



The

ROSE

BYTER

Apple Blossom Computer Club
A registered Apple/Macintosh User Group

Jun '09
still only
\$2.00

Next Meeting

**Jun 18, 7 PM
American Legion Hall
406 SE Oak Ave**

Agenda

1. Meeting starts at 7 P.M.
2. Intro's of members and guests
3. Old business
4. New biz
5. Program: Could be.
6. Questions & (maybe)Answers

Things Change

by Jim McClellan
<mcclellan@charter.net>

This morning, I received an email from Irislnk about changes to the Mac-Book Pro line. In reading this email it re-reminded me not of a new Mac, but of the real issue of what Apple has done, in my humble opinion, by changing to Intel from the PowerPC.

I'm so engrossed in this that I can never remember what I have other than that it is not a current computer.

I'm not sure I ever understood why Apple made the change, which might make an interesting meeting topic if it included information on the results to those of us with older Macs. I've wondered if it was just a "whim" of Steve Jobs, a way to improve the financial situation, an actual better technical

Big Mac attack or super-sized hype?

by Graham Cluley - Senior Technology Consultant

Experts at SophosLabs™, Sophos's global network of virus, spyware and spam analysis centers, have announced the discovery of the first virus for the Apple Mac OS X platform. The virus, named OSX/Leap-A (also known as OSX/Oompa-A) spreads via instant messaging systems.

The OSX/Leap-A worm spreads via the iChat instant messaging system, forwarding itself as a file called **latestpics.tgz** to contacts on the infected users' buddy list. When the latestpics.tgz archive file is opened on a computer it disguises its contents with a JPEG graphic icon in an attempt to fool people into thinking it is harmless.

The worm uses the text "oompa" as an infection marker in the resource forks of infected programs to prevent it from reinfecting the same files.

"Some owners of Mac computers

have held the belief that Mac OS X is incapable of harboring computer viruses, but Leap-A will leave them shellshocked, as it shows that the malware threat on Mac OS X is real," said Graham Cluley, senior technology consultant for Sophos. "Mac users shouldn't think it's okay to lie back and not worry about viruses."

Sophos customers have been automatically protected against the worm since 12:25 GMT, 16 February 2006.

"This is the first real virus for the Mac OS X platform," continued Cluley. "Apple Mac users need to be just as careful running unknown or unsolicited code on their computers as their friends and colleagues running Windows."

Sophos advises all computer users, whether running PCs or Macs, to practise safe computing and keep their anti-virus software updated.

[Editor's Note: the article above does go on ... and on. It's concerns are not entirely vacuous.

That said, they are highly self-serving and demonstrably misleading. In what followed, they attempted to justify calling the malware a virus, rather than a Trojan Horse, because it contains a means of spreading itself. I suspect, however, that many bits of malware long dubbed Trojan Horses also have such technology. The key issue is the mechanism for spread. This one is not hands off by default. It's not very hard to write a program that sends copies of itself to a list when you run it.

You do not need anti-virus software to avoid this. Simply use normal prudence: don't accept files that aren't from trusted sources and don't run things without checking them out first.]

contributed by Dave Archer <dave@davearcher.com>

METAL DETECTING

2

by Dale Nelson <dnelson@cmspan.net>

The **Apple Blossom Computer Club** (ABCC) is an Apple Computer Inc., registered Macintosh and Apple][family user group. The ABCC publishes *The RoseByter* newsletter monthly which is posted to each paid up member and reciprocating user groups. ABCC participates in user group newsletter content exchange. The ABCC also maintains a WWW site at:

<http://www.abccmug.org>

Membership

Just \$20/year! Send with your name, snail- & e-mail address & phone to:
ABCC
13748 Lookingglass Rd.
Winston, OR 97496

Current ABCC Leadership

Treasurer

Jim McClellan
<mcclellan@charter.net>

Apple Ambassador

Jim McClellan

Web Master

Jim McClellan

AppleScript Guru

Jack Webster <jackw@rio.com>

Newsletter Editor

Walt Pawley <walt@wump.org>
Send your stories and newsletter ideas to the Editor, Walt Pawley, at <walt@wump.org>. Plain text files are preferred, sent within the body of an email message or as an attachment. Mail physical media to:

**676 River Bend Road
Roseburg, OR 97470**

Please understand that materials submitted may not be used and those that are will likely be edited.
Copyright© 2009, All Rights Reserved



Detected Metal

It seems like we are being continually being asked for stories for this rag – er, that’s not polite, I’ll say News Letter. I’ve written a couple before, so I thought I’d try another and see how it turns out. My alter ego wants me to be a writer, but in real life that’s a challenge. First off, I have a terrible time spelling, but thanks to my MAC OS X version 10.4.11 I have a pretty good spell checker, so that problem is overcome. I do still have a problem with punctuation and get some help with that via the same source, but that doesn’t do the job the spell checker does, because that function expects you to know a little bit about what you are doing, and also to know something about sentence structure. I don’t, but I do a pretty good job of faking it. You know, in order for me to use my GI Bill of Rights, and get into college, I had to take dumbbell math, but not a thing on English, like somehow I fooled the test. Honestly, in college English I got C’s, but as I recollect, the classes were mostly reading some really boring books and short stories. I don’t have the same gift for the use of adjectives that my brother does – mine tend to be improper in polite company. That said, I’ll add that, in a news letter devoted to the Mac computer, one would expect to be asked to write arti-

cles about Mac computers. That slams the door shut on me, because most all of my knowledge about computers is located in conjunction with the on and off button. Perhaps someday I should write a story about how well I can exasperate Walt when he’s trying to help me with this bloody machine. See what I mean about adjectives.

Anyhow, this is a Macintosh news letter, and I’m writing a story about White’s Metal Detectors, so if this subject isn’t of interest, I suggest you stop now, because it isn’t going to get any better.

I’m not really a metal detecting nut, I’ve found out that metal detecting nuts go out every chance they get, day and night, and search for hours at a time. I think I can get about all the fun I can stand in bursts of two or three hours, several days or a week apart. I tend to like to hunt for relics, which means I find lots of rusty stuff, and not much money. People that hunt parks and beaches will find jewelry and money, which is something I don’t turn down, but it just isn’t as much fun for me. I know, it seems kind of dumb, but I’ve never claimed to be really smart either.

My interest in metal detection started when I worked for a cattle ranch in

3 -->



Items found on the Nevada ranch. The army button would have come from a soldier stationed at Fort Churchill during the Civil War. The fort was only about two miles from where I found the button, which was just outside our yard fence on the ranch.

<—METAL DETECTING



These bullets, both loaded and the empty brass, were found using the analog machine. They were either fired and the brass ejected, or the loaded ones were dropped and lost by soldiers over 100 years ago, and were a real thrill for me to find.

Nevada. It was a sizeable spread on the Carson River, and it seemed to me that about half of the western migrating wagon trains crossed over the property. It might not of been that many wagon trains, but there were darn sure a lot of them. I got the best detector I could afford at the time, and it didn't do well at all. I found lots of stuff, but it usually wasn't because of the detector, it was because I was out there with the detector, and the stuff was on top of the ground for the most part. Not shown in the enclosed photo are the OX shoes I also found on that property. Something as large as an ox or horse shoe that inexpensive machine could find under the ground.

Because that detector was doing such a poor job, I became discouraged, and for a number of years didn't do any treasure hunting. Well, lets face it, I'm using the term treasure quite loosely, my finds were treasure to me, but I suppose it takes some kind of a nut to think of square nails as treasure.

After moving to Roseburg, I got some powerful wants for another, better machine, not necessarily one that searches for deep targets, I don't like digging deep holes, I wanted one that

would reliably find small stuff. But those kind of metal detectors can be expensive – really good ones cost more than \$1,000 – and I was raising a family and didn't have that kind of money. But time goes by, and one day the kids are grown, and divorce comes down the pike, and for a divorce present for myself, I purchased a high dollar machine

from White's up in Sweethome, Oregon. In those days the machine I bought was analog, but worked great, doing everything I wanted it to do, and I found some good stuff with it. One feature that it had was discrimination. The machine could be set so that it didn't sound off for nails or foil etc. but would let you know if there was something nonferrous, like money or jewelry.

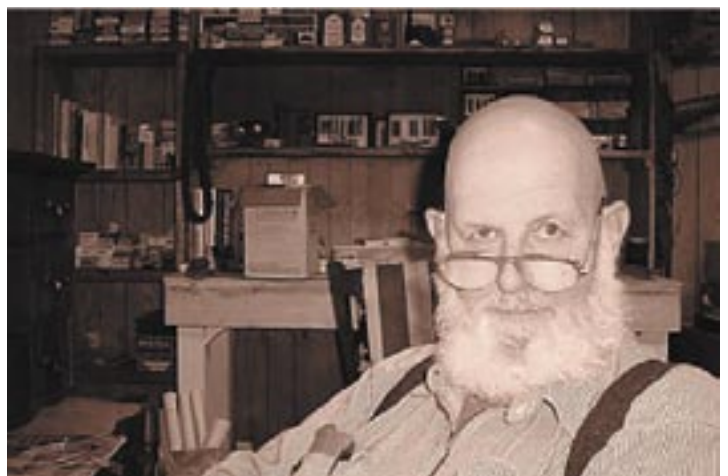
Then along came the digital age, and I again sprung for a new machine. This one has a read out, and along with discriminating out unwanted items like nails or foil, the machine tries to tell the operator what it thinks is down there under the ground, and how deep it thinks it is. Actually this works quite well, except when it comes to gold and nickels. Pop tabs sound off in the same range as gold, so it works out that if pop tabs and foil are discriminated out, most

gold rings and all of the nickels are missed; so I tend to dig a lot of pull tabs, simply because I don't want to miss something good. One other interesting tidbit is that square nails aren't steel, and will confuse the onboard computer into thinking they are something good, so if I'm relic hunting I'll find the square nails along with the goodies.

Finally, probably the best, but not the most valuable thing I've found to date is an 1893 Indian Head penny. Lets face it, I'm not getting rich, but I am having fun. And even if the gold rings I've found aren't real, it's a heart thumper when one of those comes out of the ground. That adrenalin rush at the sight of gold is probably what most folks that swing metal detectors are after, and that's a good high.



This Avon ring with a cracked stone, fake diamonds and the gold plate peeling off, is still a treasure to the author, because it's the first ring he found.



The author, Dale Nelson.

Water Blogged Wump

Any trace of organization in these paragraphs is entirely coincidental

4



Muncies Coming Along

While I haven't written anything about it in these pages before, there's a concept called "cloud computing" that's been pushed by some for quite a while now. The concept is, perhaps, an outgrowth of the sort of thinking that created the notion of the "thin client." These things are based on the availability of high speed networking coupled to the notion of aggregating a group's computing someplace where it can generate concentrated income. This "thin client" is most obviously a means of centralizing control and was long considered a means of cutting the cost of interfacing a person to a corporation's data. **Real savings have, for the most part, not arisen from such systems.** Cloud computing can be viewed as something of the opposite organization: a person interfaced to a "cloud" of computers via a network (the Internet, say), each of which works on small fragments of the computational problem. So, how does one concentrate wealth with this? One way is to serve as a broker for connecting the person with the problem to the cloud. This is especially effective when the cloud is closely held; such as the workstations in a corporation that are not being fully utilized. No need to pay for each of the rain drops in the cloud. Another way is exemplified by SETI – Search for Extra-Terrestrial Intelligence – which uses volunteer droplets to do the computing for a central purpose ... which just happens to have enough funding to pay the principals decently.

The Mac must be coming of age ...

finally. Why? Well, **the media is hard at work pushing the notion that there are now real viruses for Mac OS X.** Elsewhere in this issue you can read about an iChat exploit that is being argued into the virus category. Frankly, I side on the non-virus side of this issue since you have to open a document sent to you unbidden via iChat. If you're a curious cat who just has to investigate such things, then you'd better learn how to avoid doing things with a double-click of the mouse. If you can't do that, it's time to start being paranoid, I guess ... but it's really been that way for a very long time. It's my opinion that the exploit uncovered by Landon Fuller is more critical. First of all, Landon is no light weight when it comes to Macs. I follow, and occasionally make a fool of myself, on a mail list on which he's a principal participant. Frankly, I'm a little surprised that this exploit hasn't been more problematic to date. It seems that Web browsers not only use JavaScript but will also run Java applets. Despite the similarity in the names, these two things are NOT the same thing at all. JavaScript is a programming technology that runs in your browser. It's carefully designed not to be able to do nasty things to your computer (of course, that doesn't make it "safe," just "safer"). Java, on the other hand, is executed by an interpreter that's independent of your Web browser as a rule. Indeed, Java is used to write finished applications for your Mac (and other OSs) that look and feel just like any other program you might have on your computer. Here's the problem – Java applets, as such programs are known, can be executed by your browser merely by downloading a page containing a reference to them. In other words, you don't get to choose not to run them; they run automagically. I just looked through the Firefox preferences to see if it could choose to run or not run a Java applet. At least in the version on my PowerBook,

there's a checkbox to control it. Mine was checked on. I do not believe that's something I did specifically. I believe it came that way. I unchecked it. I advise you to **check out your browser(s) and turn off execution of Java applets if possible.** Note that this is NOT the same as turning off JavaScript, which is most probably a bad idea for the time being.

RFID, a technology in which data can be programmed into "labels" and then read back with non-contact means (radio waves, in other words), is making its way into things it most probably should not, like passports. Proponents of such use claim they improve security ... though reasons for that seem a little hard to come by. Why? In their presently form, the RFID data is easily read by small, inexpensive equipment from a distance long enough not to be readily obvious. Once captured, the RFID tag can be cloned. What does this mean? **In the case of passports, for example, it means that your friendly neighborhood terrorist can wander across borders unhindered.** If you use an RFID bank card, it means that your accounts are all readily accessible ... by someone else. You see, manufacturers of RFID technology want to sell their wares despite the fact that they are readily compromised. There are really good uses for the current technology, but anything that's critical should not be a candidate. Perhaps some sensible means of secure use will arise but that has yet to happen.

The Internet may be having its problems here on Earth but it's working in outer space. **NASA has made a test run of what's dubbed the Deep-Space Internet by some** but really known more properly as DTN (Disruption Tolerant Network). The one-way transit distance for NASA's test: 20 million miles. Well, when

5 -->

<--Water Blogged Wump

someone survives crashing on Mars, we'll be able to get the skinny from the horse via Facebook.

I was poking around in my accumulated Eudora mailing-list email and happened on the fact that **Infinity Data Systems has changed the name of their effort to provide a Eudora email client replacement from Odysseus to MailForge**. Moreover, IDS was offering a beta release for download. Now, I should preface with the statement that I'm not looking to replace my Eudora 6.2.4 – I like it far more than any other email client I've seen yet. Not that it's perfect, mind you. But it's more than the fact that I'm familiar with Eudora because I've been using it for a long time. The underlying technology is readily dealt with using simple tools like a plain text editor. It's a feature that I am extremely loath to give up. The Eudora >6.2.4 project, which is a wrapping for Mozilla's Thunderbird email client, not only provides a foreign user experience to the classical Eudora user, it also blows off all the handy underlying technology, replacing it with opaque files one can't deal with readily. MailForge is looking a lot like Eudora of old, so the appearance does not inspire attacks of xenophobia. Unfortunately, the underlying file system is based on SQLite instead of plain text. While this does have some advantages and can be dealt with outside of MailForge (or should be if they haven't locked stuff up), it's much more involved to deal with than a simple text editor. I'll stick with Eudora until I'm forced to change by either lack of equipment to run it on or changes in email standards that obviate it. If those things happen, I'll probably start using command line email.

I've seen a **number of advertisements recently for "nitrogen enriched gasoline."** I have to confess that this puzzles me a great deal. Supposedly, it's designed to keep your vehicle's engine free of gunk deposits.

But somehow simply adding nitrogen to gasoline seems like a very big waste of effort to me. After all, the atmosphere we live in something like 70% nitrogen. Since air intakes on engines don't have a nitrogen filter, there's clearly a great deal more nitrogen than oxygen already running through engines. Of course, these advertisements are not telling the whole truth, most probably because Shell's executives are of the opinion most of their customers are too stupid to understand it. In reality, nitrogen "...is a key ingredient of the gasoline's active cleaning molecule," according to some research of press releases on the Web. Is this a good thing or not? Even if I knew precisely what molecule it was and how much was being used, I would not have a clue. However, a good number of nitrogenous molecules are anything but benign – ammonia, nitrous oxide, nitroglycerin, nitric acid – to name just a few. In fact, nitrogenous compounds are some of the worst pollutants coming out of internal combustion engines and that just from burning non-nitrogenous fuels in a nitrogen atmosphere. So, is Shell's magic molecule and the results of its activity still more nasty bits of work we'll be spewing from our tailpipes?

I see that the people at AstraZeneca International have apparently decided **we're too dumb and/or lazy to deal with a word as busy as the six syllable "atherosclerosis."** They're using the word atherosclerosis in their advertisement for Crestor but they add the phrase "or athero" to their spiel on screen. Perhaps some further Murkinization can reduce this to "ahro" or, more simply, just "ro."

As those of you who are avidly awaiting the opportunity to ruin your perfectly nicely sorted out Macintosh to jump on the bandwagon of what's new and improved in Appledom are aware, the WWDC (World Wide Developer's Conference) is on (as I write this - it'll be over by the time you get to read it). Apple's web site is transmogrifying itself to announce

all their newest goodies, **the Snow Leopard version of OS X** in particular. One posting is the keynote address. I watched the first bit about Mac stuff and decided that over an hour about iPhone and iPod were not to my taste (I'm a hopelessly old fuddy-duddy). Why, yes, Virginia, Steve's little elves have been very busy. But not much of their handiwork is designed to help people who aren't running the latest Macs. It's almost all targeted straight at Intel Macs only. One major exception is Safari which has been upgraded to version 4.0 and is supposedly 100% compliant with Acid 3 (a test of a browser's compliance to open standards - Internet Explorer is not even close to complying ... which, of course, means that Safari will likely stumble on sites made for IE, a characteristic major corporations remain too dimwitted to avoid). And, Safari 4.0 is available for both Leopard and Tiger. So, naturally, I had to give a try. The installation process bugged me some. I had to install the latest security update before installing Safari. This required a reboot. I was not all that surprised by having to reboot for a security fix — they tend to muck with deep stuff. When I installed Safari, it also demanded a reboot. I don't care for that at all. User level programs should not be mucking with deep stuff. I suppose it has something to do with "integration" — that part of computing where every program is "aware" of every other program and they all do stuff you're supposed to want done automatically. Frankly, I don't care for that ... but that's just the fuddy-duddy in me. When it's first fired up, it presents a "Top Sites" page. Since I haven't been anywhere with it yet, it has to fill in some slots for me. Presumably these are the sites "everyone" goes too all the time. None of them were things I go to much, some not at all ... ever. At least Safari ran. All I can say is that it's too bad they didn't back date to Panther.



This page intentionally left almost, but not quite, blank

Ditto
(Space awaiting your input)

from <http://landonf.bikemonkey.org/>

A Real Mac OS X Virus?

by Landon Fuller
<landonf@macports.org>

Introduction

Five months ago, CVE-2008-5353 and other vulnerabilities were publicly disclosed, and fixed by Sun.

CVE-2008-5353 allows malicious code to escape the Java sandbox and run arbitrary commands with the permissions of the executing user. This may result in untrusted Java applets executing arbitrary code merely by visiting a web page hosting the applet. The issue is trivially exploitable.

Unfortunately, these vulnerabilities remain in Apple's shipping JVMs, as well as Soylatte 1.0.3. As Soylatte does not provide browser plugins, the impact of the vulnerability is reduced. The recent release of OpenJDK6/Mac OS X is not affected by CVE-2008-5353.

Work-Arounds

- * Mac OS X users should disable Java applets in their browsers and disable 'Open "safe" files after downloading' in Safari.
- * Soylatte users running untrusted code should upgrade to an OpenJDK6-based release, where possible. No future releases of the JRL-based Soylatte branch are planned at this time. If this is an issue for you, please feel free to contact me.
- * No work-around is available for users otherwise running Java untrusted code.

Proof of Concept

Unfortunately, it seems that many Mac OS X security issues are ignored if the severity of the issue is not adequately demonstrated. Due to the fact that an exploit for this issue is available in the wild, and the vulnerability has been public knowledge for six months, I have decided to release a my own proof of concept to demonstrate the issue.

If you visit the following page (<http://landonf.bikemonkey.org/static/moab-tests/CVE-2008-5353/hello.html>), "/usr/bin/say" will be executed on your system by a Java applet, with your current user permissions. This link will execute code on your system with your current user permissions. The proof of concept runs on fully-patched PowerPC and Intel Mac OS X systems.

Credit

Thanks to Jeffrey Czerniak for bringing this issue to my attention.

Also, see: <http://blog.cr0.org/2009/05/write-once-own-everyone.html>



<-1 Things Change

result, etc. Which leads to the question as to how much consideration was given to users who didn't make it a habit to always upgrade to new computers when they came out.

It wouldn't be hard to understand Apple's motives when one considers how they feel about user groups in general.

If you haven't figured me out by now, I still use at least two OS 9 applications because they do what I think I need as well or better than newer versions. In sort of an example, I have been updating my Firefox application each time a new version comes out. It

seemed to be a good idea, until Firefox added some features that I ignored until I realized that I was having problems with what I wanted to do. Now, I wish I had an earlier version.

Perhaps in some way this software issue is related to the change to an Intel Mac from a PowerPC Mac.



unClassifieds

Need a manual?

Discount for ABCC members!



Apple Blossom
Computer Club

<http://www.abccmug.org>

Give it a look.

Put in your own...

