

## Re: Problems with an Outside Threat who is accessing my computer I

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-02/0584.html>

---

*From:* Steven L Umbach (*n9rou\_at\_nospam-comcast.net*)

*Date:* 02/13/05

Date: Sun, 13 Feb 2005 14:36:22 -0600

What disabled user accounts are being accessed and how do you know they are being accessed?? How do you know there is a keylogger?? How are you determining that the items you are listed have been modified in a malicious way?? The operating system and the application will modify [write/delete files] in normal operation. Services can become disabled due to software conflicts also. You might want to try a different antivirus package.

If your NAT router is correctly configured, remote administration access to it has been disabled, and the default admin password has been changed there is not a way for someone to access your computer through the firewall from the outside via a connection not initiated by your computer. The only way that they could do such is with your cooperating as in you installing a Trojan from an email attachment or infected software that you install. Any user with physical access to your computer can also install malicious software. Then your computer would be allowing an attacker access to your computer by "phoning home".

When you reinstall the operating system, you must first format the hard drive with ntfs and install the operating system from an authentic operating system install disk – not a copy someone gave you. Right after the install go to System Properties and disable Remote Assistance and Remote Desktop [if XP Pro]. You must configure your computer to be secure [including using strong password] and not connect it to the internet until it is protected by a firewall and the first thing you should do is install critical updates from Windows Updates and the second is to update your virus definitions. Any software you install on your computer must be authentic and not a copy of something someone gave you which may perpetually infect your computer and do not install any software until your computer is current with critical updates and your antivirus is running and updated. If you are downloading software, only do it from reputable websites such as cnet.com. If you are restoring data to your new operating system install, you must scan that data for malware before you copy it to your computer. After restoring your computer do a full malware scan right away.

If your computer is indeed being hacked, more than likely it is from malware you are installing on it willingly or unwillingly assuming no one else has

microsoft.public.security: Re: Problems with an Outside Threat who is accessing my computer I

physical access to your computer. — Steve

"Sidney" <Sidney@discussions.microsoft.com> wrote in message  
news:BAE777EE-7080-4A27-9C54-6F1EDC4EE0F6@microsoft.com...

> Hello,  
> Thank You for Responding and your Time and Information,  
>  
> I have performed the steps that you have provided in your response, this  
> outside threat is Keylogging my passwords and accessing my DISABLED user  
> accounts and DISABLING my mcafee personal firewall plus services to gain  
> ILLEGAL access to this dell computer system.  
>  
> I change the passwords in my DISABLED user accounts a number of times a  
> day  
> and this outside threat is KEYLOGGING the passwords and he is also  
> compromising my emails accounts, deleting the emails from tech support  
> agents  
> who provide troubleshooting steps.  
>  
> The mcafee security center on this dell computer system has been MODIFIED:  
>  
> C:\Documents and Settings\All Users\application  
> Data\Mcafee.com\VSO\Data\mcvsrpt.dat WAs CREATED  
>  
> C:\Documents and settings\All Users\Application Data\Mcafee.com\VSO\Data  
> Was MODIFIED  
>  
> C:\Windows\Prefetch WAs MODIFIED  
>  
> C:\Windows\Prefetch\MCVSMAP.EXE-\155ED7D3.pf WAs MODIFIED  
>  
> I have performed system restores, system config, reinstalling and  
> reformatting the hard drive, changing my passwords frequently, computer  
> lock  
> and logging off when I am not using this dell computer system, clearing  
> all  
> lists and files and folders and I do not share my passwords with anyone  
> and I  
> do not save my passwords and I have a router, but none of these methods  
> are  
> preventing this outside threat from ACCESSING this dell computer system or  
> removing him from this dell computer system.  
>  
> Thank You for your Time,  
> Anita  
>  
>  
> "Steven L Umbach" wrote:  
>  
>> You are going to have to a fresh install of your operating system to a  
>> freshly formatted hard drive. Before you do this you will want to back up

Re: Problems with an Outside Threat who is accessing my computer I

>> *any important data to a cdrom or such. That data will have to be scanned*  
>> *for*  
>> *malware with a program that is current with virus definitions before you*  
>> *restore it to your newly installed operating system. If you are unsure of*  
>> *how to do all this take your computer to someone who does or the problems*  
>> *may persist.*  
>>  
>> *Steps have to be taken to prevent attacks or they will happen again. You*  
>> *don't mention your operating system but I will assume it is XP Home since*  
>> *the computer is fairly new.*  
>>  
>> *If you are using a cable/dsl modem then be sure to use a NAT router*  
>> *firewall*  
>> *device as your first line of defense. They can be purchased for as little*  
>> *as*  
>> *\$19 after rebates from the likes of Linksys, Netgear, or D-Link at Best*  
>> *Buy*  
>> *or Amazon.com. Make sure that it can not be configured remotely and*  
>> *change*  
>> *the default password for configuration – this is a must. Here are some*  
>> *more*  
>> *must do's.*  
>>  
>> *-- If using XP be sure to install Service Pack 2 and do not lower your*  
>> *Internet Explorer security settings from default. Occasionally check the*  
>> *settings for Internet Web Content Zone and make sure it is set to*  
>> *default.*  
>> *You can do that via Internet Explorer/tools/internet options/security.*  
>> *Also*  
>> *check privacy to make sure it is never lower than medium.*  
>>  
>> *-- Be very careful in what you say yes to when you are browsing the*  
>> *internet. Unless you are absolutely sure of what you are doing close the*  
>> *dialog box by selecting the X in the upper right hand corner of the pop*  
>> *up*  
>> *dialog box without selecting yes or no.*  
>>  
>> *-- Always use hard to guess passwords and do not give them out to another*  
>> *user ever. If you write them down, store them in a safe place. Change all*  
>> *passwords*  
>> *that you are currently using.*  
>>  
>> *-- Be extremely careful in using your passwords on another computer that*  
>> *you*  
>> *do not have control of to for instance access you email account, online*  
>> *banking, etc. As someone could capture your passwords that way. If at all*  
>> *possible don't do it.*  
>>  
>> *-- Always logoff of or lock your computer when you are not using it and*  
>> *other people can physically access it. Create a regular user account that*  
>> *is*

microsoft.public.security: Re: Problems with an Outside Threat who is accessing my computer I

>> *not in the local administrators group and use that account for normal  
>> computer use and also create one for other users that you may allow  
>> access  
>> to your computer.  
>>  
>> -- Never, ever go to a website from a link in an email and enter any  
>> passwords or confidential info as almost for sure these are bogus  
>> websites  
>> trying to steal your information. Often such websites will look exactly  
>> like  
>> the real thing.  
>>  
>> -- Never let the operating system, Internet Explorer, a website, or any  
>> application save your passwords for easier access at a later time. Never  
>> use  
>> your computer logon password for anything else – just use it to logon to  
>> the computer.  
>>  
>> -- Keep your computer current with critical updates at Windows Updates.  
>> This  
>> can be done automatically as explained in the first link below.  
>>  
>> -- Test your firewall configuration occasionally at a self scan site such  
>> as  
>> <http://scan.sygatetech.com/>.  
>>  
>> -- Use a quality antivirus scanning program that is kept up to date with  
>> virus definitions, preferably automatically, and have it configured to  
>> scan  
>> ALL emails no matter who they come from and all downloads, and also  
>> configure it to "monitor" your computer all the time. Norton antivirus  
>> for  
>> instance can do this. Email attachments are the number one source of  
>> malware attacks often appearing to come from trusted sources.  
>>  
>> -- Never download software from file sharing sources such as kazza and  
>> never  
>> install software on your computer that someone gives to you. There are  
>> many  
>> places to download software from such as Cnet. Don't accept files over  
>> internet chat programs. People you may trust may not realize the software  
>> or  
>> files they give you are malware infected.  
>>  
>> -- Always scan for malware immediately anytime you suspect something is  
>> wrong or that you think you allowed malware to be installed. See the last  
>> two links below for a free stand alone package from Trend Micro called  
>> Sysclean that can also be used and does not have to be installed. Just  
>> download Sysclean and the pattern file to a common folder to run from.  
>> The  
>> pattern file will need to be unzipped.*

Re: Problems with an Outside Threat who is accessing my computer I

microsoft.public.security: Re: Problems with an Outside Threat who is accessing my computer I

>>  
>> -- *If you are using wireless networking, someone could be accessing your  
>> computer or network through the wireless access point and bypass your  
>> firewall if your wireless network is not secured using WEP or WPA  
>> encryption/authentication. WEP is not very secure and the WEP keys need  
>> to  
>> be changed periodically.*  
>>  
>> -- *Keep in mind that anyone who has access to your computer can  
>> compromise  
>> it and do things like install keyboard loggers, backdoor programs, and  
>> possibly extract passwords on it. Depending on your situation this may or  
>> may not be a problem. I hope some of this helps. The links below also may  
>> help. --- Steve*  
>>  
>> <http://www.microsoft.com/athome/security/protect/default.msp> -- *Protect  
>> your PC from Microsoft.*  
>> <http://mvps.org/winhelp2002/unwanted.htm> -- *tips on securing Internet  
>> Explorer and how to check for parasites.*  
>> <http://www.trendmicro.com/download/dcs.asp>  
>> <http://www.trendmicro.com/download/pattern.asp>  
>>  
>> "Sidney" <Sidney@discussions.microsoft.com> wrote in message  
>> news:9490515A-DC16-4163-B101-3B183F31ED79@microsoft.com...  
>> > Hello,  
>> > I am having very serious problem with an outside threat who is  
>> > accessing  
>> > my  
>> > computer system Illegally, by accessing my DISABLED user's accounts and  
>> > DISABLING my mcafee personal firewall plus to gain Illegal access to  
>> > this  
>> > computer and who is keylogging my passwords, removing, modifying,  
>> > recreating  
>> > the programs on this dell computer system, stopping scheduled scans  
>> > from  
>> > running and who is also compromising my emails accounts, deleting emails  
>> > from  
>> > tech support agents who are sending troubleshooting steps to remove  
>> > this  
>> > outside threat from my computer system.  
>> >  
>> > The hard drive will be replaced on this dell computer system 3 times  
>> > and I  
>> > have only had this computer for less than one year and I performed  
>> > system  
>> > restores, reinstalling the windows operating system, system configs and  
>> > various other troubleshooting steps and still I Cannot remove this  
>> > outside  
>> > threat from this dell computer system.  
>> >  
>> > Do you have any suggestions, on how to remove this outside threat, from

Re: Problems with an Outside Threat who is accessing my computer I

microsoft.public.security: Re: Problems with an Outside Threat who is accessing my computer I

>> > *this*  
>> > *dell computer system?*  
>> >  
>> > *Thank You,*  
>> > *Anita*  
>>  
>>  
>>