Re: Can't remove Loaded DLL −− wdme.dll

Source: http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004−06/1791.html

---

From: \\~Virus Guard~/ (*vguard223_at_vgcorp.com*)
Date: 06/25/04

```
Date: Fri, 25 Jun 2004 16:26:01 −0300
```

Try going into DOS, and typing
del C:\windows\system32\wdem.dll

Virus Guard
"Robin C." <anonymous@discussions.microsoft.com> wrote in message
news:a76301c435cb$34c9cc50$a301280a@phx.gbl...
> Upon examining the 'Loaded Modules' on my Windows XP Home
> machine, I find a worrisome DLL.
>
> (Using the System Information program under START
> MENU/All Programs/Accessories/System Tools)
>
> The Name is "c:\windows\system32\wdme.dll". (The double
> quotes are actually displayed with the name)
>
> It displays no Version,Size,File Date nor Manaufacturer.
> The Path is
>
> "c:\windows\system32\wdme.dll". (Again quotes were
> displayed)
>
> Not recognizing the file, I decided to explore further.
>
> First using explorer, I examined a directory listing of
> C:\windows\system32. Wow, no file listed.
>
> I looked for hidden and system files, again no file would
> list. I dropped into the DOS prompt and did a directory
*> search − again no file listed, tried ATTRIB *wdme* − no*
*> file listed, tried >cacls *wdme* − no file again.*
>
> Hmmm. Maybe the file isn't there. I created a new text
> file and attempted to rename it to WDME.DLL. Ouch!!
> Message says − A File with the name you specified already
> exists.
>
> I tried to DOS EDIT the file −− Error Code 32 (Some
> problem), again the file seems to be there.

>
> I tried WordPad from Windows − 'An unexpected error
> occurred while reading c:\Windows\system32\wdme.dll
>
> So I'm assuming it is there. Maybe I don't have
> permission. I have entered logged on with admin rights.
>
> How do I take ownership of a file I can't see?
>
> NEXT −− Registry
>
> I went to the registry and found a reference, actually
> some information on the internet told be to check the
> following key
>
> HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
> NT\CurrentVersion\Windows\AppInit_DLLs
>
> The value in Binary was ':\windows\system32\wdme.dll'.
> The single quotes were not included −
>
> Note: there is no 'C' in front of the first character ':'.
>
> Ok, I cleared the data. Checked it again − Data is
> cleared. Closed Regedit. Reopened Regedit and checked
> the value once more − AWGHH! It is back.
>
> Something resets the value upon closing. opening regedit,
> or some other event. I suspect that regedit doesn't
> write the changes until closing and that an event upon
> the changing of the key value is propogated to some
> program (probably wdme.dll) and the program resets the
> value back to ':\windows\system32\wdme.dll'.
>
> I've tried from safe boot to change the registry − No
> luck. wdme.dll is still present as a loaded module.
>
> Note: When searching web for 'wdme.dll' it just gave one
> hit at www.computercops.biz.
>
> So please help.
>
> How do I stop wdme.dll from loading? How do I 'see' the
> file in a directory listing (windows or dos)?
>
> Boy this is really annoying...
>
> I had been hit recently with the cc.search hijack and
> cleared it up. (or so I think). This may be
>
> some residual leftover, hanging on, annoying me, driving

> *me INSANE!!!!*
>
> *Any assistance would be appreciated, just point me to a*
> *website or whitepaper.*
>
> *Thanks,*
> *Robin*