

# California Computer Care

News,  
Views,  
Tips and  
Cool Techniques  
for CCC Members

April 2004  
Vol. VII, No. 4

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

# They're heeeere!

Well, sorta...

In the horror movie *Poltergeist*, the evil spirits entered the family's home through the television set. For us, the evil spirits we all fear, try to get us through our Macs. Of course, I'm referring to computer viruses, worms and trojan horses.

In last month's *CCC News* (March, 2004), I reprinted a story about computer hackers at war with each other using all kinds of nasty, programming code and how we Mac users are immune to all that nonsense. Well, if you listen to the Windows computer pundits, we have lost our immunity.

Except we haven't. Major news stories in the computer press and even the general press, have been full of doom, gloom and an undisguised glee that Macs are now vulnerable just like Windows PCs.

Except we aren't. So, if you've seen one of these stories or heard a rumor from a friend, here is the truth of the matter.

But, first, some definitions.

**Malware:** Software with malicious intent.

**Virus:** Malware that self-duplicates and damages other software and/or hardware.

**Worm:** Malware that self-propagates over networks, crawling from computer to computer and worming its way in.

**Trojan Horse:** Malware that disguises itself as something desirable and useful to fool the user into launching it.

There are experts in the computer industry, who work, as their specialty, in the security field. With all of the emphasis on hackers, crackers, viruses, spyware and the like, computer security problems are very important to the industry. One technique that security experts use, to study security flaws, is the creation of test malware. When a security expert discovers a new way to attack computers, they do what all scientists do;



they publish their results so that other security experts can know about the problem and begin to devise fixes before the technique is discovered by the bad guys. When they create a new virus, worm or trojan horse, they name it a *Concept Virus*.

The MP3Concept (MP3Virus.Gen) flap.

In March of this year, for the first time ever, a "virus" that, theoretically, *could* affect Mac OS X was created. Technically-speaking, the MP3 Concept (MP3Virus.Gen) program is really a trojan horse. A security expert created it and published his findings, along with a harmless sample of the code, to a security discussion newsgroup to get his peers' reaction and criticism of its validity and danger.

This fact went unnoticed by everyone outside of the security industry.

Now, consider anti-virus software for Macs. As there are no viruses, worms or trojan horses that affect Mac OS X, the companies that make anti-virus software are having a great deal of trouble selling a product that no one needs. An enterprising, French anti-virus software publisher, *Intego*, found out about MP3Concept and issued a paranoia-

inducing press release “warning” the world of the first Mac OS X “virus.” Of course, their product, *VirusBarrierX*, can find and destroy the new threat. A neat bit of FUD\*.

Of course, the computer news services could speak of little else for several days. They were all aglow with the bad news. The Windows oriented news services were positively overjoyed! Rumors began to fly that Macs would at last be overrun with viruses just like *real* computers are.

Except we aren't and won't be. MP3Concept is not going to hurt anyone. After four years of study, MP3Concept is the best that experts could do. But, comparing it to a real viral threat shows that it is no threat at all.

Mac OS X is designed to repel viruses. You may have noticed that whenever you attempt to install software that can affect your Mac's operating system, a window pops up and demands that you authorize the installation with your user name and secret (I hope!) password. A virus would have to get your active permission to attack you.

Email viruses like the Windows *Blaster* virus, can't affect Macs because email attach-

---

\* FUD is an acronym of Fear, Uncertainty and Doubt. FUD is used to persuade users to behave in a way that benefits the FUD spreader. It was originally coined to describe Microsoft's business tactics.

ments are not allowed to install and run automatically. Again, you would have to approve the attack. Also, unlike Windows, Mac OS X does not have remote control software built into almost all functions just waiting to be used against you by a malicious hacker.

Since virus and worm attacks are stopped by Mac OS X, that leaves only trojan horses as a way to attack. ConceptMP3 is such a trojan horse. The victim, copies a file that looks like an MP3 music file and double-clicks to play it. But, unnoticed by the victim, hidden in the MP3 file (which plays normally) could be a malware application waiting to strike.

The actual ConceptMP3 trojan horse has nothing inside, but the security expert has demonstrated that it could. That sounds pretty bad, but even though experts have used all of their skills on ConceptMP3, they haven't been able to figure out a way to propagate it. The very act of emailing ConceptMP3 destroys the malware inside. It could be sent on removable disks like ZIPs or CDs (like 80's era Mac viruses were), but would then require a user name and password just as a regular virus or worm would.

Lastly, discovering ConceptMP3's true nature is too easy. A real MP3 file is all data and will show as such if *Get Info* is done on it. A ConceptMP3 file would show up in *Get*

*Info* as an application; that's a dead giveaway.

So, if you hear about a nasty Mac OS X virus, pay no attention. Just remember that some very competent people are out there trying hard to figure out a way to hurt us and failing at every turn! That's very nice to know.

### *April Tip—*

*Panther* (Mac OS X 10.3) has several cute kitty tricks for you. Here are two.

1) **Faxing.** *Panther* has fax functions built in, so you don't need third party software like *FAXstf* or *Page Sender*. Set up the fax functions in the *Print & Fax System Preference*. To fax a document, just click the *Fax* button in any *Print* dialog box.

2) **TextEdit**, the funny little word processor that can read to you, can now also open *Microsoft Word* documents. Pretty amazing for an application most folks ignore.

California Computer Care

P.O. Box 9445

Santa Rosa, CA 95405

(800) 540-8989

help@calcompcare.com

Like an  
auto club  
for your  
computer.