INFECTIONS

Dear Linux Magazine Reader,

Joe Casad, Editor in Chief

The prospect of devoting an issue to viruses in Linux launched a lively conversation in our 5000-mile-wide virtual office. We in the media receive a lot of press releases, and some of those press releases are from vendors with anti-virus products. We in the Linux media are supposed to like it when vendors take an interest in Linux. But the problem when it comes to anti-virus vendors is that every product is based on a need, and, in order to establish the need for their Linux virus protection products, the vendors are working overtime to sprinkle their path with ominous warnings that a Linux virus attack is on the way.

Many of the old Linux hands have been equally vociferous in their skepticism. “How is a virus going to get into Linux unless you’re checking your mail as root?” they say, and they are mostly correct, of course, but still the sound of someone saying “don’t worry” always leaves me a little worried.

It is certainly true that, in Linux, a virus can’t simply waltz in through an open door like it can in some versions of Windows. But the nastiest viruses work subtly, exploiting flaws in the system, and if Linux didn’t have any security flaws, we wouldn’t be bringing you the “Insecurity News” every month.

When I poke around the security websites for the major distros, I’m continually amazed at the diabolical things one could do with an innocent little desktop application like Zip. Of course, this is all theory. Just because an exploit is posted at a vendor website or cataloged by the Common Vulnerabilities and Exposures project (cve.mitre.org), it does not mean an attacker has actually used that exploit. The problems are often discovered by security experts and community members who are rooting out potential vulnerabilities before the attackers can find them first.

A computer virus obeys some of the laws followed by a natural virus, and one of those laws is that, in order for a virus to spread, the rate of infection must exceed the rate of eradication. Most of us are aware that the rate of infection is lower in Linux due to its natural defenses. The other side of this may be that the rate of eradication may also be higher in Linux because so many more eyes are on the code.

If you want to learn more about how viruses work in Linux, check out our lead cover story by Tomasz Kojm, founder of the ClamAV Open Source anti-virus project, who also reveals his six rules for avoiding infection.

We’re excited to unveil a pair of new features this month. We welcome author, hacker, world traveler, and noted Linux chronicler Jon Masters, who starts a new series this month on the affairs of the Linux community. And, we were so impressed with the glib erudition of Klaus Knopper, creator of the popular Knoppix live distro, that we invited him back to answer questions from readers on configuring Linux. Check out our new "Ask Klaus!" question and answer column.

And speaking of questions, how about a quiz, now that we are all feeling good about Linux security? What organization provides the funding for the Common Vulnerabilities and Exposures project, the central source cited in many of the security patches and errata of the Linux distros? You’re correct if you guessed the U.S. Department of Homeland Security.

Now doesn’t that make you feel secure?