The Denver Post

How secure is your computer?

"Honey pot" experiment shows unprotected Windows SP 1 at risk

By Ross Wehner
Denver Post Staff Writer

Monday, February 28, 2005 -

A Windows computer without the latest security patches is in big trouble.

That's the conclusion from a "honey pot" experiment conducted by StillSecure, a Louisville network security firm.

StillSecure attached six computers - loaded with different versions of the Windows, Linux and Apple's Macintosh operating systems - earlier this month to the Internet without anti-virus software.

The results show the Internet is a very rough place.

Over the course of a week, the machines were scanned a total of 46,255 times by computers around the world that crawl the Web looking for vulnerabilities in operating systems.

Once the vulnerabilities were identified, the remote computers launched 4,892 direct attacks with a staggering variety of worms, Trojan Horses, viruses, spyware and other forms of malware.

The test examined only what happens when computers are turned on and connected to the Internet. The test didn't evaluate additional dangers that computer users face when they use e-mail, surf the Web, click on Internet links or use file-sharing programs.

The good news is that none of the up-to-date, patched operating systems succumbed to a single attack.

The Windows Service Pack 2, or SP 2, system is the most up-to-date Windows operating system. It received 16 direct attacks.

The Macintosh system received three attacks. Two of the Linux systems received eight attacks each, though Red Hat's version of Linux received no attacks at all.

But in the end, none of the attacks were successful.

The Linux and Macintosh sytems were installed out of the box without any additional security patches. Windows SP 2 automatically downloads the latest security patches from the Microsoft website.

Windows Service Pack 1, or SP 1, however, was another story. It's an older version of Windows that was sold in computer stores until a few months ago.

SP 1 was attacked 4,857 times. It was infested within 18 minutes by the Blaster and Sasser worms. Within an hour it became a "bot," or a machine controlled by a remote computer, and began attacking other Windows computers.

Microsoft responded that the tests prove that any operating system is vulnerable when not patched.

"The results don't surprise me at all," said David Brandt, principal technology architect at Microsoft in Denver.

Microsoft stopped shipping SP 1 in August and replaced it with the more secure Windows SP 2. Most computers with SP 1 had been sold from stores by Christmas, said Microsoft spokesman Sean Sundwall.

SP 2 comes with a firewall and automatic security updates, said Sundwall. These features had to be manually turned on in SP 1, which meant that some users missed out on computer patches.

Many computers around the world are still running Windows SP 1, though exact numbers are hard to come by. Gartner research director Michael Silver estimates that by the end of 2005, half of the world's desktops used in businesses will still be using SP 1.

"But most companies are pretty good about keeping their PCs patched, and most have corporate firewalls," said Silver.

Large companies are switching to SP 2 slowly because they have to make adjustments to thousands of different software programs first.

The honey pot test is a good indication that many small-business and home computers are still using older versions of Windows, according to StillSecure chief technology officer Mitchell Ashley.

"Why are we getting hit by Blaster?" asked Ashley. "Because there are infected machines out there. Why are they infected? Because they don't have the updated patch."

Microsoft is concerned about security issues surrounding Windows and Internet Explorer, and the resultant surge of Linux, which can be downloaded for free from the Internet. Most companies, however, chose to pay a Linux vendor in order to receive security patches.

Experts also consider Linux less prone to viruses.

"(Security) is a huge pain point for Microsoft," said Silver. "Microsoft takes the threat of Linux very seriously."

Over the last nine months, Microsoft has gone on the offensive with a "Get the Facts" campaign that argues that Windows is cheaper and more secure than Linux.

Microsoft's leadership position means that more viruses are written for Windows, said Silver, who estimates that 96 percent of all desktops and laptops worldwide used Windows at the end of 2004. Macintosh has 2.5 percent of the market, while Linux is at 1.3 percent, Silver said.

"There are going to be security holes in just about any operating system," said Silver.

Silver predicts that Linux will climb to 3 percent of the market by 2008.

As of this month, 25 million people around the world have downloaded a free Web browser, Mozilla Firefox, which a variety of security experts have trumpeted over Microsoft's Internet Explorer.

Microsoft is racing to roll out its new Longhorn operating system in 2006.

But for the moment, it's sticking with Windows, for which it rolled out a new patch Tuesday.

"SP 1 is not a current operating system," said Sundwall. "It doesn't surprise me that it only took 18 minutes to get infected."

Staff writer Ross Wehner can be reached at 303-820-1503 or rwehner@denverpost.com .

Operation Honey Pot

StillSecure, a Louisville-based network security firm, connected six computers - with six operating systems - to the Internet for a week without any virus protection. The results: 4,892 direct attacks by viruses, worms and other types of malicious code, and 46,255 scans by remote computers looking for weaknesses.

Here's what happened:

Windows XP Service Pack 1

Attacks: 4,857

Results: Attacked successfully within 18 minutes by the Blaster and Sasser worms. Within an hour, the computer was taken over and began attacking other Windows machines.

Windows XP Service Pack 2

Attacks: 16

Results: Survived all attacks

Apple Mac OS X Jaguar

Attacks: 3

Results: Survived all attacks

Linux, Suse Professional 9.2

Attacks: 8

Results: Survived all attacks

Linux, Fedora Core 3

Attacks: 8

Results: Survived all attacks

Linux Red Hat 9

Attacks: 0

Source: StillSecure

Protecting your PC

Computers are vulnerable to viruses unless three basic protections are in place: a patched operating system, anti-virus software and a firewall for blocking viruses.

1. Patched operating system. Windows users should visit www.windowsupdate.com , a Microsoft website that will scan your computer and suggest updates. Linux vendors and Apple also offer patches.

2. Anti-virus software. Windows SP 2 automatically alerts users if they don't have a working anti-virus software program.

Experts say spyware programs are also necessary for Windows users. Microsoft is offering a free beta version of its spyware program at www.microsoft.com/athome , and Webroot is offering its spyware program free to Colorado residents through April 15 at www.webroot.com Free spyware programs are available at www.download.com

3. Firewall. Windows SP 2 comes with a firewall, as does Symantec's Norton Internet Security 2005 and other security software packages. Zone Alarm firewall can be downloaded free at www.zonelabs.com

- By Ross Wehner

Viruses vs. Spyware

There are many types of malware, or malicious software. Experts often divide them into two groups:

Viruses

Viruses are a form of computer vandalism that often have no other purpose than to prove the prowess of the virus' author. Viruses are classified by how they spread:

Trojan Horses hide themselves within an apparently innocuous computer program.

Worms take over a machine in order to attack, and spread to, other computers.

Spyware

Spyware, unlike a virus, has a financial driver. The most lethal forms help identity thieves gather information from computer users without their consent. Spyware gets on computers in the same way

viruses do. Apart from making a computer run slowly, it rarely announces its presence.

Some forms of spyware:

Key loggers record keystrokes and then transmit credit card numbers and other sensitive information to identity thieves.

Cookies are used by online companies to track user preferences.

Adware causes annoying pop-up ads but often harvests information like spyware.

The best way to know if your computer has spyware is to run an anti-spyware program.

- By Ross Wehner