

## Re: Trojan, but where?

**Source:**

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-02/13181.html>

---

**From:** Chuck (*none\_at\_example.net*)

**Date:** 02/26/04

Date: 26 Feb 2004 10:34:18 -0600

On Thu, 26 Feb 2004 06:31:07 -0800, Zee <djztoz@hotmail.com> wrote:

>Since yesterday my ISP has disconeted me from internet and when i called them they said one of the computers on the network is infected with a trojan. The problem is that there are about 45 computers that are all connected to internet using a router. My question was is there any antivirus or any thing alike that can scan the whole network so i dont have to scan each WS one by one.

>

>And how can i improve my security for future, i already have firewall and antivirus on every pc but what else should i do?

>

>Thanks in advance

>Zee

Zee,

Some Enterprise Edition versions of AntiVirus products support scanning shared drives over a network. Unfortunately, those products only scan the contents of specific shared folders.

To perform an effective virus check, you really have to do it from each possibly infected computer. The virus checking program has to have access to the system, system settings, and boot portions of the system, to be truly effective.

An essential part of virus protection is a regular – possibly daily scan of each computer. And a regular – at least weekly – update of virus protection signatures on each computer.

What make and version of AntiVirus protection do you have? Do you review the scan logs periodically on each computer?

Does your firewall log provide a record of outgoing traffic? If you have a single computer on your network that is infected, you should be able to identify it readily, by inspection of the firewall log.

Future suggestions:

microsoft.public.windowsxp.general: Re: Trojan, but where?

Harden your browser. There are various websites which will check for vulnerabilities, here are three which I use. You have to check periodically; as I said previously, new vulnerabilities are discovered all the time.

<http://www.jasons-toolbox.com/BrowserSecurity/>

<http://bcheck.scanit.be/bcheck/>

[https://testzone.secunia.com/browser\\_checker/](https://testzone.secunia.com/browser_checker/)

Harden your operating system. Check at least monthly (Microsoft releases patches on a monthly basis, with urgent ones being released as necessary).

<http://windowsupdate.microsoft.com/>

Use is common sense. Don't install software based upon advice from unknown sources. Don't install free software, without researching it carefully. Don't open email unless you know who it's from, and how and why it was sent.

Educate yourself. Know what the risks are. Stay informed. Read Usenet, and various web pages that discuss security problems. Check the logs from the other layers regularly, look for things that don't belong, and take action when necessary.

<http://www.cert.org/>

<http://isc.sans.org/index.html?type=0>

<http://www.securitywizardry.com/radar.htm>

This is just a start. Please post with additional details about your network – and computers. There may be other ways to identify the infected computer. Let's just hope that it's a single computer – and the virus didn't spread all over your LAN.

Cheers,

Chuck

Paranoia comes from experience – and is not necessarily a bad thing.