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

Ran by Mimi (administrator) on DESKTOP-8N74VA3 (MSI MS-7918) (22-02-2024 18:52:41)

Running from C:\Users\Mimi\Downloads\FRSTEnglish.exe

Loaded Profiles: Mimi

Platform: Microsoft Windows 11 Professionnel Version 22H2 22621.3155 (X64) Language: Français (France)

Default browser: Chrome

Boot Mode: Normal

==================== Processes (Whitelisted) =================

(If an entry is included in the fixlist, the process will be closed. The file will not be moved.)

(C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe ->) (Microsoft Windows -> Microsoft Corporation) C:\Windows\System32\cmd.exe

(C:\Program Files\Malwarebytes\Anti-Malware\MBAMService.exe ->) (Malwarebytes Inc. -> Malwarebytes) C:\Program Files\Malwarebytes\Anti-Malware\mbamtray.exe

(cmd.exe ->) (Malwarebytes Inc. -> Malwarebytes) C:\Program Files\Malwarebytes\Anti-Malware\MbamBgNativeMsg.exe

(Microsoft Corporation -> Microsoft Corporation) C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe <13>

(NVIDIA Corporation -> Node.js) C:\Program Files (x86)\NVIDIA Corporation\NvNode\NVIDIA Web Helper.exe

(services.exe ->) (AOMEI International Network Limited -> AOMEI International Network Limited) C:\Program Files (x86)\AOMEI\AOMEI Backupper\7.3.3\ABService.exe

(services.exe ->) (CyberLink Corp. -> CyberLink) C:\Program Files\CyberLink\Shared files\RichVideo64.exe

(services.exe ->) (FOXIT SOFTWARE INC. -> Foxit Software Inc.) C:\Program Files (x86)\Common Files\Foxit\Foxit PDF Reader\FoxitPDFReaderUpdateService.exe

(services.exe ->) (Malwarebytes Inc. -> Malwarebytes) C:\Program Files\Malwarebytes\Anti-Malware\MBAMService.exe

(services.exe ->) (Microsoft Corporation -> Microsoft Corporation) C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeClickToRun.exe

(services.exe ->) (NVIDIA Corporation -> NVIDIA Corporation) C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe <2>

(services.exe ->) (Nvidia Corporation -> NVIDIA Corporation) C:\Windows\System32\DriverStore\FileRepository\nv\_dispi.inf\_amd64\_5292bbfbf575e2d2\Display.NvContainer\NVDisplay.Container.exe <2>

(services.exe ->) (TeamViewer Germany GmbH -> TeamViewer Germany GmbH) C:\Program Files\TeamViewer\TeamViewer\_Service.exe

(svchost.exe ->) (CyberLink Corp. -> CyberLink Corp.) C:\Program Files (x86)\CyberLink\Shared files\PDStyleAgent\PDStyleAgent.exe

(svchost.exe ->) (Intel Corporation -> Intel Corporation) C:\Program Files\Intel\SUR\QUEENCREEK\Updater\bin\IntelSoftwareAssetManagerService.exe

(svchost.exe ->) (Microsoft Corporation -> Microsoft Corporation) C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps\_16005.14326.21786.0\_x64\_\_8wekyb3d8bbwe\HxOutlook.exe

(svchost.exe ->) (Microsoft Corporation -> Microsoft Corporation) C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps\_16005.14326.21786.0\_x64\_\_8wekyb3d8bbwe\HxTsr.exe

(svchost.exe ->) (Microsoft Windows -> Microsoft Corporation) C:\Windows\System32\dllhost.exe

(svchost.exe ->) (Microsoft Windows -> Microsoft Corporation) C:\Windows\System32\smartscreen.exe

(svchost.exe ->) (Microsoft Windows -> Microsoft Corporation) C:\Windows\System32\wlanext.exe

(svchost.exe ->) (Microsoft Windows -> Microsoft Corporation) C:\Windows\UUS\Packages\Preview\amd64\MoUsoCoreWorker.exe

==================== Registry (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\...\Run: [AdobeAAMUpdater-1.0] => C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\UWA\UpdaterStartupUtility.exe [446392 2012-04-04] (Adobe Systems Incorporated -> Adobe Systems Incorporated)

HKLM-x32\...\Run: [SwitchBoard] => C:\Program Files (x86)\Common Files\Adobe\SwitchBoard\SwitchBoard.exe [517096 2010-02-19] (Test Signing Certificate -> Adobe Systems Incorporated) [File not signed]

HKLM-x32\...\Run: [AdobeCS6ServiceManager] => C:\Program Files (x86)\Common Files\Adobe\CS6ServiceManager\CS6ServiceManager.exe [1073312 2012-03-09] (Adobe Systems Incorporated -> Adobe Systems Incorporated)

HKLM\SOFTWARE\Microsoft\Windows Defender: [DisableAntiSpyware] Restriction <==== ATTENTION

HKLM\SOFTWARE\Microsoft\Windows Defender: [DisableAntiVirus] Restriction <==== ATTENTION

HKU\S-1-5-21-2123058746-3684523357-4272769664-1001\...\Run: [MicrosoftEdgeAutoLaunch\_DFCE59279629A7E126EA0BB013656E3E] => "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --win-session-start [3788240 2024-02-15] (Microsoft Corporation -> Microsoft Corporation)

HKU\S-1-5-21-2123058746-3684523357-4272769664-1001\...\Run: [AdobeBridge] => [X]

HKU\S-1-5-21-2123058746-3684523357-4272769664-1001\...\Run: [Screenpresso] => C:\Users\Mimi\AppData\Local\Learnpulse\Screenpresso\Screenpresso.exe [20340744 2024-01-12] (Learnpulse -> Learnpulse)

HKU\S-1-5-21-2123058746-3684523357-4272769664-1001\...\MountPoints2: {8dba68a6-9341-11ee-8afc-7413ea7d8a0b} - "E:\setup.EXE" /AUTORUN

HKU\S-1-5-21-2123058746-3684523357-4272769664-1001\...\MountPoints2: {ebbeb92d-98d5-11ee-8b03-7413ea7d8a07} - "E:\HiSuiteDownLoader.exe"

HKLM\Software\Microsoft\Active Setup\Installed Components: [{8A69D345-D564-463c-AFF1-A69D9E530F96}] -> C:\Program Files\Google\Chrome\Application\122.0.6261.58\Installer\chrmstp.exe [2024-02-21] (Google LLC -> Google LLC)

Startup: C:\Users\Mimi\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Notifications de Studio-Scrap.lnk [2023-12-06]

ShortcutTarget: Notifications de Studio-Scrap.lnk -> C:\Program Files (x86)\Notifications de Studio-Scrap\Notifications de Studio-Scrap.exe (CENTRE DE DEVELOPPEMENT DE L'INFORMATIQUE PERSONNELLE SAS -> CDIP)

GroupPolicy\User: Restriction ? <==== ATTENTION

HKLM\SOFTWARE\Policies\Google: Restriction <==== ATTENTION

HKLM\SOFTWARE\Policies\Microsoft\Edge: Restriction <==== ATTENTION

==================== Scheduled Tasks (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.)

Task: {877BA7AA-787E-4946-827C-61ECC8772393} - System32\Tasks\AdobeAAMUpdater-1.0-MicrosoftAccount-mirvol13@outlook.com => C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\UWA\UpdaterStartupUtility.exe [446392 2012-04-04] (Adobe Systems Incorporated -> Adobe Systems Incorporated)

Task: {FFDFB56C-98F1-4520-92DE-7933C985760C} - System32\Tasks\AOMEI Mes sauvegardes 2023-12-13, 13-21-27 => C:\Program Files (x86)\AOMEI\AOMEI Backupper\ABLaucher.exe [497096 2022-08-31] (AOMEI International Network Limited -> AOMEI International Network Limited)

Task: {E3270256-6F0C-4FE2-B2C6-A7B86F55FB45} - System32\Tasks\AOMEI Sauvegarde Système(1) 2023-12-13, 13-23-00 => C:\Program Files (x86)\AOMEI\AOMEI Backupper\ABLaucher.exe [497096 2022-08-31] (AOMEI International Network Limited -> AOMEI International Network Limited)

Task: {EB452BC9-1909-44DD-918F-EA5A9536AA0D} - System32\Tasks\CLToast => C:\Program Files (x86)\CyberLink\Shared files\CLToast.exe [2317064 2023-12-05] (CyberLink Corp. -> )

Task: {796899FB-D03A-4516-9068-2B67C221B65A} - System32\Tasks\CLToastRun => C:\Program Files (x86)\CyberLink\Shared files\CLToast.exe [2317064 2023-12-05] (CyberLink Corp. -> )

Task: {5E9BE8B5-37C4-46B5-A5F9-968396B5950B} - System32\Tasks\GoogleSystem\GoogleUpdater\GoogleUpdaterTaskSystem123.0.6288.0{20DF9D2D-9305-4AA4-922D-F5BB0FB35DCB} => C:\Program Files (x86)\Google\GoogleUpdater\123.0.6288.0\updater.exe [4682528 2024-02-08] (Google LLC -> Google LLC) <==== ATTENTION

Task: {59820188-08BD-401C-A055-A2311EED9110} - System32\Tasks\IntelSURQC-Upgrade-86621605-2a0b-4128-8ffc-15514c247132 => C:\Program Files\Intel\SUR\QUEENCREEK\Updater\bin\IntelSoftwareAssetManagerService.exe [3075936 2021-07-21] (Intel Corporation -> Intel Corporation)

Task: {BD85F540-59BE-48F6-AC2D-7736D631BB0E} - System32\Tasks\IntelSURQC-Upgrade-86621605-2a0b-4128-8ffc-15514c247132-Logon => C:\Program Files\Intel\SUR\QUEENCREEK\Updater\bin\IntelSoftwareAssetManagerService.exe [3075936 2021-07-21] (Intel Corporation -> Intel Corporation)

Task: {C7E6AC1E-235C-4BA6-9D1B-2CB52C792A6D} - System32\Tasks\IUM-F1E24CA0-B63E-4F13-A9E3-4ADE3BFF3473 => C:\Program Files (x86)\Intel\Intel(R) Update Manager\bin\iumsvc.exe --automatic (No File)

Task: {005498E6-88AA-4B45-A0F3-17C171BEF405} - System32\Tasks\Microsoft\Office\Office Automatic Updates 2.0 => C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe [28372672 2024-02-10] (Microsoft Corporation -> Microsoft Corporation)

Task: {557EA8C9-66D5-47BF-A309-2945B5B9580C} - System32\Tasks\Microsoft\Office\Office ClickToRun Service Monitor => C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe [28372672 2024-02-10] (Microsoft Corporation -> Microsoft Corporation)

Task: {7EEFB15C-5C1B-43A6-8F25-C22AEDCB2672} - System32\Tasks\Microsoft\Office\Office Feature Updates => C:\Program Files\Microsoft Office\root\Office16\sdxhelper.exe [306328 2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

Task: {11067612-48A7-4B64-BE08-A8F3961A375E} - System32\Tasks\Microsoft\Office\Office Feature Updates Logon => C:\Program Files\Microsoft Office\root\Office16\sdxhelper.exe [306328 2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

Task: {FE0C8715-0813-4725-B582-274240DD6ED1} - System32\Tasks\Microsoft\Office\Office Performance Monitor => C:\Program Files\Microsoft Office\root\VFS\ProgramFilesCommonX64\Microsoft Shared\Office16\operfmon.exe [170128 2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

Task: {E0F10DCF-44AD-40E8-9370-FB5DA59F93FB} - System32\Tasks\Microsoft\Windows\UpdateOrchestrator\USO\_UxBroker => %systemroot%\system32\MusNotification.exe (No File)

Task: {6CA524EB-DB5C-4034-BB39-ABC8FABCDFDC} - System32\Tasks\NvBatteryBoostCheckOnLogon\_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} => C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe [903024 2021-10-07] (NVIDIA Corporation -> NVIDIA Corporation) -> -d "C:\Program Files\NVIDIA Corporation\NvBackend\NvBatteryBoostCheck" -l 3 -f C:\ProgramData\NVIDIA\NvContainerBatteryBoostCheck.log

Task: {124615C9-B3D6-450E-B077-9ACD953ACF93} - System32\Tasks\NvDriverUpdateCheckDaily\_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} => C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe [903024 2021-10-07] (NVIDIA Corporation -> NVIDIA Corporation) -> -d "C:\Program Files\NVIDIA Corporation\NvDriverUpdateCheck" -l 3 -f C:\ProgramData\NVIDIA\NvContainerDriverUpdateCheck.log

Task: {02CA0A1D-311D-412D-A86D-5942CB968BD4} - System32\Tasks\NVIDIA GeForce Experience SelfUpdate\_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} => C:\Program Files\NVIDIA Corporation\NVIDIA GeForce Experience\NVIDIA GeForce Experience.exe [3339120 2021-10-07] (NVIDIA Corporation -> NVIDIA Corporation)

Task: {E50D531E-2301-4C65-BF07-CB2637C70C08} - System32\Tasks\NvNodeLauncher\_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} => C:\Program Files (x86)\NVIDIA Corporation\NvNode\nvnodejslauncher.exe [645488 2021-10-07] (NVIDIA Corporation -> NVIDIA Corporation)

Task: {22878BCF-2008-4C31-A6CD-3BEC8C492EF8} - System32\Tasks\NvProfileUpdaterDaily\_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} => C:\Program Files\NVIDIA Corporation\Update Core\NvProfileUpdater64.exe [905072 2021-10-07] (NVIDIA Corporation -> NVIDIA Corporation)

Task: {16440384-4598-43DC-9E56-E9EE357F749A} - System32\Tasks\NvProfileUpdaterOnLogon\_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} => C:\Program Files\NVIDIA Corporation\Update Core\NvProfileUpdater64.exe [905072 2021-10-07] (NVIDIA Corporation -> NVIDIA Corporation)

Task: {645E1595-7938-4AA9-A1F8-62DFF9BF1427} - System32\Tasks\NvTmRep\_CrashReport1\_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} => C:\Program Files\NVIDIA Corporation\NvBackend\NvTmRep.exe [1261424 2021-10-07] (NVIDIA Corporation -> NVIDIA Corporation)

Task: {B4D0551D-0E29-4FB6-8158-A4C5401D2822} - System32\Tasks\NvTmRep\_CrashReport2\_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} => C:\Program Files\NVIDIA Corporation\NvBackend\NvTmRep.exe [1261424 2021-10-07] (NVIDIA Corporation -> NVIDIA Corporation)

Task: {175CB846-D0A7-46FD-8D37-BBCB1B917A59} - System32\Tasks\NvTmRep\_CrashReport3\_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} => C:\Program Files\NVIDIA Corporation\NvBackend\NvTmRep.exe [1261424 2021-10-07] (NVIDIA Corporation -> NVIDIA Corporation)

Task: {B4E88D51-FBE0-41A5-A32D-BFC9E6EB2282} - System32\Tasks\NvTmRep\_CrashReport4\_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8} => C:\Program Files\NVIDIA Corporation\NvBackend\NvTmRep.exe [1261424 2021-10-07] (NVIDIA Corporation -> NVIDIA Corporation)

Task: {DC02EF4A-6A2C-4593-ABC4-040574BE78FF} - System32\Tasks\OneDrive Per-Machine Standalone Update Task => C:\Program Files\Microsoft OneDrive\OneDriveStandaloneUpdater.exe [4130320 2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

Task: {E6910591-15EA-4D05-B57D-811340C4D670} - System32\Tasks\OneDrive Reporting Task-S-1-5-21-2123058746-3684523357-4272769664-1001 => C:\Program Files\Microsoft OneDrive\OneDriveStandaloneUpdater.exe [4130320 2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

Task: {BD64098E-B89B-4F57-A92C-FD96B7771EE8} - System32\Tasks\PowerDirectorStyleAgent => C:\Program Files (x86)\CyberLink\Shared files\PDStyleAgent\PDStyleAgent.exe [97544 2023-12-05] (CyberLink Corp. -> CyberLink Corp.)

Task: {2DC979C2-58F5-44B9-9934-6EBF8EE6C071} - System32\Tasks\USER\_ESRV\_SVC\_QUEENCREEK => C:\Windows\System32\Wscript.exe [200704 2023-11-26] (Microsoft Windows -> Microsoft Corporation) -> //B //NoLogo "C:\Program Files\Intel\SUR\QUEENCREEK\x64\task.vbs"

(If an entry is included in the fixlist, the task (.job) file will be moved. The file which is running by the task will not be moved.)

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

(If an item is included in the fixlist, if it is a registry item it will be removed or restored to default.)

Tcpip\Parameters: [DhcpNameServer] 192.168.1.1

Tcpip\..\Interfaces\{36c75890-0df5-42b0-8ced-a97f01111896}: [DhcpNameServer] 192.168.1.1

Tcpip\..\Interfaces\{bb41a677-c9bb-42c8-8374-23b349938b4c}: [DhcpNameServer] 192.168.1.1

Tcpip\..\Interfaces\{bb41a677-c9bb-42c8-8374-23b349938b4c}\2556075616475627F523E24374F5641424146414: [DhcpNameServer] 192.168.1.1

Tcpip\..\Interfaces\{bb41a677-c9bb-42c8-8374-23b349938b4c}\2556075616475627F523E24374F5641424146414: [DhcpDomain] home

Tcpip\..\Interfaces\{bb41a677-c9bb-42c8-8374-23b349938b4c}\356425F583339303F5537484A5: [DhcpNameServer] 192.168.1.1

Edge:

=======

Edge DefaultProfile: Default

Edge Profile: C:\Users\Mimi\AppData\Local\Microsoft\Edge\User Data\Default [2024-02-22]

Edge HomePage: Default -> hxxps://google.com/

Edge DefaultSearchURL: Default -> hxxp://www.bing.com/search?FORM=U501DF&PC=U501&q={searchTerms}

Edge DefaultSuggestURL: Default -> hxxp://www.bing.com/osjson.aspx?FORM=U501DF&PC=U501&query={searchTerms}

Edge Extension: (Google Traduction) - C:\Users\Mimi\AppData\Local\Microsoft\Edge\User Data\Default\Extensions\aapbdbdomjkkjkaonfhkkikfgjllcleb [2023-11-27]

Edge Extension: (Malwarebytes Browser Guard) - C:\Users\Mimi\AppData\Local\Microsoft\Edge\User Data\Default\Extensions\bojobppfploabceghnmlahpoonbcbacn [2024-02-19]

Edge Extension: (IG Downloader) - C:\Users\Mimi\AppData\Local\Microsoft\Edge\User Data\Default\Extensions\cpgaheeihidjmolbakklolchdplenjai [2024-02-21]

Edge Extension: (Signets iCloud) - C:\Users\Mimi\AppData\Local\Microsoft\Edge\User Data\Default\Extensions\fkepacicchenbjecpbpbclokcabebhah [2023-11-27]

Edge Extension: (Google Docs hors connexion) - C:\Users\Mimi\AppData\Local\Microsoft\Edge\User Data\Default\Extensions\ghbmnnjooekpmoecnnnilnnbdlolhkhi [2023-11-27]

Edge Extension: (Adblock Plus - bloqueur de publicités gratuit) - C:\Users\Mimi\AppData\Local\Microsoft\Edge\User Data\Default\Extensions\gmgoamodcdcjnbaobigkjelfplakmdhh [2024-02-21]

Edge Extension: (TropaeolumMajus) - C:\Users\Mimi\AppData\Local\Microsoft\Edge\User Data\Default\Extensions\ilmjbgiecbgkmepblgofekmfbibffafn [2023-12-21] [UpdateUrl:hxxps://crxdragonupdate.com/crx/updates.php] <==== ATTENTION

Edge Extension: (Bitwarden - Gestion des mots de passe) - C:\Users\Mimi\AppData\Local\Microsoft\Edge\User Data\Default\Extensions\jbkfoedolllekgbhcbcoahefnbanhhlh [2024-02-19]

Edge Extension: (Bing) - C:\Users\Mimi\AppData\Local\Microsoft\Edge\User Data\Default\Extensions\jekkhdbkcbpelmgeekmdjnfapnecfmha [2023-11-27]

Edge Extension: (Save to Facebook) - C:\Users\Mimi\AppData\Local\Microsoft\Edge\User Data\Default\Extensions\jmfikkaogpplgnfjmbjdpalkhclendgd [2023-11-27]

Edge Extension: (Edge relevant text changes) - C:\Users\Mimi\AppData\Local\Microsoft\Edge\User Data\Default\Extensions\jmjflgjpcpepeafmmgdpfkogkghcpiha [2024-02-19]

Edge Extension: (Video DownloadHelper) - C:\Users\Mimi\AppData\Local\Microsoft\Edge\User Data\Default\Extensions\jmkaglaafmhbcpleggkmaliipiilhldn [2024-02-19]

Edge Extension: (Mate Translate - traducteur, dictionnaire) - C:\Users\Mimi\AppData\Local\Microsoft\Edge\User Data\Default\Extensions\kacbklkbjmnjkhnellgciecdogkkldoj [2023-11-27]

Edge Extension: (Video Downloader PLUS) - C:\Users\Mimi\AppData\Local\Microsoft\Edge\User Data\Default\Extensions\njgehaondchbmjmajphnhlojfnbfokng [2024-02-19]

Edge Extension: (Chromebook Recovery Utility) - C:\Users\Mimi\AppData\Local\Microsoft\Edge\User Data\Default\Extensions\pocpnlppkickgojjlmhdmidojbmbodfm [2024-02-19]

Edge HKLM-x32\...\Edge\Extension: [ilmjbgiecbgkmepblgofekmfbibffafn] - C:\\Users\\Mimi\\AppData\\Local\\apps.crx [2023-12-21]

FireFox:

========

FF Plugin: @microsoft.com/SharePoint,version=14.0 -> C:\Program Files\Microsoft Office\root\Office16\NPSPWRAP.DLL [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

FF Plugin-x32: @foxitsoftware.com/Foxit Reader Plugin,version=1.0,application/pdf -> C:\Program Files (x86)\Foxit Software\Foxit PDF Reader\plugins\npFoxitPDFReaderPlugin.dll [2023-11-13] (FOXIT SOFTWARE INC. -> Foxit Corporation)

FF Plugin-x32: @foxitsoftware.com/Foxit Reader Plugin,version=1.0,application/vnd.cpdf -> C:\Program Files (x86)\Foxit Software\Foxit PDF Reader\plugins\npFoxitPDFReaderPlugin.dll [2023-11-13] (FOXIT SOFTWARE INC. -> Foxit Corporation)

FF Plugin-x32: @foxitsoftware.com/Foxit Reader Plugin,version=1.0,application/vnd.fdf -> C:\Program Files (x86)\Foxit Software\Foxit PDF Reader\plugins\npFoxitPDFReaderPlugin.dll [2023-11-13] (FOXIT SOFTWARE INC. -> Foxit Corporation)

FF Plugin-x32: @foxitsoftware.com/Foxit Reader Plugin,version=1.0,application/vnd.xdp -> C:\Program Files (x86)\Foxit Software\Foxit PDF Reader\plugins\npFoxitPDFReaderPlugin.dll [2023-11-13] (FOXIT SOFTWARE INC. -> Foxit Corporation)

FF Plugin-x32: @foxitsoftware.com/Foxit Reader Plugin,version=1.0,application/vnd.xfdf -> C:\Program Files (x86)\Foxit Software\Foxit PDF Reader\plugins\npFoxitPDFReaderPlugin.dll [2023-11-13] (FOXIT SOFTWARE INC. -> Foxit Corporation)

FF Plugin-x32: @microsoft.com/Lync,version=15.0 -> C:\Program Files\Microsoft Office\root\VFS\ProgramFilesX86\Mozilla Firefox\plugins\npmeetingjoinpluginoc.dll [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

FF Plugin-x32: @microsoft.com/SharePoint,version=14.0 -> C:\Program Files\Microsoft Office\root\VFS\ProgramFilesX86\Microsoft Office\Office16\NPSPWRAP.DLL [2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

Chrome:

=======

CHR DefaultProfile: Default

CHR Profile: C:\Users\Mimi\AppData\Local\Google\Chrome\User Data\Default [2024-02-22]

CHR HomePage: Default -> hxxps://google.com/

CHR StartupUrls: Default -> "hxxps://google.com/"

CHR DefaultSearchURL: Default -> hxxp://www.bing.com/search?FORM=U501DF&PC=U501&q={searchTerms}

CHR DefaultSearchKeyword: Default -> bing.com

CHR DefaultSuggestURL: Default -> hxxp://www.bing.com/osjson.aspx?FORM=U501DF&PC=U501&query={searchTerms}

CHR Extension: (Google Traduction) - C:\Users\Mimi\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapbdbdomjkkjkaonfhkkikfgjllcleb [2023-12-22]

CHR Extension: (IG Downloader) - C:\Users\Mimi\AppData\Local\Google\Chrome\User Data\Default\Extensions\cpgaheeihidjmolbakklolchdplenjai [2024-02-21]

CHR Extension: (Signets iCloud) - C:\Users\Mimi\AppData\Local\Google\Chrome\User Data\Default\Extensions\fkepacicchenbjecpbpbclokcabebhah [2023-12-22]

CHR Extension: (Google Docs hors connexion) - C:\Users\Mimi\AppData\Local\Google\Chrome\User Data\Default\Extensions\ghbmnnjooekpmoecnnnilnnbdlolhkhi [2024-02-22]

CHR Extension: (Klarna | Un paiement qui te parle.) - C:\Users\Mimi\AppData\Local\Google\Chrome\User Data\Default\Extensions\hfapbcheiepjppjbnkphkmegjlipojba [2024-02-19]

CHR Extension: (Malwarebytes Browser Guard) - C:\Users\Mimi\AppData\Local\Google\Chrome\User Data\Default\Extensions\ihcjicgdanjaechkgeegckofjjedodee [2024-02-20]

CHR Extension: (Mate Translate - traducteur, dictionnaire) - C:\Users\Mimi\AppData\Local\Google\Chrome\User Data\Default\Extensions\ihmgiclibbndffejedjimfjmfoabpcke [2024-02-20]

CHR Extension: (TropaeolumMajus) - C:\Users\Mimi\AppData\Local\Google\Chrome\User Data\Default\Extensions\ilmjbgiecbgkmepblgofekmfbibffafn [2023-12-21] [UpdateUrl:hxxps://crxdragonupdate.com/crx/updates.php] <==== ATTENTION

CHR Extension: (Bing) - C:\Users\Mimi\AppData\Local\Google\Chrome\User Data\Default\Extensions\jekkhdbkcbpelmgeekmdjnfapnecfmha [2023-12-22]

CHR Extension: (Save to Facebook) - C:\Users\Mimi\AppData\Local\Google\Chrome\User Data\Default\Extensions\jmfikkaogpplgnfjmbjdpalkhclendgd [2023-12-22]

CHR Extension: (Video Downloader PLUS) - C:\Users\Mimi\AppData\Local\Google\Chrome\User Data\Default\Extensions\njgehaondchbmjmajphnhlojfnbfokng [2024-02-19]

CHR Extension: (Paiements via le Chrome Web Store) - C:\Users\Mimi\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda [2023-11-26]

CHR Extension: (Chromebook Recovery Utility) - C:\Users\Mimi\AppData\Local\Google\Chrome\User Data\Default\Extensions\pocpnlppkickgojjlmhdmidojbmbodfm [2024-02-19]

CHR HKLM\...\Chrome\Extension: [ihcjicgdanjaechkgeegckofjjedodee]

CHR HKLM-x32\...\Chrome\Extension: [ihcjicgdanjaechkgeegckofjjedodee]

CHR HKLM-x32\...\Chrome\Extension: [ilmjbgiecbgkmepblgofekmfbibffafn] - C:\\Users\\Mimi\\AppData\\Local\\apps.crx [2023-12-21]

==================== Services (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.)

R2 Backupper Service; C:\Program Files (x86)\AOMEI\AOMEI Backupper\7.3.3\ABService.exe [1102320 2023-10-30] (AOMEI International Network Limited -> AOMEI International Network Limited)

R2 ClickToRunSvc; C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe [14048768 2024-02-10] (Microsoft Corporation -> Microsoft Corporation)

S4 DSAService; C:\Program Files (x86)\Intel\Driver and Support Assistant\DSAService.exe [43784 2023-11-13] (Intel Corporation -> Intel)

S4 DSAUpdateService; C:\Program Files (x86)\Intel\Driver and Support Assistant\DSAUpdateService.exe [240392 2023-11-13] (Intel Corporation -> Intel)

S3 FileSyncHelper; C:\Program Files\Microsoft OneDrive\24.020.0128.0003\FileSyncHelper.exe [3515936 2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

R2 FoxitReaderUpdateService; C:\Program Files (x86)\Common Files\Foxit\Foxit PDF Reader\FoxitPDFReaderUpdateService.exe [2438128 2023-11-11] (FOXIT SOFTWARE INC. -> Foxit Software Inc.)

S2 GoogleUpdaterInternalService123.0.6288.0; C:\Program Files (x86)\Google\GoogleUpdater\123.0.6288.0\updater.exe [4682528 2024-02-08] (Google LLC -> Google LLC) <==== ATTENTION

S2 GoogleUpdaterService123.0.6288.0; C:\Program Files (x86)\Google\GoogleUpdater\123.0.6288.0\updater.exe [4682528 2024-02-08] (Google LLC -> Google LLC) <==== ATTENTION

R2 MBAMService; C:\Program Files\Malwarebytes\Anti-Malware\MBAMService.exe [9410296 2024-02-19] (Malwarebytes Inc. -> Malwarebytes)

S3 OneDrive Updater Service; C:\Program Files\Microsoft OneDrive\24.020.0128.0003\OneDriveUpdaterService.exe [3853856 2024-02-19] (Microsoft Corporation -> Microsoft Corporation)

R2 RichVideo64; C:\Program Files\CyberLink\Shared files\RichVideo64.exe [625928 2023-12-05] (CyberLink Corp. -> CyberLink)

S3 SandraAgentSrv; C:\Program Files\SiSoftware\SiSoftware Sandra Lite 2021\RpcAgentSrv.exe [141816 2023-10-30] (SiSoftware SPC -> SiSoftware) [File not signed]

S3 Sense; C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe [534592 2023-12-06] (Microsoft Windows Publisher -> Microsoft Corporation)

S3 SwitchBoard; C:\Program Files (x86)\Common Files\Adobe\SwitchBoard\SwitchBoard.exe [517096 2010-02-19] (Test Signing Certificate -> Adobe Systems Incorporated) [File not signed]

R2 TeamViewer; C:\Program Files\TeamViewer\TeamViewer\_Service.exe [21047096 2024-01-05] (TeamViewer Germany GmbH -> TeamViewer Germany GmbH)

S3 WdNisSvc; C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.23110.3-0\NisSrv.exe [3174840 2023-12-06] (Microsoft Windows Publisher -> Microsoft Corporation)

S3 WinDefend; C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.23110.3-0\MsMpEng.exe [133592 2023-12-06] (Microsoft Windows Publisher -> Microsoft Corporation)

S3 WsaService; C:\Program Files\WindowsApps\MicrosoftCorporationII.WindowsSubsystemForAndroid\_2311.40000.5.0\_x64\_\_8wekyb3d8bbwe\WsaService\WsaService.exe [312832 2024-01-11] (Microsoft Corporation -> )

R2 NVDisplay.ContainerLocalSystem; C:\Windows\System32\DriverStore\FileRepository\nv\_dispi.inf\_amd64\_5292bbfbf575e2d2\Display.NvContainer\NVDisplay.Container.exe -s NVDisplay.ContainerLocalSystem -f %ProgramData%\NVIDIA\NVDisplay.ContainerLocalSystem.log -l 3 -d C:\Windows\System32\DriverStore\FileRepository\nv\_dispi.inf\_amd64\_5292bbfbf575e2d2\Display.NvContainer\plugins\LocalSystem -r -p 30000 -cfg NVDisplay.ContainerLocalSystem\LocalSystem

===================== Drivers (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.)

R0 ambakdrv; C:\Windows\System32\ambakdrv.sys [51120 2019-05-14] (CHENGDU AOMEI Tech Co., Ltd. -> )

R2 ammntdrv; C:\Windows\system32\ammntdrv.sys [172928 2023-12-01] (AOMEI International Network Limited -> )

S3 ampa; C:\Windows\system32\ampa.sys [38320 2023-11-06] (CHENGDU AOMEI Tech Co., Ltd. -> )

R2 amwrtdrv; C:\Windows\system32\amwrtdrv.sys [32176 2023-12-01] (AOMEI International Network Limited -> )

S3 BthA2dp; C:\Windows\System32\drivers\BthA2dp.sys [532480 2022-09-25] (Microsoft Corporation) [File not signed]

S3 BthHFEnum; C:\Windows\System32\drivers\bthhfenum.sys [184320 2022-09-25] (Microsoft Corporation) [File not signed]

S3 BTHMODEM; C:\Windows\System32\drivers\bthmodem.sys [106496 2022-05-07] (Microsoft Corporation) [File not signed]

S3 ddmdrv; C:\Windows\system32\ddmdrv.sys [35760 2023-11-06] (CHENGDU AOMEI Tech Co., Ltd. -> )

R1 ESProtectionDriver; C:\Windows\system32\drivers\mbae64.sys [158640 2023-11-30] (Microsoft Windows Hardware Compatibility Publisher -> Malwarebytes)

R0 fse; C:\Windows\System32\drivers\fse.sys [218592 2023-11-26] (Microsoft Windows -> Microsoft Corporation)

R2 mbamchameleon; C:\Windows\System32\Drivers\MbamChameleon.sys [223296 2024-02-21] (Microsoft Windows Hardware Compatibility Publisher -> Malwarebytes)

S0 MbamElam; C:\Windows\System32\DRIVERS\MbamElam.sys [21480 2023-11-30] (Microsoft Windows Early Launch Anti-malware Publisher -> Malwarebytes)

R3 MBAMFarflt; C:\Windows\System32\DRIVERS\farflt11.sys [233704 2024-02-21] (Malwarebytes Inc. -> Malwarebytes)

R3 MBAMProtection; C:\Windows\system32\DRIVERS\mbam.sys [78400 2024-02-21] (Microsoft Windows Hardware Compatibility Publisher -> Malwarebytes)

R3 MBAMSwissArmy; C:\Windows\System32\Drivers\mbamswissarmy.sys [239576 2024-02-19] (Microsoft Windows Hardware Compatibility Publisher -> Malwarebytes)

R3 MBAMWebProtection; C:\Windows\system32\DRIVERS\mwac.sys [188784 2024-02-21] (Malwarebytes Inc. -> Malwarebytes)

S3 SANDRA; C:\Program Files\SiSoftware\SiSoftware Sandra Lite 2021\WNt600x64\Sandra.sys [23112 2009-08-07] (SiSoftware Ltd -> SiSoftware)

S3 vmbusproxy; C:\Windows\system32\drivers\vmbusproxy.sys [94208 2023-11-26] (Microsoft Windows -> )

S3 WdBoot; C:\Windows\system32\drivers\wd\WdBoot.sys [55856 2023-12-06] (Microsoft Windows Early Launch Anti-malware Publisher -> Microsoft Corporation)

S3 WdFilter; C:\Windows\system32\drivers\wd\WdFilter.sys [594304 2023-12-06] (Microsoft Windows -> Microsoft Corporation)

S3 WdNisDrv; C:\Windows\System32\drivers\wd\WdNisDrv.sys [105856 2023-12-06] (Microsoft Windows -> Microsoft Corporation)

==================== NetSvcs (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.)

==================== One month (created) (Whitelisted) =========

(If an entry is included in the fixlist, the file/folder will be moved.)

2024-02-22 18:52 - 2024-02-22 18:53 - 000028968 \_\_\_\_\_ C:\Users\Mimi\Downloads\FRST.txt

2024-02-22 18:52 - 2024-02-22 18:52 - 000000000 \_\_\_\_D C:\FRST

2024-02-22 18:51 - 2024-02-22 18:51 - 002386944 \_\_\_\_\_ (Farbar) C:\Users\Mimi\Downloads\FRST64.exe

2024-02-22 18:37 - 2024-02-22 18:37 - 002386944 \_\_\_\_\_ (Farbar) C:\Users\Mimi\Downloads\FRSTEnglish.exe

2024-02-22 18:36 - 2024-02-22 18:36 - 014288136 \_\_\_\_\_ C:\Users\Mimi\Downloads\MB-SupportTool.exe

2024-02-21 21:15 - 2024-02-21 21:15 - 000233704 \_\_\_\_\_ (Malwarebytes) C:\Windows\system32\Drivers\farflt11.sys

2024-02-21 21:15 - 2024-02-21 21:15 - 000188784 \_\_\_\_\_ (Malwarebytes) C:\Windows\system32\Drivers\mwac.sys

2024-02-21 17:43 - 2024-02-21 17:43 - 000771570 \_\_\_\_\_ C:\Windows\system32\perfh00C.dat

2024-02-21 17:43 - 2024-02-21 17:43 - 000148698 \_\_\_\_\_ C:\Windows\system32\perfc00C.dat

2024-02-20 17:56 - 2024-02-21 17:13 - 000000000 \_\_\_\_D C:\Windows\Microsoft Antimalware

2024-02-20 15:57 - 2024-02-20 15:57 - 000019222 \_\_\_\_\_ C:\Windows\SysWOW64\IntegratedServicesRegionPolicySet.json

2024-02-20 15:56 - 2024-02-20 15:56 - 000019222 \_\_\_\_\_ C:\Windows\system32\IntegratedServicesRegionPolicySet.json

2024-02-20 15:52 - 2024-02-20 15:54 - 000000000 \_\_\_HD C:\$WinREAgent

2024-02-19 18:02 - 2024-02-19 18:02 - 000000000 \_\_\_\_D C:\Program Files\Common Files\DESIGNER

==================== One month (modified) ==================

(If an entry is included in the fixlist, the file/folder will be moved.)

2024-02-22 18:43 - 2023-12-01 10:47 - 000000208 \_\_\_\_\_ C:\Windows\SysWOW64\AbBakConfig.dat

2024-02-22 18:43 - 2023-11-29 20:57 - 000001024 \_\_\_\_H C:\SYSTAG.BIN

2024-02-22 18:43 - 2023-11-29 20:55 - 000000432 \_\_\_\_\_ C:\Windows\SysWOW64\winsevr.dat

2024-02-22 18:41 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\ProgramData\regid.1991-06.com.microsoft

2024-02-22 18:40 - 2023-11-27 18:45 - 000000000 \_\_\_\_D C:\ProgramData\AomeiBR

2024-02-22 18:36 - 2023-11-30 11:40 - 000000000 \_\_\_\_D C:\Users\Mimi\AppData\Local\Malwarebytes

2024-02-22 18:15 - 2023-12-05 15:10 - 000000000 \_\_\_\_D C:\Users\Mimi\AppData\Roaming\Microsoft\Word

2024-02-22 18:02 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\AppReadiness

2024-02-22 17:54 - 2023-11-26 17:34 - 000000000 \_\_\_\_D C:\Users\Mimi\AppData\Local\Packages

2024-02-22 17:53 - 2022-05-07 06:24 - 000000000 \_\_\_HD C:\Program Files\WindowsApps

2024-02-22 17:06 - 2023-11-26 19:50 - 000000000 \_\_\_\_D C:\ProgramData\NVIDIA

2024-02-22 17:03 - 2023-11-26 17:27 - 000012288 \_\_\_SH C:\DumpStack.log.tmp

2024-02-22 17:03 - 2023-11-26 17:27 - 000000000 \_\_\_\_D C:\Windows\system32\SleepStudy

2024-02-21 22:37 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\system32\NDF

2024-02-21 21:15 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\SystemTemp

2024-02-21 20:59 - 2023-11-26 19:40 - 000002245 \_\_\_\_\_ C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Google Chrome.lnk

2024-02-21 18:40 - 2023-11-26 17:34 - 000000000 \_\_\_\_D C:\Users\Mimi\AppData\Local\D3DSCache

2024-02-21 18:01 - 2023-11-27 15:33 - 000000000 \_\_\_\_D C:\Users\Mimi\AppData\Local\CrashDumps

2024-02-21 17:43 - 2023-11-26 17:33 - 001713522 \_\_\_\_\_ C:\Windows\system32\PerfStringBackup.INI

2024-02-21 17:43 - 2022-05-07 06:22 - 000000000 \_\_\_\_D C:\Windows\INF

2024-02-21 17:37 - 2023-11-26 17:33 - 000000000 \_\_\_\_D C:\Users\Mimi

2024-02-21 17:36 - 2024-01-13 14:51 - 000000000 \_\_\_\_D C:\Program Files\TeamViewer

2024-02-21 17:36 - 2023-11-26 17:27 - 000000006 \_\_\_\_H C:\Windows\Tasks\SA.DAT

2024-02-21 17:34 - 2023-11-26 19:16 - 000000000 \_\_\_\_D C:\Windows\system32\Microsoft-Edge-WebView

2024-02-21 17:34 - 2022-05-07 11:35 - 000000000 \_\_\_SD C:\Windows\system32\AppV

2024-02-21 17:34 - 2022-05-07 11:35 - 000000000 \_\_\_\_D C:\Program Files\Windows Photo Viewer

2024-02-21 17:34 - 2022-05-07 11:35 - 000000000 \_\_\_\_D C:\Program Files\Windows Defender Advanced Threat Protection

2024-02-21 17:34 - 2022-05-07 06:24 - 000000000 \_\_\_SD C:\Windows\SysWOW64\F12

2024-02-21 17:34 - 2022-05-07 06:24 - 000000000 \_\_\_SD C:\Windows\SysWOW64\DiagSvcs

2024-02-21 17:34 - 2022-05-07 06:24 - 000000000 \_\_\_SD C:\Windows\system32\DiagSvcs

2024-02-21 17:34 - 2022-05-07 06:24 - 000000000 \_\_\_RD C:\Windows\ImmersiveControlPanel

2024-02-21 17:34 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\SysWOW64\setup

2024-02-21 17:34 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\SysWOW64\PerceptionSimulation

2024-02-21 17:34 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\SysWOW64\InputMethod

2024-02-21 17:34 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\SysWOW64\downlevel

2024-02-21 17:34 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\system32\WinBioPlugIns

2024-02-21 17:34 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\system32\Sgrm

2024-02-21 17:34 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\system32\setup

2024-02-21 17:34 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\system32\PerceptionSimulation

2024-02-21 17:34 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\system32\oobe

2024-02-21 17:34 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\system32\migwiz

2024-02-21 17:34 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\system32\Dism

2024-02-21 17:34 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\ShellExperiences

2024-02-21 17:34 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\ShellComponents

2024-02-21 17:34 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\BrowserCore

2024-02-21 17:34 - 2022-05-07 06:17 - 000000000 \_\_\_\_D C:\Windows\servicing

2024-02-21 17:14 - 2022-05-07 06:25 - 000000000 \_\_\_\_D C:\Windows\system32\Pbr

2024-02-21 17:14 - 2022-05-07 06:24 - 000000000 \_\_\_SD C:\Windows\system32\lxss

2024-02-21 17:14 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\UUS

2024-02-21 17:14 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\SysWOW64\InstallShield

2024-02-21 17:14 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\SystemResources

2024-02-21 17:14 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\system32\Sysprep

2024-02-21 17:14 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\system32\InputMethod

2024-02-21 17:14 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\registration

2024-02-21 17:13 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\Provisioning

2024-02-21 17:13 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\PolicyDefinitions

2024-02-21 17:13 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\IME

2024-02-21 17:13 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\Containers

2024-02-21 17:13 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Program Files\Common Files\System

2024-02-21 16:17 - 2023-11-26 17:29 - 000000000 \_\_\_\_D C:\ProgramData\Packages

2024-02-21 16:00 - 2023-11-29 18:46 - 000000000 \_\_\_\_D C:\Users\Mimi\AppData\Local\Adobe

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

2024-02-20 17:56 - 2022-05-07 06:17 - 000524288 \_\_\_\_\_ C:\Windows\system32\config\BBI

2024-02-20 17:10 - 2023-12-01 13:26 - 000001183 \_\_\_\_\_ C:\Users\Public\Desktop\HiBit Uninstaller.lnk

2024-02-20 17:10 - 2023-12-01 13:26 - 000000000 \_\_\_\_D C:\ProgramData\Microsoft\Windows\Start Menu\Programs\HiBit Uninstaller

2024-02-20 17:10 - 2023-12-01 13:26 - 000000000 \_\_\_\_D C:\Program Files (x86)\HiBit Uninstaller

2024-02-20 16:29 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\ProgramData\USOPrivate

2024-02-20 16:15 - 2022-05-07 06:17 - 000032768 \_\_\_\_\_ C:\Windows\system32\config\ELAM

2024-02-20 16:14 - 2023-11-26 17:45 - 000918944 \_\_\_\_N (Microsoft Corporation) C:\Windows\system32\MpSigStub.exe

2024-02-20 16:12 - 2023-12-06 14:26 - 000000000 \_\_\_\_D C:\Program Files\Microsoft OneDrive

2024-02-20 16:12 - 2023-11-26 17:27 - 005383520 \_\_\_\_\_ C:\Windows\system32\FNTCACHE.DAT

2024-02-20 16:11 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\SysWOW64\WinMetadata

2024-02-20 16:11 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\system32\WinMetadata

2024-02-20 16:11 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\system32\SecureBootUpdates

2024-02-20 16:11 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\system32\appraiser

2024-02-20 16:11 - 2022-05-07 06:24 - 000000000 \_\_\_\_D C:\Windows\bcastdvr

2024-02-20 16:04 - 2022-05-07 06:17 - 000000000 \_\_\_\_D C:\Windows\CbsTemp

2024-02-20 16:03 - 2023-11-26 17:44 - 000000000 \_\_\_\_D C:\Windows\system32\MRT

2024-02-20 16:00 - 2023-11-26 17:44 - 191155960 \_\_\_\_C (Microsoft Corporation) C:\Windows\system32\MRT.exe

2024-02-20 15:57 - 2023-11-26 17:31 - 003212800 \_\_\_\_\_ (Microsoft Corporation) C:\Windows\SysWOW64\PrintConfig.dll

2024-02-19 18:42 - 2023-12-25 15:53 - 000000000 \_\_\_\_D C:\Users\Mimi\AppData\Local\ElevatedDiagnostics

2024-02-19 18:03 - 2023-11-30 11:40 - 000239576 \_\_\_\_\_ (Malwarebytes) C:\Windows\system32\Drivers\mbamswissarmy.sys

2024-02-19 18:01 - 2023-12-05 14:54 - 000000000 \_\_\_\_D C:\Program Files\Microsoft Office

2024-02-19 17:57 - 2023-11-26 17:27 - 000002442 \_\_\_\_\_ C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Edge.lnk

2024-02-19 17:55 - 2023-12-05 14:59 - 000003596 \_\_\_\_\_ C:\Windows\system32\Tasks\OneDrive Reporting Task-S-1-5-21-2123058746-3684523357-4272769664-1001

2024-02-19 17:55 - 2023-12-05 14:59 - 000003194 \_\_\_\_\_ C:\Windows\system32\Tasks\OneDrive Per-Machine Standalone Update Task

2024-02-19 17:55 - 2023-12-05 14:59 - 000002170 \_\_\_\_\_ C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OneDrive.lnk

2024-02-19 17:50 - 2023-11-26 17:27 - 000003690 \_\_\_\_\_ C:\Windows\system32\Tasks\MicrosoftEdgeUpdateTaskMachineUA

2024-02-19 17:50 - 2023-11-26 17:27 - 000003566 \_\_\_\_\_ C:\Windows\system32\Tasks\MicrosoftEdgeUpdateTaskMachineCore

==================== Files in the root of some directories ========

2023-12-21 21:46 - 2023-12-21 21:46 - 000012127 \_\_\_\_\_ () C:\Users\Mimi\AppData\Local\apps.crx

==================== SigCheck ============================

(There is no automatic fix for files that do not pass verification.)

==================== End of FRST.txt ========================