

Re: Hacker Help

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2004-02/1198.html

From: Roger Abell (*mvpNOSpam_at_asu.edu*)

Date: 02/08/04

Date: Sun, 8 Feb 2004 07:50:52 -0700

Antivirus alone is not enough. Once infected you need to clean the system, and sometimes that is not possible. Try cleaners you can get from the major AV vendors, such as Stinger from Symantec. When your AV detects those files it is likely indicating what virus is involved, so you need to research that virus at the vendors' sites and follow recommendations you will find there on the virus specific cleanup you need to do. Until cleaned, most just reappear.

That your firewall is on is good, but you need to understand the firewall as it can be set to allow things through. You should make sure that there is nothing defined as allowed to come in from outside (that is not in response to something that you have done inside).

Also, if your machine is not up-to-date on all MS released service as shown by Windows Update, then people here will not be able to assist you until it is.

--

Roger Abell

Microsoft MVP (Windows Server System: Security)

MCSE (W2k3,W2k,Nt4) MCDBA

"Deep" <anonymous@discussions.microsoft.com> wrote in message news:ccba01c3ee2a\$afeabea0\$a601280a@phx.gbl...

> I got a new pc on a cable about a month ago and have been
> inundated with major attacks since this machine went
> online.

>

> I am quite sure someone is hacking into my computer --
> someone from my work group for the cable internet. I have
> firewalled my connection, am using sygate firewall as well
> (can't figure out what to allow and what not though) and
> both quickheal and norton. If anyone can give me ideas on
> how to deal with this it will be a big help, neither my
> service providers nor hardware guys have a clue :(Heres
> is what has been happening.

>

> 1. I have huge virus attacks, NOT from emails and they go
> on till the pc crashes.(Nimda.enc, Lovegate, W32.Roro.V,
> Dupator) Always in the C drive. The same file names, same

microsoft.public.windowsxp.security_admin: Re: Hacker Help

> location...c/windows or c/windows/documents and settings.
> They are deleted...but 10 mins later the AV is deleting
> the same files again. I think someone is dumping on my pc
> or something...I don't know. Has been going on for 20 days
> now.
> Stops for sometime when the PC is restarted. Then starts
> again.
>
> 2 In my network places, I find folders created. Folder
> names like....My first hacking exp, Join me hacking on
> jayesh....I deleted these folders(not sure if it helps.)
>
> 3. In explorer, a week ago when I clicked on the E drive
> icon it started giving me an error "Cannot find
> KAMASU~1.EXE". My hardware guy says its nothing to worry
> about(im not so sure), now my icon for C drive
> says "Cannot find TEENSE~1.EXE". Both these drives can be
> accessed from the left nav. But not from the "view files"
> area of windows explorer. Also both these are names of
> files my AV had deleted
>
> This is a business pc and I have mine and my clients info
> on it.
> I need help with,
> 1. how to hide my ip add while surfing,
> 2. how to stop this madman,
> 3. I know its very difficult but CAN I BUST HIM.
>
> my email is roam_dx@yahoo.com. Any help or ideas will be
> appreciated.