

Re: Questions about my malware settings

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2006-04/msg02334.htm

- *From:* "Rusty" <RknRusty_nospam@xxxxxxxxxx>
 - *Date:* Tue, 18 Apr 2006 15:49:17 -0400
-

I don't know. I've had i-tunes installed since February and never used it. Only opened it to watch a couple of movie trailers the same day I installed it. These files turned up yesterday. I update and scan with all of my anti malware programs at least every other day. I even keep the ipod service startup status disabled which probably has nothing to do with this anyway.

I've Googled every program listed in the task manager processes list and they are all associated with programs I can identify. I'm the only one in the house that uses a computer. I've been in the habit of keeping a very lean system since DOS 5.0. and IBM 370 OS before that.

That's as clear as I can be about not having P2P. If you know where I may have missed anything I will appreciate any advice you may lend in that regard. Now if we can get over that, what I really wanted from this post was some answers to a couple of questions. Those would be the sentences followed by question marks in my original post. There are two or three of those.

Rusty

"Ted Zieglar" <teddy.z@xxxxxxxxxxxx> wrote in message
<news:%23wN0duwYGHA.444@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

In that case, where do you suppose the "Adware.P2PNetworking object" came from?

Ted Zieglar

"Backup is a computer user's best friend."

"Rusty" <RknRusty_nospam@xxxxxxxxxx> wrote in message
<news:uZiZZTwYGHA.1220@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

No I use no P2P. I recently subscribed to i-tunes because I refuse to use Kazza or Napster or any other P2P. i-tunes is not peer to peer.

Re: Questions about my malware settings

"Ted Ziegler" <teddy.z@xxxxxxxxxxxx> wrote in message
news:Okrt9yvYGHA.3328@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

If you patronize P2P networks you can pretty much count on
being

infected

with a virus or malware, no matter how much anti-this and
anti-that
software
you have installed.

--

Ted Ziegler

"Backup is a computer user's best friend."

"Rusty" <RknRusty_nospam@xxxxxxxxxx> wrote in
message

news:eVJsDtvYGHA.3532@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Along with Norton Internet Security 2005, I
run Ad-Aware, Bazooka,
Spybot-Search and Destroy,
SpywareBlaster, and Windows malicious

software

removal tool at least every couple of days.

Ad-Aware occasionally finds 1 or 2 data
miners in my temporary
internet
files, which I remove.

Bazooka always gives a clean report (I'm
wondering if it really does
anything).

I keep Spyware Blaster updated and all
protection turned on.

Spybot has detected "Windows security
center firewall and antivirus

disable

notify", which I told it to ignore, plus a
couple of others that I
removed
when I ran it the first time. I have noticed in

Re: Questions about my malware settings

the Spybot ignore
list

that

CDilla, Hitbox, and Sidestep are set to
ignore. CDilla worries me,
I'm
wondering if it's associated with itunes.
Does anyone know about
that,

and

is there any reason not to uncheck the ignore
option on any of these?

Now here's what really got my attention.
Yesterday when I ran
Ad-Aware
it
found the following 4 files, and this is how
they were described in
the

log:

Adware.P2PNetworking object : File :
C:\System Volume

Information_restore{D23EFF2A-BFEF-46A5-8364-D064E372DF2B}\RP126\A0014358.ex

e

Adware.P2PNetworking object : File :
C:\System Volume

Information_restore{D23EFF2A-BFEF-46A5-8364-D064E372DF2B}\RP126\A0014399.DL

L

Adware.P2PNetworking object : File :
C:\System Volume

Re: Questions about my malware settings

Information_restore{D23EFF2A-BFEF-46A5-8364-D064E372DF2B}\RP154\A0016637.DL

L

Adware.P2PNetworking object : File :
C:\System Volume

Information_restore{D23EFF2A-BFEF-46A5-8364-D064E372DF2B}\RP154\A0016639.ex

e

I quarantined them. Is this something that
would have corrupted a
restore
point? What can anyone tell me about these?

I know this is a lot of Q&A, so I appreciate
any expertise you

knowledgeable

people can give me.

Thanks,
Rusty