

# .dll

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2004-05/0808.html>

---

**From:** Holly (*anonymous\_at\_discussions.microsoft.com*)

**Date:** 05/10/04

Date: Sun, 9 May 2004 17:36:55 -0700

Logfile of HijackThis v1.97.7

Scan saved at 8:48:56 AM, on 5/9/2004

Platform: Windows XP SP1 (WinNT 5.01.2600)

MSIE: Internet Explorer v6.00 SP1 (6.00.2800.1106)

Running processes:

C:\WINNT\System32\smss.exe

C:\WINNT\system32\winlogon.exe

C:\WINNT\system32\services.exe

C:\WINNT\system32\lsass.exe

C:\WINNT\system32\svchost.exe

C:\WINNT\System32\svchost.exe

C:\WINNT\system32\rundll32.exe

C:\Program Files\Common Files\Symantec Shared\ccSetMgr.exe

C:\Program Files\Common Files\Symantec Shared\ccEvtMgr.exe

C:\WINNT\system32\spoolsv.exe

C:\WINNT\Explorer.EXE

C:\WINNT\GWMDMMSG.exe

C:\Program Files\Synaptics\SynTP\SynTPLpr.exe

C:\Program Files\Synaptics\SynTP\SynTPEnh.exe

C:\WINNT\System32\hkcmd.exe

C:\Program Files\Gateway Utilities\GWInkMonitor.exe

C:\Program Files\Roxio\Easy CD Creator 5

\DirectCD\DirectCD.exe

C:\Program Files\Common Files\Real\Update\_OB\realsched.exe

C:\Program Files\Support.com\bin\tgcmd.exe

C:\Program Files\MUSICMATCH\MUSICMATCH Jukebox\mmtask.exe

C:\Program Files\Common Files\Symantec Shared\ccApp.exe

C:\Program Files\QuickTime\qttask.exe

C:\Program Files\Winamp\winampa.exe

C:\Program Files\Viewpoint\Viewpoint Manager\ViewMgr.exe

C:\PROGRA~1\twomediadebug\acidroad.exe

C:\PROGRA~1\ZONELA~1\ZONEAL~1\zlclient.exe

C:\Program Files\MSN Messenger\msnmgr.exe

C:\Program Files\Common Files\Microsoft Shared\Works  
Shared\WkCalRem.exe

C:\Program Files\Norton AntiVirus\navapvc.exe

C:\Program Files\Norton AntiVirus\SAVScan.exe

microsoft.public.security: .dll

C:\WINNT\System32\svchost.exe  
C:\Program Files\Common Files\Symantec Shared\CCPD-  
LC\symlcsvc.exe  
C:\WINNT\system32\ZoneLabs\vsmon.exe  
C:\Program Files\Messenger\msmsgs.exe  
C:\Program Files\Internet Explorer\IEXPLORE.EXE  
C:\Documents and Settings\Owner\Local Settings\Temporary  
Internet Files\Content.IE5\O16F0XQ3\HijackThis[1].exe

R0 – HKLM\Software\Microsoft\Internet Explorer\Main,Start  
Page = <http://www.gateway.net>  
R0 – HKLM\Software\Microsoft\Internet  
Explorer\Search,CustomizeSearch = res://C:\PROGRA~1  
\Toolbar\toolbar.dll/sa  
R0 – HKCU\Software\Microsoft\Internet  
Explorer\Toolbar,LinksFolderName =  
R1 – HKLM\Software\Microsoft\Internet  
Explorer\Main,SearchAssistant = about:blank  
R1 – HKLM\Software\Microsoft\Internet  
Explorer\Main,CustomizeSearch = res://C:\PROGRA~1  
\Toolbar\toolbar.dll/sa  
R3 – Default URLSearchHook is missing  
O1 – Hosts: Xwý  
O1 – Hosts: WWW.LOOK2ME0.COM E972-22F0-422A-B5D0-  
6296FF9199BE}&MSKIP=1&RND=23307  
O1 – Hosts: Xwý  
O1 – Hosts: Xwý  
O3 – Toolbar: &Radio – {8E718888-423F-11D2-876E-  
00A0C9082467} – C:\WINNT\System32\msdxm.ocx  
O3 – Toolbar: REALBAR – {4E7BD74F-2B8D-469E-C0FF-  
FD60B590A87D} – C:\PROGRA~1\COMMON~1  
\Real\Toolbar\realbar.dll  
O3 – Toolbar: Norton AntiVirus – {42CDD1BF-3FFB-4238-8AD1-  
7859DF00B1D6} – C:\Program Files\Norton  
AntiVirus\NavShExt.dll  
O3 – Toolbar: (no name) – {339BB23F-A864-48C0-A59F-  
29EA915965EC} – (no file)  
O3 – Toolbar: LICENSE1 – {90043B92-D4A9-4EDE-C1CE-  
6790AA4D81B9} – C:\PROGRA~1\OPTION~1\Grey Anti.dll  
O4 – HKLM\..\Run: [GWMDMMSG] GWMDMMSG.exe  
O4 – HKLM\..\Run: [SynTPLpr] C:\Program  
Files\Synaptics\SynTP\SynTPLpr.exe  
O4 – HKLM\..\Run: [SynTPEnh] C:\Program  
Files\Synaptics\SynTP\SynTPEnh.exe  
O4 – HKLM\..\Run: [GWMDMpi] C:\WINNT\GWMDMpi.exe  
O4 – HKLM\..\Run: [IgfxTray] C:\WINNT\System32  
\igfxtray.exe  
O4 – HKLM\..\Run: [HotKeysCmds] C:\WINNT\System32  
\hkcmd.exe  
O4 – HKLM\..\Run: [Gateway Ink Monitor] "C:\Program  
Files\Gateway Utilities\GWInkMonitor.exe"

.dll

O4 – HKLM\..\Run: [AdaptecDirectCD] "C:\Program Files\Roxio\Easy CD Creator 5\DirectCD\DirectCD.exe"  
O4 – HKLM\..\Run: [TkBellExe] "C:\Program Files\Common Files\Real\Update\_OB\realsched.exe" –osboot  
O4 – HKLM\..\Run: [tgcmd] "C:\Program Files\Support.com\bin\tgcmd.exe" /server /startmonitor /def  
O4 – HKLM\..\Run: [SSRunScript] "C:\Program Files\Support.com\Charter\bin\SSRunScript.exe" /script "C:\Program Files\Support.com\Charter\vbs\verifyconnection.vbs" /args //b startupdelay  
O4 – HKLM\..\Run: [EnigmaPopupStop] C:\Program Files\SpyHunter\PopupBlocker\EnigmaPopupStop.exe  
O4 – HKLM\..\Run: [mmtask] C:\Program Files\MUSICMATCH\MUSICMATCH Jukebox\mmtask.exe  
O4 – HKLM\..\Run: [ccApp] "C:\Program Files\Common Files\Symantec Shared\ccApp.exe"  
O4 – HKLM\..\Run: [QuickTime Task] "C:\Program Files\QuickTime\qttask.exe" –atboottime  
O4 – HKLM\..\Run: [WinampAgent] C:\Program Files\Winamp\winampa.exe  
O4 – HKLM\..\Run: [ViewMgr] C:\Program Files\Viewpoint\Viewpoint Manager\ViewMgr.exe  
O4 – HKLM\..\Run: [camp heck] C:\PROGRA~1\twomediadebug\acidroad.exe  
O4 – HKLM\..\Run: [Zone Labs Client] C:\PROGRA~1\ZONEAL~1\ZONEAL~1\zlcliclient.exe  
O4 – HKCU\..\Run: [msnmsgr] "C:\Program Files\MSN Messenger\msnmsgr.exe" /background  
O4 – Startup: WkCalRem.LNK = C:\Program Files\Common Files\Microsoft Shared\Works Shared\WkCalRem.exe  
O9 – Extra 'Tools' menuitem: Sun Java Console (HKLM)  
O9 – Extra button: Messenger (HKLM)  
O9 – Extra 'Tools' menuitem: Messenger (HKLM)  
O16 – DPF: {01111F00-3E00-11D2-8470-0060089874ED} (Support.com Installer) –  
<http://support.charter.com/sdcommon/download/tgctlins.cab>  
O16 – DPF: {01113300-3E00-11D2-8470-0060089874ED} (Support.com Configuration Class) –  
<http://support.charter.com/sdcommon/download/tgctlcm.cab>  
O16 – DPF: {0246ECA8-996F-11D1-BE2F-00A0C9037DFE} (TDServer Control) –  
<http://www.truedoc.com/activex/tdserver.cab>  
O16 – DPF: {02BF25D5-8C17-4B23-BC80-D3488ABDDC6B} (QuickTime Object) –  
<http://www.apple.com/qtactivex/qtplugin.cab>  
O16 – DPF: {2253F320-AB68-4A07-917D-4F12D8884A06} (ChainCast VMR Client Proxy) –  
[http://www.streamaudio.com/download/ccpm\\_0237.cab](http://www.streamaudio.com/download/ccpm_0237.cab)  
O16 – DPF: {41F17733-B041-4099-A042-B518BB6A408C} –

microsoft.public.security: .dll

<http://a1540.g.akamai.net/7/1540/52/20031216/qtinstall.inf>  
o.apple.com/mickey/us/win/QuickTimeInstaller.exe  
O16 – DPF: {4E888414-DB8F-11D1-9CD9-00C04F98436A}  
(Microsoft.WinRep) –  
<https://webresponse.one.microsoft.com/OAS/ActiveX/winrep.cab>  
ab  
O16 – DPF: {62475759-9E84-458E-A1AB-5D2C442ADFDE} –  
<http://a1540.g.akamai.net/7/1540/52/20040427/qtinstall.inf>  
o.apple.com/saba/us/win/QuickTimeInstaller.exe  
O16 – DPF: {814EA0DA-E0D9-4AA4-833C-A1A6D38E79E9}  
(DASWebDownload Class) –  
<http://das.microsoft.com/activate/cab/x86/i486/NTANSI/retail/DASAct.cab>  
O16 – DPF: {A8658086-E6AC-4957-BC8E-7D54A7E8A78D}  
(DoomCln Object) –  
<http://www.microsoft.com/security/controls/DoomCln.CAB>  
O16 – DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000}  
(Shockwave Flash Object) –  
<http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab>  
O16 – DPF: {DDFFA75A-E81D-4454-89FC-B9FD0631E726} –  
<http://www.bundleware.com/activeX/DS3/DS3.cab>  
O16 – DPF: {DE22A7AB-A739-4C58-AD52-21F9CD6306B7}  
(CTAdjust Class) –  
<http://download.microsoft.com/download/7/E/6/7E6A8567-DFE4-4624-87C3-163549BE2704/clearadj.cab>

Sadie is this what you need?(I hope)–Holly  
>-----Original Message-----  
>Have you set your system to "display all hidden files  
and  
>folders" and to unhide protected operating system files?  
>  
>Go to control panel,click on "Tools",click "folder  
>options".Click on the view tab.Scroll down to "show  
>hidden files and folders",click on the tiny circle in  
>order that a green dot appears.  
>remove the tick/check from "hide protected operating  
>system files".click O.K. when presented with the warning  
>box.  
>Remove the tick from "hide extensions for known file  
>types".  
>  
>Try moveonboot again/or try deleting in safe mode.  
>  
>I have to say,Holly,you are making this extremely  
>complicated for yourself.this could have been sorted  
much  
>more efficiently by posting a hijack log on  
><http://cexx.org>  
>

.dll

>as it is,we're only getting afragment of a bigger  
>picture..

>

>Sadie

>>-----Original Message-----

>>I did what you said about downloaing moveonboot but  
when

>>it asks me to put in a file, I put in the

>>c:\winnt\system32\6j04svc.dll this is the one non of  
the

>>spyware can remove. Moveonboot told me this was a

>>nonexistant file or anyway it would not take it! Gosh

>>what now-Holly

>>>-----Original Message-----

>>>Holly,

>>>You can try GiPO MoveOnBoot:

>>>

>>><http://www.gibinsoft.net/>

>>>

>>>Scroll down the page til you get to the "free old

>>>Version".Install it.Mark any files you want to

>>>delete,and

>>>moveonboot will get rid of them on reboot.

>>>

>>>I WISH you'd posted a HijackThis! log on

<http://cexx.org>

>>>

>>>Just keep calm,anyhow.Make sure your important files

>are

>>>backed up in the event of a re-install.Don't worry too

>>>much about programmes,as they can be easilly

>>>redownloaded/installed afresh.I'm referring to

personal

>>>files.This is a precautionary measure-don't fret.

>>>

>>>Just keep to one thread,Holly,because,otherwise things

>>>become terribly confusing.We're trying to help,but

>>you're

>>>posting all over the show,making it difficult to keep

>>>track of events.Don't worry!You've been forced into a

>>>steep learning curve,that's all.When all this is

>>>sorted,your confidence will have increased tenfold.

>>>

>>>Sadie

>>>

>>>

>>>>-----Original Message-----

>>>>DOES ANYONE KNOW HOW TO GET RID OF MALWARE .DLL BUGS

>>>>THAT

>>>>KEEP CHANGING? i hAVE TRIED MOST ALL THE REMOVE WARE

>>>>HIJACKTHIS,CWSHEDDER,AD-AWARE NORTON BLASTER

ZONEALARM

>>>>*ETC. BUTMY COMPUTER CUT OFF FROM INTERNET ABOUT EVERY*

>>20-

>>>>30MIN. NOW.-*HOLLY I AM FADING FADING FAD....*

>>>>.

>>>>

>>>.

>>>

>>.

>>

>.

>