

## Re: can sasser& Blaster get to the computer?

**Source:**

[http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help\\_and\\_support/2004-07/0241.html](http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2004-07/0241.html)

---

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

**Date:** 07/01/04

Date: 30 Jun 2004 19:47:20 -0500

On Thu, 1 Jul 2004 02:36:40 +0300, "Kenny S" <\*email\_address\_deleted\*> wrote:

>I have updated desktop computer that is connected to the internet via ADSL  
>firewalled with the XP firewall and it sends through ICS the internet to a  
>laptop. Because of a hardware conflict I cannot update the laptop.  
>  
>My Question is this:  
>  
>Will the desktop computer with the firewall also protect the laptop even if  
>I disable the firewall on the laptop?

If I understand you correctly, you have the desktop connected to the ADSL modem, and the laptop connects to the desktop? And the desktop computer is running the XP firewall (ICF), and Internet Connection Sharing (ICS)?

In this case, the laptop IS protected from hostile net traffic (and specifically Blaster and Sasser et al) coming from the internet, by the firewall on the desktop.

However, please use additional protection on BOTH the desktop and laptop computers. Use a good layered defense. Each layer is necessary because no layer produces complete protection.

The first layer is a NAT router / hardware firewall. ICF / ICS provides this function to a limited extent. But replacing both ICF and ICS with a NAT router would be a good decision, and would cost less than a couple months DSL service.

The second layer is a software firewall, or a port monitor like Port Explorer (free) from <<http://www.diamondcs.com.au/portexplorer/index.php?page=home>>. See various discussions in comp.security.firewall for good advice on choosing a firewall.

The third layer is good software. This layer has multiple components.

AntiVirus protection. Realtime, plus a regularly scheduled virus scan. Regularly updated.

microsoft.public.windowsxp.help\_and\_support: Re: can sasser& Blaster get to the computer?

Adware / spyware protection. Realtime, plus a regularly run adware / spyware scan. Regularly updated.

Complete instructions, using Spybot S&D and HijackThis (both free) are here: <<http://forums.spywareinfo.com/index.php?showtopic=227>>.

Harden your browser. There are various websites which will check for vulnerabilities, here are three which I use.

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

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

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

Block Internet Explorer ActiveX scripting from hostile websites (Restricted Zone).

<<http://netfiles.uiuc.edu/ehowes/www/main.htm>> (IE-SpyAd)

Set up blocking of known dangerous scripts from installing.

<<http://www.javacoolsoftware.com/spywareblaster.html>>

Block known spyware from installing.

<<http://www.wilderssecurity.net/spywareguard.html>>

Harden your operating system. Check at least monthly for security updates.

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

Block possibly dangerous websites with a Hosts file. Three Hosts file sources I use:

[http://www.accs-net.com/hosts/get\\_hosts.html](http://www.accs-net.com/hosts/get_hosts.html)

<http://www.mvps.org/winhelp2002/hosts.htm>

(The third is included, and updated, with Spybot (see above)).

Maintain your Hosts file (merge / eliminate duplicate entries) with:

eDexter <[http://www.accs-net.com/hosts/get\\_hosts.html](http://www.accs-net.com/hosts/get_hosts.html)>

Hostess <<http://accs-net.com/hostess/>>

Secure your operating system, and applications. Don't use, or leave activated, any accounts with names or passwords with trivial (guessable) values. Don't use an account with administrative authority, except when you're intentionally doing administrative tasks.

The fourth layer is common sense. Yours. 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.

The fifth layer is education. 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.

Cheers,  
Chuck

Re: can sasser& Blaster get to the computer?

microsoft.public.windowsxp.help\_and\_support: Re: can sasser& Blaster get to the computer?

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