

Blaster

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-03/1197.html>

anonymous_at_discussions.microsoft.com

Date: 03/16/04

Date: Tue, 16 Mar 2004 04:25:53 -0800

Your computer is now infected with the W32.Blaster.Worm or one of its variants. This happened because you have not been using an internet connection firewall and have apparently neglected to install the critical updates available at the Windows Update website.

If your computer is constantly attempting to shutdown or reboot, quickly go to:

Start > Run and type: CMD , and hit enter.
This opens the Command Prompt window.

Then type: shutdown -a , and hit enter.

This should halt the rebooting problem.

Then immediately turn-on Windows XP's built-in Firewall:

<http://www.microsoft.com/security/protect/>

(To enable the built-in firewall, go to:

Control Panel, double-click Networking and Internet Connections, then click Network Connections. Right-click your connection, then

Click Properties, and on the Advanced tab, click the option "Protect my computer and network..." Note: the built in firewall only monitors incoming traffic not outgoing (ie spyware, trojans, etc.. you may have on your system).)

Special note if you use AOL:

America Online installs its own connection settings that override

the ones that come with Windows XP. America Online's connection settings don't include a way to turn on Windows XP's

built-in firewall.

What You Should Know About the Blaster Worm and Its Variants

<http://www.microsoft.com/security/incident/blast.asp>

A tool is available to remove Blaster worm and Nachi worm infections from computers that are running Windows 2000 or Windows XP
<http://support.microsoft.com/?kbid=833330>

A security issue has been identified that could allow an attacker to remotely compromise a computer running Microsoft Windows and gain complete control over it. You can help protect your computer by installing this update from Microsoft.
<http://www.microsoft.com/downloads/details.aspx?FamilyId=2354406C-C5B6-44AC-9532-3DE40F69C074&displaylang=en>

Above courtesy of MVP Carey

***Install a good firewall. ZoneAlarm is a free one you can install.
Install a good anti-virus program making sure you keep it's definitions up to date! ***

Microsoft Security Bulletin MS03-39
<http://support.microsoft.com/?kbid=824146>

What You Should Know About the Blaster Worm
<http://www.microsoft.com/security/incident/blast.asp>

Protect Your PC
<http://www.microsoft.com/security/protect/default.asp>

W32.Blaster.Worm a.k.a. W32/Lovesan.Worm
<http://www.symantec.com/avcenter/venc/data/w32.blaster.worm.html>

W32.Blaster.Worm Removal Tool
<http://www.symantec.com/avcenter/venc/data/w32.blaster.worm.removal.tool.html>

W32.Welchia.Worm a.k.a. W32/Nachi.Worm
<http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.html>

W32.Welchia.Worm Removal Tool
<http://www.symantec.com/avcenter/venc/data/w32.welchia.worm>

.removal.tool.html

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

>I think I have some variant of the blaster virus. I'm running Windows XP

>Home.

>I always said there was no virus that I couldn't remove from a computer,

>because if I had to I would format the hard drive. I think I met my

>Waterloo.

>Coming from a cold boot I got about 30 seconds before a window pops up that

>says Remote Procedure Call is closing down my computer. And then it counts

>down from 60 seconds and closes down. It will not allow me to go into

>administrative services and change the RPC. I double click on it and

>nothing happens. I have tried everything. Booted in safe mode, booted from

>a system disk, booted to my C: prompt. Whoever authored this virus covered

>all the bases.

>All I want to do at this point is format the hard drive.

Any

>Suggestions??

>

>

>.

>