

comp.security.firewalls: Can anyone tell me how this trojan horse program got thru' my

Can anyone tell me how this trojan horse program got thru' my

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-03/2349.html>

From: TOYOTA MR2 (toyota_mr2@netvisao.pt)

Date: 03/22/02

From: "TOYOTA MR2" <toyota_mr2@netvisao.pt>

Date: Thu, 21 Mar 2002 23:20:30 -0000

Is ur system secure???

<http://www.moosoft.com/download.php>

Go there, downalod, install, update and scan ur system for trojans. If u have them, clean them.

Scan your system for viruses online for free, just go to this url and it will look and clean all your drives without cost.

http://housecall.antivirus.com/housecall/start_corp.asp

Check for spyware on your system and remove it. Spyware Ad-aware Removal available from <http://www.lavasoftusa.com/>

This worm was found on September 18th, 2001. It quickly spread around the world. Nimda is a complex virus with a mass mailing worm component which spreads itself in attachments named README.EXE. It affects Windows 95, Windows 98, Windows Me, Windows NT 4 and Windows 2000 users. Nimda is the first worm to modify existing web sites to start offering infected files for download. Also it is the first worm to use normal end user machines to scan for vulnerable web sites. This technique enables Nimda to easily reach intranet web sites located behind firewalls – some worms such as Code Red couldn't directly do. Nimda uses the Unicode exploit to infect IIS web servers. This hole can be closed with a Microsoft patch, downloadable from:

<http://www.microsoft.com/technet/security/bulletin/ms00-078.asp>

The MIME exploit used by the worm can be fixed with this patch:

<http://www.microsoft.com/technet/security/bulletin/MS01-020.asp> For more info visit the following site:

<http://www.europe.f-secure.com/v-descs/nimda.shtml>

Check your system for open ports. Very complete tests. The most reliable one I know.

<http://scan.sygatetech.com/>

To check open ports <https://grc.com/x/ne.dll?bh0bkyd2>

Can anyone tell me how this trojan horse program got thru' my

comp.security.firewalls: Can anyone tell me how this trojan horse program got thru' my

<http://grc.com/UnPnP/UnPnP.htm>

That is for information on the Microsoft Universal Plug and Play service and download of the program that allows you to disable it. That feature being enabled MIGHT TURN YOUR PC INTO A SERVER

This is to test your ports status. <https://grc.com/x/ne.dll?bh0bkyd2>

If u have port 5000 open, please go to the 1st URL, download the program, run it and disable that feature.

That feature is enabled at least on XP, ME and 98

NoShare and LetShare are terrific solutions for quickly, easily, and reversibly disabling and enabling NetBIOS resource sharing.

When you are sharing NetBios resources, you are not fully protected, for you can still be hacked. You can download these disabling and enabling NetBios resource sharing files at <http://grc.com/faq-shieldsup.htm#139>

Windows XP users DO NOT download and install No Share file!!! Disabling NetBIOS resource sharing cannot be done by using this tiny program. If you install this file on XP you are going to need the Let Share file installed to reverse this disabling. If you already rebooted your pc...it's too late and you are going to have to format and reinstall Windows XP.

Best thing to do is download both programs, just in case. I had my ISP "knocking on my door" all the time on NetBIOS, haven't seen them in 2 months. Now they try UDP on random ports, Sygate takes care of them.

Also important...I'm not sure if No Share can be used on NT and 2000. On 95, 98, 98 SE and ME it can and works great. I'm on ME, cable connection, have no complaints. NetBIOS is safe.

Test if your firewall is safe of it is leaking in terms of security

<http://grc.com/lt/leaktest.htm>

Go to this site for an Internet Security Forum

<http://grc.com/cb-faq.htm>

Check here for software that is suspected bo be SpyWare

<http://grc.com/oo/suspects.htm>

Want a good firewall that is really simple to operate and incredibly effective???

To download the Sygate firewall to either of these URL's:

<http://www.sygate.com/swat/default.htm>

or <http://www.sygate.com/swat/free/default.php>

1- Go to [http:// www.zonealarm.com](http://www.zonealarm.com)

2- Download zonealarm

3- Install it and set it to low or medium.

Tiny Firewall <http://www.tinysoftware.com/pwall.php>

If u r networking then u might wanna try this...

http://www.sygate.com/swat/products/gate_ov.htm

Share and Secure One Internet Connection for Multiple Users Integrated

Can anyone tell me how this trojan horse program got thru' my

comp.security.firewalls: Can anyone tell me how this trojan horse program got thru' my

Security

Sygate Home Network features a built-in firewall that delivers enterprise-quality security to your connected machines. As a result, would-be intruders are prevented from viewing and accessing your network. You can also add solid protection to your gateway machine by utilizing Sygate Personal Firewall, FREE to consumers.

System Requirements

Gateway Machine:

486-class processor or higher. Microsoft Windows 95, 98, ME, XP, NT 4.0 and Windows 2000 Pro/Server. 32 MB RAM or greater. One Network Interface Card -Works with Ethernet, Home PNA and Wireless Interface cards. An analog modem with a working Internet account with Microsoft Dial-Up Networking 1.2 (or higher) or America On Line 4.0 or higher or an ISDN, xDSL, DirectPC or cable modem and Internet Service Provider

-Note: Broadband Internet connections can be shared using a single Network Interface Card. Client Machines: Any TCP/IP client including Windows, BeOS, Mac, or Unix-based systems.

Finally, here is something concerning firewall setup instructions...<http://www.firewall-net.com/>
Has firewall setup instruction

Also...if u download Sygate Personal Firewall Pro 5.0, u can prevent any application from acting as a server!!!

Think u got enough information???

Ur absolutely WRONG!!! There's never too much or enough information on this subject!!!

There is but one solution for people not to be hacked...KEEP THE HELL AWAY FROM THE INTERNET!!! That's the only way!!!

One final warning to anyone reading this message...if u r running Black Ice Defender, ur firewall is leaking and ur not fully protected....go to the Leak Test I mentioned above!!!

Greetings from Portugal!!!

- *Next message:* [TOYOTA MR2: "SPYWARE"](#)
- *Previous message:* [Berk S. Daemon: "Re: is this practice|- separate puter for int access?"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)