

Re: Vista Hacked

Source:

http://www.tech-archive.net/Archive/Vista/microsoft.public.windows.vista.performance_maintenance/2008-07/msg00

- *From:* Charlie Tame <charlie@xxxxxxxx>
 - *Date:* Wed, 02 Jul 2008 04:35:45 -0500
-

S.Quickness@xxxxxxxx wrote:

Internet Explore and Windows Host Process Server on my computer are attempting to connect multiple times a day (20 or more) to numerous google.com ip addresses across a wide viriety of ports in the 45000's. I have been unable to close the processes. The Internet Explorer process has been running as a seperate program that I am unable to see and uses 45,000k of ram. It is also not possible for me to shut the program down. I have nine svchost.exe (windows host process services) running which are also attempting to communicate with google.com. These events are of great concern to me as I work for a financial firm and keep large amounts of proprietary knowledge on my computer. Can anyone help me determine if in fact I was hacked? If I was hacked, I am not looking to have this issue repaired, I want evidence to take to the police so that I do not need to deal with these hassles again.

In the other thread you say the computer was recently "Hacked" and you had it reformatted. This implies you did not reinstall Vista yourself so who did? Did they investigate at all or just do as you asked and reinstall? In other words what confirmation do you have that the original install was actually hacked?

On my machine there are currently 12 instances of scvhost running and on explorer.exe that cannot be shut down because it is the desktop. Internet Explorer is IExplore.exe not explorer.exe.

Often when legitimate processes try to communicate and are blocked they will repeatedly try again and sometimes use a different port. The fact that your new "Firewall" is blocking things might in fact be making things look worse than they are. Software firewalls are sometimes useful but that depends on what you do with them, they can also be considered "Snake Oil".

Probably the best solution for a firewall is to use a router, even if you only have a single machine.

You can use this utility

<http://technet.microsoft.com/en-us/sysinternals/bb897437.aspx>

or go start>run?type in cmd and hit enter.

In the window type netstat -af [enter]

Re: Vista Hacked

Either should show active connections, many of which will be your machine talking (or at least listening) to itself.

The utility offered at the technet site is somewhat the better one.

If you have Google toolbar or update manager installed then random connections to google will happen, otherwise I am not sure what the connection would be between google and some alleged hacker. Can you list what security / antivirus / antispysware / search software you have installed if any? I may not be able to get back here before tomorrow but that information may help someone get a better idea of what is going on.

Getting proof of this type of thing can be difficult, it is one thing to prove that an IP address did something, quite another to establish who was using the machine at that time, so "If" something is happening it is best to stop the offender getting in rather than have it continue while investigation takes place.

.