

Re: Tracking unauthorized access to my computer

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-02/msg00080.html>

- *From:* thewinner <thewinner@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 6 Feb 2006 07:44:23 -0800
-

Hello,

I was just wondering I have the full event log that I saved. Would it be possible for me to email it to you? I know the time I was having problems with someone logging into my computer last. It was this past Friday and it's all in the event log. I was working late and went to send email to my Boss, no one else was here but when I went to send the email someone took control of my computer remotely and started entering bogus characters in the email by holding down the key continuously. Then several instances of outlook began to open and I had to disconnect my computer from the network and reboot to get out of it.

"Steven L Umbach" wrote:

One thing you want to check for is for logon events that show what users are accessing your computer either locally, through file and print sharing, or Remote Desktop. The logon types can help show that as explained in the link below. The user name, logon type, and time can give you an idea who is accessing your computer, how, and when. You will see system logons which is normal but if any other user is accessing your computer it will show that also assuming that some admin did not clear the security log which itself will leave a link. Also look at your own logon events for your user account to see if it looks like someone is logging on as you which they could do if they know your password [keyboard logger, etc]. Evidence would be when you see logon events for your account when you were not there and had logged off of the computer or logons that show your user account using type 3 and type 10 assuming you do not access your computer via a file share or remote control from another computer.

<http://www.windowsecurity.com/articles/Logon-Types.html>

It is possible for a user to access a computer via remote control if they are an administrator on your computer. You could prevent such by enabling the Windows Firewall or disabling/stopping the associated service which you would find in services.msc and you can use something like Process Explorer and TCPView from SysInternals to find out which process/service is being used for such which would be listening on a port for connections. There are activity tracking programs that may also help but I don't know of any good free ones. Below is an example of such a program though I have not tried it

Re: Tracking unauthorized access to my computer

myself.

http://www.spectorsoft.com/products/SpectorPro_Windows/index.html

Like I said before you can audit access to files and folders and you may want to do it for just those specific users that are administrators on your computers to cut down on the amount of and record more pertinent object access events. I would not do it on all folders but just the ones you want evidence of access to. Of course since you are a local administrator you can remove permissions on those that you do not want to access your files and just leave your user account as the user that can access. A problem is however that administrators can always grant themselves access again [which could show via folder auditing] or simply backup your files and restore somewhere else. Using encryption such as EFS could help prevent unwanted access but even that is not foolproof in a domain environment because of Recovery Agents. I would also increase the size of the security log to like 30MB and also enable auditing of process tracking that will show what user is running a process on your computer. Yes there will be a lot of stuff in your security log it can help you build your case. Below are a couple examples of what some log entries look like. You can use filter view of the security log or the free Event Comb from Microsoft to help search through the security log for specific events, names, and text strings. --- Steve

An example of showing me accessing My Documents Folder.

Event Type: Success Audit
Event Source: Security
Event Category: Object Access
Event ID: 560
Date: 2/5/2006
Time: 10:49:32 PM
User: STEVE-XP\Steve
Computer: STEVE-XP
Description:
Object Open:
Object Server: Security
Object Type: File
Object Name: D:\Documents and Settings\Steve\My Documents\desktop.ini
Handle ID: 1972
Operation ID: {0,4850351}
Process ID: 1768
Image File Name: D:\WINDOWS\explorer.exe
Primary User Name: Steve
Primary Domain: STEVE-XP
Primary Logon ID: (0x0,0x1A85C)
Client User Name: -
Client Domain: -
Client Logon ID: -
Accesses: READ_CONTROL
SYNCHRONIZE
ReadData (or ListDirectory)

Re: Tracking unauthorized access to my computer

ReadEA
ReadAttributes

Privileges: -
Restricted Sid Count: 0

An event showing me starting Outlook Express on my computer.

Event Type: Success Audit
Event Source: Security
Event Category: Detailed Tracking
Event ID: 592
Date: 2/5/2006
Time: 10:53:31 PM
User: STEVE-XP\Steve
Computer: STEVE-XP
Description:
A new process has been created:
New Process ID: 1236
Image File Name: D:\Program Files\Outlook Express\msimn.exe
Creator Process ID: 716
User Name: Steve
Domain: STEVE-XP
Logon ID: (0x0,0x1A85C)

For more information, see Help and Support Center at
<http://go.microsoft.com/fwlink/events.asp>.

For more information, see Help and Support Center at
<http://go.microsoft.com/fwlink/events.asp>.

"thewinner" <thewinner@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:A6BB4793-B0DD-4B38-B99F-FDC66A172F4A@xxxxxxxxxxxxxxxxxxxx

Thanks for responding, I have Windows XP. I can view the event logs my problem is knowing how to read them and knowing what I'm looking for. Also whoever is doing this is using I believe the System account or some other account other than their own. Also we use a product called "Track It" which allows you to connect remotely and I believe take remote control without asking for the Users permission. I was hoping there was some kind of system file I could disable to prevent others from accessing my computer but still have the functionality I need to still be able to work. I am going to try

Re: Tracking unauthorized access to my computer

the product you suggested and see if that helps.

"thewinner" wrote:

I am a Systems Analyst with full Admin privileges. I'm having a serious problem, someone has been connecting to my computer and controlling my email, accessing files/folder, etc. I'm certain that it is someone who also has Admin privileges but there are six people with these rights and I don't know who it is. I've spoken to my Boss about the situation but without specific proof talking about it has done nothing. I'm just wondering if there is a way to trace and log who is actually logging onto my computer remotely or if there is any software that I can install or scripts that I can run in the background that would identify the individual/individuals that are doing this? Even if there is something that I could use that would record the actions as they are happening would be helpful. I desperately need some kind of concrete evidence. It's gotten to the point where the amount of times someone is connecting to my machine is unbearable and very harassing. If anyone can help me with this please respond ASAP. Thanks.