

Computer Corner

By Jim Jeup
03/11

Blaster Worm Facts

- Between August and September 2003 – North America reported more than 46,000 infected computers
- Only NT/2000/XP and Server 2003 are affected due to a “hole” in Windows “Remote Procedure Call”
- In July, 2003 (a month before the attack) Microsoft released the security patch, which was available via Windows Update, or download from Microsoft’s web site
- Go to Windows Update (<http://v4.windowsupdate.microsoft.com/en/default.asp>) and complete “Critical Updates” to protect your system from this virus. Do it regularly!
- Norton (<http://www.norton.com>), McAfee (<http://www.mcafee.com>) and Trend Micro (<http://www.trendmicro.com>) virus software makers distribute a free removal tool for Blaster on their web sites.
- Companies were “Blasted” because most run patches through a lab environment to ensure specialty software works with each patch. Most company labs did not complete testing in time to protect company computers from this virus attack.

VIRUS PROTECTION & MAINTENANCE IS FOR EVERYONE!

Everyone should have a virus protection & system maintenance schedule. Whether you complete the updates yourself, or have a professional do it for you, it needs to be done. Virus software alone is not enough to keep your computer safe. All protection plans should include the following areas (minimum):

1. Regular Virus Scans
2. Regular Virus Pattern Updates
3. Critical Patch Updates
4. System Settings Checks
5. Delete Temporary Files & PC tune-up

If you have a professional who provides your virus protection and maintenance, be certain they include **Emergency Service** to remove a virus if you contract one under their protection & maintenance plan.

Rid Your Computer of Most Pop-up Ads

By default, Microsoft ships Windows XP with Windows Messenger turned on (A bad idea). Messenger is used by System Administrators to post messages on networked systems quickly. Most home users do not use a “Sys Admin”, so this is not needed. The Blaster worm exploited the vulnerability of this process to shut down computers.

Messenger can be turned off easily with a free program from Gibson Research Corp. (<http://grc.com>). The program is called “Shoot The Messenger”, and will take care of the vulnerability, even if you have not updated Windows “Critical Updates”. Find the program at <http://grc.com/stm/shootthemessenger.htm>

Pop-up ads and spyware come from internet sites you visit during your normal internet usage. Lavasoft (<http://www.lavasoftusa.com>) offers a free program called Ad-aware. Ad-aware searches for spyware and data mining programs on your computer, and allows you to delete them. You will notice a drastic reduction in the number of pop-up ads you see after running this application (<http://www.lavasoftusa.com/support/download>)

NOTE: Since the writing of this article, Microsoft is considering a shut down of these open ports in future releases of their operating system.