

# Re: Tracking unauthorized access to my computer

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-02/msg00057.html>

---

- *From:* "Steven L Umbach" <n9rou@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
  - *Date:* Sat, 4 Feb 2006 22:27:55 -0600
- 

You don't mention the operating system but for W2000/2003/XP you can check the security logs via Event Viewer to see who has accessed your computer. There are different logon types for console/keyboard, network, and Remote Desktop as explained in the second link below. Beware however that any administrator can clear the security logs though that itself will leave an entry in the log. You can also enable auditing of object access and then audit folder/file access though that will generate LOTS of events in the security log [be sure to increase to at least 10MB] but the info should be there. You also could install port reporter that could help show when there was activity on ports used for file and print sharing and Remote Desktop and from what source IP. Any access TO ports 139 TCP, 445 TCP, and 3389 TCP on your computer could be suspect. There are ways you can try to secure your computer from these attempts if you are allowed to such as disabling Remote Desktop on your computer, disabling and stopping the server service, and removing administrators group from your user profile folder under documents and settings. However these measures could be undone by someone that is an administrator on your computer. --- Steve

<http://support.microsoft.com/default.aspx?scid=KB:en-us;q300958>

<http://support.microsoft.com/default.aspx?scid=kb:en-us:301640>

<http://support.microsoft.com/?id=837243> --- Port Reporter

"thewinner" <thewinner@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:6CD1402E-E941-4297-822E-39CA1921A34A@xxxxxxxxxxxxxxxxxxxx>

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

Re: Tracking unauthorized access to my computer

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.