Volunteer Opportunities

Colleagues,

Our 5th Annual Cyber Focus Day is complete, with about 200 attendees joining us this year. Additionally, Fox21 News covered the event, with news reporter Sarah Ferguson spending an hour with us. She interviewed ISSA Colorado Springs members Art Cooper and Shawn Murray, and the coverage was aired on Fox21 News. It's also available online at this website: http://www.fox21news.com/news/local/pikes-peak-community-college-hosts-cyber-focus-day/1088064875. Be sure to check it out!

Thanks to everyone who attended, helped plan the event, and helped throughout the conference!

Planning is already in progress for upcoming events, and we could use your help. We need to build up our Sponsorship and Events Committee to help us plan and organize conferences, the technology days at Ft Carson and Peterson AFB, and our Professional Networking event. If you're interested in helping with any of these events, please let me know (president@issa-cos.org).

We also could use some help organizing our Mini-Seminars. Mini-Seminars are held on a Saturday morning, from 9am to noon, about seven to eight times each year. You'll receive three CEUs/CPEs for every mini-seminar you organize and attend. If you'd be interested in joining our team of organizers for training events, please let me or our Training leads (training@issa-cos.org) know.

The ISSA Colorado Springs Newsletter incorporates open source news articles in compliance with USC Title 17, Section 107, Paragraph a (slightly truncated to avoid copyright infringement) as a training method to educate readers on security matters.

The views expressed in articles obtained from public sources within this newsletter do not necessarily reflect those of ISSA, this Chapter or its leadership.

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our members, and do not constitute or imply endorsement by ISSA or the Colorado Springs Chapter of ISSA of any entity, event, product, service, or enterprise.
Facebook scraped call, text message data for years from Android phones

By Sean Gallagher, Ars Technica, March 24, 2018

[Update, March 25, 2018, 20:24 Eastern Time]: Facebook has responded to this and other reports regarding the collection of call and SMS data with a blog post that denies Facebook collected call data surreptitiously. The company also writes that it never sells the data and that users are in control of the data uploaded to Facebook. This “fact check” contradicts several details Ars found in analysis of Facebook data downloads and testimony from users who provided the data. More on the Facebook response is appended to the end of the original article below.

This past week, a New Zealand man was looking through the data Facebook had collected from him in an archive he had pulled down from the social networking site. While scanning the information Facebook had stored about his contacts, Dylan McKay discovered something distressing: Facebook also had about two years’ worth of phone call metadata from his Android phone, including names, phone numbers, and the length of each call made or received.

This experience has been shared by a number of other Facebook users who spoke with Ars, as well as independently by us—my own Facebook data archive, I found, contained call-log data for a certain Android device I used in 2015 and 2016, along with SMS and MMS message metadata.

In response to an email inquiry by Ars about this data gathering, a Facebook spokesperson replied, “The most important part of apps and services that help you make connections is to make it easy to find the people you want to connect with. So, the first time you sign in on your phone to a messaging or social app, it’s a widely used practice to begin by uploading your phone contacts.”

The spokesperson pointed out that contact uploading is optional and installation of the application explicitly requests permission to access contacts. And users can delete contact data from their profiles using a tool accessible via Web browser.

Facebook uses phone-contact data as part of its friend recommendation algorithm. And in recent versions of the Messenger application for Android and Facebook Lite devices, a more explicit request is made to users for access to call logs and SMS logs on Android and Facebook Lite devices. But even if users didn’t give that permission to Messenger, they may have given it inadvertently for years through Facebook’s mobile apps—because of the way Android has handled permissions for accessing call logs in the past. (For Facebook’s instructions on turning off continuous contact uploading, go here.)

If you granted permission to read contacts during Facebook’s installation on Android a few versions ago—specifically before Android 4.1 (Jelly Bean)—that permission also granted Facebook access to call and message logs by default. The permission structure was changed in the Android API in version 16. From Android 4.1 on, a single request from those applications would trigger two separate permission requests. But until the “Marshmallow” version of Android, even with split permissions, all permissions could still be presented all at once, without users getting the option to decline them individually. So Facebook and other applications could continue to gain access to call and SMS data with a single request by specifying an earlier Android SDK version.

Starting with Marshmallow, users could toggle these permissions separately themselves. But as many as half of Android users worldwide remain on older versions of the operating system because of carrier restrictions on updates or other issues.

Apple iOS has never allowed access to call log data by third-party apps, overt or silently, so this sort of data acquisition was never possible.

Read the rest here: https://arstechnica.com/information-technology/2018/03/facebook-scraped-call-text-message-data-for-years-from-android-phones/

There is a related article on Page 10 of this newsletter.
First, Welcome to our new members on behalf of the Chapter! Our membership has edged up slightly over the last three months and we’re now at ~504 members as of the end of March. We just completed another successful March Cyber Focus Day at Pikes Peak Community College. It was a new venue for this activity and seemed to work well. The food trucks were a great idea for lunch (thanks, Ernie)—I received numerous positive comments about the food. We have lots of upcoming activities scheduled between meetings, training and mini-seminars. Please watch the Newsletter, communications and eVites to ensure you stay aware of what’s going on in the chapter. Please continue to refer new members to the chapter. Referrals are a critical part of developing new members for ISSA. As always, if you have any membership questions don’t hesitate to contact me.

Also, I would like to welcome our new members on behalf of the Chapter! When you’re participating in Chapter activities, please take a moment to introduce yourself to members of the board, me, and other members. Don’t forget to identify yourself as a new member and feel free to ask for help or information. Thanks for joining the Chapter and don’t forget to look for opportunities to lend your expertise to improve the Chapter. We’re always open to new ideas and suggestions.

<table>
<thead>
<tr>
<th>New Members</th>
<th>March</th>
</tr>
</thead>
<tbody>
<tr>
<td>Donnie G. Bryant</td>
<td></td>
</tr>
<tr>
<td>Tim Fyock</td>
<td></td>
</tr>
<tr>
<td>Anthony Joseph</td>
<td></td>
</tr>
<tr>
<td>Kenny Mann</td>
<td></td>
</tr>
<tr>
<td>Mark M. Alder</td>
<td></td>
</tr>
<tr>
<td>Franklin D. Aguilar</td>
<td></td>
</tr>
<tr>
<td>Arthur Wakefield</td>
<td></td>
</tr>
<tr>
<td>Leonard J. Rickard</td>
<td></td>
</tr>
<tr>
<td>Greg Green</td>
<td></td>
</tr>
<tr>
<td>Nicholas O. Goddard</td>
<td></td>
</tr>
<tr>
<td>Blake Hanson</td>
<td></td>
</tr>
<tr>
<td>Jami Everett</td>
<td></td>
</tr>
<tr>
<td>Christopher Wall</td>
<td></td>
</tr>
</tbody>
</table>

Thanks,

David Reed
Membership Committee Chairman
dreed54321@comcast.net

Update Your Profile!

Don’t forget to periodically logon to www.issa.org and update your personal information.
ISSA-COS Security+ Preparation Seminar - April 7 & 14

Studying for Security+?
Need CPEs?
Need a refresher?

It is that time of year where experts from the Security Field will be presenting at our annual Security + Exam preparation seminar! Details below:

The Colorado Springs Chapter of ISSA is hosting a two-day Security+ Exam Preparation Seminar

Location: Colorado Technical University (CTU), Room 113
4435 N. Chestnut St., Colorado Springs, CO 80907

Date: Saturday, 7 April 2018, and Saturday, 14 April 2018
Time: Both days: Check in between 8:00 AM – 8:25 AM
Class starts at 8:30 AM and runs to approximately 4:30/5:00 PM (*1 hour lunch)
*If extra instruction time is needed, lunch may be less than an hour and/or end time could run past 4:30 PM, no later than 5:00 PM.

Cost: $40.00 (includes both days and refreshments)

Those who have been studying and are close to sitting for the exam will gain the most out of this exam review seminar.

Already Security+ certified? Attending this review seminar will earn you 12 Continuing Education Units (CEU). First priority seats will be to paying students not yet Security+ certified.

SY0-401 Domains Covered Include:

- Network Security
- Compliance and Operational Security
- Threats and Vulnerabilities
- Application, Data, and Host Security
- Access Control and Identity Management Cryptography


Upcoming Events

Chapter Membership Meetings:
- 17 April: Dinner Meeting at the DAV, 6880 Palmer Park Blvd, Colorado Springs, 5:30pm to 7:30pm
- 18 April: Lunch Meeting at the DAV, 6880 Palmer Park Blvd, Colorado Springs, 11:00am to 1:00pm

Watch for additional details on our website and/or via email.

Mini-Seminar: 28 April at College America
Watch for additional details on our website and/or via email.
Mentorship Committee Update

*Group meeting for mentors and mentees will be Wednesday, April 25. Please send an email to Melissa Absher at mentorship@issa-cos.org if you are interested in attending!*

**Mission Statement**

Provide curious mentees at any stage of their information security career lifecycle with access to mentors who share their knowledge and experience in ensuring the confidentiality, integrity, and availability of information resources throughout a variety of industries.

**Overview**

The ISSA-COS Mentorship Program is designed to be mentee driven. Mentees determine the number of mentors they meet with depending on their questions, needs, and availability. The goal is to provide mentees with quality mentoring opportunities in a professional and problem solving environment. There will be group meetings twice a year (April & October) for all mentors and mentees to meet, greet, and discuss information security. Individual meetings between mentees and mentors will be scheduled throughout the year determined by the mentee and mentor. Mentees and mentors are expected to prepare for individual meetings by writing down questions and discussion topics prior to the meeting. e-Mentoring is also an option for those who need remote options. Mentors will meet as a group twice a year (January & June) to collaborate and share resources. Small group meetings to discuss specific topics and field trips to companies and organizations will be scheduled ad hoc.

**Why Mentor?**

Give back to the security community by sharing your knowledge and experience, provide career insight to mentees, grow your network.

**Why be a Mentee?**

Gain access to knowledge and experience in different security areas and industries.

**Enrollment Process**

- Be an ISSA Member
- Complete the Mentorship Enrollment Form
- Submit form with your resume to mentorship@issa-cos.org
ISSA Fellow Program

2018 Fellows Cycle Closing Soon

The Colorado Springs ISSA Chapter has over 500 current members. Many of you have been members for several years and may qualify for the ISSA fellow program. The Fellow Program recognizes sustained membership and contributions to the profession. If you think you or another ISSA associate may qualify in the fellow program, please contact Erik Huffman at erik.huffman@independence.edu to coordinate the process. Erik is the chair of the chapter awards committee and will help you through the steps. Below are some additional details on the ISSA Fellow Program. Qualification information is also presented below:

No more than 1% of members may hold Distinguished Fellow status at any given time. Fellow status will be limited to a maximum of 2% of the membership.

Nominations and applications are accepted on an annual cycle. Applications will be accepted until June 17, 2018 at 5:00pm Eastern Time. Following the application period, there will be a ten week review period followed by the notification and presentation process. Fellows and Distinguished Fellows will be recognized at the 2018 ISSA International Conference.

Familiarize yourself with the Fellow Program, and the submission guidelines. If you have questions, contact Erik or The ISSA Fellow Manager or call 866 349 5818 (US toll free) extension 4082.

To Become a Senior Member

Any member can achieve Senior Member status. This is the first step in the Fellow Program. What are the criteria?

Senior Member Qualifications

- 5 years of ISSA membership
- 10 years relevant professional experience

All Senior Member applications require an endorsement from their home chapter to qualify.

Click here to access the Senior Member application.
Click here for the Senior Member endorsement form.

To Become a Fellow or Distinguished Fellow

Have you led an information security team or project for five or more years? Do you have at least eight years of ISSA membership and served for three years in a leadership role (as a chapter officer or Board member or in an International role)? You may be eligible to become an ISSA Fellow or Distinguished Fellow. Please contact Erik and become familiar with the Fellow Program Guidelines and use the current forms to ensure you comply with all requirements.

Fellow Qualifications

- 8 years of association membership.
- 3 years of volunteer leadership in the association.
- 5 years of significant performance in the profession such as substantial job responsibilities in leading a team or project, performing research with some measure of success or faculty developing and teaching courses.

(Continued on page 7)
NIST Publications

By Staff, NIST, March 19, 2018

Based on interviews with nearly 1,500 cybersecurity professionals over three years, Haystax Technology released a study that makes it clear that organizations are feeling the pressure from insider threats and are ramping up detection, prevention and remediation.

NIST is releasing Special Publication 500-325, Fog Computing Conceptual Model, which presents the conceptual models of fog and mist computing and how they relate to cloud-based computing models for the Internet of Things (IoT). Until recently, much of the data from IoT devices has been managed and stored through cloud computing, a centralized network of computers and servers connected together over the Internet. But access to data through the cloud can be slow at times, because the data needs to be transported to the cloud for processing, analysis and storage. An alternative to cloud computing is fog computing, a decentralized infrastructure in which data is accessed locally, which significantly reduces the amount of time it takes to access the data. The publication presents the conceptual model of fog computing and an alternative model called mist computing and how they relate to cloud-based computing models for IoT. The document also characterizes important properties and aspects of fog computing, including service models and deployment strategies, and provides a baseline of what fog computing is and how it may be used.

Publication details: https://csrc.nist.gov/publications/detail/sp/500-325/final

NIST Computer Security Division announces the release of the second errata update for Special Publication 800-171 Revision 1, Protecting Controlled Unclassified Information is Nonfederal Systems and Organizations.

Learn about the updates to SP 800-171 Revision 1 from the CSRC website: https://csrc.nist.gov/News/2018/NIST-Releases-Second-Errata-Update-for-SP-800-171


All Fellow applications require a nomination to qualify.

Click here to access the Fellow application.
Click here to nominate a Fellow.
Click here to submit a Fellow letter of recommendation.

Distinguished Fellow Qualifications

• 12 years association membership.
• 5 years of sustained volunteer leadership in the association.
• 10 years of documented exceptional service to the security community and a significant contribution to security posture or capability.

All Distinguished Fellow applications require a nomination to qualify.

Click here to access the Distinguished Fellow application.
Click here to nominate a Distinguished Fellow.
Click here to submit a Distinguished Fellow letter of recommendation.

Please help us identify candidates that we can recognize in our chapter! Please contact:

Erik Huffman
Awards & Recognition Committee Chair
erik.huffman@independence.edu
Who wanted a future in which AI can copy your voice and say things you never uttered? Who?!

By Katyanna Quach, The Register, February 22, 2018

Artificially intelligent software can listen to someone's voice only a few times, and then speak just like them, like some kind of creepy cybernetic myna bird... according to a paper published by researchers from Baidu.

This technology, when perfected, will be ideal for generating fake audio clips of people saying things they never actually said. In the words of Red Dwarf's Kryten: file that under 'B' for blackmail.

Chinese internet giant Baidu's AI team is well known for its work on developing realistic sounding speech from text scripts. Now, its latest research project, revealed this week, shows how a generative model can learn the characteristics of a person’s voice and recreate that sound to make the person say something else entirely.

In the first example here, the original clip a woman’s voice is heard saying: “the regional newspapers have outperformed national titles.” After her voice is cloned, she now appears to be saying: “the large items have to be put into containers for disposal”.

So, as you can hear, the results aren’t perfect. The best clips generated from the model are still pretty noisy and lower quality than the original speech. But the “neural cloning system” developed by the researchers manages to retain the British accent and sounds quite similar.

The researchers introduce two different approaches to building a neural cloning system: speaker adaptation and speaker encoding.

Speaker adaptation involves training a model on various speakers with different voices. The team used the LibriSpeech dataset, containing 2,484 speakers, to do this. The system learns to extract features from a person’s speech in order to mimic the subtle details of their pronunciation and rhythm.

Speaker encoding involves training a model to learn the particular voice embeddings from a speaker, and reproduces audio samples with a separate system that has been trained on many speakers.

After training on LibriSpeech, up to ten audio samples of any speaker are taken from another dataset. VCTK contains clips from 109 native English speakers with different accents. Basically, after being trained on voices from the LibriSpeech dataset, it has to copy new vocals from speakers in the VCTK dataset.

Sercan Arik, co-author of the paper and a research scientist at Baidu Research, explained to The Register that the speaker encoding method is much easier to implement in real life for speakers such as digital assistants compared to the speaker adaptation technique.

“A speaker adaptation approach requires users to read a specific utterance from a given text, whereas speaker encoding works with random utterances. This means speaker adaptation may not be as easily deployed on user devices, as it has more challenges to scale up to many users. Instead, speaker encoding is much easier for deployment purposes - it can even be deployed on a smartphone - as it is fast and has low memory requirements.”

Read the rest here:
http://www.theregister.co.uk/2018/02/22/ai_human_voice_cloning/
Why You Should Never Pay A Ransomware Ransom
By Lee Mathews, Forbes, March 9, 2018

A ransomware infection can be a very, very scary situation to deal with. Many victims aren’t sure what to do next when ransomware hits. There’s one thing that you should never do, and that pays the ransom.

That’s a point that cybersecurity experts have been trying to drive home ever since ransomware first started infecting computers. When faced with the frightening reality that treasured family photos or essential business documents have been encrypted, however, not everyone follows that advice.

Those who don't aren't always pleased with the results. In fact, a recent report from the CyberEdge Group revealed that only 19% of ransomware victims who pay the ransom actually get their files back. It's a risky roll of the dice, to be sure... and just as many people CyberEdge surveyed said they paid and still lost their data.

There are a couple reasons why data gets lost. Sometimes it's because the malware creator's only real goal was to scare people into paying. The criminal never intended to let his or her victims decrypt any files that were encrypted. Other times it's not intentional. In those cases, poorly-coded malware just makes it impossible to undo the encryption process.

There is some good news in the CyberEdge report, however. The numbers show that the majority of victims -- nearly two-thirds -- are refusing to pay. Of those victims, about 86% were able to recover files on their own thanks to regular backups.

It's a significant shift in the public response to ransomware infections. It also helps to explain why cybercriminals are increasingly looking to other ways to profit from malware distribution.

One approach that's taken off in recent months is cryptomining. Cryptomining malware doesn't make a bold, in-your-face grab for your cash the way ransomware does. Instead, it forces infected computers to work overtime producing cryptocurrencies like Bitcoin and Monero. Cryptomining malware won't destroy a victim's files, but it can physically damage a system in some circumstances.

Philips tests LiFi in a real office
By Swapna Krishna, Engadget, March 19, 2018

This week, Philips announced that its LiFi, or Light Fidelity, tech is currently being tested at the offices of Icade, a French real estate investment company. LiFi provides broadband internet through lights, using LEDs to transmit a high-speed connection of up to 30 Mb per second through light waves.

LiFi works through LED luminaires that are equipped with built-in modems. For now, users will need to plug a USB dongle into their computers to access LiFi, but the tech will eventually be built into other devices. The dongle uses an infrared link to access LiFi, which is purported to be more secure and more reliable than WiFi.

There are many real benefits to LiFi. First, it works in areas where WiFi radio frequencies might interfere with equipment, such as hospitals, and where these signals can't penetrate. Because LiFi is transmitted via lights, it can reach areas that are deep underground. Seamless hand-off technology ensures that the signal will remain constant as you move from one light to another. It's also easy to control the range of LiFi; because light can't penetrate walls, creating a short-range, secure signal is easier than with WiFi.

Read the rest here:
This Is So Much Bigger Than Facebook

Data misuse is a feature, not a bug—and it’s plaguing our entire culture.

By Ethan Zuckerman, The Atlantic, March 23, 2018

After five days of silence, Mark Zuckerberg finally acknowledged the massive data compromise that allowed Cambridge Analytica to obtain extensive psychographic information about 50 million Facebook users. His statement, which acknowledged that Facebook had made mistakes in responding to the situation, wasn’t much of an apology—Zuckerberg and Facebook have repeatedly demonstrated they seem to have a hard time saying they’re sorry.

For me, Zuckerberg’s statement fell short in a very specific way: He’s treating the Cambridge Analytica breach as a bad-actor problem when it’s actually a known bug.

In the 17-months-long conversation Americans have been having about social media’s effects on democracy, two distinct sets of problems have emerged. The ones getting the most attention are bad-actor problems—where someone breaks the rules and manipulates a social-media system for their own nefarious ends. Macedonian teenagers create sensational and false content to profit from online ad sales. Disinformation experts plan rallies and counterrallies, calling Americans into the streets to scream at each other. Botnets amplify posts and hashtags, building the appearance of momentum behind online campaigns like #releasethememo. Such problems are the charismatic megafauna of social-media dysfunction. They’re fascinating to watch and fun to study—who wouldn’t be intrigued by the team of Russians in St. Petersburg who pretended to be Black Lives Matter activists and anti-Clinton fanatics in order to add chaos to the presidential election in the United States? Charismatic megafauna may be the things that attract all the attention—when really there are smaller organisms, some invisible to the naked eye, that can dramatically shift the health of an entire ecosystem.

Known bugs are the set of problems with social media that aren’t the result of Russian agents, enterprising Macedonians, or even Steve Bannon, but seem to simply come with the territory of building a social network. People are mean online, and bullying, harassment, and mob behavior make online spaces unusable for many people. People tend to get stuck in cocoons of unchallenging, ideologically compatible information online, whether these are “filter bubbles” created by algorithms, or simply echo chambers built through homophily and people’s friendships with “birds of a feather.” Conspiracy theories thrive online, and searching for information can quickly lead to extreme and disturbing content.

The Cambridge Analytica breach is a known bug in two senses. Aleksandr Kogan, the Cambridge University researcher who built a quiz to collect data on tens of millions of people, didn’t break into Facebook’s servers and steal data. He used the Facebook Graph API, which until April 2015 allowed people to build apps that harvested data both from people who chose to use the app, and from their Facebook friends. As the media scholar Jonathan Albright put it, “The ability to obtain unusually rich info about users’ friends—is due to the design and functionality of Facebook’s Graph API. Importantly, the vast majority of problems that have arisen as a result of this integration were meant to be ‘features, not bugs.’”

In his non-apology, Zuckerberg claimed Facebook had already taken the most “important steps a few years ago in 2014 to prevent bad actors from accessing people’s information.” But changing the API Kogan used to collect this data is only a small part of a much bigger story.

To be clear, I believe Kogan acted unethically in allegedly collecting this data in the first place, and that giving this data to Cambridge Analytica was an unforgivable breach of research ethics. But Kogan was able to do this because Facebook made it possible, not just for him, but for anyone building apps using the Graph API. When Kogan claims he’s being made a scapegoat by both Cambridge Analytica and Facebook, he has a strong case: Selling data to Cambridge Analytica is wrong, sure, but Facebook knew that people like Kogan could access the data of millions of users. That’s precisely the functionality Facebook advertised to app developers.

Speaking with Laurie Segall on CNN this week, Zuckerberg emphasized that Facebook would investigate other app makers to see if anyone else was selling psychographic data they’ve collected through the Graph API. But Zuck didn’t mention that Facebook’s business model is based on collecting this demographic and psychographic information and selling the ability to target ads to people using this data about them.

Read the rest here:
In an effort to strengthen the talent pipeline for business services occupations and the cybersecurity industry, the CWDC is currently identifying career pathways for these industries. If you are unfamiliar with this work you can learn more about career pathways on the CWDC website.

We request your feedback via a 12-minute survey on the critical occupations and competencies in cybersecurity and business operations before April 13 by clicking on Cybersecurity Survey below.

Cybersecurity Survey

If you attended a Cybersecurity or Business Operations Regional Forum, thank you -- we have incorporated your input. We know you understand how important it is to give others in the industry an opportunity to impact this work.

The surveys will accept responses until close of business on Friday, April 13.

Thank you for your time and input in developing career pathways to critical occupations in Colorado.

In partnership,

Stephanie Veck
Director, CWDC

Thomas Hartman
Talent Development Coordinator, CWDC

These surveys are intended to collect industry feedback. If you are a public partner (education, workforce, community organization), please help us collect industry feedback by sharing these surveys with your industry partners.
Here Are The Clever Means Russia Used To Hack The Energy Industry

By James Conca, Forbes, March 28, 2018

Last July, officials from the Federal Bureau of Investigation and the Department of Homeland Security revealed that Russian hackers were behind cyber intrusions into the U.S. energy power grid. The intrusion illustrated the severe threat that hackers pose to our most critical industries - energy, finance, healthcare, manufacturing and transportation.

The DHS and FBI downplayed the danger in a joint statement: "There is no indication of a threat to public safety, as any potential impact appears to be limited to administrative and business networks."

But that might not be the end of it. Russia may be laying the groundwork for more damaging hacks, on America as well as other nations, using new cyber weapons like CrashOverride and BlackEnergy 3.

In 2015, Russia tested this on the Ukrainian capital of Kiev. These tools were specifically developed to disrupt electric power grids and it blacked out 225,000 people in the Ukraine.

One might wonder what is Russia's end game for this kind of attack. To hurt us financially? To show us how vulnerable we are? In preparation for a more sinister attack?

Is it to punish America for anti-Russian policies? The White House expelled 60 Russians from the United States this week, joining western allies in response to Russia’s poisoning of a former Russian spy in Britain with what was a banned chemical weapon.

When DHS and FBI dissected the hackers' tradecraft, it turned out to be very clever indeed. Mark Orlando, Chief Technology Officer for cyber services at Raytheon, broke down the particulars of why the new world of hacking works so well in America.

One of the attackers' main strategies is to divide targets into two groups - intended targets which are the energy companies themselves, and staging targets like vendors, suppliers, even trade journals and industry websites.

Instead of going straight to the larger and better-protected targets, like a $60 billion energy company with a cyber security department, the hackers worked their way into the smaller and less secure companies' networks like those that supply the big ones with smaller equipment. Or the local utilities that are partnered with them. Local regulators may also have good access.

There is even an Electric Utility Industry Sustainable Supply Chain Alliance that many of the large energy companies use.

When the hackers get into those systems, they use that access to gather intelligence and set traps for the larger company.

This targeting of the supply chain partners is brilliant. The manufacturer of natural gas turbines that supply a gas power plant would have great access to the plant's systems and management, would probably have password access, and would not be questioned very hard.

'It's important to raise awareness,' says Orlando. 'These details, if taken by themselves, might not seem that impactful. When presented with the entire story, we can see it was part of a larger, sustained campaign, potentially causing a lot of damage.'

This is a long-term strategy that takes patience – just the kind of thing traditional espionage has perfected over the last century.

America seems to be getting the message. A recent survey from Raytheon and Ponemon showed that two-thirds of cyber security executives and chief information security officers in America, Europe and the Middle East believe cyber extortion, such as ransomware and data breaches, will increase in frequency and payout.

The traps themselves are pretty imaginative. Many are based in social media. No one would suspect a cute kitten video of hiding malware. But they do. And if your co-worker is a kitten-nut, they may not hesitate to download that video without thinking that it is a trap.

'The weakness in cybersecurity are the users themselves, those that are not necessarily computer-savvy,' says Quinn Mockler, a young cyber security researcher at Columbia Basin College in the Tri-Cities Washington near the Hanford Nuclear Reservation. 'People overall need better awareness of cyber security. Otherwise, we will be open to constant attack.'

In one example discussed by Orlando, the attackers found a harmless-looking photo on one company's human resources site that contained valuable information - the manufacturer and model of a certain piece of control-systems equipment.

That provided critical information on how the plant runs and set up the next phase of the attack - spear phishing – which is the use of customized, highly deceptive emails designed to deliver malware. Using resumés, curricula vitae, policy documents and other common messages, the hackers made reference to these control systems creating plausible, well-informed emails likely to fool someone into opening a malware-laced attachment.

One was an invitation to a company New Year's Eve party.

Read the rest here: https://www.forbes.com/sites/jamesconca/2018/03/28/how-on-earth-did-russia-hack-our-energy-systems/#5bd4bab66104
Five things to know about Russian attacks on the energy grid

By Morgan Chalfant, The Hill, March 18, 2018

Trump administration officials on Thursday accused the Russian government of staging a multi-year cyberattack campaign against the energy grid and other elements of critical infrastructure in the United States.

The alert from the Department of Homeland Security and the FBI coincided with the administration’s decision to unveil new sanctions on Russia for 2016 election meddling and other cyber activities — developments that are sure to ramp up tensions between the U.S. and Moscow.

Here are five things to know about Russian cyberattacks against U.S. infrastructure.

1. A ‘multi-stage intrusion campaign’

Russian government hackers conducted a "multi-stage intrusion campaign" against U.S. energy infrastructure, according to the joint Homeland Security and FBI report.

The campaign, which dates back to at least March 2016, involved hackers targeting lower-level victims — networks belonging to small commercial facilities that had less security — in order to ultimately compromise their intended targets in the energy sector.

Officials said Russia targeted organizations across several sectors, including government, energy, nuclear, water, aviation and critical manufacturing. The victims were not named.

The hackers used spear-phishing emails — fraudulent messages that purport to come from a known sender and contain malicious links or documents. According to the alert, the hackers also in some cases leveraged their initial targets to develop "watering holes," an attack method in which hackers infect a trusted domain that the ultimate victim will visit.

The attacks were tailored to target those in the industry. The spear-phishing messages, for instance, included references to industrial control equipment or malicious attachments that appeared to be policy documents or invitations.

“They’re trying to target the engineers and people working on those control systems, not just the public in general,” observed Sergio Caltagirone, director of threat intelligence at Dragos, an industrial network security firm.

2. The Russians accessed information on Industrial Control Systems

Read the rest here: http://thehill.com/policy/cybersecurity/378869-five-things-to-know-about-russian-attacks-on-the-energy-grid

ISSA Nametags

Do you want an ISSA nametag for your very own to wear to meetings, conferences, and events? You can now order/pick up yours directly from:

Blue Ribbon Trophies & Awards

245 E Taylor St  (behind Johnny’s Navajo Hogan on North Nevada)

Colorado Springs

(719) 260-9911

Although their hours are officially Monday through Friday until 5:30 pm, they are occasionally in the shop on Saturdays. This is a small business so cash/check would be appreciated. Email wbusovsky@aol.com to order.
Want to know what the dark web looks like without even having to go there? A map released Tuesday by research and development outfit Hyperion Gray is bringing to life the often misunderstood and decried corner of the internet.

In what the company believes is an unprecedented effort to illuminate hidden services on the dark web, it allows anyone to zoom in and out of images containing the homepage of each website based on the Tor network. (Tor, run by the Tor Project, is designed to provide anonymity for its users and the hidden services within are considered to make up the largest section of the dark web.)

Be warned, though. The content within the Dark Web Map can be graphic. As Hyperion Gray's disclaimer notes: "These sites include mature and/or offensive content, including pornography, violence and racism."

The map shows 6,608 dark web sites crawled during January 2018. That includes all manner of webpages, from the amusing to the horrific. Amongst the myriad pages on the map, Forbes has already seen evidence of extreme sexual content, credit card cloning products, pictures of poop and penises, a large number of Bitcoin scams, Propublica's Tor website and a range of whistleblower pages based on the SecureDrop service. That includes Forbes' own SecureDrop service (feel free to drop us a tip securely anytime).

What's apparent from a cursory view of the map, zooming in and out of different areas, is that a significant proportion of mapped sites have been set up for illegal means, but there are also plenty of legal services such as whistleblower and personal pages. That's something Hyperion Gray CTO Alejandro Caceres (and co-founder with Amanda Towler) discovered too. "I like Tor's narrative that the technology preserves political freedom, privacy, freedom of speech," he said.

"But the data clearly indicates that this is at the very least a double-edged sword. While we didn't put out this research to take a side on the debate about hidden services, it's not something that can be ignored either - there's a lot of shitty stuff out there.

"I should add that I use Tor daily for many reasons, and hidden services shouldn't be taken as the core of what the Tor project is and does." Caceres also donates to the Tor Project.

From DARPA to dark web cartography

The map was partly based on an experiment carried out with the MEMEX project at Darpa, the research arm of the Pentagon. As Forbes has previously reported, the aim of MEMEX was to create simple search engines for the dark web and had proven useful for cops investigating human trafficking.

But the digital cartography was entirely self-funded, explained Mark Haase, computer scientist at Hyperion Gray and the man behind the map. Haas started with a list of 60,000 Tor addresses, also known as onions because of their .onion extensions. He wrote a script that downloaded the home page for each and took a screenshot. About 6,600 sites responded, whilst the other 53,000 either timed out or returned errors. Haase then manually redacted any screenshots that appeared to contain illegal content, going by U.S. laws.

Users will note the clusters of different sites. They're bunched together thanks to a "similarity algorithm" that assigns each page a score between 0.0 and 1.0. That similarity is based on the structure of the website's code. "The layout algorithm tries to put sites that are similar to each other close together on the map and tries to move dissimilar sites out of the way, which causes groups of similar pages to move towards each other and form into clusters," Haase explained to Forbes over encrypted chat. "Two sites can be 'similar' in terms of HTML structure but contain totally different content."

The map should provide a comprehensive view of the dark web, even if it doesn't give the entire picture. For instance, many .onion domains don't go to a webpage, but to file or chat servers. And some can be hidden, even from computer scientists who've contracted with the U.S. government. "It's representative, but definitely not exhaustive," added Haase. "If somebody really wants to hide an onion, it's very difficult for an outsider to find it."

Read the rest here:
https://www.forbes.com/sites/thomasbrewster/2018/03/13/dark-web-map-6000-webpages/#789ab2a918e7
8 questions to ask about your industrial control systems security

By Jaikumar Vijayan, CSO, March 19, 2018

A recent incident where a likely nation-state threat actor inadvertently shut down a critical infrastructure facility in the Middle East when testing new malware has stoked widespread concerns about the vulnerability of industrial control systems (ICSs) to new cyberthreats. Many security experts see the incident as a harbinger of a new wave of destructive attacks targeting ICS and want critical infrastructure owners to urgently update the security of their operational technology (OT) networks.

What is an ICS?

An ICS is any device, instrumentation, and associated software and networks used to operate or automate industrial processes. Industrial control systems are commonly used in manufacturing, but they are also vital to critical infrastructure such as energy, communications, and transportation. Many of these systems connect to sensors and other devices over the internet—the industrial Internet of things (IIoT), which increases the potential ICS attack surface.

ICS security

"It is important that organizations leverage lessons learned securing enterprise IT but adapt those lessons to the unique characteristics of OT," says Eddie Habibi, CEO and founder of ICS security vendor PAS Global. "This includes moving beyond perimeter-based security in a facility and adding security controls to the assets that matter most – the proprietary control systems, which have primary responsibility for process safety and reliability," he says.

The following are some of the key questions that plant operators, process control engineers, manufacturing IT specialists, and security personnel need to be asking when planning for ICS security, according to several experts.

1. Do I have the people to manage and sustain ICS security?

Organizational planners often tend to think of industrial cybersecurity as largely a technology issue when often the much bigger problem is a lack of skilled resources, says Sid Snitkin, an analyst with the ARC Advisory Group. In recent years operators of critical infrastructure have increasingly deployed recommended technology controls for protecting their systems, but not enough people to man them.

"Many organizations just don't have the people in place to sustain the technology they have put in," Snitkin says. "They put in anti-malware, but don't have people to put in the updates. They can identify vulnerabilities but don't have people to fix them."

Often, the ones who manage cybersecurity are the same automaton engineers and production engineers who put in the systems in the first place.

"Security is a side job for them," Snitkin says. They don't have the time and are typically more focused on keeping systems running than taking them down to address security issues. A lot of plant managers are operating under a false sense of security by thinking they have addressed their security issues by implementing a few technology controls, Snitkin says.

2. Do I know what I have installed in the field?

To properly protect you first need to figure out what you have installed in the field and which systems they connected to. If you don't have that visibility, you are dead in the water, Joe Weiss, managing director of Applied Control Solutions, says. You need to understand where you have technology controls in place already, and where technology can be used to protect. For systems that don't support modern security controls you need to be thinking about compensating controls for mitigating risk, Weiss says.

"We've seen hackers bypass firewalls, jump air gaps, and leverage ICS device vulnerabilities because of the lack of basic security protections," says Bill Diotte, CEO of industrial security vendor Mocana. It is vital for plant managers, operators and manufacturers need to make sure that the ICS devices themselves are trustworthy and support essential cybersecurity, Diotte says.

"Often PLCs [programmable logic controllers], sensors and industrial gateways do not have a secure credential [such as a] digital certificate or private key hidden in silicon as a basis of trust," he says. Basic cyber protections like secure boot, authentication, encryption, and trust chaining are not implemented on devices that impact personnel safety, uptime and the environment, he says.

Read the rest here:

A US government commission has asked the public for its thoughts on possible changes to the military's selective service rules to allow the conscription of technical talent, including those with computer-oriented skills, regardless of sex or age.

The National Commission on Military, National, and Public Service, in accordance with the Congress in the 2017 National Defense Authorization Act, has been directed to consider how to encourage more people to participate in military, national and public service, in order to assure national security.

At the behest of Congress, the commission has been directed to solicit public input on possible rule changes. The commission did so in February through a notice published to the Federal Register, the official record of US government actions.

Among the various aspects of the US Selective Service System being re-evaluated is whether it might make sense to change the process to ensure that individuals with technical skills needed for national defense – medical, language, cyber, and science, technology, engineering and mathematics (STEM) skills – are to be required to register for a possible draft "without regard to age or sex."

The US Selective Service presently requires men, ages 18 through 25, to register. Bills have been introduced in Congress to require women to register but have not become law.

Any Selective Service changes won't happen soon – the commission isn't required to submit its recommendations to the President and Congress until March 2020. But the commission wants to hear from the public by April 19, 2018, via email, web submission form (3,000 characters at most), or postal mail.

Government agencies and the military have had a difficult time attracting individuals with computer skills. In 2014, former FBI director James Comey, for example, suggested the FBI would have to loosen its drug rules to hire pot-smoking hackers, before insisting he was only joking in the wake of criticism.

In any event, the tech talent shortage is said to be serious. The US Department of Homeland Security, for example, supports the US Cyber Challenge, a program to "to significantly reduce the shortage in today’s cyber workforce," by replacing them with semi-smart computer software.

"There is a radical shortage of people with the technical skills that are needed in time of conflict," Alan Paller, director of research for The SANS Institute, told The Register.

But Paller suggests just changing the rules to cover a broader set of people with cyber skills won't achieve the desired results.

There's a very small set of people with the right skills and just calling them up from the private sector then could leave businesses vulnerable, he suggested.

Paller, however, expressed optimism that the cyber talent shortage can be addressed in a few years through the development of programs to identify those with aptitude for cybersecurity.

"The problem has never been the development of the people," he said. "It has been finding the 10 or 15 per cent of people who are naturals at it."

Paller pointed to programs like Cyber Discovery in the UK and Girls Go Cyber Start in the US, initiative to encourage the exploration of cyber security as a career possibility. The latter program, he said, nearly doubled the number of high school girls considering cyber security careers from 36 per cent before to 70 per cent afterwards.

Read the rest here:
http://www.theregister.co.uk/2018/03/21/uncle_sam_mulls_drafting_grayhaired_hackers_during_times_of_crisis/
Girl Scouts fight cybercrime with new cybersecurity badge

By Chiara Sottile and Jo Ling Kent, NBC News, March 4, 2018

If you think being a Girl Scout is all camping, crafting, and cooking, think again.

For the first time, millions of Girl Scouts nationwide are taking on hacking and cybercrime as they work towards earning newly introduced cybersecurity badges. Girl Scouts of the USA teamed up with security company Palo Alto Networks to devise a curriculum that educates young girls about the basics of computer networks, cyber attacks, and online safety.

Sylvia Acevedo, CEO of GSUSA, said they created the program based on demand from the girls themselves.

"Protecting their identity online, how to protect themselves when they're browsing, how to protect their computers, their family networks from being hacked, those are things that are of real interest to girls," Acevedo said in an interview with NBC News.

In Alameda, California, Girl Scouts of Troop 32749 are already hard at work learning about the basics of coding and computer networks.

"Evelyn, you're going to be my message sender," said troop leader Danielle Zorn, holding an unruly ball of green yarn. One by one, Zorn cut sections of string and distributed them to the nine and ten-year olds. As instructed, Girl Scout Evelyn began stringing cards with letters written on them onto the green string that connected the dozen girls in a spiderweb of yarn.

"I am sending a card to my friend Kylie," said Sophia, unleashing her card and message along her section of the yarn network. "She'll have some words to put together," Sophia explained.

While junior scouts learn these and other basics, like the fundamentals of binary code, a total of 18 cybersecurity badges will eventually be rolled out nationwide at various skill levels for girls in grades K-12.

Girl Scouts of the USA have been increasing programming in the STEM fields of science, technology, engineering, and math in recent years, but this represents another step further. And while the program is designed to be fun, the hope is that it will also inspire more girls to pursue careers in STEM.

Women are vastly underrepresented in cybersecurity, holding only 11 percent of jobs globally, according to the 2017 Global Information Security Workforce Study: Women in Cybersecurity.

"Cybersecurity is vital to protect our financial systems, our voting systems, you know, our defense systems. So we absolutely need to have the rising generation interested and prepared in cyber security," said Acevedo.

Acevedo believes that by introducing these skills to girls as young as five, they could grow up to reverse the ugly trends of underrepresented women in tech and the rampant bro-culture of tech hubs like Silicon Valley.

"It's going to just make them feel empowered that I can go and do anything," said Rinki Sethi, the Senior Director of Information Security at Palo Alto Networks, and one of the advisers for the cybersecurity badge's curriculum. "Cybersecurity's... got the toughest challenges that we need to go and solve. And we're going to need the best and the greatest minds and a really thought-diverse group to go and fill those gaps that we have today in the talent pool," said Sethi.

In Alameda, the girls in Troop 32749 are up for the challenge.

Read the rest here:
Photos are from our 5th Annual Cyber Focus Day. Just one of the benefits of ISSA membership.

ISSA Photos are courtesy of our Chapter Photographer Warren Pearce.
Additional photographs are available on the ISSA-COS.ORG website.
The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

Chapter Officers:
President: Colleen Murphy
Executive Vice President: Scott Frisch
Vice President: Ernest Campos
Vice President of Membership: David Reed
  • Deputy VP Membership: Melissa Absher
Vice President of Training: Mark Heinrich
  • Deputy VP Training: Susan Ross
Treasurer: Mark Maluschka
  • Deputy Treasurer: Vacant
Communications Officer: Anna Johnston
  • Dep. Communications Officer: Vacant
Recorder/Historian: Erik Huffman
  • Deputy Recorder/Historian: Vacant
Member at Large: James Asimah
Member at Large: Dawn Wellein
Member at Large: Bill Blake
Member at Large: Jim Blake
Dir. of Certification: Derek Isaacs
  • Dep Dir Certifications: Kurt Danis
Dir. of Professional Outreach: Vacant
  • Dep Dir. of Professional Outreach: June Shores

Committee Chairs:
Ethics: Tim Westland
IT Committee: Bill Welker
Mentorship: Melissa Absher
Recognition: Erik Huffman
Sponsorship: Ernest Campos
Transformation: Ernest Campos
Newsletter: Don Creamer

Article for the Newsletter?
If you would like to submit an article...

Do you have something that the Colorado Springs ISSA community should know about? Tell us about it!

We are always looking for articles that may be of interest to the broader Colorado Springs cyber community.

Send your article ideas to Don Creamer at:
doncreamertoutlook.com

Ensure that “Newsletter” is in the subject line.

Looking forward to seeing you in print!

Past Senior Leadership
President Emeritus: Dr. George J. Proeller
President Emeritus: Mark Spencer
Past President: Frank Gearhart
Past President: Cindy Thornburg
Past President: Pat Laverty

What the @#$%&!? Microsoft bans nudity, swearing in Skype, emails, Office 365 docs

By Simon Sharwood, The Register, March 28, 2018

Microsoft has advised customers that offensive language on Skype, in an Outlook.com email, or in an Office 365 Word document is a potentially account-closing offense under its updated terms of use.

The tweaked services agreement, which comes into effect on May 1, 2018, now includes the following code-of-conduct item:

Read the rest here:
https://www.theregister.co.uk/2018/03/28/microsoft_services_agreement_bars_offensive_language/