files (x86)\Dropbox\Client\Dropbox.exe /home =>.Dropbox, Inc®

O4 - GS\Desktop [Guest]: e5 Secure Download Manager.lnk . (.Kivuto Solutions Inc. - SDM.) C:\Users\Myriam\AppData\Local\Programs\Kivuto\e5 Secure Download Manager\SecureDownloadManager.exe {51EBA420D184E64831CAFDEB4EACCCF0} =>.Kivuto Solutions Inc.

O4 - GS\Desktop [Guest]: Shortcut to SecureDownloadManager.exe.lnk . (...) C:\Users\Myriam\AppData\Roaming\Microsoft\Installer\{E040B65B-8683-4228-8C33-D44A141E40EA}\\_80D807FC3A72E5B428F1ED.exe

O4 - GS\Desktop [Guest]: Spotify.lnk . (.Spotify Ltd - Spotify.) C:\Users\Myriam\AppData\Roaming\Spotify\spotify.exe =>.Spotify AB®

O4 - GS\Desktop [Guest]: WhatsApp.lnk . (...) C:\Users\Myriam\AppData\Local\WhatsApp\Update.exe --processStart WhatsApp.exe =>.WhatsApp, Inc.®

O4 - GS\Desktop [Guest]: Windows 10 Upgrade Assistant.lnk . (.Microsoft Corporation - Windows 10 Upgrade Assistant.) C:\Windows10Upgrade\Windows10UpgraderApp.exe =>.Microsoft Corporation®

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

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

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

O4 - GS\sendTo [Guest]: Dropbox.lnk . (...) C:\Users\Myriam\Dropbox

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

O4 - GS\sendTo [Guest]: Skype.lnk . (.Skype Technologies S.A. - Skype.) C:\Program Files (x86)\Skype\Phone\Skype.exe /sendto: =>.Skype Software Sarl®

O4 - GS\TaskBar [Guest]: File Explorer.lnk . (...) C:\Users\Myriam\AppData\Roaming\Microsoft\Windows\Libraries

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

O4 - GS\TaskBar [Guest]: Mozilla Firefox.lnk . (.Mozilla Corporation - Firefox.) C:\Program Files (x86)\Mozilla Firefox\firefox.exe =>.Mozilla Corporation®

O4 - GS\TaskBar [Guest]: Outlook 2016.lnk . (.Microsoft Corporation - Microsoft Outlook.) C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.EXE =>.Microsoft Corporation®

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

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

O4 - GS\Programs [Guest]: Spotify.lnk . (.Spotify Ltd - Spotify.) C:\Users\Myriam\AppData\Roaming\Spotify\spotify.exe =>.Spotify AB®

O4 - GS\Desktop [Myriam]: DriveNavi\_HDGDU3\_WR\_101.lnk . (...) C:\BUFFALO\DriveNavi\_HDGDU3\_WR\_101

O4 - GS\Desktop [Myriam]: Dropbox.lnk . (.Dropbox, Inc. - Dropbox.) C:\Program Files (x86)\Dropbox\Client\Dropbox.exe /home =>.Dropbox, Inc®

O4 - GS\Desktop [Myriam]: e5 Secure Download Manager.lnk . (.Kivuto Solutions Inc. - SDM.) C:\Users\Myriam\AppData\Local\Programs\Kivuto\e5 Secure Download Manager\SecureDownloadManager.exe {51EBA420D184E64831CAFDEB4EACCCF0} =>.Kivuto Solutions Inc.

O4 - GS\Desktop [Myriam]: Shortcut to SecureDownloadManager.exe.lnk . (...) C:\Users\Myriam\AppData\Roaming\Microsoft\Installer\{E040B65B-8683-4228-8C33-D44A141E40EA}\\_80D807FC3A72E5B428F1ED.exe

O4 - GS\Desktop [Myriam]: Spotify.lnk . (.Spotify Ltd - Spotify.) C:\Users\Myriam\AppData\Roaming\Spotify\spotify.exe =>.Spotify AB®

O4 - GS\Desktop [Myriam]: WhatsApp.lnk . (...) C:\Users\Myriam\AppData\Local\WhatsApp\Update.exe --processStart WhatsApp.exe =>.WhatsApp, Inc.®

O4 - GS\Desktop [Myriam]: Windows 10 Upgrade Assistant.lnk . (.Microsoft Corporation - Windows 10 Upgrade Assistant.) C:\Windows10Upgrade\Windows10UpgraderApp.exe =>.Microsoft Corporation®

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

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

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

O4 - GS\sendTo [Myriam]: Dropbox.lnk . (...) C:\Users\Myriam\Dropbox

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

O4 - GS\sendTo [Myriam]: Skype.lnk . (.Skype Technologies S.A. - Skype.) C:\Program Files (x86)\Skype\Phone\Skype.exe /sendto: =>.Skype Software Sarl®

O4 - GS\TaskBar [Myriam]: File Explorer.lnk . (...) C:\Users\Myriam\AppData\Roaming\Microsoft\Windows\Libraries

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

O4 - GS\TaskBar [Myriam]: Mozilla Firefox.lnk . (.Mozilla Corporation - Firefox.) C:\Program Files (x86)\Mozilla Firefox\firefox.exe =>.Mozilla Corporation®

O4 - GS\TaskBar [Myriam]: Outlook 2016.lnk . (.Microsoft Corporation - Microsoft Outlook.) C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.EXE =>.Microsoft Corporation®

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

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

O4 - GS\Programs [Myriam]: Spotify.lnk . (.Spotify Ltd - Spotify.) C:\Users\Myriam\AppData\Roaming\Spotify\spotify.exe =>.Spotify AB®

O4 - GS\CommonDesktop [Public]: 123 Free Solitaire.lnk . (...) C:\Program Files (x86)\123 Free Solitaire\123FreeSolitaire.exe =>.TreeCardGames®

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

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

O4 - GS\CommonDesktop [Public]: Battery Check Utility.lnk . (.TOSHIBA Corporation - TOSHIBA Battery Check Utility.) C:\Program Files\Toshiba\Battery Check Utility\TosBatCheckTool.exe =>.TOSHIBA CORPORATION®

O4 - GS\CommonDesktop [Public]: Desktop Assist.lnk . (.Microsoft - .) C:\Program Files (x86)\Toshiba\TOSHIBA Desktop Assist\TosDesktopAssist.exe =>.Microsoft

O4 - GS\CommonDesktop [Public]: EPSON Scan.lnk . (.SEIKO EPSON CORP. - EPSON Scan.) C:\Windows\twain\_32\escndv\escndv.exe =>.SEIKO EPSON CORPORATION®

O4 - GS\CommonDesktop [Public]: EPSON XP-400 User's Guide.lnk . (...) C:\Program Files (x86)\epson\guide\xp400\_el\elink.url

O4 - GS\CommonDesktop [Public]: Firefox.lnk . (.Mozilla Corporation - Firefox.) C:\Program Files (x86)\Mozilla Firefox\firefox.exe =>.Mozilla Corporation®

O4 - GS\CommonDesktop [Public]: iTunes.lnk . (.Apple Inc. - .) C:\Program Files (x86)\iTunes\iTunes.exe =>.Apple Inc.

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

O4 - GS\CommonDesktop [Public]: Skype.lnk . (...) C:\windows\Installer\{FC965A47-4839-40CA-B618-18F486F042C6}\SkypeIcon.exe =>.Skype Technologies

O4 - GS\CommonDesktop [Public]: Start Menu 8.lnk . (.IObit - .) C:\Program Files (x86)\IObit\Classic Start\ClassicStart.exe startmenu =>.IObit Information Technology®

O4 - GS\CommonDesktop [Public]: WD Backup.lnk . (.Western Digital Technologies, Inc. - WD App Manager.) C:\Program Files (x86)\Western Digital\WD App Manager\WDAppManager.exe -launchbackupdefault =>.WESTERN DIGITAL TECHNOLOGIES®

O4 - GS\CommonDesktop [Public]: WD Drive Utilities.lnk . (.Western Digital Technologies, Inc. - WD Drive Utilities.) C:\Program Files (x86)\Western Digital\WD Utilities\WDDriveUtilities.exe =>.Western Digital Technologies, Inc.®

O4 - GS\CommonDesktop [Public]: WD Security.lnk . (.Western Digital Technologies, Inc. - WD Security.) C:\Program Files (x86)\Western Digital\WD Security\WDSecurity.exe =>.Western Digital Technologies, Inc.®

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

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

O4 - GS\Programs [Public]: Spotify.lnk . (.Spotify Ltd - Spotify.) C:\Users\Myriam\AppData\Roaming\Spotify\spotify.exe =>.Spotify AB®

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

O4 - GS\Startup [Public]: Umbrella Roaming Client.lnk . (.Cisco Systems, Inc. - Umbrella RC UI.) C:\Program Files (x86)\OpenDNS\Umbrella Roaming Client\ERCInterface.exe =>.OpenDNS®

O4 - GS\Accessories [Public]: Calculator.lnk . (.Microsoft Corporation - Windows Calculator.) C:\windows\system32\calc.exe =>.Microsoft Corporation

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

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

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

O4 - GS\Accessories [Public]: Snipping Tool.lnk . (.Microsoft Corporation - Snipping Tool.) C:\windows\system32\SnippingTool.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Sound Recorder.lnk . (.Microsoft Corporation - Windows Sound Recorder.) C:\windows\system32\SoundRecorder.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Steps Recorder.lnk . (.Microsoft Corporation - Steps Recorder.) C:\windows\system32\psr.exe =>.Microsoft Corporation

O4 - GS\Accessories [Public]: Sticky Notes.lnk . (.Microsoft Corporation - Sticky Notes.) C:\windows\system32\StikyNot.exe =>.Microsoft Corporation

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

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

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

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

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

O4 - GS\ProgramsCommon [Public]: 123 Free Solitaire.lnk . (...) C:\Program Files (x86)\123 Free Solitaire\123FreeSolitaire.exe =>.TreeCardGames®

O4 - GS\ProgramsCommon [Public]: Access 2016.lnk . (.Microsoft Corporation - Microsoft Access.) C:\Program Files (x86)\Microsoft Office\root\Office16\MSACCESS.EXE =>.Microsoft Corporation®

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

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

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

O4 - GS\ProgramsCommon [Public]: Adobe Reader X.lnk . (...) C:\windows\Installer\{AC76BA86-7AD7-1033-7B44-AA1000000001}\SC\_Reader.ico =>.Adobe Inc.

O4 - GS\ProgramsCommon [Public]: Apple Software Update.lnk . (...) C:\windows\Installer\{52D87F32-70E4-4348-8148-C0B9F35B1314}\AppleSoftwareUpdateIco.exe =>.Apple Inc.

O4 - GS\ProgramsCommon [Public]: Excel 2016.lnk . (.Microsoft Corporation - Microsoft Excel.) C:\Program Files (x86)\Microsoft Office\root\Office16\EXCEL.EXE =>.Microsoft Corporation®

O4 - GS\ProgramsCommon [Public]: Firefox.lnk . (.Mozilla Corporation - Firefox.) C:\Program Files (x86)\Mozilla Firefox\firefox.exe =>.Mozilla Corporation®

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

O4 - GS\ProgramsCommon [Public]: Movie Maker.lnk . (.Microsoft Corporation - Movie Maker.) C:\Program Files (x86)\Windows Live\Photo Gallery\MovieMaker.exe =>.Microsoft Corporation®

O4 - GS\ProgramsCommon [Public]: OneDrive for Business.lnk . (.Microsoft Corporation - Microsoft OneDrive for Business.) C:\Program Files (x86)\Microsoft Office\root\Office16\GROOVE.EXE =>.Microsoft Corporation®

O4 - GS\ProgramsCommon [Public]: OneNote 2016.lnk . (.Microsoft Corporation - Microsoft OneNote.) C:\Program Files (x86)\Microsoft Office\root\Office16\ONENOTE.EXE =>.Microsoft Corporation®

O4 - GS\ProgramsCommon [Public]: Outlook 2016.lnk . (.Microsoft Corporation - Microsoft Outlook.) C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.EXE =>.Microsoft Corporation®

O4 - GS\ProgramsCommon [Public]: Photo Gallery.lnk . (.Microsoft Corporation - Photo Gallery.) C:\Program Files (x86)\Windows Live\Photo Gallery\WLXPhotoGallery.exe =>.Microsoft Corporation®

O4 - GS\ProgramsCommon [Public]: PowerPoint 2016.lnk . (.Microsoft Corporation - Microsoft PowerPoint.) C:\Program Files (x86)\Microsoft Office\root\Office16\POWERPNT.EXE =>.Microsoft Corporation®

O4 - GS\ProgramsCommon [Public]: Publisher 2016.lnk . (.Microsoft Corporation - Microsoft Publisher.) C:\Program Files (x86)\Microsoft Office\root\Office16\MSPUB.EXE =>.Microsoft Corporation®

O4 - GS\ProgramsCommon [Public]: Skype for Business 2016.lnk . (.Microsoft Corporation - Skype for Business.) C:\Program Files (x86)\Microsoft Office\root\Office16\lync.exe =>.Microsoft Corporation®

O4 - GS\ProgramsCommon [Public]: Toshiba Registration.lnk . (.TOSHIBA - TOSHIBA Registration.) C:\Program Files (x86)\Toshiba\ToshibaRegistration\TaisRegistration.exe =>.TOSHIBA CORPORATION®

O4 - GS\ProgramsCommon [Public]: Windows 10 Upgrade Assistant.lnk . (.Microsoft Corporation - Windows 10 Upgrade Assistant.) C:\Windows10Upgrade\Windows10UpgraderApp.exe =>.Microsoft Corporation®

O4 - GS\ProgramsCommon [Public]: Windows Store.lnk . (...) C:\windows\WinStore\WinStore.htm =>.Microsoft Corporation

O4 - GS\ProgramsCommon [Public]: Word 2016.lnk . (.Microsoft Corporation - Microsoft Word.) C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE =>.Microsoft Corporation®

**---\ Lop.com/Domain Hijackers (6) - 0s**

O17 - HKLM\System\CCS\Services\Tcpip\Parameters: DhcpNameServer = 68.105.28.11 68.105.29.11 68.105.28.12 =>.USA Phoenix Cox Communications

O17 - HKLM\System\CCS\Services\Tcpip\..\{AE6D12FD-6394-4DBD-A090-F815EC2C9D47}: NameServer = 172.16.129.16,172.16.32.16 =>.Hewlett-Packard

O17 - HKLM\System\CCS\Services\Tcpip\..\{D2E01A62-D838-4B7D-8991-C4D752786AF6}: NameServer = 127.0.0.1

O17 - HKLM\System\CCS\Services\Tcpip\..\{D2E01A62-D838-4B7D-8991-C4D752786AF6}: DhcpNameServer = 68.105.28.11 68.105.29.11 68.105.28.12 =>.USA Phoenix Cox Communications

O17 - HKLM\System\CCS\Services\Tcpip\..\{E9654F10-C95B-4232-A455-5B8EE9E18442}: DhcpNameServer = 172.20.10.1 =>.Private IP

O17 - HKLM\System\CCS\Services\Tcpip\..\{AE6D12FD-6394-4DBD-A090-F815EC2C9D47}: Domain = tulane.edu =>.Local Domain

**---\ Extra protocols (21) - 2s**

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

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

O18 - Handler: dvd [64Bits] - {12D51199-0DB5-46FE-A120-47A3D7D937CC} . (.Microsoft Corporation - ActiveX control for streaming video.) -- C:\Windows\System32\MSVidCtl.dll =>.Microsoft Corporation

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

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

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

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

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

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

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

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

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

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

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

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

O18 - Handler: tv [64Bits] - {CBD30858-AF45-11D2-B6D6-00C04FBBDE6E} . (.Microsoft Corporation - ActiveX control for streaming video.) -- C:\Windows\System32\MSVidCtl.dll =>.Microsoft Corporation

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

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

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

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

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

**---\ Software installed (118) - 25s**

O42 - Logiciel: 123 Free Solitaire v10.3 - (.TreeCardGames.) [HKLM][64Bits] -- 123 Free Solitaire\_is1 =>.TreeCardGames

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

O42 - Logiciel: Adobe Flash Player 29 NPAPI - (.Adobe Systems Incorporated.) [HKLM][64Bits] -- Adobe Flash Player NPAPI =>.Adobe Systems Incorporated®

O42 - Logiciel: Adobe Reader X (10.1.9) - (.Adobe Systems Incorporated.) [HKLM][64Bits] -- {AC76BA86-7AD7-1033-7B44-AA1000000001} =>.Adobe Systems Incorporated

O42 - Logiciel: Apple Application Support (32-bit) - (.Apple Inc..) [HKLM][64Bits] -- {E92BB800-BCC5-4C25-8102-AC2C3B7C7C1E} =>.Apple Inc.

O42 - Logiciel: Apple Application Support (64-bit) - (.Apple Inc..) [HKLM][64Bits] -- {9C912B1E-06DD-43EF-BB2B-45CB2C88BAAE} =>.Apple Inc.

O42 - Logiciel: Apple Mobile Device Support - (.Apple Inc..) [HKLM][64Bits] -- {0A596141-97D5-45FA-9281-98DFAF48D579} =>.Apple Inc.

O42 - Logiciel: Apple Software Update - (.Apple Inc..) [HKLM][64Bits] -- {52D87F32-70E4-4348-8148-C0B9F35B1314} =>.Apple Inc.

O42 - Logiciel: Atheros Driver Installation Program - (.Atheros.) [HKLM][64Bits] -- {C3A32068-8AB1-4327-BB16-BED9C6219DC7} =>.Atheros

O42 - Logiciel: Bonjour - (.Apple Inc..) [HKLM][64Bits] -- {56DDDFB8-7F79-4480-89D5-25E1F52AB28F} =>.Apple Inc.

O42 - Logiciel: Box Sync - (.Box Inc..) [HKLM][64Bits] -- {25e2ab6e-0bb9-479e-947c-5dd5f6a309a6} =>.Box, Inc.®

O42 - Logiciel: D3DX10 - (.Microsoft.) [HKLM][64Bits] -- {E09C4DB7-630C-4F06-A631-8EA7239923AF} =>.Microsoft

O42 - Logiciel: Driver Booster 2.1 - (.IObit.) [HKLM][64Bits] -- Driver Booster\_is1 =>.IObit Information Technology®

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

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

O42 - Logiciel: e5 Secure Download Manager - (.Kivuto Solutions Inc..) [HKLM][64Bits] -- {AA6C1199-6C2D-40BC-B7FB-530730F8BA56} =>.Kivuto Solutions Inc.

O42 - Logiciel: Easy Photo Scan - (.Seiko Epson Corporation.) [HKLM][64Bits] -- {1A6DED1E-A024-455D-AA82-203D6B3B0CBC} =>.Seiko Epson Corporation

O42 - Logiciel: Epson Connect - (.Epson/Seico.) [HKLM][64Bits] -- {64BA551C-9AF6-495C-93F3-D1270E0045FC} =>.Epson/Seico

O42 - Logiciel: Epson Connect Printer Setup - (.SEIKO EPSON CORPORATION.) [HKLM][64Bits] -- {D9B1D51B-EB56-410D-AEB5-1CCFAC4B6C8C} =>.Seiko Epson Corporation

O42 - Logiciel: Epson Customer Participation - (.SEIKO EPSON CORPORATION.) [HKLM][64Bits] -- {814FA673-A085-403C-9545-747FC1495069} =>.Seiko Epson Corporation

O42 - Logiciel: Epson Event Manager - (.Seiko Epson Corporation.) [HKLM][64Bits] -- {17FA0444-A025-43B9-862C-81AE6307C2F2} =>.Seiko Epson Corporation

O42 - Logiciel: Epson E-Web Print - (.SEIKO EPSON CORPORATION.) [HKLM][64Bits] -- {896667C8-53F8-47B8-B6B0-B113B10F05BC} =>.Seiko Epson Corporation

O42 - Logiciel: Epson Printer Connection Checker - (.Seiko Epson Corporation.) [HKLM][64Bits] -- {83475ED4-8CCD-4F42-B877-7E2CC2BBD97B} =>.Seiko Epson Corporation

O42 - Logiciel: EPSON Printer Finder - (.SEIKO EPSON CORPORATION.) [HKLM][64Bits] -- {B8ECD0D3-AE08-4891-B6C7-32F96B75EB6C} =>.Seiko Epson Corporation

O42 - Logiciel: EPSON Scan - (.Seiko Epson Corporation.) [HKLM][64Bits] -- EPSON Scanner =>.SEIKO EPSON CORPORATION®

O42 - Logiciel: EPSON XP-420 Series Printer Uninstall - (.SEIKO EPSON Corporation.) [HKLM][64Bits] -- EPSON XP-420 Series =>.SEIKO EPSON CORPORATION®

O42 - Logiciel: Epson XP-420\_424 User’s Guide version 1.0 - (.Epson/Seico.) [HKLM][64Bits] -- UsersGuideEpson XP-420\_424 User’s Guide\_is1 =>.Epson America, Inc.®

O42 - Logiciel: EpsonNet Print - (.SEIKO EPSON Corporation.) [HKLM][64Bits] -- {DF5200AB-5AE6-4598-846B-8ABC3AE121B1} =>.Seiko Epson Corporation

O42 - Logiciel: iCloud - (.Apple Inc..) [HKLM][64Bits] -- {5B1A59DA-D1EC-4C3A-A996-DF011A0A9668} =>.Apple Inc.

O42 - Logiciel: Intel(R) Management Engine Components - (.Intel Corporation.) [HKLM][64Bits] -- {65153EA5-8B6E-43B6-857B-C6E4FC25798A} =>.Intel Corporation®

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

O42 - Logiciel: Intel(R) Rapid Storage Technology - (.Intel Corporation.) [HKLM][64Bits] -- {3E29EE6C-963A-4aae-86C1-DC237C4A49FC} =>.Intel Corporation®

O42 - Logiciel: Intel(R) SDK for OpenCL - CPU Only Runtime Package - (.Intel Corporation.) [HKLM][64Bits] -- {FCB3772C-B7D0-4933-B1A9-3707EBACC573} =>.Intel Corporation

O42 - Logiciel: Intel® Trusted Connect Service Client - (.Intel Corporation.) [HKLM][64Bits] -- {F4404AFD-2EF3-40C1-8C09-29E5F3B6972B} =>.Intel Corporation

O42 - Logiciel: IObit Apps Toolbar v7.6 - (.Spigot, Inc..) [HKLM][64Bits] -- {CA980191-C880-46B2-87B8-A2C71656AD3F} =>PUP.Optional.Dealio

O42 - Logiciel: iTunes - (.Apple Inc..) [HKLM][64Bits] -- {F0C7385A-9D20-45F3-8101-05D383885180} =>.Apple Inc.

O42 - Logiciel: Java 7 Update 51 - (.Oracle.) [HKLM][64Bits] -- {26A24AE4-039D-4CA4-87B4-2F83217025FF} =>.Oracle

O42 - Logiciel: Java Auto Updater - (.Sun Microsystems, Inc..) [HKLM][64Bits] -- {4A03706F-666A-4037-7777-5F2748764D10} =>.Sun Microsystems, Inc.

O42 - Logiciel: Juniper Networks, Inc. Setup Client - (.Juniper Networks, Inc..) [HKCU][64Bits] -- Juniper\_Setup\_Client =>.Juniper Networks, Inc.®

O42 - Logiciel: Juniper Networks, Inc. Setup Client 64-bit Activex Control - (.Juniper Networks, Inc..) [HKLM][64Bits] -- Juniper\_Setup\_Client Activex Control =>.Juniper Networks, Inc.®

O42 - Logiciel: Juniper Networks, Inc. Setup Client Activex Control - (.Juniper Networks, Inc..) [HKLM][64Bits] -- Juniper\_Setup\_Client Activex Control =>.Juniper Networks, Inc.®

O42 - Logiciel: Junos Pulse - (.Juniper Networks.) [HKLM][64Bits] -- {E59CEF5A-DD72-4EE5-98D2-62FE1265941B} =>.Juniper Networks

O42 - Logiciel: Junos Pulse 3.1 - (.Juniper Networks, Inc..) [HKLM][64Bits] -- Junos Pulse 3.1 =>.Juniper Networks, Inc.®

O42 - Logiciel: Malwarebytes Anti-Malware version 2.2.1.1043 - (.Malwarebytes.) [HKLM][64Bits] -- Malwarebytes Anti-Malware\_is1 =>.Malwarebytes

O42 - Logiciel: Microsoft Access MUI (English) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-0015-0409-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft Access Setup Metadata MUI (English) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-0117-0409-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft Application Error Reporting - (.Microsoft Corporation.) [HKLM][64Bits] -- {95120000-00B9-0409-1000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft DCF MUI (English) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-0090-0409-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft Excel MUI (English) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-0016-0409-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft Groove MUI (English) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-00BA-0409-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft InfoPath MUI (English) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-0044-0409-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft Lync MUI (English) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-012B-0409-0000-0000000FF1CE} =>.Microsoft Corporation

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

O42 - Logiciel: Microsoft OneNote MUI (English) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-00A1-0409-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft Outlook MUI (English) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-001A-0409-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft PowerPoint MUI (English) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-0018-0409-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft Publisher MUI (English) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-0019-0409-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Microsoft Word MUI (English) 2013 - (.Microsoft Corporation.) [HKLM][64Bits] -- {90150000-001B-0409-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: Mozilla Firefox 58.0.2 (x64 en-US) - (.Mozilla.) [HKLM][64Bits] -- Mozilla Firefox 58.0.2 (x64 en-US) =>.Mozilla Corporation®

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

O42 - Logiciel: MSVCRT - (.Microsoft.) [HKLM][64Bits] -- {8DD46C6A-0056-4FEC-B70A-28BB16A1F11F} =>.Microsoft

O42 - Logiciel: MSVCRT110 - (.Microsoft.) [HKLM][64Bits] -- {8E14DDC8-EA60-4E18-B3E3-1937104D5BDA} =>.Microsoft

O42 - Logiciel: MSVCRT110\_amd64 - (.Microsoft.) [HKLM][64Bits] -- {F842F8B0-6942-4930-821F-543E976B2C66} =>.Microsoft

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

O42 - Logiciel: Office 16 Click-to-Run Extensibility Component 64-bit Registration - (.Microsoft Corporation.) [HKLM][64Bits] -- {90160000-00DD-0000-1000-0000000FF1CE} =>.Microsoft Corporation

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

O42 - Logiciel: Office 16 Click-to-Run Localization Component - (.Microsoft Corporation.) [HKLM][64Bits] -- {90160000-008C-0409-0000-0000000FF1CE} =>.Microsoft Corporation

O42 - Logiciel: PlayReady PC Runtime amd64 - (.Microsoft Corporation.) [HKLM][64Bits] -- {BCA9334F-B6C9-4F65-9A73-AC5A329A4D04} =>.Microsoft Corporation

O42 - Logiciel: Realtek Ethernet Controller Driver - (.Realtek.) [HKLM][64Bits] -- {8833FFB6-5B0C-4764-81AA-06DFEED9A476} =>.Realtek Semiconductor Corp®

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

O42 - Logiciel: Realtek PCIE Card Reader - (.Realtek Semiconductor Corp..) [HKLM][64Bits] -- {C1594429-8296-4652-BF54-9DBE4932A44C} =>.Realtek Semiconductor Corp®

O42 - Logiciel: Secure Download Manager - (.Kivuto Solutions Inc..) [HKLM][64Bits] -- {E040B65B-8683-4228-8C33-D44A141E40EA} =>.Kivuto Solutions Inc.

O42 - Logiciel: Security Update for Skype for Business 2015 (KB3191937) 32-Bit Edition - (.Microsoft.) [HKLM][64Bits] -- {90150000-012B-0409-0000-0000000FF1CE}\_Office15.PROPLUSR\_{D5A6637C-A144-41C6-9CE9-B98B77AABB6B} =>.Microsoft Corporation®

O42 - Logiciel: Skype Click to Call - (.Microsoft Corporation.) [HKLM][64Bits] -- {873F8E7C-10E6-449F-BD7E-5FBA7C8E1C9B} =>.Microsoft Corporation

O42 - Logiciel: Skype™ 7.32 - (.Skype Technologies S.A..) [HKLM][64Bits] -- {FC965A47-4839-40CA-B618-18F486F042C6} =>.Skype Technologies S.A.

O42 - Logiciel: Software Updater - (.SEIKO EPSON CORPORATION.) [HKLM][64Bits] -- {B307472F-7BD9-4040-9255-CE6D6A1196A3} =>.Seiko Epson Corporation

O42 - Logiciel: Spotify - (.Spotify AB.) [HKCU][64Bits] -- Spotify =>.Spotify AB®

O42 - Logiciel: SRS Premium Sound Control Panel - (.SRS Labs, Inc..) [HKLM][64Bits] -- {94F03B8E-CB73-4653-AFE9-79112C01FED2} =>.SRS Labs, Inc.

O42 - Logiciel: Start Menu 8 - (.IObit.) [HKLM][64Bits] -- IObit\_StartMenu8\_is1 =>.IObit Information Technology®

O42 - Logiciel: Toshiba App Place - (.Toshiba.) [HKLM][64Bits] -- {ED3CBA78-488F-4E8C-B33F-8E3BF4DDB4D2} =>.Toshiba

O42 - Logiciel: TOSHIBA Application Installer - (.TOSHIBA.) [HKLM][64Bits] -- {970472D0-F5F9-4158-A6E3-1AE49EFEF2D3} =>.InstallShield Software Corporation®

O42 - Logiciel: TOSHIBA Battery Check Utility - (.Toshiba Corporation.) [HKLM][64Bits] -- {5468E297-7EF8-4CB3-A091-F8714147793F} =>.Toshiba Corporation

O42 - Logiciel: Toshiba Book Place - (.K-NFB Reading Technology, Inc..) [HKLM][64Bits] -- {24B45620-22B6-4E4A-B836-FF30A0B0404E} =>.K-NFB Reading Technology, Inc.

O42 - Logiciel: TOSHIBA Desktop Assist - (.Toshiba Corporation.) [HKLM][64Bits] -- {95CCACF0-010D-45F0-82BF-858643D8BC02} =>.Toshiba Corporation

O42 - Logiciel: TOSHIBA eco Utility - (.Toshiba Corporation.) [HKLM][64Bits] -- {5944B9D4-3C2A-48DE-931E-26B31714A2F7} =>.Toshiba Corporation

O42 - Logiciel: TOSHIBA Flash Cards Support Utility - (.TOSHIBA CORPORATION.) [HKLM][64Bits] -- {620BBA5E-F848-4D56-8BDA-584E44584C5E} =>.Toshiba Corporation

O42 - Logiciel: TOSHIBA Flash Cards Support Utility - (.TOSHIBA CORPORATION.) [HKLM][64Bits] -- InstallShield\_{620BBA5E-F848-4D56-8BDA-584E44584C5E} =>.Toshiba Corporation

O42 - Logiciel: TOSHIBA Function Key - (.Toshiba Corporation.) [HKLM][64Bits] -- {16562A90-71BC-41A0-B890-D91B0C267120} =>.Toshiba Corporation

O42 - Logiciel: TOSHIBA HDD Accelerator - (.Toshiba Corporation.) [HKLM][64Bits] -- {DB4D9937-0B14-4EF1-BF9A-BB7E3B9DCB04} =>.Toshiba Corporation

O42 - Logiciel: TOSHIBA HDD Protection - (.Toshiba Corporation.) [HKLM][64Bits] -- {94A90C69-71C1-470A-88F5-AA47ECC96B40} =>.Toshiba Corporation

O42 - Logiciel: TOSHIBA Password Utility - (.Toshiba Corporation.) [HKLM][64Bits] -- {59358FD4-252B-4B38-AB81-955C491A494F} =>.Toshiba Corporation

O42 - Logiciel: TOSHIBA Password Utility - (.Toshiba Corporation.) [HKLM][64Bits] -- InstallShield\_{59358FD4-252B-4B38-AB81-955C491A494F} =>.Toshiba Corporation

O42 - Logiciel: TOSHIBA PC Health Monitor - (.Toshiba Corporation.) [HKLM][64Bits] -- {9DECD0F9-D3E8-48B0-A390-1CF09F54E3A4} =>.Toshiba Corporation

O42 - Logiciel: TOSHIBA Quality Application - (.TOSHIBA.) [HKLM][64Bits] -- {E69992ED-A7F6-406C-9280-1C156417BC49} =>.InstallShield Software Corporation®

O42 - Logiciel: TOSHIBA Recovery Media Creator - (.Toshiba Corporation.) [HKLM][64Bits] -- {B65BBB06-1F8E-48F5-8A54-B024A9E15FDF} =>.TOSHIBA CORPORATION®

O42 - Logiciel: TOSHIBA Resolution+ Plug-in for Windows Media Player - (.TOSHIBA Corporation.) [HKLM][64Bits] -- {6CB76C9D-80C2-4CB3-A4CD-D96B239E3F94} =>.Toshiba Corporation

O42 - Logiciel: TOSHIBA Service Station - (.Toshiba Corporation.) [HKLM][64Bits] -- {B1F241E1-90BF-4201-8977-A0DF85A38EBB} =>.Toshiba Corporation

O42 - Logiciel: TOSHIBA System Driver - (.Toshiba Corporation.) [HKLM][64Bits] -- {1E6A96A1-2BAB-43EF-8087-30437593C66C} =>.Toshiba Corporation

O42 - Logiciel: TOSHIBA System Settings - (.Toshiba Corporation.) [HKLM][64Bits] -- {05A55927-DB9B-4E26-BA44-828EBFF829F0} =>.Toshiba Corporation

O42 - Logiciel: TOSHIBA User's Guide - (.TOSHIBA.) [HKLM][64Bits] -- {3384E1D9-3F18-4A98-8655-180FEF0DFC02} =>.InstallShield Software Corporation®

O42 - Logiciel: TOSHIBA VIDEO PLAYER - (.Toshiba Corporation.) [HKLM][64Bits] -- {FF07604E-C860-40E9-A230-E37FA41F103A} =>.Toshiba Corporation

O42 - Logiciel: TOSHIBARegistration - (.TOSHIBA.) [HKLM][64Bits] -- {5AF550B4-BB67-4E7E-82F1-2C4300279050} =>.InstallShield Software Corporation®

O42 - Logiciel: Trend Micro OfficeScan Agent - (.Trend Micro Inc..) [HKLM][64Bits] -- OfficeScanNT =>.Trend Micro, Inc.®

O42 - Logiciel: Umbrella Roaming Client - (.OpenDNS.) [HKLM][64Bits] -- {47904E32-6950-4AF8-8F86-7DEA7F51EB56} =>.OpenDNS

O42 - Logiciel: Update for Skype for Business 2015 (KB4011046) 32-Bit Edition - (.Microsoft.) [HKLM][64Bits] -- {90150000-002A-0000-1000-0000000FF1CE}\_Office15.PROPLUSR\_{4948A05E-E21F-4A6F-BF2A-7D106E339C9B} =>.Microsoft Corporation®

O42 - Logiciel: Update for Skype for Business 2015 (KB4011046) 32-Bit Edition - (.Microsoft.) [HKLM][64Bits] -- {90150000-012B-0409-0000-0000000FF1CE}\_Office15.PROPLUSR\_{4948A05E-E21F-4A6F-BF2A-7D106E339C9B} =>.Microsoft Corporation®

O42 - Logiciel: Update for Skype for Business 2015 (KB4011046) 32-Bit Edition - (.Microsoft.) [HKLM][64Bits] -- {91150000-0011-0000-0000-0000000FF1CE}\_Office15.PROPLUSR\_{4948A05E-E21F-4A6F-BF2A-7D106E339C9B} =>.Microsoft Corporation®

O42 - Logiciel: Utility Common Driver - (.Compal.) [HKLM][64Bits] -- {12688FD7-CB92-4A5B-BEE4-5C8E0574434F} =>.Compal

O42 - Logiciel: Utility Common Driver - (.Compal.) [HKLM][64Bits] -- InstallShield\_{12688FD7-CB92-4A5B-BEE4-5C8E0574434F} =>.Compal

O42 - Logiciel: WD Backup - (.Western Digital Technologies, Inc.) [HKLM][64Bits] -- {4AACAFC7-951A-4215-B430-3DFCFF2E6CED} =>.Western Digital Technologies, Inc

O42 - Logiciel: WD Backup - (.Western Digital Technologies, Inc..) [HKLM][64Bits] -- {a8c9535a-ecd9-4172-a330-0cb5ff9dbed9} =>.WESTERN DIGITAL TECHNOLOGIES®

O42 - Logiciel: WD Drive Utilities - (.Western Digital Technologies, Inc..) [HKLM][64Bits] -- {48996CDD-DD81-4197-93FE-0971E73C5CA7} =>.Western Digital Technologies, Inc.

O42 - Logiciel: WD Drive Utilities - (.Western Digital Technologies, Inc..) [HKLM][64Bits] -- {eab1fb93-61fb-48de-b815-b4e9b68d2ef1} =>.Western Digital Technologies, Inc.®

O42 - Logiciel: WD Quick View - (.Western Digital Technologies, Inc..) [HKLM][64Bits] -- {965D28B5-3C86-41FD-994E-D6376815C9B3} =>.Western Digital Technologies, Inc.

O42 - Logiciel: WD Security - (.Western Digital Technologies, Inc..) [HKLM][64Bits] -- {249644e6-451a-4a5c-bd5c-21eeb9eec79d} =>.Western Digital Technologies, Inc.®

O42 - Logiciel: WD Security - (.Western Digital Technologies, Inc..) [HKLM][64Bits] -- {7CC2EDF2-83EC-4707-BDD3-72469236A6CC} =>.Western Digital Technologies, Inc.

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

O42 - Logiciel: Windows 10 Upgrade Assistant - (.Microsoft Corporation.) [HKLM][64Bits] -- {D5C69738-B486-402E-85AC-2456D98A64E4} =>.Microsoft Corporation®

**---\ HKCU & HKLM Software Keys (158) - 25s**

HKLM\SOFTWARE\Adobe =>.Adobe

HKLM\SOFTWARE\Apple Computer, Inc. =>.Apple Computer, Inc.

HKLM\SOFTWARE\Apple Inc. =>.Apple Inc.

HKLM\SOFTWARE\Atheros =>.Qualcomm Atheros

HKLM\SOFTWARE\Avg Secure Update =>.AVG Software

HKLM\SOFTWARE\COMPAL =>.Compal

HKLM\SOFTWARE\Dropbox =>.Dropbox

HKLM\SOFTWARE\DropboxUpdate =>.Dropbox Inc.

HKLM\SOFTWARE\Electronic Arts =>.Electronic Arts

HKLM\SOFTWARE\EPSON =>.EPSON

HKLM\SOFTWARE\Epson America Inc.

HKLM\SOFTWARE\EpsonNet =>.Epson/Seico

HKLM\SOFTWARE\Funk Software, Inc. =>.Funk Software, Inc.

HKLM\SOFTWARE\Google =>.Google

HKLM\SOFTWARE\IM Providers =>.IM Providers

HKLM\SOFTWARE\InstallShield =>.InstallShield

HKLM\SOFTWARE\Intel =>.Intel

HKLM\SOFTWARE\IObit =>.IObit

HKLM\SOFTWARE\IObit Apps =>PUP.Optional.Dealio

HKLM\SOFTWARE\JavaSoft =>.JavaSoft

HKLM\SOFTWARE\JreMetrics =>.JreMetrics

HKLM\SOFTWARE\Juniper Networks =>.Juniper Networks

HKLM\SOFTWARE\Khronos =>.Khronos

HKLM\SOFTWARE\LogMeIn Rescue =>.LogMeIn Entreprise

HKLM\SOFTWARE\Macromedia =>.Macromedia

HKLM\SOFTWARE\Malwarebytes' Anti-Malware =>.Malwarebytes' Anti-Malware

HKLM\SOFTWARE\Malwarebytes' Anti-Malware (Trial) =>.Malwarebytes

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

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

HKLM\SOFTWARE\Mozilla =>.Mozilla

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

HKLM\SOFTWARE\MozillaPlugins =>.MozillaPlugins

HKLM\SOFTWARE\Network Associates =>.Network Associates

HKLM\SOFTWARE\Norton =>.Symantec Corporation

HKLM\SOFTWARE\Norton PC Checkup =>.Symantec Corporation

HKLM\SOFTWARE\NPCCU

HKLM\SOFTWARE\ODBC =>.DB Connectivity Solutions

HKLM\SOFTWARE\PasswordBox =>.PasswordBox Inc

HKLM\SOFTWARE\PCCU\_Patch

HKLM\SOFTWARE\Qualcomm Atheros =>.Qualcomm Atheros

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

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

HKLM\SOFTWARE\Skype =>.Skype

HKLM\SOFTWARE\sMedio =>.sMedio

HKLM\SOFTWARE\Swearware =>.Swearware

HKLM\SOFTWARE\Symantec =>.Symantec

HKLM\SOFTWARE\TOSHIBA =>.Toshiba Corporation

HKLM\SOFTWARE\Toshiba Corporation =>.Toshiba Corporation

HKLM\SOFTWARE\TrendMicro =>.TrendMicro

HKLM\SOFTWARE\Volatile =>.Microsoft Corporation

HKLM\SOFTWARE\Western Digital =>.Western Digital

HKLM\SOFTWARE\WildTangent =>.WildTangent

HKLM\SOFTWARE\Wow6432Node =>.Microsoft Corporation

HKLM\SOFTWARE\RegisteredApplications =>.Microsoft Corporation

HKLM\SOFTWARE\WOW6432Node\Adobe =>.Adobe

HKLM\SOFTWARE\WOW6432Node\Apple Computer, Inc. =>.Apple Computer, Inc.

HKLM\SOFTWARE\WOW6432Node\Apple Inc. =>.Apple Inc.

HKLM\SOFTWARE\WOW6432Node\Atheros =>.Qualcomm Atheros

HKLM\SOFTWARE\WOW6432Node\Avg Secure Update =>.AVG Software

HKLM\SOFTWARE\WOW6432Node\COMPAL =>.Compal

HKLM\SOFTWARE\WOW6432Node\Dropbox =>.Dropbox

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

HKLM\SOFTWARE\WOW6432Node\Electronic Arts =>.Electronic Arts

HKLM\SOFTWARE\WOW6432Node\EPSON =>.EPSON

HKLM\SOFTWARE\WOW6432Node\Epson America Inc.

HKLM\SOFTWARE\WOW6432Node\EpsonNet =>.Epson/Seico

HKLM\SOFTWARE\WOW6432Node\Funk Software, Inc. =>.Funk Software, Inc.

HKLM\SOFTWARE\WOW6432Node\Google =>.Google

HKLM\SOFTWARE\WOW6432Node\IM Providers =>.IM Providers

HKLM\SOFTWARE\WOW6432Node\InstallShield =>.InstallShield

HKLM\SOFTWARE\WOW6432Node\Intel =>.Intel

HKLM\SOFTWARE\WOW6432Node\IObit =>.IObit

HKLM\SOFTWARE\WOW6432Node\IObit Apps =>PUP.Optional.Dealio

HKLM\SOFTWARE\WOW6432Node\JavaSoft =>.JavaSoft

HKLM\SOFTWARE\WOW6432Node\JreMetrics =>.JreMetrics

HKLM\SOFTWARE\WOW6432Node\Juniper Networks =>.Juniper Networks

HKLM\SOFTWARE\WOW6432Node\Khronos =>.Khronos

HKLM\SOFTWARE\WOW6432Node\LogMeIn Rescue =>.LogMeIn Entreprise

HKLM\SOFTWARE\WOW6432Node\Macromedia =>.Macromedia

HKLM\SOFTWARE\WOW6432Node\Malwarebytes' Anti-Malware =>.Malwarebytes' Anti-Malware

HKLM\SOFTWARE\WOW6432Node\Malwarebytes' Anti-Malware (Trial) =>.Malwarebytes

HKLM\SOFTWARE\WOW6432Node\MAXSOFT-OCRON =>.Maxsoft-Ocron, Inc

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

HKLM\SOFTWARE\WOW6432Node\Mozilla =>.Mozilla

HKLM\SOFTWARE\WOW6432Node\mozilla.org =>.mozilla.org

HKLM\SOFTWARE\WOW6432Node\MozillaPlugins =>.MozillaPlugins

HKLM\SOFTWARE\WOW6432Node\Network Associates =>.Network Associates

HKLM\SOFTWARE\WOW6432Node\Norton =>.Symantec Corporation

HKLM\SOFTWARE\WOW6432Node\Norton PC Checkup =>.Symantec Corporation

HKLM\SOFTWARE\WOW6432Node\NPCCU

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

HKLM\SOFTWARE\WOW6432Node\PasswordBox =>.PasswordBox Inc

HKLM\SOFTWARE\WOW6432Node\PCCU\_Patch

HKLM\SOFTWARE\WOW6432Node\Qualcomm Atheros =>.Qualcomm Atheros

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

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

HKLM\SOFTWARE\WOW6432Node\Skype =>.Skype

HKLM\SOFTWARE\WOW6432Node\sMedio =>.sMedio

HKLM\SOFTWARE\WOW6432Node\Swearware =>.Swearware

HKLM\SOFTWARE\WOW6432Node\Symantec =>.Symantec

HKLM\SOFTWARE\WOW6432Node\TOSHIBA =>.Toshiba Corporation

HKLM\SOFTWARE\WOW6432Node\Toshiba Corporation =>.Toshiba Corporation

HKLM\SOFTWARE\WOW6432Node\TrendMicro =>.TrendMicro

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

HKLM\SOFTWARE\WOW6432Node\Western Digital =>.Western Digital

HKLM\SOFTWARE\WOW6432Node\WildTangent =>.WildTangent

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

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

HKCU\SOFTWARE\Adobe =>.Adobe

HKCU\SOFTWARE\AppDataLow =>.Microsoft Corporation

HKCU\SOFTWARE\Apple Computer, Inc. =>.Apple Computer, Inc.

HKCU\SOFTWARE\Apple Inc. =>.Apple Inc.

HKCU\SOFTWARE\BestSoft

HKCU\SOFTWARE\BUFFALO

HKCU\SOFTWARE\Dropbox =>.Dropbox

HKCU\SOFTWARE\DropboxUpdate =>.Dropbox Inc.

HKCU\SOFTWARE\e-academy Inc. =>.e-academy Inc.

HKCU\SOFTWARE\EPSON =>.EPSON

HKCU\SOFTWARE\EPSON Software Updater =>.Epson/Seico

HKCU\SOFTWARE\IM Providers =>.IM Providers

HKCU\SOFTWARE\Intel =>.Intel

HKCU\SOFTWARE\IObit Apps =>PUP.Optional.Dealio

HKCU\SOFTWARE\JavaSoft =>.JavaSoft

HKCU\SOFTWARE\join.me =>.LogMeIn Entreprise

HKCU\SOFTWARE\Juniper Networks =>.Juniper Networks

HKCU\SOFTWARE\Kivuto

HKCU\SOFTWARE\Kivuto Solutions Inc. =>.Kivuto Solutions Inc.

HKCU\SOFTWARE\Leadertech =>.Leadertech Systems

HKCU\SOFTWARE\LogiShrd =>.LogiShrd

HKCU\SOFTWARE\Macromedia =>.Macromedia

HKCU\SOFTWARE\Malwarebytes' Anti-Malware =>.Malwarebytes' Anti-Malware

HKCU\SOFTWARE\McAfee =>.McAfee Inc.

HKCU\SOFTWARE\Mine =>.Microsoft Corporation

HKCU\SOFTWARE\Mozilla =>.Mozilla

HKCU\SOFTWARE\MozillaPlugins =>.MozillaPlugins

HKCU\SOFTWARE\Netscape =>.Netscape

HKCU\SOFTWARE\ODBC =>.DB Connectivity Solutions

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

HKCU\SOFTWARE\RegisteredApplications =>.Microsoft Corporation

HKCU\SOFTWARE\SEIKO EPSON CORPORATION =>.Seiko Epson Corporation

HKCU\SOFTWARE\Skype =>.Skype

HKCU\SOFTWARE\Spotify =>.Spotify

HKCU\SOFTWARE\Symantec =>.Symantec

HKCU\SOFTWARE\Synaptics =>.Synaptics

HKCU\SOFTWARE\SyncEngines =>.Microsoft Corporation

HKCU\SOFTWARE\Sysinternals =>.Sysinternals

HKCU\SOFTWARE\TOSHIBA =>.Toshiba Corporation

HKCU\SOFTWARE\Trolltech =>.Trolltech

HKCU\SOFTWARE\WDC =>.WDC

HKCU\SOFTWARE\Western Digital =>.Western Digital

HKCU\SOFTWARE\Wget =>.Wget

HKCU\SOFTWARE\WinRAR SFX =>.RarLab

HKCU\SOFTWARE\Wow6432Node =>.Microsoft Corporation

HKCU\SOFTWARE\ZHP =>.Nicolas Coolman

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

HKCU\SOFTWARE\AppDataLow\Software\IObit Apps =>PUP.Optional.Dealio

HKCU\SOFTWARE\AppDataLow\Software\JavaSoft =>.JavaSoft

HKCU\SOFTWARE\AppDataLow\Software\PasswordBox =>.PasswordBox Inc

**---\ Contents of the Common Files folders (285) - 16s**

O43 - CFD: 27/12/2015 - [] D -- C:\Program Files\Bonjour =>.Apple Inc.

O43 - CFD: 11/01/2017 - [] D -- C:\Program Files\Box =>.Box

O43 - CFD: 20/04/2014 - [] D -- C:\Program Files\Common Files =>.Microsoft Corporation

O43 - CFD: 27/07/2013 - [] D -- C:\Program Files\EPSON {76101A6757EFD8186742057C6A6ACAA4} =>.EPSON

O43 - CFD: 16/06/2015 - [] D -- C:\Program Files\EpsonNet =>.Epson/Seico

O43 - CFD: 02/06/2013 - [] D -- C:\Program Files\Intel =>.Intel Corporation

O43 - CFD: 13/01/2016 - [] D -- C:\Program Files\Internet Explorer =>.Microsoft Corporation

O43 - CFD: 17/07/2017 - [] D -- C:\Program Files\iPod =>.Apple Inc.®

O43 - CFD: 17/07/2017 - [] D -- C:\Program Files\iTunes =>.Apple Inc.

O43 - CFD: 27/07/2013 - [] D -- C:\Program Files\Microsoft Office =>.Microsoft Corporation

O43 - CFD: 28/04/2017 - [] D -- C:\Program Files\Microsoft Office 15 =>.Microsoft Corporation

O43 - CFD: 01/08/2012 - [] D -- C:\Program Files\MSBuild =>.Microsoft Corporation

O43 - CFD: 03/12/2012 - [] D -- C:\Program Files\PlayReady =>.Microsoft Corporation

O43 - CFD: 02/06/2013 - [] D -- C:\Program Files\Realtek =>.Realtek

O43 - CFD: 01/08/2012 - [] D -- C:\Program Files\Reference Assemblies =>.Microsoft Corporation

O43 - CFD: 02/06/2013 - [] D -- C:\Program Files\SRS Labs =>.SRS Labs, Inc.®

O43 - CFD: 10/05/2016 - [] D -- C:\Program Files\Toshiba =>.Toshiba Corporation

O43 - CFD: 26/07/2012 - [0] HD -- C:\Program Files\Uninstall Information =>.Microsoft Corporation

O43 - CFD: 19/09/2015 - [] D -- C:\Program Files\Windows Defender =>.Microsoft Corporation

O43 - CFD: 19/09/2015 - [] D -- C:\Program Files\Windows Journal =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [] D -- C:\Program Files\Windows Mail =>.Microsoft Corporation

O43 - CFD: 03/12/2012 - [] D -- C:\Program Files\Windows Media Player =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [] D -- C:\Program Files\Windows Multimedia Platform =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [] D -- C:\Program Files\Windows NT =>.Microsoft Corporation

O43 - CFD: 23/07/2013 - [] D -- C:\Program Files\Windows Photo Viewer =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [] D -- C:\Program Files\Windows Portable Devices =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [] SHD -- C:\Program Files\Windows Sidebar =>.Microsoft Corporation

O43 - CFD: 02/12/2017 - [] HD -- C:\Program Files\WindowsApps =>.Microsoft Corporation

O43 - CFD: 18/06/2016 - [] D -- C:\Program Files (x86)\123 Free Solitaire =>.TreeCardGames.com

O43 - CFD: 16/06/2013 - [] D -- C:\Program Files (x86)\Adobe =>.Adobe Systems, Incorporated®

O43 - CFD: 17/07/2017 - [] D -- C:\Program Files (x86)\Apple Software Update =>.Apple Inc.

O43 - CFD: 28/06/2014 - [] D -- C:\Program Files (x86)\Application Updater =>PUP.Optional.Dealio

O43 - CFD: 02/06/2013 - [] D -- C:\Program Files (x86)\Atheros =>.Qualcomm Atheros

O43 - CFD: 09/07/2014 - [] D -- C:\Program Files (x86)\AVG SafeGuard toolbar =>.AVG Technologies®

O43 - CFD: 27/12/2015 - [] D -- C:\Program Files (x86)\Bonjour =>.Apple Inc.

O43 - CFD: 01/09/2013 - [] D -- C:\Program Files (x86)\BUFFALO =>.Buffalo Technology

O43 - CFD: 18/03/2018 - [] D -- C:\Program Files (x86)\Common Files =>.Microsoft Corporation

O43 - CFD: 23/07/2013 - [] D -- C:\Program Files (x86)\Dantz

O43 - CFD: 18/03/2018 - [] D -- C:\Program Files (x86)\Dropbox =>.Dropbox, Inc®

O43 - CFD: 31/03/2016 - [] D -- C:\Program Files (x86)\epson =>.EPSON

O43 - CFD: 27/07/2013 - [] D -- C:\Program Files (x86)\Epson America Inc

O43 - CFD: 11/06/2017 - [] D -- C:\Program Files (x86)\Epson Software =>.Epson/Seico

O43 - CFD: 31/03/2016 - [] HD -- C:\Program Files (x86)\InstallShield Installation Information =>.InstallShield

O43 - CFD: 02/06/2013 - [] D -- C:\Program Files (x86)\Intel =>.Intel Corporation

O43 - CFD: 13/01/2016 - [] D -- C:\Program Files (x86)\Internet Explorer =>.Microsoft Corporation

O43 - CFD: 19/07/2017 - [] D -- C:\Program Files (x86)\IObit =>.IObit

O43 - CFD: 06/09/2014 - [] D -- C:\Program Files (x86)\IObit Apps Toolbar =>PUP.Optional.Dealio

O43 - CFD: 18/01/2015 - [] D -- C:\Program Files (x86)\Java =>.Oracle

O43 - CFD: 16/07/2015 - [] D -- C:\Program Files (x86)\Juniper Networks =>.Juniper Networks, Inc.®

O43 - CFD: 09/05/2016 - [] D -- C:\Program Files (x86)\Malwarebytes Anti-Malware =>.Malwarebytes

O43 - CFD: 15/08/2013 - [] D -- C:\Program Files (x86)\McAfee =>.McAfee

O43 - CFD: 27/07/2013 - [] D -- C:\Program Files (x86)\Microsoft Analysis Services =>.Microsoft Corporation

O43 - CFD: 18/03/2018 - [] D -- C:\Program Files (x86)\Microsoft Office =>.Microsoft Corporation

O43 - CFD: 29/04/2017 - [] D -- C:\Program Files (x86)\Microsoft OneDrive =>.Microsoft Corporation

O43 - CFD: 03/12/2012 - [] D -- C:\Program Files (x86)\Microsoft SkyDrive =>.Microsoft Corporation

O43 - CFD: 27/07/2013 - [] D -- C:\Program Files (x86)\Microsoft SQL Server =>.Microsoft Corporation

O43 - CFD: 03/12/2012 - [] D -- C:\Program Files (x86)\Microsoft SQL Server Compact Edition =>.Microsoft Corporation

O43 - CFD: 19/09/2015 - [] D -- C:\Program Files (x86)\Microsoft.NET =>.Microsoft Corporation

O43 - CFD: 25/02/2018 - [] D -- C:\Program Files (x86)\Mozilla Firefox =>.Mozilla

O43 - CFD: 25/02/2018 - [] D -- C:\Program Files (x86)\Mozilla Maintenance Service =>.Mozilla

O43 - CFD: 01/08/2012 - [] D -- C:\Program Files (x86)\MSBuild =>.Microsoft Corporation

O43 - CFD: 01/09/2016 - [] D -- C:\Program Files (x86)\OpenDNS =>.OpenDNS®

O43 - CFD: 21/11/2013 - [] D -- C:\Program Files (x86)\PasswordBox

O43 - CFD: 02/06/2013 - [] D -- C:\Program Files (x86)\Realtek =>.Realtek

O43 - CFD: 01/08/2012 - [] D -- C:\Program Files (x86)\Reference Assemblies =>.Microsoft Corporation

O43 - CFD: 03/02/2017 - [] RD -- C:\Program Files (x86)\Skype =>.Skype

O43 - CFD: 02/06/2013 - [] D -- C:\Program Files (x86)\Symantec =>.Symantec

O43 - CFD: 02/06/2013 - [] D -- C:\Program Files (x86)\SymSilent =>.Symantec Corporation®

O43 - CFD: 02/06/2013 - [0] HD -- C:\Program Files (x86)\Temp =>.Microsoft Corporation

O43 - CFD: 10/05/2016 - [] D -- C:\Program Files (x86)\TOSHIBA =>.Toshiba Corporation

O43 - CFD: 02/06/2013 - [] D -- C:\Program Files (x86)\TOSHIBA Corporation =>.Toshiba Corporation

O43 - CFD: 28/08/2015 - [] D -- C:\Program Files (x86)\Trend Micro =>.Trend Micro

O43 - CFD: 16/06/2013 - [0] HD -- C:\Program Files (x86)\Uninstall Information =>.Microsoft Corporation

O43 - CFD: 16/08/2013 - [] D -- C:\Program Files (x86)\Vtools {1B5D68E0AFA12E8F1159C668DD228431} =>.VTools

O43 - CFD: 13/05/2017 - [] D -- C:\Program Files (x86)\Western Digital =>.Western Digital Technologies, Inc.®

O43 - CFD: 21/04/2017 - [] D -- C:\Program Files (x86)\WildTangent Games =>.WildTangent Games

O43 - CFD: 19/09/2015 - [] D -- C:\Program Files (x86)\Windows Defender =>.Microsoft Corporation

O43 - CFD: 03/12/2012 - [] D -- C:\Program Files (x86)\Windows Live =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [] D -- C:\Program Files (x86)\Windows Mail =>.Microsoft Corporation

O43 - CFD: 03/12/2012 - [] D -- C:\Program Files (x86)\Windows Media Player =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [] D -- C:\Program Files (x86)\Windows Multimedia Platform =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [] D -- C:\Program Files (x86)\Windows NT =>.Microsoft Corporation

O43 - CFD: 23/07/2013 - [] D -- C:\Program Files (x86)\Windows Photo Viewer =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [] D -- C:\Program Files (x86)\Windows Portable Devices =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [] SHD -- C:\Program Files (x86)\Windows Sidebar =>.Microsoft Corporation

O43 - CFD: 18/06/2016 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\123 Free Solitaire =>.TreeCardGames.com

O43 - CFD: 26/07/2012 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessibility =>.Microsoft Corporation

O43 - CFD: 19/09/2015 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories =>.Microsoft Corporation

O43 - CFD: 01/01/2014 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools =>.Administrative Tools

O43 - CFD: 18/01/2015 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Driver Booster 2 =>.IObit

O43 - CFD: 18/03/2018 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Dropbox =>.Dropbox

O43 - CFD: 16/06/2015 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\EPSON =>.EPSON

O43 - CFD: 11/06/2017 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Epson Software =>.Epson/Seico

O43 - CFD: 21/04/2017 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Games =>.Microsoft Corporation

O43 - CFD: 17/07/2017 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\iCloud =>.Apple Inc.

O43 - CFD: 02/06/2013 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Intel =>.Intel Corporation

O43 - CFD: 17/07/2017 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\iTunes =>.Apple Inc.

O43 - CFD: 18/01/2015 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Java =>.Oracle

O43 - CFD: 16/07/2015 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Juniper Networks =>.Juniper Networks

O43 - CFD: 26/07/2012 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Maintenance =>.Microsoft Corporation

O43 - CFD: 09/05/2016 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Malwarebytes Anti-Malware =>.Malwarebytes

O43 - CFD: 13/09/2017 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Office 2013 =>.Microsoft Corporation

O43 - CFD: 29/04/2017 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Office 2016 Tools =>.Microsoft Corporation

O43 - CFD: 03/02/2017 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Skype =>.Skype

O43 - CFD: 02/06/2013 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\SRS Labs =>.SRS Labs

O43 - CFD: 19/07/2017 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Start Menu 8 =>.IObit

O43 - CFD: 23/09/2017 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp =>.Microsoft Corporation

O43 - CFD: 24/07/2013 - [] RD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\System Tools =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [0] RHD -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Tablet PC =>.Wacom Technology

O43 - CFD: 02/06/2013 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Toshiba =>.Toshiba Corporation

O43 - CFD: 28/08/2015 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Trend Micro OfficeScan Agent =>.Trend Micro

O43 - CFD: 13/05/2017 - [] D -- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Western Digital =>.Western Digital

O43 - CFD: 30/05/2015 - [] D -- C:\ProgramData\34BE82C4-E596-4e99-A191-52C6199EBF69 =>.GEAR Software, Inc.

O43 - CFD: 22/07/2013 - [] D -- C:\ProgramData\Adobe =>.Adobe

O43 - CFD: 20/04/2014 - [] D -- C:\ProgramData\Apple =>.Apple Inc.

O43 - CFD: 20/04/2014 - [] D -- C:\ProgramData\Apple Computer =>.Apple Inc.

O43 - CFD: 26/07/2012 - [0] SHD -- C:\ProgramData\Application Data =>.Microsoft Corporation

O43 - CFD: 22/07/2013 - [] D -- C:\ProgramData\Book Place

O43 - CFD: 02/06/2013 - [] D -- C:\ProgramData\boost\_interprocess =>.boost.org

O43 - CFD: 25/07/2013 - [] HD -- C:\ProgramData\Common Files =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [0] SD -- C:\ProgramData\Desktop =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [0] SHD -- C:\ProgramData\Documents =>.Microsoft Corporation

O43 - CFD: 19/06/2016 - [] D -- C:\ProgramData\Dropbox =>.Dropbox

O43 - CFD: 04/07/2015 - [] D -- C:\ProgramData\E1864A66-75E3-486a-BD95-D1B7D99A84A7 =>.Gearbox Software

O43 - CFD: 31/03/2016 - [] D -- C:\ProgramData\EPSON =>.EPSON

O43 - CFD: 03/12/2012 - [] D -- C:\ProgramData\Google =>.Google

O43 - CFD: 02/06/2013 - [] D -- C:\ProgramData\Intel =>.Intel Corporation

O43 - CFD: 10/12/2016 - [] D -- C:\ProgramData\IObit =>.IObit

O43 - CFD: 16/07/2015 - [] D -- C:\ProgramData\Juniper Networks =>.Juniper Networks

O43 - CFD: 26/06/2014 - [] D -- C:\ProgramData\Malwarebytes =>.Malwarebytes

O43 - CFD: 20/04/2014 - [] D -- C:\ProgramData\McAfee =>.McAfee

O43 - CFD: 28/04/2017 - [] SD -- C:\ProgramData\Microsoft =>.Microsoft Corporation

O43 - CFD: 11/03/2018 - [] D -- C:\ProgramData\Microsoft Help =>.Microsoft Corporation

O43 - CFD: 03/12/2012 - [] D -- C:\ProgramData\Microsoft OneDrive =>.Microsoft Corporation

O43 - CFD: 16/06/2013 - [] D -- C:\ProgramData\Mozilla =>.Mozilla Corporation

O43 - CFD: 24/07/2013 - [] D -- C:\ProgramData\Norton =>.Symantec Corporation

O43 - CFD: 23/07/2013 - [] D -- C:\ProgramData\NortonInstaller =>.Symantec

O43 - CFD: 01/09/2016 - [] D -- C:\ProgramData\OpenDNS =>.OpenDNS

O43 - CFD: 05/02/2014 - [0] D -- C:\ProgramData\Oracle =>.Oracle

O43 - CFD: 21/04/2017 - [] D -- C:\ProgramData\Origin =>.Electronic Arts, Inc.

O43 - CFD: 15/06/2017 - [] D -- C:\ProgramData\Package Cache =>.Microsoft Corporation

O43 - CFD: 03/12/2012 - [] D -- C:\ProgramData\PRICache =>.Microsoft Corporation

O43 - CFD: 18/03/2018 - [] D -- C:\ProgramData\ProductData =>.Microsoft Corporation

O43 - CFD: 02/06/2013 - [] D -- C:\ProgramData\Qualcomm Atheros =>.Qualcomm Atheros

O43 - CFD: 21/08/2013 - [] D -- C:\ProgramData\regid.1986-12.com.adobe =>.Adobe Inc.

O43 - CFD: 18/03/2018 - [] D -- C:\ProgramData\regid.1991-06.com.microsoft =>.Microsoft Corporation

O43 - CFD: 23/07/2013 - [] D -- C:\ProgramData\Retrospect

O43 - CFD: 03/02/2017 - [] D -- C:\ProgramData\Skype =>.Skype

O43 - CFD: 26/07/2012 - [0] SHD -- C:\ProgramData\Start Menu =>.Microsoft Corporation

O43 - CFD: 25/08/2013 - [] D -- C:\ProgramData\Sun =>.Oracle

O43 - CFD: 02/06/2013 - [] D -- C:\ProgramData\Symantec =>.Symantec

O43 - CFD: 26/07/2012 - [0] SHD -- C:\ProgramData\Templates =>.Microsoft Corporation

O43 - CFD: 22/07/2013 - [] D -- C:\ProgramData\Toshiba =>.Toshiba Corporation

O43 - CFD: 18/06/2016 - [] D -- C:\ProgramData\TreeCardGames =>.TreeCardGames

O43 - CFD: 13/05/2017 - [] D -- C:\ProgramData\Western Digital =>.Western Digital

O43 - CFD: 21/04/2017 - [] D -- C:\ProgramData\WildTangent =>.WildTangent

O43 - CFD: 02/06/2013 - [] D -- C:\ProgramData\win8\_32

O43 - CFD: 02/06/2013 - [] D -- C:\ProgramData\win8\_64

O43 - CFD: 09/12/2016 - [0] D -- C:\ProgramData\{74E9F814-C737-42CC-B721-DBBC4059367A}

O43 - CFD: 16/06/2013 - [0] D -- C:\ProgramData\{CED89F1A-945F-46EC-B23C-5EAF6D2DB12A}

O43 - CFD: 19/07/2017 - [] D -- C:\ProgramData\{EAAB5A83-3809-4B0E-83A6-E4B0DBF2157E}

O43 - CFD: 06/04/2014 - [] D -- C:\Program Files (x86)\Common Files\Adobe =>.Adobe

O43 - CFD: 30/05/2015 - [] D -- C:\Program Files (x86)\Common Files\Apple =>.Apple Inc.

O43 - CFD: 18/03/2018 - [] D -- C:\Program Files (x86)\Common Files\DESIGNER =>.Designer

O43 - CFD: 27/07/2013 - [] D -- C:\Program Files (x86)\Common Files\EPSON =>.EPSON

O43 - CFD: 23/07/2013 - [] D -- C:\Program Files (x86)\Common Files\InstallShield =>.InstallShield

O43 - CFD: 19/07/2017 - [] D -- C:\Program Files (x86)\Common Files\IObit =>.IObit

O43 - CFD: 18/01/2015 - [] D -- C:\Program Files (x86)\Common Files\Java =>.Oracle

O43 - CFD: 16/07/2015 - [] D -- C:\Program Files (x86)\Common Files\Juniper Networks =>.Juniper Networks

O43 - CFD: 18/03/2018 - [] D -- C:\Program Files (x86)\Common Files\Microsoft Shared =>.Microsoft Corporation

O43 - CFD: 02/06/2013 - [] D -- C:\Program Files (x86)\Common Files\postureAgent =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [] D -- C:\Program Files (x86)\Common Files\Services =>.Microsoft Corporation

O43 - CFD: 03/02/2017 - [] D -- C:\Program Files (x86)\Common Files\Skype =>.Skype

O43 - CFD: 23/07/2013 - [0] D -- C:\Program Files (x86)\Common Files\Symantec Shared =>.Symantec Corporation

O43 - CFD: 27/07/2013 - [] D -- C:\Program Files (x86)\Common Files\System =>.Microsoft Corporation

O43 - CFD: 02/06/2013 - [] D -- C:\Program Files (x86)\Common Files\Toshiba Shared =>.Toshiba Corporation

O43 - CFD: 13/05/2017 - [] D -- C:\Program Files (x86)\Common Files\Western Digital =>.Western Digital

O43 - CFD: 03/12/2012 - [] D -- C:\Program Files (x86)\Common Files\Windows Live =>.Microsoft Corporation

O43 - CFD: 14/09/2016 - [] D -- C:\Users\Myriam\AppData\Roaming\Adobe =>.Adobe

O43 - CFD: 16/09/2016 - [] D -- C:\Users\Myriam\AppData\Roaming\Apple Computer =>.Apple Inc.

O43 - CFD: 16/08/2013 - [] D -- C:\Users\Myriam\AppData\Roaming\BlueSprig =>.BlueSprig

O43 - CFD: 22/07/2013 - [] D -- C:\Users\Myriam\AppData\Roaming\Book Place

O43 - CFD: 04/05/2017 - [] D -- C:\Users\Myriam\AppData\Roaming\Box =>.Box

O43 - CFD: 19/09/2013 - [] D -- C:\Users\Myriam\AppData\Roaming\BUFFALO =>.Buffalo Technology

O43 - CFD: 14/09/2016 - [] D -- C:\Users\Myriam\AppData\Roaming\com.adobe.formscentral.FormsCentralForAcrobat =>.Adobe Inc.

O43 - CFD: 19/06/2016 - [] D -- C:\Users\Myriam\AppData\Roaming\Dropbox =>.Dropbox

O43 - CFD: 16/06/2013 - [] D -- C:\Users\Myriam\AppData\Roaming\e-academy Inc =>.e-academy Inc

O43 - CFD: 01/05/2014 - [] D -- C:\Users\Myriam\AppData\Roaming\Epson =>.EPSON

O43 - CFD: 27/07/2013 - [] D -- C:\Users\Myriam\AppData\Roaming\InstallShield =>.InstallShield

O43 - CFD: 09/12/2016 - [] D -- C:\Users\Myriam\AppData\Roaming\IObit =>.IObit

O43 - CFD: 16/07/2015 - [] D -- C:\Users\Myriam\AppData\Roaming\Juniper Networks =>.Juniper Networks

O43 - CFD: 27/07/2013 - [] D -- C:\Users\Myriam\AppData\Roaming\Leadertech =>.Leadertech Systems

O43 - CFD: 16/06/2013 - [] D -- C:\Users\Myriam\AppData\Roaming\Macromedia =>.Macromedia

O43 - CFD: 26/06/2014 - [0] D -- C:\Users\Myriam\AppData\Roaming\Malwarebytes =>.Malwarebytes

O43 - CFD: 16/06/2013 - [] D -- C:\Users\Myriam\AppData\Roaming\McAfee =>.McAfee

O43 - CFD: 29/04/2017 - [] SD -- C:\Users\Myriam\AppData\Roaming\Microsoft =>.Microsoft Corporation

O43 - CFD: 18/11/2017 - [] D -- C:\Users\Myriam\AppData\Roaming\Mozilla =>.Mozilla Corporation

O43 - CFD: 16/06/2013 - [] D -- C:\Users\Myriam\AppData\Roaming\PCCUStubInstaller

O43 - CFD: 27/07/2013 - [] D -- C:\Users\Myriam\AppData\Roaming\PDAppFlex =>Trojan.Elpman

O43 - CFD: 18/01/2015 - [] D -- C:\Users\Myriam\AppData\Roaming\ProductData =>.Microsoft Corporation

O43 - CFD: 03/02/2017 - [] D -- C:\Users\Myriam\AppData\Roaming\Skype =>.Skype

O43 - CFD: 12/02/2016 - [] D -- C:\Users\Myriam\AppData\Roaming\SolidDocuments =>.SolidDocuments

O43 - CFD: 27/06/2017 - [] D -- C:\Users\Myriam\AppData\Roaming\Spotify =>.Spotify

O43 - CFD: 18/06/2016 - [] D -- C:\Users\Myriam\AppData\Roaming\TreeCardGames =>.TreeCardGames

O43 - CFD: 16/06/2013 - [] D -- C:\Users\Myriam\AppData\Roaming\U3 =>.U3

O43 - CFD: 16/08/2013 - [] D -- C:\Users\Myriam\AppData\Roaming\Vtools =>.VTools

O43 - CFD: 13/05/2017 - [] D -- C:\Users\Myriam\AppData\Roaming\Western Digital =>.Western Digital

O43 - CFD: 10/09/2017 - [] D -- C:\Users\Myriam\AppData\Roaming\WhatsApp =>.WhatsApp

O43 - CFD: 21/04/2017 - [] D -- C:\Users\Myriam\AppData\Roaming\WildTangent =>.WildTangent

O43 - CFD: 16/06/2013 - [] D -- C:\Users\Myriam\AppData\Roaming\WinBatch =>.winbatch.com

O43 - CFD: 18/03/2018 - [] D -- C:\Users\Myriam\AppData\Roaming\ZHP =>.Nicolas Coolman

O43 - CFD: 11/03/2018 - [] D -- C:\Users\Myriam\AppData\Local\2F3E4A1F-490A-4346-BF37-8D6D87A92D84.aplzod

O43 - CFD: 27/10/2014 - [] D -- C:\Users\Myriam\AppData\Local\Adobe =>.Adobe

O43 - CFD: 20/04/2014 - [] D -- C:\Users\Myriam\AppData\Local\Apple =>.Apple Inc.

O43 - CFD: 24/04/2016 - [] D -- C:\Users\Myriam\AppData\Local\Apple Computer =>.Apple Inc.

O43 - CFD: 27/12/2015 - [] D -- C:\Users\Myriam\AppData\Local\Apple Inc =>.Apple Inc.

O43 - CFD: 16/06/2013 - [0] SHD -- C:\Users\Myriam\AppData\Local\Application Data =>.Microsoft Corporation

O43 - CFD: 12/08/2015 - [] D -- C:\Users\Myriam\AppData\Local\Box =>.Box

O43 - CFD: 16/06/2017 - [] D -- C:\Users\Myriam\AppData\Local\Box Sync

O43 - CFD: 04/01/2016 - [] D -- C:\Users\Myriam\AppData\Local\CEF =>.CEF

O43 - CFD: 18/03/2018 - [] D -- C:\Users\Myriam\AppData\Local\CrashDumps =>.Microsoft Corporation

O43 - CFD: 10/07/2017 - [] D -- C:\Users\Myriam\AppData\Local\Diagnostics =>.Microsoft Corporation

O43 - CFD: 14/06/2017 - [] D -- C:\Users\Myriam\AppData\Local\Dropbox =>.Dropbox

O43 - CFD: 16/06/2013 - [] D -- C:\Users\Myriam\AppData\Local\e-academy Inc =>.e-academy Inc

O43 - CFD: 16/07/2017 - [0] D -- C:\Users\Myriam\AppData\Local\ElevatedDiagnostics =>.Microsoft Corporation

O43 - CFD: 07/09/2013 - [] D -- C:\Users\Myriam\AppData\Local\Google =>.Google

O43 - CFD: 16/06/2013 - [0] SHD -- C:\Users\Myriam\AppData\Local\History =>.Microsoft Corporation

O43 - CFD: 16/07/2015 - [] D -- C:\Users\Myriam\AppData\Local\Juniper Networks =>.Juniper Networks

O43 - CFD: 22/07/2013 - [0] D -- C:\Users\Myriam\AppData\Local\LogMeIn Rescue Applet =>.LogMeIn

O43 - CFD: 23/07/2013 - [] D -- C:\Users\Myriam\AppData\Local\Macromedia =>.Macromedia

O43 - CFD: 29/04/2017 - [] D -- C:\Users\Myriam\AppData\Local\Microsoft =>.Microsoft Corporation

O43 - CFD: 21/05/2015 - [] D -- C:\Users\Myriam\AppData\Local\Microsoft Help =>.Microsoft Corporation

O43 - CFD: 01/10/2013 - [] D -- C:\Users\Myriam\AppData\Local\Mozilla =>.Mozilla Corporation

O43 - CFD: 11/03/2018 - [] D -- C:\Users\Myriam\AppData\Local\Packages =>.Microsoft Corporation

O43 - CFD: 21/12/2016 - [] D -- C:\Users\Myriam\AppData\Local\Programs =>.Microsoft Corporation

O43 - CFD: 03/02/2017 - [0] D -- C:\Users\Myriam\AppData\Local\Skype =>.Skype

O43 - CFD: 27/06/2017 - [] D -- C:\Users\Myriam\AppData\Local\Spotify =>.Spotify

O43 - CFD: 10/09/2017 - [] D -- C:\Users\Myriam\AppData\Local\SquirrelTemp =>.Squirrels

O43 - CFD: 16/06/2013 - [] D -- C:\Users\Myriam\AppData\Local\SRS Labs =>.SRS Labs

O43 - CFD: 18/03/2018 - [] D -- C:\Users\Myriam\AppData\Local\temp =>.Microsoft Corporation

O43 - CFD: 16/06/2013 - [0] SHD -- C:\Users\Myriam\AppData\Local\Temporary Internet Files =>.Microsoft Corporation

O43 - CFD: 10/05/2016 - [] D -- C:\Users\Myriam\AppData\Local\Toshiba =>.Toshiba Corporation

O43 - CFD: 19/06/2016 - [] D -- C:\Users\Myriam\AppData\Local\VirtualStore =>.Microsoft Corporation

O43 - CFD: 13/05/2017 - [] D -- C:\Users\Myriam\AppData\Local\Western Digital =>.Western Digital

O43 - CFD: 10/09/2017 - [] D -- C:\Users\Myriam\AppData\Local\WhatsApp =>.WhatsApp

O43 - CFD: 10/02/2017 - [] D -- C:\Users\Myriam\AppData\Local\Windows Live =>.Microsoft Corporation

O43 - CFD: 18/03/2018 - [] D -- C:\Users\Myriam\AppData\Local\ZHP =>.Nicolas Coolman

O43 - CFD: 22/07/2013 - [0] D -- C:\Users\Myriam\AppData\Local\Programs\Common =>.Microsoft Corporation

O43 - CFD: 21/12/2016 - [] D -- C:\Users\Myriam\AppData\Local\Programs\Kivuto

O43 - CFD: 16/06/2013 - [] D -- C:\Users\Myriam\AppData\LocalLow\Adobe =>.Adobe

O43 - CFD: 09/12/2016 - [] D -- C:\Users\Myriam\AppData\LocalLow\IObit =>.IObit

O43 - CFD: 22/07/2013 - [] D -- C:\Users\Myriam\AppData\LocalLow\IObit Apps

O43 - CFD: 26/08/2016 - [] SD -- C:\Users\Myriam\AppData\LocalLow\Microsoft =>.Microsoft Corporation

O43 - CFD: 18/03/2018 - [] D -- C:\Users\Myriam\AppData\LocalLow\Mozilla =>.Mozilla Corporation

O43 - CFD: 25/08/2013 - [] D -- C:\Users\Myriam\AppData\LocalLow\Sun =>.Oracle

O43 - CFD: 16/06/2013 - [] D -- C:\Users\Myriam\Desktop\Adobe Acrobat XI

O43 - CFD: 02/09/2013 - [] D -- C:\Users\Myriam\Desktop\Old Firefox Data

O43 - CFD: 26/07/2012 - [] RD -- C:\Users\Myriam\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [] RD -- C:\Users\Myriam\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories =>.Microsoft Corporation

O43 - CFD: 14/10/2015 - [] RD -- C:\Users\Myriam\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools =>.Administrative Tools

O43 - CFD: 21/12/2016 - [] D -- C:\Users\Myriam\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\e5 Secure Download Manager

O43 - CFD: 26/07/2012 - [] D -- C:\Users\Myriam\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance =>.Microsoft Corporation

O43 - CFD: 14/10/2015 - [] RD -- C:\Users\Myriam\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [] RD -- C:\Users\Myriam\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools =>.Microsoft Corporation

O43 - CFD: 10/09/2017 - [] D -- C:\Users\Myriam\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\WhatsApp =>.WhatsApp

O43 - CFD: 26/07/2012 - [0] SHD -- C:\Users\Default\AppData\Local\Application Data =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [0] SHD -- C:\Users\Default\AppData\Local\History =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [] D -- C:\Users\Default\AppData\Local\Microsoft =>.Microsoft Corporation

O43 - CFD: 27/07/2013 - [0] D -- C:\Users\Default\AppData\Local\Microsoft Help =>.Microsoft Corporation

O43 - CFD: 16/08/2013 - [0] D -- C:\Users\Default\AppData\Local\temp =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [0] SHD -- C:\Users\Default\AppData\Local\Temporary Internet Files =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [0] SHD -- C:\Users\Default User\AppData\Local\Application Data =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [0] SHD -- C:\Users\Default User\AppData\Local\History =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [] D -- C:\Users\Default User\AppData\Local\Microsoft =>.Microsoft Corporation

O43 - CFD: 27/07/2013 - [0] D -- C:\Users\Default User\AppData\Local\Microsoft Help =>.Microsoft Corporation

O43 - CFD: 16/08/2013 - [0] D -- C:\Users\Default User\AppData\Local\temp =>.Microsoft Corporation

O43 - CFD: 26/07/2012 - [0] SHD -- C:\Users\Default User\AppData\Local\Temporary Internet Files =>.Microsoft Corporation

O43 - CFD: 19/07/2017 - [] D -- C:\windows\System32\Config\systemprofile\AppData\Local\CrashDumps =>.Microsoft Corporation

O43 - CFD: 14/06/2017 - [] -- C:\windows\System32\Config\systemprofile\AppData\Local\Dropbox =>.Dropbox

O43 - CFD: 29/04/2017 - [] D -- C:\windows\System32\Config\systemprofile\AppData\Local\Microsoft =>.Microsoft Corporation

O43 - CFD: 20/04/2014 - [] D -- C:\windows\System32\Config\systemprofile\AppData\Roaming\Apple Computer =>.Apple Inc.

O43 - CFD: 24/06/2016 - [] -- C:\windows\System32\Config\systemprofile\AppData\Roaming\Dropbox =>.Dropbox

O43 - CFD: 10/12/2016 - [] -- C:\windows\System32\Config\systemprofile\AppData\Roaming\IObit =>.IObit

O43 - CFD: 13/10/2017 - [] -- C:\windows\System32\Config\systemprofile\AppData\Roaming\Macromedia =>.Macromedia

O43 - CFD: 03/12/2012 - [] D -- C:\windows\System32\Config\systemprofile\AppData\Roaming\Microsoft =>.Microsoft Corporation

**---\ Latest files created in Prefetcher (2) - 25s**

O45 - LFCP:[MD5.CB8CD7B164873E80938D32ED60888169] 09/12/2016 A -- C:\windows\Prefetch\ADVANCED SYSTEMCARE.TMP-C97357D3.pf =>.SUP.AdvancedSystemCare

O45 - LFCP:[MD5.6E0720F2F880D665ED0DE50827FA8BA2] 07/09/2013 A -- C:\windows\Prefetch\SEARCHSETTINGS64.EXE-E621C75D.pf =>PUP.Optional.SearchSettings

**---\ ShellIconOverlayIdentifiers (SIOI) (14) - 0s**

O106 - SIOI: DropboxExt1 Class [ DropboxExt01] - {FB314ED9-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.19.0.dll =>.Dropbox, Inc®

O106 - SIOI: DropboxExt7 Class [ DropboxExt02] - {FB314EDF-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.19.0.dll =>.Dropbox, Inc®

O106 - SIOI: DropboxExt9 Class [ DropboxExt03] - {FB314EE1-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.19.0.dll =>.Dropbox, Inc®

O106 - SIOI: DropboxExt3 Class [ DropboxExt04] - {FB314EDB-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.19.0.dll =>.Dropbox, Inc®

O106 - SIOI: DropboxExt2 Class [ DropboxExt05] - {FB314EDA-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.19.0.dll =>.Dropbox, Inc®

O106 - SIOI: DropboxExt4 Class [ DropboxExt06] - {FB314EDC-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.19.0.dll =>.Dropbox, Inc®

O106 - SIOI: DropboxExt5 Class [ DropboxExt07] - {FB314EDD-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.19.0.dll =>.Dropbox, Inc®

O106 - SIOI: DropboxExt8 Class [ DropboxExt08] - {FB314EE0-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.19.0.dll =>.Dropbox, Inc®

O106 - SIOI: DropboxExt10 Class [ DropboxExt09] - {FB314EE2-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.19.0.dll =>.Dropbox, Inc®

O106 - SIOI: DropboxExt6 Class [ DropboxExt10] - {FB314EDE-A251-47B7-93E1-CDD82E34AF8B}. (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.19.0.dll =>.Dropbox, Inc®

O106 - SIOI: Microsoft SkyDrive Pro Icon Overlay 1 (ErrorConflict) [ SkyDrivePro1 (ErrorConflict)] - {8BA85C75-763B-4103-94EB-9470F12FE0F7}. (.Microsoft Corporation - Microsoft OneDrive for Business Extensions.) -- C:\Program Files (x86)\Microsoft Office\root\vfs\ProgramFilesX64\Microsoft Office\Office16\GROOVEEX.DLL =>.Microsoft Corporation®

O106 - SIOI: Microsoft SkyDrive Pro Icon Overlay 2 (SyncInProgress) [ SkyDrivePro2 (SyncInProgress)] - {CD55129A-B1A1-438E-A425-CEBC7DC684EE}. (.Microsoft Corporation - Microsoft OneDrive for Business Extensions.) -- C:\Program Files (x86)\Microsoft Office\root\vfs\ProgramFilesX64\Microsoft Office\Office16\GROOVEEX.DLL =>.Microsoft Corporation®

O106 - SIOI: Microsoft SkyDrive Pro Icon Overlay 3 (InSync) [ SkyDrivePro3 (InSync)] - {E768CD3B-BDDC-436D-9C13-E1B39CA257B1}. (.Microsoft Corporation - Microsoft OneDrive for Business Extensions.) -- C:\Program Files (x86)\Microsoft Office\root\vfs\ProgramFilesX64\Microsoft Office\Office16\GROOVEEX.DLL =>.Microsoft Corporation®

O106 - SIOI: [EnhancedStorageShell] - {D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}. (.Microsoft Corporation - Windows Enhanced Storage Shell Extension DL.) -- C:\Windows\System32\EhStorShell.dll =>.Microsoft Corporation

**---\ Search Context Menu Handlers (SCMH) (31) - 1s**

O108 - CMH1: Adobe.Acrobat.ContextMenu [64Bits] - {A6595CD1-BF77-430A-A452-18696685F7C7} . (.Adobe Systems Inc. - Adobe Acrobat Context Menu.) -- C:\Program Files (x86)\Adobe\Acrobat 11.0\Acrobat Elements\ContextMenuShim64.dll =>.Adobe Systems, Incorporated®

O108 - CMH1: BriefcaseMenu [64Bits] - {85BBD920-42A0-1069-A2E4-08002B30309D} . (.Microsoft Corporation - Windows Briefcase.) -- C:\Windows\System32\syncui.dll =>.Microsoft Corporation

O108 - CMH1: DropboxExt [64Bits] - {ECD97DE5-3C8F-4ACB-AEEE-CCAB78F7711C} . (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.19.0.dll =>.Dropbox, Inc®

O108 - CMH1: IobitStartMenu [64Bits] - {AF8FA9C9-9907-463e-BDC3-4CC1200D6310} . (.IObit - IObitUnlockerExtension.) -- c:\program files (x86)\IObit\Classic Start\IObitStartMenuExtension.dll =>.IObit Information Technology®

O108 - CMH1: Open With [64Bits] - {09799AFB-AD67-11d1-ABCD-00C04FC30936} . (.Microsoft Corporation - Windows Shell Common Dll.) -- C:\Windows\System32\shell32.dll =>.Microsoft Corporation

O108 - CMH1: Open With EncryptionMenu [64Bits] - {A470F8CF-A1E8-4f65-8335-227475AA5C46} . (.Microsoft Corporation - Windows Shell Common Dll.) -- C:\Windows\System32\shell32.dll =>.Microsoft Corporation

O108 - CMH1: PhotoStreamsExt [64Bits] - {89D984B3-813B-406A-8298-118AFA3A22AE} . (.Apple Inc. - ShellStreams.) -- C:\Program Files\Common Files\Apple\Internet Services\ShellStreams64.dll =>.Apple Inc.®

O108 - CMH1: Sharing [64Bits] - {f81e9010-6ea4-11ce-a7ff-00aa003ca9f6} . (.Microsoft Corporation - Shell extensions for sharing.) -- C:\Windows\System32\ntshrui.dll =>.Microsoft Corporation

O108 - CMH1: ShellExtension [64Bits] - . (.Orphan.)

O108 - CMH2: DropboxExt [64Bits] - {ECD97DE5-3C8F-4ACB-AEEE-CCAB78F7711C} . (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.19.0.dll =>.Dropbox, Inc®

O108 - CMH2: IobitStartMenu [64Bits] - {AF8FA9C9-9907-463e-BDC3-4CC1200D6310} . (.IObit - IObitUnlockerExtension.) -- c:\program files (x86)\IObit\Classic Start\IObitStartMenuExtension.dll =>.IObit Information Technology®

O108 - CMH2: OpenContainingFolderMenu [64Bits] - {37ea3a21-7493-4208-a011-7f9ea79ce9f5} . (.Microsoft Corporation - Windows Shell Common Dll.) -- C:\Windows\System32\shell32.dll =>.Microsoft Corporation

O108 - CMH3: CopyAsPathMenu [64Bits] - {f3d06e7c-1e45-4a26-847e-f9fcdee59be0} . (.Microsoft Corporation - Windows Shell Common Dll.) -- C:\Windows\System32\shell32.dll =>.Microsoft Corporation

O108 - CMH3: MBAMShlExt [64Bits] - {57CE581A-0CB6-4266-9CA0-19364C90A0B3} . (.Malwarebytes - Malwarebytes Anti-Malware.) -- C:\Program Files (x86)\Malwarebytes Anti-Malware\mbamext.dll =>.Malwarebytes Corporation®

O108 - CMH3: SendTo [64Bits] - {7BA4C740-9E81-11CF-99D3-00AA004AE837} . (.Microsoft Corporation - Windows Shell Common Dll.) -- C:\Windows\System32\shell32.dll =>.Microsoft Corporation

O108 - CMH4: DropboxExt [64Bits] - {ECD97DE5-3C8F-4ACB-AEEE-CCAB78F7711C} . (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.19.0.dll =>.Dropbox, Inc®

O108 - CMH4: EncryptionMenu [64Bits] - {A470F8CF-A1E8-4f65-8335-227475AA5C46} . (.Microsoft Corporation - Windows Shell Common Dll.) -- C:\Windows\System32\shell32.dll =>.Microsoft Corporation

O108 - CMH4: IobitStartMenu [64Bits] - {AF8FA9C9-9907-463e-BDC3-4CC1200D6310} . (.IObit - IObitUnlockerExtension.) -- c:\program files (x86)\IObit\Classic Start\IObitStartMenuExtension.dll =>.IObit Information Technology®

O108 - CMH4: Sharing [64Bits] - {f81e9010-6ea4-11ce-a7ff-00aa003ca9f6} . (.Microsoft Corporation - Shell extensions for sharing.) -- C:\Windows\System32\ntshrui.dll =>.Microsoft Corporation

O108 - CMH4: ShellExtension [64Bits] - . (.Orphan.)

O108 - CMH5: DropboxExt [64Bits] - {ECD97DE5-3C8F-4ACB-AEEE-CCAB78F7711C} . (.Dropbox, Inc. - Dropbox Shell Extension.) -- C:\Program Files (x86)\Dropbox\Client\DropboxExt64.19.0.dll =>.Dropbox, Inc®

O108 - CMH5: New [64Bits] - {D969A300-E7FF-11d0-A93B-00A0C90F2719} . (.Microsoft Corporation - Windows Shell Common Dll.) -- C:\Windows\System32\shell32.dll =>.Microsoft Corporation

O108 - CMH5: Sharing [64Bits] - {f81e9010-6ea4-11ce-a7ff-00aa003ca9f6} . (.Microsoft Corporation - Shell extensions for sharing.) -- C:\Windows\System32\ntshrui.dll =>.Microsoft Corporation

O108 - CMH6: Adobe.Acrobat.ContextMenu [64Bits] - {A6595CD1-BF77-430A-A452-18696685F7C7} . (.Adobe Systems Inc. - Adobe Acrobat Context Menu.) -- C:\Program Files (x86)\Adobe\Acrobat 11.0\Acrobat Elements\ContextMenuShim64.dll =>.Adobe Systems, Incorporated®

O108 - CMH6: BriefcaseMenu [64Bits] - {85BBD920-42A0-1069-A2E4-08002B30309D} . (.Microsoft Corporation - Windows Briefcase.) -- C:\Windows\System32\syncui.dll =>.Microsoft Corporation

O108 - CMH6: IobitStartMenu [64Bits] - {AF8FA9C9-9907-463e-BDC3-4CC1200D6310} . (.IObit - IObitUnlockerExtension.) -- c:\program files (x86)\IObit\Classic Start\IObitStartMenuExtension.dll =>.IObit Information Technology®

O108 - CMH6: Library Location [64Bits] - {3dad6c5d-2167-4cae-9914-f99e41c12cfa} . (.Microsoft Corporation - Windows Shell Common Dll.) -- C:\Windows\System32\shell32.dll =>.Microsoft Corporation

O108 - CMH6: MBAMShlExt [64Bits] - {57CE581A-0CB6-4266-9CA0-19364C90A0B3} . (.Malwarebytes - Malwarebytes Anti-Malware.) -- C:\Program Files (x86)\Malwarebytes Anti-Malware\mbamext.dll =>.Malwarebytes Corporation®

O108 - CMH7: EnhancedStorageShell [64Bits] - {2854F705-3548-414C-A113-93E27C808C85} . (.Microsoft Corporation - Windows Enhanced Storage Shell Extension DL.) -- C:\Windows\System32\EhStorShell.dll =>.Microsoft Corporation

O108 - CMH7: Sharing [64Bits] - {f81e9010-6ea4-11ce-a7ff-00aa003ca9f6} . (.Microsoft Corporation - Shell extensions for sharing.) -- C:\Windows\System32\ntshrui.dll =>.Microsoft Corporation

O108 - CMH7: ShellExtension [64Bits] - . (.Orphan.)

**---\ Image File Execution Options (13) - 2s**

O50 - IFEO:C:\Windows\System32\cscript.exe - (.Microsoft Corporation - Microsoft ® Console Based Script Host.) [DisableExceptionChainValidation\\3] =>.Microsoft Corporation

O50 - IFEO:C:\Windows\System32\dllhost.exe - (.Microsoft Corporation - COM Surrogate.) [DisableExceptionChainValidation\\3] =>.Microsoft Corporation

O50 - IFEO:C:\Windows\System32\drvinst.exe - (.Microsoft Corporation - Driver Installation Module.) [DisableExceptionChainValidation\\3] =>.Microsoft Corporation

O50 - IFEO:C:\windows\System32\ie4uinit.exe - (.Microsoft Corporation - IE Per-User Initialization Utility.) [MitigationOptions\\256] =>.Microsoft Corporation

O50 - IFEO:C:\Windows\System32\ieUnatt.exe - (.Microsoft Corporation - IE 7.0 Unattended Install Utility.) [MitigationOptions\\256] =>.Microsoft Corporation

O50 - IFEO:C:\Windows\System32\mmc.exe - (.Microsoft Corporation - Microsoft Management Console.) [DisableExceptionChainValidation\\3] =>.Microsoft Corporation

O50 - IFEO:C:\Windows\System32\msfeedssync.exe - (.Microsoft Corporation - Microsoft Feeds Synchronization.) [MitigationOptions\\256] =>.Microsoft Corporation

O50 - IFEO:C:\Windows\System32\mshta.exe - (.Microsoft Corporation - Microsoft (R) HTML Application host.) [MitigationOptions\\256] =>.Microsoft Corporation

O50 - IFEO:C:\Windows\System32\PresentationHost.exe - (.Microsoft Corporation - Windows Presentation Foundation Host.) [MitigationOptions\\1118481] =>.Microsoft Corporation®

O50 - IFEO:C:\windows\System32\PrintIsolationHost.exe - (.Microsoft Corporation - PrintIsolationHost.) [MitigationOptions\\2097152] =>.Microsoft Corporation

O50 - IFEO:C:\Windows\System32\rundll32.exe - (.Microsoft Corporation - Windows host process (Rundll32).) [DisableExceptionChainValidation\\3] =>.Microsoft Corporation

O50 - IFEO:C:\windows\System32\runtimebroker.exe - (.Microsoft Corporation - Runtime Broker.) [MitigationOptions\\4294967296] =>.Microsoft Corporation

O50 - IFEO:C:\Windows\System32\searchprotocolhost.exe - (.Microsoft Corporation - Microsoft Windows Search Protocol Host.) [DisableExceptionChainValidation\\3] =>.Microsoft Corporation

**---\ System Drivers List (75) - 19s**

O58 - SDL:2012/07/26 00:00:49 A . (.LSI - LSI 3ware SCSI Storport Driver.) -- C:\windows\System32\drivers\3ware.sys [106736] =>.Microsoft Windows®

O58 - SDL:2012/07/26 00:00:49 A . (.Adaptec, Inc. - Adaptec Windows SAS/SATA Storport Driver.) -- C:\windows\System32\drivers\adp94xx.sys [492272] =>.Microsoft Windows®

O58 - SDL:2012/07/26 00:00:48 A . (.Adaptec, Inc. - Adaptec Windows SATA Storport Driver.) -- C:\windows\System32\drivers\adpahci.sys [340720] =>.Microsoft Windows®

O58 - SDL:2012/07/26 00:00:49 A . (.Adaptec, Inc. - Adaptec StorPort Ultra320 SCSI Driver (X64).) -- C:\windows\System32\drivers\adpu320.sys [184048] =>.Microsoft Windows®

O58 - SDL:2012/07/26 00:00:49 A . (.Advanced Micro Devices - AHCI 1.2 Device Driver.) -- C:\windows\System32\drivers\amdsata.sys [76016] =>.Microsoft Windows®

O58 - SDL:2012/07/26 00:00:49 A . (.AMD Technologies Inc. - AMD Technology AHCI Compatible Controller D.) -- C:\windows\System32\drivers\amdsbs.sys [258288] =>.Microsoft Windows®

O58 - SDL:2012/07/26 00:00:48 A . (.Advanced Micro Devices - Storage Filter Driver.) -- C:\windows\System32\drivers\amdxata.sys [26352] =>.Microsoft Windows®

O58 - SDL:2012/07/26 00:00:49 A . (.PMC-Sierra, Inc. - Adaptec RAID Storport Driver.) -- C:\windows\System32\drivers\arc.sys [104688] =>.Microsoft Windows®

O58 - SDL:2012/07/26 00:00:48 A . (.PMC-Sierra, Inc. - Adaptec SAS RAID WS03 Driver.) -- C:\windows\System32\drivers\arcsas.sys [108272] =>.Microsoft Windows®

O58 - SDL:2012/06/02 09:31:32 A . (.Qualcomm Atheros Communications, Inc. - Qualcomm Atheros Extensible Wireless LAN de.) -- C:\windows\System32\drivers\athrx.sys [2935808] =>.Qualcomm Atheros Communications, Inc.

O58 - SDL:2012/10/15 04:03:32 A . (.Qualcomm Atheros Communications, Inc. - Qualcomm Atheros Extensible Wireless LAN de.) -- C:\windows\System32\drivers\athw8x.sys [3701760] =>.Qualcomm Atheros Communications, Inc.

O58 - SDL:2012/09/20 02:55:24 A . (.Broadcom Corporation - Broadcom NetXtreme II GigE VBD.) -- C:\windows\System32\drivers\bxvbda.sys [533224] =>.Microsoft Windows®

O58 - SDL:2013/06/02 20:32:10 A . (.Compal Electronics, INC. - CeKbFilter.) -- C:\windows\System32\drivers\CeKbFilter.sys [20312] =>.Compal Electronics, Inc.®

O58 - SDL:2018/03/15 06:50:28 A . (.Dropbox, Inc. - Dropbox Filter Driver.) -- C:\windows\System32\drivers\dbx-canary.sys [45640] =>.Microsoft Windows Hardware Compatibility Publisher®

O58 - SDL:2018/03/15 06:50:28 A . (.Dropbox, Inc. - Dropbox Filter Driver.) -- C:\windows\System32\drivers\dbx-dev.sys [45672] =>.Microsoft Windows Hardware Compatibility Publisher®

O58 - SDL:2018/03/15 06:50:28 A . (.Dropbox, Inc. - Dropbox Filter Driver.) -- C:\windows\System32\drivers\dbx-stable.sys [45640] =>.Microsoft Windows Hardware Compatibility Publisher®

O58 - SDL:2012/09/20 02:55:27 A . (.Broadcom Corporation - Broadcom NetXtreme II 10 GigE VBD.) -- C:\windows\System32\drivers\evbda.sys [3265256] =>.Microsoft Windows®

O58 - SDL:2013/06/16 13:13:45 RSH . (...) -- C:\windows\System32\drivers\fbd.sys [13] =>.EasyCo LLC

O58 - SDL:2012/08/21 13:01:20 A . (.GEAR Software Inc. - CD DVD Filter.) -- C:\windows\System32\drivers\GEARAspiWDM.sys [33240] =>.GEAR Software Inc.®

O58 - SDL:2012/07/03 09:16:02 A . (.Intel Corporation - Intel(R) Management Engine Interface.) -- C:\windows\System32\drivers\HECIx64.sys [62784] =>.Intel Corporation®

O58 - SDL:2012/07/26 00:00:52 A . (.Hewlett-Packard Company - Smart Array SAS/SATA Controller Media Drive.) -- C:\windows\System32\drivers\HpSAMD.sys [64752] =>.Microsoft Windows®

O58 - SDL:2012/09/01 20:01:56 A . (.Intel Corporation - Intel Rapid Storage Technology driver - x64.) -- C:\windows\System32\drivers\iaStorA.sys [647736] =>.Intel Corporation - Intel® Rapid Storage Technology®

O58 - SDL:2012/07/26 00:00:52 A . (.Intel Corporation - Intel Matrix Storage Manager driver - x64.) -- C:\windows\System32\drivers\iaStorV.sys [411888] =>.Microsoft Windows®

O58 - SDL:2012/10/24 01:45:00 A . (.Intel Corporation - Intel Graphics Kernel Mode Driver.) -- C:\windows\System32\drivers\igdkmd64.sys [5332896] =>.Intel Corporation

O58 - SDL:2012/07/26 00:00:52 A . (.Intel Corp./ICP vortex GmbH - Intel/ICP Raid Storport Driver.) -- C:\windows\System32\drivers\iirsp.sys [45296] =>.Microsoft Windows®

O58 - SDL:2012/06/19 10:40:50 A . (.Intel(R) Corporation - Intel(R) Display Audio Driver.) -- C:\windows\System32\drivers\IntcDAud.sys [342528] =>.Intel(R) Corporation

O58 - SDL:2013/03/22 08:17:18 A . (.Juniper Networks, Inc. - Juniper Network Agent Intermediate Driver.) -- C:\windows\System32\drivers\jnprna6.sys [519544] =>.Juniper Networks, Inc.®

O58 - SDL:2013/04/15 04:46:10 A . (.Juniper Networks, Inc. - Juniper Tdi Driver.) -- C:\windows\System32\drivers\jnprTdi\_735\_34907.sys [108336] =>.Juniper Networks, Inc.®

O58 - SDL:2013/03/22 08:17:18 A . (.Juniper Networks, Inc. - Juniper Network Agent Virtual Adapter.) -- C:\windows\System32\drivers\jnprva.sys [26480] =>.Juniper Networks, Inc.®

O58 - SDL:2013/03/22 08:17:18 A . (.Juniper Networks, Inc. - Juniper Network Agent Virtual Adapter Manag.) -- C:\windows\System32\drivers\jnprvamgr.sys [45352] =>.Juniper Networks, Inc.®

O58 - SDL:2012/07/18 18:48:30 A . (.COMPAL ELECTRONIC INC. - LPCFilter.) -- C:\windows\System32\drivers\LPCFilter.sys [35672] =>.Compal Electronics, Inc.®

O58 - SDL:2012/07/26 00:00:52 A . (.LSI Corporation - LSI Fusion-MPT SAS Driver (StorPort).) -- C:\windows\System32\drivers\lsi\_sas.sys [108784] =>.Microsoft Windows®

O58 - SDL:2012/07/26 00:00:52 A . (.LSI Corporation - LSI SAS Gen2 Driver (StorPort).) -- C:\windows\System32\drivers\lsi\_sas2.sys [92400] =>.Microsoft Windows®

O58 - SDL:2012/07/26 00:00:52 A . (.LSI Corporation - LSI Fusion-MPT SCSI Driver (StorPort).) -- C:\windows\System32\drivers\lsi\_scsi.sys [116976] =>.Microsoft Windows®

O58 - SDL:2012/07/26 00:00:52 A . (.LSI Corporation - LSI SSS PCIe/Flash Driver (StorPort).) -- C:\windows\System32\drivers\lsi\_sss.sys [81136] =>.Microsoft Windows®

O58 - SDL:2007/05/09 21:46:36 A . (.Logitech Inc. - Audio filter for Express Plus.) -- C:\windows\System32\drivers\lv302a64.sys [16032] =>.Logitech Inc®

O58 - SDL:2007/05/09 21:46:48 A . (.Logitech Inc. - Logitech QuickCam Driver.) -- C:\windows\System32\drivers\LV302V64.SYS [1127328] =>.Logitech Inc®

O58 - SDL:2007/05/09 21:50:48 A . (.Logitech Inc. - USB Statistic Driver.) -- C:\windows\System32\drivers\LVUSBS64.sys [50208] =>.Logitech Inc®

O58 - SDL:2016/03/10 14:08:54 A . (.Malwarebytes - Malwarebytes Anti-Malware.) -- C:\windows\System32\drivers\mbam.sys [27008] =>.Malwarebytes Corporation®

O58 - SDL:2016/03/10 14:08:58 A . (.Malwarebytes - Malwarebytes Chameleon Protection Driver.) -- C:\windows\System32\drivers\mbamchameleon.sys [140672] =>.Malwarebytes Corporation®

O58 - SDL:2016/06/28 18:39:45 A . (.Malwarebytes - Malwarebytes Anti-Malware.) -- C:\windows\System32\drivers\MBAMSwissArmy.sys [192216] =>.Malwarebytes Corporation®

O58 - SDL:2012/07/26 00:00:52 A . (.LSI Corporation - MEGASAS RAID Controller Driver for Windows.) -- C:\windows\System32\drivers\megasas.sys [51952] =>.Microsoft Windows®

O58 - SDL:2012/07/26 00:00:52 A . (.LSI Corporation, Inc. - LSI MegaRAID Software RAID Driver.) -- C:\windows\System32\drivers\MegaSR.sys [353008] =>.Microsoft Windows®

O58 - SDL:2012/07/26 00:00:55 A . (.Marvell Semiconductor, Inc. - Marvell Flash Controller Driver.) -- C:\windows\System32\drivers\mvumis.sys [64240] =>.Microsoft Windows®

O58 - SDL:2016/03/10 14:09:10 A . (.Malwarebytes Corporation - Malwarebytes Web Access Control.) -- C:\windows\System32\drivers\mwac.sys [65408] =>.Malwarebytes Corporation®

O58 - SDL:2013/07/25 16:53:46 A . (.Apple Inc. - Apple Mobile Device Ethernet.) -- C:\windows\System32\drivers\netaapl64.sys [23040] =>.Apple Inc.

O58 - SDL:2012/07/26 00:00:55 A . (.IBM Corporation - IBM ServeRAID Controller Driver.) -- C:\windows\System32\drivers\nfrd960.sys [52464] =>.Microsoft Windows®

O58 - SDL:2012/07/26 00:00:55 A . (.NVIDIA Corporation - NVIDIA® nForce(TM) RAID Driver.) -- C:\windows\System32\drivers\nvraid.sys [150256] =>.Microsoft Windows®

O58 - SDL:2012/07/26 00:00:55 A . (.NVIDIA Corporation - NVIDIA® nForce(TM) Sata Performance Driver.) -- C:\windows\System32\drivers\nvstor.sys [168176] =>.Microsoft Windows®

O58 - SDL:2012/07/31 03:04:12 A . (.Realtek - Realtek 8101E/8168/8169 NDIS 6.30 64-bit Dr.) -- C:\windows\System32\drivers\Rt630x64.sys [690832] =>.Realtek Semiconductor Corp®

O58 - SDL:2012/12/05 23:01:48 A . (.Realtek Semiconductor Corp. - Realtek(r) High Definition Audio Function D.) -- C:\windows\System32\drivers\RTKVHD64.sys [3242896] =>.Realtek Semiconductor Corp®

O58 - SDL:2012/08/07 20:32:46 A . (.Realtek Semiconductor Corp. - Realtek Pcie CardReader Driver for 2K/XP/Vi.) -- C:\windows\System32\drivers\RtsP2Stor.sys [272016] =>.Realtek Semiconductor Corp®

O58 - SDL:2012/07/26 03:11:43 A . (.Macrovision Corporation, Macrovision Europe Limited, - Macrovision SECURITY Driver.) -- C:\windows\System32\drivers\secdrv.sys [23040] =>.Rovi Corporation

O58 - SDL:2012/07/26 00:00:55 A . (.Silicon Integrated Systems Corp. - SiS RAID Stor Miniport Driver.) -- C:\windows\System32\drivers\sisraid2.sys [44784] =>.Microsoft Windows®

O58 - SDL:2012/07/26 00:00:56 A . (.Silicon Integrated Systems - SiS AHCI Stor-Miniport Driver.) -- C:\windows\System32\drivers\sisraid4.sys [81648] =>.Microsoft Windows®

O58 - SDL:2012/07/26 00:00:55 A . (.Promise Technology, Inc. - Promise SuperTrak EX Series Driver for Wind.) -- C:\windows\System32\drivers\stexstor.sys [30960] =>.Microsoft Windows®

O58 - SDL:2012/07/25 04:54:00 A . (.TOSHIBA Corporation. - TOSHIBA ODD Writing Driver for x64..) -- C:\windows\System32\drivers\tdcmdpst.sys [31184] =>.TOSHIBA CORPORATION®

O58 - SDL:2012/08/10 12:56:56 A . (.TOSHIBA CORPORATION - TOSHIBA HDD Accelerator Driver for x64.) -- C:\windows\System32\drivers\THAccel.sys [131520] =>.TOSHIBA CORPORATION®

O58 - SDL:2012/07/31 14:28:54 A . (. - Toshiba Hotkey Driver.) -- C:\windows\System32\drivers\Thotkey.sys [28632] =>.TOSHIBA CORPORATION®

O58 - SDL:2012/07/28 15:10:08 A . (.TOSHIBA Corporation - TOSHIBA HDD Protection Driver.) -- C:\windows\System32\drivers\thpdrv.sys [48512] =>.TOSHIBA CORPORATION®

O58 - SDL:2012/06/25 16:59:58 A . (.TOSHIBA Corporation - TOSHIBA HDD Protection - Shock Sensor Drive.) -- C:\windows\System32\drivers\Thpevm.sys [18304] =>.TOSHIBA CORPORATION®

O58 - SDL:2014/03/19 22:02:46 A . (.Trend Micro Inc. - TrendMicro Activity Monitor Module.) -- C:\windows\System32\drivers\tmactmon.sys [106000] =>.Trend Micro, Inc.®

O58 - SDL:2013/12/09 21:00:38 A . (.Trend Micro Inc. - TrendMicro Common Module.) -- C:\windows\System32\drivers\tmcomm.sys [297592] =>.Trend Micro, Inc.®

O58 - SDL:2013/07/01 22:08:16 A . (.Trend Micro Inc. - Trend Micro early boot driver.) -- C:\windows\System32\drivers\TMEBC64.sys [50976] =>.Trend Micro, Inc.®

O58 - SDL:2014/02/14 12:57:10 A . (.Trend Micro Inc. - Trend Micro EagleEye Driver (VW) (amd64-fre.) -- C:\windows\System32\drivers\tmeevw.sys [102712] =>.Trend Micro, Inc.®

O58 - SDL:2014/03/19 22:02:42 A . (.Trend Micro Inc. - TrendMicro Event Management Module.) -- C:\windows\System32\drivers\tmevtmgr.sys [69480] =>.Trend Micro, Inc.®

O58 - SDL:2014/02/19 13:11:32 A . (.Trend Micro Inc. - Trend Micro Osprey Scanner Driver (amd64-fr.) -- C:\windows\System32\drivers\tmusa.sys [94008] =>.Trend Micro, Inc.®

O58 - SDL:2012/06/18 12:30:56 A . (.TOSHIBA Corporation - tos\_sps64.) -- C:\windows\System32\drivers\tos\_sps64.sys [499096] =>.TOSHIBA CORPORATION®

O58 - SDL:2012/07/21 17:59:02 A . (.TOSHIBA Corporation - TOSHIBA TVALZ Filter Driver.) -- C:\windows\System32\drivers\TVALZFL.sys [16768] =>.TOSHIBA CORPORATION®

O58 - SDL:2012/07/25 18:34:42 A . (.TOSHIBA Corporation - TOSHIBA ACPI-Based Value Added Logical and.) -- C:\windows\System32\drivers\TVALZ\_O.SYS [32832] =>.TOSHIBA CORPORATION®

O58 - SDL:2015/06/10 23:08:36 A . (.Apple, Inc. - Apple Mobile Device USB Driver.) -- C:\windows\System32\drivers\usbaapl64.sys [54784] =>.Apple, Inc.

O58 - SDL:2012/07/26 00:00:58 A . (.VIA Technologies, Inc. - VIA Generic PCI IDE Bus Driver.) -- C:\windows\System32\drivers\viaide.sys [19184] =>.Microsoft Windows®

O58 - SDL:2012/07/26 00:00:58 A . (.VIA Technologies Inc.,Ltd - VIA RAID DRIVER FOR AMD-X86-64.) -- C:\windows\System32\drivers\vsmraid.sys [164080] =>.Microsoft Windows®

O58 - SDL:2012/07/26 00:00:58 A . (.VIA Corporation - VIA StorX RAID Controller Driver.) -- C:\windows\System32\drivers\VSTXRAID.SYS [322800] =>.Microsoft Windows®

O58 - SDL:2015/11/12 23:50:10 A . (.Western Digital Technologies, Inc. - Western Digital SCSI Architecture Model (SA.) -- C:\windows\System32\drivers\wdcsam64.sys [26880] =>.WDKTestCert wdclab,130885612892544312®

**---\ File Associations Shell Spawning (11) - 0s**

O67 - Shell Spawning: <.bat> [HKLM\..\open\Command] (...) -- '%1' %\* =>.Default.Value

O67 - Shell Spawning: <.cpl> [HKLM\..\cplopen\Command] (.Microsoft Corporation - Windows Control Panel.) -- C:\Windows\System32\control.exe =>.Microsoft Corporation

O67 - Shell Spawning: <.cmd> [HKLM\..\open\Command] (...) -- '%1' %\* =>.Default.Value

O67 - Shell Spawning: <.com> [HKLM\..\open\Command] (...) -- '%1' %\* =>.Default.Value

O67 - Shell Spawning: <.evt> [HKLM\..\open\Command] (.Microsoft Corporation - Event Viewer Snapin Launcher.) -- C:\Windows\System32\eventvwr.exe =>.Microsoft Corporation

O67 - Shell Spawning: <.exe> [HKLM\..\open\Command] (...) -- '%1' %\* =>.Default.Value

O67 - Shell Spawning: <.html> [HKLM\..\open\Command] (.Microsoft Corporation - Internet Explorer.) -- C:\Program Files\Internet Explorer\iexplore.exe =>.Microsoft Corporation®

O67 - Shell Spawning: <.js> [HKLM\..\open\Command] (...) -- %SystemRoot%\System32\WScript.exe '%1' %\* =>.Default.Value

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

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

O67 - Shell Spawning: <.html> [HKCU\..\open\Command] (.Mozilla Corporation - Firefox.) -- C:\Program Files (x86)\Mozilla Firefox\firefox.exe =>.Mozilla Corporation®

**---\ Start Menu Internet (8) - 0s**

O68 - StartMenuInternet: [64Bits][HKLM\..\Shell\open\Command] (.Mozilla Corporation - Firefox.) -- C:\Program Files (x86)\Mozilla Firefox\firefox.exe =>.Mozilla Corporation®

O68 - StartMenuInternet: [64Bits][HKLM\..\Shell\open\Command] (.Microsoft Corporation - Internet Explorer.) -- C:\Program Files (x86)\Internet Explorer\iexplore.exe =>.Microsoft Corporation®

O68 - StartMenuInternet: [64Bits][HKLM\..\InstallInfo\ShowIconsCommand] (.Mozilla Corporation - Firefox Helper.) -- C:\Program Files (x86)\Mozilla Firefox\uninstall\helper.exe =>.Mozilla Corporation

O68 - StartMenuInternet: [64Bits][HKLM\..\InstallInfo\ShowIconsCommand] (.Microsoft Corporation - IE Per-User Initialization Utility.) -- C:\Windows\System32\ie4uinit.exe =>.Microsoft Corporation

O68 - StartMenuInternet: [64Bits][HKLM\..\InstallInfo\ReinstallCommand] (.Mozilla Corporation - Firefox Helper.) -- C:\Program Files (x86)\Mozilla Firefox\uninstall\helper.exe =>.Mozilla Corporation

O68 - StartMenuInternet: [64Bits][HKLM\..\InstallInfo\ReinstallCommand] (.Microsoft Corporation - IE Per-User Initialization Utility.) -- C:\Windows\System32\ie4uinit.exe =>.Microsoft Corporation

O68 - StartMenuInternet: [64Bits][HKLM\..\InstallInfo\HideIconsCommand] (.Mozilla Corporation - Firefox Helper.) -- C:\Program Files (x86)\Mozilla Firefox\uninstall\helper.exe =>.Mozilla Corporation

O68 - StartMenuInternet: [64Bits][HKLM\..\InstallInfo\HideIconsCommand] (.Microsoft Corporation - IE Per-User Initialization Utility.) -- C:\Windows\System32\ie4uinit.exe =>.Microsoft Corporation

**---\ Search Browser Infection (31) - 23s**

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('dom.forms.autocomplete.formautofill', true); =>PUP.Optional.PredictAd

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.irmysearch.aflt', 'dnld2msd'); =>PUP.Optional.MyWebSearch

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.irmysearch.cd', '2XzuyEtN2Y1L1Qzu0CtD0DzyyCtByCyC0B0D0FtA0D0F0AyEtN0D0Tzu0CyCtCyCtN1L2XzutBtFtBtFyEtFyBtAtCt[...] =>PUP.Optional.MyWebSearch

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.irmysearch.cr', '298223812'); =>PUP.Optional.MyWebSearch

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.irmysearch.instlRef', ''); =>PUP.Optional.MyWebSearch

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.aflt', 'dnld2msd'); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.appId', '{CA5CAA63-B27C-4963-9BEC-CB16A36D56F8}'); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.cd', '2XzuyEtN2Y1L1Qzu0CtD0DzyyCtByCyC0B0D0FtA0D0F0AyEtN0D0Tzu0CyCtCyCtN1L2XzutBtFtBtFyEtFyBtAt[...] =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.cr', '298223812'); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.dfltLng', ''); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.dfltSrch', true); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.dnsErr', true); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.excTlbr', false); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.hmpg', true); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.hmpgUrl', 'http://start.mysearchdial.com/?f=1&a=dnld2msd&cd=2XzuyEtN2Y1L1Qzu0CtD0DzyyCtByCyC0B0[...] =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.id', 'C0D96266BDF3DFA4'); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.instlDay', '15955'); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.instlRef', ''); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.newTabUrl', 'http://start.mysearchdial.com/?f=2&a=dnld2msd&cd=2XzuyEtN2Y1L1Qzu0CtD0DzyyCtByCyC0[...] =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.prdct', 'mysearchdial'); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.prtnrId', 'mysearchdial'); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.srchPrvdr', 'Mysearchdial'); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.tlbrId', 'base'); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.tlbrSrchUrl', 'http://start.mysearchdial.com/?f=3&a=dnld2msd&cd=2XzuyEtN2Y1L1Qzu0CtD0DzyyCtByCy[...] =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.vrsn', ''); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial.vrsni', ''); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial\_i.hmpg', true); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial\_i.newTab', false); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial\_i.smplGrp', 'none'); =>Adware.MySearchDial

O69 - SBI: prefs.js [Myriam - auux7g6s.default-1378140617709] user\_pref('extensions.mysearchdial\_i.vrsnTs', '19:42:11'); =>Adware.MySearchDial

O69 - SBI: SearchScopes [HKLM] [64Bits]{0A041559-87C4-581F-4F04-3F9883CFF8DA} - (Bing) - http://www.bing.com/ =>.Bing.com

**---\ Search Svchost Services (34) - 1s**

O83 - Search Svchost Services: AeLookupSvc (AeLookupSvc) . (.Microsoft Corporation - Application Experience Service.) -- C:\windows\System32\aelupsvc.dll [204288] =>.Microsoft Corporation

O83 - Search Svchost Services: CertPropSvc (CertPropSvc) . (.Microsoft Corporation - Microsoft Smartcard Certificate Propagation.) -- C:\Windows\System32\certprop.dll [149504] =>.Microsoft Corporation

O83 - Search Svchost Services: SCPolicySvc (SCPolicySvc) . (.Microsoft Corporation - Microsoft Smartcard Certificate Propagation.) -- C:\Windows\System32\certprop.dll [149504] =>.Microsoft Corporation

O83 - Search Svchost Services: lanmanserver (lanmanserver) . (.Microsoft Corporation - Server Service DLL.) -- C:\Windows\System32\srvsvc.dll [305664] =>.Microsoft Corporation

O83 - Search Svchost Services: gpsvc (gpsvc) . (.Microsoft Corporation - Group Policy Client.) -- C:\Windows\System32\gpsvc.dll [1366016] =>.Microsoft Corporation

O83 - Search Svchost Services: IKEEXT (IKEEXT) . (.Microsoft Corporation - IKE extension.) -- C:\Windows\System32\IKEEXT.DLL [1160192] =>.Microsoft Corporation

O83 - Search Svchost Services: Rasauto (Rasauto) . (.Microsoft Corporation - Remote Access AutoDial Manager.) -- C:\Windows\System32\rasauto.dll [99840] =>.Microsoft Corporation

O83 - Search Svchost Services: Rasman (Rasman) . (.Microsoft Corporation - Remote Access Connection Manager.) -- C:\Windows\System32\rasmans.dll [358400] =>.Microsoft Corporation

O83 - Search Svchost Services: Remoteaccess (Remoteaccess) . (.Microsoft Corporation - Dynamic Interface Manager.) -- C:\Windows\System32\mprdim.dll [107520] =>.Microsoft Corporation

O83 - Search Svchost Services: SENS (SENS) . (.Microsoft Corporation - System Event Notification Service (SENS).) -- C:\Windows\System32\Sens.dll [62976] =>.Microsoft Corporation

O83 - Search Svchost Services: Sharedaccess (Sharedaccess) . (.Microsoft Corporation - Microsoft NAT Helper Components.) -- C:\Windows\System32\ipnathlp.dll [438784] =>.Microsoft Corporation

O83 - Search Svchost Services: Tapisrv (Tapisrv) . (.Microsoft Corporation - Microsoft® Windows(TM) Telephony Server.) -- C:\Windows\System32\tapisrv.dll [305664] =>.Microsoft Corporation

O83 - Search Svchost Services: wuauserv (wuauserv) . (.Microsoft Corporation - Windows Update Agent.) -- C:\Windows\System32\wuaueng.dll [3286016] =>.Microsoft Corporation

O83 - Search Svchost Services: BITS (BITS) . (.Microsoft Corporation - Background Intelligent Transfer Service.) -- C:\Windows\System32\qmgr.dll [826368] =>.Microsoft Corporation

O83 - Search Svchost Services: ShellHWDetection (ShellHWDetection) . (.Microsoft Corporation - Windows Shell Services Dll.) -- C:\Windows\System32\shsvcs.dll [565760] =>.Microsoft Corporation

O83 - Search Svchost Services: iphlpsvc (iphlpsvc) . (.Microsoft Corporation - Service that offers IPv6 connectivity over.) -- C:\Windows\System32\iphlpsvc.dll [894464] =>.Microsoft Corporation

O83 - Search Svchost Services: seclogon (seclogon) . (.Microsoft Corporation - Secondary Logon Service DLL.) -- C:\Windows\System32\seclogon.dll [30720] =>.Microsoft Corporation

O83 - Search Svchost Services: AppInfo (AppInfo) . (.Microsoft Corporation - Application Information Service.) -- C:\Windows\System32\appinfo.dll [70144] =>.Microsoft Corporation

O83 - Search Svchost Services: msiscsi (msiscsi) . (.Microsoft Corporation - iSCSI Discovery service.) -- C:\Windows\System32\iscsiexe.dll [151552] =>.Microsoft Corporation

O83 - Search Svchost Services: EapHost (EapHost) . (.Microsoft Corporation - Microsoft EAPHost service.) -- C:\Windows\System32\eapsvc.dll [105472] =>.Microsoft Corporation

O83 - Search Svchost Services: schedule (schedule) . (.Microsoft Corporation - Task Scheduler Service.) -- C:\Windows\System32\schedsvc.dll [1287680] =>.Microsoft Corporation

O83 - Search Svchost Services: winmgmt (winmgmt) . (.Microsoft Corporation - WMI.) -- C:\Windows\System32\wbem\WMIsvc.dll [219648] =>.Microsoft Corporation

O83 - Search Svchost Services: MMCSS (MMCSS) . (.Microsoft Corporation - Multimedia Class Scheduler Service.) -- C:\Windows\System32\mmcss.dll [80896] =>.Microsoft Corporation

O83 - Search Svchost Services: browser (browser) . (.Microsoft Corporation - Computer Browser Service DLL.) -- C:\Windows\System32\browser.dll [134144] =>.Microsoft Corporation

O83 - Search Svchost Services: ProfSvc (ProfSvc) . (.Microsoft Corporation - ProfSvc.) -- C:\Windows\System32\profsvc.dll [210432] =>.Microsoft Corporation

O83 - Search Svchost Services: SessionEnv (SessionEnv) . (.Microsoft Corporation - Remote Desktop Configuration service.) -- C:\Windows\System32\SessEnv.dll [291328] =>.Microsoft Corporation

O83 - Search Svchost Services: wercplsupport (wercplsupport) . (.Microsoft Corporation - Problem Reports and Solutions.) -- C:\Windows\System32\wercplsupport.dll [84992] =>.Microsoft Corporation

O83 - Search Svchost Services: hkmsvc (hkmsvc) . (.Microsoft Corporation - Key Management Service.) -- C:\Windows\System32\KMSVC.DLL [97792] =>.Microsoft Corporation

O83 - Search Svchost Services: BDESVC (BDESVC) . (.Microsoft Corporation - BDE Service.) -- C:\Windows\System32\bdesvc.dll [190976] =>.Microsoft Corporation

O83 - Search Svchost Services: wlidsvc (wlidsvc) . (.Microsoft Corporation - Microsoft® Account Service.) -- C:\Windows\System32\wlidsvc.dll [1964544] =>.Microsoft Corporation

O83 - Search Svchost Services: Themes (Themes) . (.Microsoft Corporation - Windows Shell Theme Service Dll.) -- C:\Windows\System32\themeservice.dll [47104] =>.Microsoft Corporation

O83 - Search Svchost Services: DsmSvc (DsmSvc) . (.Microsoft Corporation - Device Setup Manager.) -- C:\Windows\System32\DeviceSetupManager.dll [207872] =>.Microsoft Corporation

O83 - Search Svchost Services: NcaSvc (NcaSvc) . (.Microsoft Corporation - Microsoft Network Connectivity Assistant Se.) -- C:\Windows\System32\NcaSvc.dll [161792] =>.Microsoft Corporation

O83 - Search Svchost Services: SystemEventsBroker (SystemEventsBroker) . (.Microsoft Corporation - System Events Broker.) -- C:\Windows\System32\SystemEventsBrokerServer.dll [180224] =>.Microsoft Corporation

**---\ Firewall Active Exception List (39) - 6s**

O87 - FAEL: '{A91F71E6-AE00-489D-BA4F-2D81706F3849}' [In-None-P6-TRUE] .(...) -- C:\Program Files (x86)\McAfee\Common Framework\FrameworkService.exe (.not file.) =>.SUP.Orphan

O87 - FAEL: '{EB2D8515-0D1A-4244-B9E8-18B61BD9B067}' [In-None-P17-TRUE] .(...) -- C:\Program Files (x86)\McAfee\Common Framework\FrameworkService.exe (.not file.) =>.SUP.Orphan

O87 - FAEL: '{5EC79733-02E8-4007-8B87-F0684EB91E4B}' [In-None-P6-TRUE] .(...) -- C:\Program Files (x86)\McAfee\Common Framework\FrameworkService.exe (.not file.) =>.SUP.Orphan

O87 - FAEL: '{816BA1D5-48D6-4A23-9251-AB5AC3E070FB}' [In-None-P17-TRUE] .(...) -- C:\Program Files (x86)\McAfee\Common Framework\FrameworkService.exe (.not file.) =>.SUP.Orphan

O87 - FAEL: '{36E4F7A8-C4BE-4D97-BFE5-D2F855E6BD1D}' [In-None-P6-TRUE] .(...) -- D:\Common\EpsonNet Setup\ENEasyApp.exe (.not file.) =>.SUP.Orphan

O87 - FAEL: '{DD353AB8-174A-4770-8C8E-0EEEFEC603A7}' [In-None-P17-TRUE] .(...) -- D:\Common\EpsonNet Setup\ENEasyApp.exe (.not file.) =>.SUP.Orphan

O87 - FAEL: 'TCP Query User{F266E0A6-7C72-4625-8114-E17805615B13}C:\program files (x86)\epson software\event manager\eeventmanager.exe' [In-None-P6-TRUE] .(.SEIKO EPSON CORPORATION - EEventManager Application.) -- C:\program files (x86)\epson software\event manager\eeventmanager.exe =>.SEIKO EPSON CORPORATION®

O87 - FAEL: 'UDP Query User{B9F3856E-B474-4FFD-9654-AF13E9810797}C:\program files (x86)\epson software\event manager\eeventmanager.exe' [In-None-P17-TRUE] .(.SEIKO EPSON CORPORATION - EEventManager Application.) -- C:\program files (x86)\epson software\event manager\eeventmanager.exe =>.SEIKO EPSON CORPORATION®

O87 - FAEL: 'TCP Query User{EFEC3005-747B-477B-88C3-EE09EBA0148E}C:\program files (x86)\epson software\event manager\eeventmanager.exe' [In-None-P6-TRUE] .(.SEIKO EPSON CORPORATION - EEventManager Application.) -- C:\program files (x86)\epson software\event manager\eeventmanager.exe =>.SEIKO EPSON CORPORATION®

O87 - FAEL: 'UDP Query User{112D68F8-6889-4D4C-81A6-6A3848FE1334}C:\program files (x86)\epson software\event manager\eeventmanager.exe' [In-None-P17-TRUE] .(.SEIKO EPSON CORPORATION - EEventManager Application.) -- C:\program files (x86)\epson software\event manager\eeventmanager.exe =>.SEIKO EPSON CORPORATION®

O87 - FAEL: 'TCP Query User{3EAB0BB4-8B60-47B1-8C21-7B87A17D08DE}C:\users\myriam\appdata\roaming\spotify\spotify.exe' [In-None-P6-TRUE] .(.Spotify Ltd - Spotify.) -- C:\users\myriam\appdata\roaming\spotify\spotify.exe =>.Spotify AB®

O87 - FAEL: 'UDP Query User{6E8B4FB5-C79A-4945-8C71-47894B0F6EAD}C:\users\myriam\appdata\roaming\spotify\spotify.exe' [In-None-P17-TRUE] .(.Spotify Ltd - Spotify.) -- C:\users\myriam\appdata\roaming\spotify\spotify.exe =>.Spotify AB®

O87 - FAEL: '{5E65BE58-918E-48D4-9951-9AE950007AB3}' [In-None-P17-TRUE] .(...) -- C:\Users\Myriam\AppData\Local\Microsoft\SkyDrive\SkyDrive.exe (.not file.) =>.SUP.Orphan

O87 - FAEL: '{7020F699-236B-486F-A9F9-F1DD681ABDDB}' [In-None-P6-TRUE] .(.Mozilla Corporation - Firefox.) -- C:\Program Files (x86)\Mozilla Firefox\firefox.exe =>.Mozilla Corporation®

O87 - FAEL: '{2AF9DC13-2540-4EF6-98BB-4C69378A1293}' [In-None-P17-TRUE] .(.Mozilla Corporation - Firefox.) -- C:\Program Files (x86)\Mozilla Firefox\firefox.exe =>.Mozilla Corporation®

O87 - FAEL: 'TCP Query User{5C3A11F2-E0AE-47E4-9C43-3733B0F7BB19}C:\program files (x86)\mozilla firefox\firefox.exe' [In-None-P6-TRUE] .(.Mozilla Corporation - Firefox.) -- C:\program files (x86)\mozilla firefox\firefox.exe =>.Mozilla Corporation®

O87 - FAEL: 'UDP Query User{9B8A3FB0-3360-4DB9-A294-7902293D456E}C:\program files (x86)\mozilla firefox\firefox.exe' [In-None-P17-TRUE] .(.Mozilla Corporation - Firefox.) -- C:\program files (x86)\mozilla firefox\firefox.exe =>.Mozilla Corporation®

O87 - FAEL: '{5A8B45EA-A736-45F1-9E24-A30EAF8E60D9}' [In-None-P6-TRUE] .(...) -- D:\Network\EpsonNetSetup\ENEasyApp.exe (.not file.) =>.SUP.Orphan

O87 - FAEL: '{B1498BD8-A57E-4846-9D14-9CCA426613B1}' [In-None-P17-TRUE] .(...) -- D:\Network\EpsonNetSetup\ENEasyApp.exe (.not file.) =>.SUP.Orphan

O87 - FAEL: '{7808E7A1-C5B0-4116-987E-4E94667DD1DC}' [In-None-P6-TRUE] .(.SEIKO EPSON CORPORATION - Epson Connect Printer Setup.) -- C:\Program Files (x86)\Epson Software\ECPrinterSetup\ENPApp.exe =>.SEIKO EPSON CORPORATION®

O87 - FAEL: '{01D9D0A1-F735-4665-AA48-3D053E1FB675}' [In-None-P17-TRUE] .(.SEIKO EPSON CORPORATION - Epson Connect Printer Setup.) -- C:\Program Files (x86)\Epson Software\ECPrinterSetup\ENPApp.exe =>.SEIKO EPSON CORPORATION®

O87 - FAEL: 'TCP Query User{25249221-0EED-480D-8306-F101B7C21BAA}C:\program files (x86)\skype\phone\skype.exe' [In-None-P6-TRUE] .(.Skype Technologies S.A. - Skype.) -- C:\program files (x86)\skype\phone\skype.exe =>.Skype Software Sarl®

O87 - FAEL: 'UDP Query User{29763E86-D5F1-4301-89A4-25E81BB993FC}C:\program files (x86)\skype\phone\skype.exe' [In-None-P17-TRUE] .(.Skype Technologies S.A. - Skype.) -- C:\program files (x86)\skype\phone\skype.exe =>.Skype Software Sarl®

O87 - FAEL: 'TCP Query User{2320B5E8-93BC-4943-AFD5-286B1184AA69}C:\program files (x86)\skype\phone\skype.exe' [In-None-P6-TRUE] .(.Skype Technologies S.A. - Skype.) -- C:\program files (x86)\skype\phone\skype.exe =>.Skype Software Sarl®

O87 - FAEL: 'UDP Query User{6E82DDF3-2648-495B-BC4F-3F7B09349C27}C:\program files (x86)\skype\phone\skype.exe' [In-None-P17-TRUE] .(.Skype Technologies S.A. - Skype.) -- C:\program files (x86)\skype\phone\skype.exe =>.Skype Software Sarl®

O87 - FAEL: '{1AC58D3D-8399-4802-8C65-2102FAC89161}' [In-None-P6-TRUE] .(.Mozilla Corporation - Firefox.) -- C:\Program Files (x86)\Mozilla Firefox\firefox.exe =>.Mozilla Corporation®

O87 - FAEL: '{88AAFA3E-53B2-496C-8BA3-167110B58CFC}' [In-None-P17-TRUE] .(.Mozilla Corporation - Firefox.) -- C:\Program Files (x86)\Mozilla Firefox\firefox.exe =>.Mozilla Corporation®

O87 - FAEL: '{54C7EB92-8886-4F71-813F-D32CEBE47C67}' [In-None-P6-TRUE] .(.Apple Inc. - Bonjour Service.) -- C:\Program Files\Bonjour\mDNSResponder.exe =>.Apple Inc.®

O87 - FAEL: '{FEED4B2F-E743-4242-AEE4-7C21C95B1FE1}' [In-None-P17-TRUE] .(.Apple Inc. - Bonjour Service.) -- C:\Program Files\Bonjour\mDNSResponder.exe =>.Apple Inc.®

O87 - FAEL: '{C6A5ED18-9F65-4170-B325-E7912180B9D6}' [In-None-P6-TRUE] .(.Apple Inc. - Bonjour Service.) -- C:\Program Files (x86)\Bonjour\mDNSResponder.exe =>.Apple Inc.®

O87 - FAEL: '{6DF3BB91-B359-461E-9D96-93F7F139FEDC}' [In-None-P17-TRUE] .(.Apple Inc. - Bonjour Service.) -- C:\Program Files (x86)\Bonjour\mDNSResponder.exe =>.Apple Inc.®

O87 - FAEL: '{7CE942A9-91FD-4F52-9D21-D8BC7927750B}' [In-None-P6-TRUE] .(.SEIKO EPSON CORPORATION - EEventManager Application.) -- C:\Program Files (x86)\Epson Software\Event Manager\EEventManager.exe =>.SEIKO EPSON CORPORATION®

O87 - FAEL: '{7089CB11-6B33-4847-8377-1C8EFD96122E}' [In-None-P17-TRUE] .(.SEIKO EPSON CORPORATION - EEventManager Application.) -- C:\Program Files (x86)\Epson Software\Event Manager\EEventManager.exe =>.SEIKO EPSON CORPORATION®

O87 - FAEL: '{04A64927-F9F6-4F80-BEEE-70F40FE7F01C}' [In-None-P17-TRUE] .(...) -- C:\Program Files (x86)\IObit\Advanced SystemCare\Surfing Protection\FFNativeMessage.exe (.not file.) =>.SUP.AdvancedSystemCare

O87 - FAEL: '{AA62DBE2-BDD1-4BAB-AE40-716719A72661}' [Out-None-P17-TRUE] .(...) -- C:\Program Files (x86)\IObit\Advanced SystemCare\Surfing Protection\FFNativeMessage.exe (.not file.) =>.SUP.AdvancedSystemCare

O87 - FAEL: 'TCP Query User{8F1FB95C-E62D-46B6-A5CC-A4B9BFC6DEDB}C:\users\myriam\appdata\roaming\spotify\spotify.exe' [In-None-P6-TRUE] .(.Spotify Ltd - Spotify.) -- C:\users\myriam\appdata\roaming\spotify\spotify.exe =>.Spotify AB®

O87 - FAEL: 'UDP Query User{BF606A8D-7838-4472-B2FB-6D217D2669D7}C:\users\myriam\appdata\roaming\spotify\spotify.exe' [In-None-P17-TRUE] .(.Spotify Ltd - Spotify.) -- C:\users\myriam\appdata\roaming\spotify\spotify.exe =>.Spotify AB®

O87 - FAEL: '{0610831C-40A5-4712-B382-E9E66F2A092A}' [In-None-P17-TRUE] .(.Apple Inc. - iTunes.) -- C:\Program Files\iTunes\iTunes.exe =>.Apple Inc.®

O87 - FAEL: '{3F9AEC84-2C68-413C-AE11-0009F043F6DF}' [In-None-P17-TRUE] .(.Dropbox, Inc. - Dropbox.) -- C:\Program Files (x86)\Dropbox\Client\Dropbox.exe =>.Dropbox, Inc®

**---\ Product Upgrade Codes (1) - 3s**

O90 - PUC: '191089AC088C2B64788B2A7C6165DAF3' . (.IObit Apps Toolbar v7.6.) -- C:\windows\Installer\{CA980191-C880-46B2-87B8-A2C71656AD3F}\ARPPRODUCTICON.exe =>PUP.Optional.Dealio

**---\ Windows Installer Scan (58) - 621s**

[MD5.1B7C1FDDB641474AC4340CCE72AD90C3] [WIS][2017/07/17 21:26:00] (.Apple Inc. - Apple Application Support Installer.) -- C:\windows\Installer\10a466b.msi [48156672] =>.Apple Inc.

[MD5.54FCF46D877C3B3FA8AB0495CB6B06BD] [WIS][2017/07/17 21:26:10] (.Apple Inc. - Apple Application Support Installer.) -- C:\windows\Installer\10a4701.msi [43057152] =>.Apple Inc.

[MD5.E5D5BE27EE42AA69A3C9C14B75502A97] [WIS][2017/07/17 21:26:12] (.Apple Inc. - Apple Software Update Installer.) -- C:\windows\Installer\10a4775.msi [2420736] =>.Apple Inc.

[MD5.5792A6B2CD304664BE8DEBFB9F3DEA47] [WIS][2017/07/17 21:29:25] (.Apple Inc. - iCloud for Windows installer.) -- C:\windows\Installer\10a4861.msi [36315136] =>.Apple Inc.

[MD5.D74A72659B78CB88EB36EF3C35B1C6D2] [WIS][2017/07/17 21:31:27] (.Apple Inc. - Apple Mobile Device Support Installer.) -- C:\windows\Installer\10a4983.msi [13926400] =>.Apple Inc.

[MD5.B86DB6386AA72E09CF30CB59C12FF295] [WIS][2017/07/17 21:32:21] (.Apple Inc. - iTunes Installer.) -- C:\windows\Installer\10a5907.msi [161579008] =>.Apple Inc.

[MD5.E1168CC5789BFAB592EF2B2792331AD2] [WIS][2013/06/02 20:32:06] (.TOSHIBA CORPORATION - TOSHIBA Flash Cards Support Utility.) -- C:\windows\Installer\12096.msi [4784128] =>.TOSHIBA CORPORATION

[MD5.33A78838EB03E5DAB81B24C8AAA7E632] [WIS][2013/06/02 20:32:27] (.Toshiba Corporation - TOSHIBA Password Utility.) -- C:\windows\Installer\1209d.msi [6554112] =>.Toshiba Corporation

[MD5.03DE051B5167A3DE8A58CF98AFCFBAB8] [WIS][2013/06/02 20:32:36] (.Compal - Utility Common Driver.) -- C:\windows\Installer\120b1.msi [999424] =>.Compal

[MD5.E38757BA4F9BA777242D7F368AB5039D] [WIS][2013/06/02 20:33:02] (.InstallShield - InstallShield® 2010 - Premier Edition 16.) -- C:\windows\Installer\120ba.msi [17974272] =>.InstallShield

[MD5.54CE5EA33454EE5FD1D94F5B4FB3900F] [WIS][2012/08/24 20:45:04] (.Toshiba Corporation - TOSHIBA eco Utility.) -- C:\windows\Installer\120bf.msi [6126080] =>.Toshiba Corporation

[MD5.84C660080F00EF0DC4E6CCCF58909D99] [WIS][2012/08/08 13:28:02] (.Toshiba Corporation - TOSHIBA PC Health Monitor.) -- C:\windows\Installer\120c3.msi [63428096] =>.Toshiba Corporation

[MD5.8C082781AB532D4620AF6B8302E2D170] [WIS][2013/06/02 20:34:16] (.Toshiba Corporation - TOSHIBA System Settings.) -- C:\windows\Installer\120c8.msi [12800512] =>.Toshiba Corporation

[MD5.DC9B56810CD7011FED7EC49EDD35A5E9] [WIS][2012/08/10 17:06:40] (.Toshiba Corporation - TOSHIBA HDD Accelerator.) -- C:\windows\Installer\120cc.msi [14968320] =>.Toshiba Corporation

[MD5.85905CE6E76C0E017891C1BFCFBA66C9] [WIS][2013/06/02 20:34:48] (.TOSHIBA Corporation - TOSHIBA HDD Protection.) -- C:\windows\Installer\120d1.msi [17072128] =>.TOSHIBA Corporation

[MD5.90A79A5F47996AE06CB1BD0153D7D175] [WIS][2012/08/23 20:08:26] (.Toshiba Corporation - TOSHIBA VIDEO PLAYER.) -- C:\windows\Installer\120de.msi [7507968] =>.Toshiba Corporation

[MD5.93214D0A859A53E6281AE774EDBA7724] [WIS][2010/09/23 13:03:36] (.Toshiba - Toshiba App Place.) -- C:\windows\Installer\120f1.msi [390656] =>.Toshiba

[MD5.5C43A76F5EF9883204C044FBD1A62982] [WIS][2012/04/20 23:23:42] (.Intel Corporation - Intel(R) Trusted Connect Service Client.) -- C:\windows\Installer\145a2.msi [5363712] =>.Intel Corporation

[MD5.D241785668AA08DC43CFC1A623B7C8EF] [WIS][2016/02/03 16:54:52] (.InstallShield - Toshiba Corporation.) -- C:\windows\Installer\1e9aee.msi [9537536] =>.InstallShield

[MD5.C40E4712DD832A79767ACB3E9E0AF788] [WIS][2015/12/09 16:08:32] (.Toshiba Corporation - TOSHIBA Service Station.) -- C:\windows\Installer\1e9b9d.msi [2863104] =>.Toshiba Corporation

[MD5.86E2B390629665FBC20E06DFBF01A48F] [WIS][2015/12/27 21:15:04] (.Apple Inc. - [ProductName] Installer.) -- C:\windows\Installer\213b05a.msi [2732032] =>.Apple Inc.

[MD5.E705E1C0A7C10EFD74E64331E17382EE] [WIS][2016/12/21 21:36:56] (.Kivuto Solutions Inc. - e5 Secure Download Manager.) -- C:\windows\Installer\2302329.msi [2641920] =>.Kivuto Solutions Inc.

[MD5.56024790CC1B1239123A4EC6AED13AF8] [WIS][2013/06/02 20:27:31] (.SRS Labs, Inc. - SRS Premium Sound Control Panel.) -- C:\windows\Installer\24ef5.msi [13074432] =>.SRS Labs, Inc.

[MD5.24584125598B57E8F4A46893C11EFB07] [WIS][2013/06/02 20:30:23] (.Toshiba Corporation - TOSHIBA System Driver.) -- C:\windows\Installer\24efa.msi [4643328] =>.Toshiba Corporation

[MD5.B505F48886F2E4D25FC2F130AB7E636E] [WIS][2014/08/19 19:52:20] (.SEIKO EPSON Corporation - EpsonNet Print.) -- C:\windows\Installer\258b58.msi [5709824] =>.SEIKO EPSON Corporation

[MD5.6ED3BFCEBE7AEC34E6000779183BE45A] [WIS][2014/11/04 17:00:00] (..) -- C:\windows\Installer\259148.msi [1966080]

[MD5.7D51E9556BEB2DDB15733206DDC72BC5] [WIS][2013/08/25 21:01:12] (.Oracle - Java SE Runtime Environment 7.0.) -- C:\windows\Installer\2741b7a.msi [28045824] =>.Oracle

[MD5.8ED1CD592F0438E74A39FC6CBA6A49F3] [WIS][2014/06/24 04:31:00] (..) -- C:\windows\Installer\313f8c.msi [7312896]

[MD5.8AD9A5167B2B3CAF364111BE6FB3DB90] [WIS][2014/02/05 19:32:11] (.The J2SE Runtime Environment with European languages. - Additional Font and Media Support.) -- C:\windows\Installer\31c2f5.msi [185344]

[MD5.B381630F9A7D0E1F3A0521A9AF2C1484] [WIS][2016/07/26 17:56:28] (.Seiko Epson Corporation - Epson Printer Connection Checker.) -- C:\windows\Installer\4b5cce.msi [5296128] =>.Seiko Epson Corporation

[MD5.B4CBDEA34FE1BC78E98700AEBF619C07] [WIS][2015/06/16 18:14:25] (.SEIKO EPSON CORPORATION - Epson Connect Printer Setup.) -- C:\windows\Installer\58be62.msi [6615552] =>.SEIKO EPSON CORPORATION

[MD5.6762C5BFB3126B2A36BBD209F5185C45] [WIS][2015/08/28 20:07:28] (.Kivuto Solutions Inc..) -- C:\windows\Installer\5aa391.msi [774656] =>.Kivuto Solutions Inc.

[MD5.54B8F72B737F3BC5EA942F5822AD6827] [WIS][2016/04/19 11:59:48] (.Western Digital Technologies, Inc - WD Backup plugin.) -- C:\windows\Installer\7d42f9.msi [4661248] =>.Western Digital Technologies, Inc

[MD5.4B784FCC41288054DFA14B0CA57EF7A8] [WIS][2015/12/07 17:11:46] (.Western Digital Technologies, Inc. - Installs WD Security.) -- C:\windows\Installer\7d42ff.msi [14548992] =>.Western Digital Technologies, Inc.

[MD5.82BB364D85659E4BAF0CE9565AD2DD31] [WIS][2016/01/14 11:47:42] (.Western Digital Technologies, Inc. - Installs WD Drive Utilities.) -- C:\windows\Installer\7d4305.msi [10616832] =>.Western Digital Technologies, Inc.

[MD5.3ABE1BB9ACC60CC0301C5475AAB29094] [WIS][2015/09/15 11:45:08] (.Western Digital Technologies, Inc. - Installs WD Quick View.) -- C:\windows\Installer\7d430d.msi [7790592] =>.Western Digital Technologies, Inc.

[MD5.86EFE4AB4E10B2B46F7DD98FD03289A7] [WIS][2017/02/03 21:03:37] (.Skype Technologies S.A. - Skype.) -- C:\windows\Installer\89f661.msi [43479040] =>.Skype Technologies S.A.

[MD5.F2B947DE87F6238362B5004962332FAA] [WIS][2016/11/29 17:51:22] (.Dropbox, Inc. - Dropbox Update Helper.) -- C:\windows\Installer\94f91.msi [31232] =>.Dropbox, Inc.

[MD5.4DE49166AFB9E01B447106C4B306B27B] [WIS][2017/09/23 11:09:05] (.OpenDNS - Umbrella Roaming Client.) -- C:\windows\Installer\95c68.msi [3186688] =>.OpenDNS

[MD5.BD379D9BD326AEE35A3A8D23E0B56896] [WIS][2012/09/23 23:02:16] (.Adobe Systems Incorporated - Installers.) -- C:\windows\Installer\9bc416.msi [9826304] =>.Adobe Systems Incorporated

[MD5.EC7B6510E220D69D1198C62B456DF069] [WIS][2015/07/16 19:36:55] (.Juniper Networks - Junos Pulse.) -- C:\windows\Installer\a22393.msi [17990144] =>.Juniper Networks

[MD5.AA9D0A4DE1056EC806AB889C76E78B2D] [WIS][2014/08/17 13:45:56] (.SEIKO EPSON CORPORATION - EPSON Printer Finder.) -- C:\windows\Installer\a3a0a3.msi [4668928] =>.SEIKO EPSON CORPORATION

[MD5.DAB13D0A4DACC770A5D3C8D4855ABA46] [WIS][2015/08/28 12:28:54] (.Seiko Epson Corporation - Epson Event Manager.) -- C:\windows\Installer\a9b3aa.msi [22405120] =>.Seiko Epson Corporation

[MD5.09A99D67C3409A872DF9DE79C1B38B19] [WIS][2015/05/28 10:38:02] (.Seiko Epson Corporation - Easy Photo Scan.) -- C:\windows\Installer\a9b641.msi [8155136] =>.Seiko Epson Corporation

[MD5.F29D8115B1ED2A76B5134E6E89A89AA1] [WIS][2014/08/19 10:53:48] (.SEIKO EPSON CORPORATION - Epson E-Web Print.) -- C:\windows\Installer\ba1628.msi [6565888] =>.SEIKO EPSON CORPORATION

[MD5.749A57F9CB8E06860E12B82FF612CF56] [WIS][2011/06/06 15:45:15] (.Adobe Systems Incorporated - ADOBER~1.0

Adobe Reader X (10.0.1).) -- C:\windows\Installer\ee17a.msi [2318848] =>.Adobe Systems Incorporated

[MD5.897C82095021D190D3A3F8CDBFB3237C] [WIS][2012/12/03 00:49:32] (.K-NFB Reading Technology, Inc..) -- C:\windows\Installer\ee183.msi [69089792] =>.K-NFB Reading Technology, Inc.

[MD5.031CF129BE3A0C99AE3489BE3016D214] [WIS][2012/12/03 01:16:15] (.InstallShield - InstallShield® 2010 - Premier Edition 16.) -- C:\windows\Installer\f0598.msi [5215744] =>.InstallShield

[MD5.98A748F45087E20B0553A66E021FEF0C] [WIS][2013/05/11 07:30:56] (.Adobe Systems, Incorporated.) -- C:\windows\Installer\1cc2a.msp [121290752] =>.SUP.Obsolete.Adobe

[MD5.DFB6BF9259D80F50F675227C91F31883] [WIS][2014/01/08 07:27:08] (.Adobe Systems, Incorporated.) -- C:\windows\Installer\23c8d18.msp [20111360] =>.SUP.Obsolete.Adobe

[MD5.839B3FDD01D96AC7535BC196F2A83D98] [WIS][2013/09/03 13:01:59] (.Adobe Systems, Incorporated.) -- C:\windows\Installer\4035b9.msp [19845120] =>.SUP.Obsolete.Adobe

[MD5.9636275EC162AA63562D7F6C0EAEE363] [WIS][2014/01/08 07:17:22] (.Adobe Systems, Incorporated.) -- C:\windows\Installer\4ed808.msp [142704640] =>.SUP.Obsolete.Adobe

[MD5.667661DC34DFAB5AD1789C462C1C0322] [WIS][2014/05/10 06:40:31] (.Adobe Systems, Incorporated.) -- C:\windows\Installer\76c9f8.msp [213078016] =>.SUP.Obsolete.Adobe

[MD5.665DB7F8999A1A35B9B8326FB6619360] [WIS][2013/09/05 11:00:53] (.Adobe Systems, Incorporated.) -- C:\windows\Installer\7b5f81.msp [134643712] =>.SUP.Obsolete.Adobe

[MD5.0BE76A1A7FF21B9A5082823F0A474C40] [WIS][2013/09/26 13:48:57] (.Adobe Systems, Incorporated.) -- C:\windows\Installer\806b14.msp [8671232] =>.SUP.Obsolete.Adobe

[MD5.E25EDBCCE190F1894734DF8A04991797] [WIS][2013/05/10 07:03:40] (.Adobe Systems, Incorporated.) -- C:\windows\Installer\9bc4e3.msp [19456000] =>.SUP.Obsolete.Adobe

[MD5.FBA7EBD975E572319A41583366C7D08B] [WIS][2012/04/04 06:17:36] (.Adobe Systems, Incorporated.) -- C:\windows\Installer\ee17b.msp [16613376] =>.SUP.Obsolete.Adobe

**---\ Search Tracing Registry Key (4) - 1s**

HKLM\SOFTWARE\Microsoft\Tracing\updateluckyleap\_RASAPI32 =>PUP.Optional.LuckyLeap

HKLM\SOFTWARE\Microsoft\Tracing\updateluckyleap\_RASMANCS =>PUP.Optional.LuckyLeap

HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\WebCakeDesktop\_RASAPI32 =>PUP.Optional.WebCake

HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\WebCakeDesktop\_RASMANCS =>PUP.Optional.WebCake

**---\ Additional Scan (O88) (28) - 49s**

C:\windows\System32\Tasks\AV\_PWB =>Adware.TasksRedirect

C:\Users\Myriam\AppData\Roaming\Mozilla\Firefox\Profiles\auux7g6s.default-1378140617709\extensions\iobitapps@mybrowserbar.com =>PUP.Optional.WidgiToolbar

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{CA980191-C880-46B2-87B8-A2C71656AD3F} =>PUP.Optional.Dealio

HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{CA980191-C880-46B2-87B8-A2C71656AD3F} =>PUP.Optional.Dealio

C:\Program Files (x86)\Application Updater =>PUP.Optional.Dealio

C:\Program Files (x86)\IObit Apps Toolbar =>PUP.Optional.Dealio

C:\Users\Myriam\AppData\Roaming\PDAppFlex =>Trojan.Elpman

C:\windows\Prefetch\ADVANCED SYSTEMCARE.TMP-C97357D3.pf =>.SUP.AdvancedSystemCare

C:\windows\Prefetch\SEARCHSETTINGS64.EXE-E621C75D.pf =>PUP.Optional.SearchSettings

HKLM\Software\Classes\\*\ShellEx\ContextMenuHandlers\ShellExtension =>.SUP.Orphan

HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers\ShellExtension =>.SUP.Orphan

HKLM\Software\Classes\Drive\shellex\ContextMenuHandlers\ShellExtension =>.SUP.Orphan

C:\windows\Installer\{CA980191-C880-46B2-87B8-A2C71656AD3F}\ARPPRODUCTICON.exe =>PUP.Optional.Dealio

HKLM\Software\Classes\Installer\Products\191089AC088C2B64788B2A7C6165DAF3 =>PUP.Optional.Dealio

HKLM\Software\Classes\Installer\Features\191089AC088C2B64788B2A7C6165DAF3 =>PUP.Optional.Dealio

C:\windows\Installer\1cc2a.msp =>.SUP.Obsolete.Adobe

C:\windows\Installer\23c8d18.msp =>.SUP.Obsolete.Adobe

C:\windows\Installer\4035b9.msp =>.SUP.Obsolete.Adobe

C:\windows\Installer\4ed808.msp =>.SUP.Obsolete.Adobe

C:\windows\Installer\76c9f8.msp =>.SUP.Obsolete.Adobe

C:\windows\Installer\7b5f81.msp =>.SUP.Obsolete.Adobe

C:\windows\Installer\806b14.msp =>.SUP.Obsolete.Adobe

C:\windows\Installer\9bc4e3.msp =>.SUP.Obsolete.Adobe

C:\windows\Installer\ee17b.msp =>.SUP.Obsolete.Adobe

HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\updateluckyleap\_RASAPI32 =>PUP.Optional.LuckyLeap

HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\updateluckyleap\_RASMANCS =>PUP.Optional.LuckyLeap

HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\WebCakeDesktop\_RASAPI32 =>PUP.Optional.WebCake

HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\WebCakeDesktop\_RASMANCS =>PUP.Optional.WebCake

**---\ Summary of the elements found (13) - 0s**

https://nicolascoolman.eu/2017/09/12/origine-lignes-orphelines/ =>.SUP.Orphan

https://nicolascoolman.eu/2017/10/13/adware-tasksredirect/ =>Adware.TasksRedirect

https://nicolascoolman.eu/2017/01/27/repaquetage-et-infection/ =>PUP.Optional.WidgiToolbar

https://www.nicolascoolman.com/fr/pup-dealio/ =>PUP.Optional.Dealio

https://nicolascoolman.eu/2017/09/23/trojan-elpman/ =>Trojan.Elpman

https://nicolascoolman.eu/2017/12/26/sup-advancedsystemcare/ =>.SUP.AdvancedSystemCare

https://www.nicolascoolman.com/fr/adware-searchsettings/ =>PUP.Optional.SearchSettings

https://www.nicolascoolman.com/fr/adware-predictad/ =>PUP.Optional.PredictAd

https://nicolascoolman.eu/2017/12/17/adware-mywebsearch/ =>PUP.Optional.MyWebSearch

https://nicolascoolman.eu/2017/12/23/adware-mysearchdial/ =>Adware.MySearchDial

https://nicolascoolman.eu/2017/01/20/logiciels-superflus/ =>.SUP.Obsolete.Adobe

https://nicolascoolman.eu/2017/01/27/repaquetage-et-infection/ =>PUP.Optional.LuckyLeap

https://www.nicolascoolman.com/fr/adware-webcake/ =>PUP.Optional.WebCake

~ Unselected Options: O82,

~ End of the scan, 10945 items in 16mn28s (1581)(0)