Zoek.exe v5.0.0.0 Updated 07-March-2015
Tool run by B on za 07-03-2015 at 1:15:08,30.
Microsoft® Windows Vista™ Home Basic 6.0.6002 Service Pack 2 x86
Running in: Normal Mode Internet Access Detected
Launched: c:\Users\Bosman\Downloads\zoek.exe [Scan all users] [Script inserted] [Checkboxes used]

==== Older Logs ====================

C:\zoek-results2015-03-06-235626.log 36188 bytes

==== Running Processes ====================

C:\Windows\system32\csrss.exe
C:\Windows\system32\wininit.exe
C:\Windows\system32\csrss.exe
C:\Windows\system32\winlogon.exe
C:\Windows\system32\services.exe
C:\Windows\system32\lsass.exe
C:\Windows\system32\lsm.exe
C:\Windows\system32\svchost.exe -k DcomLaunch
C:\Windows\system32\svchost.exe -k rpcss
C:\Program Files\Trusteer\Rapport\bin\RapportMgmtService.exe
C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
C:\Windows\system32\svchost.exe -k netsvcs
C:\Windows\system32\svchost.exe -k GPSvcGroup
C:\Windows\system32\SLsvc.exe
C:\Windows\system32\svchost.exe -k LocalService
C:\Windows\system32\svchost.exe -k NetworkService
C:\Windows\System32\spoolsv.exe
C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
C:\Program Files\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe
C:\Program Files\AVG\AVG2015\avgwdsvc.exe
C:\Program Files\Bonjour\mDNSResponder.exe
C:\Windows\system32\svchost.exe -k hpdevmgmt
C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted
C:\Program Files\Microsoft\BingBar\SeaPort.EXE
C:\Windows\system32\svchost.exe -k imgsvc
C:\Windows\System32\svchost.exe -k WerSvcGroup
C:\Program Files\Common Files\Microsoft Shared\Windows Live\WLIDSVC.EXE
C:\Windows\system32\SearchIndexer.exe
C:\Program Files\Common Files\Microsoft Shared\Windows Live\WLIDSvcM.exe
C:\Windows\system32\taskeng.exe
C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
C:\Windows\system32\taskeng.exe
C:\Windows\system32\Dwm.exe
C:\Windows\Explorer.EXE
C:\Program Files\Trusteer\Rapport\bin\RapportService.exe
C:\Windows\RtHDVCpl.exe
C:\Program Files\DivX\DivX Update\DivXUpdate.exe

C:\Program Files\AVG\AVG2015\avgui.exe
C:\Program Files\iTunes\iTunesHelper.exe
C:\Program Files\Common Files\Java\Java Update\jusched.exe
C:\Program Files\Windows Media Player\wmpnscfg.exe
C:\Program Files\Windows Media Player\wmpnetwk.exe
C:\Program Files\Mozilla Firefox\firefox.exe
C:\Program Files\iPod\bin\iPodService.exe
C:\Windows\system32\ctfmon.exe
C:\Windows\system32\taskeng.exe
C:\Windows\system32\sdclt.exe
c:\Users\Bosman\Downloads\zoek.exe
C:\Windows\system32\wbem\wmiprvse.exe
C:\Windows\system32\taskeng.exe

==== Windows Installer Info ======================

Adobe Reader 9.5.5 - Nederlands
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\68AB67CA7DA73401B7449A0500000010]C:\Windows\Installer\179e25.msi
Apple Application Support (32-bit)
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\55000EF23F4CA7F4EADD1E895DC41FF2]C:\Windows\Installer\1297052a.msi
Apple Mobile Device Support
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\A284DE82BD659D74D8E999F08ADCD7D3]C:\Windows\Installer\12970599.msi
Apple Software Update
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\56A9756CEAC913B4B8B633600E36A066]C:\Windows\Installer\9e48d.msi
AVG 2015
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\7E7ACF6B233FE5C46A5E05650F1553D2]C:\Windows\Installer\8a84628.msi
AVG 2015
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\8576B8A088C66B3418CFED3DA792F1BC]C:\Windows\Installer\297b99b.msi
Bing Bar
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\D21EC9447C2E79B41BE9551D36AE4953]C:\Windows\Installer\127ad78.msi
Bonjour
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\B2F5519759897D9468219D52080EEDB5]C:\Windows\Installer\7681d.msi
BufferChm
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\42C2662EE13B94340A4823BE678E7B06]C:\Windows\Installer\e7072d.msi
D2400
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\E6E764F22D7Fcc34199BF4CC01A53ED0]C:\Windows\Installer\e707b1.msi
D2400_Help
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\818B1259EC9182d42800DD6231E3916E]C:\Windows\Installer\e707b8.msi

D3DX10
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\7BD4C90EC03660F46A13E87A329932FA]C:\Windows\Installer\5fb0e.msi
DeviceDiscovery
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\A5ADA1FEA1B02664C85547576AD1B856]C:\Windows\Installer\2aafc8.msi
DeviceManagementQFolder
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\EA15D5BA3CBED83478C207C5C702480B]C:\Windows\Installer\e70733.msi
dj_sf_ProductContext
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\46007C513642dd94A9887B007FB54B82]C:\Windows\Installer\e707ab.msi
dj_sf_software
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\D011936BF747CD046928599DE47F7309]C:\Windows\Installer\e7070b.msi
dj_sf_software_req
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\04B22C5721D6934408CDAC3B13E3DA5A]C:\Windows\Installer\e70711.msi
Google Toolbar for Internet Explorer
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\18555481990E8AB4CBB63FB4F26006C0]C:\Windows\Installer\3201e9.msi
Google Update Helper
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\93BAD29AC2E44034A96BCB446EB8552E]C:\Windows\Installer\5900966.msi
Google Update Helper
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\A089CE062ADB6BC44A720BA745894BAC]C:\Windows\Installer\47f8590.msi
HP Photosmart Essential2.01
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\B2839838AB3578A48845193E8DA0A57C]C:\Windows\Installer\e7079f.msi
HP Update
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\C4E4AFE2F5B77F841A0CA18A287B9A3C]C:\Windows\Installer\a618e01.msi
HPSSupply
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\B9B0B7844DCDD044980A6ADE1E5A543A]C:\Windows\Installer\e70792.msi
iCloud
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\2B66DB97EAD4B3C40BE8CD275E701C36]C:\Windows\Installer\b5edd0.msi
iTunes
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\B6A2308B0D4C44747BF5D9CD5BB6C5F6]C:\Windows\Installer\129716a5.msi
Java 8 Update 40
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\4EA42A62D9304AC4784BF2381208040F]C:\Windows\Installer\a732ac.msi
JavaFX 2.1.0
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData

\S-1-5-18\Products\F6071111A6667304777712308267D401]C:\Windows\Installer\14a5451.msi
Messenger Companion
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\E52D2418A820365468DE755587C30892]C:\Windows\Installer\5fbd3.msi
Microsoft .NET Framework 3.5 Language Pack SP1 - nld
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\7D837101508D9A73BB19F1C2537128FB]C:\Windows\Installer\2514d26.msi
Microsoft .NET Framework 3.5 SP1
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-
18\Products\26DDC2EC4210AC63483DF9D4FCC5B59D]C:\Windows\Installer\98c21e.msi
Microsoft .NET Framework 4.5.1 (NLD)
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\E68D19A1421347534AFB04761662C5AF]C:\Windows\Installer\24910e1.msi
Microsoft .NET Framework 4.5.1
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-
18\Products\271D3094BCCDF293393A43ACD974EFD3]C:\Windows\Installer\3a0c292.msi
Microsoft Application Error Reporting
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\000021599B0090400000000000F01FEC]C:\Windows\Installer\5fb18.msi
Microsoft Silverlight
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-
18\Products\D7314F9862C648A4DB8BE2A5B47BE100]C:\Windows\Installer\1371678.msi
Microsoft Visual C++ 2005 ATL Update kb973923 - x86 8.0.50727.4053
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\0D756077321A70C3E844C138CE981581]C:\Windows\Installer\331fd09.msi
Microsoft Visual C++ 2005 Redistributable
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\c1c4f01781cc94c4c8fb1542c0981a2a]C:\Windows\Installer\12aacf3.msi
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30411
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-
18\Products\DC6F8AD5E07C8D934803D389806DDB71]C:\Windows\Installer\162ad99.msi
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\CFD2C1F142D260E3CB8B271543DA9F98]C:\Windows\Installer\14595b.msi
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\6E815EB96CCE9A53884E7857C57002F0]C:\Windows\Installer\1ffabaa.msi
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-
18\Products\1D5E3C0FEDA1E123187686FED06E995A]C:\Windows\Installer\240e1799.msi
MobileMe Control Panel
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\8E0DB6293A422D14FAB943F0A173DE21]C:\Windows\Installer\36e783.msi
MSVCRT
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\A6C64DD86500CEF47BA082BB611A1FF1]C:\Windows\Installer\5fb09.msi
OpenOffice.org 3.4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\7FB3CE3A012E94A42964597AAD183FC9]C:\Windows\Installer\162ad9d.msi
PanoStandAlone
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\4D738037E5FFBD84AB94337E23FD0F3B]C:\Windows\Installer\e70746.msi
PSSWCORE
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\CDD2E27F8BD309142AD13688D359F57E]C:\Windows\Installer\e70799.msi
QuickTime 7
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\C2CBC2D34D56364478BABBC258C9F1E3]C:\Windows\Installer\33ca310.msi
Rapport
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\D7E18DD182D0BEC4782B0C144ACF2B51]C:\Windows\Installer\3627b.msi
Security Update for CAPICOM (KB931906)
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9F2FDFE0D6387BE43AD230B83D1FBFA2]C:\Windows\Installer\98c230.msi
Segoe UI
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\DBCF4DD51C3A5514E97114167CA0AAAB]C:\Windows\Installer\5fb13.msi
Skype Click to Call
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\7692FC6BE18C0C0489510C7547EF1F02]C:\Windows\Installer\2944e21.msi
SkypeT 6.9
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\E7FF67E4ABEA78C47B88DC745E24B5D9]C:\Windows\Installer\63575.msi
Spelling Dictionaries Support For Adobe Reader 9
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\68AB67CA7DA7464543820900000000040]C:\Windows\Installer\56245.msi
Status
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\E53B982070CDa7c47901BB6D68AEB4D7]C:\Windows\Installer\2aafbe.msi
TomTom HOME
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\D484EC62E8E25D042B1551183311C496]C:\Windows\Installer\1082a6a.msi
TomTom HOME Visual Studio Merge Modules
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\5C13C3F8A3C98AA4E8AF1792A0A75D33]C:\Windows\Installer\16d13e9.msi
Toolbox
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\DBE81C9EEB580D74AA37F3DECC79B640]C:\Windows\Installer\e70723.msi
TrayApp
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\7404D2C904E0a994CAA74C9BBB21EF30]C:\Windows\Installer\2aaf7a.msi
UnloadSupport
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\C839E3454CDB33946A211092936948F5]C:\Windows\Installer\e70717.msi
VC80CRTRedist - 8.0.50727.4053
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData

\S-1-5-18\Products\952D7EE5731D8344A9F5244F23CE4012]C:\Windows\Installer\264ee84.msi
VideoToolkit01
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\9383D4281AAD51348A22A73E6E025E82]C:\Windows\Installer\e707a5.msi
Visual Studio 2012 x86 Redistributables
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-
18\Products\A91FFE89BA03B4E49B340FB6C136BE8F]C:\Windows\Installer\b3258c9.msi
WebReg
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\4B83AF924EA0D0D4A8151656BB99B00B]C:\Windows\Installer\e7071d.msi
Windows Live Communications Platform
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\3D04254D3B6B9FF42B3445CE3E1E0066]C:\Windows\Installer\5fb2c.msi
Windows Live Essentials
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\B53C70A248384AD4A95944B2C6980A37]C:\Windows\Installer\5fba5.msi
Windows Live ID Sign-in Assistant
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\A8D0516CDE683D1478BB3FBB150B7BF7]C:\Windows\Installer\5fad6.msi
Windows Live Installer
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\F132F0B0A6ECD384AA32773B467F9571]C:\Windows\Installer\5faf0.msi
Windows Live Mesh - ActiveX-besturingselement voor externe verbindingen
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\C55EC23CAB21159478799076DFFE55F6]C:\Windows\Installer\755199.msi
Windows Live Messenger
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\11F12B5E3396B0E42AC597363E0CD711]C:\Windows\Installer\5fb71.msi
Windows Live Messenger
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\59D49284A9EE7734283144CF2456BF72]C:\Windows\Installer\5fbc3.msi
Windows Live Messenger Companion Core
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\C4B69A87346AF0D4892C8A1EA666969F]C:\Windows\Installer\5fb8c.msi
Windows Live Photo Common
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\0D262DB9887B64540A5A4F5FE63C38B4]C:\Windows\Installer\5fbb3.msi
Windows Live Photo Common
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\B6ACDB9A3563B764CA384963D73AFB3E]C:\Windows\Installer\5fb4d.msi
Windows Live PIMT Platform
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\7B292C385A83B0447A137070E0186AF4]C:\Windows\Installer\5fb3d.msi
Windows Live SOXE
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\F4E3B286A696ED244AC1C470AE61874B]C:\Windows\Installer\5fb22.msi
Windows Live SOXE Definitions
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\26CEF00243C306D4C98ECE73E2100CF8]C:\Windows\Installer\5fb1d.msi
Windows Live UX Platform
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData

\S-1-5-18\Products\E97A59ECCF4EFFF4A857920FB449F22F]C:\Windows\Installer\5fadb.msi
Windows Live UX Platform Language Pack
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData
\S-1-5-18\Products\9FC52F6D78E4BE343B421CB29EDC6D86]C:\Windows\Installer\5fb9a.msi

==== Checking Systemdrive for Symlinks ======================

 Het volume in station C heeft geen naam.
 Het volumenummer is D270-79FF

 Map van C:\

02-11-2006 13:59   <KOPPELING>   Documents and Settings [C:\Users]
               0 bestand(en)   0 bytes

 Map van C:\Program Files\Windows NT

29-09-2009 15:05   <KOPPELING>   Bureau-accessoires [C:\Program Files\Windows
NT\Accessories]
               0 bestand(en)   0 bytes

 Map van C:\ProgramData

02-11-2006 13:59   <KOPPELING>   Application Data [C:\ProgramData]
29-09-2009 15:05   <KOPPELING>   Bureaublad [C:\Users\Public\Desktop]
02-11-2006 13:59   <KOPPELING>   Desktop [C:\Users\Public\Desktop]
29-09-2009 15:05   <KOPPELING>   Documenten [C:\Users\Public\Documents]
02-11-2006 13:59   <KOPPELING>   Documents [C:\Users\Public\Documents]
29-09-2009 15:05   <KOPPELING>   Favorieten [C:\Users\Public\Favorites]
02-11-2006 13:59   <KOPPELING>   Favorites [C:\Users\Public\Favorites]
29-09-2009 15:05   <KOPPELING>   Menu Start [C:\ProgramData\Microsoft\Windows\Start
Menu]
29-09-2009 15:05   <KOPPELING>   Sjablonen
[C:\ProgramData\Microsoft\Windows\Templates]
02-11-2006 13:59   <KOPPELING>   Start Menu [C:\ProgramData\Microsoft\Windows\Start
Menu]
02-11-2006 13:59   <KOPPELING>   Templates
[C:\ProgramData\Microsoft\Windows\Templates]
               0 bestand(en)   0 bytes

 Map van C:\ProgramData\Microsoft\Windows\Start Menu

29-09-2009 15:05   <KOPPELING>   Programma's [C:\ProgramData\Microsoft\Windows\Start
Menu\Programs]
               0 bestand(en)   0 bytes

 Map van C:\ProgramData\Oracle\Java\javapath

04-03-2015 15:39   <SYMLINK>   java.exe [C:\Program Files\Java\jre1.8.0_40\bin\java.exe]
04-03-2015 15:39   <SYMLINK>   javaw.exe [C:\Program Files\Java\jre1.8.0_40\bin\javaw.exe]
04-03-2015 15:39   <SYMLINK>   javaws.exe [C:\Program
Files\Java\jre1.8.0_40\bin\javaws.exe]

```
               3 bestand(en)              0 bytes

 Map van C:\Users

02-11-2006  13:59    <SYMLINKD>     All Users [C:\ProgramData]
02-11-2006  13:59    <KOPPELING>    Default User [C:\Users\Default]
               0 bestand(en)              0 bytes

 Map van C:\Users\All Users

02-11-2006  13:59    <KOPPELING>    Application Data [C:\ProgramData]
29-09-2009  15:05    <KOPPELING>    Bureaublad [C:\Users\Public\Desktop]
02-11-2006  13:59    <KOPPELING>    Desktop [C:\Users\Public\Desktop]
29-09-2009  15:05    <KOPPELING>    Documenten [C:\Users\Public\Documents]
02-11-2006  13:59    <KOPPELING>    Documents [C:\Users\Public\Documents]
29-09-2009  15:05    <KOPPELING>    Favorieten [C:\Users\Public\Favorites]
02-11-2006  13:59    <KOPPELING>    Favorites [C:\Users\Public\Favorites]
29-09-2009  15:05    <KOPPELING>    Menu Start [C:\ProgramData\Microsoft\Windows\Start
Menu]
29-09-2009  15:05    <KOPPELING>    Sjablonen
[C:\ProgramData\Microsoft\Windows\Templates]
02-11-2006  13:59    <KOPPELING>    Start Menu [C:\ProgramData\Microsoft\Windows\Start
Menu]
02-11-2006  13:59    <KOPPELING>    Templates
[C:\ProgramData\Microsoft\Windows\Templates]
               0 bestand(en)              0 bytes

 Map van C:\Users\All Users\Microsoft\Windows\Start Menu

29-09-2009  15:05    <KOPPELING>    Programma's [C:\ProgramData\Microsoft\Windows\Start
Menu\Programs]
               0 bestand(en)              0 bytes

 Map van C:\Users\All Users\Oracle\Java\javapath

04-03-2015  15:39    <SYMLINK>      java.exe [C:\Program Files\Java\jre1.8.0_40\bin\java.exe]
04-03-2015  15:39    <SYMLINK>      javaw.exe [C:\Program Files\Java\jre1.8.0_40\bin\javaw.exe]
04-03-2015  15:39    <SYMLINK>      javaws.exe [C:\Program
Files\Java\jre1.8.0_40\bin\javaws.exe]
               3 bestand(en)              0 bytes

 Map van C:\Users\Bosman

29-09-2009  15:07    <KOPPELING>    Application Data [C:\Users\Bosman\AppData\Roaming]
29-09-2009  15:07    <KOPPELING>    Cookies
[C:\Users\Bosman\AppData\Roaming\Microsoft\Windows\Cookies]
29-09-2009  15:07    <KOPPELING>    Local Settings [C:\Users\Bosman\AppData\Local]
29-09-2009  15:07    <KOPPELING>    Menu Start
[C:\Users\Bosman\AppData\Roaming\Microsoft\Windows\Start Menu]
29-09-2009  15:07    <KOPPELING>    Mijn documenten [C:\Users\Bosman\Documents]
29-09-2009  15:07    <KOPPELING>    NetHood
[C:\Users\Bosman\AppData\Roaming\Microsoft\Windows\Network Shortcuts]
```

```
29-09-2009  15:07    <KOPPELING>    Netwerkprinteromgeving
[C:\Users\Bosman\AppData\Roaming\Microsoft\Windows\Printer Shortcuts]
29-09-2009  15:07    <KOPPELING>    Recent
[C:\Users\Bosman\AppData\Roaming\Microsoft\Windows\Recent]
29-09-2009  15:07    <KOPPELING>    SendTo
[C:\Users\Bosman\AppData\Roaming\Microsoft\Windows\SendTo]
29-09-2009  15:07    <KOPPELING>    Sjablonen
[C:\Users\Bosman\AppData\Roaming\Microsoft\Windows\Templates]
               0 bestand(en)              0 bytes

 Map van C:\Users\Bosman\AppData\Local

29-09-2009  15:07    <KOPPELING>    Application Data [C:\Users\Bosman\AppData\Local]
29-09-2009  15:07    <KOPPELING>    Geschiedenis
[C:\Users\Bosman\AppData\Local\Microsoft\Windows\History]
29-09-2009  15:07    <KOPPELING>    Temporary Internet Files
[C:\Users\Bosman\AppData\Local\Microsoft\Windows\Temporary Internet Files]
               0 bestand(en)              0 bytes

 Map van C:\Users\Bosman\AppData\LocalLow

30-07-2011  23:33    <KOPPELING>    PlayReady [C:\ProgramData\Microsoft\PlayReady]
               0 bestand(en)              0 bytes

 Map van C:\Users\Bosman\AppData\Roaming\Microsoft\Windows\Start Menu

29-09-2009  15:07    <KOPPELING>    Programma's
[C:\Users\Bosman\AppData\Roaming\Microsoft\Windows\Start Menu\Programs]
               0 bestand(en)              0 bytes

 Map van C:\Users\Bosman\Documents

29-09-2009  15:07    <KOPPELING>    Mijn afbeeldingen [C:\Users\Bosman\Pictures]
29-09-2009  15:07    <KOPPELING>    Mijn muziek [C:\Users\Bosman\Music]
29-09-2009  15:07    <KOPPELING>    Mijn video's [C:\Users\Bosman\Videos]
               0 bestand(en)              0 bytes

 Map van C:\Users\Default

02-11-2006  13:59    <KOPPELING>    Application Data [C:\Users\Default\AppData\Roaming]
02-11-2006  13:59    <KOPPELING>    Cookies
[C:\Users\Default\AppData\Roaming\Microsoft\Windows\Cookies]
02-11-2006  13:59    <KOPPELING>    Local Settings [C:\Users\Default\AppData\Local]
29-09-2009  15:05    <KOPPELING>    Menu Start
[C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu]
29-09-2009  15:05    <KOPPELING>    Mijn documenten [C:\Users\Default\Documents]
02-11-2006  13:59    <KOPPELING>    My Documents [C:\Users\Default\Documents]
02-11-2006  13:59    <KOPPELING>    NetHood
[C:\Users\Default\AppData\Roaming\Microsoft\Windows\Network Shortcuts]
29-09-2009  15:05    <KOPPELING>    Netwerkprinteromgeving
[C:\Users\Default\AppData\Roaming\Microsoft\Windows\Printer Shortcuts]
02-11-2006  13:59    <KOPPELING>    PrintHood
```

[C:\Users\Default\AppData\Roaming\Microsoft\Windows\Printer Shortcuts]
02-11-2006 13:59 <KOPPELING> Recent
[C:\Users\Default\AppData\Roaming\Microsoft\Windows\Recent]
02-11-2006 13:59 <KOPPELING> SendTo
[C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo]
29-09-2009 15:05 <KOPPELING> Sjablonen
[C:\Users\Default\AppData\Roaming\Microsoft\Windows\Templates]
02-11-2006 13:59 <KOPPELING> Start Menu
[C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu]
02-11-2006 13:59 <KOPPELING> Templates
[C:\Users\Default\AppData\Roaming\Microsoft\Windows\Templates]
0 bestand(en) 0 bytes

Map van C:\Users\Default\AppData\Local

02-11-2006 13:59 <KOPPELING> Application Data [C:\Users\Default\AppData\Local]
29-09-2009 15:05 <KOPPELING> Geschiedenis
[C:\Users\Default\AppData\Local\Microsoft\Windows\History]
02-11-2006 13:59 <KOPPELING> History
[C:\Users\Default\AppData\Local\Microsoft\Windows\History]
02-11-2006 13:59 <KOPPELING> Temporary Internet Files
[C:\Users\Default\AppData\Local\Microsoft\Windows\Temporary Internet Files]
0 bestand(en) 0 bytes

Map van C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu

29-09-2009 15:05 <KOPPELING> Programma's
[C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs]
0 bestand(en) 0 bytes

Map van C:\Users\Default\Documents

29-09-2009 15:05 <KOPPELING> Mijn afbeeldingen [C:\Users\Default\Pictures]
29-09-2009 15:05 <KOPPELING> Mijn muziek [C:\Users\Default\Music]
29-09-2009 15:05 <KOPPELING> Mijn video's [C:\Users\Default\Videos]
02-11-2006 13:59 <KOPPELING> My Music [C:\Users\Default\Music]
02-11-2006 13:59 <KOPPELING> My Pictures [C:\Users\Default\Pictures]
02-11-2006 13:59 <KOPPELING> My Videos [C:\Users\Default\Videos]
0 bestand(en) 0 bytes

Map van C:\Users\Public\Documents

29-09-2009 15:05 <KOPPELING> Mijn afbeeldingen [C:\Users\Public\Pictures]
29-09-2009 15:05 <KOPPELING> Mijn muziek [C:\Users\Public\Music]
29-09-2009 15:05 <KOPPELING> Mijn video's [C:\Users\Public\Videos]
02-11-2006 13:59 <KOPPELING> My Music [C:\Users\Public\Music]
02-11-2006 13:59 <KOPPELING> My Pictures [C:\Users\Public\Pictures]
02-11-2006 13:59 <KOPPELING> My Videos [C:\Users\Public\Videos]
0 bestand(en) 0 bytes

Totaal aantal weergegeven bestanden:
6 bestand(en) 0 bytes

77 map(pen) 16.321.331.200 bytes beschikbaar

==== Deleting CLSID Registry Keys ==========

==== Deleting CLSID Registry Values ==========

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

Aangifte inkomstenbelasting 2012
Aangifte inkomstenbelasting 2013
Adobe Flash Player 16 ActiveX
Adobe Flash Player 16 NPAPI
Adobe Reader 9.5.5 - Nederlands
Apple Application Support (32-bit)
Apple Mobile Device Support
Apple Software Update
AVG 2015
Bing Bar
Bonjour
BufferChm
CCleaner
D2400
D2400_Help
D3DX10
DeviceDiscovery
DeviceManagementQFolder
DivX-Setup
dj_sf_ProductContext
dj_sf_software
dj_sf_software_req
Dropbox
Facebook Video Calling 3.1.0.521
FoxTab PDF Creator
GIMP 2.8.14
Google Toolbar for Internet Explorer
Google Update Helper
Hotfix for Microsoft .NET Framework 3.5 SP1 (KB953595)
Hotfix for Microsoft .NET Framework 3.5 SP1 (KB958484)
HP Deskjet Printer Driver Software 9.0
HP Imaging Device Functions 9.0
HP Photosmart Essential 2.01
HP Photosmart Essential2.01
HP Update
HPSSupply
iCloud
iPhone Explorer 2.100
iTunes
IZArc 4.1.2
Java 8 Update 40

Java Auto Updater
JavaFX 2.1.0
Logitech Desktop Messenger
Logitech QuickCam-stuurprogrammapakket
McAfee Security Scan Plus
Messenger Companion
Microsoft .NET Framework 3.5 Language Pack SP1 - nld
Microsoft .NET Framework 3.5 SP1
Microsoft .NET Framework 4.5.1
Microsoft .NET Framework 4.5.1 (Nederlands)
Microsoft .NET Framework 4.5.1 (NLD)
Microsoft Application Error Reporting
Microsoft Silverlight
Microsoft Visual C++ 2005 ATL Update kb973923 - x86 8.0.50727.4053
Microsoft Visual C++ 2005 Redistributable
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30411
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219
MobileMe Control Panel
Mozilla Firefox 36.0 (x86 nl)
Mozilla Maintenance Service
MSVCRT
OpenOffice.org 3.4
PanoStandAlone
Pharao
Pharaoh
PSSWCORE
QuickTime 7
Rapport
Realtek High Definition Audio Driver
Security Update for CAPICOM (KB931906)
Security Update for Microsoft .NET Framework 3.5 SP1 (KB2604111)
Security Update for Microsoft .NET Framework 3.5 SP1 (KB2736416)
Security Update for Microsoft .NET Framework 3.5 SP1 (KB2840629)
Security Update for Microsoft .NET Framework 3.5 SP1 (KB2861697)
Security Update for Microsoft .NET Framework 4.5.1 (KB2894854v2)
Security Update for Microsoft .NET Framework 4.5.1 (KB2898869)
Security Update for Microsoft .NET Framework 4.5.1 (KB2901126)
Security Update for Microsoft .NET Framework 4.5.1 (KB2931368)
Security Update for Microsoft .NET Framework 4.5.1 (KB2972107)
Security Update for Microsoft .NET Framework 4.5.1 (KB2972216)
Security Update for Microsoft .NET Framework 4.5.1 (KB2978128)
Security Update for Microsoft .NET Framework 4.5.1 (KB2979578v2)
Segoe UI
Sierra Utilities
Skype Click to Call
SkypeT 6.9
Spelling Dictionaries Support For Adobe Reader 9
Status
Taalpakket voor Microsoft .NET Framework 3.5 SP1 - NL
TomTom HOME

TomTom HOME 2.8.2.2264
TomTom HOME Visual Studio Merge Modules
Toolbox
TrayApp
Trusteer Eindpuntbeveiliging
UnloadSupport
Update for Microsoft .NET Framework 3.5 SP1 (KB963707)
VC80CRTRedist - 8.0.50727.4053
VideoToolkit01
Visual Studio 2012 x86 Redistributables
VLC media player 1.1.11
WebReg
Windows Live Communications Platform
Windows Live Essentials
Windows Live ID Sign-in Assistant
Windows Live Installer
Windows Live Mesh - ActiveX-besturingselement voor externe verbindingen
Windows Live Messenger
Windows Live Messenger Companion Core
Windows Live Photo Common
Windows Live PIMT Platform
Windows Live SOXE
Windows Live SOXE Definitions
Windows Live UX Platform
Windows Live UX Platform Language Pack
Windows Media Player Firefox Plugin

==== Deleting Services ==========

==== Registry Fix Code ==========

Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"Facebook Update"=-

==== Deleting Files \ Folders ==========

C:\Users\Bosman\AppData\Local\Facebook\Update deleted
C:\Program Files\Mozilla Firefox\extensions\{82AF8DCA-6DE9-405D-BD5E-43525BDAD38A} deleted
C:\Users\Bosman\AppData\Roaming\Mozilla\Firefox\Profiles\irxf5u4v.default\extensions\{b9db16a4-6edc-47ec-a1f4-b86292ed211d} deleted
C:\ProgramData\B0FFCDD9-5261-4e59-B29A-17A4FABDEBAB deleted
C:\Users\B\AppData\Roaming\Mozilla\Firefox\Profiles\irxf5u4v.default\jetpack deleted

==== System Specs ==========

Windows: Windows Vista Home Basic Edition Service Pack 2 (Build 6002)
Memory (RAM): 2431 MB
CPU Info: Intel(R) Celeron(R) D CPU 3.46GHz

CPU Speed: 3520,9 MHz
Sound Card: Luidsprekers (Realtek High Defi |
Realtek Digital Output (Realtek |
Display Adapters: SiS Mirage 3 Graphics | SiS Mirage 3 Graphics | LogMeIn Mirror Driver |
RDPDD Chained DD | RDP Encoder Mirror Driver
Monitors: 1x; Algemeen PnP-beeldscherm |
Screen Resolution: 1024 X 768 - 32 bit
Network: Network Present
Network Adapters: SiS191 Ethernet Controller
CD / DVD Drives: 1x (E: |) E: HL-DT-STDVD-RW_GSA-H41N
Ports: COM1 | COM2 LPT1
Mouse: 5 Button Wheel Mouse Present
Hard Disks: C: 69,8GB | D: 69,5GB
Hard Disks - Free: C: 15,2GB | D: 52,6GB
Manufacturer *: Phoenix Technologies, LTD
BIOS Info: AT/AT COMPATIBLE | 03/17/07 | ACRSYS - 42302e31
Time Zone: West-Europa (standaardtijd)
Motherboard *: Acer F671CR
Country: Nederland
Language: NLD

==== System Specs (Software) ====================

Anti-Virus: AVG AntiVirus Free Edition 2015 On-access scanning disabled (Outdated)
Anti-Spyware: Windows Defender disabled (Outdated)
Anti-Spyware: AVG AntiVirus Free Edition 2015 disabled (Outdated)
Default Browser: Firefox 36.0
Internet Explorer Version: 9.0.8112.16421
Mozilla Firefox version: 36.0 (x86 nl)
Adobe Reader version: 9.5.5.316
Sun Java version: 1.8.0_40 (32-bit)
Flash Player version: 16.0.0.305

==== Files Recently Created / Modified ====================

====== C:\Windows ====
====== C:\Users\Bosman\AppData\Local\Temp ====
====== Java Cache =====
====== C:\Windows\system32 =====
2015-03-04 14:41:33 6C9FF3DDAB045FE7375FA33663DF6922 96680 ----a-w- C:\Windows\System32\WindowsAccessBridge.dll
2015-03-03 05:13:06 D7A5F5C99AB5A40F3F64488934D2850D 3758 ----a-w- C:\Windows\System32\cc_20150303_061300.reg
====== C:\Windows\system32\drivers =====
2015-02-19 20:28:38 D4899370855466D65A5565544BB3BC05 217568 ----a-w- C:\Windows\System32\drivers\avgidsdriverx.sys
2015-02-12 09:00:04 4685116CD48FF06496ECE8731C0D0E4F 208856 ----a-w- C:\Windows\System32\drivers\RapportKELL.sys
2015-02-12 02:01:53 5035EDF1F2E72F78BB1EC5BD9B97463F 440760 ----a-w- C:\Windows\System32\drivers\ksecdd.sys
====== C:\Windows\Tasks ======
====== C:\Windows\Temp ======

======= C:\Program Files =====
2015-03-04 14:41:49 -------- dc----w- C:\Program Files\Common Files\Java
2015-02-07 13:07:20 -------- dc----w- C:\Program Files\iPod
2015-02-07 13:07:07 -------- dc----w- C:\Program Files\iTunes
======= C: =====
====== C:\Users\Bosman\AppData\Roaming ======
2015-03-04 16:28:39 -------- d-----w-
C:\Windows\system32\config\systemprofile\AppData\Local\Temp
2015-03-04 16:28:39 -------- d-----w-
C:\Windows\serviceprofiles\networkservice\AppData\Local\Temp
2015-03-04 16:28:39 -------- d-----w-
C:\Windows\serviceprofiles\Localservice\AppData\Local\Temp
2015-03-04 16:28:38 -------- d-----w- C:\Users\Default\AppData\Local\Temp
2015-03-04 16:28:38 -------- d-----w- C:\Users\Default User\AppData\Local\Temp
2015-03-04 16:28:37 -------- dc----w- C:\Users\Bosman\AppData\Local\Temp
====== C:\Users\Bosman ======
2015-03-04 14:39:55 -------- dc----w- C:\ProgramData\Microsoft\Windows\Start
Menu\Programs\Java
2015-03-04 14:39:21 -------- dc----w- C:\ProgramData\Oracle
2015-03-04 11:19:34 5570B2EB9992035925838FFA930BCA3A 561064 -c--a-w-
C:\Users\Bosman\Downloads\jxpiinstall(1).exe
2015-03-04 11:18:34 5570B2EB9992035925838FFA930BCA3A 561064 -c--a-w-
C:\Users\Bosman\Downloads\jxpiinstall.exe
2015-03-04 09:50:58 8685FAF50C04F9A9C2F56FF64B0B7ACB 1107968 -c--a-w-
C:\Users\Bosman\Downloads\RSIT.exe
2015-02-07 13:09:15 -------- dc----w- C:\ProgramData\Microsoft\Windows\Start
Menu\Programs\iTunes

====== C: exe-files ==
2015-03-04 14:39:55 C731C96456335BDAA2F58220AE25A202 0 -c--a-we
C:\ProgramData\Oracle\Java\javapath\javaw.exe
2015-03-04 14:39:55 9DAEE3842461575137940096 4713D6D7 0 -c--a-we
C:\ProgramData\Oracle\Java\javapath\javaws.exe
2015-03-04 14:39:55 6F4EB294ACF731771AFE3EF6F7EE812D 0 -c--a-we
C:\ProgramData\Oracle\Java\javapath\java.exe
2015-03-04 14:39:40 32F50E7E4D45A38E60EA7D6D701A08C9 159656 -c--a-w-
C:\Program Files\Java\jre1.8.0_40\bin\unpack200.exe
2015-03-04 14:39:39 F340F09E5124455FA81AB8EFE04DCCC3 16296 -c--a-w-
C:\Program Files\Java\jre1.8.0_40\bin\policytool.exe
2015-03-04 14:39:39 EF59DABB7C9789B9335841A595748C0B 16296 -c--a-w-
C:\Program Files\Java\jre1.8.0_40\bin\rmiregistry.exe
2015-03-04 14:39:39 E57ED773B6CB41DE8225A10AFE149510 15784 -c--a-w-
C:\Program Files\Java\jre1.8.0_40\bin\jjs.exe
2015-03-04 14:39:39 E2E61790688574F5F058AD01145E0473 15784 -c--a-w- C:\Program
Files\Java\jre1.8.0_40\bin\rmid.exe
2015-03-04 14:39:39 CE2F700CA51229054C9A03D96646DE5151112 -c--a-w- C:\Program
Files\Java\jre1.8.0_40\bin\ssvagent.exe
2015-03-04 14:39:39 C96C6041829212284EFB5A85B08B1536 16296 -c--a-w- C:\Program
Files\Java\jre1.8.0_40\bin\servertool.exe
2015-03-04 14:39:39 C126BE266A4D76737EEDD0CFB436D7E3 15784 -c--a-w-
C:\Program Files\Java\jre1.8.0_40\bin\keytool.exe
2015-03-04 14:39:39 8C71D92983B9BBB5B8D823D8C0FDD129 15784 -c--a-w-

C:\Program Files\Java\jre1.8.0_40\bin\klist.exe
2015-03-04 14:39:39 879578D2FAE8E10DBE30FD0B829313DE 15784 -c--a-w- C:\Program Files\Java\jre1.8.0_40\bin\ktab.exe
2015-03-04 14:39:39 5D5801D096F9F362F442673632013727 16296 -c--a-w- C:\Program Files\Java\jre1.8.0_40\bin\tnameserv.exe
2015-03-04 14:39:39 5BF6CD8A5984AA5F2607364B5BEBBA11 16296 -c--a-w- C:\Program Files\Java\jre1.8.0_40\bin\orbd.exe
2015-03-04 14:39:39 30791C426723A4D76ADE3EF276F3F9FC 15784 -c--a-w- C:\Program Files\Java\jre1.8.0_40\bin\kinit.exe
2015-03-04 14:39:39 228AAF84B541C80BCFE7C1EE57502B61 15784 -c--a-w- C:\Program Files\Java\jre1.8.0_40\bin\pack200.exe
2015-03-04 14:39:39 113298AC181C026AB425E38CB7F963A3 76712 -c--a-w- C:\Program Files\Java\jre1.8.0_40\bin\jp2launcher.exe
2015-03-04 14:39:38 CBE5D74B4ECC80BF2C792C18CCEA92BF 15784 -c--a-w- C:\Program Files\Java\jre1.8.0_40\bin\java-rmi.exe
2015-03-04 14:39:38 C731C96456335BDAA2F58220AE25A202 191400 -c--a-w- C:\Program Files\Java\jre1.8.0_40\bin\javaw.exe
2015-03-04 14:39:38 B189CEE3C0CB5C9EABBF70329E0F4195 68520 -c--a-w- C:\Program Files\Java\jre1.8.0_40\bin\javacpl.exe
2015-03-04 14:39:38 9DAEE3842461575137940096 4713D6D7 272296 -c--a-w- C:\Program Files\Java\jre1.8.0_40\bin\javaws.exe
2015-03-04 14:39:38 9A97AB583FB5BD6FFFCE8C47E6DCCA62 30632 -c--a-w- C:\Program Files\Java\jre1.8.0_40\bin\jabswitch.exe
2015-03-04 14:39:38 6F4EB294ACF731771AFE3EF6F7EE812D 190888 -c--a-w- C:\Program Files\Java\jre1.8.0_40\bin\java.exe
2015-03-04 11:19:34 5570B2EB9992035925838FFA930BCA3A 561064 -c--a-w- C:\Users\Bosman\Downloads\jxpiinstall(1).exe
2015-03-04 11:18:34 5570B2EB9992035925838FFA930BCA3A 561064 -c--a-w- C:\Users\Bosman\Downloads\jxpiinstall.exe
2015-03-04 09:50:58 8685FAF50C04F9A9C2F56FF64B0B7ACB 1107968 -c--a-w- C:\Users\Bosman\Downloads\RSIT.exe
2015-03-01 00:11:20 78206B34BD050DB564BF5B4B8C6979251617224 -c--a-w- C:\Program Files\Google\Google Toolbar\Component\SearchWithGoogleUpdate_6F4EEAE8D7FCDAD8.exe
2015-03-01 00:11:15 327C893AA5966AC436CA275F8D64C8C0 1072072 -c--a-w- C:\Program Files\Google\Google Toolbar\Component\GoogleToolbarManager_BA9226F4C70BECC2.exe
2015-03-01 00:10:54 D15EE16B871FE911D8D7C91FD5F57EBA 532312 -c--a-w- C:\Program Files\Google\Update\Install\{98A9454F-7361-46F8-AA75-C966D81506D8}\GoogleToolbarInstaller_updater_signed.exe
2015-03-01 00:10:54 D15EE16B871FE911D8D7C91FD5F57EBA 532312 -c--a-w- C:\Program Files\Google\Update\Download\{F69EABDD-A4BB-4555-BE7E-1EA5F59BBA24}\7.5.6227.252\GoogleToolbarInstaller_updater_signed.exe
=== C: other files ==
2015-03-04 14:39:40 0A513FB75ADF2580D0F0D55D0A245C4F 14130 -c--a-w- C:\Program Files\Java\jre1.8.0_40\lib\deploy\ffjcext.zip

======== System Restore Points ========

RP729: 6-3-2015 0:00:02 - Gepland herstelpunt
RP730: 7-3-2015 0:00:02 - Gepland herstelpunt

==== Startup Registry Enabled ====================

[HKEY_USERS\S-1-5-19\Software\Microsoft\Windows\CurrentVersion\Run]
"WindowsWelcomeCenter"="rundll32.exe oobefldr.dll,ShowWelcomeCenter"
"Sidebar"="%ProgramFiles%\Windows\Sidebar.exe /detectMem"

[HKEY_USERS\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Run]
"WindowsWelcomeCenter"="rundll32.exe oobefldr.dll,ShowWelcomeCenter"
"Sidebar"="%ProgramFiles%\Windows\Sidebar.exe /detectMem"

[HKEY_USERS\S-1-5-21-2909120250-2823181194-1062834500-1000\Software\Microsoft\Windows\CurrentVersion\Run]
"WMPNSCFG"="C:\Program Files\Windows Media Player\WMPNSCFG.exe"
"CCleaner"="C:\Program Files\CCleaner\CCleaner.exe /AUTO"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"RtHDVCpl"="RtHDVCpl.exe"
"DivXUpdate"="C:\Program Files\DivX\DivX Update\DivXUpdate.exe /CHECKNOW"
"AVG_UI"="C:\Program Files\AVG\AVG2015\avgui.exe /TRAYONLY"
"APSDaemon"="C:\Program Files\Common Files\Apple\Apple Application Support\APSDaemon.exe"
"QuickTime Task"="C:\Program Files\QuickTime\QTTask.exe -atboottime"
"iTunesHelper"="C:\Program Files\iTunes\iTunesHelper.exe"
"SunJavaUpdateSched"="C:\Program Files\Common Files\Java\Java Update\jusched.exe"
"Windows Defender"="%ProgramFiles%\Windows Defender\MSASCui.exe -hide"

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"WMPNSCFG"="C:\Program Files\Windows Media Player\WMPNSCFG.exe"
"CCleaner"="C:\Program Files\CCleaner\CCleaner.exe /AUTO"

==== Startup Registry Disabled ====================

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig\startupreg]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig\startupreg\Adobe ARM]
"key"="SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run"
"item"="Adobe ARM"
"hkey"="HKLM"
"command"="\"C:\\Program Files\\Common Files\\Adobe\\ARM\\1.0\\AdobeARM.exe\""

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig\startupreg\Adobe Reader Speed Launcher]
"key"="SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run"
"item"="Adobe Reader Speed Launcher"
"hkey"="HKLM"
"command"="\"C:\\Program Files\\Adobe\\Reader 9.0\\Reader\\Reader_sl.exe\""

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig\startupreg\AppleSyncNotifier]
"key"="SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run"
"item"="AppleSyncNotifier"

"hkey"="HKLM"
"command"="C:\\Program Files\\Common Files\\Apple\\Mobile Device Support\\AppleSyncNotifier.exe"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig\startupreg\APSDaemon]
"key"="SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run"
"item"="APSDaemon"
"hkey"="HKLM"
"command"="\"C:\\Program Files\\Common Files\\Apple\\Apple Application Support\\APSDaemon.exe\""

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig\startupreg\iTunesHelper]
"key"="SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run"
"item"="iTunesHelper"
"hkey"="HKLM"
"command"="\"C:\\Program Files\\iTunes\\iTunesHelper.exe\""

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig\startupreg\Skype]
"key"="SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run"
"item"="Skype"
"hkey"="HKCU"
"command"="\"C:\\Program Files\\Skype\\Phone\\Skype.exe\" /minimized /regrun"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig\startupreg\TomTomHOME.exe]
"key"="SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run"
"item"="TomTomHOME.exe"
"hkey"="HKCU"
"command"="\"C:\\Program Files\\TomTom HOME 2\\TomTomHOMERunner.exe\""

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig\startupfolder]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig\startupfolder\C:^ProgramData^Microsoft^Windows^Start Menu^Programs^Startup^HP Digital Imaging Monitor.lnk]
"path"="C:\\ProgramData\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\HP Digital Imaging Monitor.lnk"
"backup"="C:\\Windows\\pss\\HP Digital Imaging Monitor.lnk.CommonStartup"
"backupExtension"=".CommonStartup"
"command"="C:\\PROGRA~1\\HP\\DIGITA~1\\bin\\hpqtra08.exe "
"item"="HP Digital Imaging Monitor"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig\startupfolder\C:^ProgramData^Microsoft^Windows^Start Menu^Programs^Startup^Logitech Desktop Messenger.lnk]
"path"="C:\\ProgramData\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\Logitech Desktop Messenger.lnk"
"backup"="C:\\Windows\\pss\\Logitech Desktop Messenger.lnk.CommonStartup"
"backupExtension"=".CommonStartup"

"command"="C:\\PROGRA~1\\Logitech\\DESKTO~1\\8876480\\Program\\LOGITE~1.EXE -startup"
"item"="Logitech Desktop Messenger"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig\startupfolder\C:^Users^Bosman^AppData^Roaming^Microsoft^Windows^Start Menu^Programs^Startup^Dropbox.lnk]
"path"="C:\\Users\\Bosman\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\Dropbox.lnk"
"backup"="C:\\Windows\\pss\\Dropbox.lnk.Startup"
"backupExtension"=".Startup"
"command"="C:\\Users\\Bosman\\AppData\\Roaming\\Dropbox\\bin\\Dropbox.exe /systemstartup"
"item"="Dropbox"

==== Task Scheduler Jobs ========================

C:\Windows\tasks\Adobe Flash Player Updater.job --a------ C:\Windows\system32\Macromed\Flash\FlashPlayerUpdateService.exe [05-02-2015 01:47]
C:\Windows\tasks\FacebookUpdateTaskUserS-1-5-21-2909120250-2823181194-1062834500-1000Core.job --a------ C:\Users\Bosman\AppData\Local\Facebook\Update\FacebookUpdate.exe []
C:\Windows\tasks\FacebookUpdateTaskUserS-1-5-21-2909120250-2823181194-1062834500-1000UA.job --a------ C:\Users\Bosman\AppData\Local\Facebook\Update\FacebookUpdate.exe []
C:\Windows\tasks\GoogleUpdateTaskMachineCore.job --a------ C:\Program Files\Google\Update\GoogleUpdate.exe [17-10-2014 23:52]
C:\Windows\tasks\GoogleUpdateTaskMachineUA.job --a------ C:\Program Files\Google\Update\GoogleUpdate.exe [17-10-2014 23:52]

==== Other Scheduled Tasks ========================

"C:\Windows\system32\tasks\Ad-Aware Update (Weekly)" [C:\Program Files\Lavasoft\Ad-Aware\Ad-AwareAdmin.exe]
"C:\Windows\system32\tasks\Adobe Flash Player Updater" [C:\Windows\system32\Macromed\Flash\FlashPlayerUpdateService.exe]
"C:\Windows\system32\tasks\CCleanerSkipUAC" ["C:\Program Files\CCleaner\CCleaner.exe"]
"C:\Windows\system32\tasks\CreateChoiceProcessTask" [C:\Windows\System32\browserchoice.exe]
"C:\Windows\system32\tasks\FacebookUpdateTaskUserS-1-5-21-2909120250-2823181194-1062834500-1000Core" [C:\Users\Bosman\AppData\Local\Facebook\Update\FacebookUpdate.exe]
"C:\Windows\system32\tasks\FacebookUpdateTaskUserS-1-5-21-2909120250-2823181194-1062834500-1000UA" [C:\Users\Bosman\AppData\Local\Facebook\Update\FacebookUpdate.exe]
"C:\Windows\system32\tasks\GoogleUpdateTaskMachineCore" [C:\Program Files\Google\Update\GoogleUpdate.exe]
"C:\Windows\system32\tasks\GoogleUpdateTaskMachineUA" [C:\Program Files\Google\Update\GoogleUpdate.exe]
"C:\Windows\system32\tasks\{691E71DD-192F-435D-8E85-1E46D03764C4}" [C:\Program Files\Skype\Phone\Skype.exe]
"C:\Windows\system32\tasks\Apple\AppleSoftwareUpdate" [C:\Program Files\Apple Software Update\SoftwareUpdate.exe]

==== Firefox Start and Search pages ========================

ProfilePath: C:\Users\Bosman\AppData\Roaming\Mozilla\Firefox\Profiles\irxf5u4v.default
user_pref("browser.startup.homepage", "http://www.google.com");
user_pref("browser.search.defaulturl", "http://www.google.com/search?
btnG=Google+Search&q=");
user_pref("browser.newtab.url", "http://www.google.com/");
user_pref("browser.search.defaultengine", "Google");
user_pref("keyword.URL", "http://www.google.com/search?btnG=Google+Search&q=");

==== Firefox Extensions Registry ====================

[HKEY_LOCAL_MACHINE\Software\Mozilla\Firefox\Extensions]
"{20a82645-c095-46ed-80e3-
08825760534b}"="C:\Windows\Microsoft.NET\Framework\v3.5\Windows Presentation
Foundation\DotNetAssistantExtension" [01-10-2009 23:20]
[HKEY_CURRENT_USER\Software\Mozilla\Firefox\Extensions]
"{e4f94d1e-2f53-401e-8885-681602c0ddd8}"="C:\ProgramData\McAfee Security
Scan\Extensions\{e4f94d1e-2f53-401e-8885-681602c0ddd8}.xpi" [04-04-2014 11:36]

==== Firefox Extensions ====================

ProfilePath: C:\Users\Bosman\AppData\Roaming\Mozilla\Firefox\Profiles\irxf5u4v.default
- Undetermined - adblockpopups@jessehakanen.net
- Undetermined - leethax@leethax.net
- Undetermined - {b9db16a4-6edc-47ec-a1f4-b86292ed211d}
- Undetermined - {73a6fe31-595d-460b-a920-fcc0f8843232}
- Adblock Plus Pop-up Addon - %ProfilePath%\extensions\adblockpopups@jessehakanen.net.xpi
- Facebook Color Changer - %ProfilePath%\extensions\jid0-
Eyur3vR97jbHklhdHVBnn9OBILU@jetpack.xpi
- Pin It Button - %ProfilePath%\extensions\jid1-YcMV6ngYmQRA2w@jetpack.xpi
- leethax.net extension - %ProfilePath%\extensions\leethax@leethax.net.xpi
- Flagfox - %ProfilePath%\extensions\{1018e4d6-728f-4b20-ad56-37578a4de76b}.xpi
- Microsoft .NET Framework Assistant - %ProfilePath%\extensions\{20a82645-c095-46ed-80e3-
08825760534b}.xpi
- NoScript - %ProfilePath%\extensions\{73a6fe31-595d-460b-a920-fcc0f8843232}.xpi
- YouTube High Definition - %ProfilePath%\extensions\{7b1bf0b6-a1b9-42b0-b75d-
252036438bdc}.xpi
- Adblock Plus - %ProfilePath%\extensions\{d10d0bf8-f5b5-c8b4-a8b2-2b9879e08c5d}.xpi

ProfilePath: C:\Users\Bosman\AppData\Roaming\TomTom\HOME\Profiles\thmv4w7n.default
- Map status indicator - C:\Program Files\TomTom HOME 2\xul\extensions\MapShare-
status@tomtom.com
- TomTom HOME default theme - C:\Program Files\TomTom HOME
2\xul\extensions\baseTheme@tomtom.com

AppDir: C:\Program Files\Mozilla Firefox
- Default - %AppDir%\browser\extensions\{972ce4c6-7e08-4474-a285-3208198ce6fd}

==== Firefox Plugins ====================

Profilepath: C:\Users\Bosman\AppData\Roaming\Mozilla\Firefox\Profiles\irxf5u4v.default
59492511D7A8BC90A2F6023218E80F9C - C:\Program Files\QuickTime\Plugins\npqtplugin.dll -
QuickTime Plug-in 7.7.6

17D7FEB824594E6446059EB3987D1AA9 - C:\Program Files\QuickTime\Plugins\npqtplugin2.dll - QuickTime Plug-in 7.7.6
0900BBAB5745ECEC21C5E8254F05B7B0 - C:\Program Files\QuickTime\Plugins\npqtplugin3.dll - QuickTime Plug-in 7.7.6
B239D122D14692FC5EFBA7121C770F61 - C:\Program Files\QuickTime\Plugins\npqtplugin4.dll - QuickTime Plug-in 7.7.6
847C1A6B649D406FDB721E1BCE4E1E38 - C:\Program Files\QuickTime\Plugins\npqtplugin5.dll - QuickTime Plug-in 7.7.6
AE84791D996D1F05A2446B0C447D937A - C:\Program Files\Adobe\Reader 9.0\Reader\browser\nppdf32.dll - Adobe Acrobat
AE84791D996D1F05A2446B0C447D937A - C:\Program Files\Adobe\Reader 9.0\Reader\AIR\nppdf32.dll - Adobe Acrobat
98137411B9C632095F919E2CE70B288A - C:\Program Files\Google\Update\1.3.26.9\npGoogleUpdate3.dll - Google Update
AB87EEFFD18F2BAAFC274E7075EA6C67 - C:\Windows\Microsoft.NET\Framework\v3.5\Windows Presentation Foundation\NPWPF.dll - Windows Presentation Foundation / Windows Presentation Foundation
343BA8F3ABC8CE69700F37DB4A82300F - C:\Program Files\Microsoft Silverlight\5.1.31211.0\npctrl.dll - Silverlight Plug-In
D7492728A4C06EC99B10F8219B1F31F5 - C:\Program Files\Java\jre1.8.0_40\bin\plugin2\npjp2.dll - Java(TM) Platform SE 8 U40
F47B4F0D0DF0C28759B60CF0B0090A11 - C:\Program Files\Java\jre1.8.0_40\bin\dtplugin\npdeployJava1.dll - Java Deployment Toolkit 8.0.400.25
B938C1AE3ADCE166190895685B0BEB0D - C:\Program Files\DivX\DivX OVS Helper\npovshelper.dll - DivX VOD Helper Plug-in
46A59E6F7F7C1679AC7C4655E055326D - C:\Program Files\iTunes\Mozilla Plugins\npitunes.dll - iTunes Application Detector
C62322C77D1AAB77B1CF1130FCC3673A - C:\Windows\system32\Macromed\Flash\NPSWF32_16_0_0_305.dll - Shockwave Flash
3CD19649B2C3023D65E67C056457A2BC - C:\Users\Bosman\AppData\Local\Facebook\Video\Skype\npFacebookVideoCalling.dll - Facebook Video Calling Plugin
AB3546B509E4B89096078EB2081C39C7 - C:\Program Files\Microsoft Silverlight\5.1.31211.0\npctrlui.dll - Microsoft® Silverlight

==== Chromium Look ======================

HKEY_LOCAL_MACHINE\SOFTWARE\Google\Chrome\Extensions
bopakagnckmlgajfccecajhnimjiiedh - No path found[]
lifbcibllhkdhoafpjfnlhfpfgnpldfl - C:\Program Files\Skype\Toolbars\Skype for Chromium\skype_chrome_extension.crx[02-10-2012 12:14]

==== Set IE to Default ======================

Old Values:
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]
"Start Page"="https://www.google.nl/"

New Values:
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]
"Start Page"="https://www.google.nl/"

==== All HKCU SearchScopes ====================

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\SearchScopes
"DefaultScope"="{0633EE93-D776-472f-A0FF-E1416B8B2E3A}"
{012E1000-F331-11DB-8314-0800200C9A66} Google Url="http://www.google.com/search?q={searchTerms}"
{0633EE93-D776-472f-A0FF-E1416B8B2E3A} Bing Url="http://www.bing.com/search?q={searchTerms}&src=IE-SearchBox&FORM=IE8SRC"
{1109C8E2-D651-4652-98F9-FD04A95DF911} Bing Url="http://www.bing.com/search?FORM=UP97DF&PC=UP97&dt=072413&q={searchTerms}&src=IE-SearchBox"
{6A1806CD-94D4-4689-BA73-E35EA1EA9990} Google Url="http://www.google.com/search?q={searchTerms}&rls=com.microsoft:{language}&ie={inputEncoding}&oe={outputEncoding}&startIndex={startIndex?}&startPage={startPage}"

==== Reset Google Chrome ====================

Nothing found to reset

==== shortcuts on Users Desktops ====================

C:\Users\Bosman\Desktop\DivX Movies.lnk - C:\Users\Bosman\Videos\DivX Movies
C:\Users\Bosman\Desktop\Dropbox.lnk - C:\Users\Bosman\AppData\Roaming\Dropbox\bin\Dropbox.exe /home
C:\Users\Bosman\Desktop\Logitech Desktop Messenger.lnk - C:\Program Files\Logitech\Desktop Messenger\8876480\Program\LogitechDesktopMessenger.exe -startup
C:\Users\Bosman\Desktop\Prullenbak - Snelkoppeling.lnk -
C:\Users\Bosman\Desktop\Video Player.lnk - C:\Program Files\FLVPlayer\FLVPlayer.exe

==== shortcuts on All Users Desktop ====================

C:\Users\Public\Desktop\Aangifte inkomstenbelasting 2013.lnk - C:\Program Files\Belastingdienst\Aangifte inkomstenbelasting\2013\ib2013.exe
C:\Users\Public\Desktop\Adobe Reader 9.lnk - C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe
C:\Users\Public\Desktop\AVG 2015.lnk - C:\Program Files\AVG\AVG2015\avgui.exe
C:\Users\Public\Desktop\CCleaner.lnk - C:\Program Files\CCleaner\CCleaner.exe
C:\Users\Public\Desktop\DivX Plus Player.lnk - C:\Program Files\DivX\DivX Plus Player\DivX Plus Player.exe
C:\Users\Public\Desktop\iPhone Explorer.lnk - C:\Program Files\iPhone Explorer\iPhone Explorer.exe
C:\Users\Public\Desktop\iTunes.lnk - C:\Program Files\iTunes\iTunes.exe
C:\Users\Public\Desktop\Logitech-webcamsoftware.lnk - C:\Program Files\Logitech\Logitech WebCam Software\LWS.exe
C:\Users\Public\Desktop\Mozilla Firefox.lnk - C:\Program Files\Mozilla Firefox\firefox.exe
C:\Users\Public\Desktop\OpenOffice.org 3.4.lnk - C:\Program Files\OpenOffice.org 3\program\soffice.exe
C:\Users\Public\Desktop\QuickTime Player.lnk - C:\Program Files\QuickTime\QuickTimePlayer.exe
C:\Users\Public\Desktop\Skype.lnk - C:\Windows\Installer\{4E76FF7E-AEBA-4C87-B788-CD47E5425B9D}\SkypeIcon.exe

C:\Users\Public\Desktop\VLC media player.lnk - C:\Program Files\VideoLAN\VLC\vlc.exe

==== shortcuts in All Users Start Menu ========================

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\AVG\AVG 2015.lnk - C:\Program Files\AVG\AVG2015\avgui.exe
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\iTunes\Info iTunes.lnk - C:\Program Files\iTunes\iTunes.Resources\nl.lproj\About iTunes.rtf
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\iTunes\iTunes.lnk - C:\Program Files\iTunes\iTunes.exe
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Java\About Java.lnk - C:\Program Files\Java\jre1.8.0_40\bin\javacpl.exe -tab about
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Java\Check For Updates.lnk - C:\Program Files\Java\jre1.8.0_40\bin\javacpl.exe -tab update
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Java\Configure Java.lnk - C:\Program Files\Java\jre1.8.0_40\bin\javacpl.exe
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Java\Get Help.lnk -
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Java\Visit Java.com.lnk -
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Silverlight\Microsoft Silverlight.lnk - C:\Program Files\Microsoft Silverlight\5.1.31211.0\Silverlight.Configuration.exe
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\QuickTime\Over QuickTime.lnk - C:\Windows\Installer\{3D2CBC2C-65D4-4463-87AB-BB2C859C1F3E}\RichText.ico
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\QuickTime\QuickTime deïnstalleren.lnk -
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\QuickTime\QuickTime Player.lnk - C:\Windows\Installer\{3D2CBC2C-65D4-4463-87AB-BB2C859C1F3E}\QTPlayer.ico
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Trusteer Eindpuntbeveiliging\Trusteer Eindpuntbeveiliging Console.lnk - C:\Program Files\Trusteer\Rapport\bin\RapportService.exe -config
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Trusteer Eindpuntbeveiliging\Trusteer Eindpuntbeveiliging starten.lnk - C:\Program Files\Trusteer\Rapport\bin\RapportService.exe -userstart
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Trusteer Eindpuntbeveiliging\Trusteer Eindpuntbeveiliging stoppen.lnk - C:\Program Files\Trusteer\Rapport\bin\RapportService.exe -shutdown

==== shortcuts in Quick Launch ========================

C:\Users\Bosman\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Adobe Reader 9 (2).lnk - C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe
C:\Users\Bosman\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Adobe Reader 9.lnk - C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe
C:\Users\Bosman\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\AVG 2014.lnk - C:\Program Files\AVG\AVG2014\avgui.exe
C:\Users\Bosman\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Launch Internet Explorer Browser.lnk - C:\Program Files\Internet Explorer\iexplore.exe
C:\Users\Bosman\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Mozilla Firefox.lnk - C:\Program Files\Mozilla Firefox\firefox.exe
C:\Users\Bosman\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Shows Desktop (2).lnk -
C:\Users\Bosman\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Shows Desktop (3).lnk -

C:\Users\Bosman\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Shows Desktop.lnk -
C:\Users\Bosman\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Window Switcher.lnk -
C:\Users\Bosman\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Windows Media Player.lnk - C:\Program Files\Windows Media Player\wmplayer.exe /prefetch:1
C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Shows Desktop.lnk -
C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Window Switcher.lnk -
C:\Users\Default User\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Shows Desktop.lnk -
C:\Users\Default User\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Window Switcher.lnk -

==== Uninstall List x86 ========================

Aangifte inkomstenbelasting 2012 [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Aangifte inkomstenbelasting 2012]
Aangifte inkomstenbelasting 2013 [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Aangifte inkomstenbelasting 2013]
Adobe Flash Player 16 ActiveX [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX]
Adobe Flash Player 16 NPAPI [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI]
Adobe Reader 9.5.5 - Nederlands [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{AC76BA86-7AD7-1043-7B44-A95000000001}]
Apple Application Support (32-bit) [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{2FE00055-C4F3-4F7A-AEDD-E198D54CF12F}]
Apple Mobile Device Support [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{28ED482A-56DB-47D9-8D9E-990FA8CD7D3D}]
Apple Software Update [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{C6579A65-9CAE-4B31-8B6B-3306E0630A66}]
AVG 2015 [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{0A8B6758-6C88-43B6-81FC-DED37A291FCB}]
AVG 2015 [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{B6FCA7E7-F332-4C5E-A6E5-5056F051352D}]
AVG 2015 [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\AVG]
Bing Bar [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{449CE12D-E2C7-4B97-B19E-55D163EA9435}]
Bonjour [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{79155F2B-9895-49D7-8612-D92580E0DE5B}]
BufferChm [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\

{E2662C24-B31E-4349-A084-32EB76E8B760}]
CCleaner
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\CCleaner]
D2400 [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{2F467E6E-F7D2-43cc-91B9-4FCC105AE30D}]
D2400_Help
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{9521B818-
19CE-4d28-8200-DD26133E19E6}]
D3DX10 [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{E09C4DB7-630C-4F06-A631-8EA7239923AF}]
DeviceDiscovery
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{EF1ADA5A-0B1A-4662-8C55-7475A61D8B65}]
DeviceManagementQFolder
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{AB5D51AE-EBC3-438D-872C-705C7C2084B0}]
DivX-Setup
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\DivX
Setup.divx.com]
dj_sf_ProductContext
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{15C70064-
2463-49dd-9A88-B700F75BB428}]
dj_sf_software
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{B639110D-
747F-40DC-9682-95D94EF73790}]
dj_sf_software_req
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{75C22B40-
6D12-4439-80DC-CAB3313EADA5}]
Dropbox
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Dropbox]
Facebook Video Calling 3.1.0.521
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{2091F234-
EB58-4B80-8C96-8EB78C808CF7}]
FoxTab PDF Creator
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\FoxTab PDF
Creator]
GIMP 2.8.14
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\GIMP-
2_is1]
Google Toolbar for Internet Explorer
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{18455581-
E099-4BA8-BC6B-F34B2F06600C}]
Google Toolbar for Internet Explorer
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{2318C2B1-
4965-11d4-9B18-009027A5CD4F}]
Google Update Helper
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{60EC980A-BDA2-4CB6-A427-B07A5498B4CA}]
Google Update Helper
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{A92DAB39-4E2C-4304-9AB6-BC44E68B55E2}]
HP Deskjet Printer Driver Software 9.0

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{03E66394-42F0-4745-85F7-0A2F8F35C09F}]
HP Imaging Device Functions 9.0
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\HP Imaging Device Functions]
HP Photosmart Essential 2.01
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\HP Photosmart Essential]
HP Photosmart Essential2.01
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{8389382B-53BA-4A87-8854-91E3D80A5AC7}]
HP Update [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{2EFA4E4C-7B5F-48F7-A1C0-1AA882B7A9C3}]
HPSSupply [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{487B0B9B-DCD4-440D-89A0-A6EDE1A545A3}]
iCloud [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{79BD66B2-4DAE-4C3B-B08E-DC72E507C163}]
iPhone Explorer 2.100
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{7FD8B0C1-CDDA-4B4D-A577-B2E3570EA3A3}_is1]
iTunes [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{B8032A6B-C4D0-4744-B75F-9DDCB56B5C6F}]
IZArc 4.1.2 [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{97C82B44-D408-4F14-9252-47FC1636D23E}_is1]
Java 8 Update 40
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{26A24AE4-039D-4CA4-87B4-2F83218040F0}]
JavaFX 2.1.0
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{1111706F-666A-4037-7777-210328764D10}]
Logitech Desktop Messenger
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{900B1197-53F5-4F46-A882-2CFFFE2EEDCB}]
Logitech QuickCam-stuurprogrammapakket
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\lvdrivers_11.80]
McAfee Security Scan Plus
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\McAfee Security Scan]
Messenger Companion
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{8142D25E-028A-4563-86ED-5755783C8029}]
Microsoft .NET Framework 3.5 Language Pack SP1 - nld
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{101738D7-D805-37A9-BB91-1F2C351782BF}]
Microsoft .NET Framework 3.5 SP1
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{CE2CDD62-0124-36CA-84D3-9F4DCF5C5BD9}]
Microsoft .NET Framework 4.5.1 (Nederlands)
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-E685-45AD-9B20-CADF4CABA132} - 1043]
Microsoft .NET Framework 4.5.1 (NLD)

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{1A91D86E-3124-3574-A4BF-406761265CFA}]
Microsoft .NET Framework 4.5.1
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{4903D172-
DCCB-392F-93A3-34CA9D47FE3D}]
Microsoft .NET Framework 4.5.1
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{92FB6C44-
E685-45AD-9B20-CADF4CABA132} - 1033]
Microsoft Silverlight
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{89F4137D-
6C26-4A84-BDB8-2E5A4BB71E00}]
Microsoft Visual C++ 2005 ATL Update kb973923 - x86 8.0.50727.4053
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{770657D0-
A123-3C07-8E44-1C83EC895118}]
Microsoft Visual C++ 2005 Redistributable
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-
cc18-4c49-8cbf-51240c89a1a2}]
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30411
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{5DA8F6CD-C70E-39D8-8430-3D9808D6BD17}]
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{1F1C2DFC-2D24-3E06-BCB8-725134ADF989}]
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-
ECC6-35A9-88E4-87755C07200F}]
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}]
MobileMe Control Panel
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{926BD0E8-24A3-41D2-AF9B-340F1A37ED12}]
Mozilla Firefox 36.0 (x86 nl)
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Mozilla
Firefox 36.0 (x86 nl)]
Mozilla Maintenance Service
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\MozillaMain
tenanceService]
MSVCRT [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{8DD46C6A-0056-4FEC-B70A-28BB16A1F11F}]
OpenOffice.org 3.4
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{A3EC3BF7-E210-4A49-9246-95A7DA81F39C}]
PanoStandAlone
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{730837D4-
FF5E-48DB-BA49-33E732DFF0B3}]
Pharao
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Pharao]
Pharaoh
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Pharaoh]
PSSWCORE
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\

{F72E2DDC-3DB8-4190-A21D-63883D955FE7}]
QuickTime 7
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{3D2CBC2C-65D4-4463-87AB-BB2C859C1F3E}]
Rapport [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{1DD81E7D-0D28-4CEB-87B2-C041A4FCB215}]
Realtek High Definition Audio Driver
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{F132AF7F-
7BCA-4EDE-8A7C-958108FE7DBC}]
Security Update for CAPICOM (KB931906)
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{0EFDF2F9-836D-4EB7-A32D-038BD3F1FB2A}]
Segoe UI [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{5DD4FCBD-A3C1-4155-9E17-4161C70AAABA}]
Sierra Utilities
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Sierra
Utilities]
Skype Click to Call
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{B6CF2967-
C81E-40C0-9815-C05774FEF120}]
SkypeT 6.9 [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{4E76FF7E-AEBA-4C87-B788-CD47E5425B9D}]
Spelling Dictionaries Support For Adobe Reader 9
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{AC76BA86-7AD7-5464-3428-900000000004}]
Status [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{0289B35E-DC07-4c7a-9710-BBD686EA4B7D}]
TomTom HOME
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{26CE484D-2E8E-40D5-B251-158133114C69}]
TomTom HOME 2.8.2.2264
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\TomTom
HOME]
TomTom HOME Visual Studio Merge Modules
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{8F3C31C5-
9C3A-4AA8-8EFA-71290A7AD533}]
Toolbox [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{E9C18EBD-85BE-47D0-AA73-3FEDCC976B04}]
TrayApp [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{9C2D4047-0E40-499a-AC7A-C4B9BB12FE03}]
Trusteer Eindpuntbeveiliging
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Rapport_msi
]
UnloadSupport
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{543E938C-
BDC4-4933-A612-01293996845F}]
VC80CRTRedist - 8.0.50727.4053
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{5EE7D259-
D137-4438-9A5F-42F432EC0421}]
VideoToolkit01
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{824D3839-
DAA1-4315-A822-7AE3E620E528}]

Visual Studio 2012 x86 Redistributables
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{98EFF19A-30AB-4E4B-B943-F06B1C63EBF8}]
VLC media player 1.1.11
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\VLC media player]
WebReg [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{29FA38B4-0AE4-4D0D-8A51-6165BB990BB0}]
Windows Live Communications Platform
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{D45240D3-B6B3-4FF9-B243-54ECE3E10066}]
Windows Live Essentials
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{2A07C35B-8384-4DA4-9A95-442B6C89A073}]
Windows Live Essentials
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\WinLiveSuite]
Windows Live ID Sign-in Assistant
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{C6150D8A-86ED-41D3-87BB-F3BB51B0B77F}]
Windows Live Installer
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{0B0F231F-CE6A-483D-AA23-77B364F75917}]
Windows Live Mesh - ActiveX-besturingselement voor externe verbindingen
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{C32CE55C-12BA-4951-8797-0967FDEF556F}]
Windows Live Messenger
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{48294D95-EE9A-4377-8213-44FC4265FB27}]
Windows Live Messenger
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{E5B21F11-6933-4E0B-A25C-7963E3C07D11}]
Windows Live Messenger Companion Core
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{78A96B4C-A643-4D0F-98C2-A8E16A6669F9}]
Windows Live Photo Common
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{9BD262D0-B788-4546-A0A5-F4F56EC3834B}]
Windows Live Photo Common
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{A9BDCA6B-3653-467B-AC83-94367DA3BFE3}]
Windows Live PIMT Platform
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{83C292B7-38A5-440B-A731-07070E81A64F}]
Windows Live SOXE
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{682B3E4F-696A-42DE-A41C-4C07EA1678B4}]
Windows Live SOXE Definitions
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{200FEC62-3C34-4D60-9CE8-EC372E01C08F}]
Windows Live UX Platform
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\

{CE95A79E-E4FC-4FFF-8A75-29F04B942FF2}]
Windows Live UX Platform Language Pack
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{D6F25CF9-4E87-43EB-B324-C12BE9CDD668}]
Windows Media Player Firefox Plugin
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{69FDFBB6-351D-4B8C-89D8-867DC9D0A2A4}]

==== HijackThis Entries ======================

O1 - Hosts: ::1 localhost
O2 - BHO: MSS+ Identifier - {0E8A89AD-95D7-40EB-8D9D-083EF7066A01} - C:\Program Files\McAfee Security Scan\3.8.150\McAfeeMSS_IE.dll
O2 - BHO: AcroIEHelperStub - {18DF081C-E8AD-4283-A596-FA578C2EBDC3} - C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll
O2 - BHO: Java(tm) Plug-In SSV Helper - {761497BB-D6F0-462C-B6EB-D4DAF1D92D43} - C:\Program Files\Java\jre1.8.0_40\bin\ssv.dll
O2 - BHO: Windows Live ID Sign-in Helper - {9030D464-4C02-4ABF-8ECC-5164760863C6} - C:\Program Files\Common Files\Microsoft Shared\Windows Live\WindowsLiveLogin.dll
O2 - BHO: Windows Live Messenger Companion Helper - {9FDDE16B-836F-4806-AB1F-1455CBEFF289} - C:\Program Files\Windows Live\Companion\companioncore.dll
O2 - BHO: Google Toolbar Helper - {AA58ED58-01DD-4d91-8333-CF10577473F7} - C:\Program Files\Google\Google Toolbar\GoogleToolbar_32.dll
O2 - BHO: SkypeIEPluginBHO - {AE805869-2E5C-4ED4-8F7B-F1F7851A4497} - C:\Program Files\Skype\Toolbars\Internet Explorer\skypeieplugin.dll
O2 - BHO: Java(tm) Plug-In 2 SSV Helper - {DBC80044-A445-435b-BC74-9C25C1C588A9} - C:\Program Files\Java\jre1.8.0_40\bin\jp2ssv.dll
O3 - Toolbar: Google Toolbar - {2318C2B1-4965-11d4-9B18-009027A5CD4F} - C:\Program Files\Google\Google Toolbar\GoogleToolbar_32.dll
O4 - HKLM\..\Run: [Windows Defender] %ProgramFiles%\Windows Defender\MSASCui.exe -hide
O4 - HKLM\..\Run: [RtHDVCpl] RtHDVCpl.exe
O4 - HKLM\..\Run: [DivXUpdate] "C:\Program Files\DivX\DivX Update\DivXUpdate.exe" /CHECKNOW
O4 - HKLM\..\Run: [AVG_UI] "C:\Program Files\AVG\AVG2015\avgui.exe" /TRAYONLY
O4 - HKLM\..\Run: [APSDaemon] "C:\Program Files\Common Files\Apple\Apple Application Support\APSDaemon.exe"
O4 - HKLM\..\Run: [QuickTime Task] "C:\Program Files\QuickTime\QTTask.exe" -atboottime
O4 - HKLM\..\Run: [iTunesHelper] "C:\Program Files\iTunes\iTunesHelper.exe"
O4 - HKLM\..\Run: [SunJavaUpdateSched] "C:\Program Files\Common Files\Java\Java Update\jusched.exe"
O4 - HKCU\..\Run: [WMPNSCFG] C:\Program Files\Windows Media Player\WMPNSCFG.exe
O4 - HKCU\..\Run: [CCleaner] "C:\Program Files\CCleaner\CCleaner.exe" /AUTO
O4 - HKUS\S-1-5-19\..\Run: [Sidebar] %ProgramFiles%\Windows Sidebar\Sidebar.exe /detectMem (User 'LOCAL SERVICE')
O4 - HKUS\S-1-5-19\..\Run: [WindowsWelcomeCenter] rundll32.exe oobefldr.dll,ShowWelcomeCenter (User 'LOCAL SERVICE')
O4 - HKUS\S-1-5-20\..\Run: [Sidebar] %ProgramFiles%\Windows Sidebar\Sidebar.exe /detectMem (User 'NETWORK SERVICE')
O8 - Extra context menu item: Google Sidewiki... - res://C:\Program Files\Google\Google Toolbar\Component\GoogleToolbarDynamic_mui_en_96D6FF0C6D236BF8.dll/cmsidewiki.html
O9 - Extra button: @C:\Program Files\Windows Live\Companion\companionlang.dll,-600 -

{0000036B-C524-4050-81A0-243669A86B9F} - C:\Program Files\Windows Live\Companion\companioncore.dll
O9 - Extra button: Skype Click to Call - {898EA8C8-E7FF-479B-8935-AEC46303B9E5} - C:\Program Files\Skype\Toolbars\Internet Explorer\skypeieplugin.dll
O11 - Options group: [ACCELERATED_GRAPHICS] Accelerated graphics
O16 - DPF: {05317530-B882-449D-9421-18D94FA3ED34} (OSInfo Control) - http://w3.sis.com/ocis/OSInfo.cab
O16 - DPF: {16095503-786F-4097-AED6-5D567A26D760} (SiS_OCX Control) - http://w3.sis.com/ocis/SiSAutodetectNT.cab
O16 - DPF: {BFF1950D-B1B4-4AE8-B842-B2CCF06D9A1B} (Zylom Games Player) - http://game.zylom.com/activex/zylomgamesplayer.cab
O16 - DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000} (Shockwave Flash Object) - http://fpdownload2.macromedia.com/get/shockwave/cabs/flash/swflash.cab
O16 - DPF: {E2883E8F-472F-4FB0-9522-AC9BF37916A7} - http://platformdl.adobe.com/NOS/getPlusPlus/1.6/gp.cab
O16 - DPF: {FD0B6769-6490-4A91-AA0A-B5AE0DC75AC9} (Performance Viewer Activex Control) - https://secure.logmein.com/activex/ractrl.cab?lmi=100
O18 - Protocol: bwfile-8876480 - {9462A756-7B47-47BC-8C80-C34B9B80B32B} - C:\Program Files\Logitech\Desktop Messenger\8876480\Program\GAPlugProtocol-8876480.dll
O18 - Protocol: linkscanner - {F274614C-63F8-47D5-A4D1-FBDDE494F8D1} - (no file)
O18 - Protocol: skype-ie-addon-data - {91774881-D725-4E58-B298-07617B9B86A8} - C:\Program Files\Skype\Toolbars\Internet Explorer\skypeieplugin.dll
O18 - Protocol: skype4com - {FFC8B962-9B40-4DFF-9458-1830C7DD7F5D} - C:\PROGRA~1\COMMON~1\Skype\SKYPE4~1.DLL
O18 - Protocol: viprotocol - {B658800C-F66E-4EF3-AB85-6C0C227862A9} - (no file)
O22 - SharedTaskScheduler: Component Categories cache daemon - {8C7461EF-2B13-11d2-BE35-3078302C2030} - C:\Windows\system32\browseui.dll
O23 - Service: Adobe Flash Player Update Service (AdobeFlashPlayerUpdateSvc) - Adobe Systems Incorporated - C:\Windows\system32\Macromed\Flash\FlashPlayerUpdateService.exe
O23 - Service: Apple Mobile Device - Apple Inc. - C:\Program Files\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe
O23 - Service: AVGIDSAgent - AVG Technologies CZ, s.r.o. - C:\Program Files\AVG\AVG2015\avgidsagent.exe
O23 - Service: AVG WatchDog (avgwd) - AVG Technologies CZ, s.r.o. - C:\Program Files\AVG\AVG2015\avgwdsvc.exe
O23 - Service: Bonjour-service (Bonjour Service) - Apple Inc. - C:\Program Files\Bonjour\mDNSResponder.exe
O23 - Service: Google Updateservice (gupdate) (gupdate) - Google Inc. - C:\Program Files\Google\Update\GoogleUpdate.exe
O23 - Service: Google Update-service (gupdatem) (gupdatem) - Google Inc. - C:\Program Files\Google\Update\GoogleUpdate.exe
O23 - Service: Google Software Updater (gusvc) - Google - C:\Program Files\Google\Common\Google Updater\GoogleUpdaterService.exe
O23 - Service: iPod-service (iPod Service) - Apple Inc. - C:\Program Files\iPod\bin\iPodService.exe
O23 - Service: McAfee Security Scan Component Host Service (McComponentHostService) - McAfee, Inc. - C:\Program Files\McAfee Security Scan\3.8.150\McCHSvc.exe
O23 - Service: Mozilla Maintenance Service (MozillaMaintenance) - Mozilla Foundation - C:\Program Files\Mozilla Maintenance Service\maintenanceservice.exe
O23 - Service: Rapport Management Service (RapportMgmtService) - IBM Corp. - C:\Program Files\Trusteer\Rapport\bin\RapportMgmtService.exe
O23 - Service: Skype C2C Service - Skype Technologies S.A. -

C:\ProgramData\Skype\Toolbars\Skype C2C Service\c2c_service.exe
O23 - Service: Skype Updater (SkypeUpdate) - Skype Technologies - C:\Program Files\Skype\Updater\Updater.exe
O23 - Service: TomTomHOMEService - TomTom - C:\Program Files\TomTom HOME 2\TomTomHOMEService.exe

==== Silent Runners ========================

"Silent Runners.vbs", revision 69.2, http://www.silentrunners.org/
Output limited to non-default values, except where indicated by "{++}"

Startup items buried in registry:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ {++}
WMPNSCFG = C:\Program Files\Windows Media Player\WMPNSCFG.exe [MS]
CCleaner = "C:\Program Files\CCleaner\CCleaner.exe" /AUTO [Piriform Ltd]

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ {++}
Windows Defender = C:\Program Files\Windows Defender\MSASCui.exe -hide
RtHDVCpl = RtHDVCpl.exe [Realtek Semiconductor]
DivXUpdate = "C:\Program Files\DivX\DivX Update\DivXUpdate.exe" /CHECKNOW [null data]
AVG_UI = "C:\Program Files\AVG\AVG2015\avgui.exe" /TRAYONLY [AVG Technologies CZ, s.r.o.]
APSDaemon = "C:\Program Files\Common Files\Apple\Apple Application Support\APSDaemon.exe" [Apple Inc.]
QuickTime Task = "C:\Program Files\QuickTime\QTTask.exe" -atboottime [Apple Inc.]
iTunesHelper = "C:\Program Files\iTunes\iTunesHelper.exe" [Apple Inc.]
SunJavaUpdateSched = "C:\Program Files\Common Files\Java\Java Update\jusched.exe" [Oracle Corporation]

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\

{0E8A89AD-95D7-40EB-8D9D-083EF7066A01}\(Default) = MSS+ Identifier
  -> {HKLM...CLSID} = MSS+ Identifier
        \InProcServer32\(Default) = C:\Program Files\McAfee Security Scan\3.8.150\McAfeeMSS_IE.dll [McAfee, Inc.]

{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\(Default) = AcroIEHelperStub
  -> {HKLM...CLSID} = Adobe PDF Link Helper
        \InProcServer32\(Default) = C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll [Adobe Systems Incorporated]

{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\(Default) = (no title provided)
  -> {HKLM...CLSID} = Java(tm) Plug-In SSV Helper
        \InProcServer32\(Default) = C:\Program Files\Java\jre1.8.0_40\bin\ssv.dll [Oracle Corporation]

{9030D464-4C02-4ABF-8ECC-5164760863C6}\(Default) = (no title provided)
  -> {HKLM...CLSID} = Windows Live ID Sign-in Helper
        \InProcServer32\(Default) = C:\Program Files\Common Files\Microsoft

Shared\Windows Live\WindowsLiveLogin.dll [MS]

{9FDDE16B-836F-4806-AB1F-1455CBEFF289}\(Default) = (no title provided)
 -> {HKLM...CLSID} = Windows Live Messenger Companion Helper
 \InProcServer32\(Default) = C:\Program Files\Windows Live\Companion\companioncore.dll [MS]

{AA58ED58-01DD-4d91-8333-CF10577473F7}\(Default) = (no title provided)
 -> {HKLM...CLSID} = Google Toolbar Helper
 \InProcServer32\(Default) = C:\Program Files\Google\Google Toolbar\GoogleToolbar_32.dll [Google Inc.]

{AE805869-2E5C-4ED4-8F7B-F1F7851A4497}\(Default) = SkypeIEPluginBHO
 -> {HKLM...CLSID} = Skype Browser Helper
 \InProcServer32\(Default) = C:\Program Files\Skype\Toolbars\Internet Explorer\skypeieplugin.dll [Skype Technologies S.A.]

{DBC80044-A445-435b-BC74-9C25C1C588A9}\(Default) = (no title provided)
 -> {HKLM...CLSID} = Java(tm) Plug-In 2 SSV Helper
 \InProcServer32\(Default) = C:\Program Files\Java\jre1.8.0_40\bin\jp2ssv.dll [Oracle Corporation]

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\

DropboxExt1\(Default) = {FB314ED9-A251-47B7-93E1-CDD82E34AF8B}
 -> {HKCU...CLSID} = DropboxExt
 \InProcServer32\(Default) = C:\Users\Bosman\AppData\Roaming\Dropbox\bin\DropboxExt.19.dll [Dropbox, Inc.]

DropboxExt2\(Default) = {FB314EDA-A251-47B7-93E1-CDD82E34AF8B}
 -> {HKCU...CLSID} = DropboxExt
 \InProcServer32\(Default) = C:\Users\Bosman\AppData\Roaming\Dropbox\bin\DropboxExt.19.dll [Dropbox, Inc.]

DropboxExt3\(Default) = {FB314EDB-A251-47B7-93E1-CDD82E34AF8B}
 -> {HKCU...CLSID} = DropboxExt
 \InProcServer32\(Default) = C:\Users\Bosman\AppData\Roaming\Dropbox\bin\DropboxExt.19.dll [Dropbox, Inc.]

HKCU\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved\

{FB314ED9-A251-47B7-93E1-CDD82E34AF8B} = DropboxExt
 -> {HKCU...CLSID} = DropboxExt
 \InProcServer32\(Default) = C:\Users\Bosman\AppData\Roaming\Dropbox\bin\DropboxExt.19.dll [Dropbox, Inc.]

{FB314EDA-A251-47B7-93E1-CDD82E34AF8B} = DropboxExt
 -> {HKCU...CLSID} = DropboxExt
 \InProcServer32\(Default) = C:\Users\Bosman\AppData\Roaming\Dropbox\bin\DropboxExt.19.dll [Dropbox, Inc.]

{FB314EDB-A251-47B7-93E1-CDD82E34AF8B} = DropboxExt

-> {HKCU...CLSID} = DropboxExt
\InProcServer32\(Default) =
C:\Users\Bosman\AppData\Roaming\Dropbox\bin\DropboxExt.19.dll [Dropbox, Inc.]

{FB314EDC-A251-47B7-93E1-CDD82E34AF8B} = DropboxExt
-> {HKCU...CLSID} = DropboxExt
\InProcServer32\(Default) =
C:\Users\Bosman\AppData\Roaming\Dropbox\bin\DropboxExt.19.dll [Dropbox, Inc.]

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved\

{BC593DF5-466F-44EC-8FFD-C4DBC603B917} = IZArc Shell Context Menu
-> {HKLM...CLSID} = IZArc Shell Context Menu
\InProcServer32\(Default) = C:\PROGRA~1\IZArc\IZArcCM.dll [null data]

{CA5FEE26-14C1-4B5A-86E9-233FC0EE2682} = IZArc DragDrop Menu
-> {HKLM...CLSID} = IZArc DragDrop Menu
\InProcServer32\(Default) = C:\PROGRA~1\IZArc\IZArcCM.dll [null data]

{9F97547E-4609-42C5-AE0C-81C61FFAEBC3} = AVG Shell Extension
-> {HKLM...CLSID} = AVG Shell Extension Class
\InProcServer32\(Default) = C:\Program Files\AVG\AVG2015\avgse.dll [AVG
Technologies CZ, s.r.o.]

{AE424E85-F6DF-4910-A6A9-438797986431} = OpenOffice.org Property Handler
-> {HKLM...CLSID} = OpenOffice.org Property Handler
\InProcServer32\(Default) = C:\Program Files\OpenOffice.org
3\Basis\program\shlxthdl\propertyhdl.dll [Apache Software Foundation]

{C52AF81D-F7A0-4AAB-8E87-F80A60CCD396} = OpenOffice.org Column Handler
-> {HKLM...CLSID} = (no title provided)
\InProcServer32\(Default) = C:\Program Files\OpenOffice.org
3\Basis\program\shlxthdl\shlxthdl.dll [Apache Software Foundation]

{087B3AE3-E237-4467-B8DB-5A38AB959AC9} = OpenOffice.org Infotip Handler
-> {HKLM...CLSID} = (no title provided)
\InProcServer32\(Default) = C:\Program Files\OpenOffice.org
3\Basis\program\shlxthdl\shlxthdl.dll [Apache Software Foundation]

{63542C48-9552-494A-84F7-73AA6A7C99C1} = OpenOffice.org Property Sheet Handler
-> {HKLM...CLSID} = (no title provided)
\InProcServer32\(Default) = C:\Program Files\OpenOffice.org
3\Basis\program\shlxthdl\shlxthdl.dll [Apache Software Foundation]

{3B092F0C-7696-40E3-A80F-68D74DA84210} = OpenOffice.org Thumbnail Viewer
-> {HKLM...CLSID} = (no title provided)
\InProcServer32\(Default) = C:\Program Files\OpenOffice.org
3\Basis\program\shlxthdl\shlxthdl.dll [Apache Software Foundation]

{B9E1D2CB-CCFF-4AA6-9579-D7A4754030EF} = iTunes
-> {HKLM...CLSID} = iTunes
\InProcServer32\(Default) = C:\Program Files\iTunes\iTunesMiniPlayer.dll [Apple Inc.]

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\

{65CD7F9B-E8F3-4bb0-82EB-6F6875B745DF}\(Default) = LogMeInCredProv
 -> {HKLM...CLSID} = LogMeInCredProv
 \InProcServer32\(Default) = LMIinit.dll [LogMeIn, Inc.]

HKLM\SOFTWARE\Classes\PROTOCOLS\Handler\

<<!>> bwfile-8876480\CLSID = {9462A756-7B47-47BC-8C80-C34B9B80B32B}
 -> {HKLM...CLSID} = BackWeb GA Pluggable Protocol
 \InProcServer32\(Default) = C:\Program Files\Logitech\Desktop Messenger\8876480\Program\GAPlugProtocol-8876480.dll [Logitech Inc.]

<<!>> skype-ie-addon-data\CLSID = {91774881-D725-4E58-B298-07617B9B86A8}
 -> {HKLM...CLSID} = Skype IE add-on Pluggable Protocol
 \InProcServer32\(Default) = C:\Program Files\Skype\Toolbars\Internet Explorer\skypeieplugin.dll [Skype Technologies S.A.]

<<!>> skype4com\CLSID = {FFC8B962-9B40-4DFF-9458-1830C7DD7F5D}
 -> {HKLM...CLSID} = IEProtocolHandler Class
 \InProcServer32\(Default) = C:\PROGRA~1\COMMON~1\Skype\SKYPE4~1.DLL [Skype Technologies]

HKCU\Software\Classes*\shellex\ContextMenuHandlers\

DropboxExt\(Default) = {FB314ED9-A251-47B7-93E1-CDD82E34AF8B}
 -> {HKCU...CLSID} = DropboxExt
 \InProcServer32\(Default) = C:\Users\Bosman\AppData\Roaming\Dropbox\bin\DropboxExt.19.dll [Dropbox, Inc.]

HKLM\SOFTWARE\Classes*\shellex\ContextMenuHandlers\

AVG Shell Extension\(Default) = {9F97547E-4609-42C5-AE0C-81C61FFAEBC3}
 -> {HKLM...CLSID} = AVG Shell Extension Class
 \InProcServer32\(Default) = C:\Program Files\AVG\AVG2015\avgse.dll [AVG Technologies CZ, s.r.o.]

IZArcCM\(Default) = {BC593DF5-466F-44EC-8FFD-C4DBC603B917}
 -> {HKLM...CLSID} = IZArc Shell Context Menu
 \InProcServer32\(Default) = C:\PROGRA~1\IZArc\IZArcCM.dll [null data]

PhotoStreamsExt\(Default) = {89D984B3-813B-406A-8298-118AFA3A22AE}
 -> {HKLM...CLSID} = ContextMenuHandler Class
 \InProcServer32\(Default) = C:\Program Files\Common Files\Apple\Internet Services\ShellStreams.dll [Apple Inc.]

HKCU\Software\Classes\Directory\shellex\ContextMenuHandlers\

DropboxExt\(Default) = {FB314ED9-A251-47B7-93E1-CDD82E34AF8B}
 -> {HKCU...CLSID} = DropboxExt
 \InProcServer32\(Default) =

C:\Users\Bosman\AppData\Roaming\Dropbox\bin\DropboxExt.19.dll [Dropbox, Inc.]

HKLM\SOFTWARE\Classes\Directory\shellex\ContextMenuHandlers\

IZArcCM\(Default) = {BC593DF5-466F-44EC-8FFD-C4DBC603B917}
 -> {HKLM...CLSID} = IZArc Shell Context Menu
 \InProcServer32\(Default) = C:\PROGRA~1\IZArc\IZArcCM.dll [null data]

HKLM\SOFTWARE\Classes\Directory\shellex\DragDropHandlers\

IZArcCM\(Default) = {CA5FEE26-14C1-4B5A-86E9-233FC0EE2682}
 -> {HKLM...CLSID} = IZArc DragDrop Menu
 \InProcServer32\(Default) = C:\PROGRA~1\IZArc\IZArcCM.dll [null data]

HKCU\Software\Classes\Directory\Background\shellex\ContextMenuHandlers\

DropboxExt\(Default) = {FB314ED9-A251-47B7-93E1-CDD82E34AF8B}
 -> {HKCU...CLSID} = DropboxExt
 \InProcServer32\(Default) =
C:\Users\Bosman\AppData\Roaming\Dropbox\bin\DropboxExt.19.dll [Dropbox, Inc.]

HKLM\SOFTWARE\Classes\Folder\shellex\ColumnHandlers\

{C52AF81D-F7A0-4AAB-8E87-F80A60CCD396}\(Default) = OpenOffice.org Column Handler
 -> {HKLM...CLSID} = (no title provided)
 \InProcServer32\(Default) = C:\Program Files\OpenOffice.org
3\Basis\program\shlxthdl\shlxthdl.dll [Apache Software Foundation]

{F9DB5320-233E-11D1-9F84-707F02C10627}\(Default) = PDF Column Info
 -> {HKLM...CLSID} = PDF Shell Extension
 \InProcServer32\(Default) = C:\Program Files\Common
Files\Adobe\Acrobat\ActiveX\PDFShell.dll [Adobe Systems, Inc.]

HKLM\SOFTWARE\Classes\Folder\shellex\ContextMenuHandlers\

AVG Shell Extension\(Default) = {9F97547E-4609-42C5-AE0C-81C61FFAEBC3}
 -> {HKLM...CLSID} = AVG Shell Extension Class
 \InProcServer32\(Default) = C:\Program Files\AVG\AVG2015\avgse.dll [AVG
Technologies CZ, s.r.o.]

HKLM\SOFTWARE\Classes\Folder\shellex\DragDropHandlers\

IZArcCM\(Default) = {CA5FEE26-14C1-4B5A-86E9-233FC0EE2682}
 -> {HKLM...CLSID} = IZArc DragDrop Menu
 \InProcServer32\(Default) = C:\PROGRA~1\IZArc\IZArcCM.dll [null data]

Active Desktop and Wallpaper:

Active Desktop may be disabled at this entry:
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellState

Displayed if Active Desktop enabled and wallpaper not set by Group Policy:
HKCU\Software\Microsoft\Internet Explorer\Desktop\General\
Wallpaper =
C:\Windows\system32\config\systemprofile\AppData\Roaming\Mozilla\Firefox\Bureaubladachterg
rond.bmp

Displayed if Active Desktop disabled and wallpaper not set by Group Policy:
HKCU\Control Panel\Desktop\
Wallpaper = C:\Users\Bosman\AppData\Roaming\Mozilla\Firefox\Bureaubladachtergrond.bmp

Enabled Screen Saver:

HKCU\Control Panel\Desktop\
SCRNSAVE.EXE = C:\Windows\system32\Aurora.scr [MS]

Windows Portable Device AutoPlay Handlers

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\AutoplayHandlers\Handlers\

DropboxAutoplayProxy\
Provider = Dropbox
InvokeProgID = Dropbox.AutoplayEventHandlerProxy
InvokeVerb = import
HKLM\SOFTWARE\Classes\Dropbox.AutoplayEventHandlerProxy\shell\import\DropTarget\CLSI
D = {F38F335B-BC2E-450E-8FC6-0E13E17FC8FE}
  -> {HKLM...CLSID} = Dropbox Autoplay Proxy COM Server
        \LocalServer32\(Default) = C:\Program Files\Dropbox\DropboxProxy.exe
/autoplayproxy [Dropbox, Inc.]

HPAutoplayPSE\
Provider = HP Photosmart Essential 2.01
InvokeProgID = HpqPSApl.Autoplay
InvokeVerb = Play
HKLM\SOFTWARE\Classes\HpqPSApl.Autoplay\shell\Play\DropTarget\CLSID = {A6873065-
D632-4615-A3A9-C5F05EE109C1}
  -> {HKLM...CLSID} = (no title provided)
        \LocalServer32\(Default) = C:\Program Files\HP\Digital Imaging\bin\HpqPsApl.exe
[Hewlett-Packard]

iTunesBurnCDOnArrival\
Provider = iTunes
InvokeProgID = iTunes.BurnCD
InvokeVerb = burn
HKLM\SOFTWARE\Classes\iTunes.BurnCD\shell\burn\command\(Default) = "C:\Program
Files\iTunes\iTunes.exe" /AutoPlayBurn "%L" [Apple Inc.]

iTunesImportSongsOnArrival\

Provider = iTunes
InvokeProgID = iTunes.ImportSongsOnCD
InvokeVerb = import
HKLM\SOFTWARE\Classes\iTunes.ImportSongsOnCD\shell\import\command\(Default) =
"C:\Program Files\iTunes\iTunes.exe" /AutoPlayImportSongs "%L" [Apple Inc.]

iTunesPlaySongsOnArrival\
Provider = iTunes
InvokeProgID = iTunes.PlaySongsOnCD
InvokeVerb = play
HKLM\SOFTWARE\Classes\iTunes.PlaySongsOnCD\shell\play\command\(Default) =
"C:\Program Files\iTunes\iTunes.exe" /playCD "%L" [Apple Inc.]

iTunesShowSongsOnArrival\
Provider = iTunes
InvokeProgID = iTunes.ShowSongsOnCD
InvokeVerb = showsongs
HKLM\SOFTWARE\Classes\iTunes.ShowSongsOnCD\shell\showsongs\command\(Default) =
"C:\Program Files\iTunes\iTunes.exe" /AutoPlayShowSongs "%L" [Apple Inc.]

VLCPlayCDAudioOnArrival\
Provider = VideoLAN VLC media player
InvokeProgID = VLC.CDAudio
InvokeVerb = Open
HKLM\SOFTWARE\Classes\VLC.CDAudio\shell\Open\command\(Default) = "C:\Program
Files\VideoLAN\VLC\vlc.exe" --started-from-file cdda://%1 [the VideoLAN Team]

VLCPlayDVDAudioOnArrival\
Provider = VideoLAN VLC media player
InvokeProgID = VLC.OPENFolder
InvokeVerb = Open
HKLM\SOFTWARE\Classes\VLC.OPENFolder\shell\Open\command\(Default) = "C:\Program
Files\VideoLAN\VLC\vlc.exe" %1 [the VideoLAN Team]

VLCPlayDVDMovieOnArrival\
Provider = VideoLAN VLC media player
InvokeProgID = VLC.DVDMovie
InvokeVerb = Open
HKLM\SOFTWARE\Classes\VLC.DVDMovie\shell\Open\command\(Default) = "C:\Program
Files\VideoLAN\VLC\vlc.exe" --started-from-file dvd://%1 [the VideoLAN Team]

VLCPlayMusicFilesOnArrival\
Provider = VideoLAN VLC media player
InvokeProgID = VLC.OPENFolder
InvokeVerb = Open
HKLM\SOFTWARE\Classes\VLC.OPENFolder\shell\Open\command\(Default) = "C:\Program
Files\VideoLAN\VLC\vlc.exe" %1 [the VideoLAN Team]

VLCPlaySVCDMovieOnArrival\
Provider = VideoLAN VLC media player
InvokeProgID = VLC.SVCDMovie
InvokeVerb = Open

HKLM\SOFTWARE\Classes\VLC.SVCDMovie\shell\Open\command\(Default) = "C:\Program Files\VideoLAN\VLC\vlc.exe" --started-from-file vcd://%1 [the VideoLAN Team]

VLCPlayVCDMovieOnArrival\
Provider = VideoLAN VLC media player
InvokeProgID = VLC.VCDMovie
InvokeVerb = Open
HKLM\SOFTWARE\Classes\VLC.VCDMovie\shell\Open\command\(Default) = "C:\Program Files\VideoLAN\VLC\vlc.exe" --started-from-file vcd://%1 [the VideoLAN Team]

VLCPlayVideoFilesOnArrival\
Provider = VideoLAN VLC media player
InvokeProgID = VLC.OPENFolder
InvokeVerb = Open
HKLM\SOFTWARE\Classes\VLC.OPENFolder\shell\Open\command\(Default) = "C:\Program Files\VideoLAN\VLC\vlc.exe" %1 [the VideoLAN Team]

Windows Sidebar Gadgets: {++}

C:\Users\Bosman\AppData\Local\Microsoft\Windows Sidebar\Settings.ini
%PROGRAMFILES%\windows sidebar\gadgets\Clock.gadget
%PROGRAMFILES%\windows sidebar\gadgets\SlideShow.Gadget
%PROGRAMFILES%\windows sidebar\gadgets\RSSFeeds.Gadget

Non-disabled Scheduled Tasks: {++}

C:\Windows\System32\Tasks
Ad-Aware Update (Weekly) -> launches: C:\Program Files\Lavasoft\Ad-Aware\Ad-AwareAdmin.exe update all silent repair [file not found]
Adobe Flash Player Updater -> launches: C:\Windows\system32\Macromed\Flash\FlashPlayerUpdateService.exe [Adobe Systems Incorporated]
CCleanerSkipUAC -> launches: "C:\Program Files\CCleaner\CCleaner.exe" $(Arg0) [Piriform Ltd]
CreateChoiceProcessTask -> launches: C:\Windows\System32\browserchoice.exe /launch [MS]
FacebookUpdateTaskUserS-1-5-21-2909120250-2823181194-1062834500-1000Core -> launches: C:\Users\Bosman\AppData\Local\Facebook\Update\FacebookUpdate.exe /c /nocrashserver [file not found]
FacebookUpdateTaskUserS-1-5-21-2909120250-2823181194-1062834500-1000UA -> launches: C:\Users\Bosman\AppData\Local\Facebook\Update\FacebookUpdate.exe /ua /installsource scheduler [file not found]
GoogleUpdateTaskMachineCore -> launches: C:\Program Files\Google\Update\GoogleUpdate.exe /c [Google Inc.]
GoogleUpdateTaskMachineUA -> launches: C:\Program Files\Google\Update\GoogleUpdate.exe /ua /installsource scheduler [Google Inc.]
{0DF60E66-51EC-4317-89A0-6B85CDC036B4} -> launches: C:\Windows\system32\pcalua.exe -a E:\Setup.now.exe -d E:\ [MS]
{691E71DD-192F-435D-8E85-1E46D03764C4} -> launches: C:\Program

Files\Skype\Phone\Skype.exe [Skype Technologies S.A.]
{6FD4499E-9B10-420E-AAED-35EB8C9DA10D} -> launches: C:\Windows\system32\pcalua.exe -a C:\Windows\unasetup.exe [MS]

C:\Windows\System32\Tasks\Apple
AppleSoftwareUpdate -> launches: C:\Program Files\Apple Software Update\SoftwareUpdate.exe -task [Apple Inc.]

C:\Windows\System32\Tasks\Microsoft\Windows\Active Directory Rights Management Services Client
AD RMS Rights Policy Template Management (Manual) -> launches: {BF5CB148-7C77-4d8a-A53E-D81C70CF743C}
-> {HKLM...CLSID} = AD RMS Rights Policy Template Management (Manual) Task Handler
\InProcServer32\(Default) = C:\Windows\system32\msdrm.dll [MS]

C:\Windows\System32\Tasks\Microsoft\Windows\Bluetooth
UninstallDeviceTask -> launches: BthUdTask.exe $(Arg0) [MS]

C:\Windows\System32\Tasks\Microsoft\Windows\CertificateServicesClient
SystemTask -> launches: {58fb76b9-ac85-4e55-ac04-427593b1d060}
-> {HKLM...CLSID} = Certificate Services Client Task Handler
\InProcServer32\(Default) = C:\Windows\system32\dimsjob.dll [MS]
UserTask -> launches: {58fb76b9-ac85-4e55-ac04-427593b1d060}
-> {HKLM...CLSID} = Certificate Services Client Task Handler
\InProcServer32\(Default) = C:\Windows\system32\dimsjob.dll [MS]
UserTask-Roam -> launches: {58fb76b9-ac85-4e55-ac04-427593b1d060}
-> {HKLM...CLSID} = Certificate Services Client Task Handler
\InProcServer32\(Default) = C:\Windows\system32\dimsjob.dll [MS]

C:\Windows\System32\Tasks\Microsoft\Windows\Customer Experience Improvement Program
Consolidator -> launches: %SystemRoot%\System32\wsqmcons.exe [MS]
OptinNotification -> launches: %SystemRoot%\System32\wsqmcons.exe -n 0x1C577FA2B69CAD0 [MS]

C:\Windows\System32\Tasks\Microsoft\Windows\Defrag
ManualDefrag -> launches: %windir%\system32\defrag.exe \\?\Volume{9249a7fc-acfe-11de-bb63-806e6f6e6963}\ \\?\Volume{9249a7fd-acfe-11de-bb63-806e6f6e6963}\ \\?\Volume{9249a7fe-acfe-11de-bb63-806e6f6e6963}\ \\?\Volume{39d90fb9-d12c-11e2-ba31-001558bb82a6}\ [MS]
ScheduledDefrag -> launches: %windir%\system32\defrag.exe -c -i [MS]

C:\Windows\System32\Tasks\Microsoft\Windows\MobilePC
HotStart -> launches: {06DA0625-9701-43da-BFD7-FBEEA2180A1E}
-> {HKLM...CLSID} = HotStart User Agent
\InProcServer32\(Default) = C:\Windows\System32\HotStartUserAgent.dll [MS]
TMM -> launches: {35EF4182-F900-4632-B072-8639E4478A61}
-> {HKLM...CLSID} = Transient Multi-Monitor Manager
\InProcServer32\(Default) = C:\Windows\System32\TMM.dll [MS]

C:\Windows\System32\Tasks\Microsoft\Windows\MUI
LPRemove -> launches: %windir%\system32\lpremove.exe [MS]

C:\Windows\System32\Tasks\Microsoft\Windows\Multimedia

SystemSoundsService -> launches: {2DEA658F-54C1-4227-AF9B-260AB5FC3543}
-> {HKLM...CLSID} = Microsoft PlaySoundService Class
\InProcServer32\(Default) = C:\Windows\System32\PlaySndSrv.dll [MS]

C:\Windows\System32\Tasks\Microsoft\Windows\NetworkAccessProtection
NAPStatus UI -> launches: {f09878a1-4652-4292-aa63-8c7d4fd7648f}
-> {HKLM...CLSID} = Nap ITask Handler Implementation
\InProcServer32\(Default) = C:\Windows\System32\QAgent.dll [MS]

C:\Windows\System32\Tasks\Microsoft\Windows\RAC
RACAgent -> (HIDDEN!) launches: %windir%\system32\RacAgent.exe [MS]

C:\Windows\System32\Tasks\Microsoft\Windows\RemoteAssistance
RemoteAssistanceTask -> (HIDDEN!) launches: %windir%\system32\RAServer.exe /offerraupdate
[MS]

C:\Windows\System32\Tasks\Microsoft\Windows\Shell
CrawlStartPages -> launches: {51653423-e62d-4ff7-894a-dabb2b8e21e2}
-> {HKLM...CLSID} = CrawlStartPages Task Handler
\InProcServer32\(Default) = C:\Windows\System32\srchadmin.dll [MS]

C:\Windows\System32\Tasks\Microsoft\Windows\SystemRestore
SR -> launches: %windir%\system32\rundll32.exe /d srrstr.dll,ExecuteScheduledSPPCreation
[MS]

C:\Windows\System32\Tasks\Microsoft\Windows\Tcpip
IpAddressConflict1 -> launches: rundll32 ndfapi.dll,NdfRunDllDuplicateIPOffendingSystem [MS]
IpAddressConflict2 -> launches: rundll32 ndfapi.dll,NdfRunDllDuplicateIPDefendingSystem [MS]
WSHReset -> (HIDDEN!) launches: %systemroot%\system32\netsh.exe interface tcp set heuristic
wsh=default [MS]

C:\Windows\System32\Tasks\Microsoft\Windows\TextServicesFramework
MsCtfMonitor -> (HIDDEN!) launches: {01575cfe-9a55-4003-a5e1-f38d1ebdcbe1}
-> {HKLM...CLSID} = MsCtfMonitor task handler
\InProcServer32\(Default) = C:\Windows\system32\MsCtfMonitor.dll [MS]

C:\Windows\System32\Tasks\Microsoft\Windows\UPnP
UPnPHostConfig -> launches: sc.exe config upnphost start= auto [MS]

C:\Windows\System32\Tasks\Microsoft\Windows\WDI
ResolutionHost -> (HIDDEN!) launches: {900be39d-6be8-461a-bc4d-b0fa71f5ecb1}
-> {HKLM...CLSID} = DiagnosticInfrastructureCustomHandler
\InProcServer32\(Default) = C:\Windows\System32\wdi.dll [MS]

C:\Windows\System32\Tasks\Microsoft\Windows\Windows Error Reporting
QueueReporting -> launches: %windir%\system32\wermgr.exe -queuereporting [MS]

C:\Windows\System32\Tasks\Microsoft\Windows\WindowsBackup
AutomaticBackup -> launches: %systemroot%\system32\rundll32.exe /d
sdengin2.dll,ExecuteScheduledBackup [MS]
Windows Backup Monitor -> launches: sdclt.exe /DETECTFAILURE [MS]

C:\Windows\System32\Tasks\Microsoft\Windows\WindowsCalendar
Reminders - Bosman -> launches: C:\Program Files\Windows Calendar\wincal.exe /reminder [MS]

C:\Windows\System32\Tasks\Microsoft\Windows\Wired
GatherWiredInfo -> launches: %windir%\system32\gatherWiredInfo.vbs [null data]

C:\Windows\System32\Tasks\Microsoft\Windows\Wireless
GatherWirelessInfo -> launches: %windir%\system32\gatherWirelessInfo.vbs [null data]

C:\Windows\System32\Tasks\Microsoft\Windows Live\SOXE
Extractor Definitions Update Task -> launches: {3519154C-227E-47F3-9CC9-12C3F05817F1}
  -> {HKLM...CLSID} = Windows Live Social Object Extractor Engine Definition Updater
		\InProcServer32\(Default) = C:\Program Files\Windows Live\SOXE\wlsoxe.dll [MS]

C:\Windows\System32\Tasks\WPD
SqmUpload_S-1-5-21-2909120250-2823181194-1062834500-1000 -> (HIDDEN!) launches:
%windir%\system32\rundll32.exe portabledeviceapi.dll,#1 [MS]

Winsock2 Service Provider DLLs:

Namespace Service Providers

HKLM\SYSTEM\CurrentControlSet\Services\Winsock2\Parameters\NameSpace_Catalog5\Catalog
_Entries\ {++}
000000000001\LibraryPath = %SystemRoot%\system32\NLAapi.dll [MS]
000000000002\LibraryPath = %SystemRoot%\system32\napinsp.dll [MS]
000000000003\LibraryPath = %SystemRoot%\system32\pnrpnsp.dll [MS]
000000000004\LibraryPath = %SystemRoot%\system32\pnrpnsp.dll [MS]
000000000005\LibraryPath = %SystemRoot%\System32\mswsock.dll [MS]
000000000006\LibraryPath = %SystemRoot%\System32\winrnr.dll [MS]
000000000007\LibraryPath = C:\Program Files\Bonjour\mdnsNSP.dll [Apple Inc.]

Transport Service Providers

HKLM\SYSTEM\CurrentControlSet\Services\Winsock2\Parameters\Protocol_Catalog9\Catalog_E
ntries\ {++}
0000000000##\PackedCatalogItem (contains) DLL [Company Name], (at) ## range:
%SystemRoot%\system32\mswsock.dll [MS], 01 - 18

Toolbars, Explorer Bars, Extensions:

Toolbars

HKCU\Software\Microsoft\Internet Explorer\Toolbar\WebBrowser\

{2318C2B1-4965-11D4-9B18-009027A5CD4F}
  -> {HKLM...CLSID} = Google Toolbar
		\InProcServer32\(Default) = C:\Program Files\Google\Google

Toolbar\GoogleToolbar_32.dll [Google Inc.]

HKLM\SOFTWARE\Microsoft\Internet Explorer\Toolbar\
{2318C2B1-4965-11D4-9B18-009027A5CD4F} = (no title provided)
 -> {HKLM...CLSID} = Google Toolbar
 \InProcServer32\(Default) = C:\Program Files\Google\Google
Toolbar\GoogleToolbar_32.dll [Google Inc.]

Extensions (Tools menu items, main toolbar menu buttons)

HKLM\SOFTWARE\Microsoft\Internet Explorer\Extensions\
{0000036B-C524-4050-81A0-243669A86B9F}\
ButtonText = @C:\Program Files\Windows Live\Companion\companionlang.dll,-600
CLSIDExtension = {B63DBA5F-523F-4B9C-A43D-65DF1977EAD3}
 -> {HKLM...CLSID} = Windows Live Messenger Companion Command Bar Button
 \InProcServer32\(Default) = C:\Program Files\Windows
Live\Companion\companioncore.dll [MS]

{898EA8C8-E7FF-479B-8935-AEC46303B9E5}\
ButtonText = Skype Click to Call
CLSIDExtension = {898EA8C8-E7FF-479B-8935-AEC46303B9E5}
 -> {HKLM...CLSID} = Skype Browser Helper
 \InProcServer32\(Default) = C:\Program Files\Skype\Toolbars\Internet
Explorer\skypeieplugin.dll [Skype Technologies S.A.]

Miscellaneous IE Hijack Points

HKLM\SOFTWARE\Microsoft\Internet Explorer\AboutURLs\
<<H>> Tabs = about:newtab [file not found]

Running Services (Display Name, Service Name, Path {Service DLL}):

Apple Mobile Device, Apple Mobile Device, "C:\Program Files\Common Files\Apple\Mobile
Device Support\AppleMobileDeviceService.exe" [Apple Inc.]
AVG WatchDog, avgwd, "C:\Program Files\AVG\AVG2015\avgwdsvc.exe" [AVG Technologies
CZ, s.r.o.]
Bonjour-service, Bonjour Service, "C:\Program Files\Bonjour\mDNSResponder.exe" [Apple Inc.]
HP CUE DeviceDiscovery-service, hpqddsvc, C:\Windows\system32\svchost.exe -k hpdevmgmt
{C:\Program Files\HP\Digital Imaging\bin\hpqddsvc.dll [Hewlett-Packard Co.]}
hpqcxs08, hpqcxs08, C:\Windows\system32\svchost.exe -k hpdevmgmt {C:\Program
Files\HP\Digital Imaging\bin\hpqcxs08.dll [Hewlett-Packard Co.]}
iPod-service, iPod Service, "C:\Program Files\iPod\bin\iPodService.exe" [Apple Inc.]
Rapport Management Service, RapportMgmtService, "C:\Program
Files\Trusteer\Rapport\bin\RapportMgmtService.exe" [IBM Corp.]
SeaPort, SeaPort, "C:\Program Files\Microsoft\BingBar\SeaPort.EXE" [MS]
Windows Live ID Sign-in Assistant, wlidsvc, "C:\Program Files\Common Files\Microsoft
Shared\Windows Live\WLIDSVC.EXE" [MS]

Safe Mode Drivers & Services (subkey name, subkey default value):

HKLM\System\CurrentControlSet\Control\SafeBoot\Minimal\

<<!>> PEVSystemStart, Service

HKLM\System\CurrentControlSet\Control\SafeBoot\Network\

<<!>> hitmanpro35,
<<!>> hitmanpro35.sys,
<<!>> PEVSystemStart, Service

Print Monitors:

HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors\
LIDIL hpzll5ha\Driver = hpzll5ha.dll [Hewlett-Packard Company]
LIDIL hpzll64X\Driver = hpzll64X.dll [Hewlett-Packard Company]
LogMeIn Printer Port Monitor\Driver = LMIport.dll [LogMeIn, Inc.]
Redmon\Driver = redmonnt.dll [null data]

<<H>>: Suspicious data at a browser hijack point.

==== Empty IE Cache ==========

C:\Users\Default\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5 emptied successfully
C:\Windows\serviceprofiles\networkservice\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5 emptied successfully
C:\Windows\serviceprofiles\Localservice\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5 emptied successfully
C:\Users\Bosman\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\6AAB8MQW will be deleted at reboot
C:\Users\Bosman\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\EZENTCRQ will be deleted at reboot
C:\Users\Bosman\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\LSUBE236 will be deleted at reboot
C:\Users\Bosman\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat will be deleted at reboot
C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat will be deleted at reboot
C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat will be deleted at reboot

==== Empty FireFox Cache ==========

C:\Users\Bosman\AppData\Local\Mozilla\Firefox\Profiles\irxf5u4v.default\cache2 emptied

successfully

==== Empty Chrome Cache ==========

No Chrome User Data found

==== Empty All Flash Cache ==========

Flash Cache Emptied Successfully

==== Empty All Java Cache ==========

Java Cache cleared successfully

==== C:\zoek_backup content ==========

C:\zoek_backup (files=2792 folders=781 230647495 bytes)

==== Empty Temp Folders ==========

C:\Users\Bosman\AppData\Local\Temp will be emptied at reboot
C:\Users\Default\AppData\Local\Temp emptied successfully
C:\Users\Default User\AppData\Local\Temp emptied successfully
C:\Windows\system32\config\systemprofile\AppData\Local\Temp emptied successfully
C:\Windows\serviceprofiles\networkservice\AppData\Local\Temp emptied successfully
C:\Windows\serviceprofiles\Localservice\AppData\Local\Temp emptied successfully
C:\Windows\Temp will be emptied at reboot

==== After Reboot ==========

==== Empty Temp Folders ==========

C:\Windows\Temp successfully emptied
C:\Users\Bosman\AppData\Local\Temp successfully emptied

==== Empty Recycle Bin ==========

C:\$RECYCLE.BIN successfully emptied

==== Deleting Files / Folders ==========

"C:\Users\Bosman\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat" not deleted
"C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat" not deleted
"C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat" not deleted
"C:\Users\Bosman\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\6AAB8MQW" not found
"C:\Users\Bosman\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\EZENTCRQ" not found
"C:\Users\Bosman\AppData\Local\Microsoft\Windows\Temporary Internet

Files\Content.IE5\LSUBE236" not found

==== EOF on za 07-03-2015 at 12:05:52,73 ==========