

Re: Hacked or.....Would appreciate expert help

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-01/msg00628.html>

- *From:* Maryellen <Maryellen@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 27 Jan 2006 17:52:27 -0800
-

"Patrick Dickey" wrote:

> Hi Maryellen, my answers are in line....

>

> Maryellen wrote:

>> I am not sure how to post a reply, as you can see from the previous post. I

>> hope this is right because I can't believe, or I should say, I really can

>

> When you find a post that you want to reply to, simply click the Reply

> button (or Press CTRL-R in some newsreaders). Scroll down to where you

> want to reply, then press the Enter key, and type in your reply (or

> scroll completely down to the bottom and press the Enter key and start

> typing).

Thank you Patrick. Thanks for understanding that I am not stupid just because a) I'm a woman, and b) I have never used a newsgroup before.

I cannot believe the a-hole, Philip, who told me I might as well ask Sponge Bob Square Pants for help. Like most male computer users, he didn't hear what I am saying because he assumed I am just the sort of stupid woman who would go through four new dcomputers in three years, and spend a quarter of my time trying to get help, because of just the event viewer? Give me a break. I'll deal with him later.

>

> <Snipped to conserve space>

>

>> crazy about all the security holes and vulnerabilities in Windows XP that let

>> hackers practically just hop on and create a domain. If you want to

>> compare notes that would be great. If you find someone who knows what you're

>> talking about, please, please let me know. Okay, the new thing the NT

>> Authority is doing is to turn on my computer on every night at 11:58 p.m. If

>> I don't hear it running, they can be on for hours. Sometimes I turn it off

>> and it comes right back on. I now have to unplug it at night. I am a

>> standalone. No one uses my computer but me. I am not on a domain network,

>

> AFAIK (As Far As I Know) NTAauthority cannot turn your computer on from a

> Powered off state. That being said, Wake-On-LAN can do so, possibly.

> If the computer is in hibernation or standby, then Wake-On-LAN will most

> definitely turn it on.

Re: Hacked or.....Would appreciate expert help

>
> Wake-On-LAN is a feature of your NIC (Network Interface Card) that
> allows it to wake the computer up when an incoming connection starts.
> (For a more accurate description of Wake-On-LAN, I would suggest
> searching online for it).
>
> In your situation, NTAAuthority ****may**** be the application that is
> receiving a connection, which would cause the computer to wake up.
>
> Instead of unplugging the computer tonight, try unhooking the ethernet
> connector, and see if it still wakes up at 11:58. If not, then it's
> something to do with Wake-On-LAN, which you can disable. However, if it
> does turn on, there is something installed on the computer which is
> causing it. But, once again, AFAIK, nothing can cause your computer to
> start up from a completely powered off state, except someone or
> something pushing the button.
>
>> and yet, NT Authority has become my domain and they have all the absolute
>> powers. In the middle of the night while I am sleeping, they are busy
>> creating new logons (exactly like the ones you mentioned), making policy
>> changes and disbursing auditing privileges. Sometimes I find the permissions
>
> I think you're under a misconception here. NTAAuthority is not an
> organization or a person. NTAAuthority is another term for the operating
> system itself. Or more accurately the System-Level account (much like
> Administrator or your user account). It is the authority that allows
> scheduled tasks to run. I'm sure someone else can give you a better,
> more accurate description of what NTAAuthority is.
>
> <snipped to conserve space>
>> I have paid professional computer
>> people to work on this thing over and over until I got to where I am now: I
>> pretty much give up. All the computer people I have talked to don't know how
>> to do anything but reformat and install. Shit. I do that at least once a
>> month, sometimes more just to gain entrance to my computer for a while. They
>
> First of all, if you're paying someone to fix this, then they aren't
> doing their job (which you already know). The next time you Reformat
> and reinstall, try this method instead of what you've been doing in the
> past.
>
> 1. Backup ONLY your documents and pictures.. You can either do a
> backup with NTBackup, or simply burn CD's (my personal recommendation)
> Any programs that you have installed, you ****Should**** have setup programs
> (CD's or downloaded files) to reinstall them. Do not back them up at
> all. If you don't have the CD's or setup files, you'll need to get them
> from wherever you originally got them. Get them on a different computer
> (not yours).
>
> a. One of the files that you need to download is called MBSA
> (Microsoft Baseline Security Analyzer). You'll want to put this on a

Re: Hacked or.....Would appreciate expert help

Re: Hacked or.....Would appreciate expert help

> different CD, so you can install it after you've reformatted.

>

>

<http://www.microsoft.com/downloads/details.aspx?FamilyId=4B4ABA06-B5F9-4DAD-BE9D-7B51EC2E5AC9&d>

> b. In step 8, I discuss Firewalls and Antivirus software. If you

> don't already have one of these, I would download their installer and

> burn it to the same CD as the MBSA. Then, I would install them in step

> 2. Please pay special note to my warning if your System Restore CD

> provides you an Antivirus program.

>

> 2. Use the System Restore CD's that came with your computer. Install

> your programs from the CD's or setup files that you have. Don't restore

> your documents and pictures yet. Also, DO NOT go onto the Internet or

> even connect your network up until later on.

>

> 3. If you don't already have Service Pack 2, you'll be getting it soon.

> Open up the Control Panel (Start Menu----> Control Panel) then go

> into Administrative Tools, and double click on the Services icon.

>

> 4. Inside of the Services icon, do the following and only the following.

> a. Scroll down until you find a service called Messenger. Right

> click on this, and select Properties. Stop it, if it's running, and

> choose the option for Disabled in "Startup". Click Apply, then OK.

> b, Scroll down a little further, until you see Remote Procedure

> Call. (There will be 2 of these, you'll do the same steps for both of

> them). Right click on the RPC service and select Properties. DO NOT

> Stop the service or change the startup option. Click on the tab that

> says "Recovery" and change all of the options to "Take No Action."

> Click Apply and then OK (Do this for both of them).

>

> You can close the Services window after this.

>

> 5. Install the MBSA (that you downloaded prior to reformatting) and

> then run it. It will give you steps for disabling Anonymous login and

> the Guest account. Follow these steps exactly. It will also recommend

> updates that you need (which will be most of them, since you haven't

> updated yet).

>

> 5. In the Control Panel window (should be at Administrative Tools),

> click the Back Button. Go to Users and turn the Guest account OFF (If

> it's turned on).

>

> 6. Also, in the Control Panel, you'll want to double click on Internet

> Connection Firewall (Windows Firewall) and turn it on.

>

> 7. Now, you're ready to connect to the Internet. The FIRST site you

> need to go to is <http://windowsupdate.microsoft.com>. Get all of the

> Critical Updates, even if it takes a week to download them. Don't go

> anywhere else, until you've done this.

>

> 8. I highly suggest that you check into a personal Firewall. ZoneAlarm

Re: Hacked or.....Would appreciate expert help

> (<http://www.zonelabs.com>) Kerio (<http://www.sunbelt-software.com/kerio>)
> are the two that I recommend. However, there are others that are
> recommended in this newsgroup which are just as good. Install this, and
> if necessary turn Windows Firewall off (The firewall that you install
> may do this for you).
>
> 9. If you don't have an antivirus software, get one. There are a lot
> of good 'free' versions out there, as well as some good commercial
> versions. Symantec (Norton's Antivirus) is alright (IMHO) Panda Security
> is good, Trend Micro is good also. As for the 'free' ones, I personally
> use Avast! and have used AVG. I'll provide links for these next.
>
> *** If you already have an antivirus that is installed during the System
> Restore, your best bet is to get the latest updates for that (this may
> require you to pay for a new subscription). DO NOT, under any
> circumstances, run more than one antivirus on your computer at the same
> time. (This doesn't apply to 'Online Virus scanners')
>
> 10. Scan your CD's that you copied all of your documents and pictures
> to. If they have viruses on them, make note of which files are
> infected. You won't be able to (and you wouldn't want to) get these
> files back. After you've scanned the CD's, you can proceed to copy them
> back to your computer.
>
> <Snipped to conserve space>
>
> I have found files suggesting that they use my newish computer with
> lots of
>> memory to hack others. Check out your MMC and see if you are allowed to
>> change anything. Last week I turned the computer on and discovered there was
>> a new account: NET Framework. Oh I could go on and on. I really think if I
>
> Once again, you're under a misconception. .NET Framework is not an
> account. It's the backbone that makes a lot of your programs
> (especially programs from Microsoft) run. It is a required item, and
> you will end up getting it in your Windows Updates.
>
>
> I'm hoping that you find some useful information in what I've told you.
> The most important thing, when you buy a new computer (or restore an
> older one) is to get your antivirus and your firewall up and running.
> Truthfully, if you can get a firewall before you reformat, include it in
> your Installed programs. That way, you don't have to worry about
> turning on Windows Firewall before you go to Windows Update. Then, go
> to Windows Update, and get whatever security patches they have for you.
>
> If you have any questions about what I've posted, or about NTAuthority
> or .NET Framework, please ask them. The only way you're going to learn,
> is by asking what is this?. We're here to help you out.
>
> ---

Re: Hacked or.....Would appreciate expert help

Re: Hacked or.....Would appreciate expert help

> Patrick Dickey <pd1ckey43@xxxxxxxxxxxxxxxxxxxx>
> <http://www.pats-computer-solutions.com>
> Smile.. someone out there cares deeply for you.
>
.

• *Follow-Ups:*

◆ *Re: Hacked or.....Would appreciate expert help*

◇ *From:* Maryellen

• Prev by Date: *Re: Kama Sutra / W32.Blackmal.E worm questions*

• Next by Date: *Re: Has my Hotmail account been infiltrated?*

• Previous by thread: *Re: Hacked or.....Would appreciate expert help*

• Next by thread: *Re: Hacked or.....Would appreciate expert help*

• Index(es):

◆ *Date*

◆ *Thread*