

## Re: looking for answers about detecting and deleting rootkits on windows XP OS, and getting really annoyed!!!!

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2005-04/0290.html>

---

*From:* roofy (rneilen216\_at\_comcast.net)

*Date:* 04/20/05

Date: 20 Apr 2005 14:09:13 -0700

> *What address does lxupmon.exe try to connect to?*

Well I never thought to look to see what address it was trying to connect to, considering that I recall there wasn't too much info but I forget exactly what it said

> *I don't wish to appear rude but are you sure you're not just putting this stuff down to a "root kit" because you've been reading about them a lot lately?*

Robert, I didn't take this for being rude. In fact I can understand how you high tech geniuses get some really lame questions, but you do have to realize that when a person scans their system, constantly and still doesn't see any improvements, sometimes they go to the extreme. And then when these newsgroups say search other people's post or search on google, to find answers there can be some really far fetch info on the internet. And besides, this is my whole point of explaining how much junky info is out on the net that you don't know what to believe. I think that some of these computer geeks needs to be placed in some of these other peoples shoes who are computer illiterate think what would I do if I got a virus and all there is, is junky info that is out on the internet. I am not saying that I am not computer illiterate, in fact I have much far more skills then most people do when we use to use DOS and you needed to know dos commands to execute programs or other commands to find files as well as setup batch files that autoexecute programs to run when you booted the computer. I mean it would be the same thing as if I laughed at you because you don't know how to list a folder of file in dos, which is now called command prompt or cmd.exe, or make a com port printer to print from the command prompt window. Or how about if you were posting a question in the desktop publishing newsgroup on something that a web site says that full color printing stands for mixing rgb colors together, when truly the process of full color printing or also known as 4 color process stands for mixing the four pigments of cmyk together which will create full color.

Re: looking for answers about detecting and deleting rootkits on windows XP OS, and getting really annoyed

soft.public.security.virus: Re: looking for answers about detecting and deleting rootkits on windows XP OS, and getting really

So all in all I would say that I am like the mom and pop style person when VCR's first came out and they didn't know how to program the timer to record a movie that was being aired at 6:00 pm etc. So they have their children like me to program the dumb VCR., but maybe the child didn't know how to play a movie. My point is we all have our areas of strength, and mine isn't internet security, which I think it is a pain when all I want to do is do my graphic design art work, but yet I like to use the internet to keep up with my updates of my artwork on my homepage, or maybe because I need to update my drivers or maybe share my artwork with others etc.

anywho, to answer your question, whether am I sure I am not just putting this stuff down to a "root kit" because you've been reading about them a lot lately.

Well, my answer to that is considering that I don't know how people can hack into a computer, and I am not asking how, I would have to say that I am doing a process of limitation more than just saying oh its got a be a rootkit.

So far I have scanned with Nortans, nothing. I have scanned with Adaware, found some entries but still no improvement. I did a chkdsk scan from the command prompt and said that there were some problems with the hard drive. So I rebooted and did a chkdsk -f, and there was a little improvement but then the problem still persists. So I heard something about rootkits a long time ago, and now that I am having so many problems that when I tried looking on the internet and this is where I stand now.

> *Try running 'hijack this' and*  
looking at what that says is loading at startup and if that looks normal.

I heard of this but wasn't sure what it was and how to read its log.

Also, I have recently looked in the event viewer, and had a look in the security folder, and I found 3 Usernames, named "Anonymous Logon" but they all failed as well as a lot of bad password errors that failed to log on from the Username SYSTEM.

Now I will go to the reply of lanwench.

> *Wow! You are today's recipient of the Usenet Faulkner award for that sentence. ;-)* Also, I doubt you can hear your processor. Your hard drive,  
sure. If you can hear your processor, drop the mouse and run very very fast  
away from your computer.

Well whatever it is, it sounds like a huge fan running at full speed.

Re: looking for answers about detecting and deleting rootkits on windows XP OS, and getting really2annoyed

soft.public.security.virus: Re: looking for answers about detecting and deleting rootkits on windows XP OS, and getting really

> *really really really am having a hard time reading your post – but*  
at the  
end of the day, if you're that concerned that your PC has a  
trojan/virus/rootkit or some other nasty lurking beast, and you can't  
find  
it,

I am not sure "concern" is the word I feel. I more feel like I wish I  
do have some sort of virus that can be found and that is what is  
causing my computer to slow down. Sort of like when you first start  
with the sniffles and headaches and feeling naustious but you can't  
throw up because your not sick enough, and then you wish that you do  
get sick so that you can throw up and and feel better, or see the  
doctor to get medicine. I know I sound strange, but thats how I feel.

> *then it might be best to back up your data and reinstall. It might be*  
a  
lot faster. Just my \$.02. :)

I have just recently spoke with a live sony tech that said to do a  
Recovery install which I will probably do tonight, considering that I  
here it can take awhile

Thanks to all for your comments and I will let you know how this works  
out.

Re: looking for answers about detecting and deleting rootkits on windows XP OS, and getting really3annoyed