Additional scan result of Farbar Recovery Scan Tool (x64) Version: 14.01.2019 01
Ran by o (15-01-2019 16:39:25)
Running from C:\Users\o\Downloads
Windows 10 Home Version 1809 17763.253 (X64) (2018-10-03 14:28:58)
Boot Mode: Normal
==========

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

Administrator (S-1-5-21-2671679121-1364000227-736312402-500 - Administrator - Disabled)
DefaultAccount (S-1-5-21-2671679121-1364000227-736312402-503 - Limited - Disabled)
Guest (S-1-5-21-2671679121-1364000227-736312402-501 - Limited - Disabled)
o (S-1-5-21-2671679121-1364000227-736312402-1003 - Administrator - Enabled) => C:\Users\o
OEM (S-1-5-21-2671679121-1364000227-736312402-1001 - Administrator - Enabled) => C:\Users\OEM
WDAGUtilityAccount (S-1-5-21-2671679121-1364000227-736312402-504 - Limited - Disabled)

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

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

AV: Windows Defender (Disabled - Up to date) {D68DDC3A-831F-4fae-9E44-DA132C1ACF46}
AV: ESET Security (Enabled - Up to date) {EC1D6F37-E411-475A-DF50-12FF7FE4AC70}
AS: ESET Security (Enabled - Up to date) {577C8ED3-C22B-48D4-E5E0-298D0463E6CD}
AS: Windows Defender (Disabled - Up to date) {D68DDC3A-831F-4fae-9E44-DA132C1ACF46}
FW: ESET Firewall (Enabled) {D426EE12-AE7E-4602-F40F-BBCA8137EB0B}

========== 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 Acrobat Reader DC - Czech (HKLM-x32\...\{AC76BA86-7AD7-1029-7B44-AC0F074E4100}) (Version: 19.010.20069 - Adobe Systems Incorporated)
Canon Utilities Digital Photo Professional (HKLM-x32\...\Digital Photo Professional) (Version: 3.13.10.0 - Canon Inc.)
Canon Utilities EOS Sample Music (HKLM-x32\...\EOS Sample Music) (Version: 1.0.1.1 - Canon Inc.)
Canon Utilities EOS Utility (HKLM-x32\...\EOS Utility) (Version: 2.13.10.0 - Canon Inc.)
Canon Utilities ImageBrowser EX (HKLM-x32\...\ImageBrowser EX) (Version: 1.5.2.8 - Canon Inc.)
Canon Utilities PhotoStitch (HKLM-x32\...\PhotoStitch) (Version: 3.1.23.47 - Canon Inc.)
Canon Utilities Picture Style Editor (HKLM-x32\...\Picture Style Editor) (Version: 1.13.10.0 - Canon Inc.)
Canon Utilities Uploader for CANON iMAGE GATEWAY (HKLM-x32\...\Uploader for CANON iMAGE GATEWAY Plugin) (Version: 10.0.1.2 - Canon Inc.)
CCleaner (HKLM\...\CCleaner) (Version: 5.51 - Piriform)
Double Commander 0.8.4 beta (HKLM\...\Double Commander_is1) (Version: -)
eM Client (HKLM-x32\...\{EFE5C7F6-0061-4E14-B7D2-C50457FAAEA6}) (Version: 7.2.33988.0 - eM Client Inc.)
ESET Security (HKLM\...\{C26AA376-9D1B-4B7B-A1F0-DC41E8530176}) (Version: 11.2.49.0 -

ESET, spol. s r.o.)
Google Chrome (HKLM-x32\...\Google Chrome) (Version: 71.0.3578.98 - Google Inc.)
Google Update Helper (HKLM-x32\...\{60EC980A-BDA2-4CB6-A427-B07A5498B4CA}) (Version: 1.3.33.23 - Google Inc.) Hidden
Google Update Helper (HKLM-x32\...\{A92DAB39-4E2C-4304-9AB6-BC44E68B55E2}) (Version: 1.3.21.169 - Google Inc.) Hidden
HP DeskJet 5820 series Nápověda (HKLM-x32\...\{89D0B45E-D5AC-4B97-9C7D-6F0D2308A0CA}) (Version: 36.0.0 - HP)
HP Dropbox Plugin (HKLM-x32\...\{9FF252C8-B146-47A2-9336-3A1A83056F51}) (Version: 36.0.39.57346 - HP)
HP Google Drive Plugin (HKLM-x32\...\{BBF796CE-5068-47C7-8A6D-4120C0CE47E5}) (Version: 36.0.39.57346 - HP)
HP Photo Creations (HKLM-x32\...\HP Photo Creations) (Version: 1.0.0.9572 - HP)
Microsoft OneDrive (HKU\S-1-5-21-2671679121-1364000227-736312402-1003\...\OneDriveSetup.exe) (Version: 18.222.1104.0007 - Microsoft Corporation)
Microsoft Silverlight (HKLM\...\{89F4137D-6C26-4A84-BDB8-2E5A4BB71E00}) (Version: 5.1.50907.0 - Microsoft Corporation)
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161 (HKLM\...\{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}) (Version: 9.0.30729.6161 - Microsoft Corporation)
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (HKLM-x32\...\{9BE518E6-ECC6-35A9-88E4-87755C07200F}) (Version: 9.0.30729.6161 - Microsoft Corporation)
Microsoft Visual C++ 2017 Redistributable (x64) - 14.14.26429 (HKLM-x32\...\{80586c77-db42-44bb-bfc8-7aebbb220c00}) (Version: 14.14.26429.4 - Microsoft Corporation)
Mozilla Firefox 64.0.2 (x64 cs) (HKLM\...\Mozilla Firefox 64.0.2 (x64 cs)) (Version: 64.0.2 - Mozilla)
Mozilla Maintenance Service (HKLM\...\MozillaMaintenanceService) (Version: 61.0.1 - Mozilla)
OpenOffice 4.1.5 (HKLM-x32\...\{2FEA9841-64DE-4FA5-A36F-1CD23E2790EB}) (Version: 4.15.9789 - Apache Software Foundation)
Ovládací panel NVIDIA 398.36 (HKLM\...\{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_Display.ControlPanel) (Version: 398.36 - NVIDIA Corporation) Hidden
Realtek High Definition Audio Driver (HKLM-x32\...\{F132AF7F-7BCA-4EDE-8A7C-958108FE7DBC}) (Version: 6.0.1.7524 - Realtek Semiconductor Corp.)
Revo Uninstaller 2.0.6 (HKLM\...\{A28DBDA2-3CC7-4ADC-8BFE-66D7743C6C97}_is1) (Version: 2.0.6 - VS Revo Group, Ltd.)
Seznam Software (HKU\S-1-5-21-2671679121-1364000227-736312402-1003\...\SeznamInstall) (Version: 2.1.32 - Seznam.cz)
Spotify (HKU\S-1-5-21-2671679121-1364000227-736312402-1003\...\Spotify) (Version: 1.0.96.181.gf6bc1b6b - Spotify AB)
Studie vylepšování produktu HP DeskJet 5820 series (HKLM\...\{CAE450AC-801B-44FC-A200-0244F6AD5479}) (Version: 36.1.108.65692 - Hewlett-Packard Co.)
VLC media player (HKLM\...\VLC media player) (Version: 3.0.4 - VideoLAN)
WhatsApp (HKU\S-1-5-21-2671679121-1364000227-736312402-1003\...\WhatsApp) (Version: 0.3.1847 - WhatsApp)
Základní software zařízení HP DeskJet 5820 series (HKLM\...\{322E6CCD-0436-478E-A61B-EB11869234C3}) (Version: 36.1.108.65692 - Hewlett-Packard Co.)

========== 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.)

ContextMenuHandlers1: [7-Zip] -> {23170F69-40C1-278A-1000-000100020000} => -> No File

ContextMenuHandlers1: [ANotepad++64] -> {B298D29A-A6ED-11DE-BA8C-A68E55D89593} => -> No File
ContextMenuHandlers1: [BriefcaseMenu] -> {85BBD920-42A0-1069-A2E4-08002B30309D} => -> No File
ContextMenuHandlers1: [ESET Security Shell] -> {B089FE88-FB52-11D3-BDF1-0050DA34150D} => C:\Program Files\ESET\ESET Security\shellExt.dll [2018-12-05] (ESET)
ContextMenuHandlers2: [ESET Security Shell] -> {B089FE88-FB52-11D3-BDF1-0050DA34150D} => C:\Program Files\ESET\ESET Security\shellExt.dll [2018-12-05] (ESET)
ContextMenuHandlers3: [{4A7C4306-57E0-4C0C-83A9-78C1528F618C}] -> {4A7C4306-57E0-4C0C-83A9-78C1528F618C} => -> No File
ContextMenuHandlers4: [7-Zip] -> {23170F69-40C1-278A-1000-000100020000} => -> No File
ContextMenuHandlers4: [Offline Files] -> {474C98EE-CF3D-41f5-80E3-4AAB0AB04301} => -> No File
ContextMenuHandlers5: [NvCplDesktopContext] -> {3D1975AF-48C6-4f8e-A182-BE0E08FA86A9} => C:\WINDOWS\system32\nvshext.dll [2018-06-24] (NVIDIA Corporation)
ContextMenuHandlers6: [BriefcaseMenu] -> {85BBD920-42A0-1069-A2E4-08002B30309D} => -> No File
ContextMenuHandlers6: [ESET Security Shell] -> {B089FE88-FB52-11D3-BDF1-0050DA34150D} => C:\Program Files\ESET\ESET Security\shellExt.dll [2018-12-05] (ESET)
ContextMenuHandlers6: [Offline Files] -> {474C98EE-CF3D-41f5-80E3-4AAB0AB04301} => -> No File

========== 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: {11616A63-2794-4B78-A5E8-7FD59649BF21} - System32\Tasks\CCleaner Update => C:\Program Files\CCleaner\CCUpdate.exe [2018-12-10] (Piriform Ltd)
Task: {908F6C75-3F37-44AC-9B6F-7512DA2DE27E} - System32\Tasks\HPCustParticipation HP DeskJet 5820 series => C:\Program Files\HP\HP DeskJet 5820 series\Bin\HPCustPartic.exe [2016-08-04] (Hewlett-Packard Development Company, LP)
Task: {980BE6C9-83BA-4AD7-9157-A01F67784BBE} - System32\Tasks\CCleanerSkipUAC => C:\Program Files\CCleaner\CCleaner.exe [2018-12-10] (Piriform Software Ltd)
Task: {C066B677-8C84-4DCF-913E-D5C0BEA2829D} - System32\Tasks\GoogleUpdateTaskMachineCore => C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [2018-08-05] (Google Inc.)
Task: {C80FFEA1-EE6F-4240-83FF-F5D11F1571C6} - System32\Tasks\Adobe Acrobat Update Task => C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe [2018-08-13] (Adobe Systems Incorporated)
Task: {E39F8E32-F4B6-44B2-B8AF-D84A6CFEB7B8} - System32\Tasks\Microsoft\Windows\HelloFace\FODCleanupTask => C:\WINDOWS\System32\WinBioPlugIns\FaceFodUninstaller.exe [2018-09-15] ()
Task: {E7DF2A2A-E524-4370-BB02-B212AFD161E5} - System32\Tasks\GoogleUpdateTaskMachineUA => C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [2018-08-05] (Google Inc.)

(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.)

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

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

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

2018-08-05 14:15 - 2017-11-13 15:46 - 000092368 _____ ()
C:\Users\o\AppData\Roaming\Seznam.cz\bin\12542libfoxloader-x64.dll
2018-09-15 08:28 - 2018-09-15 08:28 - 000834088 _____ ()
C:\WINDOWS\SYSTEM32\inputhost.dll
2018-09-15 08:28 - 2018-09-15 08:28 - 000474624 _____ ()
C:\Windows\ShellExperiences\TileControl.dll
2018-12-12 06:53 - 2018-12-12 06:53 - 002801152 _____ ()
C:\Windows\ShellComponents\TaskFlowUI.dll
2018-09-15 08:28 - 2018-09-15 08:28 - 001740288 _____ ()
C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\Cortana.Core.dll
2018-12-08 12:14 - 2018-12-08 12:14 - 034870272 _____ () C:\Program
Files\WindowsApps\Microsoft.ZuneVideo_10.18102.12011.0_x64__8wekyb3d8bbwe\Video.UI.exe
2018-12-08 12:14 - 2018-12-08 12:14 - 000292352 _____ () C:\Program
Files\WindowsApps\Microsoft.ZuneVideo_10.18102.12011.0_x64__8wekyb3d8bbwe\SharedUI.dll
2018-04-12 16:57 - 2018-04-12 16:57 - 000902656 _____ () C:\Program
Files\WindowsApps\Microsoft.ZuneVideo_10.18102.12011.0_x64__8wekyb3d8bbwe\Microsoft.Membership.MeControl.UI.Xaml.dll
2018-11-29 17:18 - 2018-11-29 17:18 - 004202208 _____ () C:\Program
Files\WindowsApps\Microsoft.ZuneVideo_10.18102.12011.0_x64__8wekyb3d8bbwe\Microsoft.UI.Xaml.dll
2018-12-08 12:14 - 2018-12-08 12:14 - 005967872 _____ () C:\Program
Files\WindowsApps\Microsoft.ZuneVideo_10.18102.12011.0_x64__8wekyb3d8bbwe\EntCommon.dll
2018-12-08 12:14 - 2018-12-08 12:14 - 009072128 _____ () C:\Program
Files\WindowsApps\Microsoft.ZuneVideo_10.18102.12011.0_x64__8wekyb3d8bbwe\EntPlat.dll
2018-12-15 08:06 - 2018-12-15 08:09 - 000182272 _____ () C:\Program
Files\WindowsApps\Microsoft.SkypeApp_14.36.52.0_x64__kzf8qxf38zg5c\SkypeBackgroundHost.exe
2018-12-15 08:06 - 2018-12-15 08:09 - 000019456 _____ () C:\Program
Files\WindowsApps\Microsoft.SkypeApp_14.36.52.0_x64__kzf8qxf38zg5c\SkypeProxiesAndStubs.dll
2019-01-11 09:20 - 2019-01-11 09:20 - 005172224 _____ () C:\Program
Files\WindowsApps\Microsoft.YourPhone_1.0.20094.0_x64__8wekyb3d8bbwe\YourPhone.exe
2019-01-11 09:20 - 2019-01-11 09:20 - 002172928 _____ () C:\Program
Files\WindowsApps\Microsoft.YourPhone_1.0.20094.0_x64__8wekyb3d8bbwe\YourPhone.AppCore.dll
2019-01-11 09:20 - 2019-01-11 09:20 - 001795584 _____ () C:\Program
Files\WindowsApps\Microsoft.YourPhone_1.0.20094.0_x64__8wekyb3d8bbwe\PhoneContentDataStore.dll
2018-10-31 07:05 - 2018-10-31 07:06 - 001004032 _____ () C:\Program
Files\WindowsApps\Microsoft.YourPhone_1.0.20094.0_x64__8wekyb3d8bbwe\RuntimeConfiguration.dll
2019-01-11 09:20 - 2019-01-11 09:20 - 002907136 _____ () C:\Program
Files\WindowsApps\Microsoft.YourPhone_1.0.20094.0_x64__8wekyb3d8bbwe\PhoneCommunicationAppService.dll

2018-08-05 14:15 - 2017-11-13 15:38 - 000506064 _____ ()
C:\Users\o\AppData\Roaming\Seznam.cz\bin\szndesktop.exe
2018-08-05 14:15 - 2017-02-08 12:39 - 000080576 _____ ()
C:\Users\o\AppData\Roaming\Seznam.cz\bin\listicka-x64.exe
2012-08-30 12:46 - 2015-02-10 14:08 - 000069120 _____ () C:\Program Files
(x86)\Canon\ImageBrowser EX\MFManager.exe
2018-12-10 11:09 - 2018-12-10 11:09 - 000093648 _____ () C:\Program Files\CCleaner\lang\lang-
1029.dll
2018-11-06 07:16 - 2018-11-06 07:16 - 000194048 _____ () C:\Program
Files\WindowsApps\Microsoft.WindowsStore_11810.1001.12.0_x64__8wekyb3d8bbwe\WinStore.
Preview.dll
2018-11-06 07:16 - 2018-11-06 07:16 - 002538056 _____ () C:\Program
Files\WindowsApps\Microsoft.WindowsStore_11810.1001.12.0_x64__8wekyb3d8bbwe\Microsoft.
UI.Xaml.dll
2018-11-06 07:16 - 2018-11-06 07:16 - 001754112 _____ () C:\Program
Files\WindowsApps\Microsoft.WindowsStore_11810.1001.12.0_x64__8wekyb3d8bbwe\Microsoft.
Membership.MeControl.dll
2018-12-05 07:34 - 2018-12-05 07:35 - 003464192 _____ () C:\Program
Files\WindowsApps\Microsoft.MSPaint_5.1811.20017.0_x64__8wekyb3d8bbwe\PaintStudio.View.
exe
2018-12-05 07:34 - 2018-12-05 07:35 - 001073152 _____ () C:\Program
Files\WindowsApps\Microsoft.MSPaint_5.1811.20017.0_x64__8wekyb3d8bbwe\TelemetryUWP.dl
l
2018-12-05 07:34 - 2018-12-05 07:35 - 000016384 _____ () C:\Program
Files\WindowsApps\Microsoft.MSPaint_5.1811.20017.0_x64__8wekyb3d8bbwe\SharedMemoryU
WP.dll
2018-12-05 07:34 - 2018-12-05 07:35 - 000816640 _____ () C:\Program
Files\WindowsApps\Microsoft.MSPaint_5.1811.20017.0_x64__8wekyb3d8bbwe\Utils.CX.dll
2018-04-12 16:53 - 2018-04-12 16:53 - 003553704 _____ () C:\Program
Files\WindowsApps\Microsoft.MSPaint_5.1811.20017.0_x64__8wekyb3d8bbwe\Microsoft.UI.Xa
ml.dll
2018-12-05 07:34 - 2018-12-05 07:35 - 008004096 _____ () C:\Program
Files\WindowsApps\Microsoft.MSPaint_5.1811.20017.0_x64__8wekyb3d8bbwe\PaintStudio.View
Elements.dll
2018-12-05 07:34 - 2018-12-05 07:35 - 009120768 _____ () C:\Program
Files\WindowsApps\Microsoft.MSPaint_5.1811.20017.0_x64__8wekyb3d8bbwe\PaintStudio.View
Model.dll
2018-12-05 07:34 - 2018-12-05 07:34 - 000506880 _____ () C:\Program
Files\WindowsApps\Microsoft.MSPaint_5.1811.20017.0_x64__8wekyb3d8bbwe\ConfigurationMa
nager.dll
2018-12-05 07:34 - 2018-12-05 07:35 - 000626176 _____ () C:\Program
Files\WindowsApps\Microsoft.MSPaint_5.1811.20017.0_x64__8wekyb3d8bbwe\MSASignIn.dll
2018-12-18 08:31 - 2018-12-18 08:34 - 001436760 _____ () C:\Program
Files\WindowsApps\microsoft.windowscommunicationsapps_16005.11029.20108.0_x64__8wekyb
3d8bbwe\Office.UI.Xaml.Word.dll
2018-09-15 18:35 - 2018-09-15 18:35 - 000009216 _____ () C:\Program
Files\WindowsApps\Microsoft.SkypeApp_14.36.52.0_x64__kzf8qxf38zg5c\ImagePipelineNative.d
ll
2018-12-15 08:06 - 2018-12-15 08:06 - 000060416 _____ () C:\Program
Files\WindowsApps\Microsoft.SkypeApp_14.36.52.0_x64__kzf8qxf38zg5c\ChakraBridge.dll
2018-12-15 08:06 - 2018-12-15 08:07 - 010927616 _____ () C:\Program
Files\WindowsApps\Microsoft.SkypeApp_14.36.52.0_x64__kzf8qxf38zg5c\LibWrapper.dll

2018-12-15 08:06 - 2018-12-15 08:09 - 002916864 _____ () C:\Program Files\WindowsApps\Microsoft.SkypeApp_14.36.52.0_x64__kzf8qxf38zg5c\skypert.dll
2018-12-15 08:06 - 2018-12-15 08:07 - 000688128 _____ () C:\Program Files\WindowsApps\Microsoft.SkypeApp_14.36.52.0_x64__kzf8qxf38zg5c\RtmMvrUap.dll
2018-08-05 14:15 - 2017-11-13 15:49 - 000085200 _____ () C:\Users\o\AppData\Roaming\Seznam.cz\bin\12542libfoxloader.dll
2018-08-05 14:15 - 2018-02-21 10:36 - 000869584 _____ () C:\Users\o\AppData\Roaming\Seznam.cz\bin\lightspeed.dll
2012-08-30 12:39 - 2015-02-18 13:11 - 000112128 _____ () C:\Program Files (x86)\Canon\ImageBrowser EX\MFMFileSystemWatcher.dll

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

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

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

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

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

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

========== Internet Explorer trusted/restricted ==========

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

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

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

2018-08-05 10:09 - 2018-08-05 10:08 - 000000824 _____ C:\WINDOWS\system32\drivers\etc\hosts

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

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

HKU\S-1-5-21-2671679121-1364000227-736312402-1003\Control Panel\Desktop\\Wallpaper -> C:\Users\o\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\LocalState\PhotosAppBackground\ranní lomničák.png
DNS Servers: 85.93.160.254 - 85.93.160.118
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System => (ConsentPromptBehaviorAdmin: 5) (ConsentPromptBehaviorUser: 3) (EnableLUA: 1)
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer => (SmartScreenEnabled: RequireAdmin)

Windows Firewall is enabled.

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

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

========== 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: [{D0511E3E-3A7F-4E1B-9ABC-A325461B7A98}] => (Allow) C:\Program Files\HP\HP DeskJet 5820 series\Bin\HPNetworkCommunicatorCom.exe (Hewlett-Packard Development Company, LP)
FirewallRules: [{509F87A7-35EE-4559-A4B3-16AF11E8F964}] => (Allow) LPort=5357
FirewallRules: [{ABCA079F-6210-4AA9-9A48-02854ABFE4FE}] => (Allow) C:\Program Files\HP\HP DeskJet 5820 series\Bin\DeviceSetup.exe (Hewlett-Packard Development Company, LP)
FirewallRules: [{D6FE37A1-1D14-4D1D-984E-5E79C2C55BD1}] => (Block) C:\users\o\appdata\roaming\spotify\spotify.exe (Spotify Ltd)
FirewallRules: [{66DBF78D-7F33-413B-A784-8BB554FFBD06}] => (Block) C:\users\o\appdata\roaming\spotify\spotify.exe (Spotify Ltd)
FirewallRules: [UDP Query User{E3972142-1428-4B40-93A7-479B4EA9CF3D}C:\users\o\appdata\roaming\spotify\spotify.exe] => (Allow) C:\users\o\appdata\roaming\spotify\spotify.exe (Spotify Ltd)
FirewallRules: [TCP Query User{60B11243-D286-4A87-A86D-2B083836908E}C:\users\o\appdata\roaming\spotify\spotify.exe] => (Allow) C:\users\o\appdata\roaming\spotify\spotify.exe (Spotify Ltd)
FirewallRules: [{39E9C860-4CC5-48E0-BA99-079BCDC6F42A}] => (Allow) C:\Program Files\Mozilla Firefox\firefox.exe (Mozilla Corporation)
FirewallRules: [{4E58E12F-0CA7-442C-9A8F-04BBCA046A13}] => (Allow) C:\Program Files\Mozilla Firefox\firefox.exe (Mozilla Corporation)
FirewallRules: [{660E0951-5A18-4E21-A4AE-FF4BA7CE8CE8}] => (Allow) C:\Program Files (x86)\Google\Chrome\Application\chrome.exe (Google Inc.)
FirewallRules: [{74EF2E72-8999-4C9D-B3C9-45C71A20E2AB}] => (Allow) C:\Program Files\CCleaner\CCUpdate.exe (Piriform Ltd)
FirewallRules: [{8AD5C1B0-4316-4CFE-A003-4C9099F9D275}] => (Allow) C:\Program Files\CCleaner\CCUpdate.exe (Piriform Ltd)

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

29-12-2018 16:53:37 Naplánovaný kontrolní bod
07-01-2019 09:57:50 Naplánovaný kontrolní bod

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

Name: Standardní klávesnice PS/2
Description: Standardní klávesnice PS/2
Class Guid: {4d36e96b-e325-11ce-bfc1-08002be10318}
Manufacturer: (Standardní klávesnice)
Service: i8042prt

Problem: : This device is not present, is not working properly, or does not have all its drivers installed. (Code 24)
Resolution: The device is installed incorrectly. The problem could be a hardware failure, or a new driver might be needed.
Devices stay in this state if they have been prepared for removal.
After you remove the device, this error disappears.Remove the device, and this error should be resolved.

Name: Myš Microsoft PS/2
Description: Myš Microsoft PS/2
Class Guid: {4d36e96f-e325-11ce-bfc1-08002be10318}
Manufacturer: Microsoft
Service: i8042prt
Problem: : This device is not present, is not working properly, or does not have all its drivers installed. (Code 24)
Resolution: The device is installed incorrectly. The problem could be a hardware failure, or a new driver might be needed.
Devices stay in this state if they have been prepared for removal.
After you remove the device, this error disappears.Remove the device, and this error should be resolved.

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

Application errors:
==========
Error: (01/07/2019 12:16:03 PM) (Source: ESENT) (EventID: 489) (User:)
Description: CCleaner64 (8220,G,0) Pokus o otevření souboru C:\Users\o\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat jen pro čtení selhal. Došlo k systémové chybě 32 (0x00000020): Proces nemá přístup k souboru, neboť jej právě využívá jiný proces. . Operace otevření souboru selže a dojde k chybě -1032 (0xfffffbf8).

Error: (12/26/2018 06:46:49 AM) (Source: Application Error) (EventID: 1000) (User:)
Description: Název chybující aplikace: SettingSyncHost.exe, verze: 10.0.17763.1, časové razítko: 0x96accf1d
Název chybujícího modulu: SettingSyncHost.exe, verze: 10.0.17763.1, časové razítko: 0x96accf1d
Kód výjimky: 0xc0000005
Posun chyby: 0x0000000000027964
ID chybujícího procesu: 0x1700
Čas spuštění chybující aplikace: 0x01d49cde63c88ade
Cesta k chybující aplikaci: C:\WINDOWS\system32\SettingSyncHost.exe
Cesta k chybujícímu modulu: C:\WINDOWS\system32\SettingSyncHost.exe
ID zprávy: 5355b431-b9e7-4710-af10-ab6d1ebde55a
Úplný název chybujícího balíčku:
ID aplikace související s chybujícím balíčkem:

Error: (12/16/2018 01:52:14 PM) (Source: Application Hang) (EventID: 1002) (User:)
Description: Program wordpad.exe verze 10.0.17763.1 přestal spolupracovat s Windows a byl ukončen. Pokud chcete zjistit, jestli je k dispozici více informací o tomto problému, vyhledejte historii problému na ovládacím panelu Zabezpečení a údržba.

ID procesu: b48

Čas spuštění: 01d4953e1e8148ab

Čas ukončení: 12

Cesta k aplikaci: C:\Program Files\windows nt\accessories\wordpad.exe

ID hlášení: cfaa2671-aca7-41f3-95db-a01dd4d90fba

Úplný název balíčku s chybou:

ID aplikace relativní podle balíčku s chybou:

Typ zablokování: Unknown

Error: (12/16/2018 01:51:05 PM) (Source: Application Hang) (EventID: 1002) (User:)
Description: Program wordpad.exe verze 10.0.17763.1 přestal spolupracovat s Windows a byl ukončen. Pokud chcete zjistit, jestli je k dispozici více informací o tomto problému, vyhledejte historii problému na ovládacím panelu Zabezpečení a údržba.

ID procesu: 186c

Čas spuštění: 01d4953df99f791e

Čas ukončení: 16

Cesta k aplikaci: C:\Program Files\windows nt\accessories\wordpad.exe

ID hlášení: 16ca07ca-242d-44ec-9a18-2fdde13e2cbb

Úplný název balíčku s chybou:

ID aplikace relativní podle balíčku s chybou:

Typ zablokování: Unknown

Error: (12/12/2018 01:15:36 PM) (Source: Application Error) (EventID: 1000) (User:)
Description: Název chybující aplikace: HxTsr.exe, verze: 16.0.11001.20091, časové razítko: 0x5bdbefe7
Název chybujícího modulu: hxcomm.dll, verze: 16.0.11001.20116, časové razítko: 0x5bf31dcb
Kód výjimky: 0x022c1799
Posun chyby: 0x00000000001e59a0
ID chybujícího procesu: 0x17bc
Čas spuštění chybující aplikace: 0x01d491de017eff5a
Cesta k chybující aplikaci: C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_16005.11001.20116.0_x64__8wekyb3d8bbwe\HxTsr.exe
Cesta k chybujícímu modulu: C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_16005.11001.20116.0_x64__8wekyb3d8bbwe\hxcomm.dll
ID zprávy: a5ef4ecd-dcdb-4f58-80bb-4c6959ded012
Úplný název chybujícího balíčku:

microsoft.windowscommunicationsapps_16005.11001.20116.0_x64__8wekyb3d8bbwe
ID aplikace související s chybujícím balíčkem: ppleae38af2e007f4358a809ac99a64a67c1

Error: (11/28/2018 10:25:11 AM) (Source: Application Error) (EventID: 1000) (User:)
Description: Název chybující aplikace: HPDiagnosticCoreUI.exe, verze: 5.1.1.4, časové razítko: 0x5ac4b851
Název chybujícího modulu: HPDiagnosticCore.dll, verze: 1.0.16.0, časové razítko: 0x5ac4b7c9
Kód výjimky: 0xc0000005
Posun chyby: 0x001cbf6e
ID chybujícího procesu: 0x2128
Čas spuštění chybující aplikace: 0x01d486fa7d93990d
Cesta k chybující aplikaci: C:\Users\o\AppData\Local\Temp\7zS1087\HPDiagnosticCoreUI.exe
Cesta k chybujícímu modulu: C:\Users\o\AppData\Local\Temp\7zS1087\HPDiagnosticCore.dll
ID zprávy: 382f54f1-86dc-4372-87bd-e06ce50ffe2e
Úplný název chybujícího balíčku:
ID aplikace související s chybujícím balíčkem:

Error: (11/28/2018 10:25:11 AM) (Source: .NET Runtime) (EventID: 1026) (User:)
Description: Aplikace: HPDiagnosticCoreUI.exe
Verze Framework: v4.0.30319
Popis: Proces byl ukončen z důvodu neošetřené výjimky.
Informace o výjimce: kód výjimky c0000005, adresa výjimky 6C5DBF6E

Error: (11/23/2018 05:51:09 PM) (Source: Application Error) (EventID: 1000) (User:)
Description: Název chybující aplikace: MailClient.exe, verze: 7.1.33101.0, časové razítko: 0x5b47441a
Název chybujícího modulu: KERNELBASE.dll, verze: 10.0.17763.134, časové razítko: 0xc30ded87
Kód výjimky: 0xc000041d
Posun chyby: 0x0011ab32
ID chybujícího procesu: 0x1824
Čas spuštění chybující aplikace: 0x01d4834c98837e1a
Cesta k chybující aplikaci: C:\Program Files (x86)\eM Client\MailClient.exe
Cesta k chybujícímu modulu: C:\WINDOWS\System32\KERNELBASE.dll
ID zprávy: d3eef8f8-d9c4-48c3-933b-d363c388ea0b
Úplný název chybujícího balíčku:
ID aplikace související s chybujícím balíčkem:

System errors:
==========
Error: (01/15/2019 03:40:56 PM) (Source: DCOM) (EventID: 10016) (User: DESKTOP-BAS7282)
Description: Nastavení oprávnění specifické pro aplikaci neuděluje oprávnění Místní Aktivace pro serverovou aplikaci COM s identifikátorem CLSID
{2593F8B9-4EAF-457C-B68A-50F6B8EA6B54}
a APPID
{15C20B67-12E7-4BB6-92BB-7AFF07997402}
uživateli DESKTOP-BAS7282\o (SID: S-1-5-21-2671679121-1364000227-736312402-1003) z adresy LocalHost (pomocí LRPC) běžící v kontejneru aplikací Není k dispozici – SID (Není k dispozici). Toto oprávnění zabezpečení lze změnit pomocí nástroje správy Služba komponent.

Error: (01/15/2019 03:40:56 PM) (Source: DCOM) (EventID: 10016) (User: DESKTOP-BAS7282)

Description: Nastavení oprávnění specifické pro aplikaci neuděluje oprávnění Místní Aktivace pro serverovou aplikaci COM s identifikátorem CLSID
{2593F8B9-4EAF-457C-B68A-50F6B8EA6B54}
a APPID
{15C20B67-12E7-4BB6-92BB-7AFF07997402}
uživateli DESKTOP-BAS7282\o (SID: S-1-5-21-2671679121-1364000227-736312402-1003) z adresy LocalHost (pomocí LRPC) běžící v kontejneru aplikací Není k dispozici – SID (Není k dispozici). Toto oprávnění zabezpečení lze změnit pomocí nástroje správy Služba komponent.

Error: (01/15/2019 10:00:23 AM) (Source: DCOM) (EventID: 10016) (User: DESKTOP-BAS7282)
Description: Nastavení oprávnění specifické pro aplikaci neuděluje oprávnění Místní Aktivace pro serverovou aplikaci COM s identifikátorem CLSID
{2593F8B9-4EAF-457C-B68A-50F6B8EA6B54}
a APPID
{15C20B67-12E7-4BB6-92BB-7AFF07997402}
uživateli DESKTOP-BAS7282\o (SID: S-1-5-21-2671679121-1364000227-736312402-1003) z adresy LocalHost (pomocí LRPC) běžící v kontejneru aplikací Není k dispozici – SID (Není k dispozici). Toto oprávnění zabezpečení lze změnit pomocí nástroje správy Služba komponent.

Error: (01/15/2019 10:00:23 AM) (Source: DCOM) (EventID: 10016) (User: DESKTOP-BAS7282)
Description: Nastavení oprávnění specifické pro aplikaci neuděluje oprávnění Místní Aktivace pro serverovou aplikaci COM s identifikátorem CLSID
{2593F8B9-4EAF-457C-B68A-50F6B8EA6B54}
a APPID
{15C20B67-12E7-4BB6-92BB-7AFF07997402}
uživateli DESKTOP-BAS7282\o (SID: S-1-5-21-2671679121-1364000227-736312402-1003) z adresy LocalHost (pomocí LRPC) běžící v kontejneru aplikací Není k dispozici – SID (Není k dispozici). Toto oprávnění zabezpečení lze změnit pomocí nástroje správy Služba komponent.

Error: (01/15/2019 08:13:50 AM) (Source: DCOM) (EventID: 10016) (User: DESKTOP-BAS7282)
Description: Nastavení oprávnění specifické pro aplikaci neuděluje oprávnění Místní Aktivace pro serverovou aplikaci COM s identifikátorem CLSID
{2593F8B9-4EAF-457C-B68A-50F6B8EA6B54}
a APPID
{15C20B67-12E7-4BB6-92BB-7AFF07997402}
uživateli DESKTOP-BAS7282\o (SID: S-1-5-21-2671679121-1364000227-736312402-1003) z adresy LocalHost (pomocí LRPC) běžící v kontejneru aplikací Není k dispozici – SID (Není k dispozici). Toto oprávnění zabezpečení lze změnit pomocí nástroje správy Služba komponent.

Error: (01/15/2019 08:13:50 AM) (Source: DCOM) (EventID: 10016) (User: DESKTOP-BAS7282)
Description: Nastavení oprávnění specifické pro aplikaci neuděluje oprávnění Místní Aktivace pro serverovou aplikaci COM s identifikátorem CLSID
{2593F8B9-4EAF-457C-B68A-50F6B8EA6B54}
a APPID
{15C20B67-12E7-4BB6-92BB-7AFF07997402}
uživateli DESKTOP-BAS7282\o (SID: S-1-5-21-2671679121-1364000227-736312402-1003) z adresy LocalHost (pomocí LRPC) běžící v kontejneru aplikací Není k dispozici – SID (Není k dispozici). Toto oprávnění zabezpečení lze změnit pomocí nástroje správy Služba komponent.

Error: (01/15/2019 07:16:46 AM) (Source: DCOM) (EventID: 10016) (User: NT AUTHORITY)
Description: Nastavení oprávnění specifické pro aplikaci neuděluje oprávnění Místní Spuštění pro serverovou aplikaci COM s identifikátorem CLSID

Windows.SecurityCenter.WscBrokerManager
a APPID
Není k dispozici
uživateli NT AUTHORITY\SYSTEM (SID: S-1-5-18) z adresy LocalHost (pomocí LRPC) běžící v kontejneru aplikací Není k dispozici – SID (Není k dispozici). Toto oprávnění zabezpečení lze změnit pomocí nástroje správy Služba komponent.

Error: (01/15/2019 07:16:46 AM) (Source: DCOM) (EventID: 10016) (User: NT AUTHORITY)
Description: Nastavení oprávnění specifické pro aplikaci neuděluje oprávnění Místní Spuštění pro serverovou aplikaci COM s identifikátorem CLSID
Windows.SecurityCenter.SecurityAppBroker
a APPID
Není k dispozici
uživateli NT AUTHORITY\SYSTEM (SID: S-1-5-18) z adresy LocalHost (pomocí LRPC) běžící v kontejneru aplikací Není k dispozici – SID (Není k dispozici). Toto oprávnění zabezpečení lze změnit pomocí nástroje správy Služba komponent.

CodeIntegrity:
==========

Date: 2018-10-12 09:08:24.848
Description:
Windows is unable to verify the image integrity of the file \Device\HarddiskVolume4\Program Files\ESET\ESET Security\ecmds.exe because file hash could not be found on the system. A recent hardware or software change might have installed a file that is signed incorrectly or damaged, or that might be malicious software from an unknown source.

Date: 2018-10-12 09:08:24.843
Description:
Windows is unable to verify the image integrity of the file \Device\HarddiskVolume4\Program Files\ESET\ESET Security\ecmds.exe because file hash could not be found on the system. A recent hardware or software change might have installed a file that is signed incorrectly or damaged, or that might be malicious software from an unknown source.

Date: 2018-10-12 09:08:24.835
Description:
Windows is unable to verify the image integrity of the file \Device\HarddiskVolume4\Program Files\ESET\ESET Security\ecmds.exe because file hash could not be found on the system. A recent hardware or software change might have installed a file that is signed incorrectly or damaged, or that might be malicious software from an unknown source.

Date: 2018-10-12 09:08:24.830
Description:
Windows is unable to verify the image integrity of the file \Device\HarddiskVolume4\Program Files\ESET\ESET Security\ecmds.exe because file hash could not be found on the system. A recent hardware or software change might have installed a file that is signed incorrectly or damaged, or that might be malicious software from an unknown source.

Date: 2018-10-12 09:08:24.821
Description:
Windows is unable to verify the image integrity of the file \Device\HarddiskVolume4\Program

Files\ESET\ESET Security\ecmds.exe because file hash could not be found on the system. A recent hardware or software change might have installed a file that is signed incorrectly or damaged, or that might be malicious software from an unknown source.

Date: 2018-10-12 09:08:24.815
Description:
Windows is unable to verify the image integrity of the file \Device\HarddiskVolume4\Program Files\ESET\ESET Security\ecmds.exe because file hash could not be found on the system. A recent hardware or software change might have installed a file that is signed incorrectly or damaged, or that might be malicious software from an unknown source.

Date: 2018-10-12 09:08:15.218
Description:
Windows is unable to verify the image integrity of the file \Device\HarddiskVolume4\Program Files\ESET\ESET Security\ecmds.exe because file hash could not be found on the system. A recent hardware or software change might have installed a file that is signed incorrectly or damaged, or that might be malicious software from an unknown source.

Date: 2018-10-12 09:08:15.213
Description:
Windows is unable to verify the image integrity of the file \Device\HarddiskVolume4\Program Files\ESET\ESET Security\ecmds.exe because file hash could not be found on the system. A recent hardware or software change might have installed a file that is signed incorrectly or damaged, or that might be malicious software from an unknown source.

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

Processor: Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz
Percentage of memory in use: 40%
Total physical RAM: 8155.09 MB
Available physical RAM: 4878.2 MB
Total Virtual: 9435.09 MB
Available Virtual: 3399.26 MB

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

Drive c: () (Fixed) (Total:222.58 GB) (Free:149.53 GB) NTFS
Drive d: () (Fixed) (Total:931.39 GB) (Free:353.9 GB) NTFS

\\?\Volume{dda794df-29ce-4260-955c-5d488ec41ee3}\ (Obnovení) (Fixed) (Total:0.44 GB) (Free:0.13 GB) NTFS
\\?\Volume{ecf4ecbd-0631-42eb-8356-f7cd4b5debb6}\ () (Fixed) (Total:0.44 GB) (Free:0.05 GB) NTFS
\\?\Volume{0e88439b-e7a7-474c-b178-fade1ac6c8f1}\ () (Fixed) (Total:0.1 GB) (Free:0.07 GB) FAT32

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

==========
Disk: 0 (Protective MBR) (Size: 223.6 GB) (Disk ID: 00000000)

Partition: GPT.

==
Disk: 1 (Protective MBR) (Size: 931.5 GB) (Disk ID: 00000000)

Partition: GPT.

==================== End of Addition.txt ============================can result of Farbar Recovery Scan Tool (FRST) (x64) Version: 14.01.2019 01
Ran by o (administrator) on DESKTOP-BAS7282 (15-01-2019 16:39:01)
Running from C:\Users\o\Downloads
Loaded Profiles: o (Available Profiles: OEM & o)
Platform: Windows 10 Home Version 1809 17763.253 (X64) Language: Čeština (Česko)
Internet Explorer Version 11 (Default browser: FF)
Boot Mode: Normal
Tutorial for Farbar Recovery Scan Tool: http://www.geekstogo.com/forum/topic/335081-frst-tutorial-how-to-use-farbar-recovery-scan-tool/

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

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

(ESET) C:\Program Files\ESET\ESET Security\ekrn.exe
(NVIDIA Corporation) C:\Program Files\NVIDIA Corporation\Display.NvContainer\NVDisplay.Container.exe
(NVIDIA Corporation) C:\Program Files\NVIDIA Corporation\Display.NvContainer\NVDisplay.Container.exe
() C:\Program Files\WindowsApps\Microsoft.ZuneVideo_10.18102.12011.0_x64__8wekyb3d8bbwe\Video.UI.exe
() C:\Program Files\WindowsApps\Microsoft.SkypeApp_14.36.52.0_x64__kzf8qxf38zg5c\SkypeBackgroundHost.exe
() C:\Program Files\WindowsApps\Microsoft.YourPhone_1.0.20094.0_x64__8wekyb3d8bbwe\YourPhone.exe
(Microsoft Corporation) C:\Program Files\WindowsApps\Microsoft.SkypeApp_14.36.52.0_x64__kzf8qxf38zg5c\SkypeBridge\SkypeBridge.exe
(Microsoft Corporation) C:\Windows\System32\smartscreen.exe
(Realtek Semiconductor) C:\Program Files\Realtek\Audio\HDA\RtkNGUI64.exe
(ESET) C:\Program Files\ESET\ESET Security\egui.exe
() C:\Users\o\AppData\Roaming\Seznam.cz\bin\szndesktop.exe
() C:\Users\o\AppData\Roaming\Seznam.cz\bin\listicka-x64.exe
() C:\Program Files (x86)\Canon\ImageBrowser EX\MFManager.exe
(Piriform Software Ltd) C:\Program Files\CCleaner\CCleaner64.exe
(Microsoft Corporation) C:\Program Files\WindowsApps\Microsoft.WindowsStore_11810.1001.12.0_x64__8wekyb3d8bbwe\WinStore.App.exe
(Microsoft Corporation) C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\RemindersServer.exe
(Microsoft Corporation) C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdge.exe
(Microsoft Corporation) C:\Windows\System32\browser_broker.exe

(Microsoft Corporation) C:\Windows\System32\MicrosoftEdgeCP.exe
(Microsoft Corporation) C:\Windows\System32\MicrosoftEdgeSH.exe
() C:\Program Files\WindowsApps\Microsoft.MSPaint_5.1811.20017.0_x64__8wekyb3d8bbwe\PaintStudio.View.exe
(Microsoft Corporation) C:\Windows\ImmersiveControlPanel\SystemSettings.exe
(Mozilla Corporation) C:\Program Files\Mozilla Firefox\firefox.exe
(Mozilla Corporation) C:\Program Files\Mozilla Firefox\firefox.exe
(Mozilla Corporation) C:\Program Files\Mozilla Firefox\firefox.exe
(Mozilla Corporation) C:\Program Files\Mozilla Firefox\firefox.exe
(Microsoft Corporation) C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_16005.11029.20108.0_x64__8wekyb3d8bbwe\HxOutlook.exe
(Microsoft Corporation) C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_16005.11029.20108.0_x64__8wekyb3d8bbwe\HxTsr.exe
(Microsoft Corporation) C:\Program Files\WindowsApps\Microsoft.SkypeApp_14.36.52.0_x64__kzf8qxf38zg5c\SkypeApp.exe
(Mozilla Corporation) C:\Program Files\Mozilla Firefox\firefox.exe
(Mozilla Corporation) C:\Program Files\Mozilla Firefox\firefox.exe
(Microsoft Corporation) C:\Windows\SystemApps\InputApp_cw5n1h2txyewy\WindowsInternal.ComposableShell.Experiences.TextInput.InputApp.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: [RTHDVCPL] => C:\Program Files\Realtek\Audio\HDA\RtkNGUI64.exe [8491888 2015-06-15] (Realtek Semiconductor)
HKLM\...\Run: [egui] => C:\Program Files\ESET\ESET Security\ecmds.exe [177928 2018-12-05] (ESET)
HKLM-x32\...\Run: [seznam-listicka-distribuce] => C:\Program Files (x86)\Seznam.cz\distribution\szninstall.exe [1069296 2018-03-27] ()
HKU\S-1-5-19\...\RunOnce: [WAB Migrate] => C:\Program Files\Windows Mail\wab.exe [518656 2018-09-15] (Microsoft Corporation)
HKU\S-1-5-20\...\RunOnce: [WAB Migrate] => C:\Program Files\Windows Mail\wab.exe [518656 2018-09-15] (Microsoft Corporation)
HKU\S-1-5-21-2671679121-1364000227-736312402-1003\...\Run: [cz.seznam.software.autoupdate] => C:\Users\o\AppData\Roaming\Seznam.cz\szninstall.exe [1069296 2018-03-27] ()
HKU\S-1-5-21-2671679121-1364000227-736312402-1003\...\Run: [cz.seznam.software.szndesktop] => C:\Users\o\AppData\Roaming\Seznam.cz\bin\wszndesktop.exe [109808 2018-03-27] ()
HKU\S-1-5-21-2671679121-1364000227-736312402-1003\...\Run: [Spotify] => C:\Users\o\AppData\Roaming\Spotify\Spotify.exe [25972968 2018-12-23] (Spotify Ltd)
HKU\S-1-5-21-2671679121-1364000227-736312402-1003\...\Run: [CCleaner Smart Cleaning] => C:\Program Files\CCleaner\CCleaner64.exe [19589208 2018-12-10] (Piriform Software Ltd)
HKU\S-1-5-21-2671679121-1364000227-736312402-1003\Control Panel\Desktop\\SCRNSAVE.EXE -> C:\WINDOWS\system32\PhotoScreensaver.scr [570880 2018-09-15] (Microsoft Corporation)

HKLM\...\Drivers32: [vidc.i420] => C:\WINDOWS\system32\lvcod64.dll [475672 2008-07-26] (Logitech Inc.)
HKLM\...\Drivers32: [MSVideo] => C:\WINDOWS\system32\vfwwdm32.dll [68096 2018-09-15] (Microsoft Corporation)
HKLM\...\Drivers32-x32: [vidc.i420] => C:\Windows\SysWOW64\lvcodec2.dll [416280 2008-07-26] (Logitech Inc.)
HKLM\Software\Microsoft\Active Setup\Installed Components: [{8A69D345-D564-463c-AFF1-A69D9E530F96}] -> C:\Program Files (x86)\Google\Chrome\Application\71.0.3578.98\Installer\chrmstp.exe [2018-12-13] (Google Inc.)
Startup: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\ImageBrowser EX Agent.lnk [2018-08-06]
ShortcutTarget: ImageBrowser EX Agent.lnk -> C:\Program Files (x86)\Canon\ImageBrowser EX\MFManager.exe ()
Startup: C:\Users\o\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Sledovat výstrahy inkoustu - HP DeskJet 5820 series.lnk [2018-10-11]
ShortcutTarget: Sledovat výstrahy inkoustu - HP DeskJet 5820 series.lnk -> C:\Program Files\HP\HP DeskJet 5820 series\Bin\HPStatusBL.dll (HP Inc.)

========== 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] 85.93.160.254 85.93.160.118
Tcpip\..\Interfaces\{7ca960af-b27a-4434-a2b9-ddc5ddff558b}: [DhcpNameServer] 85.93.160.254 85.93.160.118

Internet Explorer:
==========
HKU\S-1-5-21-2671679121-1364000227-736312402-1003\Software\Microsoft\Internet Explorer\Main,Start Page = hxxp://www.seznam.cz/?clid=12454
SearchScopes: HKU\S-1-5-21-2671679121-1364000227-736312402-1003 -> {06BE88D4-C56F-45D6-B96E-0706AC13E02E} URL = hxxp://slovnik.seznam.cz/?q={searchTerms}&lang=en_cz&sourceid=QuickSearch_12454
SearchScopes: HKU\S-1-5-21-2671679121-1364000227-736312402-1003 -> {0C406B93-9027-4ECC-B4DA-1E3F4312BC1E} URL = hxxp://www.firmy.cz/?q={searchTerms}&sourceid=QuickSearch_12454
SearchScopes: HKU\S-1-5-21-2671679121-1364000227-736312402-1003 -> {29931245-55B2-4C2D-A765-C602E520BC03} URL = hxxp://www.zbozi.cz/?q={searchTerms}&r=campmoz&sourceid=QuickSearch_12454
SearchScopes: HKU\S-1-5-21-2671679121-1364000227-736312402-1003 -> {38370AE7-97A8-4044-97BC-47EC95577E69} URL = hxxp://www.novinky.cz/hledej?w={searchTerms}&sourceid=QuickSearch_12454
SearchScopes: HKU\S-1-5-21-2671679121-1364000227-736312402-1003 -> {67831AFC-77FA-43C3-ABA1-8B3A05D56A64} URL = hxxp://www.mapy.cz/?query={searchTerms}&sourceid=QuickSearch_12454
SearchScopes: HKU\S-1-5-21-2671679121-1364000227-736312402-1003 -> {89E6C160-8EB3-4D7D-B929-840E318CC52A} URL = hxxp://search.seznam.cz/?q={searchTerms}&sourceid=QuickSearch_12454
SearchScopes: HKU\S-1-5-21-2671679121-1364000227-736312402-1003 -> {96F7DBBC-8149-4334-AC47-E15E9020321E} URL = hxxp://tv.seznam.cz/hledej?w={searchTerms}&sourceid=QuickSearch_12454
SearchScopes: HKU\S-1-5-21-2671679121-1364000227-736312402-1003 -> {A06BEA29-9DF8-

4C87-88BF-6C471F2EC5ED} URL = hxxp://slovnik.seznam.cz/?q={searchTerms}&lang=cz_en&sourceid=QuickSearch_12454
SearchScopes: HKU\S-1-5-21-2671679121-1364000227-736312402-1003 -> {F0714C88-0AD9-44AF-B905-73C25E12875F} URL = hxxp://encyklopedie.seznam.cz/search?q={searchTerms}&sourceid=QuickSearch_12454

FireFox:
========
FF DefaultProfile: epktbmwu.default
FF ProfilePath: C:\Users\o\AppData\Roaming\Mozilla\Firefox\Profiles\epktbmwu.default [2019-01-15]
FF Homepage: Mozilla\Firefox\Profiles\epktbmwu.default -> hxxps://atlas.centrum.cz/?redirected=1533474501
FF Extension: (Video Downloader professional) - C:\Users\o\AppData\Roaming\Mozilla\Firefox\Profiles\epktbmwu.default\Extensions\ffext_basicvideoext@startpage24.xpi [2018-08-06]
FF Extension: (Forget Me Not - Forget cookies & other data) - C:\Users\o\AppData\Roaming\Mozilla\Firefox\Profiles\epktbmwu.default\Extensions\forget-me-not@lusito.info.xpi [2018-09-03]
FF Extension: (Privacy Badger) - C:\Users\o\AppData\Roaming\Mozilla\Firefox\Profiles\epktbmwu.default\Extensions\jid1-MnnxcxisBPnSXQ@jetpack.xpi [2018-12-18]
FF Extension: (Vývojové sestavení Adblock Plus) - C:\Users\o\AppData\Roaming\Mozilla\Firefox\Profiles\epktbmwu.default\Extensions\{d10d0bf8-f5b5-c8b4-a8b2-2b9879e08c5d}.xpi [2018-12-04]
FF Extension: (No Name) - C:\Users\o\AppData\Roaming\Mozilla\Firefox\Profiles\epktbmwu.default\extensions\{ea614400-e918-4741-9a97-7a972ff7c30b} [not found]
FF Plugin: @Microsoft.com/NpCtrl,version=1.0 -> C:\Program Files\Microsoft Silverlight\5.1.50907.0\npctrl.dll [2017-05-03] (Microsoft Corporation)
FF Plugin: @videolan.org/vlc,version=3.0.3 -> C:\Program Files\VideoLAN\VLC\npvlc.dll [2018-08-10] (VideoLAN)
FF Plugin: @videolan.org/vlc,version=3.0.4 -> C:\Program Files\VideoLAN\VLC\npvlc.dll [2018-08-10] (VideoLAN)
FF Plugin-x32: @Microsoft.com/NpCtrl,version=1.0 -> C:\Program Files (x86)\Microsoft Silverlight\5.1.50907.0\npctrl.dll [2017-05-03] (Microsoft Corporation)
FF Plugin-x32: @tools.google.com/Google Update;version=3 -> C:\Program Files (x86)\Google\Update\1.3.33.23\npGoogleUpdate3.dll [2018-12-20] (Google Inc.)
FF Plugin-x32: @tools.google.com/Google Update;version=9 -> C:\Program Files (x86)\Google\Update\1.3.33.23\npGoogleUpdate3.dll [2018-12-20] (Google Inc.)
FF Plugin-x32: Adobe Reader -> C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AIR\nppdf32.dll [2018-12-04] (Adobe Systems Inc.)

Chrome:
=======
CHR Profile: C:\Users\o\AppData\Local\Google\Chrome\User Data\Default [2019-01-14]
CHR Extension: (Prezentace) - C:\Users\o\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek [2018-08-05]
CHR Extension: (Dokumenty) - C:\Users\o\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake [2018-08-05]
CHR Extension: (Disk Google) - C:\Users\o\AppData\Local\Google\Chrome\User Data\Default\Extensions\apdfllckaahabafndbhieahigkjlhalf [2018-08-05]

CHR Extension: (YouTube) - C:\Users\o\AppData\Local\Google\Chrome\User Data\Default\Extensions\blpcfgokakmgnkcojhhkbfbldkacnbeo [2018-08-05]
CHR Extension: (Dokumenty Google offline) - C:\Users\o\AppData\Local\Google\Chrome\User Data\Default\Extensions\ghbmnnjooekpmoecnnnilnnbdlolhkhi [2018-08-23]
CHR Extension: (Platby Internetového obchodu Chrome) - C:\Users\o\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda [2018-08-05]
CHR Extension: (Gmail) - C:\Users\o\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia [2018-08-05]
CHR Extension: (Chrome Media Router) - C:\Users\o\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm [2018-12-07]

========== 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 ekrn; C:\Program Files\ESET\ESET Security\ekrn.exe [2302160 2018-12-05] (ESET)
R3 ekrnEpfw; C:\Program Files\ESET\ESET Security\ekrn.exe [2302160 2018-12-05] (ESET)
S4 ssh-agent; C:\WINDOWS\System32\OpenSSH\ssh-agent.exe [384512 2018-09-15] ()
S3 WdNisSvc; C:\ProgramData\Microsoft\Windows Defender\platform\4.18.1807.18075-0\NisSrv.exe [3905952 2018-08-05] (Microsoft Corporation)
S3 WinDefend; C:\ProgramData\Microsoft\Windows Defender\platform\4.18.1807.18075-0\MsMpEng.exe [110944 2018-08-05] (Microsoft Corporation)
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

========== 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.)

R1 eamonm; C:\WINDOWS\System32\DRIVERS\eamonm.sys [143448 2018-10-25] (ESET)
R0 edevmon; C:\WINDOWS\System32\DRIVERS\edevmon.sys [107896 2018-10-25] (ESET)
S0 eelam; C:\WINDOWS\System32\DRIVERS\eelam.sys [15872 2018-07-12] (ESET)
R1 ehdrv; C:\WINDOWS\system32\DRIVERS\ehdrv.sys [188832 2018-10-25] (ESET)
R2 ekbdflt; C:\WINDOWS\System32\drivers\ekbdflt.sys [50144 2018-10-25] (ESET)
R1 epfw; C:\WINDOWS\system32\DRIVERS\epfw.sys [82304 2018-10-25] (ESET)
R1 epfwwfp; C:\WINDOWS\system32\DRIVERS\epfwwfp.sys [109864 2018-10-25] (ESET)
S3 iaLPSS2_GPIO2; C:\WINDOWS\System32\drivers\iaLPSS2_GPIO2.sys [84264 2015-06-16] (Intel Corporation)
S3 leusbser; C:\WINDOWS\System32\drivers\leusbser.sys [238080 2015-04-14] (QUALCOMM Incorporated)
R3 nvlddmkm; C:\WINDOWS\System32\DriverStore\FileRepository\nv_dispi.inf_amd64_485c1c3102021986\nvlddmkm.sys [17200392 2018-06-25] (NVIDIA Corporation)
S3 nvvhci; C:\WINDOWS\System32\drivers\nvvhci.sys [65792 2018-04-24] (NVIDIA Corporation)
S3 qcusbser; C:\WINDOWS\System32\drivers\qcusbser.sys [254520 2017-03-15] (QUALCOMM Incorporated)

R3 rt640x64; C:\WINDOWS\System32\drivers\rt640x64.sys [605696 2018-09-15] (Realtek)
S3 WdBoot; C:\WINDOWS\system32\drivers\wd\WdBoot.sys [46584 2018-08-05] (Microsoft Corporation)
S3 WdFilter; C:\WINDOWS\system32\drivers\wd\WdFilter.sys [340008 2018-08-05] (Microsoft Corporation)
S3 WdNisDrv; C:\WINDOWS\System32\drivers\wd\WdNisDrv.sys [61992 2018-08-05] (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) ========

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

2019-01-15 16:32 - 2019-01-15 16:32 - 000035445 _____ C:\Users\o\Downloads\Addition.txt
2019-01-15 16:31 - 2019-01-15 16:39 - 000014768 _____ C:\Users\o\Downloads\FRST.txt
2019-01-15 16:30 - 2019-01-15 16:39 - 000000000 ____D C:\FRST
2019-01-15 16:29 - 2019-01-15 16:29 - 002427904 _____ (Farbar) C:\Users\o\Downloads\FRST64.exe
2019-01-15 07:16 - 2019-01-15 07:16 - 000000000 ___HD C:\OneDriveTemp
2019-01-09 12:26 - 2019-01-09 12:26 - 026806784 _____ (Microsoft Corporation) C:\WINDOWS\system32\edgehtml.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 023440384 _____ (Microsoft Corporation) C:\WINDOWS\system32\mshtml.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 020811776 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\edgehtml.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 019024384 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\mshtml.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 012858368 _____ (Microsoft Corporation) C:\WINDOWS\system32\ieframe.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 012151808 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\ieframe.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 009677352 _____ (Microsoft Corporation) C:\WINDOWS\system32\ntoskrnl.exe
2019-01-09 12:26 - 2019-01-09 12:26 - 007857152 _____ (Microsoft Corporation) C:\WINDOWS\system32\Chakra.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 007645600 _____ (Microsoft Corporation) C:\WINDOWS\system32\Windows.Media.Protection.PlayReady.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 006544800 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\Windows.Media.Protection.PlayReady.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 006057984 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\Chakra.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 005440016 _____ (Microsoft Corporation) C:\WINDOWS\system32\mfcore.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 004588544 _____ (Microsoft Corporation) C:\WINDOWS\system32\sppsvc.exe
2019-01-09 12:26 - 2019-01-09 12:26 - 003952952 _____ (Microsoft Corporation) C:\WINDOWS\system32\Windows.Mirage.dll

2019-01-09 12:26 - 2019-01-09 12:26 - 003550592 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\mfcore.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 003380224 _____ (Microsoft Corporation) C:\WINDOWS\system32\AppXDeploymentServer.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 003338328 _____ (Microsoft Corporation) C:\WINDOWS\system32\combase.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 003270144 _____ (Microsoft Corporation) C:\WINDOWS\system32\esent.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 002986352 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\Windows.Mirage.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 002929152 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\esent.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 002777432 _____ (Microsoft Corporation) C:\WINDOWS\system32\iertutil.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 002626360 _____ (Microsoft Corporation) C:\WINDOWS\system32\Drivers\ntfs.sys
2019-01-09 12:26 - 2019-01-09 12:26 - 002594872 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\combase.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 002469648 _____ (Microsoft Corporation) C:\WINDOWS\system32\msmpeg2vdec.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 002437552 _____ (Microsoft Corporation) C:\WINDOWS\system32\msxml6.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 002323696 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\msmpeg2vdec.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 002275896 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\iertutil.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 002186752 _____ (Microsoft Corporation) C:\WINDOWS\system32\AppXDeploymentExtensions.onecore.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 002021584 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\msxml6.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 001641616 _____ (Microsoft Corporation) C:\WINDOWS\system32\sppobjs.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 001616384 _____ (Microsoft Corporation) C:\WINDOWS\system32\lsasrv.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 001602560 _____ (Microsoft Corporation) C:\WINDOWS\system32\AppXDeploymentExtensions.desktop.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 001388032 _____ (Microsoft Corporation) C:\WINDOWS\system32\bcastdvruserservice.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 001309696 _____ (Microsoft Corporation) C:\WINDOWS\system32\webplatstorageserver.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 001255736 _____ (Microsoft Corporation) C:\WINDOWS\system32\hvix64.exe
2019-01-09 12:26 - 2019-01-09 12:26 - 001212416 _____ (Microsoft Corporation) C:\WINDOWS\system32\rpcss.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 001201136 _____ (Microsoft Corporation) C:\WINDOWS\system32\mfmpeg2srcsnk.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 001058848 _____ (Microsoft Corporation) C:\WINDOWS\system32\ApplyTrustOffline.exe
2019-01-09 12:26 - 2019-01-09 12:26 - 001050936 _____ (Microsoft Corporation) C:\WINDOWS\system32\hvax64.exe
2019-01-09 12:26 - 2019-01-09 12:26 - 001022464 _____ (Microsoft Corporation) C:\WINDOWS\system32\Windows.Media.MixedRealityCapture.dll

2019-01-09 12:26 - 2019-01-09 12:26 - 000998912 _____ (Microsoft Corporation) C:\WINDOWS\system32\kerberos.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 000912384 _____ (Microsoft Corporation) C:\WINDOWS\system32\EdgeManager.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 000870400 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\Windows.Media.MixedRealityCapture.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 000833536 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\webplatstorageserver.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 000773120 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\kerberos.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 000735232 _____ (Microsoft Corporation) C:\WINDOWS\system32\Windows.Web.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 000663040 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\EdgeManager.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 000662528 ____R (Microsoft Corporation) C:\WINDOWS\system32\MixedRealityCapture.Pipeline.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 000570368 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\Windows.Web.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 000463672 _____ (Microsoft Corporation) C:\WINDOWS\system32\msv1_0.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 000448000 _____ (Microsoft Corporation) C:\WINDOWS\system32\Windows.Graphics.Printing.Workflow.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 000387384 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\msv1_0.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 000352768 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\msrd3x40.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 000312832 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\Windows.Graphics.Printing.Workflow.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 000178696 _____ (Microsoft Corporation) C:\WINDOWS\system32\Drivers\ksecpkg.sys
2019-01-09 12:26 - 2019-01-09 12:26 - 000155648 _____ (Microsoft Corporation) C:\WINDOWS\system32\dssvc.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 000140808 _____ (Microsoft Corporation) C:\WINDOWS\system32\Drivers\tm.sys
2019-01-09 12:26 - 2019-01-09 12:26 - 000139776 _____ (Microsoft Corporation) C:\WINDOWS\SysWOW64\PrintWorkflowService.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 000098816 ____R (Microsoft Corporation) C:\WINDOWS\system32\MixedRealityCapture.Broker.dll
2019-01-09 12:26 - 2019-01-09 12:26 - 000092160 _____ (Microsoft Corporation) C:\WINDOWS\system32\Drivers\wanarp.sys
2019-01-09 12:26 - 2019-01-09 12:26 - 000047112 _____ (Microsoft Corporation) C:\WINDOWS\system32\browser_broker.exe
2019-01-09 12:26 - 2019-01-09 12:26 - 000000315 _____ C:\WINDOWS\system32\DrtmAuth8.bin
2019-01-09 12:26 - 2019-01-09 12:26 - 000000315 _____ C:\WINDOWS\system32\DrtmAuth7.bin
2019-01-09 12:26 - 2019-01-09 12:26 - 000000315 _____ C:\WINDOWS\system32\DrtmAuth6.bin
2019-01-09 12:26 - 2019-01-09 12:26 - 000000315 _____ C:\WINDOWS\system32\DrtmAuth5.bin
2019-01-09 12:26 - 2019-01-09 12:26 - 000000315 _____ C:\WINDOWS\system32\DrtmAuth4.bin

2019-01-09 12:26 - 2019-01-09 12:26 - 000000315 _____
C:\WINDOWS\system32\DrtmAuth3.bin
2019-01-09 12:26 - 2019-01-09 12:26 - 000000315 _____
C:\WINDOWS\system32\DrtmAuth2.bin
2019-01-09 12:26 - 2019-01-09 12:26 - 000000315 _____
C:\WINDOWS\system32\DrtmAuth1.bin
2018-12-26 17:01 - 2018-12-26 17:01 - 000017582 _____
C:\WINDOWS\system32\cc_20181226_170121.reg
2018-12-20 17:08 - 2018-12-20 17:08 - 000000000 ___RD
C:\Users\o\Downloads\Microsoft.SkypeApp_kzf8qxf38zg5c!App
2018-12-20 06:59 - 2018-12-20 06:59 - 000840192 _____ (Microsoft Corporation)
C:\WINDOWS\system32\jscript.dll
2018-12-20 06:59 - 2018-12-20 06:59 - 000684032 _____ (Microsoft Corporation)
C:\WINDOWS\SysWOW64\jscript.dll
2018-12-18 06:56 - 2018-12-18 06:57 - 014034832 _____ C:\Users\o\Downloads\zasilka-
HW8CJ883GMTWZ5JW.zip

========== One month (Modified) ========

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

2019-01-15 16:32 - 2018-09-15 08:31 - 000000000 ____D C:\WINDOWS\INF
2019-01-15 15:31 - 2018-09-15 08:33 - 000000000 ____D C:\ProgramData\regid.1991-
06.com.microsoft
2019-01-15 15:05 - 2018-08-06 06:40 - 000000000 ____D C:\Users\o\AppData\Roaming\eM
Client
2019-01-15 15:05 - 2016-12-16 15:46 - 000000000 ____D C:\Users\o\AppData\LocalLow\Mozilla
2019-01-15 15:04 - 2018-08-05 09:15 - 000000000 _____
C:\WINDOWS\system32\Drivers\lvuvc.hs
2019-01-15 13:22 - 2018-08-06 15:15 - 000000000 ____D
C:\Users\o\AppData\Roaming\WhatsApp
2019-01-15 12:27 - 2018-10-03 15:24 - 000000000 ____D C:\WINDOWS\system32\SleepStudy
2019-01-15 07:24 - 2018-09-15 08:33 - 000000000 ____D C:\WINDOWS\AppReadiness
2019-01-15 07:21 - 2018-08-05 14:14 - 000000000 ____D
C:\Users\o\AppData\Roaming\Seznam.cz
2019-01-15 07:20 - 2018-10-03 15:31 - 001693636 _____
C:\WINDOWS\system32\PerfStringBackup.INI
2019-01-15 07:20 - 2018-09-15 18:32 - 000716776 _____ C:\WINDOWS\system32\perfh005.dat
2019-01-15 07:20 - 2018-09-15 18:32 - 000144856 _____ C:\WINDOWS\system32\perfc005.dat
2019-01-15 07:17 - 2018-08-05 15:20 - 000000000 ____D C:\Users\o\AppData\Local\Spotify
2019-01-15 07:16 - 2018-10-03 15:28 - 000000006 ____H C:\WINDOWS\Tasks\SA.DAT
2019-01-15 07:16 - 2018-08-05 15:19 - 000000000 ____D C:\Users\o\AppData\Roaming\Spotify
2019-01-15 07:16 - 2018-08-05 09:15 - 000000000 ____D C:\ProgramData\NVIDIA
2019-01-15 07:16 - 2016-12-16 15:11 - 000000000 ___RD C:\Users\o\OneDrive
2019-01-14 17:32 - 2018-09-15 07:09 - 000524288 _____ C:\WINDOWS\system32\config\BBI
2019-01-14 09:58 - 2018-09-25 12:08 - 000000000 ____D C:\Users\o\Downloads\Zlatá promoce
2018
2019-01-12 07:39 - 2018-09-15 08:33 - 000000000 ___HD C:\Program Files\WindowsApps
2019-01-12 07:30 - 2018-08-05 14:06 - 000000000 ____D C:\Program Files\Mozilla Firefox
2019-01-12 07:30 - 2018-08-05 14:06 - 000000000 ____D C:\Program Files (x86)\Mozilla
Maintenance Service
2019-01-11 09:00 - 2018-08-05 14:06 - 000001005 _____

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Firefox.lnk
2019-01-09 17:34 - 2018-09-15 18:34 - 000000000 ____D C:\Program Files\Windows Photo Viewer
2019-01-09 17:34 - 2018-09-15 18:34 - 000000000 ____D C:\Program Files (x86)\Windows Photo Viewer
2019-01-09 17:34 - 2018-09-15 08:33 - 000000000 ____D C:\WINDOWS\bcastdvr
2019-01-09 12:26 - 2018-09-15 08:23 - 000000000 ____D C:\WINDOWS\CbsTemp
2019-01-09 12:24 - 2018-08-05 16:39 - 000000000 ____D C:\WINDOWS\system32\MRT
2019-01-09 12:23 - 2018-08-05 16:39 - 132790320 ____C (Microsoft Corporation) C:\WINDOWS\system32\MRT.exe
2019-01-04 14:53 - 2016-12-05 09:57 - 000002457 _____ C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Acrobat Reader DC.lnk
2019-01-02 20:48 - 2018-09-15 08:36 - 000835480 _____ (Adobe Systems Incorporated) C:\WINDOWS\SysWOW64\FlashPlayerApp.exe
2019-01-02 20:48 - 2018-09-15 08:36 - 000179600 _____ (Adobe Systems Incorporated) C:\WINDOWS\SysWOW64\FlashPlayerCPLApp.cpl
2019-01-02 15:50 - 2018-08-20 16:21 - 000000000 ____D C:\Users\o\AppData\Roaming\vlc
2019-01-02 09:42 - 2018-08-30 09:31 - 000000000 ____D C:\Users\o\Documents\Platby od 8. 2018
2019-01-01 12:27 - 2018-08-05 09:19 - 000000000 ____D C:\Users\o\AppData\Local\Comms
2018-12-26 17:04 - 2018-08-06 06:08 - 000001079 _____ C:\Users\Public\Desktop\Revo Uninstaller.lnk
2018-12-26 17:04 - 2016-11-25 17:44 - 000000000 ____D C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Revo Uninstaller
2018-12-24 10:16 - 2018-08-06 15:15 - 000000000 ____D C:\Users\o\AppData\Local\WhatsApp
2018-12-24 10:15 - 2018-08-06 15:15 - 000002241 _____ C:\Users\o\Desktop\WhatsApp.lnk
2018-12-24 10:15 - 2018-08-06 15:15 - 000000000 ____D C:\Users\o\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\WhatsApp
2018-12-24 10:14 - 2018-08-06 15:15 - 000000000 ____D C:\Users\o\AppData\Local\SquirrelTemp
2018-12-20 12:25 - 2018-10-03 15:28 - 000003472 _____ C:\WINDOWS\System32\Tasks\GoogleUpdateTaskMachineUA
2018-12-20 12:25 - 2018-10-03 15:28 - 000003348 _____ C:\WINDOWS\System32\Tasks\GoogleUpdateTaskMachineCore

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

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

C:\WINDOWS\system32\winlogon.exe => File is digitally signed
C:\WINDOWS\system32\wininit.exe => File is digitally signed
C:\WINDOWS\explorer.exe => File is digitally signed
C:\WINDOWS\SysWOW64\explorer.exe => File is digitally signed
C:\WINDOWS\system32\svchost.exe => File is digitally signed
C:\WINDOWS\SysWOW64\svchost.exe => File is digitally signed
C:\WINDOWS\system32\services.exe => File is digitally signed
C:\WINDOWS\system32\User32.dll => File is digitally signed
C:\WINDOWS\SysWOW64\User32.dll => File is digitally signed
C:\WINDOWS\system32\userinit.exe => File is digitally signed
C:\WINDOWS\SysWOW64\userinit.exe => File is digitally signed
C:\WINDOWS\system32\rpcss.dll => File is digitally signed
C:\WINDOWS\system32\dnsapi.dll => File is digitally signed

C:\WINDOWS\SysWOW64\dnsapi.dll => File is digitally signed
C:\WINDOWS\system32\Drivers\volsnap.sys => File is digitally signed

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