Access

Newsletter of the Louisville Computer Society
Kentuckiana’s Macintosh Users Group
March 2005

Security

Thanks Tom and Bill for the link to the following which was on MacGroup today and got a lot of interest. For those of you who use the Internet but don’t read our e-mail discussion group MacGroup, this important information about computer security is printed here; edited for space.

http://www.securityfocus.com/columnists/215

A Visit from the FBI
By ***Scott Granneman*** Jan 21 2004

I teach technology classes at Washington University in St. Louis , a fact that I mentioned in a column from 22 October 2003 titled, " Joe Average User Is In Trouble ". In that column, I talked about the fact that most ordinary computer users have no idea about what security means. They don't practice secure computing because they don't understand what that means. After that column came out, I received a lot of email. One of those emails was from Dave Thomas, former chief of computer intrusion investigations at FBI headquarters, and current Assistant Special Agent in Charge of the St. Louis Division of the FBI.

Dave had this to say: "I have spent a considerable amount in the computer underground and have seen many ways in which clever individuals trick unsuspecting users. I don't think most people have a clue just how bad things are." He then offered to come speak to my students about his experiences. I did what I think most people would do: I emailed Dave back immediately and we set up a date for his visit to my class.

Dave arrived and set his laptop up, an IBM ThinkPad A31. He didn't connect to the Internet - too dangerous, and against regulations, if I recall - but instead ran his presentation software using movies and videos where others would have actually gone online to demonstrate their points. While he was getting everything ready, I took a look at the first FBI agent I could remember meeting in person.

Dave focused most of his talk on the threats that ordinary computer users face: what those threats are, who's behind them, and why they exist. He spent quite a bit of time talking about the intersection of Trojans and viruses. He started by showing us how easy it is to create a virus, using one of several virus creation wizards that can be easily found on the Net (of course, real men and women write their own).

More and more, however, the viruses circulating on the Internet are quite purposeful in design. The goal is to install a Trojan on the unsuspecting user's machine that will then allow the bad guy to control the machine from afar, turning it into a Zombie machine under the control of another. All too often, this tactic is successful. Hundreds of thousands if not millions of machines are "owned" by someone other that the user sitting in front of the keyboard and monitor.

These Trojans are often the ones that security pros have been watching for years: SubSeven, Back Orifice, and NetBus . A lot of the time, script kiddies are the ones behind these Trojans, and they do the usual stuff once they have control of a user's PC: grab passwords, use groups of machines to organized DDOS attacks (often against other script kiddies), and jump from machine to machine to machine in order to hide their tracks.

The scary part came in when Dave started talking about the other group behind the explosion of viruses and Trojans: Eastern European hackers, backed by organized crime, such as the Russian mafia. In other words, the professionals.

These people are after one thing: money. The easiest way to illegally acquire money now is through the use of online tools like Trojans, or through phishing : set up a fake Web site for PayPal or eBay or Amazon, and then convince the naíve to enter their usernames, passwords, and credit card information. Viruses and spam also intersect in this nasty spiderweb. Viruses help spread Trojans, and Trojans are used to turn unsuspecting users' computers into spam factories, or hosts for phishing expeditions, and thus furthering the spread of all the elements in this process: viruses, Trojans, spam, and phishing. It's a vicious cycle, and unfortunately, it appears to be getting worse. The FBI is working as hard as it can, but the nations of Eastern Europe are somewhat powerless to solve the problem at this time.

One way to trace just how bad the situation has gotten: track the price for a million credit card numbers. Just a few years ago, Dave saw prices of $100 or more for a million stolen credit card numbers. Now? Pennies. Stealing credit cards is so easy, and so rampant, that prices have dropped precipitously, in a grotesque parody of capitalist supply and demand.

Along with this comes intrusions into banks and other financial institutions. Dave wouldn't name names, but he said several organizations that we would all know have been infiltrated electronically by Eastern Europeans, who then grab customer data. A few days later, the unsuspecting president of the bank gets an email demanding $50,000, or else the media will be told of the break-in. Of course, the break-in is news to the bank. As proof of

Con’t on Page 2

Louisville Computer Society, Inc.
P. O. Box 9021, Louisville KY 40209-9021

Access is a service mark of the Louisville Computer Society, Inc. Our newsletter is publisher monthly as a service to Macintosh users. We are dedicated to the education and benefit of Louisville and southern Indiana computer-oriented communities.

Subscription rate is $26 a year; it is mailed free with your membership in LCS, a Macintosh Users Group (MUG).

Trademark names are sometimes used in this publication. rather than put a trademark symbol in every occurrence of a trademark name, we state that we are using the names only in an editorial fashion, and to the benefit of the trademark owner, with no intention of infringement of the trademark.

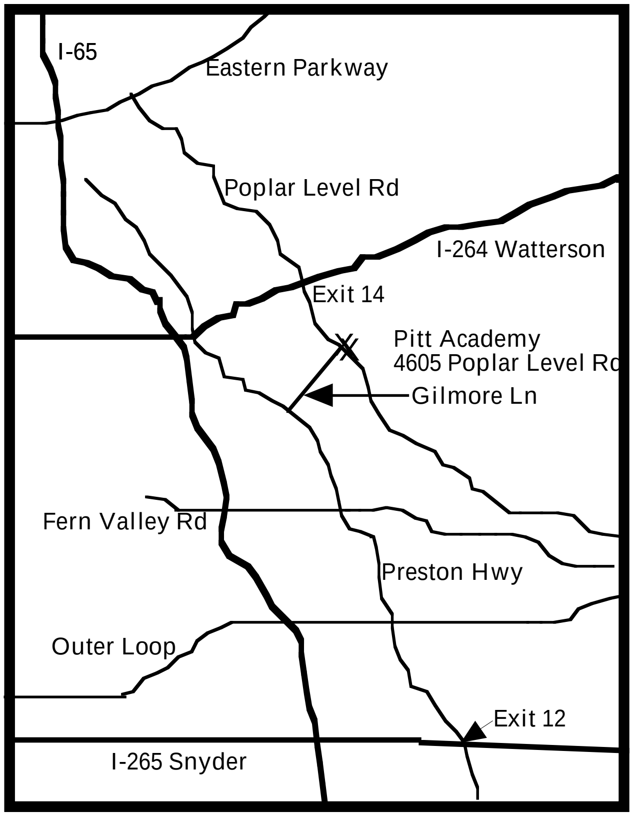
For more information write to the above address or call 502-363-3113 between 5 and 9 P.M. only.

Other users groups may reprint articles from Access provided proper credit is given to the Louisville Computer Society, to Access, and to the authors, unless otherwise noted. ©2004

Come to our monthly meetings

The Louisville Computer Society meets the 4th Tuesday of each month, 7-9 P.M. (except December) at Pitt Academy, 4605 Poplar Level Rd. (Poplar Level Rd. at Gilmore Lane), Louisville KY 40213 (see map below).

Pitt Academy is 1 mile south of the Watterson on Poplar Level Rd. If coming from the Snyder Freeway, Gilmore Ln is 5 miles north of I-265 on Preston Hwy. Turn right and when you get to the end (Poplar Level Rd), Pitt Academy is directly across the intersection.



Security -- Con't from Page 1

their exploit, a spreadsheet is attached to the email, with a few hundred rows of client data: bank account numbers, home addreses, balances.

Unfortunately, many banks decide to keep it all a secret from their customers, so they reluctantly decide to go ahead and pay the extortion. $50,000 goes to the criminals, and the bank breathes a sigh of relief.

Three days later, ten emails arrive, from ten different criminal organizations, each demanding $25,000. Ooops. Far from buying protection, the bank revealed itself as a easy mark, amenable to blackmail. And it will only get worse. Time to call in the FBI, as it should have done from the beginning.

American companies have tried to respond to the massive fraud being perpetrated online. One common preventive, adopted by most companies that sell products online, has been to refuse shipments outside of North America, or allow international shipping, except for Eastern Europe. Criminals have figured out a way around this, however. They hire folks to act as middlemen for them. Basically, these people get paid to sit at home, sign for packages from Dell, Amazon, and other companies, and then turn around and reship the packages to Russia, Belorussia, and Ukraine. You know those signs you see on telephone poles that read "Make money! Work at home!"? A lot of that "work" is actually laundering products for the Russian mob. Of course, anyone caught acting as a middleman denies knowledge of their employer: "I had no idea *why* I was shipping 25 Dell computers a day to Minsk! I just assumed they liked computers!"

Proof once again that social engineering, coupled with greed, is the easiest way to subvert any security.

Some surprises

Dave had some surprises up his sleeve as well. You'll remember that I said he was using a ThinkPad (running Windows!). I asked him about that, and he told us that many of the computer security folks back at FBI HQ use Macs running OS X, since those machines can do just about anything: run software for Mac, Unix, or Windows, using either a GUI or the command line. And they're secure out of the box. In the field, however, they don't have as much money to spend, so they have to stretch their dollars by buying WinTel-based hardware. Are you listening, Apple? The FBI wants to buy your stuff. Talk to them!

Dave also had a great quotation for us: "If you're a bad guy and you want to frustrate law enforcement, use a Mac." Basically, police and government agencies know what to do with seized Windows machines. They can recover whatever information they want, with tools that they've used countless times. The same holds true, but to a lesser degree, for Unix-based machines. But Macs evidently stymie most law enforcement personnel. They just don't know how to recover data on them. So what do they do? By and large, law enforcement personnel in American end up sending impounded Macs needing data recovery to the acknowledged North American Mac experts: the Royal Canadian Mounted

Con't on Page 3

LCS e-mail address book

Andrew Arnold	a0arno01@athena.louisville.edu
Jim Bennett	bennetts29@insightbb.com
Anne Cartwright	cartwrig@aye.net
Marta Edie	meld@insightbb.com
Jonathan Fletcher	jfletch@newmediaconstco.com
Bernard Griffins	latigopc@bellsouth.net
Tom Guenthner	Tom@aye.net
Nelson Helm	helmkyny@clockwinders.net
Glenn Hoehler	glenn@insightbb.com
Harry Jacobson-Beyer	harryjb@bellsouth.net
Bill King	bk0413@insightbb.com
Lee Arson	leelarson@mac.com
Jeanie Montgomery	jerryandjeanne@aol.com
Tympana Oberhausen	tympana@bellsouth.net
Brian O'Neal	iMac@mac.com
Ed Stirrers	stivers1@earthlink.net
Jan Webber	kyjweber@mac.com
George Yankee	jeffco13@bellsouth.net

If you wish to be added, contact cartwrig@aye.net

LCS Web Page, List Serve & Officers

Web Page	www.kymac.org
List Serve	macgroup@erdos.math.louisville.edu
Tom Guenthner, President	Tom@aye.net
Lee Arson, Vice President	leelarson@mac.com
Bill Rising, Program Director	braising@louisville.edu
Brian O'Neal, Web Master	iMac@mac.com
Anne Cartwright, Newsletter Editor	cartwrig@aye.net

Security -- Con't from Page 2

Police. Evidently the Mounties have built up a knowledge and technique for Mac forensics that is second to none.

(I hope I'm not helping increase the number of sales Apple has to drug trafficers.)

The biggest surprise was how approachable and helpful Dave was to everyone in the room. According to Dave, the FBI has really made reaching out to the local communities it's in more of a priority. Since the September 11th attacks, the FBI has shifted its number one focus to preventing terrorism, but the number two priority remains preventing and capturing crimes based around technology. In order to best achieve both goals, the FBI has been working hard to reach out to American citizens, and Dave's talk to my class was part of that effort.

If interested in joining the Louisville Compuer Society's e-mail discussion group just:
Send email to majordomo@erdos.math.louisville.edu
containing the single line

subscribe macgroup

A few minutes after you do this, you will receive two messages from majordomo. One will be general information and instructions. The other will contain instructions how to confirm your subscription request.
(The reason for this baroque procedure is to cut down on spamming.)

Upcoming Programs 7 P. M. at Pitt Academy (see map on page 2)

March 22 Lee Larson will demonstrate the new iWork software from Apple.

Future programs according to interest of members will probably deal with iPod, Palm, Genealogy, and other topics which I can't remember. If you have any special requests, please conract Bill Rising at braising@louisville.edu.

Louisville Computer Society

Macintosh Users Group
Membership Application

Please send your $26 check for a year's membership, made out to Louisville Computer Society to:

Louisville Computer Society
P.O.Box 9021
Louisville,KY 40209-9021.

Thanks! See you at the next meeting.

Fill out the following ; clip on the dotted line (or copy to another piece of paper) and send in with your check .

❑ New or ❑ Renewal Membership

Name: ______

Home Address: ______

City: ______ State: ______ Zip+4: ______

Home Phone: ( ) Your E-Mail: Your Home Page: ______

How did you hear about LCS" ______

iPods- not just for iTunes

Next we need an iPod that shuffles tunes and photos together to make an AV program to while away your time!

Looks like Apple is coming out with the gadget I need last summer.

Apple describes this new accessory as follows: The new iPod Camera Connector is an optional accessory that enables customers to connect their digital camera to iPod photo and import their photos into the iPod. By connecting the iPod Camera Connector and a digital camera, customers can transfer digital images to their iPod photo, providing tremendous storage space so they can take more pictures. Imported photos are immediately viewable on iPod photo's color screen, and can also be brought back to iPhoto on the Mac or various photo applications on the PC. The iPod Camera Connector is expected to be available in late March for $29.

At an press briefing held February 27 by Representatives from Apple Japan on the company's new iPod offerings, a keynote slide with (what appears to be) a photo of Apple’s new iPod Camera Connector appeared.

That’s a lot less than the $199. I paid for a 10GB digital wallet called MindStor. Of course to use this $29 gadget I would also have to by an iPod and naturally I would want the iPod Photo, so that’s a bigger bunch of bucks.

Now if you already have an iPod, one of the older full size ones, and you’re interested in such a gadget for downloading your camera to a storage device without the use of your computer and you need it NOW, Belkin has two such devices on the market already. (http://www.belkin.com/iPod/matrix/index.asp?cid=1&lid=1&dock=y)

The one most like what I used is called the **Belkin iPod Media Reader for iPods with Docking Connector ($59.99)**. Their Web site description says “the iPod's new photo storage feature allows users to use a Belkin Media Reader to import, store and backup over 20,000 digital photos from a 3 megapixel camera onto a 40GB iPod and take them anywhere. This frees up valuable camera and memory card storage space so users can continue to take pictures without the hassle and expense of buying and carrying multiple memory cards. Once the iPod is connected to a Mac or Windows PC, the digital photos are easily transferred to a user's computer and photo editing software.

With Mac OS X, iPhoto will automatically recognize the iPod as a media storage device and prompt users to transfer their photos into the iPhoto library -- just as if it were a camera, allowing users to erase the photos after transfer if desired.”

Belkin’s other device, **Belkin’s Digital Camera Link for iPod w/ Dock Connector ($79.99)** allows you to transfer your photos directly from the camera to the iPod using the USB cable that came with your camera.

To use either of the Belkin products you’ll need is Apple’ s latest iPod upgrade. In addition to adding ‘Shuffle Songs’ functionality to iPods other than the Shuffle, You’ll see the “Photo Import” option. There’s hope that this “Photo Option” indicates Apple’s new iPod camera connector will also be able you transfer photos directly from your camera and/or storage media card, directly to your iPod.

Note this works with all the full size iPods from the 3rd generation on, not just iPod Photo. So if you don’t mind waiting until you get back home to view your photos again (after you have taken them off your camera and you need portable photo storage), this sounds like it would do the trick.

This transfer will take longer than just switching media cards, so if you have enough cards to get you through until you have time for a break, the media Reader seems better, and less expensive, than the Camera Link.

The real advantage of Apple’s proposed new product will be the ability to view your photos on an iPod Photo. neither Belkin device allows viewing, on the iPod Photo.

37¢

www.kymac.org

The Louisville Computer Society
P. O. Box 9021
Louisville KY 40209-9021

Mailing Label