ISSA Information Systems Security Association Rochester Chapter

Q1 2016 Newsletter

ISSA Rochester News

Chapter of ISSA International
www.rocissa.org

Past Events:

On January 27th, **GreyCastle Security** sponsored a chapter meeting and Happy Hour at Mulconry's Irish Pub in Fairport. GreyCastle announced their soon to be open Rochester Office at the meeting. Fun was had by all at the first chapter event of the new year.

February's ISSA Chapter Meeting was hosted at **Systems Management Planning (SMP)** office in Henrietta. A great presentation on SSL Air Gap and NFV Firewalling in OpenStack was a great draw, along with another fun Happy Hour. We would like to thank SMP for not only providing exceptional content, but a very nice venue for the event.

Upcoming Events:

Chapter Meeting

We have several meetings in the works for the next few months!

April 13th – Bruce Oliver!

Check our website (www.rocissa.org) for more details as the dates draw near!

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

News and Notes

The news has been flooded recently with stories of ransomware infections across many different industries. While ransomware is nothing new, the problem has not gone away. Attackers keep getting smarter and organizations continue to struggle with how to stop these attacks.

A lot of conferences feature famous speakers who preach about information sharing and how that can solve all of our problems. The more I talk with other security professionals the more I see that all this information sharing only helps us if we have the proper infrastructure and tools in place to automate all these information sharing feeds. IP addresses of Command and Control servers, or other indicators of compromise come at us from all different directions and consuming those is a full time job, let alone all the other projects we are all tasked with on a daily basis.

While the information sharing and IOCs are great for detecting a breach, they are not much help unless you can take data and immediately take action to prevent an attack.

There are very few options to fight these types of attacks, whitelisting applications, strict SPAM filters, knowledgeable and proactive employees and strict web filtering seem to be the only ways to help protect our organizations, and some of these just aren't feasible.

While I don't have a hard and fast answer, take a look under **What we're reading** at some of the articles that hopefully will provide some low cost but practical solutions to ransomware like Locky.

While information sharing of IOCs may not be extremely valuable in these types of attacks, it is still important for all of us to keep an open dialog with other colleagues in an attempt to share ideas to thwart these attacks with the tools we already have. May be this means getting more involved in a SIEM user group, joining the Rochester ISSA LinkedIn group or an organization like FS-ISAC. As an officer for the Rochester ISSA we strive to bring people together, so if you have any suggestions on how we can better facilitate these conversations please let us know!

What we're reading…

Proactively Reacting to Ransomware

By FreeForensics.org**:** http://bit.ly/1RqtyCt

Abusing bugs in the Locky ransomware to create a vaccine

By Sylvain Sarmejeanne: http://bit.ly/21K7nZx

Two more healthcare networks caught up in outbreak of hospital ransomware

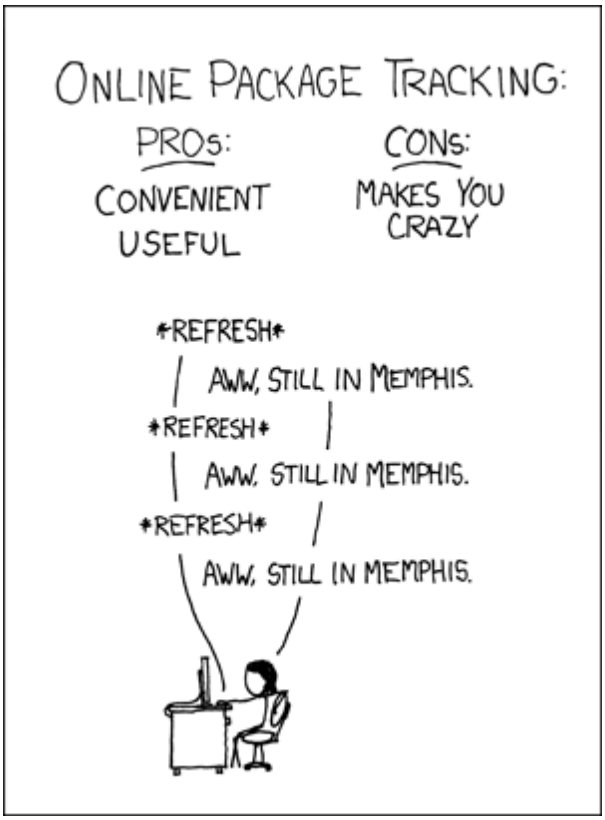
By Sean Gallagher: http://bit.ly/1Y0nTU6

FBI Cracks Terrorist's iPhone – Sans Apple

By Kelly Jackson Higgins: http://ubm.io/1V4y4Yw

Dangerous New USB Trojan Discovered

By Jai Vijayan: http://ubm.io/1RFZp0O



Source: xkcd.com

Membership:

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.