

Re: Databaseben, I sent you a message below

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2006-10/msg03153.htm

- *From:* "DatabaseBen" <databaseben@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sat, 21 Oct 2006 15:44:32 -0500
-

hello mtnlady,
yeh found the other posting with
your discovery.

i'm very interested with your analysis
and will take a look into it.

but, lets not be hasty in considering
that the ntregopt is the perpetrator of
a trojan. i checked that website and
followed that link to the home page at
<http://www.larshederer.homepage.t-online.de/erunt/index.htm>
and when the file sizes are compared they are both 472kb.
Then when i clicked to download a copy from majorgeek
the file size was also 472. (Of course i already had
a copy for a long time, but wanted to double check
out the download.)

This is important to know, because if the file
size was bigger or smaller than the original file
found at <http://www.larshederer.homepage.t-online.de/erunt/index.htm>
then we know the code was rewritten.

now a days, there are softwares that
pretend to have discovered something
bad, but they are the cause of
the infiltration. But trojans can also
be snucked onto your system, with
music, videos and lots of other ways.

remember that a trojan by design hides
malacious code but figuring out
how it got on your system and where
that file is located is the question.
you discovered the malacious code but
the trojan imay still on your system and
hiding until the time is right to unleash
the malware....

Re: Databaseben, I sent you a message below

Have you downloaded or allowed somekind of toolbars to be installed recently?

Just to top of my head right now, it sounds like the data you pasted on the other posting is referring to an explorer toolbar.

I know that today I was searching for old music from that cold case tv show, and i swear i had to install 3 different kinds of music players and all of them kept asking me if i wanted a toolbar. Of course, i said "no"....

again, thanks for the update.

btw, until the trojan can be discovered and eliminated, it may not be wise to make any restore points or backups because you would only be helping with saving the trojan...

"MtnLadyinBlackHills1986"

<MtnLadyinBlackHills1986@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:B1FFC50D-CB70-44EC-BBA7-EDF35BFA2402@xxxxxxxxxxxxxxxxxxxx

Hi, Databaseben, I sent a message to you below titled "Danger Warning! to the public" and had put "note to Databaseben" on the end, but the title was too long and cut your name off! You helped me out last July with computer problems.

Now I can't get my message of today to load. Maybe it was too long. Could you let me know if you can get it to load so you can read it? If not, I'll shorten it and tell you the situation.

I don't understand why it won't open! Maybe it's just my luck.

Re: Databaseben, I sent you a message below