

Re: Help, I've been hacked

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2005-03/0848.html

From: Wesley Vogel (123WVogel955_at_comcast.net)

Date: 03/10/05

Date: Wed, 9 Mar 2005 20:55:48 -0700

Kim,

My advice is to ignore Event ID 680 & 529. That's what I do. I get them both quite often.

ID: 540 Source: Security

[[User Action

No user action is required.]]

<http://www.microsoft.com/technet/support/ee/result.aspx?EvtSrc=Security&EvtID=540&ProdName=Windows+Opera>

After the novelty wears off you'll quit worrying about what the firewall reports and just block every incoming. Although the SPACE AND NAVAL WARFARE SYSTEM COMMAND is more interesting than anything I ever got. ;-) Maybe they need some more computing power and heard about you. <LOL>

Keep having fun!

--

Hope this helps. Let us know.

Wes

MS-MVP Windows Shell/User

In news:81A8C14C-071B-47D5-8BE4-AE5E5A6F52EC@microsoft.com,

TxRose <TxRose@discussions.microsoft.com> hunted and pecked:

> LOL Wes...

>

> Actually I am now more confused.

>

> I have checked out the articles at:

>

> <http://support.microsoft.com/?kbid=305822>

>

> <http://support.microsoft.com/?kbid=811082>

>

> <http://support.microsoft.com/?kbid=305822>

>

> Mine are similiar, but not the same. I am not sure if that matters or

> not. There are always 4 failures in a row.

>

> The first being:

>

> Event Type: Failure Audit

Re: Help, I've been hacked

microsoft.public.windowsxp.security_admin: Re: Help, I've been hacked

```
> Event Source: Security
> Event Category: Account Logon
> Event ID: 680
> Date: date
> Time: time
> User: NT AUTHORITY\SYSTEM
> Computer: %computer name%
> Description:
> Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
> Logon account: %user name%
> Source Workstation: %computer name%
> Error Code: 0xC000006A
>
> Then
>
> Event Type: Failure Audit
> Event Source: Security
> Event Category: Logon/Logoff
> Event ID: 529
> Date: date
> Time: time
> User: NT AUTHORITY\SYSTEM
> Computer: %computer name%
> Description:
> Logon Failure:
> Reason: Unknown user name or bad password
> User Name: %user name%
> Domain: %computer name%
> Logon Type: 2
> Logon Process: Advapi
> Authentication Package: Negotiate
> Workstation Name: %computer name%
>
> Then
>
> Both of the two errors above repeated once again.
>
> What I got out of the MS articles is:
>
> 1. Disable the Welcome screen and use the classic logon screen
> (which I don't know how to do)
> 2.This was supposed to be fixed with sp1. Guess what? It wasn't ...LOL
> 3.Turn off auditing of logon events.
> To do this, the article on:
> http://support.microsoft.com/?kbid=305822
> tells me to:
>
> To turn off auditing in the Microsoft Management Console (MMC)
> snap-in for Group Policy:
>
> 1. Click Start, click Run, type gpedit.msc, and then click OK.
>
> But
>
> My computer stops me from going any farther, as I get an error
> saying my computer can't find gpedit.msc.
>
> 2. In the left pane, expand the following items:
> Policy
> Computer Configuration
> Windows Settings
> Security Settings
> Local Policy
```

microsoft.public.windowsxp.security_admin: Re: Help, I've been hacked

> 3. Click Audit Policy.
> 4. Double-click Audit Logon Events.
> 5. Click to clear the Success and Failure check boxes.
> 6. Click OK.
> 7. Close the Group Policy window.
>
> Do you know why I would be getting this success event?
>
> Date: Source: Security
> Time: Category: Logon/Logoff
> Type: Success A Event ID: 540
> User: NT AUTHORITY\ANONYMOUS LOGON
> Computer: owner
> Successful Network Logon:
> User Name:
> Domain:
> Logon ID: (0x0,0x2C33D)
> Logon Type: 3
> Logon Process: NtLmSsp
> Authentication Package: NTLM
> Workstation Name:
> Logon GUID: {00000000-0000-0000-0000-000000000000}
>
> This is all getting to be too much. I just want to use my computer to
> have fun, and enjoy myself.
> All this spyware, adware, trojans, worms, yada yada yada is to the
> point of being ridiculous.
> If there is help on the way for us home computer users, it can't come
> soon enough.
>
> I don't ever remember having this many problems using 98, or ME. At
> least not to my knowledge.
> I'm sure they had their problems too.....but everyday, I look at
> those other 2 computers sitting there on the other side of the room,
> and my thoughts are getting closer to swapping them out to use,
> instead of this XP one..LOL
>
> And, if those people in China and Korea don't stop pinging me, I
> think I'll scream.
>
> I just got probed by someone with the IP address of 205.98.250.77,
> using the name:
> SPACE AND NAVAL WARFARE SYSTEM COMMAND
> City: WASHINGTON
>
> Don't these people have anything better to do? And what's in it for
> them?
>
> Thanks for the help Wes,
>
> Kim
>
> "Wesley Vogel" wrote:
>
>> Kim,
>>
>> These??
>>
>> Event Type: Failure Audit
>> Event Source: Security
>> Event Category: Account Logon
>> Event ID: 680

microsoft.public.windowsxp.security_admin: Re: Help, I've been hacked

```
>>
>> Failure Events Are Logged When the Welcome Screen Is Enabled
>> http://support.microsoft.com/?kbid=305822
>>
>> Event Type: Failure Audit
>> Event Source: Security
>> Event Category: Logon/Logoff
>> Event ID: 529
>>
>> [[The event occurred on Windows XP if the machine environment meets
>> the following criteria:
>> - The machine is a member of a domain.
>> - The machine is using a machine local account.
>> - Logon failure auditing is enabled.
>> When the user logs off, Windows will write event ID 529 to the log
>> file because
>> the OS incorrectly tries to contact the domain controller (DC),
>> despite the fact that the machine is using a local account.
>> Microsoft currently doesn't provide a fix for this problem, but you
>> can safely ignore this event ID.]]
>>
>> Security Event 529 Is Logged for Local User Accounts
>> http://support.microsoft.com/?kbid=811082
>>
>> Failure Events Are Logged When the Welcome Screen Is Enabled
>> http://support.microsoft.com/?kbid=305822
>>
>> --
>> Hope this helps. Let us know.
>>
>> Wes
>> MS-MVP Windows Shell/User
>>
>> In news:0A64EB31-56BB-4716-A7A7-6BF5085C43AA@microsoft.com,
>> TxRose <TxRose@discussions.microsoft.com> hunted and pecked:
>>> Hi Wes,
>>> Yes that information does help. Thank you.
>>> I agree that the information of the Event ID & the Event Source are
>>> very important.
>>> To bad it wasn't you that I talked with while on the phone with
>>> Microsoft.
>>>
>>> The Microsoft tech and I talked for hours on the phone yesterday,
>>> and I was told that my computer is clean, and everything is fine. We
>>> tried all sorts of things looking for viruses/worms. We purged the
>>> cache, cleared out SSL state, ran scans, and cleaned out passwords,
>>> and even deleted a couple of folders in the registry.
>>> I ended up telling him I would just take my computer into the shop.
>>> I was told it would be a waste of my money..LOL
>>> He did not seem to care about the info of the Event ID & the Event
>>> Source.
>>> I am still having way too many unknown user name/bad password
>>> entries. I also do not like the successful ANONYMOUS LOGONS.
>>>
>>> Maybe I'm crazy, but these two entires alone, do not look right to
>>> me, as they are still happening.
>>>
>>> Thanks for the links. Especially the one for events and errors help.
>>>
>>> Kim
>>>
>>> "Wesley Vogel" wrote:
```

Re: Help, I've been hacked

microsoft.public.windowsxp.security_admin: Re: Help, I've been hacked

```
>>>
>>>> Kim,
>>>>
>>>> Event ID & the Event Source are very important.
>>>>
>>>> To open the Event Viewer...
>>>> Start | Run | Type:      eventvwr      | OK
>>>>
>>>> For any Events that seem related to the problem...
>>>>
>>>> Double click the event in Event Viewer | Click: the button below
>>>> the second arrow (looks like two pages) [[Copies the details of the
>>>> event to the Clipboard.]] | Paste into Notepad | Click:
>>>> For more information, see Help and Support Center at
>>>> http://go.microsoft.com/fwlink/events.asp.
>>>>
>>>> Read all info | Copy and paste to Notepad | Click the [+] Related
>>>> Knowledge Base articles | Follow any links that might be useful
>>>>
>>>> HOW TO: View and Manage Event Logs in Event Viewer in Windows XP
>>>> http://support.microsoft.com/default.aspx?scid=kb;en-us;308427
>>>>
>>>> Event Viewer overview
>>>>
>>
http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/event\_overview\_01.
>>>>
>>>> This can also be very useful.
>>>> You need to have the Event ID & the Event Source.
>>>>
>>>> To view Windows XP Events and Errors, type the Source (for example,
>>>> Print) and/or the Event code (for example, 20) into the ID field,
>>>> then click the Go button. Source and Event codes may be found in
>>>> the Event Viewer logs.
>>>>
>>>> Windows XP Home/Professional Events and Errors
>>>>
>>
http://www.microsoft.com/technet/support/ee/search.aspx?DisplayName=Windows%20XP%20Professional&P
>>>>
>>>> --
>>>> Hope this helps. Let us know.
>>>>
>>>> Wes
>>>> MS-MVP Windows Shell/User
>>>>
>>>> In news:36B7EF3A-84CB-43FF-AE71-0809F24ED301@microsoft.com,
>>>> TxRose <TxRose@discussions.microsoft.com> hunted and pecked:
>>>>> Hi Wes,
>>>>> Yes, it appears that did help.
>>>>> It shows disabled, instead of being started.
>>>>> I also see no entries listed of a remote access in the event
>>>>> viewer. Whoo hoo..LOL
>>>>>
>>>>> This entry in the event viewer looks good:
>>>>> The Remote Access Connection Manager service was successfully
>>>>> sent a stop control.
>>>>> Thank you for helping me get that turned off.
>>>>>
>>>>> However, when I just rebooted, I did see these, which do not look
>>>>> good in my opinion, but I could be wrong:
>>>>>
```

microsoft.public.windowsxp.security_admin: Re: Help, I've been hacked

```
>>>> The first one has been going on for a long time, and is still
>>>> showing.
>>>>
>>>> Logon Failure:
>>>> Reason: Unknown user name or bad password
>>>> User Name: Owner
>>>> Domain: OWNER-1E81AA74C
>>>> Logon Type: 2
>>>> Logon Process: Advapi
>>>> Authentication Package: Negotiate
>>>> Workstation Name: OWNER-1E81AA74C
>>>>
>>>> The protected system file c:\windows\system32\racpldlg.dll could
>>>> not be verified as valid because Windows File Protection is
>>>> terminating. Use the SFC utility to verify the integrity of the
>>>> file at a later time.
>>>>
>>>> The TCP/IP NetBIOS Helper service depends on the AFD service which
>>>> failed to start because of the following error:
>>>> A device attached to the system is not functioning.
>>>>
>>>> Your computer was not able to renew its address from the network
>>>> (from the DHCP Server) for the Network Card with network address
>>>> 0011099706B4. The following error occurred:
>>>> The semaphore timeout period has expired. . Your computer will
>>>> continue to try and obtain an address on its own from the network
>>>> address (DHCP) server.
>>>>
>>>> Your computer has detected that the IP address 66.25.204.98 for
>>>> the Network Card with network address 0011099706B4 is already in
>>>> use on the network. Your computer will automatically attempt to
>>>> obtain a different address.
>>>>
>>>> Your computer has detected that the IP address 0.0.0.0 for the
>>>> Network Card with network address 0011099706B4 is already in use
>>>> on the network. Your computer will automatically attempt to
>>>> obtain a different address.
>>>>
>>>> Your computer was not able to renew its address from the network
>>>> (from the DHCP Server) for the Network Card with network address
>>>> 0011099706B4. The following error occurred:
>>>> The semaphore timeout period has expired. . Your computer will
>>>> continue to try and obtain an address on its own from the network
>>>> address (DHCP) server.
>>>>
>>>> The following boot-start or system-start driver(s) failed to load:
>>>> Aavmker4
>>>> AFD
>>>> aswTdi
>>>> Fips
>>>> intelppm
>>>> IPsec
>>>> MRxSmb
>>>> NetBIOS
>>>> NetBT
>>>> RasAcid
>>>> Rdbss
>>>> Tcpip
>>>> vsdatant
>>>>
>>>> Looks like a fun time huh?
>>>>
```

microsoft.public.windowsxp.security_admin: Re: Help, I've been hacked

```
>>>> Kim
>>>>
>>>> "Wesley Vogel" wrote:
>>>>
>>>>> Kim,
>>>>>
>>>>> Reboot.
>>>>>
>>>>> And then check on the Remote Access Connection Manager in
>>>>> Services, it probably won't have started since you disabled it.
>>>>>
>>>>> --
>>>>> Hope this helps. Let us know.
>>>>>
>>>>> Wes
>>>>> MS-MVP Windows Shell/User
>>>>>
>>>>> In news:452BD71A-2811-4B73-AFCA-5A9930F9F063@microsoft.com,
>>>>> TxRose <TxRose@discussions.microsoft.com> hunted and pecked:
>>>>>> Hi Wesley,
>>>>>> Here ae the results from what I just did in the services.msc.
>>>>>>
>>>>>> The Remote Access Auto Connection was already stopped, and I did
>>>>>> the type set to disabled.
>>>>>>
>>>>>> The Remote Desktop Help Session Manager, was also stopped, and I
>>>>>> did the type set to disabled.
>>>>>>
>>>>>> The Remote Access Connection Manager would not allow me to stop
>>>>>> it. The type set is set to Start, but I got an error saying :
>>>>>> Could not stop the Remote Access Connection Manager on Local
>>>>>> Computer. Error 1053: The service did not respond to the start
>>>>>> or control request in a timely fashion.
>>>>>> Anyway, I did the type set to Disabled.
>>>>>>
>>>>>> I am not sure if I should have, but I stopped the secondary
>>>>>> logon, and set it to disabled too.
>>>>>>
>>>>>> It looks like there are alot of things there I would like to
>>>>>> disable, but I won't without some kind of assistance first.
>>>>>>
>>>>>> Now, when I right click on my computer/properties/remote tab, it
>>>>>> is unchecked to Allow REmote Assistance invitations to be sent
>>>>>> from this computer.
>>>>>> There was not another option listed.
>>>>>>
>>>>>> Kim
>>>>>>
>>>>>> "Wesley Vogel" wrote:
>>>>>>
>>>>>>> [[Remote Access Auto Connection Manager is on by default in
>>>>>>> Windows XP Professional computers that are not members of a
>>>>>>> domain and in Windows XP Home Edition.]]
>>>>>>>
>>>>>>> Open Services and disable Remote Access Auto Connection
>>>>>>> Manager...
>>>>>>>
>>>>>>> Start | Run | Type:  services.msc  | Click OK |
>>>>>>> Scroll down to and double click: Remote Access Auto Connection
>>>>>>> Manager | If the service is running, click the Stop button |
>>>>>>> When
>>>>>>> it has stopped, under Startup
```

microsoft.public.windowsxp.security_admin: Re: Help, I've been hacked

```
>>>>>>> type set to Disabled | Apply | OK |
>>>>>>>
>>>>>>> Do the same for Remote Access Connection Manager & Remote
>>>>>>> Desktop
>>>>>>> Help Session Manager.
>>>>>>>
>>>>>>> Right click My Computer | Properties | Remote tab |
>>>>>>> Make sure that both of these are UNChecked:
>>>>>>> Allow Remote Assistance invitations to be
>>>>>>> sent from this computer Allow users to
>>>>>>> connect remotely to this computer
>>>>>>>
>>>>>>> Turn on a firewall.
>>>>>>>
>>>>>>> --
>>>>>>> Hope this helps. Let us know.
>>>>>>>
>>>>>>> Wes
>>>>>>> MS-MVP Windows Shell/User
>>>>>>>
>>>>>>> In news:E8DF3AE0-4FCB-47DB-8EEA-BAED4DBF1773@microsoft.com,
>>>>>>> TxRose <TxRose@discussions.microsoft.com> hunted and pecked:
>>>>>>> I have very very stramge entries in my registry and event
>>>>>>> viewer that are adding up to no good.
>>>>>>>
>>>>>>> I have talked with Microsoft today, and what we tried did not
>>>>>>> solve the problem.
>>>>>>> I really don't want to wait until Monday to call them back.
>>>>>>>
>>>>>>> Does anyone know where I might find where remote access
>>>>>>> connection manager is in the registry?
```