

California Computer Care

News,
Views,
Tips and
Cool Techniques
for CCC Members

November 2007
Vol. X, No. 11

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

Eeeeeek!!!

Hallowe'en came late for us Mac users this year. In early November, the first, real, honest to gosh, Mac monster was found in the wild. Our Microsoft Windows using friends couldn't be happier!

For the past seven years, since the introduction of Mac OS X, we have had no nasty software to fear. No viruses, worms, trojan horses or spyware of any kind. But, the inevitable has finally happened. Oh, pooh!

Not all that scary. The reason that we have had this seven year immunity is because Mac OS X is maniacal about security. The bad guys have not been able to crack that security and gain access to our Macs. The funny thing about this newly discovered monster is that they still haven't found a way. So, they have had to be very clever and get you to hurt yourself!

The monster is a trojan horse. This trojan horse doesn't have Greeks inside. Instead it contains a malicious application that seeks to commandeer your Mac and force it to do the bad guy's bidding. But, on the surface, the trojan horse looks like an innocuous video player add-on.

The trojan horse works like this... As of now, this monster lurks on pornographic web sites (it could appear elsewhere, but so far hasn't). It waits for a Mac user to visit the porn site and click to watch a dirty movie. Upon clicking, a message pops up advising the victim that they need to download and install a video add-on (technically a video codec) in order to watch the movie. If they click and agree to the download, the file will be sent to their Mac. When Mac OS X notices that this is a software program, it puts up a warning and asks if the user really wants to do this. If the user says yes, the download completes. The user then has to find the downloaded file and double-click



on it. When they do, a window opens and requests the user's administrative password. If the user provides the administrative password, the trojan horse installs itself. The damage is now done. But, the user doesn't know that anything bad happened.

Next, the user attempts again to watch the dirty movie, and again, it doesn't play. Most users would now throw up their hands, give up and forget all about the incident.

However, behind the scenes, the trojan horse is beginning to do its work. First, it sends a message to its creator informing that Ukrainian bad guy that he has a new Mac slave. Next, the trojan horse takes over the infected Mac's ability to go to web addresses. It then begins its primary mission, sending the user to various pornographic web sites in the hope that the user will click on the services and advertisements that they find there (the bad guy gets paid for each click).

That is pretty much all that it does. While not destructive or terribly invasive, the trojan horse is still a very large problem as its bad guy owner could change its programming, any time he likes, and morph it into something really dangerous.

So, why isn't it scary? First, the trojan horse cannot infect your Mac without your express permission. Not only do you have to go and find it (in a place you are not likely

to be visiting), but you then have to do these things that no sensible person would do:

- 1) Download a mysterious piece of software, you didn't ask for, from a dodgy web site.
- 2) Ignore a warning about the downloaded software being potentially dangerous.
- 3) Click to allow the download.
- 4) Find the downloaded file (many of us are confused by this).
- 5) Double-click the file to start the install process.
- 6) Read a warning and agree to enter your secret, administrative password when asked.

A cynic would say that if you did all of the above, you would deserve what you get. But, I'm nicer than that and won't say it.

You can check to see if you have it. Do this to check:

- 1) Open your Mac's hard drive and find the Library folder.
- 2) Open the Library folder and find the Internet Plug-ins folder.
- 3) Open the Internet Plug-ins folder and look for a file named:
plugins.settings

If you find that file (you won't if you haven't been naughty) call me immediately for disinfection.

You haven't been naughty in the past and you probably won't be naughty in the future, but the trojan horse just might change its tactics. So, you need to take to heart these simple rules of safe internet computing:

- Don't download any file that you don't know is safe.
- Don't ignore warnings from your Mac. If you don't understand a message from your Mac, please contact me before taking action.
- Don't install any software that you don't know is safe.
- Don't type in your administrative password unless you know exactly why it is being requested. Ever!
- Don't click on web links in emails unless you know who sent them, why they did so and where they will take you.

And, for good measure:

- Never supply personal information if requested to do so in an email!
Only the worst bad guys ever do this.

These tips will keep you safe. And, being safe means that you'll have fun.

November Tip —

A couple of changes to *Safari's* preference settings will go far in keeping you safe on the internet.

First, turn off *Safari's* automatic password sending feature:

- 1) From the *Safari* menu, choose *Preferences...*
- 2) Click the *Autofill* button.
- 3) Uncheck the check box next to: *User names and passwords*.
- 4) Close *Safari Preferences*.

You will now have to manually type in your passwords.

Second, stop *Safari* from automatically opening downloaded files without asking for your permission. As the main article in this issue illustrates, this can be exploited to attack you. So, it is wise to turn this feature off.

Please do this:

- 1) From the *Safari* menu, choose *Preferences...*
- 2) Click on the *General* button.
- 3) Uncheck the check box next to: *Open "safe" files after downloading*.
- 4) Close *Safari Preferences*.

For more information, please see these past CCC Newsletters:

November 2006, March 2006, April 2004
Available at <http://www.calcompcare.com>

California Computer Care
P.O. Box 9445
Santa Rosa, CA 95405
(800) 540-8989
help@calcompcare.com

Like an
auto club
for your
computer.