SUPERCOM COMPUTER CLUB TECH TIMES

Volume 06 January 31, 2017

Objective:

To bring the latest technology news to you, our members. Tips and suggestions will help you to keep your device(s) running smoothly and help you be aware of threats. Technical tips will be coming to you through our Technical Committee.

Committee Members: (Pictured Below)

Ben Tarbell, Mike Gerkin, Jim Oliver, Peggy Bullock, Jim Mills, Rick Heesen, Lowell Lee and Steve Andreasen (Apple/Mac).

Dick Strong is on “time off” for season 2016-2017.

Greetings

I thought we were going to stretch into the first of February before sending out another newsletter to our membership, but there is way too much happening both in the club and the hacker’s world. We strive to be diligent in keeping you all informed on what is happening. Sometimes we could make that a daily task.

Of special note from our Executive Board if you were not in attendance last Friday, January 27, 2017:

Proposed changes to the By-Laws of the SuperCom Computer Club were announced at the meeting in accordance with the bylaws. It was made 7 days prior to the meeting to vote on these changes. The following are the proposed changes:

The Board is proposing two changes to our SuperCom Computer Club by-laws. According to the by-laws individual members shall be notified of the proposed amendments at least seven days prior to the called meeting. The proposed amendments are as follows:

Change in Article IX

One third (1/3) of the paid up members

-to-

One fourth (1/4) of the paid up members

Change to the wording in Article V Section 3

Associate membership may be granted to non-residents of SSLRVR only if they were members prior to April 1, 2010 and upon payment of such dues and/or assessments as are set for Associate Membership by the Executive Board. Associate Members may not serve on the Executive Board and have no voting privileges.

-to-

Associate Membership may be granted to non-residents of SSLRVR with paid consecutive membership and upon payment of such dues and/or assessments as are set for Associate Membership by the Executive Board. Associate Members may not serve on the Executive Board or be Chairman on any Board.

These changes are posted on the SuperCom bulletin board. The current by-laws are included in our SuperCom web site. Please check there, Website to further study the changes. We will hold a meeting of the members next week, February 3, 2017, to vote on these changes. This notification fulfills the seven day prior notification requirement.

****

From Mike Gerkin:

BACKUPS:

We have sent to you this year some suggestions on how you can keep your computing device in top condition. One of the key items we shared with you is the importance of having a backup of your important data, programs, and system.

Doing regular backup is neither complicated nor difficult. I do it regularly. Maybe it would help you understand more about how to replicate your information in a usable form if I simply told you how I approach protecting my computer and data. You can decide for yourself just how you should apply a backup philosophy to be effective for yourself.

I use a combination of software and hardware tools to make backups. It might be more or less than you choose to do, or you might adapt it for your own backups. Here are the tools and techniques that I've chosen to use for backups.

My personal backup strategy is to make a **full Image backup** (also called a drive image) the first of every month. That means, at best I could be one full month out of date in relationship to the current status of my computer if it crashed. I find that acceptable. I could do weekly or daily backups to reduce the out-of-date time. I could do more frequent **incremental backups** between my monthly backups to catch just any new or changed files. The full image file is stored on an external hard drive. I'm currently using separate 500GB or larger external drives for each of my family computers.

It is done manually, not scheduled, using Acronis True Image software. I usually keep **three revisions of monthly files.** This affords me more than just the latest month's backup.

I also subscribe to a Backup Your Backup philosophy. So in addition to making monthly backups on my external hard drive, I copy some important files, such as my Documents files, to a larger capacity flash drive. Some people store their backup offsite like at a friend's house, or even on the cloud over the Internet to offer another level of protection.

Whatever form of backup or which software or hardware suits your needs is what you should choose, but you should do backup, or one day you will say that you wish you had!

****

Kim Komando has been actively sending out advice more and more. Sometime I am afraid to open her newsletters! I also received an email from our last Friday's presenter, Ron Brown, verifying one of her recent articles regarding Gmail users.

Here is one article about how Malware strikes Google Chrome users with tricky new technique

Another article: Even tech-savvy Gmail users are getting fooled by this phishing scam

BUT – there is good news for Gmail users too……

Gmail is about to get its best new security feature in a long time

Chris Smith @chris_writes January 26th, 2017 at 11:39 AM


SecurityImage Source: Shutterstock

Malware attacks often creep in via email, as attachments that unsuspecting users open on their work and personal computers. These malicious programs can potentially unleash hell on those machines in the process. Google is now looking to make Gmail even safer when it comes to malware attacks by adding a new feature that blocks any JavaScript that would otherwise hit your inbox.

Google already blocks certain file types that can execute programs on a computer, including .exe, .bat, and .msc files. But starting February 13th, Gmail users won't be able to open .js files from Gmail. In fact, Google will not even let you receive JavaScript attachments anymore.

A warning telling you that some files are blocked will pop up, and you won't be able to attach a .js file to an outgoing email in Gmail no matter what you do. You can't even archive it. Google will detect .js files in archives including .zip, .tgz, .gz, and .bz2 files, so there's no point trying.

Naturally, if you have genuine reasons to share .js files, you still can do it, but you'll have to go through Google Drive instead of attaching them to Gmail emails.

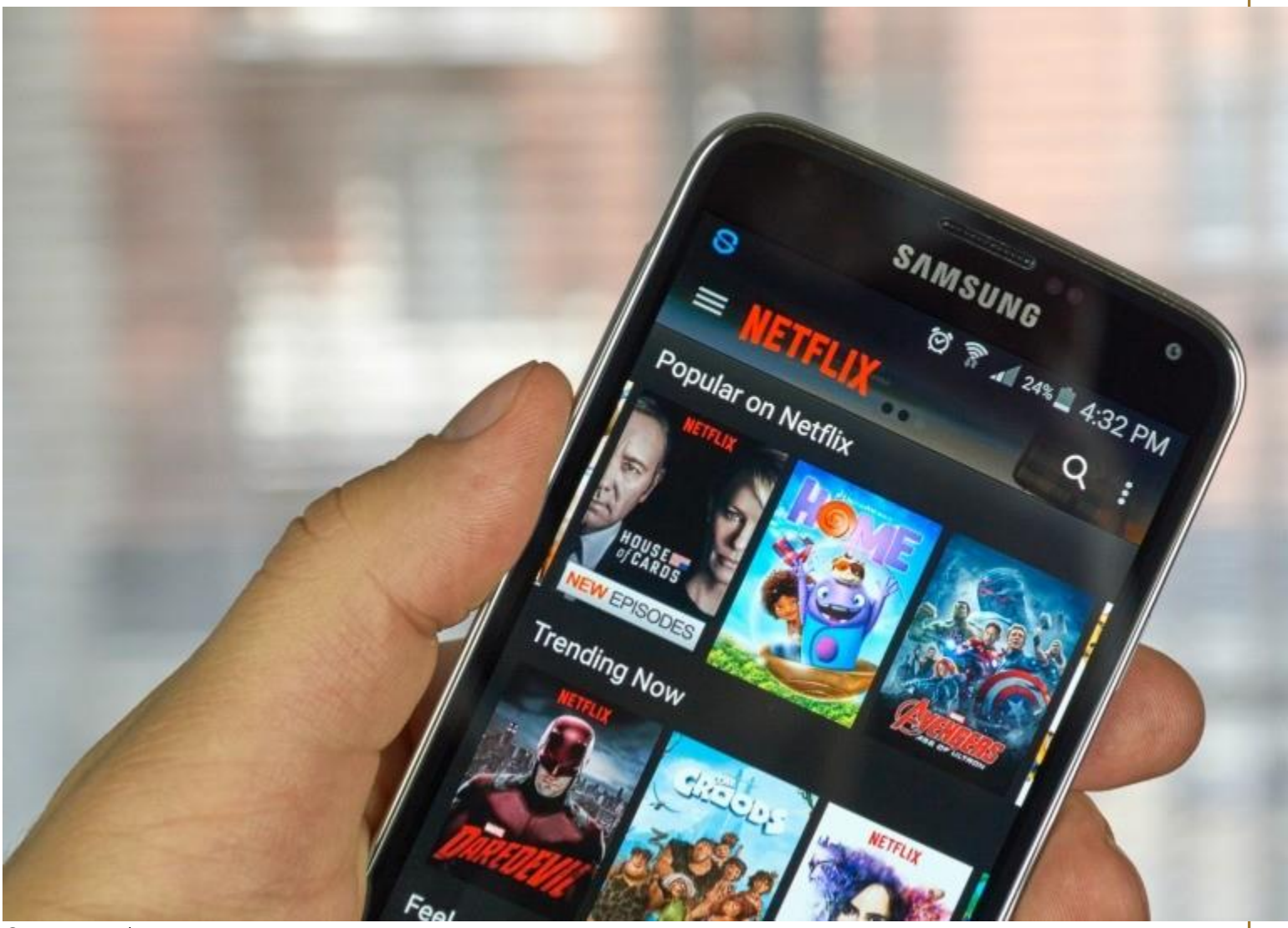
The worry with JavaScript attachments is that they can open the door to severe malware attacks, including ransomware. The malicious .js files might not do any harm by themselves, but they can act as downloaders for other programs that could lock you out of your computer or install other malware.

It's great to see Google strengthening Gmail security, especially in light of the fact that hackers continuously come up with more sophisticated attacks. Just recently, Gmail users discovered a pretty scary phishing attack that's able to fool even some of the savviest Android users into handing hackers their Google account credentials.

Here is another Kim Komando warning. I've included it here, just in case you don't want to take the time to click on the safe link:

Warning! Fake Netflix app lets hackers read your texts and take X-rated pictures

By Mark Jones, Komando.com



© Dennizn | Dreamstime.com

Cybercriminals are always on the attack, looking for new ways to rip us off. That makes it more important than ever to keep your guard up to try and stay ahead of these thieves.

One thing fraudsters especially like to do is target people who use popular sites and apps. That's why you need to know about the latest Netflix scam.

Researchers with Zscaler recently discovered malware hidden inside a fraudulent Netflix app. This fake app was created with the SpyNote Trojan builder, which first appeared on the Dark Web in 2016.

How this Netflix malware impacts you

After downloading this fake app, an icon that looks like the real Netflix logo appears on the victim's gadget. When this icon is clicked, the logo disappears, making it seem like the app was removed from the device.

What's actually happening is, a Remote Access Trojan (RAT) is installed. RAT malware allows a hacker to take over your gadget completely.

The scammer can copy files from your gadget and send them to its Command and Control (C&C) center, view a list of your contacts and steal all of your text messages.

Even creepier is the fact that they could activate the gadget's microphone and listen in on your conversations. They could also take pictures or screen captures without you knowing about it.

The criminal is able to execute commands from the victim's gadget. This means the thief can uninstall apps, along with antivirus protections, from your device. This makes it more likely the malware will stick around on the infected gadget.

This fraudulent app was not found in the Google Play Store and has nothing to do with the legitimate Netflix app. It was only available in third-party app stores for Android users.

The malware has only been discovered in the fake Netflix app, as of now. Zscaler researchers say this threat could expand to others in the very near future.

If you want the Netflix app, make sure it does not come from a third-party app store. That is too much of a risk.

How to avoid malicious apps

Here are some ways to avoid being infected by a malicious app:

- **App stores** - Stay away from third-party app stores. There have been a few examples of malicious apps in the Google Play Store and Apple's App Store, but they are very rare. Third-party app stores do little vetting of apps, making it easier for scammers to spread malware there.
- **Check the apps' developer** - Verifying the name of the app developer is important. Copycat apps will have a different developer's name than the actual one. Before downloading an app, do a Google search to find the original developer.
- **Reviews** - Most of the popular apps will have reviews by other users in the app store. You can sometimes find reviews by experts online. These are helpful at pointing out malicious or faulty apps. If you find a review warning the app is malicious, do NOT download it.
- **Update your gadget** - Make sure that you have downloaded the latest security and operating system updates. These updates usually include patches to help protect your device from the most recent threats.

****

Sometimes when we see something in big print & pictures, we take more notice. With so many gadgets that access the Internet and Websites, we need to be extra vigilant. The above are some very good tips!

Friday Morning Presentations coming up:

February 3	LastPass Passwords & Cloud Storage	Ben Tarbell
February 10	Annual Meeting Security Programs	Rick Heesen
February 17	Download & Play Games	Bev Hooper
February 24	Q and A	Tech Committee (Geeks)
March 3	Winners of Photo Contest	Carol Heesen
March 10	Google Maps (Tentative)	Rick Heesen

****

CLASSES

Friday morning meetings (9:00 AM in Ballroom) are an opportunity to find out about the classes being offered and sign up for them.

You can visit the Club's website at supercomcomputerclub.weebly.com for more details on the classes currently running.

Keep your eyes and ears open because more classes will be added soon.

****

SIGs (Special Interest Groups)

These meetings are facilitated by a club member. It is an opportunity for like-minded club members to gather and ask questions to learn more about the particular area of interest.

Current SIGs running in January are – iPad, Windows 10, Android Phones, iPhones and Facebook. **See the website and/or bulletin board for additional information on when and where they meet.**

****

OPEN LABS

A reminder of dates for **February Open Labs:** Feb. 3rd, 17th and 24th. These are opportunities for the club members to bring their computer to the Lab to have a member of the Tech Squad help them with something that does not work correctly or some change they need made.

****

A reminder of the Photo Contest. Here are the Entry Guidelines, Contest Categories and Important Dates:

3rd Annual SuperCom Photography Contest

Entry Guidelines

- Photographer must be a current member of the SuperCom Computer Club (bring your membership card when you bring your entry).
- One entry per category in up to two different categories. No more than two entries per photographer**.**
- Entry must be an 8" x 10" unframed, unmated print.
- Place each 8 x 10 unframed entry in a separate envelope labeled with your name, space #, phone number, the title of your image and the category you are entering. Do not put any identifying marks on the image itself.

Contest Categories

- Landscapes
- Manmade structures
- Living things (i.e. People, Animals, Bugs, Fungi, etc.)
- Amazing Arizona

Important Dates

• January 6th, 20th	Call for Entries
• February 3rd & 10th	Contest entries accepted in Hopi Room immediately after the SuperCom meeting
• February 13th	Voting open to all park residents
• February 27th	Voting closed
• March 3rd	Winning entries announced. Please plan to attend this meeting if you submit an entry.
• March 10th	Non-winning entries can be picked up after computer club meeting.

Winning entries will be framed and remain on display until the completion of next year's contest.

Important Note: PLEASE do NOT share with others which photographs are yours. Let your image win or lose on its own merit!

Remember, this newsletter is just one of our ways of keeping in communication with our members. Check the Bulletin Board in the Hallway by the restrooms, check the Website (www.supercomcomputerclub.weebly.com) and attend meetings to hear some great programs.

From Mike, Ben and Peggy