```
Logfile of random's system information tool 1.10 (written by
random/random)
Run by user at 2016-04-10 17:07:42
Microsoft Windows 10 Pro
System drive C: has 60 GB (39%) free of 152 GB
Total RAM: 2996 MB (32% free)

Logfile of Trend Micro HijackThis v2.0.4
Scan saved at 17:07:54, on 10.4.2016
Platform: Unknown Windows (WinNT 6.02.1008)
MSIE: Internet Explorer v11.0 (11.00.10586.0020)
Boot mode: Normal

Running processes:
C:\Program Files\AVG PC TuneUp\TuneUpUtilitiesApp32.exe
C:\Program Files\Synaptics\SynTP\SynTPEnh.exe
C:\WINDOWS\system32\sihost.exe
C:\WINDOWS\system32\taskhostw.exe
C:\Windows\System32\RuntimeBroker.exe
C:\WINDOWS\Explorer.EXE
C:\PROGRAM FILES\SYNAPTICS\SYNTP\SYNTPHELPER.EXE
C:\Program
Files\WindowsApps\Microsoft.Messaging_2.13.20000.0_x86__8wekyb3d8bbwe\Sky
peHost.exe
C:\Program Files\Synaptics\SynTP\SynTPLpr.exe
C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHo
st.exe
C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.ex
e
C:\Windows\System32\hkcmd.exe
C:\Windows\System32\igfxpers.exe
C:\Program Files\AVAST Software\Avast\avastui.exe
C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe
C:\WINDOWS\system32\wbem\unsecapp.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\SettingSyncHost.exe
C:\WINDOWS\system32\ApplicationFrameHost.exe
C:\WINDOWS\ImmersiveControlPanel\SystemSettings.exe
C:\Program
Files\WindowsApps\Microsoft.WindowsStore_2016.29.13.0_x86__8wekyb3d8bbwe\
WinStore.Mobile.exe
C:\Program
Files\WindowsApps\E046963F.LenovoCompanion_3.42.1.0_x86__k1h2ywk1493x8\Le
novo.Discovery.exe
C:\Program
Files\Lenovo\iMController\PluginHost\Lenovo.Modern.ImController.PluginHos
t.exe
C:\Program Files\Google\Chrome\Application\chrome.exe
C:\Program Files\Google\Chrome\Application\chrome.exe
C:\Program Files\Google\Chrome\Application\chrome.exe
C:\Program Files\Google\Chrome\Application\chrome.exe
C:\Program Files\Google\Chrome\Application\chrome.exe
C:\Program Files\Google\Chrome\Application\chrome.exe
C:\Program Files\Google\Chrome\Application\chrome.exe
C:\Program Files\Google\Chrome\Application\chrome.exe
C:\Program
Files\Lenovo\iMController\PluginHost\Lenovo.Modern.ImController.PluginHos
t.exe
```

```
C:\Program Files\Google\Chrome\Application\chrome.exe
C:\Program Files\CCleaner\CCleaner.exe
C:\Program Files\CCleaner\CCleaner.exe
C:\WINDOWS\system32\SearchProtocolHost.exe
C:\WINDOWS\system32\SearchFilterHost.exe
C:\Program Files\Google\Chrome\Application\chrome.exe
C:\Users\user\Downloads\RSIT.exe
C:\Program Files\trend micro\user.exe

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar =
https://www.google.com/?trackid=sp-006
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page =
https://www.google.com/search?trackid=sp-006&q={searchTerms}
R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page =
http://stadsear.com/search5
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL =
http://go.microsoft.com/fwlink/p/?LinkId=255141
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL =
http://go.microsoft.com/fwlink/?LinkId=54896
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Bar =
https://www.google.com/?trackid=sp-006
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page =
https://www.google.com/search?trackid=sp-006&q={searchTerms}
R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Start Page =
https://www.google.com/?trackid=sp-006
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant =
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =
R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName =
O2 - BHO: Lync Click to Call BHO - {31D09BA0-12F5-4CCE-BE8A-2923E76605DA}
- C:\Program Files\Microsoft Office\Office15\OCHelper.dll
O2 - BHO: Java(tm) Plug-In SSV Helper - {761497BB-D6F0-462C-B6EB-
D4DAF1D92D43} - C:\Program Files\Java\jre1.8.0_73\bin\ssv.dll
O2 - BHO: avast! Online Security - {8E5E2654-AD2D-48bf-AC2D-D17F00898D06}
- C:\Program Files\AVAST Software\Avast\aswWebRepIE.dll
O2 - BHO: URLRedirectionBHO - {B4F3A835-0E21-4959-BA22-42B3008E02FF} -
C:\PROGRA~1\MICROS~1\Office15\URLREDIR.DLL
O2 - BHO: Microsoft SkyDrive Pro Browser Helper - {D0498E0A-45B7-42AE-
A9AA-ABA463DBD3BF} - C:\PROGRA~1\MICROS~1\Office15\GROOVEEX.DLL
O2 - BHO: Java(tm) Plug-In 2 SSV Helper - {DBC80044-A445-435b-BC74-
9C25C1C588A9} - C:\Program Files\Java\jre1.8.0_73\bin\jp2ssv.dll
O4 - HKLM\..\Run: [IgfxTray] C:\WINDOWS\system32\igfxtray.exe
O4 - HKLM\..\Run: [HotKeysCmds] C:\WINDOWS\system32\hkcmd.exe
O4 - HKLM\..\Run: [Persistence] C:\WINDOWS\system32\igfxpers.exe
O4 - HKLM\..\Run: [AvastUI.exe] "C:\Program Files\AVAST
Software\Avast\AvastUI.exe" /nogui
O4 - HKLM\..\Run: [SynLenovoHelper]
%ProgramFiles%\Synaptics\SynTP\SynLenovoHelper.exe
O4 - HKLM\..\Run: [SDTray] "C:\Program Files\Spybot - Search & Destroy
2\SDTray.exe"
O4 - HKLM\..\Run: [SynTPEnh] %ProgramFiles%\Synaptics\SynTP\SynTPEnh.exe
O4 - HKLM\..\Run: [SunJavaUpdateSched] "C:\Program Files\Common
Files\Java\Java Update\jusched.exe"
O4 - HKCU\..\Run: [OneDrive]
"C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
O4 - HKCU\..\Run: [SpybotPostWindows10UpgradeReInstall] "C:\Program
Files\Common Files\AV\Spybot - Search and Destroy\Test.exe"
```

```
O4 - HKCU\..\Run: [Google Photos Backup]
"C:\Users\user\AppData\Local\Programs\Google\Google Photos Backup\Google
Photos Backup.exe" /autostart
O4 - HKCU\..\Run: [CCleaner Monitoring] "C:\Program
Files\CCleaner\CCleaner.exe" /MONITOR
O4 - HKUS\S-1-5-19\..\Run: [OneDriveSetup]
C:\Windows\System32\OneDriveSetup.exe /thfirstsetup (User 'LOCAL
SERVICE')
O4 - HKUS\S-1-5-20\..\Run: [OneDriveSetup]
C:\Windows\System32\OneDriveSetup.exe /thfirstsetup (User 'NETWORK
SERVICE')
O4 - Global Startup: Digital Line Detect.lnk = C:\Program Files\Digital
Line Detect\DLG.exe
O8 - Extra context menu item: E&xport to Microsoft Excel -
res://C:\Program Files\Microsoft Office\Office15\EXCEL.EXE/3000
O8 - Extra context menu item: E&xportovat do aplikace Microsoft Excel -
res://C:\Program Files\Microsoft Office\Office14\EXCEL.EXE/3000
O8 - Extra context menu item: Se&nd to OneNote - res://C:\Program
Files\Microsoft Office\Office15\ONBttnIE.dll/105
O9 - Extra button: Send to OneNote - {2670000A-7350-4f3c-8081-
5663EE0C6C49} - C:\Program Files\Microsoft Office\Office15\ONBttnIE.dll
O9 - Extra 'Tools' menuitem: Se&nd to OneNote - {2670000A-7350-4f3c-8081-
5663EE0C6C49} - C:\Program Files\Microsoft Office\Office15\ONBttnIE.dll
O9 - Extra button: @C:\Windows\WindowsMobile\INetRepl.dll,-222 -
{2EAF5BB1-070F-11D3-9307-00C04FAE2D4F} -
C:\Windows\WindowsMobile\INetRepl.dll
O9 - Extra button: (no name) - {2EAF5BB2-070F-11D3-9307-00C04FAE2D4F} -
C:\Windows\WindowsMobile\INetRepl.dll
O9 - Extra 'Tools' menuitem: @C:\Windows\WindowsMobile\INetRepl.dll,-223
- {2EAF5BB2-070F-11D3-9307-00C04FAE2D4F} -
C:\Windows\WindowsMobile\INetRepl.dll
O9 - Extra button: Lync Click to Call - {31D09BA0-12F5-4CCE-BE8A-
2923E76605DA} - C:\Program Files\Microsoft Office\Office15\OCHelper.dll
O9 - Extra 'Tools' menuitem: Lync Click to Call - {31D09BA0-12F5-4CCE-
BE8A-2923E76605DA} - C:\Program Files\Microsoft
Office\Office15\OCHelper.dll
O9 - Extra button: OneNote Lin&ked Notes - {789FE86F-6FC4-46A1-9849-
EDE0DB0C95CA} - C:\Program Files\Microsoft
Office\Office15\ONBttnIELinkedNotes.dll
O9 - Extra 'Tools' menuitem: OneNote Lin&ked Notes - {789FE86F-6FC4-46A1-
9849-EDE0DB0C95CA} - C:\Program Files\Microsoft
Office\Office15\ONBttnIELinkedNotes.dll
O11 - Options group: [ACCELERATED_GRAPHICS] Accelerated graphics
O18 - Protocol: osf - {D924BDC6-C83A-4BD5-90D0-095128A113D1} - C:\Program
Files\Microsoft Office\Office15\MSOSB.DLL
O18 - Protocol: tbauth - {14654CA6-5711-491D-B89A-58E571679951} -
C:\Windows\System32\tbauth.dll
O18 - Protocol: windows.tbauth - {14654CA6-5711-491D-B89A-58E571679951} -
C:\Windows\System32\tbauth.dll
O18 - Filter hijack: text/xml - {807583E5-5146-11D5-A672-00B0D022E945} -
C:\Program Files\Common Files\Microsoft Shared\OFFICE15\MSOXMLMF.DLL
O20 - Winlogon Notify: SDWinLogon - SDWinLogon.dll (file missing)
O23 - Service: Adobe Flash Player Update Service
(AdobeFlashPlayerUpdateSvc) - Adobe Systems Incorporated -
C:\Windows\system32\Macromed\Flash\FlashPlayerUpdateService.exe
O23 - Service: Avast Antivirus (avast! Antivirus) - AVAST Software -
C:\Program Files\AVAST Software\Avast\AvastSvc.exe
```

```
O23 - Service: AvastVBox COM Service (AvastVBoxSvc) - Avast Software -
C:\Program Files\AVAST Software\Avast\ng\vbox\AvastVBoxSVC.exe
O23 - Service: Služba Google Update (gupdate) (gupdate) - Google Inc. -
C:\Program Files\Google\Update\GoogleUpdate.exe
O23 - Service: Služba Google Update (gupdatem) (gupdatem) - Google Inc. -
C:\Program Files\Google\Update\GoogleUpdate.exe
O23 - Service: @oem8.inf,%ibm.svcDesc0%;Lenovo PM Service (IBMPMSVC) -
Lenovo. - C:\WINDOWS\system32\ibmpmsvc.exe
O23 - Service: System Interface Foundation Service (ImControllerService)
- Lenovo Group Limited - C:\Program
Files\Lenovo\ImController\Service\Lenovo.Modern.ImController.exe
O23 - Service: Spybot-S&D 2 Scanner Service (SDScannerService) - Safer-
Networking Ltd. - C:\Program Files\Spybot - Search & Destroy
2\SDFSSvc.exe
O23 - Service: Spybot-S&D 2 Updating Service (SDUpdateService) - Safer-
Networking Ltd. - C:\Program Files\Spybot - Search & Destroy
2\SDUpdSvc.exe
O23 - Service: Spybot-S&D 2 Security Center Service (SDWSCService) -
Safer-Networking Ltd. - C:\Program Files\Spybot - Search & Destroy
2\SDWSCSvc.exe
O23 - Service: SynTPEnh Caller Service (SynTPEnhService) - Synaptics
Incorporated - C:\Program Files\Synaptics\SynTP\SynTPEnhService.exe
O23 - Service: AVG PC TuneUp Service (TuneUp.UtilitiesSvc) - AVG
Technologies - C:\Program Files\AVG PC
TuneUp\TuneUpUtilitiesService32.exe

--
End of file - 9695 bytes

======Scheduled tasks folder======

C:\WINDOWS\tasks\Adobe Flash Player Updater.job -
C:\Windows\system32\Macromed\Flash\FlashPlayerUpdateService.exe
C:\WINDOWS\tasks\GoogleUpdateTaskMachineCore.job - C:\Program
Files\Google\Update\GoogleUpdate.exe  /c
C:\WINDOWS\tasks\GoogleUpdateTaskMachineUA.job - C:\Program
Files\Google\Update\GoogleUpdate.exe  /ua /installsource scheduler
C:\WINDOWS\tasks\GoogleUpdateTaskUserS-1-5-21-506022658-3350514639-
206302717-1000Core.job -
C:\Users\user\AppData\Local\Google\Update\GoogleUpdate.exe  /c
C:\WINDOWS\tasks\GoogleUpdateTaskUserS-1-5-21-506022658-3350514639-
206302717-1000UA.job -
C:\Users\user\AppData\Local\Google\Update\GoogleUpdate.exe  /ua
/installsource scheduler

======Registry dump======

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Br
owser Helper Objects\{31D09BA0-12F5-4CCE-BE8A-2923E76605DA}]
Lync Browser Helper - C:\Program Files\Microsoft
Office\Office15\OCHelper.dll [2012-10-01 139368]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Br
owser Helper Objects\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}]
Java(tm) Plug-In SSV Helper - C:\Program
Files\Java\jre1.8.0_73\bin\ssv.dll [2016-02-07 460384]
```

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Br
owser Helper Objects\{8E5E2654-AD2D-48bf-AC2D-D17F00898D06}]
avast! Online Security - C:\Program Files\AVAST
Software\Avast\aswWebRepIE.dll [2015-08-14 559624]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Br
owser Helper Objects\{B4F3A835-0E21-4959-BA22-42B3008E02FF}]
Office Document Cache Handler -
C:\PROGRA~1\MICROS~1\Office15\URLREDIR.DLL [2012-10-01 704664]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Br
owser Helper Objects\{D0498E0A-45B7-42AE-A9AA-ABA463DBD3BF}]
Microsoft SkyDrive Pro Browser Helper -
C:\PROGRA~1\MICROS~1\Office15\GROOVEEX.DLL [2012-10-01 1720976]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Br
owser Helper Objects\{DBC80044-A445-435b-BC74-9C25C1C588A9}]
Java(tm) Plug-In 2 SSV Helper - C:\Program
Files\Java\jre1.8.0_73\bin\jp2ssv.dll [2016-02-07 172640]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
"IgfxTray"=C:\WINDOWS\system32\igfxtray.exe [2012-11-27 143392]
"HotKeysCmds"=C:\WINDOWS\system32\hkcmd.exe [2012-11-27 178208]
"Persistence"=C:\WINDOWS\system32\igfxpers.exe [2012-11-27 178720]
"AvastUI.exe"=C:\Program Files\AVAST Software\Avast\AvastUI.exe [2015-11-
09 6111312]
"SynLenovoHelper"=C:\Program Files\Synaptics\SynTP\SynLenovoHelper.exe
[2015-09-20 126120]
"SDTray"=C:\Program Files\Spybot - Search & Destroy 2\SDTray.exe [2015-
06-16 4127488]
"SynTPEnh"=C:\Program Files\Synaptics\SynTP\SynTPEnh.exe [2015-09-20
3519656]
"SunJavaUpdateSched"=C:\Program Files\Common Files\Java\Java
Update\jusched.exe [2016-01-29 594992]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"OneDrive"=C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe
[2016-03-11 551104]
"SpybotPostWindows10UpgradeReInstall"=C:\Program Files\Common
Files\AV\Spybot - Search and Destroy\Test.exe [2015-07-28 1011200]
"Google Photos Backup"=C:\Users\user\AppData\Local\Programs\Google\Google
Photos Backup\Google Photos Backup.exe [2015-12-11 3791176]
"CCleaner Monitoring"=C:\Program Files\CCleaner\CCleaner.exe [2016-03-11
6667992]

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Digital Line Detect.lnk - C:\Program Files\Digital Line Detect\DLG.exe

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\Notify\igfxcui]
C:\WINDOWS\system32\igfxdev.dll [2012-11-27 293888]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\Notify\SDWinLogon]
SDWinLogon.dll []

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\Ahc
ache.sys]

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\CoreMessagingRegistrar]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\iai2c.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\iaioi2c.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\SpbCx.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\StateRepository]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\TileDataModelSvc]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\uefi.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\UserManager]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{F2E7DD72-6468-4E36-B6F1-6488F42C1B52}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\Ahcache.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\CoreMessagingRegistrar]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\SpbCx.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\StateRepository]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\TileDataModelSvc]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\uefi.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\UserManager]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{F2E7DD72-6468-4E36-B6F1-6488F42C1B52}]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"DSCAutomationHostEnabled"=2
"SoftwareSASGeneration"=1
"ConsentPromptBehaviorAdmin"=0
"PromptOnSecureDesktop"=0
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\exp
lorer]
"NoDriveTypeAutoRun"=145

[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\sharedaccess\parame
ters\firewallpolicy\standardprofile\authorizedapplications\list]
"C:\Program Files\Spybot - Search & Destroy 2\SDTray.exe"="C:\Program
Files\Spybot - Search & Destroy 2\SDTray.exe:*:Enabled:Spybot - Search &
Destroy tray access"
"C:\Program Files\Spybot - Search & Destroy 2\SDFSSvc.exe"="C:\Program
Files\Spybot - Search & Destroy 2\SDFSSvc.exe:*:Enabled:Spybot-S&D 2
Scanner Service"
"C:\Program Files\Spybot - Search & Destroy 2\SDUpdate.exe"="C:\Program
Files\Spybot - Search & Destroy 2\SDUpdate.exe:*:Enabled:Spybot-S&D 2
Updater"
"C:\Program Files\Spybot - Search & Destroy 2\SDUpdSvc.exe"="C:\Program
Files\Spybot - Search & Destroy 2\SDUpdSvc.exe:*:Enabled:Spybot-S&D 2
Background update service"

[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\sharedaccess\parame
ters\firewallpolicy\domainprofile\authorizedapplications\list]


[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\AcroRd32.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\DATABASECOMPARE.EXE]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\effectextractor.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\excel.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\groove.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\infopath.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\lync.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\misc.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\msaccess.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\msoev.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\msotd.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\msoxmled.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\mspub.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\OcPubMgr.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\onenote.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\outlook.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\pdr13.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\powerpnt.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\powersuitestart.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\privacyiconclient.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\shareit.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\SPREADSHEETCOMPARE.EXE]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image
File Execution Options\Winword.exe]
"Debugger=""C:\Program Files\AVG PC TuneUp\TUAutoReactivator32.exe"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Drivers32]
"midimapper"=midimap.dll
"msacm.imaadpcm"=imaadp32.acm
"msacm.l3acm"=C:\Windows\System32\l3codeca.acm
"msacm.msadpcm"=msadp32.acm
"msacm.msg711"=msg711.acm
"msacm.msgsm610"=msgsm32.acm
"vidc.cvid"=iccvid.dll
"vidc.i420"=iyuv_32.dll
"vidc.iyuv"=iyuv_32.dll
"vidc.mrle"=msrle32.dll
"vidc.msvc"=msvidc32.dll
"vidc.uyvy"=msyuv.dll
"vidc.yuy2"=msyuv.dll
"vidc.yvu9"=tsbyuv.dll
"vidc.yvyu"=msyuv.dll
"wavemapper"=msacm32.drv
"wave"=wdmaud.drv
"midi"=wdmaud.drv
"mixer"=wdmaud.drv
```

```
"aux"=wdmaud.drv
"wave1"=wdmaud.drv
"midi1"=wdmaud.drv
"mixer1"=wdmaud.drv
"aux1"=wdmaud.drv
"MSVideo8"=VfWWDM32.dll
"msacm.ac3filter"=ac3filter.acm

======File associations======

.js - edit - C:\Windows\System32\Notepad.exe %1
.js - open - C:\Windows\System32\WScript.exe "%1" %*

======List of files/folders created in the last 1 month======

2016-04-10 17:07:42 ----D---- C:\rsit
2016-04-10 17:07:42 ----D---- C:\Program Files\trend micro
2016-04-10 17:05:12 ----D---- C:\Program Files\CCleaner
2016-04-09 09:47:42 ----HD---- C:\OneDriveTemp
2016-04-09 09:36:11 ----A---- C:\WINDOWS\system32\WudfUpdate_01011.dll
2016-04-09 02:31:12 ----D---- C:\Users\user\AppData\Roaming\FreeVPN
2016-04-09 02:30:28 ----D---- C:\Users\user\AppData\Roaming\SPI

======List of files/folders modified in the last 1 month======

2016-04-10 17:07:42 ----RD---- C:\Program Files
2016-04-10 17:06:36 ----D---- C:\WINDOWS\Prefetch
2016-04-10 17:05:16 ----D---- C:\WINDOWS\system32\Tasks
2016-04-10 17:00:26 ----D---- C:\WINDOWS\Temp
2016-04-10 17:00:05 ----D---- C:\Users\user\AppData\Roaming\uTorrent
2016-04-10 16:59:58 ----D---- C:\WINDOWS\system32\sru
2016-04-10 12:44:36 ----D---- C:\WINDOWS\system32\config
2016-04-10 12:44:05 ----D---- C:\WINDOWS\Microsoft.NET
2016-04-10 10:38:06 ----D---- C:\WINDOWS\AppReadiness
2016-04-09 14:41:08 ----AD---- C:\WINDOWS\System32
2016-04-09 14:41:08 ----A---- C:\WINDOWS\system32\PerfStringBackup.INI
2016-04-09 14:41:07 ----D---- C:\WINDOWS\INF
2016-04-09 09:36:37 ----SHD---- C:\WINDOWS\Installer
2016-04-09 09:36:31 ----D---- C:\WINDOWS\system32\drivers\UMDF
2016-04-09 09:36:30 ----D---- C:\WINDOWS\system32\DriverStore
2016-04-09 09:36:11 ----A---- C:\WINDOWS\system32\iMDriverHelper.dll
2016-04-09 09:35:35 ----D---- C:\ProgramData\Package Cache
2016-04-09 04:54:18 ----SHD---- C:\System Volume Information
2016-04-09 03:14:51 ----HD---- C:\Program Files\WindowsApps
2016-04-09 03:03:54 ----AD---- C:\KMPlayer
2016-04-09 02:38:51 ----D---- C:\WINDOWS\Tasks
2016-04-09 02:31:03 ----HD---- C:\ProgramData
2016-04-09 02:30:33 ----D---- C:\WINDOWS\system32\GroupPolicy
2016-04-09 02:16:10 ----D---- C:\WINDOWS\WinSxS
2016-03-23 19:51:22 ----D---- C:\WINDOWS\CbsTemp
2016-03-23 19:51:09 ----D---- C:\WINDOWS\system32\catroot2
2016-03-13 22:37:08 ----D---- C:\Windows
2016-03-13 18:57:25 ----A---- C:\WINDOWS\system32\log.txt
2016-03-13 18:18:36 ----D---- C:\WINDOWS\system32\drivers
2016-03-13 18:18:16 ----D---- C:\ProgramData\tmp
2016-03-12 22:44:20 ----RSD---- C:\WINDOWS\Fonts
2016-03-12 22:44:20 ----D---- C:\ProgramData\simplitec
2016-03-12 17:19:58 ----RSD---- C:\WINDOWS\assembly
```

```
2016-03-12 03:30:50 ----D---- C:\WINDOWS\system32\migration
2016-03-12 03:30:49 ----D---- C:\WINDOWS\apppatch
2016-03-12 03:30:49 ----D---- C:\Program Files\Windows Portable Devices
2016-03-12 03:30:49 ----D---- C:\Program Files\Windows Multimedia
Platform
2016-03-12 03:30:49 ----D---- C:\Program Files\Windows Media Player
2016-03-12 03:30:49 ----D---- C:\Program Files\Internet Explorer

======List of drivers (R=Running, S=Stopped, 0=Boot, 1=System, 2=Auto,
3=Demand, 4=Disabled)======

R0 aswRvrt;avast! Revert; C:\WINDOWS\system32\drivers\aswRvrt.sys [2015-
08-14 49776]
R0 aswVmm;avast! VM Monitor; C:\WINDOWS\system32\drivers\aswVmm.sys
[2015-08-14 208664]
R0 ngvss;ngvss; C:\WINDOWS\system32\drivers\ngvss.sys [2015-08-14 95112]
R1 aswRdr;aswRdr; C:\WINDOWS\system32\drivers\aswRdr2.sys [2015-08-14
81728]
R1 aswSnx;aswSnx; C:\WINDOWS\system32\drivers\aswSnx.sys [2015-11-09
794952]
R1 aswSP;aswSP; C:\WINDOWS\system32\drivers\aswSP.sys [2015-11-09 435464]
R1 ElbyCDIO;ElbyCDIO Driver; C:\WINDOWS\System32\Drivers\ElbyCDIO.sys
[2013-03-04 30616]
R1 FileCrypt;@%systemroot%\system32\drivers\filecrypt.sys,-100;
C:\WINDOWS\system32\drivers\filecrypt.sys [2015-10-30 76288]
R1 GpuEnergyDrv;@%SystemRoot%\system32\drivers\gpuenergydrv.sys,-100;
C:\WINDOWS\System32\drivers\gpuenergydrv.sys [2015-10-30 7680]
R2 aswHwid;avast! HardwareID; C:\WINDOWS\system32\drivers\aswHwid.sys
[2015-08-14 24016]
R2 aswMonFlt;aswMonFlt; C:\WINDOWS\system32\drivers\aswMonFlt.sys [2015-
08-14 76000]
R2 aswStm;aswStm; C:\WINDOWS\system32\drivers\aswStm.sys [2015-08-14
113592]
R2 giveio;giveio; C:\WINDOWS\system32\giveio.sys [1996-04-03 5248]
R2 mdmxsdk;mdmxsdk; C:\WINDOWS\system32\DRIVERS\mdmxsdk.sys [2010-05-11
19384]
R2 MMCSS;@%systemroot%\system32\drivers\mmcss.sys,-100;
C:\WINDOWS\system32\drivers\mmcss.sys [2015-10-30 36864]
R2 speedfan;speedfan; \??\C:\WINDOWS\system32\speedfan.sys [2012-12-29
24184]
R2 storqosflt;@%SystemRoot%\System32\drivers\storqosflt.sys,-101;
C:\WINDOWS\system32\drivers\storqosflt.sys [2015-10-30 62464]
R3 5U877;@oem3.inf,%USBVideo.SvcDesc%;USB Video Device;
C:\WINDOWS\system32\DRIVERS\5U877.sys [2011-05-24 132864]
R3
CnxtHdAudService;@oem45.inf,%UAAFunctionDriverForHdAudio.SvcDesc%;Conexan
t UAA Function Driver for High Definition Audio Service;
C:\WINDOWS\system32\drivers\CHDRT32.sys [2016-01-23 486016]
R3 e1kexpress;@oem15.inf,%e1kExpress.Service.DispName%;Intel(R) PRO/1000
PCI Express Network Connection Driver K;
C:\WINDOWS\system32\DRIVERS\e1k6232.sys [2011-07-20 268968]
R3 HECI;@oem37.inf,%HECI_SvcDesc%;Intel(R) Management Engine Interface;
C:\WINDOWS\System32\drivers\HECI.sys [2009-09-17 41088]
R3 HSF_DPV;HSF_DPV; C:\WINDOWS\system32\DRIVERS\HSX_DPV.sys [2010-12-18
988800]
R3 HSXHWAZL;HSXHWAZL; C:\WINDOWS\system32\DRIVERS\HSXHWAZL.sys [2010-12-
18 214144]
```

R3 IBMPMDRV;IBMPMDRV; C:\WINDOWS\system32\DRIVERS\ibmpmdrv.sys [2015-06-26 59216]
R3 igfx;igfx; C:\WINDOWS\system32\DRIVERS\igdkmd32.sys [2012-11-27 10860032]
R3 Impcd;Impcd; C:\WINDOWS\System32\drivers\Impcd.sys [2010-02-27 132480]
R3 IntcDAud;@oem33.inf,%IntcDAud.SvcDesc%;Intel(R) Display Audio; C:\WINDOWS\system32\DRIVERS\IntcDAud.sys [2011-08-23 270336]
R3 MQAC;@mqutil.dll,-6101; C:\WINDOWS\system32\drivers\mqac.sys [2016-01-24 130560]
R3 NETwNs32;___ Intel(R) Wireless WiFi Link 5000 Series Adapter Driver for Windows 7 - 32 Bit; C:\WINDOWS\System32\drivers\Netwsn00.sys [2015-10-30 10372096]
R3 SmbDrvI;SmbDrvI; C:\WINDOWS\system32\DRIVERS\Smb_driver_Intel.sys [2015-09-20 26792]
R3 SynTP;@oem40.inf,%SynTP.SvcDesc%;Synaptics TouchPad Driver; C:\WINDOWS\system32\DRIVERS\SynTP.sys [2015-09-20 456872]
R3 tap0901;@oem41.inf,%DeviceDescription%;TAP-Windows Adapter V9; C:\WINDOWS\System32\drivers\tap0901.sys [2013-08-22 35288]
R3 tapoas;@oem0.inf,%DeviceDescription%;TAP-Win32 Adapter OAS; C:\WINDOWS\System32\drivers\tapoas.sys [2012-07-15 26112]
S0 LSI_SAS2i;LSI_SAS2i; C:\WINDOWS\System32\drivers\lsi_sas2i.sys [2015-10-30 88928]
S0 LSI_SAS3i;LSI_SAS3i; C:\WINDOWS\System32\drivers\lsi_sas3i.sys [2015-10-30 83288]
S0 percsas2i;percsas2i; C:\WINDOWS\System32\drivers\percsas2i.sys [2015-10-30 51040]
S0 percsas3i;percsas3i; C:\WINDOWS\System32\drivers\percsas3i.sys [2015-10-30 51552]
S0 storufs;@storufs.inf,%UfsServiceDesc%;Microsoft Universal Flash Storage (UFS) Driver; C:\WINDOWS\System32\drivers\storufs.sys [2015-10-30 27992]
S3 bcmfn;@bcmfn.inf,%bcmfn.SVCDESC%;bcmfn Service; C:\WINDOWS\System32\drivers\bcmfn.sys [2015-10-30 8192]
S3 BtHidBus;Bluetooth HID Bus Service; C:\WINDOWS\System32\Drivers\BtHidBus.sys [2008-08-01 20616]
S3 btnetBUs;Bluetooth PAN Bus Service; C:\WINDOWS\System32\Drivers\btnetBus.sys [2008-12-07 30088]
S3 buttonconverter;@buttonconverter.inf,%btnconv.SvcDesc%;Service for Portable Device Control devices; C:\WINDOWS\System32\drivers\buttonconverter.sys [2015-10-30 26624]
S3 CapImg;@capimg.inf,%CapImgHid_Service%;HID driver for CapImg touch screen; C:\WINDOWS\System32\drivers\capimg.sys [2016-01-24 96768]
S3 genericusbfn;@genericusbfn.inf,%genericusbfn.ServiceName%;Generic USB Function Class; C:\WINDOWS\System32\drivers\genericusbfn.sys [2015-10-30 17408]
S3 GPIO;@iaiogpio.inf,%GPIO.SVCDESC%;Intel SoC GPIO Controller Driver; C:\WINDOWS\System32\drivers\iaiogpio.sys [2015-10-30 22016]
S3 hidinterrupt;@hidinterrupt.inf,%HID_Interrupt.SvcDesc%;Common Driver for HID Buttons implemented with interrupts; C:\WINDOWS\System32\drivers\hidinterrupt.sys [2015-10-30 38240]
S3 iai2c;@iai2c.inf,%iai2c.SVCDESC%;Intel(R) Serial IO I2C Host Controller; C:\WINDOWS\System32\drivers\iai2c.sys [2015-10-30 66048]
S3 iaioi2c;@iaioi2c.inf,%Driver_Service.Desc%;Intel(R) Atom(TM) Processor I2C Controller Service; C:\WINDOWS\System32\drivers\iaioi2c.sys [2015-10-30 61936]
S3 IoQos;@%SystemRoot%\system32\drivers\ioqos.sys,-100; C:\WINDOWS\system32\drivers\ioqos.sys [2015-10-30 23040]

```
S3 IvtBtBUs;IVT Bluetooth Bus Service;
C:\WINDOWS\System32\Drivers\IvtBtBus.sys [2008-07-02 26248]
S3 LeadCore_57XX_AutoEjecDiskDrv;LeadCore_57XX Auto-Eject Disk Monitor
Filter Driver; C:\WINDOWS\system32\drivers\LeadCore_57XX_AutoEjectCD.sys
[2010-04-03 14848]
S3 PSI;PSI; C:\WINDOWS\system32\DRIVERS\psi_mf_x86.sys [2016-02-02 16024]

======List of services (R=Running, S=Stopped, 0=Boot, 1=System, 2=Auto,
3=Demand, 4=Disabled)======

R2 AppHostSvc;@%windir%\system32\inetsrv\iisres.dll,-30011;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
R2 avast! Antivirus;Avast Antivirus; C:\Program Files\AVAST
Software\Avast\AvastSvc.exe [2015-08-14 146600]
R2 CoreMessagingRegistrar;@%SystemRoot%\system32\coremessaging.dll,-1;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
R2 DiagTrack;@%SystemRoot%\system32\diagtrack.dll,-3001;
C:\WINDOWS\System32\svchost.exe [2015-10-30 37256]
R2 HsfXAudioService;@oem14.inf,%XAudio2.SVCDESC%;HsfXAudioService;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
R2 IBMPMSVC;@oem8.inf,%ibm.svcDesc0%;Lenovo PM Service;
C:\WINDOWS\system32\ibmpmsvc.exe [2015-06-26 113904]
R2 ImControllerService;System Interface Foundation Service; C:\Program
Files\Lenovo\ImController\Service\Lenovo.Modern.ImController.exe [2016-
01-29 36808]
R2 MSMQ;@mqutil.dll,-6102; C:\WINDOWS\system32\mqsvc.exe [2016-01-24
25088]
R2
NetMsmqActivator;@%systemroot%\Microsoft.NET\Framework\v4.0.30319\Service
ModelInstallRC.dll,-8195;
C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\SMSvcHost.exe [2015-10-30
135848]
R2
NetPipeActivator;@%systemroot%\Microsoft.NET\Framework\v4.0.30319\Service
ModelInstallRC.dll,-8197;
C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\SMSvcHost.exe [2015-10-30
135848]
R2 OneSyncSvc_4bb53;Sync Host_4bb53; C:\WINDOWS\system32\svchost.exe
[2015-10-30 37256]
R2 SDScannerService;Spybot-S&D 2 Scanner Service; C:\Program Files\Spybot
- Search & Destroy 2\SDFSSvc.exe [2015-06-16 1750712]
R2 SDUpdateService;Spybot-S&D 2 Updating Service; C:\Program Files\Spybot
- Search & Destroy 2\SDUpdSvc.exe [2015-06-16 2102496]
R2 SDWSCService;Spybot-S&D 2 Security Center Service; C:\Program
Files\Spybot - Search & Destroy 2\SDWSCSvc.exe [2015-07-24 224712]
R2 SynTPEnhService;SynTPEnh Caller Service; C:\Program
Files\Synaptics\SynTP\SynTPEnhService.exe [2015-09-20 208552]
R2 tiledatamodelsvc;@%SystemRoot%\system32\tileobjserver.dll,-1;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
R3 DsSvc;@%SystemRoot%\system32\dssvc.dll,-10003;
C:\WINDOWS\System32\svchost.exe [2015-10-30 37256]
R3 LicenseManager;@%SystemRoot%\system32\licensemanagersvc.dll,-200;
C:\WINDOWS\System32\svchost.exe [2015-10-30 37256]
R3 PimIndexMaintenanceSvc_4bb53;Contact Data_4bb53;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
R3 SensorService;@%SystemRoot%\System32\sensorservice.dll,-1000;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
```

```
R3 StateRepository;@%SystemRoot%\system32\windows.staterepository.dll,-1;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S2 DoSvc;@%systemroot%\system32\dosvc.dll,-100;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S2 gupdate;Služba Google Update (gupdate); C:\Program
Files\Google\Update\GoogleUpdate.exe [2015-08-31 144200]
S2 MapsBroker;@%SystemRoot%\System32\moshost.dll,-100;
C:\WINDOWS\System32\svchost.exe [2015-10-30 37256]
S2
NetTcpActivator;@%systemroot%\Microsoft.NET\Framework\v4.0.30319\ServiceM
odelInstallRC.dll,-8199;
C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\SMSvcHost.exe [2015-10-30
135848]
S2 OneSyncSvc;@%SystemRoot%\system32\APHostRes.dll,-10002;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S2 OneSyncSvc_178a89;Sync Host_178a89; C:\WINDOWS\system32\svchost.exe
[2015-10-30 37256]
S2 OneSyncSvc_252b2385;Sync Host_252b2385;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S2 OneSyncSvc_47dac;Sync Host_47dac; C:\WINDOWS\system32\svchost.exe
[2015-10-30 37256]
S2 OneSyncSvc_52cb3;Sync Host_52cb3; C:\WINDOWS\system32\svchost.exe
[2015-10-30 37256]
S2 OneSyncSvc_533d0;Sync Host_533d0; C:\WINDOWS\system32\svchost.exe
[2015-10-30 37256]
S2 OneSyncSvc_73f26;Sync Host_73f26; C:\WINDOWS\system32\svchost.exe
[2015-10-30 37256]
S2 OneSyncSvc_8e81e;Sync Host_8e81e; C:\WINDOWS\system32\svchost.exe
[2015-10-30 37256]
S3 AdobeFlashPlayerUpdateSvc;Adobe Flash Player Update Service;
C:\Windows\system32\Macromed\Flash\FlashPlayerUpdateService.exe [2015-08-
19 269000]
S3 AJRouter;@%SystemRoot%\system32\AJRouter.dll,-2;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 AvastVBoxSvc;AvastVBox COM Service; C:\Program Files\AVAST
Software\Avast\ng\vbox\AvastVBoxSVC.exe [2015-08-14 3218624]
S3 BthHFSrv;@%SystemRoot%\System32\BthHFSrv.dll,-103;
C:\WINDOWS\System32\svchost.exe [2015-10-30 37256]
S3 ClipSVC;@%SystemRoot%\system32\ClipSVC.dll,-103;
C:\WINDOWS\System32\svchost.exe [2015-10-30 37256]
S3 DcpSvc;@%SystemRoot%\system32\dcpsvc.dll,-3001;
C:\WINDOWS\System32\svchost.exe [2015-10-30 37256]
S3 DevQueryBroker;@%SystemRoot%\system32\DevQueryBroker.dll,-100;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3
diagnosticshub.standardcollector.service;@%SystemRoot%\system32\DiagSvcs\
DiagnosticsHub.StandardCollector.ServiceRes.dll,-1000;
C:\WINDOWS\system32\DiagSvcs\DiagnosticsHub.StandardCollector.Service.exe
[2015-10-30 26112]
S3
DmEnrollmentSvc;@%systemroot%\system32\Windows.Internal.Management.dll,-
100; C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 dmwappushservice;@%SystemRoot%\system32\dmwappushsvc.dll,-200;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 embeddedmode;@%SystemRoot%\system32\embeddedmodesvc.dll,-200;
C:\WINDOWS\System32\svchost.exe [2015-10-30 37256]
S3 EntAppSvc;@EnterpriseAppMgmtSvc.dll,-1;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
```

S3 FontCache3.0.0.0;@%SystemRoot%\system32\PresentationHost.exe,-3309;
C:\WINDOWS\Microsoft.Net\Framework\v3.0\WPF\PresentationFontCache.exe
[2015-10-24 43696]
S3 gupdatem;Služba Google Update (gupdatem); C:\Program
Files\Google\Update\GoogleUpdate.exe [2015-08-31 144200]
S3 icssvc;@%SystemRoot%\System32\tetheringservice.dll,-4097;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 MessagingService;@%SystemRoot%\system32\MessagingService.dll,-100;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 MessagingService_178a89;MessagingService_178a89;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 MessagingService_252b2385;MessagingService_252b2385;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 MessagingService_47dac;MessagingService_47dac;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 MessagingService_4bb53;MessagingService_4bb53;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 MessagingService_52cb3;MessagingService_52cb3;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 MessagingService_533d0;MessagingService_533d0;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 MessagingService_73f26;MessagingService_73f26;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 MessagingService_8e81e;MessagingService_8e81e;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 NetSetupSvc;@%SystemRoot%\system32\NetSetupSvc.dll,-3;
C:\WINDOWS\System32\svchost.exe [2015-10-30 37256]
S3 NgcCtnrSvc;@%SystemRoot%\System32\NgcCtnrSvc.dll,-1;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 NgcSvc;@%SystemRoot%\System32\ngcsvc.dll,-100;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 ose;Office Source Engine; C:\Program Files\Common Files\Microsoft
Shared\Source Engine\OSE.EXE [2012-10-01 150648]
S3 PhoneSvc;@%SystemRoot%\system32\PhoneserviceRes.dll,-10000;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 PimIndexMaintenanceSvc;@%SystemRoot%\system32\UserDataAccessRes.dll,-
15001; C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 PimIndexMaintenanceSvc_178a89;Contact Data_178a89;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 PimIndexMaintenanceSvc_252b2385;Contact Data_252b2385;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 PimIndexMaintenanceSvc_47dac;Contact Data_47dac;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 PimIndexMaintenanceSvc_52cb3;Contact Data_52cb3;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 PimIndexMaintenanceSvc_533d0;Contact Data_533d0;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 PimIndexMaintenanceSvc_73f26;Contact Data_73f26;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 PimIndexMaintenanceSvc_8e81e;Contact Data_8e81e;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S3 RetailDemo;@%SystemRoot%\System32\RDXService.dll,-256;
C:\WINDOWS\System32\svchost.exe [2015-10-30 37256]
S3 SensorDataService;@%SystemRoot%\system32\SensorDataService.exe,-101;
C:\WINDOWS\System32\SensorDataService.exe [2015-10-30 900096]
S3 SmsRouter;@%SystemRoot%\System32\SmsRouterSvc.dll,-10001;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]

```
S3 TieringEngineService;@%SystemRoot%\system32\TieringEngineService.exe,-
702; C:\WINDOWS\system32\TieringEngineService.exe [2015-10-30 256512]
S4 AdobeARMservice;Adobe Acrobat Update Service; C:\Program Files\Common
Files\Adobe\ARM\1.0\armsvc.exe [2015-12-14 82128]
S4
aspnet_state;@%SystemRoot%\Microsoft.NET\Framework\v4.0.30319\aspnet_rc.d
ll,-1; C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\aspnet_state.exe
[2015-10-30 45752]
S4 CDPSvc;@%SystemRoot%\system32\cdpsvc.dll,-100;
C:\WINDOWS\system32\svchost.exe [2015-10-30 37256]
S4 LMS;Intel(R) Management and Security Application Local Management
Service; C:\Program Files\Intel\Intel(R) Management Engine
Components\LMS\LMS.exe [2010-05-03 325656]
S4 LSCWinService;LSCWinService; C:\Program Files\Lenovo\Lenovo Solution
Center\App\LSCWinService.exe [2015-09-29 271328]
S4 osppsvc;Office Software Protection Platform; C:\Program Files\Common
Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE
[2010-01-10 4640000]
S4 RichVideo;Cyberlink RichVideo Service(CRVS); C:\Program
Files\CyberLink\Shared files\RichVideo.exe [2014-10-03 253776]
S4 ShareItSvc;ShareItSvc; C:\Program
Files\Lenovo\SHAREit\Shareit.Service.exe [2016-01-20 31176]

-----------------EOF-----------------
```