CAEUG Computers Are Easy User Group

Abort, Retry, Ignore....

Founded 1984 ARI is the Official Newsletter of Computers Are Easy User Group

January 2019

Volume XXXVII Issue 1

Confirmed meeting dates
:: ::
January 26 2019
Room A

February 23
Room A
9:15-11:45

March 23
Room A
9:15-12:15
:: ::
Mailing address:
CAEUG
P.O. Box 3150
Glen Ellyn, IL 60138
:: ::
MEETING PLACE is the Glenside Public Library
:: ::
Visitors Welcome
HOPE TO SEE YOU THERE!!

****

January 26, 2019 4th Saturday
Room A
Open presentations

REMINDER: $20.00 Membership dues for 2019 are due
See John StClair at the meeting or mail dues to
CAEUG, P.O. Box 3150, Glen Ellyn, IL 60138

****

Lamp Post 209

January 2019
by John Spizzirri

The U. S. Department of Justice (DOJ (1)) revealed the names of two Iranian crackers that used the SamSam Ransomware (2) to extort money from a number of businesses and governmental entities over the last few years. The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC (3)) identified the digital currency addresses of the crackers, a first for this department. Those addresses are 1AjZPMsnmpdK2Rv9KQNfMurTXinscVro9V

Table of Contents

and 149w62rY42aZBox8fGcmqNsXUzSStKeq8C. Together they contain 5,901 Bitcoin or the equivalent at today's value of about $23 million. As an individual, you probably do not have to worry about this situation. These crackers did their homework and only attacked large organizations that could pay significant amounts of loot. That is why OFAC has now made that a crime by placing sanctions on sending money or Bitcoin to those accounts or other accounts owned by the crackers named by the DOJ. Their names were added to the Specially Designated Nationals And Blocked Persons List (SDN (4)). This is a list of individuals and companies that U.S. citizens and companies are prohibited from dealing or doing business with. If you are ever hit with Ransomware and consider paying the ransom, you should check the list or seek the guidance of a ransomware incident response company like Coveware (5) or Sword & Shield (6). They do not accept individuals as clients. As I have said in the past there is no guarantee that any criminal will honor any commitment. Paying to get your data encrypted might not get it back. Always back up your data / hard drives in order to recover from criminal activities or disasters. I got this story from Bleeping Computer (7).

1) https://www.justice.gov/
2) https://www.us-cert.gov/node/11950
3) https://is.gd/INkJKr
4) https://is.gd/kidDhh
5) https://www.coveware.com/
6) https://www.swordshield.com/
7) https://is.gd/EOnKpJ

Mick Hedrick and others sent me this link. It is an interesting site that puts the demographics of Earth in perspective (1).

1) https://is.gd/XOvDno

I recently received the following e-mail at my business website email address helpme@johnspizzirri.com:

"ATTN: helpme@johnspizzirri.com

THIS IS NOT A JOKE - I AM DEAD SERIOUS!

Hi perv,

The last time you visited a p0rnographic website with teens, you downloaded and installed software I developed.

My program has turned on your camera and recorded the process of your masturbation.

My software has also downloaded all your email contact lists and a list of your friends

on Facebook.

I have both the 'Helpme.mp4' with your masturbation as well as a file with all your contacts on my hard drive.

You are very perverted!

If you want me to delete both the files and keep the secret, you must send me Bitcoin payment. I give you 72 hours for payment.

If you don't know how to send Bitcoins, visit Google.

Send 2.000 USD to this Bitcoin address immediately:

3EKGVncjV5ZmCB9fWyMsG2yHXGvYihHkfe
(copy and paste)

1 BTC = 3,580 USD right now, so send exactly 0.568690 BTC to the address provided above.

Do not try to cheat me! As soon as you open this Email I will know you opened it.

This Bitcoin address is linked to you only, so I will know if you sent the correct amount.
When you pay in full, I will remove the files and deactivate my program.

If you don't send the payment, I will send your masturbation video to ALL YOUR FRIENDS AND ASSOCIATES from your contact list I hacked.

Here are the payment details again:

Send 0.568690 BTC to this Bitcoin address:

3EKGVncjV5ZmCB9fWyMsG2yHXGvYihHkfe

You can visit police but nobody will help you. I know what I am doing. I don't live in your country and I know how to stay anonymous.

Don't try to deceive me - I will know it immediately - my spy ware is recording all the websites you visit and all keys you press.
If you do - I will send this ugly recording to everyone you know, including your family.

Don't cheat me! Don't forget the shame and if you ignore this message your life will be ruined.

I am waiting for your Bitcoin payment.

If you need more time to buy and send 0.568690 BTC, open your notepad and write '48h plz'.
I will consider giving you another 48 hours before I release the vid.

Anonymous Hacker"

The return address was debera554@a.anonymoushacked.ga. The top domain ga is the Republic of Gabon which is on the west coast of Africa south of Cameroon and Equatorial Guinea and north of the Republic of the Congo. Apparently, criminals from Gabon have been able to extort Americans using this poorly worded shotgun method e-mail. It is a shotgun method in that they obviously do not know me. I rarely use a PC that is webcam equipped. I do not accept Facebook friends. Some of the e-mail addresses I use have no contact lists. The result is this lying criminal has no helpme.mp4 video of me doing anything. The criminal demanded that I send him 2.000 USD. I guess in Gabonese that is two thousand dollars but to most Americans that reads two bucks. If any of you receive a helpme.mp4 video file in e-mail, please send it to me so I can include it on the DVD of the Month.

I came across this average income per state (1). I found these numbers hard to believe. I found the previous site when I found that in 20 states teachers (on average) make more than most Americans (2).

1) https://www.gobankingrates.com/?p=395593
2) https://www.gobankingrates.com/?p=623601

Last month Kim Komando (1) had an interesting article about emergency broadcasts now being available on the Internet (2). The site she cited was Broadcastify.com (3). I found many others. The one I found with local channels was Tunein.com (4).

1) https://www.komando.com/
2) https://is.gd/tYZz16
3) https://www.broadcastify.com/
4) https://is.gd/qM21jz

Recently, I have tried to help a couple of people that Microsoft Windows (MS (1)) product Activation have stung when they received a notice. They had used machines or refurbished machines. They received notices that Windows needed Activation even though the machine had been working well for months or years prior to the notification. Calling MS was useless. They had a pat answer. Pay for a license even though it had already been paid for. Thanks MS. I tried re-installing the OS in hopes that MS would recognize the machine and activate Windows. As you may recall, that

was the promise with Windows 10. There would be no need to call MS for a specific activation because MS would have a database of all activated machines. If a machine had to have a new hard drive because of drive failure or upgrade the activation would take place automatically. That, obviously does not always work. Getting through to the MS employees that the MS data base may be flawed is like talking to a wall. The Windows 10 Forum covers a number of incidents similar to the ones I have encountered (2). ZDNet also wrote about what they call the Activation Bug (3). When ZDNet got involved, a spokesperson for MS, Jeff Jones, "senior director" said they were looking into the problem. That was last November (2018). The MS web site addressed the issue (4) telling users that it would be fixed by itself. That was a lie. The people I helped had to have the OS re-installed as Windows stopped working for them. As far as I know, the problem has yet to be solved.

1) https://www.microsoft.com/
2) https://is.gd/fsqObN
3) https://is.gd/v6p4Ld
4) https://is.gd/5TjTzI

If the activation problem affects you, you may want to get a copy of Windows so that you can re-install the OS. You can get that copy at the MS site (1). You have to answer some questions, but that is not a problem.

1) https://is.gd/f2Kz4g

Splashdata (1) published the 100 worst passwords of 2018 (2). These passwords are the most likely to get you hacked. I came to the Splashdata site by reading BRG (3) site which listed the top 25 worst passwords. Here they are; 123456, password, 123456789, 12345678, 12345, 111111, 1234567, sunshine, qwerty, iloveyou, princess, admin, welcome, 666666, abc123, football, 123123, monkey, 654321, !@#$%^&*, charlie, aa123456, donald, password1, qwerty123. Please, DO NOT USE THESE PASSWORDS.

1) https://www.teamsid.com/
2) https://www.teamsid.com/?p=3793
3) https://wp.me/p2sPFm-nLEB

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

Have you taken control of your passwords yet?

By John Fair
Smartphone & Tablet leader, Computer Users of Erie, PA
December 2018 issue, CUE Newsletter
www.cuerie.com
grimcyber (at) yahoo.com

CUE's April and May 2018 General Meeting Programs addressed passwords, two factor authentication and password managers. More than half of CUE's

Con't pg 6

members missed one or both of these meetings and some who attended may not yet have taken seriously the suggestions made in these presentations. I am so passionate about this subject I wrote this article to give you a second chance.

No one can guarantee you will never be hacked, however there are published guidelines that I'll summarize that can minimize the risk. Only you can decide what to do with these recommendations. First, create strong passwords. This is not easy. We have repeatedly been told to create unique passwords combining numbers, special characters, upper- and lower-case letters. Complexity or randomness is good but you can add strength by making your passwords longer - as long as the site allows. Consider pass phrases or a collection of random words but remember that hackers have access to databases of song and book titles, lyrics, poems, etc. so randomize what you use.

Second, treat your email password with special care. Make it as strong as you can and never use that password or a variation of it for anything else. If hackers gain access to your email they can use it as a key to resetting passwords of your other accounts thus locking you out.

Stop thinking of hackers only as the lonely figure in a hoodie crouched over a laptop in a dimly lit room. Hacking is also done by businesses employing many folks using lots of computing power and large databases to try to separate you from your personal information and hard earned cash. They buy and sell information from data breaches and scour social media and public databases to use in their pursuits. This realization might spur you to take more seriously protecting yourself online.

Never reuse a password! If you do, your security is only as good as the weakest site on which that password is used. It's easy for a hacking program to test one stolen password on all of your sites. And slight variations of that password (add a number) or simple substitutions ($ for s) still make it easy to guess. Don't use as passwords what has become public information because of social media (pet names, birthdays, family names, addresses, phone numbers, etc.) or what can be found in public databases. They are easy guesses for hackers. And, of course, passwords that are user names, simple dictionary words, adjacent keyboard combinations, etc. make it too easy for hacking schemes. Perhaps it should go without saying, don't keep a file containing your passwords on your computer. That list of passwords you keep in writing is a bit safer if inconvenient to update.

Why do we violate good password guidelines? The National Institute for Standards and Technology (NIST) had issued password guidelines we have all been following for the last 15 years. Use at least 8 alphanumeric characters sprinkled with capitals and special characters and change passwords every three months. The unintended result of this complexity was that most people gravitated toward common patterns and hackers exploited these predictable patterns. One author of the original guidelines described the results of imposing these arbitrary rules: "It drives people bananas and they don't pick good passwords no matter what you do."

Con't pg 7

NIST's newly released password guidelines are more user friendly, requiring only what significantly improves security, putting more burden on the verifier and using 2 factor authentication where possible. Longer passwords are better. Further, they recommend you change passwords only in the event of a data breach. Arbitrary complexity that drives poor practices shouldn't be required. The verifier should screen for and not allow commonly used passwords, eliminate the need for hints and security questions and limit the number of incorrect guesses allowed. You might find that verifiers are a bit slow to adopt their end of these guidelines because of the cost involved.

Because of the number of passwords people (should) use and the complexity of each one, security experts now suggest considering the use of a password manager.

Password managers store your passwords and other information in an encrypted vault, either on your computer or in the cloud, that is accessed by a single VERY STRONG master password that is encrypted and never stored in plain text.

They can generate complex, random passwords of any length for you to use on any site. They work in conjunction with your browser and can autofill username and password for sites you have chosen.

Most have a subscription fee of from $12 to $40 a year, but a few have a limited function version for free. While Wikipedia lists over 30 password managers on the market, most experts suggest staying with one of the top four: LastPass, Dashlane, 1Password or KeePass.

I purchased 1Password before they moved to a subscription-based service and am grandfathered in using it. I found it relatively easy to use, love the excellent security ratings and have it on my Mac, iPad and iPhone. However, if you choose to follow security experts recommendations and give a password manager a try, you might want to avoid paying even a nominal subscription fee in the beginning until you understand what additional features you might need that you must pay for. I suggested giving LastPass a try since the free version does what most folks want from a password manager and, since it is cloud based, can synchronize across computer, smartphone and tablet. It is also very highly rated for security.

If you think LastPass might be of interest, first review their website for information and user forums. That will help you to understand how LastPass might be of value to you. If you want to try out LastPass, STOP!! Don't take any action until you have devised a very strong master password. The LastPass website will offer guidance in how to do that but note that you can use a very long master password and you could take advantage of the security that will offer. One way to generate a long but memorable master password is to use four or more random, unrelated words separated by spaces. To understand the logic behind this just Google "correct horse battery staple."

Con't pg 8

Really. You want a master password that is easy to remember so that you can access your password manager vault without consulting a written password.

Think this through before you download and try any password manager. You want a master password you will never forget since the password manager company does not store an unencrypted version of your password and thus will not be able to help you recover your vault contents if you should forget your master password.

If you are at all nervous about using a password manager, do not put your banking information or email password in it. I have not. You will see a real benefit from using it for all the rest of your passwords. I have also used 2 factor authentication in LastPass. That gives me the additional convenience of using my fingerprint on my iPhone and iPad to open LastPass since they are identified as trusted devices (the second factor).

Currently there are three authentication factors used to prove your identity in the digital world. One factor is username, password, PIN - something you know.

The second factor is something you have - ID badge, smart card, device (phone, tablet, computer). And the third factor is something you are - biometric factor such as fingerprint, facial recognition, iris scan.

Using at least two of these factors provides more proof of your identity and is one of the new NIST recommendations for digital security.

Using a password manager requires some setup time. When you log in to a new site LastPass will ask if you want to save the login information (username and password) and that is very convenient. What is not convenient is changing the passwords you currently have to much more secure ones. You will have to go to each site or app and change its password.

LastPass will suggest complex, random passwords you would never remember, but the password manager will. Think about all the passwords you have and the time it will take to log in to each site or app and go through the process to change the password. This effort is what limits most people in the use of a password manager. But if all you do is institutionalize your poor password practices by saving your existing poor or repeated passwords, the password manager will do you no good. You need to make all those passwords stronger - that is the point of having that password manager: to allow you to use individual passwords that are so complex you could never remember them. You don't have to change all your passwords at one time, just start with the most important ones and work on them gradually.

Password managers can also encrypt and store other information that is convenient to have such as passport, drivers license and credit cards. I have entered all this information including the phone numbers of the credit card companies if my cards are lost or stolen. This has replaced the (insecure) scanned paper copies that I used

Con't on pg 9

to carry with me when I traveled.

I can't end this article without mentioning that Apple has made using password mangers easer on smartphones and tablets using iOS 12. That mobile device operating system now supports autofill in Safari and third-party apps if you are using LastPass, Dashlane or 1Password. And it makes using password managers very convenient when you are out and about.

No more list of passwords tucked into my iPad case. How insecure was that! Android Oreo and Pie operating systems support autofill with LastPass but older versions do not. Adoption of new Android operating systems is far slower than new versions of Apple iOS so Android users will be limited in their convenient use of autofill. Browser extensions of LastPass on your computer provide autofill as well as the option to fill in forms online including your credit card number. I like and trust password managers but not enough to automatically fill in my credit card number on a form whose origin may not be as trustworthy. 1Password at least requires you to acknowledge you want to fill in a credit card number, an extra step to verify that you are comfortable doing so.

I cannot guarantee your online safety nor can I guarantee your password manager can never be hacked. I don't think you would use "Password123" as your master password but in the event, you do, all bets are off. You can, however, reduce the risk of bad things happening by carefully using a password manager with a strong master password.

Tech Talk
Cure desktop clutter

By Joe Isaac
Tech Talk, Central Kentucky Computer Society
September 2018 issue, CKCS Newsletter
www.ckcs.org
joeisaac1234 (at) gmail.com

If you have more than four rows of icons on your desktop, you probably have too many for efficient use. Desktop icons should only be something used often. The icon idea is to put a program or project up front, so you don’t have to spend a lot of time looking for it. Quick access is the key! If you have several dozen icons there, the ability to find something quickly is much less likely. We usually start with just a few, but they tend to grow in number as we install a new program. Every program writer thinks his/her program is the absolute most important one, so they hang another icon on your desktop.

So here is what I recommend you do. Look over the icons on your desktop and identify the ones you haven’t clicked on in weeks or maybe months. Right click somewhere on your Desktop. Select NEW, then click on FOLDER, name the new

Con't pg 10

folder Misc. or Stuff. Then hit Enter.

Now, left click and drag your least used icons into this one folder. Leave only the frequently used icons in view. Those rarely used icons are still available to you should you need one of them.

Get to work! You will be glad you did!

January 2019
DVD of the Month

ARI - Monthly newsletter
AudioBook - Free audio book
AvastClear - Completely remove Avast anti-virus software

Boxoft - Optical character recognition software
Calibre - Updated e-book file reader
cCleaner - Updated drive / registry cleaner / utility

DesktopOK - Restores desktop icons to original positions
Dooble - Updated web browser
DVDOMlists - Contents of CDs and DVDs of the Month

Exodus - Bitcoin wallet software
EZPaint - Paint replacement

IcecreamPDFeditor - PDF editor
LinuxReader - Allows Windows to read Linux HD partitions

MemberContributions - Things members send me
OldTimeRadio - Old radio audio files
PasswordCracker - Allows reading passwords behind screen asterisk or dots

SimpleOCR - Optical character recognition software
Teamviewer - Updated remote control of other computers software

VirtualBox - Updated virtual environment for other OSs
VLC - Updated media player
Waterfox - Updated web browser

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.

Mailing address:
CAEUG
P.O. Box 3150
Glen Ellyn, IL 60138

Members Helpline

Any member with a specific expertise can volunteer to be on the Members Helpline.

Hardware problems, Win 7, Win 10, Linux and Virus Removal
- John Spizzirri

CAEUG OFFICERS

President Mike Goldberg
president(at)caeug.net

V.P. (Programs) Roger Kinzie

Secretary Al Skwara

Treasurer John St. Clair

Newsletter Kathy Groce

Board Member Frank Braman

Webmaster John Spizzirri
webmaster(at)caeug.net