ISSA Information Systems Security Association Rochester Chapter

Q3 2015 Newsletter

ISSA Rochester News

Chapter of ISSA International
www.rocissa.org

Past Events:

We have had several events over the past few months including a social "engineering" event with GreyCastle in July and a very lively talk from Bit9/Carbon Black in September.

GreyCastle setup a live "iSpy" game for attendees at our July social gathering, giving the most observant attendees a free drone! Free food, drink and fun were shared by all who could make it.

September's Chapter meeting brought a great presentation by Chris Meile from Bit9/Carbon Black called Modern Threats Require Modern Defenses. Dinosaur BBQ and good conversation was had with everyone!

Upcoming Events:

Chapter Meeting

We have several meeting topics lined up for the next few months!

Oct – Rochester Security Summit (Register Now!)

We are still planning for November, December and January, but check out website (www.rocissa.org) for details of upcoming events like chapter meetings, social events and educational seminars!

If you have an idea for a meeting, or any suggestions or comments on past meetings for events please let us know at membership@rocissa.org.

Need CPEs?

- Attend an ISSA Chapter Meeting
- Speak at RSS or a chapter meeting
- Volunteer for a committee
- Write a journal article

Membership:

We have 78 chapter members currently and are always looking for more. This is the highest member count we have had in several years, showing the board that we are moving in the right direction.

We strive to provide value to our members and the security community at large. If you have an idea for a chapter meeting, social gathering, or other event please contact membership@rocissa.org.

Remember we are here to help you! So please let us know what you want and we can hopefully tailor our events to fit the needs of our members.

Communications:
Have an article you really enjoyed or are you writing an article you really want to share with everyone? Send it to info@rocissa.org and we can put it in the newsletter!

Have a question you really need help with? Join us on LinkedIn and start a discussion in the ***Rochester Chapter Information Systems Security Association*** group.

Rochester ISSA is now on twitter. Check us out at @RocISSA and stay up on the latest infosec news.

Elections:

This December we will be holding our annual elections. Please be on the lookout for emails from our independent Elections Committee (or volunteer to help with the committee!), for not only your opportunity to vote, but also to run.

We are always in need of fresh faces and ideas for the board, so please consider running for one of our many positions (President, Vice President, Secretary, Treasurer, Web Master, Communications and Membership).

What we're reading…

Held Hostage By Ransomware
Very few of us in the infosec field have not gotten the dreaded phone call from a user, "Hey! There's a screen on my computer asking me to send them Bitcoins if I want to unlock my files. How do I use Tor?" You want to reply, "Your data, my friend, is being held hostage by the bad guys. Kiss your files goodbye!"

Ransomware is a particularly nasty form of malware that goes through and encrypts your files--typically documents, spreadsheets, and pictures--and then demands payment in order to decrypt them. Early versions of ransomware would simply delete the original files before writing the newly encrypted versions onto the drive. This allowed tech-savvy folks with forensic tools to recover the deleted files without paying the ransom. It was not long before the ransomware started shredding the original files so that no recovery (outside of purchasing the decryption key) would be successful.

Here are a few tips for dealing with a ransomware outbreak:

1. Maintain good backups(off-net). Tape backups are still an excellent way to preserve data. If you do disk-to-disk backups, make sure that users cannot write to the share containing those backups. For home computers using an external drive for backups, be sure to unplug it when not in use. Ransomware will happily encrypt your local drive as well as any other external drives it can find.

2. Avoid open file shares. Having wide-open shares where all of your users can write data is just begging ransomware to ruin your day. Limiting access and permissions will also help limit the damage in the event of an outbreak (and is also good security hygiene).

3. Block end users from being able to execute malware. If you prevent files from being run from the user's %AppData% directory, you will prevent a majority of downloaded threats from being launched. Many security tools, such as antivirus, support similar application and device control policies that do much the same thing.

4. Perform content filtering. Malicious attachments are no big deal if they are stripped on the way in before arriving in the user's mailbox. Be sure to scan for known threats and block common malicious attachment types (.exe, .com, etc.). For even better results, filter outbound requests as well as inbound.

5. Educate your users. Awareness is the best defense -- let them know not to open suspicious e-mail messages. Better yet, show them what common things to check in order to make sure that a message is legit.

For those of you interested in a deeper technical dive into the world of ransomware, be sure to attend Nick Bilogorskiy's presentation entitled, "Dissecting CryptoWall," at the Rochester Security Summit in October.

Provided By Rich Savacool

Other Articles….

The Inside Story Behind MS08-067

By John Lambert**:** http://bit.ly/1KDKssM

Microsoft Explains Windows 10 Privacy Policies

By Kelly Sheridan: http://ubm.io/1RdYrru

The 'Remediation Gap:' A 4-Month Invitation To Attack

By Ericka Chickowski: http://ubm.io/1h8N8E9

Google, Others Seek to Make Cybercrime Costlier For Criminals

By Jai Vijayan: http://ubm.io/1KFOgK5

Dissecting Powershell Attacks

By dfirblog: http://bit.ly/1JB8Nvm

Rochester Security Summit 2015

Tuesday October 6th and Wednesday October 7th

Hyatt Regency Rochester

www.rochestersecurity.org

We are currently sold out. But look for highlights in the next quarter end newsletter!