

Re: Detecting spy software

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2002-06/1093.html>

From: x y (jamescagney90210@yahoo.com)

Date: 06/08/02

From: "x y" <jamescagney90210@yahoo.com>

Date: Sat, 8 Jun 2002 16:12:26 -0400

I agree, posting some hints about what you're seeing would be helpful. Once someone has broken into your computer, there is no way to be 100% sure you've removed every back door they installed, which could allow further intrusion. The only way to be 100% sure is to format and reinstall Windows and everything else to your computer, and use the manufacturer's recommendations to secure it before putting it on the internet [including installing all security patches, antivirus, firewall, and following the checklists at www.microsoft.com/security .

If that is not something you want to do and are willing to live with the risk, you can try these tools. Actually, it's a good idea to try these tools first to confirm that your machine was hacked before you do all that work. The book Intrusion Detection for \$30 may be overkill for one incident but is a good introduction to dealing with this sort of thing.

there is a trojan scanning tool from www.gfi.com that is very inexpensive but can give false alarms.

running the NETSTAT -AN command at a dos prompt / command prompt
fport from www.foundstone.com

process explorer, filemon and pstools from <http://www.sysinternals.com> ,
including pslist and psloggedon

sygate personal firewall [free for non-commercial]

norton antivirus or other antivirus that is set to download the latest updates daily

Languard file integrity checker from www.gfi.com [is free]

Or call a consultant that knows security for assistance.

If you have trouble interpreting the results of these tools, try posting them here and see if someone responds, or compare the results to another computer running similar software.

"Dolly Jack" <shadowdancer35@hotmail.com> wrote in message
news:c61901c20eeb\$717f0b50\$9be62ecf@tkmsftngxa03...

> *If you suspect that someone might have had access to your
> computer and installed spy software in order to read your
> mail and messaging, by maybe getting your passwords, or*

microsoft.public.security: Re: Detecting spy software

- > *however it works, how do you go in and locate the program*
- > *and uninstall it? Sure hope someone out there can answer*
- > *this question, so I can figure out if something is going*
- > *on, or I'm extremely paranoid.*
- >
- > *Thanks*