Résultats d'analyse de Farbar Recovery Scan Tool (FRST) (x64) Version: 15.07.2018

Exécuté par Cirile (administrateur) sur MONPC (16-07-2018 23:29:04)

Exécuté depuis C:\Users\Cirile\AppData\Local\Microsoft\Windows\INetCache\IE\H7E4KE1H

Profils chargés: Cirile & Administrateur (Profils disponibles: Cirile & Administrateur)

Platform: Windows 8.1 (Update) (X64) Langue: Français (France)

Internet Explorer Version 11 (Navigateur par défaut: IE)

Mode d'amorçage: Normal

Tutoriel pour Farbar Recovery Scan Tool: http://www.geekstogo.com/forum/topic/335081-frst-tutorial-how-to-use-farbar-recovery-scan-tool/

==================== Processus (Avec liste blanche) =================

(Si un élément est inclus dans le fichier fixlist.txt, le processus sera arrêté. Le fichier ne sera pas déplacé.)

(NVIDIA Corporation) C:\Program Files\NVIDIA Corporation\Display.NvContainer\NVDisplay.Container.exe

(Intel Corporation) C:\Windows\System32\igfxCUIService.exe

(Realtek Semiconductor) C:\Program Files\Realtek\Audio\HDA\RtkAudioService64.exe

(AVG Technologies CZ, s.r.o.) C:\Program Files (x86)\AVG\Antivirus\AVGSvc.exe

(Apple Inc.) C:\Program Files\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe

(AVG Technologies CZ, s.r.o.) C:\Program Files (x86)\AVG\Framework\Common\avgsvca.exe

(Apple Inc.) C:\Program Files\Bonjour\mDNSResponder.exe

(Intel(R) Corporation) C:\Program Files\Intel\iCLS Client\HeciServer.exe

(Intel Corporation) C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\DAL\Jhi\_service.exe

(Atheros Communications, Inc.) C:\Program Files (x86)\NETGEAR\WNA1100\jswpbapi.exe

(pdfforge GmbH) C:\Program Files\PDF Architect 4\creator-ws.exe

(Â© pdfforge GmbH.) C:\ProgramData\pdfforge\PDF Architect 4 Manager\PDF Architect 4\Architect Manager.exe

(AVG Technologies CZ, s.r.o.) C:\Program Files (x86)\AVG\AVG PC TuneUp\TuneUpUtilitiesService64.exe

() C:\Program Files (x86)\NETGEAR\WNA1100\WifiSvc.exe

(Yahoo Inc.) C:\Program Files (x86)\Yahoo!\yset\{CBF3F570-CBCE-6D4F-9BD0-9F3C47D2AFB7}\YSearchUtilSVC.exe

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

(AVG Technologies CZ, s.r.o.) C:\Program Files (x86)\AVG\Antivirus\x64\aswidsagenta.exe

(HP Inc.) C:\Program Files (x86)\Hewlett-Packard\HP Support Solutions\HPSupportSolutionsFrameworkService.exe

(Google Inc.) C:\Program Files (x86)\Google\Update\1.3.33.17\GoogleCrashHandler.exe

(Google Inc.) C:\Program Files (x86)\Google\Update\1.3.33.17\GoogleCrashHandler64.exe

(HP Inc.) C:\Program Files\HP\HP Touchpoint Analytics Client\TouchpointAnalyticsClientService.exe

(Intel Corporation) C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\FWService\IntelMeFWService.exe

(Intel Corporation) C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe

(Intel Corporation) C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\UNS\UNS.exe

(Microsoft Corporation) C:\Windows\Microsoft.NET\Framework64\v3.0\WPF\PresentationFontCache.exe

(Apple Inc.) C:\Program Files\iPod\bin\iPodService.exe

(HP) C:\Program Files (x86)\HP\Shared\hpqwmiex.exe

(NVIDIA Corporation) C:\Program Files\NVIDIA Corporation\Display.NvContainer\NVDisplay.Container.exe

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

(Realtek Semiconductor) C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe

(AVG Technologies CZ, s.r.o.) C:\Program Files (x86)\AVG\AVG PC TuneUp\TuneUpUtilitiesApp64.exe

(Intel Corporation) C:\Windows\System32\igfxEM.exe

(Intel Corporation) C:\Windows\System32\igfxHK.exe

(NVIDIA Corporation) C:\Program Files (x86)\NVIDIA Corporation\Update Core\NvBackend.exe

(AVG Technologies CZ, s.r.o.) C:\Program Files (x86)\AVG\Framework\Common\avguix.exe

(Apple Inc.) C:\Program Files\iTunes\iTunesHelper.exe

() C:\Program Files (x86)\NETGEAR\WNA1100\WNA1100.exe

(Oracle Corporation) C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe

(CyberLink) C:\Program Files (x86)\CyberLink\Power2Go8\CLMLSvc\_P2G8.exe

(AVG Technologies CZ, s.r.o.) C:\Program Files (x86)\AVG\Antivirus\AVGUI.exe

(Piriform Ltd) C:\Program Files\CCleaner\CCleaner64.exe

(Microsoft Corporation) C:\Program Files\Internet Explorer\iexplore.exe

==================== Registre (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. Le fichier ne sera pas déplacé.)

HKLM\...\Run: [NvBackend] => C:\Program Files (x86)\NVIDIA Corporation\Update Core\NvBackend.exe [1793736 2015-03-26] (NVIDIA Corporation)

HKLM\...\Run: [AvgUi] => C:\Program Files (x86)\AVG\Framework\Common\avguirna.exe [239192 2018-06-14] (AVG Technologies CZ, s.r.o.)

HKLM\...\Run: [AVGUI.exe] => C:\Program Files (x86)\AVG\Antivirus\AvLaunch.exe [291568 2018-07-07] (AVG Technologies CZ, s.r.o.)

HKLM\...\Run: [iTunesHelper] => C:\Program Files\iTunes\iTunesHelper.exe [303928 2017-05-09] (Apple Inc.)

HKLM-x32\...\Run: [AvgUi] => C:\Program Files (x86)\AVG\Framework\Common\avguirna.exe [239192 2018-06-14] (AVG Technologies CZ, s.r.o.)

HKLM-x32\...\Run: [SunJavaUpdateSched] => C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe [588704 2018-03-28] (Oracle Corporation)

HKU\S-1-5-21-3539592496-772588293-4036759407-1002\...\Run: [CCleaner Monitoring] => C:\Program Files\CCleaner\CCleaner64.exe [9363672 2017-02-08] (Piriform Ltd)

HKU\S-1-5-21-3539592496-772588293-4036759407-500\...\RunOnce: [WAB Migrate] => C:\Program Files\Windows Mail\wab.exe [516608 2014-11-21] (Microsoft Corporation)

AppInit\_DLLs: C:\windows\system32\nvinitx.dll => C:\windows\system32\nvinitx.dll [182080 2018-02-01] (NVIDIA Corporation)

AppInit\_DLLs: , C:\WINDOWS\system32\nvinitx.dll => C:\WINDOWS\system32\nvinitx.dll [182080 2018-02-01] (NVIDIA Corporation)

AppInit\_DLLs-x32: C:\WINDOWS\SysWOW64\nvinit.dll => C:\WINDOWS\SysWOW64\nvinit.dll [159896 2018-02-01] (NVIDIA Corporation)

Startup: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\NETGEAR WNA1100 Genie.lnk [2016-12-19]

ShortcutTarget: NETGEAR WNA1100 Genie.lnk -> C:\Program Files (x86)\NETGEAR\WNA1100\WNA1100.exe ()

==================== Internet (Avec liste blanche) ====================

(Si un élément est inclus dans le fichier fixlist.txt, s'il s'agit d'un élément du Registre, il sera supprimé ou restauré à la valeur par défaut.)

Tcpip\Parameters: [DhcpNameServer] 89.2.0.1 89.2.0.2

Tcpip\..\Interfaces\{694901EF-43F2-4258-BF34-0FEDEA2BF6F3}: [DhcpNameServer] 89.2.0.1 89.2.0.2

Tcpip\..\Interfaces\{D7353DFE-5BB7-45A2-8BB6-8F1400F250FA}: [DhcpNameServer] 89.2.0.1 89.2.0.2

Internet Explorer:

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

HKLM\Software\Microsoft\Internet Explorer\Main,Start Page = hxxp://g.uk.msn.com/HPDSK13/3

HKLM\Software\Microsoft\Internet Explorer\Main,Default\_Page\_URL = hxxp://g.uk.msn.com/HPDSK13/3

HKU\S-1-5-21-3539592496-772588293-4036759407-1002\Software\Microsoft\Internet Explorer\Main,Start Page = hxxp://www.msn.com/?pc=U453&ocid=U453DHP&osmkt=fr-fr

HKU\S-1-5-21-3539592496-772588293-4036759407-1002\Software\Microsoft\Internet Explorer\Main,Default\_Page\_URL = hxxp://g.uk.msn.com/HPDSK13/3

HKU\S-1-5-21-3539592496-772588293-4036759407-500\Software\Microsoft\Internet Explorer\Main,Default\_Page\_URL = hxxp://g.uk.msn.com/HPDSK13/3

SearchScopes: HKLM -> {D944BB61-2E34-4DBF-A683-47E505C587DC} URL = hxxp://rover.ebay.com/rover/1/709-29563-11896-9/4 ?mpre=http%3A%2F%2Fwww.ebay.com%2Fsch%2F%3F\_nkw%3D{searchTerms}&keyword={searchTerms}

SearchScopes: HKLM -> {F5B0EB7E-8684-4251-AF41-00D571384D6B} URL = hxxp://www.amazon.fr/s/ref=azs\_osd\_ieafr?ie=UTF-8&tag=hp-fr1-vsb-21&link%5Fcode=qs&index=aps&field-keywords={searchTerms}

SearchScopes: HKLM-x32 -> {D944BB61-2E34-4DBF-A683-47E505C587DC} URL = hxxp://rover.ebay.com/rover/1/709-29563-11896-9/4 ?mpre=http%3A%2F%2Fwww.ebay.com%2Fsch%2F%3F\_nkw%3D{searchTerms}&keyword={searchTerms}

SearchScopes: HKLM-x32 -> {F5B0EB7E-8684-4251-AF41-00D571384D6B} URL = hxxp://www.amazon.fr/s/ref=azs\_osd\_ieafr?ie=UTF-8&tag=hp-fr1-vsb-21&link%5Fcode=qs&index=aps&field-keywords={searchTerms}

SearchScopes: HKU\S-1-5-21-3539592496-772588293-4036759407-1002 -> DefaultScope {3744FB13-BF33-4401-9F4B-16B35C589E4A} URL = hxxp://www.bing.com/search?FORM=U453DF&PC=U453&q={searchTerms}&src=IE-SearchBox

SearchScopes: HKU\S-1-5-21-3539592496-772588293-4036759407-1002 -> {0633EE93-D776-472f-A0FF-E1416B8B2E3A} URL =

SearchScopes: HKU\S-1-5-21-3539592496-772588293-4036759407-1002 -> {3744FB13-BF33-4401-9F4B-16B35C589E4A} URL = hxxp://www.bing.com/search?FORM=U453DF&PC=U453&q={searchTerms}&src=IE-SearchBox

SearchScopes: HKU\S-1-5-21-3539592496-772588293-4036759407-1002 -> {4A9D418E-37BB-4CC1-AFDB-AB1D4384D452} URL = hxxps://fr.search.yahoo.com/search?p={searchTerms}&intl=fr&fr=yset\_ie\_syc\_oracle&type=orcl\_default&partnerexternal-oracle=external-oracle

SearchScopes: HKU\S-1-5-21-3539592496-772588293-4036759407-1002 -> {4B9AC332-A056-4142-BCFC-88BC84CFC306} URL = hxxps://www.google.com/search?q={searchTerms}&sourceid=ie7&rls=com.microsoft:{language}:{referrer:source}&ie={inputEncoding?}&oe={outputEncoding?}

SearchScopes: HKU\S-1-5-21-3539592496-772588293-4036759407-1002 -> {95B7759C-8C7F-4BF1-B163-73684A933233} URL = hxxps://mysearch.avg.com/search?cid={7A1FE7F6-9EFE-4959-8A8C-B8DD7D0F382A}&mid=457cc72ffb9b47cf9dd7ad4c41757902-8547b08cde9ce134046dc6439122476cd153999c&lang=fr&ds=AVG&coid=avgtbavg&cmpid=0117tb&pr=fr&d=2016-12-19 01:23:13&v=4.3.6.255&pid=wtu&sg=&sap=dsp&q={searchTerms}

SearchScopes: HKU\S-1-5-21-3539592496-772588293-4036759407-1002 -> {D944BB61-2E34-4DBF-A683-47E505C587DC} URL = hxxp://rover.ebay.com/rover/1/709-29563-11896-9/4 ?mpre=http%3A%2F%2Fwww.ebay.com%2Fsch%2F%3F\_nkw%3D{searchTerms}&keyword={searchTerms}

SearchScopes: HKU\S-1-5-21-3539592496-772588293-4036759407-1002 -> {F5B0EB7E-8684-4251-AF41-00D571384D6B} URL = hxxp://www.amazon.fr/s/ref=azs\_osd\_ieafr?ie=UTF-8&tag=hp-fr1-vsb-21&link%5Fcode=qs&index=aps&field-keywords={searchTerms}

SearchScopes: HKU\S-1-5-21-3539592496-772588293-4036759407-500 -> DefaultScope {3744FB13-BF33-4401-9F4B-16B35C589E4A} URL = hxxp://www.bing.com/search?FORM=U453DF&PC=U453&q={searchTerms}&src=IE-SearchBox

SearchScopes: HKU\S-1-5-21-3539592496-772588293-4036759407-500 -> {0633EE93-D776-472f-A0FF-E1416B8B2E3A} URL =

SearchScopes: HKU\S-1-5-21-3539592496-772588293-4036759407-500 -> {3744FB13-BF33-4401-9F4B-16B35C589E4A} URL = hxxp://www.bing.com/search?FORM=U453DF&PC=U453&q={searchTerms}&src=IE-SearchBox

SearchScopes: HKU\S-1-5-21-3539592496-772588293-4036759407-500 -> {4B9AC332-A056-4142-BCFC-88BC84CFC306} URL = hxxps://www.google.com/search?q={searchTerms}&sourceid=ie7&rls=com.microsoft:{language}:{referrer:source}&ie={inputEncoding?}&oe={outputEncoding?}

SearchScopes: HKU\S-1-5-21-3539592496-772588293-4036759407-500 -> {95B7759C-8C7F-4BF1-B163-73684A933233} URL = hxxps://mysearch.avg.com/search?cid={7A1FE7F6-9EFE-4959-8A8C-B8DD7D0F382A}&mid=457cc72ffb9b47cf9dd7ad4c41757902-8547b08cde9ce134046dc6439122476cd153999c&lang=fr&ds=AVG&coid=avgtbavg&cmpid=ZenTest\_B\_0&pr=fr&d=2016-12-19 01:23:13&v=4.3.6.255&pid=wtu&sg=&sap=dsp&q={searchTerms}

SearchScopes: HKU\S-1-5-21-3539592496-772588293-4036759407-500 -> {D944BB61-2E34-4DBF-A683-47E505C587DC} URL = hxxp://rover.ebay.com/rover/1/709-29563-11896-9/4 ?mpre=http%3A%2F%2Fwww.ebay.com%2Fsch%2F%3F\_nkw%3D{searchTerms}&keyword={searchTerms}

SearchScopes: HKU\S-1-5-21-3539592496-772588293-4036759407-500 -> {F5B0EB7E-8684-4251-AF41-00D571384D6B} URL = hxxp://www.amazon.fr/s/ref=azs\_osd\_ieafr?ie=UTF-8&tag=hp-fr1-vsb-21&link%5Fcode=qs&index=aps&field-keywords={searchTerms}

BHO: Canon Easy-WebPrint EX BHO -> {3785D0AD-BFFF-47F6-BF5B-A587C162FED9} -> C:\Program Files\Canon\Easy-WebPrint EX\ewpexbho.dll [2016-02-23] (CANON INC.)

BHO: AVG Web TuneUp -> {95B7759C-8C7F-4BF1-B163-73684A933233} -> C:\Program Files\AVG Web TuneUp\4.3.6.255\AVG Web TuneUp.dll [2017-01-20] (AVG)

BHO: Google Toolbar Helper -> {AA58ED58-01DD-4d91-8333-CF10577473F7} -> C:\Program Files (x86)\Google\Google Toolbar\GoogleToolbar\_64.dll [2017-03-06] (Google Inc.)

BHO: HP Network Check Helper -> {E76FD755-C1BA-4DCB-9F13-99BD91223ADE} -> C:\Program Files (x86)\Hewlett-Packard\HP Support Framework\Resources\HPNetworkCheck\HPNetworkCheckPluginx64.dll [2016-12-06] (HP Inc.)

BHO-x32: Canon Easy-WebPrint EX BHO -> {3785D0AD-BFFF-47F6-BF5B-A587C162FED9} -> C:\Program Files (x86)\Canon\Easy-WebPrint EX\ewpexbho.dll [2016-02-23] (CANON INC.)

BHO-x32: PDF Architect 4 Helper -> {38279E1A-7019-40C1-B579-E99DFB3312E8} -> C:\Program Files (x86)\PDF Architect 4\creator-ie-helper.dll [2016-08-05] (pdfforge GmbH)

BHO-x32: Java(tm) Plug-In SSV Helper -> {761497BB-D6F0-462C-B6EB-D4DAF1D92D43} -> C:\Program Files (x86)\Java\jre1.8.0\_171\bin\ssv.dll [2018-04-29] (Oracle Corporation)

BHO-x32: Pas de nom -> {95B7759C-8C7F-4BF1-B163-73684A933233} -> Pas de fichier

BHO-x32: Google Toolbar Helper -> {AA58ED58-01DD-4d91-8333-CF10577473F7} -> C:\Program Files (x86)\Google\Google Toolbar\GoogleToolbar\_32.dll [2017-03-06] (Google Inc.)

BHO-x32: Java(tm) Plug-In 2 SSV Helper -> {DBC80044-A445-435b-BC74-9C25C1C588A9} -> C:\Program Files (x86)\Java\jre1.8.0\_171\bin\jp2ssv.dll [2018-04-29] (Oracle Corporation)

BHO-x32: HP Network Check Helper -> {E76FD755-C1BA-4DCB-9F13-99BD91223ADE} -> C:\Program Files (x86)\Hewlett-Packard\HP Support Framework\Resources\HPNetworkCheck\HPNetworkCheckPlugin.dll [2016-12-06] (HP Inc.)

Toolbar: HKLM - Canon Easy-WebPrint EX - {759D9886-0C6F-4498-BAB6-4A5F47C6C72F} - C:\Program Files\Canon\Easy-WebPrint EX\ewpexhlp.dll [2016-02-23] (CANON INC.)

Toolbar: HKLM - Google Toolbar - {2318C2B1-4965-11d4-9B18-009027A5CD4F} - C:\Program Files (x86)\Google\Google Toolbar\GoogleToolbar\_64.dll [2017-03-06] (Google Inc.)

Toolbar: HKLM-x32 - PDF Architect 4 Toolbar - {23FD9C33-A9E1-48A1-8404-E5925CF1C8E1} - C:\Program Files (x86)\PDF Architect 4\creator-ie-plugin.dll [2016-08-05] (pdfforge GmbH)

Toolbar: HKLM-x32 - Canon Easy-WebPrint EX - {759D9886-0C6F-4498-BAB6-4A5F47C6C72F} - C:\Program Files (x86)\Canon\Easy-WebPrint EX\ewpexhlp.dll [2016-02-23] (CANON INC.)

Toolbar: HKLM-x32 - Google Toolbar - {2318C2B1-4965-11d4-9B18-009027A5CD4F} - C:\Program Files (x86)\Google\Google Toolbar\GoogleToolbar\_32.dll [2017-03-06] (Google Inc.)

Toolbar: HKU\S-1-5-21-3539592496-772588293-4036759407-1002 -> Pas de nom - {7FEBEFE3-6B19-4349-98D2-FFB09D4B49CA} - Pas de fichier

Toolbar: HKU\S-1-5-21-3539592496-772588293-4036759407-500 -> Pas de nom - {7FEBEFE3-6B19-4349-98D2-FFB09D4B49CA} - Pas de fichier

FireFox:

========

FF HKLM\...\Firefox\Extensions: [pdf\_architect\_4\_conv@pdfarchitect.org] - C:\Program Files\PDF Architect 4\resources\pdfarchitect4firefoxextension

FF Extension: (PDF Architect 4 Creator) - C:\Program Files\PDF Architect 4\resources\pdfarchitect4firefoxextension [2016-12-20] [Legacy] [non signé]

FF Plugin: @adobe.com/FlashPlayer -> C:\WINDOWS\system32\Macromed\Flash\NPSWF64\_30\_0\_0\_134.dll [2018-07-10] ()

FF Plugin-x32: @adobe.com/FlashPlayer -> C:\WINDOWS\SysWOW64\Macromed\Flash\NPSWF32\_30\_0\_0\_134.dll [2018-07-10] ()

FF Plugin-x32: @avg.com/AVG SiteSafety plugin,version=11.0.0.1,application/x-avg-sitesafety-plugin -> C:\Program Files (x86)\Common Files\AVG Secure Search\SiteSafetyInstaller\40.3.6\\npsitesafety.dll [Pas de fichier]

FF Plugin-x32: @intel-webapi.intel.com/Intel WebAPI ipt;version=2.1.42 -> C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\IPT\npIntelWebAPIIPT.dll [2012-07-18] (Intel Corporation)

FF Plugin-x32: @intel-webapi.intel.com/Intel WebAPI updater -> C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\IPT\npIntelWebAPIUpdater.dll [2012-07-18] (Intel Corporation)

FF Plugin-x32: @java.com/DTPlugin,version=11.171.2 -> C:\Program Files (x86)\Java\jre1.8.0\_171\bin\dtplugin\npDeployJava1.dll [2018-04-29] (Oracle Corporation)

FF Plugin-x32: @java.com/JavaPlugin,version=11.171.2 -> C:\Program Files (x86)\Java\jre1.8.0\_171\bin\plugin2\npjp2.dll [2018-04-29] (Oracle Corporation)

FF Plugin-x32: @microsoft.com/WLPG,version=16.4.3505.0912 -> C:\Program Files (x86)\Windows Live\Photo Gallery\NPWLPG.dll [2012-09-12] (Microsoft Corporation)

FF Plugin-x32: @nvidia.com/3DVision -> C:\Program Files (x86)\NVIDIA Corporation\3D Vision\npnv3dv.dll [2017-12-19] (NVIDIA Corporation)

FF Plugin-x32: @nvidia.com/3DVisionStreaming -> C:\Program Files (x86)\NVIDIA Corporation\3D Vision\npnv3dvstreaming.dll [2017-12-19] (NVIDIA Corporation)

FF Plugin-x32: @tools.google.com/Google Update;version=3 -> C:\Program Files (x86)\Google\Update\1.3.33.17\npGoogleUpdate3.dll [2018-05-17] (Google Inc.)

FF Plugin-x32: @tools.google.com/Google Update;version=9 -> C:\Program Files (x86)\Google\Update\1.3.33.17\npGoogleUpdate3.dll [2018-05-17] (Google Inc.)

FF Plugin-x32: @WildTangent.com/GamesAppPresenceDetector,Version=1.0 -> C:\Program Files (x86)\WildTangent Games\App\BrowserIntegration\Registered\0\NP\_wtapp.dll [2012-10-12] ()

FF Plugin-x32: PDF Architect 4 -> C:\Program Files (x86)\PDF Architect 4\np-previewer.dll [2016-08-05] (pdfforge GmbH)

Chrome:

=======

CHR HomePage: Default -> mysearch.avg.com

CHR DefaultSearchURL: Default -> hxxps://mysearch.avg.com/search?rvt=1&sap=dsp&q={searchTerms}

CHR DefaultSearchKeyword: Default -> hxxps://mysearch.avg.com

CHR DefaultSuggestURL: Default -> hxxps://toolbar.avg.com/acp?q={searchTerms}&o=1

CHR Profile: C:\Users\Cirile\AppData\Local\Google\Chrome\User Data\Default [2018-07-07]

CHR Extension: (Slides) - C:\Users\Cirile\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek [2017-10-12]

CHR Extension: (Docs) - C:\Users\Cirile\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake [2017-10-12]

CHR Extension: (Google Drive) - C:\Users\Cirile\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf [2016-12-19]

CHR Extension: (YouTube) - C:\Users\Cirile\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo [2016-12-19]

CHR Extension: (AVG Secure Search) - C:\Users\Cirile\AppData\Local\Google\Chrome\User Data\Default\Extensions\chfdnecihphmhljaaejmgoiahnihplgn [2017-01-22]

CHR Extension: (Sheets) - C:\Users\Cirile\AppData\Local\Google\Chrome\User Data\Default\Extensions\felcaaldnbdncclmgdcncolpebgiejap [2017-10-12]

CHR Extension: (Google Docs hors connexion) - C:\Users\Cirile\AppData\Local\Google\Chrome\User Data\Default\Extensions\ghbmnnjooekpmoecnnnilnnbdlolhkhi [2016-12-19]

CHR Extension: (Yahoo Partner) - C:\Users\Cirile\AppData\Local\Google\Chrome\User Data\Default\Extensions\ibbfklbaljofpaanmpaeadejijfdddco [2018-06-04]

CHR Extension: (Paiements via le Chrome Web Store) - C:\Users\Cirile\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda [2018-06-03]

CHR Extension: (Gmail) - C:\Users\Cirile\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia [2016-12-19]

CHR Extension: (Chrome Media Router) - C:\Users\Cirile\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm [2018-06-20]

CHR HKU\S-1-5-21-3539592496-772588293-4036759407-1002\SOFTWARE\Google\Chrome\Extensions\...\Chrome\Extension: [chfdnecihphmhljaaejmgoiahnihplgn] - hxxps://clients2.google.com/service/update2/crx

CHR HKLM-x32\...\Chrome\Extension: [ibbfklbaljofpaanmpaeadejijfdddco] - hxxps://clients2.google.com/service/update2/crx

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

R2 Apple Mobile Device Service; C:\Program Files\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe [83768 2017-04-03] (Apple Inc.)

R2 AVG Antivirus; C:\Program Files (x86)\AVG\Antivirus\AVGSvc.exe [323512 2018-07-07] (AVG Technologies CZ, s.r.o.)

R3 avgbIDSAgent; C:\Program Files (x86)\AVG\Antivirus\x64\aswidsagenta.exe [7829784 2018-07-07] (AVG Technologies CZ, s.r.o.)

R2 avgsvc; C:\Program Files (x86)\AVG\Framework\Common\avgsvca.exe [1428264 2018-06-14] (AVG Technologies CZ, s.r.o.)

R3 hpqcaslwmiex; C:\Program Files (x86)\HP\Shared\hpqwmiex.exe [1031704 2016-06-03] (HP)

R2 HPSupportSolutionsFrameworkService; C:\Program Files (x86)\Hewlett-Packard\HP Support Solutions\HPSupportSolutionsFrameworkService.exe [333688 2018-06-13] (HP Inc.)

R2 HPTouchpointAnalyticsService; C:\Program Files\HP\HP Touchpoint Analytics Client\TouchpointAnalyticsClientService.exe [332216 2017-11-22] (HP Inc.)

R2 igfxCUIService1.0.0.0; C:\WINDOWS\system32\igfxCUIService.exe [314696 2014-05-27] (Intel Corporation)

R2 Intel(R) ME Service; C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\FWService\IntelMeFWService.exe [128896 2012-07-18] (Intel Corporation)

R2 jhi\_service; C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\DAL\jhi\_service.exe [165760 2012-07-18] (Intel Corporation)

R2 jswpbapi; C:\Program Files (x86)\NETGEAR\WNA1100\jswpbapi.exe [241664 2012-03-26] (Atheros Communications, Inc.) [Fichier non signé]

S3 jswpsapi; C:\Program Files (x86)\NETGEAR\WNA1100\jswpsapi.exe [1102848 2012-03-26] (Atheros Communications, Inc.) [Fichier non signé]

R2 MBAMService; C:\Program Files\Malwarebytes\Anti-Malware\mbamservice.exe [6541008 2018-05-09] (Malwarebytes)

S3 PDF Architect 4; C:\Program Files\PDF Architect 4\ws.exe [2438880 2016-08-05] (pdfforge GmbH)

S3 PDF Architect 4 CrashHandler; C:\Program Files\PDF Architect 4\crash-handler-ws.exe [1038048 2016-08-05] (pdfforge GmbH)

R2 PDF Architect 4 Creator; C:\Program Files\PDF Architect 4\creator-ws.exe [851168 2016-08-05] (pdfforge GmbH)

R2 PDF Architect 4 Manager; C:\ProgramData\pdfforge\PDF Architect 4 Manager\PDF Architect 4\Architect Manager.exe [972056 2016-05-18] (Â© pdfforge GmbH.)

R2 RtkAudioService; C:\Program Files\Realtek\Audio\HDA\RtkAudioService64.exe [289496 2017-01-03] (Realtek Semiconductor)

R2 TuneUp.UtilitiesSvc; C:\Program Files (x86)\AVG\AVG PC TuneUp\TuneUpUtilitiesService64.exe [5614592 2018-01-22] (AVG Technologies CZ, s.r.o.)

S3 WdNisSvc; C:\Program Files\Windows Defender\NisSrv.exe [361824 2017-01-12] (Microsoft Corporation)

S3 WinDefend; C:\Program Files\Windows Defender\MsMpEng.exe [119872 2017-01-12] (Microsoft Corporation)

R2 WSWNA1100; C:\Program Files (x86)\NETGEAR\WNA1100\WifiSvc.exe [307928 2013-11-11] ()

R2 YSearchUtilSvc; C:\Program Files (x86)\Yahoo!\yset\{CBF3F570-CBCE-6D4F-9BD0-9F3C47D2AFB7}\YSearchUtilSvc.exe [182736 2017-03-21] (Yahoo Inc.)

R2 NVDisplay.ContainerLocalSystem; "C:\Program Files\NVIDIA Corporation\Display.NvContainer\NVDisplay.Container.exe" -s NVDisplay.ContainerLocalSystem -f "C:\ProgramData\NVIDIA\NVDisplay.ContainerLocalSystem.log" -l 3 -d "C:\Program Files\NVIDIA Corporation\Display.NvContainer\plugins\LocalSystem" -r -p 30000

===================== Pilotes (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.)

R3 athur; C:\WINDOWS\system32\DRIVERS\athuw8x.sys [3301888 2013-04-15] (Qualcomm Atheros Communications, Inc.)

R1 avgArPot; C:\WINDOWS\System32\drivers\avgArPot.sys [189544 2018-07-07] (AVG Technologies CZ, s.r.o.)

R1 avgbidsdriver; C:\WINDOWS\System32\drivers\avgbidsdrivera.sys [222288 2018-07-07] (AVG Technologies CZ, s.r.o.)

R0 avgbidsh; C:\WINDOWS\System32\drivers\avgbidsha.sys [194224 2018-07-07] (AVG Technologies CZ, s.r.o.)

R0 avgblog; C:\WINDOWS\System32\drivers\avgbloga.sys [339048 2018-07-07] (AVG Technologies CZ, s.r.o.)

R0 avgbuniv; C:\WINDOWS\System32\drivers\avgbuniva.sys [51952 2018-07-07] (AVG Technologies CZ, s.r.o.)

S3 avgHwid; C:\WINDOWS\System32\drivers\avgHwid.sys [39352 2018-07-07] (AVG Technologies CZ, s.r.o.)

R2 avgMonFlt; C:\WINDOWS\System32\drivers\avgMonFlt.sys [152016 2018-07-07] (AVG Technologies CZ, s.r.o.)

R1 avgRdr; C:\WINDOWS\System32\drivers\avgRdr2.sys [104256 2018-07-07] (AVG Technologies CZ, s.r.o.)

R0 avgRvrt; C:\WINDOWS\System32\drivers\avgRvrt.sys [78352 2018-07-07] (AVG Technologies CZ, s.r.o.)

R1 avgSnx; C:\WINDOWS\System32\drivers\avgSnx.sys [1020112 2018-07-07] (AVG Technologies CZ, s.r.o.)

R1 avgSP; C:\WINDOWS\System32\drivers\avgSP.sys [455464 2018-07-07] (AVG Technologies CZ, s.r.o.)

R2 avgStm; C:\WINDOWS\System32\drivers\avgStm.sys [203544 2018-07-07] (AVG Technologies CZ, s.r.o.)

R0 avgVmm; C:\WINDOWS\System32\drivers\avgVmm.sys [373944 2018-07-07] (AVG Technologies CZ, s.r.o.)

R1 CLVirtualDrive; C:\WINDOWS\system32\DRIVERS\CLVirtualDrive.sys [92536 2012-06-25] (CyberLink)

R3 MBAMSwissArmy; C:\WINDOWS\System32\Drivers\mbamswissarmy.sys [253664 2018-07-12] (Malwarebytes)

S3 PVUSB; C:\WINDOWS\System32\drivers\CESG64.sys [63808 2007-02-19] (CASIO COMPUTER CO.,LTD.)

R3 TuneUpUtilitiesDrv; C:\Program Files (x86)\AVG\AVG PC TuneUp\TuneUpUtilitiesDriver64.sys [32304 2017-02-21] (AVG Netherlands B.V.)

S3 WdBoot; C:\WINDOWS\system32\drivers\WdBoot.sys [46600 2017-02-10] (Microsoft Corporation)

S3 WdFilter; C:\WINDOWS\system32\drivers\WdFilter.sys [274776 2017-01-12] (Microsoft Corporation)

S3 WdNisDrv; C:\WINDOWS\System32\Drivers\WdNisDrv.sys [117592 2017-01-12] (Microsoft Corporation)

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

==================== Un mois - Créés - fichiers et dossiers ========

(Si un élément est inclus dans le fichier fixlist.txt, le fichier/dossier sera déplacé.)

2018-07-16 23:26 - 2018-07-16 23:29 - 000000000 \_\_\_\_D C:\FRST

2018-07-16 23:19 - 2018-07-16 23:19 - 000026101 \_\_\_\_\_ C:\Users\Cirile\Desktop\MONPC.speccy

2018-07-16 23:12 - 2018-07-16 23:12 - 000000815 \_\_\_\_\_ C:\Users\Public\Desktop\Speccy.lnk

2018-07-16 23:12 - 2018-07-16 23:12 - 000000000 \_\_\_\_D C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Speccy

2018-07-16 23:12 - 2018-07-16 23:12 - 000000000 \_\_\_\_D C:\Program Files\Speccy

2018-07-12 13:25 - 2018-07-12 13:25 - 000011505 \_\_\_\_\_ C:\Users\Cirile\Desktop\mondial relay.pdf

2018-07-12 13:24 - 2018-07-12 13:24 - 000011505 \_\_\_\_\_ C:\Users\Cirile\Downloads\Etiquettes-FV33805396.pdf

2018-07-12 10:53 - 2018-06-29 00:07 - 000835064 \_\_\_\_\_ (Adobe Systems Incorporated) C:\WINDOWS\SysWOW64\FlashPlayerApp.exe

2018-07-12 10:53 - 2018-06-29 00:07 - 000179704 \_\_\_\_\_ (Adobe Systems Incorporated) C:\WINDOWS\SysWOW64\FlashPlayerCPLApp.cpl

2018-07-11 22:04 - 2018-07-11 22:04 - 000037976 \_\_\_\_\_ C:\Users\Cirile\Downloads\ticket\_5625\_20180711193503.pdf

2018-07-11 02:21 - 2018-06-20 22:01 - 007398232 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\ntoskrnl.exe

2018-07-11 02:21 - 2018-06-20 21:44 - 001676064 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\winload.efi

2018-07-11 02:21 - 2018-06-20 21:44 - 001536120 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\winload.exe

2018-07-11 02:21 - 2018-06-20 20:48 - 000095744 \_\_\_\_C (Microsoft Corporation) C:\WINDOWS\system32\Drivers\amdk8.sys

2018-07-11 02:21 - 2018-06-20 20:48 - 000027136 \_\_\_\_C (Microsoft Corporation) C:\WINDOWS\system32\Drivers\fxppm.sys

2018-07-11 02:21 - 2018-06-20 18:58 - 000098816 \_\_\_\_C (Microsoft Corporation) C:\WINDOWS\system32\Drivers\intelppm.sys

2018-07-11 02:21 - 2018-06-20 18:58 - 000098816 \_\_\_\_C (Microsoft Corporation) C:\WINDOWS\system32\Drivers\amdppm.sys

2018-07-11 02:21 - 2018-06-20 18:58 - 000092672 \_\_\_\_C (Microsoft Corporation) C:\WINDOWS\system32\Drivers\processr.sys

2018-07-11 02:21 - 2018-06-15 05:01 - 004169216 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\win32k.sys

2018-07-11 02:21 - 2018-06-12 10:00 - 022374248 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\shell32.dll

2018-07-11 02:21 - 2018-06-12 09:57 - 019790760 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\shell32.dll

2018-07-11 02:21 - 2018-06-11 18:55 - 025744896 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\mshtml.dll

2018-07-11 02:21 - 2018-06-11 18:36 - 003119616 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\ExplorerFrame.dll

2018-07-11 02:21 - 2018-06-11 18:14 - 000576512 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\vbscript.dll

2018-07-11 02:21 - 2018-06-11 18:06 - 005779968 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\jscript9.dll

2018-07-11 02:21 - 2018-06-11 18:04 - 000794624 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\jscript.dll

2018-07-11 02:21 - 2018-06-11 17:39 - 001033216 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\inetcomm.dll

2018-07-11 02:21 - 2018-06-11 17:36 - 015283200 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\ieframe.dll

2018-07-11 02:21 - 2018-06-11 17:31 - 000809472 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\msfeeds.dll

2018-07-11 02:21 - 2018-06-11 17:22 - 003241472 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\wininet.dll

2018-07-11 02:21 - 2018-06-11 17:11 - 001545216 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\urlmon.dll

2018-07-11 02:21 - 2018-06-11 16:59 - 000800768 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\ieapfltr.dll

2018-07-11 02:21 - 2018-06-09 18:40 - 020286976 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\mshtml.dll

2018-07-11 02:21 - 2018-06-09 18:26 - 002712064 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\ExplorerFrame.dll

2018-07-11 02:21 - 2018-06-09 18:09 - 000498176 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\vbscript.dll

2018-07-11 02:21 - 2018-06-09 17:59 - 000662016 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\jscript.dll

2018-07-11 02:21 - 2018-06-09 17:37 - 004496384 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\jscript9.dll

2018-07-11 02:21 - 2018-06-09 17:37 - 000880640 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\inetcomm.dll

2018-07-11 02:21 - 2018-06-09 17:36 - 013680128 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\ieframe.dll

2018-07-11 02:21 - 2018-06-09 17:32 - 000696320 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\msfeeds.dll

2018-07-11 02:21 - 2018-06-09 17:11 - 002767872 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\wininet.dll

2018-07-11 02:21 - 2018-06-09 17:08 - 001313792 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\urlmon.dll

2018-07-11 02:21 - 2018-06-09 17:06 - 000710144 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\ieapfltr.dll

2018-07-11 02:21 - 2018-06-09 04:47 - 002176072 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\combase.dll

2018-07-11 02:21 - 2018-06-09 03:44 - 001565528 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\combase.dll

2018-07-11 02:21 - 2018-06-08 20:26 - 000440832 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\zipfldr.dll

2018-07-11 02:21 - 2018-06-08 19:54 - 000656384 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\dnsapi.dll

2018-07-11 02:21 - 2018-06-08 19:53 - 000252416 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\dnsrslvr.dll

2018-07-11 02:21 - 2018-06-08 19:07 - 000404992 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\zipfldr.dll

2018-07-11 02:21 - 2018-06-08 18:44 - 000499200 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\dnsapi.dll

2018-07-11 02:21 - 2018-06-07 20:51 - 000074240 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\Drivers\mpsdrv.sys

2018-07-11 02:21 - 2018-05-24 23:29 - 002449752 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\Drivers\tcpip.sys

2018-07-11 02:21 - 2018-05-24 23:29 - 000428888 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\Drivers\FWPKCLNT.SYS

2018-07-11 02:21 - 2018-05-15 10:42 - 000590680 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\Drivers\fvevol.sys

2018-07-11 02:21 - 2018-05-04 01:02 - 000439640 \_\_\_\_C (Microsoft Corporation) C:\WINDOWS\system32\Drivers\usbport.sys

2018-07-11 02:21 - 2018-05-04 01:02 - 000325456 \_\_\_\_C (Microsoft Corporation) C:\WINDOWS\system32\Drivers\USBXHCI.SYS

2018-07-11 02:21 - 2018-05-04 01:02 - 000187728 \_\_\_\_C (Microsoft Corporation) C:\WINDOWS\system32\Drivers\UCX01000.SYS

2018-07-11 02:21 - 2018-04-26 15:43 - 000918296 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\ucrtbase.dll

2018-07-11 02:21 - 2018-04-26 15:43 - 000065880 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\api-ms-win-crt-private-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:43 - 000021848 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\api-ms-win-crt-math-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:43 - 000018776 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\api-ms-win-crt-multibyte-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:43 - 000017240 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\api-ms-win-crt-string-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:43 - 000017240 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\api-ms-win-crt-stdio-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:43 - 000015704 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\api-ms-win-crt-runtime-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:43 - 000015192 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\api-ms-win-crt-convert-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:43 - 000013656 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\api-ms-win-crt-time-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:43 - 000013152 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\api-ms-win-crt-filesystem-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:43 - 000012120 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\api-ms-win-crt-process-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:43 - 000012120 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\api-ms-win-crt-conio-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:43 - 000011608 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\api-ms-win-crt-utility-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:43 - 000011608 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\api-ms-win-crt-locale-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:43 - 000011608 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\api-ms-win-crt-heap-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:43 - 000011608 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\SysWOW64\api-ms-win-crt-environment-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:19 - 000998912 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\ucrtbase.dll

2018-07-11 02:21 - 2018-04-26 15:19 - 000063832 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\api-ms-win-crt-private-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:19 - 000020824 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\api-ms-win-crt-math-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:19 - 000019288 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\api-ms-win-crt-multibyte-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:19 - 000017752 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\api-ms-win-crt-string-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:19 - 000017752 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\api-ms-win-crt-stdio-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:19 - 000016216 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\api-ms-win-crt-runtime-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:19 - 000015704 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\api-ms-win-crt-convert-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:19 - 000014168 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\api-ms-win-crt-time-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:19 - 000013656 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\api-ms-win-crt-filesystem-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:19 - 000012640 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\api-ms-win-crt-conio-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:19 - 000012632 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\api-ms-win-crt-process-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:19 - 000012120 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\api-ms-win-crt-utility-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:19 - 000012120 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\api-ms-win-crt-locale-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:19 - 000012120 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\api-ms-win-crt-heap-l1-1-0.dll

2018-07-11 02:21 - 2018-04-26 15:19 - 000012120 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\api-ms-win-crt-environment-l1-1-0.dll

2018-07-11 02:21 - 2018-04-25 19:38 - 000243200 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\Drivers\srvnet.sys

2018-07-11 02:10 - 2018-06-12 21:01 - 000149632 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\CompatTelRunner.exe

2018-07-11 02:10 - 2018-06-08 15:15 - 002860032 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\aitstatic.exe

2018-07-11 02:10 - 2018-06-08 15:15 - 001602048 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\appraiser.dll

2018-07-11 02:10 - 2018-06-08 15:15 - 000783872 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\generaltel.dll

2018-07-11 02:10 - 2018-06-08 15:15 - 000680960 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\aeinv.dll

2018-07-11 02:10 - 2018-06-08 15:15 - 000612352 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\devinv.dll

2018-07-11 02:10 - 2018-06-08 15:15 - 000470016 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\centel.dll

2018-07-11 02:10 - 2018-06-08 15:15 - 000443392 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\invagent.dll

2018-07-11 02:10 - 2018-06-08 15:15 - 000301056 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\acmigration.dll

2018-07-11 02:10 - 2018-06-08 15:15 - 000246272 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\aepic.dll

2018-07-08 22:17 - 2018-07-08 22:17 - 000161367 \_\_\_\_\_ C:\Users\Cirile\Downloads\CONSIGNES HFA secteur RN (3).pdf

2018-07-07 14:21 - 2018-07-07 14:21 - 000144554 \_\_\_\_\_ C:\Users\Cirile\Downloads\eTicket\_546830841.pdf

2018-07-07 14:21 - 2018-07-07 14:21 - 000144554 \_\_\_\_\_ C:\Users\Cirile\Downloads\eTicket\_546830841 (5).pdf

2018-07-07 14:21 - 2018-07-07 14:21 - 000144554 \_\_\_\_\_ C:\Users\Cirile\Downloads\eTicket\_546830841 (4).pdf

2018-07-07 14:21 - 2018-07-07 14:21 - 000144554 \_\_\_\_\_ C:\Users\Cirile\Downloads\eTicket\_546830841 (3).pdf

2018-07-07 14:21 - 2018-07-07 14:21 - 000144554 \_\_\_\_\_ C:\Users\Cirile\Downloads\eTicket\_546830841 (2).pdf

2018-07-07 14:21 - 2018-07-07 14:21 - 000144554 \_\_\_\_\_ C:\Users\Cirile\Downloads\eTicket\_546830841 (1).pdf

2018-07-07 14:21 - 2018-07-07 14:21 - 000144418 \_\_\_\_\_ C:\Users\Cirile\Downloads\eTicket\_548397334 (1).pdf

2018-07-07 14:19 - 2018-07-07 14:19 - 000144418 \_\_\_\_\_ C:\Users\Cirile\Downloads\eTicket\_548397334.pdf

2018-07-07 12:53 - 2018-07-07 12:52 - 000379120 \_\_\_\_\_ (AVG Technologies CZ, s.r.o.) C:\WINDOWS\system32\avgBoot.exe

2018-07-05 20:11 - 2018-07-05 20:11 - 000211041 \_\_\_\_\_ C:\Users\Cirile\Downloads\QE AESH - Ministère de l'Education nationale.pdf

2018-06-28 22:29 - 2018-06-28 22:29 - 000010068 \_\_\_\_\_ C:\Users\Cirile\Documents\cc\_20180628\_222909juin 2018.reg

2018-06-20 21:29 - 2018-06-20 21:29 - 018305443 \_\_\_\_\_ C:\Users\Cirile\Downloads\fa124\_2\_win (1).zip

2018-06-20 21:29 - 2018-06-20 21:29 - 000002023 \_\_\_\_\_ C:\Users\Public\Desktop\CASIO FA-124.lnk

2018-06-20 21:29 - 2018-06-20 21:29 - 000000000 \_\_\_\_D C:\ProgramData\Microsoft\Windows\Start Menu\Programs\CASIO

2018-06-20 21:29 - 2018-06-20 21:29 - 000000000 \_\_\_\_D C:\Program Files (x86)\CASIO

2018-06-20 21:05 - 2018-06-20 21:05 - 000000000 \_\_\_\_D C:\Users\Cirile\Documents\CASIO

2018-06-19 21:20 - 2018-06-19 21:20 - 000000000 \_\_\_\_D C:\Users\Cirile\AppData\Local\Downloaded Installations

2018-06-19 21:19 - 2018-06-19 21:20 - 018305443 \_\_\_\_\_ C:\Users\Cirile\Downloads\fa124\_2\_win.zip

==================== Un mois - Modifiés - fichiers et dossiers ========

(Si un élément est inclus dans le fichier fixlist.txt, le fichier/dossier sera déplacé.)

2018-07-16 22:17 - 2016-12-24 13:30 - 000003928 \_\_\_\_\_ C:\WINDOWS\System32\Tasks\User\_Feed\_Synchronization-{6DCC6368-7874-4E8A-B5FF-34458E0EDA5A}

2018-07-16 20:20 - 2013-08-22 15:36 - 000000000 \_\_\_\_D C:\WINDOWS\Inf

2018-07-16 19:01 - 2017-11-21 14:39 - 000003164 \_\_\_\_\_ C:\WINDOWS\System32\Tasks\HPCeeScheduleForCirile

2018-07-16 19:01 - 2017-11-21 14:39 - 000000348 \_\_\_\_\_ C:\WINDOWS\Tasks\HPCeeScheduleForCirile.job

2018-07-16 15:55 - 2017-02-24 14:06 - 000003866 \_\_\_\_\_ C:\WINDOWS\System32\Tasks\Opera scheduled Autoupdate 1482112993

2018-07-16 15:55 - 2016-12-19 04:03 - 000000000 \_\_\_\_D C:\Program Files (x86)\Opera

2018-07-16 15:50 - 2013-09-27 06:15 - 000000000 \_\_\_\_D C:\ProgramData\NVIDIA

2018-07-16 00:43 - 2016-12-19 03:19 - 000003600 \_\_\_\_\_ C:\WINDOWS\System32\Tasks\AVG EUpdate Task

2018-07-14 15:08 - 2016-12-19 03:00 - 000003598 \_\_\_\_\_ C:\WINDOWS\System32\Tasks\Optimize Start Menu Cache Files-S-1-5-21-3539592496-772588293-4036759407-1002

2018-07-14 10:48 - 2013-08-22 17:36 - 000000000 \_\_\_HD C:\Program Files\WindowsApps

2018-07-14 10:48 - 2013-08-22 17:36 - 000000000 \_\_\_\_D C:\WINDOWS\AppReadiness

2018-07-12 11:40 - 2013-08-22 17:36 - 000000000 \_\_\_\_D C:\WINDOWS\rescache

2018-07-12 10:57 - 2014-11-21 00:46 - 002018128 \_\_\_\_\_ C:\WINDOWS\system32\PerfStringBackup.INI

2018-07-12 10:57 - 2014-11-21 00:03 - 000879470 \_\_\_\_\_ C:\WINDOWS\system32\perfh00C.dat

2018-07-12 10:57 - 2014-11-21 00:03 - 000188954 \_\_\_\_\_ C:\WINDOWS\system32\perfc00C.dat

2018-07-12 10:53 - 2018-06-08 19:48 - 000253664 \_\_\_\_\_ (Malwarebytes) C:\WINDOWS\system32\Drivers\mbamswissarmy.sys

2018-07-12 10:52 - 2013-08-22 16:45 - 000000006 \_\_\_\_H C:\WINDOWS\Tasks\SA.DAT

2018-07-12 10:52 - 2013-08-22 16:44 - 000516384 \_\_\_\_\_ C:\WINDOWS\system32\FNTCACHE.DAT

2018-07-12 01:19 - 2013-08-22 15:25 - 000262144 \_\_\_SH C:\WINDOWS\system32\config\BBI

2018-07-12 01:16 - 2017-03-18 15:56 - 000000000 \_\_\_\_D C:\WINDOWS\system32\appraiser

2018-07-12 01:16 - 2013-08-22 17:36 - 000000000 \_\_\_RD C:\WINDOWS\ToastData

2018-07-11 05:28 - 2012-07-26 09:59 - 000000000 \_\_\_\_D C:\WINDOWS\CbsTemp

2018-07-11 05:25 - 2016-12-20 15:15 - 000000000 \_\_\_\_D C:\WINDOWS\system32\MRT

2018-07-11 05:23 - 2016-12-20 15:14 - 134675576 \_\_\_\_C (Microsoft Corporation) C:\WINDOWS\system32\MRT.exe

2018-07-11 02:08 - 2018-05-09 13:39 - 000685568 \_\_\_\_\_ (Microsoft Corporation) C:\WINDOWS\system32\Drivers\srv2.sys

2018-07-10 16:28 - 2016-12-31 00:53 - 000004594 \_\_\_\_\_ C:\WINDOWS\System32\Tasks\Adobe Flash Player PPAPI Notifier

2018-07-10 16:28 - 2016-12-24 00:44 - 000004460 \_\_\_\_\_ C:\WINDOWS\System32\Tasks\Adobe Flash Player Updater

2018-07-10 16:28 - 2013-08-22 17:36 - 000000000 \_\_\_\_D C:\WINDOWS\SysWOW64\Macromed

2018-07-10 16:28 - 2013-08-22 17:36 - 000000000 \_\_\_\_D C:\WINDOWS\system32\Macromed

2018-07-10 14:53 - 2018-03-14 16:25 - 000004630 \_\_\_\_\_ C:\WINDOWS\System32\Tasks\Adobe Flash Player NPAPI Notifier

2018-07-07 17:11 - 2017-03-12 19:49 - 000004174 \_\_\_\_\_ C:\WINDOWS\System32\Tasks\Antivirus Emergency Update

2018-07-07 13:39 - 2017-05-22 17:07 - 000007604 \_\_\_\_\_ C:\Users\Cirile\AppData\Local\resmon.resmoncfg

2018-07-07 12:52 - 2017-11-27 17:57 - 000189544 \_\_\_\_\_ (AVG Technologies CZ, s.r.o.) C:\WINDOWS\system32\Drivers\avgArPot.sys

2018-07-07 12:52 - 2017-03-12 19:48 - 001020112 \_\_\_\_\_ (AVG Technologies CZ, s.r.o.) C:\WINDOWS\system32\Drivers\avgSnx.sys

2018-07-07 12:52 - 2017-03-12 19:48 - 000455464 \_\_\_\_\_ (AVG Technologies CZ, s.r.o.) C:\WINDOWS\system32\Drivers\avgSP.sys

2018-07-07 12:52 - 2017-03-12 19:48 - 000373944 \_\_\_\_\_ (AVG Technologies CZ, s.r.o.) C:\WINDOWS\system32\Drivers\avgVmm.sys

2018-07-07 12:52 - 2017-03-12 19:48 - 000339048 \_\_\_\_\_ (AVG Technologies CZ, s.r.o.) C:\WINDOWS\system32\Drivers\avgbloga.sys

2018-07-07 12:52 - 2017-03-12 19:48 - 000222288 \_\_\_\_\_ (AVG Technologies CZ, s.r.o.) C:\WINDOWS\system32\Drivers\avgbidsdrivera.sys

2018-07-07 12:52 - 2017-03-12 19:48 - 000203544 \_\_\_\_\_ (AVG Technologies CZ, s.r.o.) C:\WINDOWS\system32\Drivers\avgStm.sys

2018-07-07 12:52 - 2017-03-12 19:48 - 000194224 \_\_\_\_\_ (AVG Technologies CZ, s.r.o.) C:\WINDOWS\system32\Drivers\avgbidsha.sys

2018-07-07 12:52 - 2017-03-12 19:48 - 000152016 \_\_\_\_\_ (AVG Technologies CZ, s.r.o.) C:\WINDOWS\system32\Drivers\avgMonFlt.sys

2018-07-07 12:52 - 2017-03-12 19:48 - 000104256 \_\_\_\_\_ (AVG Technologies CZ, s.r.o.) C:\WINDOWS\system32\Drivers\avgRdr2.sys

2018-07-07 12:52 - 2017-03-12 19:48 - 000078352 \_\_\_\_\_ (AVG Technologies CZ, s.r.o.) C:\WINDOWS\system32\Drivers\avgRvrt.sys

2018-07-07 12:52 - 2017-03-12 19:48 - 000051952 \_\_\_\_\_ (AVG Technologies CZ, s.r.o.) C:\WINDOWS\system32\Drivers\avgbuniva.sys

2018-07-07 12:52 - 2017-03-12 19:48 - 000039352 \_\_\_\_\_ (AVG Technologies CZ, s.r.o.) C:\WINDOWS\system32\Drivers\avgHwid.sys

2018-06-26 21:48 - 2016-12-19 04:08 - 000002249 \_\_\_\_\_ C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Google Chrome.lnk

2018-06-26 21:48 - 2016-12-19 04:08 - 000002208 \_\_\_\_\_ C:\Users\Public\Desktop\Google Chrome.lnk

2018-06-20 21:18 - 2016-12-19 02:41 - 000000000 \_\_\_\_D C:\Users\Cirile\AppData\Local\VirtualStore

==================== Fichiers à la racine de certains dossiers =======

2017-05-22 17:07 - 2018-07-07 13:39 - 000007604 \_\_\_\_\_ () C:\Users\Cirile\AppData\Local\resmon.resmoncfg

==================== Bamital & volsnap ======================

(Il n'y a pas de correction automatique pour les fichiers qui ne satisfont pas à la vérification.)

C:\WINDOWS\system32\winlogon.exe => Le fichier est signé numériquement

C:\WINDOWS\system32\wininit.exe => Le fichier est signé numériquement

C:\WINDOWS\explorer.exe => Le fichier est signé numériquement

C:\WINDOWS\SysWOW64\explorer.exe => Le fichier est signé numériquement

C:\WINDOWS\system32\svchost.exe => Le fichier est signé numériquement

C:\WINDOWS\SysWOW64\svchost.exe => Le fichier est signé numériquement

C:\WINDOWS\system32\services.exe => Le fichier est signé numériquement

C:\WINDOWS\system32\User32.dll => Le fichier est signé numériquement

C:\WINDOWS\SysWOW64\User32.dll => Le fichier est signé numériquement

C:\WINDOWS\system32\userinit.exe => Le fichier est signé numériquement

C:\WINDOWS\SysWOW64\userinit.exe => Le fichier est signé numériquement

C:\WINDOWS\system32\rpcss.dll => Le fichier est signé numériquement

C:\WINDOWS\system32\dnsapi.dll => Le fichier est signé numériquement

C:\WINDOWS\SysWOW64\dnsapi.dll => Le fichier est signé numériquement

C:\WINDOWS\system32\Drivers\volsnap.sys => Le fichier est signé numériquement

LastRegBack: 2018-07-12 11:03

==================== Fin de FRST.txt ============================