

RE: Possible Virus or Trojan?

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2004-12/2847.html

From: Dawn Loree (*Loree_at_discussions.microsoft.com*)

Date: 12/09/04

Date: Thu, 9 Dec 2004 05:39:02 -0800

I have the same msg from my anti-virus program. It states that the Trojan virus came from Windows Update. Can someone explain this? Please???? Dawn Loree

"Howard Hartman" wrote:

>
> -----BEGIN PGP SIGNED MESSAGE-----
> Hash: SHA1
>
> Hello.
>
> I have an unusual problem on an XP Professional computer that I think may be
> a virus or trojan, but Norton Antivirus 2005 is ambiguous as to whether the
> computer is infected or not.
>
> I noticed one day that the process upnpclient.exe was running on this
> machine. That was suspicious since the UPnP component was not installed. I
> deleted the process.
>
> As soon as I ended the process, Norton Antivirus popped up and issued a
> virus warning in the category of Trojan Horse on the file c:\acrobat.dll.
> Norton was unable to either repair or quarantine this file.
>
> A few minutes later the upnpclient.exe process was running again.
>
> I can delete c:\acrobat.dll in a DOS window. It only exists if the
> upnpclient.exe process is ended via Task Manager. When the upnpclient.exe
> process is reinstated, it creates the file c:\acrobat.dll which is 32,768
> bytes in size. Each time it is created, Norton flags it as a possible virus
> or trojan.
>
> I do have Adobe Acrobat 6 installed on this computer. The UPnP Client is
> still not installed. I have tried installing the UPnP Client and then
> removing it. That had no affect. I tried deleting all files with the
> specification upnp*.* on the computer. That had no affect either.
>

microsoft.public.windowsxp.help_and_support: RE: Possible Virus or Trojan?

> *I have another computer that also has Adobe Acrobat 6 installed and this
> behavior is not seen on that computer. The upnpclient.exe process is also
> not running.*
>
> *I have looked at the TCP/IP activity on the computer. The upnpclient.exe
> process opens a port only to localhost so it doesn't seem to be posing a
> risk to outside intrusion at this point.*
>
> *Is this an infection? Why is the upnpclient.exe running and why does it
> restart by itself? I don't think I have anything running that requires it.
> Even if it was required by another process, wouldn't I be prompted to
> install it rather than Windows running it itself?*
>
> *Thanks.*
>
> -----BEGIN PGP SIGNATURE-----
> Version: PGP 8.0.3
> Comment: Digital signature guarantees authenticity
>
> *iQA/AwUBQbdAoN/hBQ7O4WklEQL7fQCg16VwygF/tSaz+Uhn4GoZR7KDxJMAoMBa
> Ay14R9UUtBrCV7sEgpr856Va
> =XFB5*
> -----END PGP SIGNATURE-----
>
>
>