washingtonpost.com

Microsoft Windows: Insecure by Design

By Rob Pegoraro
The Washington Post
Sunday, August 24, 2003; Page F07

Between the Blaster worm and the Sobig virus, it's been a long two weeks for Windows users. But nobody with a Mac or a Linux PC has had to lose a moment of sleep over these outbreaks -- just like in earlier "malware" epidemics.

This is not a coincidence.

The usual theory has been that Windows gets all the attacks because almost everybody uses it. But millions of people do use Mac OS X and Linux, a sufficiently big market for plenty of legitimate software developers -- so why do the authors of viruses and worms rarely take aim at either system?

Even if that changed, Windows would still be an easier target. In its default setup, Windows XP on the Internet amounts to a car parked in a bad part of town, with the doors unlocked, the key in the ignition and a Post-It note on the dashboard saying, "Please don't steal this."

Not opening strange e-mail attachments helps to keep Windows secure (not to mention it's plain common sense), but it isn't enough.

The vulnerabilities built in: Security starts with closing doors that don't need to be open. On a PC, these doors are called "ports" -- channels to the Internet reserved for specific tasks, such as publishing a Web page.

These ports are what network worms like Blaster crawl in through, exploiting bugs in an operating system to implant themselves. (Viruses can't move on their own and need other mechanisms, such as e-mail or floppy disks, to spread.) It's canonical among security experts that unneeded ports should be closed.

Windows XP Home Edition, however, ships with five ports open, behind which run "services" that serve no purpose except on a computer network.

"Messenger Service," for instance, is designed to listen for alerts sent out by a network's owner, but on a home computer all it does is receive ads broadcast by spammers. The "Remote Procedure Call" feature exploited by Blaster is, to quote a Microsoft advisory, "not intended to be used in hostile environments such as the Internet."

Jeff Jones, Microsoft's senior director for "trustworthy computing," said the company was heeding user requests when XP was designed: "What customers were demanding was network compatibility, application compatibility."

But they weren't asking for easily cracked PCs either. Now, Jones said, Microsoft believes it's better to leave ports shut until users open the ones they need. But any change to this dangerous default configuration will only come in some future update.

In comparison, Mac OS X ships with zero ports open to the Internet.

The firewall that's down: A firewall provides further defense against worms, rejecting dangerous Internet traffic.

Windows XP includes basic firewall software (it doesn't monitor outgoing connections), but it's inactive unless you use its "wizard" software to set up a broadband connection. Turning it on is a five-step task in Microsoft's directions (www.microsoft.com/protect) that must be repeated for every Internet connection on a PC.

Mac OS X's firewall isn't enabled by default either, but it's much simpler to enable. Red Hat Linux is better yet: Its firewall is on from the start.

The patches that aren't downloaded: Windows is better than most operating systems at easing the drudgery of staying on top of patches and bug fixes, since it can automatically download them. A PC kept current with Microsoft's security updates would have survived this week unscathed.

But hundreds of thousands, if not millions, of Windows systems still got Blasted, even though the patch to stop this worm was released weeks ago.

Part of this is users' fault. "Critical updates" are called that for a reason, and it's foolish to ignore them. (The same goes for not installing and updating anti-virus software.)

The chance of a patch wrecking Windows is dwarfed by the odds that an unpatched PC will get hit. And for those saying they don't trust Microsoft to fix their systems, I have one question: If you don't trust this company, why did you give it your money?

Microsoft, however, must share blame, too. Windows XP's pop-up invitations to use Windows Update must compete for attention with all of XP's other, less important nags -- get a Passport account, take a tour of XP, hide unused desktop icons, blah, blah, blah.

Microsoft's critical updates also are absent from retail copies of Windows XP, forcing buyers into lengthy Windows Update sessions to get the fixes since last year's Service Pack 1 upgrade. At least the version of XP provided to PC manufacturers is refreshed once a quarter or so -- and Microsoft says it's working to shorten this lag.

The lack of any limit to damage: Windows XP, by default, provides unrestricted, "administrator" access to a computer. This sounds like a good thing but is not, because any program, worms and viruses included, *also* has unrestricted access.

Yet administrator mode is the only realistic choice: XP Home's "limited account," the only other option, doesn't even let you adjust a PC's clock.

Mac OS X and Linux get this right: Users get broad rights, but critical system tasks require entering a password. If, for instance, a virus wants to install a "backdoor" for further intrusions, you'll have to authorize it. This fail-safe isn't immune to user gullibility and still allows the total loss or theft of your data, but it beats Windows' anything-goes approach.

Because Microsoft blew off security concerns for so long, millions of PCs remain unpatched, ready for the next Windows-transmitted disease. Microsoft needs to do more than order up another round of "Protect Your PC" ads.

Here's a modest proposal: Microsoft should use some of its $49 billion hoard to mail an update CD to anybody who wants one. At $3 a pop (a liberal estimate), it could ship a disc to every human being on Earth -- and still have $30 billion in the bank.

Living with technology, or trying to? E-mail Rob Pegoraro at rob@twp.com.

© 2003 The Washington Post Company