

Forum:[Hack Forums](#)

Thread: [My PC is completely fucked up](#)

Malacka - January 4, 2011, 8:50 am

I had a Bluescreen of Death after it my pc won't run any programs, I click on shortcuts, but it won't do anything, I can run them via Windows Explorer, System restore isn't working, it says VSS not working bla bla bla, did malwarebytes search, idk if my HDD is bad or idk :(Please help!

Quote:Logfile of HijackThis v1.99.1

Scan saved at 17:13:40, on 2011.01.04.

Platform: Unknown Windows (WinNT 6.01.3504)

MSIE: Internet Explorer v8.00 (8.00.7600.16385)

Running processes:

C:\Users\Malacka\AppData\Local\Google\Update\GoogleUpdate.exe

C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe

C:\Windows\SysWOW64\DllHost.exe

C:\Program Files (x86)\Malwarebytes' Anti-Malware\mbam.exe

C:\Program Files (x86)\Hijackthis\HijackThis.exe

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://go.microsoft.com/fwlink/?LinkId=69157>

R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL =

<http://go.microsoft.com/fwlink/?LinkId=69157>

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/?LinkId=69157>

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,ProxyOverride = *.local

R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName =

F2 - REG:system.ini: UserInit=userinit.exe

O1 - Hosts: 74.208.10.249 gs.apple.com

O2 - BHO: Windows Live ID bejelentkezési segítség -

{9030D464-4C02-4ABF-8ECC-5164760863C6} - C:\Program Files (x86)\Common Files\Microsoft Shared\Windows Live\WindowsLiveLogin.dll

O2 - BHO: SkypeIEPluginBHO - {AE805869-2E5C-4ED4-8F7B-F1F7851A4497} - C:\Program Files (x86)\Skype\Toolbars\Internet Explorer\skypeieplugin.dll

O2 - BHO: Java™ Plug-In 2 SSV Helper - {DBC80044-A445-435b-BC74-9C25C1C588A9} - C:\Program Files (x86)\Java\jre6\bin\jp2ssv.dll

O4 - HKLM\..\Run: [QuickTime Task] "C:\Program Files (x86)\QuickTime\QTTask.exe" -atboottime

O4 - HKLM\..\Run: [iTunesHelper] "C:\Program Files (x86)\iTunes\iTunesHelper.exe"

O4 - HKLM\..\Run: [SunJavaUpdateSched] "C:\Program Files (x86)\Common Files\Java\Java

Update\jusched.exe"

O4 - HKLM\..\RunOnce: [Malwarebytes' Anti-Malware] C:\Program Files (x86)\Malwarebytes' Anti-Malware\mbamgui.exe /install /silent

O4 - HKCU\..\Run: [Google Update]

"C:\Users\Malacka\AppData\Local\Google\Update\GoogleUpdate.exe" /c

O4 - HKCU\..\Run: [msnmsgr] "D:\Program Files\Windows Live\Messenger\msnmsgr.exe" /background

O9 - Extra button: Skype Plug-In - {898EA8C8-E7FF-479B-8935-AEC46303B9E5} - C:\Program Files (x86)\Skype\Toolbars\Internet Explorer\skypeieplugin.dll

O9 - Extra 'Tools' menuitem: Skype Plug-In - {898EA8C8-E7FF-479B-8935-AEC46303B9E5} - C:\Program Files (x86)\Skype\Toolbars\Internet Explorer\skypeieplugin.dll

O10 - Unknown file in Winsock LSP: c:\windows\system32\nlaapi.dll

O10 - Unknown file in Winsock LSP: c:\windows\system32\napinsp.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:\program files (x86)\common files\microsoft shared\windows live\wlidnsp.dll

O10 - Unknown file in Winsock LSP: c:\program files (x86)\bonjour\mdnssnp.dll

O11 - Options group: [INTERNATIONAL] International

O13 - Gopher Prefix:

O16 - DPF: {E2883E8F-472F-4FB0-9522-AC9BF37916A7} -

<http://platformdl.adobe.com/NOS/getPlusPlus/1.6/gp.cab>

O18 - Protocol: livecall - {828030A1-22C1-4009-854F-8E305202313F} - C:\Program Files (x86)\Windows Live\Messenger\msgrapp.dll

O18 - Protocol: msnim - {828030A1-22C1-4009-854F-8E305202313F} - C:\Program Files (x86)\Windows Live\Messenger\msgrapp.dll

O18 - Protocol: skype-ie-addon-data - {91774881-D725-4E58-B298-07617B9B86A8} - C:\Program Files (x86)\Skype\Toolbars\Internet Explorer\skypeieplugin.dll

O18 - Protocol: skype4com - {FFC8B962-9B40-4DFF-9458-1830C7DD7F5D} - C:\PROGRA~2\COMMON~1\Skype\SKYPE4~1.DLL

O23 - Service: @%SystemRoot%\system32\Alg.exe,-112 (ALG) - Unknown owner - C:\Windows\System32\alg.exe (file missing)

O23 - Service: Apple Mobile Device - Apple Inc. - C:\Program Files (x86)\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe

O23 - Service: AppleChargerSrv - Unknown owner - C:\Windows\system32\AppleChargerSrv.exe (file missing)

O23 - Service: Bonjour Service - Apple Inc. - C:\Program Files (x86)\Bonjour\mDNSResponder.exe

O23 - Service: @%SystemRoot%\system32\efssvc.dll,-100 (EFS) - Unknown owner - C:\Windows\System32\lsass.exe (file missing)

O23 - Service: @%systemroot%\system32\fxsresm.dll,-118 (Fax) - Unknown owner - C:\Windows\system32\fxssvc.exe (file missing)

O23 - Service: iPod Service - Apple Inc. - C:\Program Files\iPod\bin\iPodService.exe

O23 - Service: @keyiso.dll,-100 (KeyIso) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)

O23 - Service: Intel® Management and Security Application Local Management Service (LMS) - Intel Corporation - C:\Program Files (x86)\Intel\Intel® Management Engine Components\LMS\LMS.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: NVIDIA Display Driver Service (nvsvc) - Unknown owner - C:\Windows\system32\nvsvc.exe (file missing)

O23 - Service: OpenVPN Service (OpenVPNService) - Unknown owner - C:\Program Files (x86)\OpenVPN\bin\openvpnserv.exe

O23 - Service: @%systemroot%\system32\psbase.dll,-300 (ProtectedStorage) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)

O23 - Service: @%SystemRoot%\system32\qwave.dll,-1 (QWAVE) - Unknown owner - %windir%\system32\svchost.exe (file missing)

O23 - Service: @%systemroot%\system32\Locator.exe,-2 (RpcLocator) - Unknown owner - C:\Windows\system32\locator.exe (file missing)

O23 - Service: @%SystemRoot%\system32\samsrv.dll,-1 (SamSs) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)

O23 - Service: @%SystemRoot%\system32\seclogon.dll,-7001 (seclogon) - Unknown owner - %windir%\system32\svchost.exe (file missing)

O23 - Service: @%SystemRoot%\system32\snmptrap.exe,-3 (SNMPTRAP) - Unknown owner - C:\Windows\System32\snmptrap.exe (file missing)

O23 - Service: @%systemroot%\system32\spoolsv.exe,-1 (Spooler) - Unknown owner - C:\Windows\System32\spoolsv.exe (file missing)

O23 - Service: @%SystemRoot%\system32\sppsvc.exe,-101 (sppsvc) - Unknown owner - C:\Windows\system32\sppsvc.exe (file missing)

O23 - Service: @%SystemRoot%\system32\ui0detect.exe,-101 (UI0Detect) - Unknown owner - C:\Windows\system32\UI0Detect.exe (file missing)

O23 - Service: Intel® Management & Security Application User Notification Service (UNS) - Intel Corporation - C:\Program Files (x86)\Intel\Intel® 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: @%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 - %PROGRAMFILES%\Windows Media Player\wmpnetwk.exe (file missing)

I don't know if its a virus, pleas help!

Infallible - January 4, 2011, 10:43 am

Please download [OTL](#) to your Desktop. (If you already have it downloaded, then just follow the instructions below). Double click on the icon to run it. Make sure all other windows are closed and to let it run uninterrupted.

Under the Custom Scan box paste this in

```
%systemroot%\*. /mp /s
%systemroot%\system32\*.dll /lockedfiles
%systemroot%\system32\*.exe /lockedfiles
%systemroot%\Tasks\*.job /lockedfiles
%systemroot%\system32\drivers\*.sys /lockedfiles
%systemroot%\System32\config\*.sav
```

%systemroot%\system32*.sys
%systemroot%\system32\drivers*.dll
%systemroot%\system32\drivers*.ini
%systemroot%\system32\drivers*.exe
%SYSTEMDRIVE%*.*
%PROGRAMFILES%*.*
%appdata%*.*
netsvcs
msconfig
safebootminimal
safebootnetwork
activex
drivers32
/md5start
eventlog.dll
scecli.dll
netlogon.dll
cngaudit.dll
sceclt.dll
ntelogon.dll
logevent.dll
iaStor.sys
nvstor.sys
atapi.sys
IdeChnDr.sys
viasraid.sys
AGP440.sys
vaxscsi.sys
nvatabus.sys
viamraid.sys
nvata.sys
nvgts.sys
iastorv.sys
ViPrt.sys
eNetHook.dll
ahcix86.sys
KR10N.sys
disk.sys
nvstor32.sys
ahcix86s.sys
nvr32.sys
symmpi.sys
adp3132.sys
mv61xx.sys
usbstor.sys
/md5stop
CREATERESTOREPOINT
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto
Update\Results\Install\LastSuccessTime /rs

Click the Run Scan button. Do not change any settings unless otherwise told to do so. The scan wont take long. When the scan completes, it will open two notepad windows. OTL.Txt and Extras.Txt

. These are saved in the same location as OTL.

Please copy (Edit->Select All, Edit->Copy) and paste (Edit->Paste) the contents of these files, one at a time

Note: in the event that OTL fails to run, please use alternate download links to try again:

<http://oldtimer.geekstogo.com/OTL.com>

<http://oldtimer.geekstogo.com/OTL.scr>