

Re: HELP! I've been made a client on my own PC!

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2002-06/1516.html>

From: JM (Jose.Matthews@med.ge.com)

Date: 06/21/02

From: "JM" <Jose.Matthews@med.ge.com>

Date: Fri, 21 Jun 2002 11:42:43 -0700

Thanks. Frankly, I do believe that it is someone who knows me and has targeted me. While I do have access to certain BIOS settings, I do not have access to passwords, etc...files that have been titled in a manner that gives hints to who this may be....I have looked at some log files and can see where a person/system was "calling" and or the results of pinging ports for signals. Firstly, I have tried to reformat and re-install quite a few times, and it doesn't seem to help. I've also downloaded a BIOS upgrade from HP, with no change. I have removed all network options....always seem to have a "Entire Network" icon, that when selected gets denied due to no access.....LOTS of restore type files all over the place....I disable Taskmanager, to no avail...same with PCHealth...the default web addy on Explorer says something like "blahblahblah....redir....)...ScanDisk always runs ok, but never seems to do a complete surface scan....I have Norton System Works, which includes antivirus applications, but have seen messages that the definition files have been corrupted....I have Symantec Internet Security loaded as a firewall, etc.....There are just too many thing. Um, again, I'm running a home/Desktop PC, yet in certain logs I've seen references made to a certain laptop.....a "wireless" device icon suddenly showed up one night...Feeling pretty dumb. Is there someone maybe I could send the HD to for analysis? Thanks again for your help...I sure appreciate it. It has been frustrating.

>-----Original Message-----

>I don't think it's very common for a hacker to lock you out of BIOS

>selections. If this is a hacker, it sounds like someone who knows you and

>has targeted you. But it sounds more likely to me that this could be some

>sort of system failure or maybe a virus. Can you

describe in more detail

>*the things that are going wrong?*

>

>*One sure test would be to format and reinstall Windows again, and don't*

>*connect it to the internet. If you still have problems*

[or if you know that

>*you had problems after installing Windows and before connecting it to the*

>*internet], the problem is probably not a hacker. Use a hardware and/or*

>*software firewall, starting with Netgear or Linksys*

BEFSR41 around \$70, and

>*consider installing Sygate firewall as well [free for non-commercial use]*

>*and check the log of blocked packets. Install an antivirus program like*

>*Norton that is set to download the latest updates every day. Search your*

>*machine for files that have changed in the past day or two or three to look*

>*for possible evidence of hacking. Download and run fport from*

>*foundstone.com and pstools including pslist and psloggedon from*

>*www.sysinternals.com to look for anything unusual. You may want to run*

>*Scandisk, and download and run some sort of hardware diagnostic tools on*

>*your computer, and/or have someone else look at your computer for problems.*

>

>*I'm not convinced that fdisk is always necessary or beneficial when*

>*reinstalling Windows. One issue is that any sectors marked bad on your hard*

>*drive are I believe marked good again after the reformatting.*

>

>

>*"JM" <Jose.Matthews@med.ge.com> wrote in message*

>*news:f3e501c21948\$adeec000\$37ef2ecf@TKMSFTNGXA13...*

>> *Hi folks... please help...My home PC is an HP Pavillion*

>> *8670C, was running Windows 98 and upgraded to ME and I*

>> *believe I was struck by a virus and/or a hacker.*

Anyway,

>> *this person has gained control at his/her will, and I am*

>> *now a client on my own PC and have virtually no control,*

>> *have been locked out of lots of BIOS selections, and have*

>> *no access to the network that appears to have been*

microsoft.public.security: Re: HELP! I've been made a client on my own PC!

>> *established on my PC. Whoever has done this continually*
>> *fu**s with me when I'm trying to use this system, and*
I'm
>> *not skilled enough to know what to do. Have tried*
>> *changing hard drives, have fdisk'd a million times, but*
to
>> *no avail. This person is even accessing my system via*
>> *wireless technology. I'm desperate, what can I do?*
Would
>> *really appreciate your help. How can I fix this, and*
are
>> *there any telltale signs/logs that might lead me to who*
>> *this person is? (Just in case, I have pretty much taken*
>> *the system apart, including removing the hard drives,*
just
>> *in case). Thanks so much!*
>
>
>
>