

Re: Can't delete folder!!! (Xere Inc)

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2006-05/msg00427.html

- *From:* "Steven L Umbach" <n9rou@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sun, 14 May 2006 21:47:24 -0500
-

While logged on as an administrator try booting into Safe Mode to see if you can access and delete the files. If you can not access them try taking ownership first and then granting yourself full control permissions. Since it seems you can not access the folder/files via Explorer you will need to try the command prompt. You can use attrib to see/change a files attributes, use dir /a and specify attributes to see hidden files etc, and use cacls to view/manage permissions. Fileacl is free and can be used to take ownership, view and manage permissions if need be. Of course you should verify that Explorer is configured to show hidden and system folders/files for the program files folder.

Free tools from SysInternals such as Process Explorer Autoruns and can help you determine what is going on. See if Process Explorer shows a publisher name which may help identify the process/file and if there is none it certainly lays some suspicion on it. Since it is in the program files directory check Control Panel/add and remove programs to see if it shows up there. You also should scan for spyware and malware in Safe Mode being sure to use the latest definitions for what ever program you scan with and it is a good idea to run Check Disk selecting the option to automatically fix file errors just to make sure there are no problems with corrupt file tables. AdAware SE is a pretty decent free for persoanl use spyware program.--- Steve

<http://www.sysinternals.com/Utilities/ProcessExplorer.html> --- Process Explorer and link to SysInternals
<http://www.gbordier.com/gbtools/fileacl.htm> --- fileacl link
<http://www.trendmicro.com/download/dcs.asp> --- Sysclean free stand alone malware scanning program from Trend Micro
<http://www.trendmicro.com/download/pattern.asp> ---latest pattern file for Sysclean in zip format
<http://www.ewido.net/en/> --- Ewido may find trojans that other malware programs do not.

"mbaprog1978" <mbaprog1978@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:3ADDF444-9A16-475D-ADA5-E2AF538A92B3@xxxxxxxxxxxxxxxxxxxx>

I have been cleaning stuff off of my computer lately. After performing a defrag on my system drive I received a log that noted a number of files

Re: Can't delete folder!!! (Xere Inc)

that
could not be defragmented. Here's a couple:

11 448 KB \Program Files\Xere
inc\Cache\000037e6_4452d0a8_0007270e
12 496 KB \Program Files\Xere
inc\Cache\00006732_4452d040_0002625a
15 741 KB \Program Files\Xere inc\Cache\index
420 2 MB \Program Files\Xere inc\Cache

I tried to find the "Xere inc" directory, but I couldn't. Not only that,
I
ran a couple other utilities and realized that there is a process that
hits
this directory! This is from filemon.exe:

```
57644 6:31:12 PM lftconfig.exe:592 WRITE C:\PROGRAM FILES\XERE  
INC\Cache\dns SUCCESS Offset: 56520 Length: 48  
57645 6:31:12 PM lftconfig.exe:592 WRITE C:\PROGRAM FILES\XERE  
INC\Cache\dns SUCCESS Offset: 56568 Length: 51
```

After all of this, I tried to create a directory in C:\Program Files call
"Xere Inc" and I got the following error message:

"Cannot rename New Folder: A file with the name you specified already
exists. Specify a different file name."

Lastly, I found a couple of reg keys, one of them being:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ESSENT\Process\LFTCONFIG
```

I consider myself a pretty advanced user, so I don't think that this is
anything simple like a (normal) "hidden" folder or protected operating
system
file. Then again it could be something I just haven't thought of. Any
help
is appreciated, I'm at my wit's end!!!

--

A Human Being