1Analyse de FRST

Résultats de l'Analyse supplémentaire de Farbar Recovery Scan Tool (x64) Version: 15-03-2017

Exécuté par user (12-04-2017 17:37:26)

Exécuté depuis E:\

Windows 10 Home Version 1607 (X64) (2017-02-01 17:44:27)

Mode d'amorçage: Normal

==========================================================

==================== Comptes: =============================

Administrateur (S-1-5-21-3731384482-835117897-2332532976-500 - Administrator - Disabled)

DefaultAccount (S-1-5-21-3731384482-835117897-2332532976-503 - Limited - Disabled)

Invité (S-1-5-21-3731384482-835117897-2332532976-501 - Limited - Disabled)

user (S-1-5-21-3731384482-835117897-2332532976-1001 - Administrator - Enabled) => C:\Users\user

==================== Centre de sécurité ========================

(Si un élément est inclus dans le fichier fixlist.txt, il sera supprimé.)

AV: Windows Defender (Enabled - Up to date) {D68DDC3A-831F-4fae-9E44-DA132C1ACF46}

AS: Windows Defender (Enabled - Up to date) {D68DDC3A-831F-4fae-9E44-DA132C1ACF46}

==================== Programmes installés ======================

(Seuls les logiciels publicitaires ('adware') avec la marque 'caché' ('Hidden') sont susceptibles d'être ajoutés au fichier fixlist.txt pour qu'ils ne soient plus masqués. Les programmes publicitaires devront être désinstallés manuellement.)

Acer Care Center (HKLM\...\{1AF41E84-3408-499A-8C93-8891F0612719}) (Version: 2.00.3019 - Acer Incorporated)

Acer Configuration Manager (HKLM-x32\...\{414D554E-4453-454E-0201-000000016258}) (Version: 2.1.16258 - Acer)

Acer Portal (HKLM-x32\...\{A5AD0B17-F34D-49BE-A157-C8B3D52ACD13}) (Version: 3.12.2004 - Acer Incorporated)

Acer Quick Access (HKLM\...\{8BBF04F1-C68A-441C-B5EF-446EE9960EAF}) (Version: 2.01.3007 - Acer Incorporated)

Acer UEIP Framework (HKLM\...\{12A718F2-2357-4D41-9E1F-18583A4745F7}) (Version: 3.01.3001 - Acer Incorporated)

Amazon Assistant (HKLM-x32\...\{065E406C-5309-4CE8-9935-189A1EAE1004}) (Version: 10.17.0228 - Amazon) <==== ATTENTION

AOP Framework (HKLM-x32\...\{4A37A114-702F-4055-A4B6-16571D4A5353}) (Version: 3.22.2001.0 - Acer Incorporated)

CyberLink PowerDVD 12 (HKLM-x32\...\InstallShield\_{B46BEA36-0B71-4A4E-AE41-87241643FA0A}) (Version: 12.0.5917.02 - CyberLink Corp.)

Dashlane (HKU\S-1-5-21-3731384482-835117897-2332532976-1001\...\Dashlane) (Version: 4.6.8.26847 - Dashlane, Inc.)

Dashlane Upgrade Service (HKLM-x32\...\Dashlane Upgrade Service) (Version: 2.0.14.0 - Dashlane SAS)

Intel(R) Management Engine Components (HKLM\...\{1CEAC85D-2590-4760-800F-8DE5E91F3700}) (Version: 11.0.0.1153 - Intel Corporation)

Intel(R) Processor Graphics (HKLM-x32\...\{F0E3AD40-2BBD-4360-9C76-B9AC9A5886EA}) (Version: 20.19.15.4531 - Intel Corporation)

Intel(R) Rapid Storage Technology (HKLM\...\{409CB30E-E457-4008-9B1A-ED1B9EA21140}) (Version: 14.5.0.1081 - Intel Corporation)

Intel(R) Serial IO (HKLM\...\{9FD91C5C-44AE-4D9D-85BE-AE52816B0294}) (Version: 1.1.253.0 - Intel Corporation)

Intel® Security Assist (HKLM-x32\...\{4B230374-6475-4A73-BA6E-41015E9C5013}) (Version: 1.0.0.532 - Intel Corporation)

Logiciel pour périphérique à chipset Intel® (x32 Version: 10.1.1.7 - Intel(R) Corporation) Hidden

Malwarebytes version 3.0.6.1469 (HKLM\...\{35065F43-4BB2-439A-BFF7-0F1014F2E0CD}\_is1) (Version: 3.0.6.1469 - Malwarebytes)

McAfee WebAdvisor (HKLM-x32\...\{35ED3F83-4BDC-4c44-8EC6-6A8301C7413A}) (Version: 4.0.124 - McAfee, Inc.)

Microsoft Office 365 - fr-fr (HKLM\...\O365HomePremRetail - fr-fr) (Version: 16.0.7870.2031 - Microsoft Corporation)

Microsoft OneDrive (HKU\S-1-5-21-3731384482-835117897-2332532976-1001\...\OneDriveSetup.exe) (Version: 17.3.6799.0327 - Microsoft Corporation)

Microsoft Visual C++ 2005 Redistributable (HKLM-x32\...\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}) (Version: 8.0.61001 - Microsoft Corporation)

Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.17 (HKLM\...\{8220EEFE-38CD-377E-8595-13398D740ACE}) (Version: 9.0.30729 - Microsoft Corporation)

Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161 (HKLM\...\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}) (Version: 9.0.30729.6161 - Microsoft Corporation)

Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17 (HKLM-x32\...\{9A25302D-30C0-39D9-BD6F-21E6EC160475}) (Version: 9.0.30729 - Microsoft Corporation)

Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 (HKLM-x32\...\{1F1C2DFC-2D24-3E06-BCB8-725134ADF989}) (Version: 9.0.30729.4148 - Microsoft Corporation)

Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (HKLM-x32\...\{9BE518E6-ECC6-35A9-88E4-87755C07200F}) (Version: 9.0.30729.6161 - Microsoft Corporation)

Microsoft Visual C++ 2010 x64 Redistributable - 10.0.30319 (HKLM\...\{DA5E371C-6333-3D8A-93A4-6FD5B20BCC6E}) (Version: 10.0.30319 - Microsoft Corporation)

Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319 (HKLM-x32\...\{196BB40D-1578-3D01-B289-BEFC77A11A1E}) (Version: 10.0.30319 - Microsoft Corporation)

Microsoft Visual C++ 2012 Redistributable (x86) - 11.0.61030 (HKLM-x32\...\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}) (Version: 11.0.61030.0 - Microsoft Corporation)

Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.23026 (HKLM-x32\...\{74d0e5db-b326-4dae-a6b2-445b9de1836e}) (Version: 14.0.23026.0 - Microsoft Corporation)

Mises à jour NVIDIA 2.5.11.45 (Version: 2.5.11.45 - NVIDIA Corporation) Hidden

Mozilla Firefox 51.0.1 (x86 fr) (HKLM-x32\...\Mozilla Firefox 51.0.1 (x86 fr)) (Version: 51.0.1 - Mozilla)

Mozilla Maintenance Service (HKLM-x32\...\MozillaMaintenanceService) (Version: 51.0.1 - Mozilla)

NVIDIA GeForce Experience 2.5.11.45 (HKLM\...\{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_Display.GFExperience) (Version: 2.5.11.45 - NVIDIA Corporation)

NVIDIA Logiciel système PhysX 9.15.0428 (HKLM\...\{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_Display.PhysX) (Version: 9.15.0428 - NVIDIA Corporation)

NVIDIA Pilote graphique 376.54 (HKLM\...\{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_Display.Driver) (Version: 376.54 - NVIDIA Corporation)

Office 16 Click-to-Run Extensibility Component (x32 Version: 16.0.7870.2024 - Microsoft Corporation) Hidden

Office 16 Click-to-Run Extensibility Component 64-bit Registration (Version: 16.0.7830.1018 - Microsoft Corporation) Hidden

Office 16 Click-to-Run Licensing Component (Version: 16.0.7870.2024 - Microsoft Corporation) Hidden

Office 16 Click-to-Run Localization Component (x32 Version: 16.0.7668.2066 - Microsoft Corporation) Hidden

OpenOffice 4.1.2 (HKLM-x32\...\{DCB1B348-C94E-4D6D-8CE0-7D9DA5CF663E}) (Version: 4.12.9782 - Apache Software Foundation)

Panneau de configuration NVIDIA 376.54 (Version: 376.54 - NVIDIA Corporation) Hidden

Qualcomm Atheros 11ac Wireless LAN&Bluetooth Installer (HKLM-x32\...\{3241744A-BA36-41F0-B4AA-EF3946D00632}) (Version: 11.0.0.10164 - Qualcomm Atheros)

Realtek Card Reader (HKLM-x32\...\{5BC2B5AB-80DE-4E83-B8CF-426902051D0A}) (Version: 10.0.10125.31214 - Realtek Semiconductor Corp.)

Realtek Ethernet Controller Driver (HKLM-x32\...\{8833FFB6-5B0C-4764-81AA-06DFEED9A476}) (Version: 10.1.505.2015 - Realtek)

Realtek High Definition Audio Driver (HKLM-x32\...\{F132AF7F-7BCA-4EDE-8A7C-958108FE7DBC}) (Version: 6.0.1.7553 - Realtek Semiconductor Corp.)

SHIELD Streaming (Version: 4.1.3000 - NVIDIA Corporation) Hidden

SHIELD Wireless Controller Driver (Version: 2.5.11.45 - NVIDIA Corporation) Hidden

Spotify Weblink (HKLM-x32\...\{8CADF0CB-E834-4019-9B11-B84E051F2A8E}) (Version: 1.16.1210 - Acer)

==================== Personnalisé CLSID (Avec liste blanche): ==========================

(Si un élément est inclus dans le fichier fixlist.txt, il sera supprimé du Registre. Le fichier ne sera pas déplacé, sauf s'il est inscrit séparément.)

==================== Tâches planifiées (Avec liste blanche) =============

(Si un élément est inclus dans le fichier fixlist.txt, il sera supprimé du Registre. Le fichier ne sera pas déplacé, sauf s'il est inscrit séparément.)

Task: {016D8165-4344-412A-8606-495046BEF82A} - System32\Tasks\AcerCMUpdateTask2.1.16258 => C:\Program Files (x86)\Acer\Amundsen\2.1.16258\AWC.exe [2016-09-20] ()

Task: {0481BC6E-5635-4CA5-9A47-AC5F661D507F} - System32\Tasks\ACC => C:\Program Files (x86)\Acer\Care Center\LiveUpdateChecker.exe [2016-01-20] ()

Task: {355F852A-7001-4393-A65A-7457F7E17AF9} - System32\Tasks\ACCBackgroundApplication => C:\Program Files (x86)\Acer\Care Center\ACCStd.exe [2016-01-20] ()

Task: {4A7AC980-D9BE-4D30-95BA-FA799A76B973} - System32\Tasks\Microsoft\Windows\RemovalTools\MRT\_ERROR\_HB => C:\Windows\system32\MRT.exe [2017-03-18] (Microsoft Corporation)

Task: {5A8C5CDE-3D27-4211-A3B4-D4A8D5FBB8DA} - System32\Tasks\BacKGroundAgent => C:\Program Files (x86)\Acer\AOP Framework\BackgroundAgent.exe [2016-08-30] (Acer Incorporated)

Task: {5D4263AA-0684-4E61-8CE0-7BABD1E32D4B} - System32\Tasks\Quick Access => C:\Program Files\Acer\Acer Quick Access\QALauncher.exe [2016-07-29] (Acer Incorporated)

Task: {7A42161B-05F9-4232-9519-7FFBB1E9A8C1} - System32\Tasks\Microsoft\Office\Office ClickToRun Service Monitor => C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe [2017-03-26] (Microsoft Corporation)

Task: {86434968-EE8C-4516-BCB8-6D64719AFCCE} - System32\Tasks\FUBTrackingByPLD => C:\OEM\Preload\FubTracking\FubTracking.exe [2015-05-14] ()

Task: {982E8A31-B494-42FC-8CFE-1062953DD965} - System32\Tasks\AcerCloud => C:\Program Files (x86)\Acer\Acer Portal\AcerPortal.exe [2016-09-09] (Acer)

Task: {9DAAB51A-ED8E-467E-A0E8-12C95E06EEA6} - System32\Tasks\Power Button => C:\Program Files\Acer\Acer Quick Access\ePowerButton\_NB.exe [2016-07-29] (Acer Incorporated)

Task: {B0A1AD74-05A7-4252-8130-70601E0180A2} - System32\Tasks\UbtFrameworkService => C:\Program Files\Acer\User Experience Improvement Program\Framework\TriggerFramework.exe [2014-03-13] (TODO: <Company name>)

Task: {BDE1BE1C-A759-42B1-9B2D-218176652810} - System32\Tasks\Microsoft\Office\Office Automatic Updates => C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe [2017-03-26] (Microsoft Corporation)

Task: {E28D7D70-5F9A-4819-90B5-C2819368534A} - System32\Tasks\ACCAgent => C:\Program Files (x86)\Acer\Care Center\LiveUpdateAgent.exe [2016-01-20] ()

(Si un élément est inclus dans le fichier fixlist.txt, le fichier tâche (.job) sera déplacé. Le fichier exécuté par la tâche ne sera pas déplacé.)

==================== Raccourcis =============================

(Les éléments sont susceptibles d'être inscrits dans le fichier fixlist.txt afin d'être supprimés ou restaurés.)

==================== Modules chargés (Avec liste blanche) ==============

2017-02-28 16:19 - 2017-02-28 16:19 - 00102064 \_\_\_\_\_ () C:\Program Files (x86)\Amazon\Amazon Assistant\amazonAssistantService.exe

2017-02-28 16:20 - 2017-02-28 16:20 - 00141488 \_\_\_\_\_ () C:\Program Files (x86)\Amazon\Amazon Assistant\aaLoader64.dll

2017-04-11 19:28 - 2017-03-24 04:09 - 02271520 \_\_\_\_\_ () C:\PROGRAM FILES\MALWAREBYTES\ANTI-MALWARE\PoliciesControllerImpl.dll

2016-07-16 13:42 - 2016-07-16 13:42 - 00231424 \_\_\_\_\_ () C:\WINDOWS\SYSTEM32\ism32k.dll

2017-03-18 23:20 - 2017-03-04 09:19 - 02681200 \_\_\_\_\_ () C:\WINDOWS\System32\CoreUIComponents.dll

2017-02-01 19:15 - 2016-12-29 15:16 - 00134712 \_\_\_\_\_ () C:\Program Files\NVIDIA Corporation\Display\NvSmartMax64.dll

2017-03-18 23:20 - 2017-03-04 09:19 - 02681200 \_\_\_\_\_ () C:\WINDOWS\system32\CoreUIComponents.dll

2017-03-18 23:20 - 2017-03-04 09:19 - 02681200 \_\_\_\_\_ () C:\WINDOWS\SYSTEM32\CoreUIComponents.dll

2017-02-01 02:01 - 2017-02-01 02:01 - 00410616 \_\_\_\_\_ () C:\WINDOWS\system32\igfxTray.exe

2017-02-01 23:20 - 2016-09-07 06:56 - 00134656 \_\_\_\_\_ () C:\Windows\ShellExperiences\Windows.UI.Shell.SharedUtilities.dll

2017-03-18 23:19 - 2017-03-04 08:31 - 00474112 \_\_\_\_\_ () C:\Windows\ShellExperiences\QuickActions.dll

2017-03-18 23:20 - 2017-03-04 08:12 - 09760768 \_\_\_\_\_ () C:\Windows\SystemApps\Microsoft.Windows.Cortana\_cw5n1h2txyewy\CortanaApi.dll

2017-03-18 23:20 - 2017-03-04 08:05 - 01401856 \_\_\_\_\_ () C:\Windows\SystemApps\Microsoft.Windows.Cortana\_cw5n1h2txyewy\Cortana.Core.dll

2017-03-18 23:20 - 2017-03-04 08:05 - 00757248 \_\_\_\_\_ () C:\Windows\SystemApps\Microsoft.Windows.Cortana\_cw5n1h2txyewy\CSGSuggestLib.dll

2017-03-18 23:21 - 2017-03-04 08:05 - 01033216 \_\_\_\_\_ () C:\Windows\SystemApps\Microsoft.Windows.Cortana\_cw5n1h2txyewy\Cortana.Actions.dll

2017-03-18 23:20 - 2017-03-04 08:05 - 02424320 \_\_\_\_\_ () C:\Windows\SystemApps\Microsoft.Windows.Cortana\_cw5n1h2txyewy\Cortana.BackgroundTask.dll

2017-03-18 23:21 - 2017-03-04 08:08 - 04853760 \_\_\_\_\_ () C:\Windows\SystemApps\Microsoft.Windows.Cortana\_cw5n1h2txyewy\RemindersUI.dll

2017-02-01 17:15 - 2017-03-17 17:48 - 00544208 \_\_\_\_\_ () C:\Users\user\AppData\Roaming\Dashlane\DashlanePlugin.exe

2016-08-16 04:09 - 2015-05-14 09:10 - 00030976 \_\_\_\_\_ () C:\OEM\Preload\FubTracking\FubTracking.exe

2017-03-18 23:20 - 2017-03-04 08:04 - 00114176 \_\_\_\_\_ () C:\Windows\SystemApps\Microsoft.Windows.Cortana\_cw5n1h2txyewy\Cortana.Dss.BackgroundTask.dll

2015-06-24 01:07 - 2015-06-24 01:07 - 01243936 \_\_\_\_\_ () C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\ACE.dll

2016-08-16 03:40 - 2015-07-14 21:06 - 00011920 \_\_\_\_\_ () C:\Program Files (x86)\NVIDIA Corporation\Update Core\detoured.dll

2017-02-28 16:23 - 2017-02-28 16:23 - 00116912 \_\_\_\_\_ () C:\Program Files (x86)\Amazon\Amazon Assistant\aaLoader.dll

2017-04-10 17:54 - 2017-03-17 17:48 - 00338896 \_\_\_\_\_ () C:\Users\user\AppData\Roaming\Dashlane\4.6.8.26847\bin\Firefox\_Extension\{442718d9-475e-452a-b3e1-fb1ee16b8e9f}\components\KWDebugDll\_win32.4.6.8.26847.dll

2017-04-10 17:54 - 2017-03-17 17:48 - 00441808 \_\_\_\_\_ () C:\Users\user\AppData\Roaming\Dashlane\4.6.8.26847\bin\Firefox\_Extension\{442718d9-475e-452a-b3e1-fb1ee16b8e9f}\components\KWDebug.4.6.8.26847.dll

2017-04-10 17:54 - 2017-03-17 17:48 - 00464848 \_\_\_\_\_ () C:\Users\user\AppData\Roaming\Dashlane\4.6.8.26847\bin\Firefox\_Extension\{442718d9-475e-452a-b3e1-fb1ee16b8e9f}\components\KWUtils.4.6.8.26847.dll

2017-04-10 17:54 - 2017-03-17 17:48 - 62708176 \_\_\_\_\_ () C:\Users\user\AppData\Roaming\Dashlane\4.6.8.26847\bin\Firefox\_Extension\{442718d9-475e-452a-b3e1-fb1ee16b8e9f}\components\KWExternLib.4.6.8.26847.dll

2017-04-10 17:54 - 2017-03-17 17:48 - 00285648 \_\_\_\_\_ () C:\Users\user\AppData\Roaming\Dashlane\4.6.8.26847\bin\Firefox\_Extension\{442718d9-475e-452a-b3e1-fb1ee16b8e9f}\components\KWMainLib\_win.4.6.8.26847.dll

2017-04-10 17:54 - 2017-03-17 17:48 - 06183888 \_\_\_\_\_ () C:\Users\user\AppData\Roaming\Dashlane\4.6.8.26847\bin\Firefox\_Extension\{442718d9-475e-452a-b3e1-fb1ee16b8e9f}\components\KWData.4.6.8.26847.dll

2017-04-10 17:54 - 2017-03-17 17:48 - 07271888 \_\_\_\_\_ () C:\Users\user\AppData\Roaming\Dashlane\4.6.8.26847\bin\Firefox\_Extension\{442718d9-475e-452a-b3e1-fb1ee16b8e9f}\components\KWApplication.4.6.8.26847.dll

2017-04-10 17:54 - 2017-03-17 17:48 - 13684176 \_\_\_\_\_ () C:\Users\user\AppData\Roaming\Dashlane\4.6.8.26847\bin\Firefox\_Extension\{442718d9-475e-452a-b3e1-fb1ee16b8e9f}\components\KWMainLib.4.6.8.26847.dll

2017-04-10 17:54 - 2017-03-17 17:48 - 02215888 \_\_\_\_\_ () C:\Users\user\AppData\Roaming\Dashlane\4.6.8.26847\bin\Firefox\_Extension\{442718d9-475e-452a-b3e1-fb1ee16b8e9f}\components\KWMainLibData.4.6.8.26847.dll

2017-04-10 17:54 - 2017-03-17 17:48 - 00334288 \_\_\_\_\_ () C:\Users\user\AppData\Roaming\Dashlane\4.6.8.26847\bin\Firefox\_Extension\{442718d9-475e-452a-b3e1-fb1ee16b8e9f}\components\Kwift\_DP.4.6.8.26847.dll

2017-02-01 19:23 - 2017-02-01 19:23 - 00015064 \_\_\_\_\_ () C:\WINDOWS\assembly\GAC\_MSIL\MyService\1.0.0.1\_\_2dfa3f50f0bed57d\MyService.dll

2016-08-30 16:09 - 2016-08-30 16:09 - 00013016 \_\_\_\_\_ () C:\Program Files (x86)\Acer\AOP Framework\ServiceInterface.dll

2016-08-30 16:05 - 2016-08-30 16:05 - 00277856 \_\_\_\_\_ () C:\Program Files (x86)\Acer\AOP Framework\libcurl.dll

2016-09-09 11:51 - 2016-09-09 11:51 - 00202456 \_\_\_\_\_ () C:\Program Files (x86)\Acer\Acer Portal\curllib.dll

2016-09-09 11:51 - 2016-09-09 11:51 - 00119000 \_\_\_\_\_ () C:\Program Files (x86)\Acer\Acer Portal\OpenLDAP.dll

2016-09-20 11:20 - 2016-09-20 11:20 - 00152880 \_\_\_\_\_ () C:\Program Files (x86)\Acer\Amundsen\2.1.16258\AWC.exe

==================== Alternate Data Streams (Avec liste blanche) =========

(Si un élément est inclus dans le fichier fixlist.txt, seul le flux de données additionnel (ADS - Alternate Data Stream) sera supprimé.)

==================== Mode sans échec (Avec liste blanche) ===================

(Si un élément est inclus dans le fichier fixlist.txt, il sera supprimé du Registre. Le "AlternateShell" sera restauré.)

HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\MBAMService => ""="Service"

HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\MBAMService => ""="Service"

==================== Association (Avec liste blanche) ===============

(Si un élément est inclus dans le fichier fixlist.txt, l'élément de Registre sera restauré à la valeur par défaut ou supprimé.)

==================== Internet Explorer sites de confiance/sensibles ===============

(Si un élément est inclus dans le fichier fixlist.txt, il sera supprimé du Registre.)

==================== Hosts contenu: ===============================

(Si nécessaire, la commande Hosts: peut être incluse dans le fichier fixlist.txt afin de réinitialiser le fichier hosts.)

2015-10-30 09:24 - 2015-10-30 09:21 - 00000824 \_\_\_\_A C:\WINDOWS\system32\Drivers\etc\hosts

==================== Autres zones ============================