

## Re: i might be hacked if...

**Source:**

[http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security\\_admin/2002-07/6392.html](http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2002-07/6392.html)

---

**From:** peter ([peter@my.monarch.net](mailto:peter@my.monarch.net))

**Date:** 07/25/02

From: "peter" <[peter@my.monarch.net](mailto:peter@my.monarch.net)>  
Date: Wed, 24 Jul 2002 17:44:50 -0600

Time for the drastic step of going out and spending some hard earned cash  
Buy a new HD and a retail copy of XP for a clean install  
take out the old HD....hook up the new one in its place.Change the BIOS  
startup to CD..floppy...HD. Reboot with XP CD in place and follow the  
prompts to do a clean new install.

remove CD and reboot..dont change back yet

When this all works fine.Hook up the old HD as a slave and going into  
control panel/administrative tools/....and delete all partitions and format  
the sucker.Twice

Now change it back put the old HD as master and remove the new  
reinstall XP onto the formatted old HD....if all works well without any  
"hacks...download

ZoneAlarm(<http://download.com.com/3120-20-0.html?qt=ZoneAlarm&tg=dl-20&search=+Go%21+>) and install before anymore "hacks".Now test and run XP for a week  
if the problem is gone take the new HD and format it then return to store  
for refund.Dont forget this also requires you to reload all hardware drivers  
and all software.

I would not use any of the SONY disks without running them through a virus  
scanner and definitely not the restore discs.Not only do I bitch loudly when  
I feel I,ve been screwed by a company I also dont have the patience to track  
down a complicated problem like this.If all else fails format

...format..format and reinstall

peter

"ToasTd" <[blister@attbi.com](mailto:blister@attbi.com)> wrote in message  
news:096b01c23342\$7be3f3f0\$19ef2ecf@tkmsftngxa01...

- >
- > *what the heck...i just read this as it got posted and cant*
- > *think of anything else to do but keep going.*
- >
- > *there was a trojan security site that offered a "Message*
- > *The Tech" feature at their website that got me very*
- > *excited as i've had to accept all my email is compromised*
- > *and routinely fails on the send and/or no reply is returned*
- >

> the tech who responded to my SOS said it was most likely a  
> hardware conflict...i could just go to device manager and  
> deal with the yellow ! and it'll be ok ..that no..i wasnt  
> hacked and then he was just too busy to deal with it  
> anymore. it was the first solid contact id had with a  
> professional security tech after having given up on email  
> getting through outbound or inbound....it just doesnt  
> happen for me and i'm only being a nuisance to him with  
> this hardware "glitch" . a damn interenet security site i  
> paid for their software and was a customer its their  
> industry and livlihood this internet security stuff and  
> yet he couldnt kick me to the curb fast enough. hardware  
> conflict....gotcha  
>  
> ok...lets continue ...  
>  
> i might be hacked if...when i execute the system restore  
> command knowing that i've dilligently assigned a half  
> dozen strategic times to choose from over the last 2 weeks  
> and when i go to pick one...  
>  
> none are there  
>  
> none  
> there is nowhere to restore to nothing is available  
>  
> i might be hacked if....programs show up installed that i  
> have nothing to do with and don't wish them to be  
> installed...i'm a single man in a studio apartment noone  
> else uses or touches my computer i don't care to network  
> with anyone and don't wish anyone to network or have  
> access to me and i attempt to rigidly assign that criteria  
> to the policy and permissions refusing anything to do with  
> file sharing or remote access and yet...  
>  
> today it was gator..GAIN the password assistant type  
> program that keeps track of all your passwords and does in  
> line completion for you when it's installed so it  
> remembers every password and executes them in the command  
> line by script...  
>  
> isnt that a lovely thing to find  
>  
> voila...first thing this morning i notice a GAIN folder in  
> my start menu not with an .exe to start it but only a link  
> to their website. when i go to their website they kindly  
> inform us that if i want to uninstall it all i have to do  
> is click the uninstall command or backtrack it out with  
> the remove programs function in the control panel...  
>  
> ya..right

>  
> *there is no folder there is no readme there is no anything*  
> *and i havent been in every corner yet but there isn't even*  
> *anything openly visible in HKLM Software of the registry.*  
> *theres an install log i'll attach to this you can all look*  
> *at and yet theres no trace of it accessible to remove.*  
>  
> *\*sigh\**  
>  
> *i might be hacked if i remember finding my way into MSN*  
> *chat back in late december and having to accept an activeX*  
> *chat engine downloaded upon entering their proprietary*  
> *chat rooms....*  
>  
> *i also noticed that i continually bogged down to where the*  
> *mouse wouldnt even click buttons like syrup it seemed to*  
> *be flooding me without anything noticable in my processes*  
> *or open programs...*  
>  
> *3 weeks later the announcement from microsoft about a*  
> *buffer overflow patch available for their chat module it*  
> *seems you could overflow the buffer and then execute code*  
> *remotely on another machine.*  
>  
> *that is mostlikely where it began although i also remember*  
> *being offered a really neat website i should take a look*  
> *at and in my eagerness for all things neat i clicked the*  
> *link and noticed this wasnt a website as much as just a*  
> *page whith no other links out ...that may have been where*  
> *i had something introduced to my machine.*  
>  
> *i may be hacked if....i install a program that operates*  
> *with beauty and precision in giving me access to*  
> *background information and activity making things visible*  
> *to help me become more aware of just exactly what the hell*  
> *i'm victim to and this program (pick one of the 4 dozen*  
> *i've experienced this situation with) ...after i've*  
> *rebooted or left the computer to go to work i'll have to*  
> *accept it's very quickly and very completely become*  
> *benign...or impotent ..or it just plain dissapears from*  
> *the machine.*  
>  
> *stuff like tiny firewall and outpost firewall...tds-3*  
> *trojan system...o man these are all the sexiast powerful*  
> *security tools known to man...and within a couple reboots*  
> *they've been taken over by the kernel level system files*  
> *that own the 0 ring of my hard drive. the worst thing to*  
> *deal with is when i click on the icon to start this*  
> *program and nothing happens*  
> *no interface no nothing*  
> *and sometimes the button doesnt even click or move*

microsoft.public.windowsxp.security\_admin: Re: i might be hacked if...

>  
>  
> *i might be hacked if i experience first hand and*  
> *unfailingly constant denial of access to things on my*  
> *computer that i expect to have access to. its my computer*  
> *and yet...*  
> *...process explorer is a program that operates in debug*  
> *mode and i'm told by the error message that i'll need*  
> *administrator priveledge to use it.*  
>  
> *i logon with administrator priveledge i guess i'm just not*  
> *administrator enough.*  
>  
> *i'm very anxious for anything constructive to come my way*  
> *for me to try that i havent thought of or tried 9 or 10*  
> *times already and will be very grateful for anything you*  
> *guys can offer. understand that i've most likely*  
> *considerd it and either done it or cant afford to do it*  
> *already but still i hold on to the desparate optimism that*  
> *theres someone who's gonna know all about this and toss me*  
> *a nice little fix so i can be on my way and out of*  
> *everyones hair with this situation.*  
>  
> *thankyou for staying with me through this it's nice for a*  
> *change to not be helpless and alone with this problem*  
>  
>

---

Outgoing mail is certified Virus Free.

Checked by AVG anti-virus system (<http://www.grisoft.com>).

Version: 6.0.377 / Virus Database: 211 - Release Date: 15/07/2002