

Note to new Linux users: No antivirus needed

Monday, 26 February 2007 08:00 Linux.com

SOURCE: <http://linux.com/news/software/applications/8261-note-to-new-linux-users-no-antivirus-needed>

By Joe Barr

Savvy Windows users have to watch their virus checkers as closely as the head nurse in the ICU keeps an eye on patient monitors. Often, the buzz in the Windows security world is about which protection-for-profit firm was the first to discover and offer protection for the *malware du jour* -- or should I say *malware de l'heure*? The only thing better than having backed the winning Super Bowl team come Monday morning at the office coffeepot is having the virus checker you use be the one winning the malware sweepstakes that weekend.

If a rogue program finds a crack in your Windows armor, paying \$200 per infection to have your machine scrubbed and sanitized by the local goon^H^H^H geek squad not only helps to reinforce the notion that you have to have malware protection, but that it has to be the right protection, too. The malware firms are aware of this, and all of their advertising plays upon the insecurity fears of Windows users and the paranoia that results. Chronic exposure and vulnerability to malware has conditioned Windows users to accept this security tax.

It's no wonder, then, that when Windows users are finally able to break their chains and experience freedom on a Linux desktop, they stare at me in disbelief when I tell them to lay that burden down. They are reluctant to stop totin' that load. They have come to expect to pay a toll for a modicum of security.

I try to explain that permissions on Linux make such tribute unnecessary. Without quibbling over the definitions of viruses and trojans, I tell them that neither can execute on your machine unless you explicitly give them permission to do so.

Permissions on Linux are universal. They cover three things you can do with files: read, write, and execute. Not only that, they come in three levels: for the root user, for the individual user who is signed in, and for the rest of the world. Typically, software that can impact the system as a whole requires root privileges to run.

Microsoft designed Windows to enable outsiders to execute software on your system. The company justifies that design by saying it enriches the user experience if a Web site can do "cool" things on your desktop. It should be clear by now that the only people being enriched by that design decision are those who make a buck providing additional security or repairing the damage to systems caused by it.

Malware in Windows Land is usually spread by email clients, browser bits, or IM clients, which graciously accept the poisoned fruit from others, then neatly deposit it on their

masters' systems, where malware authors know it will likely be executed and do their bidding -- without ever asking permission.

Some malware programs require that you open an attachment. Others don't even require that user error. By hook or by crook, malware on Windows often gets executed, infecting the local system first, then spreading itself to others. What a terrible neighborhood. I'm glad I don't live there.

On Linux, there is built-in protection against such craft. Newly deposited files from your email client or Web browser are not given execute privileges. Cleverly renaming executable files as something else doesn't matter, because Linux and its applications don't depend on file extensions to identify the properties of a file, so they won't mistakenly execute malware as they interact with it.

Whether newcomers grok permissions or not, I try to explain the bottom line to them: that because they have chosen Linux, they are now free of having to pay either a security tax up front to protect themselves from malware, or one after the fact to have their systems sterilized after having been infected.

So Linux is bulletproof? No. Bulletproof is one of the last stages of drunkenness, not a state of security. Linux users, like users on every operating system, must always be aware of security issues. They must act intelligently to keep their systems safe and secure. They should not run programs with root privileges when they are not required, and they should apply security patches regularly.

Misleading claims and false advertising by virus protection rackets to the contrary, you simply don't need antivirus products to keep your Linux box free of malware.
