Logfile of random's system information tool 1.09 (written by random/random)
Run by Lusinka at 2013-08-01 10:43:58
Microsoft Windows 8
System drive C: has 197 GB (77%) free of 257 GB
Total RAM: 1606 MB (60% free)

Logfile of Trend Micro HijackThis v2.0.4
Scan saved at 10:44:09, on 1. 8. 2013
Platform: Unknown Windows (WinNT 6.02.1008)
MSIE: Internet Explorer v10.0 (10.00.9200.16537)
Boot mode: Normal

Running processes:
C:\Program Files (x86)\Lenovo\YouCam\YCMMirage.exe
C:\Users\Lusinka\AppData\Local\Google\Update\GoogleUpdate.exe
C:\Program Files (x86)\USB Camera\VM331STI.EXE
C:\Program Files (x86)\Lenovo\YouCam\YouCamTray.exe
C:\Program Files (x86)\Lenovo\PowerDVD10\PDVD10Serv.exe
C:\Program Files\trend micro\Lusinka.exe

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Default_Page_URL =
http://lenovo13.msn.com
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page =
http://go.microsoft.com/fwlink/?LinkId=54896
R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page =
http://lenovo13.msn.com
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 Page =
http://go.microsoft.com/fwlink/?LinkId=54896
R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Start Page =
http://go.microsoft.com/fwlink/p/?LinkId=255141
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant =
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =
R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Local Page =
C:\Windows\SysWOW64\blank.htm
R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName =
F2 - REG:system.ini: UserInit=userinit.exe
O4 - HKLM\..\Run: [331BigDog] C:\Program Files (x86)\USB Camera\VM331STI.EXE
O4 - HKLM\..\Run: [Dolby Advanced Audio v2] "C:\Program Files (x86)\Dolby
Advanced Audio v2\pcee4.exe" -autostart
O4 - HKLM\..\Run: [YouCam Mirage] "C:\Program Files
(x86)\Lenovo\YouCam\YCMMirage.exe"
O4 - HKLM\..\Run: [YouCam Tray] "C:\Program Files
(x86)\Lenovo\YouCam\YouCamTray.exe" /s
O4 - HKLM\..\Run: [UpdateP2GShortCut] "C:\Program Files
(x86)\Lenovo\Power2Go\MUITransfer\MUIStartMenu.exe" "C:\Program Files
(x86)\Lenovo\Power2Go" UpdateWithCreateOnce "SOFTWARE\CyberLink\Power2Go\5.0"
O4 - HKLM\..\Run: [RemoteControl10] "C:\Program Files
(x86)\Lenovo\PowerDVD10\PDVD10Serv.exe"
O4 - HKLM\..\Run: [Intel AppUp(SM) center] "C:\Program Files
(x86)\Intel\IntelAppStore\bin\ismagent.exe" --domain-id
F0399437-FD0C-4A48-B101-F0314A6172E4
O4 - HKCU\..\Run: [Google Update]
"C:\Users\Lusinka\AppData\Local\Google\Update\GoogleUpdate.exe" /c
O11 - Options group: [ACCELERATED_GRAPHICS] Accelerated graphics
O23 - Service: @%SystemRoot%\system32\Alg.exe,-112 (ALG) - Unknown owner -
C:\windows\System32\alg.exe (file missing)
O23 - Service: AMD External Events Utility - Unknown owner -
C:\windows\system32\atiesrxx.exe (file missing)
O23 - Service: AMD FUEL Service - Advanced Micro Devices, Inc. - C:\Program
Files\ATI Technologies\ATI.ACE\Fuel\Fuel.Service.exe
O23 - Service: AtherosSvc - Qualcomm Atheros Commnucations - C:\Program Files
(x86)\Bluetooth Suite\adminservice.exe
O23 - Service: @C:\windows\system32\CxAudMsg64.exe,-100 (CxAudMsg) - Unknown
owner - C:\windows\system32\CxAudMsg64.exe (file missing)

```
O23 - Service: @%SystemRoot%\system32\efssvc.dll,-100 (EFS) - Unknown owner -
C:\windows\System32\lsass.exe (file missing)
O23 - Service: Elan Service (ETDService) - ELAN Microelectronics Corp. -
C:\Program Files\Elantech\ETDService.exe
O23 - Service: @%systemroot%\system32\fxsresm.dll,-118 (Fax) - Unknown owner -
C:\windows\system32\fxssvc.exe (file missing)
O23 - Service: @keyiso.dll,-100 (KeyIso) - Unknown owner -
C:\windows\system32\lsass.exe (file missing)
O23 - Service: @comres.dll,-2797 (MSDTC) - Unknown owner -
C:\windows\System32\msdtc.exe (file missing)
O23 - Service: @%SystemRoot%\System32\netlogon.dll,-102 (Netlogon) - Unknown
owner - C:\windows\system32\lsass.exe (file missing)
O23 - Service: @%systemroot%\system32\Locator.exe,-2 (RpcLocator) - Unknown
owner - C:\windows\system32\locator.exe (file missing)
O23 - Service: @%SystemRoot%\system32\samsrv.dll,-1 (SamSs) - Unknown owner -
C:\windows\system32\lsass.exe (file missing)
O23 - Service: @%SystemRoot%\system32\snmptrap.exe,-3 (SNMPTRAP) - Unknown owner
- C:\windows\System32\snmptrap.exe (file missing)
O23 - Service: @%systemroot%\system32\spoolsv.exe,-1 (Spooler) - Unknown owner -
C:\windows\System32\spoolsv.exe (file missing)
O23 - Service: @%SystemRoot%\system32\sppsvc.exe,-101 (sppsvc) - Unknown owner -
C:\windows\system32\sppsvc.exe (file missing)
O23 - Service: @%SystemRoot%\system32\ui0detect.exe,-101 (UI0Detect) - Unknown
owner - C:\windows\system32\UI0Detect.exe (file missing)
O23 - Service: @%SystemRoot%\system32\vaultsvc.dll,-1003 (VaultSvc) - Unknown
owner - C:\windows\system32\lsass.exe (file missing)
O23 - Service: @%SystemRoot%\system32\vds.exe,-100 (vds) - Unknown owner -
C:\windows\System32\vds.exe (file missing)
O23 - Service: @%systemroot%\system32\vssvc.exe,-102 (VSS) - Unknown owner -
C:\windows\system32\vssvc.exe (file missing)
O23 - Service: @%systemroot%\system32\wbengine.exe,-104 (wbengine) - Unknown
owner - C:\windows\system32\wbengine.exe (file missing)
O23 - Service: @%ProgramFiles%\Windows Defender\MpAsDesc.dll,-310 (WinDefend) -
Unknown owner - C:\Program Files (x86)\Windows Defender\MsMpEng.exe (file
missing)
O23 - Service: @%Systemroot%\system32\wbem\wmiapsrv.exe,-110 (wmiApSrv) -
Unknown owner - C:\windows\system32\wbem\WmiApSrv.exe (file missing)
O23 - Service: @%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe,-101
(WMPNetworkSvc) - Unknown owner - C:\Program Files (x86)\Windows Media
Player\wmpnetwk.exe (file missing)
O23 - Service: ZAtheros Bt and Wlan Coex Agent - Atheros - C:\Program Files
(x86)\Bluetooth Suite\Ath_CoexAgent.exe

--
End of file - 5896 bytes

======Listing Processes======

\SystemRoot\System32\smss.exe
%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,20480,768 Windows=On SubSystemType=Windows
ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3
ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,20480,768 Windows=On SubSystemType=Windows
ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3
ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
wininit.exe
winlogon.exe
C:\windows\system32\services.exe
C:\windows\system32\lsass.exe
C:\windows\system32\svchost.exe -k DcomLaunch
C:\windows\system32\svchost.exe -k RPCSS
C:\windows\system32\atiesrxx.exe
C:\windows\System32\svchost.exe -k LocalServiceNetworkRestricted
"dwm.exe"
C:\windows\system32\svchost.exe -k netsvcs
C:\windows\system32\svchost.exe -k LocalService
```

```
atieclxx
C:\windows\System32\svchost.exe -k LocalSystemNetworkRestricted
C:\windows\system32\svchost.exe -k NetworkService
C:\windows\System32\spoolsv.exe
C:\windows\system32\svchost.exe -k LocalServiceNoNetwork
taskhostex.exe
C:\windows\Explorer.EXE
"C:\Program Files\ATI Technologies\ATI.ACE\Fuel\Fuel.Service.exe" /launchService
"C:\Program Files (x86)\Bluetooth Suite\adminservice.exe"
C:\windows\system32\CxAudMsg64.exe
"C:\Program Files\Elantech\ETDService.exe"
"C:\Program Files\Elantech\ETDCtrl.exe"
C:\windows\system32\svchost.exe -k imgsvc
"C:\Program Files (x86)\Bluetooth Suite\Ath_CoexAgent.exe"
"C:\Windows\System32\WUDFHost.exe"
-HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa}
-IoEventPortName:HostProcess-a1582c73-8d5b-4ed2-becf-7cac45c90027
-SystemEventPortName:HostProcess-84552c6a-c6d4-4844-8c56-25ddd495445e
-IoCancelEventPortName:HostProcess-c2275a37-5059-4e45-8cf2-5ffd320b7900
-NonStateChangingEventPortName:HostProcess-19b5159c-15eb-48ca-961e-cb25a156fec5
-ServiceSID:S-1-5-80-2652678385-582572993-1835434367-1344795993-749280709
-LifetimeId:edb12285-4fbd-4db2-ab31-86ba9e31a8bf
-DeviceGroupId:WudfDefaultDevicePool
C:\windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
"C:\Program Files\Elantech\ETDCtrlHelper.exe"
"C:\Program Files\Elantech\ETDIntelligent.exe"
C:\windows\system32\SearchIndexer.exe /Embedding
"C:\Windows\System32\WUDFHost.exe"
-HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa}
-IoEventPortName:HostProcess-9fcc420a-6ff0-492b-8caa-6dac64b42470
-SystemEventPortName:HostProcess-45cf24c5-65e0-435c-8116-678c105db4dc
-IoCancelEventPortName:HostProcess-1073c533-9cb8-4996-bf4b-291bdb168a94
-NonStateChangingEventPortName:HostProcess-d1ea7261-3733-4c1f-bd0e-86e7d299ce4d
-ServiceSID:S-1-5-80-2652678385-582572993-1835434367-1344795993-749280709
-LifetimeId:f11d7171-7870-47d6-b84c-d63cf92ef571 -DeviceGroupId:WpdFsGroup
"C:\Program Files (x86)\Lenovo\YouCam\YCMMirage.exe"
"C:\Program Files\CONEXANT\CAudioFilterAgent\CAudioFilterAgent64.exe"
"C:\Program Files (x86)\Bluetooth Suite\BtPreLoad.exe"
"C:\Program Files (x86)\Lenovo\Energy Management\Energy Management.exe"
"C:\Program Files (x86)\Lenovo\Energy Management\utility.exe"
"C:\Users\Lusinka\AppData\Local\Google\Update\GoogleUpdate.exe" /c
"C:\Program Files (x86)\USB Camera\VM331STI.EXE"
"C:\Program Files (x86)\Dolby Advanced Audio v2\pcee4.exe" -autostart
"C:\Program Files (x86)\Lenovo\YouCam\YouCamTray.exe" /s
"C:\Program Files (x86)\Lenovo\PowerDVD10\PDVD10Serv.exe"
"F:\RSITx64.exe"
C:\windows\system32\wbem\wmiprvse.exe

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

C:\windows\tasks\GoogleUpdateTaskUserS-1-5-21-1725720331-840875839-1428669064-10
02Core.job
C:\windows\tasks\GoogleUpdateTaskUserS-1-5-21-1725720331-840875839-1428669064-10
02UA.job

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

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser
Helper Objects\{8D10F6C4-0E01-4BD4-8601-11AC1FDF8126}]
CIESpeechBHO Class - C:\Program Files (x86)\Bluetooth Suite\IEPlugIn.dll
[2012-09-30 64640]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
"ETDCtrl"=C:\Program Files\Elantech\ETDCtrl.exe [2012-10-03 2872720]
"SmartAudio"=C:\Program Files\CONEXANT\SAII\SACpl.exe [2012-06-13 1647616]
"cAudioFilterAgent"=C:\Program
Files\Conexant\cAudioFilterAgent\cAudioFilterAgent64.exe [2012-06-15 887968]
"BtPreLoad"=C:\Program Files (x86)\Bluetooth Suite\BtPreLoad.exe [2012-09-30
```

```
64640]
"Energy Management"=C:\Program Files (x86)\Lenovo\Energy Management\Energy
Management.exe [2013-02-14 17079376]
"EnergyUtility"=C:\Program Files (x86)\Lenovo\Energy Management\Utility.exe
[2013-02-14 191568]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"Google Update"=C:\Users\Lusinka\AppData\Local\Google\Update\GoogleUpdate.exe
[2013-06-21 116648]

[HKEY_LOCAL_MACHINE\Software\wow6432node\Microsoft\Windows\CurrentVersion\Run]
"331BigDog"=C:\Program Files (x86)\USB Camera\VM331STI.EXE [2012-05-02 548864]
"Dolby Advanced Audio v2"=C:\Program Files (x86)\Dolby Advanced Audio
v2\pcee4.exe [2012-07-26 508656]
"YouCam Mirage"=C:\Program Files (x86)\Lenovo\YouCam\YCMMirage.exe [2012-07-27
136488]
"YouCam Tray"=C:\Program Files (x86)\Lenovo\YouCam\YouCamTray.exe [2012-07-27
167024]
"UpdateP2GShortCut"=C:\Program Files
(x86)\Lenovo\Power2Go\MUITransfer\MUIStartMenu.exe [2012-04-19 217088]
"RemoteControl10"=C:\Program Files (x86)\Lenovo\PowerDVD10\PDVD10Serv.exe
[2012-03-29 91432]
"Intel AppUp(SM) center"=C:\Program Files
(x86)\Intel\IntelAppStore\bin\ismagent.exe [2012-07-12 155488]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObject
DelayLoad]
WebCheck - {E6FB5E20-DE35-11CF-9C87-00AA005127ED}

[HKEY_LOCAL_MACHINE\system\currentcontrolset\control\securityproviders]
"SecurityProviders"=credssp.dll

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

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\BasicDispl
ay.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\BasicRende
r.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\Boot Bus
Extender]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\Boot file
system]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\BrokerInfr
astructure]

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\DeviceInst
all]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\dxgkrnl.sy
s]

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\File system]

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

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

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

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

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

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

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\PCI Configuration]

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\PNP Filter]

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\Primary disk]

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

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

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\SCSI Class]

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\System Bus Extender]

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

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

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

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

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\volmgrx.sy
s]

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

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

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

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{36FC9E60-
C465-11CF-8056-444553540000}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E965-
E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E967-
E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E969-
E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E96A-
E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E96B-
E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E96F-
E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E977-
E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E97B-
E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E97D-
E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E980-
E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{533C5B84-
EC70-11D2-9505-00C04F79DEAF}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{6BDD1FC1-
810F-11D0-BEC7-08002BE2092F}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{71A27CDD-
812A-11D0-BEC7-08002BE2092F}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{745A17A0-
74D3-11D0-B6FE-00A0C90F57DA}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{9DA2B80F-
F89F-4A49-A5C2-511B085B9E8A}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{A0A588A4-
C46F-4B37-B7EA-C82FE89870C6}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{D48179BE-
EC20-11D1-B6B8-00C04FA372A7}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{D94EE5D8-

D189-4994-83D2-F68D7D41B0E6}]

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

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

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\BasicDispl
ay.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\BasicRende
r.sys]

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\Boot Bus
Extender]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\Boot file
system]

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\BrokerInfr
astructure]

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

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\DeviceInst
all]

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

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\Dot3Svc]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\dxgkrnl.sy
s]

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

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\File
system]

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

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

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

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

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\LanmanServ
er]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\LanmanWork
station]

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

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

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

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

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

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\mrxsmb10]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\mrxsmb20]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\NativeWifi
P]

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\NDIS
Wrapper]

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

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\NetBIOSGro
up]

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\NetDDEGrou
p]

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

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

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\NetworkPro
vider]

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\nsiproxy.s
ys]

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\PCI Configuration]

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\PNP Filter]

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

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\Primary disk]

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

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

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

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

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

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

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\SCSI Class]

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

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\Streams Drivers]

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\System Bus Extender]

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

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

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\TrustedIns

taller]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{36FC9E60-C465-11CF-8056-444553540000}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{4D36E965-E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{4D36E967-E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{4D36E969-E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{4D36E96A-E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{4D36E96B-E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{4D36E96F-E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{4D36E972-E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{4D36E973-E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{4D36E974-E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{4D36E975-E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{4D36E977-

```
E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{4D36E97B-
E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{4D36E97D-
E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{4D36E980-
E325-11CE-BFC1-08002BE10318}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{50DD5230-
BA8A-11D1-BF5D-0000F805F530}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{533C5B84-
EC70-11D2-9505-00C04F79DEAF}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{6BDD1FC1-
810F-11D0-BEC7-08002BE2092F}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{71A27CDD-
812A-11D0-BEC7-08002BE2092F}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{745A17A0-
74D3-11D0-B6FE-00A0C90F57DA}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{9DA2B80F-
F89F-4A49-A5C2-511B085B9E8A}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{A0A588A4-
C46F-4B37-B7EA-C82FE89870C6}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{D48179BE-
EC20-11D1-B6B8-00C04FA372A7}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{D94EE5D8-
D189-4994-83D2-F68D7D41B0E6}]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"ConsentPromptBehaviorAdmin"=5
"EnableUIADesktopToggle"=0
"EnableCursorSuppression"=1
"ConsentPromptBehaviorUser"=3
"dontdisplaylastusername"=0
"legalnoticecaption"=
"legalnoticetext"=
"shutdownwithoutlogon"=1
"undockwithoutlogon"=1
"DisableCAD"=1

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\explorer]
"ForceActiveDesktopOn"=0
"NoActiveDesktop"=1

[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\sharedaccess\parameters\fi
rewallpolicy\standardprofile\authorizedapplications\list]

[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\sharedaccess\parameters\fi
rewallpolicy\domainprofile\authorizedapplications\list]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32]
"msacm.l3acm"=C:\Windows\System32\l3codeca.acm
"VIDC.YUY2"=msyuv.dll
"vidc.i420"=iyuv_32.dll
"msacm.msgsm610"=msgsm32.acm
"msacm.msg711"=msg711.acm
"VIDC.YVYU"=msyuv.dll
"VIDC.YVU9"=tsbyuv.dll
```

```
"wavemapper"=msacm32.drv
"midimapper"=midimap.dll
"VIDC.UYVY"=msyuv.dll
"VIDC.IYUV"=iyuv_32.dll
"vidc.mrle"=msrle32.dll
"msacm.imaadpcm"=imaadp32.acm
"msacm.msadpcm"=msadp32.acm
"vidc.msvc"=msvidc32.dll
"MSVideo8"=VfWWDM32.dll
"wave1"=wdmaud.drv
"midi1"=wdmaud.drv
"mixer1"=wdmaud.drv
"aux1"=wdmaud.drv
"wave"=wdmaud.drv
"midi"=wdmaud.drv
"mixer"=wdmaud.drv
"aux"=wdmaud.drv
"wave2"=wdmaud.drv
"mixer2"=wdmaud.drv
"midi2"=wdmaud.drv

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

2013-08-01 10:44:00 ----D---- C:\Program Files\trend micro
2013-08-01 10:43:58 ----D---- C:\rsit
2013-08-01 08:31:16 ----D---- C:\Users\Lusinka\AppData\Roaming\Malwarebytes
2013-08-01 08:30:03 ----A---- C:\AdwCleaner[R1].txt
2013-08-01 08:29:58 ----D---- C:\ProgramData\Malwarebytes
2013-08-01 08:29:52 ----D---- C:\Program Files (x86)\Malwarebytes' Anti-Malware
2013-08-01 08:29:52 ----A---- C:\windows\system32\drivers\mbam.sys
2013-08-01 07:18:24 ----D---- C:\ldiag
2013-07-21 18:07:25 ----A---- C:\windows\system32\dwmcore.dll
2013-07-21 18:07:22 ----A---- C:\windows\SYSWOW64\dwmcore.dll
2013-07-21 18:07:21 ----A---- C:\windows\SYSWOW64\explorer.exe
2013-07-21 18:07:21 ----A---- C:\windows\system32\ntoskrnl.exe
2013-07-21 18:07:21 ----A---- C:\windows\explorer.exe
2013-07-21 18:07:18 ----A---- C:\windows\system32\samsrv.dll
2013-07-21 18:07:17 ----A---- C:\windows\system32\mfcore.dll
2013-07-21 18:07:17 ----A---- C:\windows\system32\drivers\tcpip.sys
2013-07-21 18:07:16 ----A---- C:\windows\SYSWOW64\mfcore.dll
2013-07-21 18:07:16 ----A---- C:\windows\system32\drivers\volsnap.sys
2013-07-21 18:07:13 ----A---- C:\windows\system32\winload.exe
2013-07-21 18:07:12 ----A---- C:\windows\system32\XpsGdiConverter.dll
2013-07-21 18:07:10 ----A---- C:\windows\system32\winresume.exe
2013-07-21 18:07:10 ----A---- C:\windows\system32\vds.exe
2013-07-21 18:07:09 ----A---- C:\windows\system32\mscms.dll
2013-07-21 18:07:08 ----A---- C:\windows\system32\mfasfsrcsnk.dll
2013-07-21 18:07:08 ----A---- C:\windows\system32\audiosrv.dll
2013-07-21 18:07:07 ----A---- C:\windows\SYSWOW64\XpsGdiConverter.dll
2013-07-21 18:07:07 ----A---- C:\windows\SYSWOW64\mscms.dll
2013-07-21 18:07:06 ----A---- C:\windows\system32\wwansvc.dll
2013-07-21 18:07:06 ----A---- C:\windows\system32\samlib.dll
2013-07-21 18:07:06 ----A---- C:\windows\system32\drivers\UCX01000.SYS
2013-07-21 18:07:03 ----A---- C:\windows\SYSWOW64\mfasfsrcsnk.dll
2013-07-21 18:07:03 ----A---- C:\windows\system32\MbaeParserTask.exe
2013-07-21 18:07:03 ----A---- C:\windows\system32\DeviceSetupManager.dll
2013-07-21 18:07:02 ----A---- C:\windows\system32\drivers\USBXHCI.SYS
2013-07-21 18:07:02 ----A---- C:\windows\system32\drivers\sdbus.sys
2013-07-21 18:07:01 ----A---- C:\windows\system32\drivers\dumpsd.sys
2013-07-21 18:06:58 ----A---- C:\windows\SYSWOW64\samlib.dll
2013-07-21 18:06:58 ----A---- C:\windows\system32\vdsutil.dll
2013-07-21 18:06:56 ----A---- C:\windows\system32\drivers\BthAvrcpTg.sys
2013-07-21 18:06:43 ----A---- C:\windows\system32\drivers\ndis.sys
```

2013-07-19 22:06:02 ----A---- C:\windows\system32\FNTCACHE.DAT
2013-07-16 09:55:35 ----A---- C:\windows\system32\tssdisai.dll
2013-07-11 08:53:30 ----A---- C:\windows\system32\DWrite.dll
2013-07-11 08:53:29 ----A---- C:\windows\SYSWOW64\DWrite.dll
2013-07-11 08:51:22 ----A---- C:\windows\system32\qedit.dll
2013-07-11 08:51:21 ----A---- C:\windows\SYSWOW64\qedit.dll
2013-07-11 08:51:18 ----A---- C:\windows\system32\win32k.sys
2013-07-11 08:50:02 ----A---- C:\windows\system32\mshtml.dll
2013-07-11 08:49:52 ----A---- C:\windows\system32\ieframe.dll
2013-07-11 08:49:44 ----A---- C:\windows\system32\jscript9.dll
2013-07-11 08:49:35 ----A---- C:\windows\SYSWOW64\mshtml.dll
2013-07-11 08:49:28 ----A---- C:\windows\SYSWOW64\ieframe.dll
2013-07-11 08:49:14 ----A---- C:\windows\system32\iertutil.dll
2013-07-11 08:49:13 ----A---- C:\windows\SYSWOW64\iertutil.dll
2013-07-11 08:49:12 ----A---- C:\windows\system32\urlmon.dll
2013-07-11 08:49:12 ----A---- C:\windows\system32\jscript.dll
2013-07-11 08:49:11 ----A---- C:\windows\system32\wininet.dll
2013-07-11 08:49:10 ----A---- C:\windows\SYSWOW64\urlmon.dll
2013-07-11 08:49:10 ----A---- C:\windows\SYSWOW64\jscript9.dll
2013-07-11 08:49:09 ----A---- C:\windows\SYSWOW64\wininet.dll
2013-07-11 08:49:06 ----A---- C:\windows\system32\msfeeds.dll
2013-07-11 08:49:04 ----A---- C:\windows\SYSWOW64\msfeeds.dll
2013-07-11 08:48:59 ----A---- C:\windows\SYSWOW64\jscript.dll
2013-07-11 08:48:58 ----A---- C:\windows\system32\ie4uinit.exe
2013-07-11 08:48:51 ----A---- C:\windows\system32\WMVDECOD.DLL
2013-07-11 08:48:49 ----A---- C:\windows\SYSWOW64\WMVDECOD.DLL

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

2013-08-01 10:44:00 ----RD---- C:\Program Files
2013-08-01 10:42:48 ----D---- C:\ProgramData\McAfee
2013-08-01 10:42:48 ----D---- C:\Program Files\Common Files
2013-08-01 10:42:47 ----RD---- C:\Program Files (x86)
2013-08-01 10:42:47 ----D---- C:\Program Files (x86)\Common Files
2013-08-01 10:42:12 ----AD---- C:\windows\System32
2013-08-01 10:41:20 ----D---- C:\windows\Temp
2013-08-01 10:41:20 ----D---- C:\windows\Prefetch
2013-08-01 10:40:38 ----D---- C:\windows\system32\Drivers
2013-08-01 10:40:34 ----HD---- C:\windows\ELAMBKUP
2013-08-01 10:27:41 ----A---- C:\windows\system32\PerfStringBackup.INI
2013-08-01 10:27:40 ----D---- C:\windows\Inf
2013-08-01 10:26:16 ----D---- C:\windows\system32\sru
2013-08-01 08:29:58 ----HD---- C:\ProgramData
2013-08-01 08:27:23 ----D---- C:\windows\system32\config
2013-08-01 08:24:37 ----D---- C:\windows\Microsoft.NET
2013-08-01 07:39:35 ----D---- C:\windows\system32\NDF
2013-08-01 07:27:04 ----SD---- C:\Users\Lusinka\AppData\Roaming\Microsoft
2013-07-30 21:46:13 ----SHD---- C:\System Volume Information
2013-07-26 10:54:04 ----D---- C:\windows\WinSxS
2013-07-26 09:43:06 ----D---- C:\windows\AUInstallAgent
2013-07-26 09:42:12 ----HD---- C:\Program Files\WindowsApps
2013-07-22 22:06:07 ----D---- C:\windows\SysWOW64
2013-07-22 22:05:52 ----D---- C:\windows\system32\Boot
2013-07-22 22:05:48 ----AD---- C:\Windows
2013-07-22 22:05:43 ----D---- C:\windows\system32\DriverStore
2013-07-21 20:42:15 ----D---- C:\windows\Downloaded Installations
2013-07-21 19:52:13 ----D---- C:\windows\CbsTemp
2013-07-21 18:02:17 ----D---- C:\windows\system32\catroot2
2013-07-19 22:04:13 ----D---- C:\windows\servicing
2013-07-17 21:21:48 ----RD---- C:\windows\assembly
2013-07-15 17:39:59 ----D---- C:\windows\rescache
2013-07-15 17:01:11 ----AD---- C:\windows\system32\oobe
2013-07-15 17:01:07 ----D---- C:\Program Files\Windows Journal
2013-07-15 17:00:40 ----D---- C:\Program Files\Internet Explorer
2013-07-15 17:00:40 ----D---- C:\Program Files (x86)\Internet Explorer
2013-07-12 11:18:54 ----A---- C:\windows\system32\MRT.exe
2013-07-07 22:35:12 ----D---- C:\windows\system32\drivers\UMDF
2013-07-02 15:42:55 ----D---- C:\windows\SYSWOW64\cs-CZ

2013-07-02 15:42:55 ----D---- C:\windows\system32\cs-CZ
2013-07-02 15:42:32 ----D---- C:\windows\SYSWOW64\en-US
2013-07-02 15:42:26 ----D---- C:\windows\system32\en-US
2013-07-02 15:42:01 ----RSD---- C:\windows\Fonts
2013-07-02 15:41:54 ----RD---- C:\windows\ToastData

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

R0 ACPI;@acpi.inf,%ACPI.SvcDesc%;Microsoft ACPI Driver;
C:\windows\System32\drivers\ACPI.sys [2012-09-20 425192]
R0 acpiex;Microsoft ACPIEx Driver; C:\windows\System32\Drivers\acpiex.sys [2012-07-26 77040]
R0 CLFS;@%SystemRoot%\system32\drivers\clfs.sys,-100;
C:\windows\System32\drivers\CLFS.sys [2012-07-26 361200]
R0 CNG;CNG; C:\windows\System32\Drivers\cng.sys [2012-10-11 562392]
R0 disk;@disk.inf,%disk_ServiceDesc%;Disk Driver;
C:\windows\System32\drivers\disk.sys [2012-07-26 102640]
R0 FileInfo;@%SystemRoot%\system32\drivers\fileinfo.sys,-100;
C:\windows\System32\drivers\fileinfo.sys [2012-07-26 71920]
R0 FltMgr;@%SystemRoot%\system32\drivers\fltmgr.sys,-10001;
C:\windows\system32\drivers\fltmgr.sys [2012-07-26 374512]
R0 fvevol;@%SystemRoot%\system32\drivers\fvevol.sys,-100;
C:\windows\System32\DRIVERS\fvevol.sys [2012-09-20 465128]
R0 KSecDD;KSecDD; C:\windows\System32\Drivers\ksecdd.sys [2012-09-20 100072]
R0 KSecPkg;KSecPkg; C:\windows\System32\Drivers\ksecpkg.sys [2012-10-11 172264]
R0 LHDmgr;LHDmgr; C:\windows\System32\DRIVERS\LhdX64.sys [2013-02-14 39008]
R0 mountmgr;@%SystemRoot%\system32\drivers\mountmgr.sys,-100;
C:\windows\System32\drivers\mountmgr.sys [2012-07-26 93936]
R0 msisadrv;msisadrv; C:\windows\System32\drivers\msisadrv.sys [2012-07-26 17136]
R0 Mup;@%systemroot%\system32\drivers\mup.sys,-101;
C:\windows\System32\Drivers\mup.sys [2012-07-26 83696]
R0 NDIS;@%SystemRoot%\system32\drivers\ndis.sys,-200;
C:\windows\system32\drivers\ndis.sys [2013-06-17 997632]
R0 partmgr;@%SystemRoot%\system32\drivers\partmgr.sys,-100;
C:\windows\System32\drivers\partmgr.sys [2013-01-10 91880]
R0 pci;@machine.inf,%pci_svcdesc%;PCI Bus Driver;
C:\windows\System32\drivers\pci.sys [2012-07-26 234224]
R0 pcw;Performance Counters for Windows Driver;
C:\windows\System32\drivers\pcw.sys [2012-07-26 52464]
R0 pdc;@%SystemRoot%\system32\drivers\pdc.sys,-100;
C:\windows\system32\drivers\pdc.sys [2013-03-02 69864]
R0 rdyboost;ReadyBoost; C:\windows\System32\drivers\rdyboost.sys [2012-07-26 217328]
R0 spaceport;@spaceport.inf,%Spaceport_ServiceDesc%;Storage Spaces Driver;
C:\windows\System32\drivers\spaceport.sys [2013-05-04 284416]
R0 storahci;@mshdc.inf,%storahci_ServiceDescription%;Microsoft Standard SATA AHCI Driver; C:\windows\System32\drivers\storahci.sys [2013-03-02 77544]
R0 Tcpip;@%SystemRoot%\system32\tcpipcfg.dll,-50003;
C:\windows\System32\drivers\tcpip.sys [2013-06-01 2233600]
R0 vdrvroot;@vdrvroot.inf,%vdrvroot_svcdesc%;Microsoft Virtual Drive Enumerator;
C:\windows\System32\drivers\vdrvroot.sys [2012-07-26 36080]
R0 volmgr;@volmgr.inf,%volmgr_svcdesc%;Volume Manager Driver;
C:\windows\System32\drivers\volmgr.sys [2012-07-26 83184]
R0 volmgrx;@%SystemRoot%\system32\drivers\volmgrx.sys,-100;
C:\windows\System32\drivers\volmgrx.sys [2012-07-26 378608]
R0 volsnap;@volume.inf,%VolumeClassName%;Storage volumes;
C:\windows\System32\drivers\volsnap.sys [2013-06-01 327936]
R0 Wdf01000;@%SystemRoot%\system32\drivers\Wdf01000.sys,-1000;
C:\windows\system32\drivers\Wdf01000.sys [2013-01-10 785504]
R0 WFPLWFS;@%SystemRoot%\System32\drivers\wfplwfs.sys,-6000;
C:\windows\system32\DRIVERS\wfplwfs.sys [2012-07-26 96496]
R1 AFD;@%systemroot%\system32\drivers\afd.sys,-1000;
C:\windows\system32\drivers\afd.sys [2012-11-06 560640]
R1 BasicDisplay;BasicDisplay; C:\windows\System32\drivers\BasicDisplay.sys [2012-07-26 48640]
R1 BasicRender;BasicRender; C:\windows\System32\drivers\BasicRender.sys

[2012-07-26 29696]
R1 Beep;Beep; C:\windows\system32\drivers\Beep.sys [2012-07-26 7680]
R1 cdrom;@cdrom.inf,%cdrom_ServiceDesc%;CD-ROM Driver;
C:\windows\System32\drivers\cdrom.sys [2012-07-26 174080]
R1 Dfsc;@%systemroot%\system32\wkssvc.dll,-1008;
C:\windows\System32\Drivers\dfsc.sys [2012-07-26 118784]
R1 discache;@%systemroot%\system32\drivers\discache.sys,-102;
C:\windows\System32\drivers\discache.sys [2012-07-26 50688]
R1 Msfs;Msfs; C:\windows\system32\drivers\Msfs.sys [2012-07-26 26112]
R1 mssmbios;@mssmbios.inf,%mssmbios_svcdesc%;Microsoft System Management BIOS
Driver; C:\windows\System32\drivers\mssmbios.sys [2012-07-26 37616]
R1 NetBIOS;@netnb.inf,%NetBIOS_Desc%;NetBIOS Interface;
C:\windows\system32\DRIVERS\netbios.sys [2012-07-26 46080]
R1 NetBT;@%SystemRoot%\system32\drivers\netbt.sys,-2;
C:\windows\System32\DRIVERS\netbt.sys [2012-07-26 331776]
R1 Npfs;Npfs; C:\windows\system32\drivers\Npfs.sys [2012-07-26 49152]
R1 npsvctrig;@npsvctrig.inf,%NPSVCTRIG.SvcDisplayName%;Named pipe service
trigger provider; C:\windows\System32\drivers\npsvctrig.sys [2012-07-26 23552]
R1 nsiproxy;@%SystemRoot%\system32\drivers\nsiproxy.sys,-2;
C:\windows\system32\drivers\nsiproxy.sys [2012-07-26 34304]
R1 Null;Null; C:\windows\system32\drivers\Null.sys [2012-07-26 5632]
R1 Psched;@%SystemRoot%\System32\drivers\pacer.sys,-101;
C:\windows\system32\DRIVERS\pacer.sys [2012-07-26 145408]
R1 rdbss;@%systemroot%\system32\wkssvc.dll,-1000;
C:\windows\system32\DRIVERS\rdbss.sys [2013-05-04 427520]
R1 tdx;@%SystemRoot%\system32\tcpipcfg.dll,-50004;
C:\windows\system32\DRIVERS\tdx.sys [2012-07-26 117248]
R1 vwififlt;@%SystemRoot%\System32\drivers\vwififlt.sys,-259;
C:\windows\system32\DRIVERS\vwififlt.sys [2012-07-26 64000]
R1 Wanarpv6;@%systemroot%\system32\rascfg.dll,-32012;
C:\windows\system32\DRIVERS\wanarp.sys [2013-04-09 83456]
R2 lltdio;@%SystemRoot%\system32\lltdres.dll,-6;
C:\windows\system32\DRIVERS\lltdio.sys [2012-07-26 60416]
R2 luafv;@%systemroot%\system32\drivers\luafv.sys,-100;
C:\windows\system32\drivers\luafv.sys [2012-07-26 134144]
R2 NativeWifiP;@%SystemRoot%\System32\drivers\nwifi.sys,-101;
C:\windows\system32\DRIVERS\nwifi.sys [2012-07-26 427520]
R2 Ndu;@%SystemRoot%\system32\drivers\Ndu.sys,-10001;
C:\windows\system32\drivers\Ndu.sys [2012-07-26 97792]
R2 PEAUTH;PEAUTH; C:\windows\system32\drivers\peauth.sys [2013-04-09 805376]
R2 rspndr;@%SystemRoot%\system32\lltdres.dll,-5;
C:\windows\system32\DRIVERS\rspndr.sys [2012-07-26 78848]
R2 secdrv;Security Driver; C:\windows\system32\drivers\secdrv.sys [2012-07-26
23040]
R2 tcpipreg;TCP/IP Registry Compatibility;
C:\windows\System32\drivers\tcpipreg.sys [2012-07-26 45056]
R3 ACPIVPC;@oem14.inf,%ACPIVPC.SvcDesc%;Lenovo Virtual Power Controller Driver;
C:\windows\System32\drivers\AcpiVpc.sys [2013-02-14 33560]
R3 amdkmdag;amdkmdag; C:\windows\system32\DRIVERS\atikmdag.sys [2012-08-01
10280960]
R3 amdkmdap;amdkmdap; C:\windows\system32\DRIVERS\atikmpag.sys [2012-08-01
368640]
R3 AmdPPM;@cpu.inf,%AmdPPM.SvcDesc%;AMD Processor Driver;
C:\windows\System32\drivers\amdppm.sys [2012-11-06 88064]
R3 athr;@oem8.inf,%ATHR.Service.DispName%;Qualcomm Atheros Extensible Wireless
LAN device driver; C:\windows\system32\DRIVERS\athw8x.sys [2012-09-19 3653632]
R3 AtiHDAudioService;@oem2.inf,%ATIHdAudioDriver.SvcDesc%;AMD Function Driver
for HD Audio Service; C:\windows\system32\drivers\AtihdW86.sys [2012-07-17
98472]
R3 bowser;@%systemroot%\system32\browser.dll,-102;
C:\windows\system32\DRIVERS\bowser.sys [2012-07-26 101888]
R3 BTATH_BUS;@oem9.inf,%BTATH_BUS.SVCDESC%;Qualcomm Atheros Bluetooth Bus;
C:\windows\System32\drivers\btath_bus.sys [2012-09-30 33944]
R3 CmBatt;@cmbatt.inf,%CmBatt.SvcDesc%;Microsoft ACPI Control Method Battery
Driver; C:\windows\System32\drivers\CmBatt.sys [2012-07-26 25600]
R3 CnxtHdAudService;@oem7.inf,%UAAFunctionDriverForHdAudio.SvcDesc%;Conexant UAA
Function Driver for High Definition Audio Service;
C:\windows\system32\drivers\CHDRT64.sys [2012-06-27 1608864]

R3 CompositeBus;@CompositeBus.inf,%CompositeBus.SVCDESC%;Composite Bus Enumerator Driver; C:\windows\System32\drivers\CompositeBus.sys [2012-07-26 36352]
R3 condrv;Console Driver; C:\windows\System32\drivers\condrv.sys [2012-07-26 33792]
R3 DXGKrnl;LDDM Graphics Subsystem; C:\windows\System32\drivers\dxgkrnl.sys [2013-04-16 1455368]
R3 ETD;@oem5.inf,%PS2DeviceDesc%;ELAN PS/2 Port Input Device; C:\windows\system32\DRIVERS\ETD.sys [2012-10-03 323920]
R3 fastfat;FAT12/16/32 File System Driver; C:\windows\system32\drivers\fastfat.sys [2012-07-26 210672]
R3 HDAudBus;@hdaudbus.inf,%HDAudBus.SVCDESC%;Microsoft UAA Bus Driver for High Definition Audio; C:\windows\System32\drivers\HDAudBus.sys [2012-09-20 71168]
R3 HidUsb;@input.inf,%HID.SvcDesc%;Microsoft HID Class Driver; C:\windows\System32\drivers\hidusb.sys [2013-04-09 27648]
R3 HTTP;@%SystemRoot%\system32\drivers\http.sys,-1; C:\windows\system32\drivers\HTTP.sys [2013-03-15 861184]
R3 i8042prt;@msmouse.inf,%i8042prt.SvcDesc%;PS/2 Keyboard and Mouse Port Driver; C:\windows\System32\drivers\i8042prt.sys [2012-07-26 112640]
R3 kbdclass;@keyboard.inf,%kbdclass.SvcDesc%;Keyboard Class Driver; C:\windows\System32\drivers\kbdclass.sys [2012-07-26 48368]
R3 kdnic;@kdnic.inf,%KdNic.Service.DispName%;Microsoft Kernel Debug Network Miniport (NDIS 6.20); C:\windows\system32\DRIVERS\kdnic.sys [2012-07-26 18432]
R3 ksthunk;Kernel Streaming Thunks; C:\windows\system32\drivers\ksthunk.sys [2012-07-26 21376]
R3 monitor;@monitor.inf,%Monitor.SVCDESC%;Služba ovladače funkce třídy monitorů Microsoft; C:\windows\System32\drivers\monitor.sys [2013-03-01 30720]
R3 mouclass;@msmouse.inf,%mouclass.SvcDesc%;Mouse Class Driver; C:\windows\System32\drivers\mouclass.sys [2012-07-26 45808]
R3 mouhid;@msmouse.inf,%MOUHID.SvcDesc%;Mouse HID Driver; C:\windows\System32\drivers\mouhid.sys [2013-03-02 26112]
R3 mpsdrv;@%SystemRoot%\system32\FirewallAPI.dll,-23092; C:\windows\System32\drivers\mpsdrv.sys [2012-10-11 74752]
R3 mrxsmb;@%systemroot%\system32\wkssvc.dll,-1002; C:\windows\system32\DRIVERS\mrxsmb.sys [2013-02-06 370688]
R3 mrxsmb10;@%systemroot%\system32\wkssvc.dll,-1004; C:\windows\system32\DRIVERS\mrxsmb10.sys [2012-07-26 279552]
R3 mrxsmb20;@%systemroot%\system32\wkssvc.dll,-1006; C:\windows\system32\DRIVERS\mrxsmb20.sys [2013-02-06 215552]
R3 mshidumdf;@%SystemRoot%\system32\drivers\mshidumdf.sys,-100; C:\windows\System32\drivers\mshidumdf.sys [2012-07-26 10752]
R3 NdisTapi;@%systemroot%\system32\rascfg.dll,-32001; C:\windows\system32\DRIVERS\ndistapi.sys [2012-09-20 25088]
R3 Ndisuio;@ndisuio.inf,%NDISUIO_Desc%;NDIS Usermode I/O Protocol; C:\windows\system32\DRIVERS\ndisuio.sys [2012-07-26 58880]
R3 NdisWan;@%systemroot%\system32\rascfg.dll,-32002; C:\windows\system32\DRIVERS\ndiswan.sys [2012-07-26 174080]
R3 NDProxy;NDIS Proxy; C:\windows\system32\drivers\NDProxy.sys [2013-04-09 60416]
R3 Ntfs;Ntfs; C:\windows\system32\drivers\Ntfs.sys [2013-02-02 1933544]
R3 PptpMiniport;@%systemroot%\system32\rascfg.dll,-32006; C:\windows\system32\DRIVERS\raspptp.sys [2012-07-26 114176]
R3 RasAgileVpn;@netavpna.inf,%Svc-Mp-AgileVpn-DispName%;WAN Miniport (IKEv2); C:\windows\system32\DRIVERS\AgileVpn.sys [2012-07-26 68608]
R3 Rasl2tp;@%systemroot%\system32\rascfg.dll,-32005; C:\windows\system32\DRIVERS\rasl2tp.sys [2012-07-26 124928]
R3 RasPppoe;@%systemroot%\system32\rascfg.dll,-32007; C:\windows\system32\DRIVERS\raspppoe.sys [2012-07-26 81920]
R3 RasSstp;@%systemroot%\system32\sstpsvc.dll,-202; C:\windows\system32\DRIVERS\rassstp.sys [2012-07-26 92672]
R3 rdpbus;@rdpbus.inf,%rdpbus_svcdesc%;Remote Desktop Device Redirector Bus Driver; C:\windows\System32\drivers\rdpbus.sys [2012-07-26 22528]
R3 RTL8168;@oem3.inf,%rtl8168.Service.DispName%;Realtek 8168 NT Driver; C:\windows\system32\DRIVERS\Rt630x64.sys [2012-07-30 690832]
R3 srv;@%systemroot%\system32\srvsvc.dll,-102; C:\windows\System32\DRIVERS\srv.sys [2012-07-26 416768]
R3 srv2;@%systemroot%\system32\srvsvc.dll,-104; C:\windows\System32\DRIVERS\srv2.sys [2013-04-09 623104]

R3 srvnet;srvnet; C:\windows\System32\DRIVERS\srvnet.sys [2013-04-09 247808]
R3 swenum;@swenum.inf,%SWENUM.SVCDESC%;Software Bus Driver;
C:\windows\System32\drivers\swenum.sys [2012-07-26 13680]
R3 tunnel;@nettun.inf,%TUNNEL.Service.DisplayName%;Microsoft Tunnel Miniport
Adapter Driver; C:\windows\system32\DRIVERS\tunnel.sys [2012-07-26 149504]
R3 UCX01000;USB Controller Extension; C:\windows\System32\drivers\ucx01000.sys
[2013-06-01 213248]
R3 umbus;@umbus.inf,%umbus.SVCDESC%;UMBus Enumerator Driver;
C:\windows\System32\drivers\umbus.sys [2012-07-26 48128]
R3 usbccgp;@usb.inf,%GenericParent.SvcDesc%;Microsoft USB Generic Parent Driver;
C:\windows\System32\drivers\usbccgp.sys [2012-07-26 120832]
R3 usbehci;@usbport.inf,%EHCIMP.SvcDesc%;Microsoft USB 2.0 Enhanced Host
Controller Miniport Driver; C:\windows\System32\drivers\usbehci.sys [2012-09-20
79080]
R3 usbhub;@usbport.inf,%ROOTHUB.SvcDesc%;Microsoft USB Standard Hub Driver;
C:\windows\System32\drivers\usbhub.sys [2013-02-02 496872]
R3 USBHUB3;@usbhub3.inf,%UsbHub3.SVCDESC%;SuperSpeed Hub;
C:\windows\System32\drivers\UsbHub3.sys [2013-05-04 446720]
R3 usbohci;@usbport.inf,%OHCIMP.SvcDesc%;Microsoft USB Open Host Controller
Miniport Driver; C:\windows\System32\drivers\usbohci.sys [2012-11-20 27136]
R3 USBSTOR;@usbstor.inf,%USBSTOR.SvcDesc%;USB Mass Storage Driver;
C:\windows\System32\drivers\USBSTOR.SYS [2012-07-26 119024]
R3 USBXHCI;@usbxhci.inf,%PCI\CC_0C0330.DeviceDesc%;USB xHCI Compliant Host
Controller; C:\windows\System32\drivers\USBXHCI.SYS [2013-06-01 337152]
R3 vm331avs;@oem6.inf,%USBCamera.DeviceDesc2%;Digital Camera 1;
C:\windows\System32\Drivers\vm331avs.sys [2012-08-24 975104]
R3 vwifibus;@%SystemRoot%\System32\drivers\vwifibus.sys,-257;
C:\windows\System32\drivers\vwifibus.sys [2012-07-26 24064]
R3 vwifimp;@%SystemRoot%\System32\drivers\vwifimp.sys,-261;
C:\windows\system32\DRIVERS\vwifimp.sys [2012-07-26 17920]
R3 WpdUpFltr;@%systemroot%\System32\drivers\WpdUpFltr.sys,-100;
C:\windows\System32\drivers\WpdUpFltr.sys [2012-07-26 19968]
R3 WudfPf;@%SystemRoot%\system32\drivers\Wudfpf.sys,-1000;
C:\windows\system32\drivers\WudfPf.sys [2012-07-26 87040]
R3 WUDFRd;@hidbthle.inf,%WudfRdDisplayName%;Windows Driver Foundation -
User-mode Driver Framework Reflector; C:\windows\System32\drivers\WUDFRd.sys
[2012-07-26 198656]
R3 WUDFWpdFs;WUDFWpdFs; C:\windows\system32\DRIVERS\WUDFRd.sys [2012-07-26
198656]
R3 WUDFWpdMtp;WUDFWpdMtp; C:\windows\system32\DRIVERS\WUDFRd.sys [2012-07-26
198656]
S0 3ware;3ware; C:\windows\System32\drivers\3ware.sys [2012-07-26 106736]
S0 adp94xx;adp94xx; C:\windows\System32\drivers\adp94xx.sys [2012-07-26 492272]
S0 adpahci;adpahci; C:\windows\System32\drivers\adpahci.sys [2012-07-26 340720]
S0 adpu320;adpu320; C:\windows\System32\drivers\adpu320.sys [2012-07-26 184048]
S0 agp440;@machine.inf,%agp440_svcdesc%;Intel AGP Bus Filter;
C:\windows\System32\drivers\agp440.sys [2012-07-26 63216]
S0 amdsata;amdsata; C:\windows\System32\drivers\amdsata.sys [2012-07-26 76016]
S0 amdsbs;amdsbs; C:\windows\System32\drivers\amdsbs.sys [2012-07-26 258288]
S0 amdxata;amdxata; C:\windows\System32\drivers\amdxata.sys [2012-07-26 26352]
S0 arc;arc; C:\windows\System32\drivers\arc.sys [2012-07-26 104688]
S0 arcsas;@arcsas.inf,%arcsas_ServiceName%;Adaptec SAS/SATA-II RAID Windows
Inbox Miniport Driver; C:\windows\System32\drivers\arcsas.sys [2012-07-26
108272]
S0 atapi;@mshdc.inf,%idechannel.DeviceDesc%;IDE Channel;
C:\windows\System32\drivers\atapi.sys [2012-07-26 25840]
S0 b06bdrv;@netbvbda.inf,%vbd_srv_desc%;Broadcom NetXtreme II VBD;
C:\windows\System32\drivers\bxvbda.sys [2012-09-20 533224]
S0 ebdrv;@netevbda.inf,%vbd_srv_desc%;Broadcom NetXtreme II 10 GigE VBD;
C:\windows\System32\drivers\evbda.sys [2012-09-20 3265256]
S0 EhStorClass;@%SystemRoot%\system32\drivers\EhStorClass.sys,-100;
C:\windows\System32\drivers\EhStorClass.sys [2012-07-26 81136]
S0 EhStorTcgDrv;@ehstortcgdrv.inf,%EhStorTcgDrv.Desc%;Microsoft driver for
storage devices supporting IEEE 1667 and TCG protocols;
C:\windows\System32\drivers\EhStorTcgDrv.sys [2012-07-26 113904]
S0 gagp30kx;@machine.inf,%gagp30kx_svcdesc%;Microsoft Generic AGPv3.0 Filter for
K8 Processor Platforms; C:\windows\System32\drivers\gagp30kx.sys [2012-07-26
66800]

S0 HpSAMD;HpSAMD; C:\windows\System32\drivers\HpSAMD.sys [2012-07-26 64752]
S0 hwpolicy;@%systemroot%\system32\drivers\hwpolicy.sys,-101;
C:\windows\System32\drivers\hwpolicy.sys [2012-07-26 24816]
S0 iaStorV;@iastorv.inf,%*PNP0600.DeviceDesc%;Intel RAID Controller Windows 7;
C:\windows\System32\drivers\iaStorV.sys [2012-07-26 411888]
S0 iirsp;iirsp; C:\windows\System32\drivers\iirsp.sys [2012-07-26 45296]
S0 intelide;intelide; C:\windows\System32\drivers\intelide.sys [2012-07-26
18672]
S0 isapnp;isapnp; C:\windows\System32\drivers\isapnp.sys [2012-07-26 22256]
S0 LSI_SAS;LSI_SAS; C:\windows\System32\drivers\lsi_sas.sys [2012-07-26 108784]
S0 LSI_SAS2;LSI_SAS2; C:\windows\System32\drivers\lsi_sas2.sys [2012-07-26
92400]
S0 LSI_SCSI;LSI_SCSI; C:\windows\System32\drivers\lsi_scsi.sys [2012-07-26
116976]
S0 LSI_SSS;LSI_SSS; C:\windows\System32\drivers\lsi_sss.sys [2012-07-26 81136]
S0 megasas;megasas; C:\windows\System32\drivers\megasas.sys [2012-07-26 51952]
S0 MegaSR;MegaSR; C:\windows\System32\drivers\MegaSR.sys [2012-07-26 353008]
S0 mvumis;mvumis; C:\windows\System32\drivers\mvumis.sys [2012-07-26 64240]
S0 nfrd960;nfrd960; C:\windows\System32\drivers\nfrd960.sys [2012-07-26 52464]
S0 nv_agp;@machine.inf,%agpnvidia_svcdesc%;NVIDIA nForce AGP Bus Filter;
C:\windows\System32\drivers\nv_agp.sys [2012-07-26 125168]
S0 nvraid;nvraid; C:\windows\System32\drivers\nvraid.sys [2012-07-26 150256]
S0 nvstor;nvstor; C:\windows\System32\drivers\nvstor.sys [2012-07-26 168176]
S0 pciide;pciide; C:\windows\System32\drivers\pciide.sys [2012-07-26 14064]
S0 pcmcia;pcmcia; C:\windows\System32\drivers\pcmcia.sys [2012-07-26 237808]
S0 sbp2port;@sbp2.inf,%sbp2_ServiceDesc%;SBP-2 Transport/Protocol Bus Driver;
C:\windows\System32\drivers\sbp2port.sys [2012-07-26 107760]
S0 SiSRaid2;SiSRaid2; C:\windows\System32\drivers\SiSRaid2.sys [2012-07-26
44784]
S0 SiSRaid4;SiSRaid4; C:\windows\System32\drivers\sisraid4.sys [2012-07-26
81648]
S0 stexstor;stexstor; C:\windows\System32\drivers\stexstor.sys [2012-07-26
30960]
S0 storflt;@%SystemRoot%\system32\vmstorfltres.dll,-1000;
C:\windows\system32\DRIVERS\vmstorfl.sys [2012-07-26 45160]
S0 storvsc;storvsc; C:\windows\System32\drivers\storvsc.sys [2012-07-26 37992]
S0 uagp35;@machine.inf,%uagp35_svcdesc%;Microsoft AGPv3.5 Filter;
C:\windows\System32\drivers\uagp35.sys [2012-07-26 65776]
S0 uliagpkx;@machine.inf,%uliagpkx_svcdesc%;Uli AGP Bus Filter;
C:\windows\System32\drivers\uliagpkx.sys [2012-07-26 66800]
S0 viaide;viaide; C:\windows\System32\drivers\viaide.sys [2012-07-26 19184]
S0 vmbus;@%SystemRoot%\system32\vmbusres.dll,-1000;
C:\windows\System32\drivers\vmbus.sys [2012-07-26 137832]
S0 vsmraid;vsmraid; C:\windows\System32\drivers\vsmraid.sys [2012-07-26 164080]
S0 VSTXRAID;@vstxraid.inf,%Driver.DeviceDesc%;VIA StorX Storage Controller
Windows Driver; C:\windows\System32\drivers\vstxraid.sys [2012-07-26 322800]
S0 Wd;@wd.inf,%WdServiceDisplayName%;Microsoft Watchdog Timer Driver;
C:\windows\System32\drivers\wd.sys [2012-07-26 23792]
S1 dam;@%SystemRoot%\system32\drivers\dam.sys,-100;
C:\windows\system32\drivers\dam.sys [2012-10-11 58088]
S3 1394ohci;@1394.inf,%PCI\CC_0C0010.DeviceDesc%;1394 OHCI Compliant Host
Controller; C:\windows\System32\drivers\1394ohci.sys [2012-07-26 226304]
S3 acpipagr;@acpipagr.inf,%SvcDesc%;ACPI Processor Aggregator Driver;
C:\windows\System32\drivers\acpipagr.sys [2012-07-26 10240]
S3 AcpiPmi;@acpipmi.inf,%AcpiPmi.SvcDesc%;ACPI Power Meter Driver;
C:\windows\System32\drivers\acpipmi.sys [2012-07-26 12288]
S3 acpitime;@acpitime.inf,%AcpiTime.SvcDesc%;ACPI Wake Alarm Driver;
C:\windows\System32\drivers\acpitime.sys [2012-07-26 10752]
S3 AmdK8;@cpu.inf,%AmdK8.SvcDesc%;AMD K8 Processor Driver;
C:\windows\System32\drivers\amdk8.sys [2012-11-06 90624]
S3 AppID;@%systemroot%\system32\appidsvc.dll,-102;
C:\windows\system32\drivers\appid.sys [2012-07-26 79360]
S3 AsyncMac;@%systemroot%\system32\rascfg.dll,-32000;
C:\windows\system32\DRIVERS\asyncmac.sys [2012-07-26 26624]
S3 AthBTPort;@oem13.inf,%BTHSUPPORT.SvcDesc%;Qualcomm Atheros Virtual Bluetooth
Class; C:\windows\system32\DRIVERS\btath_flt.sys [2012-09-30 88728]
S3 BTATH_A2DP;@oem12.inf,%BTATH_A2DP.SvcDesc%;Bluetooth A2DP Audio Driver;
C:\windows\system32\drivers\btath_a2dp.sys [2012-09-30 344216]

S3 btath_avdt;@oem12.inf,%btath_avdt.SvcDesc%;Qualcomm Atheros Bluetooth AVDT Service; C:\windows\system32\drivers\btath_avdt.sys [2012-09-30 114840]
S3 BTATH_HCRP;@oem15.inf,%BTATH_HCRP.SvcDesc%;Bluetooth HCRP Server driver; C:\windows\System32\drivers\btath_hcrp.sys [2012-09-30 178840]
S3 BTATH_LWFLT;@oem16.inf,%BTATH_LWFLT%;Bluetooth LWFLT Device; C:\windows\system32\DRIVERS\btath_lwflt.sys [2012-09-30 76952]
S3 BTATH_RCP;@oem18.inf,%BTATH_RCP%;Bluetooth AVRCP Device; C:\windows\System32\drivers\btath_rcp.sys [2012-09-30 135832]
S3 BtFilter;BtFilter; C:\windows\system32\DRIVERS\btfilter.sys [2012-09-30 575128]
S3 BthAvrcpTg;@bthaudhid.inf,%BthAvrcpTg_SvcDesc%;Bluetooth Audio/Video Remote Control HID; C:\windows\System32\drivers\BthAvrcpTg.sys [2013-06-01 37632]
S3 BthEnum;@bth.inf,%BthEnum.SVCDESC%;Bluetooth Enumerator Service; C:\windows\System32\drivers\BthEnum.sys [2013-01-09 51712]
S3 BthHFEnum;@bthhfenum.inf,%BthHFEnum.SVCDESC%;Bluetooth Hands-Free Audio and Call Control HID Enumerator; C:\windows\System32\drivers\bthhfenum.sys [2012-07-26 51200]
S3 bthhfhid;@bthaudhid.inf,%BthAudioHFHid.SVCDESC%;Bluetooth Hands-Free Call Control HID; C:\windows\System32\drivers\BthHFHid.sys [2012-11-27 29952]
S3 BthLEEnum;@bthleenum.inf,%BthLEEnum.SVCDESC%;Bluetooth Low Energy Driver; C:\windows\system32\DRIVERS\BthLEEnum.sys [2012-07-26 202752]
S3 BTHMODEM;@bthspp.inf,%BthSerial.DisplayName%;Bluetooth Serial Communications Driver; C:\windows\System32\drivers\bthmodem.sys [2012-07-26 65536]
S3 BthPan;@bthpan.inf,%BthPan.DisplayName%;Bluetooth Device (Personal Area Network); C:\windows\system32\DRIVERS\bthpan.sys [2012-07-26 119808]
S3 BTHPORT;@bth.inf,%BTHPORT.SvcDesc%;Ovladač portu Bluetooth; C:\windows\System32\Drivers\BTHport.sys [2013-03-01 1175040]
S3 BTHUSB;@bth.inf,%BTHUSB.SvcDesc%;Ovladač rozhraní USB radiostanice Bluetooth; C:\windows\System32\Drivers\BTHUSB.sys [2013-01-09 74752]
S3 circlass;@circlass.inf,%circlass.SVCDESC%;Consumer IR Devices; C:\windows\System32\drivers\circlass.sys [2012-07-26 45056]
S3 dmvsc;dmvsc; C:\windows\System32\drivers\dmvsc.sys [2012-07-26 33280]
S3 drmkaud;@wdmaudio.inf,%drmkaud.SvcDesc%;Microsoft Trusted Audio Drivers; C:\windows\system32\drivers\drmkaud.sys [2012-10-11 5632]
S3 e1iexpress;@net1ic64.inf,%E1IExpress.Service.DispName%;Intel(R) PRO/1000 PCI Express Network Connection Driver I; C:\windows\system32\DRIVERS\e1i63x64.sys [2012-06-02 333824]
S3 ErrDev;@errdev.inf,%ERRDEV.SvcDesc%;Microsoft Hardware Error Device Driver; C:\windows\System32\drivers\errdev.sys [2012-07-26 10240]
S3 exfat;exFAT File System Driver; C:\windows\system32\drivers\exfat.sys [2012-07-26 194560]
S3 fdc;@fdc.inf,%fdc_ServiceDesc%;Floppy Disk Controller Driver; C:\windows\System32\drivers\fdc.sys [2012-07-26 30720]
S3 Filetrace;@%SystemRoot%\system32\drivers\filetrace.sys,-10001; C:\windows\system32\drivers\filetrace.sys [2012-07-26 34816]
S3 flpydisk;@flpydisk.inf,%floppy_ServiceDesc%;Floppy Disk Driver; C:\windows\System32\drivers\flpydisk.sys [2012-07-26 24576]
S3 FsDepends;@%SystemRoot%\system32\drivers\fsdepends.sys,-10001; C:\windows\System32\drivers\FsDepends.sys [2012-07-26 57584]
S3 FxPPM;@cpu.inf,%FxPPM.SvcDesc%;Power Framework Processor Driver; C:\windows\System32\drivers\fxppm.sys [2012-11-06 22528]
S3 gencounter;@wgencounter.inf,%GenCounter.SVCDESC%;Microsoft Hyper-V Generation Counter; C:\windows\System32\drivers\vmgencounter.sys [2012-07-26 12288]
S3 GPIOClx0101;Microsoft GPIO Class Extension Driver; C:\windows\System32\Drivers\msgpioclx.sys [2012-09-20 120040]
S3 HdAudAddService;@hdaudio.inf,%UAAFunctionDriverForHdAudio.SvcDesc%;Microsoft 1.1 UAA Function Driver for High Definition Audio Service; C:\windows\system32\drivers\HdAudio.sys [2013-01-09 341504]
S3 HidBatt;@hidbatt.inf,%HidBatt.SvcDesc%;HID UPS Battery Driver; C:\windows\System32\drivers\HidBatt.sys [2012-07-26 27136]
S3 HidBth;@hidbth.inf,%HIDBTH.SvcDesc%;Microsoft Bluetooth HID Miniport; C:\windows\System32\drivers\hidbth.sys [2013-04-09 95744]
S3 hidi2c;@hidi2c.inf,%hidi2c.SVCDESC%;Microsoft I2C HID Miniport Driver; C:\windows\System32\drivers\hidi2c.sys [2012-11-20 39936]
S3 HidIr;@hidir.inf,%HIDIR.SvcDesc%;Microsoft Infrared HID Driver; C:\windows\System32\drivers\hidir.sys [2012-07-26 46080]
S3 hyperkbd;hyperkbd; C:\windows\System32\drivers\hyperkbd.sys [2012-07-26 11776]

S3 HyperVideo;HyperVideo; C:\windows\system32\DRIVERS\HyperVideo.sys [2012-07-26
24576]
S3 igfx;igfx; C:\windows\system32\DRIVERS\igdkmd64.sys [2012-06-24 15283200]
S3 intelppm;@cpu.inf,%IntelPPM.SvcDesc%;Intel Processor Driver;
C:\windows\System32\drivers\intelppm.sys [2012-11-06 89088]
S3 IpFilterDriver;@%systemroot%\system32\rascfg.dll,-32013;
C:\windows\system32\DRIVERS\ipfltdrv.sys [2012-07-26 89088]
S3 IPMIDRV;IPMIDRV; C:\windows\System32\drivers\IPMIDrv.sys [2012-07-26 78336]
S3 IPNAT;IP Network Address Translator; C:\windows\System32\drivers\ipnat.sys
[2012-07-26 145920]
S3 IRENUM;@%SystemRoot%\system32\drivers\irenum.sys,-100;
C:\windows\system32\drivers\irenum.sys [2012-07-26 17920]
S3 iScsiPrt;@iscsi.inf,%iScsiPortName%;iScsiPort Driver;
C:\windows\System32\drivers\msiscsi.sys [2012-11-06 277736]
S3 kbdhid;@keyboard.inf,%KBDHID.SvcDesc%;Keyboard HID Driver;
C:\windows\System32\drivers\kbdhid.sys [2012-07-26 29184]
S3 Modem;Modem; C:\windows\system32\drivers\modem.sys [2012-07-26 40448]
S3 MRxDAV;@%systemroot%\system32\webclnt.dll,-104;
C:\windows\system32\drivers\mrxdav.sys [2012-07-26 141312]
S3 MsBridge;@%SystemRoot%\system32\bridgeres.dll,-1;
C:\windows\system32\DRIVERS\bridge.sys [2012-07-26 129536]
S3 msgpiowin32;@msgpiowin32.inf,%GPIO.SvcDesc%;GPIO Buttons Driver;
C:\windows\System32\drivers\msgpiowin32.sys [2013-01-10 28904]
S3 mshidkmdf;@%SystemRoot%\system32\drivers\mshidkmdf.sys,-100;
C:\windows\System32\drivers\mshidkmdf.sys [2012-07-26 8704]
S3 MSKSSRV;@ksfilter.inf,%MSKSSRV.DeviceDesc%;Microsoft Streaming Service Proxy;
C:\windows\system32\drivers\MSKSSRV.sys [2012-07-26 11008]
S3 MsLldp;@C:\Windows\system32\DRIVERS\mslldp.sys,-200;
C:\windows\system32\DRIVERS\mslldp.sys [2012-07-26 68608]
S3 MSPCLOCK;@ksfilter.inf,%MSPCLOCK.DeviceDesc%;Microsoft Streaming Clock Proxy;
C:\windows\system32\drivers\MSPCLOCK.sys [2012-07-26 7168]
S3 MSPQM;@ksfilter.inf,%MSPQM.DeviceDesc%;Microsoft Streaming Quality Manager
Proxy; C:\windows\system32\drivers\MSPQM.sys [2012-07-26 6912]
S3 MsRPC;MsRPC; C:\windows\system32\drivers\MsRPC.sys [2012-07-26 390896]
S3 MSTEE;@ksfilter.inf,%MSTEE.DeviceDesc%;Microsoft Streaming Tee/Sink-to-Sink
Converter; C:\windows\system32\drivers\MSTEE.sys [2012-07-26 8192]
S3 MTConfig;@mtconfig.inf,%MTConfig.SVCDESC%;Microsoft Input Configuration
Driver; C:\windows\System32\drivers\MTConfig.sys [2012-07-26 14848]
S3 NdisCap;@%SystemRoot%\System32\drivers\ndiscap.sys,-5000;
C:\windows\system32\DRIVERS\ndiscap.sys [2012-07-26 46592]
S3 NdisImPlatform;@%SystemRoot%\System32\drivers\ndisimplatform.sys,-501;
C:\windows\system32\DRIVERS\NdisImPlatform.sys [2012-07-26 126464]
S3 NDISWANLEGACY;@%systemroot%\system32\rascfg.dll,-32014;
C:\windows\system32\DRIVERS\ndiswan.sys [2012-07-26 174080]
S3 NETwNs64;@netwns64.inf,___ %NIC_Service_DispName_WIN7_64%;___ Intel(R)
Wireless WiFi Link 5000 Series Adapter Driver for Windows 7 - 64 Bit;
C:\windows\system32\DRIVERS\NETwNs64.sys [2012-06-02 8604672]
S3 Parport;@msports.inf,%Parport.SVCDESC%;Parallel port driver;
C:\windows\System32\drivers\parport.sys [2012-07-26 105984]
S3 Processor;@cpu.inf,%Processor.SvcDesc%;Processor Driver;
C:\windows\System32\drivers\processr.sys [2012-11-06 87552]
S3 QWAVEdrv;@%SystemRoot%\system32\drivers\qwavedrv.sys,-1;
C:\windows\system32\drivers\qwavedrv.sys [2012-07-26 46592]
S3 RasAcd;Remote Access Auto Connection Driver;
C:\windows\System32\DRIVERS\rasacd.sys [2012-07-26 16384]
S3 RDPDR;@%SystemRoot%\System32\DRIVERS\rdpdr.sys,-100;
C:\windows\System32\drivers\rdpdr.sys [2012-07-26 179712]
S3 RdpVideoMiniport;Remote Desktop Video Miniport Driver;
C:\windows\System32\drivers\rdpvideominiport.sys [2012-10-12 27880]
S3 RDPWD;RDP Winstation Driver; C:\windows\system32\drivers\RDPWD.sys
[2012-07-26 208384]
S3 RFCOMM;@tdibth.inf,%RFCOMM.DisplayName%;Bluetooth Device (RFCOMM Protocol
TDI); C:\windows\System32\drivers\rfcomm.sys [2013-03-01 156672]
S3 RSUSBVSTOR;@oem4.inf,%RSUSBVSTOR.SvcDesc%;RtsUVStor.Sys Realtek USB Card
Reader; C:\windows\System32\Drivers\RtsUVStor.sys [2012-06-15 315536]
S3 s3cap;s3cap; C:\windows\System32\drivers\vms3cap.sys [2012-07-26 7168]
S3 scfilter;@%SystemRoot%\System32\drivers\scfilter.sys,-11;
C:\windows\System32\DRIVERS\scfilter.sys [2012-07-26 36864]

S3 sdbus;sdbus; C:\windows\System32\drivers\sdbus.sys [2013-06-01 194816]
S3 sdstor;@sdstor.inf,%sdstor_ServiceDesc%;SD Storage Port Driver;
C:\windows\System32\drivers\sdstor.sys [2012-10-11 56552]
S3 SerCx;Serial UART Support Library; C:\windows\system32\drivers\SerCx.sys
[2012-07-26 62976]
S3 Serenum;@msports.inf,%Serenum.SVCDESC%;Serenum Filter Driver;
C:\windows\System32\drivers\serenum.sys [2012-07-26 23040]
S3 Serial;@msports.inf,%Serial.SVCDESC%;Serial port driver;
C:\windows\System32\drivers\serial.sys [2012-07-26 76800]
S3 sermouse;@msmouse.inf,%sermouse.SvcDesc%;Serial Mouse Driver;
C:\windows\System32\drivers\sermouse.sys [2012-07-26 27136]
S3 sfloppy;@flpydisk.inf,%sfloppy_devdesc%;High-Capacity Floppy Disk Drive;
C:\windows\System32\drivers\sfloppy.sys [2012-07-26 16896]
S3 SpbCx;Simple Peripheral Bus Support Library;
C:\windows\system32\drivers\SpbCx.sys [2012-07-26 59392]
S3 TCPIP6;@netip6.inf,%MS_TCPIP6.TCPIP6.ServiceDescription%;Microsoft IPv6
Protocol Driver; C:\windows\system32\DRIVERS\tcpip.sys [2013-06-01 2233600]
S3 terminpt;@termmou.inf,%TermInpt.SVCDESC%;Microsoft Remote Desktop Input
Driver; C:\windows\System32\drivers\terminpt.sys [2012-07-26 36592]
S3 TPM;@tpm.inf,%TPM%;TPM; C:\windows\system32\drivers\tpm.sys [2013-03-02
148712]
S3 TsUsbFlt;TsUsbFlt; C:\windows\system32\drivers\tsusbflt.sys [2012-07-26
57344]
S3 TsUsbGD;@tsgenericusbdriver.inf,%TsUsbGD.DeviceDesc.Generic%;Remote Desktop
Generic USB Device; C:\windows\System32\drivers\TsUsbGD.sys [2012-07-26 30208]
S3 UASPStor;@uaspstor.inf,%UASPortName%;USB Attached SCSI (UAS) Driver;
C:\windows\System32\drivers\uaspstor.sys [2012-07-26 97008]
S3 UmPass;@umpass.inf,%UmPass.SVCDESC%;Microsoft UMPass Driver;
C:\windows\System32\drivers\umpass.sys [2012-07-26 11776]
S3 usbcir;@usbcir.inf,%usbcir.SVCDESC%;eHome Infrared Receiver (USBCIR);
C:\windows\System32\drivers\usbcir.sys [2012-07-26 99328]
S3 usbprint;@usbprint.inf,%USBPRINT.SvcDesc%;Microsoft USB PRINTER Class;
C:\windows\System32\drivers\usbprint.sys [2012-07-26 25600]
S3 usbuhci;@usbport.inf,%UHCIMP.SvcDesc%;Microsoft USB Universal Host Controller
Miniport Driver; C:\windows\System32\drivers\usbuhci.sys [2012-09-20 32256]
S3 usbvideo;@usbvideo.inf,%USBVideo.SvcDesc%;USB Video Device (WDM);
C:\windows\System32\Drivers\usbvideo.sys [2012-09-20 210304]
S3 VerifierExt;@%SystemRoot%\system32\drivers\VerifierExt.sys,-1000;
C:\windows\system32\drivers\VerifierExt.sys [2012-07-26 106224]
S3 vhdmp;vhdmp; C:\windows\System32\drivers\vhdmp.sys [2013-03-02 495336]
S3 VMBusHID;VMBusHID; C:\windows\System32\drivers\VMBusHID.sys [2012-07-26
22144]
S3 vpci;@wvpci.inf,%vpci.SVCDESC%;Microsoft Hyper-V Virtual PCI Bus;
C:\windows\System32\drivers\vpci.sys [2012-07-26 67824]
S3 WacomPen;@hiddigi.inf,%WacomPen.SVCDESC%;Wacom Serial Pen HID Driver;
C:\windows\System32\drivers\wacompen.sys [2012-07-26 27008]
S3 Wanarp;@%systemroot%\system32\rascfg.dll,-32011;
C:\windows\system32\DRIVERS\wanarp.sys [2013-04-09 83456]
S3 WdBoot;@%ProgramFiles%\Windows Defender\MpAsDesc.dll,-390;
C:\windows\system32\drivers\WdBoot.sys [2013-01-29 35232]
S3 WdFilter;@%ProgramFiles%\Windows Defender\MpAsDesc.dll,-330;
C:\windows\system32\drivers\WdFilter.sys [2013-01-29 230904]
S3 WIMMount;WIMMount; C:\windows\system32\drivers\wimmount.sys [2012-07-26
33520]
S3 WinUsb;@wpdmtp.inf,%WinUsb.SvcDesc%;WinUsb;
C:\windows\system32\DRIVERS\WinUsb.sys [2012-07-26 57344]
S3 WmiAcpi;@wmiacpi.inf,%WMIMAP.SvcDesc%;Microsoft Windows Management Interface
for ACPI; C:\windows\System32\drivers\wmiacpi.sys [2012-07-26 17408]
S3 wpcfltr;Family Safety Filter Driver; C:\windows\system32\DRIVERS\wpcfltr.sys
[2012-07-26 45056]
S3 wsvd;wsvd; C:\windows\system32\DRIVERS\wsvd.sys [2012-06-14 102376]
S4 cdfs;CD/DVD File System Reader; C:\windows\system32\DRIVERS\cdfs.sys
[2012-07-26 108544]
S4 udfs;udfs; C:\windows\system32\DRIVERS\udfs.sys [2012-07-26 321024]
S4 ws2ifsl;@%systemroot%\System32\drivers\ws2ifsl.sys,-1000;
C:\windows\system32\drivers\ws2ifsl.sys [2012-09-20 22528]

======List of services (R=Running, S=Stopped, 0=Boot, 1=System, 2=Auto,

3=Demand, 4=Disabled)======

R2 AMD External Events Utility;AMD External Events Utility;
C:\windows\system32\atiesrxx.exe [2012-08-01 239616]
R2 AMD FUEL Service;AMD FUEL Service; C:\Program Files\ATI
Technologies\ATI.ACE\Fuel\Fuel.Service.exe [2012-08-06 361984]
R2 AtherosSvc;AtherosSvc; C:\Program Files (x86)\Bluetooth
Suite\adminservice.exe [2012-09-30 220288]
R2 AudioEndpointBuilder;@%SystemRoot%\system32\AudioEndpointBuilder.dll,-204;
C:\windows\System32\svchost.exe [2012-09-20 29696]
R2 Audiosrv;@%SystemRoot%\system32\audiosrv.dll,-200;
C:\windows\System32\svchost.exe [2012-09-20 29696]
R2 BFE;@%SystemRoot%\system32\bfe.dll,-1001; C:\windows\system32\svchost.exe
[2012-09-20 29696]
R2 BrokerInfrastructure;@%windir%\system32\bisrv.dll,-100;
C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 CryptSvc;@%SystemRoot%\system32\cryptsvc.dll,-1001;
C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 CxAudMsg;@C:\windows\system32\CxAudMsg64.exe,-100;
C:\windows\system32\CxAudMsg64.exe [2012-06-08 201376]
R2 DcomLaunch;@combase.dll,-5012; C:\windows\system32\svchost.exe [2012-09-20
29696]
R2 Dhcp;@%SystemRoot%\system32\dhcpcore.dll,-100;
C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 Dnscache;@%SystemRoot%\System32\dnsapi.dll,-101;
C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 DPS;@%systemroot%\system32\dps.dll,-500; C:\windows\System32\svchost.exe
[2012-09-20 29696]
R2 ETDService;Elan Service; C:\Program Files\Elantech\ETDService.exe [2012-09-05
83968]
R2 EventLog;@%SystemRoot%\system32\wevtsvc.dll,-200;
C:\windows\System32\svchost.exe [2012-09-20 29696]
R2 EventSystem;@comres.dll,-2450; C:\windows\system32\svchost.exe [2012-09-20
29696]
R2 FontCache;@%systemroot%\system32\FntCache.dll,-100;
C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 gpsvc;@gpapi.dll,-112; C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 IKEEXT;@%SystemRoot%\system32\ikeext.dll,-501;
C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 iphlpsvc;@%SystemRoot%\system32\iphlpsvc.dll,-500;
C:\windows\System32\svchost.exe [2012-09-20 29696]
R2 LanmanServer;@%systemroot%\system32\srvsvc.dll,-100;
C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 LanmanWorkstation;@%systemroot%\system32\wkssvc.dll,-100;
C:\windows\System32\svchost.exe [2012-09-20 29696]
R2 lmhosts;@%SystemRoot%\system32\lmhsvc.dll,-101;
C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 LSM;@%windir%\system32\lsm.dll,-1001; C:\windows\system32\svchost.exe
[2012-09-20 29696]
R2 MMCSS;@%systemroot%\system32\mmcss.dll,-100; C:\windows\system32\svchost.exe
[2012-09-20 29696]
R2 MpsSvc;@%SystemRoot%\system32\FirewallAPI.dll,-23090;
C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 NlaSvc;@%SystemRoot%\System32\nlasvc.dll,-1; C:\windows\System32\svchost.exe
[2012-09-20 29696]
R2 nsi;@%SystemRoot%\system32\nsisvc.dll,-200; C:\windows\system32\svchost.exe
[2012-09-20 29696]
R2 PcaSvc;@%SystemRoot%\system32\pcasvc.dll,-1; C:\windows\system32\svchost.exe
[2012-09-20 29696]
R2 Power;@%SystemRoot%\system32\umpo.dll,-100; C:\windows\system32\svchost.exe
[2012-09-20 29696]
R2 ProfSvc;@%systemroot%\system32\profsvc.dll,-300;
C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 RpcEptMapper;@%windir%\system32\RpcEpMap.dll,-1001;
C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 RpcSs;@combase.dll,-5010; C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 SamSs;@%SystemRoot%\system32\samsrv.dll,-1; C:\windows\system32\lsass.exe
[2012-09-20 35840]

R2 SENS;@%SystemRoot%\system32\Sens.dll,-200; C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 ShellHWDetection;@%SystemRoot%\System32\shsvcs.dll,-12288; C:\windows\System32\svchost.exe [2012-09-20 29696]
R2 Schedule;@%SystemRoot%\system32\schedsvc.dll,-100; C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 Spooler;@%systemroot%\system32\spoolsv.exe,-1; C:\windows\System32\spoolsv.exe [2012-07-26 769024]
R2 stisvc;@%SystemRoot%\system32\wiaservc.dll,-9; C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 SysMain;@%SystemRoot%\system32\sysmain.dll,-1000; C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 Themes;@%SystemRoot%\System32\themeservice.dll,-8192; C:\windows\System32\svchost.exe [2012-09-20 29696]
R2 TrkWks;@%SystemRoot%\system32\trkwks.dll,-1; C:\windows\System32\svchost.exe [2012-09-20 29696]
R2 Wcmsvc;@%SystemRoot%\System32\wcmsvc.dll,-4097; C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 Winmgmt;@%Systemroot%\system32\wbem\wmisvc.dll,-205; C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 WlanSvc;@%SystemRoot%\System32\wlansvc.dll,-257; C:\windows\system32\svchost.exe [2012-09-20 29696]
R2 WSearch;@%systemroot%\system32\SearchIndexer.exe,-103; C:\windows\system32\SearchIndexer.exe [2013-04-09 816128]
R3 AeLookupSvc;@%SystemRoot%\system32\aelupsvc.dll,-1; C:\windows\system32\svchost.exe [2012-09-20 29696]
R3 Appinfo;@%systemroot%\system32\appinfo.dll,-100; C:\windows\system32\svchost.exe [2012-09-20 29696]
R3 DeviceAssociationService;@%SystemRoot%\system32\das.dll,-100; C:\windows\system32\svchost.exe [2012-09-20 29696]
R3 hidserv;@%SystemRoot%\System32\hidserv.dll,-101; C:\windows\system32\svchost.exe [2012-09-20 29696]
R3 netprofm;@%SystemRoot%\system32\netprofmsvc.dll,-202; C:\windows\System32\svchost.exe [2012-09-20 29696]
R3 PlugPlay;@%SystemRoot%\system32\umpnpmgr.dll,-200; C:\windows\system32\svchost.exe [2012-09-20 29696]
R3 SystemEventsBroker;@%windir%\system32\SystemEventsBrokerServer.dll,-1001; C:\windows\system32\svchost.exe [2012-09-20 29696]
R3 TimeBroker;@%windir%\system32\TimeBrokerServer.dll,-1001; C:\windows\system32\svchost.exe [2012-09-20 29696]
R3 WdiServiceHost;@%systemroot%\system32\wdi.dll,-502; C:\windows\System32\svchost.exe [2012-09-20 29696]
R3 WdiSystemHost;@%systemroot%\system32\wdi.dll,-500; C:\windows\System32\svchost.exe [2012-09-20 29696]
R3 WinHttpAutoProxySvc;@%SystemRoot%\system32\winhttp.dll,-100; C:\windows\system32\svchost.exe [2012-09-20 29696]
R3 WPDBusEnum;@%SystemRoot%\system32\wpdbusenum.dll,-100; C:\windows\system32\svchost.exe [2012-09-20 29696]
R3 wudfsvc;@%SystemRoot%\system32\wudfsvc.dll,-1000; C:\windows\system32\svchost.exe [2012-09-20 29696]
S2 BITS;@%SystemRoot%\system32\qmgr.dll,-1000; C:\windows\System32\svchost.exe [2012-09-20 29696]
S2 sppsvc;@%SystemRoot%\system32\sppsvc.exe,-101; C:\windows\system32\sppsvc.exe [2012-07-26 4881408]
S2 wscsvc;@%SystemRoot%\System32\wscsvc.dll,-200; C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 ALG;@%SystemRoot%\system32\Alg.exe,-112; C:\windows\System32\alg.exe [2012-07-26 94208]
S3 AllUserInstallAgent;@%SystemRoot%\System32\AUInstallAgent.dll,-101; C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 AppIDSvc;@%systemroot%\system32\appidsvc.dll,-100; C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 AxInstSV;@%SystemRoot%\system32\AxInstSV.dll,-103; C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 BDESVC;@%SystemRoot%\system32\bdesvc.dll,-100; C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 Browser;@%systemroot%\system32\browser.dll,-100; C:\windows\System32\svchost.exe [2012-09-20 29696]

S3 bthserv;@%SystemRoot%\System32\bthserv.dll,-101;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 CertPropSvc;@%SystemRoot%\System32\certprop.dll,-11;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 COMSysApp;@comres.dll,-947; C:\windows\system32\dllhost.exe [2012-07-26
10752]
S3 defragsvc;@%SystemRoot%\system32\defragsvc.dll,-101;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 DeviceInstall;@%SystemRoot%\system32\umpnpmgr.dll,-100;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 dot3svc;@%systemroot%\system32\dot3svc.dll,-1102;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 DsmSvc;@%SystemRoot%\system32\DeviceSetupManager.dll,-1000;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 Eaphost;@%systemroot%\system32\eapsvc.dll,-1; C:\windows\System32\svchost.exe
[2012-09-20 29696]
S3 EFS;@%SystemRoot%\system32\efssvc.dll,-100; C:\windows\System32\lsass.exe
[2012-09-20 35840]
S3 Fax;@%systemroot%\system32\fxsresm.dll,-118; C:\windows\system32\fxssvc.exe
[2012-07-26 669696]
S3 fdPHost;@%systemroot%\system32\fdPHost.dll,-100;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 FDResPub;@%systemroot%\system32\fdrespub.dll,-100;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 fhsvc;@%systemroot%\system32\fhsvc.dll,-101; C:\windows\system32\svchost.exe
[2012-09-20 29696]
S3 FontCache3.0.0.0;@%SystemRoot%\system32\PresentationHost.exe,-3309;
C:\windows\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe
[2012-07-26 43616]
S3 hkmsvc;@%SystemRoot%\system32\kmsvc.dll,-6; C:\windows\System32\svchost.exe
[2012-09-20 29696]
S3 HomeGroupListener;@%SystemRoot%\System32\ListSvc.dll,-100;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 HomeGroupProvider;@%SystemRoot%\System32\provsvc.dll,-100;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 KeyIso;@keyiso.dll,-100; C:\windows\system32\lsass.exe [2012-09-20 35840]
S3 KtmRm;@comres.dll,-2946; C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 lltdsvc;@%SystemRoot%\system32\lltdres.dll,-1;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 MSDTC;@comres.dll,-2797; C:\windows\System32\msdtc.exe [2012-07-26 144384]
S3 MSiSCSI;@%SystemRoot%\system32\iscsidsc.dll,-5000;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 msiserver;@%SystemRoot%\system32\msimsg.dll,-27;
C:\windows\system32\msiexec.exe [2012-07-26 124416]
S3 napagent;@%SystemRoot%\system32\qagentrt.dll,-6;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 NcaSvc;@%SystemRoot%\system32\ncasvc.dll,-3009;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 NcdAutoSetup;@%SystemRoot%\system32\NcdAutoSetup.dll,-100;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 Netlogon;@%SystemRoot%\System32\netlogon.dll,-102;
C:\windows\system32\lsass.exe [2012-09-20 35840]
S3 Netman;@%SystemRoot%\system32\netman.dll,-109;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 p2pimsvc;@%SystemRoot%\system32\pnrpsvc.dll,-8004;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 p2psvc;@%SystemRoot%\system32\p2psvc.dll,-8006;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 PerfHost;@%systemroot%\sysWow64\perfhost.exe,-2;
C:\windows\SysWow64\perfhost.exe [2012-07-26 20992]
S3 pla;@%systemroot%\system32\pla.dll,-500; C:\windows\System32\svchost.exe
[2012-09-20 29696]
S3 PNRPAutoReg;@%SystemRoot%\system32\pnrpauto.dll,-8002;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 PNRPsvc;@%SystemRoot%\system32\pnrpsvc.dll,-8000;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 PolicyAgent;@%SystemRoot%\System32\polstore.dll,-5010;
C:\windows\system32\svchost.exe [2012-09-20 29696]

S3 PrintNotify;@C:\Windows\system32\spool\DRIVERS\x64\3\PrintConfig.dll,-1;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 QWAVE;@%SystemRoot%\system32\qwave.dll,-1; C:\windows\system32\svchost.exe
[2012-09-20 29696]
S3 RasAuto;@%Systemroot%\system32\rasauto.dll,-200;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 RasMan;@%Systemroot%\system32\rasmans.dll,-200;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 RpcLocator;@%systemroot%\system32\Locator.exe,-2;
C:\windows\system32\locator.exe [2012-07-26 9728]
S3 SCPolicySvc;@%SystemRoot%\System32\certprop.dll,-13;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 SDRSVC;@%SystemRoot%\system32\sdrsvc.dll,-107;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 seclogon;@%SystemRoot%\system32\seclogon.dll,-7001;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 SensrSvc;@%SystemRoot%\System32\sensrsvc.dll,-1000;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 SessionEnv;@%SystemRoot%\System32\SessEnv.dll,-1026;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 SNMPTRAP;@%SystemRoot%\system32\snmptrap.exe,-3;
C:\windows\System32\snmptrap.exe [2012-07-26 14848]
S3 SSDPSRV;@%systemroot%\system32\ssdpsrv.dll,-100;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 SstpSvc;@%SystemRoot%\system32\sstpsvc.dll,-200;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 StorSvc;@%SystemRoot%\System32\StorSvc.dll,-100;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 svsvc;@%SystemRoot%\system32\svsvc.dll,-101; C:\windows\system32\svchost.exe
[2012-09-20 29696]
S3 swprv;@%SystemRoot%\System32\swprv.dll,-103; C:\windows\System32\svchost.exe
[2012-09-20 29696]
S3 TabletInputService;@%SystemRoot%\system32\TabSvc.dll,-100;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 TapiSrv;@%SystemRoot%\system32\tapisrv.dll,-10100;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 TermService;@%SystemRoot%\System32\termsrv.dll,-268;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 THREADORDER;@%systemroot%\system32\mmcss.dll,-102;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 TrustedInstaller;@%SystemRoot%\servicing\TrustedInstaller.exe,-100;
C:\windows\servicing\TrustedInstaller.exe [2013-05-16 98304]
S3 UIODetect;@%SystemRoot%\system32\uiodetect.exe,-101;
C:\windows\system32\UIODetect.exe [2012-07-26 40960]
S3 UmRdpService;@%SystemRoot%\system32\umrdp.dll,-1000;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 upnphost;@%systemroot%\system32\upnphost.dll,-213;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 VaultSvc;@%SystemRoot%\system32\vaultsvc.dll,-1003;
C:\windows\system32\lsass.exe [2012-09-20 35840]
S3 vds;@%SystemRoot%\system32\vds.exe,-100; C:\windows\System32\vds.exe
[2013-06-01 680960]
S3 vmickvpexchange;@%systemroot%\system32\vmicres.dll,-201;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 vmicrdv;@%systemroot%\system32\vmicres.dll,-601;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 vmicshutdown;@%systemroot%\system32\vmicres.dll,-301;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 vmictimesync;@%systemroot%\system32\vmicres.dll,-401;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 vmicvss;@%systemroot%\system32\vmicres.dll,-501;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 vmicheartbeat;@%systemroot%\system32\vmicres.dll,-101;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 VSS;@%systemroot%\system32\vssvc.exe,-102; C:\windows\system32\vssvc.exe
[2013-05-04 1483776]
S3 W32Time;@%SystemRoot%\system32\w32time.dll,-200;
C:\windows\system32\svchost.exe [2012-09-20 29696]

```
S3 wbengine;@%systemroot%\system32\wbengine.exe,-104;
C:\windows\system32\wbengine.exe [2012-07-26 1616896]
S3 WbioSrvc;@%systemroot%\system32\wbiosrvc.dll,-100;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 wcncsvc;@%SystemRoot%\system32\wcncsvc.dll,-3;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 WcsPlugInService;@%SystemRoot%\system32\WcsPlugInService.dll,-200;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 WebClient;@%systemroot%\system32\webclnt.dll,-100;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 Wecsvc;@%SystemRoot%\system32\wecsvc.dll,-200;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 wercplsupport;@%SystemRoot%\System32\wercplsupport.dll,-101;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 WerSvc;@%SystemRoot%\System32\wersvc.dll,-100;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 WiaRpc;@%SystemRoot%\system32\wiarpc.dll,-2; C:\windows\system32\svchost.exe
[2012-09-20 29696]
S3 WinDefend;@%ProgramFiles%\Windows Defender\MpAsDesc.dll,-310; C:\Program
Files\Windows Defender\MsMpEng.exe [2013-01-29 14920]
S3 WinRM;@%Systemroot%\system32\wsmsvc.dll,-101; C:\windows\System32\svchost.exe
[2012-09-20 29696]
S3 wlidsvc;@%SystemRoot%\system32\wlidsvc.dll,-100;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 wmiApSrv;@%Systemroot%\system32\wbem\wmiapsrv.exe,-110;
C:\windows\system32\wbem\WmiApSrv.exe [2012-07-26 198144]
S3 WMPNetworkSvc;@%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe,-101;
C:\Program Files\Windows Media Player\wmpnetwk.exe [2012-09-20 1314816]
S3 WPCSvc;@%SystemRoot%\system32\wpcsvc.dll,-100;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 WSService;@%SystemRoot%\system32\WSService.dll,-103;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S3 wuauserv;@%systemroot%\system32\wuaueng.dll,-105;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S3 WwanSvc;@%SystemRoot%\System32\wwansvc.dll,-257;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S4
NetTcpPortSharing;@%systemroot%\Microsoft.NET\Framework64\v4.0.30319\ServiceMode
lInstallRC.dll,-8201;
C:\windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe [2012-07-12
139696]
S4 RemoteAccess;@%Systemroot%\system32\mprdim.dll,-200;
C:\windows\System32\svchost.exe [2012-09-20 29696]
S4 RemoteRegistry;@regsvc.dll,-1; C:\windows\system32\svchost.exe [2012-09-20
29696]
S4 SCardSvr;@%SystemRoot%\System32\SCardSvr.dll,-1;
C:\windows\system32\svchost.exe [2012-09-20 29696]
S4 SharedAccess;@%SystemRoot%\system32\ipnathlp.dll,-106;
C:\windows\System32\svchost.exe [2012-09-20 29696]

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