

Re: unknown dll and exe: ezbewvi.dll, ezbewvi.exe

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-09/0031.html>

From: sponge (yosponge_at_yahoo.com)

Date: 09/03/03

Date: 2 Sep 2003 21:48:00 -0700

On 2 Sep 2003 12:11:26 -0700, peter1712@gmx.net (ppunk) wrote:

>hello,
>by visiting a website several DLLs and an EXE were saved in my TEMP
>and WINNT/SYSTEM32 folder. I removed all with exception of
ezbewvi.exe
>and ezbewvi.dll. Removal of these was impossible, even immediatly
>after system startup. Inspection with Process Explorer showed, that
>many processes are using this dll but the exe was not in the process
>list (?). I'm using Windows2000. Does anybody know something about
>this dll or exe? Is there a virus using them? How can I get rid of
>them?
>
>thanks for an answer.

Naturally, the first step is downloading and running the "Big Three", SpyBot, Ad-Aware, and SpywareBlaster (yes, all three) at least occasionally. Make sure to run their updaters first.

It sounds like you've been the victim of a drive-by hijacking, and that looks like Lop. This is one of the most dangerous spywares around, because it hijacks your DNS configuration. Give Spybot a crack at it first, then Ad-Aware, then SpywareBlaster. That should remove everything. However, after running them, go into your DNS Configuration menu (use Help to find it if necessary) and make sure that there are no funny-looking names in the DNS Search Suffix field. Actually, there should almost NEVER be anything in these fields. To prevent this sort of thing, the best thing you can do is not use Internet Explorer. IE is the entrance point of most parasites and hacks.

Whether or not you discard IE, do the following: turn off all ActiveX downloads and functionality. This is one of the most significant security threats in existence. Go into Tools, then Internet Options, Security, then click the Custom button. Set all items on the list referring to "ActiveX" to Disable. Click Apply, then Ok. Additionally, run these patches to fix some bugs and extremely severe exploits in IE.

comp.security.misc: Re: unknown dll and exe: ezbewvi.dll, ezbewvi.exe

Disables the HTA (HTML Application) service. You won't miss it.

<http://www.wilders.org/HTMLobj-647/htastop.exe>

Disables Data Source Object exploit.

<http://www.wilders.org/HTMLobj-1170/dsostop2.exe>

Disables Windows Scripting Host – a must.

http://www.wilders.org/HTMLobj-844/se_wsh.exe

Sponge

Sponge's Anti-Spyware Source

www.geocities.com/yosponge