Additional scan result of Farbar Recovery Scan Tool (x64) Version: 19.02.2024 02

Ran by Mimi (22-02-2024 18:53:54)

Running from C:\Users\Mimi\Downloads

Microsoft Windows 11 Professionnel Version 22H2 22621.3155 (X64) (2023-11-26 16:29:37)

Boot Mode: Normal

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

==================== Accounts: =============================

(If an entry is included in the fixlist, it will be removed.)

Administrateur (S-1-5-21-2123058746-3684523357-4272769664-500 - Administrator - Disabled)

DefaultAccount (S-1-5-21-2123058746-3684523357-4272769664-503 - Limited - Disabled)

Invité (S-1-5-21-2123058746-3684523357-4272769664-501 - Limited - Disabled)

Mimi (S-1-5-21-2123058746-3684523357-4272769664-1001 - Administrator - Enabled) => C:\Users\Mimi

WDAGUtilityAccount (S-1-5-21-2123058746-3684523357-4272769664-504 - Limited - Disabled)

==================== Security Center ========================

(If an entry is included in the fixlist, it will be removed.)

AV: Malwarebytes (Enabled - Up to date) {0D452135-A081-B000-D6B6-132E52638543}

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

==================== Installed Programs ======================

(Only the adware programs with "Hidden" flag could be added to the fixlist to unhide them. The adware programs should be uninstalled manually.)

Adobe Photoshop CS6 (HKLM-x32\...\{74EB3499-8B95-4B5C-96EB-7B342F3FD0C6}) (Version: 13.0 - Adobe Systems Incorporated)

Amazon Appstore (HKU\S-1-5-21-2123058746-3684523357-4272769664-1001\...\com.amazon.venezia) (Version: release-60.22.1.0.210093.0\_646810 - amazon.com)

AOMEI Backupper (HKLM-x32\...\{A83692F5-3E9B-4E95-9E7E-B5DF5536CE9D}\_is1) (Version: 7.3.3 - AOMEI International Network Limited.)

AOMEI Partition Assistant 10.2.1 (HKLM-x32\...\{04F850ED-FD0F-4ED1-AE1B-4498165BF3D2}\_is1) (Version: 10.2.1 - AOMEI International Network Limited.)

Assistant de téléchargement de composants pour Studio-Scrap (HKLM-x32\...\{0DBE7DEA-1DC9-4B00-8396-FC81C5D24DD8}}\_is1) (Version: - CDIP)

Audible (HKU\S-1-5-21-2123058746-3684523357-4272769664-1001\...\com.audible.application) (Version: 3.67.0 - audible.com)

calibre 64bit (HKLM\...\{9E38FA2A-6295-45FA-880A-C7F3E151B248}) (Version: 7.1.0 - Kovid Goyal)

Documentation Manager (HKLM\...\{87CA98A2-FF74-4CBE-81D8-0E9145F4A97C}) (Version: 22.30.0.11 - Intel Corporation) Hidden

Foxit PDF Reader (HKLM-x32\...\Foxit Reader\_is1) (Version: 2023.3.0.23028 - Foxit Software Inc.)

Freemake Video Converter version 4.1.13 (HKLM-x32\...\Freemake Video Converter\_is1) (Version: 4.1.13 - Mixbyte Inc.)

Google Chrome (HKLM-x32\...\Google Chrome) (Version: 122.0.6261.58 - Google LLC)

HiBit Uninstaller 3.1.90.100 (HKLM-x32\...\{318AF7D1-C350-4F69-8C13-83B88BFF1355}\_is1) (Version: 3.1.90.100 - HiBitSoftware)

Intel Driver && Support Assistant (HKLM-x32\...\{7D392FB7-64D5-4813-B7F7-8AA462D3968D}) (Version: 23.4.39.9 - Intel) Hidden

Intel(R) Chipset Device Software (HKLM\...\{7FB35D08-C75C-4A18-B593-1D7C3E8970AD}) (Version: 10.1.1.45 - Intel Corporation) Hidden

Intel(R) Computing Improvement Program (HKLM\...\{88B98508-2D8F-46F1-90AD-557BE40C7067}) (Version: 2.4.07642 - Intel Corporation)

Intel(R) Wireless Bluetooth(R) (HKLM-x32\...\{00000030-0220-1036-84C8-B8D95FA3C8C3}) (Version: 22.30.0.4 - Intel Corporation)

Intel® Driver & Support Assistant (HKLM-x32\...\{b82e9573-04fb-4a9d-819f-6c358a1cf31a}) (Version: 23.4.39.9 - Intel)

Intel® Software Installer (HKLM-x32\...\{469cd1ee-2994-481c-ad19-874d4d32525b}) (Version: 22.30.0.11 - Intel Corporation) Hidden

Logiciel pour périphérique à chipset Intel® (HKLM-x32\...\{44ded3eb-1686-46a6-9770-fd79096c29f7}) (Version: 10.1.1.45 - Intel(R) Corporation) Hidden

Malwarebytes version 4.6.9.314 (HKLM\...\{35065F43-4BB2-439A-BFF7-0F1014F2E0CD}\_is1) (Version: 4.6.9.314 - Malwarebytes)

Microsoft Edge (HKLM-x32\...\Microsoft Edge) (Version: 121.0.2277.128 - Microsoft Corporation)

Microsoft Edge WebView2 Runtime (HKLM-x32\...\Microsoft EdgeWebView) (Version: 121.0.2277.128 - Microsoft Corporation)

Microsoft Office Professional Plus 2021 - fr-fr (HKLM\...\ProPlus2021Retail - fr-fr) (Version: 16.0.17231.20236 - Microsoft Corporation)

Microsoft Office Professionnel Plus 2019 - fr-fr (HKLM\...\ProPlus2019Retail - fr-fr) (Version: 16.0.17231.20236 - Microsoft Corporation)

Microsoft OneDrive (HKLM\...\OneDriveSetup.exe) (Version: 24.020.0128.0003 - Microsoft Corporation)

Microsoft Update Health Tools (HKLM\...\{C6FD611E-7EFE-488C-A0E0-974C09EF6473}) (Version: 5.72.0.0 - Microsoft Corporation)

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

Microsoft Visual C++ 2005 Redistributable (x64) (HKLM\...\{ad8a2fa1-06e7-4b0d-927d-6e54b3d31028}) (Version: 8.0.61000 - Microsoft Corporation)

Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148 (HKLM\...\{4B6C7001-C7D6-3710-913E-5BC23FCE91E6}) (Version: 9.0.30729.4148 - 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++ 2010 x64 Redistributable - 10.0.40219 (HKLM\...\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}) (Version: 10.0.40219 - Microsoft Corporation)

Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (HKLM-x32\...\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}) (Version: 10.0.40219 - Microsoft Corporation)

Microsoft Visual C++ 2012 Redistributable (x64) - 11.0.61030 (HKLM-x32\...\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}) (Version: 11.0.61030.0 - Microsoft Corporation)

Microsoft Visual C++ 2012 x64 Additional Runtime - 11.0.61030 (HKLM\...\{37B8F9C7-03FB-3253-8781-2517C99D7C00}) (Version: 11.0.61030 - Microsoft Corporation) Hidden

Microsoft Visual C++ 2012 x64 Minimum Runtime - 11.0.61030 (HKLM\...\{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}) (Version: 11.0.61030 - Microsoft Corporation) Hidden

Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.32.31332 (HKLM-x32\...\{3746f21b-c990-4045-bb33-1cf98cff7a68}) (Version: 14.32.31332.0 - Microsoft Corporation)

Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.32.31332 (HKLM-x32\...\{a98dc6ff-d360-4878-9f0a-915eba86eaf3}) (Version: 14.32.31332.0 - Microsoft Corporation)

Microsoft Visual C++ 2022 X64 Additional Runtime - 14.32.31332 (HKLM\...\{F4499EE3-A166-496C-81BB-51D1BCDC70A9}) (Version: 14.32.31332 - Microsoft Corporation) Hidden

Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.32.31332 (HKLM\...\{3407B900-37F5-4CC2-B612-5CD5D580A163}) (Version: 14.32.31332 - Microsoft Corporation) Hidden

Microsoft Visual C++ 2022 X86 Additional Runtime - 14.32.31332 (HKLM-x32\...\{8972AC25-452E-4FFE-945A-EB9E28C20322}) (Version: 14.32.31332 - Microsoft Corporation) Hidden

Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.32.31332 (HKLM-x32\...\{AEAA18F7-9C96-4A43-BC07-8B88A4913EEB}) (Version: 14.32.31332 - Microsoft Corporation) Hidden

Microsoft\_VC80\_CRT\_x86 (HKLM-x32\...\{92D58719-BBC1-4CC3-A08B-56C9E884CC2C}) (Version: 8.0.50727.4053 - Adobe) Hidden

Microsoft\_VC90\_CRT\_x86 (HKLM-x32\...\{08D2E121-7F6A-43EB-97FD-629B44903403}) (Version: 1.00.0000 - Adobe) Hidden

MyRecover (HKLM-x32\...\{2219F43E-84A9-44A6-8179-B0D4C2D077FB}\_is1) (Version: 3.6.0 - AOMEI International Network Limited.)

Notifications de Studio-Scrap 1.0.0.0 (HKLM-x32\...\{DC2AE926-8223-49E8-A055-FDDE9B567F89}\_is1) (Version: 1.0.0.0 - CDIP)

NVIDIA FrameView SDK 1.1.4923.29968894 (HKLM\...\{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_FrameViewSdk) (Version: 1.1.4923.29968894 - NVIDIA Corporation)

NVIDIA GeForce Experience 3.23.0.74 (HKLM\...\{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_Display.GFExperience) (Version: 3.23.0.74 - NVIDIA Corporation)

NVIDIA Logiciel système PhysX 9.21.0713 (HKLM\...\{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_Display.PhysX) (Version: 9.21.0713 - NVIDIA Corporation)

NVIDIA Pilote audio HD : 1.3.38.92 (HKLM\...\{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_HDAudio.Driver) (Version: 1.3.38.92 - NVIDIA Corporation)

NVIDIA Pilote graphique 496.13 (HKLM\...\{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_Display.Driver) (Version: 496.13 - NVIDIA Corporation)

NVIDIA USBC Driver 1.46.831.832 (HKLM\...\{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}\_USBC) (Version: 1.46.831.832 - NVIDIA Corporation)

Office 16 Click-to-Run Extensibility Component (HKLM\...\{90160000-008C-0000-1000-0000000FF1CE}) (Version: 16.0.17231.20236 - Microsoft Corporation) Hidden

Office 16 Click-to-Run Licensing Component (HKLM\...\{90160000-007E-0000-1000-0000000FF1CE}) (Version: 16.0.17231.20236 - Microsoft Corporation) Hidden

Office 16 Click-to-Run Localization Component (HKLM\...\{90160000-008C-040C-1000-0000000FF1CE}) (Version: 16.0.17231.20236 - Microsoft Corporation) Hidden

OpenShot Video Editor 3.1.1 (HKLM\...\{4BB0DCDC-BC24-49EC-8937-72956C33A470}\_is1) (Version: 3.1.1 - OpenShot Studios, LLC)

PDF Settings CS6 (HKLM-x32\...\{BFEAAE77-BD7F-4534-B286-9C5CB4697EB1}) (Version: 11.0 - Adobe Systems Incorporated) Hidden

Screenpresso (HKU\S-1-5-21-2123058746-3684523357-4272769664-1001\...\Screenpresso) (Version: 2.1.22.0 - Learnpulse)

SiSoftware Sandra Lite 2021 (HKLM\...\{C3113E55-7BCB-4de3-8EBF-60E6CE6B2596}\_is1) (Version: 31.137.2021.12 - SiSoftware)

Studio-Scrap 8 (HKLM-x32\...\{EC8E8290-0DDD-4935-BD43-F51021D1BEA3}\_is1) (Version: 8.1.0.1 - CDIP)

Studio-Scrap 9 (HKLM-x32\...\{16F7C22C-8039-4C8B-872B-00DE56A9EF16}\_is1) (Version: 9.0.4.0 - CDIP)

TeamViewer (HKLM\...\TeamViewer) (Version: 15.49.3 - TeamViewer)

Chrome apps:

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

Google Password Manager (HKU\S-1-5-21-2123058746-3684523357-4272769664-1001\...\45cf5902ac22c16dc55d4e85fa43bec5) (Version: 1.0 - Google\Chrome)

Pinterest (HKU\S-1-5-21-2123058746-3684523357-4272769664-1001\...\75a973f257be0e99ddf32f24e3454461) (Version: 1.0 - Google\Chrome)

Packages:

=========

Microsoft.WindowsAppRuntime.CBS -> C:\Windows\SystemApps\Microsoft.WindowsAppRuntime.CBS\_8wekyb3d8bbwe [2024-02-22] (Microsoft Corporation)

==================== Custom CLSID (Whitelisted): ==============

(If an entry is included in the fixlist, it will be removed from the registry. The file will not be moved unless listed separately.)

ShellIconOverlayIdentifiers: [ OneDrive1] -> {BBACC218-34EA-4666-9D7A-C78F2274A524} => C:\Program Files\Microsoft OneDrive\24.020.0128.0003\FileSyncShell64.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

ShellIconOverlayIdentifiers: [ OneDrive2] -> {5AB7172C-9C11-405C-8DD5-AF20F3606282} => C:\Program Files\Microsoft OneDrive\24.020.0128.0003\FileSyncShell64.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

ShellIconOverlayIdentifiers: [ OneDrive3] -> {A78ED123-AB77-406B-9962-2A5D9D2F7F30} => C:\Program Files\Microsoft OneDrive\24.020.0128.0003\FileSyncShell64.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

ShellIconOverlayIdentifiers: [ OneDrive4] -> {F241C880-6982-4CE5-8CF7-7085BA96DA5A} => C:\Program Files\Microsoft OneDrive\24.020.0128.0003\FileSyncShell64.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

ShellIconOverlayIdentifiers: [ OneDrive5] -> {A0396A93-DC06-4AEF-BEE9-95FFCCAEF20E} => C:\Program Files\Microsoft OneDrive\24.020.0128.0003\FileSyncShell64.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

ShellIconOverlayIdentifiers: [ OneDrive6] -> {9AA2F32D-362A-42D9-9328-24A483E2CCC3} => C:\Program Files\Microsoft OneDrive\24.020.0128.0003\FileSyncShell64.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

ShellIconOverlayIdentifiers: [ OneDrive7] -> {C5FF006E-2AE9-408C-B85B-2DFDD5449D9C} => C:\Program Files\Microsoft OneDrive\24.020.0128.0003\FileSyncShell64.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

ShellIconOverlayIdentifiers-x32: [ OneDrive1] -> {BBACC218-34EA-4666-9D7A-C78F2274A524} => C:\Program Files\Microsoft OneDrive\24.020.0128.0003\FileSyncShell64.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

ShellIconOverlayIdentifiers-x32: [ OneDrive2] -> {5AB7172C-9C11-405C-8DD5-AF20F3606282} => C:\Program Files\Microsoft OneDrive\24.020.0128.0003\FileSyncShell64.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

ShellIconOverlayIdentifiers-x32: [ OneDrive3] -> {A78ED123-AB77-406B-9962-2A5D9D2F7F30} => C:\Program Files\Microsoft OneDrive\24.020.0128.0003\FileSyncShell64.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

ShellIconOverlayIdentifiers-x32: [ OneDrive4] -> {F241C880-6982-4CE5-8CF7-7085BA96DA5A} => C:\Program Files\Microsoft OneDrive\24.020.0128.0003\FileSyncShell64.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

ShellIconOverlayIdentifiers-x32: [ OneDrive5] -> {A0396A93-DC06-4AEF-BEE9-95FFCCAEF20E} => C:\Program Files\Microsoft OneDrive\24.020.0128.0003\FileSyncShell64.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

ShellIconOverlayIdentifiers-x32: [ OneDrive6] -> {9AA2F32D-362A-42D9-9328-24A483E2CCC3} => C:\Program Files\Microsoft OneDrive\24.020.0128.0003\FileSyncShell64.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

ShellIconOverlayIdentifiers-x32: [ OneDrive7] -> {C5FF006E-2AE9-408C-B85B-2DFDD5449D9C} => C:\Program Files\Microsoft OneDrive\24.020.0128.0003\FileSyncShell64.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

ContextMenuHandlers1: [ FileSyncEx] -> {CB3D0F55-BC2C-4C1A-85ED-23ED75B5106B} => C:\Program Files\Microsoft OneDrive\24.020.0128.0003\FileSyncShell64.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

ContextMenuHandlers3: [MBAMShlExt] -> {57CE581A-0CB6-4266-9CA0-19364C90A0B3} => C:\Program Files\Malwarebytes\Anti-Malware\mbshlext.dll [2023-11-30] (Malwarebytes Inc. -> Malwarebytes)

ContextMenuHandlers4: [ FileSyncEx] -> {CB3D0F55-BC2C-4C1A-85ED-23ED75B5106B} => C:\Program Files\Microsoft OneDrive\24.020.0128.0003\FileSyncShell64.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

ContextMenuHandlers5: [ FileSyncEx] -> {CB3D0F55-BC2C-4C1A-85ED-23ED75B5106B} => C:\Program Files\Microsoft OneDrive\24.020.0128.0003\FileSyncShell64.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

ContextMenuHandlers5: [NvCplDesktopContext] -> {3D1975AF-48C6-4f8e-A182-BE0E08FA86A9} => C:\Windows\System32\DriverStore\FileRepository\nv\_dispi.inf\_amd64\_5292bbfbf575e2d2\nvshext.dll [2021-10-07] (Nvidia Corporation -> NVIDIA Corporation)

ContextMenuHandlers6: [MBAMShlExt] -> {57CE581A-0CB6-4266-9CA0-19364C90A0B3} => C:\Program Files\Malwarebytes\Anti-Malware\mbshlext.dll [2023-11-30] (Malwarebytes Inc. -> Malwarebytes)

==================== Codecs (Whitelisted) ====================

(If an entry is included in the fixlist, the registry item will be restored to default or removed. The file will not be moved.)

HKLM\...\Drivers32: [vidc.spv1] => C:\Users\Mimi\AppData\Local\Learnpulse\Screenpresso\ScreenpressoCodec.dll [167656 2024-01-12] (Learnpulse -> LearnPulse)

HKLM\...\Drivers32: [vidc.spv1] => C:\Users\Mimi\AppData\Local\Learnpulse\Screenpresso\SysWOW64\ScreenpressoCodec.dll [146664 2024-01-12] (Learnpulse -> LearnPulse)

==================== Shortcuts & WMI ========================

(The entries could be listed to be restored or removed.)

ShortcutWithArgument: C:\Users\Mimi\AppData\Local\Google\Chrome\User Data\Default\Web Applications\\_crx\_pmncileebcgjlaigmolmknmnnfpfcckj\Pinterest.lnk -> C:\Program Files\Google\Chrome\Application\chrome\_proxy.exe (Google LLC) -> --profile-directory=Default --app-id=pmncileebcgjlaigmolmknmnnfpfcckj

ShortcutWithArgument: C:\Users\Mimi\AppData\Local\Google\Chrome\User Data\Default\Web Applications\\_crx\_kajebgjangihfbkjfejcanhanjmmbcfd\Google Password Manager.lnk -> C:\Program Files\Google\Chrome\Application\chrome\_proxy.exe (Google LLC) -> --profile-directory=Default --app-id=kajebgjangihfbkjfejcanhanjmmbcfd

ShortcutWithArgument: C:\Users\Mimi\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Applications Chrome\Google Password Manager.lnk -> C:\Program Files\Google\Chrome\Application\chrome\_proxy.exe (Google LLC) -> --profile-directory=Default --app-id=kajebgjangihfbkjfejcanhanjmmbcfd

ShortcutWithArgument: C:\Users\Mimi\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Applications Chrome\Pinterest.lnk -> C:\Program Files\Google\Chrome\Application\chrome\_proxy.exe (Google LLC) -> --profile-directory=Default --app-id=pmncileebcgjlaigmolmknmnnfpfcckj

ShortcutWithArgument: C:\Users\Mimi\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Google Password Manager.lnk -> C:\Program Files\Google\Chrome\Application\chrome\_proxy.exe (Google LLC) -> --profile-directory=Default --app-id=kajebgjangihfbkjfejcanhanjmmbcfd

==================== Loaded Modules (Whitelisted) =============

2023-11-29 18:50 - 2023-11-29 18:50 - 000065536 \_\_\_\_\_ (Microsoft Corporation) [File not signed] C:\Windows\WinSxS\Fusion\x86\_microsoft.vc80.openmp\_1fc8b3b9a1e18e3b\_none\_ffd3ce2ff7491d9e\8.0\8.0.50727.6195\vcomp.dll

==================== Alternate Data Streams (Whitelisted) ========

(If an entry is included in the fixlist, only the ADS will be removed.)

AlternateDataStreams: C:\Users\Mimi:com.affinity.designer.2 [151]

AlternateDataStreams: C:\Users\Mimi:com.affinity.designer.3 [197]

AlternateDataStreams: C:\Users\Mimi:com.affinity.publisher.2 [151]

AlternateDataStreams: C:\Users\Mimi:com.affinity.publisher.3 [197]

AlternateDataStreams: C:\Users\Mimi\Downloads\adwcleaner\_8.4.0.exe:MBAM.Zone.Identifier [156]

AlternateDataStreams: C:\Users\Mimi\Downloads\FoneTool\_free\_installer\_20231130.8354666.exe:MBAM.Zone.Identifier [166]

AlternateDataStreams: C:\Users\Mimi\Downloads\FoxitPDFReader20233\_L10N\_Setup\_Prom.exe:MBAM.Zone.Identifier [187]

AlternateDataStreams: C:\Users\Mimi\Downloads\inPixioPhotoStudio12Installer.exe:MBAM.Zone.Identifier [888]

AlternateDataStreams: C:\Users\Mimi\Downloads\msg-viewer-pro.exe:MBAM.Zone.Identifier [121]

AlternateDataStreams: C:\Users\Mimi\Downloads\MyRecover\_WinSetup.exe:MBAM.Zone.Identifier [146]

AlternateDataStreams: C:\Users\Mimi\Downloads\OfficeSetup.exe:MBAM.Zone.Identifier [194]

AlternateDataStreams: C:\Users\Mimi\Downloads\PStory\_3.msi:MBAM.Zone.Identifier [208]

AlternateDataStreams: C:\Users\Mimi\Downloads\Screenpresso.exe:MBAM.Zone.Identifier [158]

AlternateDataStreams: C:\Users\Mimi\Downloads\TeamViewer\_Setup\_x64.exe:MBAM.Zone.Identifier [280]

==================== Safe Mode (Whitelisted) ==================

(If an entry is included in the fixlist, it will be removed from the registry. The "AlternateShell" will be restored.)

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

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

==================== Association (Whitelisted) =================

==================== Internet Explorer (Whitelisted) ==========

BHO: Skype for Business Browser Helper -> {31D09BA0-12F5-4CCE-BE8A-2923E76605DA} -> C:\Program Files\Microsoft Office\root\Office16\OCHelper.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

BHO-x32: Skype for Business Browser Helper -> {31D09BA0-12F5-4CCE-BE8A-2923E76605DA} -> C:\Program Files\Microsoft Office\root\VFS\ProgramFilesX86\Microsoft Office\Office16\OCHelper.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

Handler: mso-minsb-roaming.16 - {83C25742-A9F7-49FB-9138-434302C88D07} - C:\Program Files\Microsoft Office\root\Office16\MSOSB.DLL [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

Handler-x32: mso-minsb-roaming.16 - {83C25742-A9F7-49FB-9138-434302C88D07} - C:\Program Files\Microsoft Office\root\VFS\ProgramFilesX86\Microsoft Office\Office16\MSOSB.DLL [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

Handler: mso-minsb.16 - {42089D2D-912D-4018-9087-2B87803E93FB} - C:\Program Files\Microsoft Office\root\Office16\MSOSB.DLL [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

Handler-x32: mso-minsb.16 - {42089D2D-912D-4018-9087-2B87803E93FB} - C:\Program Files\Microsoft Office\root\VFS\ProgramFilesX86\Microsoft Office\Office16\MSOSB.DLL [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

Handler: osf-roaming.16 - {42089D2D-912D-4018-9087-2B87803E93FB} - C:\Program Files\Microsoft Office\root\Office16\MSOSB.DLL [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

Handler-x32: osf-roaming.16 - {42089D2D-912D-4018-9087-2B87803E93FB} - C:\Program Files\Microsoft Office\root\VFS\ProgramFilesX86\Microsoft Office\Office16\MSOSB.DLL [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

Handler: osf.16 - {5504BE45-A83B-4808-900A-3A5C36E7F77A} - C:\Program Files\Microsoft Office\root\Office16\MSOSB.DLL [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

Handler-x32: osf.16 - {5504BE45-A83B-4808-900A-3A5C36E7F77A} - C:\Program Files\Microsoft Office\root\VFS\ProgramFilesX86\Microsoft Office\Office16\MSOSB.DLL [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

==================== Hosts content: =========================

(If needed Hosts: directive could be included in the fixlist to reset Hosts.)

2022-05-07 06:24 - 2022-05-07 06:22 - 000000824 \_\_\_\_\_ C:\Windows\system32\drivers\etc\hosts

2023-12-09 21:55 - 2024-02-20 18:02 - 000000445 \_\_\_\_\_ C:\Windows\system32\drivers\etc\hosts.ics

172.20.176.1 DESKTOP-8N74VA3.mshome.net # 2029 2 0 18 17 2 51 255

==================== Other Areas ===========================

(Currently there is no automatic fix for this section.)

HKU\S-1-5-21-2123058746-3684523357-4272769664-1001\Control Panel\Desktop\\Wallpaper ->

DNS Servers: 192.168.1.1

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System => (ConsentPromptBehaviorAdmin: 5) (ConsentPromptBehaviorUser: 3) (EnableLUA: 1)

Windows Firewall is enabled.

==================== MSCONFIG/TASK MANAGER disabled items ==

(If an entry is included in the fixlist, it will be removed.)

MSCONFIG\Services: DSAService => 2

MSCONFIG\Services: DSAUpdateService => 3

MSCONFIG\Services: ESRV\_SVC\_QUEENCREEK => 2

MSCONFIG\Services: FvSvc => 3

MSCONFIG\Services: GoogleChromeElevationService => 3

MSCONFIG\Services: gupdate => 2

MSCONFIG\Services: gupdatem => 3

MSCONFIG\Services: Intel(R) SUR QC SAM => 3

MSCONFIG\Services: NvContainerLocalSystem => 2

MSCONFIG\Services: NVDisplay.ContainerLocalSystem => 2

MSCONFIG\Services: SystemUsageReportSvc\_QUEENCREEK => 2

MSCONFIG\Services: USER\_ESRV\_SVC\_QUEENCREEK => 3

HKLM\...\StartupApproved\Run: => "AdobeAAMUpdater-1.0"

HKLM\...\StartupApproved\Run32: => "AdobeCS6ServiceManager"

HKLM\...\StartupApproved\Run32: => "SwitchBoard"

HKU\S-1-5-21-2123058746-3684523357-4272769664-1001\...\StartupApproved\StartupFolder: => "Notifications de Studio-Scrap.lnk"

HKU\S-1-5-21-2123058746-3684523357-4272769664-1001\...\StartupApproved\Run: => "MicrosoftEdgeAutoLaunch\_DFCE59279629A7E126EA0BB013656E3E"

HKU\S-1-5-21-2123058746-3684523357-4272769664-1001\...\StartupApproved\Run: => "Screenpresso"

==================== FirewallRules (Whitelisted) ================

(If an entry is included in the fixlist, it will be removed from the registry. The file will not be moved unless listed separately.)

FirewallRules: [{2516BDDA-E8AD-4C86-8B1D-E90284F9FB46}] => (Block) C:\Program Files\Intel\SUR\QUEENCREEK\x64\esrv\_svc.exe (Intel Corporation -> )

FirewallRules: [{A36814B9-339D-4199-90A7-B946D1A676F5}] => (Block) C:\Program Files\Intel\SUR\QUEENCREEK\x64\esrv\_svc.exe (Intel Corporation -> )

FirewallRules: [{E1A68D76-3E9E-47A5-851D-0A618177702E}] => (Allow) C:\Program Files\Intel\SUR\QUEENCREEK\x64\esrv\_svc.exe (Intel Corporation -> )

FirewallRules: [{57D68118-0BC4-4246-B12A-DB647F8BAD01}] => (Allow) C:\Program Files\Intel\SUR\QUEENCREEK\x64\esrv\_svc.exe (Intel Corporation -> )

FirewallRules: [{BA0FE811-3821-4791-87F2-957F3F59BEF9}] => (Allow) C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe (NVIDIA Corporation -> NVIDIA Corporation)

FirewallRules: [{7518960E-514D-4919-8D99-8755855EE441}] => (Allow) C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe (NVIDIA Corporation -> NVIDIA Corporation)

FirewallRules: [{86CE14F6-6C7B-47C3-8730-75FD4199B31A}] => (Allow) C:\Users\Mimi\Documents\Studio-Scrap 9\StudioScrap.exe => No File

FirewallRules: [{0F215B1B-50BE-4BCC-AEA9-5204E9864DA0}] => (Allow) C:\Users\Mimi\Documents\Studio-Scrap 9\StudioScrap.exe => No File

FirewallRules: [{22365E18-1023-413A-B398-84231DB69181}] => (Block) C:\Program Files (x86)\Adobe\Adobe Photoshop CS6\Photoshop.exe (Adobe Systems Incorporated -> Adobe Systems, Incorporated)

FirewallRules: [{6C037D84-D419-4712-9357-4468738A48C5}] => (Block) C:\Program Files (x86)\Adobe\Adobe Photoshop CS6\Photoshop.exe (Adobe Systems Incorporated -> Adobe Systems, Incorporated)

FirewallRules: [{5B8720CE-8A15-476A-9AC0-B4FF25B4A61A}] => (Block) C:\Program Files\Adobe\Adobe Photoshop CS6 (64 Bit)\Photoshop.exe (Adobe Systems Incorporated -> Adobe Systems, Incorporated)

FirewallRules: [{05107432-84FD-4AE6-8197-1EFE872046C2}] => (Allow) C:\Program Files (x86)\AOMEI\AOMEI Backupper\7.3.3\ABService.exe (AOMEI International Network Limited -> AOMEI International Network Limited)

FirewallRules: [{7463191B-6C85-4500-98A7-004D1CE31AE6}] => (Allow) C:\Program Files (x86)\AOMEI\AOMEI Backupper\7.3.3\ABService.exe (AOMEI International Network Limited -> AOMEI International Network Limited)

FirewallRules: [{77578C6A-3455-40FC-8F35-54CB2B2DE0BB}] => (Allow) C:\Program Files\Microsoft Office\root\Office16\outlook.exe (Microsoft Corporation -> Microsoft Corporation)

FirewallRules: [{A5B5BA9E-DCEE-4F6D-B05E-609C6B565D2C}] => (Allow) C:\Program Files\Microsoft Office\root\Office16\Lync.exe (Microsoft Corporation -> Microsoft Corporation)

FirewallRules: [{357FE9ED-B9DB-49B8-8A67-2C81FC2858E3}] => (Allow) C:\Program Files\Microsoft Office\root\Office16\Lync.exe (Microsoft Corporation -> Microsoft Corporation)

FirewallRules: [{FCC271FF-D583-48E8-8FBD-302C19304602}] => (Allow) C:\Program Files\Microsoft Office\root\Office16\UcMapi.exe (Microsoft Corporation -> Microsoft Corporation)

FirewallRules: [{FBF01D1B-A397-453B-BCFF-FC1C9DF3D756}] => (Allow) C:\Program Files\Microsoft Office\root\Office16\UcMapi.exe (Microsoft Corporation -> Microsoft Corporation)

FirewallRules: [{92D8315B-EEF4-463D-A0E4-668B04513C27}] => (Allow) C:\Program Files\SiSoftware\SiSoftware Sandra Lite 2021\RpcAgentSrv.exe (SiSoftware SPC -> SiSoftware) [File not signed]

FirewallRules: [{2D28ECB6-C203-49E3-9B2C-E7D299F0A2A7}] => (Allow) C:\Program Files\SiSoftware\SiSoftware Sandra Lite 2021\WNt600x64\RpcSandraSrv.exe (SiSoftware SPC -> SiSoftware) [File not signed]

FirewallRules: [{42A1080F-59C0-4B69-9AD6-4B34DDF3A992}] => (Allow) C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe (NVIDIA Corporation -> NVIDIA Corporation)

FirewallRules: [{8038C31E-C7A2-4D0A-A109-84B1541217E8}] => (Allow) C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe (NVIDIA Corporation -> NVIDIA Corporation)

FirewallRules: [{A183D044-A6AF-4640-9CA9-AC2ED4A7AC64}] => (Allow) C:\Program Files\NVIDIA Corporation\NvStreamSrv\nvstreamer.exe (NVIDIA Corporation -> NVIDIA Corporation)

FirewallRules: [{B093302C-00C0-4DC3-86A3-D40A7BE61865}] => (Allow) C:\Program Files\NVIDIA Corporation\NvStreamSrv\nvstreamer.exe (NVIDIA Corporation -> NVIDIA Corporation)

FirewallRules: [TCP Query User{A233D686-4DF5-4F17-9752-42B27014F953}C:\program files\openshot video editor\openshot-qt.exe] => (Allow) C:\program files\openshot video editor\openshot-qt.exe (OpenShot Studios, LLC) [File not signed]

FirewallRules: [UDP Query User{7155A97E-FCF0-4B84-BDE0-ACA2B5474D7C}C:\program files\openshot video editor\openshot-qt.exe] => (Allow) C:\program files\openshot video editor\openshot-qt.exe (OpenShot Studios, LLC) [File not signed]

FirewallRules: [{67AB59EF-A562-4EA7-8204-26FB873CACD8}] => (Allow) C:\Program Files\OpenShot Video Editor\openshot-qt.exe (OpenShot Studios, LLC) [File not signed]

FirewallRules: [TCP Query User{F6BAD4B0-3D07-4E8F-8AC7-DCD866CA4BD1}C:\program files (x86)\studio-scrap 8\studioscrap.exe] => (Block) C:\program files (x86)\studio-scrap 8\studioscrap.exe (CENTRE DE DEVELOPPEMENT DE L'INFORMATIQUE PERSONNELLE -> CDIP)

FirewallRules: [UDP Query User{0671E694-5F40-4FD8-B3B8-61CFE815209F}C:\program files (x86)\studio-scrap 8\studioscrap.exe] => (Block) C:\program files (x86)\studio-scrap 8\studioscrap.exe (CENTRE DE DEVELOPPEMENT DE L'INFORMATIQUE PERSONNELLE -> CDIP)

FirewallRules: [{2A3075A7-177C-41B5-9912-80BABC6F3ECB}] => (Allow) C:\Program Files\WindowsApps\MicrosoftCorporationII.WindowsSubsystemForAndroid\_2311.40000.5.0\_x64\_\_8wekyb3d8bbwe\WsaClient\WsaClient.exe (Microsoft Corporation -> )

FirewallRules: [{8F586559-9FAD-4558-B1D5-16104B8C8437}] => (Allow) C:\Program Files\TeamViewer\TeamViewer.exe (TeamViewer Germany GmbH -> TeamViewer Germany GmbH)

FirewallRules: [{D29D7361-41D9-4849-AA71-EE5E1865A4F9}] => (Allow) C:\Program Files\TeamViewer\TeamViewer.exe (TeamViewer Germany GmbH -> TeamViewer Germany GmbH)

FirewallRules: [{C8E54BC5-9B9D-4925-99D8-BA5C4B4E2071}] => (Allow) C:\Program Files\TeamViewer\TeamViewer\_Service.exe (TeamViewer Germany GmbH -> TeamViewer Germany GmbH)

FirewallRules: [{9F66DFFB-C9DC-4E25-AFC0-A2995D9684D4}] => (Allow) C:\Program Files\TeamViewer\TeamViewer\_Service.exe (TeamViewer Germany GmbH -> TeamViewer Germany GmbH)

FirewallRules: [{AF94C4D2-6BF9-4716-9E40-D62F40B5A291}] => (Allow) C:\Program Files (x86)\Microsoft\EdgeWebView\Application\121.0.2277.128\msedgewebview2.exe (Microsoft Corporation -> Microsoft Corporation)

FirewallRules: [{B63232F5-454F-4D45-8A3F-4D3D29EB8CB2}] => (Allow) C:\Program Files\WindowsApps\MicrosoftTeams\_24004.1403.2634.2418\_x64\_\_8wekyb3d8bbwe\msteams.exe (Microsoft Corporation -> Microsoft Corporation)

FirewallRules: [{C80226EB-69EE-40E7-9F90-4228F958E2C8}] => (Allow) C:\Program Files\WindowsApps\MicrosoftTeams\_24004.1403.2634.2418\_x64\_\_8wekyb3d8bbwe\msteams.exe (Microsoft Corporation -> Microsoft Corporation)

FirewallRules: [{9097A192-B75E-438D-B5E4-FA2D9570D1B6}] => (Allow) C:\Program Files\Google\Chrome\Application\chrome.exe (Google LLC -> Google LLC)

==================== Restore Points =========================

19-02-2024 19:02:32 Point de contrôle planifié

21-02-2024 16:43:07 Opération de restauration

==================== Faulty Device Manager Devices ============

==================== Event log errors: ========================

Application errors:

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

Error: (02/21/2024 10:56:46 PM) (Source: SideBySide) (EventID: 33) (User: )

Description: La création du contexte d’activation a échoué pour « C:\Program Files\Google\Chrome\Temp\scoped\_dir1216\_264084159\old\_chrome.exe ».

Assembly dépendant 121.0.6167.185,language="&#x2a;",type="win32",version="121.0.6167.185" introuvable.

Utilisez sxstrace.exe pour un diagnostic détaillé.

Error: (02/21/2024 06:01:51 PM) (Source: Application Error) (EventID: 1000) (User: DESKTOP-8N74VA3)

Description: Nom de l’application défaillante mmc.exe, version : 10.0.22621.2506, horodatage : 0x307870ca

Nom du module défaillant : KERNELBASE.dll, version : 10.0.22621.3155, horodatage : 0x8c2ee5db

Code d’exception : 0xc000041d

Décalage d’erreur : 0x0000000000065b0c

ID du processus défaillant : 0x0x29c4

Heure de début de l’application défaillante : 0x0x1da64e79b399d3c

Chemin d’accès de l’application défaillante : C:\Windows\system32\mmc.exe

Chemin d’accès du module défaillant: C:\Windows\System32\KERNELBASE.dll

ID de rapport : e168a9c1-8356-4cac-850d-4ab6576d76a6

Nom complet du package défaillant :

ID de l’application relative au package défaillant :

Error: (02/21/2024 06:01:47 PM) (Source: Application Error) (EventID: 1000) (User: DESKTOP-8N74VA3)

Description: Nom de l’application défaillante mmc.exe, version : 10.0.22621.2506, horodatage : 0x307870ca

Nom du module défaillant : KERNELBASE.dll, version : 10.0.22621.3155, horodatage : 0x8c2ee5db

Code d’exception : 0xe0434352

Décalage d’erreur : 0x0000000000065b0c

ID du processus défaillant : 0x0x29c4

Heure de début de l’application défaillante : 0x0x1da64e79b399d3c

Chemin d’accès de l’application défaillante : C:\Windows\system32\mmc.exe

Chemin d’accès du module défaillant: C:\Windows\System32\KERNELBASE.dll

ID de rapport : 07553d67-6e35-4f35-bf3b-f180325dc117

Nom complet du package défaillant :

ID de l’application relative au package défaillant :

Error: (02/21/2024 06:01:46 PM) (Source: .NET Runtime) (EventID: 1026) (User: )

Description: Application : mmc.exe

Version du Framework : v4.0.30319

Description : le processus a été arrêté en raison d'une exception non gérée.

Informations sur l'exception : System.OutOfMemoryException

à System.Drawing.Graphics.FromHwndInternal(IntPtr)

à System.Windows.Forms.SplitContainer.RepaintSplitterRect()

à System.Windows.Forms.SplitContainer.ResizeSplitContainer()

à System.Windows.Forms.SplitContainer.OnLayout(System.Windows.Forms.LayoutEventArgs)

à System.Windows.Forms.Control.PerformLayout(System.Windows.Forms.LayoutEventArgs)

à System.Windows.Forms.Control.OnResize(System.EventArgs)

à System.Windows.Forms.Control.OnSizeChanged(System.EventArgs)

à System.Windows.Forms.Control.UpdateBounds(Int32, Int32, Int32, Int32, Int32, Int32)

à System.Windows.Forms.Control.UpdateBounds()

à System.Windows.Forms.Control.WmWindowPosChanged(System.Windows.Forms.Message ByRef)

à System.Windows.Forms.Control.WndProc(System.Windows.Forms.Message ByRef)

à System.Windows.Forms.SplitContainer.WndProc(System.Windows.Forms.Message ByRef)

à System.Windows.Forms.NativeWindow.Callback(IntPtr, Int32, IntPtr, IntPtr)

Informations sur l'exception : System.Reflection.TargetInvocationException

à Microsoft.ManagementConsole.Internal.SnapInMessagePumpProxy.OnThreadException(System.Object, System.Threading.ThreadExceptionEventArgs)

à System.Windows.Forms.Application+ThreadContext.OnThreadException(System.Exception)

à System.Windows.Forms.Control.WndProcException(System.Exception)

à System.Windows.Forms.NativeWindow.Callback(IntPtr, Int32, IntPtr, IntPtr)

Error: (02/21/2024 05:37:35 PM) (Source: Application Error) (EventID: 1000) (User: DESKTOP-8N74VA3)

Description: Nom de l’application défaillante Explorer.EXE, version : 10.0.22621.3155, horodatage : 0x3fb2d7a4

Nom du module défaillant : ucrtbase.dll, version : 10.0.22621.2506, horodatage : 0x097c794c

Code d’exception : 0xc0000409

Décalage d’erreur : 0x000000000007f61e

ID du processus défaillant : 0x0x1390

Heure de début de l’application défaillante : 0x0x1da64e44288ed50

Chemin d’accès de l’application défaillante : C:\Windows\Explorer.EXE

Chemin d’accès du module défaillant: C:\Windows\System32\ucrtbase.dll

ID de rapport : 833add02-069f-4c20-a022-52dfab4a2207

Nom complet du package défaillant :

ID de l’application relative au package défaillant :

Error: (02/21/2024 05:36:11 PM) (Source: ESENT) (EventID: 455) (User: )

Description: svchost (4724,R,98) SRUJet: L’erreur -1811 (0xfffff8ed) s’est produite lors de l’ouverture d’un fichier journal C:\Windows\system32\SRU\SRU01532.log.

Error: (02/21/2024 05:11:54 PM) (Source: COM) (EventID: 10031) (User: )

Description: Une vérification de stratégie d’unmarshaling a été effectuée lors de l’unmarshaling d’un objet marshalé personnalisé et la classe {BE88F957-42CC-4DA7-92CF-9BC35C5D5EE2} a été refusée

Error: (02/21/2024 05:11:54 PM) (Source: COM) (EventID: 10031) (User: )

Description: Une vérification de stratégie d’unmarshaling a été effectuée lors de l’unmarshaling d’un objet marshalé personnalisé et la classe {BE88F957-42CC-4DA7-92CF-9BC35C5D5EE2} a été refusée

System errors:

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

Error: (02/22/2024 06:15:35 PM) (Source: DCOM) (EventID: 10001) (User: DESKTOP-8N74VA3)

Description: Impossible de démarrer un serveur DCOM : MicrosoftWindows.Client.WebExperience\_424.1301.140.0\_x64\_\_cw5n1h2txyewy!WindowsUdk.UI.Shell.Dashboard.DashboardExtension en tant que Non disponible/Non disponible. L’erreur

« 2147942402 »

s’est produite lors du démarrage de la commande :

"C:\Program Files\WindowsApps\MicrosoftWindows.Client.WebExperience\_424.1301.140.0\_x64\_\_cw5n1h2txyewy\Dashboard\Widgets.exe" -ServerName:Microsoft.Windows.DashboardServer

Error: (02/22/2024 06:15:35 PM) (Source: DCOM) (EventID: 10001) (User: DESKTOP-8N74VA3)

Description: Impossible de démarrer un serveur DCOM : MicrosoftWindows.Client.WebExperience\_424.1301.140.0\_x64\_\_cw5n1h2txyewy!WindowsUdk.UI.Shell.Dashboard.DashboardExtension en tant que Non disponible/Non disponible. L’erreur

« 2147942402 »

s’est produite lors du démarrage de la commande :

"C:\Program Files\WindowsApps\MicrosoftWindows.Client.WebExperience\_424.1301.140.0\_x64\_\_cw5n1h2txyewy\Dashboard\Widgets.exe" -ServerName:Microsoft.Windows.DashboardServer

Error: (02/22/2024 05:55:16 PM) (Source: DCOM) (EventID: 10001) (User: DESKTOP-8N74VA3)

Description: Impossible de démarrer un serveur DCOM : MicrosoftWindows.Client.WebExperience\_424.1301.140.0\_x64\_\_cw5n1h2txyewy!WindowsUdk.UI.Shell.Dashboard.DashboardExtension en tant que Non disponible/Non disponible. L’erreur

« 2147942402 »

s’est produite lors du démarrage de la commande :

"C:\Program Files\WindowsApps\MicrosoftWindows.Client.WebExperience\_424.1301.140.0\_x64\_\_cw5n1h2txyewy\Dashboard\Widgets.exe" -ServerName:Microsoft.Windows.DashboardServer

Error: (02/22/2024 05:55:16 PM) (Source: DCOM) (EventID: 10001) (User: DESKTOP-8N74VA3)

Description: Impossible de démarrer un serveur DCOM : MicrosoftWindows.Client.WebExperience\_424.1301.140.0\_x64\_\_cw5n1h2txyewy!WindowsUdk.UI.Shell.Dashboard.DashboardExtension en tant que Non disponible/Non disponible. L’erreur

« 2147942402 »

s’est produite lors du démarrage de la commande :

"C:\Program Files\WindowsApps\MicrosoftWindows.Client.WebExperience\_424.1301.140.0\_x64\_\_cw5n1h2txyewy\Dashboard\Widgets.exe" -ServerName:Microsoft.Windows.DashboardServer

Error: (02/22/2024 05:54:04 PM) (Source: DCOM) (EventID: 10001) (User: DESKTOP-8N74VA3)

Description: Impossible de démarrer un serveur DCOM : MicrosoftWindows.Client.WebExperience\_424.1301.140.0\_x64\_\_cw5n1h2txyewy!WindowsUdk.UI.Shell.Dashboard.DashboardExtension en tant que Non disponible/Non disponible. L’erreur

« 2147942402 »

s’est produite lors du démarrage de la commande :

"C:\Program Files\WindowsApps\MicrosoftWindows.Client.WebExperience\_424.1301.140.0\_x64\_\_cw5n1h2txyewy\Dashboard\Widgets.exe" -ServerName:Microsoft.Windows.DashboardServer

Error: (02/22/2024 05:54:04 PM) (Source: DCOM) (EventID: 10001) (User: DESKTOP-8N74VA3)

Description: Impossible de démarrer un serveur DCOM : MicrosoftWindows.Client.WebExperience\_424.1301.140.0\_x64\_\_cw5n1h2txyewy!WindowsUdk.UI.Shell.Dashboard.DashboardExtension en tant que Non disponible/Non disponible. L’erreur

« 2147942402 »

s’est produite lors du démarrage de la commande :

"C:\Program Files\WindowsApps\MicrosoftWindows.Client.WebExperience\_424.1301.140.0\_x64\_\_cw5n1h2txyewy\Dashboard\Widgets.exe" -ServerName:Microsoft.Windows.DashboardServer

Error: (02/22/2024 05:53:42 PM) (Source: DCOM) (EventID: 10001) (User: DESKTOP-8N74VA3)

Description: Impossible de démarrer un serveur DCOM : MicrosoftWindows.Client.WebExperience\_424.1301.140.0\_x64\_\_cw5n1h2txyewy!WindowsUdk.UI.Shell.Dashboard.DashboardExtension en tant que Non disponible/Non disponible. L’erreur

« 2147942402 »

s’est produite lors du démarrage de la commande :

"C:\Program Files\WindowsApps\MicrosoftWindows.Client.WebExperience\_424.1301.140.0\_x64\_\_cw5n1h2txyewy\Dashboard\Widgets.exe" -ServerName:Microsoft.Windows.DashboardServer

Error: (02/22/2024 05:53:42 PM) (Source: DCOM) (EventID: 10001) (User: DESKTOP-8N74VA3)

Description: Impossible de démarrer un serveur DCOM : MicrosoftWindows.Client.WebExperience\_424.1301.140.0\_x64\_\_cw5n1h2txyewy!WindowsUdk.UI.Shell.Dashboard.DashboardExtension en tant que Non disponible/Non disponible. L’erreur

« 2147942402 »

s’est produite lors du démarrage de la commande :

"C:\Program Files\WindowsApps\MicrosoftWindows.Client.WebExperience\_424.1301.140.0\_x64\_\_cw5n1h2txyewy\Dashboard\Widgets.exe" -ServerName:Microsoft.Windows.DashboardServer

Windows Defender:

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

Date: 2024-02-20 17:23:50

Description:

L’analyse Antivirus Microsoft Defender a été arrêtée avant la fin.

ID de l’analyse : {65F33E55-8689-4418-9421-B576588CFCF8}

Type de l’analyse : Logiciel anti-programme malveillant

Paramètres de l’analyse : Analyse rapide

Utilisateur : AUTORITE NT\Système

Date: 2024-01-01 11:52:24

Description:

Antivirus Microsoft Defender a détecté un logiciel malveillant ou potentiellement indésirable.

Pour plus d’informations, reportez-vous aux éléments suivants :

https://go.microsoft.com/fwlink/?linkid=37020&name=PUADlManager:Win32/InstallCore&threatid=311991&enterprise=0

Nom : PUADlManager:Win32/InstallCore

ID : 311991

Gravité : Faible

Catégorie : Logiciel potentiellement non désiré

Chemin : file:\_C:\Users\Mimi\Downloads\clipgrab-3.9.7-dotinstaller.exe

Origine de la détection : Ordinateur local

Type de détection : Concret

Source de détection : Protection en temps réel

Utilisateur : DESKTOP-8N74VA3\Mimi

Nom du processus : C:\Windows\explorer.exe

Version de la veille de sécurité : AV: 1.403.1467.0, AS: 1.403.1467.0, NIS: 1.403.1467.0

Version du moteur : AM: 1.1.23110.2, NIS: 1.1.23110.2

Date: 2023-11-29 16:17:42

Description:

L’analyse Antivirus Microsoft Defender a été arrêtée avant la fin.

ID de l’analyse : {67B82441-9135-461C-9E1A-50625005E4E6}

Type de l’analyse : Logiciel anti-programme malveillant

Paramètres de l’analyse : Analyse rapide

Utilisateur : AUTORITE NT\Système

Date: 2023-11-28 16:03:50

Description:

L’analyse Antivirus Microsoft Defender a été arrêtée avant la fin.

ID de l’analyse : {47EFD8E6-A9A8-42CA-9F30-CF65EE9572CD}

Type de l’analyse : Logiciel anti-programme malveillant

Paramètres de l’analyse : Analyse rapide

Utilisateur : AUTORITE NT\Système

Date: 2023-11-27 17:47:28

Description:

L’analyse Antivirus Microsoft Defender a été arrêtée avant la fin.

ID de l’analyse : {2542F9F6-C007-4DC3-992D-8EFF01CE8DF9}

Type de l’analyse : Logiciel anti-programme malveillant

Paramètres de l’analyse : Analyse rapide

Utilisateur : AUTORITE NT\Système

﻿Event[0]

Date: 2024-02-20 16:13:46

Description:

Antivirus Microsoft Defender a rencontré une erreur lors de la mise à jour de la veille de sécurité.

Nouvelle version de la veille de sécurité :

Version précédente de la veille de sécurité : 1.403.1928.0

Source de mise à jour : Serveur Microsoft Update

Type de veille de sécurité : Anti-virus

Type de mise à jour : Complet

Utilisateur : AUTORITE NT\Système

Version actuelle du moteur :

Version précédente du moteur : 1.1.23110.2

Code d’erreur : 0x8024001e

Description de l’erreur : Un problème inattendu s’est produit lors de la vérification des mises à jour. Pour plus d’informations sur l’installation ou la résolution des problèmes de mise à jour, voir Aide et support.

CodeIntegrity:

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

Date: 2024-02-22 18:51:24

Description:

Code Integrity determined that a process (\Device\HarddiskVolume3\Program Files\Google\Chrome\Application\chrome.exe) attempted to load \Device\HarddiskVolume3\Program Files\Malwarebytes\Anti-Malware\mbae64.dll that did not meet the Microsoft signing level requirements.

==================== Memory info ===========================

BIOS: American Megatrends Inc. V1.11 02/16/2016

Motherboard: MSI H97 GAMING 3 (MS-7918)

Processor: Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz

Percentage of memory in use: 28%

Total physical RAM: 16315.1 MB

Available physical RAM: 11625.12 MB

Total Virtual: 17339.1 MB

Available Virtual: 11334.45 MB

==================== Drives ================================

Drive a: (AOMEI (Save)PC Steph) (Fixed) (Total:1863.01 GB) (Free:1511.75 GB) (Model: TOSHIBA External USB 3.0 USB Device) NTFS

Drive c: () (Fixed) (Total:465.02 GB) (Free:340.42 GB) (Model: Samsung SSD 980 PRO 500GB) NTFS

Drive d: (Divers) (Fixed) (Total:512.1 GB) (Free:496.51 GB) (Model: ST2000DM008-2UB102) NTFS

Drive g: (Graphisme-Photos) (Fixed) (Total:546.74 GB) (Free:80.14 GB) (Model: ST2000DM008-2UB102) NTFS

Drive s: (Sauvegarde) (Fixed) (Total:804.16 GB) (Free:774.12 GB) (Model: ST2000DM008-2UB102) NTFS

\\?\Volume{a48aab32-a515-4441-8924-ebbae704440e}\ () (Fixed) (Total:0.62 GB) (Free:0.08 GB) NTFS

\\?\Volume{27cab195-54ce-40ab-b076-0322a048acf6}\ () (Fixed) (Total:0.09 GB) (Free:0.07 GB) FAT32

==================== MBR & Partition Table ====================

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

Disk: 0 (Size: 1863 GB) (Disk ID: 50E6CAE9)

Partition: GPT.

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

Disk: 1 (Size: 465.8 GB) (Disk ID: 00F84D5C)

Partition: GPT.

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

Disk: 2 (Size: 1863 GB) (Disk ID: AA4F0B53)

Partition 1: (Not Active) - (Size=1863 GB) - (Type=07 NTFS)

==================== End of Addition.txt =======================