```
Logfile of random's system information tool 1.10 (written by
random/random)
Run by ACER at 2016-09-20 12:33:15
Microsoft Windows 7 Home Premium  Service Pack 1
System drive C: has 255 GB (55%) free of 463 GB
Total RAM: 3948 MB (25% free)

Logfile of Trend Micro HijackThis v2.0.4
Scan saved at 12:33:22, on 20. 9. 2016
Platform: Windows 7 SP1 (WinNT 6.00.3505)
MSIE: Internet Explorer v11.0 (11.00.9600.18427)
Boot mode: Normal

Running processes:
C:\Program Files (x86)\Acer\clear.fi\MVP\clear.fiAgent.exe
C:\Program Files (x86)\Acer\clear.fi\MVP\.\Kernel\DMR\DMREngine.exe
C:\Program Files (x86)\Clarus\Samsung Drive Manager\ABRTMon.exe
C:\Program Files (x86)\NTI\Acer Backup Manager\BackupManagerTray.exe
C:\Program Files (x86)\Launch Manager\LManager.exe
C:\Program Files (x86)\Acer\clear.fi\Movie\clear.fiMovieService.exe
C:\Program Files (x86)\Canon\Solution Menu EX\CNSEMAIN.EXE
C:\Program Files (x86)\Clarus\Samsung Drive Manager\Drive Manager.exe
C:\Program Files (x86)\Launch Manager\LMworker.exe
C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe
C:\Program Files (x86)\Clarus\Samsung Drive Manager\SZDrvMon.exe
C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE
C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\BingApp.exe
C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\BingBar.exe
C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\BingSurrogate.exe
C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\BingSurrogate.exe
C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\BingSurrogate.exe
C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\BingSurrogate.exe
C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE
C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE
C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE
C:\Users\ACER\Desktop\adwcleaner_6.020.exe
C:\Program Files (x86)\Windows Media Player\wmplayer.exe
C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Program Files\trend micro\ACER.exe

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Default_Page_URL =
http://acer.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://start.icq.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
R1 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings,ProxyServer = cache34.ics.muni.cz:5555
R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName =
R3 - URLSearchHook: (no name) - {00000000-6E41-4FD3-8538-502F5495E5FC} -
(no file)
R3 - URLSearchHook: (no name) -  - (no file)
F2 - REG:system.ini: Shell=C:\PROGRA~3\z6oti.bat
F2 - REG:system.ini: UserInit=userinit.exe,
O2 - BHO: Lync Click to Call BHO - {31D09BA0-12F5-4CCE-BE8A-2923E76605DA}
- C:\Program Files (x86)\Microsoft Office\root\Office16\OCHelper.dll
O2 - BHO: Java(tm) Plug-In SSV Helper - {761497BB-D6F0-462C-B6EB-
D4DAF1D92D43} - C:\Program Files (x86)\Java\jre1.8.0_71\bin\ssv.dll
O2 - BHO: Windows Live ID Sign-in Helper - {9030D464-4C02-4ABF-8ECC-
5164760863C6} - C:\Program Files (x86)\Common Files\Microsoft
Shared\Windows Live\WindowsLiveLogin.dll
O2 - BHO: STATISTICA Browser Helper - {990A8747-93BF-4EF7-B72E-
94A6884B98C2} - C:\Program Files\StatSoft\STATISTICA
12\Support\StaBHO.dll
O2 - BHO: URLRedirectionBHO - {B4F3A835-0E21-4959-BA22-42B3008E02FF} -
C:\Program Files (x86)\Microsoft Office\root\Office16\URLREDIR.DLL
O2 - BHO: Microsoft OneDrive for Business Browser Helper - {D0498E0A-
45B7-42AE-A9AA-ABA463DBD3BF} - C:\Program Files (x86)\Microsoft
Office\root\Office16\GROOVEEX.DLL
O2 - BHO: Bing Bar Helper - {d2ce3e00-f94a-4740-988e-03dc2f38c34f} -
C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\BingExt.dll
O2 - BHO: Java(tm) Plug-In 2 SSV Helper - {DBC80044-A445-435b-BC74-
9C25C1C588A9} - C:\Program Files (x86)\Java\jre1.8.0_71\bin\jp2ssv.dll
O3 - Toolbar: Bing Bar - {8dcb7100-df86-4384-8842-8fa844297b3f} -
C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\BingExt.dll
O4 - HKLM\..\Run: [BackupManagerTray] "C:\Program Files (x86)\NTI\Acer
Backup Manager\BackupManagerTray.exe" -h -k
O4 - HKLM\..\Run: [LManager] C:\Program Files (x86)\Launch
Manager\LManager.exe
O4 - HKLM\..\Run: [SuiteTray] "C:\Program Files (x86)\EgisTec
MyWinLockerSuite\x86\SuiteTray.exe"
O4 - HKLM\..\Run: [ArcadeMovieService] "C:\Program Files
(x86)\Acer\clear.fi\Movie\clear.fiMovieService.exe"
O4 - HKLM\..\Run: [Norton Online Backup] C:\Program Files
(x86)\Symantec\Norton Online Backup\NOBuClient.exe
O4 - HKLM\..\Run: [KurupiraNet] "C:\Program Files
(x86)\Kurupira\WebFilter\kurupirawf.exe"
```

```
O4 - HKLM\..\Run: [CanonSolutionMenuEx] C:\Program Files
(x86)\Canon\Solution Menu EX\CNSEMAIN.EXE /logon
O4 - HKLM\..\Run: [Clarus Drive Manager] C:\Program Files
(x86)\Clarus\Samsung Drive Manager\Drive Manager.exe -Hide
O4 - HKLM\..\Run: [SunJavaUpdateSched] "C:\Program Files (x86)\Common
Files\Java\Java Update\jusched.exe"
O4 - HKCU\..\Run: [Sidebar] C:\Program Files\Windows Sidebar\sidebar.exe
/autoRun
O4 - HKCU\..\Run: [ctfmon32.exe] C:\PROGRA~3\rundll32.exe
C:\PROGRA~3\ito6z.dat,XFG00
O4 - HKCU\..\Run: [KurupiraNet] "C:\Program Files
(x86)\Kurupira\WebFilter\kurupirawf.exe"
O4 - HKCU\..\Run: [RESTART_STICKY_NOTES] C:\Windows\System32\StikyNot.exe
O4 - HKCU\..\Run: [Skype] "C:\Program Files (x86)\Skype\Phone\Skype.exe"
/minimized /regrun
O4 - HKUS\S-1-5-19\..\Run: [Sidebar] %ProgramFiles%\Windows
Sidebar\Sidebar.exe /autoRun (User 'LOCAL SERVICE')
O4 - HKUS\S-1-5-19\..\RunOnce: [mctadmin]
C:\Windows\System32\mctadmin.exe (User 'LOCAL SERVICE')
O4 - HKUS\S-1-5-20\..\Run: [Sidebar] %ProgramFiles%\Windows
Sidebar\Sidebar.exe /autoRun (User 'NETWORK SERVICE')
O4 - HKUS\S-1-5-20\..\RunOnce: [mctadmin]
C:\Windows\System32\mctadmin.exe (User 'NETWORK SERVICE')
O4 - Global Startup: Samsung Drive Manager Real-Time.lnk = ?
O4 - Global Startup: Virtual Router Manager.lnk = ?
O8 - Extra context menu item: Add to Google Photos Screensa&ver -
res://C:\Windows\system32\GPhotos.scr/200
O8 - Extra context menu item: E&xport to Microsoft Excel -
res://C:\Program Files (x86)\Microsoft
Office\Root\Office16\EXCEL.EXE/3000
O8 - Extra context menu item: Se&nd to OneNote - res://C:\Program Files
(x86)\Microsoft Office\Root\Office16\ONBttnIE.dll/105
O9 - Extra button: @C:\Program Files (x86)\Windows
Live\Writer\WindowsLiveWriterShortcuts.dll,-1004 - {219C3416-8CB2-491a-
A3C7-D9FCDDC9D600} - C:\Program Files (x86)\Windows
Live\Writer\WriterBrowserExtension.dll
O9 - Extra 'Tools' menuitem: @C:\Program Files (x86)\Windows
Live\Writer\WindowsLiveWriterShortcuts.dll,-1003 - {219C3416-8CB2-491a-
A3C7-D9FCDDC9D600} - C:\Program Files (x86)\Windows
Live\Writer\WriterBrowserExtension.dll
O9 - Extra button: Send to OneNote - {2670000A-7350-4f3c-8081-
5663EE0C6C49} - C:\Program Files (x86)\Microsoft
Office\root\Office16\ONBttnIE.dll
O9 - Extra 'Tools' menuitem: Se&nd to OneNote - {2670000A-7350-4f3c-8081-
5663EE0C6C49} - C:\Program Files (x86)\Microsoft
Office\root\Office16\ONBttnIE.dll
O9 - Extra button: Lync Click to Call - {31D09BA0-12F5-4CCE-BE8A-
2923E76605DA} - C:\Program Files (x86)\Microsoft
Office\root\Office16\OCHelper.dll
O9 - Extra 'Tools' menuitem: Lync Click to Call - {31D09BA0-12F5-4CCE-
BE8A-2923E76605DA} - C:\Program Files (x86)\Microsoft
Office\root\Office16\OCHelper.dll
O9 - Extra button: ICQ7.5 - {7578ADEA-D65F-4C89-A249-B1C88B6FFC20} -
C:\Program Files (x86)\ICQ7.5\ICQ.exe
O9 - Extra 'Tools' menuitem: ICQ7.5 - {7578ADEA-D65F-4C89-A249-
B1C88B6FFC20} - C:\Program Files (x86)\ICQ7.5\ICQ.exe
```

O9 - Extra button: OneNote Lin&ked Notes - {789FE86F-6FC4-46A1-9849-EDE0DB0C95CA} - C:\Program Files (x86)\Microsoft Office\root\Office16\ONBttnIELinkedNotes.dll
O9 - Extra 'Tools' menuitem: OneNote Lin&ked Notes - {789FE86F-6FC4-46A1-9849-EDE0DB0C95CA} - C:\Program Files (x86)\Microsoft Office\root\Office16\ONBttnIELinkedNotes.dll
O9 - Extra button: @C:\Program Files (x86)\Evernote\Evernote\Resource.dll,-101 - {A95fe080-8f5d-11d2-a20b-00aa003c157a} - res://C:\Program Files (x86)\Evernote\Evernote\EvernoteIE.dll/204 (file missing)
O9 - Extra 'Tools' menuitem: @C:\Program Files (x86)\Evernote\Evernote\Resource.dll,-101 - {A95fe080-8f5d-11d2-a20b-00aa003c157a} - res://C:\Program Files (x86)\Evernote\Evernote\EvernoteIE.dll/204 (file missing)
O10 - Unknown file in Winsock LSP: c:\program files (x86)\common files\microsoft shared\windows live\wlidnsp.dll
O10 - Unknown file in Winsock LSP: c:\program files (x86)\common files\microsoft shared\windows live\wlidnsp.dll
O10 - Unknown file in Winsock LSP: c:\windows\system32\svcproxy.dll
O10 - Unknown file in Winsock LSP: c:\windows\system32\svcproxy.dll
O10 - Unknown file in Winsock LSP: c:\windows\system32\svcproxy.dll
O10 - Unknown file in Winsock LSP: c:\windows\system32\svcproxy.dll
O10 - Unknown file in Winsock LSP: c:\windows\system32\svcproxy.dll
O11 - Options group: [ACCELERATED_GRAPHICS] Accelerated graphics
O15 - Trusted Zone: http://help.eset.com (HKLM)
O15 - ESC Trusted Zone: http://help.eset.com (HKLM)
O18 - Protocol: mso-minsb-roaming.16 - {83C25742-A9F7-49FB-9138-434302C88D07} - C:\Program Files (x86)\Microsoft Office\root\Office16\MSOSB.DLL
O18 - Protocol: mso-minsb.16 - {42089D2D-912D-4018-9087-2B87803E93FB} - C:\Program Files (x86)\Microsoft Office\root\Office16\MSOSB.DLL
O18 - Protocol: osf-roaming.16 - {42089D2D-912D-4018-9087-2B87803E93FB} - C:\Program Files (x86)\Microsoft Office\root\Office16\MSOSB.DLL
O18 - Protocol: osf.16 - {5504BE45-A83B-4808-900A-3A5C36E7F77A} - C:\Program Files (x86)\Microsoft Office\root\Office16\MSOSB.DLL
O18 - Protocol: skype4com - {FFC8B962-9B40-4DFF-9458-1830C7DD7F5D} - C:\PROGRA~2\COMMON~1\Skype\SKYPE4~1.DLL
O18 - Protocol: wlpg - {E43EF6CD-A37A-4A9B-9E6F-83F89B8E6324} - C:\Program Files (x86)\Windows Live\Photo Gallery\AlbumDownloadProtocolHandler.dll
O23 - Service: Adobe Acrobat Update Service (AdobeARMservice) - Adobe Systems Incorporated - C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe
O23 - Service: @%SystemRoot%\system32\Alg.exe,-112 (ALG) - Unknown owner - C:\Windows\System32\alg.exe (file missing)
O23 - Service: Dritek WMI Service (DsiWMIService) - Dritek System Inc. - C:\Program Files (x86)\Launch Manager\dsiwmis.exe
O23 - Service: @%SystemRoot%\system32\efssvc.dll,-100 (EFS) - Unknown owner - C:\Windows\System32\lsass.exe (file missing)
O23 - Service: EgisTec Ticket Service - Egis Technology Inc. - C:\Program Files (x86)\Common Files\EgisTec\Services\EgisTicketService.exe
O23 - Service: ESET Service (ekrn) - ESET - C:\Program Files\ESET\ESET Smart Security\ekrn.exe
O23 - Service: ePower Service (ePowerSvc) - Acer Incorporated - C:\Program Files\Acer\Acer ePower Management\ePowerSvc.exe
O23 - Service: @%systemroot%\system32\fxsresm.dll,-118 (Fax) - Unknown owner - C:\Windows\system32\fxssvc.exe (file missing)

O23 - Service: FLEXnet Licensing Service - Acresso Software Inc. - C:\Program Files (x86)\Common Files\Macrovision Shared\FLEXnet Publisher\FNPLicensingService.exe
O23 - Service: GamesAppService - WildTangent, Inc. - C:\Program Files (x86)\WildTangent Games\App\GamesAppService.exe
O23 - Service: GREGService - Acer Incorporated - C:\Program Files (x86)\Acer\Registration\GREGsvc.exe
O23 - Service: Služba Google Update (gupdate) (gupdate) - Google Inc. - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
O23 - Service: Služba Google Update (gupdatem) (gupdatem) - Google Inc. - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
O23 - Service: Google Updater Service (gusvc) - Google - C:\Program Files (x86)\Google\Common\Google Updater\GoogleUpdaterService.exe
O23 - Service: Intel(R) Rapid Storage Technology (IAStorDataMgrSvc) - Intel Corporation - C:\Program Files (x86)\Intel\Intel(R) Rapid Storage Technology\IAStorDataMgrSvc.exe
O23 - Service: @%SystemRoot%\system32\ieetwcollectorres.dll,-1000 (IEEtwCollectorService) - Unknown owner - C:\Windows\system32\IEEtwCollector.exe (file missing)
O23 - Service: @keyiso.dll,-100 (KeyIso) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)
O23 - Service: KNet - Kurupira.net - C:\Windows\svcproxy\svcproxy.exe
O23 - Service: Live Updater Service - Acer Incorporated - C:\Program Files\Acer\Acer Updater\UpdaterService.exe
O23 - Service: Intel(R) Management and Security Application Local Management Service (LMS) - Intel Corporation - C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe
O23 - Service: Mozilla Maintenance Service (MozillaMaintenance) - Mozilla Foundation - C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe
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: Norton Online Backup (NOBU) - Symantec Corporation - C:\Program Files (x86)\Symantec\Norton Online Backup\NOBuAgent.exe
O23 - Service: NTI IScheduleSvc - NTI Corporation - C:\Program Files (x86)\NTI\Acer Backup Manager\IScheduleSvc.exe
O23 - Service: @%systemroot%\system32\psbase.dll,-300 (ProtectedStorage) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)
O23 - Service: Protexis Licensing V2 (PSI_SVC_2) - Protexis Inc. - c:\Program Files (x86)\Common Files\Protexis\License Service\PsiService_2.exe
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: Skype Updater (SkypeUpdate) - Skype Technologies - C:\Program Files (x86)\Skype\Updater\Updater.exe
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: Process Control (svcprocess) - Kurupira.NET - C:\Windows\svcproxy\svcprocess.exe

```
O23 - Service: Samsung Drive Manager Service (SZDrvSvc) - Clarus, Inc. -
C:\Program Files (x86)\Clarus\Samsung Drive Manager\SZDrvSvc.exe
O23 - Service: @%SystemRoot%\system32\ui0detect.exe,-101 (UI0Detect) -
Unknown owner - C:\Windows\system32\UI0Detect.exe (file missing)
O23 - Service: Intel(R) Management and Security Application User
Notification Service (UNS) - Intel Corporation - C:\Program Files
(x86)\Intel\Intel(R) Management Engine Components\UNS\UNS.exe
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: VirtualRouterService (Virtual Router) - Chris Pietschmann
(http://pietschsoft.com) - C:\Program Files (x86)\Virtual
Router\VirtualRouterService.exe
O23 - Service: @%systemroot%\system32\vssvc.exe,-102 (VSS) - Unknown
owner - C:\Windows\system32\vssvc.exe (file missing)
O23 - Service: @%SystemRoot%\system32\Wat\WatUX.exe,-601 (WatAdminSvc) -
Unknown owner - C:\Windows\system32\Wat\WatAdminSvc.exe (file missing)
O23 - Service: @%systemroot%\system32\wbengine.exe,-104 (wbengine) -
Unknown owner - C:\Windows\system32\wbengine.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)

--
End of file - 17267 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=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4
ProfileControl=Off MaxRequestThreads=16
wininit.exe
%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,20480,768 Windows=On SubSystemType=Windows
ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3
ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4
ProfileControl=Off MaxRequestThreads=16
C:\Windows\system32\services.exe
C:\Windows\system32\lsass.exe
C:\Windows\system32\lsm.exe
winlogon.exe
C:\Windows\system32\svchost.exe -k DcomLaunch
"C:\Program Files\ESET\ESET Smart Security\ekrn.exe"
C:\Windows\system32\svchost.exe -k RPCSS
C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
C:\Windows\system32\svchost.exe -k LocalService
C:\Windows\system32\svchost.exe -k netsvcs
C:\Windows\system32\svchost.exe -k NetworkService
C:\Windows\System32\spoolsv.exe
```

```
C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
"C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe"
"C:\Program Files\Common Files\Microsoft
Shared\ClickToRun\OfficeClickToRun.exe" /service
C:\Windows\System32\svchost.exe -k utcsvc
"C:\Program Files (x86)\Launch Manager\dsiwmis.exe"
"C:\Program Files\Acer\Acer ePower Management\ePowerSvc.exe"
"C:\Program Files (x86)\Launch Manager\LMutilps32.exe" --system-level-
mutex="Local\{B904A927-FE6B-48fd-8C83-6B807BED1F9C}"
"C:\Program Files (x86)\Acer\Registration\GREGsvc.exe"
C:\Windows\svcproxy\svcproxy.exe
"C:\Program Files\Acer\Acer Updater\UpdaterService.exe"
"C:\Program Files (x86)\Symantec\Norton Online Backup\NOBuAgent.exe"
SERVICE
"C:\Program Files (x86)\NTI\Acer Backup Manager\IScheduleSvc.exe"
"c:\Program Files (x86)\Common Files\Protexis\License
Service\PsiService_2.exe"
"C:\Program Files (x86)\Microsoft Application Virtualization
Client\sftvsa.exe"
C:\Windows\system32\svchost.exe -k imgsvc
C:\Windows\svcproxy\svcprocess.exe
"taskhost.exe"
"C:\Windows\system32\Dwm.exe"
"C:\Program Files (x86)\Clarus\Samsung Drive Manager\SZDrvSvc.exe"
"C:\Program Files (x86)\Virtual Router\VirtualRouterService.exe"
C:\Windows\Explorer.EXE
"C:\Program Files (x86)\Microsoft Application Virtualization
Client\sftlist.exe"
taskeng.exe {24BB202F-84D8-4226-A77F-86C8A590CFE0}
"C:\Program Files (x86)\Acer\clear.fi\MVP\clear.fiAgent.exe"
"C:\Program Files (x86)\Acer\clear.fi\MVP\.\Kernel\DMR\DMREngine.exe"
"C:\Program Files (x86)\AmIcoSingLun\AmIcoSinglun64.exe"
"C:\Windows\System32\igfxtray.exe"
"C:\Windows\System32\hkcmd.exe"
"C:\Windows\System32\igfxpers.exe"
"C:\Program Files\Synaptics\SynTP\SynTPEnh.exe"
"C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe" -s
"C:\Program Files\Canon\MyPrinter\BJMYPRT.EXE" /logon
"C:\Program Files\Synaptics\SynTP\SynTPHelper.exe"
"C:\Program Files\Windows Sidebar\sidebar.exe" /autoRun
"C:\Windows\System32\StikyNot.exe"
"C:\Program Files (x86)\Clarus\Samsung Drive Manager\ABRTMon.exe"
"C:\Program Files (x86)\NTI\Acer Backup Manager\BackupManagerTray.exe" -h
-k
"C:\Program Files (x86)\Launch Manager\LManager.exe"
"C:\Program Files (x86)\Acer\clear.fi\Movie\clear.fiMovieService.exe"
"C:\Program Files (x86)\Canon\Solution Menu EX\CNSEMAIN.EXE" /logon
"C:\Program Files (x86)\Common Files\Microsoft Shared\Virtualization
Handler\CVHSVC.EXE"
"C:\Program Files (x86)\Launch Manager\MMDx64Fx.exe"
"C:\Program Files (x86)\Clarus\Samsung Drive Manager\Drive Manager.exe" -
Hide
"C:\Program Files (x86)\Launch Manager\LMworker.exe"
C:\Windows\system32\wbem\wmiprvse.exe
"C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe"
C:\Windows\system32\wbem\unsecapp.exe -Embedding
C:\Windows\system32\SearchIndexer.exe /Embedding
C:\Windows\servicing\TrustedInstaller.exe
```

```
"C:\Program Files (x86)\Clarus\Samsung Drive Manager\SZDrvMon.exe"
C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted
C:\Windows\splwow64.exe 12288
"C:\Program Files\ESET\ESET Smart Security\egui.exe"
C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
C:\Windows\system32\DllHost.exe /Processid:{B366DEBE-645B-43A5-B865-
DDD82C345492}
C:\Windows\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe
"C:\Program Files (x86)\Intel\Intel(R) Rapid Storage
Technology\IAStorDataMgrSvc.exe"
"C:\Windows\system32\wuauclt.exe"
"C:\Program Files (x86)\Intel\Intel(R) Management Engine
Components\LMS\LMS.exe"
C:\Windows\System32\svchost.exe -k secsvcs
"C:\Windows\system32\taskmgr.exe" /4
"C:\Program Files\Windows Media Player\wmpnetwk.exe"
"C:\Program Files (x86)\Intel\Intel(R) Management Engine
Components\UNS\UNS.exe"
"C:\Program Files\Internet Explorer\iexplore.exe"
"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:4368
CREDAT:275457 /prefetch:2
"C:\Program Files\Common Files\Microsoft Shared\Windows Live\WLIDSVC.EXE"
WLIDSvcM.exe 6252
"C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\BingApp.exe" -
Embedding
"C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\BingBar.exe" -
Embedding
"C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\BingSurrogate.exe" -
Embedding
"C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\BingSurrogate.exe" -
Embedding
"C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\BingSurrogate.exe" -
Embedding
"C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\BingSurrogate.exe" -
Embedding
"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:4368
CREDAT:275534 /prefetch:2
"C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\SeaPort.exe"
"C:\Program Files\EgisTec IPS\PMMUpdate.exe"
"C:\Program Files\EgisTec IPS\EgisUpdate.exe"
"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:4368
CREDAT:3748936 /prefetch:2
C:\Windows\system32\svchost.exe -k SDRSVC
"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:4368
CREDAT:3159077 /prefetch:2
"C:\Users\ACER\Desktop\adwcleaner_6.020.exe"
"C:\Program Files (x86)\Windows Media Player\wmplayer.exe" /Play -
Embedding
"C:\Windows\system32\NOTEPAD.EXE" C:\AdwCleaner\AdwCleaner[S0].txt
"C:\Windows\System32\MsSpellCheckingFacility.exe" -Embedding

"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:4368
CREDAT:3880031 /prefetch:2
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --
type=crashpad-handler /prefetch:7 --no-rate-limit "--
database=C:\Users\ACER\AppData\Local\Google\Chrome\User Data\Crashpad" --
url=https://clients2.google.com/cr/report --annotation=channel=-m --
```

```
annotation=plat=Win32 --annotation=prod=Chrome --
annotation=ver=53.0.2785.116 --handshake-handle=0xb4
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=gpu-
process --channel="3064.0.57032493\1736513541" --mojo-application-
channel-token=B517E040A28103BD1AD57F370A86B455 --enable-
features=AutomaticTabDiscarding<AutomaticTabDiscarding,*BlockSmallPluginC
ontent<PluginPowerSaverTiny,DocumentWriteEvaluator<DisallowFetchForDocWri
ttenScriptsInMainFrame,MaterialDesignUserManager<MaterialDesignUserManage
r,*PreconnectMore<PreconnectMore,*TranslateUI2016Q2<TranslateUI2016Q2,Use
PasswordSeparatedSigninFlow<PasswordSeparatedSigninFlow --disable-
features=UpdateRendererPriorityOnStartup<UpdateRendererPriorityOnStartup
--force-fieldtrials=AppBannerTriggering/site-engagement-
liberal/AutomaticTabDiscarding/Enabled_Once_10-
gen2/CaptivePortalInterstitial/Enabled/ChildAccountDetection/Disabled/Cli
entSideDetectionModel/Model0/DisallowFetchForDocWrittenScriptsInMainFrame
/DocumentWriteEvaluatorGroup/EnableMediaRouter/Enabled/ExtensionDeveloper
ModeWarning/Enabled/*GFE/Default/GoogleBrandedContextMenu/default/Instanc
eID/Enabled/MaterialDesignDownloads/Enabled/MaterialDesignUserManager/Ena
bled/*NetworkQualityEstimator/Enabled/OmniboxBundledExperimentV1/Standard
R7/PasswordBranding/Disabled/*PasswordGeneration/Disabled/PasswordManager
SettingsMigration/Disable/PasswordSeparatedSigninFlow/Enabled/PasswordSma
rtBubble/3-
Times/PluginPowerSaverTiny/Default/PreconnectMore/Default/*QUIC/EnabledNo
Id/ReportCertificateErrors/ShowAndPossiblySend/SHA1IdentityUIWarning/Enab
led/SHA1ToolbarUIJanuary2016/Warning/SHA1ToolbarUIJanuary2017/Error/*SRTP
romptFieldTrial/BiMonthlyPrompt/SSLCommonNameMismatchHandling/Enabled/Saf
eBrowsingIncidentReportingService/Default/SafeBrowsingUnverifiedDownloads
/DisableByParameterMostSbTypes2/SafeBrowsingUpdateFrequency/Default/SignI
nPasswordPromo/Default/StrictSecureCookies/Default/SyncHttpContentCompres
sion/Enabled/TranslateUI2016Q2/DefaultTranslateUI2016Q2/TriggeredResetFie
ldTrial/On/*UMA-Dynamic-Uniformity-Trial/Group6/*UMA-Population-
Restrict/normal/*UMA-Uniformity-Trial-1-Percent/group_49/*UMA-Uniformity-
Trial-10-Percent/group_02/*UMA-Uniformity-Trial-100-
Percent/group_01/*UMA-Uniformity-Trial-20-Percent/group_01/*UMA-
Uniformity-Trial-5-Percent/group_08/*UMA-Uniformity-Trial-50-
Percent/group_01/WebBluetoothBlacklist/BlacklistUpdate1/ --disable-d3d11
--disable-direct-composition --supports-dual-gpus=false --gpu-driver-bug-
workarounds=5,11,13,14,15,18,31,48,56 --gpu-vendor-id=0x8086 --gpu-
device-id=0x0106 --gpu-driver-vendor="Intel Corporation" --gpu-driver-
version=8.15.10.2342 --gpu-driver-date=3-25-2011 --mojo-platform-channel-
handle=948 --ignored=" --type=renderer " /prefetch:2
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --
type=renderer --enable-
features=AutomaticTabDiscarding<AutomaticTabDiscarding,*BlockSmallPluginC
ontent<PluginPowerSaverTiny,DocumentWriteEvaluator<DisallowFetchForDocWri
ttenScriptsInMainFrame,MaterialDesignUserManager<MaterialDesignUserManage
r,*PreconnectMore<PreconnectMore,*TranslateUI2016Q2<TranslateUI2016Q2,Use
PasswordSeparatedSigninFlow<PasswordSeparatedSigninFlow --disable-
features=UpdateRendererPriorityOnStartup<UpdateRendererPriorityOnStartup
--force-fieldtrials=*AppBannerTriggering/site-engagement-
liberal/*AutomaticTabDiscarding/Enabled_Once_10-
gen2/CaptivePortalInterstitial/Enabled/ChildAccountDetection/Disabled/*Cl
ientSideDetectionModel/Model0/DisallowFetchForDocWrittenScriptsInMainFram
e/DocumentWriteEvaluatorGroup/*EnableMediaRouter/Enabled/ExtensionDevelop
erModeWarning/Enabled/*GFE/Default/GoogleBrandedContextMenu/default/Insta
nceID/Enabled/MaterialDesignDownloads/Enabled/MaterialDesignUserManager/E
nabled/*NetworkQualityEstimator/Enabled/OmniboxBundledExperimentV1/Standa
rdR7/PasswordBranding/Disabled/*PasswordGeneration/Disabled/*PasswordMana
```

```
gerSettingsMigration/Disable/PasswordSeparatedSigninFlow/Enabled/Password
SmartBubble/3-
Times/PluginPowerSaverTiny/Default/PreconnectMore/Default/*QUIC/EnabledNo
Id/ReportCertificateErrors/ShowAndPossiblySend/SHA1IdentityUIWarning/Enab
led/SHA1ToolbarUIJanuary2016/Warning/SHA1ToolbarUIJanuary2017/Error/*SRTP
romptFieldTrial/BiMonthlyPrompt/SSLCommonNameMismatchHandling/Enabled/*Sa
feBrowsingIncidentReportingService/Default/SafeBrowsingUnverifiedDownload
s/DisableByParameterMostSbTypes2/SafeBrowsingUpdateFrequency/Default/Sign
InPasswordPromo/Default/StrictSecureCookies/Default/SyncHttpContentCompre
ssion/Enabled/TranslateUI2016Q2/DefaultTranslateUI2016Q2/*TriggeredResetF
ieldTrial/On/*UMA-Dynamic-Uniformity-Trial/Group6/*UMA-Population-
Restrict/normal/*UMA-Uniformity-Trial-1-Percent/group_49/*UMA-Uniformity-
Trial-10-Percent/group_02/*UMA-Uniformity-Trial-100-
Percent/group_01/*UMA-Uniformity-Trial-20-Percent/group_01/*UMA-
Uniformity-Trial-5-Percent/group_08/*UMA-Uniformity-Trial-50-
Percent/group_01/WebBluetoothBlacklist/BlacklistUpdate1/ --primordial-
pipe-token=0026F87D1525B65F210C155FA31AB556 --lang=sk --extension-process
--enable-webrtc-hw-h264-encoding --enable-offline-auto-reload --enable-
offline-auto-reload-visible-only --blink-
settings=disallowFetchForDocWrittenScriptsInMainFrame=false,disallowFetch
ForDocWrittenScriptsInMainFrameOnSlowConnections=false --enable-pinch --
device-scale-factor=1 --num-raster-threads=1 --content-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --video-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --disable-accelerated-video-decode --mojo-channel-
token=D5178354273AF696939021D66C7772F1 --mojo-application-channel-
token=0026F87D1525B65F210C155FA31AB556 --
channel="3064.1.1561883720\280399862" --mojo-platform-channel-handle=1760
/prefetch:1
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --
type=renderer --enable-
features=AutomaticTabDiscarding<AutomaticTabDiscarding,*BlockSmallPluginC
ontent<PluginPowerSaverTiny,DocumentWriteEvaluator<DisallowFetchForDocWri
ttenScriptsInMainFrame,MaterialDesignUserManager<MaterialDesignUserManage
r,*PreconnectMore<PreconnectMore,*TranslateUI2016Q2<TranslateUI2016Q2,Use
PasswordSeparatedSigninFlow<PasswordSeparatedSigninFlow --disable-
features=UpdateRendererPriorityOnStartup<UpdateRendererPriorityOnStartup
--force-fieldtrials=*AppBannerTriggering/site-engagement-
liberal/*AutomaticTabDiscarding/Enabled_Once_10-
gen2/CaptivePortalInterstitial/Enabled/ChildAccountDetection/Disabled/*Cl
ientSideDetectionModel/Model0/*DisallowFetchForDocWrittenScriptsInMainFra
me/DocumentWriteEvaluatorGroup/*EnableMediaRouter/Enabled/ExtensionDevelo
perModeWarning/Enabled/*GFE/Default/GoogleBrandedContextMenu/default/Inst
anceID/Enabled/MaterialDesignDownloads/Enabled/MaterialDesignUserManager/
Enabled/*NetworkQualityEstimator/Enabled/*OmniboxBundledExperimentV1/Stan
dardR7/PasswordBranding/Disabled/*PasswordGeneration/Disabled/*PasswordMa
nagerSettingsMigration/Disable/PasswordSeparatedSigninFlow/Enabled/Passwo
rdSmartBubble/3-
Times/PluginPowerSaverTiny/Default/PreconnectMore/Default/*QUIC/EnabledNo
Id/ReportCertificateErrors/ShowAndPossiblySend/SHA1IdentityUIWarning/Enab
led/SHA1ToolbarUIJanuary2016/Warning/SHA1ToolbarUIJanuary2017/Error/*SRTP
romptFieldTrial/BiMonthlyPrompt/SSLCommonNameMismatchHandling/Enabled/*Sa
feBrowsingIncidentReportingService/Default/SafeBrowsingUnverifiedDownload
s/DisableByParameterMostSbTypes2/SafeBrowsingUpdateFrequency/Default/Sign
InPasswordPromo/Default/StrictSecureCookies/Default/SyncHttpContentCompre
ssion/Enabled/TranslateUI2016Q2/DefaultTranslateUI2016Q2/*TriggeredResetF
ieldTrial/On/*UMA-Dynamic-Uniformity-Trial/Group6/*UMA-Population-
```

```
Restrict/normal/*UMA-Uniformity-Trial-1-Percent/group_49/*UMA-Uniformity-
Trial-10-Percent/group_02/*UMA-Uniformity-Trial-100-
Percent/group_01/*UMA-Uniformity-Trial-20-Percent/group_01/*UMA-
Uniformity-Trial-5-Percent/group_08/*UMA-Uniformity-Trial-50-
Percent/group_01/WebBluetoothBlacklist/BlacklistUpdate1/ --primordial-
pipe-token=C4AAF7642C4D45EF635A02C69486AE6E --lang=sk --enable-offline-
auto-reload --enable-offline-auto-reload-visible-only --blink-
settings=disallowFetchForDocWrittenScriptsInMainFrame=false,disallowFetch
ForDocWrittenScriptsInMainFrameOnSlowConnections=false --enable-pinch --
device-scale-factor=1 --num-raster-threads=1 --content-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --video-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --disable-accelerated-video-decode --mojo-channel-
token=8AF48BA5814E7DE343AC8B4D51BAA1AC --mojo-application-channel-
token=C4AAF7642C4D45EF635A02C69486AE6E --
channel="3064.2.236954507\1238216165" --mojo-platform-channel-handle=1984
/prefetch:1
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --
type=renderer --enable-
features=AutomaticTabDiscarding<AutomaticTabDiscarding,*BlockSmallPluginC
ontent<PluginPowerSaverTiny,DocumentWriteEvaluator<DisallowFetchForDocWri
ttenScriptsInMainFrame,MaterialDesignUserManager<MaterialDesignUserManage
r,*PreconnectMore<PreconnectMore,*TranslateUI2016Q2<TranslateUI2016Q2,Use
PasswordSeparatedSigninFlow<PasswordSeparatedSigninFlow --disable-
features=UpdateRendererPriorityOnStartup<UpdateRendererPriorityOnStartup
--force-fieldtrials=*AppBannerTriggering/site-engagement-
liberal/*AutomaticTabDiscarding/Enabled_Once_10-
gen2/CaptivePortalInterstitial/Enabled/ChildAccountDetection/Disabled/*Cl
ientSideDetectionModel/Model0/*DisallowFetchForDocWrittenScriptsInMainFra
me/DocumentWriteEvaluatorGroup/*EnableMediaRouter/Enabled/ExtensionDevelo
perModeWarning/Enabled/*GFE/Default/GoogleBrandedContextMenu/default/Inst
anceID/Enabled/MaterialDesignDownloads/Enabled/MaterialDesignUserManager/
Enabled/*NetworkQualityEstimator/Enabled/*OmniboxBundledExperimentV1/Stan
dardR7/PasswordBranding/Disabled/*PasswordGeneration/Disabled/*PasswordMa
nagerSettingsMigration/Disable/PasswordSeparatedSigninFlow/Enabled/Passwo
rdSmartBubble/3-
Times/PluginPowerSaverTiny/Default/PreconnectMore/Default/*QUIC/EnabledNo
Id/ReportCertificateErrors/ShowAndPossiblySend/SHA1IdentityUIWarning/Enab
led/SHA1ToolbarUIJanuary2016/Warning/SHA1ToolbarUIJanuary2017/Error/*SRTP
romptFieldTrial/BiMonthlyPrompt/SSLCommonNameMismatchHandling/Enabled/*Sa
feBrowsingIncidentReportingService/Default/SafeBrowsingUnverifiedDownload
s/DisableByParameterMostSbTypes2/SafeBrowsingUpdateFrequency/Default/Sign
InPasswordPromo/Default/StrictSecureCookies/Default/SyncHttpContentCompre
ssion/Enabled/TranslateUI2016Q2/DefaultTranslateUI2016Q2/*TriggeredResetF
ieldTrial/On/*UMA-Dynamic-Uniformity-Trial/Group6/*UMA-Population-
Restrict/normal/*UMA-Uniformity-Trial-1-Percent/group_49/*UMA-Uniformity-
Trial-10-Percent/group_02/*UMA-Uniformity-Trial-100-
Percent/group_01/*UMA-Uniformity-Trial-20-Percent/group_01/*UMA-
Uniformity-Trial-5-Percent/group_08/*UMA-Uniformity-Trial-50-
Percent/group_01/WebBluetoothBlacklist/BlacklistUpdate1/ --primordial-
pipe-token=444714CD9CCEA1FE184FF2E03104D520 --lang=sk --extension-process
--enable-webrtc-hw-h264-encoding --enable-offline-auto-reload --enable-
offline-auto-reload-visible-only --blink-
settings=disallowFetchForDocWrittenScriptsInMainFrame=false,disallowFetch
ForDocWrittenScriptsInMainFrameOnSlowConnections=false --enable-pinch --
device-scale-factor=1 --num-raster-threads=1 --content-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
```

```
553,3553 --video-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --disable-accelerated-video-decode --mojo-channel-
token=3D476F992C70F31F2E0978C24B9F51E8 --mojo-application-channel-
token=444714CD9CCEA1FE184FF2E03104D520 --
channel="3064.3.2069512473\1174758253" --mojo-platform-channel-
handle=2192 /prefetch:1
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --
type=renderer --enable-
features=AutomaticTabDiscarding<AutomaticTabDiscarding,*BlockSmallPluginC
ontent<PluginPowerSaverTiny,DocumentWriteEvaluator<DisallowFetchForDocWri
ttenScriptsInMainFrame,MaterialDesignUserManager<MaterialDesignUserManage
r,*PreconnectMore<PreconnectMore,*TranslateUI2016Q2<TranslateUI2016Q2,Use
PasswordSeparatedSigninFlow<PasswordSeparatedSigninFlow --disable-
features=UpdateRendererPriorityOnStartup<UpdateRendererPriorityOnStartup
--force-fieldtrials=*AppBannerTriggering/site-engagement-
liberal/*AutomaticTabDiscarding/Enabled_Once_10-
gen2/CaptivePortalInterstitial/Enabled/ChildAccountDetection/Disabled/*Cl
ientSideDetectionModel/Model0/*DisallowFetchForDocWrittenScriptsInMainFra
me/DocumentWriteEvaluatorGroup/*EnableMediaRouter/Enabled/ExtensionDevelo
perModeWarning/Enabled/*GFE/Default/GoogleBrandedContextMenu/default/Inst
anceID/Enabled/MaterialDesignDownloads/Enabled/MaterialDesignUserManager/
Enabled/*NetworkQualityEstimator/Enabled/*OmniboxBundledExperimentV1/Stan
dardR7/PasswordBranding/Disabled/*PasswordGeneration/Disabled/*PasswordMa
nagerSettingsMigration/Disable/PasswordSeparatedSigninFlow/Enabled/Passwo
rdSmartBubble/3-
Times/PluginPowerSaverTiny/Default/*PreconnectMore/Default/*QUIC/EnabledN
oId/ReportCertificateErrors/ShowAndPossiblySend/SHA1IdentityUIWarning/Ena
bled/SHA1ToolbarUIJanuary2016/Warning/SHA1ToolbarUIJanuary2017/Error/*SRT
PromptFieldTrial/BiMonthlyPrompt/SSLCommonNameMismatchHandling/Enabled/*S
afeBrowsingIncidentReportingService/Default/SafeBrowsingUnverifiedDownloa
ds/DisableByParameterMostSbTypes2/SafeBrowsingUpdateFrequency/Default/Sig
nInPasswordPromo/Default/*StrictSecureCookies/Default/SyncHttpContentComp
ression/Enabled/TranslateUI2016Q2/DefaultTranslateUI2016Q2/*TriggeredRese
tFieldTrial/On/*UMA-Dynamic-Uniformity-Trial/Group6/*UMA-Population-
Restrict/normal/*UMA-Uniformity-Trial-1-Percent/group_49/*UMA-Uniformity-
Trial-10-Percent/group_02/*UMA-Uniformity-Trial-100-
Percent/group_01/*UMA-Uniformity-Trial-20-Percent/group_01/*UMA-
Uniformity-Trial-5-Percent/group_08/*UMA-Uniformity-Trial-50-
Percent/group_01/WebBluetoothBlacklist/BlacklistUpdate1/ --primordial-
pipe-token=AD2F08D930B54BCD2B9E959EDE4DD795 --lang=sk --enable-offline-
auto-reload --enable-offline-auto-reload-visible-only --blink-
settings=disallowFetchForDocWrittenScriptsInMainFrame=false,disallowFetch
ForDocWrittenScriptsInMainFrameOnSlowConnections=false --enable-pinch --
device-scale-factor=1 --num-raster-threads=1 --content-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --video-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --disable-accelerated-video-decode --mojo-channel-
token=F1ED1B256E99F95C5977F69CA0C965BC --mojo-application-channel-
token=AD2F08D930B54BCD2B9E959EDE4DD795 --
channel="3064.5.555259393\1280324637" --mojo-platform-channel-handle=4268
/prefetch:1
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --
type=renderer --enable-
features=AutomaticTabDiscarding<AutomaticTabDiscarding,*BlockSmallPluginC
ontent<PluginPowerSaverTiny,DocumentWriteEvaluator<DisallowFetchForDocWri
ttenScriptsInMainFrame,MaterialDesignUserManager<MaterialDesignUserManage
```

```
r,*PreconnectMore<PreconnectMore,*TranslateUI2016Q2<TranslateUI2016Q2,Use
PasswordSeparatedSigninFlow<PasswordSeparatedSigninFlow --disable-
features=UpdateRendererPriorityOnStartup<UpdateRendererPriorityOnStartup
--force-fieldtrials=*AppBannerTriggering/site-engagement-
liberal/*AutomaticTabDiscarding/Enabled_Once_10-
gen2/*CaptivePortalInterstitial/Enabled/ChildAccountDetection/Disabled/*C
lientSideDetectionModel/Model0/*DisallowFetchForDocWrittenScriptsInMainFr
ame/DocumentWriteEvaluatorGroup/*EnableMediaRouter/Enabled/ExtensionDevel
operModeWarning/Enabled/*GFE/Default/GoogleBrandedContextMenu/default/Ins
tanceID/Enabled/MaterialDesignDownloads/Enabled/MaterialDesignUserManager
/Enabled/*NetworkQualityEstimator/Enabled/*OmniboxBundledExperimentV1/Sta
ndardR7/PasswordBranding/Disabled/*PasswordGeneration/Disabled/*PasswordM
anagerSettingsMigration/Disable/PasswordSeparatedSigninFlow/Enabled/Passw
ordSmartBubble/3-
Times/PluginPowerSaverTiny/Default/*PreconnectMore/Default/*QUIC/EnabledN
oId/ReportCertificateErrors/ShowAndPossiblySend/SHA1IdentityUIWarning/Ena
bled/SHA1ToolbarUIJanuary2016/Warning/SHA1ToolbarUIJanuary2017/Error/*SRT
PromptFieldTrial/BiMonthlyPrompt/*SSLCommonNameMismatchHandling/Enabled/*
SafeBrowsingIncidentReportingService/Default/SafeBrowsingUnverifiedDownlo
ads/DisableByParameterMostSbTypes2/SafeBrowsingUpdateFrequency/Default/Si
gnInPasswordPromo/Default/*StrictSecureCookies/Default/SyncHttpContentCom
pression/Enabled/TranslateUI2016Q2/DefaultTranslateUI2016Q2/*TriggeredRes
etFieldTrial/On/*UMA-Dynamic-Uniformity-Trial/Group6/*UMA-Population-
Restrict/normal/*UMA-Uniformity-Trial-1-Percent/group_49/*UMA-Uniformity-
Trial-10-Percent/group_02/*UMA-Uniformity-Trial-100-
Percent/group_01/*UMA-Uniformity-Trial-20-Percent/group_01/*UMA-
Uniformity-Trial-5-Percent/group_08/*UMA-Uniformity-Trial-50-
Percent/group_01/WebBluetoothBlacklist/BlacklistUpdate1/ --primordial-
pipe-token=5346D8FE108C8A6AD1207A23DD465032 --lang=sk --enable-offline-
auto-reload --enable-offline-auto-reload-visible-only --blink-
settings=disallowFetchForDocWrittenScriptsInMainFrame=false,disallowFetch
ForDocWrittenScriptsInMainFrameOnSlowConnections=false --enable-pinch --
device-scale-factor=1 --num-raster-threads=1 --content-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --video-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --disable-accelerated-video-decode --mojo-channel-
token=80DBF71AF9479B99B7F72CEAB7F165C6 --mojo-application-channel-
token=5346D8FE108C8A6AD1207A23DD465032 --
channel="3064.6.2033044532\6604139" --mojo-platform-channel-handle=4360
/prefetch:1
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --
type=renderer --enable-
features=AutomaticTabDiscarding<AutomaticTabDiscarding,*BlockSmallPluginC
ontent<PluginPowerSaverTiny,DocumentWriteEvaluator<DisallowFetchForDocWri
ttenScriptsInMainFrame,MaterialDesignUserManager<MaterialDesignUserManage
r,*PreconnectMore<PreconnectMore,*TranslateUI2016Q2<TranslateUI2016Q2,Use
PasswordSeparatedSigninFlow<PasswordSeparatedSigninFlow --disable-
features=UpdateRendererPriorityOnStartup<UpdateRendererPriorityOnStartup
--force-fieldtrials=*AppBannerTriggering/site-engagement-
liberal/*AutomaticTabDiscarding/Enabled_Once_10-
gen2/*CaptivePortalInterstitial/Enabled/ChildAccountDetection/Disabled/*C
lientSideDetectionModel/Model0/*DisallowFetchForDocWrittenScriptsInMainFr
ame/DocumentWriteEvaluatorGroup/*EnableMediaRouter/Enabled/ExtensionDevel
operModeWarning/Enabled/*GFE/Default/GoogleBrandedContextMenu/default/Ins
tanceID/Enabled/MaterialDesignDownloads/Enabled/MaterialDesignUserManager
/Enabled/*NetworkQualityEstimator/Enabled/*OmniboxBundledExperimentV1/Sta
ndardR7/PasswordBranding/Disabled/*PasswordGeneration/Disabled/*PasswordM
```

```
anagerSettingsMigration/Disable/PasswordSeparatedSigninFlow/Enabled/Passw
ordSmartBubble/3-
Times/PluginPowerSaverTiny/Default/*PreconnectMore/Default/*QUIC/EnabledN
oId/*ReportCertificateErrors/ShowAndPossiblySend/SHA1IdentityUIWarning/En
abled/SHA1ToolbarUIJanuary2016/Warning/SHA1ToolbarUIJanuary2017/Error/*SR
TPromptFieldTrial/BiMonthlyPrompt/*SSLCommonNameMismatchHandling/Enabled/
*SafeBrowsingIncidentReportingService/Default/SafeBrowsingUnverifiedDownl
oads/DisableByParameterMostSbTypes2/SafeBrowsingUpdateFrequency/Default/S
ignInPasswordPromo/Default/*StrictSecureCookies/Default/SyncHttpContentCo
mpression/Enabled/TranslateUI2016Q2/DefaultTranslateUI2016Q2/*TriggeredRe
setFieldTrial/On/*UMA-Dynamic-Uniformity-Trial/Group6/*UMA-Population-
Restrict/normal/*UMA-Uniformity-Trial-1-Percent/group_49/*UMA-Uniformity-
Trial-10-Percent/group_02/*UMA-Uniformity-Trial-100-
Percent/group_01/*UMA-Uniformity-Trial-20-Percent/group_01/*UMA-
Uniformity-Trial-5-Percent/group_08/*UMA-Uniformity-Trial-50-
Percent/group_01/WebBluetoothBlacklist/BlacklistUpdate1/ --primordial-
pipe-token=A6E01569901C8DB7E46298FFA0FAF67C --lang=sk --enable-offline-
auto-reload --enable-offline-auto-reload-visible-only --blink-
settings=disallowFetchForDocWrittenScriptsInMainFrame=false,disallowFetch
ForDocWrittenScriptsInMainFrameOnSlowConnections=false --enable-pinch --
device-scale-factor=1 --num-raster-threads=1 --content-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --video-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --disable-accelerated-video-decode --mojo-channel-
token=17BDC0CF7CFA605EDC166D8C9BEF473D --mojo-application-channel-
token=A6E01569901C8DB7E46298FFA0FAF67C --
channel="3064.7.661221111\1765459958" --mojo-platform-channel-handle=4532
/prefetch:1
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --
type=renderer --enable-
features=AutomaticTabDiscarding<AutomaticTabDiscarding,*BlockSmallPluginC
ontent<PluginPowerSaverTiny,DocumentWriteEvaluator<DisallowFetchForDocWri
ttenScriptsInMainFrame,MaterialDesignUserManager<MaterialDesignUserManage
r,*PreconnectMore<PreconnectMore,*TranslateUI2016Q2<TranslateUI2016Q2,Use
PasswordSeparatedSigninFlow<PasswordSeparatedSigninFlow --disable-
features=UpdateRendererPriorityOnStartup<UpdateRendererPriorityOnStartup
--force-fieldtrials=*AppBannerTriggering/site-engagement-
liberal/*AutomaticTabDiscarding/Enabled_Once_10-
gen2/*CaptivePortalInterstitial/Enabled/ChildAccountDetection/Disabled/*C
lientSideDetectionModel/Model0/*DisallowFetchForDocWrittenScriptsInMainFr
ame/DocumentWriteEvaluatorGroup/*EnableMediaRouter/Enabled/ExtensionDevel
operModeWarning/Enabled/*GFE/Default/GoogleBrandedContextMenu/default/Ins
tanceID/Enabled/MaterialDesignDownloads/Enabled/MaterialDesignUserManager
/Enabled/*NetworkQualityEstimator/Enabled/*OmniboxBundledExperimentV1/Sta
ndardR7/PasswordBranding/Disabled/*PasswordGeneration/Disabled/*PasswordM
anagerSettingsMigration/Disable/PasswordSeparatedSigninFlow/Enabled/Passw
ordSmartBubble/3-
Times/PluginPowerSaverTiny/Default/*PreconnectMore/Default/*QUIC/EnabledN
oId/*ReportCertificateErrors/ShowAndPossiblySend/SHA1IdentityUIWarning/En
abled/SHA1ToolbarUIJanuary2016/Warning/SHA1ToolbarUIJanuary2017/Error/*SR
TPromptFieldTrial/BiMonthlyPrompt/*SSLCommonNameMismatchHandling/Enabled/
*SafeBrowsingIncidentReportingService/Default/SafeBrowsingUnverifiedDownl
oads/DisableByParameterMostSbTypes2/SafeBrowsingUpdateFrequency/Default/S
ignInPasswordPromo/Default/*StrictSecureCookies/Default/SyncHttpContentCo
mpression/Enabled/TranslateUI2016Q2/DefaultTranslateUI2016Q2/*TriggeredRe
setFieldTrial/On/*UMA-Dynamic-Uniformity-Trial/Group6/*UMA-Population-
Restrict/normal/*UMA-Uniformity-Trial-1-Percent/group_49/*UMA-Uniformity-
```

```
Trial-10-Percent/group_02/*UMA-Uniformity-Trial-100-
Percent/group_01/*UMA-Uniformity-Trial-20-Percent/group_01/*UMA-
Uniformity-Trial-5-Percent/group_08/*UMA-Uniformity-Trial-50-
Percent/group_01/WebBluetoothBlacklist/BlacklistUpdate1/ --primordial-
pipe-token=8DB039FBE54C1704D82EDC076F6440F8 --lang=sk --enable-offline-
auto-reload --enable-offline-auto-reload-visible-only --blink-
settings=disallowFetchForDocWrittenScriptsInMainFrame=false,disallowFetch
ForDocWrittenScriptsInMainFrameOnSlowConnections=false --enable-pinch --
device-scale-factor=1 --num-raster-threads=1 --content-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --video-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --disable-accelerated-video-decode --mojo-channel-
token=73F3B1511A61B9CDE5509437871D5687 --mojo-application-channel-
token=8DB039FBE54C1704D82EDC076F6440F8 --
channel="3064.8.1712453953\205081878" --mojo-platform-channel-handle=5384
/prefetch:1
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --
type=renderer --enable-
features=AutomaticTabDiscarding<AutomaticTabDiscarding,*BlockSmallPluginC
ontent<PluginPowerSaverTiny,DocumentWriteEvaluator<DisallowFetchForDocWri
ttenScriptsInMainFrame,MaterialDesignUserManager<MaterialDesignUserManage
r,*PreconnectMore<PreconnectMore,*TranslateUI2016Q2<TranslateUI2016Q2,Use
PasswordSeparatedSigninFlow<PasswordSeparatedSigninFlow --disable-
features=UpdateRendererPriorityOnStartup<UpdateRendererPriorityOnStartup
--force-fieldtrials=*AppBannerTriggering/site-engagement-
liberal/*AutomaticTabDiscarding/Enabled_Once_10-
gen2/*CaptivePortalInterstitial/Enabled/ChildAccountDetection/Disabled/*C
lientSideDetectionModel/Model0/*DisallowFetchForDocWrittenScriptsInMainFr
ame/DocumentWriteEvaluatorGroup/*EnableMediaRouter/Enabled/ExtensionDevel
operModeWarning/Enabled/*GFE/Default/GoogleBrandedContextMenu/default/Ins
tanceID/Enabled/MaterialDesignDownloads/Enabled/MaterialDesignUserManager
/Enabled/*NetworkQualityEstimator/Enabled/*OmniboxBundledExperimentV1/Sta
ndardR7/PasswordBranding/Disabled/*PasswordGeneration/Disabled/*PasswordM
anagerSettingsMigration/Disable/PasswordSeparatedSigninFlow/Enabled/Passw
ordSmartBubble/3-
Times/PluginPowerSaverTiny/Default/*PreconnectMore/Default/*QUIC/EnabledN
oId/*ReportCertificateErrors/ShowAndPossiblySend/SHA1IdentityUIWarning/En
abled/SHA1ToolbarUIJanuary2016/Warning/SHA1ToolbarUIJanuary2017/Error/*SR
TPromptFieldTrial/BiMonthlyPrompt/*SSLCommonNameMismatchHandling/Enabled/
*SafeBrowsingIncidentReportingService/Default/SafeBrowsingUnverifiedDownl
oads/DisableByParameterMostSbTypes2/SafeBrowsingUpdateFrequency/Default/S
ignInPasswordPromo/Default/*StrictSecureCookies/Default/SyncHttpContentCo
mpression/Enabled/TranslateUI2016Q2/DefaultTranslateUI2016Q2/*TriggeredRe
setFieldTrial/On/*UMA-Dynamic-Uniformity-Trial/Group6/*UMA-Population-
Restrict/normal/*UMA-Uniformity-Trial-1-Percent/group_49/*UMA-Uniformity-
Trial-10-Percent/group_02/*UMA-Uniformity-Trial-100-
Percent/group_01/*UMA-Uniformity-Trial-20-Percent/group_01/*UMA-
Uniformity-Trial-5-Percent/group_08/*UMA-Uniformity-Trial-50-
Percent/group_01/WebBluetoothBlacklist/BlacklistUpdate1/ --primordial-
pipe-token=6F15D8643DDC9F48206017C9566840B3 --lang=sk --enable-offline-
auto-reload --enable-offline-auto-reload-visible-only --blink-
settings=disallowFetchForDocWrittenScriptsInMainFrame=false,disallowFetch
ForDocWrittenScriptsInMainFrameOnSlowConnections=false --enable-pinch --
device-scale-factor=1 --num-raster-threads=1 --content-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --video-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
```

```
553,3553 --disable-accelerated-video-decode --mojo-channel-
token=F1F1241071369EF35180498C7913E29C --mojo-application-channel-
token=6F15D8643DDC9F48206017C9566840B3 --
channel="3064.9.1294216416\461008971" --mojo-platform-channel-handle=2448
/prefetch:1
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --
type=renderer --enable-
features=AutomaticTabDiscarding<AutomaticTabDiscarding,*BlockSmallPluginC
ontent<PluginPowerSaverTiny,DocumentWriteEvaluator<DisallowFetchForDocWri
ttenScriptsInMainFrame,MaterialDesignUserManager<MaterialDesignUserManage
r,*PreconnectMore<PreconnectMore,*TranslateUI2016Q2<TranslateUI2016Q2,Use
PasswordSeparatedSigninFlow<PasswordSeparatedSigninFlow --disable-
features=UpdateRendererPriorityOnStartup<UpdateRendererPriorityOnStartup
--force-fieldtrials=*AppBannerTriggering/site-engagement-
liberal/*AutomaticTabDiscarding/Enabled_Once_10-
gen2/*CaptivePortalInterstitial/Enabled/ChildAccountDetection/Disabled/*C
lientSideDetectionModel/Model0/*DisallowFetchForDocWrittenScriptsInMainFr
ame/DocumentWriteEvaluatorGroup/*EnableMediaRouter/Enabled/ExtensionDevel
operModeWarning/Enabled/*GFE/Default/GoogleBrandedContextMenu/default/Ins
tanceID/Enabled/MaterialDesignDownloads/Enabled/MaterialDesignUserManager
/Enabled/*NetworkQualityEstimator/Enabled/*OmniboxBundledExperimentV1/Sta
ndardR7/PasswordBranding/Disabled/*PasswordGeneration/Disabled/*PasswordM
anagerSettingsMigration/Disable/PasswordSeparatedSigninFlow/Enabled/Passw
ordSmartBubble/3-
Times/PluginPowerSaverTiny/Default/*PreconnectMore/Default/*QUIC/EnabledN
oId/*ReportCertificateErrors/ShowAndPossiblySend/SHA1IdentityUIWarning/En
abled/SHA1ToolbarUIJanuary2016/Warning/SHA1ToolbarUIJanuary2017/Error/*SR
TPromptFieldTrial/BiMonthlyPrompt/*SSLCommonNameMismatchHandling/Enabled/
*SafeBrowsingIncidentReportingService/Default/SafeBrowsingUnverifiedDownl
oads/DisableByParameterMostSbTypes2/SafeBrowsingUpdateFrequency/Default/S
ignInPasswordPromo/Default/*StrictSecureCookies/Default/SyncHttpContentCo
mpression/Enabled/TranslateUI2016Q2/DefaultTranslateUI2016Q2/*TriggeredRe
setFieldTrial/On/*UMA-Dynamic-Uniformity-Trial/Group6/*UMA-Population-
Restrict/normal/*UMA-Uniformity-Trial-1-Percent/group_49/*UMA-Uniformity-
Trial-10-Percent/group_02/*UMA-Uniformity-Trial-100-
Percent/group_01/*UMA-Uniformity-Trial-20-Percent/group_01/*UMA-
Uniformity-Trial-5-Percent/group_08/*UMA-Uniformity-Trial-50-
Percent/group_01/WebBluetoothBlacklist/BlacklistUpdate1/ --primordial-
pipe-token=BFE4E28728825D37C9D387769192A97A --lang=sk --enable-offline-
auto-reload --enable-offline-auto-reload-visible-only --blink-
settings=disallowFetchForDocWrittenScriptsInMainFrame=false,disallowFetch
ForDocWrittenScriptsInMainFrameOnSlowConnections=false --enable-pinch --
device-scale-factor=1 --num-raster-threads=1 --content-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --video-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --disable-accelerated-video-decode --mojo-channel-
token=1253E4BA553C46B2AEADC5644A6AC825 --mojo-application-channel-
token=BFE4E28728825D37C9D387769192A97A --
channel="3064.10.712674443\1728465215" --mojo-platform-channel-
handle=5804 /prefetch:1
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --
type=ppapi-broker --mojo-channel-token=55B75F6E8D95193A35561E9F4DA027CF -
-lang=sk --device-scale-factor=1 --mojo-platform-channel-handle=7248
/prefetch:4
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --
type=renderer --enable-
features=AutomaticTabDiscarding<AutomaticTabDiscarding,*BlockSmallPluginC
```

ontent<PluginPowerSaverTiny,DocumentWriteEvaluator<DisallowFetchForDocWri
ttenScriptsInMainFrame,MaterialDesignUserManager<MaterialDesignUserManage
r,*PreconnectMore<PreconnectMore,*TranslateUI2016Q2<TranslateUI2016Q2,Use
PasswordSeparatedSigninFlow<PasswordSeparatedSigninFlow --disable-
features=UpdateRendererPriorityOnStartup<UpdateRendererPriorityOnStartup
--force-fieldtrials=*AppBannerTriggering/site-engagement-
liberal/*AutomaticTabDiscarding/Enabled_Once_10-
gen2/*CaptivePortalInterstitial/Enabled/ChildAccountDetection/Disabled/*C
lientSideDetectionModel/Model0/*DisallowFetchForDocWrittenScriptsInMainFr
ame/DocumentWriteEvaluatorGroup/*EnableMediaRouter/Enabled/ExtensionDevel
operModeWarning/Enabled/*GFE/Default/GoogleBrandedContextMenu/default/Ins
tanceID/Enabled/MaterialDesignDownloads/Enabled/MaterialDesignUserManager
/Enabled/*NetworkQualityEstimator/Enabled/*OmniboxBundledExperimentV1/Sta
ndardR7/*PasswordBranding/Disabled/*PasswordGeneration/Disabled/*Password
ManagerSettingsMigration/Disable/PasswordSeparatedSigninFlow/Enabled/Pass
wordSmartBubble/3-
Times/*PluginPowerSaverTiny/Default/*PreconnectMore/Default/*QUIC/Enabled
NoId/*ReportCertificateErrors/ShowAndPossiblySend/SHA1IdentityUIWarning/E
nabled/SHA1ToolbarUIJanuary2016/Warning/SHA1ToolbarUIJanuary2017/Error/*S
RTPromptFieldTrial/BiMonthlyPrompt/*SSLCommonNameMismatchHandling/Enabled
/*SafeBrowsingIncidentReportingService/Default/SafeBrowsingUnverifiedDown
loads/DisableByParameterMostSbTypes2/SafeBrowsingUpdateFrequency/Default/
SignInPasswordPromo/Default/*StrictSecureCookies/Default/SyncHttpContentC
ompression/Enabled/*TranslateUI2016Q2/DefaultTranslateUI2016Q2/*Triggered
ResetFieldTrial/On/*UMA-Dynamic-Uniformity-Trial/Group6/*UMA-Population-
Restrict/normal/*UMA-Uniformity-Trial-1-Percent/group_49/*UMA-Uniformity-
Trial-10-Percent/group_02/*UMA-Uniformity-Trial-100-
Percent/group_01/*UMA-Uniformity-Trial-20-Percent/group_01/*UMA-
Uniformity-Trial-5-Percent/group_08/*UMA-Uniformity-Trial-50-
Percent/group_01/WebBluetoothBlacklist/BlacklistUpdate1/ --primordial-
pipe-token=6D6D49280E3A68264C34679E4554F936 --lang=sk --extension-process
--enable-webrtc-hw-h264-encoding --enable-offline-auto-reload --enable-
offline-auto-reload-visible-only --blink-
settings=disallowFetchForDocWrittenScriptsInMainFrame=false,disallowFetch
ForDocWrittenScriptsInMainFrameOnSlowConnections=false --enable-pinch --
device-scale-factor=1 --num-raster-threads=1 --content-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --video-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --disable-accelerated-video-decode --mojo-channel-
token=D6575D4FC6663C427A7EE37BF5D59A91 --mojo-application-channel-
token=6D6D49280E3A68264C34679E4554F936 --
channel="3064.17.1642256689\860444609" --mojo-platform-channel-
handle=6436 /prefetch:1
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --
type=renderer --enable-
features=AutomaticTabDiscarding<AutomaticTabDiscarding,*BlockSmallPluginC
ontent<PluginPowerSaverTiny,DocumentWriteEvaluator<DisallowFetchForDocWri
ttenScriptsInMainFrame,MaterialDesignUserManager<MaterialDesignUserManage
r,*PreconnectMore<PreconnectMore,*TranslateUI2016Q2<TranslateUI2016Q2,Use
PasswordSeparatedSigninFlow<PasswordSeparatedSigninFlow --disable-
features=UpdateRendererPriorityOnStartup<UpdateRendererPriorityOnStartup
--force-fieldtrials=*AppBannerTriggering/site-engagement-
liberal/*AutomaticTabDiscarding/Enabled_Once_10-
gen2/*CaptivePortalInterstitial/Enabled/ChildAccountDetection/Disabled/*C
lientSideDetectionModel/Model0/*DisallowFetchForDocWrittenScriptsInMainFr
ame/DocumentWriteEvaluatorGroup/*EnableMediaRouter/Enabled/ExtensionDevel
operModeWarning/Enabled/*GFE/Default/GoogleBrandedContextMenu/default/Ins

tanceID/Enabled/MaterialDesignDownloads/Enabled/MaterialDesignUserManager
/Enabled/*NetworkQualityEstimator/Enabled/*OmniboxBundledExperimentV1/Sta
ndardR7/*PasswordBranding/Disabled/*PasswordGeneration/Disabled/*Password
ManagerSettingsMigration/Disable/PasswordSeparatedSigninFlow/Enabled/Pass
wordSmartBubble/3-
Times/*PluginPowerSaverTiny/Default/*PreconnectMore/Default/*QUIC/Enabled
NoId/*ReportCertificateErrors/ShowAndPossiblySend/SHA1IdentityUIWarning/E
nabled/SHA1ToolbarUIJanuary2016/Warning/SHA1ToolbarUIJanuary2017/Error/*S
RTPromptFieldTrial/BiMonthlyPrompt/*SSLCommonNameMismatchHandling/Enabled
/*SafeBrowsingIncidentReportingService/Default/SafeBrowsingUnverifiedDown
loads/DisableByParameterMostSbTypes2/SafeBrowsingUpdateFrequency/Default/
SignInPasswordPromo/Default/*StrictSecureCookies/Default/SyncHttpContentC
ompression/Enabled/*TranslateUI2016Q2/DefaultTranslateUI2016Q2/*Triggered
ResetFieldTrial/On/*UMA-Dynamic-Uniformity-Trial/Group6/*UMA-Population-
Restrict/normal/*UMA-Uniformity-Trial-1-Percent/group_49/*UMA-Uniformity-
Trial-10-Percent/group_02/*UMA-Uniformity-Trial-100-
Percent/group_01/*UMA-Uniformity-Trial-20-Percent/group_01/*UMA-
Uniformity-Trial-5-Percent/group_08/*UMA-Uniformity-Trial-50-
Percent/group_01/WebBluetoothBlacklist/BlacklistUpdate1/ --primordial-
pipe-token=7032B5AB15D276877FD42DD3F8E4C795 --lang=sk --enable-offline-
auto-reload --enable-offline-auto-reload-visible-only --blink-
settings=disallowFetchForDocWrittenScriptsInMainFrame=false,disallowFetch
ForDocWrittenScriptsInMainFrameOnSlowConnections=false --enable-pinch --
device-scale-factor=1 --num-raster-threads=1 --content-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --video-image-texture-
target=3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3553,3
553,3553 --disable-accelerated-video-decode --mojo-channel-
token=5388F8457D284779D51126C3BFA4728B --mojo-application-channel-
token=7032B5AB15D276877FD42DD3F8E4C795 --
channel="3064.18.1915356435\711473409" --mojo-platform-channel-
handle=8216 /prefetch:1
"C:\Windows\system32\SearchProtocolHost.exe"
Global\UsGthrFltPipeMssGthrPipe24_ Global\UsGthrCtrlFltPipeMssGthrPipe24
1 -2147483646 "Software\Microsoft\Windows Search" "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT; MS Search 4.0 Robot)"
"C:\ProgramData\Microsoft\Search\Data\Temp\usgthrsvc" "DownLevelDaemon"
"C:\Windows\system32\SearchFilterHost.exe" 0 516 520 528 65536 524
"C:\Users\ACER\Downloads\RSITx64.exe"
C:\Windows\system32\wbem\wmiprvse.exe

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

C:\Windows\tasks\GoogleUpdateTaskMachineCore.job - C:\Program Files
(x86)\Google\Update\GoogleUpdate.exe18 /c18
C:\Windows\tasks\GoogleUpdateTaskMachineUA.job - C:\Program Files
(x86)\Google\Update\GoogleUpdate.exe18 /ua /installsource scheduler18
C:\Windows\tasks\GoogleUpdateTaskMachineUA1cffea81fe46797.job -
C:\Program Files (x86)\Google\Update\GoogleUpdate.exe18 /ua
/installsource scheduler18

=========Mozilla firefox=========

ProfilePath -
C:\Users\ACER\AppData\Roaming\Mozilla\Firefox\Profiles\fbo057wi.default

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@adobe.com/FlashP
layer]

"Description"=Adobe® Flash® Player 21.0.0.242 Plugin
"Path"=C:\Windows\SysWOW64\Macromed\Flash\NPSWF32_21_0_0_242.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@canon.com/EPPEX]
"Description"=Canon Easy-PhotoPrint EX
"Path"=C:\Program Files (x86)\Canon\Easy-PhotoPrint EX\NPEZFFPI.DLL

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@Google.com/GooglEarthPlugin]
"Description"=Google Earth in your browser
"Path"=C:\Program Files (x86)\Google\Google Earth\plugin\npgeplugin.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@google.com/npPicasa3,version=3.0.0]
"Description"=Picasa3 plugin
"Path"=C:\Program Files (x86)\Google\Picasa3\npPicasa3.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@java.com/DTPlugin,version=11.71.2]
"Description"=Java™ Deployment Toolkit
"Path"=C:\Program Files (x86)\Java\jre1.8.0_71\bin\dtplugin\npDeployJava1.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@java.com/JavaPlugin,version=11.71.2]
"Description"=Oracle® Next Generation Java™ Plug-In
"Path"=C:\Program Files (x86)\Java\jre1.8.0_71\bin\plugin2\npjp2.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@microsoft.com/GENUINE]
"Description"=
"Path"=disabled

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@microsoft.com/Lync,version=15.0]
"Description"=Microsoft Lync Plug-in for Firefox
"Path"=C:\Program Files (x86)\Microsoft Office\root\VFS\ProgramFilesX86\Mozilla Firefox\plugins\npmeetingjoinpluginoc.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@Microsoft.com/NpCtrl,version=1.0]
"Description"=Ag Player Plugin
"Path"=c:\Program Files (x86)\Microsoft Silverlight\5.1.50428.0\npctrl.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@microsoft.com/SharePoint,version=14.0]
"Description"=Microsoft SharePoint Plug-in for Firefox
"Path"=C:\Program Files (x86)\Microsoft Office\root\Office16\NPSPWRAP.DLL

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@microsoft.com/WLPG,version=15.4.3502.0922]
"Description"=WLPG Install MIME type
"Path"=C:\Program Files (x86)\Windows Live\Photo Gallery\NPWLPG.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@microsoft.com/WLPG,version=15.4.3538.0513]

```
"Description"=WLPG Install MIME type
"Path"=C:\Program Files (x86)\Windows Live\Photo Gallery\NPWLPG.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@real.com/nppl326
0;version=6.0.12.709]
"Description"=RealPlayer(tm) LiveConnect-Enabled Plug-In
"Path"=C:\Program Files (x86)\K-Lite Codec
Pack\Real\browser\plugins\nppl3260.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@real.com/nprpjpl
ug;version=6.0.12.709]
"Description"=6.0.12.709
"Path"=C:\Program Files (x86)\K-Lite Codec
Pack\Real\browser\plugins\nprpjplug.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@real.com/nsJSRea
lPlayerPlugin;version=]
"Description"=
"Path"=

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@tools.google.com
/Google Update;version=3]
"Description"=Google Update
"Path"=C:\Program Files (x86)\Google\Update\1.3.31.5\npGoogleUpdate3.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@tools.google.com
/Google Update;version=9]
"Description"=Google Update
"Path"=C:\Program Files (x86)\Google\Update\1.3.31.5\npGoogleUpdate3.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@WildTangent.com/
GamesAppPresenceDetector,Version=1.0]
"Description"=WildTangent Games App V2 Presence Detector Plugin
"Path"=C:\Program Files (x86)\WildTangent
Games\App\BrowserIntegration\Registered\0\NP_wtapp.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\Adobe Reader]
"Description"=Handles PDFs in-place in Firefox
"Path"=C:\Program Files (x86)\Adobe\Reader 10.0\Reader\AIR\nppdf32.dll


[HKEY_LOCAL_MACHINE\SOFTWARE\MozillaPlugins\@adobe.com/FlashPlayer]
"Description"=Adobe® Flash® Player 21.0.0.242 Plugin
"Path"=C:\Windows\system32\Macromed\Flash\NPSWF64_21_0_0_242.dll

[HKEY_LOCAL_MACHINE\SOFTWARE\MozillaPlugins\@microsoft.com/GENUINE]
"Description"=
"Path"=disabled

[HKEY_LOCAL_MACHINE\SOFTWARE\MozillaPlugins\@Microsoft.com/NpCtrl,version
=1.0]
"Description"=Ag Player Plugin
"Path"=c:\Program Files\Microsoft Silverlight\5.1.50428.0\npctrl.dll


C:\Program Files (x86)\Mozilla Firefox\plugins\
nppdf32.DEU
nppdf32.dll
```

nppdf32.FRA
nppdf32.JPN

======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 (x86)\Microsoft
Office\root\VFS\ProgramFilesX64\Microsoft Office\Office16\OCHelper.dll
[2016-07-31 231104]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Br
owser Helper Objects\{9030D464-4C02-4ABF-8ECC-5164760863C6}]
Windows Live ID Sign-in Helper - C:\Program Files\Common Files\Microsoft
Shared\Windows Live\WindowsLiveLogin.dll [2011-03-29 529280]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Br
owser Helper Objects\{990A8747-93BF-4EF7-B72E-94A6884B98C2}]
STATISTICA Browser Helper - C:\Program Files\StatSoft\STATISTICA
12\StaBHO.dll [2013-04-02 281088]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Br
owser Helper Objects\{B4F3A835-0E21-4959-BA22-42B3008E02FF}]
Office Document Cache Handler - C:\Program Files (x86)\Microsoft
Office\root\VFS\ProgramFilesX64\Microsoft Office\Office16\URLREDIR.DLL
[2016-07-31 586528]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Br
owser Helper Objects\{D0498E0A-45B7-42AE-A9AA-ABA463DBD3BF}]
Microsoft OneDrive for Business Browser Helper - C:\Program Files
(x86)\Microsoft Office\root\VFS\ProgramFilesX64\Microsoft
Office\Office16\GROOVEEX.DLL [2016-07-31 2095912]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Br
owser Helper Objects\{d2ce3e00-f94a-4740-988e-03dc2f38c34f}]
Bing Bar Helper - C:\Program Files
(x86)\Microsoft\BingBar\7.3.132.0\amd64\BingExt.dll [2014-03-11 1154720]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion
\Explorer\Browser Helper Objects\{31D09BA0-12F5-4CCE-BE8A-2923E76605DA}]
Lync Browser Helper - C:\Program Files (x86)\Microsoft
Office\root\Office16\OCHelper.dll [2016-07-31 170688]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion
\Explorer\Browser Helper Objects\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}]
Java(tm) Plug-In SSV Helper - C:\Program Files
(x86)\Java\jre1.8.0_71\bin\ssv.dll [2016-01-20 460384]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion
\Explorer\Browser Helper Objects\{9030D464-4C02-4ABF-8ECC-5164760863C6}]
Windows Live ID Sign-in Helper - C:\Program Files (x86)\Common
Files\Microsoft Shared\Windows Live\WindowsLiveLogin.dll [2011-03-29
441216]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion
\Explorer\Browser Helper Objects\{990A8747-93BF-4EF7-B72E-94A6884B98C2}]
STATISTICA Browser Helper - C:\Program Files\StatSoft\STATISTICA
12\Support\StaBHO.dll [2013-04-02 232448]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{B4F3A835-0E21-4959-BA22-42B3008E02FF}]
Office Document Cache Handler - C:\Program Files (x86)\Microsoft Office\root\Office16\URLREDIR.DLL [2016-07-31 414496]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{D0498E0A-45B7-42AE-A9AA-ABA463DBD3BF}]
Microsoft OneDrive for Business Browser Helper - C:\Program Files (x86)\Microsoft Office\root\Office16\GROOVEEX.DLL [2016-07-31 1538344]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{d2ce3e00-f94a-4740-988e-03dc2f38c34f}]
Bing Bar Helper - C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\BingExt.dll [2014-03-11 1431712]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{DBC80044-A445-435b-BC74-9C25C1C588A9}]
Java(tm) Plug-In 2 SSV Helper - C:\Program Files (x86)\Java\jre1.8.0_71\bin\jp2ssv.dll [2016-01-20 172640]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Toolbar]
{318A227B-5E9F-45bd-8999-7F8F10CA4CF5}
{8dcb7100-df86-4384-8842-8fa844297b3f} - Bing Bar - C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\amd64\BingExt.dll [2014-03-11 1154720]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Internet Explorer\Toolbar]
{8dcb7100-df86-4384-8842-8fa844297b3f} - Bing Bar - C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\BingExt.dll [2014-03-11 1431712]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
"AmIcoSinglun64"=C:\Program Files (x86)\AmIcoSingLun\AmIcoSinglun64.exe [2011-01-26 368728]
"IgfxTray"=C:\Windows\system32\igfxtray.exe [2011-05-09 168216]
"HotKeysCmds"=C:\Windows\system32\hkcmd.exe [2011-05-09 391960]
"Persistence"=C:\Windows\system32\igfxpers.exe [2011-05-09 419096]
"SynTPEnh"=C:\Program Files\Synaptics\SynTP\SynTPEnh.exe [2010-10-08 2392360]
"RTHDVCPL"=C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe [2011-06-09 11860072]
"Power Management"=C:\Program Files\Acer\Acer ePower Management\ePowerTray.exe [2011-08-02 1831016]
"CanonMyPrinter"=C:\Program Files\Canon\MyPrinter\BJMyPrt.exe [2011-03-14 2779024]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"Sidebar"=C:\Program Files\Windows Sidebar\sidebar.exe [2010-11-21 1475584]
"ctfmon32.exe"=C:\PROGRA~3\rundll32.exe C:\PROGRA~3\ito6z.dat,XFG00 []
"KurupiraNet"=C:\Program Files (x86)\Kurupira\WebFilter\kurupirawf.exe []
"RESTART_STICKY_NOTES"=C:\Windows\System32\StikyNot.exe [2009-07-14 427520]
"Skype"=C:\Program Files (x86)\Skype\Phone\Skype.exe [2016-08-22 29544576]

[HKEY_LOCAL_MACHINE\software\microsoft\shared tools\msconfig\startupreg\ICQ]

C:\Program Files (x86)\ICQ7.5\ICQ.exe [2011-08-01 124480]

[HKEY_LOCAL_MACHINE\software\microsoft\shared tools\msconfig\startupreg\Skype]
C:\Program Files (x86)\Skype\Phone\Skype.exe [2016-08-22 29544576]

[HKEY_LOCAL_MACHINE\software\microsoft\shared tools\msconfig\startupfolder\C:^Users^ACER^AppData^Roaming^Microsoft^Windows^Start Menu^Programs^Startup^regmonstd.lnk]
C:\PROGRA~3\ito6z.dat,XFG00 []

[HKEY_LOCAL_MACHINE\software\microsoft\shared tools\msconfig\startupfolder\C:^Users^ACER^AppData^Roaming^Microsoft^Windows^Start Menu^Programs^Startup^RUN.lnk]
D:\RUN.exe []

[HKEY_LOCAL_MACHINE\Software\wow6432node\Microsoft\Windows\CurrentVersion\Run]
"BackupManagerTray"=C:\Program Files (x86)\NTI\Acer Backup Manager\BackupManagerTray.exe [2011-04-24 297280]
"LManager"=C:\Program Files (x86)\Launch Manager\LManager.exe [2011-03-14 1081424]
"SuiteTray"=C:\Program Files (x86)\EgisTec MyWinLockerSuite\x86\SuiteTray.exe [2011-09-20 341360]
"ArcadeMovieService"=C:\Program Files (x86)\Acer\clear.fi\Movie\clear.fiMovieService.exe [2011-10-27 177448]
"Norton Online Backup"=C:\Program Files (x86)\Symantec\Norton Online Backup\NOBuClient.exe [2010-06-02 1155928]
""= []
"KurupiraNet"=C:\Program Files (x86)\Kurupira\WebFilter\kurupirawf.exe []
"CanonSolutionMenuEx"=C:\Program Files (x86)\Canon\Solution Menu EX\CNSEMAIN.EXE [2011-08-04 1612920]
"Clarus Drive Manager"=C:\Program Files (x86)\Clarus\Samsung Drive Manager\Drive Manager.exe [2013-12-18 8135744]
"SunJavaUpdateSched"=C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe [2015-12-22 596528]

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Samsung Drive Manager Real-Time.lnk - C:\Program Files (x86)\Clarus\Samsung Drive Manager\ABRTMon.exe
Virtual Router Manager.lnk - C:\Windows\Installer\{BE905C46-2B34-4D73-AEE1-769ED138E0FF}_118D1A4EFFA6998C3492EB.exe

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\igfxcui]
C:\Windows\system32\igfxdev.dll [2011-03-25 385024]

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

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

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

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

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\MCO
DS]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Sys
tem]
"LogonHoursAction"=2
"DontDisplayLogonHoursWarnings"=1

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Sy
stem]
"ConsentPromptBehaviorAdmin"=0
"ConsentPromptBehaviorUser"=3
"EnableLUA"=0
"EnableUIADesktopToggle"=0
"PromptOnSecureDesktop"=0
"dontdisplaylastusername"=0
"legalnoticecaption"=
"legalnoticetext"=
"shutdownwithoutlogon"=1
"undockwithoutlogon"=1

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

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\ex
plorer]
"NoActiveDesktop"=1
"NoActiveDesktopChanges"=1
"ForceActiveDesktopOn"=0

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

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

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Drivers32]
"vidc.mrle"=msrle32.dll
"vidc.msvc"=msvidc32.dll
"msacm.imaadpcm"=imaadp32.acm
"msacm.msg711"=msg711.acm
"msacm.msgsm610"=msgsm32.acm
"msacm.msadpcm"=msadp32.acm
"midimapper"=midimap.dll
"wavemapper"=msacm32.drv
"VIDC.UYVY"=msyuv.dll
"VIDC.YUY2"=msyuv.dll
"VIDC.YVYU"=msyuv.dll
"VIDC.IYUV"=iyuv_32.dll
"vidc.i420"=iyuv_32.dll
"VIDC.YVU9"=tsbyuv.dll
"msacm.l3acm"=C:\Windows\System32\l3codeca.acm
"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
"vidc.XVID"=xvidvfw.dll

======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 3 months======

2016-09-20 09:41:53 ----D---- C:\AdwCleaner
2016-09-19 17:41:13 ----A----
C:\Windows\system32\drivers\MBAMSwissArmy.sys
2016-09-19 17:38:47 ----A---- C:\Windows\system32\drivers\mwac.sys
2016-09-19 17:38:47 ----A----
C:\Windows\system32\drivers\mbamchameleon.sys
2016-09-19 17:38:47 ----A---- C:\Windows\system32\drivers\mbam.sys
2016-08-22 20:46:44 ----A---- C:\Windows\system32\drivers\ekbdflt.sys
2016-08-20 03:44:17 ----A---- C:\Windows\SYSWOW64\shortcut_ex.dat
2016-08-17 12:56:45 ----A---- C:\Windows\SYSWOW64\tzres.dll
2016-08-17 12:56:45 ----A---- C:\Windows\system32\tzres.dll
2016-08-10 21:04:52 ----A---- C:\Windows\SYSWOW64\mshtmled.dll
2016-08-10 21:04:52 ----A---- C:\Windows\SYSWOW64\inseng.dll
2016-08-10 21:04:52 ----A---- C:\Windows\SYSWOW64\iernonce.dll
2016-08-10 21:04:52 ----A---- C:\Windows\SYSWOW64\ieetwproxystub.dll
2016-08-10 21:04:52 ----A---- C:\Windows\system32\iernonce.dll
2016-08-10 21:04:52 ----A---- C:\Windows\system32\ieetwproxystub.dll
2016-08-10 21:04:52 ----A---- C:\Windows\system32\ieetwcollector.exe
2016-08-10 21:04:51 ----A---- C:\Windows\SYSWOW64\MshtmlDac.dll
2016-08-10 21:04:49 ----A---- C:\Windows\SYSWOW64\urlmon.dll
2016-08-10 21:04:49 ----A---- C:\Windows\SYSWOW64\occache.dll
2016-08-10 21:04:49 ----A---- C:\Windows\SYSWOW64\iedkcs32.dll
2016-08-10 21:04:49 ----A---- C:\Windows\system32\inseng.dll
2016-08-10 21:04:49 ----A---- C:\Windows\system32\ie4uinit.exe
2016-08-10 21:04:48 ----A---- C:\Windows\SYSWOW64\vbscript.dll
2016-08-10 21:04:48 ----A----
C:\Windows\SYSWOW64\JavaScriptCollectionAgent.dll
2016-08-10 21:04:47 ----A---- C:\Windows\SYSWOW64\msfeeds.dll
2016-08-10 21:04:47 ----A---- C:\Windows\SYSWOW64\dxtrans.dll
2016-08-10 21:04:47 ----A----
C:\Windows\system32\JavaScriptCollectionAgent.dll
2016-08-10 21:04:46 ----A---- C:\Windows\SYSWOW64\mshtml.dll
2016-08-10 21:04:42 ----A---- C:\Windows\SYSWOW64\iesetup.dll
2016-08-10 21:04:42 ----A---- C:\Windows\SYSWOW64\ieapfltr.dll
2016-08-10 21:04:42 ----A---- C:\Windows\system32\occache.dll
2016-08-10 21:04:41 ----A---- C:\Windows\system32\urlmon.dll
2016-08-10 21:04:41 ----A---- C:\Windows\system32\iedkcs32.dll
2016-08-10 21:04:40 ----A---- C:\Windows\SYSWOW64\jscript9diag.dll
2016-08-10 21:04:40 ----A---- C:\Windows\SYSWOW64\jscript.dll
2016-08-10 21:04:40 ----A---- C:\Windows\SYSWOW64\iertutil.dll
2016-08-10 21:04:40 ----A---- C:\Windows\system32\ieetwcollectorres.dll
2016-08-10 21:04:39 ----A---- C:\Windows\SYSWOW64\jsproxy.dll
```

```
2016-08-10 21:04:39 ----A----
C:\Windows\system32\MsSpellCheckingFacility.exe
2016-08-10 21:04:38 ----A---- C:\Windows\SYSWOW64\ieui.dll
2016-08-10 21:04:38 ----A---- C:\Windows\SYSWOW64\dxtmsft.dll
2016-08-10 21:04:38 ----A---- C:\Windows\system32\msfeeds.dll
2016-08-10 21:04:38 ----A---- C:\Windows\system32\dxtrans.dll
2016-08-10 21:04:37 ----A---- C:\Windows\SYSWOW64\ieframe.dll
2016-08-10 21:04:36 ----A---- C:\Windows\system32\iesetup.dll
2016-08-10 21:04:36 ----A---- C:\Windows\system32\ieapfltr.dll
2016-08-10 21:04:33 ----A---- C:\Windows\SYSWOW64\mshtmlmedia.dll
2016-08-10 21:04:33 ----A---- C:\Windows\system32\iertutil.dll
2016-08-10 21:04:32 ----A---- C:\Windows\SYSWOW64\ieUnatt.exe
2016-08-10 21:04:31 ----A---- C:\Windows\SYSWOW64\webcheck.dll
2016-08-10 21:04:31 ----A---- C:\Windows\SYSWOW64\jscript9.dll
2016-08-10 21:04:31 ----A---- C:\Windows\system32\vbscript.dll
2016-08-10 21:04:30 ----A---- C:\Windows\SYSWOW64\wininet.dll
2016-08-10 21:04:29 ----A---- C:\Windows\system32\jsproxy.dll
2016-08-10 21:04:28 ----A---- C:\Windows\SYSWOW64\msrating.dll
2016-08-10 21:04:25 ----A---- C:\Windows\system32\dxtmsft.dll
2016-08-10 21:04:24 ----A---- C:\Windows\system32\ieui.dll
2016-08-10 21:04:24 ----A---- C:\Windows\system32\ieframe.dll
2016-08-10 21:04:23 ----A---- C:\Windows\system32\mshtmlmedia.dll
2016-08-10 21:04:23 ----A---- C:\Windows\system32\mshtmled.dll
2016-08-10 21:04:22 ----A---- C:\Windows\system32\ieUnatt.exe
2016-08-10 21:04:21 ----A---- C:\Windows\system32\webcheck.dll
2016-08-10 21:04:20 ----A---- C:\Windows\system32\jscript.dll
2016-08-10 21:04:19 ----A---- C:\Windows\system32\jscript9diag.dll
2016-08-10 21:04:17 ----A---- C:\Windows\system32\jscript9.dll
2016-08-10 21:04:15 ----A---- C:\Windows\system32\wininet.dll
2016-08-10 21:04:12 ----A---- C:\Windows\system32\msrating.dll
2016-08-10 21:04:12 ----A---- C:\Windows\system32\MshtmlDac.dll
2016-08-10 21:04:10 ----A---- C:\Windows\system32\mshtml.dll
2016-08-10 21:03:10 ----A---- C:\Windows\system32\schannel.dll
2016-08-10 21:03:10 ----A---- C:\Windows\system32\lsasrv.dll
2016-08-10 21:03:08 ----A---- C:\Windows\SYSWOW64\schannel.dll
2016-08-10 21:03:08 ----A---- C:\Windows\SYSWOW64\certcli.dll
2016-08-10 21:03:08 ----A---- C:\Windows\system32\rpcrt4.dll
2016-08-10 21:03:08 ----A---- C:\Windows\system32\drivers\ksecpkg.sys
2016-08-10 21:03:08 ----A---- C:\Windows\system32\drivers\ksecdd.sys
2016-08-10 21:03:08 ----A---- C:\Windows\system32\certcli.dll
2016-08-10 21:03:07 ----A---- C:\Windows\SYSWOW64\rpcrt4.dll
2016-08-10 21:03:07 ----A---- C:\Windows\system32\drivers\mrxsmb.sys
2016-08-10 21:03:06 ----A---- C:\Windows\SYSWOW64\sspicli.dll
2016-08-10 21:03:06 ----A---- C:\Windows\SYSWOW64\kerberos.dll
2016-08-10 21:03:06 ----A---- C:\Windows\system32\TSpkg.dll
2016-08-10 21:03:06 ----A---- C:\Windows\system32\ncrypt.dll
2016-08-10 21:03:06 ----A---- C:\Windows\system32\msv1_0.dll
2016-08-10 21:03:06 ----A---- C:\Windows\system32\kerberos.dll
2016-08-10 21:03:06 ----A---- C:\Windows\system32\drivers\mrxsmb10.sys
2016-08-10 21:03:05 ----A---- C:\Windows\SYSWOW64\msv1_0.dll
2016-08-10 21:03:05 ----A---- C:\Windows\system32\wdigest.dll
2016-08-10 21:03:05 ----A---- C:\Windows\system32\sspicli.dll
2016-08-10 21:03:05 ----A---- C:\Windows\system32\rpchttp.dll
2016-08-10 21:03:05 ----A---- C:\Windows\system32\drivers\mrxsmb20.sys
2016-08-10 21:03:04 ----A---- C:\Windows\SYSWOW64\wdigest.dll
2016-08-10 21:03:04 ----A---- C:\Windows\SYSWOW64\TSpkg.dll
2016-08-10 21:03:04 ----A---- C:\Windows\SYSWOW64\secur32.dll
2016-08-10 21:03:04 ----A---- C:\Windows\SYSWOW64\rpchttp.dll
```

```
2016-08-10 21:03:04 ----A---- C:\Windows\SYSWOW64\ncrypt.dll
2016-08-10 21:03:04 ----A---- C:\Windows\system32\sspisrv.dll
2016-08-10 21:03:04 ----A---- C:\Windows\system32\secur32.dll
2016-08-10 21:03:04 ----A---- C:\Windows\system32\lsass.exe
2016-08-10 21:03:04 ----A---- C:\Windows\system32\cryptbase.dll
2016-08-10 21:03:04 ----A---- C:\Windows\system32\credssp.dll
2016-08-10 21:03:03 ----A---- C:\Windows\SYSWOW64\cryptbase.dll
2016-08-10 21:03:02 ----A---- C:\Windows\SYSWOW64\credssp.dll
2016-08-10 21:03:02 ----A---- C:\Windows\SYSWOW64\auditpol.exe
2016-08-10 21:03:02 ----A---- C:\Windows\system32\auditpol.exe
2016-08-10 21:03:00 ----A---- C:\Windows\SYSWOW64\msobjs.dll
2016-08-10 21:03:00 ----A---- C:\Windows\SYSWOW64\msaudite.dll
2016-08-10 21:03:00 ----A---- C:\Windows\SYSWOW64\adtschema.dll
2016-08-10 21:03:00 ----A---- C:\Windows\system32\msobjs.dll
2016-08-10 21:03:00 ----A---- C:\Windows\system32\msaudite.dll
2016-08-10 21:03:00 ----A---- C:\Windows\system32\adtschema.dll
2016-08-10 20:40:21 ----A---- C:\Windows\system32\win32k.sys
2016-08-10 11:53:13 ----D---- C:\Program Files (x86)\ESET
2016-08-02 10:08:59 ----D---- C:\Program Files (x86)\Virtual Router
2016-08-02 09:55:27 ----SHD---- C:\AppCache
2016-07-30 02:39:25 ----D---- C:\Users\ACER\AppData\Roaming\Apowersoft
2016-07-25 22:02:23 ----A---- C:\Windows\SYSWOW64\sho4FF7.tmp
2016-07-24 16:56:03 ----A---- C:\Windows\system32\localspl.dll
2016-07-24 16:56:02 ----A---- C:\Windows\SYSWOW64\win32spl.dll
2016-07-24 16:56:02 ----A---- C:\Windows\SYSWOW64\ntprint.exe
2016-07-24 16:56:02 ----A---- C:\Windows\SYSWOW64\ntprint.dll
2016-07-24 16:56:02 ----A---- C:\Windows\system32\wpnpinst.exe
2016-07-24 16:56:02 ----A---- C:\Windows\system32\win32spl.dll
2016-07-24 16:56:02 ----A---- C:\Windows\system32\ntprint.exe
2016-07-24 16:56:02 ----A---- C:\Windows\system32\ntprint.dll
2016-07-24 16:56:02 ----A---- C:\Windows\system32\inetppui.dll
2016-07-24 16:56:02 ----A---- C:\Windows\system32\inetpp.dll
2016-07-24 16:55:58 ----A---- C:\Windows\system32\invagent.dll
2016-07-24 16:55:58 ----A---- C:\Windows\system32\devinv.dll
2016-07-24 16:55:58 ----A---- C:\Windows\system32\appraiser.dll
2016-07-24 16:55:58 ----A---- C:\Windows\system32\aepic.dll
2016-07-24 16:55:58 ----A---- C:\Windows\system32\aeinv.dll
2016-07-24 16:55:57 ----A---- C:\Windows\system32\generaltel.dll
2016-07-24 16:55:57 ----A---- C:\Windows\system32\CompatTelRunner.exe
2016-07-24 16:55:57 ----A---- C:\Windows\system32\centel.dll
2016-07-24 16:55:57 ----A---- C:\Windows\system32\acmigration.dll

======List of files/folders modified in the last 3 months======

2016-09-20 12:33:20 ----D---- C:\Windows\Temp
2016-09-20 12:33:19 ----D---- C:\Program Files\trend micro
2016-09-20 09:57:14 ----SD---- C:\Users\ACER\AppData\Roaming\Microsoft
2016-09-20 09:17:45 ----D---- C:\Users\ACER\AppData\Roaming\Skype
2016-09-20 09:16:08 ----A---- C:\Windows\SYSWOW64\log.txt
2016-09-20 09:14:12 ----D---- C:\ProgramData\clear.fi
2016-09-20 09:13:42 ----D---- C:\Windows\system32\config
2016-09-20 09:00:57 ----A---- C:\Windows\ntbtlog.txt
2016-09-19 20:48:39 ----D---- C:\Windows\winsxs
2016-09-19 20:46:23 ----D---- C:\Windows\system32\catroot2
2016-09-19 20:29:01 ----D---- C:\Windows\system32\drivers
2016-09-19 20:29:01 ----D---- C:\Windows\pt-pt
2016-09-19 20:00:11 ----D---- C:\Windows\System32
2016-09-19 20:00:11 ----D---- C:\Windows\inf
```

```
2016-09-19 20:00:11 ----A---- C:\Windows\system32\PerfStringBackup.INI
2016-09-19 17:39:23 ----D---- C:\Program Files (x86)\Malwarebytes Anti-
Malware
2016-09-19 08:18:54 ----D---- C:\Program Files (x86)\Mozilla Firefox
2016-09-19 07:51:09 ----SHD---- C:\Windows\Installer
2016-09-19 07:51:00 ----RD---- C:\Program Files (x86)\Skype
2016-09-19 07:50:31 ----D---- C:\ProgramData\Skype
2016-09-18 02:02:06 ----D---- C:\Windows\Minidump
2016-09-18 02:02:04 ----D---- C:\Windows
2016-09-18 01:49:48 ----D---- C:\Users\ACER\AppData\Roaming\SoftGrid
Client
2016-09-17 16:37:23 ----D---- C:\Program Files (x86)\Opera
2016-09-17 16:37:22 ----D---- C:\Windows\system32\Tasks
2016-08-31 23:19:56 ----D---- C:\Windows\Microsoft.NET
2016-08-30 18:43:45 ----SHD---- C:\System Volume Information
2016-08-24 16:16:53 ----D---- C:\Windows\rescache
2016-08-22 20:47:11 ----D---- C:\Windows\system32\DriverStore
2016-08-21 18:49:34 ----D---- C:\Users\ACER\AppData\Roaming\Synthesia
2016-08-20 03:44:18 ----D---- C:\Windows\SysWOW64
2016-08-19 08:27:43 ----D---- C:\ProgramData\regid.1991-06.com.microsoft
2016-08-19 08:23:47 ----D---- C:\Program Files (x86)\Microsoft Office
2016-08-17 16:13:34 ----D---- C:\Windows\SYSWOW64\sk-SK
2016-08-17 16:13:34 ----D---- C:\Windows\system32\sk-SK
2016-08-10 23:01:44 ----D---- C:\Windows\SYSWOW64\en-US
2016-08-10 23:01:43 ----D---- C:\Windows\system32\en-US
2016-08-10 23:01:39 ----D---- C:\Program Files\Internet Explorer
2016-08-10 23:01:27 ----D---- C:\Program Files (x86)\Internet Explorer
2016-08-10 22:20:56 ----D---- C:\Windows\system32\MRT
2016-08-10 22:09:35 ----AC---- C:\Windows\system32\MRT.exe
2016-08-10 11:53:13 ----RD---- C:\Program Files (x86)
2016-08-02 10:13:20 ----D---- C:\Windows\system32\drivers\etc
2016-07-29 00:50:55 ----D---- C:\Windows\Tasks
2016-07-27 19:30:31 ----RSD---- C:\Windows\assembly
2016-07-26 14:24:24 ----N---- C:\Windows\system32\MpSigStub.exe
2016-07-24 18:07:49 ----D---- C:\Program Files\Windows Journal
2016-07-24 18:07:47 ----D---- C:\Windows\system32\appraiser
2016-07-24 18:07:42 ----SD---- C:\Windows\SYSWOW64\GWX
2016-07-24 18:07:42 ----SD---- C:\Windows\system32\GWX
2016-07-24 18:07:41 ----D---- C:\Windows\AppPatch
2016-07-06 23:06:49 ----D---- C:\Windows\Prefetch
2016-06-30 23:55:06 ----A---- C:\Windows\SYSWOW64\PerfStringBackup.INI
2016-06-23 19:26:32 ----D---- C:\Program Files\Microsoft Silverlight
2016-06-23 19:26:28 ----D---- C:\Program Files (x86)\Microsoft
Silverlight

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

R0 epfwwfp;epfwwfp; C:\Windows\system32\DRIVERS\epfwwfp.sys [2016-08-22
84640]
R0 iaStor;Intel AHCI Controller; C:\Windows\system32\drivers\iaStor.sys
[2010-09-14 437272]
R0 rdyboost;ReadyBoost; C:\Windows\System32\drivers\rdyboost.sys [2010-
11-21 213888]
R1 eamonm;eamonm; C:\Windows\system32\DRIVERS\eamonm.sys [2016-08-22
263296]
R1 ehdrv;ehdrv; C:\Windows\system32\DRIVERS\ehdrv.sys [2016-08-22 197288]
R1 epfw;epfw; C:\Windows\system32\DRIVERS\epfw.sys [2016-08-22 208552]
```

R1 EpfwLWF;ESET Personal Firewall;
C:\Windows\system32\DRIVERS\EpfwLWF.sys [2016-08-22 61608]
R1 mwlPSDFilter;mwlPSDFilter;
C:\Windows\system32\DRIVERS\mwlPSDFilter.sys [2012-01-17 22648]
R1 mwlPSDNServ;mwlPSDNServ; C:\Windows\system32\DRIVERS\mwlPSDNServ.sys [2012-01-17 20520]
R1 mwlPSDVDisk;mwlPSDVDisk; C:\Windows\system32\DRIVERS\mwlPSDVDisk.sys [2012-01-17 62776]
R1 vwififlt;Virtual WiFi Filter Driver;
C:\Windows\system32\DRIVERS\vwififlt.sys [2009-07-14 59904]
R2 ekbdflt;ekbdflt; C:\Windows\system32\DRIVERS\ekbdflt.sys [2016-08-22 153248]
R3 athr;Atheros Extensible Wireless LAN device driver;
C:\Windows\system32\DRIVERS\athrx.sys [2011-03-17 2712064]
R3 igfx;igfx; C:\Windows\system32\DRIVERS\igdkmd64.sys [2011-03-25 12262336]
R3 IntcAzAudAddService;Service for Realtek HD Audio (WDM);
C:\Windows\system32\drivers\RTKVHD64.sys [2011-06-14 2899176]
R3 IntcDAud;Intel(R) Display Audio;
C:\Windows\system32\DRIVERS\IntcDAud.sys [2010-10-14 317440]
R3 L1C;NDIS Miniport Driver for Atheros AR813x/AR815x PCI-E Ethernet Controller; C:\Windows\system32\DRIVERS\L1C62x64.sys [2011-04-20 169584]
R3 mdf16;mdf16; \??\C:\Program Files (x86)\Clarus\Samsung Drive Manager\mdf16.sys [2012-06-21 20400]
R3 MEIx64;Intel(R) Management Engine Interface;
C:\Windows\system32\DRIVERS\HECIx64.sys [2010-10-19 56344]
R3 mvd23;mvd23; \??\C:\Program Files (x86)\Clarus\Samsung Drive Manager\mvd23.sys [2012-06-21 99248]
R3 NTIDrvr;NTIDrvr; \??\C:\Windows\system32\drivers\NTIDrvr.sys [2011-09-20 18432]
R3 Sftfs;Sftfs; C:\Windows\system32\DRIVERS\Sftfslh.sys [2009-12-02 721768]
R3 Sftplay;Sftplay; C:\Windows\system32\DRIVERS\Sftplaylh.sys [2009-12-02 269672]
R3 Sftredir;Sftredir; C:\Windows\system32\DRIVERS\Sftredirlh.sys [2009-12-02 25960]
R3 Sftvol;Sftvol; C:\Windows\system32\DRIVERS\Sftvollh.sys [2009-12-02 22376]
R3 SynTP;Synaptics TouchPad Driver; C:\Windows\system32\DRIVERS\SynTP.sys [2010-10-08 1395248]
R3 UBHelper;UBHelper; \??\C:\Windows\system32\drivers\UBHelper.sys [2011-09-20 17408]
R3 vwifimp;Microsoft Virtual WiFi Miniport Service;
C:\Windows\system32\DRIVERS\vwifimp.sys [2009-07-14 17920]
S3 AmUStor;AM USB Stroage Driver; C:\Windows\system32\drivers\AmUStor.SYS [2011-01-14 74840]
S3 HWiNFO32;HWiNFO32/64 Kernel Driver;
\??\C:\Users\ACER\AppData\Local\Temp\HWiNFO64A.SYS []
S3 pciide;pciide; C:\Windows\system32\drivers\pciide.sys [2009-07-14 12352]
S3 TsUsbFlt;TsUsbFlt; C:\Windows\system32\drivers\tsusbflt.sys [2010-11-21 59392]
S3 TsUsbGD;Remote Desktop Generic USB Device;
C:\Windows\system32\drivers\TsUsbGD.sys [2010-11-21 31232]
S3 usbscan;USB Scanner Driver; C:\Windows\system32\DRIVERS\usbscan.sys [2013-07-03 42496]
S3 WinUsb;WinUsb; C:\Windows\system32\DRIVERS\WinUsb.sys [2010-11-21 41984]

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

R2 AdobeARMservice;Adobe Acrobat Update Service; C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe [2016-09-08 82128]
R2 ClickToRunSvc;Služba Microsoft Office Klikni a spusť; C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe [2016-07-31 2854640]
R2 cvhsvc;Client Virtualization Handler; C:\Program Files (x86)\Common Files\Microsoft Shared\Virtualization Handler\CVHSVC.EXE [2010-02-28 821664]
R2 DiagTrack;@%SystemRoot%\system32\UtcResources.dll,-3001; C:\Windows\System32\svchost.exe [2009-07-14 27136]
R2 DsiWMIService;Dritek WMI Service; C:\Program Files (x86)\Launch Manager\dsiwmis.exe [2011-03-14 352336]
R2 ekrn;ESET Service; C:\Program Files\ESET\ESET Smart Security\ekrn.exe [2016-08-22 2780160]
R2 ePowerSvc;ePower Service; C:\Program Files\Acer\Acer ePower Management\ePowerSvc.exe [2011-08-02 872552]
R2 GREGService;GREGService; C:\Program Files (x86)\Acer\Registration\GREGsvc.exe [2011-05-30 36456]
R2 IAStorDataMgrSvc;Intel(R) Rapid Storage Technology; C:\Program Files (x86)\Intel\Intel(R) Rapid Storage Technology\IAStorDataMgrSvc.exe [2010-09-14 13336]
R2 KNet;KNet; C:\Windows\svcproxy\svcproxy.exe [2012-07-16 3557560]
R2 Live Updater Service;Live Updater Service; C:\Program Files\Acer\Acer Updater\UpdaterService.exe [2011-04-22 244624]
R2 LMS;Intel(R) Management and Security Application Local Management Service; C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe [2011-02-01 326168]
R2 NOBU;Norton Online Backup; C:\Program Files (x86)\Symantec\Norton Online Backup\NOBuAgent.exe [2010-06-02 2804568]
R2 NTI IScheduleSvc;NTI IScheduleSvc; C:\Program Files (x86)\NTI\Acer Backup Manager\IScheduleSvc.exe [2011-04-24 256832]
R2 PSI_SVC_2;Protexis Licensing V2; c:\Program Files (x86)\Common Files\Protexis\License Service\PsiService_2.exe [2010-03-10 189728]
R2 sftlist;Application Virtualization Client; C:\Program Files (x86)\Microsoft Application Virtualization Client\sftlist.exe [2009-12-02 483688]
R2 svcprocess;Process Control; C:\Windows\svcproxy\svcprocess.exe [2012-07-16 166072]
R2 SZDrvSvc;Samsung Drive Manager Service; C:\Program Files (x86)\Clarus\Samsung Drive Manager\SZDrvSvc.exe [2013-12-18 18432]
R2 UNS;Intel(R) Management and Security Application User Notification Service; C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\UNS\UNS.exe [2011-02-01 2656280]
R2 Virtual Router;VirtualRouterService; C:\Program Files (x86)\Virtual Router\VirtualRouterService.exe [2013-02-10 12288]
R3 BBUpdate;BBUpdate; C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\SeaPort.exe [2014-03-11 247968]
R3 sftvsa;Application Virtualization Service Agent; C:\Program Files (x86)\Microsoft Application Virtualization Client\sftvsa.exe [2009-12-02 209768]
R3 wlidsvc;Windows Live ID Sign-in Assistant; C:\Program Files\Common Files\Microsoft Shared\Windows Live\WLIDSVC.EXE [2011-03-29 2292096]
S2 BBSvc;BingBar Service; C:\Program Files (x86)\Microsoft\BingBar\7.3.132.0\BBSvc.exe [2014-03-11 193696]

S2 clr_optimization_v4.0.30319_32;Microsoft .NET Framework NGEN v4.0.30319_X86; C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe [2015-11-05 105144]
S2 clr_optimization_v4.0.30319_64;Microsoft .NET Framework NGEN v4.0.30319_X64; C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe [2015-11-05 125112]
S2 gupdate;Služba Google Update (gupdate); C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [2015-09-01 144200]
S2 SkypeUpdate;Skype Updater; C:\Program Files (x86)\Skype\Updater\Updater.exe [2016-07-25 324224]
S3 EgisTec Ticket Service;EgisTec Ticket Service; C:\Program Files (x86)\Common Files\EgisTec\Services\EgisTicketService.exe [2011-06-21 173424]
S3 FLEXnet Licensing Service;FLEXnet Licensing Service; C:\Program Files (x86)\Common Files\Macrovision Shared\FLEXnet Publisher\FNPLicensingService.exe [2012-01-17 655624]
S3 GamesAppService;GamesAppService; C:\Program Files (x86)\WildTangent Games\App\GamesAppService.exe [2010-10-12 206072]
S3 gupdatem;Služba Google Update (gupdatem); C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [2015-09-01 144200]
S3 gusvc;Google Updater Service; C:\Program Files (x86)\Google\Common\Google Updater\GoogleUpdaterService.exe [2014-08-13 136120]
S3 IEEtwCollectorService;@%SystemRoot%\system32\ieetwcollectorres.dll,-1000; C:\Windows\system32\IEEtwCollector.exe [2016-08-02 114688]
S3 MozillaMaintenance;Mozilla Maintenance Service; C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe [2016-01-02 147624]
S3 ose;Office Source Engine; C:\Program Files (x86)\Common Files\Microsoft Shared\Source Engine\OSE.EXE [2016-07-31 212184]
S3 osppsvc;Office Software Protection Platform; C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE [2016-04-02 5132888]
S3 WatAdminSvc;@%SystemRoot%\system32\Wat\WatUX.exe,-601; C:\Windows\system32\Wat\WatAdminSvc.exe [2012-08-05 1255736]
S4 aspnet_state;ASP.NET State Service; C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe [2015-11-05 51376]
S4 NetMsmqActivator;@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelInstallRC.dll,-8195; C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe [2015-11-05 135848]
S4 NetPipeActivator;@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelInstallRC.dll,-8197; C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe [2015-11-05 135848]
S4 NetTcpActivator;@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelInstallRC.dll,-8199; C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe [2015-11-05 135848]
S4 wlcrasvc;Windows Live Mesh remote connections service; C:\Program Files\Windows Live\Mesh\wlcrasvc.exe [2010-09-23 57184]

----------EOF----------