

California Computer Care

News,
Views,
Tips and
Cool Techniques
for CCC Members

July 2002
Vol. V, No. 7

We
speak
Geek,
so you
don't
have to.

The Klez Worm

What an annoyance to the innocent!

There's a nasty, new computer virus going around called the Klez worm. Normally I wouldn't bother you with a virus that only attacks *Windows* computers (as usual, we Mac users are immune from infection and damage), but this one plays a cruel trick.

The new trend.

The rotten, little creeps that write computer viruses, not content to just damage other people's computers, have exploited a huge flaw in *Windows* computers to assure that as many people as possible are infected. They have found a way to force the victim's computer to send a copy of the virus to everyone in the victim's email address book.

The Microsoft Windows flaw.

The reason that virus writers can do this is directly attributable to Microsoft's policies. Because MS (with rare exceptions) forces all computer manufacturers (except Apple) to install *Microsoft Windows* on every computer sold, the purchaser has no choice of operating system. Also, MS forces manufacturers to include Microsoft's email applications with every computer (and makes sure that non-Microsoft email programs perform poorly). So, the buyer accepts and uses what they are given. This results in the computer version of a million acres of the same variety of wheat. That lack of diversity assures that if a disease gets into the wheat field, it kills every stalk. A virus writer is guaranteed by Microsoft's requirements that 98% of potential victims are all using the same software! Easy target.

An aside. . .

We Mac users all use the same operating system (Mac OS 7-9), but we don't have this vulnerability. For one, we use many different email applications: *Outlook Express*, *Netscape Messenger*, *Eudora*, *First Class* and others. We have much more diversity than

Windows users, making the propagation of viruses so difficult that those with the needed skills are too busy doing useful (or at the very least, profitable) things to bother.

Back to Klez.

The Klez worm brings an even newer wrinkle to the field of email virus propagation. Previous email viruses, when they mailed themselves to the poor folks in an infected address book, used the victim's return address on the email. Klez goes one better! Klez selects a name or names at random from the infected address book and uses that random name as return address. So, if you, as a Mac user, are part of a *Windows* user's address book and that person gets the Klez worm, you stand a good chance of having your name used as return address on several hundred infected emails. The victim receiving these emails will trace their infection back to you! You, of course, are absolutely innocent. You weren't even involved. Some of you have already received angry email from infected *Windows* users and, probably, many more of you will, as well. It's sort of like guilt by association.

What can we Mac users do?

Unfortunately, not much. Being aware of the reason for the irate emails, at least lets you know that you are not infected and have not done anyone harm.

It would be a good idea to encourage your *Windows* using friends to make sure that their anti-virus software is up to date and aware of the Klez worm (and its many sub-varieties). Anti-virus updates are free.

While Mac viruses are very, very rare, they do exist. So, take some care when trading files and disks with other users. Anti-virus software can be useful if you trade lots of files, so you may want to look at *Symantec Norton AntiVirus for Mac* or *Virex*.

Mac Virus Information

Yes, there are Mac viruses, but most of you will never, ever see one. In 17 years of Mac use I've only dealt with three infected machines. Meanwhile, almost every *Windows* user will be victimized dozens of times.

Mac viruses do not spread through email.

Most *Microsoft Windows* viruses propagate through the email system (see page 1). The rare Mac virus propagates through shared disks (primarily floppy disks). One result of Apple dropping built-in floppy disk support back in 1998, has been the near extinction of most species of Mac virus. The only Mac viruses still around aren't Mac viruses at all.

Microsoft, again.

Where do most Macintosh viruses come from? *Windows* PC users, of course. Despite *Windows* users' claims of greater software availability, they all use the same basic applications! We use several, different word processors, *Windows* users use only one: *Microsoft Word*. In the past, *Microsoft Word for Mac* (it was originally a Mac program and went to *Windows* about six years later) was very different than *Microsoft Word for Windows*. As a result, the hundreds of macro viruses that plagued *MS Word for Windows*, were incapable of harming *MS Word for Mac*. In 1996, Microsoft introduced version 6 of *MS Word for Mac*. With version 6, Microsoft made files created in *MS Word for*

Mac identical to files created by *MS Word for Windows*. The result? *Word* macro viruses spread through the *Mac Word* community like wildfire. The same thing happened to folks who use the *Microsoft Excel* spreadsheet application.

Macro viruses.

Microsoft Word and *Excel* both offer macro functions* that are a nice convenience, but not a necessity to these applications. *Microsoft Word* and *Excel* users should suspect macro viruses in every *Microsoft Word* and *Excel* document. Fortunately, Microsoft has changed *Word* and *Excel* to assure that you are warned about the presence of macros in a document; you then have the choice to allow them to run. If macros do not run, they cannot harm you. Of course, the surest way to avoid macro viruses is to not use any Microsoft products at all.

Anti-virus software.

For the greatest security from virus attacks, anti-virus software is needed. I recommend *Symantec Norton Antivirus for Mac* and *Vir-ex*. Both of these products work well provided you take advantage of their free virus updates. Both cost about \$65.00.

* Macros allow programming to be inserted into data files and since viruses can only be inserted into programming and not into data, this allows malicious virus writers to insert viruses into innocent data.

July Tip—

Inside almost every computer, there is a small battery. In a Mac this is known as the PRAM battery or the clock battery. As the second name suggests, the function of the battery is to run your Mac's clock (it also preserves your preferences such as printer choice). The battery does its job when your Mac has no other source of power, like during an electrical outage or if your Mac is unplugged.

The PRAM battery will last about 5 years of normal use. However, if you unplug your Mac or turn off your surge protector, you may shorten the life of the battery to a year or less. Replacing the battery will cost about \$35.00, so you may want to leave that surge protector turned on.

California Computer Care

P.O. Box 9445

Santa Rosa, CA 95405

(800) 540-8989

help@calcompcare.com

Like an
auto club
for your
computer.