Script ZhpFix

SysRestore

EmptyPrefetch

EmptyTemp

EmtyFlash

ShortcutFix

FirewallRaz

O42 - Logiciel: Google Update Helper - (.Google Inc..) [HKLM] -- {A92DAB39-4E2C-4304-9AB6-BC44E68B55E2}

O43 - CFD: 18/12/2013 - [0] SHD -- C:\ProgramData\{01BD4FC9-2F86-4706-A62E-774BB7E9D308}

O43 - CFD: 16/01/2016 - [] D -- C:\windows\System32\Config\systemprofile\AppData\Local\LavasoftTcpService

HKLM64\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{A92DAB39-4E2C-4304-9AB6-BC44E68B55E2} HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{A92DAB39-4E2C-4304-9AB6-BC44E68B55E2} C:\windows\System32\Config\systemprofile\AppData\Local\LavasoftTcpService

 [MD5.00000000000000000000000000000000] [APT] [AVG-SSU\_0616tb] (...) -- C:\ProgramData\Avg\_Update\_0616tb\AVG-Secure-Search-Update\_0616tb.exe (.not file.) [0] (.Activate.)

[MD5.00000000000000000000000000000000] [APT] [AVG-SSU\_0616tb\_DELETE] (...) -- C:\ProgramData\Avg\_Update\_0616tb\AVG-Secure-Search-Update\_0616tb.exe (.not file.) [0] (.Activate.) [MD5.00000000000000000000000000000000] [APT] [{7F282B1F-500C-4314-B580-69138AE62446}] (...) -- C:\Program Files\WonTube\Free Video Converter\FreeVideoConverter.exe (.not file.) [0] (.Activate.)

[MD5.00000000000000000000000000000000] [APT] [{896459BF-076A-4AA5-B872-832CD80F6078}] (...) -- C:\Program Files\Empire Interactive\Ford Racing 2\fr2.exe (.not file.) [0] (.Activate.)

[MD5.00000000000000000000000000000000] [APT] [{91F35AA1-79A1-4820-BE29-E48CA5771BCA}] (...) -- C:\Program Files\Empire Interactive\Ford Racing 2\fr2.exe (.not file.) [0] (.Activate.)

[MD5.00000000000000000000000000000000] [APT] [{D7CFE890-65EB-479B-90D1-DFFE8B505EE6}] (...) -- C:\Program Files\FIFA 15\OriginSetup.exe (.not file.) [0] (.Activate.)

O39 - APT: AVG-SSU\_0616tb - (...) -- C:\windows\Tasks\AVG-SSU\_0616tb.job [572] (.Orphan.)

O39 - APT: AVG-SSU\_0616tb\_DELETE - (...) -- C:\windows\Tasks\AVG-SSU\_0616tb\_DELETE.job [434] (.Orphan.)

O39 - APT: AVG-SSU\_0616tb - (...) -- C:\windows\System32\Tasks\AVG-SSU\_0616tb [2868] (.Orphan.)

O39 - APT: AVG-SSU\_0616tb\_DELETE - (...) -- C:\windows\System32\Tasks\AVG-SSU\_0616tb\_DELETE [2936] (.Orphan.)

O87 - FAEL: "TCP Query User{DA6F22AD-F54C-4244-8BD6-4F9F5B2372E4}C:\program files\winter sports 2011\wintersports\_stripped\_dx9.exe" [In-None-P6-TRUE] .(...) -- C:\program files\winter sports 2011\wintersports\_stripped\_dx9.exe (.not file.)

O87 - FAEL: "UDP Query User{9BB50A6E-9D80-4716-AB0C-E993A9D4C882}C:\program files\winter sports 2011\wintersports\_stripped\_dx9.exe" [In-None-P17-TRUE] .(...) -- C:\program files\winter sports 2011\wintersports\_stripped\_dx9.exe (.not file.)

O87 - FAEL: "TCP Query User{02A5B8EE-FEDC-4838-90F4-DC70F109D554}C:\users\oriane\appdata\local\popcorn time\node-webkit\popcorn time.exe" [In-None-P6-TRUE] .(...) -- C:\users\oriane\appdata\local\popcorn time\node-webkit\popcorn time.exe (.not file.)

O87 - FAEL: "UDP Query User{4FFED7C3-099A-4380-896D-A9C512FC5086}C:\users\oriane\appdata\local\popcorn time\node-webkit\popcorn time.exe" [In-None-P17-TRUE] .(...) -- C:\users\oriane\appdata\local\popcorn time\node-webkit\popcorn time.exe (.not file.)

O87 - FAEL: "TCP Query User{0BDE8CC5-EE30-4DD7-AFF2-7E099ED8737A}C:\program files\emuletorrent\emuletorrent.exe" [In-None-P6-TRUE] .(...) -- C:\program files\emuletorrent\emuletorrent.exe (.not file.)

O87 - FAEL: "UDP Query User{288FD314-EFFA-496C-94A3-F1AD41E726D2}C:\program files\emuletorrent\emuletorrent.exe" [In-None-P17-TRUE] .(...) -- C:\program files\emuletorrent\emuletorrent.exe (.not file.)

O87 - FAEL: "TCP Query User{936B374E-BC60-405C-B289-58CEDCA8D2E9}C:\program files\emule\emule.exe" [In-None-P6-TRUE] .(...) -- C:\program files\emule\emule.exe (.not file.)

O87 - FAEL: "UDP Query User{26EC70B3-8737-4805-9B71-73C7C850E408}C:\program files\emule\emule.exe" [In-None-P17-TRUE] .(...) -- C:\program files\emule\emule.exe (.not file.)

 G2 - GCE: Preference [User Data\Default] [pkedcjkdefgpdelpbcmbmeomcjbeemfm] Chrome Media Router

O4 - HKCU\..\Run: [AVG-Secure-Search-Update\_1213b] C:\Users\Oriane\AppData\Roaming\AVG 1213b Campaign\AVG-Secure-Search-Update-1213b.exe (.not file.)

O4 - HKCU\..\Run: [AVG-Secure-Search-Update\_0214c] C:\Users\Oriane\AppData\Roaming\AVG 0214c Campaign\AVG-Secure-Search-Update-0214c.exe (.not file.)

O4 - HKUS\S-1-5-21-1072828290-3828818215-1948454868-1001\..\Run: [AVG-Secure-Search-Update\_1213b] C:\Users\Oriane\AppData\Roaming\AVG 1213b Campaign\AVG-Secure-Search-Update-1213b.exe (.not file.)

O4 - HKUS\S-1-5-21-1072828290-3828818215-1948454868-1001\..\Run: [AVG-Secure-Search-Update\_0214c] C:\Users\Oriane\AppData\Roaming\AVG 0214c Campaign\AVG-Secure-Search-Update-0214c.exe (.not file.) => HKLM\SOFTWARE\ASK

HKLM\SOFTWARE\AVG Web TuneUp

HKCU\SOFTWARE\AVG Web TuneUp

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\NOHIDDEN] CheckedValue: Modified