

Re: Paranoia or something more sinister?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-01/msg00006.html>

- *From:* "Steven L Umbach" <n9rou@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sun, 1 Jan 2006 01:29:40 -0600
-

I should add that you want to verify that your current firewall is correctly configured to protect your network from inbound traffic that is not in response to traffic that came from your computer. One easy way is to use one of the self scan sites such as <http://scan.sygatetech.com/> and do at least a couple of the scans available there. --- Steve

"Steven L Umbach" <n9rou@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:OTHULRqDGHA.516@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

- > Use lusrmgr.msc to check what users are in the local users on your
- > computer or use the command net users it may not be what you expect. Also
- > make sure that auditing of logon events is enabled in Local Security
- > Policy so you can see what users are logging onto the computer and via
- > what logon type as explained in the link below by reviewing the security
- > log via Event Viewer. I would also enable auditing of account management.
- > A user account will not survive a pristine install to a formatted system
- > drive [assuming System State restore was not done afterwards] but it will
- > for an upgrade/repair install. It almost sounds like someone has remote
- > control of your computer and all what you describe sounds very strange and
- > I would be concerned. You should not rely on intrusion detections alone
- > and should do full system scans for malware and spyware in Safe Mode also
- > being sure that you are using the latest updates for your programs.
- > Keeping current with critical security updates at Windows Updates is also
- > a must.
- >
- > <http://www.windowsecurity.com/articles/Logon-Types.html>
- >
- > Try using the free tools from SysInternals – Process Explorer, TCPView,
- > and Autoruns to see what processes are starting up at startup/logon, to
- > see advanced information on what processes are running on your computer
- > including the associated executable and publisher, and what ports are
- > being used and by what process/executable. Also I would consider using a
- > firewall that is more advanced than the Windows Firewall in your case.
- > Something like Zone Alarm is free and fairly easy to use. Such a firewall
- > will alert you when an application on your computer that have not approved
- > tries to access the internet but you need to review the list of
- > applications periodically to make sure that nothing unusual has been added
- > to the list by someone or some process. If any other users have access to
- > your computer [friends, family, strangers, or foe] they could be installing

Re: Paranoia or something more sinister?

> or configuring something that may be causing your problem. ---- Steve
>
> <http://www.sysinternals.com/Utilities/TcpView.html> ---- TCPView and link
> to SysInternals
>
> <tp://www.microsoft.com/athome/security/protect/windowsxpsp2/Default.msp>
> ---- Protect Your PC tips and other links.
>
> "shreaker" <shreaker@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
> <news:7E4E6B43-6C25-4D6F-BCC7-7250815DBEA6@xxxxxxxxxxxxxxxxxxxx>
>> Hi All
>>
>> I believe I may have a few internet security issues that I'd like to run
>> by
>> you guys -
>>
>> I have performed a number of professionally assisted operating system
>> reinstalls, upgraded Norton Security to 05, I'm operating Service Pack 2
>> and
>> also use Microsoft AntiSpyware, Search & Destroy and a Windows Firewall.
>>
>> I also like to ensure I am closely observing generic security advice and
>> practices and applying basic common sense (- eg: windows passwords are
>> changed intermittently, regular and comprehensive security scans are
>> executed
>> on a regular basis, password protection for "sensitive" info within
>> Outlook
>> and Word is used and I aim to minimise any time spent logged on with
>> Administrative rights.
>>
>> However, despite the above, I continue to experience issues that cause me
>> some concern. These are as follows -
>>
>> * The Task Manager "Users" tab displays an old username that I used PRIOR
>> to
>> full system reinstalls
>>
>> * Sluggish navigational performance - (eg, desktop icons lagging while
>> populating)
>>
>> * IE browser & Word forms changing size - and I don't believe at my doing
>>
>> * I don't seem to receive any notifications or Intrusion Detections
>> regarding random security breach attempts from either Norton or Search &
>> Destroy, as I have done in the past when I've been online for reasonably
>> long
>> periods of time and/or navigating around less reputable sites
>>
>> * When attempting to log off I often get the following prompt - "Other
>> users
>> are currently using this computer. Logging off may cause them to loose

Re: Paranoia or something more sinister?

Re: Paranoia or something more sinister?

>> data,
>> are you sure you want to log off?"
>>
>> (I do not and have not ever operated a LAN and I am aware of issues
>> others
>> have noted that are suspected to have been compromised remotely?)
>>
>> * The mouse often moves across the screen without me operating it – at
>> first, I put this down to the nature of an aging infrared mouse –
>> however,
>> this is occurring more and more frequently
>>
>> * The clicking sound of a mouse pointer in action – when I am not
>> touching
>> any parts of the computer or running any operations that could cause this
>> to
>> take place
>>
>> From observation of any the above – does anything stand out that would
>> indicate to you that my PC security may still be at risk? If so, what
>> should
>> I do that I'm not
>> already doing?
>>
>> I'm hoping it's all just a healthy dose of paranoia – please let me know
>> if
>> you suspect otherwise and what you would recommend?
>>
>> Any help here is much appreciated!
>>
>> Kind Regards
>> Damien
>>
>
>

• **References:**

◆ **[Paranoia or something more sinister?](#)**

◇ *From:* shreaker

◆ **[Re: Paranoia or something more sinister?](#)**

◇ *From:* Steven L Umbach

- Prev by Date: **[Re: Paranoia or something more sinister?](#)**
- Next by Date: **[Re: Norton Internet Security 2006](#)**
- Previous by thread: **[Re: Paranoia or something more sinister?](#)**
- Next by thread: **[Re: Paranoia or something more sinister?](#)**

Re: Paranoia or something more sinister?

- Index(es):

- ◆ *Date*

- ◆ *Thread*