

KaZaA the Virus Desktop

By [John Thornton, Hacker's Digest](#)

KaZaA the media desktop has been one of the most successful replacements for file sharing after U.S. courts ordered Napster to shut down. KaZaA offers its users a way of sharing music, video, documents, images, and software.



But six per cent of all music downloaded from KaZaA is not music at all, but a virus. Currently, there is no way to infect mp3s with a virus; however KaZaA's poor filtering allows someone to rename a virus to - say - cant_touch_this.mp3.vbs. When you do a search for the song named "Can't Touch This" KazaA will display this as "cant_touch_this.mp3", without displaying the .vbs extension.

This problem affects more than music: [Hacker's Digest Labs](#) has found the Love Letter Virus disguise as videos, images and executables.

What does KaZaA say about this? This is what the FAQ has to say:

"Q: Can I get viruses using KaZaA?"

A: As always when you are downloading or receiving files from the Internet, you must exercise caution. Certain file types may contain viruses or so-called Trojan horses. You should protect yourself by using regularly updated anti-virus software, for example Norton Antivirus (www.norton.com) or McAfee (www.mcafee.com). Both Norton and McAfee offer free 30-day trial versions that you can download directly from their web sites. Not all file types can contain viruses or Trojans. Music, video, and picture files are generally safe - that includes files with the extensions .mp3, .vaw, .mpg, .avi, .mov, .bmp and .jpg. PDF documents (.pdf) and text files (.txt) are also in general safe. You should be cautious of executable files (.exe) and Microsoft Word and Excel documents (.doc and .xls). These files are specified with a icon in the search results on KaZaA.com."

This is true, however with the poor filtering in the KaZaA media desktop, it is extremely easy for anyone to be tricked into running a virus thinking it is his or her favorite song. ®

I think this must be one of the WORST programmes around for spyware and hijackware... Here's just a small sample.

Dlder.exe (Advertising)

Noted as a trojan by some antivirus programmes (W32.D1Der.Trojan), this little nasty tracks your web surfing *and* uploads this information to a website (now apparently shut down). It can also download *and activate* exe files (programmes). You can expect to find a file called explorer.exe in your ..\windows\system or ..\windows\explorer file (note that a legitimate Windows file is also called explorer.exe, but that is in ..\windows

Cydoor (Advertising)

Fastseeker toolbar

Dw.exe (DiskWare)

Causes invalid page faults.... removable via Control Panel, Add/Remove Programmes.

(Updated 14 July 2002). Thanks to Robert Aldwinckle who referred me to the following URL about dw.exe - what a NASTY piece of work the software is:

<http://and.doxdesk.com/parasite/DownloadWare.html>

Some choice quotes:

"...The EULA, when found, claims that it may clash with various other software and so **if it finds any it will remove it. (!)...**"

"...As well as removing DownloadWare you should check your system for other things it has installed and get rid of them too..."

Hot Text, Top Text, Ezula, ContextPro

...Yellow underlining on web pages...

This is caused by a programme installed with Kazaa Media Desktop called .

It can be removed via Control Panel, add/remove programmes. Search for "eZula-README.html" on your computer. This file contains information from Kazaa about the ...service.

Bdview.exe (Advertising)

Ctbclick.exe ([information here](#))

CommonName toolbar plug-in ([information here](#))

The error noted below is known to be caused by the toolbar plug-in. Uninstall it.

Microsoft Visual C++ Runtime Library

MICROSOFT VISUAL C++ RUNTIME LIBRARY
runtime error
Program C:\Program Files\Internet Explorer\
IEplorer.Exe
Abnormal Program Termination

It seems the CommonName browser bar can be installed independently of Kazaa (thanks Jon Kennedy and Ian Phillips). Advice on how to get rid of the toolbar can be found here:

<http://www.commonname.com/english/ug/toolbar/default.asp?idx=10#4>

Brilliant Digital software installed with Kazaa
<http://news.com.com/2100-1023-875016.html>

"...Two days after disclosures that file-swappers using Kazaa were unwittingly downloading software that could turn their computers into part of a new network, Kazaa's owner spoke up to defend the company's actions.

As previously reported, Kazaa quietly has been bundled for two months with software that contains the core of a new peer-to-peer network. This software, from a California company called Brilliant Digital Entertainment, has been installed on potentially tens of millions of computers. Brilliant Digital plans to "turn on" this software in four to six weeks, tapping the resources of potentially tens of millions of ordinary PCs **to distribute content or advertising** or to run complicated computer tasks...."

<http://news.com.com/2100-1023-873181.html>

"...Brilliant Digital Entertainment, a California-based digital advertising technology company, has been distributing its 3D ad technology along with the Kazaa software since late last fall. But in a federal securities filing Monday, the company revealed it also has been installing more ambitious technology that could turn every computer running Kazaa into a node in a new network controlled by Brilliant Digital.

The company plans to wake up the millions of computers that have installed its software in as soon as four weeks. It plans to use the machines--with their owners' permission--to host and distribute other companies' content, such as **advertising** or music. Alternatively, it might borrow people's unused processing power to help with other companies' complicated computing tasks...."

and

<http://news.com.com/2102-1023-875274.html>

A treatise on the potential uses of the Brilliant Software:

<http://www.cs.berkeley.edu/~nweaver/0wn2.html>

Uninstall instructions for the Brilliant Digital Entertainment software

<http://news.com.com/2100-1023-875274.html>

All trademarks are hereby acknowledged as the property of their respective owners." So don't even THINK about suing me :)