CAEUG Computers Are Easy User Group

Abort,
Retry,
Ignore....

Founded 1984 **ARI** is the
Official Newsletter of
Computers **A**re **E**asy **U**ser **G**roup

November / December
2012
Volume XXIX Issue 11

Confirmed
meeting
dates for
2012
Room A

2013
January 26
4th Saturday

February 23
4th Saturday

Check
www.caeug.net
for confirmed
meeting dates

MEETING
PLACE
will be the
Glenside Public
Library
** **
*** ***
Visitors
Welcome

HOPE TO SEE
YOU THERE!!

Our December 1st 2012 (first Saturday) Presentation:

Our November / December 2012 presenter will be Michael Goldberg demonstrating security based software Secunia PSI, PCPitStop, and Advance System Care

Can QR Codes Spread Computer Viruses?

by Bob Rankin, Ask Bob Rankin
www.askbobrankin.com

From Rankin’s June 4, 2012 newsletter, reprinted with permission

Any doubts I may have had about the viability of QR codes have evaporated. You know a new technology is catching on when malware authors start using it to snare unwary users. Read on to learn how those funny black squares can carry a nasty (and expensive) payload...

QR codes are squares of black and white patterns that encode the URLs of Web sites in a format that can be scanned and deciphered by smartphones equipped with the right apps. Instead of typing a URL into your phone's browser, you can just snap a picture of a QR code and be whisked to an ad, an informative Web page... or a malicious site that silently downloads a virus, rootkit, or trojan to your phone.

Kasperky Labs has detected two samples of malware delivered via QR codes, both targeting Android phones. One of them sends SMS messages from the infected phone to a premium-priced number; each text message costs the victim six dollars! Other types of malware can scoop up your contacts list, send

Con't pg 2

Table of Contents

spam emails in your name, and wreak other sorts of mischief.

(https://www.securelist.com/en/blog/208193145/Malicious_QR_Codes_Pushing_Android_Malware) <http://bit.ly/qGXZig>
http://bit.ly/qGXZig
Can a QR code itself contain malware? Theoretically, yes, but it wouldn't do much. A QR code can contain only a limited amount of data: 7089 numeric characters or 4296 alphanumeric characters. You can't write much of a program in that space. But a QR code can easily take you to a malicious site.

Humans cannot tell one QR code from another, generally speaking. You have no idea where a QR code is going to take you until you scan it, and then it's too late. So it pays to be skeptical of all QR codes, while exercising some common sense.

QR codes printed in paper publications, on in-store posters, on coupons from well-known retailers, and similar places are unlikely to be malicious. But never forget the days when shrink-wrapped software packages were infected with malware at the factory by disgruntled workers.

A QR code on a Web page is more easily compromised. If a hacker can crack the site's security, he can replace a legitimate QR code with a malicious one of his own. There have already been reports of malicious QR codes showing up in spam emails. Be a bit more cautious before scanning online QR codes, and especially if they arrive in unsolicited emails.

If you notice a sticker bearing a QR code just randomly slapped up on a wall or a sign post, think twice before scanning it. On the other hand, this method of distributing malicious QR codes is so inefficient that it probably isn't used much.

Malicious QR codes can be countered by anti-malware apps that translate a QR code into a URL and allow a user to review it in plain text before deciding whether to let the Web page be fetched. Better still, look for an app that prescreens all URLs against a blacklist of known attack sites. Norton Snap is one such app that works on both Android and iOS devices. In addition, Lookout Mobile Security and the McAfee Antivirus & Security app (both for Android) claim to protect you from malicious URLs in QR codes.

On a semi-related note, I should mention that Microsoft has invented its own version of QR codes, presumably to inject a little more confusion into the world of computing. Microsoft Tag barcodes are similar to QR codes, but different. Some QR code readers can understand Tags, and some Tag readers can understand QR codes. But not all of the code reader apps do both. Hopefully, a unified qr/barcode/tag standard will evolve in our lifetime, and malware authors won't have to work so hard to scam smartphone users who scan random codes.

Malicious QR codes are still rare, but if they work you can be sure that many more will appear quite rapidly. It's better to be on your guard now than after you scan the wrong QR Code.

Create Safe Passwords

By Sandy Berger, CompuKISS
www.compukiss.com
sandy (at) compukiss.com

Using passwords correctly is one of the best ways to protect yourself and your computer. If you use the same password for everything, read this article and make some changes as soon as possible.

Just about everyone can relate to the frustration of trying to make an online purchase or to access information at a website and not being able to remember your user name and password. If you are over 50 and have that problem, you may attribute it to senior memory loss. That, however, is not really the problem. Even younger folks forget passwords. It is because so many websites and web services require passwords. When written down, my list of passwords spans 12 sheets of double-column letter-sized paper.

Obviously if you use a different password for each website, you will have pages of passwords, as well. Yet, if you're like many others, you may use the same password for all of your websites A recent Washington Post survey show that 30% of respondents said they use the same password for different websites including banking, social networking and shopping sites. This is a very risky practice.

We are constantly bombarded with news about stolen passwords. Recently 6 million passwords were stolen from LinkedIn. Recently more than 400,000 email addresses and passwords were stolen from Yahoo and posted online. It is obvious that if people use the same password at numerous websites, it was only time before hackers would use those passwords to try to access different websites.

BestBuy recently confirmed that hackers are using credentials stolen from other sites to make purchases at their online retail site. The same thing is happening at other retail and banking sites.

So the first rule of thumb is to use unique passwords for any e-commerce or banking websites. The second rule is to never use commonly used passwords. What are the most common? Although different research on this produces different results, several passwords are always in the top 25 most common. If you think you are being unique by choosing the word "password", you are wrong. It is usually the most commonly used password choice. This is often followed by 1234, 123456, 1234567, 1234567, 111111, 123abc, and querty. Anyone who uses "letmein" as a password has many like-minded friends. It is usually on the top password lists along with other simple words like baseball, football, michael, jennifer, and monkey. Seems like everyone is a dreamer as indicated by other popular passwords like harley, mustang, master, and superman.

It is also a known fact that hackers can use words from a dictionary to perform an automated attack to "guess" your password. So you don't want to use plain words, even in combination. Hackers now also use rainbow tables which are alphanumeric combinations of words and numbers. They also have common substitutions included. So using a zero instead of the letter "o" or an eight instead of the letter "B" is not always enough to keep your passwords safe. Some of

Con't Page 4

these tables also have symbols, but using a password with one or more symbols is still much safer than one without any symbols.

A really safe password will use a combination of uppercase and lowercase letters, numbers, and symbols that do not spell out any words. The length of the password is also very important. To give you an example of that, let's consider a password that includes letters and numbers, but no upper and lower case combinations and no symbols. If the password has six characters there are 2.25 billion possible combinations. A ten character password will have 3.76 quadrillion possible combinations. Every time you add a character, you make the password exponentially more difficult to break.

If all this makes your head spin, remember that you can use simple passwords at websites that require passwords, but have none of your personal information. These sites usually also require an email address. So if you open a Gmail or other email account and use that specific email address only for this type of website, you don't have to worry about compromising your security.

You should, however, be very careful with passwords for banking and e-commerce websites where your personal information and/or credit card numbers are stored. Use strong passwords for these sites and have a different password for each site.

Hotel Wi-Fi Networks Installing Malware

By Sandy Berger, CompuKISS
www.compukiss.com   sandy (at) compukiss.com

If you are traveling this year, there is a new hacking scheme that you should be aware of. The Federal Bureau of Investigation is warning travelers to watch out for malware that comes through hotel Internet connections.

Here's how it works. When you get to the hotel and connect to the Internet through their wireless or wired Internet connection, you get a pop-up notifying you that you must update your Java in order to have the connection work. When you give your approval, malware is installed on your computer giving the hackers access to your personal information. The malware also serves third-party advertisements to infected computers.

Bloomberg has recently reported that Chinese hackers have stolen private data from as many as 760 firms by hacking into the iBahn, a broadband and entertainment service that offered to guests of hotel chains such as Marriott International Inc.

The advice offered by the FBI's Internet Crime Complaint Center (ISC3) includes:

* Carry out all software updates before traveling.
* Checking the author or digital certificate of any prompted update to see if it corresponds to the software vendor.
* Download software updates direct from the vendor's website.

I recommend skipping any software updates that you are offered when traveling and using an encrypted connection for handling email when you are on the road. The way to do this depends on how you access your email when you travel.

Gmail is secure since it is encrypted. Other email, however, may not be encrypted. For instance, Time Warner's Road Runner Web Mail that you can use when you travel encrypts your user name and password, but not your email itself. Other services may be different. You will

Con't pg 9

Lamp Post 143

by John Spizzirri
November December 2012

If you attended last month's CAEUG meeting, you know that the library did not have power (or Internet). The cause was a blown transformer that fed only the library. Commonwealth Edison (ComEd **(1)**) was called but could not fix the problen in a timely manner. The library was closed about an hour and a half after it opened. Hopefully, ComEd put in a new transformer so it will not happen again, soon.

1) https://www.comed.com/Pages/default.aspx

YouTube's **(1)** most watched video has now topped 815 million views. It is a hard pounding techno **(2)** music video of the South Korean rock star Park Jae-sang known as PSY **(3)**. The song is Gangnam Style **(4)**. Guinness World Records **(5)** recognizes it as the most viewed video online **(6)**. The 35 year old PSY took the title away from the 18 year old Justin Bieber's **(7)** Baby **(8)**. Guinness predicts that Gangnam Style will reach 1 billion views before December 25th.

1) https://www.youtube.com/
2) https://en.wikipedia.org/wiki/Techno
3) http://sn.im/25p3n11
4) https://www.youtube.com/watch?v=9bZkp7q19f0
5) http://www.guinnessworldrecords.com/
6) http://sn.im/25p3muj
7) https://en.wikipedia.org/wiki/Justin_Bieber
8) https://www.youtube.com/watch?v=kffacxfA7G4

Forbes Magazine has an article about Windows 8. Chris Pirillo **(1)**, of Lockergnome **(2)** fame, is featured. His videos are included in the piece showing everyday computer users first encounter with Win 8. One of the users is an information technology (IT) systems manager. The article **(3)** and videos are very revealing. Pirillo also has a video on the Lockergnome site that features Bill Gates views on Windows 8 **(4)**. I note that Gates talks about bringing Windows into the tablet and phone market. He seems to neglect that the operating systems designed for those devices are not on standard PCs. Even Apple **(5)** understands that touch screens are not coming to the desktop any time soon. It seems that Microsoft (MS **(6)**) wants to force an unnatural change on the PC market. I remember IBM **(7)** tried to do the same thing with the MicroChannel architecture **(8)**. They failed miserably. We'll see if MS can succeed where IBM failed. The Forbes article hypes a startup company that brings back the Start Menu to Windows 8. Pokki **(9)** offers the product for free. They also offer portable apps that can operate on a PC (some for free). The Pokki's start menu program is on the DVD of the Month. (It's a DVD because there was not enough room on a CD.)

1) http://chris.pirillo.com/
2) http://www.lockergnome.com/
3) http://sn.im/25p8z82

Con't pg 6

4) http://sn.im/25p8zc1
5) https://www.apple.com/
6) https://www.microsoft.com/
7) http://www.ibm.com/
8) https://en.wikipedia.org/wiki/Micro_Channel_architecture
9) https://www.pokki.com

Patrick Leahy, Senator from Vermont **(1)** and the guy who brought us the Protect IP Act (PIPA **(2)**), is at it again. He is the chair of the Senate Judiciary Committee **(3)**. He has a proposed amendment for H. R. 2471 **(4)**. The amendment would allow federal regulatory agencies to read anyone's e-mail without a warrant and would allow federal law enforcement agencies to do likewise under certain circumstances. If this bill with the amendment is passed, cloud services **(5)** will be stunted in their growth. Cloud services not only include storage but software, security, infrastructure, and platform as a service function. If government agencies can rummage pellmell through anyone's files, why would anyone trust a system that is tilted so radically against them? Business depends on secrecy of plans, design, direction, and methodology. The cloud cannot function without trust. The users must trust the providers for security, accuracy, and dependability. Government interlopers change that equation making adoption of this technology slower or non-existent. You can read more about this at CNet **(6)**.

1) https://www.leahy.senate.gov/
2) http://sn.im/25p8zfx
3) http://www.judiciary.senate.gov/
4) http://sn.im/25p8zjq
5) https://en.wikipedia.org/wiki/Cloud_computing
6) http://sn.im/25p8zmn

One of the things I detest about the vote on H. R. 2471 is that it will take place during the time period when Congress is least responsive to public opinion. In this case, during this week. The time period following an election until the installation of the new Congress is called a lame duck session **(1)**. Representatives and Senators that have not been re-elected or are retiring get to vote. They have no legal obligation to represent the views of their constituency. Moral obligation is another question that most Congress people have already answered in the negative. During a lame duck session anything can be passed. Because it occurs during the holiday period, almost no one notices these votes. The lame duck session should be abolished but too many monied interests have a vested interest in keeping it. Congress ignores the voters and vote for the money (as usual). Congress already ignores its constituency most of the time due the rule made in 1911 and never Constitutionally challenged in court. That rule stated that the House will have 435 members. The Constitution states in Article 1 Section 2, "The Number of Representatives shall not exceed one for every thirty Thousand, but each State shall have at Least one Representative;..." **(2)**. If the Constitution was followed, there would be about 10,380 members in the House. This may seem like an large number, but if you called your representative, they would listen because you became important to their re-election. You would be one out of 30,000 instead of the current one of 715,000. This would not insure that they would act in the interests of the voters, but it would make them harder to buy off. Illinois voters are represented in the legislature based on districts that have populations of about 109,000. This representative to voter ratio did

Con't pg 7

not stop them from passing the Build Illinois **(3)** and Illinois First **(4)** spending initiatives in the face of massive budget deficits and state employee pension shortfalls. Today we face the results of our reckless rulers.

1) https://en.wikipedia.org/wiki/Lame_duck_session
2) http://www.law.cornell.edu/constitution/articlei#section2
3) http://www.lib.niu.edu/1985/im851111.html
4) http://sn.im/25p8zra

I recently rented a movie from Redbox **(1)**. It was a comedy starring Will Ferrell **(2)**. Comedy aside, "The Campaign" shows the dark side of American politics that I described above. At $1.20 per day to rent, you can't get a better education. You may want to give it a try.

1) https://www.redbox.com/
2) http://www.imdb.com/name/nm0002071/

The United States and Israeli governments **(1)** created and disseminated the Stuxnet **(2)** computer worm to attack Iranian uranium centrifuges now has Chevron Oil computer systems as collateral damage **(3)**. Democratic Senator Dianne Feinstein's reaction was typical. She was upset with the 'leak to the media'. What about the ethical and moral depravity of governmental agencies waging cyberwar on countries that have not attacked us. Waging war without consent of Congress. Using taxpayer money developing a weapon that hurt innocent taxpayers. You would think that murdering Iranian nuclear scientists **(4)** would be enough, but no, our public servants must create weapons that attack us. Incidentally, The Flame virus **(5)** and the Stuxnet worm can reside on computers and other devices without affecting their operation. They specifically attack industrial systems. If they reside on a USB flash drive and that drive is inserted into an industrial control computer, the virus and or worm are activated. We have no idea how many other American corporations will be affected by the U.S. and Israeli cyberwar in the future. Using a good anti-virus product can prevent the spread of these types of weapons. I recommend MS Security Essentials **(6)**, a free solution. If you think you must pay for a good solution, try Node32 by eSet **(7)** or Kaspersky **(8)**.

1) http://sn.im/25p8zwr
2) https://en.wikipedia.org/wiki/Stuxnet
3) http://rt.com/usa/news/stuxnet-chevron-cyber-virus-348/
4) http://sn.im/25p8zzy
5) https://en.wikipedia.org/wiki/Flame_%28malware%29
6) http://sn.im/25p9038
7) http://sn.im/25p906n
8) http://usa.kaspersky.com/?domain=kaspersky.com

Throwing out old magazines recently, I came across the pricing of a 1.5 GB hard drive at $325 and a 23 GB hard drive for the low, low price of $3,500. The magazine date was 1998. Checking TigerDirect/CompUSA I find a 1.6 TB hard drive for $65 **(1)** and a 3 TB hard drive for $330 **(2)**. MicroCenter prices are comparable **(3)**. The smallest drive listed was 20 GB for $14 (refurbished **(4)**). The largest drive available was 4 TB for $250 **(5)**. Currently, any drive listings larger than 4

Con't pg 8

TB are actually a multiple drive network attached storage (NAS **(6)**) device. FYI, a 4 TB hard drive is 174 times larger than a 23 GB hard drive.

1) http://sn.im/25p90a8
2) http://sn.im/25p90fx
3) http://www.microcenter.com/
4) http://sn.im/25p90jv
5) http://sn.im/25p90or
6) https://en.wikipedia.org/wiki/Network-attached_storage

Adobe Flash player **(1)** has changed the way it is updated. The player requires that a browser be opened and the player downloaded from the site. Adobe **(2)** made a deal with McAfee **(3)**. On the site **(1)**, a prechecked check box gets you the "Free! McAfee Security Scan Plus check the status of your PC security" **(4)**. If you leave the check box checked, McAfee installs software on your computer. It puts an icon on your desktop. It takes up hard drive space. It nags you to buy McAfee virus protection. It uses memory space every time you start your machine. Every time Adobe Flash player is updated you are presented with the same check box. You must UNCHECK that box each time in order to be free of the McAfee nagware and conserve your computer resources. Adobe may be making some extra money but I personally do not like the tactic.

1) http://sn.im/25p90ro
2) https://www.adobe.com/
3) http://www.mcafee.com/us/
4) http://promos.mcafee.com/en-US/PDF/adobe_mssp_faq.pdf

Do you have a Mastercard **(1)**? They have a plan to incorporate a keypad and display into the card **(2)**. This is to increase the functionality of the card. It may show available balance before a transaction. It may be used as a calculator. Right now this is all speculation, but it is something to keep in mind.

1) http://www.mastercard.com/index.html
2) http://sn.im/25p90ux

Finally, for the good news with a dose of bad news on the side. I warned about extortion-ware scams in February 2010 issue of ARI... in Lamp Post 113 **(1)**. The Federal Trade Commission (FTC **(2)**) filed a complaint against the owners of one of these companies in 2008. A federal court granted an injunction against the company to prohibit them from operating **(3)**. The company was formed in Belize **(4)** but operates out of the Ukraine **(5)** with 600 international employees including the U.S. and India. Settlement with some of the owners was reached for about $8.4 million before a most recent ruling against vice-president Kristy Ross for $163,167,539.95. That number is the estimated loss by the victims of the scam **(6)**. Computerworld Magazine tipped me off to the story **(7)**. The bad news is that none of the victims will get a cent. If the government collects (not likely), the funds go to the government. I find it interesting that the order to cease was given in 2008 yet my clients were scammed in 2010 and 2011.

1) http://www.caeug.net/newsletters/2010/Feb2010.pdf

2) http://ftc.gov/
3) http://ftc.gov/opa/2008/12/winsoftware.shtm
4) http://sn.im/25p90xo
5) http://sn.im/25p910m
6) http://sn.im/25p913j
7) http://sn.im/25p9173

Happy Holidays!

Between you, me and the LampPost, that's all for now.

---

want to investigate the service you are using. If you are not sure if your email is encrypted, you can use a free service called Mail2Web at www.mail2web.com. To use it you simply click on “Secure Login” then put in your email address and password. (Make sure you don’t just click “Check Mail” which gives you an unencrypted connection.)

If you are not traveling, you still need to keep your guard up. I recently received a very real-looking email that was supposed to be from Order-update@amazon.com. Since I often make purchases at Amazon, this piqued my interest. The email said that my Amazon order had been successfully canceled and gave a link to the order in question as well as to Amazon’s website. I didn’t want any orders cancelled, so I read the entire email. Then I hovered my mouse over the two links that supposedly went to Amazon and found that they went to some other website. (This is a great way to check the links in an email. Just remember that you only put your mouse over the link rather than actually clicking on it).

Remember that if you come across these or any other suspected hacking or phishing schemes, you can report them to the FBI’s Internet Crime Complaint Center (ISC3) at www.ic3.gov. This website also has great information and alerts for the latest scams.

You will be amazed by the sheer number of crime schemes that are floating around the Internet. There is everything from Ponzi and Pyramid schemes to Internet Extortion. So check out this website. Just as in real life, you have to be aware of the pitfalls to keep yourself safe. It’s always good to follow the advice given by Sergeant Phil Esterhaus in Hill Street Blues. “Let’s be careful out there.”

Happy Holidays to ALL
From the CAEUG Board

November 2012
DVD of the Month

ARI - November/December newsletter
AVSAudioEditor - Edits audio files
cCleaner - Updated Hard drive cleaner
CDOMlists - Lists of past CDOMs
CloudMagic - Browser add-on for searching (registration req.)
DOSbox - DOS emulator
FetchYahoo - Script that downloads mail from a Yahoo! account
FreePops - Download mail from the most famous webmails via POP
FreeSizer - Tool to quickly create resized copies of your pictures
Gmelius - Removes all the ads present in Gmail (Browser add-on)
Gmvault - Backup and restore your gmail account
HitmanPro - Security software program protects your PC against malware
MemberContributions - Things e-mailed to me from members
OldTimeRadio - Old time radio broadcasts
ParetologicPCHealthAdvisor - Checks PC health and speed
PhotoMagician - Resize, convert format, add effects to images
Ping - CD image file to create a CD to backup and restore HD partitions
PokkiWin8StartMenu - Windows 8 start menu
RipBot264 - Rip Blu-Ray DVDs
ShrinkPic - Creates a smaller copy of images for e-mail
SimRecovery - Phone sim card recovery
SlimCleaner - cCleaner workalike with other features
Web2Pop - Get your web-based e-mail messages in your favorite e-mail client
Win7BackgroundChanger - Change the login screen background
YoSucker - Last good version to get Yahoo! e-mail POP for free
YPOPS - Open source software that provides POP3 and SMTP access to Yahoo! Mail

Meeting Location and Special Accommodations

The Glenside Public Library address is at 25 E Fullerton Avenue, Glendale Heights, Illinois. Please park away from the building. Thank you. The meeting(s) are not library sponsored and all inquiries should be directed to Mike Goldberg at. Individuals with disabilities who plan to attend this program and who require certain accommodations in order to observe and / or participate in the program are requested to contact CAEUG president, Mike Goldberg , at least five (5) days prior to the program, so that reasonable accommodation can be made.

Members Helpline
Any member with a specific expertise can volunteer to be on the Members Helpline.
Beginner Helpline
- Billy Douglas

Beginner hardware problems
- Dick Fergus

Hardware problems, XP, Win 7 & Linux
- John Spizzirri

CAEUG OFFICERS

President	Mike Goldberg
V.P. (Programs)	Roger Kinzie
Secretary	Al Skwara
Treasurer	John St. Clair
Newsletter Ed	Kathy Groce
Board Member	Billy Douglas
Webmaster	John Spizzirri