

Re: help again !!!

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-05/3111.html>

From: Phil Weldon (*notdisclosed_at_example.com*)

Date: 05/28/04

Date: Fri, 28 May 2004 18:10:04 GMT

This time I WOULD suggest a new post starting a new thread, just mentioning the virus problem. Include information like

Version of Norton AV? Were the virus definitions up-to-date?

Version of Windows? Were all the critical patches installed?

If Windows XP, was internal firewall enabled?

Third party firewall (like Zone Alarm or Norton Personal Firewall) present?
Hardware firewall present?

While waiting for an answer to your new post, you might want to try the following.

(This is not an exhaustive test, but it is better than doing nothing, and will give you more diagnostic information to post)

Go to your start menu (in 'Settings') and rename the 'Startup' directory (rename it so that it is "hidden" from the system, but can be restored just by changing the name back.) Then restart your system.

Start 'Task Manager' (CTRL-ALT-DELETE) or 'RUN' taskmanager.exe from the 'Start Menu'. Go to the 'Processes' Tab and copy the list of all processes to end processes, one at a time. You will not be allowed to end critical processes, and will be denied access to other processes. Write down name of each process, whether or not it could be ended, and the exact message if it could not be ended. This may be tedious as there are likely to be over 30 processes to start. Once you have ended what can be ended, you should have a list that differentiates between processes that can be ended and those that can't. Save that list, then try to use NAV and also try to go on line. Post the list and the results of trying to go on line and the results of trying to use NAV.

Once you get a solution for removing your mal-ware problem, you will also need enough protection to keep your system protected. That includes

microsoft.public.security.virus: Re: help again !!!

#1. Keep a good AntiVirus program with up-to-date virus definitions (at least weekly updates) running ALL the time.

#2. Keep up with all Microsoft critical security updates.

#3. Download, install, update, and run weekly Spybot Search&Destroy (free)

<http://www.safer-networking.org/>

#4. Download, install, update, and run weekly AdAware from LavaSoft (free)

<http://www.lavasoftusa.com/>

#5. If you have Windows XP, make sure the internal firewall is enabled, if you don't have Windows XP, get a third party firewall, install it and keep it enabled.

#6. Consider purchasing a simple hardware firewall (sometimes found incorporated into routers or wireless base stations)

#7. Consider using a email filter/text previewer program (Magic Mail Monitor, for example; it useful as a spam filter as well as blocking the flood of email that the worm swen can send to your mailbox even though your system is not infected. Magic Mail Monitor is free and available at <http://www.geeba.org/magic/>. I use it to identify spam. Magic Mail Monitor can download just the header information from your ISP mail server and display just that information in a list of all mail waiting for you. I sort the messages in ascending order of length, and can usually eliminate ALL spam by just scanning the 'To', 'From' and 'Subject' columns, then deleting those messages as a batch without ever downloading. If necessary, you can view any entire message in text mode, which protects against viral infection. Checking 50 emails a day this way eliminates ALL my spam in about two minutes.

#8. Try to avoid suspicious websites and email attachments (ah, but how to tell a suspicious website or email attachment?)

#9. I'm sure others have additional suggestions.

Finally, and I hope you get this far, it is all well and good to use the Microsoft anonymous connection to post here, but when you don't also use some 'From' name, there is no way to associate different threads you have posted. That IS a problem for you and for those who try to provide help. You could either use some 'From' name (could be anything as long as nobody else is using it in this forum, as long as you stick with the same name) OR (and this works for ALL newsgroups), you could set up an email identity in your newsreader that is invalid. That will protect against getting spam or messages generated by worms like 'swen' that harvest email address from newsgroup postings. If you want the possibility of being contacted directly by a newsgroup participant, you can create an extra, valid email address, just for newsgroup use, and sign your post at the bottom with a version of that email address that is easily interpreted by a human, but beyond the capability of any simple program (or even complex program. See my signature for an example. If you right click on this message you will see in the properties sheet the email address identity I created for newsgroup posting. This address,

notdisclosed@example.com

is associated with no real email box, and can't be, the domain, example.com is reserved for testing purposes. You can set up your on syntatically correct but invalid email address by using any letters followed by the 'at'

Re: help again !!!

microsoft.public.security.virus: Re: help again !!!

sign and 'example.com'. The reserved domain name ensures that you are not duplicating a existing email address and that useless, bouncing email is not generated that becomes a problem for Internet Service Providers.

At anyrate, I would appreciate feedback if you use 'Task Manager' to get a list of processes that can not be shut down.

--

```
Phil Weldon, pweldonatmindjumpdotcom
For communication,
replace "at" with the 'at sign'
replace "mindjump" with "mindspring."
replace "dot" with "."
<anonymous@discussions.microsoft.com> wrote in message
news:1421701c44495$7cac50a0$a001280a@phx.gbl...
> Thanks so much Phil,
>
>
> > You were right, there were 2 problems, I changed the mouse
> and it's much better (the windows opening alltogether
> came from the cable probably...)
> My problem now is that my Internet connection disconnects
> itself every 10 minutes and also Norton is disabled : no
> way to scan on or off line...
>
>
>
> >-----Original Message-----
> >Well, pretty clearly you have two, unconnected,
> >problems; a bad mouse/cable
> >and a virus. The virus is NOT causing the mouse problem.
> >Replace the mouse
> >and try posting with whatever other information you
> >gave in your original
> >post (that is why it is a good idea to posts followups
> >under the original
> >post, rather than start a new thread; few will bother to
> >try to find the
> >other thread.)
> >
> >
> >---
> >Phil Weldon, pweldonatmindjumpdotcom
> >For communication,
> >replace "at" with the 'at sign'
> >replace "mindjump" with "mindspring."
> >replace "dot" with "."
> >
> ><anonymous@discussions.microsoft.com> wrote in message
> >news:1218201c44268$7087b370$a001280a@phx.gbl...
> >> Here I go again.
> >>
> >> I got a XXXXXX virus which drives my mouse mad : it
> >opens
> >> all windows and software alltogether.
> >>
> >> My Norton is switched off and when I try to switch it
> >back
> >> on then it vanishes.
> >>
> >> A member of the group suggested me to unplug it and try
```

Re: help again !!!

microsoft.public.security.virus: Re: help again !!!

```
> to
> >> scan online using the keyboard.
> >>
> >> When I unplug the mouse, I don't have any problem of
> >> everything opening at the same time.
> >>
> >> BUT when I come to try to scann online, my internet
> >> connection switch suddenly off. My Norton can neither be
> >> opened...
> >>
> >> Any other idea ?
> >
> >
> >.
> >
```